Sterling Secure Proxy

Sterling Connect:Direct Proxy Configuration

Version 34

Sterling Secure Proxy

Sterling Connect:Direct Proxy Configuration

Version 34

Note

Before using this information and the product it supports, read the information in “Notices” on page 51.

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.

Contents

Chapter 1. Sterling Connect:Direct Proxy configuration overview

The Sterling Connect:Direct® configuration scenarios describe how to configure Sterling Connect:Direct protocol connections to and from the Sterling Secure Proxy engine with the Configuration Manager.

Attention: Configuration information must be available at the engine before communication sessions with Sterling Connect:Direct can be established.

Organization of the Sterling Connect:Direct Configuration Scenarios

The first scenario instructs you how to do a basic setup. Each successive scenario adds a security feature to the basic configuration. After you go through each scenario, test the connection to ensure that it is correctly configured. You determine your security needs and configure the security features applicable to your environment.

The scenarios include:

- Create a basic Sterling Connect:Direct configuration
- Add SSL/TLS support
- Configure PNODE-based routing
- Add local user authentication
- Copy data or run a program that is based on the success or failure of a Sterling Connect:Direct Process step
- Block Sterling Connect:Direct tasks from a PNODE

The remaining configuration scenarios require Sterling External Authentication Server Server, an optional security feature of Sterling Secure Proxy that must be configured independently of Sterling Secure Proxy. After Sterling External Authentication Server is configured, you can update your basic security definitions to enable Sterling Secure Proxy to connect to Sterling External Authentication Server to enforce the following advanced security features:

- Authenticate an inbound certificate or user with Sterling External Authentication Server
- Configure user mapping
- Configure certificate-based routing
- Perform user mapping to the SNODE with Sterling External Authentication Server

Additional procedures are provided to instruct you how to configure the following features:

- Define alternate nodes for failover support
- Enable action that is based on protocol errors

Chapter 2. Completing scenario worksheets

Before you configure each Sterling Connect:Direct scenario, gather the information and record it on the worksheet provided.

About this task

Complete worksheets as follows:

Procedure

1. Enter a value for each listed Sterling Secure Proxy feature. Fields that are listed in the worksheet are required.
2. Accept default values for fields that are not listed in the worksheet.
3. The worksheet identifies the Configuration Manager fields where you specify each value.

Chapter 3. Completing and testing configuration scenarios

Work through the sequence of Sterling Connect:Direct configuration scenarios in the order in which they are presented to add security features.

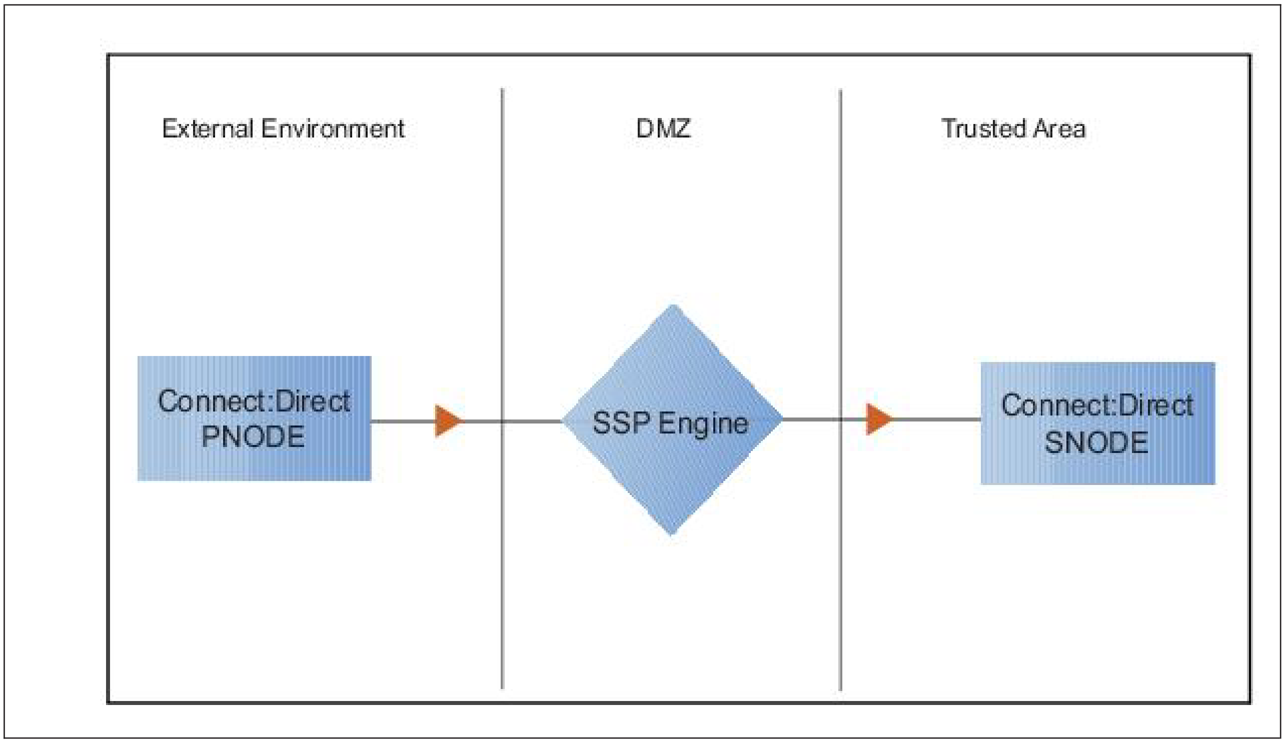
About this task

Be sure to test each feature before you add the next one to the configuration. Before you move Sterling Secure Proxy into production, ensure that you configure and test all security features you need for your environment.

Important: As you complete each task, provide all required information. If information is not provided or is incorrect, an error icon is displayed. To view more information about the error, hover over the icon.

Chapter 4. Create a Basic Sterling Connect:Direct Configuration

This scenario contains all the information and tools you need to configure Sterling Secure Proxy to establish a basic connection between Sterling Connect:Direct servers. Using default values, the PNODE presents a User ID to connect to the SNODE without Sterling External Authentication Server. As a result, no authentication occurs in Sterling Secure Proxy and the user ID presented by the PNODE is used to connect to the SNODE. The basic configuration uses standard routing to route connections to the node you define in the adapter. You are instructed on how to configure PNODE routing, mixed routing, and certificate-based routing in later scenarios.



Before you configure a Sterling Connect:Direct connection, make sure that an engine has been configured. Refer to *Install or Upgrade Sterling Secure Proxy on UNIX or Linux* or *Install or Upgrade Sterling Secure Proxy on Microsoft Windows* for instructions.

After you configure Sterling Secure Proxy, validate the configuration by initiating a Sterling Connect:Direct connection from the PNODE. For more information on testing the configuration, see *Test the Sterling Connect:Direct Connections*.

Complete the following tasks to define a basic Sterling Connect:Direct configuration:

- Create a policy
- Define Sterling Connect:Direct nodes in a netmap

- Define a Sterling Connect:Direct adapter

Basic Sterling Connect:Direct configuration worksheet

Before you configure Sterling Secure Proxy for Sterling Connect:Direct connections, gather the information about the basic Sterling Connect:Direct configuration worksheet. You use this information as you configure a basic Sterling Connect:Direct connection for Sterling Secure Proxy.

About this task

After you configure Sterling Connect:Direct connections, validate the configuration by initiating a Sterling Connect:Direct connection from the PNODE.

Procedure

1. Create a basic policy. In a later Sterling Connect:Direct configuration scenario, you edit this policy to add security features to it.

Configuration Manager Field	Feature	Value
Policy Name	Name of policy	

2. Create a netmap that contains connection information for the nodes that connect to and from Sterling Secure Proxy. For each node, associate a policy with the node.

Configuration Manager Field	Feature	Value
Netmap Name	Netmap name	
Sterling Connect:Direct Node Definitions		
Node Name	Name to assign to the Sterling Connect:Direct node definition	
Sterling Connect:Direct Server Address	Host name or IP address of the Sterling Connect:Direct server	
Sterling Connect:Direct Port	Listening port number of the Sterling Connect:Direct server	
Policy	Name of policy you create (Select from a pull-down list.)	
Node Name	Name to assign to the Sterling Connect:Direct node definition	
Sterling Connect:Direct Server Address	Host name or IP address of the Sterling Connect:Direct server	
Sterling Connect:Direct Port	Listening port number of the Sterling Connect:Direct server	

Configuration Manager Field	Feature	Value
Policy	Name of policy you create (Select from a pull-down list.)	

3. Create a Sterling Connect:Direct adapter that defines information necessary to establish Sterling Connect:Direct connections to and from Sterling Secure Proxy. When you configure the adapter, select the basic netmap and the Sterling Connect:Direct server where connections are routed and defined in the netmap definition.

Configuration Manager Field	Feature	Value
Name	Adapter name	
Listen Port	Listen port to use for inbound connections	
Netmap	Netmap to associate with the adapter	
SNODE Netmap Entry	Name of Sterling Connect:Direct node where the connection is routed	
Engine	Engine to run the Sterling Connect:Direct adapter on	

Creating a basic Sterling Connect:Direct policy

The policy defines how you impose controls to authenticate a Sterling Connect:Direct PNODE trying to communicate with a Sterling Connect:Direct SNODE over the public Internet.

About this task

The basic policy does not enforce any controls over the defined node. You add security controls when you define more advanced security settings.

To define a basic policy:

Procedure

1. Select **Configuration** from the menu bar.
2. Click **Actions** > **New Policy** > **C:D Policy**.
3. Type a **Policy Name**.
4. Click **Save**.

Creating a Sterling Connect:Direct netmap

You define connection information for every Sterling Connect:Direct node that communicates by using Sterling Secure Proxy. These values are stored in a netmap. The netmap is associated with a policy and an adapter.

About this task

Before you begin this procedure, create a policy to associate with the netmap.

To create a netmap and define Sterling Connect:Direct nodes:

Procedure

1. Select **Configuration** from the menu bar.
2. Click **Actions** > **New Netmap** > **C:D Netmap**.
3. Type a **Netmap Name**.
4. To define a Sterling Connect:Direct node definition, click **New**.
5. Specify the following values:
   - **Node Name**
   - **Connect:Direct Server Address or hostname**
   - **Connect:Direct Server Port (listening port)**
   - **Policy**

   Attention: If you did not define a policy, click the green plus sign to define one.
6. Click **OK**.
7. Repeat steps 3 through 5 for each node you want to define. Define at least one PNODE and at least one SNODE to establish a connection between two Sterling Connect:Direct nodes.
8. Click **Save**.

Version 3.4.1.7

What to do next

You can limit which SNodes that specific PNodes can communicate with by creating an Access Control List (ACL) for each PNode. Complete the following steps to create an ACL:

1. Check **Enable Access Control for Outbound connections**.
2. Select a node from the list of nodes.
3. Click **Edit**.
4. Click the **Outbound ACL** tab.
5. From the **Available Outbound Nodes:** list, select the nodes that you want the PNode to communicate with.
6. Click **Add** to move the selected nodes to **Authorized Outbound Nodes**.
7. Repeat steps 2 through 6 to create more ACLs.
8. Click **Save**.

   Attention: If you check **Enable Access Control for Outbound connections** and do not configure any ACLs, a warning message is displayed when you click **Save**. The netmap is successfully saved.

   Attention: If you do not check **Enable Access Control for Outbound connections** and configure one or more ACLs, Sterling Secure Proxy does not enforce the ACLs.

   Important: If you use standard routing to connect to Sterling Connect:Direct in the secure zone, you identify a primary server to connect to in the adapter. You can also identify up to three alternate outbound nodes for situations when the primary Sterling Connect:Direct server is not available. Two methods of configuring alternate server routing are available:

- Select a previously defined outbound node from the netmap–you must include this alternate outbound node in the ACL or the connection fails.
- Enter an IP address and port–the ACL is not applied to this alternate outbound node and the connection does not fail because of the ACL.
- If the ACL check fails on the primary outbound node, the Sterling Connect:Direct proxy adapter does not attempt connections with any of the specified alternate nodes.
- If the ACL check fails on any specified alternate node, the Sterling Connect:Direct proxy adapter attempts connections with the remaining alternate nodes.

Defining the Sterling Connect:Direct adapter used for the connection

A Sterling Connect:Direct adapter definition specifies system-level communications information necessary for Sterling Connect:Direct connections through Sterling Secure Proxy.

About this task

Before you begin this procedure, create a netmap and an engine to associate with the adapter.

To define a Sterling Connect:Direct adapter:

Procedure

1. Select **Configuration** from the menu bar.
2. Click **Actions** > **New Adapter** > **C:D Proxy**.
3. Specify values for the following fields:
   - Name
   - Listen Port
   - Netmap
   - SNODE Netmap Entry
   - Engine
4. Click **Save**.

What you defined with the basic Sterling Connect:Direct configuration scenario

Creating connections between Sterling Connect:Direct nodes when you route them through Sterling Secure Proxy requires that you organize information about the Sterling Connect:Direct nodes in a policy, a netmap, and an adapter definition. You created these items when you defined the basic Sterling Connect:Direct configuration.

The next step is to test the configuration to ensure that the connections work. Before you test the configuration, be sure that:

- The Sterling Connect:Direct SNODE server has a definition in its netmap for the Sterling Connect:Direct PNODE. For Sterling Connect:Direct for Microsoft Windows, set the netmap.check parameter to N.

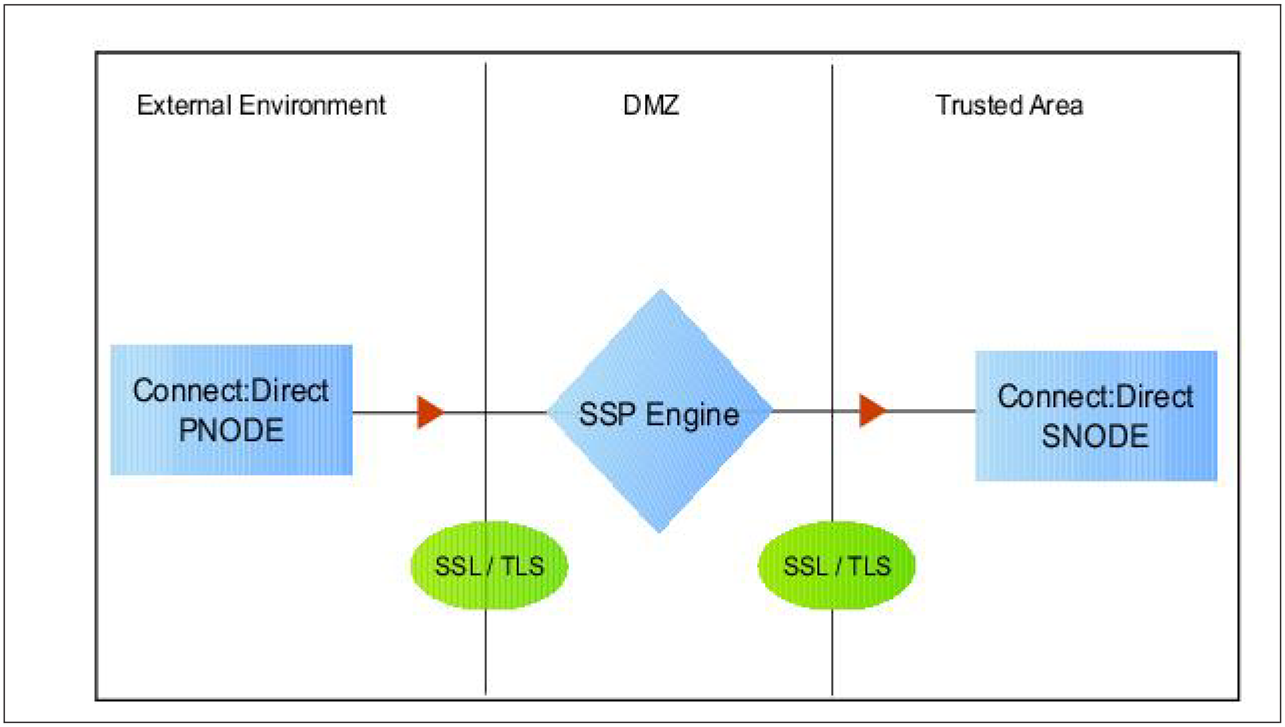
- The PNODE server has a definition in its netmap for the SNODE, by using the IP address and port of the Sterling Secure Proxy server.
- The user ID and password that is provided by the PNODE are defined at the Sterling Connect:Direct SNODE.

Refer to *Test the Sterling Connect:Direct Connections* for information about testing the Sterling Connect:Direct proxy configuration that is outlined in this scenario.

You add complexity to your security configurations by using the procedures in the remaining scenarios. Modify the basic configuration to configure more complex authentication and certificate validation measures.

Chapter 5. Add SSL or TLS support

This scenario builds on the basic Sterling Connect:Direct configuration by enabling security for the nodes you defined in the netmap.



Adding SSL or TLS support to the netmap for the nodes involves selecting the following options for the connections:

- SSL or TLS Protocol
- Cipher suites
- Certificate stores and certificates

Add SSL or TLS support to the PNODE and the SNODE definitions. Set up Sterling Connect:Direct Secure Plus parameter files at both the SNODE and the PNODE servers. Obtain certificates for both sessions and check them into the certificate store. Then, test the connection.

Note: This procedure assumes that you checked in your certificates. For more information, see *About SSL/TLS certificates*.

SSL and TLS Support worksheet

Before you add SSL or TLS support to the connection information you created in the basic Sterling Connect:Direct configuration scenario, gather the information in the SSL and TLS Support worksheet. You use this information as you configure the inbound and outbound nodes for SSL or TLS support.

Select the security setting and cipher suites to be used to secure the connection. To require that the certificate common name is validated in a certificate that is presented, enable this option and identify the common name value to check. Select the key or system certificate to use to validate the connection.

Configuration Manager	Feature	Value
Node Name	Name of the node to add security to	Select a node definition that you already defined
Use Secure+	Enable this option to enable security checking	Enabled
Verify Common Name	Enable this option to enable common name checking. This feature is optional.	
Certificate Common Name	Value of common name in certificate that is presented, if **Common Name Checking** is enabled.	
Security Setting	Security protocol to use. Options include **SSL**, **TLS**, or **The PNODE host controls SSL Protocol**.	
Trust Store	Name of the store for the CA certificate or trusted root certificate.	
CA Certificates/Trusted Root	Name of CA certificate or trusted root	
Key Store	Name of the store for the key or system certificate is stored.	
Key/System Certificate	Name of the Sterling Secure Proxy system certificate that is presented to the Sterling Connect:Direct server.	
Available Cipher Suites	Select the ciphers to enable by moving them from the **Available Cipher Suites** to the **Selected Cipher Suites** field.	

Securing the Sterling Connect:Direct connection by using the SSL or TLS protocol

The first step to strengthen security is to secure the communications channel. This procedure describes how to enable the SSL or TLS protocol for the Sterling Connect:Direct connections to and from Sterling Secure Proxy in a netmap you created in the basic configuration.

About this task

To require that Sterling Secure Proxy perform common name checking, enable this option and identify the common name in the configuration.

Before you can configure this option, you must obtain the necessary certificates and place them in the Sterling Secure Proxy Cert Store. Refer to*About SSL/TLS certificates* for instructions.

To enable the SSL or TLS protocol:

Procedure

1. Select **Configuration** from the menu bar.
2. Expand the **Netmaps** tree and select a netmap to modify.
3. Select a node to modify, and click **Edit**.
4. Click the **Security** tab, and then click **Use secure+ to enable security**.
5. To enable common name checking:
    a. Click **Verify Common Name**.
    b. Type the certificate common name in the **Certificate Common Name** field.
6. Select values for the following fields:
    - **Security Setting**
    - **Trust Store**
    - **CA Certificates/Trusted Root**

      Important: Be sure to highlight the certificate to select. If only one certificate is displayed in the field, it is not selected until you highlight it.
    - **Key Store**
    - **Key/System Certificate**
    - **Selected Cipher Suites**
7. Click **OK**.
8. Click **Save**.
9. Establish a session that is initiated by a Sterling Connect:Direct PNODE to test the configuration.

Variation on the add SSL or TLS support configuration

After you confirm that the communications session you established by using the Add SSL or TLS Support scenario was successful, you can further modify your configuration. After you test the SSL or TLS configuration, you can configure the environment to allow the inbound and outbound sessions to use different levels of encryption.

Configuring different levels of encryption for the inbound and outbound nodes

You can configure one level of encryption between the PNODE and Sterling Secure Proxy and another level of encryption between Sterling Secure Proxy and the SNODE.

About this task

In a Sterling Connect:Direct environment where Sterling Secure Proxy is not being used, one session is established between an SNODE and a PNODE. In the Sterling Secure Proxy environment, a session break is created; therefore, two sessions are established: one between the PNODE and Sterling Secure Proxy and another between Sterling Secure Proxy and the SNODE. To use the same protocol on both sessions, use the default settings.

Complete this procedure to define one protocol for the inbound node and a different protocol for the outbound node. This function is useful when you want to secure the inbound connection but allow a nonsecure session between Sterling Secure Proxy and the outbound node.

To enable different levels of encryption for the inbound and the outbound connection:

Procedure

1. Select **Configuration** from the menu bar.
2. Expand the **Adapter** tree, and select the adapter that you want to modify.
3. Click the **Advanced** tab.
4. Enable the **Inbound and outbound sessions can have different levels of encryption** option.
5. Click **Save**.

Chapter 6. Configure PNODE-based routing overview

This scenario builds on the basic Sterling Connect:Directconfiguration by enabling PNODE-based routing.

The basic configuration uses standard routing to determine where a connection is routed. If you configure standard routing, all sessions through an adapter are routed to the same connection. To allow a PNODE to determine what SNODE it connects to, configure PNODE-based routing. For PNODE-based routing, you must configure a node definition in the netmap for the PNODE and for all the SNODEs you route to.

Note: PNODE-based routing is supported for Sterling Connect:Direct for z/OS® version 4.6 or higher, Sterling Connect:Direct for UNIX version 3.8 or higher, and Sterling Connect:Direct for Microsoft Windows version 4.4 or higher.

PNODE-based routing worksheet

Before you add PNODE-based routing to the connection information you created in the basic Sterling Connect:Direct configuration scenario, gather the information in the PNODE-based routing worksheet. You use this information as you configure PNODE-based routing.

In the netmap you select, make sure that you have a node definition for the PNODE and for every node where the connection is routed.

Configuration Manager field	Feature	Value
Name	Adapter name	
Netmap	Netmap to associate with the adapter	
Listen Port	Adapter port number	
Routing Type	Routing type to use for this connection	PNODE-specified

Chapter 7. Configuring PNODE-based routing

You can configure Sterling Secure Proxy so that a Sterling Connect:Direct PNODE determines what SNODE it connects to with PNODE-based routing.

About this task

To configure a Sterling Connect:Direct adapter to use PNODE-based routing:

Procedure

1. Select **Configuration** from the menu bar.
2. Expand the **Adapter** tree and select the adapter that you want to modify.
3. Select **PNODE-specified** in the **Routing** field.
4. Click **Save**.

Chapter 8. Configure mixed routing

Mixed routing allows a PNODE to determine what SNODE it connects to. If the PNODE does not identify what SNODE to connect to, mixed routing then routes to the SNODE identified in the Sterling Secure Proxy configuration.

Before PNODE-based routing can be implemented, you must configure a node definition in the netmap for the PNODE and the SNODE.

Restriction: PNODE-based routing is supported for:

- Sterling Connect:Direct for z/OS version 4.6 or higher
- Sterling Connect:Direct for UNIX version 3.8 or higher
- Sterling Connect:Direct for Microsoft Windows version 4.4 or higher

Mixed routing worksheet

This scenario builds on the basic Sterling Connect:Direct configuration by enabling PNODE-based routing. Before you add PNODE-based routing to the connection information you created in the basic Sterling Connect:Direct configuration scenario, gather the information in the mixed routing worksheet. You use this information as you configure PNODE-based routing.

Make sure that you have a node definition for the PNODE and for the node where the connection is routed in the netmap you select.

Configuration Manager field	Feature	Value
Name	Adapter name	
Netmap	Netmap to associate with the adapter	
SNODE Netmap Entry	Name of Sterling Connect:Direct node where the connection is routed	
Routing Type	Routing type to use for this connection	PNODE-specified and then Standard (mixed)

Configuring PNODE specified and then standard (mixed) routing

You can configure Sterling Secure Proxy so that a Sterling Connect:Direct PNODE can determine what SNODE it connects to. If the PNODE does not specify the SNODE to connect to, the SNODE identified in the Sterling Secure Proxy configuration is used.

About this task

To configure a Sterling Connect:Direct adapter to use the PNODE specified and then standard (mixed) routing:

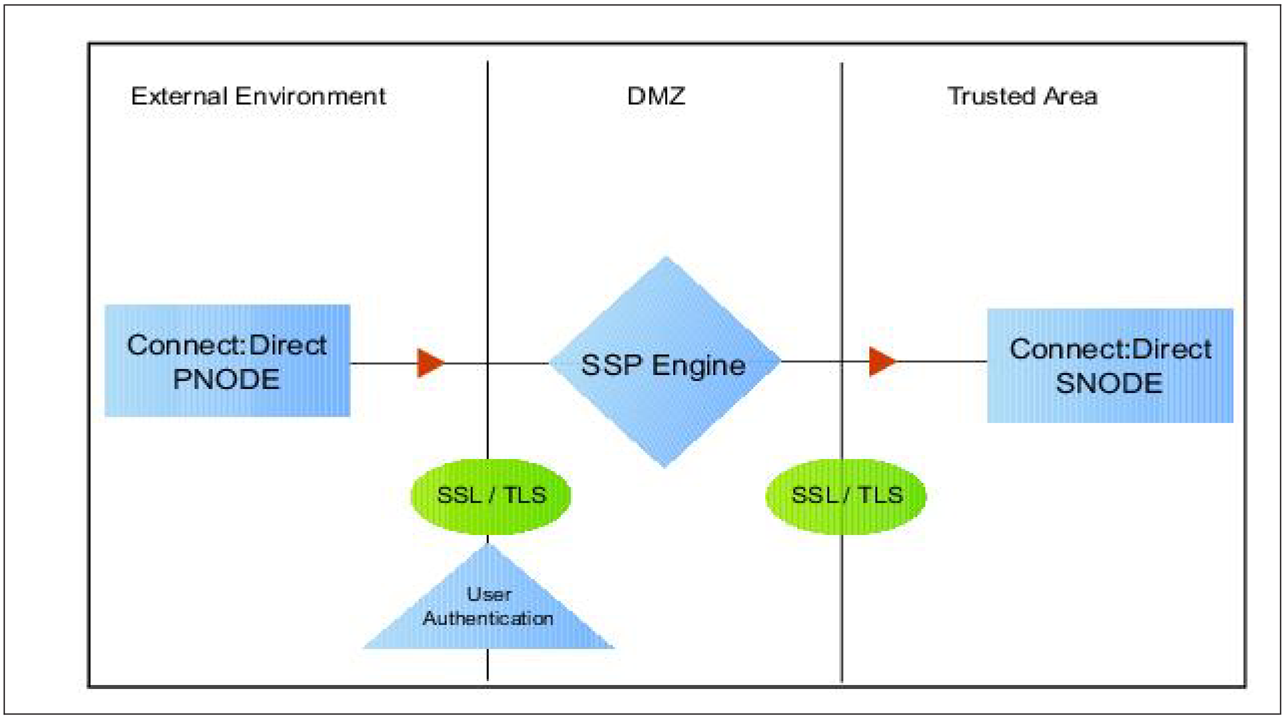
Procedure

1. Select **Configuration** from the menu bar.
2. Expand the **Adapter** tree and select the adapter that you want to modify.
3. Select **PNODE-Specified**, then **Standard (mixed)** in the **Routing Type** field.
4. Select the SNODE to route connections to in the **SNODE Netmap Entry** field.
5. Click **Save**.

Chapter 9. Add local user authentication to a Sterling Connect:Direct connection

This scenario builds on the basic Sterling Connect:Direct configuration by adding local user authentication to the PNODE connection by using information that is defined in the local user store.

The user ID and password that is presented by the PNODE are authenticated against information that is stored in the local user store. The values must match before a connection is established. You must add this information to the local user store before you can test this scenario.



Adding user authentication to the PNODE connection defined in the basic Sterling Connect:Direct configuration involves enabling user authentication and specifying information about the PNODE.

After you configure local user authentication, validate the configuration by establishing a session that is initiated by a Sterling Connect:Direct PNODE.

Sterling Connect:Direct PNODE connection (local user authentication) worksheet

Before you add local user authentication to the PNODE connection you created in the basic Sterling Connect:Direct configuration scenario, gather the information in the Sterling Connect:Direct PNODE connection (local user authentication) worksheet. Use this information as you configure user authentication for the PNODE connection.

In this scenario, you edit the policy that you created in the Sterling Connect:Direct basic configuration scenario and enable user authentication. You also add a user ID and password for the Sterling Connect:Direct PNODE to the default user store.

Configuration Manager Field	**Feature**	**Value**
Policy Name	Name of policy that is associated with the inbound node	
User Authentication	Method to use to authenticate the inbound node	Through local user store
User Store	Name of the user store you create	
User Name	Name of the user you define in the User Store	
Password Confirm Password	The password value to use to validate the inbound connection	

Chapter 10. Adding user authentication to the Sterling Connect:Direct inbound connection

You can strengthen the security of Sterling Connect:Direct PNODE connections by enabling local user authentication.

About this task

This procedure describes how to configure local user authentication.

Attention: Check the netmap to ensure that the policy you select is associated with the PNODE you want to authenticate.

To add local user authentication for a PNODE connection:

Procedure

1. Select **Configuration** from the menu bar.
2. Expand the **Policies** tree and select a policy.
3. Click the **Advanced** tab.
4. Enable the **User Authentication Through Local User Store** option.
5. Click **Save**.

Adding credentials to the local user store

If you enable user authentication through the local user store, you also add user information to the local user store. This user information is validated by Sterling Secure Proxy during a Sterling Connect:Direct client connection.

Before you begin

Before you begin this procedure:

- Enable user authentication for the inbound connection.
- Ensure that the engine is configured to use the user store that contains the user credentials.

About this task

To add user information to the local user store:

Procedure

1. Select **Credentials** from the menu bar.
2. Click **User Stores** to expand the list of user stores.
3. Select the default user store called **defUserStore**.
4. From the **User Store Configuration** panel, click **New**.
5. Specify values for the following fields:
   - **User Name**
   - **Password**
   - **Confirm Password**

6. Click **OK**.
7. Click **Save**.

Chapter 11. Copying data or running a program based on the success or failure of a Process step (step injection)

This scenario builds on the basic Sterling Connect:Direct configuration by adding step injection functions to the PNODE connection.

About this task

Step injection allows you to insert Sterling Connect:Direct Process statements into the communications session with the SNODE independent of the PNODE Process statements. These injected statements can provide real-time notification of file delivery, submit applications, run operating system jobs and commands, and submit other Sterling Connect:Direct Processes, all without needing to provide an exit program on the SNODE or without changing the PNODE Process. Even though the PNODE has no indication that these steps executed on the SNODE, step injection is defined on the PNODE record in Sterling Secure Proxy. The results of these steps are logged in the statistics file of the SNODE.

Procedure

To use step injection, define one or more of the following step injection functions:

- Copy session or certificate information to a file at the SNODE at the end of a successful step.
- Execute a Sterling Connect:Direct Runtask, Runjob, or Submit step on the SNODE at the end of a successful step or run operating system commands, jobs, or programs.
- Copy session or certificate information to a file at the SNODE at the end of a failed step.
- Execute a Sterling Connect:Direct Runtask, Runjob, or Submit step on the SNODE at the end of a failed step or run operating system commands, jobs, or programs.
- Use variables to define file names and parameters in a Runtask, Runjob, or Process step.

Results

Step Injection actions that are referenced in a netmap entry are only performed when the node is communicating as the PNODE in the transaction.

Configure a Step Injection

About this task

Before you can associate a step injection with a node, you must first define the actions to take in a step injection function.

To configure a step injection:

Procedure

1. Select **Advanced** from the menu bar.
2. Click **Actions** > **New C:D Step Injection**.

3. Type a step injection name.
4. Click the **Advanced** tab.
5. To copy information into a file at the SNODE:
   a. Take one of the following actions:
      - Enable **Copy on success** to copy information to a file after a successful Process copy statement has occurred.
      - Enable **Copy on failure** to copy information to a file after a Process copy statement has failed.

   b. Select the type of information to copy to the file in the Copy identifying information field. Options include:
      - Copy All Information
      - Copy Certificate Information
      - Copy Session Information

   c. Type the name of the file where the information is copied in the **Session information output file** field.

   d. Enter how many seconds to wait until the session is timed out in the **Tcp timeout for copy** field.
6. To execute a Runtask, Runjob, or submit another Sterling Connect:Direct Process or execute an operating system command or program at the SNODE:
   a. Take one of the following actions:
      - Enable **Execute on success** to perform an action after a successful Process copy statement.
      - Enable **Execute on failure** to perform an action created after a Process copy statement fails.

   b. Select the type of step to perform in the **Step selection** field. Options include Runtask, Runjob, or Submit a Sterling Connect:Direct Process or execute an operating system command or program.

   c. Define the step parameters to use. Refer to the Sterling Connect:Direct documentation for more information.

   d. Enter how many seconds to wait before the session is timed out in the **Tcp timeout for step** field.
7. Click **Save**.

Configure step injections worksheet

Before you create step injection definitions and associate them with a node definition you created in the basic Sterling Connect:Direct configuration scenario, gather the information in this worksheet. Use this information as you configure a node with step injection support.

Configuration Manager Field	Feature	Value
Step Injection Name	The name to assign to the step injection you define.	
Copy on success	Turn on this option to copy session-specific data to the SNODE at the end of a successful step.	Enabled? Yes or No

Configuration Manager Field	Feature	Value
Copy identifying information	The information to copy to the SNODE. This setting is required if you turn on Enable Copy on success.	Select one of the following options: • Copy All Information • Copy Certificate Information • Copy Session Information
Session information output file	Destination file on the SNODE where information is copied. Variables can be used to define the file name. Refer to *Use variables in a step injection definition*.	
Tcp timeout for copy	Number of seconds to wait for a request or response before Sterling Secure Proxy ends the session.	
Execute on success	Turn on this option to execute a Runtask, Runjob, or Submit with a Process at the end of a successful step or execute an operating system command or program.	Enabled? Yes or No
Step selection	The step type to execute when a successful step occurs.	Select one of the following options: • Runtask • Runjob • Submit
Step parameter	Type the parameters to use for the step. Variables can be used to define the parameters. Refer to *Use variables in a step injection definition*.	
Tcp timeout for step	Number of seconds to wait before timing out.	
Copy on failure	Turn on this option to copy session-specific data to the SNODE at the end of a failed step.	Enabled? Yes or No
Copy identifying information	Type of information to copy to the SNODE if a Process step is unsuccessful.	Select one of the following options: • Copy All Information • Copy Certificate Information • Copy Session Information
Session information output file	Destination file where the copy information is written. Variables can be used to define the file name. Refer to *Use variables in a step injection definition*.	
Tcp timeout for step	Number of seconds to wait before the copy instruction is timed out.	

Configuration Manager Field	Feature	Value
Execute on failure	Turn on this option to execute a Runtask, Runjob, or Submit Process on the SNODE as defined in a submitted Process at the end of a unsuccessful step or execute an operating system command or program.	Enabled? Yes or No
Step selection	Select the step type to execute when a successful step occurs.	Select one of the following options: • Runtask • Runjob • Submit
Step parameter	Define the parameters to use for the step. Variables can be used to define the parameters. Refer to *Use variables in a step injection definition*.	
Tcp timeout for copy	Identify how many seconds to wait before the copy instruction is timed out.	

Use Variables in a Step Injection Definition

When you configure a step injection function, you can use variables in the Session information output field and Step parameter field. These variables allow you to name output files or execute step parameters based on information obtained during the session. Use the following variables within a step injection action definition:

Variable	Description
${%DESTFILE%}	Destination file name defined in the Process. Example: Runtask - cmd (copy ${%DESTFILE%} C:\outout\sspfile\dest.txt)
${%DESTUID%}	Destination user ID defined in the Process.
${%DESTWPATH%}	Destination file name defined in the Process, including the path.
${%FROMNODE%}	The node that is sending the file. Returned values are P for PNODE or S for SNODE. Example: CopyonSuccess = C:\Output\copysuccessallinfo_${%FROMNODE%}_${ %SNODE%}_.txt
${%ORGININUID%}	User ID of the person who initiated the Process.
${%PNAME%}	Process name.
${%PNODE%}	Name of the PNODE that initiated the Process.
${%PNUM%}	Process number.
${%SNODE%}	Name of the destination SNODE name where the session is running.
${%SOURCEFILE%}	Source file name defined in the Process step.
${%SOURCEWPATH%}	Source file name defined in the Process step, including the path.

Variable	Description
${%STEPCOMPLETE%}	What time and date the step completed, in the format yyyyddd_hhmmsshh, where yyyy = year, ddd = day of year, hh =.hours, mm = minutes, ss = seconds, and hh = hundredths of seconds. **Note:** The hundredth of seconds field is not supported for all Sterling Connect:Direct platforms.
${%STEPMSG%}	A message ID.
${%STEPNAME%}	Name of the step.
${%STEPSTART%}	The time and date the step started, in the format yyyyddd_hhmmsshh, where yyyy = year, ddd = day of year, hh =.hours, mm = minutes, ss = seconds, and hh = hundredths of seconds. **Note:** The hundredth of seconds field is not supported for all Sterling Connect:Direct platforms.
${%TS%}	The time the session began, in milliseconds.
${%TSNOW%}	The current time, in milliseconds, in the format 1132599441883.

Associate a Step Injection With a Sterling Connect:Direct Node

About this task

After you configure step injection functions, you can then associate a step injection with a Sterling Connect:Direct node. Process steps are activated by a PNODE; therefore, step injection functions must be defined in a PNODE record.

To associate a step injection with a Sterling Connect:Direct node:

Procedure

1. Select **Configuration** from the menu bar.
2. Expand the Netmaps tree, and select the netmap that contains the PNODE definition you want to modify.
3. Select the node to modify and click **Edit**.
4. Select the step injection function to associate with the node from the **Step Injection** drop-down list. If you have not defined the step injection function, click ✓ and define a step injection. Refer to *Copy Data or Run a Program Based on the Success or Failure of a Process Step (Step Injection)* for instructions.
5. Click **OK**.
6. Click **Save**.

Chapter 12. Block Sterling Connect:Direct Tasks Allowed on a Node

About this task

This scenario builds on the basic Sterling Connect:Direct configuration by adding the capability to prevent Sterling Connect:Direct statements from being executed.

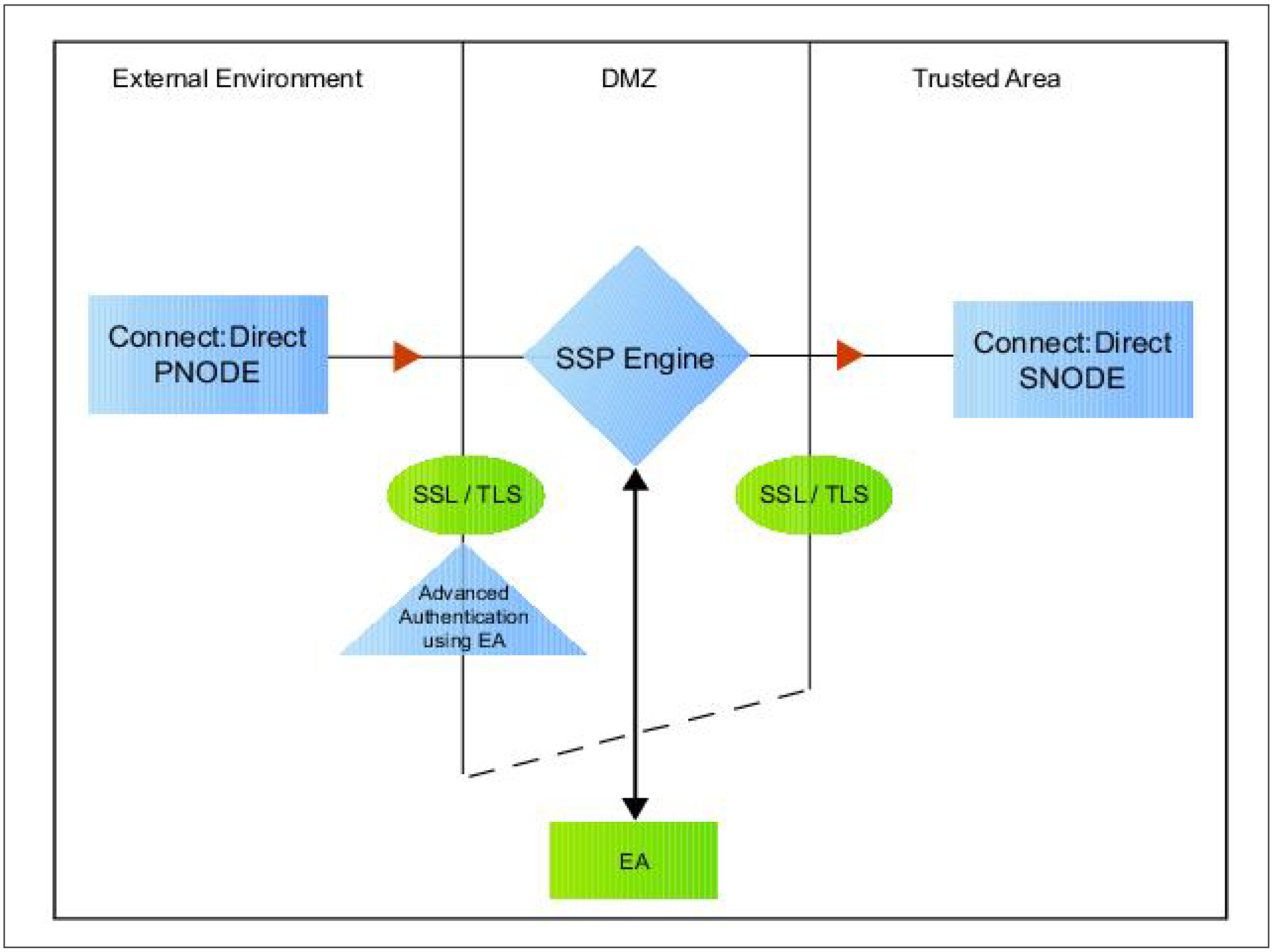
To prevent a Sterling Connect:Direct statement from being executed:

Procedure

1. Select **Configuration** from the menu bar.
2. Expand the **Policies** tree and click the policy to modify.
3. On the **Policy Configuration panel**, click the **Step Permissions** tab.
4. Click on one or more of the following tasks to disable the task:
   - Runjob step allowed
   - Runtask step allowed
   - Copy step allowed
   - Submit step allowed
5. Click **Save**.

Chapter 13. Strengthen User Authentication Using Sterling External Authentication Server

This scenario builds on the basic Sterling Connect:Direct configuration by adding user authentication to the PNODE connection using information defined in Sterling External Authentication Server. To provide a more advanced method of securing a Sterling Connect:Direct connection, use Sterling External Authentication Server such as, authenticating certificate information or user credentials presented by the inbound node or performing user ID and password mapping.



Authenticate an Inbound Certificate or User Using Sterling External Authentication Server

You can authenticate an inbound connection against information stored in an LDAP database by configuring Sterling External Authentication Server to define how the connection is authenticated. The Sterling External Authentication Server definition determines the options that are enabled. Refer to Sterling External Authentication Server Server help for a complete list of the functions that can be performed in Sterling External Authentication Server.

Authenticate a Certificate or User Using Sterling External Authentication Server - Worksheet

Use the following worksheet to identify the information needed to authenticate a Sterling Connect:Direct connection using information in Sterling External Authentication Server. Update the policy you created in the basic Sterling Connect:Direct configuration for this scenario.

Configuration Manager Field	Information	Value
Certificate Authentication - External Authentication Certificate Validation	Will you validate the certificate presented by the PNODE?	(Yes or No)
Certificate Authentication - External Authentication Profile	If yes, provide the Sterling External Authentication Server certificate validation definition.	
User Authentication - Through External Authentication	Will you validate user information?	(Yes or No)
User Authentication - External Authentication Profile	If yes, provide the Sterling External Authentication Server user validation definition.	

Authenticate a Sterling Connect:Direct Certificate or User Using Sterling External Authentication Server

About this task

To authenticate certificate information or user information about the Sterling Connect:Direct node against information stored in an LDAP database, you must configure Sterling External Authentication Server. After you configure Sterling External Authentication Server to enable certificate or user authentication, complete this procedure to configure Sterling Secure Proxy to use the authentication method you defined.

Before you configure Sterling Secure Proxy to use Sterling External Authentication Server to authenticate a node connection, obtain the name of the Sterling External Authentication Server definition.

In addition, ensure that the following procedures have been performed:

- The public keys for Sterling Secure Proxy have been sent to the Sterling External Authentication Server server and imported into the Sterling External Authentication Server keystore.
- The Sterling External Authentication Server server connection has been configured in Sterling Secure Proxy.

To configure authentication of a Sterling Connect:Direct node using Sterling External Authentication Server:

Procedure

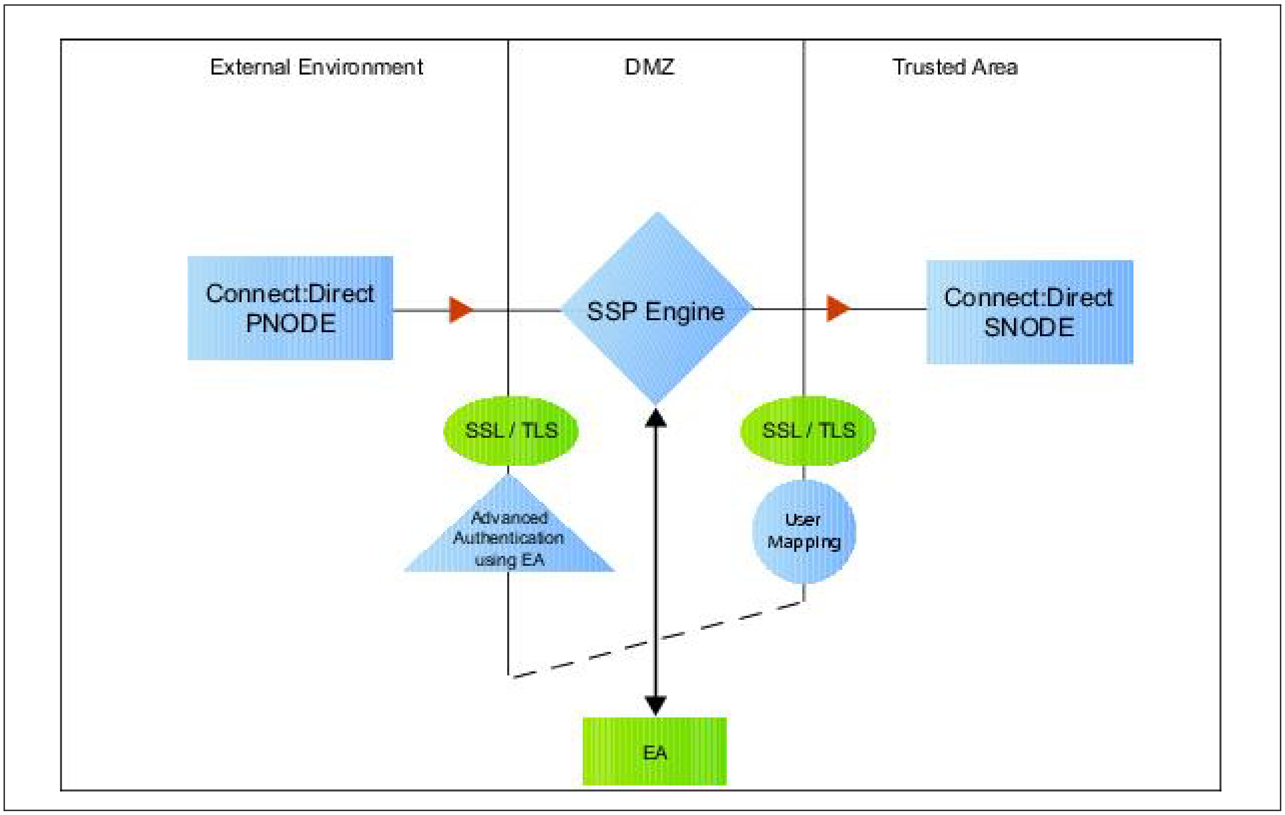
1. Select **Configuration** from the menu bar.
2. Expand the **Policies** tree and click the policy to modify.
3. On the **Policy Configuration** panel, click the **Advanced** tab.
4. Configure one or more of the following options:
   - To validate the certificate presented by the node against information defined in Sterling External Authentication Server, enable **Certificate Authentication - External Authentication Certificate Validation** and enter the name of the profile you defined in Sterling External Authentication Server in the **Certificate Authentication - External Authentication Profile** field.
   - To enable user authentication through Sterling External Authentication Server, enable **User Authentication - Through External Authentication** and type the name of the definition you defined in Sterling External Authentication Server in the **User Authentication - External Authentication Profile** field.
5. If you do not want to authenticate the user using information in the local user store, deselect the **Through Local User Store** option.
6. Click **Save**.

Results

You can now associate this policy with a Sterling Connect:Direct node where you want to perform user authentication using information stored in an LDAP database.

Chapter 14. Strengthen the Connection to the SNODE With User Mapping

This scenario builds on the basic Sterling Connect:Direct configuration by adding user mapping using information defined in Sterling External Authentication Server Server . To provide a more advanced method of a more advanced method of securing a Sterling Connect:Direct connection, use Sterling External Authentication Server to map a PNODE user ID and password or PNODE submitter ID to login credentials stored in Sterling External Authentication Server. The mapped login credentials are then used to connect to the SNODE.



Perform User Mapping Using Sterling External Authentication Server - Worksheet

Use this worksheet to identify the user mapping method to enable for the SNODE connection with information in Sterling External Authentication Server:

Configuration Manager Field	Feature	Value
Replace SNODEID with Userid mapped in External Authentication	The PNODE requires a user ID for access to the SNODE and the user ID provided is replaced with a value defined in Sterling External Authentication Server.	Enabled? Yes or No

Configuration Manager Field	Feature	Value
Replace submitter id with Userid mapped in External Authentication	The PNODE requires a submitter ID to access the SNODE. The submitter ID supplied by the PNODE is replaced by a valued defined in Sterling External Authentication Server.	Enabled? Yes or No
Destination Service Name	The name of the service. If no value is provided, the SNODE is used as the service name.	

Perform User Mapping Using Information Stored in Sterling External Authentication Server

About this task

If you store user credentials in an LDAP database, use this procedure to map a user ID and password, or a submitter ID provided by the SNODE, to information stored in Sterling External Authentication Server. Two methods are available:

- Replace the SNODE ID with information stored in Sterling External Authentication Server
- Replace the submitter ID

Destination Service Name needs to be selected on the Advanced tab of the Netmap Node screen of the PNODE. If Destination Service Name is not provided, the SNODE name is used.

Before you configure this option:

- Configure a definition in Sterling External Authentication Server.
- Obtain the name of the Sterling External Authentication Server definition.
- Configure a connection between Sterling External Authentication Server and the engine.

To configure user mapping:

Procedure

1. Select **Configuration** from the menu bar.
2. Expand the Policies tree and click the policy to modify.
3. On the **Policy Configuration** panel, click the **Advanced** tab.
4. To enable user authentication through Sterling External Authentication Server, enable the **User Authentication Through External Authentication** option and type the name of the definition you defined in Sterling External Authentication Server in the **External Authentication Profile** field.
5. Do one of the following:
   - To map the user ID presented by the PNODE to information in Sterling External Authentication Server, select **Replace SNODEID with UserId mapped in External Authentication**.
   - To map the submitter ID presented by the PNODE to information in Sterling External Authentication Server, select **Replace SubmitterID with UserId mapped in External Authentication**.

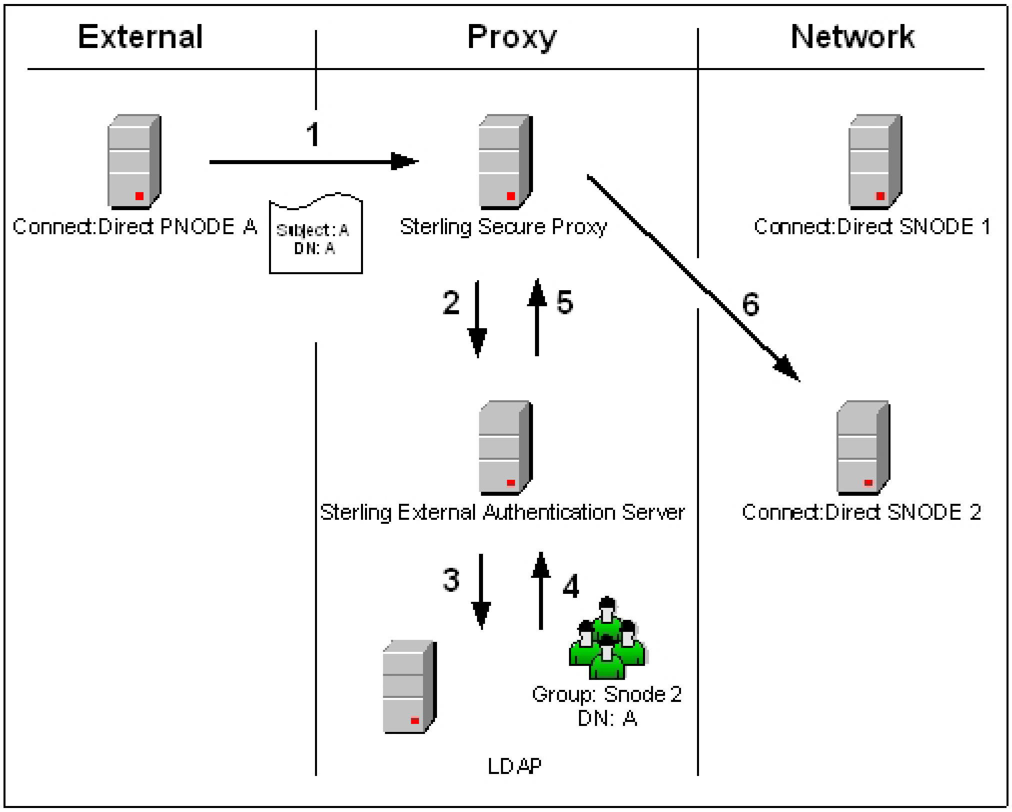
6. Click **Save**.
7. In the **Configuration** panel, expand the **Netmap** option and click the netmap to modify.
8. Select the PNODE to modify and click **Edit**.
9. Click the **Advanced** tab.
10. Type the name of the service in the **Destination Service Name** field. If no value is provided, the SNODE name is used as the service name.
11. Click **OK**.
12. Click **Save**.

Chapter 15. Configure Certificate-Based Routing

About this task

This scenario builds on the basic Sterling Connect:Direct configuration by configuring certificate-based routing. Certificate-based routing uses a routing name returned by Sterling External Authentication Server. It is associated with the subject distinguished name found in the PNODE certificate. Sterling Secure Proxy uses this routing name to determine the SNODE where the incoming Sterling Secure Proxy connection is routed. To perform certificate-based routing, modify an adapter you defined in the basic Sterling Connect:Direct configuration.

The following diagram illustrates the certificate-based routing function:



Summary of Certificate-Based Routing

Following are the steps performed during certificate-based routing:

1. The PNODE passes a certificate chain during an SSL/TLS session. This certificate includes several attributes, such as subject and distinguished name (DN).
2. Sterling Secure Proxy passes the certificate chain to Sterling External Authentication Server Server.
3. Using the configuration parameters in a certificate validation request, Sterling External Authentication Server attempts to match PNODE certificate attributes to the LDAP server and requests the associated routing value.

4. LDAP returns the routing value to Sterling External Authentication Server.
5. Sterling External Authentication Server passes the routing value to the Sterling Secure Proxy engine.
6. Sterling Secure Proxy routes the PNODE request to the SNODE using the routing value.

Configure Certificate-Based Routing in Sterling Secure Proxy

About this task

Before you test certificate-based routing, you must create a certificate validation request in Sterling External Authentication Server that includes an attribute query definition called Routing Names. This attribute query definition is created to retrieve a routing name value using certificate attributes as search criteria. You must also configure a connection between Sterling Secure Proxy and Sterling External Authentication Server.

Refer to *Configure Sterling Secure Proxy for Sterling External Authentication Server Server for instructions.*

To configure certificate-based routing:

Procedure

1. Select **Configuration** from the menu bar.
2. Expand the Adapters tree and select the adapter you want to modify.
3. Select Certificate-based in the **Routing Type** field.
4. Click **Save**.
5. Click the Netmap navigation panel, expand the Netmap tree, and select the Sterling Connect:Direct adapter that contains the SNODE where the connection are routed.
6. Select the node to modify and click **Edit**.
7. Type the routing value to be returned from the LDAP server in the **Routing Name** field. The routing name must exactly match the routing value returned from the LDAP server. This routing name identifies the SNODE for routing the PNODE request.
8. Click **OK**.
9. Click **Save**.
10. Configure Sterling Secure Proxy to enable certificate authentication using Sterling External Authentication Server. *Refer to Authenticate an Inbound Certificate or User Using Sterling External Authentication Server*.

Chapter 16. Test the Sterling Connect:Direct Connections

About this task

To verify that the engine can receive and initiate communications sessions, you have to establish a connection between a Sterling Connect:Direct PNODE and the engine, initiate a session from the engine to the Sterling Connect:Direct SNODE in the trusted zone, and review the Sterling Secure Proxy log for the results.

This procedure enables you to verify that the engine can:

- Establish a Sterling Connect:Direct session between a PNODE and Sterling Secure Proxy
- Initiate a session to a Sterling Connect:Direct SNODE on behalf of the Sterling Connect:Direct PNODE connection

To verify the communications sessions:

Procedure

1. View the secureproxy.log.
2. Confirm that the sessions were established, as shown in the following example.

```
21 Dec 2010 16:47:16,874 INFO [PASConduit1pnode] sys.NODE.CD_Netmap_Secure.ea
- protocol=cd sessid=111111111111 CSP004I 0 Pnode session established.
Pnode=ea_cd3800 HNIPP=server.company.com,10.20.20.200;45892 XMLErrPolicy=NONE
FMHUpdate=granted NMCheck=NA RTPolicy=Yes RJPolicy=Yes SBPolicy=Yes CPPolicy=Yes
S+Policy=SA_OPTIONAL ExecPolicy=EX_STRONG SessLimit=20 Routing=STD
CSList=TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,
CSSelected=RSA_WITH_AES_128_CBC_SHA PNCert=Serial number: 230 Issuer:O=SCI,
L=city, ST=Texas, C=US Subject:C=US, ST=Texas, O=SCI, OU=SV, CN=donnieaix,
EMAIL=user@company.com Not Valid Before:Mon Dec 04 11:41:55 CST
2006 Not Valid After:Thu Dec 01 11:41:55 CST 2016 Signature Algorithm:MD5withRSA
21 Dec 2010 16:47:17,490 INFO [PASConduit1pnode_3016_sessid=119827723531001]
sys.NODE.CD_Netmap_Secure.ea_cd3800
- protocol=cd sessid=11111 CSP005I 0 Snode session established with
Snode=ea_unix_cd3800 HNIPP=ea_unix;23564 XMLErrPolicy=NONE FMHUpdate=granted
NMCheck=NA RTPolicy=Yes RJPolicy=Yes SBPolicy=Yes CPPolicy=Yes S+Policy=SA_OPTIONAL
ExecPolicy=EX_STRONG SessLimit=20 Routing=STD
CSList=TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,
CSSelected=RSA_WITH_3DES_EDE_CBC_SHA SNCert=Serial number: 230 Issuer:O=company,
L=city, ST=Texas, C=US Subject:C=US, ST=Texas, O=SCI, OU=SV, CN=donnieaix,
EMAIL=qatest1024@stercomm.com Not Valid Before:Mon Dec 04 11:41:55
CST 2006 Not Valid After:Thu Dec 01 11:41:55 CST 2016 Signature Algorithm:MD5withRSA
21 Dec 2009 16:47:17,492 INFO [PASConduit1pnode_3016_sessid=119827723531001]
sys.NODE.CD_Netmap_Secure.ea_unix_cd3800 - protocol=cd sessid=119827723531001 CSP006I 0 Pnode/Snode proxy
session established. Pnode=ea_rhas40_cd3800
.
.
.
```

3. If your session was unsuccessful, review the log information to determine the likely cause of the failure and the corrective action to take.

Chapter 17. Additional Sterling Connect:Direct Configuration Options

Additional Sterling Connect:Direct configuration options support the following features:

- Define alternate nodes for failover support
- Configure IP Address Checking (Netmap Check)
- Record an error message or shutdown a connection based on protocol errors

Define Alternate Nodes for Failover Support

About this task

If you are using standard routing to connect to a Sterling Connect:Direct server in the secure zone, you identify a primary server to connect to in the adapter. The primary nodes are defined in the netmap. For each PNODE definition in the netmap, you can identify up to three alternate outbound nodes to connect to if the primary Sterling Connect:Direct server is not available.

Two methods of configuring alternate server routing are available.

- Select a previously defined outbound node from the drop-down list on the Netmap - Advanced tab. To configure this method, you first configure an outbound node definition in the netmap for each alternate node you want to use. Each connection uses the security and Sterling External Authentication Server settings defined for that outbound node in the netmap.
- Select IP address/port from the drop-down Node list on the Advanced tab and enter values for the IP address and port. If you use this method, you do not have to define the alternate outbound nodes in the netmap, and each alternate connection shares the security and Sterling External Authentication Server settings defined in the primary node definition.

If you configure alternate server definitions in the PNODE definition, when a connection to the primary outbound node is unsuccessful Sterling Secure Proxy tries to connect to the alternate node you defined as Node 1. If the connection to the first alternate node is unsuccessful, Sterling Secure Proxy tries to connect to the second alternate node, Node 2 and then to the third alternate, Node 3. If all are unsuccessful, the inbound connection fails.

To configure alternate outbound connections:

Procedure

1. Select **Configuration** from the menu bar.
2. Expand the **Netmaps** tree and click the netmap to modify.
3. Select the node to modify and click **Edit**.
4. Click the **Advanced** tab.
5. To identify an alternate node that is defined in the netmap and use the security settings defined in the alternate node definition, select the outbound node name from the drop-down list.
6. To configure an alternate node that is not in the netmap and use the security settings defined in the primary node definition:

   a. Select **Address/Port** from the drop-down list in the **Alternate Destinations Node** field.
   b. Provide the **IP Address** and **Port number** for the alternate outbound node.
7. Click **OK**.
8. Click **Save**.

Configure IP Address Checking (Netmap Check)

About this task

Once netmap checking is enabled in your Sterling Connect:Direct Proxy configuration, you can add additional IP addresses to your Sterling Connect:Direct netmap for IP address checking. For each PNODE definition in the netmap, you can identify up to 50 additional IP addresses to use for IP address checking.

Two types of additional IP addresses are available for IP address checking:

- Sterling Secure Proxy can use up to three alternate outbound nodes in your netmap for IP address checking. The alternate outbound nodes can be used for inbound IP address checking and outbound failover node addresses. To configure alternate outbound nodes, refer to *Define Alternate Nodes for Failover Support*.
- If you need more than three additional addresses for IP Address Checking, configure IP check addresses in the Sterling Connect:Direct netmap. Sterling Secure Proxy uses these IP check addresses for inbound IP address checking only. They cannot be used for outbound failover support.

To configure IP check addresses:

Procedure

1. Select **Configuration** from the menu bar.
2. Expand the Netmaps tree and select the netmap to modify.
3. Select the Sterling Connect:Direct node that you want to add IP addresses to and click Edit.
4. Click the **IP Checks** tab.
5. If there are existing IP addresses in the Additional IP Checks table, click **New** to add a new blank record to the table.
6. Type the additional IP address in the table. To add another IP address, click **New**.

   Note: Before you navigate to another page in the Additional IP Checks table, click **OK** to save your last IP address entry.
7. When you finish adding IP addresses, click **OK** at the bottom of the page.
8. Click **Save**.

Record an Error Message or Shut Down a Connection Based on Protocol Errors

About this task

To write a warning message to the log file or shut down a connection when a protocol violation occurs during a file transfer, enable this function in the Policy definition.

To enable an action based on a protocol error:

Procedure

1. Select **Configuration** from the menu bar.
2. Expand the **Policies** tree and select the policy to modify.
3. Select the action to take on a protocol error in the **Protocol Error Action** field.
4. 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.

19-21, Nihonbashi-Hakozakicho, Chuo-ku

Tokyo 103-8510, 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 2013. Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2013.

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

Trademarks

IBM, the IBM logo, and 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.

Product Number: 5725-D03

Printed in USA