

Citrixxperience.com

**1Y0-A05 Implementing Citrix XenApp
5.0 for Windows Server 2008**

Study Guide

Version 1.2

(February 12, 2009)

Implementing Citrix® XenApp 5.0 with Windows Server 2008 Study Guide

This study guide was created by Citrixexperience.com. The following materials were used to create this study guide. All are copyrighted by Citrix® Systems: CXA-201-1I Implementing Citrix® XenApp 5.0 for Windows Server 2008, CTX-1259AI Citrix® XenApp: Administration, CTX-1251AI Citrix® MetaFrame Presentation Server 3.0: Management and Maintenance for the Enterprise, 1Y0-A05 Exam Enablement Guide, Citrix® Knowledge Center articles, Citrix® eDocs, Citrix® XenApp 5.0 for Windows Server 2008 Administrator's Guide, Getting Started with Citrix® XenApp 5.0, Citrix® XenApp 5.0 Installation Guide, Citrix® Access Suite 4.0 - Disaster Recovery Planning and Configuration, Load Manager Administrator's Guide, Licensing: Generating Usage Reports Using the License Management Console, Licensing Architecture: An Overview, Licensing: Firewalls and Security Considerations, Web Interface 5.0.1 Administrator's Guide, and XenApp Plugin for Hosted Apps 11.x for Windows Administrator's Guide.

Along with the materials listed above, this study guide is meant to be used in preparation for the 1Y0-A05 Implementing Citrix XenApp 5.0 for Windows Server 2008 exam. Also suggested for preparation are other books that relate to the subjects and above all, personal experience with the products. Citrixexperience.com recommends further preparation by using other 1Y0-A05 products found at www.Citrixexperience.com.

The license for this study guide is for one user only. It is a copyright of Citrixexperience.com and may not be reprinted, copied, reproduced, distributed, republished, downloaded, displayed, posted or transmitted in any form or by any means, including but not limited to electronic, mechanical, photocopying, recording, or other means, in full or in part, without the prior express written permission of Citrixexperience.com.

Citrix, the Citrix logo, Citrix ICA, Citrix MetaFrame, Citrix MetaFrame XP, Citrix Nfuse, Citrix Extranet, Citrix Program Neighborhood, Citrix WinFrame, and other Citrix product names referenced herein are registered trademarks or trademarks of Citrix Systems, Inc. in the United States and other jurisdictions. All other product names, company names, marks, logos, and symbols are trademarks of their respective owners.

Citrix® Systems, Inc. is not affiliated with Citrixexperience.com in any way.

Table of Contents

<u>Subject</u>	<u>Page</u>
Understanding the Citrix Architecture	1
Licensing and Installing XenApp	6
Installing and Configuring Web Interface	11
Configuring ICA Sessions	20
Managing Applications	30
Managing XenApp Policies	37
Managing and Maintaining the Server Farm	41
Configuring Printing	53
Troubleshooting XenApp	60

Understanding the Citrix Architecture

XenApp Features and Components

Citrix XenApp 5.0 is an end-to-end application delivery solution that delivers Windows applications to users.

The *XenApp Document Library* contains the technical documentation shipped with XenApp and is a core resource for additional information for:

- ❖ Installation
- ❖ Configuration
- ❖ Management

Load Manager ensures that each user connects to the server with the lightest load and can best handle the connection.

- ❖ Load Manager uses load evaluators with rules to determine resource load.

Resource Manager is based on *Citrix EdgeSight* functionality to provide administrators with the ability to monitor, report and collect server resource metrics for all servers in the farm.

Network Manager provides the administrator the ability to manage XenApp using SNMP and provides seamless integration with network management consoles such as:

- ❖ HP OpenView
- ❖ Tivoli NetView
- ❖ CA UniCenter

The *Web Interface* provides users with access to resources published in one or more server farms through either:

- ❖ A web browser
- ❖ The Citrix XenApp plugin

The *Secure Gateway* provides secure remote access to published applications and resources on XenApp servers through SSL/TLS encrypted sessions.

- ❖ XenApp uses the Secure Gateway in combination with the Web Interface to secure communications.

The *Citrix XenApp Provider* provides XenApp health information systems such as Microsoft Systems Center Operations Manager.

- ❖ MOM 2005 is supported.

The *Access Management Console* allows administrators to configure administrator permissions, server and server farm properties.

- ❖ Administrators publish applications in the Access Management Console.

The *License Management Console* is a browser-based utility that allows administrators to manage licenses, track license usage, create license reports and configure licensing alerts.

The *XenApp Advanced Configuration tool* is a utility that allows an administrator to manage zones, implement policies and manage certain aspects of Load Manager.

- ❖ The XenApp Advanced Configuration tool was known as the Presentation Server Console previous to XenApp 5.0.

XenApp provides a variety of *plugins* (formerly called clients) that make it possible for users to access published resources regardless of the operating system installed on the client device.

- ❖ Examples of XenApp plugins include:
 - ◆ XenApp Plugin for Streamed Apps
 - ◆ Java plugin (formerly called Client for Java)
 - The Java plugin deploys *automatically* when a user connects from a *Macintosh* computer with the *Safari* web browser.
 - ◆ XenApp Web plugin (formerly called Client for Web)
 - ◆ XenApp plugin (formerly called Program Neighborhood Agent)
 - ◆ Program Neighborhood

A *server farm* is a group of XenApp servers made up of one or more zones, all using the same data store, sharing information among them for load balancing purposes.

A logical group of XenApp servers communicating with a single data collector is called a *zone*.

- ❖ Zones are typically based on subnets and highly-available subnets.

A *data collector* contains dynamic information about XenApp servers in a zone such as:

- ❖ Session load

- ❖ Session status

- ❖ User information

The *data collector election* process involves a server in the zone taking over the role of data collector when the original data collector becomes unavailable.

Zone preference and failover allows user connections in a particular zone to failover to another zone in the event that the primary zone is not available.

Every farm has one *data store* that holds all of the static information for all of the XenApp servers in the farm.

- ❖ The data store can be created on one of the following databases:

- ◆ Microsoft Access
- ◆ SQL Server Express

- ❖ or enterprise-level databases:

- ◆ Microsoft SQL Server
- ◆ Oracle
- ◆ IBM DB2

A subset of the data in the data store that is on every XenApp server in the farm is called the *local host cache*.

The *Independent Management Architecture (IMA)* provides the framework for all server-to-server communication in the server farm.

Microsoft Terminal Services is a presentation virtualization platform for Windows Server.

- ❖ Terminal Services functionality is extended by Citrix XenApp by adding dimensions of security, flexibility, manageability, security and performance.

Services, Protocols, Port Numbers

The IMA Service:

- ❖ Provides a centralized framework used by administrative tools for XenApp.
- ❖ Delivers subsystems that collectively provide functionality to current and future Citrix products.

- ❖ Runs on all servers with XenApp installed.
 - ◆ Enabled by default during installation.
- ❖ Communicates through port 2512 for server-to-server communication.
- ❖ Uses port 2513 for communication between the XenApp Advanced Configuration tool and XenApp servers.

During XenApp installation, you can choose to have the Citrix XML Service share the same port as IIS.

- ❖ The default IIS port is 80.

The Access Management Console uses port 135.

Citrix SSL Relay uses port 443.

ICA sessions use port 1494.

Client-to-server UDP sessions use port 1604.

Session reliability uses port 2598.

Secure Computing SafeWord authentication uses port 5031.

Farm and Zone Configurations

In general, a single server farm meets the needs of most environments.

- ❖ Sometimes business reasons dictate the need for multiple server farms.
- ❖ Use *separate* server farms for *test* and *development* environments.
 - ◆ Because data collectors communicate with one another, zones within a server farm have an impact on one another.

Citrix does not recommend creating a zone for each subnet in your environment.

- ❖ Unless your farm is dispersed across a WAN, Citrix recommends having only one zone in your environment.
 - ◆ For performance reasons on WANs, Citrix recommends using only one zone for each large geographically dispersed data center.
 - To minimize the number of zones, Citrix recommends connecting locations with only a few servers to a larger zone if good WAN connectivity exists.

Zone Preference and Failover:

- ❖ Is configured in the User Workspace folder in the properties of a policy.
- ❖ Connections can be directed to a preferred zone and failover to a backup zone.
- ❖ Is supported by Web Plugin and XenApp Plugin.

By default, a data collector does not communicate the load information to other data collectors in the server farm.

- ❖ If the administrator wants to share load information across zones, the **Share load information across zones** option must be selected in the server farm properties of the XenApp Advanced Configuration tool.

Data Store Data

The data store contains persistent information for the server farm such as:

- ❖ Server farm configuration information
- ❖ Published application configurations
- ❖ Server configurations
- ❖ Server farm management security (administrator accounts)
- ❖ Printer configurations
- ❖ Policy configurations

A subset of the data in the data store is stored in the local host cache on each server in the server farm.

- ❖ The local host cache contains all the farm-wide information needed for a server to resolve user requests in the event that the data store is unavailable.

Licensing and Installing XenApp

Licensing Functionality and Ports

Prior to the installation of a valid license, the *XenApp start-up license*:

- ❖ Allows for one administrator.
- ❖ Allows up to 2 user connections to XenApp.
- ❖ Grace period expires and user sessions will not be able to connect to servers running XenApp after 96-hours.
 - ◆ An administrator can continue to configure XenApp after the start-up license grace period expires.

The *License Management Console* uses port 8082 by default.

The *license manager daemon* uses port 27000 by default.

By default, the *license server vendor daemon* uses a random port.

- ❖ When using a firewall, the recommended port for the license server vendor daemon is port 7279.

Allocate Licenses

To install a new license for XenApp:

- ❖ In the **License Management Console** on the **Welcome** page click **Configure License Server > Step 1: Download license file from MyCitrix.com**.
- ❖ Login to **My Citrix** and from the **Current Tool** drop-down list, select **Activate/Allocate**.
- ❖ Download the license file.
- ❖ Copy the license file to your license server with the **License Server Management Console**.
- ❖ Make sure the directory appears in the **Upload license page**, or browse to it and click **Upload**.
- ❖ On the **License Files** page, click **Update license data**.
 - ◆ The file will appear in the table on the page.

To allocate licenses to the server farm, the administrator needs:

- ❖ The license code.
- ❖ A MyCitrix user ID and password.
- ❖ The license server host name.
- ❖ The number of desired licenses.

Server Report Log Files

Before an administrator can generate a historical report the report logging feature must be enabled.

To enable the report logging feature:

- ❖ In the **License Manager Console**, click **Configure License Server**.
 - ◆ The **License File** page appears.
- ❖ Click **File Locations**.
- ❖ Under **Report Log**, click **Change**.
- ❖ Enter the path to where you want to create your log and specify a meaningful name with a .rl extension for the report log.
- ❖ Click **Change** and the report log is created and appears in the **License Management Console**.

In order not to degrade the speed at which historical reports are generated, do not let your license report log files grow larger than 50MB.

Report logs are required to generate historical reports.

- ❖ Logs can grow excessively large if they are not archived on a regular basis.
- ❖ Excessive report log growth can negatively impact your licensing system in two ways:
 - ◆ By consuming hard drive space.
 - ◆ By slowing down report generation.
 - Citrix recommends that you estimate growth by watching report log growth over a period of time in your environment and not relying on a formula.

- ❖ You can address excessive report log growth by performing one of the following:
 - ◆ Archiving report logs using a standard file compression tool, such as WinZip, starting a report log with a new name, and moving the archived report log to a new location.
 - ◆ Changing the location or name of report logs.
 - When you *change the name* of a licensing report log, a *new report log is created*.
 - ◆ Specifying that the report log overwrite itself whenever you restart the license server.
 - Do not let your report logs grow larger than 50MB.
 - Report logs larger than 50MB can seriously degrade the speed at which the License Management Console generates reports.

To maintain license report logs, Citrix recommends:

- ❖ Rotating and archiving reports regularly.
- ❖ Giving report logs a meaningful name.
 - ◆ With the time interval in the name to make it easier to locate the log file in the license management console.
- ❖ Save report logs according to blocks of time such as weekly or monthly.
- ❖ In clustered license servers, do not give the report log the same name as either of the servers in the cluster.
 - ◆ If you do, the logs cannot be backed up properly.

Creating and Joining a Farm

To create a new server farm using an Oracle, Microsoft SQL or IBM DB2 database as the data store:

- ❖ On the **Create a Server Farm** setup page, enter a new name for the farm.
- ❖ Select **Use the following database on a separate database server** and select the database from the list.
- ❖ Either choose **Use default zone name** or create a name for the zone.

- ❖ Click **Next** and create a new data source connection to the database.

To create a new server farm using Microsoft Access or SQL Server Express for the data store:

- ❖ On the **Create a Server Farm** setup page, enter a name for the new server farm.
- ❖ Select **Use a local database on this server** and select the database from a list.
 - ◆ If using Microsoft Access, it will automatically be created during setup
 - ◆ If using SQL Server Express, install it on the server before installing XenApp.
- ❖ Either choose **Use default zone name** or create a name for the zone.
- ❖ Click **Next** and continue with setup.

To join an already existing server farm using a data store on a dedicated Oracle, Microsoft SQL Server or IBM DB2 database server:

- ❖ In the **Create or Join a Server farm** page of the installation wizard, choose **Join an existing farm**.
- ❖ Choose **Connect directly to the database using ODBC** and configure the ODBC driver for the database.
- ❖ To access the database, you'll need to enter the logon credentials of a user authorized to access the database.
- ❖ You do not need to create a new zone unless desired.

To join an existing server farm where the data store exists on the first XenApp server in the farm (Microsoft Access or SQL Server Express):

- ❖ In the **Create or Join a Server Farm** page of the installation wizard, choose **Join an existing farm**.
- ❖ Choose **Connect to a database on this server**; specify the name of the server hosting the Access or SQL Server Express database and click **Next**.
 - ◆ The default communication port is 2512.
- ❖ On the **Access the Database on a Citrix XenApp computer** page, specify the credentials for the server to which you are connecting.
- ❖ You do not need to create a new zone unless desired.

Remote Desktop Users Group

During the installation of XenApp, the existing users and groups and the anonymous user accounts created by XenApp can be added to the local *Remote Desktop Users* group on the server.

- ❖ During the **Remote Desktop Users** group step of XenApp installation, an administrator can choose to:
 - ◆ **Add the Authenticated Users now**
 - ◆ **Add the list of users from the Users group now**
 - ◆ **Skip this step, and add users later**
 - ◆ **Add anonymous users also**

Only users and groups that are members of the local Remote Desktop Users group can access resources on the server using the ICA or RDP protocol.

If the users and groups do not exist at the time of the installation or the administrator wants to manually add the users and groups, the administrator can use the Computer Management utility on the server to perform this task after the installation completes.

Miscellaneous Licensing and Installing

To upgrade from an existing server farm to XenApp 5.0, there are three different ways in which you can do so:

- ❖ Server migration,
 - ◆ A new installation of XenApp is performed (not using the **Upgrade Wizard**) on a clean system in an existing farm.
 - ◆ Farm upgrade, in which the existing farm and data store are maintained but at least one server in the farm is migrated to the new XenApp release
 - ◆ Farm migration, in which a new farm and data store are created, based on the installation of at least one new server (that is, the first server in the farm).

Shadowing restrictions set during the installation of XenApp are permanent.

- ❖ If shadowing was disabled or capabilities restricted during the installation, neither shadowing nor the restricted capabilities can be enabled after the installation is complete without reinstalling XenApp.

Installing and Configuring Web Interface

Web Interface in the Network Environment

The recommended design for a *Web Interface with Access Gateway Advanced Edition installation*:

- ❖ The Access Gateway server should be placed behind the first firewall in the DMZ.
- ❖ The Web Interface server should be placed behind the second firewall in the internal network.
 - ◆ Placing the Web Interface server (the server with IIS) in the internal network is more secure than leaving it in the DMZ where some security experts consider it a major risk.

In the case that the *Secure Gateway is in the DMZ and the Web Interface is in the internal network*:

- ❖ Use Citrix SSL Relay to secure Citrix XML traffic.
- ❖ Be sure that port 443 is open on the firewall between the Secure Gateway (in the DMZ) and the Web Interface (on the internal network) since Citrix SSL Relay uses port 443 by default.
 - ◆ This port number can be changed using the SSL Relay Configuration utility.

By placing *Secure Gateway as well as Web Interface in the DMZ*:

- ❖ No unauthenticated traffic can reach the secure, internal network.
- ❖ If a user fails to authenticate, the user traffic will not pass beyond the DMZ.
 - ◆ In this case, the Secure Gateway and Web Interface can be located on the same server or separate servers.

Web Interface Communication Path

Plain vanilla Web Interface implementation communication path:

- ❖ When a user logs into the Web Interface, the Web Interface forwards the logon credentials to the Citrix XML Service on the XenApp server.
- ❖ The Citrix XML Service retrieves a list of applications (the application set) that the user can access based on the supplied credentials.

The communication process of a Web Interface with Secure Gateway implementation:

- ❖ A remote user types the URL address of the Secure Gateway into a web browser.
- ❖ The Secure Gateway receives the request and relays it to the web interface.
- ❖ The web interface responds by sending the logon page to the web browser.
- ❖ The user submits credentials to the Secure Gateway server.
- ❖ The Secure Gateway sends the credentials to the Web Interface.
- ❖ The Web Interface sends the user credentials to the XML Service in the server farm which obtains the list of published resources the user is authorized to access and returns the list to the Web Interface.
 - ◆ The Citrix XML Service retrieves the resource set from the Independent Management Architecture (IMA) system.
- ❖ The Web Interface populates the web page with the list of published resources that the user is authorized to access.
- ❖ The user clicks a published resource and the Web Interface sends the request to the Secure Ticket Authority (STA).
- ❖ XenApp identifies the least busy server hosting the application and provides the IP address and port of that server to the STA.
- ❖ The STA saves the IP address and port number and issues the requested ticket to the Web Interface.
- ❖ The Web Interface generates an ICA file containing the ticket issued by the STA and the FQDN of the Secure Gateway server and sends it to the client device through the Secure Gateway.
- ❖ The web browser on the client device uses the ICA file it receives from the Web Interface to open a XenApp plugin and connect to the Secure Gateway server identified in the ICA file.
- ❖ The initial SSL/TLS handshaking is performed to establish the identity of the Secure Gateway server.
- ❖ The Secure Gateway receives the session ticket from the plugin and contacts the Secure Ticket Authority (STA) for ticket validation.
- ❖ The STA returns the IP address of the server hosting the published application to the Secure Gateway.

- ❖ The Secure Gateway establishes an ICA connection to the client device and begins encrypting and decrypting data flowing through the connection.

Web Interface Authentication

The following browsers can log on to the Web Interface:

- ❖ Internet Explorer 6.x and 7.0 (32-bit)
- ❖ Safari 2.0 or 3.x
- ❖ Firefox 2.x or 2.0
- ❖ Mozilla 1.7
- ❖ Symbian Browser
- ❖ Pocket IE

By enabling *Active Directory Federation Services (ADFS)*, an administrator in a resource domain can create sites for users in an account partner's domain and the users in the account partner's domain will have single sign-on access to the published applications in the resource domain.

Web Interface can be configured with:

- ❖ **Pass-through with smart card**
- ❖ **Anonymous**
- ❖ **Pass-through**
- ❖ **Smart card**
- ❖ **Explicit authentication**

Web Interface with Secure Gateway or Access Gateway

Secure Gateway can:

- ❖ Secure large server environments.
- ❖ Provide Internet access to servers in a server farm with a single point of encryption.
- ❖ Keep the internal IP addresses of servers hidden.

- ❖ Use two-factor authentication support through Web Interface.
- ❖ Keep costs and management lower than Access Gateway.

If users access a site directly or through *Access Gateway Enterprise Edition*, you can enable *published resource URL support*.

- ❖ Published resource URL support allows users to create persistent links to published resources accessed using the Web Interface.
 - ◆ These links can be added to the user's shortcut list or desktop.

When Secure Gateway or Access Gateway is used, the following *access methods* can be configured:

- ❖ *Direct access (Gateway direct)*, which sends the actual address of the XenApp server to the Access Gateway or Secure Gateway, is typically configured in situations where:
 - ◆ Internal users connect from trusted environments, such as a corporate intranet.
 - ◆ There is no need to keep the address of the XenApp server private.
- ❖ *Alternate access (Gateway alternate)*, which sends the alternate address assigned to the XenApp server to the Access Gateway or Secure Gateway, is configured in situations where:
 - ◆ The IP address of the XenApp server must be kept private from users.
 - If multiple servers are being used to provide application access, translated access would be used.
 - ◆ An administrator must configure XenApp to use an alternate address by using the **ALTADDR** command.
- ❖ *Translated access (Gateway translated)*, which uses the address translation mappings set in the Web Interface to determine which address is sent to the Access Gateway or Secure Gateway, is configured in situations where:
 - ◆ The IP address of the XenApp server must be kept private from users.
 - ◆ Multiple servers in the server farm are used to provide application access.
 - ◆ When a firewall is used, Web Interface must be configured with the appropriate IP address in the client files.

To configure *Gateway translation*:

- ❖ In the **Access Management Console** click the **Manage secure client access** task and click **Edit secure client access settings**.
- ❖ On the **Specify Access Methods** page, click **Add** to add a new access route.
 - ◆ Or select an entry from the list and click **Edit** to edit an existing route.
- ❖ Select **Translated** from the **Access method** list.
- ❖ Enter the network address and subnet mask that identify the client network.
- ❖ Use the **Move Up** and **Move Down** buttons to place the access routes in order of priority in the **Client addresses** table and click **Next**.
- ❖ On the **Specify Address Translations** page, click **Add** to add a new address translation
 - ◆ Or select an entry from the list and click **Edit** to edit an existing address translation.
- ❖ In the **Access Type** area, select **Client route translation** if you want the plugin to use the translated address to connect to the Citrix server.
 - ◆ Or select **Client and gateway route translation** if you already configured a gateway translated route in the **Client addresses** table and want both the plugin and the gateway server to use the translated address to connect to the Citrix server.

In a *single-hop DMZ deployment of Secure Gateway*:

- ❖ A *server certificate* must be installed on
 - ◆ The Secure Gateway Server
 - ◆ Web Interface Server
 - ◆ XenApp servers
 - Where communication must be secured between the Secure Gateway and Secure Ticket Authorities.
- ❖ A *root certificate* will be installed on:
 - ◆ The Secure Gateway
 - ◆ The Web Interface servers

Secure Ticket Authority URL

The URL of the STA is entered in the Secure Gateway configuration.

The URL of the STA can be changed based on whether or not IIS/XML port sharing is used or XML is being run on a different port.

- ❖ If the *XML port is changed* from the default port 80, be sure to *configure the STA URL with the new port number* when configuring Secure Gateway.
 - ◆ If the port were changed to 778, the URL would look like this:
 - `http://servername:778/Scripts/CtxSta.dll`

XenApp Web and Services Site

A *XenApp Web site* allows users to access published resources through a web browser.

- ❖ If users are going to access the applications through Web Interface, only XenApp Web sites can be configured.

A *XenApp Services site* allows users to access published resources through the Citrix XenApp plugin.

An administrator can create a XenApp Web site or a XenApp Services site using:

- ❖ The Access Management Console
 - ◆ The XenApp Web site configuration information is stored in a local file.

If a scenario calls for users to be able to access applications that are *installed on servers* in the server farm *and* access other applications that are *streamed to servers or the desktops* of client devices *through Web Interface*, there are two solutions:

- ❖ One *XenApp Web site* must be configured to use **Dual mode streaming**.

Or

- ❖ Two *XenApp Web sites* must be configured:
 - ◆ One site must be configured to use the **Remote** application type.
 - ◆ The other site must be configured to use the **Streaming** application type.

If a scenario calls for users to be able to access applications that are *installed on servers* in the server farm *and* access other applications that are *streamed to servers or the desktops* of client

devices *through Citrix XenApp plugin*, there are two solutions:

- ❖ One *XenApp Services site* must be configured to use **Dual mode streaming**.
- ❖ Two *XenApp Web sites* must be configured:
 - ◆ One site must be configured to use the **Remote** application type.
 - ◆ The other site must be configured to use the **Streaming** application type.

To restrict *access based on domains*:

- ❖ Click **Domain Restriction** in the left pane of the **Access Platform authentication methods** properties.
- ❖ Choose **Restrict domains to the following domains**.
- ❖ Add the domains that are allowed access.

To configure a *XenApp Web site to work with Secure Gateway*:

- ❖ In the **Access Management Console** click the **Manage secure access task**.
- ❖ Click **Edit gateway settings** and type the FQDN of the Secure Gateway server in the **Address (FQDN)** field.
- ❖ Configure session reliability.
- ❖ Configure the STA settings.
- ❖ Click **OK**.

Configure Application Streaming on Web Interface

Web Interface can be configured using either:

- ❖ Settings in the Access Management Console.
- ❖ Editing the WEBINTERFACE.CONF file.

After creating a XenApp Web site, the administrator configures the initial settings. During the initial configuration, the administrator can configure one of three settings for the type of applications made available to users:

- ❖ **Remote**

- ◆ Only allows users to access applications *provided by a server*.
- ◆ Through an *ICA or RDP connection*.
- ❖ **Streaming**
 - ◆ Only allows users to access applications *streamed to client devices*.
- ❖ **Dual mode streaming**
 - Allows users to access applications *streamed to the client device or provided by the server*.
 - Through an *ICA connection only*.

ICA Files

Use the default.ica or template.ica file to override hotkeys for applications that users connect to through Web Interface.

Web Interface Troubleshooting

Issue: A user browses to the main Web Interface web page, successfully logs in, but is *not presented with a list of applications*.

Probably cause: The user does not have access to any applications.

Solution: The user's account must be added to the correct groups in Active Directory that give the users access to the published applications.

Issue: A *remote* user is given instructions to *securely* browse <http://apps.abcxyzcompany.com/>, login and launch the applications that she will regularly use. She followed the instructions closely. She is unable to connect to the Web Interface web site and instead receives an error page.

Probable cause: The instructions were incorrect.

Solution: The remote users should make a secure connection using Secure HTTP, so the URL should be <https://apps.abcxyzcompany.com/>.

Issue: Web Interface users are reporting that when they enter their username and password in the appropriate fields of the initial web page that they always browse to for their applications they are receiving an error that the XenApp servers cannot process their request at this time.

Probable cause: In the Web Interface communication process, when a user enters their logon credentials in the login screen of Web Interface, the login credentials are forwarded to the Citrix XML Service in the server farm to determine whether the login credentials are valid or invalid. Since the users made it to the login screen, it is obvious that the Web Interface server is not offline. The more likely issue is that *the Citrix XML Service on the dedicated XenApp server in the server farm has stopped.*

Solution: Manually restart the Citrix XML Service or reboot the server and if it still does not work, a different XenApp server should be designated as the dedicated Citrix XML Service server.

Issue: Alternate addressing is configured for connections through the firewall to the XenApp servers. Users who connect to their applications through Web Interface report that, after logging in and receiving a list of applications in their web browser, they click on an application to launch it but it fails every time with an error that there is no server available at the specified address.

Probable cause: The Web Interface automatically generates an ICA file with information about the XenApp server that the client device is supposed to connect to. The ICA file is delivered to the web browser on the client device from the Web Interface. If the connection information in the ICA file is incorrect, the XenApp plugin on the client device will not be able to make a connection to the published application. The wrong IP address for the XenApp server was most likely configured when configuring the alternate IP address, so the wrong IP address is on the ICA file.

Solution: An administrator should check the ICA file and make any corrections needed on the Web Interface server.

If you experience problems with a XenApp Web site, try using the Web Interface **Repair** option to fix the problem.

- ❖ On Windows IIS, Web Interface has a **Repair** option that you can try to fix problems with your XenApp Web sites.
 - ◆ To repair Web Interface: run the **WebInterface.exe** file, select **Repair**, click **Next** and follow the instructions on screen.
- ❖ If that still doesn't work, or the **Repair** option doesn't exist because of being a Java web server installation, try uninstalling and reinstalling Web Interface.
 - ◆ If you have to uninstall and reinstall Web Interface you will have to recreate all of the XenApp Web sites.

Configuring ICA Sessions

ICA Session Policies

To allow some users in a company to have more sessions running than the server farm is configured to allow:

- ❖ Create a new policy in XenApp and add the policy rule **User Workspace > Connections > Limit total concurrent sessions**.
- ❖ Configure the sessions to as many as needed and apply the policy to the desired users or groups.

The audio rules available in the **Client Devices > Resources > Audio** folder for XenApp policies are:

- ❖ **Microphones**
 - ◆ Allows microphones on client devices to be used in a session.
- ❖ **Sound Quality**
 - ◆ Configures the maximum allowable client audio quality per session.
- ❖ **Turn off speakers**
 - ◆ Disables audio mapping to client speakers.

To configure **PDA synchronization using USB-tethering**:

- ❖ Enable the policy rule **Turn on automatic virtual COM port mapping**.
 - ◆ This rule allows USB to virtual COM port emulation in client sessions.
 - This rule is found in a policy at **Client Devices > Resources > PDA Devices**.

In the **User Workspace** folder of a XenApp policy, an administrator can configure:

- ❖ **Connections**
 - ◆ Including **Limit total concurrent sessions** and **Zone preference and failover**.
- ❖ **Server-to-client content redirection**
- ❖ **Shadowing**

- ◆ Including configuration and permissions.

- ❖ **Time Zones**

- ◆ Including **Do not estimate local time for legacy clients** and **Do not use Client's local time**.

- ❖ **Citrix Password Manager**

- ◆ Including **Central Credential Store** and **Do not use Citrix Password Manager**.

- ◆ **Streamed Application**

- Including **Configure delivery protocol**.
 - Specifies the application delivery method used to stream applications to the desktops of client devices or servers.

An administrator can configure the required SecureICA encryption level per session in:

- ❖ **Security > Encryption > SecureICA encryption**

- ◆ This is the only encryption rule available in a XenApp policy.

Maintain Plugins

The *Citrix XenApp Plugin* allows users to access all of their published resources in a familiar Windows desktop environment.

- ❖ Users work with published resources the same way they work with local applications and files.
- ❖ Published resources are represented throughout the client desktop, including the Start Menu and Windows notification area, by icons that behave just like local icons.
- ❖ You configure the Citrix XenApp Plugin using a Citrix XenApp site created in the Access Management Console.
 - ◆ The plugin is associated with the site for the Web Interface server.

If you want the users to be prompted for authentication to a XenApp server every time, select **No** when configuring pass-through authentication during XenApp Plugin installation.

When configuring the XenApp Plugin:

- ❖ Depending on whether you are connecting to a secure connection or not, type the name of the server hosting the XenApp Services site in one of these formats:
 - ◆ `http://servername`
 - Not secure.
 - Replace *servername* with the *name of the Web Interface server*.
 - ◆ `https://servername`
 - Secured by Secure HTTP.
 - Replace *servername* with the *name of the Web Interface server*.

XenApp Web Plugin:

- ❖ It is a smaller client that can be installed from **XenAppWeb.msi** or **XenAppWeb.exe**.
- ❖ The XenApp Web Plugin setup files are significantly smaller than the other clients.
 - ◆ The small size allows users to quickly download and install the client software.
- ❖ Users access the published resources by clicking on links from a Web page or corporate intranet.
 - ◆ The Web Client does not require user configuration and does not have a user interface.

The XenApp Web Plugin can automatically be installed on the client devices before users try to use the Web Interface. To configure automatic deployment of the XenApp Web Plugin:

- ❖ *Create a home page and run an Internet Explorer script* to download the **XenAppWeb.exe** package automatically from the web server and install it for the user.

Program Neighborhood:

- ❖ Supports the full XenApp feature set and it requires user configuration and maintenance.
- ❖ Choose Program Neighborhood if you do not want to publish your resources using Web Interface.
 - ◆ If you choose to implement the Web Interface at a later time, Program Neighborhood users can also access resources published through Web Interface.

- ❖ **Enable Quick Launch Bar** and **Enable Custom ICA Connections** are both configuration choices for Program Neighborhood.

While creating a *Program Neighborhood package*:

- ❖ To help ensure duplicate client names do not exist on the network, use a name different for the client than the computer name by choosing **Specify a client name**.
- ❖ To let users open sessions without entering their username and password, choose **Use Kerberos only** to enable pass-through authentication.
- ❖ To allow users to make server connections without using the **ICA Connection Wizard**, choose **Enable Quick Launch Bar**.
- ❖ To ensure older client versions are overwritten with newer clients, leave the default client replacement option chosen, which is **Allow upgrade if package is newer than existing client version**.

Administrators can use *Active Directory to deploy clients using the .MSI file* on the installation media or using a custom client file package created with *Client Packager*.

To deploy the Citrix XenApp Plugin software using an MSI package via Client Packager to *Windows 2000 Professional computers* using Active Directory:

- ❖ *Windows Installer 3.0 Redistributable for Windows* must be installed.
- ❖ Windows XP, Windows Vista, Windows Server 2003 and Windows Server 2008 already have the supported Windows Installer by default.

When creating a package with the *Client Packager*:

- ❖ The default client name option is **Use machine name as client name**.
- ❖ The other client name option is **Let users specify a client name**.
 - ◆ By choosing **No** on the **Pass-Through Authentication** screen, the administrator would make sure that the users must enter their username and password to log on to sessions.

By default, Citrix plugins get the *same name as the machine* at deployment.

To assign a client package to an Organizational Unit (OU):

- ❖ Create a network share and copy the .MSI file containing the client to the network share location.

- ❖ In **Active Directory Users and Computers**, right-click the appropriate **OU** and click **Properties**.
- ❖ Click the **Group Policy** tab and click **New** to create a new Group Policy.
- ❖ Type the name for the Group Policy, press **Enter** and click **Edit**.
- ❖ Navigate to **Computer Configuration > Software Settings > Software Installation**.
- ❖ Right-click the blank area in the right pane and click **New > Package**.
- ❖ Locate the client package on the network share and click **Open**.
- ❖ Click **Assigned** in the **Deploy Software** dialog and click **OK**.

As the client *restarts*, Active Directory Group Policy *automatically installs the client* on the computer.

After deploying a client package via Active Directory and restarting the client device, the *administrator should log in* to the client device to *verify that the client is installed*.

Configure Display Settings

An administrator can improve WAN performance:

- ❖ By configuring the display settings that control bandwidth usage of graphics that are transferred to the client.
 - ◆ The display settings can be configured for use by the entire farm or for a specific server.

Configure display settings at the server or farm level:

- ❖ **Discard queued image that is replaced by another image**
 - ◆ Graphics that are immediately replaced by other graphics will not be sent.
- ❖ **Cache image to make scrolling smoother**
 - ◆ Sections of bitmap graphics will be retrieved from the client cache to make pages scroll more smoothly.
- ❖ **Maximum memory to use for the graphics in each session**
 - ◆ Limits the size of the memory buffer each client connection uses.

- If *multiple monitors* are being used, this setting should be set to the *maximum*.

❖ **Degrade resolution first**

- ◆ Lowers the resolution to accommodate the memory buffer limit before lowering the color depth.

❖ **Notify user of session degradation**

- ◆ A message will be displayed on the user's client device when the session is degraded as a result of the memory buffer limit being exceeded or the client device being unable to support the requested parameters.

TWCONFIG can be used to set the maximum amount of memory used for session graphics on a server.

SpeedScreen

SpeedScreen Latency Reduction Manager provides mouse click feedback and local text echo to reduce the user's perception of latency when typing and clicking.

SpeedScreen Browser Acceleration optimizes the responsiveness of graphics-rich HTML pages in published versions of Microsoft Outlook, Outlook Express and Internet Explorer.

- ❖ To further accelerate the accessibility of Web pages and email using SpeedScreen Browser Acceleration
 - ◆ JPEG compression can be enabled.
 - JPEG compression offers a trade-off between the quality of the JPEG images as they appear on the client devices and the amount of bandwidth the files consume transferring from server-to-client.
 - JPEG image acceleration results in slightly lower image resolution and slightly higher resource consumption on both server and client.
 - When enabled, select the image compression level: **Low**, **Medium** or **High** or select **Adjust compression level based on available bandwidth**.
 - SpeedScreen Browser Acceleration is enabled by default at the farm level.
 - It can be customized at the farm or server level.

SpeedScreen Multimedia Acceleration allows you to control and optimize the way XenApp passes streaming audio and video to users.

SpeedScreen Flash Acceleration allows you to control and optimize the way XenApp passes Macromedia Flash animations to users.

SpeedScreen Image Acceleration offers you a trade-off between the quality of photographic image files as they appear on client devices and the amount of bandwidth the files consume on their way from the server to the client.

- ❖ SpeedScreen Image Acceleration is the only SpeedScreen technology that is configured in a XenApp policy.
 - ◆ To configure SpeedScreen Image Acceleration:
 - Create a new policy using the **XenApp Advanced Configuration** tool
 - Expand the **Bandwidth** folder.
 - Expand the **SpeedScreen** folder and click the **Image acceleration using lossy compression** node.
 - In the right pane, enable it.
 - Set the **Image Acceleration compression level**
 - Set bandwidth restrictions
 - Set the **Progressive Display compression level**
 - Determine whether to use **Heavyweight compression**
 - Click **OK** and apply the policy using a policy filter.

SpeedScreen Progressive Display allows you to improve interactivity when displaying high-detail images by temporarily increasing the level of compression (decreasing the quality) of such an image when it is first transmitted over a limited bandwidth connection, to provide a fast (but low quality) initial display.

- ❖ If the image is not immediately changed or overwritten by the application, it is then improved in the background to produce the normal quality image, as defined by the normal lossy compression level.

Heavyweight compression allows you to increase the compression of the SpeedScreen Image Acceleration and SpeedScreen Progressive Display without impacting image quality.

- ❖ Because heavyweight compression is *CPU intensive and affects server scalability*, it is recommended for use only with *low bandwidth connections*.

Bandwidth Policy

In a policy, bandwidth can be configured by either:

- ❖ *Kilobytes per second*
 - ◆ The bandwidth rules for kilobytes per second are configured in the **Session Limits** folder.
- ❖ *Percentage*
 - ◆ The bandwidth rules for percentage are found in the **Session Limits (%)** folder.
 - ◆ In order for a bandwidth rule to work as a percentage in a policy, the administrator must also configure the **Overall Session** rule in the **Session Limits (%)** folder.

If the same rule is set with a fixed value in **Session Limits** *and* a percentage value in **Session Limits (%)**, the *most restrictive* rule (that is, the lower value) is the one that is *applied*.

- ❖ For example, if the maximum amount of bandwidth usage was configured for 250Kbps and **Audio** was configured with both a fixed value of *60Kbps* and a percentage of *20%* (or 50Kbps), the 50Kbps would be used since it is the lower, or more restrictive, setting.

If an administrator is concerned about bandwidth and needs to create a policy or policies to help contend with bandwidth issues, there are many policy rules that can be configured. In the **Bandwidth** folder of a XenApp policy, the administrator can configure:

- ❖ **Visual effects**
 - ◆ **Turn off desktop wallpaper**
 - ◆ **Turn off animations**
 - ◆ **Turn off windows content while dragging**
- ❖ **SpeedScreen Image Acceleration using lossy compression**
- ❖ **Session limits**
 - ◆ Including the maximum bandwidth to use for:
 - Client audio
 - Client clipboard mapping
 - Client COM and LPT port mapping

- Client drive access
- OEM virtual channels
- Overall client session
- Printing
 - Printing bandwidth can be limited through *server properties* or with a *policy rule*.
- TWAIN driver redirection

To cut down on the bandwidth used for audio in an audio-enabled application:

- ❖ Create a XenApp policy.
- ❖ Enable the **Sound Quality** rule in:
 - ◆ The **Client Devices > Resources > Audio** folder.
 - Limit the **Audio bandwidth per session** to desired level.

Session Reliability

Session reliability:

- ❖ Keeps sessions active on the user's screen when network connectivity is interrupted.
 - ◆ Users continue to see the application they are using until network connectivity resumes, but the display freezes and the cursor changes to a spinning hourglass.
- ❖ The advantage is that when network connectivity resumes, they don't have to reconnect to the application.
- ❖ To enable session reliability, choose **Allow users to view sessions during broken connection** in the **Session Reliability** settings.
- ❖ Disable it by deselecting **Allow users to view sessions during a broken connection**.
- ❖ Change the port number in the **Port number** field
- ❖ Change the amount of time sessions remain active when connectivity is lost in the **Seconds to keep sessions active** field.

- ❖ If an administrator wants users to re-authenticate before reconnecting to active sessions, **Auto-client reconnect** should be enabled.
- ❖ When session reliability is enabled, **Keep Alive** settings are not used even when they are configured in the server farm.

Session reliability is *provided by the Citrix XTE Service* through the Common Gateway Protocol on port 2598.

Auto-Client Reconnect

Auto-client reconnect allows the following clients to detect broken connections and automatically reconnect users to disconnected sessions:

- ❖ Client for Windows
- ❖ Client for Java
- ❖ Client for Windows CE

When a client detects an involuntary disconnection of a session, it *attempts to reconnect* the user to the session *until there is a successful reconnection* or the user *cancels the reconnection* attempts.

ICA Keep-Alive

ICA Keep-Alive is a setting used to manage the states of the ICA sessions to ensure that they are accurately reported.

When ICA Keep-Alive is configured:

- ❖ Packets are sent to each client device to determine whether a connection still exists.
 - ◆ If the client device does not respond, the state of the session using the connection is changed from **Active** to **Disconnected**.

SmoothRoaming

SmoothRoaming allows a user to disconnect from one ICA session and *reconnect from another device* to continue that *same session*.

Managing Applications

Remote and Streaming Application Delivery Methods

Using a web browser, a XenApp Web site allows users to access:

- ❖ Remote and streamed applications
- ❖ Content

Streamed applications can be pre-deployed in one of two ways:

- ❖ Using **RADEPLOY.EXE**.
- ❖ Configured in the published application.

When configuring an application delivery method policy the administrator can configure the policy to:

- ❖ **Force server access**
 - ◆ Forces streamed applications to *always launch from the server*.
- ❖ **Force streamed delivery**
 - ◆ Forces the applications to *always stream to the desktops of the client devices*.

Publish an Application

When *published*, users can access applications installed on the XenApp servers.

- ❖ The applications *appear to run locally on the client devices*.
- ❖ Published applications *provide the administrators control over what resources users can access on a server*.
 - ◆ Unlike published server desktops.
 - Published server desktops allow users *unlimited access to the resources on a server* which can result in *users changing configurations and settings that can cause server vulnerabilities*.

If you install and publish an application *after installing XenApp*, you must *update the file type association* in the server's Windows registry.

- ❖ To update file type associations:
- ❖ In the **Access Management Console**, select the server where the application is published.
- ❖ Select **Action > All Tasks > Update file types from registry**.

By *default*, all resources are published to the *root folder* of the application set.

- ❖ An administrator can *organize published resources* in an application set by placing the published resources in *folders* during the resource publishing process or afterwards.
 - ◆ For example, if many Microsoft Office applications are published, an administrator might decide to place the Microsoft Office applications into a folder called **Microsoft Office** making it *easier for users to locate* these applications.

Users can open published content using two types of *content redirection*:

- ❖ *Client-to-server*
 - ◆ Allows users to *use a published application on the XenApp server* to access files residing on the *local client device*.
 - *Requires XenApp Plugin* on the client devices.
 - **Client drive mapping** must be enabled so that the local content can be accessed by the application on the server.
 - If drive mapping is not enabled, the *published application opens and displays an error*
 - Application is unable to access the local content that initially triggered the application to start.
- ❖ *Server-to-client*
 - ◆ Server-to-client is a policy rule that can be configured for specific connections to *open web browsers on the user's computer* instead of the XenApp server.

Users might frequently access web and multimedia URLs they encounter when running an email program published on a server.

- ❖ *If you do not enable server-to-client content redirection*, users open these URLs with web browsers or multimedia players *on the XenApp servers*.

❖ To free servers from processing these types of requests, you can redirect application launching for supported URLs from the server to the local client device.

◆ The following URL types are redirected:

- HTTP
- HTTPS
- RTSP (Real Player and QuickTime)
- RTSPU (Real Player and QuickTime)
- PNM (Legacy Real Player)
- MMS (Microsoft's Media Format)

Published resources can be configured to control the following options for the client device:

❖ **CPU Priority**

◆ Changes the CPU priority of the published resource.

❖ **Client audio**

◆ Allows support for applications to which SpeedScreen Multimedia Acceleration does not apply.

❖ **SSL and TLS protocols**

◆ Requests the use of the SSL and TLS protocols for plugins connecting to the published resource.

❖ **Encryption**

◆ Controls which plugins are allowed to connect based on their encryption level.

❖ **Client printers**

◆ Allows the published resource to open without waiting for the client printers to be created.

Session Sharing

Session Sharing:

- ❖ When a user starts a published application, an ICA connection is made to a XenApp server.
- ❖ If the user starts a published application on a different server, another ICA connection is made.
- ❖ If a user starts a published application on a server that the user already has an ICA connection to, the same ICA connection will be used
 - ◆ If the user is already at the ICA connection limit, a new ICA connection will not be started.

Configure ICA connections limits in a single published application:

- ❖ When publishing the application.
- ❖ In the properties of the published application.

Configure farm-wide ICA connection limits:

- ❖ By configuring the farm properties in the Access Management Console.

For applications to launch and use session sharing, certain criteria must be met:

- ❖ All applications need to be installed on the same server.
- ❖ All applications need to be published seamlessly
 - ◆ As opposed to a fixed sized or full screen window size.
- ❖ Connection limits at the farm level and application level should be set to 1.
- ❖ Session sharing requires that *color depths, screen resolutions, audio quality and encryption levels* (if used) are equal on all published applications that will share the session.

Profiling an Application

Before publishing a streamed application, an administrator must use the *Streaming Profiler* to *profile the application*.

- ❖ Publishing a streamed application makes profiled applications available to users.

- ❖ An administrator publishes a streamed application using the Access Management Console.
- ❖ The application profile is stored on a file share.

To maximize streamed application compatibility:

- ❖ It is a best practice to install a profiler on each operating system in use within the environment.
 - ◆ If one operating system is used to create all of the profiles there is a good possibility that a profile created on one operating system will not work properly on a different operating system.
- ❖ When installing the Citrix streaming profiler on a profiling computer, the computer *should have standard software*, such as anti-virus programs, Service Packs and updates that are part of the company image installed.

When creating a streaming profile, an administrator can configure how restrictive the *client isolation environment* should be.

- ❖ *Enhanced security*, which is the recommended best practice, prevents the running of the executable content that the user downloads into the isolation space.
 - ◆ This setting protects against users running malicious code or spyware.
- ❖ *Relaxed security* permits the running of executable content that the user downloads into the isolation space.

Publish a Streaming Application to a Client

To publish a streaming application to be streamed to the client:

- ❖ In the **Access Management Console**, right-click the **Applications** node and select **New > Publish Application**.
- ❖ Click **Next** on the **Welcome** screen.
- ❖ Type the application name and click **Next**.
- ❖ Select **Application**, configure **Streamed to client** and click **Next**.
- ❖ Specify the location of the profile being published.

- ❖ Select the application from the **Application to launch from the Citrix streaming application profile** drop-down list and click **Next**.
- ❖ Select the users that will be allowed to access the published application.
- ❖ Configure the appearance and location of the application shortcuts and click **Next** and click **Finish**.

Publish a Streaming Application to a Server

To publish a streaming application to stream to the server and be accessed by the client devices using ICA:

- ❖ In the **Access Management Console**, right-click the **Applications** node and select **New > Publish Application**.
- ❖ Click **Next** on the **Welcome** screen.
- ❖ Type the application name and click **Next**.
- ❖ Select **Application**, configure **Accessed from server** and click **Next**.
- ❖ Choose **Remote** to grant users access to the published application installed on the server via ICA or RDP and click **Next**.
- ❖ Specify the location of the profile being published.
- ❖ Select the application from the **Application to launch from the Citrix streaming application profile** drop-down list and click **Next**.
- ❖ Select the servers on which the application will run to be accessed through an ICA connection and click **Next**.
- ❖ Select the users that will be allowed to access the published application.
- ❖ Configure the appearance and location of the application shortcuts and click **Next**.
- ❖ Click **Finish**.

Configure Encryption for a Published Application

ICA encryption:

- ❖ Guards against the threat of eavesdropping.

- ❖ Secures the information sent between client devices and XenApp servers
- ❖ Is configured in:
 - ◆ XenApp policies
 - ◆ Published applications
- ❖ Is available in several encryption strengths:
 - ◆ **Basic**
 - ◆ **RC5 (128-bit) logon only**
 - ◆ **RC5 (40-bit)**
 - ◆ **RC5 (56-bit)**
 - ◆ **RC5 (128-bit)**

SSL Relay:

- ❖ Secures end-to-end ICA communication between:
 - ◆ Client devices and XenApp servers.
- ❖ Secures XML communications between:
 - ◆ Web Interface servers and XenApp servers.
- ❖ Is a great security solution for a very small implementation of five or less XenApp servers.
- ❖ Is a good choice when:
 - ◆ Secure communication for the Citrix XML Service is required.
 - ◆ A DMZ is not required.
 - ◆ IP addresses do not need to be hidden.
 - Or NAT is configured.
 - ◆ End-to-end encryption of data between the clients and servers is required.

To configure SSL Relay:

- ❖ Obtain and install a unique server certificate on each XenApp server.
- ❖ Install a root certificate on each client device and Web Interface server.
- ❖ Using the **SSL Relay Configuration** tool, configure:
 - ◆ Relay credentials
 - ◆ Connections
 - ◆ Ciphersuites
- ❖ Restart the XenApp servers.

Ciphersuites:

- ❖ Are an encryption/decryption algorithm.
- ❖ Are used when SSL Relay is being used.
- ❖ Provide *COM* and *GOV* by default in XenApp.

Managing XenApp Policies

Impact to Users with Multiple Policies

XenApp policies:

- ❖ Are applied when an ICA session begins.
 - ◆ If a policy is changed while users are connected to a session, the change does not take effect until a new session is initiated.
 - ◆ The rules remain in affect for the duration of the session.
- ❖ Receive a number upon creation.
 - ◆ By default, a *new policy* has the *lowest priority* of all policies.
 - ◆ The number assigned is based on the number of policies that exist in a server farm.

To *prioritize* a policy:

- ❖ In the **XenApp Advanced Configuration** tool, click the **Policy** node.
- ❖ Right-click the policy in the right pane and click **Priority**.
 - ◆ If you want to assign the policy the highest priority, click **Make Highest Priority**.
 - ◆ If you want to assign the policy the lowest priority, click **Make Lowest Priority**.
 - ◆ If you want to increase the priority of the policy one level, click **Increase Priority**.
 - ◆ If you want to decrease the priority one level, click **Decrease Priority**.

Apply Policies to Whom or What

After a policy has been created and configured, an administrator can *filter the policy* using:

- ❖ Client names
- ❖ Access control (connections made through Access Gateway)
- ❖ Users and user groups
- ❖ Servers
- ❖ Client IP addresses

To filter a policy to *affect only a certain range of IP addresses*:

- ❖ Click the **Policy** node in the **XenApp Advanced Configuration** tool.
- ❖ Right-click the appropriate policy in the right pane and select **Apply this policy to**.
- ❖ Click **Client IP Address**.
- ❖ Click **Filter based on client IP address**.
- ❖ Click **Add**.
- ❖ Click **IP Range** and click **OK**.
- ❖ Click **Allow** and click **OK**.

Issue: Remote users are complaining that an audio-enabled application that they use is performing badly. There are no complaints from the local users.

Probable cause: Not enough bandwidth available over remote connection.

Solution: 1) Cut down on the bandwidth used for audio in an audio-enabled application by creating a XenApp policy and enable the **Sound Quality** rule in the **Client Devices > Resources > Audio** folder. 2) Limit the audio bandwidth per session to desired level. 3) *Apply the policy* to the users that are experiencing the application degradation.

To apply a XenApp policy *to a user or group*:

- ❖ In the **XenApp Advanced Configuration** tool, click the **Policy** node.
- ❖ Right-click the appropriate policy and click **Apply this policy to**.
- ❖ Click **Users**.
- ❖ Click **Filter based on users**.
- ❖ Configure the users and groups filter option in one of four ways:
 - ◆ **Apply the policy to all explicit users (non-anonymous).**
 - ◆ **Apply the policy to all anonymous users.**
 - ◆ **Apply the policy to a specific user account or user group.**
 - ◆ **Avoid applying the policy to a specific user account or user group.**
- ❖ Click **OK**.

Shadowing Policy

To create a new *shadowing policy* that will *give notification* to the users being shadowed and *will not allow the users shadowing to control the desktop*:

- ❖ Create a *new policy* in the **XenApp Advanced Configuration** tool.
- ❖ In the policy's properties open the **Shadowing** folder under the **User Workspace** folder in the left pane.
- ❖ Select the **Configuration** rule and enable it.

- ❖ Select **Allow shadowing**.
- ❖ Select **Prohibit being shadowed without notification**.
- ❖ Select **Prohibit remote input when being shadowed**.
- ❖ Select the rule named **Permissions** in the left pane and enable it.
- ❖ Click **Configure** to select the users or group who will do the shadowing and click **OK** when done adding the users.
- ❖ Click **OK** at the bottom of the policy's properties.
- ❖ Apply the policy to the users or group who will be shadowed.

After creating a policy to allow Group01 to shadow Group02, the policy needs to be *filtered by users* to specify that the policy *should be applied to Group02*. Take the following steps:

- ❖ Select the policy and choose **Actions > Policy > Apply this policy to**.
- ❖ Select **Users** in the left pane.
- ❖ Select **Filter based on users**.
- ❖ Select Group02 from the correct domain, click **Add** and click **OK**.

Resultant Policy

The *policy search engine*:

- ❖ Is a feature of the XenApp Advanced Configuration tool.
- ❖ Allows an administrator to find all policies that can potentially apply to a specific connection and confirm how final policy rules are merged for that connection.
 - ◆ Verifies that a policy will be applied correctly.

To use the policy search engine:

- ❖ Right-click on the **Policies** node in the **XenApp Advanced Configuration** tool and click **Search**.
- ❖ Configure the search criteria
 - ◆ **IP Address**

- ◆ **Client Name**
- ◆ **User**
- ◆ **Server**
- ◆ **Access Control**
- ❖ Click **Search**.
- ❖ Click **Yes** to search the entire Active Directory if desired.
- ❖ Optionally, double-click a policy in the search results to view the policy priorities.
- ❖ Click **View Resultant Policy** and the **Resultant Policy Properties** screen launches.
- ❖ Expand each node to view individual resultant policy rules.
- ❖ Click **OK** to close the **Resultant Policy Properties** screen.
- ❖ Click **OK** to close the **Search** screen.

Managing and Maintaining the Server and the Farm

CPU Utilization

When you enable *CPU utilization management*:

- ❖ The server allocates an *equal share* of the CPU to each user.
 - ◆ This prevents one user from impacting the productivity of other users.
 - ◆ It allows more users to connect to a server.

The default *Local System Account CPU reservation* for XenApp servers is 20% divided by the number of CPUs in the server.

- ❖ If a server has one CPU, the CPU reservation is 20%.
- ❖ If a server has two CPUs, the reservation is 10%.
- ❖ And so on...
 - ◆ That means that if 20 users are connected to a server with one CPU, they will each get 4% of the CPU resources.

- ◆ If there are 10 users connected to a server with two CPUs, 10% of the total CPU resource is reserved for the Local System Account which leaves 90% for the users.
 - 90% CPU divided by 10 users equals 9% per user.

The *Rebalancer Service* is responsible for enhancing resource management on servers with multiple CPUs.

- ❖ If this service is not started on servers with multiple CPUs, the benefits of CPU utilization management are lost.
- ❖ The service is set to **Manual** by default
 - ◆ If you decide to use it long-term, set it to **Automatic**.

Administrative Rights

To modify permissions for a Citrix administrator account:

- ❖ Open the **Access Management Console**, click the server farm node.
- ❖ Double-click **Administrators** in the drop-down list details pane, right-click the administrator account or group in the details pane and click **Modify administrator properties**.
- ❖ Click **Permissions** in the left pane of the **Properties** screen.
- ❖ Click a folder and then select the permissions in the right pane that the selected administrator or group will have for that folder.
- ❖ Repeat the last step until all the appropriate permissions are set and click **OK**.

Issue: A Senior Systems Administrator created a new Systems Administrator's account and gave the account full control permissions to the XenApp farm before the new administrator had permission from the IT director to administer the XenApp farm.

Probable Cause: The Senior Systems Administrator had not been informed that the new Systems Administrator must receive two weeks of Citrix training before the IT director will let him administer the server farm.

Solution: Disabling the new Systems Administrator's Citrix administrator account will keep him from making any configurations to the server farm before being fully trained. After training is completed, the Senior Systems Administrator can enable the account for the Systems Administrator.

Issue: The IT department needs to delegate some of the more simple tasks to the Help Desk department.

Probable cause: With a cutback in staff, the IT department is having trouble keeping up with all of the calls for one of the most common issues: User sessions freezing or unexpectedly disconnecting.

Solution: Give the Help Desk the **View Session Management** right so they will be able to view the user sessions to be able to help them. Give them **Connect Sessions** to allow them to connect to user sessions to be able to assist the users. Give them **Reset Sessions** so they can reset the users' sessions that have become frozen.

Configuration Logging

The *Configuration Logging* feature:

- ❖ Allows you to keep track of administrative changes made to your server farm.
- ❖ Generates reports that show:
 - ◆ What changes were made.
 - ◆ When the changes were made.
 - ◆ Who made the changes.

To *configure configuration logging*:

- ❖ Create the configuration logging database.
- ❖ Verify the configuration logging database is specified in the **Database type** field.
- ❖ Configure the configuration settings for the server farm.
- ❖ When the administrator needs to, she can clear the data stored in the configuration logging database.

To set up *logging of administrative tasks*:

- ❖ Open the **Access Management Console**, right-click the server farm node and click **Properties**.
- ❖ Expand the **Farm-wide** node and click **Configuration Logging**.

- ❖ Verify that a configuration logging database is specified in the **Database type** field.
- ❖ Select **Log administrative tasks to the logging database** and click **OK**.

XenApp can be *configured to encrypt*:

- ❖ The *IMA communications* used to send information *to the data store and configuration logging databases*.
 - ◆ This encryption can add a layer of *security to the sensitive data stored in the databases*.

XML Service Trust

The *Citrix XML Service trust relationship* should be configured:

- ❖ When **Pass-through** or **Smart card** authentication methods are used.
- ❖ Between Web Interface and the XenApp servers.
 - ◆ This trust relationship must be established for Web Interface to be able to authenticate users.
 - ◆ If **Explicit** or **Anonymous** authentication is used, there is *no reason for the trust relationship*.

Data Collector Preference Settings

By default, XenApp uses the following *criteria to determine which server wins the election* and becomes the data collector:

- ❖ 1. Highest Host Record version.
 - ◆ Servers with the most recent XenApp software will have a Host Record of 1, which is the highest.
 - A XenApp 5.0 server with an election preference of **Default Preference** will win an election over a XenApp 4.5 server with an election preference of **Most Preferred** because the XenApp 5.0 server will have the highest Host Record.
- ❖ 2. Highest rank as configured in the XenApp Advanced Configuration tool.
 - ◆ Most Preferred (1)

- ◆ Preferred (2)
- ◆ Default Preference (3)
- ◆ Not Preferred (4)
 - A XenApp 5.0 server with an election preference of **Most Preferred** will win an election versus a XenApp 5.0 server with an election preference of **Preferred**.

3. In the event that multiple XenApp servers with the same XenApp software version (XenApp 5.0 for example) have the same election preference priority setting, the election winner will be determined by the server with the highest *Host ID number*, which is a *random number assigned to servers during XenApp installation*.

To *configure* data collector election settings for a server:

- ❖ In the left pane of the **XenApp Advanced Configuration** tool, select the farm.
- ❖ On the **Actions** menu, click **Properties**.
- ❖ Select **Zones**.
- ❖ In the list of zones and their servers, locate the server, select it and click **Set Election Preference**.

Issue: An administrator supports ten servers in a farm consisting of one zone. ServerA is the data collector, but the administrator wants to configure a less utilized server, ServerB, as the data collector. The administrator also wants to make sure that ServerA does not become the data collector.

Probable cause: By accident, the data collector election setting of ServerA, which hosts the most applications, was set to **Most Preferred**.

Solution: To configure ServerB as the data collector, the administrator should set ServerB's election preference to **Most Preferred**. To configure ServerA to never become the data collector, she should set ServerA's election preference to **Not Preferred**. After each setting she should *restart the IMA Service or reboot the server*.

QUERYHR is:

- ❖ A command line utility that allows an administrator to list and view all of the values of the servers in the server farm.
 - ◆ Including the *Host ID number*.

- A random number assigned to XenApp servers at installation to determine the data collector for a zone in case more than one XenApp server has the same election preference during a data collector election.

Create and Manage Data Store

Microsoft SQL Server, Oracle and IBM DB2 enterprise-level databases:

- ❖ Support replication.
- ❖ Are suitable for large farms.
- ❖ Should only be installed on a server that XenApp *will not* be installed on.

The user account that is used to access the data store on Microsoft SQL Server:

- ❖ Has *public* and *database owner (db_owner)* roles on the server and database.
 - ◆ *System administrator* account credentials are *not needed* for data store access;
 - Do not use a system administrator account as it poses a security risk.

Microsoft Access and SQL Server 2005 Express Edition SP1 databases:

- ❖ Do not support replication.
- ❖ Are better suited for smaller implementations.
 - ◆ Preferably located in one physical location.
- ❖ Require much less administration than enterprise-level databases.
- ❖ Can be installed on the same server as the first XenApp server in the farm.
 - ◆ If using Microsoft SQL Server Express, you must create the database on the same server on which you will install XenApp and *before you install XenApp*.
 - ◆ If using Microsoft Access, XenApp *automatically creates and configures* the database on the *first XenApp server* installed in the farm.

DSMAINT is used to perform XenApp data store maintenance tasks, including:

- ❖ Data store parameter changes, such as:
 - ◆ Password (**config /pwd**)

- ◆ Access database backup (**backup**)
- ◆ Access database compacting (**compactdb**)
- ◆ Migrating the database (**migrate**)
- ◆ Recreating and verifying the local host cache of XenApp servers (**recreatelhc** and **verifylhc**)
- ◆ Recreating the Application Streaming offline database (**recreaterade**)
- ◆ And much more...

DSCHECK:

- ❖ Validates the integrity of the data in the XenApp data store.
- ❖ Repairs any inconsistencies.
- ❖ Is often used after running **DSMAINT**.

Run **QUERYHR** to display information about member servers in a farm.

- ❖ Executing **QUERYHR** with no parameters lists all servers in the farm.

Run **QFARM /APP** to display the load for all applications and servers in the farm.

Run **QFARM /LOAD** to display the load for all servers in the server farm.

Run **QUERYDS** to view dynamic store tables.

- ❖ Shows the actual load along with the additional information as reported to the data collector.

Patching and Recovery

In XenApp 5.0, *Installation Manager* requires the following components:

- ❖ 1) *A task manager computer.*
 - ◆ The system on which the *Microsoft Management Console (MMC)* is installed and is used to manage and schedule tasks with the *Windows Task Scheduler*.
- ❖ 2) *A Windows file share (SMB) folder.*

- ◆ Located on any Windows server and is used to transfer task files to be deployed by Installation Manager and store cache files containing previously-scheduled tasks and results.
- ❖ 3) A *target server*.
 - ◆ The server on which tasks are deployed.
 - Must be a XenApp server *or* be running Windows Server 2008.

A *Microsoft Windows Installer Patch (.MSP)* file is a package format type created by a software manufacturer to *patch or update* installations that were *packaged using the Windows Installer Service*.

Following the creation of a task or operation using Windows Task Scheduler, an administrator can distribute the *task XML file* to a XenApp environment.

The ability to save and recall user's personalized settings on a XenApp server is available because of the *shadow key replication process*.

- ❖ XenApp creates a shadow key when an application is installed.
 - ◆ Installation Manager *eliminates the need for a shadow key* if the **Install MSI/MSP** option is used.

Hotfix Management

With *Hotfix Management*:

- ❖ *Check* which hotfixes are applicable to your Citrix products,
- ❖ *Search* for particular updates on your system
- ❖ *Identify servers* where up-to-date hotfixes must be applied.

To use Hotfix Management:

- ❖ In the **Access Management Console** left pane, select **Citrix Resources > Configuration Tools > Hotfix Management**.

Single- and Multi-Server Reboot Schedules

To schedule a *multi-server reboot*:

- ❖ In the left pane of the **Access Management Console**, select the **Servers** folder.
- ❖ In the **Contents** display in the right pane, press the **SHIFT** key and select the servers to restart.
- ❖ From the **Action** menu, choose **Select All Tasks > Set restart options > Set restart schedule**.
 - ◆ This starts the **Set Restart Schedule** wizard.
 - Use the wizard to configure your restart options.

To schedule a *single-server reboot*:

- ❖ In the left pane of the **Access Management Console**, select a server.
- ❖ From the **Action** menu, select **All Tasks > Modify server properties > Modify all properties**.
- ❖ In the **Server Properties** dialog box, select **Restart Schedule** and configure your restart options.

To *stop restarts* for servers that are scheduled to restart:

- ❖ In the **Access Management Console**, select the servers that you do not want to restart.
- ❖ In the center pane, select **Other Tasks > Set restart options > Disable restarts**.

Load Evaluators

Load evaluators can be assigned to:

- ❖ Servers
 - ◆ *All servers* must have a load evaluator applied to them.
 - Servers can only have one load evaluator applied to them at a time.
- ❖ Applications
 - ◆ *Each published application* must have only one load rule assigned to it.

Load evaluator rules:❖ *Moving Average rules:*

- ◆ **CPU Utilization** defines the range of processor utilization for a selected server.

- The default loads for the **CPU Utilization** rule:

- Full load is 90%.
- No load is 10%.

- ◆ **Memory Usage** defines the range of memory (RAM) usage for a server.

- The default loads for the **Memory Usage** rule:

- Full load is 90%.
- No load is 10%.

❖ *Moving Average Compared to High Threshold rules:*

- ◆ **Context Switches** defines the number of times the operating system is allowed to switch from one process to another.

- ◆ **Disk Data I/O** defines the range of data throughput in Kbps for a selected server.

- ◆ **Disk Operations** defines the range of disk operation (read and write cycles per second) for a selected server.

- ◆ **Load Throttling** limits the number of concurrent connection attempts a server is expected to handle.

- Must be attached to a server. *If it is attached to a published application, the rule is ignored.*

- ◆ **Page Fault** defines the range of page faults (transfers of data between physical memory and the page file) per second for a selected server.

- ◆ **Page Swap** defines the range of page swaps (transfers of data between physical memory and the page file) per second for a selected server.

❖ *Incremental rules:*

- ◆ **Application User Load** limits the number of users allowed to connect to a selected hosted or streamed application.

- Monitors the number of active and disconnected sessions using the hosted or streamed application.
- ◆ **Server User Load** limits the number of sessions allowed to connect to a selected server.
 - *Cannot be applied to an individual application.*
- ❖ *Boolean* rules are based on conditions being true or false and must be used in conjunction with at least one other rule because they do not return actual load values for a server:
 - ◆ **IP Range** defines the range of allowed or denied client IP addresses for a published application.
 - ◆ **Scheduling** schedules the availability of selected published applications.

Load evaluators:

- ❖ The *Default load evaluator* is based on the following rules:
 - ◆ **Load Throttling**
 - ◆ **Server User Load**
- ❖ The *Advanced load evaluator* is based on the following rules:
 - ◆ **CPU Utilization**
 - ◆ **Memory Usage**
 - ◆ **Load Throttling**
 - ◆ **Page Swap**

A custom load evaluator:

- ❖ May be created by an administrator if the Default or Advanced load evaluators are not adequate.
 - ◆ *Create a new load evaluator or copy and existing load evaluator and modify it.*

To create a custom load evaluator:

- ❖ Open the **XenApp Advanced Configuration** tool, right-click the **Load Evaluators** node and click **New Load Evaluator**.

- ❖ Type the name for the custom load evaluator in the **Name** field.
- ❖ Optionally, type a description in the **Description** field.
- ❖ Click a rule in the **Available Rules** list and click **Add**.
- ❖ Configure the parameters for the selected rule and click **OK**.

When *creating a custom load evaluator*:

- ❖ The *full load threshold value* should be *set below* the value determined as the *maximum sever load*.
 - ◆ To determine the *maximum server load*, an administrator must first *determine the baseline and peak values* for key metrics on the server.

To *copy an existing load evaluator*:

- ❖ Open the **XenApp Advanced Configuration** tool and click the **Load Evaluators** node.
- ❖ Right-click the load evaluator in the **Contents** tab.
- ❖ Click **Duplicate Load Evaluator**.
- ❖ Optionally, type the name for the custom load evaluator in the **Name** field.
- ❖ Optionally, type a description in the **Description** field if desired.
- ❖ Customize the load evaluator by removing an existing rule from the **Assigned Rules** field or adding a rule from the **Applications Rules** field.
- ❖ Configure parameters for the newly added rules and click **OK**.

Virtual Memory Optimization

Schedule virtual memory optimization at a time when your servers have their lightest loads.

Configuring Printing

Printer Types

In *local printing*:

- ❖ Print jobs are spooled *directly on the Windows device*.
 - ◆ Can be a *client device or a server*.
- ❖ Local printers can be connected:
 - ◆ To a client device or a server *by local ports*.
 - Such as *LPT* and *USB*
 - ◆ To *network ports*.
 - Such as *TCP* and *SMB*.

In *network printing*:

- ❖ Print jobs are spooled *directly onto the remote print server*.
- ❖ Network printers can be connected:
 - ◆ To a print server *by local ports*.
 - Such as *LPT* and *USB*.
 - ◆ To network ports.
 - Such as *TCP* and *SMB*.

In *redirected client printing*:

- ❖ Print jobs are spooled *on the XenApp server and routed over the ICA connection to the client-side print device*.
 - ◆ Redirected client printers can be connected:
 - ◆ To a client device or a server *by local ports*.
 - Such as *LPT* and *USB*.
 - ◆ To network ports.

- Such as *TCP* and *SMB*.

Universal Print Driver and Native Drivers

The policy rule **Native driver auto-install**:

- ❖ With the setting **Install Windows native drivers as needed**.
 - ◆ Allows the *manufacturer's print drivers* to be used in the farm.

The policy rule **Universal driver**:

- ❖ With the setting **Use universal driver only if requested driver is unavailable**.
 - ◆ Allows the drivers to *first try to use the manufacturer's drivers*, but if they are *not available*, the *universal driver will be a fallback*.
- ❖ With the setting **Use only printer model specific drivers**.
 - ◆ Allows *only the manufacturer's drivers* to be used in the farm.

The *print driver compatibility list* allows an administrator to control print drivers available to users.

- ❖ During user logon, *native drivers are permitted* and the auto-created printers are *checked against the list of allowed or denied print drivers*.

Benefits of the universal print driver:

- ❖ *Reduces the size* of some print jobs.
- ❖ Allows jobs to *print faster*.
- ❖ Allows users to *set printer properties* and *preview documents* ready for printing.
- ❖ *Reduces load* on the server and *bandwidth* and *CPU processing* are saved.
- ❖ *Reduces delays* when spooling over slow connections.
- ❖ *Avoids more problems* in a diverse environment.
- ❖ *Limits the installation and duplication of print drivers* on servers.

- ❖ *Ensures that client printers auto-create regardless of print driver availability on the server.*
- ❖ *Minimizes Help Desk calls.*
- ❖ *Enables users to print to almost any printer.*
- ❖ *Redirects client printers only.*

Some *native and universal print driver best practices*:

- ❖ *By not allowing native print drivers to automatically be installed from auto-created printers, you can guarantee that no rogue drivers make it into the farm.*
- ❖ *By using a driver compatibility list, you can control which drivers are allowed in the farm.*
 - ◆ *Since you don't know always know which drivers might try to install in your server farm, use the setting **Allow only drivers in the list** and adds the known acceptable drivers to the list.*
- ❖ *By selecting the policy rule **Universal driver** setting **Use universal driver only if the requested driver is unavailable** rule, you guarantee there is always a driver available, whether it's the manufacturer's driver or the universal driver.*

Universal XPS Printer Driver

The *Universal XPS Printer Driver* is based on Microsoft's XPS (XML Paper Specification) technology, which uses platform-independent XML for a product that is similar to Adobe's Acrobat.

- ❖ XPS technology was introduced in Windows Server 2008.

Client devices *must have .NET 3.0* installed on them to use the Citrix Universal XPS Printer driver.

- ❖ .NET 3.0 comes with Windows Vista.

Install and Replicate Drivers

Before a printer can be used, a *print driver must be installed* on the XenApp server.

To *add, remove and reinstall* print drivers on a server:

- ❖ Use the **Drivers** utility on a Windows Server by going to **Printers > File > Server Properties > Drivers**.

To make the print driver available on other servers in the server farm an administrator can leverage *print driver replication* to deploy the print driver to all member servers.

- ❖ Print driver replication requires that *the driver be installed and available on one server per base operating system*.
- ❖ The driver replication process can *take a considerable amount of time* and requires a *substantial amount of system resources*.
 - ◆ Because of these resource requirements, the *replication should be performed during off-peak hours* when higher priority traffic is not impacted.

Auto-replication list:

- ❖ Created using the XenApp Advanced Configuration tool.
- ❖ If a *server is added to the server farm that does not have the print driver detected, the driver is installed*.

To create a driver auto-replication list:

- ❖ Expand the **Printer Management** node in the **XenApp Advanced Configuration** tool.
- ❖ Right-click **Drivers**.
- ❖ Select **Auto-replication**.
- ❖ In the **Auto-replication** dialog box, select the appropriate operating system platform from the **Platform** drop-down list.
- ❖ Click **Add** to add a print driver to replicate for the selected platform.
- ❖ Select the appropriate source server in the **Server** drop-down list.
 - ◆ If no specific source is required, the **Any** option can be used to list all print drivers available on all servers in the farm.
- ❖ Optionally, select **Overwrite existing drivers** and click **OK** in the confirmation if **Any** was chosen as the source server.
- ❖ Click **OK** in the **Auto-replication** dialog box.
- ❖ Click **OK** in the replication queue confirmation message.

Printing Policies

Legacy client printers enables the use of *old-style client printer names* as used by Terminal Services or Presentation Server versions prior to 4.0.

Printer properties retention controls whether or not *printer properties are stored on the client device or the user profile* on the server.

Print job routing controls whether or not *network print jobs flow directly from XenApp to the print server or takes an extra step and are routed back through the client device*.

Turn off client printer mapping *disables the mapping of all client printers*.

Session printers allows an administrator to *control the assignment of network printers*.

- ❖ Administrators can *assign the default printer as well as designate the connection to network printers based on the desired policy filter*.
- ◆ Many times **Session printers** is filtered by IP address so that the *IP range of the computers determines the print devices that are available* on each level of a building.

Troubleshoot Printing

Issue: Other departments have started complaining that the Sales users are tying up their printers.

Probable cause: All of the users in the Sales department have several network printers configured on their client devices. They have been printing to print devices in other departments.

Solution: The **Session printers** policy rule allows an administrator to control the assignment of network printers *based on specific attributes of user sessions*. Allow the Sales users to only connect to the network printers in their area by configuring the **Session printers** policy rule.

Issue: The users in the Reporting department often complain that they have to make several attempts before they can see their printers on their client device, so they have to wait to print.

Probable cause: The Reporting group uses several applications and does a lot of printing. Sometimes they require printing from an application immediately after opening it.

Solution: An administrator configures *synchronous printer creation* for the applications in the Reporting department so that all printers will be created first *before the users have access to interact with and use their sessions*.

Issue: The Reporting department is complaining about slow logon times.

Probable cause: Each person in the Reporting department has their own print device connected to their client device and that printer is configured as the default printer. They also have ten network printers on their floor which are all configured on their client device.

Solution: By creating a policy with **Auto-create client's default printer only**, logon times will be sped up because the client devices will no longer try to connect to and auto-create the ten network print devices on the Reporting department's floor.

Issue: The Reporting department is complaining about applications running slow. The applications that they are complaining about are published applications in the server farm.

Probable cause: The Reporting department is in a remote office that connects to the server farm over a WAN which has become quite congested with network traffic.

Solution: The administrator has already optimally configured printer auto-creation and print job routing. *Applying a printer bandwidth policy* will allow the administrator to *control the amount of maximum bandwidth* in kilobytes per second that may be *used for printing*. This will *free up some bandwidth* for other resources, including applications, using the WAN link.

Test New Print Drivers

StressPrinters:

- ❖ Is a tool that can be used to *simulate multiple sessions of auto-creating printers* using the *same print driver*.
- ❖ Can be used to *compare CPU load and time required* while creating a printer *using a particular driver*.

Auto-Created and Networked Printers

By using the rule **Auto-create local (non-network) client printers only:**

- ❖ Only the printers *connected directly to the user's client device* through an LPT or other local port will be *automatically connected*.
- ❖ Enabling this setting *ensures any network printers defined on the client device are not auto-created* within the ICA session.
 - ◆ *Logon times will be reduced* for those who have several network printers configured on their client device.

Auto-creation enables the auto-creation of either:

- ❖ All client printers
- ❖ Local client printers
- ❖ Default client printers
- ❖ No client printers

Print job routing *determines* whether or not a client *printer is auto-connected*.

Auto-create all client printers automatically connects all the printers on a client device.

Connect directly to network print server if possible routes the print jobs *directly from the XenApp server to the network print server*.

Always connect indirectly as a client printer routes print jobs through the client device, where it is redirected to the network print server.

- ❖ Data sent to the client device is *compressed using the ICA protocol*; therefore, *less bandwidth* is consumed as the data travels across the WAN.

Turn off client printer mapping to auto-create *only network printers or printers connected directly to the server*.

- ❖ In some instances, it might be preferable to not auto-create client printers.

With *synchronous printer creation*:

- ❖ Printers create before the users have access to interact with and use their sessions.
- ❖ The users must wait for all printers to create in the background before they can perform any activities.
- ❖ Is enabled by deselecting the **Start this application without waiting for printers to be created** option in the application properties.

With *asynchronous printer creation*:

- ❖ *Printers create in the background* while the users have control of and are using their sessions.
- ❖ *Minimizes the amount of time* it takes for the users to begin using the application.
- ❖ Asynchronous printer creation is enabled by selecting the **Start this application without waiting for printers to be created** option in the application properties.

Importing a Print Server

To import a print server:

- ❖ In the **XenApp Advanced Configuration** tool, right-click **Printer Management** and click **Import Network Print Server**.
- ❖ In the **Network Print Server** dialog box, type the name or IP address of the print server in the **Server** field.
- ❖ Type a user account name that has access rights to the specified printer in the **Connected As** field.
- ❖ Type the password for the user account in the **Password** field and click **OK**.

Print Driver Mapping

A *print driver mapping list* should be created to *resolve compatibility issues* between print drivers that have *different names for the same printer* on different server operating systems.

An administrator can configure:

- ❖ The file **WTSUPRN.INF** to map printer drivers for a *specific server*.
- ❖ The **XenApp Advanced Configuration** tool to map printer drivers for *all servers in the farm*.

The **WTSPRNT.INF** file lists the print driver mappings made using the XenApp Advanced Configuration tool and *should not be edited*.

- ❖ The administrator can *edit the WTSUPRN.INF file*.

Troubleshooting XenApp

XenApp Services

If the user account for direct mode access to the database is changed at a later time:

- ❖ The Citrix IMA Service will fail to start on all servers configured with that account.
- ❖ To *reconfigure the Citrix IMA Service password*, use the **DSMAINT CONFIG** command on each affected server.

An administrator can use **CTXXMLSS** to *change the Citrix XML Service port number*.

If the port that is used by Session Reliability (default port 2598) is not responding:

- ❖ The administrator should *troubleshoot the Citrix XTE Service* to resolve the issue.
 - ◆ *Session Reliability uses the Citrix XTE Service to operate.*

To find out what ports and services are being used on a server, type **NETSTAT -a**.

If the *IMA Service is not responding*, it may be from a *corrupted Local Host Cache*.

- ❖ Run **DSMAINT /recreatelhc** to *recreate the local host cache database* on the XenApp server on which it is run.

XenApp Troubleshooting Tools

Citrix provides a standard set of *Health Monitoring and Recovery tests*:

- ❖ Microsoft Print Spooler Service test
- ❖ Citrix IMA Service test
- ❖ Check DNS test
- ❖ Citrix XML Service test
- ❖ Logon Monitor test
- ❖ Check Local Host Cache test
- ❖ Check XML Threads test
- ❖ Check Print Manager Service test
- ❖ Terminal Services test
- ❖ ICA Listener test.
 - ◆ You can also develop your own tests using the Health Monitoring and Recovery SDK.

If a Health Monitoring and Recovery test *identifies an issue with a server*, one of the following *actions can be taken*:

- ❖ **Alert Only**
 - ◆ Allows new connections.

❖ **Remove Server from Load Balancing**

- ◆ Keeps current connections to the server but does not allow new connections.

❖ **Shutdown IMA**

- ◆ Terminates all of the existing sessions.

❖ **Restart IMA**

- ◆ Terminates all of the existing sessions.

❖ **Reboot Server**

- ◆ Terminates all of the existing sessions.

RDP Troubleshooting Tool

Use the RDP command line tool, *mstsc* (Terminal Services Configuration) to *troubleshoot ICA connection problems* by attempting to connect to Terminal Services.

With *mstsc*, an administrator can:

- ❖ *Enable and disable ICA connections.*
- ❖ *Set security permissions for ICA connections.*
- ❖ *Configure:*
 - ◆ Client settings
 - ◆ Session settings
 - ◆ ICA settings

Client Connectivity Troubleshooting using Telnet

To find out if a port is reachable or not:

- ❖ Use the network command **Telnet** followed by the *hostname or IP address* and the *port number* you want to reach.
 - ◆ Examples:

- **telnet 192.168.55.109 2598** (for the Session Reliability port)
- **telnet ctxserver55 1494** (for the ICA port)