Consulting Solutions

Best Practices for Citrix XenDesktop with Provisioning Server

Overview

Citrix XenDesktop offers a next-generation, user-centric desktop virtualization solution that provides a complete system for desktop delivery. For information technology (IT) organizations, XenDesktop greatly simplifies the desktop lifecycle management process and drives down the cost of desktop ownership by separating the delivery of the desktop operating system from applications and user settings. Citrix XenDesktop, in concert with Provisioning Server for Desktops' virtual desktop provisioning capabilities, provides a powerful solution that simplifies the delivery of desktops to end users.

When designing a Citrix XenDesktop solution, it is important to take into account how XenDesktop with Provisioning Server will interact with an organization's existing critical infrastructure and services. These components include: directory services, network and security architecture, server hardware types, storage infrastructure, virtualization strategies and desktop operating system types.

This whitepaper discusses considerations when designing and implementing Citrix XenDesktop with Provisioning Server in an enterprise environment. It is important to note that this whitepaper is not a step-by-step guide to deploying XenDesktop architectures, but rather it looks to identify best practices for providing the best performing, most stable, and scalable implementation of XenDesktop with Provisioning Server.

Target Audience

This document has been developed for information technology (IT) infrastructure specialists who are responsible for planning and designing a Citrix XenDesktop infrastructure for desktop virtualization. These specialists include consultants, system architects, and others who are concerned with design decisions related to virtualization, specifically the virtualization of desktop systems.

CITRIX®

Table of Contents

Citrix XenDesktop Overview

Citrix XenDesktop provides a complete virtual desktop delivery solution by integrating several components with advanced configuration tools that simplify the creation and real-time management of the virtual desktop infrastructure.

The core components of XenDesktop discussed in this paper are:

- **Desktop Delivery Controller (DDC).** Installed as an infrastructure component on servers, the controller authenticates users, manages the assembly of users' virtual desktop environments, and brokers connections between users and their virtual desktops.
- **Virtual Desktop Agent (VDA).** Installed on each virtual desktop, the agent communicates with the DDC and enables a direct ICA (Independent Computing Architecture) connection between the virtual desktop and the users' endpoint device.
- **Desktop Receiver.** Installed on users' endpoint devices, the Desktop Receiver enables direct ICA connections from endpoint devices to virtual desktops. The XenApp plug-in can also be used in place of the Desktop Receiver, but the new features within the ICA toolbar would not be available.

Citrix Provisioning Server Overview

Provisioning Server's infrastructure is based on software-streaming technology. Using Provisioning Server, administrators prepare a device (Master Target Device) to be imaged by installing an operating system and any required software on that device. A virtual disk (vDisk) image is then created from the Master Target Device's hard drive and saved to the network (on Provisioning Server or back-end storage device). Once the vDisk is available from the network, a target device no longer needs its local hard drive to operate, as it boots directly from the network. The Provisioning Server streams the contents of the vDisk to the target device on demand, in real time. The target device behaves as if it is running from its local drive. Unlike thin-client technology, processing takes place on the target device.

The components of Citrix Provisioning Server discussed in this paper are:

- **Provisioning Server (PVS).** A Provisioning Server is any server that has the Stream Service installed. It is used to stream software from vDisks as needed, to target devices. In some implementations, vDisks reside directly on the Provisioning Server. In larger implementations, Provisioning Servers obtain the vDisk from a network storage device. Provisioning Servers also retrieve and provide configuration information to and from the Provisioning Server database. Provisioning Server architecture includes options to ensure high availability and load-balancing of connections between target devices and their vDisks.
- **vDisk Images.** vDisks are disk image files on a Provisioning Server or on a shared storage device. vDisks are configured to be in either Private Image mode, where changes made by the user are kept on the image, or Standard Image mode (read-only), where changes made by the end user are discarded upon shutdown.
- **Target Devices**. A device, such as a desktop computer or server, that boots and gets its operating system and software from a vDisk on the network, is considered a target device.
- **Write Cache Files**. When using a standard image mode the vDisk is set to read-only mode. Each target device then builds a cache that stores any writes that the operating system needs to perform such as application streaming, routine application processing tasks or system paging. Several scenarios and options for storing the write cache files will be discussed later in this document.
- **Network Storage.** vDisks are generally stored on network storage devices (SAN, NAS, Windows File Servers, etc.). Leveraging network storage devices allows for redundancy and high availability of the vDisk images.

Best Practices

This section contains the best practices for a XenDesktop and Provisioning Server deployment. These best practices are divided into the following areas:

- **Networking**
- **Storage**
- **XenDesktop Desktop Delivery Controller**
- **Provisioning Server for Desktops**
- **Virtual Desktop Images/Target Devices**
- **Scalability**

Caution! This document contains recommendations that require using the Registry Editor. Using the Registry Editor incorrectly can cause serious problems that may require reinstalling the operating system. Citrix cannot guarantee that problems resulting from the incorrect use of the Registry Editor can be solved. Use the Registry Editor at your own risk. Always back up the registry before editing any values.

Networking

Domain Name System. A key infrastructure component used when registering target devices with the DDC is the existing Domain Name System (DNS) environment. When target VM begin the registration process, the DDC will perform a DNS query and try to communicate with the target device using the Fully Qualified Domain Name (FQDN) of the registering machine. The target devices, which typically obtain their IP addresses via DHCP, need to be able to dynamically update their Host (A) records in DNS. It is also recommended that the DDCs also be able to update their own DNS records should additional DDCs be brought online, changed moved or added to the environment.

While standard file-based storage such as a hosts file will provide proper DNS resolution in Proof of Concept (POC) environments, Citrix recommends implementing Active Directory integrated DNS in enterprise deployments. If the DNS zone is integrated with Active Directory, organizations have the benefit of *secure* dynamic updates, as well as the ability to use Access Control List (ACL) editing features to control which machines can update the DNS system. This allows an organization to specify the computers that are allowed to update their DNS records (XenDesktop VMs/Provisioning Server target devices and DDCs).

Dynamic updates are a key feature of DNS, which allow domain computers to register their name and IP address with the DNS server automatically when they come online or change IP addresses through the DHCP server. This form of update eliminates the need for manual entries of names and IP addresses into the DNS database. The security aspect comes into play when an automatic update from a client to the DNS database could possibly open an attack vector for a malicious entry. Therefore, secure dynamic updates will verify that the computer that is requesting the update to the DNS server also has an entry in the Active Directory database. This means that only computers that have joined the Active Directory domain can dynamically update the DNS database.

Note: When using Windows based standard zone storage, the DNS Server service is configured to disallow dynamic updates on its zones by default; therefore, dynamic updates must be explicitly allowed for the zone. It is also important to note that reverse lookup zones are used when the virtual desktops are added to a desktop group within the Access Management Console. The IP address of the virtual desktop is mapped to the FQDN using the reverse lookup DNS zone.

Provisioning Server. To provide optimal throughput, Citrix recommends using multiple Network Interface Cards (NIC)s in Provisioning Server machines. One NIC should be configured for PXE communication on the network. A teamed pair should be configured for streaming the vDisks via the PVS Stream Service. A second teamed pair may be required for network access to enterprise storage systems or file shares. When possible, streaming vDisk data should be isolated from normal production network traffic such as Internet browsing, printing, file sharing, etc. using dedicated networks or VLAN's.

Storage

Storage requirements for Provisioning Server implementations greatly depend upon the number of vDisk images to be created and maintained, the type of vDisks that will be used (Standard Image Mode vs. Private Image Mode), the operating system installed in the image, what components or applications are installed on each image, plans for potential future application installations, and storage location of the write cache file for each provisioned workstation.

Types of vDisks. When using Standard Mode vDisks, many target devices boot from the same vDisk. However, space is only required to store one copy of each vDisk. A second copy should be created and be used for updates to the vDisk. When using Private Mode vDisks, each target device must have its own copy of the vDisk, requiring additional storage space for each target device. When using a Private Mode disk as the base image for a Standard Image deployment, do not add the vDisk to Active Directory if it will be used as the Standard Image. When a previously installed Private Mode image boots the vDisk in Standard Image Mode, the Domain Controller will already contain the unique machine information (SID) in Active Directory and an error message will occur. Instead, let PVS manage the Active Directory machine accounts.

vDisk Size Estimates. The size of the vDisk depends greatly on the operating system and number of applications to be installed on the vDisk. The vDisk grows larger as more applications are installed in the vDisk. Citrix recommends creating vDisks larger than are initially necessary to leave room for additional application installs or patches if necessary. Based on past experience, Citrix recommends organizations use the following general sizing estimates when determining the storage requirements. The estimates were made based on an operating system with only a few applications installed such as Microsoft Office. These estimates may not accurately reflect the required sizes of vDisks in every environment; thus, each organization should determine the space requirements for their vDisk images individually.

Operating System	Estimated vDisk Size
Windows XP	15GB
Windows Vista	25GB

To estimate the size of the vDisk required, follow these guidelines:

- **Target Device Space.** Identify the amount of space currently in use by the master target device. This can be accomplished by examining the properties of the disk. A typical installation of Windows XP with no local applications added could consume between 1 and 3GB of space on a disk drive. A typical installation of Windows Vista consumes approximately 6GB of space on a disk drive.
- **Application Sizing.** As applications are installed, the amount of space in use increases. If the plan is to add applications into the vDisk image after capture, then the vDisk should be sized to allow for the additional space requirements. Citrix recommends adding an additional 25% of space to the initial footprint of the image, allowing room for any additional application installations.

To minimize the storage space required, Citrix recommends the following:

- **Minimize Applications on Each vDisk.** Minimizing the number of installed applications helps reduce the footprint of each vDisk. In addition to reducing the storage capacity, keeping the vDisk as generic as possible allows an organization to leverage the same vDisk for many workloads. Delivering personalized application sets to the desktop via published applications hosted on XenApp servers or application streaming via Citrix Streaming Server further minimizes the applications on each vDisk.
- **Minimize the Number of vDisks.** Each vDisk requires physical disk space equal to the size of the vDisk. Consequently, reducing the number of vDisks reduces the storage space requirements. Citrix recommends keeping at least one backup copy of each vDisk to be used to make updates when required. An organization should consider allocating 2x the amount of disk space required for each vDisk that it plans to maintain.

Write Cache File. Each target machine contains a volatile write cache file that is deleted upon each reboot cycle. The size of the cache file for each VM depends on several factors, including the types of applications used, user workloads, and reboot frequency. A general estimate of the file cache size for a provisioned workstation running only text-based

applications such as Microsoft Word and Outlook and is rebooted daily is about 300-500MB. If workstations are rebooted less often, or graphic intensive applications (such as Microsoft PowerPoint, Visual Studio, or CAD/CAM type applications) are used, cache file sizes can grow much larger. As each environment's application workload can vary, Citrix recommends that each organization perform a detailed analysis to determine the expected cache file size required for their environment.

Cache File Location. There are several options for storing the cache file for provisioned desktops. Common locations include; target based physical local storage, client disk (virtual machine vDisks), and enterprise storage based (SAN/NAS) disk environments. Each of these options has benefits and limitations; thus, it is important to evaluate the specific requirements of the organization before determining the cache file location. The benefits and limitations of each option are described below.

- **Physical Local Storage.** If physical desktops or blade servers are being used, Citrix recommends leveraging the target device's RAM or hard disk to store the cache files. When locating the cache file on a local physical storage device, consider the following:
    - Since accessing RAM is considerably faster than reading and writing data to a hard disk, placing the cache file in RAM will yield better performance when compared to a hard disk. Placing the cache file in RAM will often provide the best performance for a single application environment.
    - When RAM is used for the cache file, the cache file is limited in size by the amount of physical RAM available in the target machine. If the cache file is expected to grow larger than the amount of available physical RAM in the device, the device's hard drive should be used instead. Should the RAM based cache file become filled, undesired result/errors may occur since there is not enough space to write the cached data.
    - There is generally more space available for the cache file on the hard drive on a target machine than in memory. If the target devices are diskless and do not contain hard drives or enough memory for the required size of the cache file, then the cache files can be stored on a shared enterprise storage device and proxied via the Provisioning Server for Desktops.
- **Client Disk (Virtual Machine vDisks).** When leveraging a virtual machine infrastructure to host the desktops, an organization can also leverage enterprise storage associated with each VM or the VM's allocated RAM for the write cache location. For example, each VM may be created with an additional 1 GB disk to store the cache file on each target device's vDisk. When using virtual machine vDisk based cache locations, consider the following:
    - Storing the cache file as part of the VM requires additional RAM or disk space equal to that of the cache file to be allocated in addition to the size required for each unique VM. If the target cache file is hosted on the PVS server, high availability of the cache file will not be present. To enable a cache file that is highly available, use the PVS Proxy Mode model below.
    - This model generally provides good performance, when the PVS server contains a fiber channel or dedicated Host Bus Adapter (HBA) card connected to a SAN. Should fiber channel cards not be available, Gigabit NICs may be used to connect to CIFS based network shares. Citrix recommends that the PVS server contain multiple NICs; one teamed pair dedicated for streaming and one teamed pair dedicated for network traffic to the enterprise storage network (iSCSI, CIFS, NAS, etc.) and one NIC configured for PXE traffic.
    - This option provides added resiliency in the event of a failure since only a single VM will be affected if the local disk associated with the VM runs out of space.
    - Each VM must be able to see the additional disk that is associated with the VM for this option.
    - Utilizing a client disk for the cache file will lower the overall network traffic when compared to the enterprise server based option. In addition, a local file is required for full system dump tracing.
- **Enterprise Server Based (PVS Proxy Mode).** The cache file can also be stored on a shared enterprise storage solution (SAN/NAS) accessed via the Provisioning Server. In this case, the Provisioning Server would act as a proxy between the virtual machine and the storage solution. To create High Availability (HA) architectures, a minimum of two PVS servers are required.

  - This solution allows for the configuration of PVS in High Availability (HA) mode. If an HA mode failure occurs within the PVS infrastructure, any remaining servers can begin servicing the failed requests without interruption to the target device. If the vDisk file is also placed on the shared storage location, XenMotion features can also be enabled
  - Proxying the cache traffic through the PVS in this manner impacts the network I/O and reduces the scalability of each PVS server. This will impact the number of active clients that can be supported by a single PVS architecture. .
  - Proper sizing of the storage location is critical in this scenario. If the shared storage location fills up and no disk space remains for cache, all virtual machines may experience performance issues.
  - The Write Cache needs to be located on shared storage to benefit from XenServer's HA feature (XenMotion between XenServers)
- For enterprise deployments using HA configurations, Citrix does not recommend storing the cache file locally on the PVS server. If the cache file is stored locally on the PVS, each PVS becomes a single point of failure, and HA configurations are not available.

Each organization will need to determine their individual Service Level Agreements (SLA) to determine whether an HA configuration is required for their unique desktop use cases. When a small SLA window is required, one may choose to use both XenMotion and PVS in HA mode to provide a complete fault tolerant solution. This would require the vDisk and cache file to be located on shared storage at the expense of lowering the overall scalability of the PVS server. If a large SLA window is available, then Citrix recommends using locally stored cache files when possible for optimal performance.

SAN vs. NAS. In HA scenarios, a shared SAN is required and a LUN must be accessible from multiple hosts (PVS Servers or targets). Read-only LUN's can be utilized for storing vDisks in standard mode. Private Image Mode vDisks require read and write access. When HA architectures are required, using a NAS head to allow multiple machines access to the LUN or traditional NAS architectures with RAID disks should be used. Storage optimizations such as placing vDisks on LUNs that span separate disk spindles rather than contiguous blocks will further improve throughput.

Determining Expected Cache File Size. Citrix recommends using a pilot/POC environment to determine the expected size of the cache files. To determine the file size within the pilot/POC environment, configure the write cache to be located on the Provisioning Server and have several different types of end-users (graphical application users, text-based task workers, etc.) work on their provisioned desktops. After several full days of heavy use, the administrators can look at the size of each of the cache files on the Provisioning Server. This will give a rough estimate of how large the cache files can grow in the production environment. In the production environment, gracefully rebooting the desktops everyday will help reduce the size of the cache file since the files are purged on each reboot cycle.

Reboot Provisioned Workstations Frequently. The write cache file for provisioned workstations can grow quite large, and will continue to grow until the workstation is rebooted. Depending upon the applications used and the frequency of reboots, the write cache can grow as large enough to impact an organization's storage solution. The cache file is cleared out upon workstation reboot. Subsequently, the more frequently the workstation is rebooted, the less of an impact the cache files will have. Citrix recommends rebooting workstations daily if possible. If daily reboots are not possible, Citrix recommends rebooting workstations at least once per week to reduce the storage impact of cache files. **Note:** A graceful shutdown or restart is required to clear the cache file. Powering down the machine without a graceful shutdown will not clear out the cache file. XenDesktop allows configuration of logoff behavior so this process can be automated as well.

XenDesktop Desktop Delivery Controller

Uninstall Web Interface and IIS. XenDesktop automatically installs IIS and Web Interface as part of the Desktop Delivery Controller (DDC) installation. Most organizations have existing web server infrastructure that can be leveraged for Web Interface for XenDesktop. Not installing these components will help increase the performance and scalability of the DDCs in a production environment. Organizations can take two approaches if they have an existing IIS infrastructure:

- During the install, use the **Setup.exe -nosites** parameter, which will not install Web Interface.
- If the install has already occurred, an organization should consider uninstalling this component or disabling the associated services.

Separate the Farm Master and Controller. By default, in a XenDesktop farm the initial Desktop Delivery Controller (DDC) installed is the farm master with specific duties as the data collector, performing desktop resolution operations during desktop launches, and managing the hosting infrastructure. This single server has the role of Data Collector and Controller. When there are multiple servers in a farm, it is often desirable to separate the functions of Controller and Data Collector by delegating these functions to different servers. These other duties can be better performed by other Desktop Delivery Controller machines in the farm, leaving the farm master machine to concentrate on its own role requirements. To separate the roles, the actions to be taken fall into two parts: ensure that a particular machine is chosen to be the farm master and ensure that unnecessary duties are not performed by that machine.

Each Desktop Delivery Controller machine in the farm can potentially become the farm master in an election process. This election process can be influenced by settings on the various server machines, and one (or more) machines can be configured so that they are the preferred farm master, while other machines are configured to only take on the farm master role if the preferred machines are unavailable. This preference indication is achieved by use of registry entries on the various server machines. Each machine can be configured to have one of three settings:

- Master – servers with this setting are preferentially chosen as the farm master.
- Backup – servers with this setting are preferentially chosen as the farm master when the master server is unavailable.
- Member – servers with this setting are normally not the farm master, but can assume the farm master role when none of the master or backup servers is available.

The desktop launch request is the sole function of the DDC master and handles the logic of launching connections. When configuring Web Interface to point to a DDC member, Web Interface will forward the launch request to the DDC master. If the DDC master server becomes unavailable, an election occurs and another member server will assume the DDC master role. Once the Desktop Delivery Controller has established the connection to the virtual desktop, ICA establishes a direct connection between the virtual desktop and the endpoint (client machine). The Delivery Controller is no longer in the line of traffic. As such, the demand on it is diminished and it can scale sufficiently.

When using multiple DDCs, Citrix recommends dedicating a machine as the master controller and all other servers should be configured as member servers. Web Interface servers should be configured to point to member servers to minimize the CPU load placed on the controller server during periods of heavy logon rates. To configure a server these settings, edit the following registry keys and restart the server:

HKLM\Software\Citrix\IMA\RUNTIME\UseRegistrySetting

DWORD=UseRegistrySetting

Value=1

HKLM\Software\Citrix\IMA\RUNTIME\MasterRanking

DWORD=Value

Value= 1 indicates ‘Master’

2 indicates ‘Backup’

3 indicates ‘Member’

For more information, please see Citrix Knowledge Base Article CTX117477.

Throttle Commands to Virtual Machine Hosting Infrastructure. When sending a high number of power on/off commands to the virtual machine hosting infrastructure (VMware Virtual Center, XenCenter, Hyper-V), the hosting infrastructure could become overwhelmed and unresponsive for a short period of time while all of the requests are queued and processed. By default, the communication between the pool management service on the DDC and the hosting infrastructure is throttled to 10% of the total pool. For example, if there are 500 VMs in the desktop group, only 50 VM power operation requests will be sent at a time. When pools grow even larger, (over 1000 desktops), this could result in approximately 100+ power on/off requests being sent concurrently to the hosting infrastructure.

The hosting infrastructure may become overloaded during the following scenarios:

- When the idle pool count significantly increases for a concurrent peak time
- There is a small duration between logon and logoff events. For example, a company employs a three shift working day. A group of users will logon in the morning and logout when their shift is finished. The next shift of users will begin to logon at the same time that the previous group logs off resulting in a very small window where large numbers of users log on and logoff (5-15 minutes).

It may be necessary to throttle the number of power requests sent to the virtual machine infrastructure at a single time. To modify the number of concurrent requests, edit the following configuration on each DDC. This example throttles the number to 20 concurrent commands.

- Open C:\Program Files\Citrix\VmManagement\CdsPoolMgr.exe.config
- Add the following line in **red**:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
    <appSettings>
        <add key="LogToCdf" value ="1"/>
        <add key="LogFileName" value ="C:\cdslogs\VMManager.log"/>
        <add key="LogDebug" value="1"/>
        <add key=”MaximumTransitionRate” value=”20”/>
    </appSettings>
</configuration>
```

- Save the file and restart the DDC. The DDC or the Pool Management Service must be restarted for the new value in the .NET configuration file to be read by the DDC.

The value (”MaximumTransitionRate” value=”20”) included in this example should only be considered as a point of reference when configuring the concurrent command values. This value will vary based on each environment’s unique hardware platform and use case. Citrix recommends that each organization properly test the configuration before determining the optimal balance between the number of concurrent commands that can be serviced and the performance/responsiveness of the hosting infrastructure when sending power commands from the DDC.

Provisioning Server

Disable Checksum Offloading on Network Adapter. Checksum offload parameters, which are not compatible with the Provisioning Server network stack, may cause slow performance when enabled on the physical network adapter.

Symptoms of slow performance can include:

- Excessive amount of retries
- Slow ICA performance within virtual machines
- Freezing or locking while using Windows XP Service Pack 2 virtual machines
- vDisk retries during normal operation when a Windows XP Service Pack 2 virtual machine is already online and in waiting mode
- Slow hosted application launch when using Presentation Server 4.5 and publishing applications in XenDesktop

Citrix recommends disabling Checksum Offload on the network adapter of both the Provisioning Server as well as the target devices. On many NICs, checksum offloading can be disabled by opening the Network Interface Card (NIC) properties and selecting the advanced configuration tab.

Some NICs do not offer this setting in the properties page (i.e. target devices running on virtual machines). To change the Checksum Offload parameter value, create and edit the following registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

DWORD = DisableTaskOffload

Value = 1

Note: The registry value described above may not exist by default on some systems and may need to be created for this value to be applied properly. For more information, please see Microsoft Knowledge Base Article 904946.

Disable TCP Large Send Offload. The TCP Large Send Offload option allows the TCP layer to build a TCP message up to 64 KB long and send it in one call via IP and the Ethernet device driver. The adapter then re-segments the message into multiple TCP frames for wire transmission. The TCP packets sent on the wire are either 1500 byte frames for a Maximum Transmission Unit (MTU) of 1500 or up to 9000 byte frames for a MTU of 9000 (jumbo frames). Re-segmenting and queuing packets to send in large frames can cause latency and timeouts to the Provisioning Server and therefore this should be disabled on all Provisioning Servers and target devices.

To disable the Large Send Offload values, open the Network Interface Card (NIC) properties and select the advanced configuration tab.

Some NICs do not offer this setting in the properties page (i.e. target devices running on virtual machines). To disable the Large Send Offload parameter value, create and edit the following registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BNNS\Parameters\

DWORD = EnableOffload

Value “0”

For more information, please see Citrix Knowledge Base Article CTX117374.

Auto Negotiation. Auto Negotiation can cause long booting times and PXE timeouts, especially when booting multiple target devices. Citrix recommends hard-coding all Provisioning Server ports (server and client) on the NIC and on the switch port to disable the auto negotiation feature configure the connection speed.

Disable Spanning Tree or Enable PortFast. With Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol, the ports are placed into a "blocked" state while the switch transmits Bridged Protocol Data Units (BPDU) and listens to ensure that the BPDUs are not in a loopback configuration. The amount of time it takes for this process to converge depends on the size of the switched network that might allow the Preboot Execution Environment (PXE) to time out causing the VM to enter a wait state or reboot until the condition is cleared and the PXE process can resume. To resolve this issue, disable STP on edge ports connected to clients or enable PortFast or Fast Link depending on the managed switch brand. Refer to the table below:

Switch Manufacturer	Fast Link Option Name
Cisco	PortFast or STP Fast Link
Dell	Spanning Tree FastLink
Foundry	Fast Port
3COM	Fast Start

Maximize the System Cache. All traffic that occurs between the vDisk and the target device passes through the PVS machine regardless of where the vDisk resides. Using Windows Server 2003 file caching features can improve vDisk deployment efficiency. The operating system caches the file reads and write data operations at the block level. When a single target device is booted from a shared vDisk, subsequent clients will not require disk read I/O to perform similar operations. The OS caching mechanism will only cache the blocks that were accessed, not the entire vDisk file. The file read data will stay in the cache until it is flushed to make space for newer data. To increase the speed at which the vDisk is streamed, the Provisioning Server should be optimized for file caching such that the file cache is contained in server RAM rather than increasing disk I/O by reading the files from the server’s hard disk. The system cache can be maximized on the Provisioning Server by following these steps:

- Right-click **My Computer** and select the **Advanced** tab.

- Click the **Settings** button in the **Performance** section of the Advanced tab.
- Click the **Advanced** tab of the Performance Options window.
- Ensure **System Cache** is selected under the Memory Usage section.

Alternatively, the system cache value can be configured through the registry by using the following key:

KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\MemoryManagement

DWORD=LargeSystemCache

Value=1

For more information, please see Microsoft Knowledge Base Article 837331.

Team NICs for Increased Throughput. Network I/O on the Provisioning Server can be a limiting factor in the scalability of the server. Teaming two NICs for throughput provides the server with a maximum of 2Gb of network I/O, increasing the network performance helping to alleviate this potential bottleneck. In addition, teaming the NICs eliminates a single point of failure if only one NIC is enabled.

Isolate Streaming Traffic. When possible, vDisk streaming traffic should be isolated from normal production network traffic such as Internet browsing, printing, file sharing, etc. In this scenario it is best to use multiple NICs; one for PXE and teamed NICs for streaming the vDisks to target machines.

Make a Copy of Each vDisk. In order to modify images created with Provisioning Server, it is recommended that an organization saves a copy of each vDisk and places it in Private Image mode. By keeping a copy of the vDisk in Private Mode, the administrator can modify the vDisk to include any required updates without affecting the production image. Once all required modifications have been made, the administrator can use the Provisioning Server Console to configure the target devices to boot from the newly created vDisk image. Backing up each vDisk is also recommended for disaster recovery and business continuity purposes.

Virtual Desktop Images/Target Devices

A clean virtual disk image is critical to the successful delivery of the vDisk to the target device when using Provisioning Server. When developing this vDisk image, it is important to ensure that the master target disk does not contain any unwanted information, such as unused applications or user profiles. The order in which the master target disk is prepared is also important to ensure the image is clean and NICs are bonded correctly.

Recommended Desktop Operating System Modifications

Increase Service Timeouts. When rebooting a large number of virtual machines within a short period of time (5-15 minutes, such as during a shift change), it may be necessary to increase the Service Control Manager timeout value to allow enough time for the critical XenDektop services to start and register successfully with the available DDCs. Stress testing conducted by Citrix Consulting has shown that increasing this value to 3 minutes on all virtual target devices may be necessary to allow ample time for the critical services to start. This timeout can be increased by modifying the vDisk image with the following registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control

DWORD=ServicesPipeTimeout

Decimal Value=180000 (3 Minutes)

For more information, please see http://support.microsoft.com/kb/839803.

Disable the Windows XP Tour Prompt for New Users. By default, Windows XP notifies all new users that an XP tour can be taken. While this is a nice feature for new Windows XP users, it typically is annoying for existing users. To suppress the Windows XP tour prompt for all new users, follow these steps edit the following registry key:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Applets\Tour

DWORD=RunCount

Value=0

For more information, please see http://support.microsoft.com/kb/311489.

Disable Last Access Time Stamp. Whenever Windows XP reads a file, it stamps the file with the date and time that it was accessed. This feature impacts performance and is generally not required for normal use, especially when using Standard Image mode. Putting a timestamp on the file that has just been read requires that a write is made to disk, so every time a read is executed, a corresponding write is also executed. With Provisioning Server, these writes go to the vDisk cache file, which subsequently increases the network traffic if the cache file is stored on the PVS server. Use the u *fsutil.exe* to disable the last access timestamp behavior. Execute the following command detailed below and reboot the workstation:

"FSUTIL behavior set disablelastaccess 1"

Turn off System Restore. System Restore is the feature that allows a computer system to be rolled back, or restored, to a point before certain events took place, for example, prior to specific software or hardware installations. When using a Standard Image mode (read-only) vDisk, system restore points should be disabled. This can be accomplished by using the PVS Optimizer tool. In addition, the system restore feature can de disabled by completing the following steps:

- Right-click **My Computer** and then click **Properties.**
- On the Performance tab, click **File System**.
- On the **Troubleshooting** tab, select **Disable System Restore.**
- Restart the computer.

For more information, please see http://support.microsoft.com/kb/264887.

Disable Windows Indexing Service. Windows Indexing Service adds overhead to the PVS vDisk by reading the files from the vDisk for indexing. The Windows Indexing Service can be disabled using one of the following three methods:

- Use the **PVS Optimizer tool** and leave the "Disable Indexing Services" setting enabled.
- To turn off indexing for a specific drive:
  - Right click and Select **Properties.**
  - Under the **General** tab, disable the "Allow the Indexing Service to index this disk for fast file searching" setting.
- To disable the indexing service at the service level:
  - Click Start, **Run**, type *services.msc***.**
  - Change the "Indexing Service" **Startup type** to "Manual" or "Disable" and **Apply.**
  - Verify that the Indexing Service has stopped**.**

Zero out Deleted Files. SDelete is a secure file delete utility that can be used to free and cleanup unused space on the image. In short, it zeroes out any files that have been freed up by the operating system and helps the image run faster. For more information about how it works or where to download it, visit http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx.

Usage: sdelete [-p passes] [-s] [-q] <file or directory>
sdelete [-p passes] [-z|-c] [drive letter]

-c	Zero free space (good for virtual disk optimization)
-p passes	Specifies number of overwrite passes
-s	Recurse subdirectories
-q	Don't print errors (quiet)
-z	Cleanse free space.

Citrix recommends cleaning and zeroing the free space by using the following command: **sdelete –c –z**.

XenDesktop User Profiles

Special consideration should be taken when designing profiles for a XenDesktop environment as users' existing profile settings will apply to both XenDesktop VM's and traditional desktops. When a user has an existing roaming profile and associated Group Policy Objects (GPOs) configured for their traditional desktop environment, these settings will be applied to the XenDesktop VM upon logon. These pre-existing settings may not contain the proper optimizations that benefit the XenDesktop environment and may cause undesired performance degradation and inconsistent results within both platforms. Before migrating users to the XenDesktop platform, Citrix recommends carefully designing a profile strategy that meets the needs of each unique environment. When possible, Citrix recommends using roaming profiles with folder redirection and leveraging Windows 2008 preferences with Group Policy client-side extensions (CSEs) for Windows XP and Windows Vista or using the Citrix User Profile Manager. Additional information about using CSEs can found in the following Microsoft Knowledgebase Article: http://support.microsoft.com/kb/943729

Settings for the Default User Profile

Users that do not have a pre-existing .dat files in their profile or do not have a profile strategy can benefit from settings configured within the default user profile of the XenDesktop VM. This section details settings that will improve the user experience but are contained at the user profile level. To modify the default user profile, Citrix recommends creating a generic user with the appropriate settings and replacing the default user profile contents with the generic user profile settings. The steps to accomplish this are found at the end of this section.

Remove Unnecessary Visual Effects. Visual effects such as menu animations and shadow effects can slow down the response time of the desktop. Citrix recommends disabling any unnecessary visual effects. This can be done by selecting the "Adjust for best performance" setting in the advanced properties of My Computer. To keep the Windows XP Visual Style, scroll to the bottom and check the last box titled "Use visual styles on windows and buttons."

Disable the Windows XP Tour Prompt. If the Windows XP Tour Prompt was not turned off before logging in as the base user for the default profile, this can be manually disabled on a per-user basis. To disable the Windows XP Tour Prompt change the following registry key:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Applets\Tour

DWORD=RunCount

Value=0

For more information, please see http://support.microsoft.com/kb/311489.

Force Offscreen Composition for Internet Explorer. Turning this setting off removes any of the flickering that may display when using Internet Explorer through XenDesktop, by telling Internet Explorer to render the page completely prior to displaying it. This is especially helpful on Internet Explorer 7.

- Open Internet Explorer.
- Select **Tools** > **Internet Options > Advanced** from the menu.
- Enable "Force offscreen compositing even under Terminal Services." and restart Internet Explorer.

For more information, please see http://support.microsoft.com/kb/271246/en-us.

Remove the Menu Show Delay. The Start menu has a built-in delay of 400 milliseconds. To increase the menu response time, configure the following registry key:follow these steps to set the delay to 100:

HKEY_CURRENT_USER\Control Panel\Desktop

REG_SZ=MenuShowDelay

Value=100

Disable the Desktop Cleanup Wizard. It is unnecessary to run the desktop cleanup wizard when using Standard Image mode since the desktop is refreshed at each reboot. To stop the wizard from automatically running every 60 days disable the "Run Desktop Cleanup Wizard every 60 days" setting within the **Display Properties > Desktop > Customize > Desktop Items** dialog box. For more information please see http://support.microsoft.com/kb/320154.

Disable Automatic Searching of Network Printers and Shares. Automatic search periodically polls your network to check for new shared resources and adds relevant icons into My Network Places if anything is found. To prevent Windows XP from regularly searching your network disable the "Automatically Search for Network Folders and Printers" setting within **Control Panel > Folder Options;** if using the Control Panel Category View, Folder Options appears under Appearance and Themes.

Turn off Automatic Updates. When running in Standard Image mode, using automatic updates will cause the operating system to download the same updates each time the image is booted. Citrix recommends turning off this feature to avoid downloading the same updates since the vDisk image configured as read-only. Three options can be used to disable the service:

- Use the **PVS Optimizer tool** and leave the "Disable automatic update service" box checked.
- In the Services Control Panel, change the **Startup Type** of the **Automatic Updates** service to "Disabled."
- Run GPEDIT.MSC and navigate to: **Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Windows Update**. Set the "Configure Automatic Updates" to "Disabled."

Copy the Base User Profile the Default User Profile. After completing all the User Profile Settings using a generic user, the profile must be copied to become the default user profile. This can be done using the process below.

Note: Before copying the profile, be sure to remove any user or machine specific data for the ICA Client, Password Manager, and EdgeSight. Delete the ICAClient and Password Manager data in the base user's Application Data\Citrix folder and the associated HKey Current User (HKCU) registry keys. Do not start the EdgeSight agent before the image is taken.

- Login as an administrator (Local Administrator is recommended) not as the base user used to make the changes for the profile because you cannot copy a profile that is in use.
- Right-click on **My Computer > Properties > Advanced > Settings**
- In the **User Profiles** section, select the base user profile that was used to make the changes above and click **Copy To** and browse **to C:\Documents and Settings\Default User.**
- **Sa**ve the path location and change the owner and rights assignment to: Everyone and "Permitted to use" and confirm overwriting the profile.

Preparing a vDisk Image

Citrix recommends the following checklist to prepare the master vDisk image. **Note:** Except where specifically stated, when preparing the master target image, all actions should be performed while logged into the master target device as a local (non-domain account) administrator. Also, note that the order is slightly different for some tasks when creating a Windows XP and Vista image. Follow the steps described below for the appropriate operating system where specified.

1. **Prepare the Hardware.**
    - Update the BIOS of the master target device, if needed.
    - Open Device Manager and resolve any unknown drivers.
    - Ensure that Windows has no issues with the disk and network devices and resolve or delete any devices that appear to be unknown.
    - Join the machine to the Active Directory domain and identify any network configurations that are incorrect (i.e., TCP settings, DHCP, DNS, WINS, or Time sources).
    - Verify disk is clean and functioning properly. Run CHKDSK /F to verify the integrity of the disk drive.
2. **Remove Unused Features and Files.**
    - Remove any files in the temporary directories that are not needed. Use the operating system's disk cleanup utility or third-party products that remove unwanted files and settings.
    - Verify the contents of the C:\TEMP and C:\Windows\Temp directory structure to identify files that can be removed prior to image capture.

- Local user profiles will be captured in the master image if they are on the disk during the image capture. Remove any user profiles that are not needed.
- Remove any applications that are not needed by using the Control Panel.
- Step through the C:\Program Files\ directory structure to identify any applications that should be removed.
- Remove any base Windows applications or features to conserve space in the vDisk.
- Remove any data files and personal settings that are not needed.
- Remove any policy objects that are not needed.
- Review the local settings and policies to identify policies that can be removed prior to image capture.

3. **Desktop Operating System Optimizations.**

- Configure the system page file. The page file size should be determined based on the amount of memory allocated to each machine and observed page file use in the current environment. This is generally between 300 - 500MB. The initial and maximum file size should be the same.
- Review the Windows Registry settings to identify settings that may no longer be needed. Use the Registry Editor (Regedit) or other third-party tools to cleanup registry settings prior to capturing the image.

For Windows XP workstations:

- Install the paravirtualization tools (XenServer Tools or VMware Tools.) and reboot the target workstation.
- Install any local running software to be included in the image. Citrix recommends minimizing the number of applications installed on the base image. Keeping the number of installed applications to a minimum will reduce complexity with the image and reduce the overall number of images that need to be maintained.
- Log in to the desktop using a *domain account* with local administrative privileges and install and reboot the workstation.

For Windows Vista workstations:

- Log in to the desktop using a *domain account* with local administrative privileges and install the Citrix Virtual Desktop Agent (VDA) and reboot the workstation.
- Install paravirtualization tools (XenServer Tools, VMware Tools, etc.) and reboot the workstation.
    - **Note:** The paravirtualization tools should be installed *after* the XDA is installed to avoid errors when the XDA executes its startup routine. This applies only when using Windows Vista as the target machine's operating system.
- Install any local running software to be included in the image. Citrix recommends minimizing the number of applications installed on the base image. Keeping the number of installed applications to a minimum will reduce complexity with the image and reduce the overall number of images that need to be maintained.

4. **Test Connectivity:**

- Test connection to VDA using Web Interface and verify that the desktop can be accessed.
- Disabling the Windows Firewall may be necessary for communication with the XenDesktop Desktop Delivery Controller. If the firewall cannot be disabled due to security requirements, ensure exceptions are made so the DDCs can contact the VMs.
- Verify connectivity through proxy connections. If a proxy server is used in the environment, the proxy server may need to be configured to allow traffic from the client machine to the VDA.

5. **Install ICA Clients.**

- When XenApp hosted applications will be accessed from the desktop, install the Citrix XenApp Plugin (Program Neighborhood Agent) and configure it to communicate with the XenApp Services (Program Neighborhood Agent Services) site.
- If Application Streaming will be used, install the Citrix XenApp Plugin for Streamed Apps (Citrix Streaming Client) then reboot the workstation. Configure all streamed applications to pre-cache and run. This will improve network performance by not having to stream all of the applications to each provisioned workstation upon first use.

6. **Optimize PVS.**
   - Disable TCP checksum and Large Send Offload as described here.
   - Retest VDA connection.
   - Verify the Domain\XenDesktop group (Controllers) has "Access this computer from the network" privileges. This is configured on the workstation through Local Security Policy > User Rights Assignment.
7. **Prepare the Target Machine.**
   - Defragment the disk drive.
   - Install PVS target device software, then reboot the workstation.
   - Flush the DNS cache using **ipconfig /flushdns** on the workstation.
   - Optimize then build image using PVS Optimizer.
   - Shutdown the workstation (do not reboot), then export the vDisk as a backup.
   - Switch the PVS image to Standard Image Mode. If this machine will be used as a template (i.e. one has not been created for the XenDesktop Setup Wizard) make sure to delete the local storage on the Template before running the Setup Tool.
   - Convert the machine to a Template in XenServer, VMware, or Hyper-V.
   - Add a 1MB local disk to the template if using VMware or plan to use XenMotion with XenServer 4.1 or earlier. When using VMware, the SCSI driver required for Provisioning Server is not installed if there is no local disk attached. XenServer 4.1 XenMotion requires a file on the storage repository, which is not the case for a diskless VM (even though memory is transferred between XenServer hosts). Use XenServer 5.0 for XenMotion for diskless VMs.
   - If your target devices both belong to an Active Directory domain and are sharing a vDisk, complete the following additional steps:
     - Enable Password Management:
       - In the Provisioning Server console, right click the vDisk you want to share among the domain member target devices. Select **Properties > Options** and select the **Enable Active Directory Machine Account Password Management** check box.
       - Optionally, enable automatic password re-negotiation and set the maximum machine account password age on the Service Preferences/Active Directory tab.

Scalability

When considering XenDesktop scalability, it is important to examine the scalability of the constituent parts of XenDesktop rather than just viewing XenDesktop scalability in a generalized fashion. Scalability is observed for the Desktop Delivery Controller, for Provisioning Server, and for the virtual machine infrastructure. This section will discuss the factors that impact scalability for the Desktop Delivery Controller and Provisioning Server.

Desktop Delivery Controller

The heaviest toll on the Desktop Delivery Controller occurs during peak connection times such as when users simultaneously logon in the morning or during shift changes. Most of the logon load on the server is caused by IMA, the Desktop Delivery Controller and the Pool management services. Upon connection completion, the ICA protocol connects the endpoint and the virtual desktop – the Delivery Controller is engaged only to receive heartbeat notifications from the virtual desktops. These desktop notifications are far less taxing than the activity at times of peak logon.

When considering large deployments, it is important to note that there are several services that only run on the Delivery Controller Zone Master and that all connection requests from end users go through the Zone Master. As a result, the master cannot be scaled out by adding servers. It can only be scaled up by upgrading to a more robust server (more processing power). However, a XenDesktop farm can be scaled out for *failover* by adding new Delivery Controllers, which handle the XDA keep-alives and registration with the virtual desktops. The Zone Master can become a bottleneck when desktop groups grow large. As such, Citrix recommends limiting the number of desktops per group to 3000.

The most common factor that limits scalability of a single Delivery Controller is processing power. In order to maximize the number of simultaneous connections a single DDC can handle, Citrix recommends that organizations dedicate servers with the maximum processing power (dual socket or higher with quad core processors) to serve as the Zone Masters in a XenDesktop environment.

Provisioning Server

The number of target devices that can be supported per Provisioning Server depends upon the size of the vDisk, storage solution for the vDisk placement, location of the write cache file, and workflow of end users. The most common bottlenecks that affect scalability of Provisioning Server are network I/O of the Provisioning Server, disk I/O of the vDisk storage location, and cache file location.

The Provisioning Server Streaming Service manages traffic (i.e. a proxy). If the vDisk is located on a share, then the Provisioning Server will retrieve the image and distribute it to the target devices (virtual desktops). Therefore as the number of target devices increases per Provisioning Server, the Provisioning Server's NIC will heavily utilized and become saturated at peak intervals. Teaming multiple NICs can help increase the number of target devices that can be supported before the NIC becomes a bottleneck.

Disk I/O of the storage solution can become a bottleneck as well, as the Provisioning Server (or multiple Provisioning Servers) will be reading from the disk to obtain the vDisk and cache files. The faster the network storage solution (SAN, NAS, Windows DFS, etc.) can output the data from the hard disk, the better the performance of the Provisioning Server will be, and thus increase the number of devices that a single Provisioning Server can support without reducing performance. Additionally, scalability and throughput can be impacted by the location of the vDisks and cache files within the backend storage system. When storing files on the same storage system, Citrix recommends placing the vDisks and write cache files on separate dedicated LUNs to decrease (and distribute) disk spindle loads and increase vDisk and cache file access speeds.

As discussed earlier in this paper, locating the write-cache on the Provisioning Server reduces the scalability of each Provisioning Server by increasing the processor, network I/O, and disk I/O requirements of the Provisioning Server.

Citrix recommends each organization perform scalability testing specific to their environment based on the existing infrastructure and use cases to determine the number of target devices that can be supported by a single Provisioning Server. Additional Provisioning Servers can be added to the architecture to distribute the load, as well as to provide redundancy and high availability (HA). Citrix recommends implementing additional Provisioning Servers as part of an organization's HA and disaster recovery plans.

Recommended Scalability by Architecture Component

The following chart contains recommended maximum values for each component within the XenDesktop architecture. These values are based on a reference architecture[1] using XenDesktop with XenApp published applications.

Component	Recommended Maximums
Desktops Per XenDesktop Farm	3000
Tested Logon rate[2]	1500 connections over a five minute period
vDisks per XenServer	30
XenServers[3] in a Pool	Up to 28
Provisioning Server for Desktops (PVS)	500 VM's per machine when using local cache files[4].

[1]The following represents the critical items to note about the testing architecture:

- **XenServer**: 8 cores, 64GB RAM server running XenServer 5
- **Desktop Delivery Controller**: 2 cores, 8GB RAM running XenDesktop 2.1
- **Provisioning Server**: 2 cores, 8GB RAM running Provisioning Server 5
- **Desktop Operating System Configuration**
    - **Windows XP**: Service Pack 3, 1 processor, 512MB RAM
    - **Windows Vista**: Service Pack 1, 1 processor, 1GB RAM

[2] A 1500 connection limit has been verified over a five minute duration, 50 simultaneous connections occurred per logon instance
[3]XenServer 5.0 was used to determine this value.
[4] Local cache files were used when determining this value. Using other cache file locations will decrease the scalability of Provisioning Server

Resources

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

Getting Started with Citrix XenDesktop 2.1 (CTX118041)

Desktop Delivery Controller 2.0 Administrator's Guide (CTX116843)

Citrix Provisioning Server Administrator's Guide (CTX117916)

Citrix Provisioning Server 5.0 Installation and Configuration Guide (CTX117917)

Best Practices for Configuring Provisioning Server on a Network (CTX 117374)

Provisioning Server 5.0 Technotes

XenDesktop 2.0 Technotes

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.

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.

Version History			
Author	Version	Change Log	Date
Jay Leblang	0.1	Original Content	10/2/2008
Nick Rintalan	0.2	Technical Review	10/8/2008
Jay Leblang	0.3	Additional Content provided by Paul Wilson	10/24/2008
Nick Rintalan	0.4	Additional Content and Revisions	10/28/2008
Douglas Demskis	0.5	Technical Content, Technical QA and Revisions	11/25/2008
Chris Straight	0.6	Technical Review	11/26/2008
Douglas Demskis	0.7	Final Revisions and Technical Review	11/26/2008

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