

**Citrixxperience.com**

**1Y0-264 Citrix XenApp (Presentation  
Server 4.5): Support**

**Study Guide**

**Version 1.0**

(March 7, 2009)

## 1Y0-264 Citrix XenApp (Presentation Server 4.5): Support 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: 1Y0-264 Exam Enablement Guide, CTX-1264AI Citrix XenApp (Presentation Server 4.5): Support Courseware, CTX-1259AI Citrix Presentation Server 4.5: Administration Courseware, Citrix Presentation Server 4.5 Administrator's Guide, Citrix Knowledge Center Articles, Monitoring Server Performance with Citrix Presentation Server, Citrix Smart Auditor for Presentation Server 4.5 Guide, Licensing: Troubleshooting Guide, Secure Gateway for Windows Administrator's Guide, Web Interface 4.5 Administrator's Guide, Presentation Server 4.5 Application Streaming Delivery and Profiling Best Practices, Application Streaming with Citrix Presentation Server Implementation Guide and Citrix Application Streaming Guide for Presentation Server 4.5.

Along with the materials listed above, this study guide is meant to be used in preparation for the 1Y0-264 Citrix XenApp (Presentation Server 4.5): Support 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 1Y0-264 products found at [www.Citrixexperience.com](http://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

---

<b><u>Subject</u></b>	<b><u>Page</u></b>
Monitoring, Managing and Maintaining the Environment	1
Troubleshooting	9
Optimizing the Environment	26

## Monitoring, Managing and Maintaining the Environment

---

### Configuration Logging

The *Configuration Logging* feature allows you to keep track of administrative changes made to your server farm environment.

By generating the reports that this with Configuration Logging, you can determine:

- ❖ *What* changes were made to your server farm.
- ❖ *When* the changes were made.
- ❖ *Which* administrators made the changes.
  - ◆ This is especially useful when *multiple administrators are modifying* the configuration of your server farm.
  - ◆ It also facilitates the identification and, if necessary, *reversion of administrative changes* that may be *causing problems for the server farm*.

To find out the *maximum number of concurrent users* a published application had over a period of time, an administrator should generate an **Application Usage** report.

### Web Interface / XML Connection Issues

When users are having problems connecting to the Presentation Server farm through Web Interface, unless there is another known network problem going on at the time that is affecting everything, a *likely cause is an issue with the XML Service* on one of the Presentation Servers.

Users of *Web Interface* who are *attempting to log in with Smart Cards* may receive a message to the effect that the *request is too large*:

- ❖ The Citrix *XML Service* *limits requests to 4096 KB* in order to prevent security problems.
  - ◆ The desktop credentials *pass-through authentication* feature works by sending the user group membership to the *XML Service*.
- ❖ If a user belongs to a *large number of groups*, all of their group SID's may exceed *4096KB*.
- ❖ *A Hotfix will fix this issue.*

---

*Issue:* Some users who connect to their published applications *through Web Interface* are experiencing connection problems; others are connecting just fine.

*Probable cause:* When users are having problems connecting to the Presentation Server farm through Web Interface, unless there is another known network problem going on at the time that is affecting everything, a *likely cause is an issue with the XML Service* on one of the Presentation Servers.

*Solution:* An administrator should *investigate the XML Service* on all of the load balanced servers in the farm that those particular users are trying to connect to.

## **Alerts**

Both *yellow (warning)* and *red (error)* alerts occur when the value for a metric *falls outside of the normal limits* and *remains there* for a defined period of time.

When a *critical alert* appears for a *Farm Metric Server*:

- ❖ The summary database software version for the primary Farm Metric Server is not accepted because *another server in the server farm has a later version* of Presentation Server installed.
- ❖ You need to *upgrade Presentation Server* on the primary Farm Metric Server.

When a *critical alert* appears for a *Database Connection Server*:

- ❖ The summary database software version for the Database Connection Server is not accepted because *another server in the server farm has a later version* of Presentation Server installed.
- ❖ You need to *upgrade Presentation Server* on the Database Connection Server.

If an administrator sees **Unreachable alert** in the Access Management Console, this could mean that the *MFCOM Service is not running* on the server used to discover the farm.

## **SmartAuditor**

*SmartAuditor:*

- ❖ Allows you to record *any user's session, over any type of connection, from any Presentation Server*.
- ❖ Recorded sessions are *cataloged and archived for retrieval and playback*.
- ❖ Available *only* in the Citrix Presentation Server *Platinum Edition*.
- ❖ SmartAuditor uses flexible policies to *automatically trigger recordings of Presentation Server sessions*.

- ◆ Enables IT to *monitor and examine user activity of applications* – such as financial operations and healthcare patient information systems – demonstrating internal control.
- ◆ Ensures *regulatory compliance* and successful *security audits*.
- ◆ Aids in technical support by *speeding problem identification* and time-to-resolution.

### **Citrix Suite Monitoring and Alerting (SMA) Service**

*Citrix Suite Monitoring and Alerting (SMA) Service:*

- ❖ *Watches the event log and the Citrix WMI for issues.*
- ❖ *Raises alerts in the Access Management Console.*

### **ADF Installer Service**

The *ADF Installer Service* must be installed and enabled so that the packages that were created with the *Installation Manager Packager* can be installed on the target servers.

### **Licensing Ports**

When a *firewall sits between the Citrix License Server and the Presentation Server farm*, the firewall needs to be configured to *allow the License Manager daemon and the Citrix vendor daemon* communicate with the server farm:

- ❖ By default, the license server has two daemons that are used in the license check in and check out process:
  - ◆ The License Manager daemon.
    - Uses port *27000*.
  - ◆ The Citrix vendor daemon.
    - Uses a *random* port.
- ❖ To prevent licensing communication issues, an administrator needs to:
  - ◆ Configure the Citrix vendor daemon with a *static port* and open the configured port on the firewall.
  - ◆ Open port 27000 on the firewall for the License Manager daemon.

## **License Server Administration**

If you *change the port* number that the *license server* communicates over, you must specify the *new port number* in *all license files* on the server.

If you *change the license server name*, you must *download a newly generated license file*.

- ❖ This may involve returning and reallocating the licenses at MyCitrix.

## **Health and Monitoring Recovery Tests**

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

- ❖ **Alert Only**
  - ◆ *Does not disturb connected users and allows new connections* to the server.
- ❖ **Remove Server from Load Balancing**
  - ◆ Use this when a Health Monitoring and Recovery test is *continuously sending an alert* to the Event Log because a *test has failed* and *users are connected* to the server so you *do not want to disrupt those connections* but you need to *disallow new connections* to the server.
  - ◆ Depending on whether it's *for all servers or just a select server*, this action can be configured in the *properties of the server or the server farm*.
- ❖ **Shutdown IMA**
  - ◆ *Disconnects all ICA sessions and does not allow new connections*.
- ❖ **Restart IMA**
  - ◆ *Disconnects all ICA sessions and does not allow new connections until the IMA Service is started*.
- ❖ **Reboot Server**
  - ◆ *Disconnects all ICA sessions and does not allow new connections until the IMA Service is started*.

When a Systems Administrator needs to create a *custom Health and Monitoring Recovery test*, the administrator will use the executable **HRMSDKTESTER.EXE**.

## **Session Reliability**

*Session Reliability:*

- ❖ Provided by the *Citrix XTE Service*.
- ❖ Through the *Common Gateway Protocol*.
- ❖ On port *2598*.

## **Ports**

SNMP uses UDP 161 and 162.

Server-to-server communication using the IMA Service uses 2512.

Access Management Console uses 135.

Citrix SSL Relay uses 443.

ICA sessions use 1494.

Client-to-server UDP sessions use 1604.

Session Reliability uses 2598.

The License Management Console uses 8082.

License server to Presentation Server communication uses 27000.

Hewlett Packard and other printers print using 9100.

Presentation Server to IBM DB2 database uses 5000.

Presentation Server to Oracle database uses 5000.

Presentation Server to Microsoft SQL database uses 1433.

## **Port Considerations**

If there is a *firewall sitting between the Presentation Servers* and the administrators using the *Presentation Server Console*, be sure and *open port 2513* to allow those administrators to manage and configure the Presentation Servers via the Presentation Server Console.

When a *Presentation Server client* attempts to launch an application, it *establishes a connection to the listener over port 1494*.

- ❖ The *default port* on servers for *inbound traffic* from ICA sessions is 1494.
- ❖ The *outbound port* from the server used for the ICA session is *allocated dynamically* when the session is established.
- ❖ If *Session Reliability* is in use, a connection will instead be established with the *Citrix XTE Service over port 2598*.
  - ◆ Like ICA traffic, the designated port is used *for inbound sessions* to Presentation Server, and a *dynamically allocated port is used for outbound traffic*.
- ❖ Ports 1494 and 2598 should be opened *only* to internal inbound traffic.
- ❖ Sessions originating from *clients connecting over the Internet* should be secured by means of the *Secure Gateway or Access Gateway*.

### **Database Migration**

To move data from an Access database to a Microsoft SQL database use **DSMAINT MIGRATE**.

- ❖ This command *moves data from one data store database to another*.
- ❖ It can also be used to *move a data store* to a different server or *rename a data store*.

Use the following *steps to migrate from Access to Microsoft SQL Server*:

- ❖ 1. *Create a new database* on Microsoft SQL Server.
- ❖ 2. *Create a new Mf20.dsn file pointing to the new SQL Server database*.
- ❖ 3. *On the database server, execute the DSMAINT MIGRATE command*.
  - ◆ Enter the *current DSN file as the source* and the *new DSN file created in Step 2 as the destination*.
- ❖ 4. Execute **DSMAINT CONFIG** on *the original host server (Access server)* to point to the new DSN file.
- ❖ 5. Stop and *restart the IMA Service on the host server*.
  - ◆ When the IMA Service on the host server is restarted, the remaining indirect servers begin accessing the new data store indirectly through the host server.
- ❖ 6. *Copy the DSN file created in Step 2 to all remaining indirect servers in the farm*.

- ❖ 7. Execute **DSMAINT CONFIG** on *all remaining indirect servers* to establish a direct connection to the new database through the DSN copied in Step 6.
- ❖ 8. Stop and *restart the IMA Service on all remaining indirect servers* in the farm.

When migrating a database using **DSMAINT MIGRATE**, such as an Access database to Microsoft SQL Server, enter the full path of the DSN file.

- ❖ For example: **C:\SQL\Citrix\IMA\Mf20.dsn**

If the *path contains spaces*, use *quotation marks*.

- ❖ For example: **"C:\Program Files\Citrix\Independent Management Architecture\Mf20.dsn"**

### **Database Replication**

To allow an *existing Microsoft SQL database* to be *replicated* use **DSMAINT PUBLISHSQLDS**.

- ❖ This command publishes a Microsoft SQL data store to allow replication.

### **Database Backup and Recovery**

To *restore a Microsoft SQL or Oracle data store database* from backup:

- ❖ 1. *Restore the database.*
- ❖ 2. Create a *new DSN file* that points to the restored database.
- ❖ 3. Execute the **DSMAINT CONFIG** command on the server with the new DSN file.
- ❖ 4. Stop and *restart the IMA Service.*
- ❖ 5. *Verify that the server is using the correct DSN* by checking at the following registry setting: **HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\IMA\DataSourceName**
- ❖ 6. If the IMA Service started successfully, *copy the DSN file created in Step 2 to all Presentation Servers in the farm and update each server's registry.*
- ❖ 7. Execute the **DSMAINT CONFIG** command to change the IMA service configuration on all servers in the farm.
- ❖ 8. Stop and restart the IMA service on all servers in the farm.

When restoring a Microsoft SQL database to a new server:

- ❖ On the **Options** page, select **Overwrite the existing database**.
  - ◆ This way you avoid receiving a **Restore failed** error.

## **ICACLIENT.ADM**

**ICACLIENT.ADM** is a Citrix-provided GPO that contains rules for connection parameters.

To *allow or deny a Presentation Server client from connecting to a Presentation Server*, configure the **Trusted server configuration** rule in **ICACLIENT.ADM**.

Four connection settings contain all of the **ICACLIENT.ADM** rules:

- ❖ **1. Network routing**
  - ◆ **TLS/SSL data encryption and server identification**
  - ◆ **Configure trusted server configuration**
  - ◆ **Session reliability and automatic reconnection**
  - ◆ **Configure client proxy settings**
  - ◆ **Configure client failover proxy settings**
  - ◆ **Configure SOCKS proxy settings**
  - ◆ **Configure proxy authentication**
- ❖ **2. User authentication**
  - ◆ **Smart card authentication**
  - ◆ **Kerberos authentication**
  - ◆ **Local user name and password**
  - ◆ **Locally stored credentials**
  - ◆ **Web Interface authentication ticket**
- ❖ **3. Remoting client devices**

- ◆ Client drive mapping
- ◆ Client printers
- ◆ Client hardware access
- ◆ Image capture
- ◆ Client microphone
- ◆ Clipboard
- ❖ 4. User experience
  - ◆ Client audio settings
  - ◆ Client graphics settings
  - ◆ Client display settings
  - ◆ Remote applications

## Troubleshooting

---

### Driver Best Practices

To keep a driver from crashing the Citrix Print Manager Service (CPSVC.EXE), use the following best practices:

- ❖ Use *native Windows* drivers or the *Citrix universal print driver*.
- ❖ Use driver *mapping* to native drivers.
- ❖ See CTX089874 Troubleshooting and Explaining the Citrix Universal Print Driver.
- ❖ *Avoid updating* a driver.
  - ◆ Always *attempt to uninstall a driver, restart, and then install* the new/replacement driver.
- ❖ *Unused drivers* should be *uninstalled or restricted* within the Presentation Server Console.
- ❖ Try to *avoid using version 2 kernel-mode drivers*.

- ❖ Give users write access to **<root directory>\system\spool** to handle third-party printer drivers that are not 100 percent Terminal Server-aware.
- ❖ Try avoiding third-party *PCL6 drivers*.
  - ◆ It is preferable to *use PCL5 or PS*.
  - ◆ *Never install untested printer drivers in a production environment.*
  - ◆ Do not install *all* native printer drivers on the server.
    - This causes *unneeded growth* of the data store.
    - Will *slow down* logon performance.
  - ◆ *Don't try to fight problems by scheduled spooler restarts and spool directory cleanups during a server restart.*
    - Find the *source* of the problems and *fix* them.

### **Session Printers Policy**

The **Session printers** policy rule is used to *assign network printers* to users.

- ❖ Can assign the *default printer*.
- ❖ *Designate* the connection to network printers based on the *desired policy filter*.

---

*Issue:* Users are complaining that users from another department are tying up their printers.

*Probable cause:* Users from the other department have several network printers configured on their client devices. They have been printing to print devices in departments other than their own.

*Solution:* Allow each user to only connect to the network printers in their area by assigning network printers using the **Session printers** policy rule and filtering the policy by users and groups.

---

*Issue:* Users need to be able to print from a nearby print device no matter which floor of the building they are on. Of course, they must use the same login credentials no matter which computer they are working on. The IT department needs to assign the IP range of the computers on each level of the building so when a user is on the fifth floor they will have access to the fifth floor printers and when they have to move to floor two, they will have access to the second floor printers, etc.

*Probable cause:* Several users in the company have to work on different floors of the building and different client devices throughout the day.

*Solution:* The **Session printers** policy rule filtered by IP address allows an administrator to control the assignment of network printers.

### **Print Job Routing Policy**

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

- ❖ When the rule is configured to **Connect directly to network print server if possible**, the print jobs are *routed directly from the Presentation Server to the network print server.*
- ❖ When **Always connect indirectly as a client printer** is configured, print jobs are *routed through the client device via the ICA protocol and redirected to the network print server.*

---

*Issue:* Users that usually work on the second floor of a building often work with other users on the eighth floor. They still need to print to their printers on the second floor to allow their assistants to receive the print jobs. The assistants are complaining that *print jobs are taking a long time to print.*

*Probable cause:* The second floor and eighth floor are on *different subnets* and sending a print job to a different subnet *makes printing slow.*

*Solution:* Configure **Print job routing** in a policy with the rule **Connect directly to network print server if possible** enabled. *Routing print jobs directly to the print server can increase printing speeds* for LAN users.

### **Native Printer Drivers**

Printer policy rule **Native printer driver auto-install:**

- ❖ The setting **Install Windows native drivers as needed** is selected by *default.*
  - ◆ Because of this, there is a potential of a *large number of undesired print drivers to be installed in the farm.*
    - An administrator can *limit which drivers are installed* by using the *driver compatibility list.*
    - Change the rule setting to **Do not automatically install drivers** to make sure that *no rogue drivers* make it into the farm.

## **Driver Compatibility**

The *print driver compatibility list* allows an administrator to *control print drivers available* in the farm.

- ❖ During user logon, *native drivers are permitted* and the *auto-created printers are checked* against the list of allowed or denied print drivers.
- ❖ Select **Allow only drivers in the list** and add the acceptable drivers to the list if drivers that are allowed are known.
- ❖ Select **Allow drivers except those in the list** and add the unacceptable drivers to the list if drivers that are not allowed are known.

## **Print Driver Mapping**

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

---

*Scenario:* A print driver was installed in the server farm with the name **HP LaserJet 4**. Some users on an older Windows operating system have the same print driver, but it was installed with the name **HP LaserJet 4/4M**. The printer is not auto-creating for the users with the older operating system.

*Resolution:* To make sure that the printer auto-creates in the users' sessions, a print driver mapping list is used to resolve compatibility issues between print drivers that have different names for the same printer on different server operating systems.

---

To map print driver names:

- ❖ In the Presentation Server Console, expand the **Printer Management** node.
- ❖ Right-click the **Drivers** node.
- ❖ Select **Mapping**.
- ❖ The **Driver Mapping** dialog appears.
- ❖ Select the appropriate operating system from the **Platform** drop-down list.
- ❖ The **Add Mappings** dialog appears.
- ❖ Type the name of the client print driver in the **Client Driver** field.

- ❖ Select the name of the print driver from the **Server Driver** drop-down list and click **OK** to add the mapping.
- ❖ Click **OK** to close the **Driver Mapping** dialog.

### **Driver Availability**

Make sure there is *always a printer driver available*, whether it's the manufacturer's driver or the universal driver by selecting the **Use universal driver only if the requested driver is unavailable** rule.

### **Auto-Created Printers Not Deleting**

*Auto-created printers may fail to delete* after the user logs off for many different reasons:

- ❖ The *spooler service may not be working* or was not working properly upon logoff.
  - ◆ This may require the *manual deletion* of printer objects from the *server's registry* and the restarting of the print spooler service.
  - ◆ **HKLM\System\CurrentControlSet\Control\Print\Printers**
- ❖ *Print jobs were pending* in the print queue.
  - ◆ They were *not set to delete at logoff* and/or users could not delete ending jobs before logoff.
- ❖ Citrix uses the comment field of an auto-created printer to determine if this printer object should be deleted at logoff and there is *no comment field or the comment field was altered*.
- ❖ The *session is in a disconnect state* and/or the *users profile has not unloaded* successfully.
- ❖ Auto-created printers created using the *legacy naming style* might not be deleted when a session is terminated.
  - ◆ The issue occurs if the *Print Spooler and Citrix Print Manager Service* restart while a *session is active* on the server.
- ❖ *Auto-created printers* that no longer have an associated session are *not deleted* when the Citrix Print Service (*CPSVC*) restarts.

## **Session Reliability**

When Session Reliability is being used:

- ❖ This feature is designed to be convenient to the user because it *does not prompt the user for re-authentication*.
- ❖ Session Reliability has a *default of 180 seconds*, or three minutes.
- ❖ If *users are consistently losing their connections before the session becomes active again*, the **Seconds to keep sessions active** option needs to be extended.

## **Session Reliability Not Responding**

*Issue:* The port used by Session Reliability is not responding.

*Probable cause:* Session Reliability uses the Citrix XTE Service to operate.

*Solution:* The administrator should troubleshoot the Citrix XTE Service to resolve the issue.

## **SSL Relay with Web Interface**

Two steps to take for *SSL Relay configuration* for secure Web Interface to Presentation Server communication:

- ❖ Install a *root certificate* on the *Web Interface server*.
- ❖ Configure the *Presentation Server* to listen on *TCP port 443*.

## **Smart Cards with Web Interface**

To allow the use of smart cards with Web Interface:

- ❖ 1. Install the *Client for Windows on all client devices*.
  - ◆ *Web Client cannot be used* for smart cards because of security concerns.
- ❖ 2. Enable *pass-through on the client*.
- ❖ 3. Enable the *Windows Directory Service Mapper on the Web Interface server* so that authentication can be handled by Active Directory.
- ❖ 4. Enable *smart card authentication in Web Interface*.

## **Application Streaming with Web Interface**

Application streaming can be configured through Web Interface with the settings:

- ❖ **Streaming**
  - ◆ Users stream applications to their *desktop* and launch them *locally*.
- ❖ **Dual Mode Streaming**
  - ◆ Users stream applications to their *desktop* and launch them locally, but if streamed applications are *not available*, *remote versions* are launched.
- ❖ **Remote**
  - ◆ Users access published applications installed on a *remote server*.

## **Workspace Control**

*Workspace control* allows users to quickly disconnect all running applications, reconnect to disconnected applications, and log off from all running applications.

- ❖ This allows users to *move between client devices* and gain *access to all of their applications* either when they log on or manually at any time.
- ❖ Users running applications using Workspace Control *cannot reconnect* to their applications when they *manually log off*.
- ❖ When the *HTTP session times out*, users can *log in and reconnect* to their launched applications.
- ❖ Workspace Control *only works with remote applications*, not streamed.

## **IMA Service**

To troubleshoot the *IMA Service failure to start condition*:

- ❖ Examine the **CurrentlyLoadingPlugin** for its value.
- ❖ *Verify that ODBC connectivity exists* when connecting directly to the data store.
- ❖ *Verify the IMA Service is running* on the server that is connecting directly to the data store when connecting to the data store through an intermediary server.

- ❖ *Review the entries in the event log* for the IMA Service error code that is returned.
  - ❖ *Review alerts* in Resource Manager and the Access Management Console.
  - ❖ *Verify the Print Spooler Service* is started in the *System context* rather than for a user.
- 

*Scenario:* The IMA Service failed to start on a Presentation Server that is directly connected to the data store.

*Resolution:* Verify that ODBC connectivity exists.

---

*Scenario:* The IMA Service fails to start on a Presentation Server with a **Setup could not start the IMA Service** error.

*Resolution:* Verify the Print Spooler Service is started in the System context rather than for a user.

---

To troubleshoot an **IMA Service Failed** message with error code **2147483649** when *restarting a Presentation Server*:

- ❖ *Change the IMA Service startup account to the local administrator.*
- ❖ *Check for a missing TEMP directory* if the IMA Service starts under the local administrator account.
- ❖ *Switch the service back to the local system account and try manually creating the TEMP directory.*
  - ◆ *Verify that both the TMP and TEMP environment variables point to this directory.*

If an error that the IMA Service could not be started appears, but the IMA Service has *actually started*:

- ❖ The Service Control Manager has a *time-out of six minutes*.
  - ◆ *It can take longer than six minutes to start.*
- ❖ Ignore the message and *change the default time-out value*.

### **ICA Session Dropped Unexpectedly**

*Symptoms:*

- ❖ With Citrix *Presentation Server* installed on *Windows Server 2003*, the user starts a session to either a published or custom, application or desktop using *Program Neighborhood* or *Program Neighborhood Agent*.
- ❖ After being connected for an undetermined amount of time, the *session is dropped* and the *server has reset the connection*.

*Cause:*

- ❖ The Windows 2003 series of operating systems is the first to offer Smart Card Redirection.
- ❖ It is not known how this feature impairs the ICA connection; however, a workaround that resolves the issue is available.

*Resolution:* It was found that by *enabling* the **Do not allow smart card device redirection** setting in a Microsoft Group Policy, the *ICA sessions* that were exhibiting the issue *no longer lost their connections*.

### **ICA Session Becomes Unresponsive**

*Symptoms:*

- ❖ *ICA Sessions appear to freeze or hang* when using certain applications that use a *large amount of GUI resources* in sessions with corresponding *large display resolutions and high color depths*.
- ❖ Microsoft Office PowerPoint 2007 may not display consistently at the maximum session size of 1930x1447 at 24-bit color.
- ❖ The Windows Picture & Fax Viewer may not display consistently with resolutions sizes larger than 1600x1200 at 24-bit color.

*Cause:* You may have *reached the default per-user session memory limit* in Windows Server 2003.

*Solution:* Increase the *SessionPoolSize* through the *SessionPoolSize* registry entry.

## Unexpected Policy Results

The process for *troubleshooting unexpected policy results* is:

- ❖ Establish an ICA connection.
- ❖ Review Citrix policy settings by *generating a Citrix resultant policy report*.
- ❖ Initiate an RDP connection.
- ❖ Review the Active Directory policy settings, including Terminal Services policies.
- ❖ Review settings within the farm node of the Access Management Console.
- ❖ Confirm ICA listener settings.

## Shadowing

After creating a policy to allow one group to shadow another, the policy needs to be filtered by users to specify that the policy should be applied to the group being shadowed:

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

---

*Scenario:* An administrator created a Presentation Server policy for the Training group to be allowed to *shadow the Student group*.

*Resolution:* After creating a policy to allow the Training group to shadow the Student group, the policy needs to be *filtered by users* to specify that the policy should be *applied to the Student group*.

## Recording Audio

To allow users to record audio:

- ❖ Create a new *policy*.
- ❖ From the **Actions** menu, select **Properties**.
- ❖ Select **Client Devices > Resources > Audio > Microphones**.

- ❖ Select **Enabled** and **Use client microphones for audio input** and click **OK**.

### **Application Streaming**

To effectively *troubleshoot application streaming*, an administrator should ensure that:

- ❖ The *latest Streaming Client* is installed on the server used to stream the application.
- ❖ The *latest Streaming Client* is installed on the *client device*.
- ❖ The *latest Program Neighborhood Agent* client is installed on the *client device*.
- ❖ The license server has a Presentation Server 4.5 *Enterprise Edition* license that uses the *Platinum licensing model*.
- ❖ *Enterprise Edition* or *Platinum Edition* is selected in the Access Management Console.
- ❖ All servers are pointing to a license server containing the *appropriate licenses*.
- ❖ *Applications* are published for *application streaming*.
- ❖ **Enable offline access** is selected for the published application.
- ❖ *Published applications* are configured with **Offline Access Users**.
- ❖ The *Access Platform* and *Program Neighborhood Agent Services sites* are configured for *application streaming*.

### **Auto Client Reconnect**

*Auto Client Reconnect*:

- ❖ Works only if the server *disconnects sessions* when there is a *broken or timed out connection*.
- ❖ If a server's ICA-TCP connection is *configured to reset sessions* with a broken communication link, automatic *reconnection does not occur*.

### **Slow Logons**

*Slow logon times* can be contributed to:

- ❖ *Large profiles*.

- ◆ Take more time to load than smaller profiles.
- ❖ Problematic or unnecessary *virtual channels*.
- ❖ *Logon scripts*.
  - ◆ Might have *unnecessary statements* causing delays.
- ❖ *Profile paths*.
  - ◆ Can be *minimized by using roaming profiles*.
- ❖ *Font searching*.
  - ◆ Difficult to troubleshoot.
    - Might require network monitors/sniffers and third-party tools.

### **Remote Desktop Users**

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.

- ❖ Users can be *added* at *Presentation Server installation* or later using *Computer Management* on the server.

### **Session Logon Denied**

*Symptom*: Users are attempting to connect to a Presentation Server and the client stops at: **Checking your credentials**, and the following logon message appears: **You do not have access to this Session**.

*Resolution*: Enable **Any connection** in **Connection Access Control** in the **Properties** of the farm to resolve this problem.

### **Disconnected Sessions in Secure Gateway**

*Issue*:

- ❖ *A new firewall* is installed in an existing environment where *Secure Gateway* is used and *applications are delivered over the Internet*.
- ❖ Users are being *disconnected* after remaining idle for a *relatively short amount of time*.

- ◆ That didn't happen with the old firewall.

*Probable cause:*

- ❖ When using Secure Gateway in an environment where published applications are delivered over the Internet, *firewalls or other network hardware may terminate an idle session too early.*
- ❖ By default, Secure Gateway uses TCP port 443 to tunnel ICA/SSL traffic across the Internet.
  - ◆ *Port 443 is reserved for HTTPS traffic that, in most cases, does not cause problems for ICA/SSL traffic but some firewalls may terminate connections on port 443 if they remain idle for 10 minutes.*

*Resolution:* To prevent the session from becoming idle and being terminated by the firewall, you can enable an *ICA-level KeepAlive* process that *maintains traffic* between the Presentation Server, through Secure Gateway, to the ICA Client.

### **License Port Number**

*Symptom:* After changing the port number in the license file and executing the command **Imread -c**, you get the following error: **Imread failed: Cannot connect to license server (-15, 10:10061 "Winsock: Connection refused")**

*Resolution:* Change the license server port using the following steps:

- ❖ *Backup* both license files.
- ❖ *Remove the read only attribute* on the properties of each license file.
- ❖ Using a text editor, modify the **Server** line by *appending a port number after hostname or any* and save the file.
- ❖ Execute **Imreread** to reread the license file into memory without stopping and starting the Citrix Licensing Service.
- ❖ At a command prompt, type **netstat -a** to verify the new port number.
- ❖ *Modify all .lic files* in the **MyFiles** directory with the same port number and run an **Imreread** against those files as well.
- ❖ *Change the port number in the Management Console* to reflect the new port.

### **Unable to Check Out a License**

If you *allocate licenses and download the files* to your license server but are *unable to check out a license*, make sure that you:

- ❖ *Enter the hostname* of the license server in the license file.
- ❖ *Verify* that the product-side setting contains the *right license server name*.
- ❖ *Verify* that the *product is using the same port number as the license server*.
- ❖ Ensure that the license file contains *licenses for the desired product*.
  - ◆ For example, Citrix XenApp Enterprise Edition only works if the license file specifies the Enterprise Edition.

### **Using a Web Server Load Balancer**

**SSL Error 4** can be caused when:

- ❖ The Web Interface and Secure Gateway are on the *same server*.
- ❖ A *web server load balancer* is placed *between the client and the Secure Gateway*.
- ❖ *Clients* can communicate with the network *using HTTPS*, but traffic for *ICA/SSL is refused*.

---

*Issue:* In a Web Interface with Secure Gateway implementation, users attempting to launch published applications receive an **SSL Error 4**.

*Probable cause:* This is happening because the *Web Interface server and Secure Gateway are on the same server* and a *web server load balancer* is placed *between the client and the Secure Gateway*.

*Resolution:*

- ❖ There are two solutions to the *web server load balancer/Web Interface with Secure Gateway SSL Error 4 issue*:
  - ◆ Place Secure Gateway *parallel to the load balancer*.
  - ◆ Use a *network address translation (NAT)* solution and *forward all traffic to the Secure Gateway*.

## **Presentation Server Terminates Installation using Microsoft SQL Database**

### *Symptoms:*

- ❖ When installing Citrix Presentation Server to use SQL as a data store the user may receive the error message: **Error 26013. Function InitializeTree2 returned failure in CTX\_MF\_IMA\_InitializeTree2 the database username or password may be wrong.**
- ❖ This occurs even though the *user has created a DSN, and the ODBC tests completed successfully.*
- ❖ *Installation is then terminated and Presentation Server is not installed.*

### *Cause:*

- ❖ While *creating the DSN*, the user may have *cleared the following check boxes*:
  - ◆ **Use ANSI quoted identifiers**
  - ◆ **Use ANSI nulls, paddings and warnings**
    - These options are normally selected by default.

### *Resolution:*

- ❖ *Create a new, blank database and during installation ensure that these two options are enabled in the **Microsoft SQL Server DSN Configuration.***
  - ◆ Installation should now complete successfully.

## **Application Streaming Time**

To keep the *time it takes to stream an application to a client to a minimum*:

- ❖ *Locate the file server with the profile as close the client as possible.*
- ❖ *Network traffic considerations*:
  - ◆ *Bandwidth availability.*
  - ◆ *Time of day and day of week.*
- ❖ *Keep folder redirection for the Application Data folder at a minimum when rolling out Application Streaming in an enterprise environment.*

- ◆ This will allow the user's profile to load faster since the *Application Streaming cache will not be roamed* in as part of the user's profile.

---

*Issue:* A *streamed application* is taking a *long time to open* in a *remote office* that is connected to the main office, which holds the server farm and all file servers.

*Probable cause:* Being in the main office, *the file server holding the application profile is not close enough to the users* who are in the remote office connected over a WAN.

*Resolution:* To keep the *time it takes to stream an application* to a client to a *minimum*, it is important to *locate the file server with the profile as close the users as possible*.

### **Alternate Profiles**

*Alternate profiles:*

- ❖ Can be configured when *publishing a streamed application within the Access Management Console* by configuring the **Advanced** options of the published application.
  - ◆ This allows a *specific profile* to be delivered to users within a given *IP address range*.
    - For example, if an organization has two geographically dispersed data centers located in Sydney and Ft. Lauderdale, alternate profiles can be specified to direct the Australian users to a file share located in the Sydney data center and the North American users to a file share located in the Ft. Lauderdale data center.
- ❖ A *beginning and ending IP address* must be *specified* when configuring alternate profiles.

### **Streaming to Client Requirements**

To make sure that applications are properly streamed directly to clients:

- ❖ The *latest Streaming Client* is installed on the *client device*.
- ❖ The *latest Program Neighborhood Agent* is installed on the *client device*.
- ❖ The *latest Streaming Client* is installed on the *Presentation Server*.
  - ◆ Only if the application is going to be *streamed to the Presentation Server*.
- ❖ The Web Client cannot be used for application streaming.

## Process for Streaming Applications to Clients

*Client-side process* for streaming applications to the client:

- ❖ A user initiates a connection to a streamed application.
- ❖ The **.RAD** file is sent to the client and **RADERUN.EXE** (the RADE launcher) is executed.
- ❖ The RADE Launcher performs a remote procedure call into the Citrix Streaming Service (RADESVC) with all the parameters.
- ❖ The Streaming Service retrieves the application profile location from the **.RAD** file.
- ❖ The Streaming Service checks that the locally logged on user has access to the file share.
  - ◆ If not, the service will require Windows to prompt for credentials.
- ❖ The Streaming Service retrieves the appropriate target, which is a **.CAB** file, from the profile.
  - ◆ Based on the client operating system.
- ❖ The Streaming Service creates a new isolation environment.
- ❖ The Streaming Service ensures that the initial **.EXE** file and other required files are in the **RADECACHE** directory.
- ❖ The Streaming Service starts the **.EXE** file in the isolation environment.
- ❖ The Streaming Client verifies that the application has access to all it needs inside and outside the isolation environment.
- ❖ *The user is connected* to an application streaming session.

---

*Scenario:* A user attempts to launch a streamed application, but is prompted for a username and password.

*Probable cause:* During the streaming application process, the Citrix Streaming Service checks that the locally logged on user has access to the file share that contains the application profile and *if the user does not have access, the service will require Windows to prompt for credentials.*

*Resolution:* Give users of streaming applications access to the file share holding the application profile.

## **License Management Console Showing Excess of Used Licenses**

*Symptoms:* The *License Management Console* shows more licenses in use than the number of users connected.

*Cause:*

- ❖ *After applying Hotfix Rollup Pack 1 for Citrix Presentation Server 4.5, the client hardware ID identifier is written in uppercase, which causes two licenses to be consumed if you are using version 1.0 of the Streaming Client with version 10.1 of the Presentation Server Client on the same client system.*

*Resolution:*

- ❖ *Install the latest Streaming Client on the client device.*
- ❖ *Install the latest Presentation Server Client on the client device.*
- ❖ *Install the appropriate hotfix rollup pack to all servers running Presentation Server 4.5.*

## **Optimizing the Environment**

---

### **Printer Bandwidth Policy**

Applying a *printer bandwidth policy* allows the administrator to *control the amount of maximum bandwidth in kilobytes per second* that may be used for printing.

- ❖ *Frees up bandwidth for other resources over WAN link.*
- 

*Issue:*

- ❖ *Users are complaining about applications running slow.*
- ❖ *The applications that they are complaining about are published applications in the server farm.*
- ❖ *The administrator has already optimally configured printer auto-creation and print job routing.*

*Probable cause:* The users are located in a *remote office* that connects to the server farm over a WAN which has become quite *congested with network traffic*.

*Resolution:*

- ❖ Applying a *printer bandwidth policy* allows 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.

**Print Job Routing Policy**

**Print job routing** has two settings:

- ❖ **Connect directly to network print server if possible** and **Always connect indirectly as a client printer**.
  - ◆ If *concerned with bandwidth usage over a WAN* connection, use **Always connect indirectly as a client printer**.
    - *Data sent* to the client device is *compressed using the ICA protocol*.
      - *Less bandwidth is consumed* as the data travels across the WAN.

**Auto-Creation Rule Settings**

After **Auto-creation** is enabled, the following options are available:

- ❖ **Auto-create all client printers**
  - ◆ Creates *all printers* on a client device.
    - If the user has many printers defined, this settings *can increase logon time*.
- ❖ **Auto-create local (non-network) client printers only**
  - ◆ Creates *only printers connected directly* to the client device.
    - LPT, COM, USB, other local ports
  - ◆ Any *network printers* defined on the client are *not auto-created in the ICA session*.
  - ◆ This setting can *reduce logon time*.
- ❖ **Auto-create the client's default printer only**

- ◆ *Creates only the printer selected as the client's default printer.*
- ◆ *This setting reduces logon times as only one printer is auto-created in the ICA session.*
  - *This setting is optimal if it can be used.*
- ❖ **Do not auto-create client printers**
  - ◆ *Turns off the auto-create option for all client printers.*
    - *No client printers will be created in the ICA session.*

### **ICA Keep-Alive**

*ICA Keep-Alive:*

- ❖ *Used to manage the states of the ICA sessions.*
  - ◆ *Ensures that they are accurately reported.*
- ❖ *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.*

### **Auto Client Reconnect**

*Auto Client Reconnect:*

- ❖ *Allows Clients for Windows, Java and Windows CE to detect broken connections and automatically reconnect users to disconnected sessions.*
- ❖ *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.*

## 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.*

## SpeedScreen

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

### **SpeedScreen Progressive Display:**

- ❖ *Improves interactivity when displaying high-detail images.*
  - ◆ *Temporarily increases the level of compression.*
  - ◆ *Temporarily decreases the quality of an image when it is first transmitted over a limited bandwidth connection.*
    - *To provide a fast, but low quality, initial display.*
- ❖ *The image is then improved in the background to produce the normal quality image, as defined by the **Normal lossy compression** setting.*
- ❖ *AutoCAD is a good example of an application that would benefit by using **SpeedScreen Progressive Display** because of the high-detailed images and the bandwidth that is used.*

### **Heavyweight compression:**

- ❖ *Increases the compression of **SpeedScreen Image Acceleration** and **SpeedScreen Progressive Display** without impacting image quality.*
- ❖ **Heavyweight compression** *is CPU intensive and affects server scalability.*
  - ◆ *It is recommended for use only with low bandwidth connections.*

---

*Issue:* **SpeedScreen Image Acceleration** and **SpeedScreen Progressive Display** are already being used in the environment, but users are still complaining of *long load times for images*.

*Probable cause:* The users are on a low-bandwidth connection.

Solution:

- ❖ **Heavyweight compression** allows increased compression of the **SpeedScreen Image Acceleration** and **SpeedScreen Progressive Display** *without impacting image quality*.
- ❖ **Heavyweight compression** is *CPU intensive* and affects server scalability, it is *recommended for use only with low bandwidth connections*.

## Telnet

To find out if a *port is reachable or not*:

- ❖ Use the network command **Telnet** followed by the *server name or IP address*.

---

*Scenario:* Find out if the *Session Reliability port is reachable* on a server with the IP address **192.168.0.59**.

*Resolution:*

- ❖ **Telnet 192.168.0.59 2598**
  - ◆ Session Reliability uses port 2598.

## Memory Optimization

**Virtual Memory Optimization** was designed to *decrease Virtual Memory consumption* of applications and *improve application initialization time*.

*A DLL collision:*

- ❖ An application *tries to load two DLLs at the same base memory address*.
- ❖ When a *collision occurs*, the DLL has to be relocated to an available base memory address.

- ◆ When this happens, the DLL can no longer be shared by other applications, and hence this *takes up more actual memory*.
  - Increases the amount of *paging* and thus *affecting overall system performance*.
    - Ultimately, *application performance* is slowed down.
- ❖ When an administrator determines that this is happening, **Virtual Memory Optimization** *should be enabled* to fix the problem.

*DLL Rebasing* changes a DLL so that it loads at an optimal base memory address to *avoid collisions and relocations*.

**Virtual Memory Optimization** should be enabled when:

- ❖ User demand *exceeds* available RAM.
- ❖ Farm performance *degrades*.

If published applications fail after enabling **Memory Utilization Management** and running a **Scheduled Memory Optimization**, *exclude those applications from memory optimization*.