Citrix XenApp and XenDesktop 7.6 Healthcare Design Guide

This document is intended to aid business decision makers, IT architects and managers by providing an overview of the Citrix XenApp 7.6 solution architecture for healthcare. It includes an overview of healthcare business needs and goals, and information on how Citrix products and deployment methodologies provide solutions for those needs.

Last updated: July 2015
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>6</td>
</tr>
<tr>
<td>Disclaimer</td>
<td>6</td>
</tr>
<tr>
<td>Healthcare industry IT trends</td>
<td>6</td>
</tr>
<tr>
<td>Electronic medical records</td>
<td>6</td>
</tr>
<tr>
<td>Security compliance</td>
<td>6</td>
</tr>
<tr>
<td>Health Insurance Portability and Accountability Act (HIPAA)</td>
<td>6</td>
</tr>
<tr>
<td>Security threats</td>
<td>7</td>
</tr>
<tr>
<td>Storing and processing PHI data</td>
<td>8</td>
</tr>
<tr>
<td>Recommendations for enabling compliance</td>
<td>8</td>
</tr>
<tr>
<td>Handling security incidents</td>
<td>8</td>
</tr>
<tr>
<td>Benefits of Citrix solutions in healthcare</td>
<td>8</td>
</tr>
<tr>
<td>Healthcare use case needs and considerations</td>
<td>9</td>
</tr>
<tr>
<td>Architecture overview</td>
<td>10</td>
</tr>
<tr>
<td>Architectural components</td>
<td>10</td>
</tr>
<tr>
<td>Mapping HIPAA requirements to implementation</td>
<td>11</td>
</tr>
<tr>
<td>Section 3: How Citrix technologies address the HIPAA categories</td>
<td>15</td>
</tr>
<tr>
<td>Authentication</td>
<td>15</td>
</tr>
<tr>
<td>Providing unauthenticated (anonymous) access</td>
<td>15</td>
</tr>
<tr>
<td>Configuring Session Reliability and Auto Client Reconnect</td>
<td>15</td>
</tr>
<tr>
<td>Configuring workspace control</td>
<td>16</td>
</tr>
<tr>
<td>Access control</td>
<td>16</td>
</tr>
<tr>
<td>Enabling NetScaler External Authentication and command policies</td>
<td>16</td>
</tr>
<tr>
<td>Configuring XenApp and XenDesktop delegated administration</td>
<td>17</td>
</tr>
<tr>
<td>Configuring Provisioning Services administrative roles</td>
<td>18</td>
</tr>
<tr>
<td>Understanding network segmentation concepts and considerations</td>
<td>18</td>
</tr>
<tr>
<td>Configuring session idle and connection timers</td>
<td>19</td>
</tr>
<tr>
<td>Securing the environment</td>
<td>19</td>
</tr>
</tbody>
</table>
Deploying Citrix software updates and monitoring them using Director .................. 19
Understanding Windows Update strategies .............................................................. 20
Understanding network firewall configurations ...................................................... 21
Configuring the Windows Firewall ........................................................................ 21
Hypervisor security hardening considerations ....................................................... 21
NetScaler security hardening considerations ......................................................... 21
Virtual desktop security hardening considerations .............................................. 21
Preventing brute-force logon attacks to NetScaler Gateway ............................... 22
Configuring antivirus on the VDA ......................................................................... 22
Data integrity ........................................................................................................... 22
Enabling StoreFront ICA file signing ..................................................................... 22
Enabling Receiver CRL verification ....................................................................... 22
Verifying the integrity of installation sources and updates .................................... 22
Transmission security ............................................................................................. 23
Securing access with NetScaler ............................................................................. 23
Ensuring FIPS compliance of SSL server communications .................................... 23
Configuring end-to-end TLS (SSL) communication ............................................. 23
Securing access using SSL VPN ............................................................................ 24
Configuring SQL encryption .................................................................................. 25
Configuring SMB encryption for UPM profile store .......................................... 25
Audit controls ......................................................................................................... 25
Understanding XenApp and XenDesktop logging and reporting mechanisms ...... 25
Configuring NetScaler logging and reporting mechanisms .................................. 25
Monitoring licensing alerts with Citrix Director .................................................... 28
Enabling Configuration Logging .......................................................................... 28
High availability and business continuity ............................................................. 29
Providing a highly available data store and understanding connection leasing ...... 29
Understanding Provisioning Services offline database access .............................. 30
Understanding test and QA environments ............................................................ 30
Configuring NetScaler Gateway load balancing and failover .............................. 30
Providing a highly available user profile store ..................................................... 30
Compatibility with legacy systems ........................................................................ 30
Understanding Virtual IP and virtual loopback.......................... 30
Configuring session printing ..................................................... 31
Configuring StoreFront Resource shortcuts .................................. 32

Client devices ........................................................................... 32
Securing client devices .............................................................. 32
Configuring Receiver Desktop Lock ............................................. 32
Controlling device redirection ..................................................... 32
Thin client configuration ........................................................... 32

Optimizing user experience and session performance .................... 32
Understanding mandatory profiles ............................................. 32
Understanding wireless client optimizations .................................. 33
Ensuring logon time reduction ................................................... 33
Configuring Profile Management active write back ....................... 33
Configuring session prelaunch .................................................. 34
Configuring session lingering .................................................... 34
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.*

Healthcare industry IT trends

Electronic medical records

The move to electronic medical records is one of the more significant recent changes affecting IT solutions for the medical industry. Mandates, such as the one in the U.S. by the president, to convert all patient medical records to electronic format in the shortest time possible are helping speed up and increase the adoption of informational technologies in healthcare.

Security compliance

Security regulations, such as HIPAA and HITECH in the U.S., require organizations that handle protected health information (PHI), such as hospitals, insurance companies or clearinghouses as covered entities, must keep PHI safe and secure. It can be a challenge in an industry like healthcare, where staff need secure mobile access to PHI without sacrificing workforce productivity and satisfaction. Their service suppliers often also process protected information and are therefore subject to the same compliance measures.

The security compliance is not a one-time event that can be met by a single deadline. Organizations in healthcare industry must address security issues with a strategic and trusted toolset consisting of a robust business strategy and advanced technology.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) are two primary United States laws that apply to most organizations in the healthcare industry and other companies that may have access to patient information, called “protected health information,” or PHI. These laws mandate U.S. national standards to protect the privacy and security of health information.

Security threats

Many real threats exist to the security and privacy of PHI. As required by section 13402(e)(4) of the HITECH Act, the secretary of the U.S. Department of Health and Human Services is required to post a list of unsecured protected health information breaches affecting 500 or more individuals.

As of Nov. 1, 2014, there were 1,140 security breaches. These involve one or more types of breach from one or more locations or devices. The diagrams below summarize the type and location of breaches.

Chart 1: Types of PHI breaches involving more than 500 individuals (DHHS)

- Theft (51%)
- Unauthorized Access/ Disclosure (20%)
- Loss (8%)
- Other (8%)
- Hacking IT/Incident (8%)
- Improper Disposal (4%)
- Unknown (1%)

Chart 2: PHI storage location/device breached involving more than 500 individuals (DHHS)

- Laptop (24%)
- Paper (22%)
- Desktop Computer (13%)
- Other (12%)
- Network Server (11%)
- Other Portable Electronic Device (10%)

Source: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

As seen from the data, PHI theft is greatest security threat, followed by unauthorized access. Data stolen from desktops, laptops, and other portable electronic devices account for 47 percent of breaches.
Citrix solutions for remote access and virtual desktop and application delivery are secure by design and can be used to eliminate most of these threats. In a properly configured environment, the PHI data is never transferred or stored to the client device. XenDesktop provides access to applications without the need for a local copy, thus eliminating significant risk of removable storage loss.

But because new threats are constantly arising, the most secure and effective plan must include both technology and administrative IT policies and strategies. It is not enough to rely solely on the compliance of the software.

Storing and processing PHI data

While Citrix infrastructure provides access to applications and desktops that process business-critical and PHI data, none of the components of the recommended design should directly store PHI data. Citrix recommends that you train your personnel to carefully manage administrative access to Citrix Infrastructure.

Recommendations for enabling compliance

Customers are responsible for their environment once it has been deployed, including their applications, data content, virtual machines, access credentials, and compliance with their country’s regulatory requirements.

Citrix healthcare IT solutions empower customers to address key security and compliance priorities by ensuring the right level of secure access for every individual and situation, and meeting compliance mandates. However, customers are ultimately responsible for determining if the infrastructure they intend to run complies with their country’s requirements. Citrix does not analyze the customer deployment.

Each customer should have their own compliance mechanisms, policies, and procedures in place to ensure they do not use Citrix Infrastructure in a way that violates their country’s requirements. Customers should independently verify with their own legal counsel that their implementation meets all requirements.

Handling security incidents

Some recommendations in this guide enable customers to configure auditing of user access to the applications that process PHI, as well as administrative actions. However, the Citrix software components are not intended to monitor security breaches; customers are responsible for implementing appropriate monitoring in other systems they control.

A security incident is any unlawful access to PHI or applications that process PHI, or unauthorized access to the equipment or facilities resulting in loss, disclosure, or alteration of PHI. It does not include unsuccessful security incidents, such as pings and other broadcast attacks on the firewall, port scans, unsuccessful logon attempts, denial of service attacks, and any combination of the above, as long as no such incident results in unauthorized access, acquisition, use, or disclosure of PHI.

Benefits of Citrix solutions in healthcare

Citrix XenApp and XenDesktop transform healthcare IT with simple, compliant solutions that give clinicians and staff real-time access to critical Windows, mobile, web, and SaaS applications. XenApp and XenDesktop allow hospitals and health systems to:

- Improve clinician productivity and patient interaction and care by delivering seamless access to clinical information.
- Streamline IT operations, support mobile health trends, and simplify protection of PHI and sensitive information.
- Provide secure application access across devices, locations, and networks with full encryption, authentication, and logging.
XenApp and XenDesktop centralize the management and delivery of legacy custom apps, Windows apps such as electronic health record (EHR) and computerized physician order entry (CPOE) systems, graphical apps such as picture archiving and communication systems (PACS) imaging, and clinical or office desktops. Apps and associated data remain in the data center, where they are accessed using granular, policy-based user authentication. Real-time network and performance optimization technologies ensure a high-definition experience regardless of location, device, or network connection.

With Citrix app and desktop virtualization, clinicians get real-time access to complete resources from any device within a hospital, medical center, or healthcare system, or from remote locations. Seamless roaming across sites, devices, and networks ensures optimal convenience and productivity. Administrative and business personnel can securely access their apps and data from remote locations for greater flexibility, mobility, and responsiveness. IT can simplify operations and secure PHI by centrally managing, patching, and updating desktop images and apps in the data center.

To support compliance and ensure patient privacy and data protection, the inherent security of virtualization, including centralization of desktop and application processing behind the firewall, is complemented with essential features. These include standards-based encryption, secure remote access with advanced access control, password expiry management, enhanced event logging, multifactor authentication, and web application firewall.

Moving to remote access and workspace mobility solutions can help organizations to work more effectively:

- Health-care-specific software, such as EHR, prescription management, or CPOE systems, frequently require application updates, and centralization of computing resources makes day-to-day management easier.
- Enterprise medical imaging and PACS operate with graphical data that require significant investment in the networking infrastructure. HDX technologies within XenDesktop reduce network utilization while providing high-quality images over a secure connection.
- Many clinics have many locations within one or multiple regions that need IT support. Replacing traditional desktops with thin clients reduces total administration and operating costs while enhancing security.
- Remote access can help with data centralization, which makes compliance audits easier.
- Workspace mobility is not just access from a mobile device. With XenApp and XenDesktop, medical personnel are not tied to a specific PC; they can access their workspace from any thin-client-based kiosk across the hospital. Additionally, insurance organizations require secure remote access to PHI, and agencies that perform audit of hospital bills, diagnosis-related documentation, and other PHI, also need secure remote access.

Healthcare use case needs and considerations

- Many doctors and ER teams require access to PHI and other information on the go to help patients where they are.
- Fast user logons and reconnections to existing sessions are extremely important in healthcare because every second can save a patient’s life.
- Thin-client-based kiosks are used heavily for patient self-check-in using anonymous access.
- Repurposing old computers as thin clients can reduce costs.
- There is no tolerance to downtimes; access to critical applications must be highly available.
- Many SaaS applications require Single Sign-on.
- Speech-recognition systems connected to electronic health records (EHR) systems require a high-quality audio transmission to ensure correct recognition.
Architecture 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. For more information about the XenApp and XenDesktop system requirements, go to 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 (PVS) 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

This 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>Profile Management 5.1</td>
<td>Citrix</td>
<td></td>
</tr>
<tr>
<td>License Server 11.12</td>
<td>Citrix</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows 8.1</td>
<td>Microsoft</td>
<td></td>
</tr>
</tbody>
</table>
# Mapping HIPAA requirements to implementation

<table>
<thead>
<tr>
<th>Rule</th>
<th>HIPAA Security Rule Section</th>
<th>Implementation Specification</th>
<th>Citrix Response</th>
<th>Document Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security standards: General rules</td>
<td>164.306(a)</td>
<td>General requirements</td>
<td>Citrix NetScaler and XenDesktop help IT administrators ensure the confidentiality and availability of applications that process PHI by providing flexible segmentation of the environment.</td>
<td>Access control</td>
</tr>
<tr>
<td>Administrative safeguards</td>
<td>164.308(a)(1)</td>
<td>Risk management information system activity review</td>
<td>XenApp and XenDesktop centralize applications and data to minimize risk of theft or loss and maximize data security. They also provide reporting functions to help monitor application usage and configuration changes. NetScaler Gateway manages information access to help minimize risk for each access scenario.</td>
<td>Securing the environment</td>
</tr>
<tr>
<td>Category</td>
<td>Regulation</td>
<td>Description</td>
<td>Topic</td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Workforce security</td>
<td>164.308(a)(3)</td>
<td>Authorization and/or supervision termination procedures</td>
<td>Authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>XenApp and XenDesktop (de-)provision application access on demand. NetScaler Gateway can assist with provisioning or de-provisioning network access on demand and can authorize appropriate access by user, device, connection, and location based on custom policies.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information access</td>
<td>164.308(a)(4)</td>
<td>Isolating healthcare clearinghouse function access Authorization access establishment and modification</td>
<td>Access control</td>
<td></td>
</tr>
<tr>
<td>management</td>
<td></td>
<td>XenApp and XenDesktop can enable easy and secure access of isolated information clearinghouses with application publishing. XenApp, XenDesktop, and NetScaler Gateway can control application and network access authorization by user role and allow rapid modification from a centralized single point of management.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security awareness</td>
<td>164.308(a)(5)</td>
<td>Protection from malicious software Logon monitoring Password management</td>
<td>Securing the environment</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>XenApp and XenDesktop centralize critical applications, including web browsers, to help protect information from malicious code on user devices. NetScaler Gateway can check that connecting devices have adequate protection from malicious software before allowing network access.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contingency plan</td>
<td>164.308(a)(7)</td>
<td>Emergency mode operation</td>
<td>High availability and business continuity</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>XenApp and XenDesktop can enable users to access critical applications in emergency mode using normal operating procedures. Furthermore, the centralized architecture can greatly simplify data backup procedures, IT change management, and business continuity planning. NetScaler Gateway supports multiple ways of configuring high availability and disaster-recovery scenarios.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Physical safeguards

<table>
<thead>
<tr>
<th>Physical safeguards</th>
<th>164.310(a)</th>
<th>Facility access controls</th>
<th>XenApp and XenDesktop help with data centralization that in turn helps secure physical access to the servers and storage systems that store PHI.</th>
<th>High availability and business continuity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workstation use</td>
<td>164.310(b)</td>
<td>Authorization and/or supervision Termination procedures</td>
<td>XenApp and XenDesktop de-provision application access on demand. NetScaler Gateway can authorize the most appropriate access based on IT-configured policies for corporate-owned and non-owned devices.</td>
<td>Authentication Access control</td>
</tr>
<tr>
<td>Physical safeguards</td>
<td>164.310(c)</td>
<td>Workstation security</td>
<td>XenApp, XenDesktop, and NetScaler support different authentication methods, including smart cards and proximity cards.</td>
<td>Authentication Access control</td>
</tr>
<tr>
<td>Device and media controls</td>
<td>164.310(d)(1)</td>
<td>Disposal media reuse</td>
<td>XenApp and XenDesktop maintain all applications and information within the data center, leaving no residual data on user devices.</td>
<td>Access control</td>
</tr>
</tbody>
</table>

## Technical safeguards

<table>
<thead>
<tr>
<th>Access controls</th>
<th>164.312(a)</th>
<th>Unique user identification</th>
<th>XenApp, XenDesktop, and NetScaler support for standard Windows authentication, LDAP(S), RADIUS, TACACS, SAML authentication. Full support for a group-based access and role-based administration. Administrator can immediately terminate remote sessions.</th>
<th>Authentication Access control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access controls</td>
<td>164.312(a)</td>
<td>Emergency access procedure</td>
<td>In XenApp and XenDesktop, administrators can change security associations to provide emergency access to the applications, including the anonymous access.</td>
<td>Authentication Access control High availability and business continuity</td>
</tr>
<tr>
<td>Access controls</td>
<td>164.312(a)</td>
<td>Automatic logoff</td>
<td>XenApp, XenDesktop, and NetScaler policies can control various inactivity timeouts ensuring that users are logged off after a designated period of inactivity.</td>
<td>Access control</td>
</tr>
<tr>
<td>Access controls</td>
<td>164.312(a)</td>
<td>Encryption and decryption</td>
<td>With XenApp and XenDesktop, all sensitive session and control data transmitted across the network is protected using the advanced encryption standard (AES), FIPS 197.</td>
<td>Transmission security</td>
</tr>
<tr>
<td>Audit controls</td>
<td>164.312(b)</td>
<td></td>
<td>With XenApp and XenDesktop, all connection and session activity can be logged for security and quality-of-service purposes.</td>
<td>Audit controls</td>
</tr>
<tr>
<td>Integrity</td>
<td>164.312(c)</td>
<td></td>
<td>Protection from MIM attacks and ensuring session consistency.</td>
<td>Data integrity</td>
</tr>
<tr>
<td>Person or entity authentication</td>
<td>164.312(d)</td>
<td></td>
<td>Extensible StoreFront authentication. Authentication at the NetScaler.</td>
<td>Authentication</td>
</tr>
<tr>
<td>Transmission security</td>
<td>164.312(e)(1)</td>
<td>Integrity controls</td>
<td>Numerous checks are made on the encrypted data after it is received to ensure network transmission integrity.</td>
<td>Transmission security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Encryption</td>
<td>All network traffic is protected and encrypted using both SSL and a secondary layer of 128-bit AES encryption.</td>
<td>Transmission security</td>
</tr>
</tbody>
</table>

Security standards: General rules

| Security standards: General rules | 164.306(a) | General requirements | Citrix NetScaler and XenDesktop help IT administrators ensure the confidentiality and availability of applications that process PHI by providing flexible segmentation of the environment. | Securing the environment |
| Security standards: General rules | | | Audit controls | |

citrix.com
Section 3: How Citrix technologies address the HIPAA categories

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 VDA setup.

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.

Auto Client Reconnect

This setting allows or prevents automatic reconnection by the same client after a connection has been interrupted.

Allowing automatic reconnection enables users to resume working where they were interrupted when a connection was broken. Automatic reconnection detects broken connections and then reconnects the users to their sessions.

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.

**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.

**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.

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>
<tr>
<td>Read Only Administrator</td>
<td>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).</td>
</tr>
<tr>
<td>Help Desk Administrator</td>
<td>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.</td>
</tr>
<tr>
<td>Machine Catalog Administrator</td>
<td>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.</td>
</tr>
<tr>
<td>Delivery Group Administrator</td>
<td>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.</td>
</tr>
<tr>
<td>Host Administrator</td>
<td>Can manage host connections and their associated resource settings. Cannot deliver machines, applications, or desktops to users.</td>
</tr>
</tbody>
</table>

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.

### 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.

### 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

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.

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>
</tbody>
</table>
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.

**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.

**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.
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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

**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.

**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.

**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(ercial), 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.

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.

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.

**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.

**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.

**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.

**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.

**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.

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, 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.

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.

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).

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.
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.

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.

Providing a 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.

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.

**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.

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

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.

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.

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

Thin client configuration
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.

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).

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.
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.

Configuring session lingering

By default, a user session ends after user processes and visible windows end. You can use session lingering 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.
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. XenApp, XenDesktop, NetScaler, Receiver, StoreFront, and Provisioning Services 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.