CITRIX®

XenClient Advanced Configuration Guide

XenClient Advanced Configuration Guide

This document provides a number of topics about the XenClient implementation, including SCCM integration, Synchronizer-related requirements, and overview information for some XenClient functionality, including PvD.

Synchronizer Sizing Guidelines

This section details specific guidelines that can be used to size a Synchronizer installation. It is based on some fundamental assumptions concerning acceptable timeframes for deploying VMs:

- Performing an initial deployment of VMs to all users could take considerable time, possibly within a several day time period for large deployments. This particular operation should only be done one time; once all clients have received their VMs, it is only necessary to send updates to those systems. In the future, initial deployments will only be done to small numbers of systems at any given time (as new users are added, as existing users are migrated to new hardware, or to fix hardware failures). Architecting this one-time operation quickly is not recommended because the systems will be oversized for normal operation.
- It must be possible to keep up with the backup policies; so if the policy is to backup all clients every day, it must be possible to transfer the associated data to the Synchronizer servers within the 24 hour period.

In addition, there are some assumptions in this topic regarding the likely size of VMs and backups:

- A VM will likely be initially around 20 GB uncompressed (around eight to 10 GB compressed) with an absolute maximum size of 50 GB uncompressed (20 to 25 GB compressed). For example, a full Windows 7 installation together with Office 2007 professional is approximately 18 GB. If weekly updates with a maximum of four intermediate versions are created, each of which is 1 GB, and retaining the last two published versions at most, the estimate of maximum required disk space per VM (including the overhead for storing both uncompressed and compressed) is:

(50 + 8*1) * 1.5 = ~90 GB

- The size of a user backup could be the full configured size of the disk plus the configured maximum number of incremental snapshots. So, if a user disk is configured to be a maximum of 30 GB with daily backups maintained for seven days, and if we assume any given user can modify 1 GB of data per day, then the maximum on disk size at the Synchronizer server can be estimated as:

(30 + (6*1)) * 0.5 = ~20 GB

With these guidelines in place, it is possible to determine how many Synchronizer servers should be deployed to handle the end client load on the system as follows:

- A central Synchronizer server:
  - Should have three Xenon-class cores for each 1 GB LAN connection plus one to two cores for running Synchronizer server processing.
  - Should have at least 8 GB memory for the Windows instance running the central server image, plus additional memory for creating, updating, and publishing VMs,

which should be greater than the largest expected memory size of any individual VM.

- Requires sufficient storage to hold all VMs together with backups for any users directly registered to the server.

- A remote Synchronizer server:
  - Should have three Xenon-class cores for each 1 GB LAN connection.
  - Should have least 8 GB memory
  - Requires sufficient storage to hold all VMs together with backups for all users that will be registered to the server.

Synchronizer Sizing

There are several factors involved in sizing Synchronizer installations, including:

- The number of distinct virtual machines (VMs)
- The number of client systems and the expected number of VMs each client will run
- The networking topology, including WAN/LAN speeds
- The type of VMs being utilized and the chosen model for user backups

Each of these factors will impact Synchronizer installation in several ways, including:

- Processor loading, each server will require a certain amount of processing power to support the registered client population.
- Memory usage; in general, the more memory a server has, the better it will perform, but there are minimum requirements on memory size to support the number of XenClient Engines (clients).
- Storage; the storage needs of a Synchronizer deployment can vary greatly depending on the deployment model chosen, number of VMs required, number of registered computers, and other factors.
- Network; part of Synchronizer installation's design is calculating bandwidth usage requirements and any limitations that should be applied to the XenClient Enterprise traffic, designing the server structure appropriately and configuring bandwidth management policies.

Synchronizer Processor Factors

The processing requirements for Synchronizer are:

- Creating and updating VMs; the VMs are run under Hyper-V when they are being installed and updated. Follow the Microsoft guidelines for Hyper-V VMs when you're calculating the processor requirements for these operations, and take into account the largest number of VMs that will concurrently updated and published.

- Publishing VMs; the publishing process causes the VM to run under Hyper-V and also includes processing that is done in the Synchronizer OS instance itself. Because the product serializes publishing, it is only necessary to account for one VM being published at a time. The publish process consumes one processor core for the duration of the operation (typically 20-40 minutes per VM).
- Deploying VMs; the server operates as a secure web server to deploy images and take backups; this processing consumes about three Xeon-class processor cores to saturate a single 1 GB/s link (which translates to around 800 MB/s actual throughput). Central Synchronizer servers provide this service for Synchronizer remote servers and for any XenClient Engines registered directly to the central Synchronizer server.
- Control functions; this component is responsible for managing the database and user interface for the XenClient Enterprise installation and runs only in the Synchronizer central server, although it is accessible via Synchronizer Console on the remote Synchronizer servers.

Memory Factors

The memory requirements for Synchronizer server include:

- Memory required to create and update VMs (Synchronizer central server only) you should follow the Microsoft guidelines for Hyper-V VMs when calculating the memory requirements for these operations, and you should take into account the largest number of VMs that will be concurrently updated and published.
- Publishing VMs (Synchronizer central server only); the VM is run on the server system during publishing, so enough memory must be free to accommodate the largest VM during this process, which is serialized so only one VM will be published at a time.
- Deploying VMs; the normal Windows file system cache is heavily utilized when deploying VMs, so the more memory that is available, the better the system will run.

Note: The minimum memory size for Synchronizer is 6 GB, but increasing it to 16 GB or more results in improved performance; also, consider memory requirements when rolling up backups (which apply to both central and remote Synchronizer servers).

Synchronizer Network Factors

The network topology has a strong impact on the design of the Synchronizer installation. The following are the most important factors to consider:

- Slow-speed (WAN) connections to remote sites. The system will perform at its best if Synchronizer servers are installed at the end of slow-speed links, as this will mean that VMs are only downloaded once no matter how many clients there are at the remote site *and* no backups will be sent over the WAN connection. This results in greatly reduced utilization of the WAN link.

Note: If it is not feasible to install a Synchronizer remote server at every remote location, it still beneficial to install a server remotely to service a number of sites, as this will reduce the load on the outgoing WAN connection from the central data center.

- Multiple high-speed segments. If the network has multiple separate high-speed LAN segments, then it makes sense to install a Synchronizer remote server on each segment to maximize the number of clients that can be serviced concurrently and minimize the impact on the backbone network. For example, if there is a 10 GB backbone in the central data center and a series of 1 GB LAN segments distributed throughout the organization with small data centers on each segment connected to the backbone, then a good implementation strategy would be to install remote servers in each satellite data center, all connected to the 10 GB backbone and have the central server in the main data center. This results in data being distributed to the remote servers quickly and, from there, delivered in parallel to all clients on the various slow speed networks.

Windows 7 Best Practices

There are two categorical ways to improve performance on any deployed operating system. One category includes performance improvements of *installed* components, while the other includes preventing the installation and execution of *unnecessary* components.

Improving Performance on Installed Components

To improve the performance on installed components:

1. Install Windows 7 with the latest service pack.

> **Note:** Citrix recommends that you install Windows with the latest service pack instead of installing a previously released service pack and then upgrading. For example, install Windows SP2 instead of installing SP1 and then upgrading to SP2.

2. Modify the installer partition table in Windows 7; delete the larger, second partition and increase the size of the first partition to fill the disk.

3. After installing Windows, run the Windows update and enable the Microsoft update.

4. Run all updates; reboot and repeat until all updates are installed.

> **Note:** Do not install **Office Live Add-in** and disable the auto-run option for Windows Update; disable warning messages related to Windows Update.

5. Turn off System Restore:

a. Access the Control Panel > System and Security > System > **System Protection** screen.

b. Click **Configure**.

c. Select the **Turn off system restore** check box, and click **OK**.

> **Note:** In some cases, disabling Remote Assistance and Remote Desktop is often recommended; Citrix recommends that these be enabled; they allow an administrator to remotely debug an OS. While these abilities hinder performance, they provide a number of benefits.

6. Disable **SuperFetch**:

a. Start > services.msc.

b. Double-click **SuperFetch**.

c. Click the **Stop** button to halt the service.

d. Change the start-up type to **Disabled**.

7. Delete the **EnableSuperfetch** value. To delete the EnableSuperfetch value:

a. Start > regedit.

b. HKEY_LOCAL_MACHINE\SYSTEM\CurrentSetControl\Session Manager\Memory Management\PrefetchParameters.

c. Double-click on EnableSuperfetch.

d. Change the **value data** field to 0.

8. After disabling **SuperFetch** and rebooting, delete the contents of c:\Windows \prefetch.

9. Run disk cleanup; **cleanmgr** (specify **All Users** and keep defaults).

10. Set recycle bin to 100 MB.

11. Turn off scheduled disk defragmenter; Start disk defragmenter, configure schedule, and clear the recycle bin.

Preventing Unnecessary Component Installation

Many installed components, such as Sun's Java or Apple's Quick-Time, install their own updater engines. These components are not desired when running XenClient Enterprise.

Note: The website appdeploy.com has information on how to customize application installations, including the removal of unneeded components; each application has its own page of appdeploy.

Many of these installed applications have custom settings that seek to turn off the automatic-update settings of the applications; otherwise, each VM will check for updates and then try to install them, only to discard the updates at the end of the session. You will update applications in the version on Synchronizer, and then publish that version to distribute the updates to shared VMs.

1. Import the Office 2007 ISO file into the software library. Attach the ISO to the running VM. Install Office 2007, and click customize, **run-all-from-my-computer**. You can customize it further for your environment.

2. Install Firefox, and modify the **%program files%\Mozilla Firefox\defaults\pref \firefox.js** as follows (the default for these lines is true):

pref("app.update.enabled", false);

pref("extensions.update.enabled", false);

pref("browse.search.update", false);

3. Download Adobe Reader 9 from ftp://ftp.adobe.com/pub/adobe/reader/win/9.x/9.2/enu/.

4. Obtain Adobe Reader 9.x by filling out an Adobe Reader Redistribution Agreement at http://www.adobe.com/products/reader/distribution.html.

5. Download the **AdbeRdr9x_en_US.exe** from the link in the confirmation email and save the file to your desktop.

6. Extract the Adobe components using the command **AdbeRdr9x_en_US.exe-nos_ne**.

7. Download the Adobe Customization Wizard from: http://www.adobe.com/support/downloads/detail.jsp?ftpID=3993.

8. Run the Customization Wizard. Under Installation Options, clear **Enable Optimization**, and select **Suppress reboot**. Under on acrobat.com, select **disalbe all updates**. Save the package.

9. Run **setup.exe**.

10. Install Adobe AIR 1.5 from http://get.adobe.com/air. Use the default values offered.

11. Install both versions (IE and Firefox) of Flash Player. Disable Flash Player's automatic update.

12. Create or open the C:\WINDOWS\System32\Macromed\Flash\mms.cfg file in a text editor, and add the following line: **AutoUpdateDisable=1**.

13. Save the **mms.cfg** file with UTF-8 encoding.

Note: For details, see http://helpx.adobe.com/flash-player/kb/administration-configure-auto-update-notification.html.

14. Install the latest Sun Java JRE. Create the following registry keys:

- [HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Java Update\Policy]
- "EnableJavaUpdate"=dword:0 "NotifyDownload"=dword:0 "NotifyInstall=dword:0
- "UpdateSchedule"=dword:0 "Frequency"=dword:0

Note: For details, see http://www.itninja.com/software/oracle/java-2/6-1070?from=appdeploy.com.

15. Install VPN software. For the full Cisco VPN client, create an organization profile; for the SSL VPN, download the default profile with the client.

16. If iTunes is required for your environment, download iTunes from Apple.

17. After installation, disable iTunes updates in the Apple Software Update program.

18. Disable QuickTime updates through its control panel.

19. In the Registry, set HKEY_LOCAL_MACHINE\Software\Apple Computer, Inc.\iTunes\Parental Controls\Default\AdminFlags to **0x000000101**.

20. Install Skype for business using a kit from www.skype.com/business.

21. Disable the version check by setting the registry value:

- HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone\DisableVersionCheck to 1

22. Install your AV/Spyware Engine. Prior to publishing, verify that your AV services are listed in the "turn OFF before publishing and ON after NxPrep list" to prevent extremely long publish cycles.

Note: For Sophos, do not turn on regular scans. Leave the default integrated scanning of all files opened intact. Run a full app and virus definition update.

App-V Client and XenClient Enterprise Interoperation

The Microsoft App-V client is deployed as part of the central image in either VM *shared* or *dedicated* image mode. Once the virtual image is deployed with the App-V client, the virtual Windows instance is ready to utilize App-V virtual applications. All the delivery methods previously mentioned work well with XenClient Enterprise. XenClient redirects the locations for the App-V application cache, and virtualized application user preferences, to a location that is outside of the snap-back functionality and controlled through the default VM OS policy. This means the virtual application and its settings are retained after reboots regardless if the VM image is in *shared* or *dedicated* mode. The virtualized application in a VM will operate the same way as it would if loaded on a physical Windows instance.

Using SCCM with XenClient Enterprise

In order to understand the proper interactions between the two systems, it is important to understand how the client and its guest Windows instance are recognized. Because XenClient Enterprise is based on the XEN hypervisor, Active Directory and the SCCM console don't recognize it directly. Therefore, the management of the core engine (client) must be performed through Synchronizer, while the management of what is placed in the Windows guest instance can be controlled through SCCM.

The following steps will allow you to install a XenClient Windows OS instance from SCCM OSD:

1. Follow the SCCM standard procedure to create an OS image for SCCM delivery as outlined in Microsoft TechNet http://technet.microsoft.com/en-us/library/bb693478.aspx.

2. Once the image is ready, create the Task Sequence media following these steps (http://technet.microsoft.com/en-us/library/bb632725.aspx):

a. Make sure to select **Bootable media**.

b. Select CD/DVD set.

c. Select a location to save the ISO file in the Media File line.

d. Click **Next**.

e. Enable **Unknown Computer Support**.

f. Finish filling in the record according to your company's profile.

g. Click **Next**.

h. Select the **x64 Boot Image** as the Media File.

i. Select the **Distribution Point** to get the Boot Image files.

3. Click **Next** twice, and the Boot image will be created in the saved location.

4. Once created, copy the Boot Image ISO to the FileImport folder in Synchronizer.

5. In Synchronizer, import the ISO by opening the Software Library:

a. Click **Import**.

b. Fill out the name of the ISO.

c. Select the Boot Image ISO from the drop-down list.

d. Click **Finish**.

6. Create the VM; be sure to select the **SCCM OSD Boot Image ISO** as the installation media.

7. Once the system boots, it will go through the standard SCCM OSD installation process as the physical machines using the corporate image.

8. Once the process is complete, the image is ready for you to add the SCCM client and any additional finishing touches.

Synchronizer Remote Server Functionality

Leveraging the Synchronizer remote office server capability allows you to manage all remote servers from your central server. You can gain many key things by using the remote servers, such as intelligent caching of downloaded images, efficient use of bandwidth between remote offices, local storage and maintenance of backups, and fast recovery for remote clients. The remote server can be used in WAN or LAN setups. The remote server will require network access to the SQL database and the central server. The SQL port 1433 needs to be open for access to the database, and port 443 needs to be open for access to the central server. All downloads from the central server are encrypted and compressed. A user requests an image or Engine update from the remote server to which they are registered; then the remote server checks with the central server to download the update. Once the update is downloaded to the remote server, it then caches it for the next user.