Module 3

Rehosting Windchill

Module Overview

In this module, we review the process of moving Windchill solutions from one host system to another host system.

Objectives

After completing this module, you will be able to:

- Identify rehosting scenarios.
- Identify the specific activities necessary for each rehosting scenario.
- Rehost a Windchill solution.

Exercise 1: Rehosting Windchill

Objectives

After successfully completing this exercise, you will be able to:

- Rename a monolithic Windchill system.
- Set the New System Name for Rehosting.
- Preserve Vaulting and Replication.
- Copy Windchill Installation and Third-party Products.
- Clone LDAP Contents from Source LDAP to Target LDAP.
- Update Host Names in Apache.
- Export Database from Source System and Import into Target System.
- Copy Vault Content to Target System.
- Setup for reconfiguring the Database.
- Update Database on Target System.
- Configure Target Database Connection.
- Disable Remote File Server Sites.
- Restart Target Windchill System.
- Update Vaulting Configuration.
- Verify Site URL and Adjust File Server URLs.

Scenario

In this exercise, you act as a technical consultant who has been given the task of renaming an existing Windchill host system, ptc-training.ptc.com to a new hostname. You will use rehosting techniques to appropriately rename the server in all the appropriate locations and reassign other names and paths that are dependent upon the host name.

Feel free to work in groups, but ensure that your assigned image has been correctly rehosted at the end of the exercise so that it can be used to complete follow-on exercises.

Prerequisites

- Obtain a group number and a master or node assignment from your instructor. These variables are used for your windchill host name, shown as <windchill_host_name> throughout this exercise. The naming convention to be used for your <windchill_host_name> is (master|node)<group_number>-training. For example: master1–training.
- To aid in your understanding and assist with working through the exercise, you may download a copy of the Rehost Guide.

Task 1: Setting the New System Name for Rehosting

1. If running locally, perform the following steps to create a bridged network adapter for cluster creation later on:
   - From the Vmware Workstation menu, select the **VM > Settings...** option.
   - From the Virtual Machine Settings dialog box, Click the **Add…** button at the bottom of the Hardware tab.
   - From the Add Hardware Wizard, select the **Network Adapter Hardware** option.
   - Click the **Next > button**.
   - In the Network Adapter Type page of the Add Hardware Wizard, select the **Bridged network connection** option.
   - Select the **Replicate physical network connection state** check box.
   - Ensure that the **Connect at power on** check box is selected, and click the **Finish** button.
   - It will take a few minutes to install a new Network Adapter.
   - When it completes, double-click the Command Prompt shortcut on the VM desktop.
   - At the prompt, type: **ipconfig** and press ENTER.
   - Scroll up in the Administrator: Command Prompt window and locate the newly assigned IP address. It should indicate that it is an "Ethernet adapter for Local Area Connection 2". Note this address for update in the host file (as discussed below).
   - Click the Windows Explorer shortcut from the VM desktop.
   - Browse to *C:\Windows\System32\drivers\etc* and right-click the hosts file.
   - Select the **Send To > NoteTab Light** context menu option.
   - Add a new line that begins with the new IP address collected from the Command Prompt window.
   - Type the <IPv4 address>, tab and the new full hostname, tab and the new short hostname. You can get the hostname from your instructor. (Image)
     - Example: **192.168.1.116** | **master1–training.ptc.com** | **master1–training.ptc.com**
   - Click the **Save** icon.
   - Click the **Windows Exit** button to exit NoteTab Light.

Task 2: Preserving Vaulting and Replication

1. Ensure that replication and revaulting jobs are not running. If jobs are running, either wait for them to complete or cancel the jobs.
   - Double-click the **Internet Explorer** icon on the desktop of the VM.
   - Click the **Windchill Server** button on the Favorites Bar.
   - When prompted, log in as Administrator (wcadmin/wcadmin).
   - Browse to the Site Utilities page.
   - Click the **File Server Administration** link from the System Administration section of the Site Utilities page.
   - Click the **Revaulting Scheduler**.
   - The External Storage Scheduling window appears displaying any Revaulting jobs that are currently scheduled. This VM is not normally set up to perform any revaulting. If necessary, select any existing schedules and click the **Delete** button.
   - Click the **Close** button to close the External Storage Scheduling window.
   - From the Site Utilities page, click the **Replication Scheduler** link.
   - The Content Replication Schedules table displays any Replication jobs that are currently scheduled. This VM is not normally set up to perform any replication. If necessary, select the check box next to any existing schedules and click the **Delete** icon at the top of the table.
   - Leaving the Windchill browser window open, click the **Windchill Shortcuts** shortcut from the desktop of the VM.
   - Browse to the *D:\Shortcuts\Windchill PDS* folder and double-click the **JConsole** shortcut to open the Java Monitoring & Management Console window.
   - In the JConsole: New Connection dialog box, double-click the **wt.method.MethodServerMain** option from the Local Process section to open a JMX connection to the method server.
   - Select the **MBeans** tab.
   - Click the **Expand** icon to the left of the com.ptc node.
   - Click the **Expand** icon to the left of the Monitors node.
   - Click the **Expand** icon to the left of the CacheVaultSyncrhonizer node.
   - Select **Operations**.
   - Click the **sysForce Sync** button. (Image)
   - The Operation return value dialog box appears indicating that an immediate system sync has been scheduled. Click the **OK** button to close the dialog box. (Image)
   - Exit the Java Monitoring & Management Console window.
   - From the Windows Explorer window, browse to *D:\Shortcuts\Windchill PDS* and double-click the **Windchill Shell** shortcut.
   - From Windchill Shell Command Prompt window, type **sqlplus installpds/installpds** and press ENTER.
   - From the SQL command prompt, type **select count(*) from MasteredOnReplicaItem;** and press ENTER. (Image)
   - Exit the Windchill Shell Administrator window.
   - From the Windchill Administrator session browser window, select the **Queue Management** option in the System Administration section of the Site Utilities page.
   - Click the bottom part of the scroll bar to scroll down to the bottom of the Queue Management table.
   - Select the **wt.router.1.1** and **wt.router.3.1** check boxes.
   - Click the **Stop** button at the top of the Queue Management table.

Task 3: Copying Windchill Installation and Third-party Products

1. Because we already have a duplicate installation, the copy is not necessary. The two machines should be identical at this point.

Task 4: Cloning LDAP Contents from Source LDAP to Target LDAP

1. Export an ldif using **ptc > Windchill > WindchillDS > server > bat > control-panel.bat**.
2. Since we are not reinstalling or copying the installation, the WindchillDS installation and data are identical and do not need to be cloned, but a Rename is required.
   - Click the **Windchill Shortcuts** shortcut from the desktop of the VM.
   - Browse to the *D:\Shortcuts\Windchill PDS*folder and double-click the **Windchill Shell** shortcut.
   - At the prompt, type **cd bin\adminTools\rehost**and press ENTER.
   - At the prompt, type: **ant "-Dtarget-ldap=ldap://cn=manager:ldapadmin@<windchill_host_name>.ptc.com/" -Dtarget-domain=<windchill_host_name>.ptc.com** and press ENTER. (Image)
   - When prompted with **[input] About to make a copy of the source LDAP to the Target LDAP. You should only skip this step if you manually copied the source LDAP to the Target LDAP. Continue? (y, n, skip)**, type **skip** and press ENTER. (Image)
   - When prompted with [input] About to re-host the contents of the Target LDAP and local files from ptc-training.ptc.com to <windchill_host_name>.ptc.com. Continue? (y, n), type **y** and press ENTER. (Image)
   - The ant call should end with the following text: (Image)

   THE HOSTNAME MAY BE DIFFERENT FOR CLUSTER (ADVANCED DEPLOYMENT GUIDE).

3. If this rehost process fails, set the wt.rmi.server.hostname using xconfmanager and reimport the ldif.

Task 5: Updating Host Names in Apache

1. We can use the build.xml ant script in *D:\ptc\Windchill\Windchill\bin\adminTools\rehost* to complete these commands as well.
   - Click the **Windchill Shortcuts** shortcut from the desktop of the VM.
   - Browse to the *D:\Shortcuts\Windchill PDS* folder and double-click the **Windchill Shell** shortcut.
   - At the prompt, type **cd ..\Apache**and press ENTER.
   - At the prompt, type: **ant -DServerName=<windchill_host_name>.ptc.com -f config.xml reconfigure** and press ENTER.
   - At the prompt, type: **ant -DAJP_HOST=<windchill_host_name>.ptc.com -f config.xml configureAJPWorkers** and press ENTER.
2. Reconfigure the Apache LDAP Authentication
   - At the prompt, type **ant -f webAppConfig.xml addAuthProvider -DappName=Windchill -DproviderName=AdministrativeLdap -DldapUrl="ldap://<windchill_host_name>.ptc.com:389/ou=people,cn=AdministrativeLdap,cn=Windchill,o=ptc" -DbindDn="cn=Manager" -DbindPwd="ldapadmin"** and press ENTER.
   - At the prompt, type **ant -f webAppConfig.xml addAuthProvider -DappName=Windchill -DproviderName=EnterpriseLdap -DldapUrl="ldap://<windchill_host_name>.ptc.com:389/ou=people,cn=EnterpriseLdap,cn=Windchill,o=ptc" -DbindDn="cn=Manager" -DbindPwd="ldapadmin"** and press ENTER

Task 6: Exporting Database from Source System and Importing It into Target System

1. This is not used for this rehost. Appendix B of the Rehosting Guide.

Task 7: Copying Vault Content to Target System

1. This is detailed in the Rehost guide, but is not appropriate here. Pointing each system after Rehosting/renaming should occur during the cluster configuration.

Task 8: Important Setup for Reconfiguring the Database

1. Start Windchill All-in-One.
2. From a Windchill Shell prompt perform a windchill stop. (Windchill should fail due to the connection info from rehost, but to ensure that it is stopped, run the command.)

Task 9: Updating Database on Target System

1. You must update the Repository table on the target system so that it uses the target host name instead of the source host name. This update is divided into 2 tasks.
2. Updating Main Entries in the Repository Table to Use the Target Host Name
   - At a Windchill Shell command line prompt, log on to SQL*Plus as the database user (the same one that was imported from the source system) on the target system. (installpds/installpds)
   - Enter the following SQL command to update all entries in the Repository table with the source host name, changing it to the target host name and domain name:
     – **Update Repository set lastKnownDomain='<windchill_host_name>.ptc.com' where local=1;**
   - Commit and continue on in the next section
3. Updating the Repository Table for Rehosted Info*Engine Repositories
   - At a Windchill Shell command line prompt, log on to SQL*Plus as the database user (the same one that was imported from the source system) on the target system. (installpds/installpds)
   - The Ldap and EnterpriseLdap repository domain names do NOT need to be changed since the machine name is not used in the original definition of those two JNDI adapters.
   - Enter the following SQL command to update the Repository table entries for the ldap-pending JNDI adapter that contains the source domain name in the service name:
     – **Update Repository set lastKnownDomain='ldap-pending.<windchill_host_name>.ptc.com', guid='ldap-pending.<windchill_host_name>.ptc.com' where lastKnownDomain='ldap-pending.ptc-training.ptc.com';**
   - (The Windchill Rehosting Script does not change the domain portion of the pendingUsers entry in LDAP.) The step to update the RemoteObjectID is not necessary since it did not change. This is for pending users.
   - Commit and exit.
   - Repeat these steps for additional Info*Engine Repositories that have been rehosted. We don't have any additional configured repositories, so we can skip this.
     – Side check: In sqlplus we can run the following: **select lastknowndomain from repository;**
     – Side check: Log in to Windchill ahead of time and note the repository names that will be rehosted. This is from the **Site Administration > Info*Engine Administration** page. (wcadmin/wcadmin) and then (cn=Manager/ldapadmin).

4. Actually updating the database host name:
   - Open a Windows Explorer window.
   - Right-click the **listener.ora** file.
   - Select the **Send To > NoteTab Light** option.
   - In the second stanza, update the HOST value from ptc-training to <windchill_host_name> (Image: UpdatingDatabaseConfig-EditListenerOra)
   - Click the **Save** icon on the NoteTab Light toolbar.
   - Click the **Close** button to close NoteTab Light.
   - Right-click the **tnsnames.ora** file.
   - Select the **Send To > NoteTab Light**option.
   - In the second stanza, update the HOST value from ptc-training to <windchill_host_name>.
   - In the third stanza, update the HOST value from ptc-training.ptc.com to <windchill_host_name>.ptc.com (Image: UpdatingDatabaseConfig-EditTNSNamesOra)
   - Click the **Save** icon on the NoteTab Light toolbar.
   - Click the **Close** button to close NoteTab light.
   - Restart the database. You can use the Stop Windchill All-In-One and then the Start Windchill All-In-One shortcuts.

Task 10: Configuring Target Database Connection

1. Using xconfmanager, set the following properties in the db.properties file to the appropriate target database values:
   - wt.pom.jdbc.host = target database host name
   - wt.pom.jdbc.port = target database port
   - wt.pom.dbUser = target database user
   - wt.pom.dbPassword = target database password
   - wt.pom.jdbc.service = target database System Identifier (SID)
   - wt.pom.serviceName = target Oracle service name.
2. The only thing that needs changing is the wt.pom.jdbc.host (Note: wt.pom.serviceName does not appear to be set at all.)
   - At a Windchill Shell command line prompt, enter the following command:
     – **xconfmanager -s wt.pom.jdbc.host="<windchill_host_name>.ptc.com" -p**

Task 11: Disabling Remote File Server Sites

1. Nothing is necessary here.

Task 12: Restarting Target Windchill System

1. Restart Windchill using the Start Windchill All-in-One shortcut.
2. You may have to run the Stop Windchill All-in-One shortcut first.

Task 13: Updating Vaulting Configuration - Necessary step

1. Log into the target system as the site administrator (wcadmin/wcadmin) and browse to **Site > Utilities**
2. Click the File Server Administrator link.
3. The File Server Administrator page appears.
   Click **Vault Configuration**
4. Expand the tree in the left panel to display hosts. Both the source and target host will be defined. The new target host is automatically added during system start up. Select the target host and delete it.
5. Double-click the source host to open the Update Host window.
6. Enter the <windchill_host_name> and click OK.
7. If the source and target mount paths are different, you must update the mount paths. (We should not have to perform these steps on this image.)
   - Double-click the mount now displayed on the Mounts panel.
   - In the Update Mount window, enter the new target mount path and click OK.
8. To ensure that the mount status is in a valid state, click the mount to highlight it and select the **Mounts > Validate** option from the menu bar.
   If a mount is invalid, a message displays including that one or more mounts are not valid.
   Check the Mount Status column to locate mounts that are not valid.
9. Select the **File > Close** menu option to exit the Vault Configuration window.

Task 14: Verifying Site URL and Adjusting File Server URLs

1. Verify the URLs. Open a browser window.
2. In the address field, type: **http://<windchill_host_name>.ptc.com/Windchill/** and press ENTER.
3. When prompted, login as Administrator (wcadmin/wcadmin).
4. Verify that you can successfully log on to Windchill with the new hostname.

This completes the exercise.

Module 4

High Availability Windchill Architecture

Module Overview

In this module, we review the Windchill system architecture that supports clustering for high availability.

Objectives

After completing this module, you will be able to:

- Identify possible high-availability configurations.
- Create a basic Windchill cluster.

Exercise 1: Creating a Windchill Cluster

Objectives

After successfully completing this exercise, you will be able to:

- Update Host Names and Plan a Cluster Strategy
- Create a new cluster configuration prep on the master cache server
- Create Steps for Each Node
- Finalize the Cluster

Scenario

In this exercise, you act as a two-person team of technical consultants who have been given the task of creating a simple Windchill clusters without a load balancer. You will use some rehosting techniques to prepare two different Windchill application servers to point to the same database and WindchillDS server and you will configure each server to run the specified components of the overall cluster.

Some activities will require you to wait until your exercise partner is ready to continue.

Prerequisites

- You should already have been assigned either a master or node assignment and group number, shown as <master_host_name> or <node_host_name> throughout this exercise. The naming convention to be used for your is (master|node)<group_number>-training. For example: master1–training or node1–training. You will also configure IPv4 addresses to point to <cluster_host_name> and <data_host_name> using the same format for the host names that have been assigned..
- To aid in your understanding and assist with working through the exercise, you may download a copy of the Advanced Deployment Guide.

Initial Conditions

- Complete the Rehost Exercise on each of the nodes involved in the cluster.

Task 1: New cluster configuration prep on <master_host_name>

1. Export an ldif using **ptc > Windchill > WindchillDS > server > bat > control-panel.bat**.
   - Open a Windchill Explorer window.
   - Browse to *D:\ptc\Windchill\WindchillDS\server\bat*
   - Double-click the **control-panel.bat** to launch a WindchillDS control panel.
   - When prompted, type **cn=Manager** in the Bind DN field and **ldapadmin** in the Password field.
   - Click the **OK** button.
   - Click the **Export LDIF…** action in the Director Data section of the Windchill Directory Server Control Panel window.
   - In the Windchill Directory Server Control Panel - Export LDIF dialog box, click the **Browse…** button in the Export to File field.
   - In the Choose an LDIF File dialog box, browse to the *D:\ptc\Windchill\WindchillDS folder*.
   - In the File name field, type: **<master_host_name>training.ldif** Example: master2training.ldif
   - Click the **Save** button.
   - In the Windchill Directory Server Control Panel - Export LDIF dialog box, click the **OK** button.
   - Click the **Close** button to close the Export LDIF dialog box.
   - Click the **Windows Close** button on the Windchill Directory Server Control Panel window.
2. It is necessary to stop the Windchill instance on the <master_host_name> server because we are now going to rehost the ldap and database of the <node_host_name> image. Since it is not yet clustered with cache synchronization, this could cause a data corruption.
   - Click the Windchill Shortcuts shortcut from the desktop of the VM.
   - Browse to the *D:\Shortcuts\Windchill PDS* folder and double-click the Windchill Shell shortcut.
   - At the prompt, type **windchill stop** and press ENTER.

Task 2: New cluster configuration prep on <node_host_name>

1. Export an ldif using **ptc > Windchill > WindchillDS > server > bat > control-panel.bat**.
   - Open a Windchill Explorer window.
   - Browse to *D:\ptc\Windchill\WindchillDS\server\bat*
   - Double-click the **control-panel.bat** to launch a WindchillDS control panel.
   - When prompted, type **cn=Manager** in the Bind DN field and **ldapadmin** in the Password field.
   - Click the OK button.
   - Click the **Export LDIF…** action in the Director Data section of the Windchill Directory Server Control Panel window.
   - In the Windchill Directory Server Control Panel - Export LDIF dialog box, click the **Browse…** button in the Export to File field.
   - In the Choose an LDIF File dialog box, browse to the *D:\ptc\Windchill\WindchillDS* folder.
   - In the File name field, type: **<node_host_name>training.ldif**.
   - Click the **Save** button.
   - In the Windchill Directory Server Control Panel - Export LDIF dialog box, click the OK button.
   - Click the **Close** button to close the Export LDIF dialog box.
   - Click the Windows Close button on the Windchill Directory Server Control Panel window.
2. In order to perform a rehost of the ldap to the <master_host_name> WindchillDS instance, we want to stop Windchill to avoid any confusion or corruption. Although it is unlikely since there are no client interactions which would update the ldap at this time, as a best practice, we should stop Windchill before performing the rehost of the ldap since it will delete ldap entries from the <node_host_name> WindchillDS instance.
   - Click the Windchill Shortcuts shortcut from the desktop of the VM.
   - Browse to the *D:\Shortcuts\Windchill RDS* folder and double-click the Windchill Shell shortcut.
   - At the prompt, type **windchill stop** and press ENTER.

Task 3: What steps for each node

1. <master_host_name> configuration activities.
   - Add <data_host_name> to hosts file
   - Add <cluster_host_name> to hosts file
   - Remove ptc-training from hosts file
   - Rehost Info*Engine LDAP (currently <master_host_name>) to
     - Host=<data_host_name>.ptc.com
     - Domain=<cluster_host_name>.ptc.com
   - Apache will be disabled, however:
   - Apache and AJP workers should already be rehosted to the physical machine name and not the cluster alias.
   - Apache authentication should be rehosted to <data_host_name>.
   - Use sqlplus to update the repository table in the database from <master_host_name> to <cluster_host_name>
   - Update the database hostnames in TNSnames.ora and Listener.ora
     - Set the server to <data_host_name>.
   - Configure the Target Database Connection
     - wt.pom.jdbc.host="<data_host_name>.ptc.com"
   - xconfmanager -p
   - Stop All-In-One
   - Start All-In-One
   - Check to see if Windchill is viable.
   - Coordinate with <node_host_name> student - windchill stop to see if Windchill is viable from <node_host_name>. Also, apache stop.
   - Assuming Windchill on <node_host_name> is viable
   - Reconfigure site.xconf cluster settings for master cache. The details of what settings to make are in the topic, Configuring the Master Cache in the guide for this course.
   - Propagate settings.
   - Start Windchill master cache server on <master_host_name>

2. <node_host_name> configuration activities.
   - Add <data_host_name> to hosts file (as a local IP address)
   - Add <cluster_host_name> to hosts file
   - Remove ptc-training from hosts file
   - Rehost Info*Engine LDAP (currently <node_host_name>) to
     - Host-<data_host_name>
     - Domain-<cluster_host_name>
   - Set <data_host_name> to real <data_host_name> server (IP address of <master_host_name>) in hosts file.
   - Apache and AJP workers should already be rehosted to the physical machine name and not the cluster alias. (run full apache rehost anyway)
   - Apache authentication should be rehosted to <data_host_name>.
   - Use sqlplus to update the repository table from <node_host_name> to <cluster_host_name>.
   - Update the database hostnames in TNSnames.ora
     - Set the server to <data_host_name>.
   - Configure the Target Database Connection
     - wt.pom.jdbc.host="<data_host_name>.ptc.com"
   - xconfmanager -p
   - Stop All
   - Start All
   - Check to see if Windchill is viable.
   - Reset <data_host_name> in hosts file (as IP address of <master_host_name> server)
   - Stop All
   - Coordinate with student on <master_host_name> to ensure database and ldap are running.
   - Start Apache
   - Start Windchill
   - Check to see if Windchill is viable.
   - Assuming yes
   - Stop Windchill
   - Reconfigure site.xconf cluster settings for cache client. The details of what settings to make are in the topic, Configuring the Cache Clients in the guide for this course..
   - Start Windchill cache client server on <node_host_name>.

Task 4: Finishing Up Cluster

1. Installing Master Cache Server from Advanced Deployment Guide
   - Configure wt.cache.master.codebase = file:///D:/ptc/Windchill/Windchill (using Windows API format)

   Do NOT turn on RMI Tunneling by setting wt.rmi.clientSocketFactory = wt.boot.WTRMIMasterSocketFactory
   Pg 83

2. Installing Slave Cache Servers from Advanced Deployment Guide
   - Do NOT turn on RMI Tunneling by setting wt.rmi.clientSocketFactory = wt.boot.WTRMIMasterSocketFactory
   - Also wt.cache.master.codebase is also currently set as http://<master_host_name>.ptc.com/Windchill

   This shouldn't actually work since there is no http server currently on that system.
   Pg 85

3. On Master Cache
   - Xconfmanager -p
   - Ensure WindchillDS and Oracle are running.
   - Launch Apache and wait until cluster config on <node_host_name> is ready (Apache should already be configured with <master_host_name> as the server name and worker host)
   - Once ready, launch Windchill.
4. On Slave Cache
   - Xconfmanager -p
   - Launch Apache and wait until cluster config on <master_host_name> is ready (Apache should already be configured with <node_host_name> as the server name and worker host).
   - Once ready, and Master cache server manager has been launched. Start Windchill.

This completes the exercise.

Module 5

Windchill Security Architecture

Module Overview

In this module, we review the Windchill security architecture and how to configure Winchill system components for a secure environment.

Objectives

After completing this module, you will be able to:

- Identify network configuration and architecture that supports a secure Windchill environment
- Identify authentication methodologies, factors, strengths, and methods.
- Identify server hardening techniques.
- Identify encryption mechanisms for the three states of data, in use, in motion, and at rest.
- Identify ways to harden the security of the operating system.
- Harden Apache, Tomcat, and the Windchill Directory Server.
- Apply a Windchill Security Update.
- Identify the Cross Site Scripting (XSS) security vulnerability and Windchill countermeasures.
- Identify available Security Audit Reports.
- Define the Security Label feature and how to implement it in a Windchill solution.

Exercise 1: Setting Up a Reverse Proxy (After Cluster)

Objectives

After successfully completing this exercise, you will be able to:

- Identify the standard configuration actions to set an Apache installation for Reverse Proxy.
- Identify the standard configuration actions to set a working Windchill installation to support a Reverse Proxy configuration.
- Configure Apache web server and a Windchill System for a reverse proxy architecture.

Scenario

In this exercise, you act as a technical consultant who has been given the task of setting up a reverse proxy server on a clustered Windchill system. You will reconfigure the web server on one system to act as a reverse proxy server and you will reconfigure Windchill to communicate using RMI tunneling between the reverse proxy and the Windchill application server.

Feel free to work in groups. It is expected that you will use the same teams and images as used in earlier exercises for clustering.

Prerequisites

- To aid in your understanding and assist with working through the exercise, you may download a copy of the Windchill Advanced Deployment Guide.

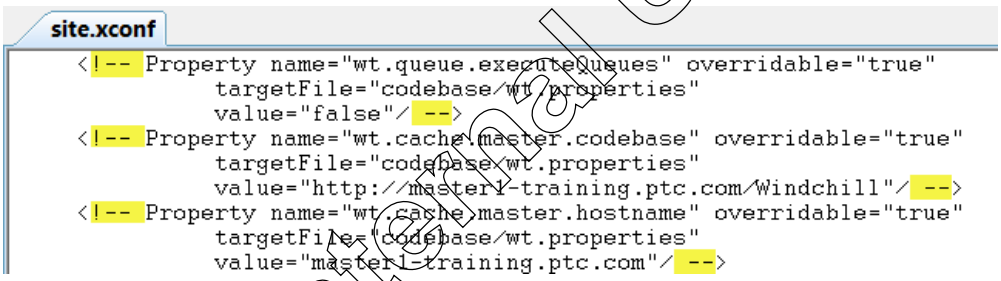
Initial Conditions

- This exercise assumes that there are two companion systems that have been configured and successfully run as a cluster with one system as the cache master and the other as a node (or cache client). In particular this exercise assumes that configuration of the reverse proxy is occurring after the successful completion of the clustering exercise from earlier in this course and that they are the same two systems that were used in that exercise.
- Ensure that the systems have been properly identified in the host files of both systems and that the host names have been changed at the operating system level.

Task 1: Disabling the cluster.

1. Stop Windchill on the node<group_number> server.
   - Double-click the **Windchill Shortcuts** shortcut from the desktop of the node<group_number>-training.ptc.com VM.
   - Browse to the *D:\Shortcuts\Windchill PDS* folder and double-click the **Windchill Shell** shortcut to open the a command window.
   - In the Windchill Shell window, type **windchill stop** and press ENTER.
2. Stop Windchill on the master<group_number> server.
   - Double-click the **Windchill Shortcuts** shortcut from the desktop of the node<group_number>-training.ptc.com VM.
   - Browse to the *D:\Shortcuts\Windchill PDS* folder and double-click the **Windchill Shell** shortcut to open the a command window.
   - In the Windchill Shell window, type **windchill stop** and press ENTER.

3. Update the node<group_number> server windchill configuration to remove cluster behavior and return the system to a single application server with remote data store..
   - Open a Windows Explorer window on the node<group_number>-training.ptc.com server.
   - Browse to the *D:\ptc\Windchill\Windchill\site.xconf* file.
   - Right-click the **site.xconf** file.
   - Select the **Send To > NoteTab Light** option.
   - Comment out the following Property elements by typing a
     !--
     at the beginning of each stanza and a
     --
     at the end of each Property element stanza.
     – Property name="wt.rmi.server.hostname"
     – Property name="wt.queue.executeQueues"
     – Property name="wt.cache.master.codebase"
     – Property name="wt.cache.master.hostname"
     – Property name="wt.cache.master.slaveHosts"
     – Property name="wt.cache.verboseServer"
     – Property name="wt.cache.verboseClient"



   - Add the following code to the site.xconf file:
     <Property name="wt.rmi.server.hostname" overridable="true" targetFile="codebase/wt.properties" value="node1-training.ptc.com"/>
     <Property name="wt.queue.executeQueues" overridable="true" targetFile="codebase/wt.properties" value="true" />
   - Click the **Save** icon on the NoteTab Light toolbar.
   - Click the **Close** button to close NoteTab Light.
4. Propagate changes from site.xconf on the node<group_number>-training server.
   - Double-click the **Windchill Shortcuts** shortcut from the desktop of the node<group_number>-training.ptc.com VM.
   - Browse to the *D:\Shortcuts\Windchill PDS* folder and double-click the **Windchill Shell** shortcut to open the a command window.
   - In the Windchill Shell window, type **xconfmanager -p** and press ENTER.
5. Start the Windchill servers on the node<group_number>-training server and check to see that it launches and runs without issues.
   - In the Windchill Shell window, type **windchill start** and press ENTER.
   - After viewing the **MethodServer ready** statement in the MethodServer window, launch a web browser.
   - From the VM desktop, double-click the **Interenet Explorer** shortcut.
   - In the address field, type **http://node<group_number>-training.ptc.com/Windchill/**
   - When prompted, login as Administrator (wcadmin/wcadmin).
   - Ensure that the login attempt is successful. Work with your exercise partner on any errors or issues.

Task 2: Update DNS entries.

1. On each host within the system, update the hosts file with a new entry for the master node of the cluster.
   - Open a Windows Explorer window on the host system.
   - Browse to the *C:\Windows\System32\drivers\etc\hosts* file.
   - Right-click the **hosts** file.
   - Select the **Send To > NoteTab Light** option.
   - Copy the line in the file that defines the IPv4 address for the master<group_number>-training.ptc.com system.
   - Paste the line below the original creating a duplicate master<group_number>-training address assignment.
   - Modify this line replacing **master** with **proxy**.
   - Click the **Save** icon on the NoteTab Light toolbar.
   - Click the **Close** button to close NoteTab Light.

```
192.168.1.113     data1-training    data1-training.ptc.com
192.168.1.113     master1-training        master1-training.ptc.com
192.168.1.113     proxy1-training         proxy1-training.ptc.com
192.168.1.111     node1-training    node1-training.ptc.com
127.0.0.1   cluster1-training       cluster1-training.ptc.com
```

Task 3: Configuring Apache on master<group_number>-training server as a Reverse Proxy.

1. Enable Apache proxy module support.
   - Open a Windows Explorer window on the master<group_number>-training.ptc.com server.
   - Browse to the *D:\ptc\Windchill\Apache\conf\httpd.conf* file.
   - Right-click the **httpd.conf** file.
   - Select the **Send To > NoteTab Light** option.
   - Scroll down to the section labeled for **Dynamic Shared Object (DSO) Support**.
   - Remove the "#" sign comment character from the beginning of the following LoadModule statements:
     - LoadModule proxy_module modules/mod_proxy.so
     - LoadModule proxy_connect_module modules/mod_proxy_connect.so
     - LoadModule proxy_http_module modules/mod_proxy_http.so

```
LoadModule mime_module modules/mod_mime.so
#LoadModule mime_magic_module modules/mod_mime_magic.so
LoadModule negotiation_module modules/mod_negotiation.so
LoadModule proxy_module modules/mod_proxy.so
#LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
#LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
#LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule rewrite_module modules/mod_rewrite.so
```

2. Add Proxy Pass and Proxy Pass Reverse directives to the Apache configuration.
   - Scroll down to the end of the file.
   - Add a "#" sign comment character to the beginning of the following include directive:
     - # Include conf/extra/additions.conf
   - At the very end of the httpd.conf file, type the following directive statements on individual lines:
     - ProxyPass /Windchill/ http://node1–training.ptc.com/Windchill/
     - ProxyPassReverse /Windchill/ http://node1–training.ptc.com/Windchill/
     - ProxyPass /Windchill http://node1–training.ptc.com/Windchill
     - ProxyPassReverse /Windchill http://node1–training.ptc.com/Windchill
   - Click the **Save** icon on the NoteTab Light toolbar.
   - Click the **Close** button to close NoteTab Light.

```
<IfModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
</IfModule>

# Include conf/extra/additions.conf

ProxyPass /Windchill/ http://node1-training.ptc.com/Windchill/
ProxyPassReverse /Windchill/ http://node1-training.ptc.com/Windchill/
ProxyPass /Windchill http://node1-training.ptc.com/Windchill
ProxyPassReverse /Windchill http://node1-training.ptc.com/Windchill
```

3. Restart Apache on the proxy server.
   - From the Windows Taskbar, select the **D:\Shortcuts\Windcchill PDS\Apache.lnk window**.
   - Click the **Windows Close** button to close the Apache window.
   - Double-click the **Windchill Shortcuts** shortcut from the desktop of the node<group_number>-training.ptc.com VM.
   - Browse to the *D:\Shortcuts\Windchill PDS* folder and double-click the **Apache** shortcut to launch an Apache httpd.exe web server process.
   - Click the **Windows Close** button to close the Windows Explorer window.

Task 4: Configuring Windchill on node<group_number>-training server to support Reverse Proxy.

1. Update the node<group_number> server windchill configuration to support RMI tunneling and generation of proxy links in the user interface. site.xconf should already be open. If site.xconf is not currently open in NoteTab light, the steps for doing so are described in Task 1 of this exercise.
   - Add the following Property elements to the site.xconf file.
     - <Property name="wt.rmi.clientSocketFactory" overridable="true" targetFile="codebase/wt.properties" value="wt.boot.WTRMIMasterSocketFactory"/>
     - <Property name="wt.rmi.serverSocketFactory" overridable="true" targetFile="codebase/wt.properties" value="wt.util.WrappedRMISocketFactory"/>
     - <Property name="wt.rmi.javarmicgi" overridable="true" targetFile="codebase/wt.properties" value="servlet/JavaRMIServlet"/>
     - <Property name="wt.server.codebase" overridable="true" targetFile="codebase/wt.properties" value="http://proxy<group_number>–training.ptc.com/Windchill"/>
     - <Property name="com.ptc.core.ca.co.client.doer.task.default.repository" overridable="true" targetFile="codebase/wt.properties" value="node<group_number>–training.ptc.com"/>
     - <Property name="wt.httpgw.mapCodebase" overridable="true" targetFile="codebase/wt.properties" value="http://node<group_number>–training.ptc.com/Windchill"/>
     - <Property name="wt.federation.rpc.endpoint" overridable="true" targetFile="codebase/wt.properties" value="http://node<group_number>–training.ptc.com:18080/Windchill/servlet.rpc"/>

```
<Property name="wt.rmi.clientSocketFactory" overridable="true"
          targetFile="codebase/wt.properties"
          value="wt.boot.WTRMIMasterSocketFactory"/>
<Property name="wt.rmi.serverSocketFactory" overridable="true"
          targetFile="codebase/wt.properties"
          value="wt.util.WrappedRMISocketFactory"/>
<Property name="wt.rmi.javarmicgi" overridable="true"
          targetFile="codebase/wt.properties"
          value="servlet/JavaRMIServlet"/>
<Property name="wt.server.codebase" overridable="true"
          targetFile="codebase/wt.properties"
          value="http://proxy1-training.ptc.com/Windchill"/>
<Property name="com.ptc.core.ca.co.client.doer.task.default.repository" overridable="true"
          targetFile="codebase/wt.properties"
          value="node1-training.ptc.com"/>
<Property name="wt.httpgw.mapCodebase" overridable="true"
          targetFile="codebase/wt.properties"
          value="http://node1-training.ptc.com/Windchill"/>
<Property name="wt.federation.rpc.endpoint" overridable="true"
          targetFile="codebase/wt.properties"
          value="http://node1-training.ptc.com:18080/Windchill/servlet/RPC"/>
```

   - Click the **Save** icon on the NoteTab Light toolbar.
   - Click the **Close** button to close NoteTab Light.

2. Propagate changes from site.xconf on the node<group_number>-training server.
   - Double-click the **Windchill Shortcuts** shortcut from the desktop of the node<group_number>-training.ptc.com VM.
   - Browse to the *D:\Shortcuts\Windchill PDS* folder and double-click the **Windchill Shell** shortcut to open the a command window.
   - In the Windchill Shell window, type **xconfmanager -p** and press ENTER.
3. Start the Windchill servers on the node<group_number>-training server and check to see that it launches and runs without issues.
   - In the Windchill Shell window, type **windchill stop** and press ENTER.
   - In the Windchill Shell window, type **windchill start** and press ENTER.
   - After viewing the **MethodServer ready** statement in the MethodServer window, launch a web browser.

Task 5: Test Reverse Proxy from both servers

1.
   - From the VM desktop, double-click the **Interenet Explorer** shortcut.
   - In the address field, type **http://proxy<group_number>-training.ptc.com/Windchill/**
   - When prompted, login as Administrator (wcadmin/wcadmin).
   - Ensure that the login attempt is successful. Work with your exercise partner on any errors or issues.

This completes the exercise.

Exercise 2: Implement HTTPS Exercise

Objectives

After successfully completing this exercise, you will be able to:

- Implement HTTPS

Scenario

In this exercise, you act as a technical consultant who has been given the task of implementing HTTPS for Windchill.

Students are expected to work on their individual images but may collaborate freely.

Prerequisites

- This exercise is written from the standpoint of each student working by themselves to implement the security measures. This requires that the training systems be reset to the original monolithic deployment model, if a cluster configuration has been implemented. The steps of this exercise are written using the ptc-training.ptc.com hostname. Your instructor should be able to reset or re-extract your image for this purpose, if necessary. You may also manually rehost your Windchill instance manually to its original single host configuration .

Task 1: Implement HTTPS

1. Create a private key (which is *not* encrypted)
   - Double-click the **Windchill Shortcuts** shortcut from the desktop of the VM.
   - Browse to the *D:\Shortcuts\Windchill PDS* folder and double-click the **Windchill Shell** shortcut to open the a command window.
   - In the Windchill Shell window, type: **cd D:\ptc\Windchill\Apache\bin** and press ENTER.
   - At the prompt, type: **openssl genrsa -out server.key 1024** and press ENTER.
2. (Optional) Create a private key (which *is* encrypted)
   - At the Windchill Shell prompt, type: **openssl genrsa -des3 -out passphrase.key 1024** and press ENTER.
3. (Optional) Remove Pass Phrase from private key:
   - At the Windchill Shell prompt, type: **openssl rsa -in passphrase.key -out server.key** and press ENTER.
4. Generate a Certificate Signing Request (CSR)
   - At the Windchill Shell prompt, type: **openssl req -new -config D:\ptc\Windchill\Apache\conf\extra\openssl.cnf -key server.key -out server.csr** and press ENTER.
   - Loading 'screen' into random state - done You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank. For some fields there will be a default value, If you enter '.', the field will be left blank.
     - Country Name (2 letter code) [AU]:
     - State or Province Name (full name) [Some-State]:
     - Locality Name (eg, city) []:
     - Organization Name (eg, company) [Internet Widgits Pty Ltd]:
     - Organizational Unit Name (eg, section) []:
     - Common Name (eg, YOUR name) []:ptc-training.ptc.com
     - Email Address []:

     Please enter the following 'extra' attributes to be sent with your certificate request:
     - A challenge password []:
     - An optional company name []:

5. Generating a Self-Signed Certificate
   - At the Windchill Shell prompt, type: **openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt** and press ENTER.
6. Installing the Private Key and Certificate in Apache
   - At the Windchill Shell prompt, type: **copy D:\ptc\Windchill\Apache\bin\server.crt D:\ptc\Windchill\Apache\conf\extra\ssl.crt** and press ENTER.
     – (Overwrite existing file? Yes)
   - At the Windchill Shell prompt, type: **copy D:\ptc\Windchill\Apache\bin\server.key D:\ptc\Windchill\Apache\conf\extra\ssl.key** and press ENTER.
     – (Overwrite existing file? Yes)

   These locations have been defined in the httpd-ssl.conf file - important to connect with these!

7. Restart Apache in SSL mode
   - (Optionally modify shortcut as well - this will be needed to get the "start all in one" command to work!)
   - At the Windchill Shell prompt, type: **cd D:\ptc\Windchill\Apache\bin** and press ENTER.
   - At the Windchill Shell prompt, type: **httpd.exe -DSSL** and press ENTER.
8. Connect to https://ptc-training.ptc.com
   - Observe "security exception" and certificate added to browser.
9. Configure Java to trust the certificate
   - At a Windchill Shell prompt, type: **keytool -import -alias windchill -file D:\ptc\Windchill\Apache\conf\extra\ssl.crt\server.crt -storetype jks -keystore %JAVA_HOME%\jre\lib\security\jssecacerts** and press ENTER.
   - Enter keystore password: **ptctraining**
   - Re-enter new password: **ptctraining**
   - Owner: CN=ptc-training.ptc.com, O=Internet Widgits Pty Ltd, ST=Some-State, C=AU
   - Issuer: CN=ptc-training.ptc.com, O=Internet Widgits Pty Ltd, ST=Some-State, C=AU
   - Serial number: a074b6376b18da47
   - Valid from: Thu Oct 17 12:10:08 EDT 2013 until: Fri Oct 17 12:10:08 EDT 2014
   - Certificate fingerprints:
     – MD5: 21:A1:95:FF:2F:92:54:44:78:BD:39:FF:A1:2C:E0:BC
     – SHA1: 82:33:3B:8B:FB:E9:4D:78:B4:2F:52:FF:FE:BB:3C:70:DC:29:85:0A
     – Signature algorithm name: SHA1withRSA
     – Version: 1
   - Trust this certificate? [no]: **y**
   - Certificate was added to keystore

10. (Optional) Verify certificate in Java
    - **keytool -list -v -keystore %JAVA_HOME%\jre\lib\security\jssecacerts**
    - Enter keystore password: **ptctraining**
    - Keystore type: **JKS**
    - Keystore provider: **SUN**
    - Your keystore contains 1 entry
    - Alias name: windchill
    - Creation date: Oct 18, 2013
    - Entry type: trustedCertEntry
    - Owner: CN=ptc-training.ptc.com, O=Internet Widgits Pty Ltd, ST=Some-State, C=AU
    - Issuer: CN=ptc-training.ptc.com, O=Internet Widgits Pty Ltd, ST=Some-State, C=AU
    - Serial number: a074b6376b18da47
    - Valid from: Thu Oct 17 12:10:08 EDT 2013 until: Fri Oct 17 12:10:08 EDT 2014
    - Certificate fingerprints:
      – MD5: 21:A1:95:FF:2F:92:54:44:78:BD:39:FF:A1:2C:E0:BC
      – SHA1: 82:33:3B:8B:FB:E9:4D:78:B4:2F:52:FF:FE:BB:3C:70:DC:29:85:0A
      – Signature algorithm name: SHA1withRSA
      – Version: 1
11. Configure Windchill for HTTPS
    - Review existing values:
      – **xconfmanager -d wt.webserver.port -d wt.webserver.protocol**
    - Set new values:
      – **xconfmanager -s wt.webserver.port=443 -s wt.webserver.protocol=https -t codebase\wt.properties**
    - Propagate changes:
      – **xconfmanager -p**
12. Restart Windchill
    - At the command prompt, type **windchill stop** and press ENTER.
    - Once the command is completed, type **windchill start** and press ENTER.

    Remember the "start windchill" short cut needs to have been updated for HTTPS

13. Test browser client
    - Login and browse around, notice new URLs generated.

    Result:
    - [ok no problems - thumbnails display and manipulate ok]
14. (Optional) Test Creo Client

    Result:
    - Notice "protocol warning" error about registered server.
    - For a while things (i.e. URLs) seemed mixed with http and https (basically things weren't quite working, but no obviouse errors). Repeating things seem to be ok now - testing needs more rigor! Viewable was working ok.
15. (Optional) Test Creo View
16. (Optional) Test Applets
    - RMI Tunneling not included in this exercise!

This completes the exercise.

Exercise 3: Windchill DS SSL

Objectives

After successfully completing this exercise, you will be able to:

- Implement Windchill DS SSL

Scenario

In this exercise, you act as a technical consultant who has been given the task of implementing SSL for WindchillDS.

Students are expected to work on their individual images but may collaborate freely.

Prerequisites

- This exercise is written from the standpoint of each student working by themselves to implement the security measures. This requires that the training systems be reset to the original monolithic deployment model, if a cluster configuration has been implemented. The steps of this exercise are written using the ptc-training.ptc.com hostname. Your instructor should be able to reset or re-extract your image for this purpose, if necessary. You may also manually rehost your Windchill instance manually to its original single host configuration .
- To aid in your understanding and assist with working through the exercise, you may visit the following web site for more information: Getting SSL Up and Running Quickly: http://docs.oracle.com/cd/E19476-01/821-0506/getting-ssl-up-and-running-quickly.html

Task 1: Implement Windchill DS SSL

1. Create Private Key, Self Signed Certificate and Stores

   User input prompts are not included with these notes. Keystore passwords were "ptctraining"

   - Create a "config" directory in Windchill DS:
     - **cd D:\ptc\Windchill\WindchillDS**
     - **mkdir .\config**
   - Create a private key using the "windchillDS" alias:
     - **keytool -genkey -alias windchillDS -keyalg rsa -dname "CN=ptc-training.ptc.com" -keystore config/keystore -storetype JKS**
   - Self Sign the Certificate:
     - **keytool -selfcert -alias windchillDS -validity 365 -keystore config/keystore -storetype JKS**
   - Export the public key:
     - **keytool -export -alias windchillDS -file config/windchillDS.crt -keystore config/keystore -rfc -storetype JKS**
   - Import the "public" key to a trust store (for later use)
     - **keytool -import -alias windchillDS -file config/windchillDS.crt -keystore config/truststore -storetype JKS**
     - **Trust this certificate? [no]: y**
   - Review contents of the "stores"
     - **keytool -list -v -keystore config/keystore**
     - **keytool -list -v -keystore config/truststore**
   - Save the password in a file for "non iteractive" clients to access.

     Can't remember the requirements and "yes" it's a security hole!

     - Create a D:\ptc\Windchill\WindchillDS\server\config\keystore.pin file containing the keystore password: ptctraining

2. Configure Windchill DS for SSL
   - At the Windchill Shell command prompt, type: **cd D:\ptc\Windchill\WindchillDS\server\bat** and press ENTER.
   - Set Key Manager [i.e. where the private keys are stored.]
     - **dsconfig -D "cn=manager" -w ldapadmin -n set-key-manager-provider-prop --provider-name JKS --set enabled:true --set "key-store-file:D:\ptc\Windchill\WindchillDS\config\keystore"**
   - Set Trust Manager [i.e. how are SSL connections accepted. In this case "blindly" but it could be set to the "trust store" created earlier]
     - **dsconfig -D "cn=manager" -w ldapadmin -n set-trust-manager-provider-prop --provider-name "Blind Trust" --set enabled:true**
   - Set Connection Manager [i.e. create/update a way of connecting, in this case via SSL]
     - **dsconfig -D "cn=manager" -w ldapadmin -n set-connection-handler-prop --handler-name "LDAPS Connection Handler" --set "trust-manager-provider:Blind Trust" --set key-manager-provider:JKS --set listen-port:1636 --set enabled:true --set ssl-cert-nickname:windchillDS**
   - Review settings
     - **dsconfig -D "cn=manager" -w ldapadmin -X get-connection-handler-prop --handler-name "LDAPS Connection Handler"**
       - **>>>> Specify WindchillDS LDAP connection parameters**
       - **Directory server hostname or IP address [edserv]: ptc-training.ptc.com**
       - **Directory server administration port number [44444]:**

3. Test Windchill DS:
   - Using the "normal" (non-SSL) connection find details of user "mjones"
     - **ldapsearch -D "cn=manager" -w ldapadmin -h ptc-training.ptc.com --baseDN "" "(uid=mjones)"**
       - dn: uid=mjones,ou=people,cn=AdministrativeLdap,cn=Windchill,o=ptc
       - objectClass: person
       - objectClass: organizationalPerson
       - objectClass: inetOrgPerson
       - objectClass: top
       - uid: mjones
       - cn: Jones, Mike
       - sn: Jones
       - userPassword: {SSHA}v1zk8wHN5JmZRZmmnXAZY7xB2QZfDeQqBb58kw==
       - mail: wc-mail@ptc-training.ptc.com
       - o: PTC Power Equipment
       - preferredLanguage: en-US
   - Using the SSL connection find details of user "mjones" [Important difference here is the certificate acceptance prompt]
     - **ldapsearch -D "cn=manager" -w ldapadmin -h ptc-training.ptc.com --port 1636 --useSSL --baseDN "" "(uid=mjones)"**
       - The server is using the following certificate:
         - Subject DN: CN=ptc-training.ptc.com
         - Issuer DN: CN=ptc-training.ptc.com
         - Validity: Wed Oct 23 09:07:07 EDT 2013 through Thu Oct 23 09:07:07 EDT 2014
       - Do you wish to trust this certificate and continue connecting to the server?
         - Please enter "yes" or "no":**y**
       - dn: uid=mjones,ou=people,cn=AdministrativeLdap,cn=Windchill,o=ptc
       - objectClass: person
       - objectClass: organizationalPerson
       - objectClass: inetOrgPerson
       - objectClass: top
       - uid: mjones
       - cn: Jones, Mike
       - sn: Jones
       - userPassword: {SSHA}v1zk8wHN5JmZRZmmnXAZY7xB2QZfDeQqBb58kw==
       - mail: wc-mail@ptc-training.ptc.com
       - o: PTC Power Equipment
       - preferredLanguage: en-US
   - (Optional): debug/observe SSL handshake
     - Using the Windchill DS Control Panel, add the following parameter to the "ldapsearch" command:
       - **-Djavax.net.debug=ssl,handshake**
     - Repeat the search and see details output of the SSL handshake
   - (Optional): Connect connect with a client using the trust store. [i.e. no certificate acceptance prompt]
     - **ldapsearch -D "cn=manager" -w ldapadmin -h ptc-training.ptc.com --port 1636 --useSSL --trustStorePath "D:\ptc\Windchill\WindchillDS\config\truststore" --baseDN "" "(uid=mjones)"**

4. Configure Windchill to connect to Windchill DS in SSL Mode
   - View Properties of "normal" LDAP connector
     - **dsconfig -D "cn=manager" -w ldapadmin -X get-connection-handler-prop --handler-name "LDAP Connection Handler"**
   - Disable "normal" LDAP Connector (and view properties to confirm disabled)
     - **dsconfig -D "cn=manager" -w ldapadmin -n set-connection-handler-prop --handler-name "LDAP Connection Handler" --set enabled:false**
   - Confirm method server does not start as LDAP cannot be accessed!
   - Apache authentication should also fail to connect as well!
   - Update Method Server to connect to LDAP using SSL:
     - ie.ldap.serverPort=1636 (from 389)
     - Changing the "protocol" to "ldaps" cause "unknown" protocol exceptions when the method server started.
   - This command is the "low level" connection mechanism that Info*Engine uses to connect to LDAP, it *should* work if the environment property gets passed correctly:
     - **windchill --javaargs=-Dcom.ptc.ptc-training.environment.java.naming.security.protocol=ssl com.infoengine.au.DirectoryPropertyInputStream ldap://cn=Manager:ldapadmin@ptc-training.ptc.com:1636/cn=configuration,cn=Windchill,o=ptc**
   - Create a Trust Store provider, this is for the Windchill DS receiving connections!! and then update Connection Handler to use it.
     - **dsconfig -D "cn=manager" -w ldapadmin -n set-trust-manager-provider-prop --provider-name "JKS" --set "trust-store-file:D:\ptc\Windchill\WindchillDS\config\truststore" --set enabled:true**
   - Confirm changes:
     - **dsconfig -D "cn=manager" -w ldapadmin -X get-connection-handler-prop --handler-name "LDAPS Connection Handler"**

This completes the exercise.

Exercise 4: Server Hardening Exercise

Objectives

After successfully completing this exercise, you will be able to:

- Disable Apache Directory Browsing
- Minimize Apache Version Info Display
- Customize Apache Error Message Files
- Minimize Tomcat Version Info Display
- Customize Tomcat Error Message Files

Scenario

In this exercise, you act as a technical consultant who has been given the task of hardening Apache and Tomcat by removing version information which could enable hackers to find and exploit vulnerabilities in the web server and servlet engine configuration.

Students are expected to work on their individual images but may collaborate freely.

Prerequisites

- This exercise is written from the standpoint of each student working by themselves to implement the security measures. This requires that the training systems be reset to the original monolithic deployment model, if a cluster configuration has been implemented. The steps of this exercise are written using the ptc-training.ptc.com hostname. Your instructor should be able to reset or re-extract your image for this purpose, if necessary. You may also manually rehost your Windchill instance manually to its original single host configuration .
- To aid in your understanding and assist with working through the exercise, you may visit the following web site for more information: Securing Tomcat: https://www.owasp.org/index.php/Securing_tomcat

Initial Conditions

- This exercise assumes that you have completed the Implement HTTPS Exercise. As a result all URLs use HTTPS protocol. However, the exercise can still be used with the HTTP protocol if the Implement HTTPS Exercise has not been completed.

Task 1: Disable Apache Directory Browsing

1. Modify the httpd.conf file to remove index browsing capabilities.
   - Open a Windows Explorer window.
   - Browse to the *D:\ptc\Windchill\Apache\conf* folder.
   - Right-click the **httpd.conf** file.
   - Select the **Send To > NoteTab Light** option.
   - Scroll down in the file to locate the following directive: **LoadModule autoindex_module modules/mod_autoindex.so**.
   - Add a "#" sign comment character to the beginning LoadModule directive:
   - Click the **Save** icon on the NoteTab Light toolbar.

   As an additional reference, review the Customer Support document: How to deactivate Apache directory browsing for entire Windchill installation? This is not a customer viewable document.

Task 2: Minimize Apache Version Info Display

1. Check the current settings for Apache's version information display.:
   - Double-click the **Windchill Shortcuts** shortcut from the desktop of the VM.
   - Browse to the *D:\Shortcuts\Windchill PDS* folder and double-click the **Windchill Shell** shortcut to open the a command window.
   - In the Windchill Shell window, type: **cd D:\ptc\Windchill\Apache\bin\conf\extra** and press ENTER.
   - At the prompt, type: **find "ServerTokens" *.conf** and press ENTER.
   - Review and record the exact file, location, and value of the **ServerTokens** setting.
   - At the prompt, type: **find "ServerSignature" *.conf** and press ENTER.
   - Review and record the exact file, location, and value of the **ServerSignature** setting.

   Notice that these are default settings.

2. Observe the HTTP Response message in FireBug which includes the Server details.
   - Double-click the **Mozilla Firefox** shortcut from the desktop of the VM.
   - In the Mozilla Firefox window, select the **Tools > Firebug > Open Firebug** option from the menu bar.
   - At the bottom of the Mozilla Firefox window in the Firebug display panel, select the **Net** option.
   - In the Net tab of the Firebug display panel, click the **Enable** link.
   - At the top of the Mozilla Firefox window, click the **Windchill Server** button.
   - When prompted by the Authentication Required dialog box, click the **Cancel** button.
   - At the bottom of the Mozilla Firefox window, click the Expand (+) icon for the **GET WindchillGW** URL.
   - In the Headers tab, review the Server field on the Response Headers section.
     - The listing should be similar to: **Server Apache/2.2.21 (Win32) mod_ssl/2.2.21 OpenSSL/0.9.8r mod_jk/1.2.32**
   - Click the **Close** button to close the Mozilla Firefox window.
3. Modify the httpd.conf file to minimize Apache version information in HTTP responses.
   - Scroll down to the bottom of the file.
   - Add the following directives:
     - ServerSignature Off
     - ServerTokens Prod
   - Click the **Save** icon on the NoteTab Light toolbar.
   - Click the **Close** button to close NoteTab light.
4. Restart Apache to deploy the configuration changes.
   - From the Windows Taskbar, select the **D:\Shortcuts\Windcchill PDS\Apache.lnk window**.
   - Click the **Windows Close** button to close the Apache window.
   - Double-click the **Windchill Shortcuts** shortcut from the desktop of the VM.
   - Browse to the *D:\Shortcuts\Windchill PDS* folder and double-click the **Windchill Shell** shortcut to open the a command window.
   - At the Windchill Shell command prompt, type: **start D:\ptc\Windchill\Apache\bin\httpd.exe -DSSL** and press ENTER.
   - Browse to the *D:\Shortcuts\Windchill PDS* folder and double-click the **Apache** shortcut to launch an Apache httpd.exe web server process.

5. Observe the HTTP Response message in FireBug which does not include the Server details.
   - Double-click the **Mozilla Firefox** shortcut from the desktop of the VM.
   - At the top of the Mozilla Firefox window, click the **Windchill Server** button.
   - When prompted by the Authentication Required dialog box, click the **Cancel** button.
   - At the bottom of the Mozilla Firefox window, click the Expand (+) icon for the **GET WindchillGW** URL.
   - In the Headers tab, review the Server field on the Response Headers section.
     - The listing should be similar to: **Server Apache**
   - Click the **Close** button to close the Mozilla Firefox window.

Task 3: Customize Apache Error Message Files

This Task is optional.

1. You may optionally perform this step by updating httpd-multilang-errordoc.conf in the *D:\ptc\Windchill\Apache\conf\extra* folder.
2. Read the directions at the top of the file to create custom error messages without changing the original error configuration.

Task 4: Minimize Tomcat Version Info Display

1. Test Tomcat error message display.
   - Double-click the **Mozilla Firefox** shortcut from the desktop of the VM.
   - At the top of the Mozilla Firefox window, type **https://ptc-training.ptc.com/Windchill/app/xxxx** in the address field and press ENTER.
   - When prompted by the Authentication Required dialog box, log on to Windchill as the Windchill Administrator (wcadmin/wcadmin).
   - At the bottom of the HTTP Status page there will be an Apache Tomcat version similar to the following. Note the version information and continue.
     - Apache Tomcat/7.0.23
   - Click the **Close** button to close the Mozilla Firefox window.
2. Extract ServerInfo.properties:
   - In the Windchill Shell window, type: **cd D:\ptc\Windchill\Windchill\tomcat\lib** and press ENTER.
   - In the Windchill Shell window, type: **jar xf catalina.jar org/apache/catalina/util/ServerInfo.properties** and press ENTER.
3. Edit ServerInfo.properties:
   - Using Windows Explorer, browse to the *D:\ptc\Windchill\Windchill\tomcat\lib\org/apache/catalina/util/ServerInfo.properties* file.
   - Right-click the **ServerInfo.properties** file.
   - Select the **Send To > NoteTab Light** option.
   - Update the **server.info** setting as follows:
     - **server.info=Apache Tomcat**
   - Click the **Save** icon on the NoteTab Light toolbar.
   - Click the **Close** button to close NoteTab light.

4. Repackage ServerInfo.properties.
   - In the Windchill Shell window, type: **cd D:\ptc\Windchill\Windchill\tomcat\lib** and press ENTER.
   - At the command prompt, type **windchill stop** and press ENTER.
   - In the Windchill Shell window, type: **jar uf catalina.jar org/apache/catalina/util/ServerInfo.properties** and press ENTER.
   - Once the command is completed, type **windchill start** and press ENTER.
   - At the command prompt, type **rd /S D:\ptc\Windchill\Windchill\tomcat\lib\org** to tidy up the extracted folder path.
5. Test Tomcat error message display.
   - Double-click the **Mozilla Firefox** shortcut from the desktop of the VM.
   - At the top of the Mozilla Firefox window, type **https://ptc-training.ptc.com/Windchill/app/xxxx** in the address field and press ENTER.
   - When prompted by the Authentication Required dialog box, log on to Windchill as the Windchill Administrator (wcadmin/wcadmin).
   - At the bottom of the HTTP Status page there will be an Apache Tomcat version similar to the following. Note the version information and continue.
     – Apache Tomcat
   - Click the **Close** button to close the Mozilla Firefox window.

Task 5: Customize Tomcat Error Message Files

This Task is optional.

1. The "error-page" element needs to be set in %WT_HOME%\codebase\WEB-INF\web.xml
2. See: https://www.owasp.org/index.php/Securing_tomcat for additional details.

This completes the exercise.