Troubleshooting a SIP Federation Integration

This section explains the method to Troubleshoot a SIP Federation Integration.

Common Cisco Adaptive Security Appliance Problems and Recommended Actions

This section provides information on the Common Cisco Adaptive Security Appliance Problems and Recommended Actions.

Certificate Configuration Problems

Certificate Failure Between the IM and Presence Service and Cisco Adaptive Security Appliance

The certificate configuration between the IM and Presence Service and Cisco Adaptive Security Appliance is failing.

The time and time zones on the Cisco Adaptive Security Appliance may not be configured correctly.

- Set the time and time zones on the Cisco Adaptive Security Appliance.
- Check that the time and time zones are configured correctly on the IM and Presence Service and Cisco Unified Communications Manager.

Prerequisite Configuration Tasks for this Integration

Certificate Failure Between the Cisco Adaptive Security Appliance and Microsoft Access Edge

The certificate configuration between the Cisco Adaptive Security Appliance and Microsoft Access Edge is failing at certificate enrollment on the Cisco Adaptive Security Appliance.

If you are using SCEP enrollment on the Cisco Adaptive Security Appliance, the SCEP add-on may not be installed and configured correctly. Install and configure the SCEP add-on.

Related Information

CA Trustpoints

Certificate Error in SSL Handshake

A certificate error displays in the SSL handshake.

There is no FQDN in the certificate. You need to configure the domain on the IM and Presence Service CLI, and regenerate the certificate on IM and Presence Service to have a FQDN. You need to restart the SIP proxy on the IM and Presence Service when you regenerate a certificate.

Error When Submitting a Certificate Signing Request to VeriSign

I am using VeriSign for certificate enrollment. When I paste the Certificate Signing Request into the VeriSign website, I get an error (usually a 9406 or 9442 error).

The subject-name in the Certificate Signing Request is missing information. If you are submitting a renewal certificate signing request (CSR) file to VeriSign, the subject-name in the Certificate Signing Request must contain the following information:

- Country (two letter country code only)
- State (no abbreviations)
- Locality (no abbreviations)
- Organization Name
- Organizational Unit
- Common Name (FQDN)

The format of the subject-name line entry should be:

```
(config-ca-trustpoint)# subject-name
cn=fqdn,U=organisational_unit_name,C=country,St=state,L=locality,O=organisation
```

Related Topics

Generate New Trustpoint for VeriSign

SSL Errors when an IM and Presence Service Domain or Hostname is Changed

I changed the IM and Presence Service domain from the CLI, and I am getting SSL certificate errors between the IM and Presence Service and the Cisco Adaptive Security Appliance.

If you change the IM and Presence Service domain name from the CLI, the IM and Presence Service self-signed cert, sipproxy.pem, regenerates. As a result you must reimport the sipproxy.pem certificate into Cisco Cisco Adaptive Security Appliance. Specifically you must delete the current sipproxy.pem certificate on Cisco Cisco Adaptive Security Appliance, and reimport the (regenerated) Cisco Adaptive Security Appliance sipproxy.pem certificate.

Errors When Creating TLS Proxy Class Maps

The following errors are displayed when configuring the TLS Proxy class maps:

```
ciscoasa(config)# class-map ent_imp_to_external
```

```
ciscoasa(config-cmap)# match access-list ent_imp_to_external
```

```
ERROR: Specified ACL (ent_imp_to_external) either does not exist or its type is not supported
by the match command.

ciscoasa(config-cmap)# exit

ciscoasa(config)# class-map ent_external_to_imp

ciscoasa(config-cmap)# match access-list ent_external_to_imp

ERROR: Specified ACL (ent_external_to_imp) either does not exist or its type is not supported
by the match command.

ciscoasa(config-cmap)#
```

The access list for the external domain does not exist. In the example above the access list called ent_external_to_imp does not exist. Create an extended access list for the external domain using the `access list` command.

Related Information -

Access List Configuration Requirements

TLS Proxy Debugging Commands

Subscriptions Do Not Reach Access Edge

Subscriptions from Microsoft Office Communicator do not reach the Access Edge. OCS reports network function error with Access Edge as the peer. The Access Edge service does not start.

On Access Edge, the IM and Presence Service domain may be configured in both the Allow tab and the IM provider tab. The IM and Presence Service domain should only be configured in the IM Provider tab. On Access Edge, remove the IM and Presence Service domain entry from the Allow tab. Make sure there is an entry for the IM and Presence Service domain on the IM Provider tab.

Note The IM and Presence Service supports multiple domains. Make sure that you check each IM and Presence domain to determine if there are erroneous entries in the Allow tab that should be removed.

Problems with Cisco Adaptive Security Appliance after Upgrade

The Cisco Adaptive Security Appliance does not boot after a software upgrade.

You can download a new software image to the Cisco Adaptive Security Appliance using a TFTP server and using the ROM Monitor (ROMMON) on the Cisco Adaptive Security Appliance. ROMMON is command line interface used for image loading and retrieval over TFTP and related diagnostic utilities.

Step 1 Attach a console cable (the blue cable that is distributed with the Cisco Adaptive Security Appliance from the console port to a port on a nearby TFTP server.

Step 2 Open hyperterminal or equivalent.

Step 3 Accept all default values as you are prompted.

Step 4 Reboot the Cisco Adaptive Security Appliance.

Step 5 Hit ESC during bootup to access ROMMON.

Step 6 Enter this sequence of commands to enable Cisco Adaptive Security Appliance to download the image from your TFTP server

```
ip asa_inside_interface server tftp_server interface ethernet 0/1 file name_of_new_image
```

Note The Ethernet interface you specify must equate to the Cisco Adaptive Security Appliance inside interface.

Step 7 Place the software image on the TFTP server in a recommended location (depending on your TFTP software).

Step 8 Enter this command to start the download:

```
tftp dnld
```

Note You need to define a gateway if the TFTP server is in a different subnet.

Cannot Install Signed Microsoft CA Server-Client Authentication Certificate on Microsoft OCS 2008

Cannot install a server-client authentication certificate that is signed by a Microsoft CA into the local computer store of a Microsoft Office Communications Server (OCS) running Windows 2008. Attempting to copy the certificate from the current user store to the local computer store fails with the error message that the private key is missing.

You can perform the following procedure:

1. Log in to the OCS as a local user.
2. Create the certificate.
3. Approve the certificate from the CA server.
4. While logged on to the OCS, export the certificate to a file and ensure that the private key is exported.
5. Log off the OCS (Local Computer).
6. Log in to the OCS again, but this time log in as an OCS domain user.
7. Use the Certificate Wizard to import the certificate file. The certificate is installed in the local computer store. You can now select the certificate in the OCS certificate tab.

Common Integration Problems and Recommended Actions

This section provides information on the Common Integration Problems and Recommended Actions.

Unable to Get Availability Exchange

Problem Unable to exchange availability information between Cisco Jabber and Microsoft Office Communicator.

Solution Perform the troubleshooting steps that are listed for the OCS/Access Edge, IM and Presence Service and Cisco Jabber.

OCS/Access Edge:

1. The certificate may have been configured incorrectly on the public interface of Access Edge. If you are using a Microsoft CA, ensure that you are using an OID value of 1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2. The incorrect value displays on the general tab of the certificate (if it is correct it is not visible). You can also see the incorrect value on an ethereal trace of the TLS handshake between IM and Presence Service and Access Edge.

   Regenerate the certificate for the public interface of the Access Edge with a certificate type of "Other" and OID value of 1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2

2. The front end server may not be running on OCS.

   Ensure that the "Office Communications Server Front-End" service is running. You can check this service by choosing **Start** > **Programs** > **Administrative Tools** > **Computer Management**. In **Services and Applications**, choose **Services** and locate the "Office Communications Server Front-End" service. If running, this service should have a status of "Started".

IM and Presence Service

1. The certificate may have been configured incorrectly on IM and Presence Service

   Generate the correct sipproxy-trust certificate for IM and Presence Service.

2. If you are using static routes, configure a static route that points to the public interface of the Access Edge. The static route should have a route type set to "domain" and have a reversed destination pattern set. For example, if the federated domain is abc.com then the destination address pattern should be set to “.com.abc.*”. Static routes are configured using Cisco Unified CM IM and Presence Administration by choosing **Presence** > **Routing** > **Static Routes**.

3. Perform a check of the DNS SRV and ensure that both sides can resolve the domain of the affected users.

Cisco Jabber client:

Cisco Jabber might retrieve incorrect DNS configuration from the client computer. You should do the following:

1. Verify the DNS configuration on the client computer.
2. If you modify the DNS configuration, restart Cisco Jabber.

Related Topics

Certificate Configuration for the External Access Edge Interface
Generate a New Certificate on the IM and Presence Service
DNS Configuration for SIP Federation

Problems Sending and Receiving IMs

Problems sending and receiving IM's between a Microsoft Office Communicator user and a Cisco Jabber 8.0 user.

Perform the troubleshooting steps that are listed for the DNS settings, Access Edge, Microsoft Office Communicator client, and the IM and Presence Service.

DNS Settings:

DNS SRV records may not have been created, or configured incorrectly. Check if the DNS SRV records have been configured correctly for all domains. Perform an nslookup for type=srv from both the IM and Presence Service and Access Edge.

On Access Edge

1. From a command prompt on Access Edge, enter `nslookup`.
2. Enter `set type=srv.`
3. Enter the SRV record for the IM and Presence domain, for example **_sipfederationtls._tcp.abc.com** where **abc.com** is the domain name. If the SRV record exists, the FQDN for IM and Presence Service/Cisco Adaptive Security Appliance is returned.

   On the IM and Presence Service:
4. Using a remote access account, ssh into the IM and Presence Service node.
5. Perform the same steps as per the Access Edge above, except in this case use the OCS domain name.

Microsoft Office Communicator client:

The Microsoft Office Communicator 2007 user may have their presence set to "Do Not Disturb" (DND). If Microsoft Office Communicator 2007 is set to DND then does not receive IM's from other users. Set the presence of the Microsoft Office Communicator user to another state.

IM and Presence Service

1. If you are using static routes instead of DNS SRV, a static route may have been configured incorrectly. Configure a static route that points to the public interface of the Access Edge. The static route should have a route type set to "domain" and have a reversed destination pattern set. For example, if the federated domain is “abc.com” then the destination address pattern should be set to “.com.abc.*”. Static routes are configured in **Cisco Unified CM IM and Presence Administration** by choosing **Presence** > **Routing** > **Static Routes**.
2. The Federation IM Controller Module Status may be disabled. In **Cisco Unified CM IM and Presence Administration**, choose **System** > **Service Parameters**, and choose the SIP Proxy service. At the bottom of the window, check that the **IM Gateway Status** parameter is set to On.
3. The Federated Domain may have not have been added, or configured incorrectly. In **Cisco Unified CM IM and Presence Administration**, choose **Presence** > **Inter-Domain Federation** and check that the correct federated domain has been added.

Related Information -

DNS Configuratino for SIP Federation

Add a SIP Federation Domain

Losing Availability and IM Exchange after a Short Period

The user can share availability and IMs between Cisco Jabber and Microsoft Office Communicator but after a short period, they start to lose each others availability, and then can no longer exchange IM's.

OCS/Access Edge:

1. On Access Edge, both the internal and external edges may have the same FQDN. Also in DNS there may be two "A" record entries for that FQDN, one resolving to the IP address of the external edge and the other to the IP address of the internal edge.

   On Access Edge, change the FQDN of the internal edge, and add an updated record entry in DNS. Remove the DNS entry that was originally resolving to the internal IP of the Access Edge. Also reconfigure the certificate for the internal edge on Access Edge.

2. On OCS, under global settings and front end properties, the FQDN for the access edge may have been entered incorrectly. On OCS, reconfigure the server to reflect the new FQDN of the internal edge.

DNS Settings:

DNS SRV records may not have created, or configured incorrectly. Add the necessary "A" records and SRV records.

Related Information -

External Server Component Configuration for SIP Federation

Delay in Availability State Changes and IM Delivery Time

There is a delay in the delivery time of IM and Presence Service state changes between Cisco Jabber and Microsoft Office Communicator.

On the IM and Presence Service node, the **Disable Empty TLS Fragments** option may not be selected for the Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context.

Step 1 Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **System** > **Security** > **TLS Context Configuration**.

Step 2 Click the link for the **Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context**.

Step 3 In the TLS Context Information area, check the **Disable Empty TLS Fragments** check box.

Step 4 Click **Save.**

403 FORBIDDEN Returned Following an Availability Subscription Attempt

IM and Presence Service attempts to subscribe to the availability of a Microsoft Office Communicator user and receives a 403 FORBIDDEN message from the OCS server.

On the Access Edge server, the IM and Presence Service node may not have been added to the IM service provider list. On the Access Edge server, add an entry for the IM and Presence Service node to the IM service provider list. On the DNS server for Access Edge, ensure that there is a _sipfederationtls record for the IM and Presence Service domain that points to the public address of the IM and Presence Service node.

Or

On the Access Edge server, the IM and Presence Service node may have been added to the Allow list. On the Access Edge server, remove any entry from the Allow list that points to the IM and Presence Service node.

Related Information -

External Server Component Configuration for SIP Federation

Time Out on NOTIFY Message

The IM and Presence Service times out when sending a NOTIFY message, when federating directly between IM and Presence Service and Microsoft OCS using TCP.

On the IM and Presence Service node, the **Use Transport in Record-Route Header** may need to be enabled.

Step 1 Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **System** > **Service Parameters**.

Step 2 From the Server drop-down list, choose the node.

Step 3 From the Service drop-down list, choose the **Cisco SIP Proxy** service.

Step 4 In the SIP Parameters (Clusterwide) section, choose **On** for the Use Transport in Record-Route Header parameter**.**

Step 5 Click **Save.**

IM and Presence Service Certificate not Accepted

Access Edge is not accepting the certificate from the IM and Presence Service.

The TLS handshake between the IM and Presence Service/Cisco Adaptive Security Appliance and the Access Edge may be failing.

OCS/Access Edge:

1. Ensure that the IM Provider list on the Access Edge contains the public FQDN of the the IM and Presence Service node, and it matches the subject CN of the IM and Presence Service certificate. If you have opted not to populate the Allow List with the FQDN of the IM and Presence Service, then you must ensure that the subject CN of the IM and Presence Service certificate resolves to the FQDN of the SRV record for the IM and Presence Service domain.

2. Ensure that FIPS is enabled on Access Edge (use TLSv1).

3. Ensure that Federation is enabled globally on OCS, and enabled on the front end server.

4. If failing to resolve DNS SRV, ensure that DNS is set up correctly and perform an nslookup for type=srv from Access Edge:

5. From a command prompt on Access Edge, enter **`nslookup`**.

6. Enter **`set type=srv.`**

7. Enter the SRV record for the IM and Presence Service domain, for example. **_sipfederationtls._tcp.abc.com** where **abc.com** is the domain name. If the SRV record exists, the FQDN for the IM and Presence Service/Cisco Adaptive Security Appliance is returned.

IM and Presence Service/Cisco Adaptive Security Appliance:

Check the ciphers on the IM and Presence Service and Cisco Adaptive Security Appliance. Log in to **IM and Presence Service Administration**, choose **System** > **Security** > **TLS Context Configuration** > **Default Cisco SIP Proxy Peer Auth TLS Context**, and ensure that the "TLS_RSA_WITH 3DES_EDE_CBC_SHA" cipher is chosen.

Problems Starting Front-End Server on OCS

The front-end server on OCS does not start.

On OCS, the FQDN of the private interface of the Access Edge may have been defined in the list of Authorized Hosts. Remove the private interface of the Access Edge from the list of Authorized Hosts on OCS.

During OCS install, two Active Directory user accounts are created called RTCService and RTCComponentService. These accounts are given an administrator-defined password, however, on both of these accounts the "Password never expires" option is not selected by default so the password expires periodically. To reset the password of the RTCService or RTCComponentService on the OCS server, follow the procedure below.

Step 1 Right-click on the user account.

Step 2 Choose **Reset Password**.

Step 3 Right-click on the user account.

Step 4 Choose **Properties**.

Step 5 Choose the **Account** tab.

Step 6 Check the **Password never expires** check box.

Step 7 Click **OK**.

Unable to Remote Desktop to Access Edge

Unable to successfully remote desktop to the Access Edge Server with FIPS enabled on Windows XP.

This is a known Microsoft issue. The workaround to resolve the issue involves installing a Remote Desktop Connection application on the Windows XP computer. To install Remote Desktop Connection 6.0, follow the instructions at the following Microsoft URL:

http://support.microsoft.com/kb/811770