Configuration Guidelines and Details for "HOSTNAME.example.com"

Overview

Warnings and Notices

The following issues occurred during the automated portion of your configuration and must be addressed before proceeding.

- Some of the clients in your environment may need access to the SAS/GRAPH Java applets to view graphical output generated by SAS processes. If so, add the APPLETLOC option to the sasv9_usermods.cfg file located in each SAS Application Server context directory specifying the location to be used in generating graphical output. APPLETLOC should point to a network accessible copy of the SAS/GRAPH Java applets.

  Since your deployment includes the SAS Web Infrastructure Platform, the applets can be made available (you must use the correct host and port) via:

  ```
  -APPLETLOC "http://mid-tier-server:mid-tier-port/sasweb/graph"
  ```

- Permissions on the logs directory (/data/SASConfigManualM2/Lev1/Web/Logs) are currently set at 777. We strongly recommend that you narrow access to this directory. To facilitate creation of logs, make sure that the SAS Installer (sasinst) and the invoker of the Web application server can write to this directory. To facilitate appropriate use of the logs, make sure that administrators can see the directory.

- Because you selected to not automatically deploy your SAS Web Applications, you will need to perform some manual steps to complete the configuration of your SAS Web Applications. Once you have deployed the SAS Web Infrastructure Platform, you will need to manually load content to the SAS Content Server. Follow the instructions below to accomplish this.

SAS Management Console

SAS Management Console is required to complete many of the following steps.

Startup command	/data/SAS92M2/SASManagementConsole/9.2/sasmc For easier access, the installation directory /data/SAS92M2/SASManagementConsole/9.2 can be placed in the executable path environment. Likewise, aliases or symbolic links can be created to reference the command.
User ID	SAS Administrator user ID
Password	Enter the password you created in the SAS Deployment Wizard.

SAS Application Servers

SASMeta - Metadata Server

Host machine	HOSTNAME.example.com
Port	8561
Log directory	/data/SASConfigManualM2/Lev1/SASMeta/MetadataServer/Logs For more details about the initial logging configuration and how to modify it, see "Administering Logging for SAS Servers" in the *SAS Intelligence Platform: System Administration Guide* at http://support.sas.com/documentation/onlinedoc/intellplatform/index.html#intell92.
Execution type	Shell script /data/SASConfigManualM2/Lev1/SASMeta/MetadataServer/MetadataServer.sh

Notes:

- The metadata server is configured to use journaling. The metadata journal file is located at **/data/SASConfigManualM2/Lev1/SASMeta/MetadataServer/Journal/MetadataJournal.dat**. The metadata journal file is updated more quickly than repositories and updated metadata becomes available to clients sooner. Journaling also improves the ability to recover the server and can be recovered from the state of the journal file when the metadata server is restarted.
- In the event of severe problems, the metadata server has been instructed to send alert e-mail to **admin@example.com** with the sender of the e-mail being identified as **SASMeta - Metadata Server (SASConfigManualM2 - Lev1) <admin@example.com>**.

SASApp - OLAP Server

Host machine	HOSTNAME.example.com
Port	5451
Log directory	/data/SASConfigManualM2/Lev1/SASApp/OLAPServer/Logs For more details about the initial logging configuration and how to modify it, see "Administering Logging for SAS Servers" in the *SAS Intelligence Platform: System Administration Guide* at http://support.sas.com/documentation/onlinedoc/intellplatform/index.html#intell92.
Validation steps	1. In the SAS Management Console, on the Plug-ins tab, select "+" to expand the Server Manager node. 2. Expand SASApp. 3. Highlight the SASApp - Logical OLAP Server. 4. Right mouse click this server and select Validate. You should see a *Validation Successful* message.
Execution type	Shell script /data/SASConfigManualM2/Lev1/SASApp/OLAPServer/OLAPServer.sh

SASApp - Stored Process Server

Host machine	HOSTNAME.example.com
Port	8601
Log directory	/data/SASConfigManualM2/Lev1/SASApp/StoredProcessServer/Logs For more details about the initial logging configuration and how to modify it, see "Administering Logging for SAS Servers" in the *SAS Intelligence Platform: System Administration Guide* at http://support.sas.com/documentation/onlinedoc/intellplatform/index.html#intell92.
Validation steps	1. In the SAS Management Console, on the Plug-ins tab, select "+" to expand the Server Manager node. 2. Expand SASApp. 3. Highlight the SASApp - Logical Stored Process Server. 4. Right mouse click this server and select Validate. You should see a *Validation Successful* message.

SASMeta - Workspace Server

Host machine	HOSTNAME.example.com
Validation steps	The SASMeta - Workspace Server should be used for only a few designated administrative tasks. It is appropriate to defer validation of this server until you have set up the SAS users who will perform these tasks. This server requires an external account and is available to only the SAS Administrators group.

Notes:

- The /data/SASConfigManualM2/Lev1/SASMeta/WorkspaceServer/Logs directory is intended to serve as a placeholder for workspace server logs. Workspace server logs may be directed to this directory in the event that your SAS or IT administrator enables logging. The following default attributes are associated with the Logs directory:
  - Universal read, write or execute access is disabled for the directory in order to comply with default installation security requirements
  - Execution of a workspace server does not populate the Logs directory
  - The Logs directory serves as a placeholder should you enable logging for workspace servers

  Enabling workspace server logging should be carefully considered, due to the proliferation of workspace server logs, as well as the requirement to grant universal write access to the Logs directory. To enable workspace server logging, perform the following steps:
  - Enable read, write and execute access to the Logs directory
  - Modify the workspace server logconfig.xml to enable the desired levels of logging
  - Alternately, enable the logconfig.trace.xml logging file to capture workspace server diagnostic logging

SASApp - Workspace Server

Host machine	HOSTNAME.example.com
Port	8591
Log directory	/data/SASConfigManualM2/Lev1/SASApp/WorkspaceServer/Logs For more details about the initial logging configuration and how to modify it, see "Administering Logging for SAS Servers" in the *SAS*

	Intelligence Platform: System Administration Guide at http://support.sas.com/documentation/onlinedoc/intellplatform/index.html#intell92.
Validation steps	1. In the SAS Management Console, on the Plug-ins tab, select "+" to expand the Server Manager node. 2. Expand SASApp. 3. Highlight the SASApp - Logical Workspace Server. 4. Right mouse click this server and select Validate (you can enter sasdemo or the SAS Spawned Servers account for the user ID). You should see a *Validation Successful* message.

Notes:

- The /data/SASConfigManualM2/Lev1/SASApp/WorkspaceServer/Logs directory is intended to serve as a placeholder for workspace server logs. Workspace server logs may be directed to this directory in the event that your SAS or IT administrator enables logging. The following default attributes are associated with the Logs directory:
  - Universal read, write or execute access is disabled for the directory in order to comply with default installation security requirements
  - Execution of a workspace server does not populate the Logs directory
  - The Logs directory serves as a placeholder should you enable logging for workspace servers

  Enabling workspace server logging should be carefully considered, due to the proliferation of workspace server logs, as well as the requirement to grant universal write access to the Logs directory. To enable workspace server logging, perform the following steps:
  - Enable read, write and execute access to the Logs directory
  - Modify the workspace server logconfig.xml to enable the desired levels of logging
  - Alternately, enable the logconfig.trace.xml logging file to capture workspace server diagnostic logging

SAS BI Report Services Workspace Configuration

	Name ="SASApp - wrstemp" 1. In SAS Management Console, on the Plug-ins tab, select the "+" to expand the Data Library Manager node. 2. Select "+" to expand Libraries. 3. Select the library listed above. 4. Right mouse click this library and select Properties. 5. Click the Options tab and locate the path to the library in the Selected items text box. Review the documentation provided to determine if permissions need to be modified for the library or directory to which the library points.
Query Cache Library	1. For details, view the http://support.sas.com/documentation/onlinedoc/intellplatform/index.html#intell92 and refer to the document called **SAS 9.2 Intelligence Platform: Web Application Administration Guide**. 2. See the section called **Improving the Performance of SAS Web Report Studio**. 3. This section will contain a list of *Suggestions for Improving the Performance of SAS Web Report Studio*. Go to the information titled **"Using the Query Cache"**. 4. Refer to the subsection called **Manage Host Access to the Query Cache Library** for information regarding permissions.
Distribution Library	Name ="SASApp - wrsdist" 1. In SAS Management Console, on the Plug-ins tab, select the "+" to expand the Data Library Manager node. 2. Select "+" to expand Libraries. 3. Select the library listed above. 4. Right mouse click this library and select Properties. 5. Click the Options tab and locate the path to the library in the Selected items text box. Review the documentation provided to determine if permissions need to be modified for the library or directory to which the library points. 1. For details, view the http://support.sas.com/documentation/onlinedoc/intellplatform/index.html#intell92 and refer to the document called **SAS 9.2 Intelligence Platform: Web Application Administration Guide**. 2. See the section called **Pre-generated Reports From SAS Web Report Studio**. 3. Refer to the subsection called **Verifying Permissions for the Distribution Library** for information regarding permissions.
Validation steps	1. In SAS Management Console, on the Plug-ins tab, select "+" to expand the Data Library Manager node. 2. Verify the libraries named above are listed under the Data Library Manager. 3. In SAS Management Console, on the Plug-ins tab, select "+" to expand the Application Management node. 4. Select "+" to expand the Configuration Manager 5. Highlight BI Rep Svc Wkspace Config 4.2 6. Right mouse click and select Properties. 7. Click the Settings tab. 8. Validate the query cache library and the distribution library. They should match the libraries listed under Data Libraries.

SAS BI Report Services 4.2

Log directory	/data/SASConfigManualM2/Lev1/Applications/SASBIReportServices4.2/Logs For more details about how to modify your log format and to see what logging entails, see the *SAS Intelligence Platform: Web Application Administration Guide* at http://support.sas.com/documentation/onlinedoc/intellplatform/index.html#intell92.
Java Batch Server	Name ="SASApp - BRM Java Batch Server"
Configuration	Configuration Directory = "/data/SASConfigManualM2/Lev1/Applications/SASBIReportServices4.2"

Validation steps	**Java Batch Server** 1. In SAS Management Console, on the Plug-ins tab, select "+" to expand the Server Manager node. 2. Select "+" to expand SASApp. 3. Select "+" to expand the SASApp - Logical SAS Java Batch Server. 4. Verify the existence of the java batch server(s) referenced above. 5. Right mouse click this server and select Properties. 6. Click the Options tab. 7. Validate the command line by examining the parameter values and verifying file locations and the repository name. **Local Services** 1. In SAS Management Console, on the Plug-ins tab, select "+" to expand the Foundation Services Manager node. 2. Select "+" to expand the SASBIReportServices4.2 Local Services Definition. 3. Select "+" to expand Core. 4. Select the Logging Service. 5. Right mouse button and choose Properties. 6. Click the Service Configuration tab. 7. Click the Configuration button. 8. Verify the logging contexts. 9. Refer to the logging documentation at the link specified above for details. **outputgen.ini file** 1. The file outputgen.ini may need to be modified. This file is located in the install folder /data/SAS92M2/SASBIReportServices/4.2. 2. The following default settings for Java command line options appear in this file: java.net.preferIPv4Stack=true and java.net.preferIPv6Addresses=false. 3. If the system is configured to use IPv6, these values must be changed to: java.net.preferIPv4Stack=false and java.net.preferIPv6Addresses=true.

SASApp - Pooled Workspace Server

Host machine	HOSTNAME.example.com
Port	8701
Validation steps	1. In the SAS Management Console, on the Plug-ins tab, select "+" to expand the Server Manager node. 2. Expand SASApp. 3. Highlight the SASApp - Logical Pooled Workspace Server. 4. Right mouse click this server and select Validate. You should see a *Validation Successful* message.

SASMeta - SAS DATA Step Batch Server

Host machine	HOSTNAME.example.com
Log directory	/data/SASConfigManualM2/Lev1/SASMeta/BatchServer/Logs For more details about the initial logging configuration and how to modify it, see "Administering Logging for SAS Servers" in the *SAS Intelligence Platform: System Administration Guide* at http://support.sas.com/documentation/onlinedoc/intellplatform/index.html#intell92.
Validation steps	1. Execute the following command: /data/SASConfigManualM2/Lev1/SASMeta/BatchServer/sasbatch.sh 2. If SAS starts successfully, the DATA step batch server has been validated.

SAS Spawners

Object Spawner

Host machine	HOSTNAME.example.com
Port	8581
Log directory	/data/SASConfigManualM2/Lev1/ObjectSpawner/Logs For more details about the initial logging configuration and how to modify it, see "Administering Logging for SAS Servers" in the *SAS Intelligence Platform: System Administration Guide* at http://support.sas.com/documentation/onlinedoc/intellplatform/index.html#intell92.
Execution type	Shell script /data/SASConfigManualM2/Lev1/ObjectSpawner/ObjectSpawner.sh

SAS Table Server

Host machine	HOSTNAME.example.com
Port	2171
Log directory	[/data/SASConfigManualM2/Lev1/SASTS/TableServer/Logs](#) For more details about the initial logging configuration and how to modify it, see "Administering Logging for SAS Servers" in the *SAS Intelligence Platform: System Administration Guide* at [http://support.sas.com/documentation/onlinedoc/intellplatform/index.html#intell92](#).
Execution type	Shell script /data/SASConfigManualM2/Lev1/SASTS/TableServer/TableServer.sh

SAS Deployment Tester Server

Host machine	HOSTNAME.example.com
Port	10021
Execution type	Shell script /data/SASConfigManualM2/Lev1/DeploymentTesterServer/DeploymentTesterServer.sh
Validation steps	1. In SAS Management Console, on the Plug-ins tab, select "+" to expand the Application Management node. 2. Select "+" to expand Deployment Tester 3. Highlight the host machine: HOSTNAME.example.com 4. Right mouse click and select Run All Test Suites. 5. Select "+" to expand the Results. 6. Validate the results for each test suite. All tests should pass.

Notes:

- Deployment Tester Server is used to run tests on SAS products and servers to validate functionality and proper operation. The Deployment Tester Server in conjunction with the Deployment Tester SMC plug-in allows for tests to be executed on remote systems from a single SMC instance. Select Help on Deployment Tester in the SMC Help menu for more information.

Remote Services

Host machine	HOSTNAME.example.com
Port	5091
Execution type	Shell script /data/SASConfigManualM2/Lev1/Web/Applications/RemoteServices/RemoteServices.sh

- SAS Remote Services needs to be restarted after each reboot of your system. The above command can be used to perform this action. Note, it is imperative that SAS Remote Services is started **before** starting the web application server.

Web Application Server

Application Server Name	WebLogic
Vendor	BEA
Version	9.2
WebLogic Install Dir (WL_HOME)	[/data/bea923sdw/weblogic92](#)
Domain Name	SASDomain
Domain Dir	[/data/SASConfigManualM2/Lev1/Web/SASDomain](#)
Java JDK Vendor	HP
Host machine	HOSTNAME.example.com
WebLogic Server Administration Console URL	[http://HOSTNAME.example.com:7501/console](#)

Configure your WebLogic Application Server (Domain Configuration)

The following instructions provide a basic WebLogic configuration that uses SAS authentication and unsecure connections. This configuration should support a small number of users. If you need to setup a more sophisticated topology that includes reverse proxy servers, web server authentication, single sign-on, or secure socket connections, please see the *SAS 9.2 Intelligence Platform: Web Application Administration Guide* at [http://support.sas.com/documentation/onlinedoc/intellplatform/index.html#intell92](#) for additional details. Detailed configuration instructions on WebLogic are also available at the third-party vendor website located at [http://edocs.bea.com/](#). Before configuring your WebLogic domain for SAS applications, be sure to review the [WebLogic Post-Installation Steps](#) if you have not already done so.

Since this is a manual configuration you will need to either create a new WebLogic domain or add servers to an existing one. You can create new domains or manage existing ones using the WebLogic Configuration Wizard. For your reference, a sample domain has been created. Depending on the SAS

applications included in your plan, you will also need to configure other resources as listed below.

Sample Domain Location: [/data/SASConfigManualM2/Lev1/Web/SASDomain](#)

Configuration steps prior to starting WebLogic servers for your SAS domain:

- **Set EnforceValidBasicAuthCredentials to False**
    1. Locate and edit the config.xml file in your domain. It is located here:

       [/data/SASConfigManualM2/Lev1/Web/SASDomain/config/config.xml](#)

    2. Add the following line within the `<security-configuration>` element:

       `<enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-credentials>`

Configure Node Manager

There are several ways to manage the starting and stopping of WebLogic servers. If you wish to launch servers through the Weblogic Server Administration Console, you will need to configure and start a WebLogic Node Manager. You can also use scripts to launch the servers. The generated sample domain includes the appropriate scripts and configuration to support both methods.

The WebLogic Server installation provides scripts to launch Node Manager in [/data/bea923sdw/weblogic92/server/bin](#). If you use these scripts to run a Node Manager that controls SAS domains, you will need to modify the script [/data/bea923sdw/weblogic92/common/bin/commEnv.sh](#). The settings in this script affect all WebLogic domains running this version of WebLogic on this machine.

The sample SAS domain contains Node Manager scripts that call a wrapper script for commEnv.sh that provides the correct settings for the SAS domain. By adopting this SAS wrapper script and the modified scripts to start Node Manager provided in the SAS sample domain, you can launch a separate copy of Node Manager for your SAS domain without impacting other WebLogic domains running on the same machine. Alternatively, you can incorporate the settings found in [/data/SASConfigManualM2/Lev1/Web/SASDomain/bin/commEnvSAS.sh](#) into your WebLogic installation directly.

By default, the Node Manager home directory is located in the WebLogic install area. The scripts provided with the SAS sample domain set the location to [/data/SASConfigManualM2/Lev1/Web/SASDomain/nodemanager](#). This prevents conflicts if other Node Managers are configured for non-SAS applications.

Start Node Manager

Be sure to read the section *Configure Node Manager* before launching the Node Manager. Depending on how you've chosen to configure your WebLogic installation and domain, you may choose to launch your own node manager script or the default script provided with WebLogic which is located at [/data/bea923sdw/weblogic92/server/bin/startNodeManager.sh](#)

You can start the process with `nohup` to allow it to continue running after you logout. Alternatively, you can run it as a daemon process.

Configure the WebLogic Administration Server (AdminServer)

There are no special SAS requirements for configuring the WebLogic Administration Server. Here are some of the configuration attributes for the sample domain:

- **Listen Port**: 7501
- **Server Logs Directory**: [/data/SASConfigManualM2/Lev1/Web/SASDomain/servers/AdminServer/logs](#)
- **JVM Options**: -Dcom.sun.xml.namespace.QName.useCompatibleSerialVersionUID=1.0 -Xms256m -Xmx512m -XX:PermSize=48m -XX:MaxPermSize=128m

Start the WebLogic Administration Server

To start the Administration Server for your domain, execute the startWebLogic.sh. For the sample domain, the script is located here: [/data/SASConfigManualM2/Lev1/Web/SASDomain/bin/bin/startWebLogic.sh](#)

Configuration steps to be performed from the WebLogic Administration Console:

Once the administration server is started, the remaining steps can be performed from the WebLogic Administration Console.

- **Ensure that Tunneling is enabled (TunnelingEnabled is set to true)**
    1. In the `Domain Structure` panel, go to `Environment -> Servers`.
    2. On the `Summary of Servers` page, select the link `AdminServer(admin)`.
    3. On the `Settings for AdminServer` page, select the `Protocols` tab.
    4. Select the `Enable Tunneling` checkbox.

Configure the WebLogic Managed Servers

There are two ways to launch the WebLogic Managed Servers. You can use the WebLogic Administration Console or batch scripts. These servers must be launched with the appropriate command line options. You will need to perform configuration steps to setup both methods.

- **Configure Managed Servers through the WebLogic Administration Console**

    For each managed server listed below, perform these instructions:

    1. In the `Domain Structure` panel, go to `Environment -> Servers`.
    2. On the `Summary of Servers` page, select the link for the Managed Server to be configured.
    3. On the "Settings for SASServerN" page, select the link `Server Start` tab.
    4. Paste the JVM Options listed below for the appropriate server into the `Arguments` text box.

- **Configure Managed Server Scripts**

    1. Locate and edit the file `setDomainEnv.sh` for your domain. Also, look at the copy in the sample domain:

/data/SASConfigManualM2/Lev1/Web/SASDomain/bin/bin/setDomainEnv.sh

2. In the sample domain version of setDomainEnv.sh, you will find SAS code between two sets of comments. You should copy this code into the equivalent location in your domain's copy of `setDomainEnv.sh`:

```
# set the following for SAS installs
...
# end set for SAS installs
```

WebLogic Managed Server Configuration Properties:

WebLogic Managed Server - SASServer1

Listen Port	7001
HTTPS Port	7002
JVM Options	-Dcom.sun.xml.namespace.QName.useCompatibleSerialVersionUID=1.0 -Dsas.server.name=Server1 -Xms768m -Xmx768m -XX:PermSize=512m -XX:MaxPermSize=512m -Xss256k -XX:NewSize=128m -XX:MaxNewSize=256m -XX:+UseConcMarkSweepGC -XX:-UseTLAB -XX:+DisableExplicitGC -XX:+CMSClassUnloadingEnabled -XX:+CMSPermGenSweepingEnabled -Dcom.sun.management.jmxremote -Djava.awt.headless=true -Dsun.rmi.dgc.client.gcInterval=3600000 -Dsun.rmi.dgc.server.gcInterval=3600000 -Dsas.jms.authentication.decorator=false -Dsas.container.identifier=weblogic -Dsas.auto.publish.port=7001 -Dcom.sas.services.logging.disableRemoteList=true -Dcom.sas.services.logging.disableRemoteLogging=true -Dtheme.sleep.time=10000 -Dtheme.max.tries=360 -Djavax.xml.soap.MessageFactory=com.sun.xml.messaging.saaj.soap.ver1_1.SOAPMessageFactory1_1Impl -Djava.net.preferIPv4Stack=true -Djava.net.preferIPv6Addresses=false -Dmulticast_udp_ip_ttl=1 -Dmulticast.address=239.9.20.36 -Dmulticast.port=8561 -Dcom.sas.log.config.url=file:///data/SASConfigManualM2/Lev1/Web/Common/LogConfig/ -Djava.security.auth.login.config=/data/SASConfigManualM2/Lev1/Web/Common/SASDomain/weblogicLogin.config
Server Logs Directory	/data/SASConfigManualM2/Lev1/Web/SASDomain/servers/SASServer1/logs

WebLogic Managed Server - SASServer2

Listen Port	7101
HTTPS Port	7102
JVM Options	-Dcom.sun.xml.namespace.QName.useCompatibleSerialVersionUID=1.0 -Dsas.server.name=Server2 -Xms768m -Xmx768m -XX:PermSize=512m -XX:MaxPermSize=512m -Xss256k -XX:NewSize=128m -XX:MaxNewSize=256m -XX:+UseConcMarkSweepGC -XX:-UseTLAB -XX:+DisableExplicitGC -XX:+CMSClassUnloadingEnabled -XX:+CMSPermGenSweepingEnabled -Dcom.sun.management.jmxremote -Djava.awt.headless=true -Dsun.rmi.dgc.client.gcInterval=3600000 -Dsun.rmi.dgc.server.gcInterval=3600000 -Dsas.jms.authentication.decorator=false -Dsas.container.identifier=weblogic -Dsas.auto.publish.port=7001 -Dcom.sas.services.logging.disableRemoteList=true -Dcom.sas.services.logging.disableRemoteLogging=true -Dtheme.sleep.time=10000 -Dtheme.max.tries=360 -Djavax.xml.soap.MessageFactory=com.sun.xml.messaging.saaj.soap.ver1_1.SOAPMessageFactory1_1Impl -Djava.net.preferIPv4Stack=true -Djava.net.preferIPv6Addresses=false -Dmulticast_udp_ip_ttl=1 -Dmulticast.address=239.9.20.36 -Dmulticast.port=8561 -Dcom.sas.log.config.url=file:///data/SASConfigManualM2/Lev1/Web/Common/LogConfig/ -Djava.security.auth.login.config=/data/SASConfigManualM2/Lev1/Web/Common/SASDomain/weblogicLogin.config
Server Logs Directory	/data/SASConfigManualM2/Lev1/Web/SASDomain/servers/SASServer2/logs

Configure MailSession - SASMailSession

Using the WebLogic Administration Console, create a mail session.

1. In the `Domain Structure` panel, go to `Services -> Mail Sessions`.
2. Click the `New` button.
3. Enter the name `SASMailSession` in the `Name` field, and click `OK`.
4. Select the link `SASMailSession`.
5. In the `JNDI Name` field, enter `sas/mail/Session`.
6. In the `JavaMail Properties` text area, enter the following lines and then save the changes:

```
mail.debug=false
mail.transport.protocol=smtp
mail.smtp.host=mailhost.example.com
```

7. Select the `Targets` tab.
8. Select the checkbox for all configured managed servers (but not AdminServer).

Configure JMS Server - SASJMSServer1

1. In the `Domain Structure` panel, go to `Services -> Messaging -> JMS Servers`.
2. Click `New`
   .
3. On the `JMS Server Properties` page, enter `SASJMSServer1` in the `Name` field; then click `Next`.

4. On the `Select targets` page, set the `Target` to `SASServer1`, and click `Finish`.

Define JMS Module - sasJmsSystemResource

1. In the `Domain Structure` panel, go to `Services -> Messaging -> JMS Modules`.
2. Click `New`.
3. On the properties page, set the `Name` to `sasJmsSystemResource`, and set the `Descriptor File Name` to `jms/sasjmssystemresource-jms.xml`; then click `Next`.
4. On the targets page, select `SASServer1`, and click `Next`.
5. On the `Add resources to this JMS system module` page, click `Finish`.

Create a SubDeployment (SASJMSServer1SubDeployment) for the JMS Module (sasJmsSystemResource)

1. In the `Domain Structure` panel, go to `Services -> Messaging -> JMS Modules`.
2. Click the link `sasJmsSystemResource`.
3. Select the `Subdeployments` tab.
4. Click `New`.
5. Enter the name `SASJMSServer1SubDeployment` in the `Subdeployment Name` field and click `Next`.
6. In the `Targets` page, select `SASJMSServer1`, and click `Finish`.

Create JMS Connection Factory - SASTopicConnectionFactory

1. In the `Domain Structure` panel, go to `Services -> Messaging -> JMS Modules`.
2. Click the link `sasJmsSystemResource`.
3. On the `Summary of Resources` page, click `New`.
4. On the `Create a New JMS System Module Resource` page, select `Connection Factory`, and click `Next`.
5. On the `ConnectionFactory Properties` page, set the `Name` to `SASTopicConnectionFactory`, and set the `JNDI Name` to `sas/jms/TopicConnectionFactory`, and click `Next`.
6. On the targets page, click `Advanced Targeting`.
7. On the next page, select the subdeployment `SASJMSServer1SubDeployment`, and click `Finish`.

Create JMS Connection Factory - SASQueueConnectionFactory

1. In the `Domain Structure` panel, go to `Services -> Messaging -> JMS Modules`.
2. Click the link `sasJmsSystemResource`.
3. On the `Summary of Resources` page, click `New`.
4. On the `Create a New JMS System Module Resource` page, select `Connection Factory`, and click `Next`.
5. On the `ConnectionFactory Properties` page, set the `Name` to `SASQueueConnectionFactory`, and set the `JNDI Name` to `sas/jms/QueueConnectionFactory`, and click `Next`.
6. On the targets page, click `Advanced Targeting`.
7. On the next page, select the subdeployment `SASJMSServer1SubDeployment`, and click `Finish`.

Create JMS Queue - AlertQueue

1. In the `Domain Structure` panel, go to `Services -> Messaging -> JMS Modules`.
2. Click the link `sasJmsSystemResource`.
3. On the `Summary of Resources` page, click `New`.
4. On the next page, select `Queue`, and click `Next`.
5. Enter `AlertQueue` in the `Name` field and the string `sas/jms/AlertQueue` in the `JNDI Name` field. Then click `Next`.
6. On the properties page, select the subdeployment `SASJMSServer1SubDeployment`, and click `Finish`.

Create JMS Queue - WorkflowQueue

1. In the `Domain Structure` panel, go to `Services -> Messaging -> JMS Modules`.
2. Click the link `sasJmsSystemResource`.
3. On the `Summary of Resources` page, click `New`.
4. On the next page, select `Queue`, and click `Next`.
5. Enter `WorkflowQueue` in the `Name` field and the string `sas/jms/WorkflowQueue` in the `JNDI Name` field. Then click `Next`.
6. On the properties page, select the subdeployment `SASJMSServer1SubDeployment`, and click `Finish`.

Create JMS Queue - WorkflowCommandQueue

1. In the `Domain Structure` panel, go to `Services -> Messaging -> JMS Modules`.
2. Click the link `sasJmsSystemResource`.
3. On the `Summary of Resources` page, click `New`.
4. On the next page, select `Queue`, and click `Next`.
5. Enter `WorkflowCommandQueue` in the `Name` field and the string `sas/jms/WorkflowCommandQueue` in the `JNDI Name` field. Then click `Next`.
6. On the properties page, select the subdeployment `SASJMSServer1SubDeployment`, and click `Finish`.

Create JMS Queue - WorkflowEventsQueue

1. In the `Domain Structure` panel, go to `Services -> Messaging -> JMS Modules`.
2. Click the link `sasJmsSystemResource`.
3. On the `Summary of Resources` page, click `New`.
4. On the next page, select `Queue`, and click `Next`.
5. Enter `WorkflowEventsQueue` in the `Name` field and the string `sas/jms/app/WorkflowEventsQueue` in the `JNDI Name` field. Then click `Next`.
6. On the properties page, select the subdeployment `SASJMSServer1SubDeployment`, and click `Finish`.

Configure JDBC Driver - com.sas.tkts.TKTSDriver for (SharedServices)

1. Copy the jars located in ${tableserver.temp.dir} to your domain `lib` directory. For the sample domain, this location is
   /data/SASConfigManualM2/Lev1/Web/SASDomain/lib
2. Restart the WebLogic Administration Server and the Node Manager. If any managed servers were already running, they should also be restarted.

Configure Data Source - SharedServices

1. In the `Domain Structure` panel, go to `Services -> JDBC -> Data Sources`.
2. Click `New`.
3. On the page `JDBC Data Source Properties` enter the following values:
   - Name: SharedServices
   - JNDI Name: sas/jdbc/SharedServices
   - Database Type: Other
   Then click `Next`.
4. On the page `Transaction Options`, click `Next`.
5. On the page `Connection Properties`, enter the following values:
   - `Database Name`: **SharedServices**
   - `Host Name`: HOSTNAME.example.com.
   - `Port`: 2171.
   - `Database User Name`: sastrust@saspw.
   - `Password` and `Confirm Password`: Enter the password for sastrust@saspw.
   Click `Next`.
6. On the `Test Database Connection` page, enter the following values:
   - `Driver Class Name`: com.sas.tkts.TKTSDriver
   - `URL`: jdbc:sastkts://HOSTNAME.example.com:2171
   - `Properties`:

     user=sastrust@saspw
     stmtPooling=0 constring=(DSN=SharedServices)

7. The other values don't require changes. Click `Next`.
8. On the `Select Targets` page, select the server `SASServer1`.
9. Click `Finish`.

Securing Your WebLogic Domain

The sample WebLogic Domain that was created by SDW has been secured with file permissions that only allow access by the installer user (sasinst). This means that other users cannot change into the domain directory and can't execute scripts in the domain bin directory. You may wish to employ similar security settings in your production domain.

Also, consider that log files and other files created and managed by the WebLogic server processes may be readable by others. If you wish to lock these files, you will need to use the Unix `umask` command to ensure that files are created with appropriate access rights. If you wish to make files in the WebLogic domain accessible to others, we recommend restricting access to a controlled group.

Start the WebLogic Managed Servers

- **Starting the managed servers using scripts**

  The startup scripts are located in your domain's `bin` directory. Enter the following command:

  /data/SASConfigManualM2/Lev1/Web/SASDomain/bin/startManagedWebLogic.sh *ServerName* t3://HOSTNAME.example.c

- **Starting the managed server using the WebLogic Administration Console**

  1. In the `Domain Structure` panel, go to `Environment -> Servers`.
  2. On the `Summary of Servers` page, select the name of the targeted server.
  3. Select the `Control` tab.
  4. Select the `Start` button.

Configure Foreign JNDI Provider

1. In the `Domain Structure` panel, go to `Services -> Foreign JNDI Providers`.
2. Click `New`.
3. On the page `Create a Foreign JNDI Provider` enter the name `SharedServicesJNDIProvider` and then click `OK`.
4. On the page `Summary of Foreign JNDI Providers`, select `SharedServicesJNDIProvider`.
5. On the page `Settings for SharedServicesJNDIProvider` enter the following values:
   - `Initial Context Factory`: SharedServicesJNDIProvider
   - `Provider URL`: SharedServicesJNDIProvider
   - Leave the remaining fields blank.
   - Select the `links` tab.
   - For each symbol in the table below, do the following:
     1. Select `New`
     2. On the `Create a Foreign JNDI Link` page, edit the fields to match a row in the table below.
     3. Select `OK`

Foreign JNDI Provider Name	SharedServicesJNDIProvider
Provider URL	t3://HOSTNAME.example.com:7001

Initial Context Factory	weblogic.jndi.WLInitialContextFactory		
Foreign Link Name		**Local JNDI Name**	**Remote JNDI Name**
SharedServicesAlertQueueLink	sas/jms/SharedServicesAlertQueue		sas/jms/AlertQueue
SharedServicesQueueConnectionFactoryLink	sas/jms/SharedServicesQueueConnectionFactory		sas/jms/QueueConnectionFactory

Deploying Applications on WebLogic Application Server

The directory /data/SASConfigManualM2/Lev1/Web/Staging contains deployable EAR files and a sub-directory called *exploded*. Please use the exploded location to deploy all the applications that exist there. Those applications that do not exist in the exploded directory may be deployed as EAR files. To deploy the SAS applications with the WebLogic Administration Console, perform the following steps for each application in the table below:

1. In the `Domain Structure` panel, go to `Deployments`.
2. Click `Install`
3. You could walk through the directory structure to locate the application EAR file from the `Install Application Assistant` page, however it is easier to click on the link labeled `upload your files` and then select the path to the ear from the table below and enter it into the `Deployment Archive` field on the next screen.
4. Select the application Ear file and then select `Next`.
5. Select `Install this deployment as an application` then select `Next`.
6. Select the recommended target from the table below and then select `Next`.
7. In the `Name` field, enter the name of the EAR from the table below. Note that the default value will include the name up to the first period in the Ear name, which will always be *sas*.
8. Select `Finish`.

Application Name	Location	Target
SASWebInfrastructurePlatformServices9.2	/data/SASConfigManualM2/Lev1/Web/Staging/exploded/sas.wip.services9.2.ear	SASServer1
SASWebInfrastructurePlatformApplications9.2	/data/SASConfigManualM2/Lev1/Web/Staging/sas.wip.apps9.2.ear	SASServer1
SASStoredProcessApplication9.2	/data/SASConfigManualM2/Lev1/Web/Staging/sas.storedprocess9.2.ear	SASServer1
SASContentServer9.2	/data/SASConfigManualM2/Lev1/Web/Staging/sas.wip.scs9.2.ear	SASServer1
SASThemes9.2	/data/SASConfigManualM2/Lev1/Web/Staging/sas.themes.ear	SASServer1
SASPortal4.2	/data/SASConfigManualM2/Lev1/Web/Staging/sas.portal4.2.ear	SASServer1
SASPackageViewer4.2	/data/SASConfigManualM2/Lev1/Web/Staging/sas.packageviewer4.2.ear	SASServer1
SASWebReportStudio4.2	/data/SASConfigManualM2/Lev1/Web/Staging/sas.webreportstudio4.2.ear	SASServer2
SASSharedServices9.2	/data/SASConfigManualM2/Lev1/Web/Staging/sas.shared9.2.ear	SASServer1
SASBIDashboard4.2	/data/SASConfigManualM2/Lev1/Web/Staging/sas.bidashboard4.2.ear	SASServer1
SASWebDoc9.2	/data/SASConfigManualM2/Lev1/Web/Staging/sas.webdocmd9.2.ear	SASServer2
SASWebOLAPViewer4.2	/data/SASConfigManualM2/Lev1/Web/Staging/sas.webolapviewer4.2.ear	SASServer2

SAS Web Applications

SAS Themes

Validation steps	SAS Themes are used by SAS theme-enabled web applications. If you go to the logon screen for the Portal or Web Report Studio and see images then SAS Themes are working properly.

SAS Web Infrastructure Platform

Log directory	/data/SASConfigManualM2/Lev1/Web/Logs
Validation steps	The SAS Web Infrastructure Platform is used by other SAS web applications, so if the validation steps for SAS web applications are successful, then the SAS Web Infrastructure Platform is working properly.

SAS Content Server

Log file	/data/SASConfigManualM2/Lev1/Web/Logs/SASContentServer.log
Validation steps	1. In the SAS Management Console, on the Plug-ins tab, select "+" to expand the Server Manager node. 2. Highlight the SAS Content Server. 3. Right mouse click this server and select Validate. 4. Log in using valid credentials for an unrestricted user defined in the SAS Metadata Server. 5. You should see a Validation Successful message.

SAS Stored Process Web Application

URL	http://HOSTNAME.example.com:7001/SASStoredProcess/do
Log file	/data/SASConfigManualM2/Lev1/Web/Logs/SASStoredProcess9.2.log
Validation steps	1. Access the URL provided above. 2. Log in using the sasdemo credentials provided during configuration. 3. On the Welcome page, click the "Sample: Shoe Sales by Region" link to access the custom input form for this sample stored process. 4. Select an ODS style or accept the default value, and click the "Display SAS Output" button. 5. The output from the stored process is a static table and a clickable chart. Click a bar segment on the chart to drill down to the data for that country.

SAS Web Report Studio

URL	http://HOSTNAME.example.com:7101/SASWebReportStudio
Log directory	/data/SASConfigManualM2/Lev1/Web/Logs/SASWebReportStudio4.2.log For more details about how to modify your log format and to see what logging entails, see "Logging for SAS Web Applications" in the *SAS Intelligence Platform: Web Application Administration Guide* at http://support.sas.com/documentation/onlinedoc/intellplatform/index.html#intell92.
Validation steps	1. Access the URL provided above. 2. Login using valid credentials defined in the SAS Metadata Server.

SAS Web OLAP Viewer for Java

;

URL	http://HOSTNAME.example.com:7101/SASWebOLAPViewer
Log file	/data/SASConfigManualM2/Lev1/Web/Logs/SASWebOLAPViewer4.2.log For more details about how to modify your log format and to see what logging entails, see "Logging for SAS Web Applications" in the *SAS Intelligence Platform: Web Application Administration Guide* at http://support.sas.com/documentation/onlinedoc/intellplatform/index.html#intell92.
Validation steps	1. Access the URL provided above. 2. Login using valid credentials defined in the SAS Metadata Server.

SAS Information Delivery Portal

URL	http://HOSTNAME.example.com:7001/SASPortal
Log file	/data/SASConfigManualM2/Lev1/Web/Logs/SASPortal4.2.log For more details about how to modify your log format and to see what logging entails, see "Logging for SAS Web Applications" in the *SAS Intelligence Platform: Web Application Administration Guide* at http://support.sas.com/documentation/onlinedoc/intellplatform/index.html#intell92.
Validation steps	1. Access the URL provided above. 2. Login using the sasdemo credentials provided during configuration. 3. Since the Portal samples were installed, verify that a Home page was created and contains two portlets, My Collections and Bookmarks. 4. Perform a search to verify that you have access to SAS content.

Notes:

- The SAS Portlets are located at: /data/SASConfigManualM2/Lev1/Web/Applications/SASPortlets4.2/Deployed
- If your network has a proxy server, you must specify the following parameters on the Application Server start-up command so that **syndication channels** and the **URL Display Portlet** can access content outside of your network.
  - -Dhttp.proxyHost=*host*
  - -Dhttp.proxyPort=*port*

SAS Shared Services

Log directory	/data/SASConfigManualM2/Lev1/Web/Logs
Validation steps	1. Access the Comment Service. 2. Log in using the sasdemo credentials provided during configuration. 3. Verify that you can add a comment.

Notes:

SAS BI Dashboard 4.2

URL	http://HOSTNAME.example.com:7001/SASBIDashboard
Log directory	/data/SASConfigManualM2/Lev1/Web/Logs/SASBIDashboard4.2.log For more details about how to modify your log format and to see what logging entails, see "Logging for SAS Web Applications" in the *SAS Intelligence Platform: Web Application Administration Guide* at http://support.sas.com/documentation/onlinedoc/intellplatform/index.html#intell92.
Validation steps	1. Grant the user SAS Demo User access to SAS BI Dashboard 4.2. In SAS Management Console, on the Plug-ins tab, click on the User Manager node. 2. Right click on "BI Dashboard Administrators" and select "Properties." 3. Click on the "members" tab 4. Double click on SAS Demo User to add it to the group. 5. Click OK. 6. Access the URL provided above. 7. Login using the sasdemo credentials provided during configuration. 8. Create a new indicator using the New Indicator option. 9. Add this indicator to a new or existing dashboard and verify that you have access to this dashboard by adding the BI Dashboard Portlet to a Portal page.

Notes:

- The SAS BI Dashboard 4.2 sample files are located at: /data/SAS92M2/SASBIDashboard/4.2/SampleData. Please refer the sample files install guide for more information.

SAS Help Viewer Metadata Configuration

URL	http://HOSTNAME.example.com:7101/SASWebDoc
Validation steps	Use the URL above and examine the Installed Products Page, if there were any errors configuring help content, they will be reported on that page.

Web Application Custom Content

If you wish to add custom content into SAS web applications, you may do so by placing your custom content into the appropriate custom content directory structure for the given application, and then running the SAS Deployment Manager to rebuild web applications. The custom content root directory for a given web application is

```
/data/SASConfigManualM2/Lev1/Web/Common/Server Name/Application Name/CustomContent
```

For example,

```
/data/SASConfigManualM2/Lev1/Web/Common/SASServer1/SASWebReportStudio4.2/CustomContent
```

Within that directory, there are subdirectories (for example, `ears` or `wars`) corresponding to specific archive types (ear and war files, respectively). Under the archive type directories, there are subdirectories for each specific archive—these are the root directories for each archive within the application. Custom content should be placed in the archive's directory tree corresponding to where the content should appear within the archive.

For example, to add the `ear_addon.xml` file into the `addons` directory in the `sas.webreportstudio` ear file, create the

```
.../CustomContent/ears/sas.webreportstudio/addons
```

directory, and place `ear_addon.xml` in it. Our process knows which war files are contained within ear files, so if you want to add `war_addon.jar` into the `WEB-INF/lib` directory in the `sas.webreportstudio` war file within the `sas.webreportstudio` ear file, then create

```
.../CustomContent/wars/sas.webreportstudio/WEB-INF/lib
```

directory, and place `war_addon.jar` in it.

Once all your custom content is ready to be consumed, run the SAS Deployment Manager and choose to rebuild web applications. Doing so will rebuild the web applications, inserting the custom content into the archives under the appropriate paths. Note that if custom content has the same path and name of content normally included in the archive, then the custom content takes precedence.

Completing Your Deployment

In order to complete your deployment on this machine, certain manual steps have to be performed. The SAS Content Server must be running before you attempt these steps.

Loading Content to the SAS Content Server

- Since you selected to not automatically deploy your SAS Web Applications, manual steps are required to ensure the proper content is loaded to the SAS Content Server. The file, /data/SASConfigManualM2/Lev1/Web/Utilities/manualLoadContent.sh, has been created to facilitate this process.

- Execute /data/SASConfigManualM2/Lev1/Web/Utilities/manualLoadContent.sh to automatically load content for the SAS Web Applications that require it.

The steps detailed above resulted in the creation of log files, which can be found in [/data/SASConfigManualM2/Lev1/Logs/Configure](). Review the contents of the scripts you executed for the name of the log files that were created. Review these logs and make sure there were no errors. Each execution of these scripts results in the logs from previous executions being overwritten. Therefore, prior to rerunning these scripts, you may wish to make appropriate backups of the logs.

These manual steps required the use of the SAS Administrator account. The scripts contain the SAS Administrator's credentials with the password encrypted at the sas002 level. The scripts are not intended for further use once your deployment is complete. Since these scripts contain the SAS Administrator's credentials, it is highly recommended that you delete them once your deployment is complete.

Obtaining Additional Information

Additional SAS Intelligence Platform documentation is available from the [SAS 9.2 administration documentation]() web site.

There may be additional configuration steps required for your SAS Foundation software. Consult the SAS Foundation Configuration instructions available for your operating system for product-specific post-installation steps. The configuration instructions are available from the [SAS Install Center]() web site.

Backing up your SAS Metadata Server

After completing your SAS Intelligence Platform configuration, we strongly recommend that you create a backup of your newly configured SAS Metadata Server. If you have adequate disk space to accommodate a copy of all of your metadata repositories on the metadata server host, use the MetadataServer.sh script provided in the /data/SASConfigManualM2/Lev1/SASMeta/MetadataServer directory. To execute the script, type:

./MetadataServer.sh backup

The script copies all critical metadata server files to a SASBackup subdirectory of the MetadataServer directory.

If disk space is an issue, then use the SAS Backup wizard provided in the SAS Management Console Metadata Manager or the %OMABAKUP macro to perform the backup. Both of these tools copy all critical metadata server files and permit you to specify a different backup destination. For more information, see "About the Backup Wizard" and "About %OMABAKUP" in the *SAS Intelligence Platform: System Administration Guide* at [http://support.sas.com/documentation/onlinedoc/intellplatform/index.html#intell92]().

Regular metadata server backups using SAS backup tools are crucial to ensuring the health of your SAS 9.2 Intelligence Platform configuration, but they are just one part of backing up a SAS Intelligence Platform configuration. To devise a backup strategy for your entire SAS Intelligence Platform configuration, see "Best Practices for Backing Up and Restoring Your System" in the *SAS Intelligence Platform: System Administration Guide* at [http://support.sas.com/documentation/onlinedoc/intellplatform/index.html#intell92]().