Citrix XenApp and XenDesktop 7.6 Implementation Guide for Healthcare

This document is intended to aid IT architects and administrators implementing the Citrix XenApp 7.6 solution architecture for healthcare. It includes an overview of the architecture and introductory implementation guidance.

Last Updated: March 2015
# Table of Contents

Section 1: Overview .................................................................................................................. 2  
Executive Summary ................................................................................................................ 2  
Section 2: Architectural Overview ........................................................................................ 3  
Section 3: Configuration Guidelines .................................................................................... 5  
  Authentication ....................................................................................................................... 5  
  Access Control ..................................................................................................................... 14  
  Securing the environment ..................................................................................................... 26  
  Data integrity ....................................................................................................................... 36  
  Transmission Security ......................................................................................................... 40  
  Audit Controls ...................................................................................................................... 51  
  High availability and business continuity .......................................................................... 59  
  Compatibility with legacy systems .................................................................................... 64  
  Client devices ....................................................................................................................... 69  
  Optimizing user experience and session performance ...................................................... 71
Section 1: Overview

Executive Summary

Today, every healthcare IT leader is expected to do more with less. To enable the best patient service possible, healthcare professionals need seamless, secure, instant access to patient information as they move across facilities, devices, and networks. They rely on IT solutions that help them focus on what matters most — patients and their families.

Designing, deploying, and managing virtual application, desktop and mobile IT solutions in the healthcare industry can be a complicated process. This document aims to guide partners and customers through the process using secure Citrix solutions.

Disclaimer

This guide is not intended to constitute legal advice. Customers should consult with their legal counsel regarding compliance with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act in the U.S., and other country-specific industry laws and regulations, and the intended use of Citrix products and services. Citrix makes no warranties, express, implied, or statutory, as to the information in this document.
Section 2: Architectural Overview

The goal of the first iteration of this guide is to show how Citrix solutions can be leveraged to meet the needs of the healthcare enterprise governance, risk, and compliance initiatives. This guide is not focused on scale or performance of the environment. The Citrix Solutions Lab architecture was focused on a single-server environment, configuration of the operating systems, virtual desktops and XenDesktop specific to the healthcare industry requirements. It was not focused on the physical hardware layout such as the hypervisor, hardware, or network layers. Find more information about system requirements at the Citrix product documentation site: http://support.citrix.com/proddocs/topic/xenapp-xendesktop-76/xad-system-requirements-76.html.

To validate the healthcare categories listed in this design guide, Citrix Solutions Lab deployed and configured a healthcare compliance-aware solution. The environment was built with Citrix XenApp and XenDesktop 7.6 with Provisioning Services 7.6 streaming hosted shared desktops and dedicated VDI desktops, running on a Microsoft Hyper-V 2012 R2.

The environment utilized virtual clients as well as physical Dell Wyse thin clients to connect to the different types of desktops, as well as map to physical network printers and USB-attached printers.

Architectural Components

Implemented architecture includes:

<table>
<thead>
<tr>
<th>Component</th>
<th>Citrix/3rd Party</th>
<th>Description/Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>XenApp and XenDesktop 7.6</td>
<td>Citrix</td>
<td></td>
</tr>
<tr>
<td>NetScaler 10.5</td>
<td>Citrix</td>
<td></td>
</tr>
<tr>
<td>Provisioning Services 7.6</td>
<td>Citrix</td>
<td></td>
</tr>
<tr>
<td>StoreFront 2.6</td>
<td>Citrix</td>
<td></td>
</tr>
<tr>
<td>License Server 11.12</td>
<td>Citrix</td>
<td></td>
</tr>
<tr>
<td>Product Name</td>
<td>Vendor</td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>----------</td>
<td></td>
</tr>
<tr>
<td>Profile Management 5.1</td>
<td>Citrix</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows 8.1</td>
<td>Microsoft</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows Server 2012 R2</td>
<td>Microsoft</td>
<td></td>
</tr>
<tr>
<td>Microsoft SQL Server 2012 R2</td>
<td>Microsoft</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows Server 2012 R2 with the Hyper-V role</td>
<td>Microsoft</td>
<td></td>
</tr>
</tbody>
</table>
Section 3: Configuration Guidelines

Authentication

Providing unauthenticated (anonymous) access

Unauthenticated user access in XenApp and XenDesktop 7.6 provides access to server-based hosted applications and server-hosted desktops without presenting credentials. In previous versions of Citrix XenApp, this feature was known as anonymous user accounts.

Use cases for unauthenticated user access include but are not limited to:

- Access applications through thin-client-based kiosks.
- Access applications that require application-specific credentials without asking users for Active Directory credentials.
- Access Windows-based desktops without creating and managing individual user accounts for a fast-changing user base.

The Delivery Group properties allow you to grant access to unauthenticated or authenticated users, or both. This behavior is different from previous versions of XenApp, in which these options were mutually exclusive. In XenApp 7.6, anonymous user accounts are created on the fly during unauthenticated user logon, compared to previous versions of XenApp, in which they’re created during the Virtual Delivery Agent (VDA) setup.

Anonymous user accounts in XenApp and XenDesktop 7.6 are created as local user accounts and named AnonXYZ, in which XYZ is a unique three-digit value up to maximum described below. Anonymous user accounts are added to the Anonymous, Guest, and Remote Desktop Users local groups.

Configuration guidelines

The process of enabling unauthenticated user access consists of two parts: granting Delivery Group access to unauthenticated users in Citrix Studio and creating an unauthenticated StoreFront store.

Granting Delivery Group access to unauthenticated users

Access to unauthenticated users can be granted by modifying delivery group settings during initial configuration or any time after.

Figure 1: Providing access to unauthenticated users

© Copyright 2015 Citrix Systems, Inc.
StoreFront configuration

When you create an unauthenticated store, it is not automatically advertised to ensure it is not automatically added as a store to Citrix Receiver. If you need to access unauthenticated sessions using Citrix Receiver without browsing to the StoreFront web site, enable advertising in the StoreFront management console.

Optional VDA configuration

By default, the idle session limit for anonymous accounts is set to 10 minutes. This default value can be changed by modifying the registry value AnonymousUserIdleTime under HKLM\SYSTEM\CurrentControlSet\Control\Citrix before accounts created.

By default, the maximum number of anonymous accounts on each VDA is set to 99. To modify this value, change the registry value MaxAnonymousUsers under HKLM\SYSTEM\CurrentControlSet\Control\Citrix.

As explained above, anonymous user accounts created on demand; this also means that if Machine Creation Services or Provisioning Services are used to manage machine catalogs, these user accounts does not persist after reboot.

If you need to configure specific parameters for anonymous accounts, such as local group membership or display name, you can use CreateAnonymousUsersApp.exe utility located in <ProgramFiles>CitrixICAConfigTool folder to pre-create user accounts. After user accounts are created, you can use the standard Windows user account management tools. CreateAnonymousUsersApp utility can also be used to remove all previously created anonymous accounts.

Special considerations

Anonymous user accounts are created with a minimal set of permissions and a nonpersistent (temporary) user profile. If you need to adjust the template used to create a temporary profile, use Microsoft guidelines described in this support article: [http://support.microsoft.com/kb/973289](http://support.microsoft.com/kb/973289).

Unauthenticated sessions are automatically logged off when the client disconnects. Reconnection, roaming between clients and Workspace Control are not supported.

Currently, anonymous sessions are only supported with VDA for Windows Server OS version 7.6 or later. Client OS VDA or previous versions of VDA for Server OS are not supported.

Be aware that anonymous user accounts are not able to access resources that require Active Directory credentials. This may include file shares, SQL databases, and SharePoint websites.

NetScaler Gateway cannot be used for remote access with unauthenticated StoreFront stores.
Configuring Session Reliability and Auto Client Reconnect

Managing session activity is necessary to ensure the best user experience. Losing network connectivity because of unreliable networks, high network latency, and limitations of wireless devices can lead to user frustration. Being able to move quickly between devices and access the same set of applications at every logon is a priority for many mobile users, especially those in healthcare. The Session Reliability and Auto Client Reconnect features increase the reliability of remote sessions, reduce the amount of downtime and loss of productivity, and provide mobile users with the ability to roam quickly and easily between devices.

Session Reliability

Session Reliability keeps sessions active on the server and visible on the user’s screen when network connectivity is interrupted. Users continue to see the application they are using until network connectivity resumes. To indicate that connectivity is lost, the user’s display freezes, and the cursor changes to a spinning hourglass. The user continues to access the display during the interruption and can resume interacting with the application when the network connection is restored, without users having to reauthenticate. If you want to require users to reauthenticate, configure the Auto Client Reconnect authentication setting. By default, Session Reliability is allowed through policy settings.

Figure 2: Session Reliability connections
You can edit the port on which the server listens for Session Reliability traffic and edit the amount of time Session Reliability keeps an interrupted session connected. Incoming Session Reliability connections use port 2598, unless you change the port number as shown below:

Figure 3: Session Reliability port number

The Session Reliability timeout policy setting has a default of 180 seconds, or three minutes. Though you can extend the amount of time Session Reliability keeps a session open, this feature is designed to be convenient for the user and, therefore, does not prompt the user for reauthentication. As you extend the amount of time a session is kept open, chances increase that a user may get distracted and walk away from the user device, potentially leaving the session accessible to unauthorized users.

Figure 4: Session Reliability timeout

© Copyright 2015 Citrix Systems, Inc.
Auto Client Reconnect

Users can be disconnected from their sessions because of unreliable networks, highly variable network latency, or range limitations of wireless devices. With the Auto Client Reconnect feature, Receiver can detect unintended disconnections of ICA sessions and reconnect users to the affected sessions automatically. When this feature is enabled on the server, users do not have to reconnect manually to continue working. Receiver attempts to reconnect to the session until there is a successful reconnection or the user cancels the reconnection attempts.

However, automatic reconnection can result in a new session being launched (instead of reconnecting to an existing session) if the Receiver’s cookie, which contains the key to the session ID and credentials, is not used. The cookie is not used if it has expired, for example, because of a delay in reconnection, or if credentials must be re-entered. Auto Client Reconnect is not triggered if users intentionally disconnect.

By default, Auto Client Reconnect is allowed.

Configure Auto Client Reconnect using the following policy settings:

- **Auto client reconnect.** Enables or disables automatic reconnection by Receiver after a connection has been interrupted.

![Edit Setting](image-url)
**Auto client reconnect authentication.** Enables or disables the requirement for user authentication upon automatic reconnection.

![Edit Setting](image)

- **Auto client reconnect logging.** Enables or disables logging of reconnection events in the event log. Logging is disabled by default. When enabled, the server’s system log captures information about successful and failed automatic reconnection events. Each server stores information about reconnection events in its own system log; the server farm does not provide a combined log of reconnection events for all servers.

![Edit Setting](image)
Special considerations

Auto Client Reconnect incorporates an authentication mechanism based on encrypted user credentials. When a user initially logs on to a site, the server encrypts and stores the user credentials in memory, and creates and sends a cookie containing the encryption key to Citrix Receiver, which submits the key to the server for reconnection. The server decrypts the credentials and submits them to Windows logon for authentication. When cookies expire, users must reauthenticate to reconnect to sessions. Cookies are not used if you enable the auto client reconnection authentication setting. Instead, users are presented with a dialog box to users requesting credentials when Receiver attempts to reconnect automatically.

Receiver users cannot override the server setting for session reliability. You can use Session Reliability with Secure Sockets Layer (SSL). You can disable Auto Client Reconnect on Citrix Receiver for Windows by using the icclient.adm file. For more information, see the Receiver for Windows documentation at http://support.citrix.com/proddocs/topic/receiver/rec-receiver-for-win.html.

If you use both Session Reliability and Auto Client Reconnect, the two features work in sequence. Session Reliability closes (or disconnects) the user session after the amount of time specified in the Session Reliability timeout setting. After that, the Auto Client Reconnect settings take effect, attempting to reconnect the user to the disconnected session.

When a NetScaler Gateway is in use, the Automatic Client Reconnect feature will only work if a full VPN connection has been established.

Additional information

| XenApp 7.6 and XenDesktop 7.6 -> Managing -> Sessions | http://support.citrix.com/proddocs/topic/xenapp-xendesktop-76/xad-sessions-maintain.html |
| Is Session Reliability Good or Bad? | http://blogs.citrix.com/2013/10/16/is-session-reliability-good-or-bad/ |
| Session Reliability | http://www.citrix.com/tv/#videos/686 |

Configuring workspace control

Workspace control lets desktops and applications follow a user from one device to another. This ability to roam enables a user to access all desktops or open applications from anywhere simply by logging on without having to restart the desktops or applications on each device. For example, workspace control can assist health-care workers in a hospital who need to move quickly among different workstations and access the same set of applications each time they log on. If you configure workspace control options to allow it, these workers can disconnect from multiple applications at one client device and then reconnect to open the same applications at a different client device.

Workspace control affects the following activities:

- **Logging on** – By default, workspace control enables users to reconnect automatically to all running desktops and applications when logging on, bypassing the need to reopen them manually. Through workspace control, users can open disconnected desktops or applications, as well as any that are active on another client device. Disconnecting from a desktop or application leaves it running on the server. If you have roaming users who need to keep some desktops or applications running on one client device while they reconnect to a subset of their desktops or applications on another client device, you can configure the logon reconnection behavior to open only the desktops or applications that the user disconnected from previously.
• **Reconnecting** – After logging on to the server, users can reconnect to all their desktops or applications at any time by clicking **Reconnect**. By default, Reconnect opens desktops or applications that are disconnected, plus any that are currently running on another client device. You can configure Reconnect to open only those desktops or applications from which the user disconnected previously.

• **Logging off** – For users opening desktops or applications through StoreFront, you can configure the Log Off command to log the user off from StoreFront and all active sessions together, or log off from StoreFront only.

• **Disconnecting** – Users can disconnect from all running desktops and applications at once, without needing to disconnect from each individually.

Workspace control is available only for Receiver users who access desktops and applications through a Citrix StoreFront connection. By default, workspace control is disabled for virtual desktop sessions but is enabled for hosted applications. Session sharing does not occur by default between published desktops and any published applications running inside those desktops.

**Configuration guidelines**

Workspace control can be enabled or disabled for a StoreFront store by setting the attribute with xpath /configuration/citrix.deliveryservices/resourcesService/@allowSessionReconnect to “True” or “False.” Another way of configuring this setting is to use PowerShell cmdlet Set-DSAllowSessionReconnect.

Before you can run the cmdlet, you have to import the necessary PowerShell modules. The following snippet does it for you:

```powershell
$dsInstallProp = Get-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DeliveryServicesManagement -Name InstallDir
$dsInstallDir = $dsInstallProp.InstallDir
& $dsInstallDir\..\Scripts\ImportModules.ps1
```

To disable workspace control for a store, run the following command:

```powershell
Set-DSAllowSessionReconnect -SiteId 1 -VirtualPath /Citrix/Store -IsAllowed $false
```

Workspace control is enabled by default for Receiver for Web sites. To disable or configure workspace control, you need edit the site configuration file.

Use a text editor to open the web.config file for the Receiver for Web site, which is typically located in the C:\inetpub\wwwroot\Citrix\storenameWeb\ directory, where storename is the name specified for the store when it was created.

Locate the following element in the file.

```xml
<workspaceControl enabled="true" autoReconnectAtLogon="true"
logoffAction="disconnect" showReconnectButton="false"
showDisconnectButton="false" />
```

Change the value of the enabled attribute to false to disable workspace control for the site. Set the value of the autoReconnectAtLogon attribute to false to prevent automatic reconnection of users to any applications that they left running. To automatically shut down users’ applications when they log off from the site, set the value of the logoffAction attribute to terminate. Set logoffAction to none to leave users’ applications running and active when they log off from the site.

By default, autoReconnectAtLogon is set to true, and logoffAction is set to disconnect. This configuration enables a user to log on to a site, start applications, and then log on to the same site using a different device and have those resources automatically transferred to the new device. All the applications the user starts from a particular site are left running but are automatically disconnected when the user logs off from that site, provided the same browser instance is used to log on, start the resources, and log off. If there is only one desktop available for a user on a Receiver for Web site that is configured to start single desktops.
automatically when the user logs on, that user’s applications are not reconnected, even if the autoReconnectAtLogon attribute is set to true.

Disable automatic reconnection of applications at logon to enable users to choose whether they want their applications to follow them from device to device. If you disable automatic reconnection of applications at logon, ensure that the Connect link is enabled so that users can manually reconnect to applications that they left running.

Change the value of the showReconnectButton attribute to true to display on the site the Connect link, which enables users to manually reconnect to applications that they left running. Set the value of the showDisconnectButton attribute to true to display the Disconnect link, which enables users to manually disconnect from applications without shutting them down.

By default, the Connect and Disconnect links do not appear on sites. Enable the links and disable automatic reconnection of applications at logon to enable users to choose whether they want their applications to follow them from device to device.

**Special considerations**

User policies, client drive mappings, and printer configurations change appropriately when a user moves to a new client device. Policies and mappings are applied according to the client device where the user is currently logged on to the session. For example, if a healthcare worker logs off from a client device in the emergency room of a hospital and then logs on to a workstation in the hospital’s X-ray laboratory, the policies, printer mappings, and client drive mappings appropriate for the session in the X-ray laboratory go into effect at the session startup.

You can customize what printers appear to users when they change locations. You can also control whether users can print to local printers, how much bandwidth is consumed when users connect remotely, and other aspects of their printing experiences.

Use of workspace control on Receiver for Web sites is subject to the following requirements and restrictions.

Workspace control is not available when Receiver for Web sites are accessed from hosted desktops and applications.

For users accessing Receiver for Web sites from Windows devices, workspace control is only enabled if the site can detect that Citrix Receiver is installed on users’ devices or if Receiver for HTML5 is used to access resources.

To reconnect to disconnected applications, users accessing Receiver for Web sites through Internet Explorer must add the site to the local intranet or trusted sites zones.

If there is only one desktop available for a user on a Receiver for Web site that is configured to start single desktops automatically when the user logs on, that user’s applications are not reconnected, regardless of the workspace control configuration.

Users must disconnect from their applications using the same browser that was originally used to start them. Resources started using a different browser or started locally from the desktop or Start menu using Citrix Receiver cannot be disconnected or shut down by Receiver for Web sites.

### Additional information

Access Control

Enabling NetScaler External Authentication and command policies

In many healthcare environments, different teams that consist of multiple administrators manage Citrix infrastructure. In such environments, it is important to have administrative accounts that are associated with a particular person and avoid sharing the default administrative account.

Citrix NetScaler supports external authentication methods for managing the appliance. These methods include Lightweight Directory Access Protocol (LDAP), including support for SSL and TLS encryption, Remote Authentication Dial in User Service (RADIUS), and Terminal Access Controller Access-Control System (TACACS). In cases when external authentication servers are not available, you can also use local users and groups configured on the NetScaler appliance.

To support principle of least privilege, it is recommended to configure and use NetScaler command policies. Command policies define list of commands, command groups, virtual servers (vservers), and other entities that users or user groups are permitted to use.

In the United States, HIPAA Technical Safeguards require implementation of technical policies that allow access to applications that process PHI only to those persons who have been granted access rights. NetScaler is commonly used as a primary access point to a secure environment, and it's important to have properly delegated authentication and command policies.

Configuration guidelines

Configuration of NetScaler external authentication consists of configuring NetScaler authentication actions and policies and then binding such policies to the system. Even both authentication actions and policies can be shared between system, AAA-TM vservers and NetScaler Gateway vservers, we recommend creating separate entities.

By default, if users are authenticated with external authentication policy, they granted minimal access to the NetScaler. To provide administrative or another type of special access, you need to define users or groups in a system configuration and bind existing command policies to them or create custom command policies.

The default NetScaler administrator user name is nsroot, and it has a well-known default password. This password should be changed during the initial setup of the NetScaler appliance and should not be shared. A list of all possible risks is outside of the scope of this document; however, most important of them are:

- Auditing and monitoring of administrative actions are complicated; when multiple administrators use the shared account for administration, it's very difficult to identify who actually performed specific system changes.
- The passwords for shared accounts are difficult to manage because coordination is required between all administrators, dedicated shared and secure storage, and as a result, password management is often omitted.

When configuring external authentication, always use encrypted channels for communication to avoid sending credentials over the network in unencrypted form.

Special considerations

When configuring and applying command policies, the following key points need to be taken into consideration:

- Command policies are combined if a user is a member of multiple defined groups, and conflicts are resolved according to the priorities assigned to command policies.
- Commands below are available to any user regardless of policies applied:
When configuring LDAP authentication for administrative access, always configure a filter group. Otherwise, anyone with valid credentials will be able to access NetScaler (although, they won’t be able to make any changes).

### Additional information

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>How to Configure Users to Log on to NetScaler Appliance Using Active Directory Password</td>
<td><a href="http://support.citrix.com/article/CTX123782">http://support.citrix.com/article/CTX123782</a></td>
</tr>
</tbody>
</table>

### Configuring XenApp and XenDesktop delegated administration

The delegated administration model offers the flexibility to match how your organization wants to delegate administration activities, using role- and object-based control. Delegated administration accommodates deployments of all sizes and allows you to configure more permission granularity as your deployment grows in complexity. Delegated administration uses three concepts: administrators, roles, and scopes.

- **Administrators** — An administrator represents an individual person or a group of people identified by their Active Directory account. Each administrator is associated with one or more role and scope pairs.
- **Roles** — A role represents a job function and has defined permissions associated with it. For example, the Delivery Group Administrator role has permissions such as “Create Delivery Group” and “Remove Desktop from Delivery Group.” An administrator can have multiple roles for a Site, so a person could be a Delivery Group Administrator and a Machine Catalog Administrator. Roles can be built-in or custom.

The built-in roles are:

<table>
<thead>
<tr>
<th>Role</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Administrator</td>
<td>Can perform all tasks and operations. A Full Administrator is always combined with the All scope.</td>
</tr>
</tbody>
</table>
Read Only Administrator
Can see all objects in specified scopes as well as global information but cannot change anything. For example, a Read Only Administrator with Scope=London can see all global objects (such as Configuration Logging) and any London-scoped objects (for example, London Delivery Groups). However, that administrator cannot see objects in the New York scope (assuming that the London and New York scopes do not overlap).

Help Desk Administrator
Can view Delivery Groups and manage the sessions and machines associated with those groups. Can see the machine catalog and host information for the Delivery Groups being monitored and can also perform session management and machine power management operations for the machines in those Delivery Groups.

Machine Catalog Administrator
Can create and manage machine catalogs and provision the machines into them. Can build machine catalogs from the virtualization infrastructure, Provisioning Services, and physical machines. This role can manage base images and install software but cannot assign applications or desktops to users.

Delivery Group Administrator
Can deliver applications, desktops, and machines, and can manage the associated sessions. Can also manage application and desktop configurations such as policies and power management settings.

Host Administrator
Can manage host connections and their associated resource settings. Cannot deliver machines, applications, or desktops to users.

In certain product editions, you can create custom roles to match the requirements of your organization, and delegate permissions with more detail. You can use custom roles to allocate permissions at the granularity of an action or task in a console.

Scopes — A scope represents a collection of objects. Scopes are used to group objects in a way that is relevant to your organization (for example, the set of Delivery Groups used by the sales team). Objects can be in more than one scope; you can think of objects being labeled with one or more scopes. There is one built-in scope: "All," which contains all objects. The Full Administrator role is always paired with the All scope.

Configuration guidelines

Create and manage administrators

When you create a Site as a local administrator, your user account automatically becomes a Full Administrator with full permissions over all objects. After a Site is created, local administrators have no special privileges.

The Full Administrator role always has the All scope; you cannot change this.

By default, an administrator is enabled. Disabling an administrator may be necessary if you are creating the new administrator now, but that person will not begin administration duties until later. For existing enabled administrators, you may want to disable several of them while you are reorganizing your object/scopes and then re-enable them when you are ready to go live with the updated configuration. You cannot disable a Full Administrator if it will result in there being no enabled Full Administrator. The enable/disable check box is available when you create, copy, or edit an administrator.

When you delete a role/scope pair while copying, editing, or deleting an administrator, it deletes only the relationship between the role and the scope for that administrator; it does not delete either the role or the scope, nor does it affect any other administrator who is configured with that role/scope pair.

To manage administrators, click Configuration > Administrators in the Studio navigation pane, and then click the Administrators tab in the upper middle pane.

© Copyright 2015 Citrix Systems, Inc.
To create an administrator, click Create new Administrator in the Actions pane. Type or browse to the user account name, select or create a scope, and select a role. The new administrator is enabled by default; you can change this.

To copy an administrator, select the administrator in the middle pane and then click Copy Administrator in the Actions pane. Type or browse to the user account name. You can select and then edit or delete any of the role/scope pairs, and add new ones. The new administrator is enabled by default; you can change this.

To edit an administrator, select the administrator in the middle pane and then click Edit Administrator in the Actions pane. You can edit or delete any of the role/scope pairs, and add new ones.

To delete an administrator, select the administrator in the middle pane and then click Delete Administrator in the Actions pane. You cannot delete a Full Administrator if it will result in there being no enabled Full Administrator.

Create and manage roles

To manage roles, click Configuration > Administrators in the Studio navigation pane, and then click the Roles tab in the upper middle pane.

To view role details, select the role in the middle pane. The lower portion of the middle pane lists the object types and associated permissions for the role. Click the Administrators tab in the lower pane to display a list of administrators who currently have this role.

To create a custom role, click Create new Role in the Actions pane. Enter a name and description. Select the object types and permissions.

To copy a role, select the role in the middle pane and then click Copy Role in the Actions pane. Change the name, description, object types, and permissions, as needed.

To edit a custom role, select the role in the middle pane and then click Edit Role in the Actions pane. Change the name, description, object types, and permissions, as needed.

To delete a custom role, select the role in the middle pane and then click Delete Role in the Actions pane. When prompted, confirm the deletion.

Create and manage scopes

When you create a Site, the only available scope is the All scope, which cannot be deleted.

You can create scopes using the procedure below. You can also create scopes when you create an administrator; each administrator must be associated with at least one role and scope pair. When you are creating or editing desktops, machine catalogs, applications, or hosts, you can add them to an existing scope; if you do not add them to a scope, they remain part of the All scope.

Neither Site creation nor Delegated Administration objects (scopes and roles) can be scoped. However, objects you cannot scope are included in the All scope. (Full Administrators always have the All scope.) Machines, power actions, desktops, and sessions are not directly scoped; administrators can be allocated permissions over these objects through the associated machine catalogs or Delivery Groups.

When you copy or edit a scope, keep in mind that removing objects from the scope can make those objects inaccessible to the administrator. If the edited scope is paired with one or more roles, ensure that the scope updates you make do not make any role/scope pair unusable.

To manage scopes, click Configuration > Administrators in the Studio navigation pane, and then click the Scopes tab in the upper middle pane.

To create a scope, click Create New Scope in the Actions pane. Enter a name and description. To include all objects of a particular type (for example, Delivery Groups), select the object type. To include specific objects, expand the type and then select individual objects (for example, Delivery Groups used by the Sales team).
To copy a scope, select the scope in the middle pane and then click **Copy Scope** in the Actions pane. Enter a name and description. Change the object types and objects, as needed.

To edit a scope, select the scope in the middle pane and then click **Edit Scope** in the Actions pane. Change the name, description, object types, and objects, as needed.

To delete a scope, select the scope in the middle pane and then click **Delete Scope** in the Actions pane. When prompted, confirm the deletion.

**Special considerations**

There are several options available based on what you are allowing that particular administrator to manage/maintain. For the purposes of this document, this user is going to be delegated as a Read Only Administrator.

Only certain product editions support custom roles. Editions that do not support custom roles do not have related entries in the Actions pane.

You cannot edit or delete a built-in role. You cannot delete a custom role if any administrator is using it.

**Additional information**

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Transferring custom roles from one XD site to another</td>
<td><a href="http://blogs.citrix.com/2013/10/10/transferring-custom-roles/">http://blogs.citrix.com/2013/10/10/transferring-custom-roles/</a></td>
</tr>
</tbody>
</table>

**Configuring Provisioning Services administrative roles**

The ability to view and manage objects within a Provisioning Services implementation is determined by the administrative role assigned to a group of users. Provisioning Services makes use of groups that already exist within the network (Windows or Active Directory groups). All members within a group will share the same administrative privileges within a farm. An administrator may have multiple roles if they belong to more than one group.

The following administrative roles can be assigned to a group:

- Farm Administrator
- Site Administrator
- Device Administrator
- Device Operator

After a group is assigned an administrator role through the Provisioning Services console, if a member of that group attempts to connect to a different farm, a dialog displays requesting that a Provisioning Services within that farm be identified (the name and port number). You are also required to use either the Windows credentials you are currently logged on with (default setting) or enter your Active Directory credentials. Provisioning Services does not support using both domain and work groups simultaneously.

When the information is sent to and received by the appropriate server farm, the role that was associated with your group determines your administrative privileges within this farm. Group role assignments can vary from farm to farm.

© Copyright 2015 Citrix Systems, Inc.
Configuration guidelines

Before configuring administrative roles for Provisioning Services, security groups must be defined in the Groups tab in Farm Properties, as shown below. This approach ensures that only groups defined by a Farm Administrator can be granted access on the site ad device group levels.
After groups are defined, you can grant access on the Security tab in Farm Properties, as shown below:
In Site Properties, you can also grant Site Administrator access to the groups defined in the Farm Properties, as shown below:

![Site Properties](image)

**Additional information**

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>How to Grant Rights to Manage Computer Accounts using Provisioning Services Console</td>
<td><a href="http://support.citrix.com/article/CTX121201">http://support.citrix.com/article/CTX121201</a></td>
</tr>
</tbody>
</table>

**Understanding network segmentation concepts and considerations**

While healthcare environments are subject to industry regulations, users such as receptionists and accountants who process credit card information must also comply with the Payment Card Industry Data Security Standard (PCI DSS).

One of the core requirements in such norms and regulations is to build and maintain a secure network and use firewalls to control the incoming and outgoing network traffic.

In general, network segmentation and segregation is one of the most effective controls that could be implemented to mitigate a network intrusion or vulnerability spread. If applied correctly, network segmentation can make it significantly harder for an attacker to locate network resources and gain access to the sensitive information.

When network segmentation and segregation are implemented, the core purpose is to minimize the surface of attack on the system and reduce the level of access to the sensitive information. This can be accomplished by using various techniques and technologies depending on architecture and configuration of your network.
Traditionally, one of the points of the network segmentation is implementation of a gateway to internal resources. Using NetScaler Gateway with XenApp and XenDesktop increases security and better enables user access to internal resources. The robust policy capabilities of NetScaler Gateway equip administrators with access control management by allowing policies that can restrict access to applications based on different factors, such as:

- user identity and group membership
- physical location of a user
- configuration and protection status of the endpoint device

NetScaler Gateway is typically located in the DMZ and can be configured to access backend resources by a direct connection or via the existing firewall.

Network segmentation often involves partitioning the network into smaller networks to isolate servers that process confidential data. Alternatively, when most of the network is highly regulated, a dedicated network segment can be used to access Internet and other public resources.

In both cases, XenApp or XenDesktop can be used to securely access isolated resources. Typical scenarios include:

- Hardened XenApp servers in isolated network segment behind the proxy server with published Internet browser
- Dedicated network segment with XenDesktop pooled desktops for third-party consultants
- Restricted applications published with XenApp

**Configuration guidelines**

When implementing network segregation, always start with a plan and network diagram that includes all components and servers including but not limited to:

- Citrix infrastructure components
- Client locations
- Core infrastructure servers such as Active Directory domain controllers, DNS, DHCP, user profile shares, etc.
- Backend resources such as application servers, SQL databases, file shares and others

Regardless of the technology used for network segmentation and segregation, always follow the recommendations below:

- Implement protection techniques at other levels, not just on the network layer. Each system may include options to control access from the data link layer up to the application layer. As example, NetScaler can use policy-based routing and traffic domains to segregate traffic based on different policy decisions. XenDesktop can direct users to a secure segment when needed.
- Use the principles of least privilege. If a system doesn’t require communication with another system on the network, such access should be restricted. Port and protocol restrictions can also be enforced on the firewall because of requirements. Consider the use of XenDesktop with internal NetScaler Gateway in such situations to reduce the number of ports that need to be opened to a restricted network.
- Separate information, users, and infrastructure. This may include using different hardware for Controllers and user-published desktops.
- Use whitelisting instead of blacklisting. This means you should grant access to a known good, rather than denying access to a known bad.
Separating infrastructure components using virtual networks (vLANs)

Virtual networks (vLANs) can be used to ensure that there is a high level of security at critical boundaries between the various infrastructure and management components and the Citrix environment. Dividing the network into smaller entities allows a fine-grained control over which servers and ports can be accessed, and minimizes the capabilities of malicious users of pivoting onto more privileged systems. A sample vLAN segmentation is provided below:

- **User vLANs:** In traditional client/server infrastructures, administrators could secure the data center by placing firewalls at the perimeter (internally and externally). For modern virtual desktop scenarios, the network security paradigm needs to be changed because user desktops are now hosted inside the data center, and a compromised desktop could access and infect backend server systems. Therefore, systems directly accessed by users should be separated in a specialized vLAN.

- **Provisioning vLAN:** Contains the provisioning servers, which provide the central image management functionality for the infrastructure.

- **Authentication vLAN:** The authentication vLAN contains the Microsoft Active Directory Forest and domains within a secured network. Only specific secured access to Active Directory capabilities are enabled in this vLAN for specific users, administrators, and machines from the other networks.

- **Management vLAN:** The management vLAN contains many of the foundational network services necessary in a hosted environment such as Domain Name Services, NTP and SNMP as well as other services provided by the CSP. In some cases, an out-of-band management vLAN is implemented, which provides access for monitoring (such as SNMP) and remote administrative access to servers and other components. In such a scenario, the Authentication vLAN will provide the foundational network services.

- **Application vLAN:** This vLAN contains the back-office applications that enable web, mail, collaboration, and line-of-business-application backend services.

Special considerations

When configuring firewalls, always consult with a vendor documentation to ensure that important communications are not blocked.

Applications that using Remote Procedure Call (RPC) require a special attention because RPC applications are using dynamic port range for communication, and the client device discovers the correct port using the RPC endpoint mapper. Many hardware firewalls understand RPC protocol and can be configured to allow or block specific applications. Consult with your hardware firewall vendor for configuration guidelines.

Additional information

| An overview of ports that are used by Citrix components | [http://support.citrix.com/article/CTX101810](http://support.citrix.com/article/CTX101810) |
| Service overview and network port requirements for Windows | [http://support.microsoft.com/KB/832017](http://support.microsoft.com/KB/832017) |
Configuring Session idle and connection timers

XenApp and XenDesktop allow users to disconnect from a session without ending the session. This keeps a session in a disconnected state and allows programs started by a user to continue to run even though the user is no longer actively connected to the session.

You can control how long active, disconnected, and idle sessions remain on the server. If a session keeps running in a disconnected state, the user can reconnect to the session and continue to work with their applications, but it’s important to note that sessions that run indefinitely continue to consume system resources.

You can configure session limits by using policies. Please note that session limits for Server OS and Desktop OS connections are configured differently.

Configuration guidelines

To configure session limits for a Desktop OS, use Citrix policies in Studio or Citrix policies node in Microsoft Group Policies.

These settings are included in a group of policies known as the Session Limits Policy Settings. The configurable options for these policy settings are as follows:

- **Session connection timer.** This setting enables or disables a timer that specifies the maximum duration of an uninterrupted connection between a user device and a desktop. By default, this timer is disabled.
- **Session connection timer interval.** This setting specifies the maximum number of minutes for an uninterrupted connection between a user device and a desktop. By default, the maximum duration is 1,440 minutes (24 hours).
- **Session idle timer.** This setting enables or disables a timer that specifies how long an uninterrupted user device connection to a desktop will be maintained if there is no input from the user. By default, this timer is enabled.
- **Session idle timer interval.** This setting specifies how many minutes an uninterrupted user device connection to a desktop will be maintained if there is no input from the user. By default, idle connections are maintained for 1,440 minutes (24 hours).

Session limits for Server OS VDAs are controlled through Session Time Limits node of the Microsoft Group Policies, and XenDesktop inherits Remote Desktop Session Host configuration.


Special Considerations

Please note that for Server OS, session limit policy settings appear in both Computer Configuration and User Configuration. If both policy settings are configured, the Computer Configuration policy setting takes precedence.

Policy settings configured using Citrix or Microsoft policies take precedence over settings configured in the properties of an active directory user account.

Additional information

Securing the environment

Deploying Citrix software updates and monitoring them using Director

Software update types

Citrix periodically releases software updates that could include bug fixes, security fixes, and enhancements for all currently supported versions of Citrix products.

Citrix releases general and limited release software updates. In some instances, software updates may be superseded or replaced. This happens only when a subsequent software update includes all fixes from the earlier software updates, as explained below.

Software update replacement

Any hotfix that includes all fixes from an earlier hotfix either supersedes or replaces the original hotfix, as mentioned in the following table:

<table>
<thead>
<tr>
<th>Original software update type</th>
<th>Subsequent software update type</th>
<th>Status of original software update</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limited release</td>
<td>General release</td>
<td>Superseded software update is no longer available</td>
<td>All customers can access the subsequent software update</td>
</tr>
<tr>
<td>Limited release</td>
<td>Limited release</td>
<td>Superseded software update is no longer available</td>
<td>Customers with access to the original software update can also access the subsequent software update</td>
</tr>
<tr>
<td>General release</td>
<td>General release</td>
<td>Superseded software update is no longer available</td>
<td>All customers can access the subsequent software update</td>
</tr>
<tr>
<td>General release</td>
<td>Limited release</td>
<td>Replaced but remains available for download from the Knowledge Center</td>
<td>Original software update remains available for customers who cannot access the limited release software update</td>
</tr>
</tbody>
</table>

© Copyright 2015 Citrix Systems, Inc.
**Limited release** | **General release** | **Superseded software update is no longer available** | **All customers can access the subsequent software update**
---|---|---|---
**Limited release** | **Limited release** | **Superseded software update is no longer available** | **Customers with access to the original software update can also access the subsequent software update**
**General release** | **General release** | **Superseded software update is no longer available** | **All customers can access the subsequent software update**
**General release** | **Limited release** | **Replaced but remains available for download from the Knowledge Center** | **Original software update remains available for customers who cannot access the limited release software update**

Citrix recommends you install general release software updates that are listed in the “Recommended software updates” section on [Support.citrix.com](http://Support.citrix.com).

**Monitoring software updates with Director**

When troubleshooting issues, it is useful to know what hotfixes are installed on the VDA. In both the Machine Details view and the User Details view, the installed hotfixes are listed. Admins can quickly determine what is installed and when that hotfix took effect. In addition, APIs are available so admins are able to quickly list all VDAs showing the hotfixes installed on each.

The hotfixes panel consists of details pertaining to the hotfixes installed on the machine selected. Details displayed include component, component version, hotfix name, hotfix file name, links to Knowledge Center articles, and effective date.

<table>
<thead>
<tr>
<th>Hotfixes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component</td>
</tr>
<tr>
<td>Virtual Desktop Agent - 64</td>
</tr>
<tr>
<td>Citrix Director VDA Plug-in</td>
</tr>
<tr>
<td>Virtual Desktop Agent - 64</td>
</tr>
</tbody>
</table>

**Configuration guidelines**

**Considerations prior to installation**

Citrix recommends that you thoroughly evaluate software updates on a test server or site. Ensure that you cover some testing comparable to the tasks of an everyday user, as well as some administrator-oriented tasks.

Examine the software update release notes. Release notes provide necessary information on the prerequisites and known installation issues. Common installation prerequisites may include an updated...
version of the license server, a particular redistributable (such as Java or .Net Framework), and so on. The release notes are kept up to date even after the software update is released to the web.

**Recommendations for upgrading the XenDesktop Site**

**Back up the database for the Site**

This must be performed regularly in any case, but a backup is advisable prior to any major change. Ensure that the backup completed successfully without any reported errors. Instructions for backing up the database is available at CTX135207 - How to Backup and Restore Your XenDesktop Database.

**Upgrade the license server**

If you upgrade the license server during the XenDesktop upgrade, ensure that the license server is upgraded before any of the other XenDesktop Controllers. If the license server is installed on a separate server, update this server before any of the other servers. If licenses have been purchased through the Subscription Advantage program, ensure that the license has been renewed recently so the license issue date is within one year of the release date of the version of XenDesktop you are upgrading to.

**Upgrade half of your desktop Delivery Controller servers**

Choose half of your servers to upgrade or apply the hotfix to first, leaving the other half of the servers to keep the Site running during the upgrade activities. On the first half of the servers, apply the upgrade or hotfix installers, and restart the server. The upgraded servers may now be incompatible with the earlier form of the database, so they may not participate in the functioning of the site at this point; this is expected, and the site can keep functioning using the nonupgraded servers until the database is itself upgraded.

**Upgrade the database**

Using the most recent version of Desktop Studio (that is, if upgrading to a new release that includes a new Desktop Studio version, the upgraded Desktop Studio must be used), start Desktop Studio, and view the dashboard for your Site. There is an update button at the top of the dashboard, which allows you to perform the update. When performing the update, you are given the option of either having Desktop Studio apply the update directly to the database or having Desktop Studio provide you with scripts, which you can run on the database at another time. If you wish to have Desktop Studio apply the update directly, you must run Desktop Studio as a user with the db_owner role on the database. When applying the upgrades directly from the Desktop Studio, a progress dialog is displayed followed by a success message. The success message notifies you if there are any controllers you must upgrade having completed the schema upgrade.

When you get the scripts from the Desktop Studio, then a directory window appears containing the script or scripts you must run. Further instructions on the use of these scripts are detailed in the header at the top of each script.

The upgrade to the database might require the site to be off-line while the actual database changes are performed. This is managed for you by Desktop Studio if it is applying the upgrade directly, but if the upgrade database script is to be applied manually, all the controllers in the site must be stopped while the script runs.

The database might now be incompatible with the non-upgraded servers, so they might not participate in the functioning of the site at this point, but the database must now be compatible with the servers that were upgraded earlier, which must allow the site to continue to function while the remaining servers are upgraded.

**Upgrade the remaining Controller Servers**

For any of the servers not chosen to be upgraded in the earlier upgrade step, apply the upgrade or hotfix installers and restart the server. All the servers must now be upgraded and the site must now be functioning at the fully upgraded state.
Updating VDA core services

For the VDA core services hotfixes, the OS type is designated in the hotfix name. “TS” for Terminal Server, the hotfix would apply to a Windows Server operating system. “WS” for workstation, the hotfix would apply to a desktop Windows operating system. There is no correlation between the hotfix numbering for the Server OS (TS) and Desktop OS (WS) hotfixes. The ICATS hotfix ending in 007 may not have the same fixed issues as the ICAWS hotfix ending in 007.

Example:

- A hotfix named ICAWS750WX86007 is a VDA core services hotfix for a Windows 7, 8, or 8.1 operating system (32-bit).
- A hotfix named ICATS750WX64007 is a VDA core services hotfix for a Windows Server 2008R2, 2012, or 2012R2 operating system (64-bit).

Special considerations

Limited Release Hotfixes must be installed only if the fix description applies to your environment.

Additional information

<table>
<thead>
<tr>
<th>Citrix Director 7.6 Deep-Dive Part 3: Determining installed hotfixes</th>
<th><a href="http://blogs.citrix.com/2014/10/23/citrix-director-7-6-deep-dive-part-3-determining-installed-hotfixes/">http://blogs.citrix.com/2014/10/23/citrix-director-7-6-deep-dive-part-3-determining-installed-hotfixes/</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Lifecycle Maintenance Hotfixes - Definitions and Examples</td>
<td><a href="http://support.citrix.com/article/CTX130337">http://support.citrix.com/article/CTX130337</a></td>
</tr>
<tr>
<td>Hotfix Name Changes for XenDesktop 7.1 and XenApp/XenDesktop 7.5</td>
<td><a href="http://support.citrix.com/article/CTX200156">http://support.citrix.com/article/CTX200156</a></td>
</tr>
</tbody>
</table>

Understanding Windows Update strategies

Update management gives you control over the deployment and maintenance of Microsoft software update releases in the production environment. It helps you maintain operational efficiency and effectiveness, overcome security vulnerabilities, and maintain a stable production environment.

Windows Server Update Services (WSUS) delivers core update management infrastructure in Windows with support for updating Windows Server system products and essential status reports that significantly increase administrative productivity and efficiency.

Microsoft updates are classified as important, recommended, optional, and featured. Here’s what they mean:

- Important updates offer significant benefits, such as improved security, privacy, and reliability. They should be installed as they become available and can be installed automatically with Windows Update.
- Recommended updates address noncritical problems or help enhance your computing experience. While these updates do not address fundamental issues with your computer or Windows software, they can offer meaningful improvements. These can be installed automatically.
- Optional updates can include updates, drivers, or new software from Microsoft to enhance your computing experience. You can only install these manually.
Citrix periodically releases interoperability and Microsoft software update validation reports and recommends reviewing these reports before deploying software updates to the production environment.

**Configuration guidelines**

When planning a Microsoft software updates strategy, use the following sources to get more information about compatibility and known issues:

**Additional information**

<table>
<thead>
<tr>
<th>Source</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Updates and Information</td>
<td><a href="http://support.citrix.com/pages/microsoft_security_past/">http://support.citrix.com/pages/microsoft_security_past/</a></td>
</tr>
<tr>
<td>Microsoft KB2601888: Available Updates for Remote Desktop Services (Terminal Services) on Windows Server 2008 R2 SP1</td>
<td><a href="http://support.microsoft.com/kb/2601888">http://support.microsoft.com/kb/2601888</a></td>
</tr>
</tbody>
</table>

**Understanding network firewall configurations**

Enterprise network firewalls are essential part of healthcare environments. Citrix products are compatible with networks separated by firewalls; however, it’s important to understand how Citrix components communicate over the network.

Citrix recommends using next-generation firewalls with deep packet inspection and application identification that provides best available network security.

**Configuration guidelines**

Check with the vendor documentation, and understand your organization’s security regulations to verify the best practices for network firewall configurations.

Use documents referenced below as a starting point when configuring network firewalls. Remember that Citrix XenDesktop is installed on top of Microsoft OS and includes Microsoft guidelines.

**Special considerations**

If your firewall supports RPC protocol inspection and filtering, use PortQry utility to identify the end points that are currently registered with the RPC endpoint mapper.

Citrix StoreFront uses Microsoft.Net NetPeerTcpBinding, which negotiates a random port on each server between the peers. This protocol requires IPv6 to be enabled on StoreFront servers.

**Additional information**

<table>
<thead>
<tr>
<th>Document</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTX101810: Communication Ports Used By Citrix Technologies</td>
<td><a href="http://support.citrix.com/article/ctx101810">http://support.citrix.com/article/ctx101810</a></td>
</tr>
</tbody>
</table>
Microsoft KB832017: Service overview and network port requirements for Windows  
http://support.microsoft.com/KB/832017

Microsoft KB929851: The default dynamic port range for TCP/IP has changed in Windows Vista and in Windows Server 2008  
http://support.microsoft.com/kb/929851

New features and functionality in PortQry version 2.0  
http://support.microsoft.com/kb/832919

Configuring the Windows firewall

Because Windows Firewall With Advanced Security plays an important part in helping to protect your computer from security threats, we recommend that you do not disable it unless you install another firewall from a reputable vendor that provides an equivalent level of protection.

You cannot uninstall Windows Firewall With Advanced Security; you can only disable the firewall functionality.

Microsoft does not support stopping the firewall service (or a third-party firewall service) except for troubleshooting, even if you are behind another edge/perimeter firewall. If another machine on the local subnet gets infected, a machine that is not running a host firewall is vulnerable.

Configuration guidelines

Check with the vendor documentation, and understand your organization’s security regulations to verify the best practices for configuring the Windows firewall.

Special considerations

Do not disable Windows Firewall by stopping the service. Instead, use Group Policy settings to turn off the firewall if needed. If you turn off the Windows Firewall With Advanced Security service, you lose other benefits provided by the service, such as the ability to use IPsec connection security rules, Windows Service Hardening, and network protection from attacks that employ network fingerprinting. Non-Microsoft Firewall software that is compatible with Windows can programmatically disable only the parts of Windows Firewall With Advanced Security that need to be disabled for compatibility. You should not disable the firewall yourself for this purpose. Microsoft does not support stopping the service associated with Windows Firewall With Advanced Security.

Additional information

Windows Firewall Integration and Best Practices  

Windows Firewall Troubleshooting Situations  

I Need to Disable Windows Firewall  

Error: Unable to Create Deployment in StoreFront  
http://support.citrix.com/article/CTX138959

© Copyright 2015 Citrix Systems, Inc.
Hypervisor security hardening considerations

Most of the new XenDesktop deployments in healthcare are fully virtualized. The hypervisor is a core platform that has access to all child virtual machines, and it’s important to implement hardening, or locking down the virtual environment.

There are five primary areas that need to be secured:

- Virtual machines
- Management console or management server
- Hosts
- Configuration database
- Hardware security

A virtual machine in most cases is equivalent to a physical server. The guest operating system that runs in the virtual machine is subject to the same security hardening recommendations as a physical system.

Configuration guidelines

When implementing hypervisors in an environment that requires a higher level of security, it is recommended that you follow the vendor documentation regarding this type of installation.

Additional information

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix XenServer free/advanced 5.6 Hardening guide</td>
<td><a href="http://www.ptsecurity.com/download/XenServer-Free-5-6-SHG.pdf">http://www.ptsecurity.com/download/XenServer-Free-5-6-SHG.pdf</a></td>
</tr>
<tr>
<td>Common Criteria Documents for XenServer 6.0.2</td>
<td><a href="http://www.citrix.com/support/security-compliance/common-criteria.html">http://www.citrix.com/support/security-compliance/common-criteria.html</a></td>
</tr>
</tbody>
</table>

NetScaler security hardening considerations

A Citrix NetScaler appliance is a multifunctional device that accelerates websites, acts as an ICA proxy and SSL-VPN, provides L4-7 traffic management, offers an integrated application firewall, and offloads servers.

To maintain security through the deployment lifecycle, Citrix recommends the following security considerations:
• Physical security
• Appliance security
• Network security
• Administration and management

Different deployments may require different security considerations.

**Configuration guidelines**

If you are looking for information regarding the NetScaler security hardening considerations, it’s recommended that you follow the Citrix documentation at Support.Citrix.com/proddocs, as well as the information below:

**Additional information**

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP Configuration on NetScaler to Avoid Traffic Amplification Attack</td>
<td><a href="http://support.citrix.com/article/CTX200286">http://support.citrix.com/article/CTX200286</a></td>
</tr>
<tr>
<td>How to Secure SSH Access to the NetScaler Appliance with Public Key Authentication</td>
<td><a href="http://support.citrix.com/article/CTX109011">http://support.citrix.com/article/CTX109011</a></td>
</tr>
<tr>
<td>How to Secure Communication Between the NetScaler Appliances</td>
<td><a href="http://support.citrix.com/article/CTX114087">http://support.citrix.com/article/CTX114087</a></td>
</tr>
<tr>
<td>How to Replace Certificates on a NetScaler Appliance</td>
<td><a href="http://support.citrix.com/article/CTX117487">http://support.citrix.com/article/CTX117487</a></td>
</tr>
</tbody>
</table>

**Virtual Desktop security hardening considerations**

Citrix recommends configuring virtual desktops to prevent Windows machines from being compromised by attackers. There are multiple recommendations available that help harden the system to reduce the attack surface.

It is important to establish baselines and regularly compare the current running system to ensure it has not modified.

Microsoft Windows is a general-purpose operating system and as such has many features designed to fit many use cases. A properly hardened virtual machine will deny and prevent hackers with layers of security.

**Configuration guidelines**

If you are looking for information regarding virtual desktop security considerations, it’s recommended that you reference the following Microsoft documentation:
Preventing brute-force logon attacks to NetScaler Gateway

A common threat many enterprises face is a password-guessing attack known as a brute-force attack — an attempt to identify a password by systematically examining every possible combination of letters, numbers, and symbols until one correct combination is discovered. NetScaler stands as the entry point to your network and requires user authentication, which makes it a good target for a brute-force attack.

These kinds of attacks are dangerous even if you have a properly configured password complexity policy because brute-force attacks can lead to account lockouts.

Configuration guidelines

To prevent account lockouts caused by brute-force attacks, Citrix recommends configuring two-factor authentication, which NetScaler Gateway supports. Normally, when authenticating users, NetScaler Gateway stops the authentication process as soon as it successfully authenticates a user through any of the configured authentication methods. In certain instances, you may need to authenticate a user to one server but extract groups from a different server. For example, if your network authenticates users against a RADIUS server, but you also use RSA SecurID token authentication and user groups are stored on that server, you may need to authenticate users to that server so you can extract the groups.

If users are authenticated by using two authentication types, and if one of those types is client certificate authentication, you can configure the certificate authentication policy as the second method of authentication. For example, you use LDAP as your primary authentication type and the client certificate as the secondary authentication. When users log on with their user name and password, they then have access to network resources.

If second factor authentication is not available, Citrix recommends use of Rate Limiting feature to block attackers.

Additional information

<table>
<thead>
<tr>
<th>Additional information</th>
<th>URL</th>
</tr>
</thead>
</table>

Configuring Multifactor Authentication
http://support.citrix.com/proddocs/topic/netscaler-gateway-105/ng-multifactor-authen-wrapper-con.html

© Copyright 2015 Citrix Systems, Inc.
<table>
<thead>
<tr>
<th>Topic</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>How to Implement Exponential Back-off Algorithm on a NetScaler Appliance</td>
<td><a href="http://support.citrix.com/article/CTX136565">http://support.citrix.com/article/CTX136565</a></td>
</tr>
</tbody>
</table>

### Configuring antivirus on the VDA

Real-time antivirus scanning often can cause performance degradation and stability issues to many software products, including XenDesktop. The common practice is to configure exclusion lists for specific folders and files.

#### Configuration guidelines

The recommendations below contain general antivirus recommendations that should be reviewed prior to implementing any type of exclusions or optimizations:

- If organizations choose to exclude particular files or folders as part of real-time or on-access scanning, Citrix recommends scanning the excluded files and folders on a regular basis using scheduled scans. It is recommended to perform scheduled scans during nonbusiness or off-peak hours to mitigate any potential performance impact.

- Integrity of excluded files and folders should be maintained at all times. Organizations should consider leveraging a commercial File Integrity Monitoring or Host Intrusion Prevention solution to protect the integrity of files and folders that have been excluded from real-time or on-access scanning. It should be noted that database and log files should not be included in this type of data integrity monitoring because these files are expected to change.

- If an entire folder must be excluded from real-time or on-access scanning, Citrix recommends monitoring very closely the creation of new files in the excluded folders.

Based on Citrix Consulting’s field experience, organizations should consider configuring antivirus software on XenApp and XenDesktop servers with the following settings:

- Scan on write events or only when files are modified. It should be noted that this configuration is typically regarded as a high security risk by most antivirus vendors. In high-security environments such as those in healthcare, organizations should consider scanning on both read and write events to protect against threats that target memory, such as Conficker variants.

- Scan local drives or disable network scanning. This assumes all remote locations, which may include file servers that host user profiles and redirected folders, are being monitored by antivirus and data integrity solutions.

- Exclude the pagefile(s) from being scanned.

- Exclude the Print Spooler directory from being scanned.
• Remove any unnecessary antivirus related entries from the Run key (HKLM\Software\Microsoft\Windows\Current Version\Run).

• If pass-through authentication is being used, for example, in a XenDesktop or Shared Hosted desktop scenario, exclude the XenApp Online Plug-in bitmap cache directory (typically %AppData%\ICAClient\Cache).

If using the streamed user profile feature of Citrix Profile management, ensure the antivirus solution is configured to be aware of Hierarchical Storage Manager (HSM) drivers.

Additional information

<table>
<thead>
<tr>
<th>Provisioning Services Antivirus Best Practices</th>
<th><a href="http://support.citrix.com/article/CTX124185">http://support.citrix.com/article/CTX124185</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Guidelines for Antivirus Software Configuration</td>
<td><a href="http://support.citrix.com/article/CTX127030">http://support.citrix.com/article/CTX127030</a></td>
</tr>
<tr>
<td>Virus scanning recommendations for Enterprise computers that are running currently supported versions of Windows</td>
<td><a href="http://support.microsoft.com/kb/822158">http://support.microsoft.com/kb/822158</a></td>
</tr>
<tr>
<td>Profile streaming and enterprise antivirus products</td>
<td><a href="http://support.citrix.com/proddocs/topic/user-profile-manager-5-x/upm-secure-antivirus.html">http://support.citrix.com/proddocs/topic/user-profile-manager-5-x/upm-secure-antivirus.html</a></td>
</tr>
<tr>
<td>Citrix Consolidated List of Antivirus Exclusions</td>
<td><a href="http://blogs.citrix.com/2013/09/22/citrix-consolidated-list-of-antivirus-exclusions/">http://blogs.citrix.com/2013/09/22/citrix-consolidated-list-of-antivirus-exclusions/</a></td>
</tr>
</tbody>
</table>

Data integrity

Enabling StoreFront ICA file signing

In healthcare’s locked-down environments, it is very important to ensure that users can connect only to approved resources. This includes connections made using Citrix Receiver.

Citrix StoreFront provides the option to sign ICA files digitally to ensure that Citrix Receiver for Windows can verify that ICA file comes from a trusted source. When ICA file signing is configured on the StoreFront server, the ICA file that is generated when a user starts an application is digitally signed using a certificate installed on the StoreFront server.

The client side of the connection can be configured to enforce signature validation. If a signature is valid, the thumbprint of the signing certificate is validated against the list of trusted certificate thumbprints. This means that connections using an ICA file signed by a third-party certificate will not be established unless the thumbprint of the certificate is explicitly added to the list of trusted certificate thumbprints.

When an ICA file is signed, a new section called [DigitalSignature] is added to the bottom. It contains the key value pair - signature=. Following the equals sign is the BASE64 encoded digital signature covering everything in the ICA file. The digital signature is in the detached X.509 digital signature format or the detached PKCS #7 digital signature format. It contains both the hash algorithm name as well as the full signer certificate. SHA-1 and SHA-256 FIPS-approved algorithms for digital signature generation can be used.
Configuration guidelines

To be used for ICA file signing with StoreFront, certificates must include the private key and be within the allowed validity period. If the certificate contains a key usage extension, this must allow the key to be used for digital signatures. Where an extended key usage extension is included, it must be set to code signing or server authentication.

The allowed Extended Key Usage (EKU) types are:

- Code-signing
- Server authentication

Follow the Citrix StoreFront documentation to configure file signing on StoreFront.

Citrix recommends using the SHA-256 algorithm and avoiding SHA-1.

The whitelist of certificate thumbprints is configured using GPO and stored in the client computer registry. To configure the whitelist and signature verification enforcement, use ica-file-signing.adm GPO administrative template located in C:\Program Files\Citrix\ICA Client\Configuration folder.

Special considerations

Clients that do not support the feature or are not configured for ICA file signing ignore the digital signature.

This feature does not protect the confidentiality of any information contained within the ICA file.

Additional information

| ICA File Signing to protect against application or desktop launches from untrusted servers | http://support.citrix.com/proddocs/topic/receiver-windows-42/ica-ica-file-signing.html |

Enabling Receiver CRL verification

When client connections to XenApp and XenDesktop applications are secured using SSL/TLS, it is critical to ensure that certificates are valid and not compromised. Certificate Revocation List (CRL) is one of the standard methods used to verify digital certificate status. This list contains IDs of revoked certificates along with the reasons for revocation. It also includes the dates of certificate issue and the certificate authorities that issued them. When Citrix Receiver attempts to access a published desktop or application, it can check CRL to ensure that the certificate is still valid.

Configuration guidelines

CRL checking must be configured on the client side; Additionally, SSLCertificateRevocationCheckPolicy can be configured in ICA file template on the StoreFront server.

You can use group policy to configure Citrix Receiver for CRL checking using the Group Policy Editor or Group Policy Management Console and importing the administrative template file icaclient.adm that is located in C:\Program Files\Citrix\ICA Client\Configuration folder on the computer where Citrix Receiver is installed.

From the Group Policy Editor, expand Administrative Templates, and navigate through Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification.

There are four options available in the CRL verification drop-down menu:
• **Disabled.** No certificate revocation list checking is performed.

• **Only check locally stored CRLs.** CRLs that were installed or downloaded previously are used in certificate validation. The connection fails if the certificate is revoked.

• **Require CRLs for connection.** CRLs locally and from relevant certificate issuers on the network are checked. The connection fails if the certificate is revoked or not found.

• **Retrieve CRLs from network.** CRLs from the relevant certificate issuers are checked. The connection fails if the certificate is revoked.

To configure SSLCertificateRevocationCheckPolicy on the StoreFront server, Complete the following steps:

• Open C:\inetpub\wwwroot\Citrix\StoreName\App_Data\default.ica file in Notepad.

• Under the [WFClient] section of the file, add the following line:

```plaintext
SSLCertificateRevocationCheckPolicy=<Value>.
```

• Where value is one of the following:

  o NoCheck. No Certificate Revocation List check is performed.

  o CheckWithNoNetworkAccess. Certificate revocation list check is performed. Only local certificate revocation list stores are used. All distribution points are ignored. Finding a Certificate Revocation List is not critical for verification of the server certificate presented by the target SSL Relay/Secure Gateway server.

  o FullAccessCheck. Certificate Revocation List check is performed. Local Certificate Revocation List stores and all distribution points are used. Finding a Certificate Revocation List is not critical for verification of the server certificate presented by the target SSL Relay/Secure Gateway server.

  o FullAccessCheckAndCRLRequired. Certificate Revocation List check is performed. Local Certificate Revocation List stores and all distribution points are used. Finding all required Certificate Revocation Lists is critical for verification.

**Special considerations**

When CRL verification is enabled, ensure that CRLs are available on the network. When using Microsoft certification authority, CRL URLs can be HTTP, FTP, LDAP, or FILE addresses. If using LDAP or FILE addresses, make sure that client has permissions to access CRL, especially when the client is in another Active Directory domain.

When CRL verification is configured both on the StoreFront and using GPO, GPO configuration takes precedence.

**Additional information**

<table>
<thead>
<tr>
<th>To enable certificate revocation list checking for improved security with Receiver</th>
<th><a href="http://support.citrix.com/proddocs/topic/receiver-windows-42/ica-cert-revocation-list-enable-v2.html">http://support.citrix.com/proddocs/topic/receiver-windows-42/ica-cert-revocation-list-enable-v2.html</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Client SSL Error Codes</td>
<td><a href="http://support.citrix.com/article/CTX113309">http://support.citrix.com/article/CTX113309</a></td>
</tr>
</tbody>
</table>
Verifying the integrity of installation sources and updates

Citrix recommends you obtain all necessary software and updates from their respective vendors to minimize the risk of compromised software and mismatched drivers for various platforms.

Corrupted software images can lead to problems during installation. Therefore, it is a good practice to check the integrity of the downloaded software image.

Rather than identifying the contents of a file by its file name, extension, or other designation, a hash assigns a unique value to the contents of a file. File names and extensions can be changed without altering the content of the file and without changing the hash value. Similarly, the file’s content can be changed without changing the name or extension. However, changing even a single character in the contents of a file changes the hash value of the file.

Configuration guidelines

Checking the integrity of the ISO image in the Windows operating system

Get-FileHash PowerShell cmdlet computes the hash value for a file by using a specified hash algorithm. By default, the Get-FileHash cmdlet uses the SHA256 algorithm; although, any of following hash algorithm can be used:

- SHA1.
- SHA256.
- SHA384.
- SHA512.
- MACTripleDES.
- MD5.
- RIPEMD160.

Alternatively, the File Checksum Integrity Verifier (FCIV) utility can generate MD5 or SHA-1 hash values for files to compare the values against a known good value. FCIV can compare hash values to make sure that the files have not been changed.

FCIV utility can be downloaded from Microsoft - http://support.microsoft.com/kb/841290

For instructions on how to use FCIV consult with following Citrix KB Article: CTX116166: How to Verify Downloaded ISO Images - http://support.citrix.com/article/CTX116166

Checking integrity of the NetScaler firmware file

To verify the integrity of a NetScaler firmware file and to confirm that the checksum file is not tampered or corrupted in network transfer. Use one of the following two checksum:

- sha2 for NetScaler Release 10.1 and later.
- MD5 for earlier NetScaler releases.

For detailed instructions, consult with following Citrix KB Article: CTX137749: How to Verify the Integrity of the NetScaler Firmware File - http://support.citrix.com/article/CTX137749

Additional information

How to Verify Downloaded ISO Images  http://support.citrix.com/article/ctx116166
How to Verify the Integrity of the NetScaler Firmware File

Get-FileHash

Transmission Security

Securing access with NetScaler

NetScaler AppFirewall prevents inadvertent or intentional disclosure of confidential information and aids in compliance with information security regulations such as PCI-DSS.

AppFirewall can tailor security policies for any application, including those using client-side JavaScript, and automatically determines the behavior of an application to strengthen security policies and enable permissible application behavior. Installation is made easy by leveraging an existing signature base for scanning known attacks.

NetScaler AppFirewall technology is included with Citrix NetScaler MPX and VPX, Platinum Edition, and is available as an optional module that can be added to NetScaler MPX appliances running NetScaler Enterprise Edition. NetScaler AppFirewall is also available as a stand-alone solution on seven NetScaler MPX appliances. The stand-alone NetScaler AppFirewall models can be upgraded via software license to a full NetScaler Application Delivery Controller (ADC).

The NetScaler Gateway module provides the Access Gateway ICA Proxy to connect hosted application and desktop execution to the Citrix Receivers on user systems. Before starting ICA relay, the Gateway receives Secure Ticket Authority (STA) tickets and commands to define proxy relays from specific host systems to specific user machines. The gateway relays ICA data only to/from specific endpoints. There is no traditional VPN between the protected and nonprotected spaces.

Configuration guidelines

Physical Security

You must deploy the NetScaler appliance in a secure location. NetScaler is intended to be physically secured from theft or tampering.

Appliance Security

- Protect the console port from unauthorized access. The serial console port can be used to configure and reset the appliance.
- Perform remote software updates. Apply updates as available to remediate any known issues. When updating the NetScaler, use a secure protocol like SFTP or HTTPS. Note: Updates require a system restart.
- Do not modify system software. NetScaler is provided as a managed appliance, and apart from performing remote software updates, additional hardening or modification of system software is not necessary or desirable. Contact Citrix Support with any additional questions.
- Secure the front panel. Ensure that those with physical access to the machine do not modify the front panel settings once the appliance has been configured.

Network Security

- Non-routable management IP. Ensure the management IP is not routable on the public Internet and is behind a firewall.
- Placement in the network. Review your organizational policy and compliance requirements to determine if NetScaler needs to be deployed behind a stateful firewall.

© Copyright 2015 Citrix Systems, Inc.
NetScaler Gateway Security

Use default DENY. Globally deny all resources and use authorization policies to selectively enable access to resources on a per-group basis by setting the value of the defaultAuthorizationAction parameter to “Allow” or “Deny” as is required. The value of this parameter decides whether the default authorization action should be Allow or Deny. In NetScaler 10, by default, the authorization action is set to Deny. Users should ensure that this value is Deny by default and they should give the access explicitly. To set the authorization action to Deny, at the NetScaler command prompt, type:

```
set vpn parameter -defaultAuthorizationAction DENY
```

Configure NetScaler to drop and log invalid HTTP requests by running the following command at the NetScaler command prompt:

```
set ns httpParam [-dropInvalReqs ( ON | OFF )]
```

Additional information

<table>
<thead>
<tr>
<th>Application Firewall</th>
<th><a href="http://support.citrix.com/proddocs/topic/ns-security-10-5-map/appfw-wrapper-con-10.html">http://support.citrix.com/proddocs/topic/ns-security-10-5-map/appfw-wrapper-con-10.html</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>NetScaler VPX How To: Initial App Firewall Configuration</td>
<td><a href="http://www.citrix.com/tv/#videos/1314">http://www.citrix.com/tv/#videos/1314</a></td>
</tr>
<tr>
<td>Basic Application Firewall Configuration</td>
<td><a href="http://www.citrix.com/tv/#videos/752">http://www.citrix.com/tv/#videos/752</a></td>
</tr>
<tr>
<td>Application Firewall Overview &amp; Demo</td>
<td><a href="http://www.citrix.com/tv/#videos/11000">http://www.citrix.com/tv/#videos/11000</a></td>
</tr>
</tbody>
</table>

Ensuring FIPS compliance of SSL server communications

To make a XenApp or XenDesktop deployment FIPS 140 compliant, you need to consider each communication channel within the installation.

To ensure only FIPS 140 compliant cipher suites and cryptographic modules are used within the deployment, you must apply FIPS 140 compliant group policies. Both root and server authentication certificates must be installed on all the computers that use IPsec with certificate authentication. All the user devices must have Certificate Authority (CA) root certificates installed that match the server authentication certificates installed on the servers running the StoreFront.

The NetScaler MPX FIPS edition is a hardened, physical appliance that is traditionally deployed in the DMZ to provide secure remote access to XenDesktop and XenApp environments. It provides FIPS 140-2 Level 2 SSL encryption of traffic to encrypt and secure communication between Citrix Receiver and the NetScaler MPX appliance, and between NetScaler MPX and XenApp/XenDesktop VDA and Web Interface.

Configuration guidelines

XenApp, XenDesktop, and StoreFront can be configured to use government-approved cryptography to protect “sensitive but unclassified” data by using the applicable ciphersuites:

- RSA_WITH_3DES_EDE_CBC_SHA supports RSA key exchange and TripleDES encryption, as defined in Internet RFC 2246 [http://www.ietf.org/rfc/rfc2246.txt](http://www.ietf.org/rfc/rfc2246.txt).
Special considerations

Three cipher suites are supported: GOV(ernment), COM(mercial), and ALL. The ciphers in those cipher suites depend on the Windows FIPS mode; see [FIPS](http://support.microsoft.com/kb/811833) for information about Windows FIPS mode. The following table lists the ciphers in each supported cipher suite:

### Additional information

<table>
<thead>
<tr>
<th>Description</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL Ciphers Available on a NetScaler VPX Appliance</td>
<td><a href="http://support.citrix.com/article/CTX126386">http://support.citrix.com/article/CTX126386</a></td>
</tr>
<tr>
<td>FAQ: FIPS-enabled NetScaler MPX Appliance</td>
<td><a href="http://support.citrix.com/article/ctx129543">http://support.citrix.com/article/ctx129543</a></td>
</tr>
<tr>
<td>&quot;System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing&quot; security setting effects in Windows XP and in later versions of Windows</td>
<td><a href="http://support.microsoft.com/kb/811833">http://support.microsoft.com/kb/811833</a></td>
</tr>
</tbody>
</table>

### Configuring end-to-end TLS (SSL) communication

Administrators can increase security on XenApp or XenDesktop by configuring the Site to use the Transport Layer Security (TLS) security protocol on the Controller or between end users and VDAs. You can enable TLS security protocol on a Site to provide server authentication, data stream encryption, and message integrity checks for a TCP/IP connection.

When you configure TLS on VDAs, it changes permissions on the installed TLS certificate, giving the ICA Service read access to the certificate’s private key, and informing the ICA Service of the following:
- Which certificate in the certificate store to use for SSL.
- Which TCP port number to use for SSL connections.
  - The Windows Firewall (if it is enabled) must be configured to allow incoming connection on this TCP port. This configuration is done for you when you use the PowerShell script.
- Which versions of the SSL protocol to allow.
  - The supported SSL protocol versions follow a hierarchy (lowest to highest): SSL 3.0, TLS 1.0, TLS 1.1, and TLS 1.2. You specify the minimum allowed version; all protocol connections using that version or a higher version are allowed. For example, if you specify TLS 1.1 as the minimum version, then TLS 1.1 and TLS 1.2 protocol connections are allowed. If you specify SSL 3.0 as the minimum version, then connections for all the supported versions are allowed. If you specify TLS 1.2 as the minimum version, only TLS 1.2 connections are allowed.
- Which SSL ciphers to allow.
  - A cipher suite is a list of common SSL ciphers. When a client connects and sends a list of supported SSL ciphers, the VDA matches one of the client’s ciphers with one of the ciphers in its configured cipher suite and accepts the connection. If the client sends a cipher that is not in the VDA’s cipher suite, the VDA rejects the connection.
  - Three cipher suites are supported: GOV(ernment), COM(mercial), and ALL. The ciphers in those cipher suites depend on the Windows FIPS mode; see http://support.microsoft.com/kb/811833 for information about Windows FIPS mode.

<table>
<thead>
<tr>
<th>SSL cipher suite</th>
<th>GOV</th>
<th>COM</th>
<th>ALL</th>
<th>GOV</th>
<th>COM</th>
<th>ALL</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIPS Mode</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>On</td>
<td>On</td>
<td>On</td>
</tr>
<tr>
<td>RSA_KEYX</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>RSA_SIGN</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>3DES</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RC4</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MD5</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>SHA_256</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>SHA_384</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>SHA_512</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>AES</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

A Delivery Group cannot have a mixture of some VDAs with SSL configured and some VDAs without SSL configured. When you configure SSL for a Delivery Group, you should have already configured SSL for all of the VDAs in that Delivery Group.

© Copyright 2015 Citrix Systems, Inc.
Communication between Citrix clients and the StoreFront server consists of passing several different types of data. As users identify themselves, browse their resources, and select a resource to access, the web browser/Receiver and web server pass user credentials, resource sets, and session initialization files. Specifically, this network traffic includes:

- **HTML form data.** StoreFront sites use a standard HTML form to transmit user credentials from the web browser to the web server when users log on. The StoreFront form passes user names and credentials in clear text.

- **HTML pages and session cookies.** After users enter their credentials on the log-on screen, the credentials are stored on the web server and are protected by a session cookie. The HTML pages sent from the web server to the browser contain resource sets. These pages list the resources available to the user.

- **ICA files.** When a user selects a resource, the web server sends an .ica file for that resource to the Citrix client (in some cases using the web browser as an intermediary). The .ica file contains a ticket that can be used to log on to the server. ICA files do not include a ticket for pass-through or smart card authentication. The ICA File Signing feature allows users to verify that they are launching applications or desktops from a trusted web server.

- Because the user device to web server communication is typically routed over networks outside the data center boundaries or on completely untrusted connections (such as the Internet), Citrix strongly recommends encrypting this traffic by means of SSL.

**Configuration guidelines**

Configuring a XenApp or XenDesktop Site to use the Secure Sockets Layer (SSL) security protocol includes the following procedures:

- Obtain, install, and register a server certificate on all Delivery Controllers, and configure a port with the SSL certificate. For details, see [Install SSL server certificates on Controllers](#). Optionally, you can change the ports the Controller uses to listen for HTTP and HTTPS traffic.

- Enable SSL connections between users and VDAs by completing the following tasks:

  - Configure SSL on the machines where the VDAs are installed. You can use a PowerShell script supplied by Citrix or configure it manually. For general information, see [About SSL settings on VDAs](#). For details, see [Configure SSL on a VDA using the PowerShell script](#) and [manually configure SSL on a VDA](#).

  - Configure SSL in the Delivery Groups containing the machines where the VDAs are installed by running a set of PowerShell cmdlets in Studio. For details, see [Configure SSL on Delivery Groups](#). Requirements and considerations:

    - Enabling SSL connections between users and machines where the VDAs are installed is valid only for XenApp 7.6 and XenDesktop 7.6 Sites, plus later supported releases.

    - Configure SSL in the Delivery Groups and on the machines where the VDAs are installed after you install components, create a Site, create machine catalogs, and create Delivery Groups. To configure SSL in the Delivery Groups, you must have permission to change Controller access rules; a Full Administrator has this permission.

    To configure SSL on the VDAs, you must be a Windows administrator on the machine where the VDA is installed.

    If you intend to configure SSL on VDAs that have been upgraded from earlier versions, uninstall any SSL relay software on those machines before upgrading them.

    The PowerShell script configures SSL on static VDAs; it does not configure SSL on pooled VDAs that are provisioned by Machine Creation Services or Provisioning Services, where the machine image resets on each restart.

  © Copyright 2015 Citrix Systems, Inc.
The following steps are needed to configure SSL communications with the VDA.

Install SSL server certificates on Controllers

- For HTTPS, the XML Service supports SSL features through the use of server certificates, not client certificates. To obtain, install, and register a certificate on a Controller, and to configure a port with the SSL certificate:
  - If the Controller has IIS installed, follow the guidance in http://support.microsoft.com/kb/299875.
  - If the Controller does not have IIS installed, one method of configuring the certificate is:
    - If you intend to use the PowerShell script to configure SSL on VDAs, and unless you intend on specifying the SSL certificate’s thumbprint, make sure the certificate is located in the Local Computer > Personal > Certificates area of the certificate store. If more than one certificate resides in that location, the first one found will be used.
  - Configure a port with the certificate; see http://msdn.microsoft.com/en-us/library/ms733791%28v=vs.110%29.aspx.

Change HTTP or HTTPS ports

By default, the XML Service on the Controller listens on port 80 for HTTP traffic and port 443 for HTTPS traffic. Although you can use nondefault ports, be aware of the security risks of exposing a Controller to untrusted networks. Deploying a standalone StoreFront server is preferable to changing the defaults.

To change the default HTTP or HTTPS ports used by the Controller, run the following command from Studio: BrokerService.exe -WSPORT <http-port> -WISSPORT <https-port>
where <http-port> is the port number for HTTP traffic and <https-port> is the port number for HTTPS traffic.

Note: After changing a port, Studio might display a message about license compatibility and upgrading. To resolve the issue, re-register service instances using the following PowerShell cmdlet sequence:

```
Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding XML_HTTPS | Unregister-ConfigRegisteredServiceInstance
Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" | Register-ConfigServiceInstance
```

If you want the XML Service to ignore HTTP or HTTPS traffic on the default ports, set the following registry values in HKLM\Software\Citrix\DesktopServer on the Controller and restart the Broker Service.

To ignore HTTP traffic, set XmlServicesEnableNonSsl to 0.
To ignore HTTPS traffic, set XmlServicesEnableSsl to 0.

Configure SSL on a VDA using the PowerShell script

The Enable-VdaSSL.ps1 script enables or disables the SSL listener on a VDA. This script is available in the Support > Tools > SslSupport folder on the installation media.

When you enable SSL, the script disables all existing Windows Firewall rules for the specified TCP port before adding a new rule that allows the ICA Service to accept incoming connections only on the SSL TCP port. It also disables the Windows Firewall rules for:

- Citrix ICA (default: 1494).
- Citrix CGP (default: 2598).
- Citrix WebSocket (default: 8008).
The result is that users can connect only over SSL; they cannot use raw ICA, CGP, or WebSocket to connect. The script contains the following syntax descriptions, plus additional examples; you can use a tool such as Notepad++ to review this information.

You must specify either the –Enable or –Disable parameter; all other parameters are optional.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-Enable</td>
<td>Installs and enables the SSL listener on the VDA. Either this parameter or the –Disable parameter is required.</td>
</tr>
<tr>
<td>-Disable</td>
<td>Disables the SSL listener on the VDA. Either this parameter or the –Enable parameter is required. If you specify this parameter, no other parameters are valid.</td>
</tr>
<tr>
<td>–SSLPort &lt;port&gt;</td>
<td>SSL port. Default: 443</td>
</tr>
<tr>
<td>-SSLMinVersion &quot;&lt;min-ssl-version&gt;&quot;</td>
<td>Minimum SSL protocol version, enclosed in quotation marks. Valid values: &quot;SSL_3.0&quot;, &quot;TLS_1.0&quot;, &quot;TLS_1.1&quot;, and &quot;TLS_1.2&quot;. Default: &quot;TLS_1.0&quot;</td>
</tr>
<tr>
<td>-SSLCipherSuite &quot;&lt;suite&gt;&quot;</td>
<td>SSL cipher suite, enclosed in quotation marks. Valid values: &quot;GOV&quot;, &quot;COM&quot;, and &quot;ALL&quot;. Default: &quot;ALL&quot;</td>
</tr>
<tr>
<td>-CertificateThumbPrint &quot;&lt;thumbprint&gt;&quot;</td>
<td>Thumbprint of the SSL certificate in the certificate store, enclosed in quotation marks. This parameter is generally used when the certificate store has multiple certificates; the script uses the thumbprint to select the certificate you want to use. Default: the first available certificate found in the Local Computer &gt; Personal &gt; Certificates area of the certificate store.</td>
</tr>
</tbody>
</table>

**Manually configure SSL on a VDA**

When configuring SSL on a VDA manually, you grant generic read access to the SSL certificate’s private key for the appropriate service on each VDA: NT SERVICE\PorticaService for a VDA for Windows Desktop OS, or NT SERVICE\TermService for a VDA for Windows Server OS. On the machine where the VDA is installed:

- Launch the Microsoft Management Console (MMC): Start > Run > mmc.exe.
- Add the Certificates snap-in to the MMC.
- Select File > Add/Remove Snap-in.
- Select Certificates and then click Add.
- When prompted with “This snap-in will always manage certificates for:” choose “Computer account” and then click Next.
- When prompted with “Select the computer you want this snap-in to manage” choose “Local computer” and then click Finish.
- Under Certificates (Local Computer) > Personal > Certificates, right-click the certificate and then select All Tasks > Manage Private Keys.
- The Access Control List Editor displays “Permissions for (FriendlyName) private keys” where (FriendlyName) is the name of your SSL certificate. Add one of the following services and give it Read access:
  - For a VDA for Windows Desktop OS, "PORTICASERVICE".
For a VDA for Windows Server OS, "TERMSERVICE".

- Double-click the installed SSL certificate. In the certificate dialog, select the Details tab and then scroll to the bottom. Click Thumbprint.

- Run regedit and go to HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd.

- Edit the SSL Thumbprint key and copy the value of the SSL certificate’s thumbprint into this binary value. You can safely ignore unknown items in the Edit Binary Value dialog box (such as '0000' and special characters).

- Edit the SSLEnabled key and change the DWORD value to 1. (To disable SSL later, change the DWORD value to 0.)

- If you want to change the default settings (optional), use the following in the same registry path:
  - SSLMinVersion DWORD – 1 = SSL 3.0, 2 = TLS 1.0, 3 = TLS 1.1, 4 = TLS 1.2. Default: 2 (TLS 1.0).
  - SSLCipherSuite DWORD – 1 = GOV, 2 = COM, 3 = ALL. Default: 3 (ALL).

- Ensure the SSL TCP port is open in the Windows Firewall if it is not the default 443. (When you create the inbound rule in Windows Firewall, make sure its properties have the "Allow the connection" and "Enabled" entries selected.)

- Ensure that no other applications or services (such as IIS) are using the SSL TCP port.

- For VDAs for Windows Server OS, restart the machine for the changes to take effect. (You do not need to restart machines containing VDAs for Windows Desktop OS.)

**Configure SSL on Delivery Groups**

Complete this procedure for each Delivery Group that contains VDAs you have configured for SSL connections.

From Studio, open the PowerShell console.

```
Run asnp Citrix.* to load the Citrix product cmdlets. .
where <delivery-group-name> is the name of the Delivery Group containing VDAs. .
```

**Additional information**

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>How to Configure NetScaler Gateway 10.5 to use with StoreFront 2.6 and XenDesktop 7.6</td>
<td><a href="http://support.citrix.com/article/CTX200287">http://support.citrix.com/article/CTX200287</a></td>
</tr>
</tbody>
</table>
Securing access using SSL VPN

Citrix NetScaler supports a variety of methods that users can use to connect to your organization’s network resources:

- ICA proxy with Citrix Receiver.
- Receiver for Web with HTML5 Receiver that allows user connections to applications, desktops, and ShareFile using a web browser.
- XenMobile Worx Home to allow users to access WorxMail, WorxWeb, and mobile apps from their iOS and Android devices.
- Clientless access that provides users with the access they need without installing user software.
- NetScaler Gateway Plug-in for Windows and Mac OS X that can establish a secure SSL VPN tunnel
- NetScaler Gateway Plug-in for Java

When users connect with a NetScaler Gateway Plug-in for Windows, Mac OS X, or Java, NetScaler supports SSL VPN tunnel, which operates at the application layer, as opposed to IPsec, which operates at the network layer. This provides ability to track authentication and authorization information. The result is easier control, simpler compliance and auditing.

Configuration guidelines

When users connect with the NetScaler Gateway Plug-in, the client software establishes a secure tunnel over port 443 (or any configured port on NetScaler Gateway) and sends authentication information. When the tunnel is established, NetScaler Gateway sends configuration information to the NetScaler Gateway Plug-in describing the networks to be secured and containing an IP address if you enable address pools.

Tunneling Private Network Traffic over Secure Connections

When the NetScaler Gateway Plug-in starts and the user is authenticated, all network traffic destined for specified private networks is captured and redirected over the secure tunnel to NetScaler Gateway.

NetScaler Gateway intercepts all network connections that the user device makes and multiplexes them over Secure Sockets Layer (SSL) to NetScaler Gateway, where the traffic is demultiplexed and the connections are forwarded to the correct host and port combination.

The connections are subject to administrative security policies that apply to a single application, a subset of applications, or an entire intranet. You specify the resources (ranges of IP address/subnet pairs) that remote users can access through the VPN connection.

The NetScaler Gateway Plug-in intercepts and tunnels the following protocols for the defined intranet applications:

- TCP (all ports)
- UDP (all ports)
- ICMP (types 8 and 0 - echo request/reply)

Connections from local applications on the user device are securely tunneled to NetScaler Gateway, which re-establishes the connections to the target server. Target servers view connections as originating from the local NetScaler Gateway on the private network, thus hiding the user device. This is also called reverse Network Address Translation (NAT). Hiding IP addresses adds security to source locations.

Locally, on the user device, all connection-related traffic, such as SYN-ACK, PUSH, ACK, and FIN packets, is recreated by the NetScaler Gateway Plug-in to appear from the private server.
Configuring SQL encryption

Citrix XenDesktop and Citrix Provisioning Services use Microsoft SQL Server to host the data store.

By default, the SQL traffic between a XenDesktop Controller and an SQL Server is unencrypted, and because of the nature of SQL, it is largely in plain text. If all the site’s Controllers and SQL Server are on a secure network, this is not a concern; however, in some cases, it may be required to encrypt the SQL traffic using SSL.

Configuration guidelines

Microsoft SQL Server provides three basic configurations for encryption of SQL traffic between the Controllers (clients) and an SQL Server.

In all cases, a suitable certificate must be installed on the SQL Server that can be verified by an appropriate certificate chain on each Controller. This requires the root certificate of the server certificate’s Certificate Authority (CA) be exported and installed on each Controller. Where connections to multiple SQL Servers are to be encrypted, the appropriate CA root certificate for each server must be installed on all Controllers.

Use of SSL in this way encrypts the data flowing through the SQL connections and authenticates the SQL Server identity to the XenDesktop Controllers.

Forcing Encryption at the SQL Server

Encryption can be specified as a requirement at the SQL Server. In this case, all incoming SQL connections from any client (XenDesktop Controller or otherwise) are encrypted. This is configured by specifying Force Encryption on the SQL Server.

If encryption is forced at the SQL Server then the appropriate CA root certificate must also be provisioned to any machine used for performing database management operations through Studio (initial database configuration, adding controllers, or schema upgrades for example).

Forcing Encryption at the Controller (client)

Encryption can be specified as a requirement at each XenDesktop Controller. In this case, all outgoing connections from a Controller to any SQL Server are encrypted. This is configured by specifying Force Protocol Encryption on each Controller (client) machine.

If encryption is forced at the Controllers for a XenDesktop 7 site using multiple SQL Servers, appropriate certificates must be provisioned for all SQL Servers because all Controllers connect to all the servers.

Forcing Encryption for each Service

Encryption can be specified as a requirement on each individual SQL connection through a setting in a service’s SQL connection string. In this case, neither the Force Encryption option on the server nor the Force Protocol Encryption option on the Controllers should be specified.

To enable encryption in this configuration requires the connection strings of the XenDesktop services on all Controllers to be modified by the addition of the ‘Encrypt=True’ option. That is, a connection string such as:
“Data Source=sqlserver.mydomain.net; Initial Catalog=CitrixXDSite; Integrated Security=True”

Becomes:
“Data Source=sqlserver.mydomain.net; Initial Catalog=CitrixXDSite; Integrated Security=True; Encrypt=True”

**Special considerations**

Where an SQL Server is mirrored, clustered, or part of an SQL Server 2012 AlwaysOn availability group, Subject Alternative Names, Server Principal Names (SPN) or wildcard certificates must be configured on the SQL servers. Refer to Microsoft SQL Server documentation for additional details.

**Additional information**

<table>
<thead>
<tr>
<th>How to Enable Secure SQL Database Connection String with XenDesktop</th>
<th><a href="http://support.citrix.com/article/CTX137556">http://support.citrix.com/article/CTX137556</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console</td>
<td><a href="http://support.microsoft.com/KB/316898">http://support.microsoft.com/KB/316898</a></td>
</tr>
</tbody>
</table>

**Configuring SMB encryption for UPM profile store**

One of the requirements for HIPAA compliance is to enforce transmission security for data. CIFS protocol that is used to access file shares on Windows Server is unencrypted by default, which means that someone who has access to the network could intercept all data located on these file shares. In older versions of Microsoft Windows, the only option available for encrypting this traffic was use of IPsec protocol. IPsec configuration may be complicated in some environments.

Microsoft Windows Server 2012 R2 and Windows Server 2012 added a new security enhancement called SMB encryption. It can be used to protect data stored on Windows file servers such as user profiles managed by Citrix Profile Management.

SMB encryption uses the Advanced Encryption Standard (AES) CCM algorithm to encrypt and decrypt the data. AES-CCM also provides data integrity validation (signing) for encrypted file shares.

**Configuration guidelines**

You can configure SMB encryption on a per-share basis or for the entire file server.

To enable SMB encryption for an individual file share, use the following PowerShell cmdlet on the file server:

```powershell
Set-SmbShare -Name <sharename> -EncryptData $true
```

To enable SMB encryption for the entire file server, use the following PowerShell cmdlet on the file server:

```powershell
Set-SmbServerConfiguration -EncryptData $true
```

To create a new SMB file share with SMB encryption enabled, use the following PowerShell cmdlet on the file:

© Copyright 2015 Citrix Systems, Inc.
New-SmbShare -Name <sharename> -Path <pathname> -EncryptData $true

You can also use Server Manager to enable SMB encryption. To do this, under File and Storage Services, open the Shares management page, right-click the share on which you want to enable SMB encryption, and then select Properties.

On the Settings page of the share, select Encrypt data access.

**Special considerations**

SMB encryption does not cover security at rest, which is typically covered by BitLocker Drive Encryption or Encrypting File System (EFS).

Be aware that there is always a performance degradation with any end-to-end encryption protection when compared to nonencrypted. This can slow down user logons and user profile write back.

When SMB encryption is enabled for a file server or share, only SMB 3.0 clients (Windows 8 or Windows Server 2012 and later) can access this share. Previous operating systems will receive access denied error.

SMB encryption may be incompatible with some WAN optimization devices.

**Additional information**


**Audit Controls**

**Understanding XenApp and XenDesktop logging and reporting mechanisms**

It’s important to understand how and where audit information is stored and how long it persists. Besides standard logging to the Windows security event log, XenDesktop also stores connection history in a SQL database.

**Configuration guidelines**

**Monitor Service**

Administrators and help-desk personnel can monitor XenApp and XenDesktop Sites with Director. Session data is stored in the Monitoring database. By default, the Monitoring database is located on the same server as the Site Configuration database. Citrix recommends that you change the location of the monitoring database after you create a Site.

Session and connection data is available in Director. In addition to using the Citrix Director to display historical data, you can query data using the Monitor Service’s API. You can use the API to:

- Analyze historical trends for future planning.
- Perform detailed troubleshooting of connection and machine failures.
- Extract information for feeding into other tools and processes; for example, using Microsoft Excel’s PowerPivot tables to display the data in different ways.
- Build a custom user interface on top of the data that the API provides.

The Monitor Service API uses the Open Data (OData) protocol, which is a web protocol for querying and updating data, built upon web technologies such as HTTP.

The Data endpoint exposes read-only access directly to the database entities and can be accessed using the OData query language. This endpoint allows highly flexible access in terms of filtering and column
selection. The Data API URI is: http://{dc-host}/Citrix/Monitor/OData/v2/Data. For more information about accessing the Monitor Service data, see Accessing data using the API.

**Broker Service**

In addition to Citrix Monitor Service, the core Citrix Broker Service stores the connection log data in a site database. You can retrieve this data by using Get-BrokerConnectionLog cmdlet.

The session connection log contains entries describing each brokered connection, or reconnection, attempt to a session in the site.

Each log entry describes a single connection brokering attempt to a new or existing session within the site. A single session can have multiple entries in the connection log; for example, where the end user brokers a connection to a new session, disconnects and later brokers a reconnection. Conversely, other sessions may have none (such as console sessions).

By default connection log entries are removed after 48 hours. This setting can be changed by modifying the registry value HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\Logging\ConnectionLogLifetimeHours.

For example following commands get all connection log entries for sessions brokered in the past 30 minutes, ordered first by machine name (ascending), then by session end time (descending):

```
C:\PS> $when = [DateTime]::Now - [TimeSpan]::FromMinutes(30)
C:\PS> Get-BrokerConnectionLog -Filter {BrokeringTime -gt $when} -SortBy '+MachineName,-EndTime'
```

**Special considerations**

When you change the location of the Configuration Logging or Monitoring database:

- The data in the previous database is not imported to the new database.
- Logs cannot be aggregated from both databases when retrieving logs.

The first log entry in the new database indicates that a database change occurred, but it does not identify the previous database.

**Additional information**

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring</td>
<td><a href="http://support.citrix.com/proddocs/topic/xenapp-xendesktop-76/xad-monitor-article.html">http://support.citrix.com/proddocs/topic/xenapp-xendesktop-76/xad-monitor-article.html</a></td>
</tr>
</tbody>
</table>

**Configuring NetScaler Logging and reporting mechanisms**

Auditing of administrative actions is necessary to meet the HIPAA requirements and provide basic configuration management capabilities. It is also important to be able to log what occurs for problem resolution and debugging. The Citrix NetScaler system provides a rich set of logging interfaces that can be used in various situations to meet the needs of a variety of customers and under different traffic conditions.

© Copyright 2015 Citrix Systems, Inc.
These logging interfaces include:

- SNMP traps
- SNMP polling
- Syslog
- Audit server
- NetScaler web logging
- Historical reporting
- Performance record logging
- SNMP traps

Through the SNMP protocol, alerts can be configured to be pushed to external management systems for a wide variety of events that occur on the system, some of which report operationally varying information, such as the CPU usage going too high, and others for platform issues, such as high temperature. This information can be logged on standard SNMP management stations and used for post-mortem analysis. Commonly configured and monitored traps include the CPU load going above 90 percent or bandwidth utilization. As a general rule, SNMP traps are designed to trigger on events that may require immediate action and can be configured based on customer needs. For more details on the available SNMP alerts, see the NetScaler documentation at the Citrix product documentation site: Support.Citrix.com/proddocs.

SNMP polling

As with most vendors, NetScaler provides the ability to gather statistics for monitoring with third-party management applications using SNMP polling. As part of this functionality, the NetScaler provides a diverse set of SNMP Object Identifiers (OIDs) that cover a wide range of functions that may need monitoring. For a complete list of SNMP OIDs available for each release of code, see the NetScaler documentation provided with each software build.

Syslog and audit server

Syslog is another commonly used protocol for providing log information to external sources and is supported by NetScaler. In terms of the information it provides, Syslog can be thought of as a superset of what SNMP alerts can provide because Syslog logs all SNMP alerts that are generated and other information that does not fit well with SNMP alerts, including:

- TCP connection logging
- SSL VPN user logging
- Configuration command auditing
- Kernel messages and errors

For a complete list of NetScaler internally generated syslog messages, see the NetScaler syslog message documentation, provided with each build.

While Syslog is a generic protocol that provides the ability to log generic messages, the NetScaler audit server is designed to deliver an alternative higher performance interface for the same information. The audit server operates as a separate process residing on an external machine or set of machines and communicates with one or more NetScalers to receive the information that otherwise goes to Syslog. The audit server not only allows for a more optimized channel of communication between the NetScaler and the log server, but it also offloads the work of formatting the log data from the NetScaler itself. As a result, when logging large volumes of data, such as with TCP connection logging, the audit server can provide vast improvements in performance. As an example, under heavy TCP connection logging, with the audit server, the NetScaler has been tested to handle as much as 2.5 times the number of TCP connections per second versus with direct Syslog logging. In most environments, the logging level does not impact performance to such a degree that this becomes a problem, but if needed, the audit server provides for a
scalable option. When needed, the audit server is available for operating systems including Windows, Linux, FreeBSD, OS X, Solaris (SPARC), and AIX.

NetScaler web logging

NetScaler web logging is similar to the audit server, where the NetScaler communicates with one or more external NetScaler web logging agents, which then format and write logs in standard W3C or NCSA formats. This approach to logging has several benefits:

- When using a farm of servers, the web logging feature provides for a centralized aggregated view of the logs, which allows easier real-time data analysis.
- When caching is involved, the NetScaler can report the transactions that never make it to the back-end server, providing a complete view of the data, not just the non-cacheable content.
- With the compression active, the server-side and client-side view of the object size is available so that actual compression ratios can be computed.
- By having logs off of the server, if a server is compromised, it is much more difficult for someone to cover their tracks if they gain access over HTTP.
- Like the audit server, the web logging client is available for most common server operating systems.

To assist with reliability and to make aggregation of logs easier, the NetScaler web logging agent can run on multiple systems. You can also insert transaction IDs into each log entry, which is an internal ID the NetScaler uses for tracking individual HTTP requests and responses. This allows for easy and reliable log aggregation.

Historical reporting

To assist users who may not have a centralized SNMP monitoring station or for debugging issues that require tracking of data that normally does not require tracking, the NetScaler provides a mechanism for creating historical reports on the system itself that allows for reports to be created with various variables and then tracked over time. As an example, a chart can be created that shows the CPU utilization versus memory usage, as well as HTTP requests per second:

To build the reports, a wide variety of information is available to select from, and once a report is built, the data is gathered in real time for the user or can be viewed as needed.

Performance record logging

In addition to the logging that is accessible externally, a final logging mechanism is performed on the NetScaler — the logging of performance records. Every seven seconds, a snapshot of internal variables is made, called a performance record. This record is logged on the NetScaler itself and stored in a file.
called newnslog. The information in this log provides a comprehensive view of the NetScaler’s performance, including variables you didn’t anticipate to need; therefore, it’s an excellent source of information for post-mortem analysis after an unexpected event.

To provide an example of the number of variables and depth of information provided, the next few pages contain a sample of the output to show the variables tracked just for interface counters. The counters cover a wide range of functions, including load balancing, memory allocation, compression, SSL behaviors, TCP retransmits, etc. In all, thousands of counters are tracked, even on an unconfigured system, and hundreds more are tracked for every object that is added to the system. No other vendor on the market tracks this type of data to this depth by default on this type of device.

Configuration guidelines

Simple Network Management Protocol (SNMP)

You can use Simple Network Management Protocol (SNMP) to configure the SNMP agent on the Citrix NetScaler appliance to generate asynchronous events, which are called traps. The traps are generated whenever there are abnormal conditions on the NetScaler. The traps are then sent to a remote device called a trap listener, which signals the abnormal condition on the NetScaler appliance. Or you can query the SNMP agent for system-specific information from a remote device called an SNMP manager. The agent then searches the management information base (MIB) for the data requested and sends the data to the SNMP manager.

To monitor a NetScaler appliance, you must download the MIB object definition files. You can obtain the MIB object definition files from the /netscaler/snmp directory or from the Downloads tab of the NetScaler GUI.

SysLog

You can customize logging of NetScaler and NetScaler Gateway Enterprise Edition access events for the needs of your Site. You can direct these logs either to files on the NetScaler or to external log servers. The NetScaler uses the Audit Server Logging feature for logging the states and status information collected by different modules in the kernel and by user-level daemons.

Syslog is used to monitor a NetScaler and to log connections, statistics, and so on. You can customize the two logging functions for system events messaging and syslog. The NetScaler internal event message generator passes log entries to the syslog server. The syslog server accepts these log entries and logs them.

Audit server

The native NSLOG protocol has two components—the NSLOG auditing module, which runs on the NetScaler appliance, and the NSLOG server, which can run on the underlying FreeBSD OS of the NetScaler appliance or on a remote system that run Microsoft Windows, RedHat Linux, SUSE Linux Enterprise or FreeBSD. NSLOG uses transmission control protocol (TCP) for transfer of data.

When you run NSLOG server, it connects to the NetScaler appliance. The NetScaler appliance then starts sending all the log information to the NSLOG server, and the server can filter the log entries before storing them in a log file. An NSLOG server can receive log information from more than one NetScaler appliance and a NetScaler appliance can send log information to more than one NSLOG server.

Web logging

To configure web server logging, you first enable the web logging feature on the NetScaler and configure the size of the buffer for temporarily storing the log entries. Then, install NSWL client that collect data on the computer that run Microsoft Windows, RedHat Linux, SUSE Linux Enterprise or FreeBSD.

Special considerations

LOG data is not automatically removed and can consume a significant amount of disk space. Consider configuring archival mechanisms for such logs.
Be aware that LOG data can contain some information that can be used by an attacker to find configuration flaws in the environment and log data needs to be protected from the unauthorized use.

The SNMP agent on the NetScaler can generate traps compliant with SNMPv1 and SNMPv2 only. For querying, the SNMP agent supports SNMP version 1 (SNMPv1), SNMP version 2 (SNMPv2), and SNMP version 3 (SNMPv3).

**Additional information**

<table>
<thead>
<tr>
<th>Additional information</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reporting Tool</td>
<td><a href="http://support.citrix.com/proddocs/topic/ns-system-10-5-map/ns-ag-rt-intro-con.html">http://support.citrix.com/proddocs/topic/ns-system-10-5-map/ns-ag-rt-intro-con.html</a></td>
</tr>
<tr>
<td>Citrix NetScaler Logging</td>
<td><a href="http://support.citrix.com/article/CTX123967">http://support.citrix.com/article/CTX123967</a></td>
</tr>
</tbody>
</table>

**Monitoring licensing alerts with Citrix Director**

With Director 7.6, we really wanted to make sure users know when they are about to be impacted by a license issue. To address this, license alerts from the license server are now made available in the Dashboard view in Director 7.6. This new capability provides greater visibility into the licensing state of XenApp/XenDesktop so administrators are aware of impending current licensing conditions, which may affect the functionality of the product. Licensing errors in an environment can cause major outages or degraded service for customers. In previous versions of XenApp and XenDesktop, it is difficult to identify when license problems affect your site or are about to impact user connections.

**Configuration guidelines**

With the exception of information under the “Special considerations” section below, there is no configuration needed to obtain licensing alerts through Director.

Special considerations

Administrators can set a threshold for license usage. If the licenses consumed exceed the set threshold value, an alert will be generated and shown in the Licensing Server panel in Director. The default value is set at 90 percent; however, it can be configured on the Delivery Controller by running the following XenDesktop PowerShell command to set a custom threshold.
Enabling Configuration Logging

Configuration Logging captures Site configuration changes and administrative activities to the database. You can use the logged content to:

- Diagnose and troubleshoot problems after configuration changes are made; the log provides a breadcrumb trail.
- Assist change management and track configurations.
- Report administration activity.

You set Configuration Logging preferences, display configuration logs, and generate HTML and CSV reports from Citrix Studio. You can filter configuration log displays by date ranges and by full text search results. Mandatory logging, when enabled, prevents configuration changes from being made unless they can be logged. With appropriate permission, you can delete entries from the configuration log. You cannot use the Configuration Logging feature to edit log content.

Configuration Logging uses a PowerShell 2.0 SDK and the Configuration Logging Service. The Configuration Logging Service runs on every Controller in the Site; if one Controller fails, the service on another Controller automatically handles logging requests.

Examples of logged configuration changes include working with (creating, editing, deleting assigning):

- Machine catalogs
- Delivery Groups (including changing power management settings)
- Administrator roles and scopes
- Host resources and connections
- Citrix policies through Studio

Examples of logged administrative changes include:

- Power management of a virtual machine or a user desktop
- Studio or Director sending a message to a user

The following operations are not logged:

- Autonomic operations such as pool management power-on of virtual machines.
- Policy actions implemented through the Group Policy Management Console (GPMC); use Microsoft tools to view logs of those actions.
- Changes made through the registry, direct access of the database, or from sources other than Studio, Director, or PowerShell.

When the deployment is initialized, Configuration Logging becomes available when the first Configuration Logging Service instance registers with the Configuration Service. Therefore, the very early stages of configuration are not logged (for example, when the database schema is obtained and applied when a hypervisor is initialized).
Configuration guidelines

By default, Configuration Logging is enabled, and mandatory logging is disabled.

Select Loggin in the Studio navigation pane.

Select Preferences in the Actions pane. The Configuration Logging dialog box contains database information and indicates whether Configuration Logging and mandatory logging are enabled or disabled.

To enable Configuration Logging, select the Enable logging radio button. This is the default setting. If the database cannot be written to, the logging information is discarded, but the operation continues.

To disable Configuration Logging, select the Disable logging radio button. If logging was previously enabled, existing logs remain readable with the PowerShell SDK.

To enable mandatory logging, clear the Allow changes when the database is disconnected checkbox. No configuration change or administrative activity that would normally be logged will be allowed unless it can be written in the database used for Configuration Logging.

You can enable mandatory logging only when Configuration Logging is enabled, that is, when the Enable Configuration Logging radio button is selected. If the Configuration Logging Service fails, and high availability is not in use, mandatory logging is assumed. In such cases, operations that would normally be logged are not performed.

To disable mandatory logging, select the Allow changes when the database is disconnected check box. Configuration changes and administrative activities are allowed, even if the database used for Configuration Logging cannot be accessed. This is the default setting.

Special considerations

By default, the Configuration Logging feature is enabled, and uses the Database that is created when you create the Site (the Site Configuration Database). Citrix strongly recommends that you change the location of the database used for Configuration Logging as soon as possible after creating a Site. The
Configuration Logging Database supports the same high availability features as the Site Configuration Database.

Access to Configuration Logging is controlled through Delegated Administration, with the Edit Logging Preferences and View Configuration Logs permissions.

**Additional information**


**High availability and business continuity**

**Providing a highly available data store and understanding connection leasing**

All information about the XenDesktop and Provisioning Services configuration is stored in the configuration database. XenDesktop Controllers communicate only with the database and not with each other.

To ensure that the Site database is always available, Citrix recommends starting with a fault-tolerant SQL Server deployment by following high availability best practices from Microsoft.

The following database features are supported:

- **SQL Mirroring** — This is the recommended solution. In case you lose the active database server, mirroring the database ensures that the automatic failover process happens in a matter of seconds so users are generally unaffected. This method, however, is more expensive than other solutions because full SQL Server licenses are required on each database server; you cannot use SQL Server Express edition for a mirrored environment.

- **Using the hypervisor's high availability features** — With this method, you deploy the database as a virtual machine and use your hypervisor’s high availability features. This solution is less expensive than mirroring, as it uses your existing hypervisor software, and you can also use SQL Express. However, the automatic failover process is slower, as it can take time for a new machine to start for the database, which may interrupt the service to users.

- **SQL Clustering** — The Microsoft SQL clustering technology can be used to automatically allow one server to take over the tasks and responsibilities of another server that has failed. However, setting up this solution is more complicated, and the automatic failover process is typically slower than with alternatives such as SQL mirroring.

- **AlwaysOn Availability Groups** is an enterprise-level high-availability and disaster recovery solution introduced in SQL Server 2012 to enable you to maximize availability for one or more user databases. AlwaysOn Availability Groups requires that the SQL Server instances reside on Windows Server Failover Clustering (WSFC) nodes.

However, network issues and interruptions may prevent Delivery Controllers from accessing the database, resulting in users not being able to connect to their applications or desktop.

The connection leasing feature supplements the SQL Server high availability best practices by enabling users to connect and reconnect to their most recently used applications and desktops, even when the Site database is not available.

**Configuration guidelines**

Configure a Site to use a mirror database. The configuration process involves tasks an administrator completes using SQL Server management tools before creating the Site. The remaining tasks occur when the administrator runs the Site creation wizard.

© Copyright 2015 Citrix Systems, Inc.
A mirror environment requires at least two SQL Server machines (in the following example, SQL Server A and SQL Server B). SQL Server Express edition cannot be used as either a principal or mirror.

Using Microsoft SQL Server management tools, configure the SQL Server databases:

1. Install the SQL Server software on SQL Server A and SQL Server B.
2. On SQL Server A, create the database intended to be used as the principal (for example, myDatabaseMirror).
3. Make sure that the database uses the full recovery model and not the simple model. (The simple model is configured by default, but prevents the transaction log from being backed up.)
4. Use the following collation setting when creating the database: Latin1_General_100_CI_AS_KS (where Latin1_General varies depending on the country; for example Japanese_100_CI_AS_KS). If this collation setting is not specified during database creation, subsequent creation of the service schemas within the database will fail, and an error similar to "<service>: schema requires a case-insensitive database" appears (where <service> is the name of the service whose schema is being created).
5. Enable a Read-Committed snapshot as described in CTX137161. It is important to enable this before the database is mirrored to avoid errors.
6. On SQL Server A, back up the database to a file and copy it to SQL Server B.
7. On SQL Server B, restore the backup file to that server (SQL Server B).

The next step depends on whether the Citrix administrator (that is, the person running the Site creation wizard) also has full database privileges:

- If the Citrix administrator has database privileges (the same person is the database administrator and the Citrix administrator), Studio does everything for you:
  1. The Citrix administrator uses Studio to create a Site, specifying the address of the previously created SQL Server A database and its name (myDatabaseMirrorForXD).
  2. The database scripts are automatically applied and the principal and mirror databases are set.

If the Citrix administrator does not have database privileges, the Citrix administrator must get help from a database administrator:

- The Citrix administrator uses Studio to create a Site, specifying the address of the previously created SQL Server and its name (myDatabaseMirrorForXD).
  1. In the Site creation wizard, selecting Generate Script generates a mirror script and a primary script. The Citrix administrator gives those scripts to the database administrator, who applies the scripts (the mirror script should be applied first). The database administrator must tell the Citrix administrator when that task is completed.
  2. Back in Studio, the Citrix administrator can now complete the Create Site wizard. The principal and mirror databases are set.
  3. To verify mirroring after creating the Site, run the PowerShell cmdlet get-configdbconnection to make sure that the Failover Partner has been set in the connection string to the mirror.

Special considerations

While connection leasing can improve connection resiliency and user productivity, there are considerations related to the availability, operation, and performance of other features.

Connection leasing is supported for server-hosted applications and desktops, and static (assigned) desktops; it is not supported for pooled VDI desktops or for users who have not been assigned a desktop when the database becomes unavailable.
When the Controller is in leased connection mode:

- Administrators cannot use Studio, Director, or the PowerShell console.
- Workspace Control is not available. When a user logs on to Receiver, sessions do not automatically reconnect; the user must relaunch the application.
- If a new lease is created immediately before the database becomes unavailable, but the lease information has not yet been synchronized across all Controllers, the user might not be able to launch that resource after the database becomes unavailable.
- Server-hosted application and desktop users may use more sessions than their configured session limits. For example:
  - A session may not roam when a user launches it from one device (connecting externally through NetScaler Gateway) when the Controller is not in leased connection mode and then connects from another device on the LAN when the Controller is in leased connection mode.
  - Session reconnection may fail if an application launches just before the database becomes unavailable; in such cases, a new session and application instance are launched.
- Static (assigned) desktops are not power-managed. VDAs that are powered off when the Controller enters leased connection mode remain unavailable until the database connection is restored, unless the administrator manually powers them on.
- If session prelaunch and session linger are enabled, new prelaunch sessions are not started. Prelaunched and lingering sessions will not be ended according to configured thresholds while the database is unavailable.
- Load management within the Site may be affected. Server-based connections are routed to the most recently used VDA. Load evaluators (and especially, session count rules) may be exceeded.
- The Controller will not enter leased connection mode if you use SQL Server Management Studio to take the database offline. Instead, use one of the following Transact-SQL statements:

  ```sql
  ALTER DATABASE <database-name> SET OFFLINE WITH ROLLBACK IMMEDIATE.
  ALTER DATABASE <database-name> SET OFFLINE WITH ROLLBACK AFTER <seconds>.
  ```
  
  Either statement cancels any pending transactions and causes the Controller to lose its connection with the database. The Controller then enters leased connection mode.

When connection leasing is enabled, there are two brief intervals during which users cannot connect or reconnect: (1) from the time the database becomes unavailable to when the Controller enters leased connection mode, and (2) from the time the Controller changes from leased connection mode to when database access is fully restored and the VDAs have re-registered.

### Additional information

|-------------------|--------------------------------------------------------------------------------------------------|
What's the right order to update XenDesktop 7.1 services for SQL mirroring?

http://blogs.citrix.com/2014/02/28/whats-the-right-order-to-update-xendesktop-7-1-services-for-sql-mirroring/

XenDesktop 7.x Database Sizing

http://support.citrix.com/article/CTX139508

Understanding Provisioning Services offline database access

The Offline Database Support option allows Provisioning Services to use a snapshot of the Provisioning Services database in the event that the connection to the database is lost.

When offline database support is enabled on the farm, a snapshot of the database is created and initialized at server startup. The Stream Process then continually updates it. If the database becomes unavailable, the Stream Process uses the snapshot to get information about Provisioning Services and the target devices available to the server; this allows Provisioning Services and target devices to remain operational. However, when the database is offline, Provisioning Services management functions and the console become unavailable.

When the database connection becomes available, the Stream Process synchronizes any Provisioning Services or target device status changes made to the snapshot back to the database.

Configuration guidelines

To enable the Offline Database Support option:

1. In the Console tree, right-click on the Farm, and then select Properties. The Farm Properties dialog appears.
2. On the Options tab, select the check box next to Offline Database Support.
3. Restart Stream services.

Special considerations

Offline Database Support is disabled by default and is only recommended for use with a stable farm running in production. It is not recommended when running an evaluation environment or when reconfiguring farm components “on the fly.” Only a farm administrator can set this option.

Additional information

- Database Mirroring: http://support.citrix.com/proddocs/topic/provisioning-7/pvs-ha-db-mirror.html

Understanding test and QA environments

A test environment is critical for testing new applications, updates, and settings before rolling them out into production. Having one or more test servers in a production XenDesktop site may be sufficient testing application updates.

Create a separate site or site for testing new XenDesktop versions with settings that closely resemble what is used in production.
Configuring NetScaler Gateway load balancing and failover

A high availability deployment of two NetScaler Gateway appliances can provide uninterrupted operation in any transaction. When you configure one appliance as the primary node and the other as the secondary node, the primary node accepts connections and manages servers while the secondary node monitors the primary. If the primary node is unable to accept connections, the secondary node takes over.

The secondary node monitors the primary by sending periodic messages (often called heartbeat messages or health checks) to determine whether the primary node is accepting connections. If a health check fails, the secondary node retries the connection for a specified period, after which it determines that the primary node is not functioning normally. The secondary node then takes over for the primary (a process called failover).

After a failover, all clients must re-establish their connections to the managed servers, but the session persistence rules are maintained as they were before the failover.

Configuration guidelines

Before configuring a high availability pair, you should review these guidelines:

- Each NetScaler Gateway appliance must be running the same version of the NetScaler Gateway software. You can find the version number at the top of the page in the configuration utility.
- NetScaler Gateway does not automatically synchronize passwords between two appliances. You can choose to configure each NetScaler Gateway with the user name and password of the other appliance in the pair.
- Entries in the configuration file, ns.conf, on both the primary and the secondary NetScaler Gateway must match, with the following exceptions:
  - The primary and secondary NetScaler Gateway appliance must each be configured with its own unique system IP address. Use the Setup Wizard to configure or modify the system IP address on either NetScaler Gateway.
  - In a high availability pair, the NetScaler Gateway ID and associated IP address must point to the other NetScaler Gateway.
    - For example, if you have two appliances, named AG1 and AG2, you must configure AG1 with the unique NetScaler Gateway ID and IP address of AG2. You must configure AG2 with the unique NetScaler Gateway ID and IP address of AG1.
    - Note: Each NetScaler Gateway appliance are always identified as Node 0. Configure each appliance with a unique node ID.
  - Each appliance in the high availability pair must have the same license.

If you create a configuration file on either node by using a method that does not go directly through the configuration utility or the command-line interface (for example, importing SSL certificates, or changing to startup scripts), you must copy the configuration file to the other node or create an identical file on that node.

Special considerations

When a failover occurs, all TCP connections are immediately dropped, and ICA session must be reestablished. However, this process require Session Reliability to be enabled on XenDesktop. If Session reliability is disabled, the affected connection disappear from the user screen without any messages.

Additional information

Load Balancing


© Copyright 2015 Citrix Systems, Inc.
Providing highly available user profile store

It is recommended that you create a highly available user profile store to prevent a single point of failure, for example, by using DFS [distributed file system] or clustered file servers.

Configuration guidelines

Profile management supports the key features required for disaster recovery (DR):

- **DFS namespaces.** Domain-based namespace servers are preferred in this scenario because they allow the DR site to have its own namespace server. (A standalone namespace server cannot be replicated, but it can be hosted on a failover cluster.).

- **Multiple folder targets and DFS Replication.** For each NUS, you provide at least two targets, but only enable one in normal operation. You set up one-way DFS Replication to ensure that the disabled targets (at the DR sites) are kept up-to-date.

- **Failover clusters for hosting individual folder targets.** This is optional. It may be wasteful of resources on the DR site.

Special considerations

In disaster recovery and high availability scenarios, Citrix Profile Management may be affected by the same issues as affect Microsoft roaming profiles, and unless stated to the contrary, Profile Management does not resolve such issues.

The cache option for offline files must be disabled on roaming user profile shares. The same restriction applies to Profile Management shares.

Additional information

| High availability and disaster recovery with Profile management | http://support.citrix.com/proddocs/topic/user-profile-manager-5-x/upm-plan-high-availability-disaster-recovery-intro.html |

Compatibility with legacy systems

Understanding Virtual IP and virtual loopback

The Microsoft virtual IP address feature provides a published application with a unique dynamically assigned IP address for each session. The Citrix virtual loopback feature allows you to configure
applications that depend on communications with localhost (127.0.0.1 by default) to use a unique virtual loopback address in the localhost range (127.*).

Certain applications, such as CRM and Computer Telephony Integration (CTI), use an IP address for addressing, licensing, identification, or other purposes and thus require a unique IP address or a loopback address in sessions. Other applications may bind to a static port, so attempts to launch additional instances of an application in a multiuser environment will fail because the port is already in use. For such applications to function correctly in a XenApp environment, a unique IP address is required for each device.

Virtual IP and virtual loopback are independent features. You can use either or both.

**Virtual IP**

When virtual IP is enabled and configured on the Windows server, each configured application running in a session appears to have a unique address. Users access these applications on a XenApp server in the same way they access any other published application. A process requires virtual IP in either of the following cases:

- The process uses a hard-coded TCP port number
- The process uses Windows sockets and requires a unique IP address or a specified TCP port number

To determine if an application needs to use virtual IP addresses:

- Obtain the TCPView tool from Microsoft. This tool lists all applications that bind specific IP addresses and ports.
- Disable the Resolve IP Addresses feature so that you see the addresses instead of host names.
- Launch the application, and use TCPView to see which IP addresses and ports are opened by the application and which process names are opening these ports.
- Configure any processes that open the IP address of the server, 0.0.0.0, or 127.0.0.1.

To ensure that an application does not open the same IP address on a different port, launch an additional instance of the application.

**Virtual loopback**

Enabling the Citrix virtual IP loopback policy settings allows each session to have its own loopback address for communication. When an application uses the localhost address (default = 127.0.0.1) in a Winsock call, the virtual loopback feature simply replaces 127.0.0.1 with 127.X.X.X, where X.X.X is a representation of the session ID + 1. For example, a session ID of 7 is 127.0.0.8. In the unlikely event that the session ID exceeds the fourth octet (more than 255), the address rolls over to the next octet (127.0.1.0), to the maximum of 127.255.255.255.

A process requires virtual loopback in either of the following cases:

- The process uses the Windows socket loopback (localhost) address (127.0.0.1).
- The process uses a hard-coded TCP port number.

Use the virtual loopback policy settings for applications that use a loopback address for interprocess communication. No additional configuration is required. Virtual loopback has no dependency on Virtual IP, so you do not have to configure the Microsoft server.

- **Virtual IP loopback support.** When enabled, this policy setting allows each session to have its own virtual loopback address. This setting is disabled by default. The feature applies only to applications specified with the Virtual IP virtual loopback programs list policy setting.
Virtual IP virtual loopback programs list. This policy setting specifies the applications that use the virtual IP loopback feature. This setting applies only when the Virtual IP loopback support policy setting is enabled.

Additional information


Configuring session printing

Session printer mapping with network printer

In the healthcare industry, it is necessary to map printers to client devices based on their location, floor, subnet, etc., to ensure print jobs are sent to the correct printer and prevent private data exposure. During our validation, we set up four network printers, two of which are directly attached to Wyse terminals, as well. Each network printer was assigned to a different client by adding the “Printer assignments” policy in Citrix Studio.

Session printer with directly attached USB printer

Two of the printers are also directly attached to two separate Wyse terminals via USB. In this scenario, we tested that the printer added to the terminal propagates to the virtual desktop, allowing the user to print directly to the attached printer from the virtual desktop.

Configuration guidelines

First, the printer needs to be added to the Wyse terminal (Windows Embedded 7) using the “add a printer” utility with an admin account (not a user account). The “File Based Write Filter Utility” service is running by default, but the service has to be disabled first.

Caution: To save any configurations you make on a thin client to persist after a thin client reboot, be sure to disable the File Based Write Filter before your configurations to the thin client, and then enable the File Based Write Filter after your configurations.

Below is a screenshot of “Device and Printers” from the Wyse thin client (WES06) with a USB Epson printer:
Below is a screenshot of “Device and Printers” from the virtual desktop through the WES06 Wyse thin client:

![Virtual Desktop Screenshot](image)

Below is a screenshot of “Device and Printers” from the Wyse thin client (WES06) with a USB HP Officejet printer:

![Wyse Thin Client Screenshot](image)
Below is a screenshot of “Device and Printers” from the Wyse thin client WES03 with a USB HP Office jet printer:

![Device and Printers](image)

**Special considerations**

Changes to the Wyse terminals need to be done with an admin account, not a user account. When making changes, it is important to turn off the File Based Write Filter Utility service in the terminal so your changes are persistent.

**Additional information**

**Printing**  
http://support.citrix.com/proddocs/topic/xenapp-xendesktop-76/xad-print-landing.html

**FAQ: Citrix Universal Print Server (UPS) 7.6**  
http://support.citrix.com/article/CTX200328

**Configuring StoreFront resource shortcuts**

You can provide users with rapid access to desktops and applications from websites hosted on the internal network. You can generate URLs for resources available through the Receiver for Web site and embed these links on your websites.

When users click on the shortcut, the application is automatically launched without displaying the StoreFront interface.

**Additional information**

**Configure Receiver for Web sites**  

© Copyright 2015 Citrix Systems, Inc.
Client devices

Securing client devices

In every IT infrastructure, one of most important lines of defense is the endpoint device. Common security measures for endpoints include implementing antivirus and antimalware software, regular patching of the operating system, applications and agents, and strict rules for the personal firewall.

Configuration Guidelines

By using group policies, you have a wide selection of settings that allow secure communication between endpoints and other components.

In addition, the following techniques can be used to increase endpoint security and the respective level of trust.

- Securing the clients by means of Microsoft security baselines
- Trusted server configuration

ICA file signing

Endpoint encryption

Additional information

|--------------------------------------|---------------------------------------------------------------------|

Configuring Receiver Desktop Lock

When you need to configure a locked-down client machine to use as a kiosk, or if you need to prevent access to the local applications on Windows endpoints, including Windows-based thin clients, you can use the Receiver Desktop Lock.

Configuration guidelines

Citrix Receiver Desktop Lock 4.2 uses native StoreFront protocols. It does not support or require legacy PNA sites and does not support Web Interface.
Citrix Receiver for Windows must be installed with the /includeSSON flag. The store and Single Sign-on must be configured, either using the adm file or cmdline option.

System requirements for Citrix Receiver Desktop Lock

- Supported on Windows 8.1, Windows 8, 7, and Windows 7 Thin PC.
- Connects to StoreFront through native protocols only.
- Domain-joined and end points only.

**Considerations when configuring the Desktop Lock**

Grant access to only one virtual desktop running the Desktop Lock per user.

Do not allow users to hibernate virtual desktops. Use Active Directory policies to prevent this.

To configure Receiver Desktop Lock

Use the same administrator account to configure Receiver Desktop Lock that you used to install it.

Ensure that the icaclient.adm and icaclient_usb.adm files are loaded into Group Policy (where the policies appear in Computer Configuration or User Configuration > Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components). The .adm files are located in %Program Files%\Citrix\ICA Client\Configuration.

When a user plugs in a USB device, that device is automatically remoted to the virtual desktop; no user interaction is required. The virtual desktop is responsible for controlling the USB device and displaying it in the user interface.

Enable the USB policy rule

In Citrix Receiver > Remoting client devices > Generic USB Remoting, enable and configure the existing and new USB devices, and the USB devices list in Desktop Viewer policies. You can use the Show All Devices policy to display all connected USB devices, including those using the generic USB virtual channel (webcams and memory sticks, for example).

Under “Remoting client devices” in Citrix Receiver, you can enable and configure drive mapping with the Client Drive Mapping policy, as well as microphones with the Client Microphone policy.

**Special considerations**

The Receiver Desktop Lock works on domain-joined machines, which are SSON-enabled and store-configured.

Windows XP (Embedded Edition) is not currently supported. Support for Windows XP ended April 8, 2014, when Microsoft ended extended support for Windows XP.

**Additional information**


**Controlling device redirection**

By controlling device redirection, you are setting up the environment to be protected from data leaks.

By default following redirectors are allowed:

- USB redirection for certain classes of USB devices
- Printer redirection
- Client clipboard redirection
• Audio and microphone redirection
• Client drives redirection

Client TWAIN device redirection

Configuration guidelines

You can use multiple policies to customize your environment to meet users’ needs based on their job functions, geographic locations, or connection types. For example, for security, you may need to place restrictions on user groups who regularly work with sensitive data. You can create a policy that prevents users from saving sensitive files on their local client drives. However, if some people in the user group need access to their local drives, you can create another policy for only those users. You then rank or prioritize the two policies to control which one takes precedence.

When using multiple policies, you must determine how to prioritize them, how to create exceptions, and how to view the effective policy when policies conflict.

Additional information

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Default policy settings</td>
<td><a href="http://support.citrix.com/proddocs/topic/xenapp-xendesktop-76/xad-policies-defaults.html">http://support.citrix.com/proddocs/topic/xenapp-xendesktop-76/xad-policies-defaults.html</a></td>
</tr>
<tr>
<td>Compare, prioritize, model, and troubleshoot policies</td>
<td><a href="http://support.citrix.com/proddocs/topic/xenapp-xendesktop-76/xad-policies-prioritize-model.html">http://support.citrix.com/proddocs/topic/xenapp-xendesktop-76/xad-policies-prioritize-model.html</a></td>
</tr>
</tbody>
</table>

Understanding thin client configuration options

To understand thin client configuration options, we recommend you acquire the specific vendor documentation.

Optimizing user experience and session performance

Understanding mandatory profiles

Mandatory profiles, sometimes called roaming mandatory profiles, are stored in a centralized network location for each user. They differ from roaming profiles in that they do not retain users' changes at logoff. Configuring a user for a mandatory profile requires an administrator to create a mandatory profile file (NTUSER.MAN) from an existing roaming or local profile, and assign users' Terminal Services profile path to the location where the file can be accessed.

With mandatory user profiles, users can modify their desktop, but the changes are not saved when a user logs off. The next time a user logs on, the mandatory user profile created by the administrator is downloaded.

User profiles become super-mandatory when the folder name of the profile path ends in .man; for example, \server\share\mandatoryprofile.man\.

Super-mandatory user profiles are similar to normal mandatory profiles, with the exception that users who have super-mandatory profiles cannot log on when the server that stores the mandatory profile is unavailable. Users with normal mandatory profiles can log on with the locally cached copy of the mandatory profile.
Configuration Guidelines

Follow Microsoft guidelines for mandatory profiles.

Additional information

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Customize the default local user profile when preparing an image of Windows</td>
<td><a href="http://support.microsoft.com/kb/973289">http://support.microsoft.com/kb/973289</a></td>
</tr>
<tr>
<td>Cryptographic Keys and Certificates Cannot Be Used with Mandatory Profiles</td>
<td><a href="http://support.microsoft.com/kb/264732">http://support.microsoft.com/kb/264732</a></td>
</tr>
</tbody>
</table>

Understanding wireless client optimizations

Millions of XenDesktop users today access their applications via wireless connections, such as Wi-Fi or LTE. While bandwidth limitations are not so critical as before, higher latency still may affect connections.

In some cases, the user experience may be degraded to the point of being unacceptable. Throughput and latency are the two elements that define the speed of a network. Throughput is the quantity of data that can pass from source to destination in a specific time. Round-trip latency is the time it takes for a single data transaction to occur — the time between requesting data and receiving it.

Latency has a critical impact on the user experience because each user action must travel across the network from the client to the server, and the server response must return to the client before the user sees an update. Latency not only affects ICA traffic but also other traffic that is traversing the link.

Wireless networks have greater latency than wired and also demonstrate jitter (variable latency).

Configuration Guidelines

HDX RealTime technology provides an optimal end user experience with real-time audio and video data in a virtualized environment through integration with HDX Adaptive Orchestration. For XenDesktop, HDX RealTime is able to utilize Real-Time Transport Protocol (RTP) built on UDP to send real-time data in a timely fashion, while still utilizing the more reliable TCP protocol for the virtual desktop delivery. UDP/RTP is well suited for delivering audio over congested or wireless networks, where packets may be delayed or lost. For both XenApp and XenDesktop, HDX RealTime is able to utilize the client’s real-time resources (such as web camera, microphone, and speakers) to render real-time data, with the audio data being transported to the client over RTP/UDP or TCP for XenDesktop VDI whereas it can only be transported over TCP for XenApp.

Citrix recommends utilizing UDP Audio when users are connected using wireless networks.

Use Citrix policies to optimize graphics acceleration and disable device mapping for unnecessary devices.

Additional information

| Audio policy settings | http://support.citrix.com/proddocs/topic/xenapp-xendesktop-76/xad-policies-settings-audio.html |
Ensuring logon time reduction

The session prelaunch and session linger features help users quickly access applications by starting sessions before they are requested (session prelaunch) and keeping application sessions active after a user closes all applications (session linger). These features are supported for Server OS machines only.

By default, session prelaunch and session linger are not used. A session starts (launches) when a user starts an application and remains active until the last open application in the session closes. You can enable the features for all users in a Delivery Group or only for specified users.

There are several ways to specify how long an unused session remains active if the user does not start an application: a configured timeout and two server load thresholds. You can configure all of them; the event that occurs first will cause the unused session to end.

Configuring Profile Management active write back

To ensure profile integrity, files and folders that are modified while user is logged on to the session can be backed up to the user store during a session before logoff. This is particularly useful in Citrix XenDesktop deployments, where a user may leave their session open for a long period and can be affected by a nonpersistent nature of many XenDesktop deployments. In many scenarios, a provisioned system generally stores user profiles on a volatile disk volume so that changes are lost if the system is restarted for any reason (a power outage, scheduled maintenance, or an extended period of disconnection).

By configuring the active write back setting, you can safeguard file writes to the profile. Profile management detects when an application has written and closed a file, and it copies the file back to the network copy of the profile during idle periods.

Configuration guidelines

Enable the active write back policy setting using Citrix Studio or Group Policy Management Console.

Special considerations

Active write back may conflict with DFS Replication when multiple concurrent sessions are in use.

This feature is not intended to support users opening multiple active sessions. However, if a user starts a second session (started at a second computer, for example), modifications made to a file in the first session will be available in the second if it was started before logging off the first.

Additional information

To configure active write back

http://support.citrix.com/proddocs/topic/user-profile-manager-5-x/upm-active-profile-write-back.html

Configuring session prelaunch

By default, a user session starts when user manually starts the published application. For many customers, session creation can take between 30 seconds and two minutes. This delay is especially annoying for users who use published applications to open documents on their local desktops using file type association. Users may complain that the launch takes much more time than launching the same application on a local desktop.
Additionally, in environments like healthcare where many users work in shifts, servers may be hit by a logon storm, when all of the shift workers are trying to open their applications in a short 10-to-15-minute timeframe.

Launching an application on a Windows desktop requires creation of a session. Due to profile loading and logon scripts, many customers see individual session creation times of one to two minutes. In a logon storm scenario, the rapid succession of logon requests overwhelms individual servers, infrastructure servers, and perhaps even the network.

The prelaunch feature reduces application launch time at high-traffic periods. It allows a prelaunch session to be created when a user logs on to the computer that has a Citrix Receiver installed and configured.

**Configuration guidelines**

To enable session prelaunch:

- Select **Delivery Groups** in the Studio navigation pane.
- Select a Delivery Group, and then click **Edit Delivery Group** in the Actions pane.
- On the Application Prelaunch page, enable session prelaunch by choosing when sessions should launch:
  - When a user starts an application. This is the default setting; session prelaunch is disabled.
  - When any user in the Delivery Group logs on to Receiver for Windows.
  - When anyone in a list of users and user groups logs on to Receiver for Windows. Be sure to also specify users or user groups if you choose this option.

A prelaunched session is replaced with a regular session when the user starts an application. If the user does not start an application (the prelaunched session is unused), the following settings affect how long that session remains active.

- When a specified time interval elapses. You can change the time interval (1-99 days, 1-2,376 hours, or 1-142,560 minutes).
• When the average load on all machines in the Delivery Group exceeds a specified percentage (1-99 percent).
• When the load on any machine in the Delivery Group exceeds a specified percentage (1-99 percent).

Recap: A prelaunched session remains active until one of the following events occurs: a user starts an application, the specified time elapses, or a specified load threshold is exceeded.

With Citrix Receiver 4.2 and higher, the session prelaunch feature is enabled by default when you install the Single Sign-on (SSO) component.

Special considerations

Prelaunched sessions consume a license but only when connected. Unused prelaunched sessions disconnect after 15 minutes by default. This value can be configured in PowerShell (New/Set-BrokerSessionPreLaunch cmdlet).

Session prelaunch is initiated on the client side; this means that it works with a supported and properly configured version of Citrix Receiver. At the time, only Citrix Receiver for Windows is supported.

Additional information

<table>
<thead>
<tr>
<th>Manage sessions through Delivery Groups</th>
<th><a href="http://support.citrix.com/proddocs/topic/xenapp-xendesktop-76/xad-dg-manage-sessions.html#xad-dg-manage-sessions__prelaunch-linger">http://support.citrix.com/proddocs/topic/xenapp-xendesktop-76/xad-dg-manage-sessions.html#xad-dg-manage-sessions__prelaunch-linger</a></th>
</tr>
</thead>
</table>

Configuring session lingering

By default, a user session ends after user processes and visible windows end. You can use session linger to provide a better user experience by eliminating the launch delay between applications.

For many customers, session creation can take between 30 seconds and two minutes. To avoid these delays, session lingering can be configured for all users or for just a subset of the user population.

With session lingering, the session is not terminated immediately; it is kept alive until one of the expiration timers being hit or the load of the desktop group or individual desktop exceeds the set load thresholds.

Configuration guidelines

To enable session linger:

• Select Delivery Groups in the Studio navigation pane.
• Select a Delivery Group, and then click Edit Delivery Group in the Actions pane.
• On the Application Lingering page, enable session linger by selecting the Keep sessions active until radio button.
Several settings affect how long a lingering session remains active if the user does not start another application:

- When a specified time interval elapses. You can change the time interval (1-99 days, 1-2,376 hours, or 1-142,560 minutes).
- When the average load on all machines in the Delivery Group exceeds a specified percentage (1-99 percent).
- When the load on any machine in the Delivery Group exceeds a specified percentage (1-99 percent).

Recap: A lingering session remains active until one of the following events occurs: a user starts an application, the specified time elapses, or a specified load threshold is exceeded.

How long unused prelaunched and lingering sessions remain active

There are several ways to specify how long an unused session remains active if the user does not start an application: a configured timeout and server load thresholds. You can configure all of them; the event that occurs first will cause the unused session to end.

- Timeout - A configured timeout specifies the number of minutes, hours, or days an unused prelaunched or lingering session remains active. If you configure too short a timeout, prelaunched sessions will end before they provide the user benefit of quicker application access. If you configure too long a timeout, incoming user connections might be denied because the server doesn't have enough resources. You cannot disable this timeout from Studio, but you can in the SDK (New/Set-BrokerSessionPreLaunch cmdlet). If you disable the timeout, it will not appear in the Studio display for that Delivery Group or in the Edit Delivery Group wizard.

- Thresholds - Automatically ending prelaunched and lingering sessions based on server load ensures that sessions remain open as long as possible, assuming server resources are available. Unused prelaunched and lingering sessions will not cause denied connections because they will be ended automatically when resources are needed for new user sessions.
You can configure two thresholds: the average percentage load of all servers in the Delivery Group, and the maximum percentage load of a single server in the Delivery Group. When a threshold is exceeded, the sessions that have been in the prelaunch or lingering state for the longest time are ended, sessions are ended one-by-one at minute intervals until the load falls below the threshold. (While the threshold is exceeded, no new prelaunch sessions are started.).

You can also configure advanced parameters of session lingering by using PowerShell SDK cmdlets Get/Set/New/Remove-BrokerSessionLinger.

For example, to configure the disconnect time for the session linger setting associated with desktop group named Accounting, use the following command:

Set-BrokerSessionLinger -DesktopGroupName Accounting -MaxTimeBeforeDisconnect 0:10.

**Special considerations**

The Delivery Group must support applications, and the machines must be running a VDA for Server OS, minimum version 7.6.

Lingering sessions consume a license, but only when connected. To configure a disconnection time, use PowerShell SDK.

If the Site database is unavailable and the Controller is in leased connection mode, lingering sessions will not be ended according to configured thresholds while the database is unavailable.

**Additional information**

<table>
<thead>
<tr>
<th>Manage sessions through Delivery Groups</th>
<th><a href="http://support.citrix.com/proddocs/topic/xenapp-xendesktop-76/xad-dg-manage-sessions.html#xad-dg-manage-sessions__prelaunch-linger">http://support.citrix.com/proddocs/topic/xenapp-xendesktop-76/xad-dg-manage-sessions.html#xad-dg-manage-sessions__prelaunch-linger</a></th>
</tr>
</thead>
</table>
About Citrix

Citrix (NASDAQ:CTXS) is a leader in mobile workspaces, providing virtualization, mobility management, networking and cloud services to enable new ways to work better. Citrix solutions power business mobility through secure, personal workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. This year Citrix is celebrating 25 years of innovation, making IT simpler and people more productive. With annual revenue in 2013 of $2.9 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million users globally. Learn more at www.citrix.com.

Copyright © 2015 Citrix Systems, Inc. All rights reserved. Citrix License Server, NetScaler, NetScaler Gateway, Citrix Profile Management, Citrix Provisioning Services, Citrix Receiver, Citrix StoreFront, Citrix XenApp and Citrix XenDesktop are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies.