

Sterling Secure Proxy



Upgrade Guide

Version 34

Sterling Secure Proxy



Upgrade Guide

Version 34

Note

Before using this information and the product it supports, read the information in "Notices" on page 69.

This edition applies to version 3.4 of IBM Sterling Secure Proxy and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2006, 2012.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Chapter 1. Overview of Upgrading Sterling Secure Proxy from Version 2.0.x to Version 3.x	1	Chapter 16. Convert Version 2.0.x Files and Ignore Warnings.	39
Chapter 2. Upgrade a Single Sterling Secure Proxy Node	3	Chapter 17. Upgrade Script Options	41
Chapter 3. Upgrade Sterling Secure Proxy Clustered Nodes	7	Chapter 18. Read the Upgrade Log File	43
Chapter 4. Upgrade an Sterling Secure Proxy Loading Balancing Environment	11	Chapter 19. Copy an Adapter	45
Chapter 5. Upgrade a Multiple Sterling Secure Proxy Nodes Configuration	15	Chapter 20. Validate an Engine Definition	47
Chapter 6. Load Balancing Multiple Node Upgrade Checklist	19	Chapter 21. Validate an Adapter	49
Chapter 7. Start and Log On to Sterling Secure Proxy Version 2.0.x	21	Chapter 22. Validate a Perimeter Server Definition for a More Secure Zone	51
Chapter 8. Export Sterling Secure Proxy Version 2.0.x Information	23	Chapter 23. Validate a Perimeter Server Definition for a Less Secure Zone	53
Chapter 9. Stop Perimeter Server Version 2.0	25	Chapter 24. Validate the Connection Between Engines and CM	55
Chapter 10. Back Up Version 3.x Configuration Files	27	Chapter 25. Maintain Changes to HTTP Properties	57
Chapter 11. Stop Sterling Secure Proxy Version 2.0.x	29	Chapter 26. New Properties in Version 3.x HTTP Adapter	59
Chapter 12. Validate an Export File	31	Chapter 27. Maintain Changes to FTP Properties	61
Chapter 13. Convert Files from Sterling Secure Proxy Version 2.0.x to Version 3.x	33	Chapter 28. New FTP Adapter Properties in Version 3.x	63
Chapter 14. Convert Version 2.0.x Files With New Engine If No Warnings Are Found	35	Chapter 29. Implement Property Changes Made to a Sterling Connect:Direct Adapter	65
Chapter 15. Convert Version 2.0.x Files With Existing Engine If No Warnings Are Found	37	Chapter 30. Change How Many Times a User Can Attempt to Log In Before a Lock Occurs	67
		Notices	69

Chapter 1. Overview of Upgrading Sterling Secure Proxy from Version 2.0.x to Version 3.x

Use the procedures in this section to upgrade Sterling Secure Proxy from version 2.0, 2.0.01, or 2.0.02 to version 3.x. To upgrade from version 3.0, follow the installation instructions.

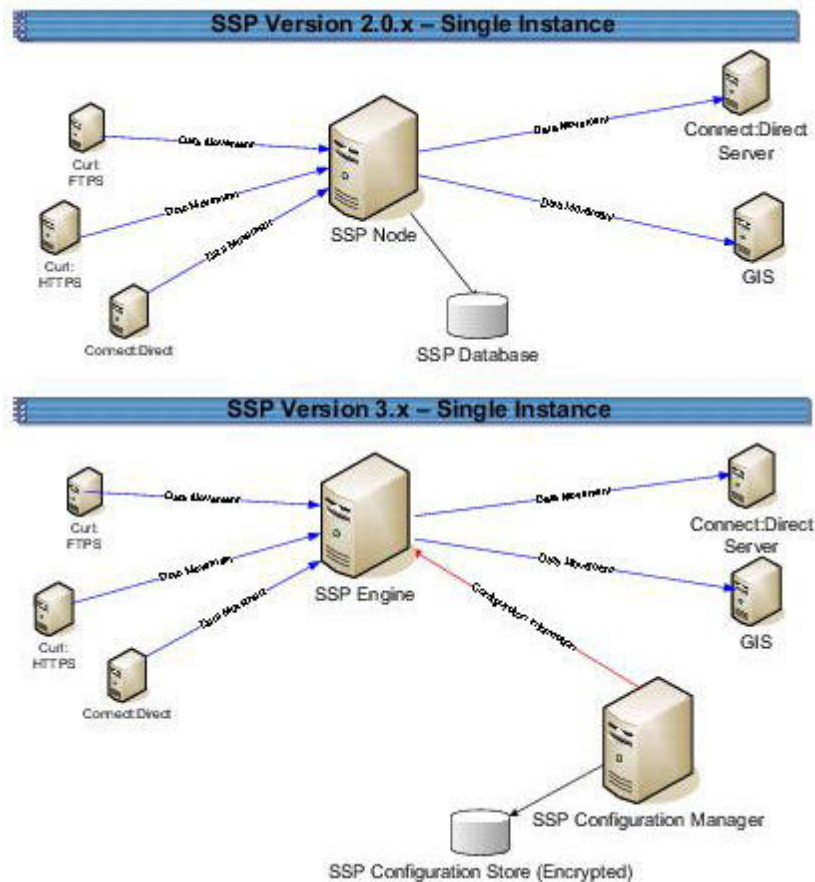
Sterling Secure Proxy version 3.x uses a different architecture from version 2.0.x. The new architecture allows you to configure your environment using the Configuration Manager (CM), then moves the configuration information to an Engine, to use during production. Sterling Secure Proxy version 2.0.x does not use an Engine or CM. Configuration and production occur on an Sterling Secure Proxy node, and data is stored in a database.

Before upgrading your environment, identify the configuration of your Sterling Secure Proxy version 2.0.x. Then, complete the procedures identified for each configuration. Configurations include:

- Single Sterling Secure Proxy environment—If you installed Sterling Secure Proxy on one node, refer to *Upgrade a Single Sterling Secure Proxy Node*
- Clustered Sterling Secure Proxy environment—If you installed Sterling Secure Proxy on two or more nodes and all nodes use the same configuration information to provide high availability and secondary engines accept incoming requests if the primary engine is not available, refer to *Upgrade Sterling Secure Proxy Clustered Nodes*.
- Load balancing Sterling Secure Proxy environment—If you installed Sterling Secure Proxy version 2.0.x on two or more nodes and created a load balancing environment to provide redundancy and share the workload among multiple servers, refer to *Upgrade an Sterling Secure Proxy Loading Balancing Environment for instructions on how to upgrade this environment*.
- Multiple Sterling Secure Proxy nodes environment—If you installed two or more Sterling Secure Proxy nodes and each node manages separate incoming requests, the configuration is unique for each node. Refer to *Upgrade a Multiple Sterling Secure Proxy Nodes Configuration* .
- Move certificates used on an HSM device in Sterling Secure Proxy version 2.0.02. Release 2.0.02 supported the use of an HSM device. To use the HSM certificates created in version 2.0.02, complete the procedure, *Move Key Certificates Created in Sterling Secure Proxy 2.0.02 on the HSM*.

Chapter 2. Upgrade a Single Sterling Secure Proxy Node

If you installed Sterling Secure Proxy version 2.0.x on one node, use the information in this section to upgrade your environment. The following diagram compares an Sterling Secure Proxy version 2.0.x single instance environment to Sterling Secure Proxy version 3.x.



To upgrade a single node configuration created in version 2.0.x, first export information from Sterling Secure Proxy 2.0.x. Then, install an Sterling Secure Proxy version 3.x CM and engine. If you use remote perimeter servers, install a new perimeter server for each instance. Be sure to identify the settings used in version 2.0.x so that you can use this information when you install the new perimeter server. To keep the existing perimeter server configuration, install the new perimeter server over the existing software. Then, run the upgrade script to convert the 2.0.x files to version 3.x. When you run the script, you define the engine to create and associate with the converted files. Refer to *Upgrade Tasks*.

Each exported object is renamed to identify the engine it is associated with. For example, if you created a Sterling Connect:Direct® adapter in version 2.0.x called CDAdapter and you define the Sterling Secure Proxy node as engine1, the adapter is renamed to CDAdapter-engine1 when it is converted to Sterling Secure Proxy 3.x.

Single Node File Conversion Illustration

The following table illustrates how version 2.0.x objects are converted to version 3.x when you convert a single Sterling Secure Proxy instance. Each object name is converted to version 3.x.0. modified by adding the engine name to the end of it.

Version 2.0.x Object	Converts to Version 3.x Object	Notes
	Engine called engine1	No engine was defined in version 2.0.x. Each Sterling Secure Proxy node performed configuration and production tasks. The engine in version 3.x performs only production tasks.
ConnectAdapter1	ConnectAdapter1-engine1 CDNETMAP-ConnectAdapter1-engine1 CDPOLICY_1-engine1 STEPINJ_1-engine1	All information associated with a Sterling Connect:Direct adapter was defined in the adapter in version 2.0.x. The conversion divides the information into four components in version 3.x: connection information in an adapter, node information in a netmap, security requirements in a policy, and step injection definitions in a step injection object. If an identical policy or step injection is defined in more than one adapter, only one item is created. The policy or step injection is then shared by the adapters.
HTTPAdapter1	HTTPAdapter1-engine1	
FTPAdapter1	FTPAdapter1-engine1	
HTTPNetmap1	HTTPNetmap1-engine1	
FTPNetmap1	FTPNetmap1-engine1	
HTTPPolicy1	HTTPPolicy1-engine1	
FTPPolicy1	FTPPolicy1-engine1	
Users	defUserStore	If you do not define a user store at conversion, a default is used. You can create one by using the -userstore argument at conversion.
System Certificates	dfltKeyStore	If you do not define a key store at conversion, a default is used. You can create one by using the -keystore argument at conversion.
CA Certificates	dfltTrustStore	If you do not define a trust store at conversion, a default is used. You can create one by using the -truststore argument at conversion.
Perimeter Server1	PerimeterServer1-engine1 EA_hostname_port-engine1 PASSWORDPOLICY-engine1	No Sterling External Authentication Server object existed. It was defined as part of an adapter. If an Sterling External Authentication Server server is defined in more than one adapter, using the same host and port, only the first instance is created and shared among the adapters.

Pre-Upgrade Checklist

Before you begin an upgrade, obtain the following information:

- Be sure the temporary license key for version 3.x is available on the computer where you will install the engine.
- If you use a remote perimeter server, obtain the perimeter server host name. If you install the perimeter server in a less secure zone than the engine, obtain the host name and port number where the perimeter server will be installed.

Upgrade Tasks

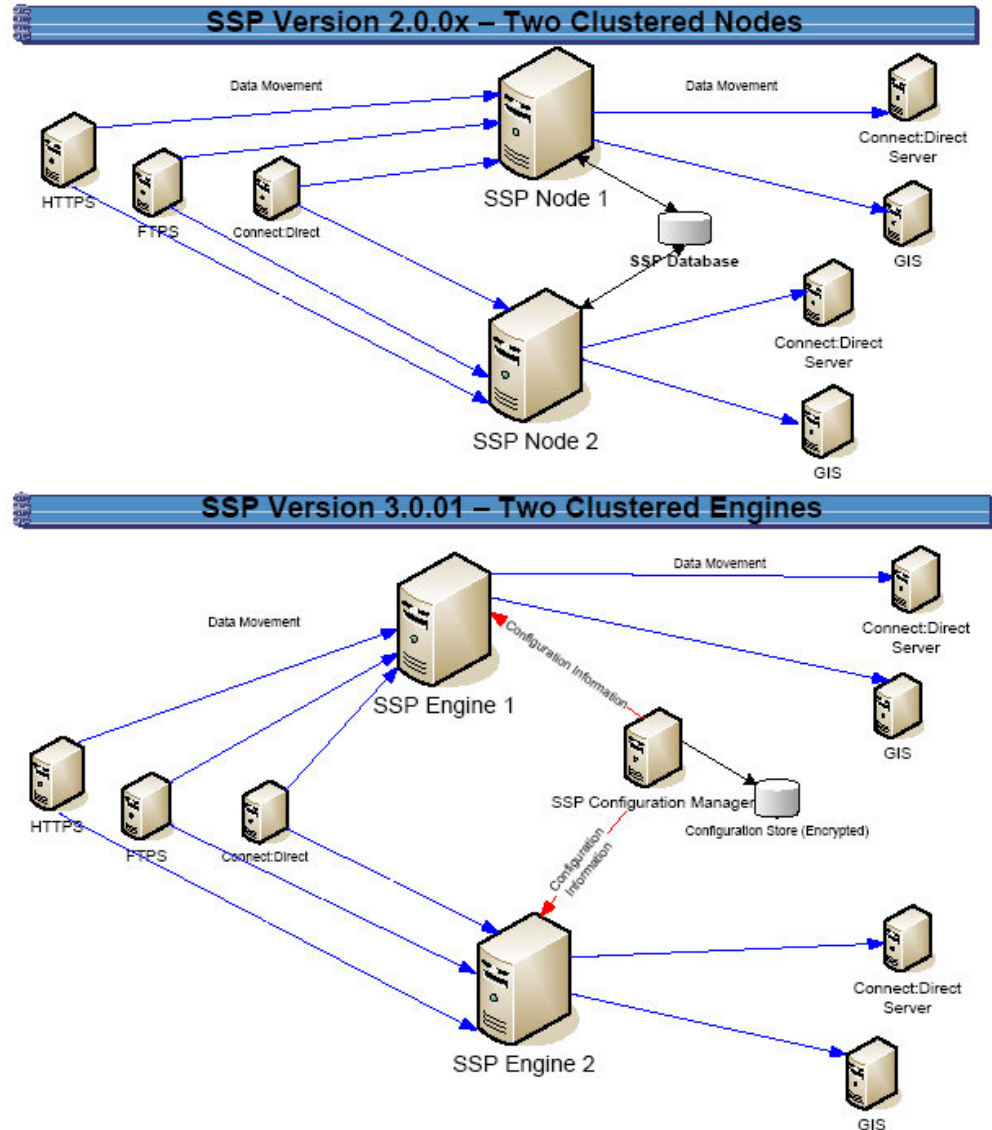
Complete the following tasks to upgrade a single instance of Sterling Secure Proxy:

Installation Task	Procedure to Complete or Information Needed
Start Sterling Secure Proxy version 2.0.x.	<i>Start and Log On to Sterling Secure Proxy Version 2.0.x</i>
Export the Sterling Secure Proxy 2.0.x resources.	<i>Export Sterling Secure Proxy Version 2.0.x Information</i>
Write down the export file name and password.	
Install the Sterling Secure Proxy 3.x Engine.	For UNIX or Linux, refer to <i>Install or Upgrade the Engine on UNIX or Linux</i>
Note: Install the engine but do not start it.	For Microsoft Windows, refer to <i>Install or Upgrade the Engine on Microsoft Windows</i>
Install Sterling Secure Proxy 3.x CM.	For UNIX or Linux, refer to <i>Install or Upgrade CM on UNIX or Linux</i>
	For Microsoft Windows, refer to <i>Install or Upgrade CM on Microsoft Windows</i>
Obtain and install a license key.	For UNIX or Linux, refer to <i>Obtain a License Key File for UNIX or Linux</i>
	For Microsoft Windows, refer to <i>Obtain and Install a License Key File on Microsoft Windows</i>
If you use an external perimeter server, do the following: Stop the version 2.0.x perimeter server. Install a version 3.x perimeter server. If Sterling Secure Proxy 2.0.x is installed on the same computer with the version 3.x engine, stop Sterling Secure Proxy 2.0.x.	<i>Stop Perimeter Server Version 2.0</i> <i>Install a Remote Perimeter Server Overview</i> <i>Stop Sterling Secure Proxy Version 2.0.x</i>
Back up Sterling Secure Proxy version 3.x configuration files.	<i>Back Up Version 3.x Configuration Files</i>
Run the upgrade script.	<i>Convert Files from Sterling Secure Proxy Version 2.0.x to Version 3.x</i>
View the upgrade log to ensure that the conversion succeeded.	<i>Read the Upgrade Log File</i>

Installation Task	Procedure to Complete or Information Needed
Start and log on to CM.	For UNIX or Linux, refer to <i>Run CM on UNIX or Linux</i> For Microsoft Windows, refer to <i>Run CM on Microsoft Windows</i> <i>Start or Stop an Sterling Secure Proxy Component</i>
Open the engine definition and verify the configuration.	<i>Validate an Engine Definition</i>
Open the adapter definitions and verify each adapter configuration.	<i>Validate an Adapter</i>
If you use a perimeter server, validate the perimeter server definition.	<i>Validate a Perimeter Server Definition for a perimeter server in a More Secure Zone</i> or <i>Validate a Perimeter Server Definition for a Perimeter Server in a Less Secure Zone</i>
If you changed any HTTP adapter property values, check the properties and make any necessary changes.	<i>Maintain Changes to HTTP Properties</i>
If you made any changes to a Sterling Connect:Direct adapter properties in version 2.0.x, make the property changes in version 3.x.	<i>Implement Property Changes Made to a Sterling Connect:Direct Adapter</i>
If you made any changes to FTP adapter properties in version 2.0.x, make the changes in version 3.x.	<i>Maintain Changes to FTP Properties</i>
If you changed the log on attempts allowed in version 2.0.x, make the changes in version 3.x.	<i>Change How Many Times a User Can Attempt to Log In Before a Lock Occurs</i>
Make sure that new FTP and HTTP adapter properties are correctly set.	<i>New FTP Adapter Properties in Version 3.x</i> or <i>New Properties in Version 3.x HTTP Adapter</i>
Start the engine.	Refer to <i>Start and Stop Configuration Manager and the Engine</i> <i>Start or Stop a Sterling Secure Proxy</i>
Verify that the engine can communicate with CM.	<i>Validate the Connection Between Engines and CM</i>

Chapter 3. Upgrade Sterling Secure Proxy Clustered Nodes

If you installed Sterling Secure Proxy version 2.0.x on two or more nodes and created a cluster environment to provide failover support, the configuration information at each node is the same and the nodes share a database. The following diagram compares an Sterling Secure Proxy version 2.0.x cluster environment to 3.x:



To upgrade a cluster configuration created in version 2.0.x, first export information from one Sterling Secure Proxy 2.0.x node. Then, install an Sterling Secure Proxy

version 3.x CM. Install an engine for each cluster node in your environment. If you use remote perimeter servers, install a new perimeter server for each instance. To keep the existing configuration, install the new perimeter server over the existing software. To install perimeter server in a new location, be sure to identify the settings used in version 2.0.x so that you can use this information when you install the new perimeter server. Then, run the upgrade script to convert the 2.0.x files to version 3.x. When you run the script, you define the primary engine to create and associate with the converted files. After you determine that the configuration is working on the primary engine, use CM to create additional engines needed in the cluster environment. For each additional engine, make a copy of the adapters and associate the copy with the engine you added.

Each object exported from version 2.0.x is renamed to identify the engine it is associated with. For example, if you created a Sterling Connect:Direct adapter in version 2.0.1 called CDAdapter and you define the Sterling Secure Proxy node1 as engine1, the adapter is renamed to CDAdapter-engine1 when it is converted.

Cluster Nodes File Conversion Illustration

The following table identifies how version 2.0.x objects are converted to version 3.x for a cluster environment. Each object name is converted to version 3.x. modified by adding the engine name to the end of it.

Version 2.0.x Object	Converts to Version 3.x Object	Notes
	Engine called engine1	No engine was defined in version 2.0.x. Each Sterling Secure Proxy node performed configuration and production tasks. The engine in version 3.x performs only production tasks.
ConnectAdapter1	ConnectAdapter1-engine1 CDNETMAP-ConnectAdapter1-engine1 CDPOLICY_1-engine1 CDSTEPINJ_1-engine1	All information associated with a Sterling Connect:Direct adapter was defined in the adapter in version 2.0.x. The conversion divides the information into four components in version 3.x: connection information in an adapter, node information in a netmap, security requirements in a policy, and step injection definitions in a step injection object. If an identical policy or step injection is defined in more than one adapter, only one item is created. The policy or step injection is then shared by the adapters.
HTTPAdapter1	HTTPAdapter1-engine1	
FTPAdapter1	FTPAdapter1-engine1	
HTTPNetmap1	HTTPNetmap1-engine1	
FTPNetmap1	FTPNetmap1-engine1	
HTTPPolicy1	HTTPPolicy1-engine1	
FTPPolicy1	FTPPolicy1-engine1	
Users	defUserStore	If you do not define a user store at conversion, a default is used. You can create one by using the -userstore argument at conversion.
System Certificates	dfltKeyStore	If you do not define a key store at conversion, a default is used. You can create one by using the -keystore argument at conversion

Version 2.0.x Object	Converts to Version 3.x Object	Notes
CA Certificates	dfltTrustStore	If you do not define a trust store at conversion, a default is used. You can create one by using the <code>-truststore</code> argument at conversion.
Perimeter Server1	Perimeter Server1-engine1	
	EA_hostname_port-engine1	No Sterling External Authentication Server object existed. It was defined as part of an adapter. If an Sterling External Authentication Server server is defined in more than one adapter, using the same host and port, only the first instance is created.
	PASSWORDPOLICY-engine1	
	Engine called engine2	This engine is not created during the conversion. Use CM to define engine2.
ConnectAdapter1	ConnectAdapter1-engine2	This adapter is not created during the conversion. Use CM to copy ConnectAdapter1-engine1 and rename it ConnectAdapter1-engine2. The netmap, policy, and step injection object are reused.
	CDNETMAP-ConnectAdapter1-engine1	
	CDPOLICY_1-engine1	
	CDSTEPINJ_1-engine1	
HTTPAdapter1	HTTPAdapter1-engine2	This adapter is not created during the conversion. Use CM to copy HTTPAdapter1-engine1 and rename it to HTTPAdapter1-engine2.
FTPAdapter1	FTPAdapter1-engine2	This adapter is not created during the conversion. Use CM to copy FTPAdapter1-engine1 and rename it to FTPAdapter1-engine2.
HTTPNetmap1	HTTPNetmap1-engine1	The netmap created during conversion is reused.
FTPNetmap1	FTPNetmap1-engine1	The netmap created during conversion is reused.
HTTPPolicy1	HTTPPolicy1-engine1	The policy created during conversion is reused.
FTPPolicy1	FTPPolicy1-engine1	The policy created during conversion is reused.
Users	defUserStore	The same user store is used by engine 1 and engine 2.
System Certificates	dfltKeyStore	The same keystore is used by engine 1 and engine 2.
CA Certificates	dfltTrustStore	The same trust store is used by engine 1 and engine 2.
PerimeterServer2	PerimeterServer2	Perimeter servers cannot be shared by engines. Install a new perimeter server and create a new perimeter server definition for the new engine.

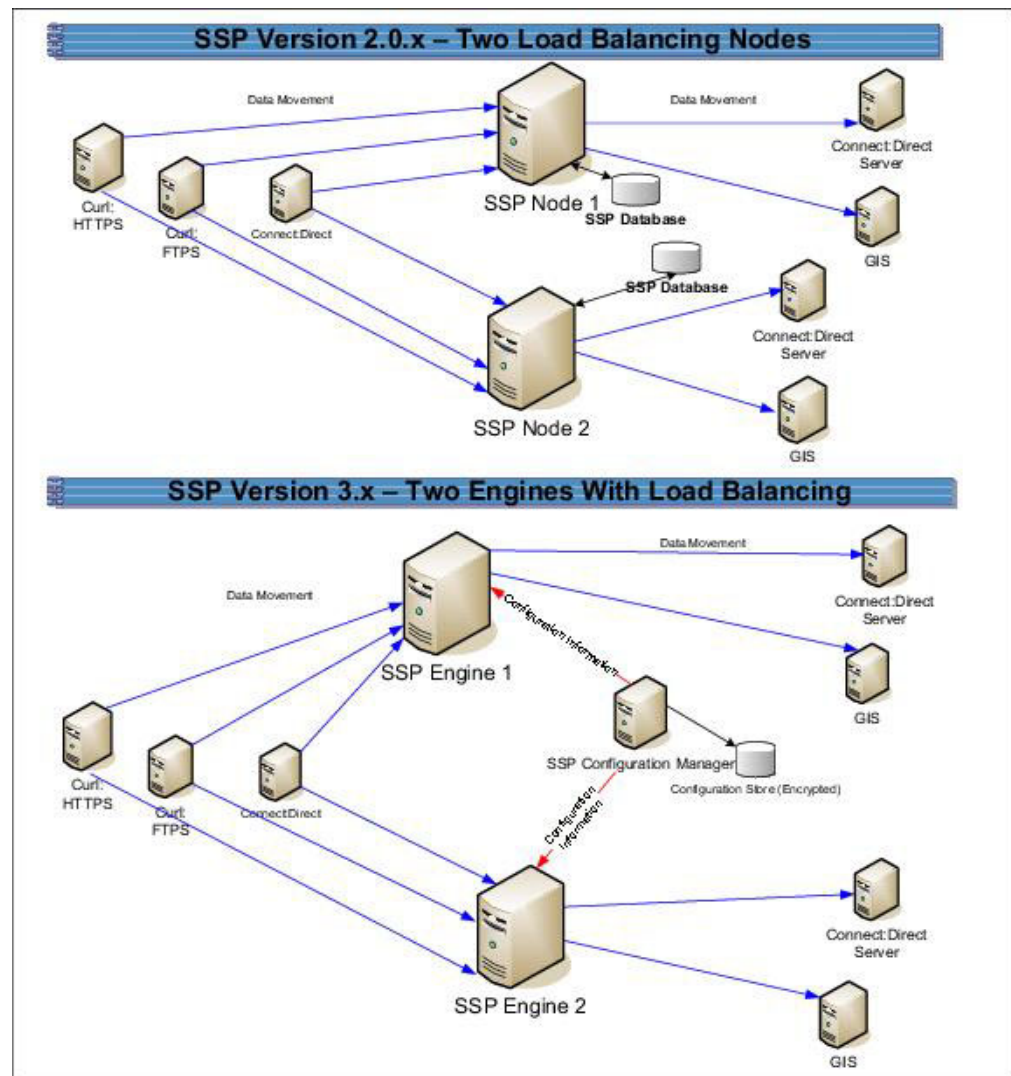
Cluster Nodes Upgrade Checklist

Complete the procedures in the *Upgrade Tasks* to begin the upgrade. Complete the following tasks to complete the cluster node upgrade:

Installation Task	Procedure to Complete or Information Needed
Install an Sterling Secure Proxy 3.x engine at each additional cluster node.	For UNIX or Linux, refer to <i>Install or Upgrade the Engine on UNIX or Linux</i>
Note: Do not start the engine.	For Microsoft Windows, refer to <i>Install or Upgrade the Engine on Microsoft Windows</i>
Obtain and install a license key file for each engine.	For UNIX or Linux, refer to <i>Obtain a License Key File for UNIX or Linux</i>
	For Microsoft Windows, refer to <i>Obtain and Install a License Key File on Microsoft Windows</i>
Create an engine definition for each additional engine in the cluster.	<i>Create an Engine Definition - UNIX</i>
Using CM, make a copy of each adapter associated with the primary engine. Associate the adapter copy with the cluster engine you create. Repeat this for each additional node in the cluster.	<i>Copy an Adapter</i>
Start all Sterling Secure Proxy cluster engines.	For UNIX or Linux, refer to <i>Create an Engine Definition - UNIX</i>
	For Microsoft Windows, <i>Create an Engine Definition - Microsoft Windows</i>
Verify that each cluster engine can communicate with CM.	

Chapter 4. Upgrade an Sterling Secure Proxy Loading Balancing Environment

If you installed Sterling Secure Proxy version 2.0.x on two or more nodes and created a load balancing environment to provide redundancy and share the workload among multiple servers, the configuration information at each node is the same but it is stored in different databases. The following diagram compares an Sterling Secure Proxy version 2.0.x load balancing environment to version 3.x.



To upgrade a load balancing configuration, export information from each Sterling Secure Proxy 2.0.x node. Be sure to specify a unique engine name and export file for each node. Then, run the upgrade script for each node.

For each export file, exported objects are renamed to identify the engine it is associated with. For example, if you created a Sterling Connect:Direct adapter in version 2.0.x called CDAdapter and you define the Sterling Secure Proxy node1 as engine1, the adapter is renamed to CDAdapter-engine1 when it is converted. When

you run the upgrade script again and specify the engine name as engine2, a new adapter definition is created and renamed CDAdapter-engine2.

Load Balancing Nodes File Conversion Illustration

The following table identifies how version 2.0.x objects are converted to version 3.x for a load balancing environment. For each engine defined, its objects are created from a unique database. Each object name is converted to version 3.x and modified to add the engine name to the end of it.

Version 2.0.x Object	Converts to Version 3.x Object	Notes
	Engine called engine1	No engine was defined in version 2.0.x. Each Sterling Secure Proxy node performed configuration and production tasks. The engine in version 3.x performs only production tasks.
ConnectAdapter1	ConnectAdapter1-engine1 CDNETMAP-ConnectAdapter1-engine1 CDPOLICY_1-engine1 CDSTEPINJ_1-engine1	All information associated with a Sterling Connect:Direct adapter was defined in the adapter in version 2.0.x. The conversion divides the information into four components in version 3.x: connection information in an adapter, node information in a netmap, security requirements in a policy, and step injection definitions in a step injection object. If an identical policy or step injection is defined in more than one adapter, only one item is created. The policy or step injection is then shared by the adapters.
HTTPAdapter1	HTTPAdapter1-engine1	
FTPAdapter1	FTPAdapter1-engine1	
HTTPNetmap1	HTTPNetmap1-engine1	
FTPNetmap1	FTPNetmap1-engine1	
HTTPPolicy1	HTTPPolicy1-engine1	
FTPPolicy1	FTPPolicy1-engine1	
Users	defUserStore	If you do not define a user store at conversion, a default is used. You can create one by using the -userstore argument at conversion.
System Certificates	dfltKeyStore	If you do not define a key store at conversion, a default is used. You can create one by using the -keystore argument at conversion.
CA Certificates	dfltTrustStore	If you do not define a trust store at conversion, a default is used. You can create one by using the -truststore argument at conversion.
PerimeterServer1	PerimeterServer1-engine1 EA_hostname_port-engine1 PASSWORDPOLICY-engine1	No Sterling External Authentication Server object existed. It was defined as part of an adapter. If an Sterling External Authentication Server server is defined in more than one adapter, using the same host and port, only the first instance is created.

Version 2.0.x Object	Converts to Version 3.x Object	Notes
	Engine called engine2	No engine was defined in version 2.0.x. Each Sterling Secure Proxy node was separately managed. In version 3.x, all engines can be managed by one CM.
ConnectAdapter1	ConnectAdapter1-engine2 CDNETMAP-ConnectAdapter1-engine2 CDPOLICY_1-engine2 CDSTEPINJ_1-engine2	All information associated with a Sterling Connect:Direct adapter was defined in the adapter in version 2.0.x. The conversion divides the information into four components in version 3.x: connection information in an adapter, node information in a netmap, security requirements in a policy, and step injection definitions in a step injection object.
HTTPAdapter1	HTTPAdapter1-engine2	
FTPAdapter1	FTPAdapter1-engine2	
HTTPNetmap1	HTTPNetmap1-engine2	
FTPNetmap1	FTPNetmap1-engine2	
HTTTPolicy1	HTTTPolicy1-engine2	
FTTPolicy1	FTTPolicy1-engine2	
Users	defUserStore	The same user store is used by engine 1 and engine 2
System Certificates	dfltKeyStore	The same keystore is used by engine 1 and engine 2
CA Certificates	dfltTrustStore	The same trust store is used by engine 1 and engine 2.
PerimeterServer2	PerimeterServer2-engine2	

Load Balancing Nodes Upgrade Checklist

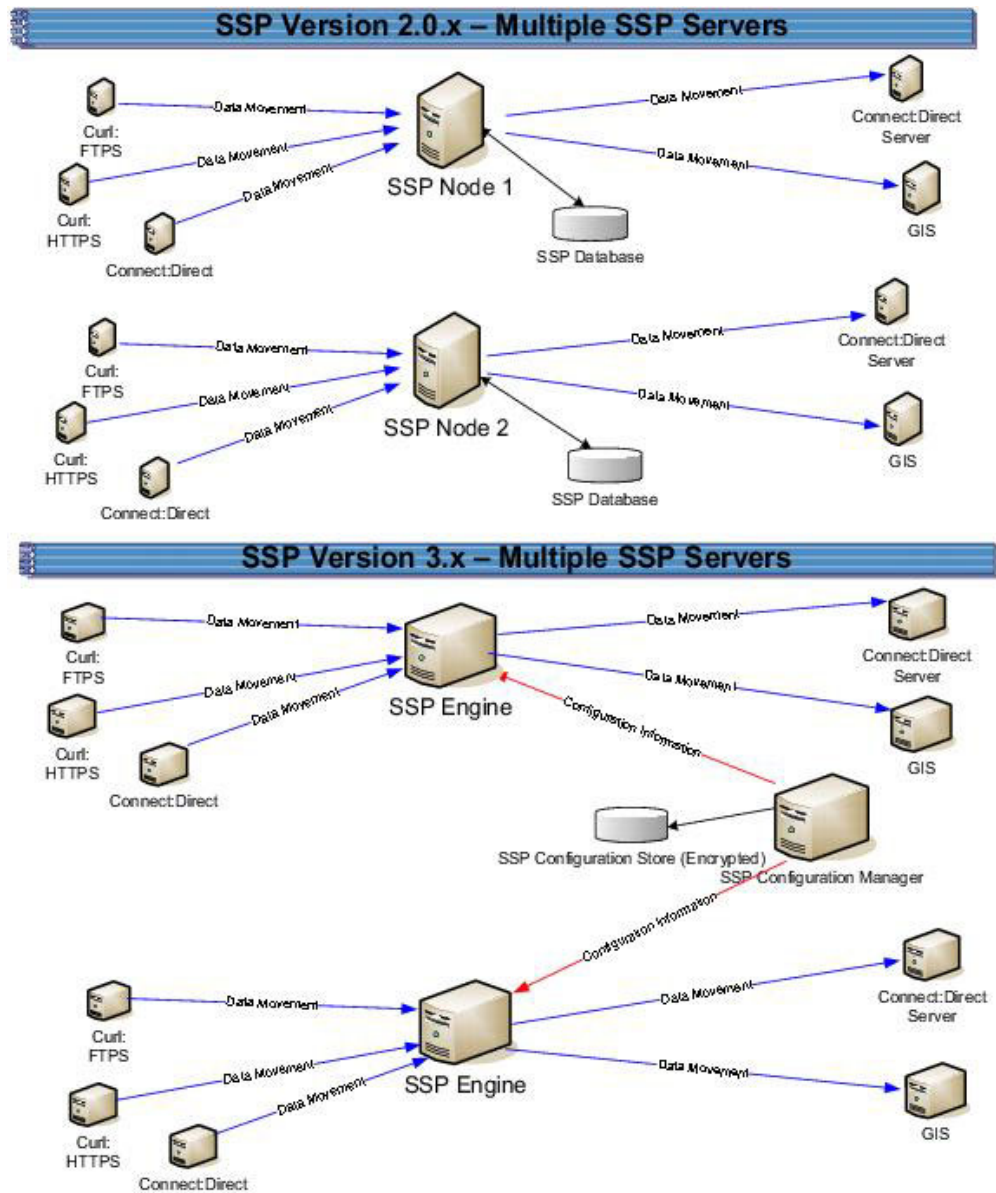
Complete the procedures in the *Upgrade Tasks* to begin the upgrade. Perform the following procedures to complete the load balancing environment upgrade:

Installation Task	Procedure to Complete or Information Needed
Install an Sterling Secure Proxy 3.x engine at each additional load balancing location.	For UNIX or Linux, refer to <i>Install or Upgrade the Engine on UNIX or Linux</i> . For Microsoft Windows, refer to <i>Install or Upgrade the Engine on Microsoft Windows</i> .
Obtain and install a license key file for each load balancing engine.	For UNIX or Linux, refer to <i>Obtain a License Key File for UNIX or Linux</i> . For Microsoft Windows, refer to <i>Obtain and Install a License Key File on Microsoft Windows</i> .
Export Sterling Secure Proxy version 2.0.x resources from each additional Sterling Secure Proxy node.	<i>Export Sterling Secure Proxy Version 2.0.x Information</i> .
Write down the export file name and password.	

Installation Task	Procedure to Complete or Information Needed
Run the upgrade script and identify the name of the additional engine (node).	<i>Convert Files from Sterling Secure Proxy Version 2.0.x to Version 3.x.</i>
View the upgrade log to ensure that the conversion for the node succeeded.	<i>Read the Upgrade Log File</i>
From CM, verify each load balancing engine definition.	<i>Validate an Engine Definition</i>
Open the adapter definitions for each load balancing engine. Make sure that each adapter is correctly defined.	<i>Validate an Adapter</i>
Start all Sterling Secure Proxy load balancing engines.	<p>For UNIX or Linux, refer to <i>Create an Engine Definition - UNIX.</i></p> <p>For Microsoft Windows, refer to <i>Create an Engine Definition - Microsoft Windows.</i></p>
Verify that the load balancing engine can communicate with CM.	<p><i>Validate the Connection Between Engines and CM</i></p> <p><i>Validate the Connection Between Engines and CM</i></p>

Chapter 5. Upgrade a Multiple Sterling Secure Proxy Nodes Configuration

If you installed Sterling Secure Proxy version 2.0.x on multiple nodes and the configuration information for each node is unique, use the information in this section to identify how to upgrade your environment. The following diagram compares an Sterling Secure Proxy version 2.0.x multiple node environment to version 3.x:



To upgrade the configuration created in version 2.0.x, export information from each node. Then, run the upgrade script at each node to convert the files to version 3.x. When you run the upgrade script, you define the engine to create and associate with the converted files. Be sure to define a unique engine name for each node.

Each exported object is renamed to identify the engine it is associated with. For example, if you created a Sterling Connect:Direct adapter in version 2.0.x called CDAdapter and you define the Sterling Secure Proxy node as engine1, the adapter is renamed to CDAdapter-engine1 when it is converted to Sterling Secure Proxy 3.x.

Multiple Node Environment File Conversion Illustration

The following table identifies how version 2.0.x objects are converted to version 3.x for a multiple node environment. For each engine defined, its objects are created from a unique database. Each object name is converted to version 3.x and modified by adding the engine name to the end of it.

Version 2.0.x Object	Converts to Version 3.x Object	Notes
	Engine called engine1	No engine was defined in version 2.0.x. Each Sterling Secure Proxy node was separately managed.
ConnectAdapter1	ConnectAdapter1-engine1 CDNETMAP-ConnectAdapter1-engine1 CDPOLICY_1-engine1 CDSTEPINJ_1-engine1	Each object name is modified by adding the engine name to the end of it in version 3.x. All information associated with a Sterling Connect:Direct adapter was defined in the adapter in version 2.0.x. The conversion divides the information into four components in version 3.x: connection information in an adapter, node information in a netmap, security requirements in a policy, and step injection definitions in a step injection object. If an identical policy or step injection is defined in more than one adapter, only one item is created. The policy or step injection is then shared by the adapters.
HTTPAdapter1	HTTPAdapter1-engine1	
FTPAdapter1	FTPAdapter1-engine1	
HTTPNetmap1	HTTPNetmap1-engine1	
FTPNetmap1	FTPNetmap1-engine1	
HTTTPolicy1	HTTTPolicy1-engine1	
FTTPolicy1	FTTPolicy1-engine1	
Users	defUserStore	If you do not define a user store at conversion, a default is used. You can create one by using the -userstore argument at conversion.
System Certificates	dfltKeyStore	If you do not define a key store at conversion, a default is used. You can create one by using the -keystore argument at conversion.
CA Certificates	dfltTrustStore	If you do not define a trust store at conversion, a default is used. You can create one by using the -truststore argument at conversion.
PerimeterServer1	PerimeterServer1-engine1	

Version 2.0.x Object	Converts to Version 3.x Object	Notes
	EA_hostname_port-engine1	No Sterling External Authentication Server object existed. It was defined as part of an adapter. If an Sterling External Authentication Server server is defined in more than one adapter, using the same host and port, only the first instance is created.
	PASSWORDPOLICY-engine1	
	Engine called engine2	No engine was defined in version 2.0.x. Each Sterling Secure Proxy node was separately managed. In version 3.x, all engines can be managed by one CM.
ConnectAdapter1	ConnectAdapter1-engine2 CDNETMAP-ConnectAdapter1-engine2 CDPOLICY_1-engine2 CDSTEPINJ_1-engine2	Each object name is modified by adding the engine name to the end of it in version 3.x. All information associated with a Sterling Connect:Direct adapter was defined in the adapter in version 2.0.x. The conversion divides the information into four components in version 3.x: connection information in an adapter, node information in a netmap, security requirements in a policy, and step injection definitions in a step injection object. If an identical policy or step injection is defined in more than one adapter, only one item is created. The policy or step injection is then shared by the adapters.
HTTPAdapter1	HTTPAdapter1-engine2	
FTPAdapter1	FTPAdapter1-engine2	
HTTPNetmap1	HTTPNetmap1-engine2	
FTPNetmap1	FTPNetmap1-engine2	
HTTPPolicy1	HTTPPolicy1-engine2	
FTPPolicy1	FTPPolicy1-engine2	
Users	defUserStore	The same user store is used by engine 1 and engine 2
System Certificates	dfltKeyStore	The same keystore is used by engine 1 and engine 2
CA Certificates	dfltTrustStore	The same trust store is used by engine 1 and engine 2.
PerimeterServer2	PerimeterServer2-engine2	

Chapter 6. Load Balancing Multiple Node Upgrade Checklist

Complete the procedures in the *Upgrade Tasks* to begin the upgrade. Perform the following procedures to complete the multiple node environment upgrade:

Installation Task	Procedure to Complete or Information Needed
Install an Sterling Secure Proxy 3.x engine at each additional server location.	<i>For UNIX or Linux, Install or Upgrade the Engine on UNIX or Linux</i> <i>For Microsoft Windows, Install or Upgrade the Engine on Microsoft Windows</i>
Obtain and install a license key file for each additional engine.	IBM® License Key Guide.
Run the upgrade script at each additional engine.	<i>Convert Files from Sterling Secure Proxy Version 2.0.x to Version 3.x</i>
View the upgrade log to ensure that the conversion succeeded.	<i>Read the Upgrade Log File</i>
Start and log on to CM.	<i>For UNIX or Linux, refer to Run CM on UNIX or Linux</i> <i>For Microsoft Windows, refer to Run CM on Microsoft Windows.</i> <i>Start or Stop an Sterling Secure Proxy Component</i>
From CM, open the engine definition and verify the configuration.	<i>Validate the Converted Components in Sterling Secure Proxy Version 3.x</i>
Open the adapter definitions. Make sure that each adapter is correctly defined.	<i>Validate an Adapter</i>
Start the Sterling Secure Proxy engine.	<i>Create an Engine Definition - UNIX</i>
Verify that the engines can communicate with CM.	<i>Validate the Connection Between Engines and CM</i>

Chapter 7. Start and Log On to Sterling Secure Proxy Version 2.0.x

About this task

To start and log on to Sterling Secure Proxy version 2.0.x:

Procedure

1. To start Sterling Secure Proxy on UNIX or Linux:
 - a. Change the directory to *install_dir/bin*.
 - b. Type `run.sh`.
 - c. Enter the passphrase that you supplied during installation.
2. To start Sterling Secure Proxy on Microsoft Windows, double-click the Sterling Secure Proxy icon on your Microsoft Windows desktop.

When startup is complete, a message such as the following is displayed:

Open your Web browser to `http://host:port/dashboard`

where *host:port* is the IP address and port number where Sterling Secure Proxy is installed.

3. Open a browser window and type the URL address for Sterling Secure Proxy version 2.0.x.
4. Type the user ID and password in the **User ID** and **Password** fields. The default values are *proxy_admin* and *password*.

Chapter 8. Export Sterling Secure Proxy Version 2.0.x Information

About this task

To move configuration information defined in Sterling Secure Proxy version 2.0.x to version 3.x, first export the resource files from version 2.0.x.

To export Sterling Secure Proxy version 2.0.x resource files:

Procedure

1. From the Deployment menu, select **Import/Export**.
2. Next to Export Resources, click **Go!**
3. With **XML Document** selected, click **Next**.
4. With **No** selected, click **Next**.
5. With **Standard** selected as the export type, click **Next**.
6. Select all of the resources to export and click **Next**. Resource types include:
 - Accounts
 - Proxy Policies
 - Perimeter Servers
 - Digital Certificates
 - Proxy Netmaps
 - Service Configurations
7. Select **Users** as the account type to export and click **Next**.
8. To export all users, click the double-right arrows to move all users to the **To Be Exported** column. Click **Next**.
9. To export all permission definitions, click the double-right arrows to move all permission definitions to the **To Be Exported** column. Click **Next**.
10. Select **CA Digital Certificates** and **System Certificates** to export all digital certificates. Click **Next**.
11. To export all CA digital certificates, click the double-right arrows to move all certificates to the **To Be Exported** column. Click **Next**.
12. To export all system certificates, click the double-right arrows to move all certificates to the **To Be Exported** column. Click **Next**.
13. To export all proxy policies, click the double-right arrows to move all policies to the **To Be Exported** column. Click **Next**.
14. To export all netmaps, click the double-right arrows to move all netmaps to the **To Be Exported** column. Click **Next**.
15. To export all perimeter servers, click the double-right arrows to move all items to the **To Be Exported** column. Click **Next**.
16. To export all service configurations (adapters), click the double-right arrows to move all items to the **To Be Exported** column. Click **Next**.
17. Type the passphrase defined during the version 2.0.x installation twice and click **Next**.
18. Click **Finish** to export the resources and create the export file.

19. To view the export report, click **View Export Report**. Make sure that all resources were successfully exported.
20. Click **Download Export data** (.xml or .jar) to save the export file.
21. Click **Return**.

Chapter 9. Stop Perimeter Server Version 2.0

About this task

To stop a version 2.0 perimeter server:

Procedure

1. Change the directory to `/install_dir/bin` where `install_dir` is the location where the perimeter server is installed.
2. Type `stopPs.sh` and press **Enter**.

Chapter 10. Back Up Version 3.x Configuration Files

About this task

Before you upgrade version 2.0.x files to version 3.x, first back up the version 3.x configuration files. Back up the folder called */install_dir/conf/* on the computer where CM is installed.

Chapter 11. Stop Sterling Secure Proxy Version 2.0.x

About this task

To stop Sterling Secure Proxy version 2.0.x:

Procedure

1. If necessary, open Sterling Secure Proxy version 2.0.x. Refer to *Start and Log On to Sterling Secure Proxy Version 2.0.x*.
2. From the Administration menu, select **System Tools > Troubleshooter**.
3. Click **Stop the System** and wait for shutdown to complete.

Chapter 12. Validate an Export File

About this task

Complete this procedure to validate an export file and write warnings that will occur at conversion to the upgrade log. This procedure does not convert the objects to version 3.x.

To validate an export file:

Procedure

1. From the `/install_dir/bin` directory, where `install_dir` is the CM installation directory, type the following command and press **Enter**:

```
./sspUpgrade export_file engine_name -v
```

Refer to *Upgrade Script Options* for a description of the parameters.
2. Type the passphrase defined at installation for Sterling Secure Proxy version 2.0.x and press **Enter**.
3. Type the passphrase defined when you installed CM.

Chapter 13. Convert Files from Sterling Secure Proxy Version 2.0.x to Version 3.x

About this task

After you export the resource files from Sterling Secure Proxy version 2.0.x, run the upgrade script. The script first validates the objects in the file. If an object is not valid, a warning is generated and written to the upgrade log. It then performs a dependency check to ensure that items associated with an object are available in the export file. For example, if you exported an HTTP adapter that uses SSL, the dependency check searches for the certificate used in the HTTP secure communications. If it is not available, a dependency warning is generated and written to the upgrade log. The script then converts the objects to version 3.x syntax and imports the objects into CM.

Procedure

Run the script using one or more of the following modes:

- Validation (-v)—reads the export file and generates a list of warnings that will occur if the file is converted. It does not convert the objects.
- Default—validates the export file and determines if it can be converted. It then performs a dependency check. If no validation or dependency warnings are generated, the objects are converted. If warnings occur, the file is not converted and warnings are written to the upgrade log.
- Ignore warning (-w)—validates the export file and performs a dependency check. Objects are then converted. Any dependency or validation warnings are written to the upgrade log.
- Dependency check (-d)—validates the export file and determines if it can be converted. It then performs a dependency check. If no validation warnings are generated, the objects are converted. It ignores dependency warnings and writes them to the upgrade log.
- Overwrite (-o)—converts an export file and if an object already exists in the version 3.x configuration, it overwrites the object with the new information. All other modes ignore an object that already exists.

Chapter 14. Convert Version 2.0.x Files With New Engine If No Warnings Are Found

About this task

Complete this procedure to convert objects from Sterling Secure Proxy version 2.0.x to version 3.x and create a new engine. You identify the name of the engine to create and the engine host and port as well as the version 2.0.x file to convert on the command line.

The upgrade script reads the export file and determines if objects are valid. It then performs a dependency check to determine if any item referenced by an exported object is missing. If any object is not valid or if a dependency check warning is generated, the files are not converted. If the objects are valid, an engine is created with the values you specify. Then, objects are converted to version 3.x format and associated with the engine.

To convert the version 2.0.x export file version 3.x and create a new engine, if no warnings are generated:

Procedure

1. From the `/install_dir/bin` directory, where *install_dir* is the CM installation directory, type the following command and press **Enter**. Refer to *Upgrade Script Options* for a description of the parameters.

```
./sspUpgrade export_file_name engine_name -enginehost enginehostvalue -engineport engineportvalue
```

2. Do one of the following:
 - If you have not backed up the `/install_dir/conf/` folder, type `n` and press **Enter** to stop the script. After you perform the backup, perform this procedure again.
 - Type `y` and press **Enter** to continue.
3. Type the passphrase defined at installation for Sterling Secure Proxy version 2.0.x and press **Enter**.
4. Type the passphrase defined when you installed CM 3.x and press **Enter**.

Chapter 15. Convert Version 2.0.x Files With Existing Engine If No Warnings Are Found

About this task

Complete this procedure to convert an export file from Sterling Secure Proxy version 2.0.x to version 3.x and associate converted files with an engine that is already defined in version 3.x. You identify the name of the engine to associate the converted objects with on the command line.

The upgrade script reads the export file and determines if objects are valid. It then performs a dependency check to determine if any item referenced by an exported object is missing. If any object is not valid or if a dependency check warning is generated, the files are not converted. If the objects are valid, they are converted to version 3.x format and associated with the engine you specified.

To convert the version 2.0.x export file to version 3.x, if no warnings are generated, and associate them with an engine that is already defined in version 3.x:

Procedure

1. From the `/install_dir/bin` directory where *install_dir* is the CM installation directory, type the following command and press **Enter**:

```
./sspUpgrade export_file_name engine_name
```
2. Do one of the following:
 - If you have not backed up the `/install_dir/conf/` folder, type `n` and press **Enter** to stop the script. After you perform the backup, perform this procedure again.
 - Type `y` and press **Enter** to continue.
3. Type the passphrase defined at installation for Sterling Secure Proxy version 2.0.x and press **Enter**.
4. Type the passphrase defined when you installed CM3.x and press **Enter**.

Chapter 16. Convert Version 2.0.x Files and Ignore Warnings

About this task

Complete this procedure to convert an export file from Sterling Secure Proxy version 2.0.x to version 3.x and ignore warnings.

Note: We strongly recommend that you resolve warnings before converting files to the version 3.x format. Converting files with warnings may prevent adapters from working. If you convert files that contain warnings or dependencies to version 3.x, be sure to resolve the warnings. Then, open and save the engine definition to ensure that the changes are pushed to the engine.

The script first reads the export file and determines if objects are valid. It then performs a dependency check to determine if any item referenced by an exported object is missing. The `-w` option allows the files to be converted to version 3.x format, even if validation warnings occur. The `-d` option allows the files to be converted to version 3.x format, even if dependency warnings occur. All warnings are written to the upgrade log.

To convert the export file even if warnings occur:

Procedure

1. From a command line prompt, go to the `/install_dir/bin` directory, where `install_dir` is the CM installation directory.
2. Do one of the following:
 - To convert the export file even if validation or dependency warnings occur, type the following command:

```
./sspUpgrade export_file_name engine_name -enginehost value -engineport value -w
```

- To convert the export file even if dependency warnings occur, type the following command:

```
./sspUpgrade export_file_name engine_name -enginehost value -engineport value -d
```

Note: To associate converted files with an engine that is already defined in version 3.x, you do not have to specify an enginehost and engineport value on the command line.

3. Do one of the following:
 - If you have not backed up the `/install_dir/conf/` folder, type `n` and press **Enter** to stop the script. After you perform the backup, start over with this procedure.
 - Type `y` and press **Enter** to continue.
4. Type the passphrase defined at installation for Sterling Secure Proxy version 2.0.x and press **Enter**.
5. Type the passphrase defined when you installed CM and press **Enter**.

Chapter 17. Upgrade Script Options

Following are the arguments to use when running the upgrade script:

Argument	Description	Required
<code>export_file_name</code>	The name assigned to the file you exported from version 2.0.x.	Y
<code>engine_name</code>	The engine name where the resources should be copied. <ul style="list-style-type: none">• If this engine has not been created, the upgrade script creates it and assigns it the default values. It then adds all the resources to the engine definition. If you do not define the <code>-enginehost</code> and <code>-engineport</code> parameters, use <code>CM</code> to complete the engine definition. If you provide a value for the parameters called <code>enginehost</code> and <code>engineport</code>, the engine is configured as part of the upgrade procedure and is ready for use.• If the engine name already exists in version 3.x, all components in the export file are added to the engine definition.	Y
<code>-enginehost <i>hostvalue</i></code>	The engine host name. The default is <code>defaultEngineHost</code> .	
<code>-engineport <i>portvalue</i></code>	The engine port used to communicate with CM and inbound nodes. The default value is 63366.	
<code>-userstore <i>userStoreName</i></code>	The name of the user store where user definitions are added. If no user store is specified, definitions are added to the default user store, called <code>defUserStore</code> .	
<code>-truststore <i>trustStoreName</i></code>	The name of the trust store where trusted certificates are added. If no trust store is specified, trusted certificates are added to the default trust store, called <code>dfltTrustStore</code> .	
<code>-keystore <i>keyStoreName</i></code>	The name of the keystore where key certificates are added. If no keystore is specified, key certificates are added to the default key store, called <code>dfltKeyStore</code> .	
<code>-conf</code>	An alternate location to copy the files after they are converted. The directory must already exist and must contain the key file needed to encrypt the files. The default directory is <code>../conf</code> .	
<code>-help</code> or <code>-h</code>	To view help for the command.	

Following are the options to identify how the script is implemented:

Argument	Description	Required
	<p>If no option is defined, the upgrade process validates the parameters in the export file and performs a dependency check to determine if items referenced by an exported object are available. If any validation or dependency warnings are identified, the upgrade is stopped. If any object being upgraded already exists in CM, it is not replaced.</p>	
-v	<p>Performs a validation to make sure that the 2.0.x export file can be converted to version 3.x format without warnings. However, the file is not converted. Any warnings are written to a log file. Use this option to identify warnings and fix them before you move the information into version 3.x.</p>	
-d	<p>Converts the export file, even when dependency warnings occur. A dependency check determines if any item referenced by an exported object is missing. Dependency check warnings are written to the log. If a validation warning occurs, the upgrade process is stopped, and no files are updated.</p>	
-w	<p>Converts the export file, even when validation or dependency warnings occur. Be sure to resolve any warnings before you begin sending data through Sterling Secure Proxy.</p>	
-o	<p>If an item already exists, overwrites the item with the new information.</p>	

Chapter 18. Read the Upgrade Log File

About this task

After you run the upgrade script, make sure that the upgrade is successful.

Procedure

Read the upgrade log located in the *Engineinstall_dir*\logs folder in the Engine installation directory.

Following is a sample log message:

```
21 Apr 2010 13:09:30,746 5281 [main]
WARN com.sterlingcommerce.server1.tools.gis.conversion.GISConverter
- General warning(s)occurred, upgrade process stopped.
```

A message includes the following information:

Field	Description	Sample Message Text
Date and timeStamp	The date when the message is written.	21 Apr 2010 13:09:30
Process ID	An ID assigned to the message.	746 5281
Message type	The type of message written: INFO or WARN. Use the WARN messages to troubleshoot a conversion problem.	WARN
Program module	The module that generated the warning.	com.sterlingcommerce. server1.tools.gis. conversionGISConverter
Message text	A description of the informational message or warning.	General warning(s) occurred, upgrade process stopped.

Following are some of the warning messages that are written to the upgrade log. Use the messages to troubleshoot any problems that occur:

Warning Message	Description
DEPENDENCY CHECK WARNING: Netmap inbound node nodename is missing key certificate certificatename	The key certificate referenced in the netmap inbound node is missing. If you specify the -d argument on the command line, the items available in the export file will be converted to version 3.x and can be used. However, you must import the certificate into Sterling Secure Proxy 3.x before you are ready for a production environment.
Warning	A problem occurred when an item was converted to the version 3.x format.
GENERAL WARNING: Engine host and/or port is not provided for newengine, using default values.	You did not define a host and port argument for the engine you created. You must use CM to update the Engine before you are ready for production. Refer to <i>Validate the Converted Components in Sterling Secure Proxy Version 3.x</i> .

Warning Message	Description
General warning(s) occurred. Upgrade process stopped.	Warnings cause the upgrade process to stop. If you want the upgrade process to continue even when warnings occur, use the -w argument.
Upgrade process begins saving configuration with warnings	The -w argument was used on the command line.
WARN:General warning (s) ignored	The -w argument was used on the command line. Even though a warning occurred the conversion continues. Be sure to validate your configuration before you move to a production environment.
Upgrade is completed successfully.	The export file was successfully converted to version 3.x format.
Validation of C:\source\temp\ssp2.0.2export\ exportfile.xml is completed	The export file has been validated.
General exception(s) occurred.	The export was stopped because a warning occurred.

Chapter 19. Copy an Adapter

About this task

When you upgrade a cluster environment, you define multiple engines. One engine is the primary engine and performs the main workload. Each additional engine performs the work, if the primary engine is unavailable. Configuration must be the same at all engines in the cluster. Engines can share configuration files for netmaps, policies, user stores, trust stores, and keystores. They cannot share adapter configuration files because each adapter is associated with one engine.

To ensure that information is the same at each engine, create a copy of each adapter defined at the primary node. Then, associate the copy of the adapter with the new engine.

To copy an adapter definition and associate it with a secondary engine:

Procedure

1. If necessary, select **Configuration** from the menu bar.
2. Expand the **Adapters** tree and select the adapter to copy.
3. Select **Actions > Copy Selected**.

A new item is renamed to *CopyofAdapterName*, where *AdapterName* is the name of the original adapter.

4. Rename the adapter. Be sure to remove the name of the primary engine and replace it with the name of the engine you are configuring.
5. From the **Engine** drop-down list, select the name of the engine you are configuring.
6. Click **Save**.
7. Repeat this process for every adapter that you want to use with this engine.

Chapter 20. Validate an Engine Definition

About this task

When you run the upgrade script, you identified an engine in the engine name parameter. If the upgrade was successful, an engine definition is now available in Sterling Secure Proxy 3.x.

- If you specified the `-enginehost` and `-engineport` arguments in the upgrade script, the engine is ready to use. Use this procedure to validate the engine definition to make sure that the host and port values are correct.
- If you did not specify the `-enginehost` and `-engineport` arguments in the upgrade command, an engine is defined but it does not have a valid host and port value. Use this procedure to define the host and port associated with the engine.

If necessary, gather the following information and use it as you configure the engine:

CM Field	Feature	Value
Engine Name	Name of the engine	
Engine Host	IP address of the engine	
Engine Listen Port	Port number of the engine	

To validate an engine definition:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the **Engines** tree and click the engine to validate.
3. Check the following values and change them as needed:
 - **Engine Host**
 - **Engine Listen Port**
4. Click **Save**.

Chapter 21. Validate an Adapter

About this task

When you perform an upgrade, version 2.0.x adapters are converted to 3.x. Before you use the adapters in a version 3.x production environment, open each adapter and validate the settings.

To view an adapter definition:

Procedure

1. If necessary, select **Configuration** from the menu bar.
2. Expand the **Adapters** tree and select the adapter to view.
3. View the configuration for the adapter. If necessary, modify the configuration.
Refer to the online help for a description of each field and valid values.
4. Click **Save**.
5. Click **OK**.

Chapter 22. Validate a Perimeter Server Definition for a More Secure Zone

About this task

To validate a perimeter server definition when the perimeter server is in a more secure zone:

Procedure

1. From CM, click **Advanced** from the menu bar.
2. Click the **Perimeter Servers** tree to expand it.
3. Click **More Secure Zone** to view the more secure PS definitions.
4. Click the more secure perimeter server to validate.
5. Make sure that the **Proxy Local Listen Port** is correctly defined.
6. Click **Save**.

Chapter 23. Validate a Perimeter Server Definition for a Less Secure Zone

About this task

To validate a perimeter server definition when the perimeter server is in a less secure zone:

Procedure

1. From CM, click **Advanced** from the menu bar.
2. Click the **Perimeter Servers** tree to expand it.
3. Click **Less Secure Zone** to view the less secure perimeter server definitions.
4. Click the less secure perimeter server to validate.
5. Make sure that the **Perimeter Server Host** and **Perimeter Server Port** are correct.
6. Click **Save**.



Chapter 24. Validate the Connection Between Engines and CM

About this task

After you ensure that the engine definition is valid, use the following procedure to make sure that the engine can connect to CM.

To validate engine connections:

Procedure

1. Click **Monitoring** from the menu bar.
2. Click **Engine Status (All)**. A list of all configured engines is displayed, including the status. Status is displayed as follows:
 -  Engine is running
 -  Engine is not running
3. Make sure that the engine is running.

Chapter 25. Maintain Changes to HTTP Properties

About this task

You had the ability to modify the following properties for version 2.0.x HTTP adapters in the *install_dir/properties/httpproxy.properties* file:

- Common exploits that are blocked for an adapter (blockexploit)
- Commands allowed (http.commands.allowed)
- Commands prohibited (http.commands.prohibited)
- Maximum length of an HTTP header in an incoming HTTP request (httpMaxHeaderFieldLength)
- Maximum number of HTTP headers allowed in the incoming HTTP request (httpMaxNumHeaderFields)

Modified properties are not maintained when you convert to version 3.x.

Note: In 2.0.x, the properties applied to all HTTP adapters. In version 3.x, properties are defined for each adapter.

To maintain HTTP property changes in version 3.x:

Procedure

1. Write down the changes you made to HTTP properties in version 2.0.x:

Property	Change
Exploit to Block	
Additions to methods allowed	
Additions to prohibited methods	
Maximum length of an HTTP header	
Maximum number of HTTP headers allowed	

2. Open CM version 3.x.
3. From the **Configuration** panel, expand the **Adapters** tree and click the adapter to modify.
4. On the **HTTP Adapter Configuration** panel, click the **Properties** tab.
5. To edit an existing value, type the new value in the **Value** field.
6. To delete an item, click the radio button to the left of an item and click **Delete**.
7. To add a new item, click **New**.
8. Modify one of the properties as required:
 - To add a block common exploits value, type `block.exploit.strings.n` as the **Key** value, where *n* is a unique number appended to the `block.exploit.strings` key. Be sure that you increment the number and do not duplicate an existing key. Type the value to block in the **Value** field.

- To add an HTTP command allowed, type `http.commands.allowed` in the **Key** value. Type the commands to allow in the Value field.
 - To add an HTTP command prohibited, type `http.commands.prohibited` in the **Key** value. Type the commands to prohibit in the Value field.
 - To modify the maximum header fields length allowed, type `httpMaxHeaderFieldLength` in the **Key** value. Type the maximum header length in the Value field.
 - To modify the maximum number of header fields allowed, type `httpMaxNumHeaderField` in the **Key** value. Type the maximum header value in the Value field.
9. Click **OK**.
 10. Click **Save**.
 11. Repeat steps 3 through 10 for each adapter you want to update.

Chapter 26. New Properties in Version 3.x HTTP Adapter

New properties are defined in version 3.x for the HTTP adapter. These properties have default values that may change the behavior of an adapter. If necessary, change one or more of these properties for your environment. Properties include:

- `max.ps.client.threads`-Maximum number of threads in the pool used during a connection with a client. Default value is 10.
- `max.ps.server.threads`-Maximum number of threads in the pool used during a connection with a server. Default value is 10.

Chapter 27. Maintain Changes to FTP Properties

About this task

You had the ability to modify the following FTP adapter properties for version 2.0.x in the *install_dir*/properties/httpproxy.properties file:

- Commands allowed in the ftp.commands.allowed string
- Commands prohibited in the ftp.commands.prohibited string

Modified values for these properties are not maintained when you convert to version 3.x.

Note: In 2.0.x, the properties applied to all HTTP adapters. In version 3.x, properties are defined for each adapter.

To maintain FTP property changes in version 3.x:

Procedure

1. Write down the changes you made to FTP properties in version 2.0.x.

Property	Change
Additions to methods allowed	
Additions to prohibited methods	

2. Open CM version 3.x.
3. From the **Configuration** navigation panel, expand the **Adapters** tree and click the FTP adapter to modify.
4. On the **FTP Adapter Configuration** panel, click the **Properties** tab.
5. To edit an existing value, type the new value in the **Value** field.
6. To delete an item, click the radio button to the left of an item and click **Delete**.
7. To add a new item, click **New**.
8. Modify one of the properties as required:
 - To add an FTP command allowed, type ftp.commands.allowed in the **Key** value. Type the command to allow in the Value field.
 - To add an FTP command prohibited, type ftp.commands.prohibited in the **Key** value. Type the command to prohibit in the Value field.
9. Click **OK**.
10. Click **Save**.
11. Repeat steps 3 through 10 for each adapter you want to update.

Chapter 28. New FTP Adapter Properties in Version 3.x

New FTP adapter properties are defined in version 3.x. These properties have default values that may change the behavior of an adapter. If necessary, change one or more of the following properties for your environment:

- `max.ps.server.threads`-Maximum number of threads in the pool used during a connection with a server. Default value is 10.
- `ftp.ssl.pbsz.required`-Identifies whether the SSL command, PBSZ, is required. Valid values include Y|Yes|y|No|N|n. The default is Y.
- `ftp.ssl.prot.required`-Identifies whether the SSL command, PROT, is required. Valid values include Y|Yes|y|No|N|n. The default is Y.
- `max.ps.client.threads`-Maximum number of threads in the pool used during a connection with a client. Default value is 10.
- `ftp.max.command.length`-Maximum length allowed for a client command. The default is 1024. The command length is unlimited if this parameter is set to 0. If this length is exceeded, an error is logged and the connection is closed.
- `ftp.max.response.length`-Maximum length allowed for a server ftp response. The default is 4096. The server ftp length is unlimited if the parameter is set to 0. If this length is exceeded, an error is logged and the connection is closed. Set this parameter to 0 when communicating with a z/OS FTP server.

Chapter 29. Implement Property Changes Made to a Sterling Connect:Direct Adapter

About this task

You had the ability to modify properties for a Sterling Connect:Direct adapter in Version 2.0.x. If you made changes, they are not maintained when you upgrade to version 3.x. Properties that may be modified include:

- CDSP|BreadCrumbAddress=granted-By default, this property is set to granted to allow information to be added to messages and identify the presence of a proxy in a communications session. You may have changed this value to denied to prevent proxy information from being added to a message.
- CDSP|BreadCrumbAddressTransparentContent=wishboneHoast-Identifies the string that is placed in the Sterling Connect:Direct FMH message if BreadCrumbAddress is set to denied. If BreadCrumbAddress is set to granted, information about the adapter is placed in the FMH message.

To implement Sterling Connect:Direct property changes in version 3.x:

Procedure

1. Identify the changes you made in version 2.0.x. Write down the changes below:

Property	Change
Connect:Direct property changes	

2. Open CM version 3.x.
3. From the Configuration navigation panel, expand the **Adapters** tree and click the Sterling Connect:Direct adapter to modify.
4. On the **Connect:Direct Adapter Configuration** panel, click the **Properties** tab.
5. Click **New**.
6. Type the property string in the **Key** field and the value in the **Value** field.
7. Click **OK**.
8. Click **Save**.

Chapter 30. Change How Many Times a User Can Attempt to Log In Before a Lock Occurs

About this task

You can modify the lock out parameter for HTTP and FTP in Sterling Secure Proxy 2.0.x to change how many consecutive times a user can attempt to log in before being locked out. Any changes made to this parameter are not maintained when you upgrade to version 3.x. In addition, version 3.x changes the behavior of a user lockout. In version 2.0.x, the user remained locked out until you unlocked the account. In version 3.x, you define a lockout duration. When the lockout duration elapses, starting from the last failed login attempt, the user can then access Sterling Secure Proxy. For each user store that you define, you must identify the lockout duration and the user lockout threshold.

To change how many times a user can attempt to log in before a lock occurs and how long to lock out a user:

Procedure

1. Write down the value you assigned to log in attempts allowed in Sterling Secure Proxy version 2.0.x. This value is defined in the `maxConsecutiveAuthAttempts` property in the `ftpproxy.properties` and `httpproxy.properties` files located in the `install_dir/properties` directory.

Property	Value
Value of Log In Attempts Allowed	

2. Open CM version 3.x.
3. Click **Credentials** on the menu bar.
4. Expand the **User Store** tree and click the user store where user definitions are defined. The default user store is `defUserStore`.
5. Set the user attempts allowed in the **User Lockout Threshold** field.
6. Identify how long a user is locked out in the **User Lockout Duration** field.
7. Click **Save**.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

1623-14, Shimotsuruma, Yamato-shi

Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be

incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

J46A/G4

555 Bailey Avenue

San Jose, CA 95141-1003

U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© IBM 2012. Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2012.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com)[®] are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at <http://www.ibm.com/legal/copytrade.shtml>.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium and the Ultrium Logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Connect Control Center[®], Connect:Direct[®], Connect:Enterprise[®], Gentran[®], Gentran[®]:Basic[®], Gentran:Control[®], Gentran:Director[®], Gentran:Plus[®], Gentran:Realtime[®], Gentran:Server[®], Gentran:Viewpoint[®], Sterling Commerce[™], Sterling Information Broker[®], and Sterling Integrator[®] are trademarks or registered trademarks of Sterling Commerce[™], Inc., an IBM Company.

Other company, product, and service names may be trademarks or service marks of others.



Printed in USA