

Technical Introduction to XenApp 5 for Windows Server 2008

Overview

Shortly after Microsoft's release of Windows Server 2008, Citrix released a new version of its flagship product, XenApp (formerly called Presentation Server). Citrix XenApp 5 for Windows Server 2008 is a major code release that runs natively on the new Windows platform. With each new release of the Windows Server platform, there are undoubtedly changes to the Operating System and Windows architecture. This whitepaper aims to identify those changes that are significant to a XenApp environment. Specifically, there are three primary goals of this whitepaper:

1. Highlight the new Windows Server 2008 features and changes from Windows Server 2003, with an emphasis on Terminal Services. Discuss the impact of these features and changes as it relates to XenApp.
2. Create a basic understanding of Windows Server 2008, especially related to those features and functionality that impact Terminal Services and Citrix XenApp 5.
3. Provide an in-depth, technical introduction of Citrix XenApp 5.

This whitepaper is intended for system administrators, architects and engineers that are interested in deploying Citrix XenApp 5 on Windows Server 2008. This analysis may also be beneficial to those individuals looking to migrate from previous versions of Citrix Presentation Server to Citrix XenApp 5 on Windows Server 2008. It is important to note that this whitepaper is not a step-by-step guide to deploying XenApp.

Windows Server 2008

Windows Server 2008 offers improvement in Web delivery, virtualization, security and management. Windows Server 2008 provides increased administration and virtualization options in addition to increased security and flexibility. New functionality such as Server Core, PowerShell, Windows Deployment Services, Server Manager and many others provide reasons to consider adopting to Windows Server 2008. For XenApp deployments, it is important to note that XenApp cannot be supported on Windows Server Core.

There are a number of key differentiators that may increase momentum for Windows Server 2008. To accompany this industry move, Citrix has developed XenApp 5 for Windows Server 2008. This product introduces a variety of new and updated functionalities, as well as changes and removal of several features. Microsoft has been promoting the four main differentiators in Windows Server 2008, which include the following:

1. Improvement in Web with Internet Information Services 7.0
2. Virtualization with the Hyper-V option
3. Increased Security with features such as Read-Only Domain Controller options
4. Better manageability with Server Core, Power Shell and Server Manager.

Below is an assessment of the new features and functionality provided with Windows Server 2008.

Internet Information Services 7.0

Internet Information Services 7.0 provides the ability to customize the installation by managing more than 40 independently installed feature modules. This level of granularity allows Administrators to customize specific server roles in the environment and helps reduce potential attacks and decrease memory footprint through the removal of unnecessary modules. In addition, IIS 7.0 increases the manageability and administration of the server by providing a new graphical user interface administration tool, a new command-line tool, a new managed API, and a new WMI provider. Finally, IIS 7.0 introduces a new set of public web server APIs available as native Win32 APIs as well as managed .NET Framework APIs.

IMPACT

Web Interface for XenApp 5 requires two specific roles: IIS and Application Server. These non-default features must be manually installed in order to complete the Web Interface 5.0.1 installation. This creates a more interactive installation process.

XenApp 5 includes Application Streaming with HTTP/S support. This allows applications to be streamed using HTTP protocol in addition to the current support of SMB protocol. HTTP(s) is WAN friendly and can leverage a company's existing HTTP infrastructure including network and security policies. The Web Server configuration for HTTP/S streaming requires specific Web Server configurations. The following requirements must be considered when configuring HTTP/S streaming.

- The virtual directory on the web server can point to your existing file share instead of copying and storing profiles in two different locations.
- The Directory Browsing feature in IIS must be enabled on the virtual directory in order to properly function.
- A MIME type needs to be created to map the .profile extension to txt/xml file.
- The web server can be load balanced in order to account for resiliency.

IIS 7.0 capabilities that should be noted for Windows Server 2008 have been identified below.

- Distributed configuration – In a Citrix environment, this means that the web.config file can be located centrally and then distributed to other IIS Servers in the farm.
- Delegated administration
 - Runtime state API, which allows Administrators to see real-time requests running on the web server.
 - GUI support for remote administration over HTTP.
 - AppCmd.exe command line tool, which provides server management functionality through the command line and via scripts. From the command line, one can create and configure sites, applications, application pools, and virtual directories; one can start and stop sites, and recycle application pools. Additionally, the AppCmd.exe provides the ability to list running worker processes, and view executing requests. There is also functionality to search, manipulate, export, and import IIS and ASP.NET configurations.
- Backwards compatibility – All existing ASP applications should be compatible and work as expected with compatible ISAPI support. This means that anything built on IIS 6.0 or legacy application should still work with IIS 7.0.

Application Server

The Windows Server 2008 Application Server provides customization for supporting and deploying custom and server-based applications. There are three key components of the Application Server: Windows Communication Foundation (WCF), Windows Workflow Foundation (WF), and Windows Presentation Foundation (WPF). WCF is a platform for building connected, workflow-enabled applications that leverage Web services while WF is a programming model used to build applications on Windows. WF is comprised of .NET classes, designers for Visual Studio, as well as a workflow engine. WPF is primarily used for client-based applications.

IMPACT

The Application Server Role is a requirement for the following Citrix technologies:

- Citrix Workflow Studio – Workflow Studio leverages the Microsoft Workflow Foundation (WF) feature to provide the required functionality.
- Citrix Web Interface 5.0.1.
- Application Server Role – the Application Server Role is required as it automatically installs .NET Framework 3.0.

The Application Server Role functionality is completely new and Microsoft has communicated that there is no migration path for the Application Server configuration tool from previous versions of Windows Server. Finally, the Application Server role is not a supported role for Windows Server Core.

Hyper-V

Windows Server 2008 incorporates a hypervisor to the x64 platform that leverages Windows Server driver support and allows multiple guest operating systems to run at the same time. Hyper-V, like XenServer, requires the host platform to be x64 and can then service guest operating systems based on single or multiple processors. Finally, Windows Hyper-V provides the ability to migrate virtual machines across hosts with minimal downtime.

IMPACT

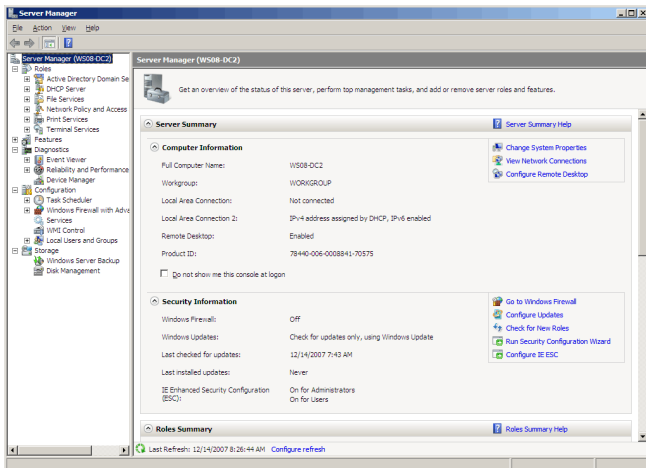
Hyper-V is a Microsoft product while XenServer extends virtualization capabilities. Shadow memory and various other enhancements have been designed specifically to allow XenApp to run at optimal performance when virtualized on XenServer. Citrix has achieved certification to run XenApp under Hyper-V furthering the functionality. Citrix has worked closely with Microsoft to enhance Hyper-V by helping to develop the shims and drivers that allow Linux to run with optimal performance on Hyper-V; as such, the Hyper-V hypervisor is fully compatible with Citrix XenServer.

Server Manager

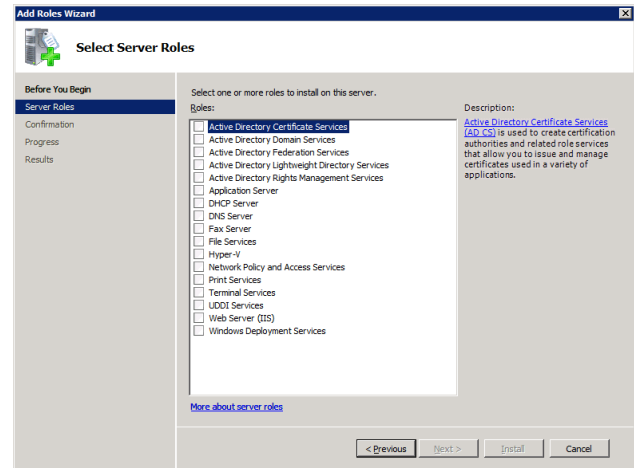
Windows Server 2008 Server Manager provides a Microsoft Management Console (MMC) integrated snap-in which can be leveraged for single server administration and can be used to install and configure various Windows Server 2008 roles. Server Manager combines the Windows Server 2003 “Manage Your Server”, “Configure Your Server”, and “Add or Remove Windows Components” features all into one component to ease installation and configuration of roles and services. Server Manager is a one-stop interface for server configuration and monitoring, providing a unified console for managing a server’s configuration and system information, displaying server status, identifying problems with server role configuration, and managing all roles installed on the server.

In addition, Windows Server 2008 includes the ServerManagerCmd.exe executable, which allows roles, services and features to be added or removed by leveraging the command-line or a script. ServerManagerCmd.exe must be run from a command prompt with elevated privileges.

For larger deployments, Microsoft has introduced Windows PowerShell, which includes a command-line and scripting platform that can be leveraged to automate management tasks for server roles such as IIS and Terminal Services. Additionally, PowerShell is used for the new Installation Manager. Windows PowerShell leverages .NET common language runtime and the .NET Framework. There are currently more than 130 standard cmdlets included with Windows Server 2008. The cmdlets are used to perform various tasks such as reading and writing text files to managing event logs or sorting and filtering data.



Server Manager Console



"Add a Role" Wizard

IMPACT

Server Manager will be one of the most leveraged tools with Windows Server 2008 as it provides the main interface for server administration and configuration. The addition of the ServerManagerCmd.exe command line utility will be very useful in automating the installation and configuration of Windows Server 2008.

PowerShell is not a default feature and must be explicitly installed. Because PowerShell has a .NET requirement and uses common language runtime, PowerShell can become a bulky addition to the server, taking time to load on the Windows Server as it loads the .NET libraries. Although VBScript will still be faster than most PowerShell equivalent features, the capabilities of PowerShell should not be overlooked. PowerShell will be leveraged more and more as more environments migrate from VBScript.

Windows Server 2008 and Group Policy Management

Microsoft acquired Desktop Standard in order to leverage a product called PolicyMaker, which now provides users with the ability to configure Group Policy Preferences. Group Policy Preferences provide the ability to change settings that are not necessarily enforced. Preferences provide over 20 Group Policy extensions that expand configurable preference settings within the GPO. Group Policy Preference extensions are part of Windows Server 2008 Group Policy Management Console (GPMC), however, they can also work with Windows Server 2003 when the environment is managed by Windows Server 2008 server and by leveraging GPMC update for Windows Vista with Service Pack 1.

Windows Server 2008 supports legacy Terminal Services Group Policy Objects in addition to a number of new configuration settings. Additionally, with Windows Server 2008 folder redirection is extended to all 13 shell folders natively, which ensures less user customization. Keep in mind that applications do not always properly behave when the Application Data folder is redirected.

ADM templates (.adm) have been updated and are now called ADMX and ADML with Windows Server 2008. ADMX/ADML is XML based. Legacy ADM templates will still be supported with Windows Server 2008, however it is likely that administrators will begin to migrate from ADM to ADMX/L. Administrators can convert existing ADM templates to ADMX using the [ADMX Migrator](#) tool. The new Administrative template files will make it easier for administrators to manage registry-based policy settings in Windows Vista and Windows Server 2008. Windows Server 2008 introduces a Central Store of ADMX files created in the SYSVOL, reducing the need for additional storage replication traffic that was inevitable in previous versions of Windows.

Some helpful additions to Windows Server 2008 include the Windows GPO search feature, which will allow Administrators to search for a specific setting within the GPMC, and a Starter GPO. A Starter GPO is a baseline of default settings that can be chosen as the basis for any new GPO created. Administrators can import and export Starter GPOs by leveraging cab files for easier distribution across environments. When a new GPO is created leveraging a Starter GPO, all Administrative template settings and values will be included.

IMPACT

Windows Server 2008 is loaded with approximately 2400 features and components that can be managed by GPO in comparison to 1700 available with Windows Server 2003. These additions can be found in the [Group Policy](#) TechNet article for Windows Server 2008. Additionally, Windows Server 2008, Windows Vista, Windows Server 2003 with SP1, and Windows XP SP2 can all be managed via Group Policy preferences. The Group Policy preference extensions currently ships as part of the Windows Server 2008 GPMC. The Group Policy preferences will be located in the Preference folder while policy settings reside in the Policy folder. Some instances such as power management, Internet Explorer, and printers' settings reside in both the Policy and Preference folders. In these cases, Policy settings have a higher priority than Preference settings. The main difference between policy settings and preference settings is that preference settings are not enforced. This means the end user can change any preference setting that is applied through Group Policy, but policy settings prevent users from changing them.

Windows Server 2008 has also changed the manner in which the Group Policy engine creates system logs. With prior Windows Server editions, the userenv.dll created a log file (userenv.log) located in the %WINDIR%\Debug\Usermode folder. Windows Server 2008 implements a new Group Policy Service that runs under the Svchost process. Group Policy event messages will now appear in the system log instead of the application log with a source of "Microsoft-Windows-GroupPolicy".

Special Folder Redirection has been included with XenApp 5 which allows administrators to map "My Documents" and "Desktop" folders from client's local device to the ICA session. Files saved to these locations in a session are accessible in the specified locations on the client device. This feature is only available with XenApp 5 and Windows Server 2008 and provides an increase in folder redirection manageability.

Finally, as Administrators migrate ADM templates to ADMX/L, it will be increasingly important for everyone to become familiar with XML.

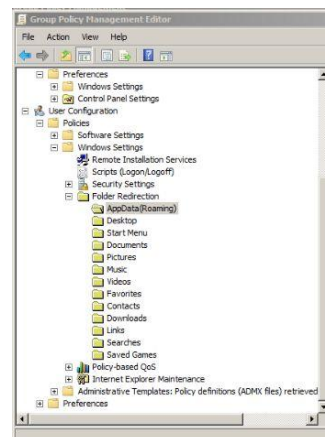
Profiles

Microsoft has completely redesigned profiles for Windows Server 2008. All Windows Server 2003 and legacy profiles are denoted v1 profiles while Windows Server 2008 profiles are v2. Windows Server 2008 maintains the same user profile settings as earlier versions of Windows; however, there are five new Terminal Services policy settings for Windows Vista. The five new policies only apply to computers running Windows Server 2008 or Vista. These policies can exist in addition to the legacy Windows Server GPOs. Older Operating Systems will ignore Windows Vista policy settings.

There are 13 shell folders included in Windows Server 2008 Group Policies that are available for redirection as follows: The shell folders have dropped the "My" and are now named Documents, Pictures, Music, etc. Additionally, the Application Data folder is now named AppData. To accommodate for backwards compatibility, Microsoft has created junction points, which are folders that look similar to a shortcut. These junction points are pointers to the new folders so that "My Documents" will point to "Documents". The folder correlation is depicted below:

Windows Vista Folder Name	Windows XP Folder Name
Contacts	Not applicable
Desktop	Desktop
Documents	My Documents
Downloads	Not applicable
Favorites	Not applicable
Music	My Music
Videos	My Videos
Pictures	My Pictures
Searches	Not applicable
AppData	Not applicable
Links	Not applicable
Saved Games	Not applicable

Windows Vista / XP Folder Names



Group Policy Folder Redirection

Another addition to Windows Server 2008 that will become important is the inclusion of the “Delete Dormant profiles” policy into GPOs. The dormant profile policy specifies the ability to delete Terminal Services user profiles older than a specified number of days on system restart. Additionally, the “Do not forcefully unload the user registry at user logoff” policy allows administrators to configure Vista and Windows Server 2008 to not forcefully unload the registry and allow the system to wait until all processes are closed, helping to alleviate issues that can be caused when the users profile fails to unload. This policy can be applied to both standard and Terminal Services profiles.

In addition, Windows Server 2008 also includes a GPO setting for Terminal Services Mandatory Profiles. Previously, administrators would have to use the Terminal Services Roaming Profile policy to configure a mandatory profile. With Windows Server 2008, Administrators can leverage the “Use Mandatory Profiles on the Terminal Server” policy in addition to the “Set path for TS Roaming Profile” setting.

IMPACT

As more customers adopt Windows Server 2008, it will become increasingly important to understand the configuration differences for profiles in addition to understanding best practices for folder redirection. The best practices for profiles and folder redirection will continue to depend on the environment and the requirements. In general, where possible, continue to limit the number of folders that are redirected ensuring that only the ones that are needed are redirected.

Server Core

Server Core is a minimal installation of Windows Server 2008 with no Windows shell and minimal GUI support. This adds an additional level of security but requires an advanced level of knowledge of the commands and provides limited functionality. This installation includes five server roles including File Server, DHCP Server, DNS Server, Media Services, Print Server, Active Directory, and Active Directory Lightweight Directory Services (AD LDS).

IMPACT

Server Core does not include support for Terminal Services or Application Server. Since XenApp deployments rely on Terminal Services and the Application Server role, Server Core role cannot be deployed in production Citrix XenApp deployments as it is not supported and cannot be installed in a XenApp environment. In general, Server Core will be leveraged for Hyper-V; Server Core was designed to provide a slim version of the operating system to be leveraged with Hyper-V.

Active Directory Domain Services

Windows Server 2008 also includes a new feature of Active Directory Domain Services called Read-Only Domain Controller (RODC). The RODC hosts read-only partitions of the Active Directory Domain Services database as well as a read-only copy of the SYSVOL folder for the purpose of deploying Domain Controllers to remote office where few users reside, where physical security is not guaranteed, for DNS DMZ support, and to remote locations that receive poor network bandwidth. The RODC supports unidirectional replication for both Active Directory Domain Services and DFS Replication.

IMPACT

The benefit to a RODC is that the RODC maintains the same AD objects and attributes that a writable domain controller maintains, however, changes are made to writable domain controllers and replicated back to the RODC. When changes are made in a site containing an RODC, the RODC forwards the change request to a writable domain controller. In order to deploy a RODC at least one writable domain controller in the domain must be running Windows Server 2008. Additionally, the functional level of the domain and forest must be Windows Server 2003 or higher.

The RODC can be useful for XenApp environments at branch offices where XenApp servers reside in order to expedite the authentication process.

New Terminal Services Features

Windows Server 2008 Terminal Services now provides administrators with the ability to present users with access to Windows-based programs hosted on the Terminal Server or provide a full Windows desktop, similar to XenApp offerings. Windows Server 2008 has numerous roles installed for Terminal Services, including Terminal Server, TS Licensing, TS Gateway, TS Web Access and TS Session Broker. Terminal Server is the only required role for customers deploying XenApp on Windows Server 2008 in addition to TS Licensing, which is required within the domain. However, it is important to understand how some of the new Windows Server 2008 Terminal Services roles compliment or compare to Citrix technologies.

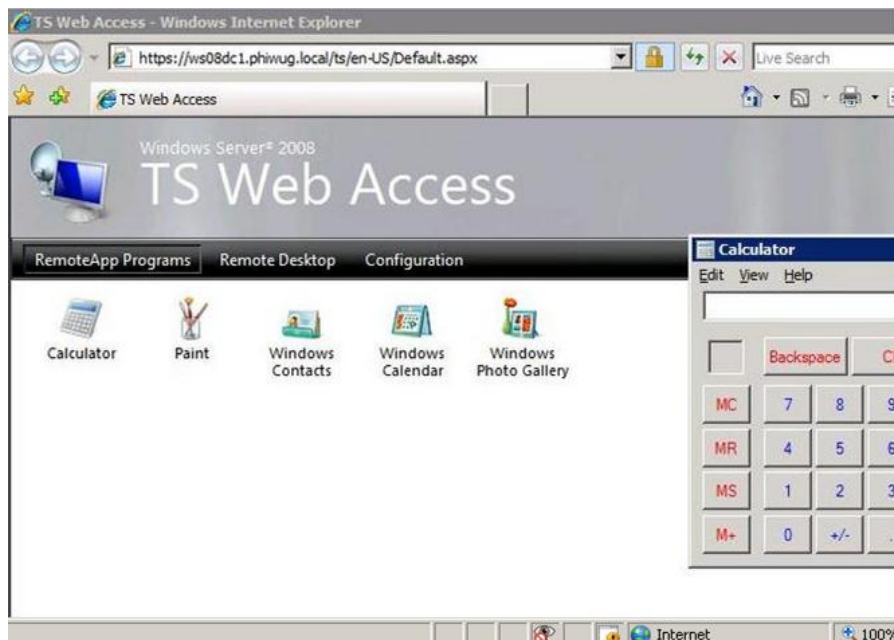
The table below compares the new Terminal Services features to existing Citrix product line:

New Terminal Services Feature	Citrix Comparable Product
TS Web Access	Web Interface
TS Remote App	Citrix Seamless Published Application
TS Gateway	Secure Gateway
TS Session Broker	Citrix Load Evaluators

TS Web Access

TS Web Access allows users to access seamless RemoteApp applications and Remote Desktop connections through a web-based interface. Users can leverage TS Web Access to launch TS RemoteApp programs accessed as links from a web browser or full Remote Desktops by specifying a particular server. To leverage TS RemoteApp launched via TS Web Access, the user's client device requires Remote Desktop Connection 6.1 and Remote Desktop access to launch a full Remote Desktop on a particular server.

Although TS Web Access does not need the Terminal Services role installed on the server to function, it is only supported on Windows Server 2008 with IIS 7.0. Once TS Web Access is installed, the basic default website is automatically created.



TS Web Access Icon Screen

IMPACT

TS Web Access provides similar functionality to Citrix Web Interface and provides users with a method to access applications hosted on the Terminal Server. Users access the application by clicking on either an .RDP or .MSI file which compares to Citrix .ICA files.

Additionally, TS Web Access allows administrators to deploy a list of TS RemoteApp programs populated from a single Terminal Server. It should be noted that this does not allow for an enterprise solution as most large deployments cannot maintain applications installed on and maintained on each server. For enterprise and large-scale deployments, XenApp provides an increased level of functionality as well as centralized management, which is critical to enterprise remote application deployment.

Terminal Services RemoteApp

Windows Server 2008 RemoteApp are programs accessed through Terminal Services. TS RemoteApp Manager provides administrators with the ability to create and distribute Windows Installer packages and .RDP files to users' desktop or in their Start menu, push a file to the user and associate it with a RemoteApp, or provide a link to access a RemoteApp from a web browser through a TS Web Access website. To access a RemoteApp, the users' client computer must have at least version 6.0 of the RDC client and have one of the following Operating Systems: Windows Vista, Windows Server 2008, Windows XP with SP1 or later, and Windows Server 2003 with SP2 or later.

IMPACT

RemoteApp compares to XenApp seamless published applications. RemoteApp applications also leverage Session Sharing to ensure that, where possible, the user accesses applications hosted on the same server to reduce logon times. The .RDP and .MSI files also contain session settings similar to an .ICA file. RemoteApp is not a required feature for XenApp on Windows Server 2008.

TS RemoteApp is not scalable for larger deployments as the administration cannot be secured or delegated and multiple server management is not available. TS RemoteApp is more suitable for smaller environments that do not require enterprise deployment and management.

Terminal Services Gateway (TS Gateway)

Windows Server 2008 Terminal Service Gateway (TS Gateway) provides administrators with a mechanism for users to access internal applications remotely from any internet-connected device that has the ability to run the Remote Desktop Connection. TS Gateway allows users to RDP over HTTPS to form a secure and encrypted connection to applications remotely without the need for a VPN.

In previous versions of Windows Server, configuring connections to internal resources was difficult due to limitations with port 3389 and firewalls and NATing. TS Gateway allows port 3389 to translate to 443 and enable users to securely connect to internal network resources remotely. Network resources can include Terminal Servers, Terminal Servers running RemoteApp programs, or computers that have Remote Desktop enabled.

It is a Microsoft best practice to manage the TS Gateway settings via Group Policy Objects. There are three Group Policy settings available for TS Gateway:

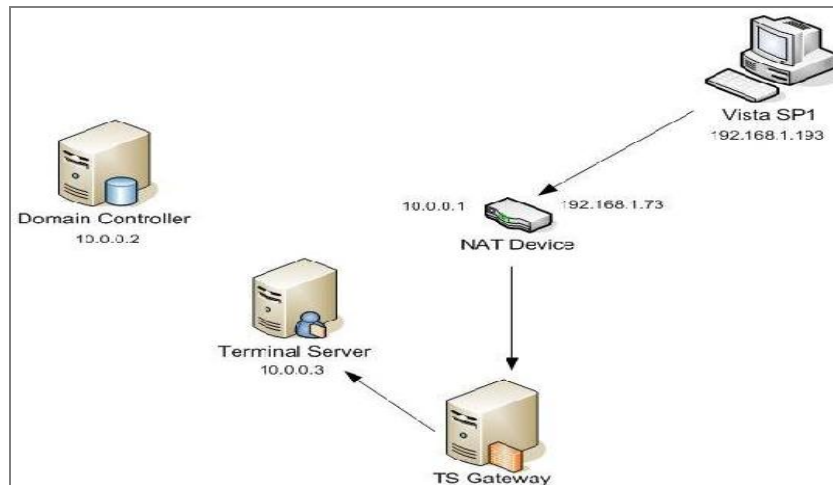
- **Set the TS Gateway Server authentication method** – Specifies the authentication method that Terminal Services clients must use when connecting to network resources through a TS Gateway server.
- **Set the TS Gateway Server Address** - Specifies the TS Gateway server that Terminal Services clients use when they cannot connect directly to a network resource.
- **Enable connections through TS Gateway** - Specifies whether Terminal Services clients that cannot directly connect to a network resource are allowed to attempt to connect to the network resource through the TS Gateway server specified under the **Set the TS Gateway Server Address** setting.

In addition, the TS Gateway Manager tool includes a console to configure authorization policies and monitor the TS Gateway connection status, health, and events. TS Gateway Manager also allows administrators to determine what groups can connect remotely, what servers the users can connect to, whether the users must be part of a specific Active Directory security group, whether device/disk redirection is permitted, and whether clients must leverage smart card authentication or password authentication.

IMPACT

Terminal Services Gateway allows RDP sessions to be tunneled over HTTPS. To use this feature this role needs to be installed on at least one Windows 2008 server, which will act as a proxy and intercept and forward RDP connections to a Terminal Server. TS Gateway is not usable in a XenApp implementation because it only tunnels RDP traffic. However, XenApp provides similar functionality with Secure Gateway in which ICA traffic is tunneled over HTTPS. Updates to Secure Gateway have been made and the new version, 3.1, will allow support on a Windows Server 2008 server and allows support for the new IP version 6 protocol.

While the TS Gateway provides administrators with more flexibility to configure RemoteApp applications for both internal and external users, it does not provide the granularity that SmartAccess provides from the Citrix Access Gateway product line. TS Gateway Manager also does not have the flexibility to fall-back to Java when a Remote Desktop Connection is not possible which would in turn make kiosk access more difficult.



TS Gateway Architecture

Terminal Services Session Broker

Windows Server 2008 Terminal Services Session Broker (TS Session Broker) provides session load balancing across Terminal Servers in the farm. Session Broker, previously known as Session Directory, distributes the load between servers in a Terminal Services farm based on sessions. To create a load balanced Terminal Server farm, the administrator must install the TS Session Broker role and populate the Session Directory local group. Session Broker leverages DNS round robin load balancing, however, a host resource record must be created for each Terminal Server in the farm mapping to the Terminal Server farm name in DNS to allow this functionality.

Session state is monitored including session IDs, user names, and the name of the server hosting the session and user session information is subsequently stored in Active Directory. Sessions are directed to servers in the following order:

- A user with an existing session will connect to the server where a session pre-exists.
- A user without an existing session will connect to the Terminal Server that has the fewest sessions.

The maximum number of pending logon requests per server is set to 16 in order to ensure that no particular Terminal Server is overwhelmed with logon requests. With TS Session Broker it is also possible to assign each server a weight value to help distribute the load depending on the server in the farm. This can be used to distribute more load to servers

with more capacity. TS Session Broker is available with Windows Server 2008 Standard, Enterprise and Windows Server Datacenter operating Systems. In order to leverage TS Session Broker, Remote Desktop Connection 5.2 or later is required.

IMPACT

The Session Broker feature is similar to the XenApp Load Manager and load balances the sessions in the farm; however, TS Session Broker only load balances based on user count and does not provide the level of granularity offered by XenApp. Finally, XenApp Load Balancing has been further enhanced with Preferential Load Balancing introduced in XenApp 5 to include session importance and priority. This new functionality is aimed at providing certain users or group of users with a prioritized user experience and allows administrators to have even more granular control of the session load balancing mechanism.

Terminal Services

Microsoft redesigned Windows Server 2008 Terminal Services to be included in part with Remote Connection Manager (RCM) and Local Session Manager (LSM). RCM manages ICA and RDP connections while LSM manages sessions running on Terminal Services. Citrix XenApp 5 has been integrated with the RCM service which currently runs at a lower privilege compared to Windows Server 2003 Terminal Services.

Windows Server 2008 allows any of these services to be restarted without requiring a reboot. If LSM is restarted, all user connections will be lost. However, if RCM is restarted, connections will become disconnected but will not be lost. Users will be able to reconnect to disconnected sessions automatically if the automatic client reconnection feature has been enabled.

IMPACT

The impact of this change means that patching Terminal Servers components can be accomplished without rebooting and losing sessions. Additionally, because Terminal Services has been redesigned into RCM and LSM services, the Terminal Server is not as vulnerable to an attack of service as the components are diversified between RCP and LSM.

Lastly, XenApp services will now have their own service specific SIDs, which will allow administrators to have more granular access control. This reduces the overall attack surface of XenApp as there is less code running at higher privilege.

Terminal Services Licensing

With Windows Server 2008 the licensing model requires a server license for each running instance of the server software. Terminal Services functionality is included in the Windows Server license. In addition to the Windows Server license, a Windows Server Client Access License (CAL) is required. A TS CAL is required for each user or device. There are two types of TS Client Access Licenses: TS Device CAL or TS User CAL. When a user/device accesses a Terminal Server, the user/device is required to have a TS CAL as well as a Windows CAL. TS CAL tokens are managed by the Windows Server 2008 TS License Manager.

Citrix XenApp 5 and Window Server 2008

Citrix XenApp 5 provides customers with improved maintenance and manageability, enhanced end-user experience for Application Delivery, and increased performance for users. XenApp 5 for Windows Server 2008 includes improved system stability and enhanced security. Citrix Web Interface 5.0.1 has also been enhanced to increase usability with an updated look and feel as well as access from both desktops and mobile devices. Updates include the addition of the new XPS-based Universal Printer driver, Special Folder Redirection addition, and Application Streaming updates including inter-isolation communication. Lastly, Citrix XenApp 5 provides increased security on Windows Server 2008 with User Account Control, Windows Firewall, protected-mode Internet Explorer and much more.

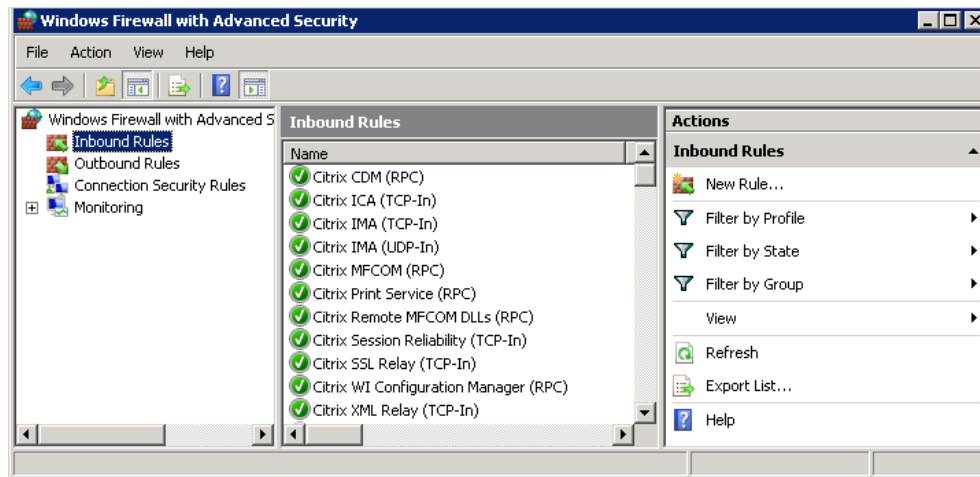
Many features have been updated or added to this release in order to increase the usability of Citrix XenApp. The sections below provide more detailed information in regards to the updated components. For more information on Citrix XenApp 5 please view the following Readme article for Citrix XenApp 5 for Windows Server 2008 <http://support.citrix.com/article/CTX113393> which provides links to the following documents: Getting Started with Citrix XenApp 5, the Installation Checklist, Installation Guide, and the Quick Start Guide for "Project Delaware".

XenApp 5 Security Improvements

Windows Server 2008 provides a number of improved Security features including Windows Firewall improvements, User Account Control, and Network Access Protection. User Account Control ensures that processes run at non-elevated privileges unless required. This includes new authentication architecture for protection against malicious software.

Network Access Protection (NAP) helps to ensure that computers that try to connect to the network comply with the organization's security policy. NAP has the ability to verify the health of connecting computers and enforce compliance with the organization's security standards.

XenApp 5 also supports the Windows Firewall which is enabled by default. XenApp components automatically register with the firewall during the installation process. Citrix XenApp processes are also User Account Control compliant and run at non-elevated privileges unless required. Additionally, to provide enhanced security non-core XenApp services are disabled by default.



Windows Firewall with Advanced Security

IMPACT

Windows Firewall is on by default in Windows Server 2008 and therefore doesn't need to be considered when configuring XenApp 5 on Windows Server 2008. Additionally, Citrix XenApp 5 components automatically register with Windows Firewall.

XenApp 5 and Printing

Windows Server 2008 introduces the XPS printing protocol which is the next generation printing protocol with enhanced printing capabilities. XPS printing was developed by Microsoft to optimize the printing architecture of Windows Vista and Windows Server 2008. XPS is based on XML paper specification and consists of structured XML markup that defines the layout of a document and the visual appearance of each page, along with rendering rules for distributing, archiving, rendering, processing and printing the documents. XPS printing significantly improves print fidelity and performance, reduces bandwidth consumption, and supports independence and resolution independence.

XenApp 5 provides improvements in printing with the XPS Universal Printer Driver. XenApp 5 installs the Citrix equivalent XPS-based Universal printer driver solution that is available via an ICA session. This driver is the default driver supported by Windows Server 2008 and Vista and is also supported with Windows XP SP2 and higher with XenApp Plug-in version

11.x. In order to leverage this feature, .NET Framework 3.0 is required on both the server and the client. By default EMF based printer is still the default UDP driver. XPS can be made the default driver by making changes to the registry. In order to modify the default Universal Printer Driver modifications to the following registry key is required: HKLM\Software\Citrix\UniversalPrintDrivers.

Microsoft TS Easy Print allows an XPS-based Universal Printer Driver to be available to users within an ICA session and allow printing from a user's local print device. TS Easy Print is included with Windows Server 2008 and is a proxy for all print actions by redirecting print jobs to the user's local machine without the need to install additional print drivers on the Terminal Server. Easy Print allows the user to leverage the drivers locally installed on their client system. The Easy Print driver redirects all calls to the driver to the client device. This feature is not required to be installed for XenApp. In order to leverage Easy Print on Windows Server 2008 Terminal Server must have .NET Framework 3.0 SP1 installed.

IMPACT

The XPS UPD is a solution very similar to the Citrix Advanced Universal Printer Driver. The XPS Universal Driver is installed by default alongside the other universal drivers. The default universal driver order is: EMF, XPS, PCL5c, PCL4 then Postscript. Through the registry, XPS printing can be enabled.

The updated universal print driver works as follows:

1. XenApp plug-in interrogates the client device print spooler for print support settings (EMF, XPS, PCL5c, PCL4, PS)
2. XenApp plugin sends client print information to server
3. Server initiates matching UPD to client (e.g., EMF on client = EMF on server, XPS on client = XPS on server, etc.)
4. UPD driver and client used for duration of session

If XPS printing is enabled on the server, client devices with .NET 3.0 will use XPS, while client devices without .NET 3.0 will fallback in the following order: EMF, PCL5c, PCL4, and then Postscript. When the XenApp plug-in connects, it is the VDSPL.DLL that queries the registry to check for the .NET 3.0 registry keys.

XenApp 5 and Win2K3 vs Win2K8

XenApp 5 for Windows Server 2003 (Scioto) provides a minor update to Presentation Server 4.5 FP1/HRP2. On the Windows Server 2003 platform, XenApp 5 is not a full product installation. There are no binaries to update on any of the farm member servers. Only the Citrix License Server and the Access Management Console must be upgraded. The plugins agents can optionally be upgraded. The prerequisites for XenApp 5 on Windows Server 2003 are the same as XenApp 4.5 and include .NET Framework 2.0 and JRE 1.5.0_09.

XenApp 5 for Windows Server 2008 (Delaware) is a full installation with product updates to reflect the new product name, XenApp, and version number. XenApp 5 prerequisites include .NET Framework 3.0 or NET Framework 3.5, Visual C++ 2005 Redistributable Package, and any 1.5x and 1.6x JRE. All prerequisites will be automatically installed during the XenApp installation including dependent components except for the JRE, which will need to be manually downloaded from sun.java.com.

XenApp 5 + Windows Server 2008 Updated Components

The following section details updates to XenApp 5 components for Windows Server 2008.

Web Interface 5.0.1



Web Interface 5.0.1 New Design

Web Interface 5.0 only supports XenDesktop 2.0. Web Interface 5.0.1 has been released with XenApp 5.0 and will fully support both XenApp and XenDesktop. However, if both XenDesktop and XenApp will be used from the same Web Interface 5.0.1 site, the XenApp plug-in 10.2x is required. Web Interface 5.0.1 can be deployed for both Windows Server 2003 and Windows Server 2008.

Web Interface 5.0.1 provides users with a brand new look and feel provided by several enhancements. Some of the enhancements include tabbing for easy access to applications, desktops, admin messages and personal preferences. Site navigation has been improved and allows the user to easily navigate through the folders replacing the “Home”, “Top”, and “Up” links in previous releases of the Web Interface. Users have the ability to select their view including details, icons, list & view for displaying applications and desktops.

Users can also search for applications and desktops when they are unable to locate the published application. The new version of Web Interface supports simple name search functionality. The search is performed within the user’s context. This functionality is particularly useful when users are presented with numerous resources, which are buried inside more than one layer of folders. The search functionality in this release is only applicable to the resource names. If there are no results matching the search criteria, an error message will be displayed to the user.

Web Interface 5.0.1 has introduced a new feature that allows users to access their Web Interface website from small screen mobile hand held devices. When accessed from a hand held device, Web Interface is displayed in a reduced graphics mode to account for the size and bandwidth limitations of hand held devices. This will extend the usability of Web Interface and improve user assistance and messaging when interacting with Web Interface over a mobile device. The Web Interface mobile version is also integrated with the Advanced Access Control (AAC) Navigation User Interface. Users access the URL by accessing <http://site/m> or <http://site/mobile>.

Additionally, Web Interface will have 64-bit support for IIS, IIS 7.0 support, support for XenDesktop 2.0, Advanced Kerberos Authentication support, and generic RADIUS support. Previous releases of Web Interface for Windows supported SecurID and SafeWord natively through an agent installed on the web server. Generic RADIUS was not supported except on UNIX. This release of Web Interface for Windows supports two-factor authentication using generic RADIUS.

Web Interface requires the Application Server Role, IIS 6 Compatibility Role, ASP.NET and .NET Framework 3.5. IIS7 does not store its configuration in the metabase as in previous versions of IIS, but there is a compatibility layer that allows administrators to configure IIS using metabase. Web Interface requires this compatibility layer. If it is not installed, the warning message below is displayed and the install process will terminate.



Web Interface Installation Error

The user’s identity is displayed when logged in to Web Interface, and the user is able to view confirmation messages when a user action has succeeded. Similarly, when a user action fails, Web Interface will provide the user with useful feedback and will identify the areas causing the problem so users can solve the problem quickly. The new version of Web

Interface also provides hints. These hints are shown to users at random to the user comprised of items in the default locale language resource file, which have keys of the form "Hint_XXXXX". A hint is chosen at random from the pool of all hints with the following restrictions - the hint must be one which can be shown within the currently selected tab of the applications screen.

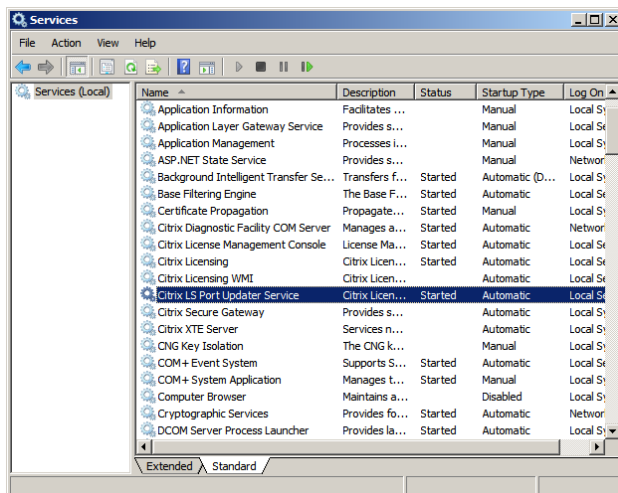
There are now two modes for the user interface logon, simple and advanced. By default, users will see the Logon screen in the simple mode. This mode removes the header, the ability to read messages, and the ability to change user preferences. Citrix recommends this mode if administrators want to limit the complexities for the users. In contrast, the advanced mode provides full functionalities to users. Users will be able to read messages and change their preferences before logon.

The new version of Web Interface also provides a revised and increased set of site customizations including branding image or color in the header area, Heading image and an optional hyperlink for the image, navigation bar font color, background color and image, content font color and background color or image, whether to display the header. Some older customizations from previous versions of Web Interface are no longer applicable.

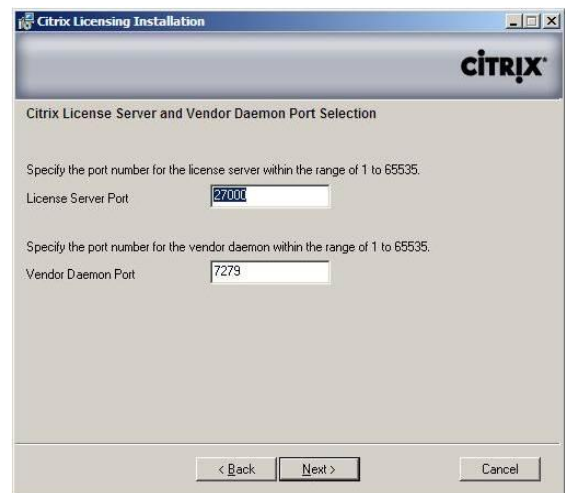
License Server 11.5

License Server 11.5 is required for XenApp 5 on Windows Server 2008. The new Citrix License Server can be deployed on Windows Server 2000, 2003, and 2008 and is backwards compatible. Citrix License Server 11.5 is required for XenApp 5.0 on Windows Server 2003.

With Citrix License Server 11.5, the static licensing ports are configured during the installation and are automatically open on the Windows Server 2008 firewall. Lmgrd.exe still uses default port 27000. Citrix.exe, the License Vendor Daemon, no longer uses a random port by default and now uses static port 7279. The licensing service has also been updated where newly added license files are automatically updated with the correct port numbers. The new licensing service "Citrix LS Port Updater Service" will automatically update newly added license files, which ensures no need to manually correct port numbers. The LSportUtil is used to change license ports after installation. In order to use the LSportUtil, browse to \Program Files\Citrix\Licensing\ls directory from the command line. The "Query" switch from the command line can be used to verify the license server ports, while the "set" switch can be used if there are no ports specified in the license file. Once ports are updated, the license service should be restarted.



Citrix LS Port Updater Service

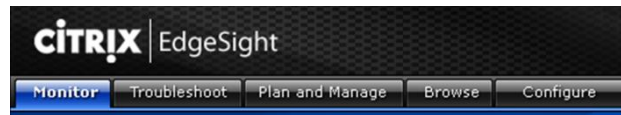


Citrix Licensing Installation

Resource Manager and Installation Manager

Resource Manager (RM) has been completely redesigned for XenApp 5. This XenApp feature has been built from the ground up leveraging EdgeSight technology. Resource Manager powered by EdgeSight no longer supports Oracle as a database platform. The new Resource Manager will provide a subset of functionality provided by EdgeSight for XenApp. Additionally, RM for XenApp 5 provides improved ICA session visibility and reporting facility which will help better

diagnose user connection problems. The new functionality provides access to a much richer set of reports to assess the health and value of XenApp.



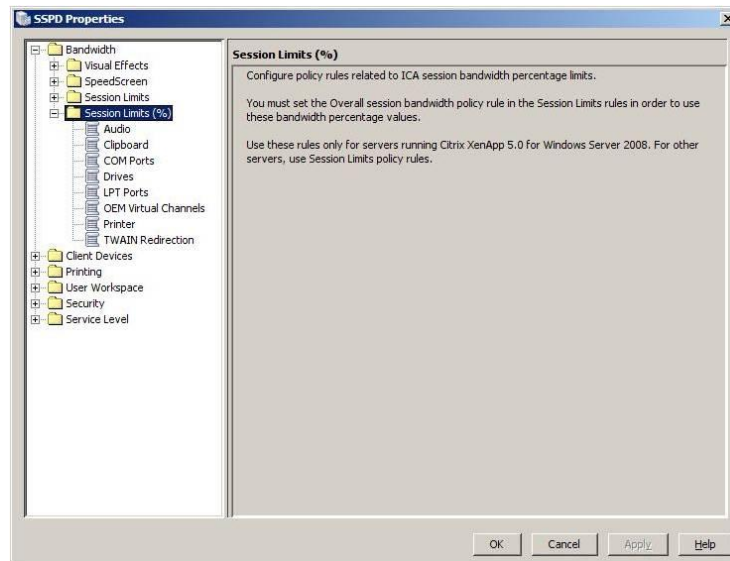
Citrix Resource Manager Powered by EdgeSight

Installation Manager has been updated and is now based on the Windows Task Scheduler and PowerShell 1.0. Additionally, Installation Manager Packager has been removed in XenApp 5. The primary function for Installation Manager going forward will be to deploy pre-packaged applications, hot fixes, and scripts pushed to XenApp servers. The new Installation Manager is only supported on XenApp 5 for Windows Server 2008, whereas the updated Resource Manager is supported on XenApp 5 on Windows Server 2003 and XenApp 5 for Windows Server 2008. Legacy Resource Manager and Installation Manager can be leveraged with XenApp 5 on Windows Server 2003.

Policy Enhancements

XenApp 5 also provides updates to the policies including SpeedScreen Progressive Display and Virtual Channel Bandwidth. SpeedScreen Progressive Display is enabled using a Citrix policy similar to XenApp 4.5. However since it is in all three editions of XenApp by default, administrators will only need to create a Citrix policy if the setting needs to be changed from the default settings. If no changes to the defaults are required, it is not necessary to create a policy to enable this feature. Please note that the default settings have changed with XenApp 5 policies. The default image compression level is set to Medium. Progressive Display compression is set to High by default.

XenApp 5 also provides improvement in Virtual Channel Bandwidth. This feature is now optionally controlled by percentages which allows for more granular control of the Virtual Channels.



XenApp Policy Properties

Access Management Console

The Access Management Console has also been updated for XenApp 5 on Windows Server 2008. There is now a unified installer for the AMC and Citrix Password Manager is included in the discovery process if installed.



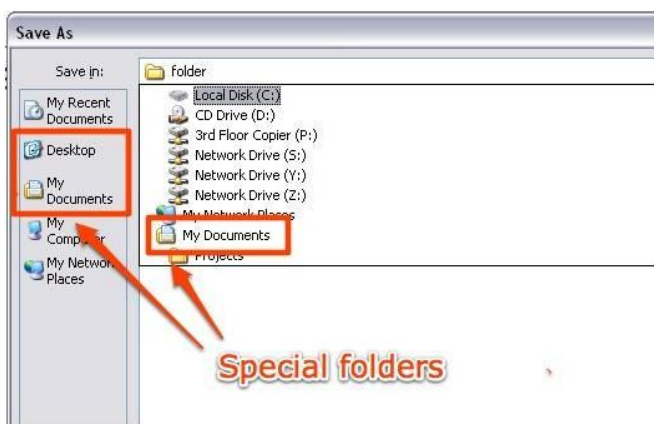
Access Management Console

Special Folder Redirection

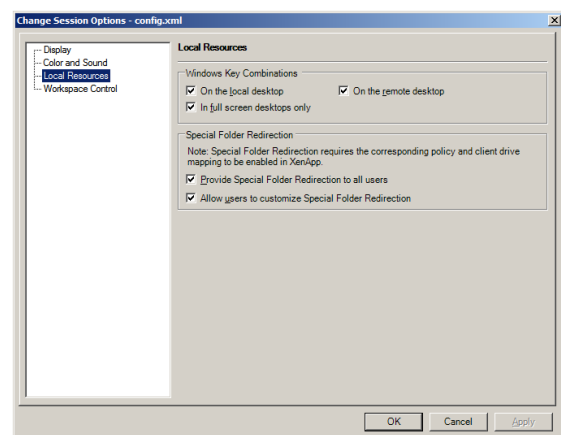
Special Folder Redirection (SFR) is a new feature with XenApp 5. On Microsoft Windows operating systems, Special Folders are folders which are presented to the user through an interface as an abstract concept, instead of an absolute folder path. 'My Documents' and 'Desktop' are the two folders configurable with Special Folder Redirection within the XenApp 5 release. Special Folder Redirection maps "My Documents" and "Desktop" from ICA session to the client's local device. This feature can only be used when connecting to application using XenApp Web or XenApp Services site and requires the XenApp plugin 11.0 or higher. In order to configure this feature, a change to the Web Interface site properties is required.

The mapping process is described in detail below:

1. Upon application click, Citrix XenApp plug-in checks if SFR enabled
2. Client gathers SFR data and builds mapping structure for VDCDN40N.dll
3. Server acquires SFR data from client drive mapping (CDM) data header
4. Server checks IMA for permission to run SFR in users' context
5. Server determines special folder location using logic in SFRhook.dll
6. I/O for special folders during session handled via CDM with SFRhook.dll



Special Folder Redirection



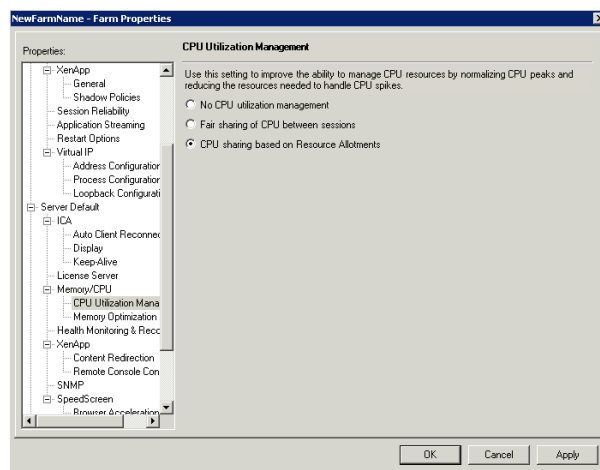
Modify Session Options

It is important to note the potential impact of redirecting certain folders leveraging Special Folder Redirection. Depending on the environment My Documents could be traversing the WAN if the documents are located on the client device. Therefore, the user experience could be slower for browsing, opening, saving files.

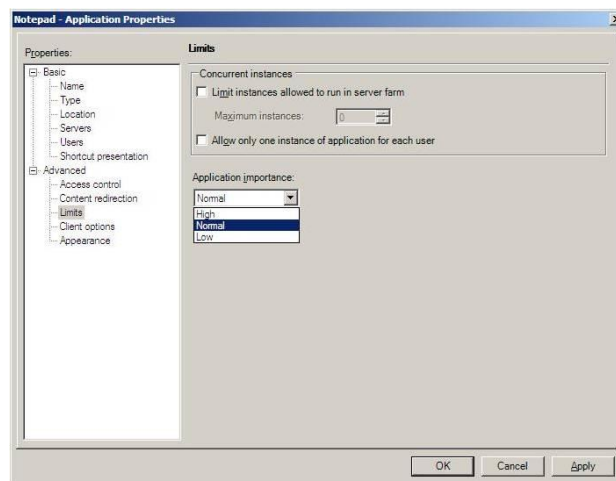
Preferential Load Balancing

XenApp now provides Preferential Load Balancing based on session importance. This allows for preferential treatment for users and applications. This feature is available on XenApp 5 on Windows Server 2008 in Platinum Edition **only**. Preferential Load Balancing enables administrators to prioritize users and group and/or applications. When a new session is launched, based on the session priority, the session will be appropriately load balanced to provide an enhanced user experience. The session importance is designated 1 (Low), 2(Normal), or 3 (High importance) within Citrix policies. Applications are also designated based on the same scale but done so within published application properties. The user rating multiplied by the application rating produces the priority level that the user session will be allocated. For example, a user with a “3” rating multiplied by a “3” application yields a rate of “9” for the session. In addition, a load evaluator that uses the Server User rule must be created and assigned to all servers. Users are then distributed to servers based on least number of shares allocated at that time. If there is a high importance session that needs to be connected then the system attempts to find a server with the lowest load but also which has the fewer high importance sessions on it.

Windows Server 2008 provides session-based load balancing where each application and user is considered equal. In contrast, XenApp 5 provides CPU cycle allocation to users, and CPU Utilization Management then takes that resource allocation one step further. CPU shares are relative and are a way of distinguishing that one user should receive more CPU cycles than another. It is a soft limit because if the number of cycles allocated are not being used, then they can be borrowed by another user until its use is re-requested by the original user.



CPU Sharing Based on Resource Allotments



Preferential Load Balancing Configuration

The idea of Preferential Load Balancing is to provide the administrator the flexibility to assign higher and lower levels of service to users and applications based on their job functions, position within the company or any other set of criteria.

Icon and Name Changes

All Icon and name changes apply to XenApp 5 for Windows Server 2003 and Windows Server 2008. XenApp 5 provides a number of icon and name changes to accommodate the rebranding of the product. Citrix XenApp Plugin replaces the Program Neighborhood Agent name. The Full Program Neighborhood client will not be changing names but will also not be installed by default on the server. XenApp Plugin for Hosted Apps incorporates the Windows XenApp Windows plugins and replaces the Presentation Server client that appears during installation on the server. The following diagram depicts the changes to icons and names in XenApp 5.

Old Icon	Old Name	New Icon	New Name
	Program Neighborhood Agent		Citrix XenApp
	WANScaler Client		Citrix Accelerator
	Citrix Communication Gateway		Citrix EasyCall
	Citrix Password Manager		Citrix Password Manager <u>Plugin v4.6.x</u>
	Secure Access <u>Plugin</u>		Citrix Secure Access
	Presentation Server Client		Citrix XenApp <u>Plugin</u> for Hosted Apps v11.x
	Application Streaming Client		Citrix XenApp <u>Plugin</u> for Streamed Apps v1.2x
	Presentation Server Web client		Citrix XenApp Web <u>Plugin</u> v11.x
	Presentation Server Console		XenApp Advanced Configuration

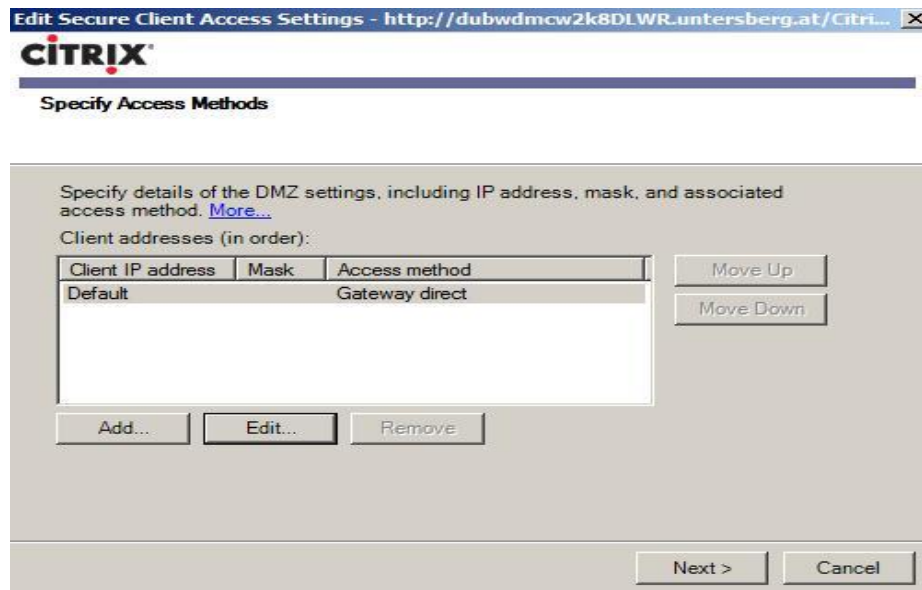
Updated Icons and Naming Convention

Secure Gateway 3.1

XenApp 5 with Secure Gateway 3.1 now supports IPv6. This is supported for XenApp 5 on Windows Server 2003 and Windows Server 2008. IPv6 expands the address length of 32 bits up to 128 bits. This is installed and enabled by default in all Windows Server 2008 and Vista machines. Support for IPv6 can also be added to Windows Server 2003 and Windows XP.

Citrix XenApp 5 supports IPv6 when using the XenApp Secure Gateway 3.1 as a proxy and can be leveraged to provide IPv6 support for external users. It is important to note that the U.S. government has mandated that new technology implementations be IPv6 compliant beginning in Q2 2008.

Secure Gateway support has also been restored in XenApp Services site (PNAgent). The updated Secure Gateway also supports half and full proxy mode. Half-Proxy is utilized when the web server enumerates applications for IPv6 connections and the Secure Gateway server proxies all IPv6 connections to the XenApp servers only. Full-proxy is utilized when Secure Gateway proxies all IPv6 to Web servers as well as the XenApp servers.

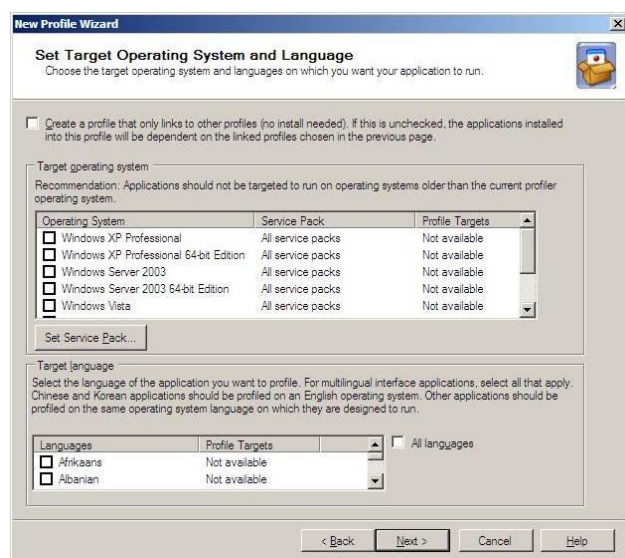
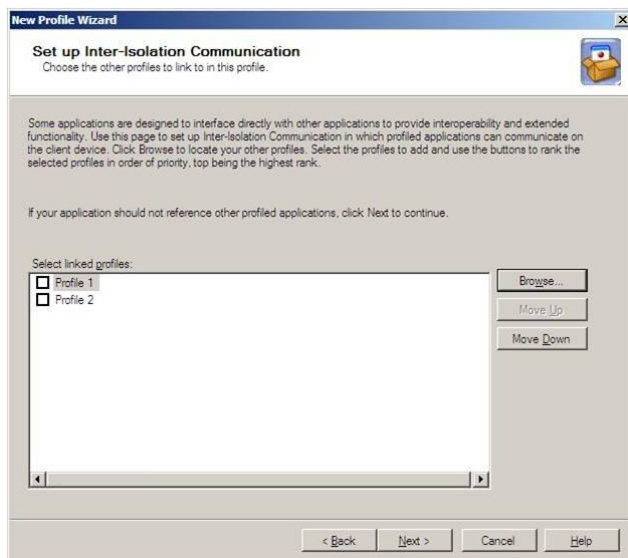


Secure Client Access Settings

Application Streaming

Application Streaming has included a number of enhancements including HTTP streaming support and inter-isolation communication between profiles. These enhancements are included in XenApp 5 for Windows Server 2003 and Windows Server 2008. In addition to these improvements, the new Application Streaming provides improvements to updating pre-cached applications. In order to deploy Application Streaming 1.2 with XenApp 5, the new Streaming Client 1.2 and the Profiler 1.2 are required. Also, please note that the Profiler machine now requires .NET Framework 3.5.

Prior to XenApp 5, applications needed to be profiled together in order to provide inter-application communication. This would require an application to run twice if two application sets were profiled separately leveraging the same base application. Inter-isolation communication enables linked applications in isolated environments to communicate with each other. This simplifies management of streamed applications as well reduces the amount of time required to update and patch streamed applications. This feature allows administrators to update core applications once; there is no need to update core applications multiple times within multiple profiles. This helps to prevent errors and inconsistencies when a patch isn't updated within all instances of an application.



Profile Wizard

Profiler Set Target Operating System

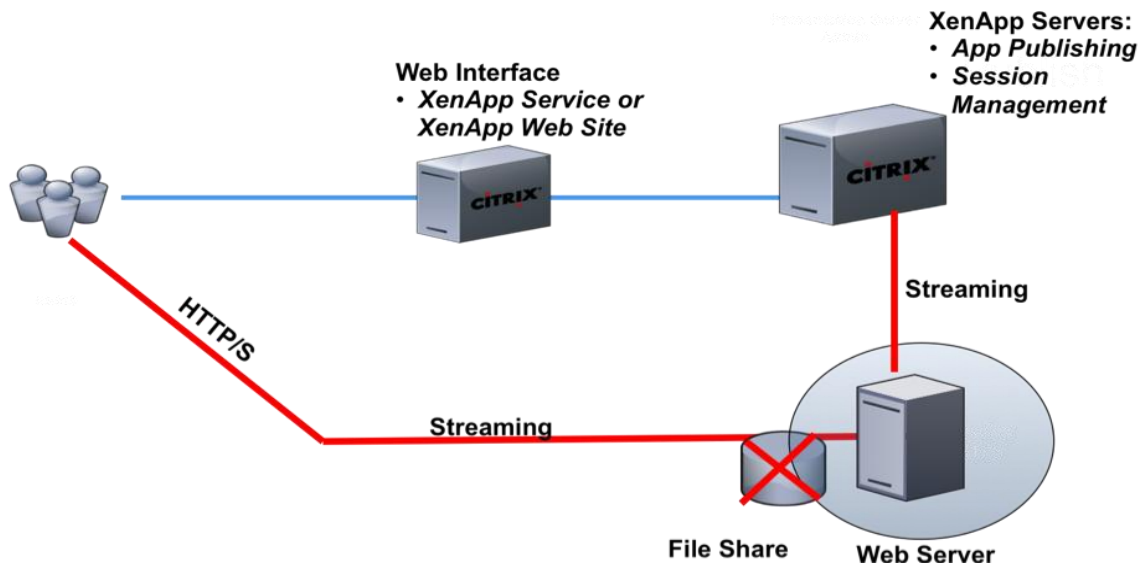
In addition to inter-isolation communication, Application Streaming has been updated to include HTTP and HTTPS protocol support. This extends the SMB protocol support to include support for applications to be streamed using HTTP protocol. HTTP and HTTPS are more efficient across the WAN, and this allows for the ability to leverage the existing web servers or even Citrix Branch Repeaters as repositories. Secure connections are now supported for streamed applications, which allows administrators to stream without the need to change network and security policies.

Previously, Application Streaming required packages to be created and placed on a file share. UNC paths and SMB protocol was leveraged on port 445. The Profiler was used to create and copy packages to the file share. The application pointed to one or more file shares during application publishing. SMB was not WAN friendly and did not provide secure communication. With XenApp 5, profiles can be streamed from a Web server instead of a file server. The Application Streaming profiler will not post to a web server. It can still only post packages to a file share. However, the package can now be streamed from a web server or web directory in addition to a file share.

Finally, offline application support has been enhanced, resulting in a much quicker and more efficient package update. This provides a reduction in the network bandwidth required when updating applications and provides faster update time. In the past, applications streamed for offline use required a re-download of the entire application profile whenever the profile was updated.

With XenApp 5 differential updates for offline applications are now much more efficient. This is because the local profile in the "deploy" folder on the client is used to create an updated version of the profile. The only files downloaded are the deltas from the profile on the application hub. These files are combined with the old profile and an updated profile is created on the client.

Finally, it is important to note that Application Isolation Environment is no longer included with XenApp 5. Application Streaming will provide the only isolation solution going forward.



What's Missing?!?

There are a number of features and components that have been removed from XenApp 5. On Windows Server 2008 there are a number of items that have been removed but still remain on the Windows Server 2003 version. These components include Application Isolation Environments which is no longer available as Application Streaming is now the best practice. The ICA Tool bar has also been removed and will require the administrator to navigate to Start → Programs Menu to view the shortcuts. Installation Manager Packager has also been removed for XenApp 5 on Windows Server 2008 due to customer use decline. The focus has now shifted to only supporting pushing pre-packaged applications, hot fixes, and scripts to the servers. This functionality has been the primary use for Installation Manager in the past and the focus will be on continuing to support only these features. The previous Installation Manager and

packager will still be included with XenApp 5 on Windows Server 2003. Conference Manager support has been removed in XenApp 5 on Windows Server 2008. Lastly, Windows Mobile PDA Sync is not supported due to platform issues.

For both Windows Server 2008 and Windows Server 2003 Application Streaming will no longer leverage the Citrix Streaming Client Package, which combined the Streaming client 1.1 and Program Neighborhood Agent 10.x. The Access Management Console no longer provides Health Monitoring dashboard alerts. The EdgeSight console will be the primary use for detailed alerting and leveraged for operational needs. Additionally, Web Interface will no longer support centralized site configurations on both platforms.

Conclusion

There are a number of new and updated features provided by both Windows Server 2008 and Citrix XenApp 5. It is critical to understand the impact of the changes in order to modify best practices and implementation techniques. Citrix XenApp 5 leverages updated Windows Server 2008 features to provide end users with a greater user experience, while optimizing the granularity of management provided to administrators.

Profiles, policies, Group Policy Objects, and updated Terminal Services features will become increasingly popular topics and it is critical to understand the impact of these changes as they relate to Citrix environments. This document provided an overview and introduction to both the updated Windows and Citrix components in order to enable further research and discussion. It is recommended to leverage the information and resources provided within this whitepaper to gain a greater understanding of Windows Server 2008 in order to successfully deploy Citrix XenApp 5.

Resources

For further information on the topics discussed throughout this whitepaper please refer to the resources listed below:

<http://learn.iis.net/page.aspx/101/introduction-to-iis7-architecture/http://learn.iis.net/page.aspx/101/introduction-to-iis7-architecture/>

<http://learn.iis.net/page.aspx/157/how-to-use-configuration-delegation-in-iis-7/>

<http://technet2.microsoft.com/windowsserver2008/en/library/4b40220c-ae1e-494e-902a-1b41057661fa1033.mspx?mfr=true>

<http://technet2.microsoft.com/windowsserver2008/en/library/4b40220c-ae1e-494e-902a-1b41057661fa1033.mspx?mfr=true>

<http://technet2.microsoft.com/windowsserver2008/en/library/84c67554-887b-4a20-8aaf-3d4b8f01251b1033.mspx?mfr=true>

<http://www.microsoft.com/windowsserver2008/en/us/server-management.aspx>

<http://technet2.microsoft.com/windowsserver2008/en/library/3b4568bc-9d3c-4477-807d-2ea149ff06491033.mspx?mfr=true>

<http://technet2.microsoft.com/windowsserver/en/technologies/featured/gp/preferencesfaq.mspx>

<http://blogs.technet.com/askds/archive/2008/06/17/user-profile-policies-in-windows-server-2008-and-windows-vista.aspx>

<http://msdn.microsoft.com/en-us/library/ms723891.aspx>

<http://technet2.microsoft.com/windowsserver2008/en/library/0b0bf633-5732-4b39-80d3-a2a4330acb141033.mspx?mfr=true>

<http://technet2.microsoft.com/windowsserver2008/en/library/e36186b2-b745-4dc7-945a-c3b83dcadb401033.mspx?mfr=true>

<http://technet2.microsoft.com/windowsserver2008/en/library/57995ee7-e204-45a4-bcee-5d1f4a51a09f1033.mspx?mfr=true>

<http://blogs.msdn.com/ts/archive/2007/04/26/introducing-terminal-services-easy-print-part-1.aspx>

<http://learn.iis.net/page.aspx/114/getting-started-with-appcmdexe/>

<http://msdn.microsoft.com/en-us/netframework/aa663328.aspx?PHPSESSID=b71095e8822903c8cb9db2e870f037e7>

<http://support.microsoft.com/?kbid=947025>

<http://learn.iis.net/page.aspx/284/using-managed-apis-in-iis7/>

<http://www.microsoft.com/windowsserver2008/en/us/licensing-terminal.aspx>

Notice

The information in this publication is subject to change without notice.

THIS PUBLICATION IS PROVIDED "AS IS" WITHOUT WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. CITRIX SYSTEMS, INC. ("CITRIX"), SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR DIRECT, INCIDENTAL, CONSEQUENTIAL OR ANY OTHER DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS PUBLICATION, EVEN IF CITRIX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE.

This publication contains information protected by copyright. Except for internal distribution, no part of this publication may be photocopied or reproduced in any form without prior written consent from Citrix.

The exclusive warranty for Citrix products, if any, is stated in the product documentation accompanying such products. Citrix does not warrant products other than its own.

Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Copyright © 2008 Citrix Systems, Inc., 851 West Cypress Creek Road, Ft. Lauderdale, Florida 33309-2009 U.S.A. All rights reserved.

Version History			
Author	Version	Change Log	Date
Erin Henry	Version 0.1	Content Created	July 7, 2008
Daniel Pinzas	Version 0.2	Review	August 3, 2008
Erin Henry	Version 0.3	Updated	August 5, 2008
Nick Rintalan	Version 0.4	Preliminary Review	August 6, 2008
Erin Henry	Version 0.5	Updated	August 7, 2008
Nick Rintalan	Version 0.6	Updated	August 10, 2008
Erin Henry	Version 0.7	Updated	August 11, 2008
Jo Harder	Version 0.8	Updated	August 20, 2008
Erin Henry	Version 0.9	Updated	August 25, 2008
Daniel Feller	Version 0.91	Review	September 2, 2008
Erin Henry	Version 0.92	Updated	September 4, 2008
Nick Rintalan	Version 1.0	Final Document	September 10, 2008



851 West Cypress Creek Road Fort Lauderdale, FL 33309 954-267-3000 <http://www.citrix.com>

Copyright © 2008 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, Citrix ICA, Citrix MetaFrame, and other Citrix product names are trademarks of Citrix Systems, Inc. All other product names, company names, marks, logos, and symbols are trademarks of their respective owners.