SAS Troubleshooter

SAS® 9.4 Content Server Issues

Table of Contents

SAS Troubleshooter documentation is designed to assist you in diagnosing and troubleshooting classes of problems that can occur in SAS software applications and third-party applications. The documents are intended to help you resolve problems on your own, and they provide the same steps that SAS Technical Support typically follows.

It is possible that your problem might not be resolved by using the steps in this troubleshooting document. In that case, the troubleshooting steps that you perform create collateral information (logs, files, or answers to questions) that you can pass to SAS Technical Support later for additional help.

Problem Overview

This troubleshooting guide specifically covers how to diagnose several problems that are related to the configuration and other errors within the SAS® 9.4 Content Server repository that impact tasks such as validation of SAS Content Server and using SAS® 9.4 Management Console to import and export SAS content.

Before you diagnose problems, you need to enable both SAS Management Console debugging traces and the SAS Content Server consistencyCheck flag. Information for enabling the traces and flag is available, respectively, in the following SAS Notes:

- SAS Note 43157, "Capturing debugging messages from SAS® Management Console" (**support.sas.com/kb/43/157.html**)
- SAS Note 58979, "Enabling the SAS® Content Server Repository consistencyCheck flag" (**support.sas.com/kb/58/979.html**)

This document discusses three categories of problem that you might encounter when you work with SAS 9.4 Content Server:

- Problems that occur when you validate SAS Content Server from SAS Management Console
- Problems that occur when you export SAS packages from SAS Management Console
- Problems that occur when you import packages into SAS Management Console

Symptoms

The following list shows the specific errors that you receive as symptoms for each of the three categories of problems that are discussed in this document. The troubleshooting steps for resolving these errors are discussed later in this document.

- **Errors that occur when you validate SAS Content Server from SAS Management Console:**
  - The WebDAV server ping fails. When this problem occurs, you might get one of the following error messages:
    - `SEVERE: java.net.ConnectException: Connection refused: connect`
    - `SEVERE: demo.test.domain`

(list continued)

- The WebDAV server connection fails. When this problem occurs, you can receive one of several errors:
  - `SEVERE: Code 502: Service Unavailable`
  - `SEVERE: Exception accessing http://demo.test.domain:80 (Unrecognized SSL message, plaintext connection?)`
  - `SEVERE: Exception accessing https://demo.test.domain:443 (sun.security.validator.ValidatorException:PKIX path building failed:`
  - `SEVERE: [Realm=SAS Content Server} Authentication required, but invalid credentials supplied`
- WebDAV enablement of the server fails. When this problem occurs, you receive this error message:

  ```
  SEVERE: Server is not WebDAV enabled!
  ```
- The path does not exist. When this problem occurs, you receive this error message:

  ```
  SEVERE: Code 404:Not found – Path
  'http://demo.test.domain:80/SASContentServer/repository/test/'
  does not exist or user ID 'sasadm@!*(generatepassworddomain)*!'
  does not have permission to access the path.
  ```

- **Errors that occur when you use SAS Management Console to export SAS packages:**
  - Retrieving dependencies: When this type of problem occurs, you receive the following message:

    ```
    Error retrieving dependencies
    com.sas.metadata.logical.LogicalTypeException:java.lang.IllegalStateException: '503: Service Unavailable'
    ```
  - Analyzing objects: When this type of problem occurs, you receive the following message:

    ```
    DEBUG – AnalyzeObjects com.sas.metadata.remote.MdException:
    Content Mapping was unable to connect to host "demo.test.domain",
    port "80"
    ```

- **Errors that occur when you use SAS Management Console to import SAS packages:**

  Analyzing dependencies: When this type of problem occurs, you receive one of the following messages:

  - `DEBUG – Analyze exception: com.sas.metadata.promotion.MetadataPromotionException: Content Mapping was unable to connect to host "demo.test.domain", port "80"`
  - `DEBUG – Analyze exception: com.sas.metadata.promotion.MetadataPromotionException: '503: Service Unavailable" error while accessing 'http://demo.test.domain/SASContentServer/repository/default/sasfolders/Shared Data/'`

Understanding the Technology

SAS® Content Server

*SAS Content Server (*part of the SAS Web Infrastructure Platform) is a content repository that stores digital content (for example, documents, reports, and images) that is created and used by SAS® client applications. Examples of such content include reports and documents that are created by users of SAS® 9.4 Web Report Studio, SAS® 9.4 Information Delivery Portal, SAS® 9.4 Visual Analytics, SAS® Enterprise Case Management, and other SAS web applications.

SAS Content Server is a web application that starts when the SAS 9.4 Web Application Server is started. *The Web Distributed Authoring and Versioning (WebDAV)* protocol is currently the main method for accessing SAS Content Server. In addition to the basic features of HTTP, the WebDAV protocol is an extension to HTTP and provides Write access, version control, search, and other features.

For additional information about SAS Content Server, see "Chapter 10: Administering the SAS Content Server" in the *SAS® 9.4 Intelligence Platform: Middle-Tier Administration Guide, Third Edition*. (**support.sas.com/documentation/cdl/en/bimtag/68217/PDF/default/bimtag.pdf**)

SAS® Management Console

As you administer the SAS® Intelligence Platform, one of your primary tools is SAS® Management Console. *SAS Management Console* is a Java application that provides a single point of control for administering your SAS servers and for managing metadata objects that are used throughout the SAS Intelligence Platform.

Whenever SAS® Metadata Server is running, you can use SAS Management Console to connect to SAS Metadata Server so that you can view and manage the metadata objects that are stored in the server's metadata repositories. The SAS Management Console user interface includes a **Plug-ins** tab, a **Folders** tab, and a **Search** tab that you can use to access and manage metadata. For additional information about SAS Management Console, see "Overview of SAS Management Console" in "Chapter3: Overview of the Administration Tools" in the *SAS® 9.4 Intelligence Platform: System Administration Guide, Fourth Edition*. (**support.sas.com/documentation/cdl/en/bisag/68240/PDF/default/bisag.pdf**)

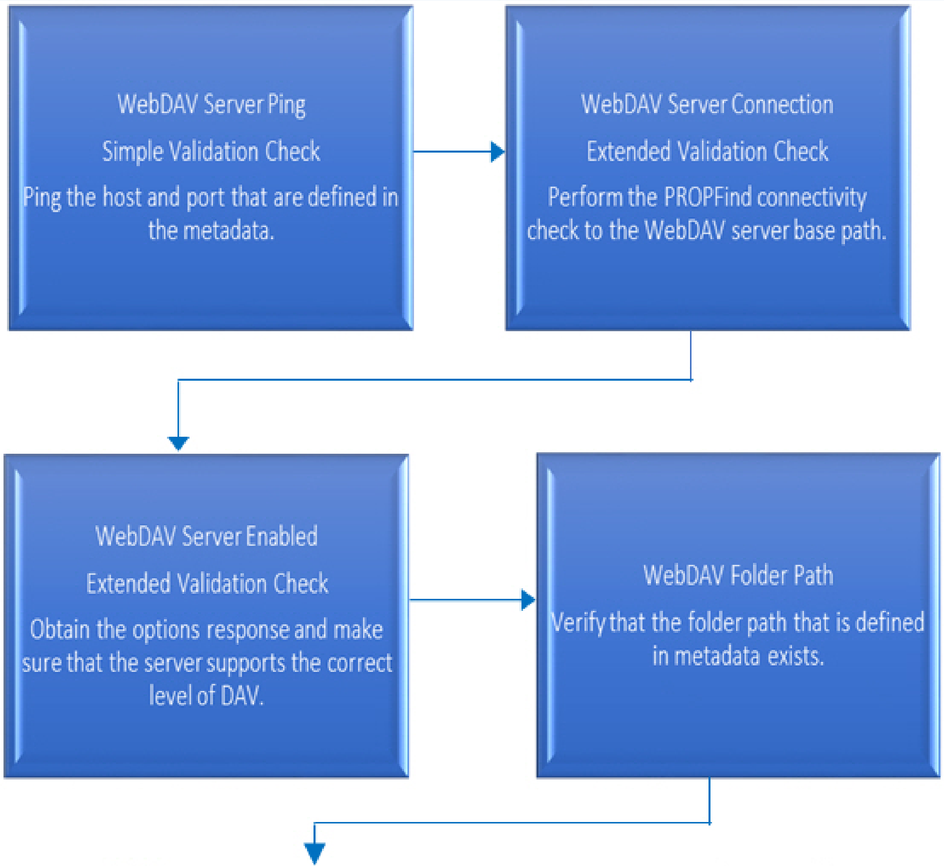
Validating SAS® Content Server from SAS® Management Console

The following sections explain the process flow that occurs when you validate SAS Content Server and show the errors that you might encounter during that process.

For details about the validation process, see "Validate the SAS Content Server" in "Chapter 7: Checking the Status of Servers" the *SAS® 9.4 Intelligence Platform: System Administration Guide, Fourth Edition. (*(**support.sas.com/documentation/cdl/en/bisag/68240/PDF/default/bisag.pdf**)

Understanding the Request Process That Occurs When You Validate SAS® Content Server

You use the **Validation Success** request in SAS Management Console to validate SAS Content Server. The validation process includes a WebDAV validation test, which includes simple and extended validation checks. The flow for the validation process is shown below:



WebDAV Server Ping

Simple Validation Check

Ping the host and port that are defined in the metadata.

WebDAV Server Connection

Extended Validation Check

Perform the PROPFind connectivity check to the WebDAV server base path.

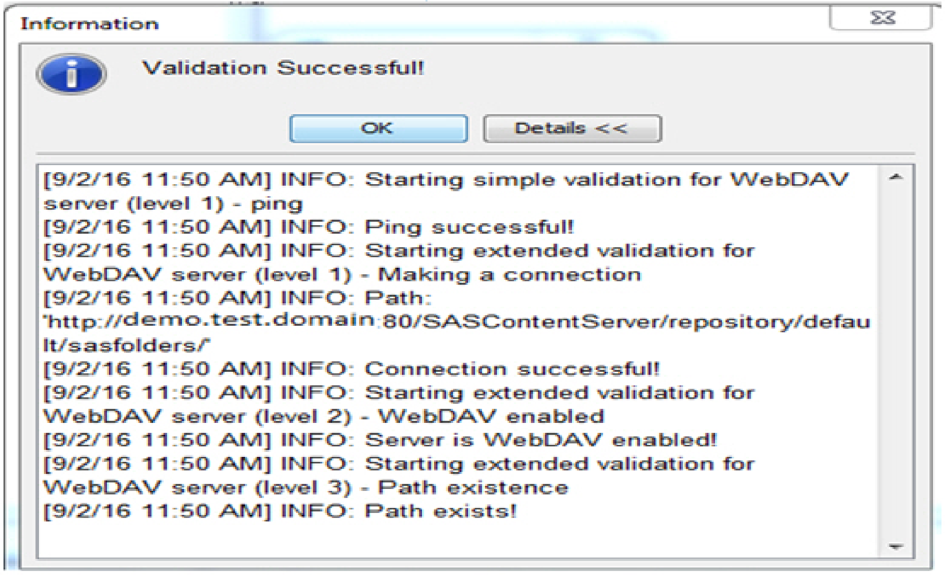
WebDAV Server Enabled

Extended Validation Check

Obtain the options response and make sure that the server supports the correct level of DAV.

WebDAV Folder Path

Verify that the folder path that is defined in metadata exists.



Validation Successful!

```
[9/2/16 11:50 AM] INFO: Starting simple validation for WebDAV
server (level 1) - ping
[9/2/16 11:50 AM] INFO: Ping successful!
[9/2/16 11:50 AM] INFO: Starting extended validation for
WebDAV server (level 1) - Making a connection
[9/2/16 11:50 AM] INFO: Path:
'http://demo.test.domain:80/SASContentServer/repository/defau
lt/sasfolders/'
[9/2/16 11:50 AM] INFO: Connection successful!
[9/2/16 11:50 AM] INFO: Starting extended validation for
WebDAV server (level 2) - WebDAV enabled
[9/2/16 11:50 AM] INFO: Server is WebDAV enabled!
[9/2/16 11:50 AM] INFO: Starting extended validation for
WebDAV server (level 3) - Path existence
[9/2/16 11:50 AM] INFO: Path exists!
```

Troubleshooting Steps

When you performing SAS Content Server validation within SAS Management Console, you might encounter the following problems:

- WebDAV server ping fails
- WebDav server connection fails
- WebDAV enablement of the server fails
- Path does not exist

The following sections provide solutions for resolving the errors listed above. (**Note:** To navigate to the solution for a specific error, click the appropriate link in the list above.)

WebDAV Server Ping Fails

When the WebDAV server ping fails, you might receive one of the following error messages:

- `SEVERE: java.net.ConnectException: Connection refused: connect`
- `SEVERE: demo.test.domain`

To resolve a ping-failed error, perform the following steps:

1. Verify the host name and port configuration for SAS Content Server in the metadata, as follows:
   a. Log on to SAS Management Console using the **`sasadm`** user ID.
   b. On the **Plug-ins** t tab, select **Environment Management ► Server Manager**.
   c. Right-click **SAS Content Server**. Then, in the right pane, right-click **Connection: SAS Content Server** and select **Properties**.
   d. In the Connection: SAS Content Server Properties dialog box, click the **Options** tab and verify that the host name and port number values on that tab are correct.

   Note: By default, **Host name** and **Port number** are set to the values for the SAS 9.4 Web Server host name and port. However, for some varied configuration architecture (which consists of an external reverse-proxy server or an F5 load balancer), the values for the host name and port are those for the configured server machine.

2. Verify that the SAS Web Server services is running. To do that, open the SAS Web Server log file (error_*date_timestamp*.log) that resides in ***`SAS-configuration-directory/`*****`Lev1/Web/WebServer/logs/`**. Search for the following message to confirm that the services are running.

   ```
   [Wed Sep 07 08:08:52 2016] [Notice] Child 12372: Starting thread to
   listen on port 80.
   The SAS [Config-Lev1] httpd-WebServer service is running.
   ```

3. Submit the following command to verify that the SAS Web Server host name is resolved properly via the Domain Name Server (DNS):

   ```
   nslookup host-name
   ```

(list continued)

In this command, *host-name* is the fully qualified host name of the machine where you are executing the NSLOOKUP command. When you execute this command, it returns the DNS location and the IP address from which the host name is resolved.

WebDAV Server Connection Fails

When the WebDAV server connection fails, you might receive one of the following error messages:

- `SEVERE: Code 502: Service Unavailable`
- `SEVERE: Exception accessing http://demo.test.domain:80 (Unrecognized SSL message, plaintext connection?)`
- `SEVERE: Exception accessing https://demo.test.domain:443 (sun.security.validator.ValidatorException:PKIX path building failed:`
- `SEVERE: [Realm=SAS Content Server} Authentication required, but invalid credentials supplied`

To resolve a connection-failure error, perform the following steps:

1. Verify the protocol and port configuration for SAS Content Server in metadata.
   a. Log on to SAS Management Console using the **`sasadm`** user ID.
   b. On the **Plug-ins** tab, select **Environment Management ► Server Manager**.
   c. Right-click **SAS Content Server**. The, in the right pane, right-click **Connection: SAS Content Server** and select **Properties**.
   d. In the Connection: SAS Content Server Properties dialog box, click the **Options** tab and verify that the protocol and port number values on that tab are correct.

   Note: For a non-secure, server-layer configuration (, the correct protocol is HTTP. For configurations that are enabled with Secure Sockets Layer (SSL), the correct protocol is HTTPS. If SAS Content Server is configured using an external URL that points to an external reverse-proxy server of an F5 load balancer, the content server's proxyName, proxyPort, and scheme definition values should match those that are in the `<connector>` HTML tag in the server.xml file for the SASServer_1 web application server.

2. Verify that the SAS® Web Application Server (SASServer1_1) services are running and that the SAS Content Server repository starts without any errors. To do that:
   a. Review the SAS SASServer1_1 log file (server.log) to verify that there are no errors during start-up. The log file resides in ***`SAS-configuration-directory`*`/Lev1/Web/WebAppServer/SASServer1_1/logs/`**.
   b. In the log file, also search for a message similar to the following to confirm that the services start successfully.

```
Server startup in 979797 ms
```

(list continued)

3. Review the SASContentServer9.4.log file to verify that there are no errors. The log file resides in ***SAS-configuration-directory*/Lev1/Web/Logs/SASServer1_1/**. In the log file, also search for the following message to confirm that SAS Content Server repository services start successfully:

   ```
   INFO org.apache.jackrabbit.core.RepositoryImpl - Repository started
   (5115ms)
   ```

   If you see the errors that are shown below in the SASContentServer9.4.log file (which indicate inconsistency between the SAS Content Server repository index and content items), collect all of the log and configuration information that is discussed in SAS Note 58979. (**support.sas.com/kb/58/979.html**) Then send the logs and other configuration information to SAS Technical Support as instructed in the note.

   - `INFO 2016-09-13 23:08:48,119 [main] - default: checking workspace consistency...`
   - `ERROR 2016-09-13 23:08:54,609 [main] - Error while reading blob id: java.io.EOFException`
   - `ERROR 2016-09-13 23:08:54,609 [main] - failed to read bundle: 12b8f4f5-5b57-4268-bed4-92fafe14b273: java.lang.Exception: invalid bundle, see previous BundleBinding error log entry`

4. If you receive PKIX security errors, verify that security cacerts or jssecacerts certificates for the SAS Management Console client are the same as those that are configured on the middle-tier machine. For more information, see SAS Note 39690, "Validating the SAS® Content Server in SAS Management Console generates the error 'unable to find valid certification path'." (**support.sas.com/kb/39/690.html**)

5. Verify that the Java Virtual Machine (JVM) parameters are set correctly in the JVM arguments for both the Central Authentication Server and the Service Server. For details about how to locate the JVM parameters, see SAS Note 52214, "The SAS 9.4 Content Server dircontens.jsp URL does not work after you implement a Secure Sockets Layer (SSL) configuration." (**support.sas.com/kb/52/214.html**)

WebDAV Enablement of the Server Fails

When WebDAV enablement of the server fails, you receive this error message:

```
SEVERE: Server is not WebDAV enabled!
```

To resolve this error, perform the following steps:

1. Determine whether SAS Content Server in SAS Management Console is configured to use one-time user ID and password authentication instead of SAS token authentication. If the configuration is for a one-time authentication, the password is not valid in certain cases. After the initial request, authentication fails during cookie handling because the password that is passed is no longer valid.

   To determine which type of authentication you have:

   a. Log on to SAS Management Console using the **sasadm** user ID.

   b. Click the **Plug-ins** tab and select **Environment Management ► Server Manager**.

   c. Right-click **SAS Content Server** in the right pane of the application window.

   d. Then, right-click **Connection: SAS Content Server** in the right pane and select **Properties**.

(list continued)

e. In the Connection: SAS Content Server Properties dialog box, click the **Options** tab. Verify that the value is **Authentication Type**, which should match to the SCHEMA= value in the web application server's server.xml file. The SCHEMA= option in the server.xml file is found in a `<connector>` parameter similar to the following example:

```
<connector acceptCount="100" bindOnInit="false"
connectionTimeout="20000" executor="tomcatThreadPool"
maxHttpHeaderSize="16384" maxKeepAliveRequests="15"
maxSwallowSize="-1" port="${bio.http.port}"
protocol="org.apache.coyote.http11.Http11Protocol"
proxyName="d7b227.na.sas.com" proxyPort="80"
redirectPort="${bio.https.port}" scheme="http"
useBodyEncodingForURI="true"/>
```

This example shows **`http`** as the value, but the value might be **`http`** if the Secure Sockets Layer protocol is enabled.

2. Navigate to the SAS Content Server (SASServer1_1 web application server) setenv.sh script (in the Linux operating environment) or the wrapper.conf file (in Microsoft Windows operating environments) and locate the following SAS Content Server JVM parameters:

```
-Dsas.scs.cas.scheme=
```

```
-Dsas.scs.svc.scheme=
```

Ensure that the protocol for both scheme parameters is set correctly. If the configuration is enabled with SSL, the parameter should be set to HTTPS. If SSL is not enabled, the parameter should be set to HTTP, which should match the SAS Content Server configuration in the SAS metadata. To verify that the correct protocol is set, follow these steps:

a. In SAS Management Console, select **Environment Management** ► **Server** ► **SAS Content Server**.

b. In the right pane, right-click **Connection: SAS Content Serve**r and select **Properties**.

c. On the **Options** tab, verify that the value for **Authentication Type** is set to the appropriate protocol parameter.

Also ensure that relevant Cross-Site Request Forgery (CSRF) filters are set correctly, as discussed in the following SAS Notes:

- SAS Note 55044**,** "SAS® Web Infrastructure Platform applications (including SAS® Logon Manager) might be vulnerable to Cross-Site Forgery attacks" (**`support.sas.com/kb/55/044.html`**)
- SAS Note 52214, "The SAS® 9.4 Content Server dircontents.jsp URL does not work after you implement a Secure Sockets Layer (SSL) configuration" (**`support.sas.com/kb/52/214.html`**)
- SAS Note 56451, "The error 'The Application is not authorized to use SAS Logon Manager' occurs when you try to log on to SAS® Environment Manager" (**`support.sas.com/kb/56/451.html`**)

Path Does Not Exist

If a path does not exist, you receive the following error message:

```
SEVERE: Code 404:Not found – Path
'http://demo.test.domain:80/SASContentServer/repository/test/' does not exist
or user ID 'sasadm@!*(generatepassworddomain)*!' does not have permission to
access the path.
```

To resolve this error, perform the following steps:

1. Verify that the user ID used to validate SAS Content Server has enough rights in SAS Metadata Server. The user ID must be valid and have `sasadm@saspw` rights or right equivalent to that.

   To verify the user ID rights:

   a. Log on to SAS Management Console using the `sasadm` user ID.

   b. Click the **Plug-ins** tab and select **Environment Management ► Select User Manager**.

   c. In the right pane, right-click the user ID and select **Properties**.

   d. In the *user-name* Properties dialog box, locate Authorization **permissions** under **Group and Roles** and verify that the user has the appropriate rights.

2. Verify that the defined base path within the metadata in the SAS Content Server configuration actually exists, as follows:

   a. Log on to SAS Management Console using the `sasadm` user ID.

   b. Click the **Plug-ins** tab and select **Environment Management ► Server Manager**.

   c. Right-click **SAS Content Server** and select **Properties**.

   d. In the Connection: SAS Content Server Properties dialog box, click the **Options** tab. On that tab, locate the **Check the Base Path (s): Select Items** definition and verify that the folder path that is defined actually does exist within the SAS Content Server repository. To verify that path, access the SAS Content Server Administration Console by using the following URL.

      ```
      protocol://host-name:port/SASContentServer/dircontents.jsp
      ```

      In this path, specify your SAS 9.4 configuration values for *protocol*, *host-name*, and *port*.

3. Verify that the WebDAV Repository configuration (under **Foundation Services**) is correct for all the listed services that are configured with WebDAV Repository, as follows.

   a. Log on to SAS Management Console with the `sasadm` user ID.

   b. Click the **Plug-ins** tab and select **Environment Management ► Foundation Services Manager ► Platform Local Services ► Core**.

   c. Right-click **Information Service** and select **Properties**.

   d. In the Information Service Properties dialog box, click the **Service Configuration** tab. On that tab, click **Configuration** to open the Information Service Configuration dialog box.

   e. On the **Repositories** tab, select `WebDAV` as the value for **Information Repositories**.

   f. Click **Edit** to open the DAV Repository Definition dialog box. In the dialog box, verify that the **Base** field is set to the following path:

      ```
      /SASContentServer/repository/default/sasdav
      ```

   Perform the steps above for each of the following services that are listed under **Foundation Services Manager** in SAS Management Console:

   - **Remote Services**
   - **SASBIPortlets4.4 Local Services**
   - **SASJSR168RemotePortlet4.4 Local Services**

(list continued)

- **SASPackageViewer4.4 Local Services**
- **SASPortal4.4 Local Services**
- **SASStoredProces9.4 Local Services**
- **SASStudioMidTier3.5 Local Services**

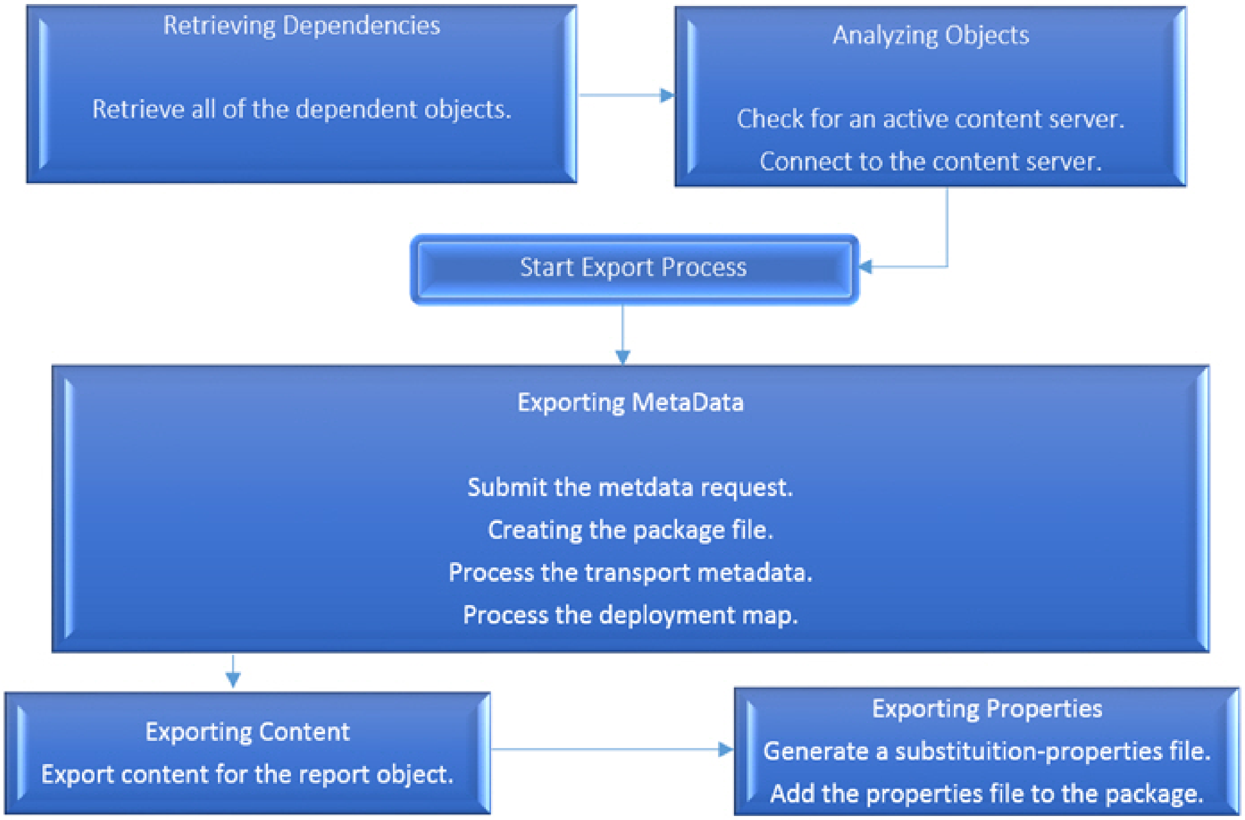
Exporting SAS® Packages from SAS® Management Console

The following sections explain the process flow that occurs when you export a SAS package from SAS Management Console and show the errors that you might encounter during that process.

For details about the export process, see "Example Usage Scenario for the Export SAS Package and Import SAS Package Wizards" in "Chapter 22: "Using the Export SAS Package and Import SAS Package Wizards" of the *SAS® 9.4 Intelligence Platform: System Administration Guide, Fourth Edition* at **support.sas.com/documentation/cdl/en/bisag/68240/PDF/default/bisag.pdf**.

Understanding the "Exporting SAS Package" Request

You use the **Exporting SAS Package** request in SAS Management Console to export a SAS Content Server item. The flow for the export process is shown below:


Retrieving Dependencies
Retrieve all of the dependent objects.
Analyzing Objects
Check for an active content server.
Connect to the content server.
Start Export Process
Exporting MetaData
Submit the metdata request.
Creating the package file.
Process the transport metadata.
Process the deployment map.
Exporting Content
Export content for the report object.
Exporting Properties
Generate a substituition-properties file.
Add the properties file to the package.

Troubleshooting Steps

When you export SAS packages from SAS Management Console, you might encounter one of the following error messages:

- **Retrieving-dependencies error:**

  ```
  Error retrieving dependencies
  com.sas.metadata.logical.LogicalTypeException:java.lang.IllegalStateExce
  ption: '503: Service Unavailable'
  ```

- **Analyze-objects error:**

  ```
  DEBUG – AnalyzeObjects com.sas.metadata.remote.MdException: Content
  Mapping was unable to connect to host "demo.test.domain", port "80"
  ```

Note: These problems can occur because the content for the packages is stored in SAS Content Server. Therefore, the troubleshooting steps in this section focus on the relevant root-cause analysis of the issue that is related to SAS Content Server. For issues that are related specifically to SAS Management Console, contact the SAS Management Console support team at **support.sas.com/ctx/supportform/createForm**.

To resolve these errors, perform the following steps:

1. Verify the status of the SAS 9.4 Apache HTTPD web server by ensuring that you can ping the server. If the ping fails, follow these steps:

   a. Verify the host name and port configuration for SAS Content Server in the metadata, as follows:

      i. Log on to SAS Management Console using the **sasadm** user ID.

      ii. On the **Plug-ins** tab, select **Environment Management** ► **Server Manager**.

      iii. Right-click **SAS Content Server**. Then, in the right pane, right-click **Connection: SAS Content Server** and select **Properties**.

      iv. In the Connection: SAS Content Server Properties dialog box, click the **Options** tab and verify that the host name and port number values on that tab are correct.

      Note: By default, **Host name** and **Port number** are set to the values for the SAS 9.4 Web Server host name and port. However, for some varied configuration architecture (which consists of an external reverse-proxy server or an F5 load balancer), the values for the host name and port are those for the configured server machine.

   b. Verify that the SAS Web Server services is running. To do that, open the SAS Web Server log file (error_*date_timestamp*.log) that resides in ***SAS-configuration-directory*/Lev1/Web/WebServer/logs/**. Search for the following message to confirm that the services are running.

      ```
      [Wed Sep 07 08:08:52 2016] [Notice] Child 12372: Starting thread
      to listen on port 80.
      The SAS [Config-Lev1] httpd-WebServer service is running.
      ```

   c. Submit the following command to verify that the SAS Web Server host name is resolved properly via the Domain Name Server (DNS):

      ```
      nslookup host-name
      ```

(list continued)

In this command, *host-name* is the fully qualified host name of the machine where you are executing the NSLOOKUP command. When you execute this command, it returns the DNS location and the IP address from which the host name is resolved.

2. Verify the availability of SAS 9.4 Content Server or the SAS 9.4 Web Application Server (SASServer1_1), as follows:

   a. Verify the protocol and port configuration for SAS Content Server in metadata.

      i. Log on to SAS Management Console using the **`sasadm`** user ID.

      ii. On the **Plug-ins** tab, select **Environment Management** ► **Server Manager**.

      iii. Right-click **SAS Content Server**. Then, in the right pane, right-click **Connection: SAS Content Server** and select **Properties**.

      iv. In the Connection: SAS Content Server Properties dialog box, click the **Options** tab and verify that the protocol and port number values on that tab are correct.

   Note: For a non-secure, server-layer configuration, the correct protocol is HTTP. For configurations that are enabled with SSL, the correct protocol is HTTPS. If SAS Content Server is configured using an external URL that points to an external reverse-proxy server of an F5 load balancer, the content server's proxyName, proxyPort, and scheme definition values should match those that are in the `<connector>` HTML tag in the server.xml file for the SASServer_1 web application server.

   b. Verify that the SAS Web Application Server (SASServer1_1) services are running and that the SAS Content Server repository starts appropriately. To do that:

      i. Review the SAS SASServer1_1 log file (server.log) to verify that there are no errors during start-up. The log file resides in the directory ***`SAS-configuration-directory`*****`/Lev1/Web/WebAppServer/SASServer1_1/logs/`**.

      ii. In the log file, also search for a message similar to the following to confirm that the services start successfully.

```
Server startup in 979797 ms
```

   c. Review the SASContentServer9.4.log file to verify that there are no errors. The log file resides in ***`SAS-configuration-directory`*****`/Lev1/Web/Logs/SASServer1_1/`**. In the log file, also search for the following message to confirm that SAS Content Server Repository services start successfully.

```
INFO org.apache.jackrabbit.core.RepositoryImpl - Repository
started (5115ms)
```

   If you see the errors that are shown below in the SASContentServer9.4.log file (which indicate inconsistency between the SAS Content Server Repository index and content items), collect all of the log and configuration information that is discussed in SAS Note 58979. (**`support.sas.com/kb/58/979.html`**) Then send the logs and other configuration information to SAS Technical Support as instructed in the note.

```
o  INFO 2016-09-13 23:08:48,119 [main] - default: checking
   workspace consistency...

o  ERROR 2016-09-13 23:08:54,609 [main] - Error while reading blob
   id: java.io.EOFException
```

(list continued)

```
o  ERROR 2016-09-13 23:08:54,609 [main] - failed to read bundle:
   12b8f4f5-5b57-4268-bed4-92fafe14b273: java.lang.Exception:
   invalid bundle, see previous BundleBinding error log entry
```

d. If you receive PKIX security errors, verify that security cacerts or jssecacerts certificates for the SAS Management Console client are the same as those that are configured on the middle-tier machine. For more information, see SAS Note 39690, "Validating the SAS® Content Server in SAS Management Console generates the error 'unable to find valid certification path'." (**support.sas.com/kb/39/690.html**)

e. Verify that the Java Virtual Machine (JVM) parameters are set correctly in the JVM arguments for both the Central Authentication Server and the Service Server. For details about how to locate the JVM parameters, see SAS Note 52214, "The SAS 9.4 Content Server dircontens.jsp URL does not work after you implement a Secure Sockets Layer (SSL) configuration." (**support.sas.com/kb/52/214.html**)

3. Verify whether the authentication information that is passed from the underlying HTTP request to SAS Content Server is correct, as follows:

a. Determine whether SAS Content Server in SAS Management Console is configured to use one-time user ID and password authentication instead of SAS token authentication. If the configuration is for a one-time authentication, the password is not valid in certain cases. After the initial request, authentication fails during cookie handling because the password that is passed is no longer valid.

To determine which type of authentication you have:

i. Log on to SAS Management Console using the **sasadm** user ID.

ii. Click the **Plug-ins** tab and select **Environment Management ► Server Manager**.

iii. Right-click **SAS Content Server** in the right pane of the application window.

iv. Then, right-click **Connection: SAS Content Server** in the right pane and select **Properties**.

b. In the Connection: SAS Content Server Properties dialog box, click the **Options** tab. Verify that the value is **Authentication Type**, which should match to the SCHEMA= value in the web application server's server.xml file. The SCHEMA= option in the server.xml file is found in a `<connector>` parameter similar to the following example:

```
<connector acceptCount="100" bindOnInit="false"
connectionTimeout="20000" executor="tomcatThreadPool"
maxHttpHeaderSize="16384" maxKeepAliveRequests="15"
maxSwallowSize="-1" port="${bio.http.port}"
protocol="org.apache.coyote.http11.Http11Protocol"
proxyName="d7b227.na.sas.com" proxyPort="80"
redirectPort="${bio.https.port}" scheme="http"
useBodyEncodingForURI="true"/>
```

This example shows **http** as the value, but the value might be **https** if the Secure Sockets Layer protocol is enabled.

(list continued)

c. Navigate to the SAS Content Server (SASServer1_1 web application server) setenv.sh script (in the Linux operating environment) or the wrapper.conf file (in Microsoft Windows operating environments) and locate the following SAS Content Server JVM parameters:

```
-Dsas.scs.cas.scheme=

-Dsas.scs.svc.scheme=
```

Ensure that the protocol for both scheme parameters is set correctly. If the configuration is enabled with SSL, the parameter should be set to HTTPS. If SSL is not enabled, the parameter should be set to HTTP, which should match the SAS Content Server configuration in the SAS metadata. To verify that the correct protocol is set, follow these steps:

   i. In SAS Management Console, select **Environment Management ► Server ► SAS Content Server**.

   ii. In the right pane, right-click **Connection: SAS Content Serve**r and select **Properties**.

   iii. On the **Options** tab, verify that the value for **Authentication Type** is set to the appropriate protocol parameter.

Also ensure that relevant Cross-Site Request Forgery (CSRF) filters are set correctly, as discussed in the following SAS Notes:

- SAS Note 55044**,** "SAS® Web Infrastructure Platform applications (including SAS® Logon Manager) might be vulnerable to Cross-Site Forgery attacks" (**support.sas.com/kb/55/044.html**)
- SAS Note 52214, "The SAS® 9.4 Content Server dircontents.jsp URL does not work after you implement a Secure Sockets Layer (SSL) configuration" (**support.sas.com/kb/52/214.html**)
- SAS Note 56451, "The error 'The Application is not authorized to use SAS Logon Manager' occurs when you try to log on to SAS® Environment Manager" (**support.sas.com/kb/56/451.html**)

4. Verify whether the object that is being exported from SAS Management Console exists in the SAS Content Server repository, as follows:

   a. Verify that the user ID used to validate SAS Content Server has sufficient Read and Write permissions in SAS Metadata Server. The user ID must be valid and have the same rights (or equivalent rights) as the **sasadm@saspw** account.

   To verify the user ID:

      i. Log on to SAS Management Console using the **sasadm** user ID.

      ii. Click the **Plug-ins** tab and select **Environment Management ► Select User Manager**.

      iii. In the right pane, right-click the user ID and select **Properties**.

      iv. In the *user-name* Properties dialog box, look at the **Authorization permissions** under **Group and Roles**, to verify that the user has the appropriate rights.

(list continued)

b. Verify that the defined base path within the metadata in the SAS Content Server configuration actually exists, as follows:

   i. Log on to SAS Management Console using the `sasadm` user ID.

   ii. Click the **Plug-ins** tab and select **Environment Management ► Server Manager**.

   iii. Right-click **SAS Content Server** and select **Properties**.

   iv. In the Connection: SAS Content Server Properties dialog box, click the **Options** tab. On that tab, locate the **Check the Base Path (s): Select Items** definition and verify that the folder path that is defined actually does exist within the SAS Content Server repository. To verify that path, access the SAS Content Server Administration Console by using the following URL.

   ```
   protocol://host-name:port/SASContentServer/dircontents.jsp
   ```

   In this path, specify your SAS 9.4 configuration values for *protocol*, *host-name*, and *port*.

c. Verify that the WebDAV Repository configuration (under **Foundation Services**) is correct for all the listed services that are configured with WebDAV Repository.

d. Log on to SAS Management Console with the `sasadm` user ID.

e. Click the **Plug-ins** tab and select **Environment Management ► Foundation Services Manager ► Platform Local Services ► Core**.

f. Right-click **Information Service** and select **Properties**.

g. In the Information Service Properties dialog box, click the **Service Configuration** tab. On that tab, click the **Configuration** button to open the Information Service Configuration dialog box.

h. On the **Repositories** tab, select `WebDAV` as the value for **Information Repositories**.

i. Click **Edit** to open the DAV Repository Definition dialog box. In the dialog box, verify that the **Base** field is set to the path:

```
/SASContentServer/repository/default/sasdav
```

Perform the steps above for each of the following services that are listed under **Foundation Services Manager** in SAS Management Console:

- **Remote Services**
- **SASBIPortlets4.4 Local Services**
- **SASJSR168RemotePortlet4.4 Local Services**
- **SASPackageViewer4.4 Local Services**
- **SASPortal4.4 Local Services**
- **SASStoredProces9.4 Local Services**
- **SASStudioMidTier3.5 Local Services**

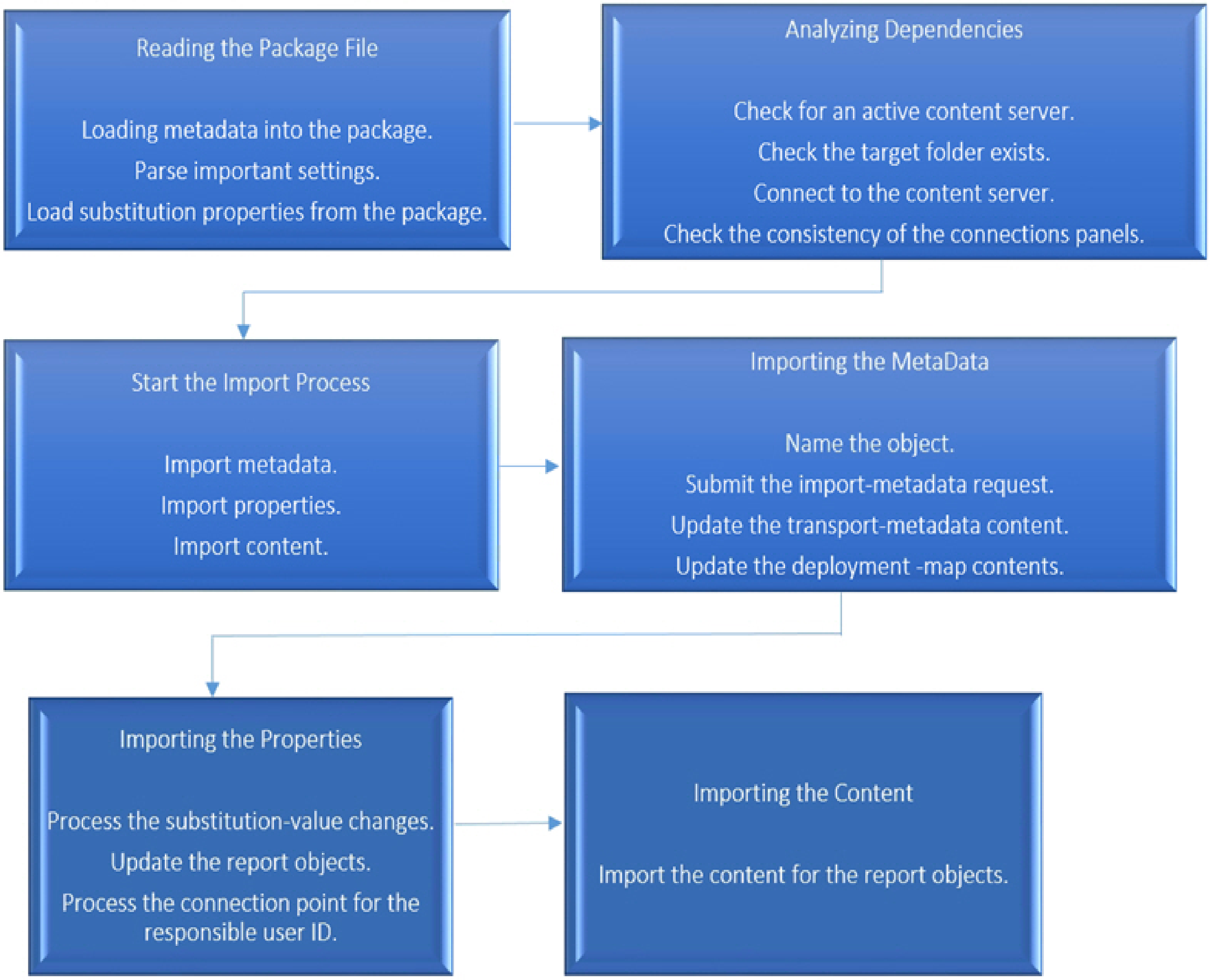
Importing SAS® Packages into SAS® Management Console

The following sections explain the process flow that occurs when you import a SAS package to SAS Management Console and show the errors that you might encounter during that process.

For details about the import process, see "Example Usage Scenario for the Export SAS Package and Import SAS Package Wizards" in "Chapter 22: Using the Export SAS Package and Import SAS Package Wizards" of the *SAS® 9.4 Intelligence Platform: System Administration Guide, Fourth Edition* at **support.sas.com/documentation/cdl/en/bisag/68240/PDF/default/bisag.pdf**.

Understanding the "Importing SAS Package" Request

You use the **Importing SAS Package** request in SAS Management Console to import a SAS Content Server item. The flow for the import process is shown below:


Reading the Package File
Loading metadata into the package.
Parse important settings.
Load substitution properties from the package.
Analyzing Dependencies
Check for an active content server.
Check the target folder exists.
Connect to the content server.
Check the consistency of the connections panels.
Start the Import Process
Import metadata.
Import properties.
Import content.
Importing the MetaData
Name the object.
Submit the import-metadata request.
Update the transport-metadata content.
Update the deployment -map contents.
Importing the Properties
Process the substitution-value changes.
Update the report objects.
Process the connection point for the responsible user ID.
Importing the Content
Import the content for the report objects.

Troubleshooting Steps

When you import packages into SAS Management Console, you might encounter one of the following errors:

- `DEBUG – Analyze exception: com.sas.metadata.promotion.MetadataPromotionException: Content Mapping was unable to connect to host "demo.test.domain", port "80"`
- `DEBUG – Analyze exception: com.sas.metadata.promotion.MetadataPromotionException: '503: Service Unavailable" error while accessing 'http://demo.test.domain/SASContentServer/repository/default/sasfolders/Shared Data/'`

Note: These problems can occur because the content for the packages is stored in SAS Content Server. Therefore, the troubleshooting steps in this section focus on the relevant root-cause analysis of the issue that is related to SAS Content Server. For issues that are related specifically to SAS Management Console, contact the SAS Management Console support team at **support.sas.com/ctx/supportform/createForm**.

To resolve these errors, perform the following steps:

1. Verify the status of the SAS 9.4 Apache HTTPD web server by ensuring that you can ping the server. If the ping fails, follow these steps:

    a. Verify the host name and port configuration for SAS Content Server in the metadata, as follows:

        i. Log on to SAS Management Console using the **sasadm** user ID.

        ii. On the **Plug-in**s tab, select **Environment Management** ► **Server Manager**.

        iii. Right-click **SAS Content Server**. Then, in the right pane, right-click **Connection: SAS Content Server** and select **Properties**.

        iv. In the Connection: SAS Content Server Properties dialog box, click the **Options** tab and verify that the host name and port number values on that tab are correct.

    Note: By default, **Host name** and **Port number** are set to the values for the SAS 9.4 Web Server host name and port. However, for some varied configuration architecture (which consists of an external reverse-proxy server or an F5 load balancer), the values for the host name and port are those for the configured server machine.

    b. Verify that the SAS Web Server services is running. To do that, open the SAS Web Server log file (error_*date_timestamp*.log) that resides in ***SAS-configuration-directory*/Lev1/Web/WebServer/logs/**. Search for the following message to confirm that the services are running.

    ```
    [Wed Sep 07 08:08:52 2016] [Notice] Child 12372: Starting thread
    to listen on port 80.
    The SAS [Config-Lev1] httpd-WebServer service is running.
    ```

    c. Submit the following command to verify that the SAS Web Server host name is resolved properly via the Domain Name Server (DNS):

    ```
    nslookup host-name
    ```

    In this command, *host-name* is the fully qualified host name of the machine where you are executing the NSLOOKUP command. When you execute this command, it returns the DNS location and the IP address from which the host name is resolved.

(list continued)

2. Verify the status of the SAS 9.4 Content Server or the SAS 9.4 Web Application Server (SASServer1_1), as follows:

   a. Verify the protocol and port configuration for SAS Content Server in metadata.

      i. Log on to SAS Management Console using the `sasadm` user ID.

      ii. On the **Plug-ins** tab, select **Environment Management** ► **Server Manager**.

      iii. Right-click **SAS Content Server**. The, in the right pane, right-click **Connection: SAS Content Server** and select **Properties**.

      iv. In the Connection: SAS Content Server Properties dialog box, click the **Options** tab and verify that the protocol and port number values on that tab are correct.

      Note: For a non-secure, server-layer configuration, the correct protocol is HTTP. For configurations that are enabled with SSL, the correct protocol is HTTPS. If SAS Content Server is configured using an external URL that points to an external reverse-proxy server of an F5 load balancer, the content server's proxyName, proxyPort, and scheme definition values should match those that are in the `<connector>` HTML tag in the server.xml file for the SASServer_1 web application server.

   b. Verify that the SAS® Web Application Server (SASServer1_1) services are running and that the SAS Content Server repository starts without errors. To do that:

      i. Review the SAS SASServer1_1 log file (server.log) to verify that there are no errors during start-up. The log file resides in this directory:

      ***SAS-configuration-directory*/Lev1/Web/WebAppServer/ SASServer1_1/logs/**

      ii. In the log file, also search for a message similar to the following to confirm that the services start successfully.

      ```
      Server startup in 979797 ms
      ```

   c. Review the SASContentServer9.4.log file to verify that there are no errors. The log file resides in ***SAS-configuration-directory*/Lev1/Web/Logs/SASServer1_1/**. In the log file, also search for the following message to confirm that SAS Content Server Repository services start successfully.

   ```
   INFO org.apache.jackrabbit.core.RepositoryImpl - Repository
   started (5115ms)
   ```

   If you see the errors that are shown below in the SASContentServer9.4.log file (which indicate inconsistency between the SAS Content Server Repository index and content items), collect all of the log and configuration information that is discussed in SAS Note 58979. (**support.sas.com/kb/58/979.html**) Then send the logs and other configuration information to SAS Technical Support as instructed in the note.

   - `INFO 2016-09-13 23:08:48,119 [main] - default: checking workspace consistency...`
   - `ERROR 2016-09-13 23:08:54,609 [main] - Error while reading blob id: java.io.EOFException`

(list continued)

- `ERROR 2016-09-13 23:08:54,609 [main] - failed to read bundle: 12b8f4f5-5b57-4268-bed4-92fafe14b273: java.lang.Exception: invalid bundle, see previous BundleBinding error log entry`

d. If you receive PKIX security errors, verify that security cacerts or jssecacerts certificates for the SAS Management Console client are the same as those that are configured on the middle-tier machine. For more information, see SAS Note 39690, "Validating the SAS® Content Server in SAS Management Console generates the error 'unable to find valid certification path'." (**support.sas.com/kb/39/690.html**)

e. Verify that the Java Virtual Machine (JVM) parameters are set correctly in the JVM arguments for both the Central Authentication Server and the Service Server. For details about how to locate the JVM parameters, see SAS Note 52214, "The SAS 9.4 Content Server dircontens.jsp URL does not work after you implement a Secure Sockets Layer (SSL) configuration." (**support.sas.com/kb/52/214.html**)

3. Verify whether the authentication information that is passed from the underlying HTTP request to SAS Content Server is correct, as follows:

a. Determine whether SAS Content Server in SAS Management Console is configured to use one-time user ID and password authentication instead of SAS token authentication. If the configuration is for a one-time authentication, the password is not valid in certain cases. After the initial request, authentication fails during cookie handling because the password that is passed is no longer valid.

To determine which type of authentication you have:

i. Log on to SAS Management Console using the **sasadm** user ID.

ii. Click the **Plug-ins** tab and select **Environment Management ► Server Manager**.

iii. Right-click **SAS Content Server** in the right pane of the application window.

iv. Then, right-click **Connection: SAS Content Server** in the right pane and select **Properties**.

b. In the Connection: SAS Content Server Properties dialog box, click the **Options** tab. Verify that the value is **Authentication Type**, which should match to the SCHEMA= value in the web application server's server.xml file. The SCHEMA= option in the server.xml file is found in a `<connector>` parameter similar to the following example:

```
<connector acceptCount="100" bindOnInit="false"
connectionTimeout="20000" executor="tomcatThreadPool"
maxHttpHeaderSize="16384" maxKeepAliveRequests="15"
maxSwallowSize="-1" port="${bio.http.port}"
protocol="org.apache.coyote.http11.Http11Protocol"
proxyName="d7b227.na.sas.com" proxyPort="80"
redirectPort="${bio.https.port}" scheme="http"
useBodyEncodingForURI="true"/>
```

This example shows **`http`** as the value, but the value might be **`http`** if the Secure Sockets Layer protocol is enabled.

(list continued)

b. Navigate to the SAS Content Server (SASServer1_1 web application server) setenv.sh script (in the Linux operating environment) or the wrapper.conf file (in Microsoft Windows operating environments) and locate the following SAS Content Server JVM parameters:

```
-Dsas.scs.cas.scheme=

-Dsas.scs.svc.scheme=
```

Ensure that the protocol for both scheme parameters is set correctly. If the configuration is enabled with SSL, the parameter should be set to HTTPS. If SSL is not enabled, the parameter should be set to HTTP, which should match the SAS Content Server configuration in the SAS metadata. To verify that the correct protocol is set, follow these steps:

i. In SAS Management Console, select **Environment Management ► Server ► SAS Content Server**.

ii. In the right pane, right-click **Connection: SAS Content Serve**r and select **Properties**.

iii. On the **Options** tab, verify that the value for **Authentication Type** is set to the appropriate protocol parameter.

Also ensure that relevant Cross-Site Request Forgery (CSRF) filters are set correctly, as discussed in the following SAS Notes:

- SAS Note 55044**,** "SAS® Web Infrastructure Platform applications (including SAS® Logon Manager) might be vulnerable to Cross-Site Forgery attacks" (**`support.sas.com/kb/55/044.html`**)
- SAS Note 52214, "The SAS® 9.4 Content Server dircontents.jsp URL does not work after you implement a Secure Sockets Layer (SSL) configuration" (**`support.sas.com/kb/52/214.html`**)
- SAS Note 56451, "The error 'The Application is not authorized to use SAS Logon Manager' occurs when you try to log on to SAS® Environment Manager" (**`support.sas.com/kb/56/451.html`**)

4. Verify whether the object that is being imported into SAS Management Console exists in the SAS Content Server Repository.

a. Verify that the user ID used to validate SAS Content Server has sufficient Read and Write permissions in SAS Metadata Server. The user ID must be valid and have the same rights (or equivalent rights) as the **`sasadm@saspw`** account.

To verify the user ID rights:

i. Log on to SAS Management Console using the **`sasadm`** user ID.

ii. Click the **Plug-ins** tab and select **Environment Management ► User Manager**.

iii. In the right pane, right-click the user ID and select **Properties**.

iv. In the *user-name* Properties dialog box, look at the **Authorization permissions** under **Group and Roles**, to verify that the user has the appropriate rights.

(list continued)

b. Verify that the defined base path within the metadata in the SAS Content Server configuration actually exists, as follows:

   i. Log on to SAS Management Console using the **`sasadm`** user ID.

   ii. Click the **Plug-ins** tab and select **Environment Management ► Server Manager**.

   iii. Right-click **SAS Content Server** and select **Properties**.

   iv. In the Connection: SAS Content Server Properties dialog box, click the **Options** tab. On that tab, locate the **Check the Base Path (s): Select Items** definition and verify that the folder path that is defined actually does exist within the SAS Content Server Repository. To verify that path, access the SAS Content Server Administration Console by using the following URL.

   ***protocol*://*host-name*:*port*/SASContentServer/dircontents.jsp**

   In this path, specify your SAS 9.4 configuration values for *protocol*, *host-name*, and *port*.

c. Verify that the WebDAV Repository configuration (under **Foundation Services**) is correct for all the listed services that are configured with WebDAV Repository, as follows:

   i. Log on to SAS Management Console with the **`sasadm`** user ID.

   ii. Click the **Plug-ins** tab and select **Environment Management ► Foundation Services Manager ► Platform Local Services ► Core.**

   iii. Right-click **Information Service** and select **Properties**.

   iv. In the Information Service Properties dialog box, click the **Service Configuration** tab. On that tab, click the **Configuration** button to open Information Service Configuration dialog box.

   v. On the **Repositories** tab, select **`WebDAV`** as the value for Information Repositories.

   vi. Click **Edit** to open the DAV Repository Definition dialog box. In the dialog box, verify that the **Base** field is set to the following path:

   `/SASContentServer/repository/default/sasdav`

   Perform the steps above for each of the following services that are listed under **Foundation Services Manager** in SAS Management Console:

   - **Remote Services**
   - **SASBIPortlets4.4 Local Services**
   - **SASJSR168RemotePortlet4.4 Local Services**
   - **SASPackageViewer4.4 Local Services**
   - **SASPortal4.4 Local Services**
   - **SASStoredProces9.4 Local Services**
   - **SASStudioMidTier3.5 Local Services**

Still Not Solved?

If you are still experiencing problems after performing the steps in the previous section, open a track with SAS Technical Support. Be sure to include the following information in the track:

- a description of the problem
- the title and URL of the specific troubleshooting document that you used
- your code and logs
- the information that you gather from SAS 9.4 Content Server

Resources

SAS Institute Inc. 2010. SAS Note 39690, "Validating SAS® Content Server in SAS® Management Console generates the error 'unable to find valid certification path' ." SAS Institute Inc.: Cary, NC. Available at **support.sas.com/kb/39/690.html**.

SAS Institute Inc. 2014. SAS Note 52214, "The SAS® 9.4 Content Server dircontents.jsp URL does not work after you implement a Secure Sockets Layer (SSL) configuration." SAS Institute Inc.: Cary, NC. Available at **support.sas.com/kb/52/214.html**.

SAS Institute Inc. 2014. SAS Note 55044, "SAS® Infrastructure Platform applications (including SAS Logon Manager) might be vulnerable to Cross-Site Request Forgery attacks." SAS Institute Inc.: Cary, NC. Available at **support.sas.com/kb/55/044.html**.

SAS Institute Inc. 2015. SAS Note 56451, "The error 'The Application is not authorized to use SAS Logon Manager' occurs when you try to log on to SAS® Environment Manager." SAS Institute Inc.: Cary, NC. Available at **support.sas.com/kb/56/451.html**.

SAS Institute Inc., 2016. *SAS® 9.4 Intelligence Platform: Middle-Tier Administration Guide, Third Edition*. SAS Institute Inc.: Cary, NC. Available at **support.sas.com/documentation/cdl/en/bimtag/68217/PDF/default/bimtag.pdf**.

SAS Institute Inc., 2016. *SAS® 9.4 Intelligence Platform: System Administration Guide, Fourth Edition*. SAS Institute Inc.: Cary, NC. Available at **support.sas.com/documentation/cdl/en/bisag/68240/PDF/default/bisag.pdf**.