CHAPTER 34

Troubleshooting

This chapter describes how to diagnose and solve problems between the ACE XML Gateway and the external service or service consumer. It covers these topics:

Troubleshooting Service Connectivity Errors

Partner connections are the most common source of difficulty in setting up the ACE XML Gateway. The complexity involved in setting up most network protocols creates many opportunities for things to go wrong.

This section can't describe every possible setup problem and every possible diagnostic procedure, but it does describe a general approach to troubleshooting partner connections, beginning with the two areas of configuration where most Gateway users have trouble: handling SOAP envelopes and setting up SSL connections.

Troubleshooting SOAP Service Issues

When processing SOAP messages, as when processing any network traffic, the ACE XML Gateway identifies and authenticates consumers, routes incoming and outgoing messages, and logs its activity according to the relevant logging preferences. In addition, the ACE XML Gateway performs a number of processing tasks related to the structure and content of the SOAP messages themselves.

When something goes wrong with SOAP message transport, there are many stages at which an error might have occurred, and so it's important to approach troubleshooting systematically.

To troubleshoot faulty SOAP connections, take the following steps, in the following order:

Step 1 Check the physical network and IP connectivity between appliances.

For more information, see "Checking the Network" section on page 34-324.

Step 2 Check the SOAP configuration of the client and server appliances.

Ensure that both ends of the connection are set up properly to support SOAP messaging; while checking the configuration, note any configuration settings that might be relevant to the connectivity problem.

For more information, see "Checking Client and Service Setup" section on page 34-324.

Step 3 Check the event log for logged errors.

If you find any, view their details in the log viewer, looking for clues that might indicate how the errors occurred. As a temporary troubleshooting measure, you might change logging levels to **Debug** and repeat the message traffic so that the ACE XML Gateway records as much information as possible. When you've finished troubleshooting, reset logging levels as appropriate to maintain optimum throughput.

For more information, see "Checking the Event Log" section on page 34-325.

Step 4 Check the message log for logged error messages.

Again, view the details of any logged errors for clues to the cause of the problem. Remember that you can change logging levels to increase the amount of information recorded.

For more information, see "Checking the Message Log" section on page 34-325.

Step 5 Use the message log to trace failed messages through the four stages of message-processing.

Finding the stage at which the error occurs can lead you quickly to the cause of the trouble.

For more information, see "Checking the Message Log" section on page 34-325.

Step 6 Use SOAP and XML tools to analyze message content.

Construct a known-valid test file, send it through the system, then verify that the processed file data matches the original.

For more information, see "Analyze Message Content" section on page 34-325.

Checking the Network

Before beginning any serious troubleshooting work, always check your network connectivity:

- Are the cables intact? Inspect the cables visually; if you have any doubts about their integrity, use a cable tester or swap the suspect cable with a known-good cable to determine that your cables are sound.
- Have the cables been disconnected? Check the appropriate cable connections.
- Has a domain name server failed?
- Has a change been made to a router or network firewall? Check the settings on your network firewalls to ensure that your client can open socket connections on the necessary ports.
- Can you make network connections using simple tools like `ping` and `telnet`? To confirm that basic connectivity between clients and services is working, ping the ACE XML Gateway from a system that should be able to reach it.

Checking Client and Service Setup

Once you've verified that your network connection is good, you can determine whether problems exist at the message-transport level:

- Are the client and the server configured correctly to send and receive SOAP traffic?
- Can the client construct and send a SOAP message?
- Does the client's SOAP message arrive intact at the backend server?
- Is the SOAP server configured properly, and is it running?

The exact process of determining the answers to these questions depends on the client and server software you are using, and the diagnostic tools available to you. If you have trouble determining the answers to these questions, contact your support representative for help.

While you're examining the states of the client and server systems, take note of any configuration settings that might affect the SOAP messages actually constructed and sent. Again, the configuration settings to examine vary depending on the client and server software, but it may be worthwhile to make notes about any settings that might be relevant.

Also, make sure that the domain names and pathnames are correct; for example, make sure that SOAP clients are sending messages to the right address and path to reach the intended service. Make sure, as well, that if the client is set up to send document-style messages, the corresponding handler on the ACE XML Gateway expects to receive document-style messages; or, similarly, that if the client sends RPC-style messages, the handler expects to receive RPC-style messages.

Checking the Event Log

Once you are satisfied that the client and server software is configured and running properly, and that messages are being sent appropriately, the next step is to check the ACE XML Manager's event log for error messages. If the client sends a SOAP message that contains some sort of error, or attempts to deliver it in a way that the current policy or SOAP settings do not allow, it is likely that the ACE XML Gateway will log an error event. Pay special attention to “Alert” or “Error” events.

The right-hand column of the event log displays a brief description next to each logged event; you can look through the descriptions in that column for problems that might have been caused by trouble with a SOAP message. If necessary, change the ACE XML Manager's event-logging level to Debug in order to record the maximum information possible, and try sending your messages again.

Checking the Message Log

If the event log doesn't suggest anything, try examining the Message Log. If a misconfiguration or other problem prevents the SOAP messages from even being processed by the ACE XML Gateway then the Message Log may not help much; in such cases, you won't see the SOAP messages recorded because the ACE XML Gateway never processes them. On the other hand, if the ACE XML Gateway does accept and process a message, you should see records of it in the log. You can then trace its progress to determine where in the four-stage process the problem occurred. At the very least, a missing message may help you determine whether the failure is in processing the request, delivering the message, or the response sent back by the server.

Even if the SOAP message itself is not recorded, an error message might appear in the log. Furthermore, if a server response is rejected before processing, you should still see the record of the incoming and outgoing requests before they reach the service; in this case, the logged messages tell you how far the request/response process got before failing, which is a valuable clue to the nature of the problem.

In a successful SOAP exchange, a SOAP client sends a message to the ACE XML Gateway, which validates the message, processes it, and delivers it to a backend service; subsequently, the service returns a response to the ACE XML Gateway, which validates, processes, and delivers the response to the client. Use the record of events and messages preserved in the logs to determine how far through this process a message went before failure, and you will have a good basis for deducing the nature of the problem.

Analyze Message Content

If everything in the configuration of the client, server, and Gateway seems correct, and if the logs provide no clue to the nature of the problem, try using XML tools such as `xmllint` or XMLSpy to examine the message itself. Use your SOAP client to generate a message and save it to a file. Then use your tools to make sure that the XML data in the message are what you expect.

As one example of the sort of problem that can be uncovered this way, some clients construct SOAP messages that contain elements that refer to data stored outside the SOAP action part of the message; for example, the message might consist of an XML document that contains both a SOAP action and also some auxiliary XML elements, and the SOAP action may contain elements that refer to data stored in the auxiliary elements. Because the ACE XML Gateway processes only the SOAP action itself, it cannot retrieve data stored in the message but outside the action, and so messages constructed in this fashion can cause problems when the ACE XML Gateway attempts to validate or otherwise process them.

Troubleshooting SSL and TLS Connections

From the client end, an SSL connection appears to be simple, whether successful or not. A successful connection simply transfers requests and responses; a failed connection drops.

The behind-the-scenes reality is more complicated, as becomes clear when you attempt to debug a failed connection. There are several stages in establishing a successful SSL connection, and several auxiliary resources that have to be just right. To find the source of trouble in a failed connection, you must examine methodically each of the stages and the auxiliary data.

The high-level steps are:

Step 1 Check the physical network and the IP connectivity between appliances.

For more information, see "“Checking the Network” section on page 34-324."

Step 2 Enable debug event logging and try sending test messages on the affected ports.

For more information, see "“Sending Test Messages” section on page 34-327."

Step 3 Check the logs for traces of the sent messages.

For more information, see "“Checking the Logs” section on page 34-327."

Step 4 Check the ACE XML Gateway's security resources.

For more information, see "“Checking the Security Resources” section on page 34-328."

Step 5 Check the consumer's identification and access privileges.

For more information, see "“Checking the Authenticator and Policy” section on page 34-328."

Step 6 Check the policy to determine how the messages are supposed to be handled.

For more information, see "“Checking the Authenticator and Policy” section on page 34-328."

The following sections describe these steps in greater detail.

Checking the Network

Before beginning any serious troubleshooting work, always check your network connectivity:

- Are the cables intact?

  Inspect the cables visually; if you have any doubts about their integrity, use a cable tester or swap the suspect cable with a known-good cable to determine that your cables are sound.

- Have the cables been disconnected?

  Check the appropriate cable connections.

- Has a domain name server failed?

- Has a change been made to a router or network firewall?

  Check the settings on your network firewalls to ensure that your client can open socket connections on the necessary ports.

- Can you make network connections using simple tools like `ping` and `telnet`?

  To confirm that basic connectivity between clients and services is working, ping the ACE XML Gateway from a system that should be able to reach it.

Sending Test Messages

Before sending test messages, enable event logging on the ACE XML Gateway at the Debug level in order to record the most data possible during your tests. Make sure traffic meant for the affected SSL connections is logged at the Debug level. For more information about configuring logging levels, see Chapter 29, "Monitoring System Status."

Next, use a client that supports SSL connections to try sending one or more test messages to the affected service.

Microsoft provides a free utility called WFetch that provides features useful for debugging web-services connections. Among other things, WFetch supports SSL connections. WFetch is available as part of Microsoft's Internet Information Server (IIS) 6.0 Resource Kit Tools, which are available as a free download.

If you need to test the connection from a UNIX-like platform, you can use the `curl` tool, which supports SSL connections. The `curl` tool may already be installed on your system. It is distributed with many UNIX-like systems. Otherwise, it is available from http://curl.haxx.se

Use the SSL features of your testing tool to send messages that are as identical as possible to the messages that failed. If at all possible, send the test messages using the same client certificate the failed messages used. If the test messages succeed, but the normal traffic still fails, then the failure is likely due to policy settings or problems with the message contents, rather than SSL configuration or handshake issues.

Note The Cisco ACE XML Gateway *Getting Started Guide* provides a walkthrough example that shows how to test the ACE XML Gateway with Wfetch.

Checking the Logs

If the test message fails, examine the event log for records of the failed communication. For more information about how to examine the event log, see the Inspecting the Logs section of Monitoring System Status.

Look in the log for evidence that your test session connected to the ACE XML Gateway, and that is tried to send the test messages on an SSL connection. To make sure you have the most complete information, set the event log to log at Debug level before sending your messages. Then, view the event log and look for evidence that the messages were received and processed.

In addition to looking for errors recorded in the event and message logs, you can check the event log specifically for SSL trace items the ACE XML Gateway records when logging is set to Debug level. Errors or warnings that the SSL trace records can lead you directly to the source of the problem. For example, if a client rejects the ACE XML Gateway server certificate then you will usually see an entry from the SSL trace that says "client unexpectedly terminated connection" or something similar.

When searching the log, look for the DN or thumbprint of the certificate that your client presents. If you don't see it, then it is likely your client didn't send it; check the client configuration.

If the DN or thumbprint is in the log, but is associated with an error message, then the ACE XML Gateway rejected the connection for some reason. Check the authenticator and authorization group associated with the handler that processes this message, and then check the security resources on the ACE XML Gateway and the client. For more information about security resources, see "Checking the Security Resources" section on page 34-328.

If you see the DN or thumbprint, but no recorded traffic and no error message, then the ACE XML Gateway mapped the incoming message to no authenticator. In this case, check the authenticator settings.

The same problems that arise between a client and the ACE XML Gateway can also arise between the ACE XML Gateway and the service; the same troubleshooting approaches apply.

Checking the Security Resources

The consumer and the ACE XML Gateway use X.509 certificates to establish the SSL connection:

- The X.509 certificates on both sides of the connection must be valid.
- The certificates must be appropriate for the use to which they are put.
- The ACE XML Gateway and the client or service must actually be able to use the certificates.

One common problem is that a client rejects the server certificate the ACE XML Gateway presents to identify itself. A client may reject a certificate for any of a variety of reasons:

- You might have uploaded a certificate whose usage field is inappropriate for a server identification.
- The certificate's signing CA may not be one that the client is configured to trust.
- There may be a subtle incompatibility between the certificate data and the particular client library.
- Certificates can be revoked.

Check any certificate revocation lists (CRLs) that the client or the ACE XML Gateway may honor.

- The current time and date may lie outside a certificate's valid period. Check the certificate's valid times.

You can test these kinds of issues by changing certificates and by trying different clients. As always, begin the process by verifying that the client software and the ACE XML Gateway are making the same assumptions about how the connection is to be established.

Also check the certificate to see if it has a multi-step validation chain. If so, then certificates for each stage of the chain must be installed on the ACE XML Gateway in order for the certificate to be used.

Any of these problems can occur on the ACE XML Gateway-to-service side of a connection as well as the consumer-to-Gateway side; the same diagnostic approach is appropriate for troubleshooting either side of the connection.

Checking the Authenticator and Policy

Before a consumer can make a connection to an open port or send a message, the ACE XML Gateway policy must define a valid authenticator for that consumer and the handler for the service must be provisioned to an authorization group that includes the authenticator.

If everything else about your setup seems to be correct (including security resources) and yet SSL connections are still failing, check the authenticator associated with the client:

- Make sure the ACE XML Gateway policy defines a valid authenticator for the client.
- Make sure that the authentication method the authenticator requires is the one your client actually uses.

Also, check the handler that routes messages to the service:

- Make sure the handler is configured to accept the messages that the client is actually sending.
- Make sure the handler is configured to deliver the client's messages to the correct service.
- Make sure you provisioned the handler to the consumer's authorization group.

Generating a Diagnostic Snapshot

The ACE XML Manager can generate a diagnostic snapshot useful for troubleshooting system issues. Cisco support can use this archive of detailed information about the system's working configuration and policy to analyze and diagnose security and performance problems.

Because a diagnostic snapshot produces a very complete record of the state of the Cisco ACE XML Gateway system, you must protect diagnostic snapshots carefully. Only users who have the Administrator role in the web console can make diagnostic snapshots. Be careful to grant this role only to users who should have access to your network's most sensitive data.

In order to help you better control the sensitive information that appears in security policies, the **Diagnostic Snapshot** page allows you to specify whether the snapshot includes certain information, such as cryptographic keys and the contents of logs.

Generating a Diagnostic Snapshot Procedures

To generate a diagnostic snapshot, take the following steps:

Step 1 Contact your support representative to confirm that it is necessary to generate a diagnostic snapshot.

In addition to confirming that generation of a diagnostic snapshot is appropriate, your support representative assigns to you a username and password you can use to log into the Cisco diagnostic snapshot upload page. Optionally, your support representative may provide a trouble ticket number that both of you can use to identify the support case and any files (such as the snap-shot) associated with it.

Step 2 Log into the ACE XML Manager web console as an `Administrator` user.

Note For security reasons, only an administrator user can generate a diagnostic snapshot.

Step 3 Click the **Diagnostic Snapshot** link in the **Administration** section of the navigation menu.

Step 4 In the **Diagnostic Snapshot** page, choose the contents of the snapshot from these options:

- Private/Keypair resource files—By default, the Public/Private Keypair resource files checkbox is not selected. For security reasons, do not include public/private keypair data in your snapshot unless your support representative requests that you do so. Such files provide encryption key information that must be kept secret under normal circumstances.
- Extension (SDK) files—Includes Jars and resources files in the snapshot that have been developed using the ACE XML Gateway SDK and installed on the appliance.

Extensions may implement proprietary authentication schemes or whole-message transformations. Access to these files might allow an attacker to compromise authentication schemes, to extract data from messages in transit, or to insert malicious code in messages. Use caution when choosing whether to include extension files.

- Event log—Typically, the event log is one of the best places to begin any investigation into unexpected behavior of a system. It is important that you allow the Event log checkbox to remain checked unless your support representative informs you that it is not necessary to include event log data in the snapshot.

  To limit the amount of event log data the snapshot includes, type the number of events in the Event log field. By default, the most recent 1000 entries in the log. After checking with your support representative, you may prefer to specify that the snapshot include fewer or more entries.

- Message Traffic Log—The message log is a valuable source of diagnostic information. Only exclude the message traffic log from the snapshot if advised to do so by your support representative.

  To limit the amount of message traffic log data the snapshot includes, type into the **most recent** field the number of message traffic log files the snapshot.

  For an ACE XML Gateway that handles large amounts of traffic or logs messages at high levels of detail, the message traffic log can become quite large. In such cases, you may prefer to restrict the amount of log data the snapshot includes. By default, the snapshot includes only the most recent message traffic log file; after checking with your support representative, you may prefer to specify that the snapshot include additional message traffic log files.

Step 5 The snapshot is encrypted using a passphrase you type into the **Encryption Passphrase** field. The ACE XML Manager uses the passphrase to encrypt the data in the diagnostic snapshot.

You must provide the passphrase to your support representative for use in decrypting the diagnostic snapshot. Therefore, it is important that you do not choose a passphrase that is proprietary to your organization or to you personally. It is recommended that you write down the passphrase so you can communicate it to your support representative precisely. However, for security reasons, do not record the passphrase on the same computer used to generate or transmit the snapshot.

Step 6 Retype the passphrase into the **Repeat Passphrase** field. This value must match exactly the passphrase you typed into the **Encryption Passphrase** field.

Step 7 If you have opened a trouble ticket with Cisco support, type that number into the **Trouble Ticket #** field. Alternatively, you can specify your own tracking number. You and Cisco support can use the value of the **Trouble Ticket #** field to track progress on the issue the snapshot describes.

Step 8 Choose one of the following options to specify a filename for the snapshot:

- To generate a filename automatically (the default), click the **Generate Automatically** button in the **Snapshot Output Options** section of the page. The ACE XML Manager generates a name of the form `snapshot[timestamp].tgz` automatically.
- To specify another filename, click **Custom** and type a unique identifier into the field at the right of the Custom button.

  The file name extension `.tgz` is automatically added to the file name you supply. For example, if you specify the name `myFile`, the resulting snapshot would be named `myFile.tgz`.

Step 9 Click the **Generate Diagnostic Snapshot** button to generate the snapshot file. In the dialog box, choose a filesystem location where you want the file to be saved.

After saving the file, transmit the snapshot to your support representative using the arranged method.