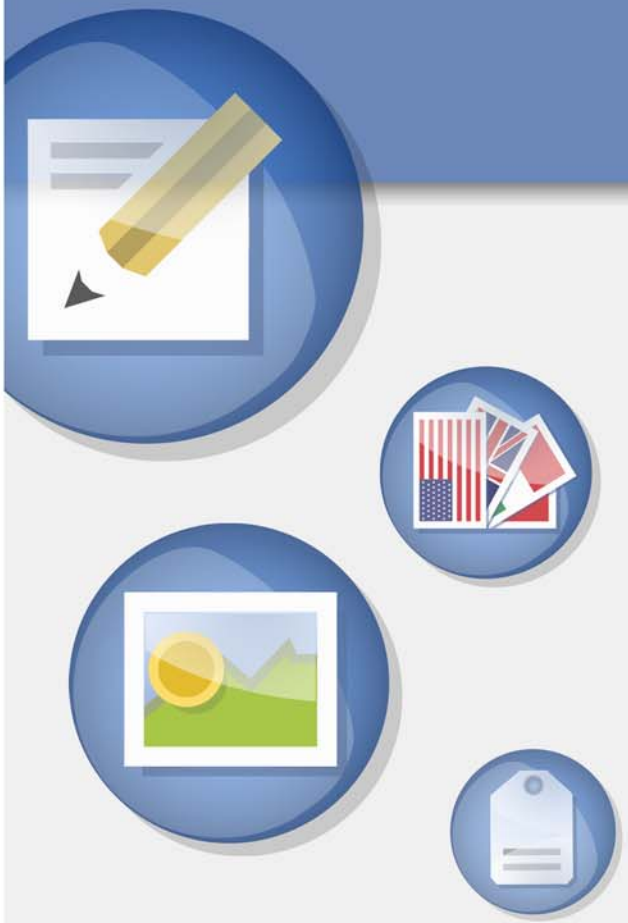
FatWire | Content Server 7

Version 7.5

Installing Content Server with Sun Java Enterprise System



Document Revision Date: Dec. 2, 2008

FatWire® SOFTWARE

Installing Content Server with Sun Java Enterprise System
Document Revision Date: Dec. 2, 2008
Product Version: 7.5

FatWire Technical Support
www.fatwire.com/Support

FatWire Headquarters
FatWire Corporation
330 Old Country Road
Suite 207
Mineola, NY 11501
www.fatwire.com

Table of

Contents

Part 3. Web Server

Part 4. Content Server

Appendices

Chapter 1

Introduction

This document provides guidelines for installing Content Server on Sun Java Enterprise System version 5, connecting to a supported database of your choice.

Note

Anyone using this guide is expected to have experience installing and configuring databases, web servers, and application servers. Selected information regarding the configuration of third-party products is given in this guide. For detailed information about a particular third-party product, refer to that product's documentation.

In this guide, Sun Java Enterprise System is called "JES."

This chapter provides information that will help you prepare for the Content Server installation. It contains the following sections:

About This Guide

This guide covers the usage of Sun Java Enterprise System version 5, as it pertains to Content Server. Topics covered include the installation and configuration of a database, installation and configuration of JES, creation of a data source, deployment of `war` and `ear` files, configuration of a cluster, configuration of a remote web server, and the installation of Content Server.

This guide does not cover the following topics, as they fall outside the scope of this guide:

- Installation of the Apache and IIS web servers
- SSL configuration on Apache and IIS

How This Guide Is Organized

The content of this guide is organized by function rather than the order in which installation steps are completed. For example, a function such as application deployment is associated with the application server. It is presented in Part II (which covers the application server), even though it is performed, later, when Content Server is installed (Part IV). Each major component of the Content Server installation is covered in its own part. A summary of the installation steps in the required order is given at the end of this chapter (see “Installation Quick Reference,” on page 9).

Terms and Acronyms

The following table defines the acronyms that are used throughout this guide.

Term	Definition
AS	Application Server
CA	Certificate Authority
JES	Java Enterprise System
lb	load balancer
SJSAS	Sun Java System Application Server
SJSWS	Sun Java System Web Server
SSL	Secure Sockets Layer
TA	Trusted Authority

Graphics in This Guide

Many steps in this guide include screen captures of dialog boxes and similar windows that you interact with in order to complete the steps. The screen captures are presented to help you follow the installation process. They are not intended to be sources of specific information, such as parameter values, options to select, or product version number.

Installation Quick Reference

After you install and configure the J2EE components that support Content Server, you will run the Content Server installer, which will guide you through the installation process. You will run the installer on each development, delivery, and management system on which you plan to use Content Server. During the Content Server installation, you will have the option to install sample sites and sample content.

Note

The names of the systems in your Content Server environment might differ from the names used in this document. Typically, the management system is also called "staging," and the delivery system is also called "production."

The steps below summarize the installation and configuration of Content Server and its supporting software. Keep the steps handy as a quick reference to the installation procedure and to chapters that provide detailed instructions.

I. Set Up the Database

Install, create, and configure your choice of supported databases. For instructions on creating and configuring the database, see our guide, *Configuring Third-Party Software*.

II. Set Up the Application Server

1. Install JES and verify the installation.

   For instructions, see Chapter 3, "Installing Sun Java Enterprise System." Note that Chapter 3 also provides supplementary information for uninstalling JES (as necessary), as well as starting and stopping JES components (the application server, identity server, and directory server).

2. Configure the JES installation. The steps that you will complete depend on the components you have selected for your installation. The steps are given in Chapter 4, "Configuring JES Application Server."

   If you are creating a portal installation, also follow the steps in "Modifying an App Server Instance to Support Portal Installations," on page 32.

3. Configure the data source (Sun Application Server; for Sun Web Server, see the next section, "III. (Optional) Set Up the Web Server," on page 10). The steps are outlined below and given in detail in Chapter 5, "Working with the Data Source."

   1) Modify the classpath of the domain (created during the JES installation) to include database connection jars.

   2) Modify the classpaths(s) of the node agent(s).

   3) Create a data source.

III. (Optional) Set Up the Web Server

Note

Web installations of Content Server are not supported on Sun Web Server 7.

If you are planning to use a web server, complete the following steps:

1. If you are going to use the Apache or the IIS web server, generate the loadbalancer plugin that comes with JES application server. (Sun Web Server 7 does not require the load balancer plugin.) For instructions, see "Generating the JES Application Server Load Balancing Plugin," on page 60.
2. Install and configure a supported web server:
   a. For instructions on installing the web server, see Chapter 8, "Installing a Web Server".
   b. For instructions on configuring the web server, see one of the following sections in Chapter 9, "Configuring the Web Server and JES Load Balancing Plugin":
      - For Sun Web Server 7, follow the steps in "Configuring Sun Web Server 7," on page 66.
      - For the Apache 2.x and Microsoft IIS web servers, follow the steps in "Configuring the Apache and IIS Web Servers," on page 74.
   c. If you are using the Apache 2.x or Microsoft IIS web server, configure the loadbalancer plugin. For instructions, see "Configuring the Load Balancing Plugin for the Web Server," on page 74.

IV. Install and Configure Content Server

1. Before you run the installer, ensure the following:
   - For clustered installations, you have created a shared file system directory that all cluster members can read from and write to; the directory name and path cannot contain spaces. Note the following:
     - For delivery systems, the default location of the shared file system directory is the directory containing the directory in which Content Server is installed.
     - For content management and development systems, the default location of the shared file system directory is inside the directory in which Content Server is installed.
   - Your system is capable of displaying the CS installer GUI. The installer will not work in text mode.
2. Install Content Server by running the supplied installer. The installer provides online help at each screen, should you need guidance. For more information, see Chapter 11, "Installing and Configuring Content Server".

   Half-way through the installation, the installer will display an "Installation Actions" pop-up window. When this window appears, you will have to deploy the CS application. For instructions, see Chapter 6, "Deploying Applications".

   If you are using an Oracle database and will require text attributes greater than 2000 characters, you will have to set the `cc.bigtext` property to `CLOB` after the CS

application is deployed. For instructions, see step 5 in "Running the Installer," on page 123.

3. Complete the Content Server installation by performing the steps described in "Post-Installation Steps," on page 123 and summarized below:

   a. If you installed Content Server on Unix, set the permissions for Content Server binaries by following the steps in "Setting File Permissions (Unix Only)," on page 124.

   b. Verify the Content Server installation by logging in as the administrator. For instructions, see "Verifying the Installation," on page 124.

   c. If you created a portal installation, configure the portal installation to display the correct portlets on the required pages, then configure portal tab accessibility. For instructions, see Chapter 10, "Configuring a Portal Installation."

   d. If you need to perform LDAP integration, follow the steps in "Integrating with LDAP (Required for Portal Installations)," on page 131. LDAP integration is mandatory for portal installations, and optional for web installations.

   e. If you are creating a clustered installation, repeat steps 2 and 3 (a–d) in this section (page 10) and follow instructions in "Working with Clusters," on page 30.

   f. Once the entire installation is completed and verified, set up Content Server for its business purpose. For instructions, see the *Content Server Administrator's Guide* and the *Content Server Developer's Guide*.

Part 1

Database

This part contains a short chapter summarizing the databases that Content Server uses. Instructions on creating and configuring the databases are given in our guide *Configuring Third-Party Software.*

This part contains the following chapter:

- Chapter 2, "Setting Up a Database"

Chapter 2

Setting Up a Database

Content Server requires access to a database that is specifically configured for Content Server. The list of supported databases (as well as other third-party components) is given in the *Supported Platform Document (SPD)* for each Content Server version. SPDs are available on the e-docs site at:

`http://support.fatwire.com`

(where you can obtain a password from FatWire Technical Support, if you do not already have a password.)

Before installing any other of Content Server's supporting software, you must complete the following steps:

1. Install the database management system.
   For instructions, refer to the product vendor's documentation.
2. Create and configure a database for Content Server.
   For instructions, consult our guide *Configuring Third-Party Software.* Note that database configuration is identical across different application servers. Refer to the correct chapter to create and configure the database of your choice.

Part 2

Application Server

This part contains information about installing and configuring the Sun JES Application Server to support and deploy your Content Server web application or portal.

This part contains the following chapters:

- Chapter 3, “Installing Sun Java Enterprise System”
- Chapter 4, “Configuring JES Application Server”
- Chapter 5, “Working with the Data Source”
- Chapter 7, “Setting Up the Sun JES Application Server Load Balancing Plugin”
- Chapter 6, “Deploying Applications”

Chapter 3

Installing Sun Java Enterprise System

This chapter provides instructions for installing and verifying JES for use by Content Server.

This chapter contains the following sections:

Start/Stop Commands

This section provides the commands for starting and stopping JES components.

Note

If Directory Server instances are present (LDAP integrated systems), start the Access Manager and Directory Servers **before** starting the application server.

Application Server

- To start:

```
/opt/<jes_home>/appserver/bin/asadmin start-domain \
   <domain-name>
```

- To stop:

```
/opt/<jes_home>/appserver/bin/asadmin stop-domain <domain_name>
```

Admin Server

- To start the admin server:

```
/var/<jes_home>/admin-server/bin/startserv
```

- To stop the admin server:

```
/var/<jes_home>/admin-server/bin/stopserv
```

Web Server 7

- To start:

```
/var/<jes_home>/webserver7/https-<hostname>/bin/startserv
```

- To stop:

```
/var/<jes_home>/https-<hostname>/bin/stopserv
```

Sun Access Manager

- To start:

```
# /opt/SUNWam/bin/amserver start
```

- To stop:

```
# /opt/SUNWam/bin/amserver stop
```

Directory Server 6

> **Note**
>
> The default Directory Server instance is `dsins1`.

- To start:

  ```
  # /opt/<jes_home>/ds6/bin/dsadm start
     /var/opt/<jes_home>/<ds_instance>
  ```

- To stop:

  ```
  # /opt/<jes_home>/ds6/bin/dsadm stop
     /var/opt/<jes_home>/<ds_instance>
  ```

Common Agent Container Management Daemon

- To start:

  ```
  # /opt/sun/cacao/bin/cacaoadm start
  ```

- To stop:

  ```
  # /opt/sun/cacao/bin/cacaoadm stop
  ```

Derby

Before starting Derby, set up your environment:

1. Set your `JAVA_HOME` variable to point to the JDK used by JES:

   ```
   export JAVA_HOME=<path_to_jdk>
   ```

   For example: **`export JAVA_HOME=/opt/jdk1.5.0_11`**

2. Add the location of your Java binaries to your `PATH` variable:

   ```
   export PATH=$PATH:<jdk location>/bin
   ```

   For example: **`export PATH=/opt/jdk1.5.0_11/bin:$PATH`**

3. Use the **`psEnv.sh`** command to set up the portal environment:

   ```
   <jes_home>/portal/lib/psEnv.sh
   ```

   For example: **`. /opt/sun/portal/lib/psEnv.sh`**

Starting and Stopping Derby

- To start:

  ```
  <jes_ant_binary> -DPS_CONFIG=<portal_config_files_dir>/
     PSConfig.properties \ -buildfile <portal_server_home>/lib/
     derby.xml start-instance
  ```

  For example:

  ```
  /opt/sun/share/bin/ant -DPS_CONFIG=/etc/opt/sun/portal/
     PSConfig.properties \ -buildfile /opt/sun/portal/lib/
     derby.xml start-instance
  ```

- To stop:

  ```
  <jes_ant_binary> -DPS_CONFIG=<portal_config_files_dir>/
     PSConfig.properties \ -buildfile <portal_server_home>/lib/
     derby.xml stop-instance
  ```

  For example:

  ```
  /opt/sun/share/bin/ant -DPS_CONFIG=/etc/opt/sun/portal/
     PSConfig.properties \ -buildfile /opt/sun/portal/lib/
     derby.xml stop-instance
  ```

Installing JES

Procedures for installing JES are environment-specific. They depend on licensing terms and the JES version, among other factors.

- For instructions on installing JES on your environment, consult the JES documentation. Commands for starting and stopping JES components are given in "Start/Stop Commands," on page 20.
- For reference, Appendix A in this guide provides a sample procedure for installing JES.

When you have completed the JES installation, complete the steps in "Completing and Verifying the JES Installation," on page 23.

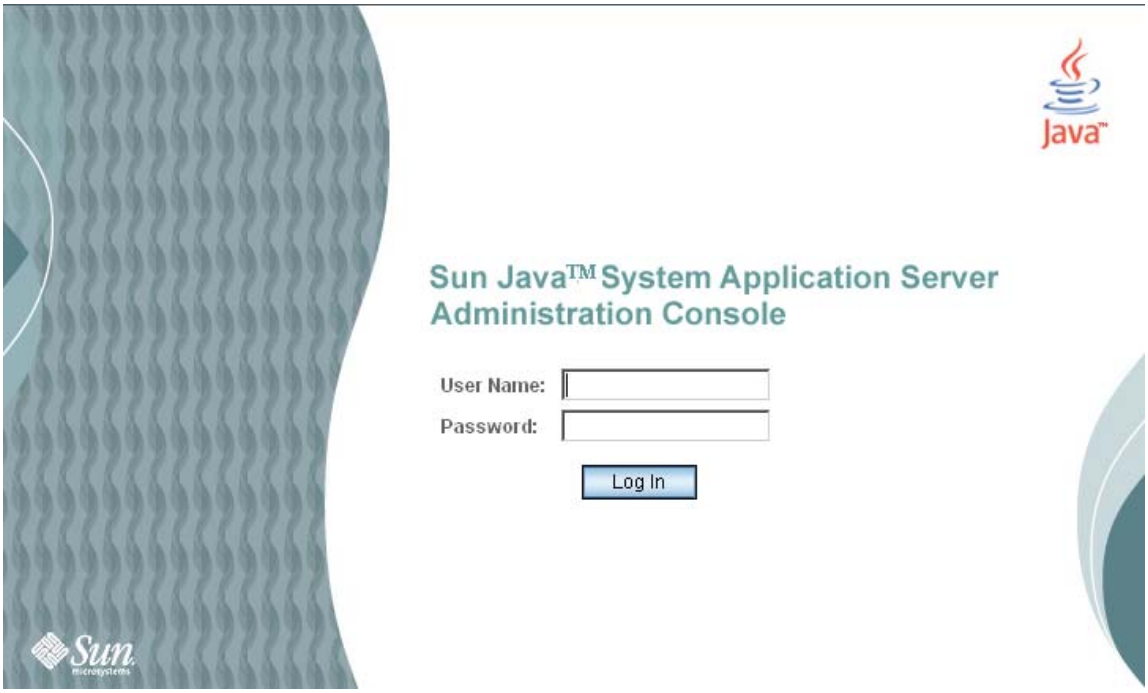
Completing and Verifying the JES Installation

This section shows you how to complete and verify your JES installation.

Verifying a Sun Application Server Installation

1. Log in to the following administrative interfaces using the `amadmin` user to confirm that the server is running:
   a. Sun Application Server Admin Console:

      `https://<hostname>:4849/admingui/`



   b. Sun Access Manager Admin Console:

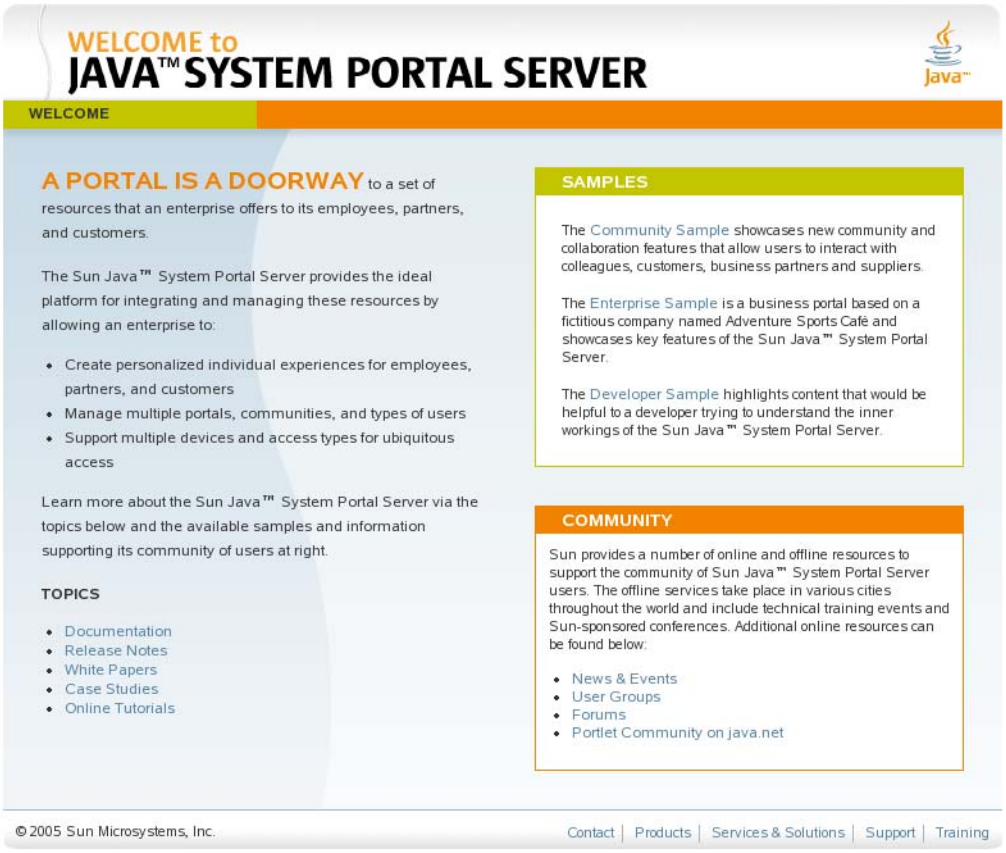
      `http:/<hostname>:8080/amserver`

2. If a portal server is installed:
   a. Log in to the Portal Server Admin Console using the `amadmin` user via the following URL:

      `http://<hostname>:8080/psconsole`

   b. Access the following URL to confirm that the portal is running:

      `http://<hostname>:8080/portal/dt`



3. Create a `password` file in `/opt/sun/portal/bin/` using the following command:

   `echo "<amadmin_password>" > /opt/sun/portal/bin/password`

4. Make sure you can access the Portal Admin Console using the **`psadmin`** command:

   `/opt/sun/portal/bin/psadmin list-portals -u -amadmin -f /opt/sun/bin/password --portal <portalname>`

5. List the applications currently deployed on the default server using the following command:

   `/opt/sun/appserver/bin/asadmin list-application-refs --host <hostname> --port 4849 --user admin server`

Completing and Verifying a Sun Web Server Installation

1. Remove the following files from `<jes_home>/webserver7/lib/`:
   - `jsf-api.jar`
   - `jsf-impl.jar`
2. Start the Directory Server:

   `<jes_home>/ds6/bin/dsadm start /var/<jes_home>/dsinst1`
3. Start the Web Server instance:

   `/var/<jes_home>/webserver7/https-<hostname>/bin/startserv`
4. Start the Web Server admin server:

   `/var/<jes_home>/webserver7/admin-server/bin/startserv`
5. Log in to the Web Server admin console as the `admin` user via the following URL to confirm that the Web Server is running:

   `http://<hostname>:8800`
6. Log in to the following admin interfaces using the `amadmin` user to confirm that the corresponding server is running:
   a. Access Manager console:

      `http://<hostname>:80/amconsole`
   b. Portal Server console:

      `http://<hostname>:80/psconsole`
7. Access the following URL to confirm that the portal is running:

   `http://<hostname>:80/portal/dt`
8. Create a password file in `<jes_home>/portal/bin/` using the following command:

   `echo <amadmin_password> > <jes_home>/portal/bin/password`
9. Make sure you can access the Portal Admin console using the **`psadmin`** command:

   `<jes_home>/portal/bin/psadmin list-portals -u -amadmin -f <jes_home>/bin/password --portal portal1`

Uninstalling JES

For reference, Appendix A provides a sample procedure for uninstalling JES by the use of scripts obtained from Sun Microsystems.

Chapter 4

Configuring JES Application Server

This chapter provides instructions for configuring JES Application Server for use by Content Server.

This chapter contains the following sections:

Working with Domains

This section provides instructions for completing the following operations:

- Backing Up a Domain
- Restoring a Domain

Backing Up a Domain

You may wish to back up your domain before you attempt to modify it. This allows you to restore the domain later on if something fails to work properly.

To back up a domain

1. Stop the domain you wish to back up:

   ```
   ./asadmin stop-domain domain1
   ```

2. Back up the domain:

   ```
   ./asadmin backup-domain --domaindir  /var/opt/<jes_home>/
        domains/ --description 032507backup_domain1 domain1
   ```

3. Write down the name of the backup file. The name of the backup file is displayed after the backup task is complete. You will need this file name to restore the domain.

   For example:

   ```
   Backup Filename: /var/opt/<jes_home>/domains/domain1/
      backups/sjsas_backup_v00001.zip
   Date and time backup was performed: Sun Mar 25 12:13:44 EDT
      2007
   Domains Directory: /var/opt/<jes_home>/domains
   Domain Directory: /var/opt/<jes_home>/domains/domain1
   Domain Name: domain1
   Name of the user that performed the backup: root
   ```

4. Restart the domain:

   ```
   ./asadmin start-domain --user admin --password demo4132 domain1
   ```

Restoring a Domain

1. Stop the domain you wish to back up:

   ```
   ./asadmin stop-domain domain1
   ```

2. Restore the domain:

   ```
   ./asadmin restore-domain --filename /var/opt/<jes_home>/
         domains/domain1/backups/sjsas_backup_v00001.zip domain1
   ```

3. Restart the domain:

   ```
   ./asadmin start-domain --user admin --password demo4132 domain1
   ```

Working with Application Server Instances

In order to deploy your CS application on JES, you must create a domain. When you create a domain, JES automatically creates a server instance under the domain. (Note that JES allows only one server instance per domain.)

Once the domain has been created, you must also create an HTTP listener which enables the server instance to accept connections on the port of your choice.

This section provides instructions for completing the following operations:

- Creating a Domain and Server Instance
- Deleting a Domain and Server Instance
- Creating an HTTP Listener
- Deleting an HTTP Listener

Creating a Domain and Server Instance

To create a domain (and a corresponding server instance), perform the following steps:

1. Execute the following command:

   ```
   ./asadmin create-domain --adminport 4949 --adminuser admin
      --instanceport 9090 --savelogin=true <domain_name>
   ```

2. When prompted, enter the `admin` user password, then re-enter it for verification.
3. When prompted, enter the master password, then re-enter it for verification.

   You will see output similar to the following:

   ```
   Using default port 7676 for JMS.
   Using default port 3700 for IIOP.
   Using default port 8181 for HTTP_SSL.
   Using default port 3820 for IIOP_SSL.
   Using default port 3920 for IIOP_MUTUALAUTH.
   Using default port 8686 for JMX_ADMIN.
   Domain <domain-name> created.
   Admin login information for host [localhost] and port [4949] is
   being overwritten with credentials provided. This is because
   the --savelogin option was used during create-domain command.
   Login information relevant to admin user name [admin] for this
   domain [<domain_name>] stored at [/root/.asadminpass]
   successfully.
   Make sure that this file remains protected. Information stored
   in this file will be used by asadmin commands to manage this
   domain.
   ```

Deleting a Domain and Server Instance

To delete a domain (and the corresponding server instance), execute the following command:

```
./asadmin/delete-domain <domain_name>
```

Creating an HTTP Listener

Once you create a domain (and server instance), you must create an HTTP listener which enables the application server to accept connections for that domain on a port of your choice (`9191` in our example). To create a listener, execute the following command:

```
./asadmin create-http-listener --host localhost --port 4949 --user
   admin --listeneraddress 0.0.0.0 --listenerport 9191 --defaultvs
   server --securityenabled=true --enabled=true <listener-name>
```

Deleting an HTTP Listener

To delete a listener, execute the following command:

```
./asadmin delete-http-listener --host localhost --port 4949
   --user admin <listener-name>
```

Working with Clusters

This section provides instructions for completing the following operations:

- Creating a Cluster
- Migrating EJB Timers on a Cluster
- Deleting a Cluster

Creating a Cluster

1. List existing clusters:

   ```
   ./asadmin list-clusters --user admin --password demo4132 \
      --host localhost --port 4849
   ```

2. Create a new cluster:

   ```
   ./asadmin create-cluster --user admin --password demo4132 \
      --host localhost --port 4849 testCluster
   ```

3. Create a new instance to add to your cluster:

   Note

   For detailed instructions on creating an instance, see "Working with Application Server Instances," on page 29. Follow the instructions as given; however, add the `--cluster <name>` option to the `create-instance` command.

   ```
   ./asadmin create-instance --user admin --password demo4132 \
      --host localhost --port 4849 --cluster testCluster \
      --nodeagent portalTest Ctest
   ```

4. Start the new cluster:

   ```
   ./asadmin start-cluster --user admin --password demo4132 \
      --host localhost --port 4849 testCluster
   ```

Migrating EJB Timers on a Cluster

1. Locate the stopped instance by using the list command:

```
./asadmin list-instances --host localhost --port 4849 \
   --user admin --password demo4132
```

2. Move the EJB timers from the stopped instance to one that is running on the same cluster. In this case move the EJB timers from Dtest to Ctest:

```
./asadmin migrate-timers --user admin --password demo4132 \
   --host localhost --port 4849 --destination Ctest Dtest
```

3. Restart the instance to which the timers were moved:

```
./asadmin stop-instance --user admin --password demo4132 \
   --host localhost --port 4849 Ctest
```

```
./asadmin start-instance --host localhost --port 4849 \
   --user admin --password demo4132 Ctest
```

Deleting a Cluster

1. Delete all instances located in the cluster:

```
./asadmin delete-instance --user admin --password demo4132 \
   --host localhost --port 4849 Ctest
```

2. Stop the cluster:

```
./asadmin stop-cluster --user admin --password demo4132 \
   --host localhost --port 4849 testCluster
```

3. Delete the cluster:

```
./asadmin delete-cluster  --user admin --password demo4132 \
   --host localhost --port 4849 testCluster
```

4. List the remaining clusters to ensure that the deletion was completed:

```
./asadmin list-clusters --user admin --password demo4132 \
   --host localhost --port 4849
```

Modifying an App Server Instance to Support Portal Installations

By default, the portal is installed on the `server` instance, which was created during the installation of the portal. If you wish to deploy the portal to a new instance, follow the steps in this section.

1. Execute `/opt/SUNWps/bin/multiserverinstance` (the location may vary with the installation).
   a. Select option 1: "**`Create a new portalserver instance`**"
   b. Select option 3: "**`Sun Java System Application Server 8.1`**"
   c. Answer the following questions when prompted:

```
Where is the Web Container installed? [/opt/<jes_home>/
   appserver]

What is the domain name? [domain1]

What is the domain (DAS) path? [] /var/opt/<jes_home>/
   domains/domain1/

What is the Web Container instance path? [] /var/opt/
   <jes_home>/nodeagents/<node agent name>/<instance name>/

What is the Web Container administrator? [admin]

What is the Web Container administration port? [4849]

Is the Web Container administration port secure? [y]/n y

Instance name? <instance to add portal to>

Instance port? <port on which the instance is running>

Is the instance port secure? y/[n] n

What is the Web Container document root directory? [/var/
   opt/<jes_home>/nodeagents/realsun03a/csInstanceA//
   docroot]

What is the Application Server administration password?
   <hidden>

What is the Identity Server administration password?
   <hidden>
```

   d. Confirm that your previous selections are correct and press **y**.
   e. Wait for the installation to complete.
2. If you already have a portal configured on another instance, the script will not redeploy the portal applications. To correct the situation, do the following:
   a. Log in to the admin console.
   b. Complete the steps below for each of the following web applications: `amserver`, `ampassword`, `amcommon`, `amconsole`, `portal`, `portalsamples`.
      1) Select the application.
      2) Select the **Targets** tab.
      3) Click the **Manage Targets** button.

4) Add the instance that was added above (in step 1 on page 32).

5) Click **OK**.

c. Restart the affected instance and domain.

Creating an Additional Portal Server Instance

On development systems, it is often desirable to install Content Server on a Portal Server instance other than the default instance. This section shows you how to create an additional Portal Server instance running Content Server with the DeveloperSample sample portal.

The procedure consists of the following steps:

A. Create a New Application Server Node and Instance. You will deploy the new Portal Server instance on this application server instance.

B. Create a Portal Server Instance on the New Application Server Instance. This will be your additional Portal Server instance (that is, other than the default instance).

C. Test the New Portal Server Instance. Make sure that the Portal Server instance has been deployed properly.

D. Add the DeveloperSample Sample Portal to the New Portal Server Instance. This a sample portal through which you will access Content Server portlets.

E. Test the DeveloperSample Sample Portal. Make sure that the sample portal has been deployed properly.

Note

In the examples in this section, the following values will be used:

- New node agent name: `csnodeagent`
- New application server instance name: `csinstance`
- New Portal Server instance name: `csportal`
- New Portal instance URI: `/csportal`

A. Create a New Application Server Node and Instance

This section shows you how to create a new application server node and instance that will hold the additional Portal Server instance.

1. Create a new node agent:

```
<jes_home>/appserver/bin/asadmin create-node-agent --host
   <host_name> \ --port 4849 --user admin <node_agent_name>
```

For example:

```
/opt/sun/appserver/bin/asadmin create-node-agent \ --host
   rh4u5asoracle120gr2sjes5.vm.fatwire.com --port 4849 --user
   admin csnodeagent
```

Sample output:

```
Please enter the admin password>      (enter the admin password)
Please enter the master password>     (enter the admin password)
Command create-node-agent executed successfully.
```

2. Create a new application server instance under the newly created node:

```
<jes_home>/appserver/bin/asadmin create-instance --user admin -
   -host <hostname> \ --nodeagent <new_node_agent_name> --port
   4849 <instance_name>
```

For example:

```
/opt/sun/appserver/bin/asadmin create-instance --user admin \ -
   -host rh4u5asoracle120gr2sjes5.vm.fatwire.com --nodeagent
   csnodeagent \ --port 4849 csinstance
```

Sample output:

```
Please enter password>      (enter your admin password)
Command create-node-agent executed successfully.
```

3. Start the new node agent and application server instance:

```
<jes_home>/bin/asadmin start-node-agent --user admin
   <new_node_agent_name>
```

For example:

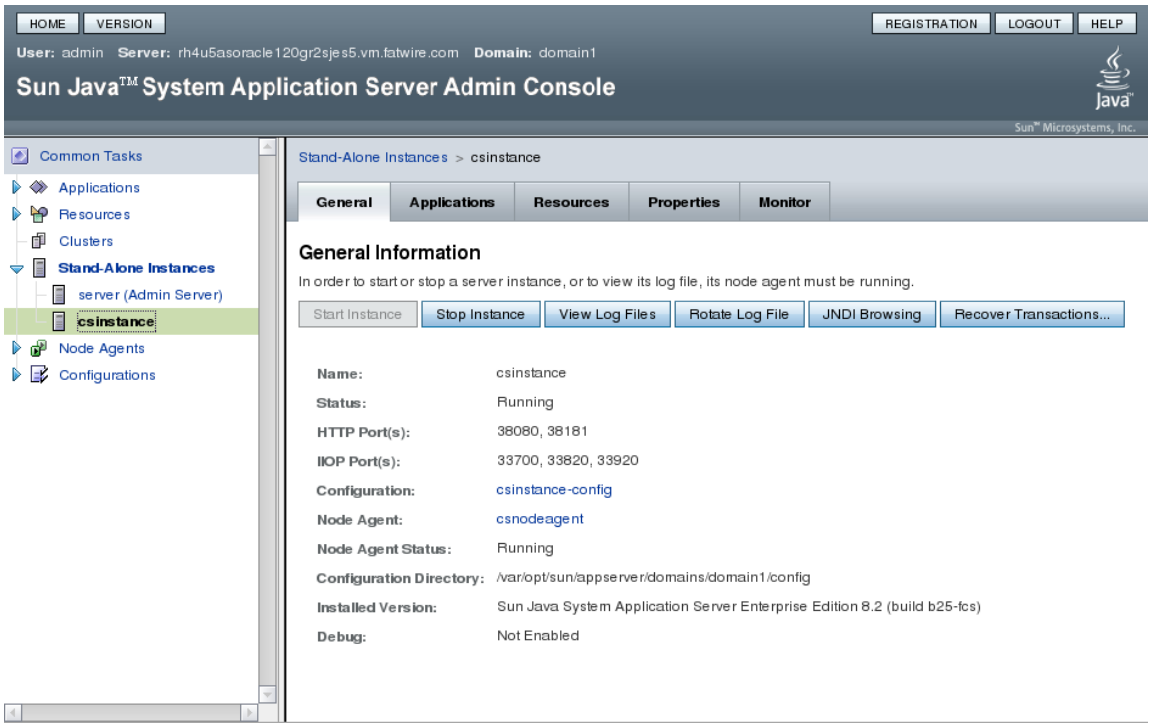
```
/opt/sun/appserver/bin/asadmin start-node-agent --user admin
   csnodeagent
```

Sample output:

```
Please enter the admin password>      (enter your admin password)
Please enter the master password>     (enter your admin password)
Command start-node-agent executed successfully.
```

4. Retrieve the port numbers for the new application server instance:
   a. Log in to the SJES administration console.
   b. In the tree on the left, expand the **Stand-Alone Instances** node and select the newly created application server instance (**csinstance** in our example).

The console displays the “General Information” screen showing a summary of the instance’s parameters.



c. Make a record of the **HTTP Port(s)** field value (usually, `38080`).

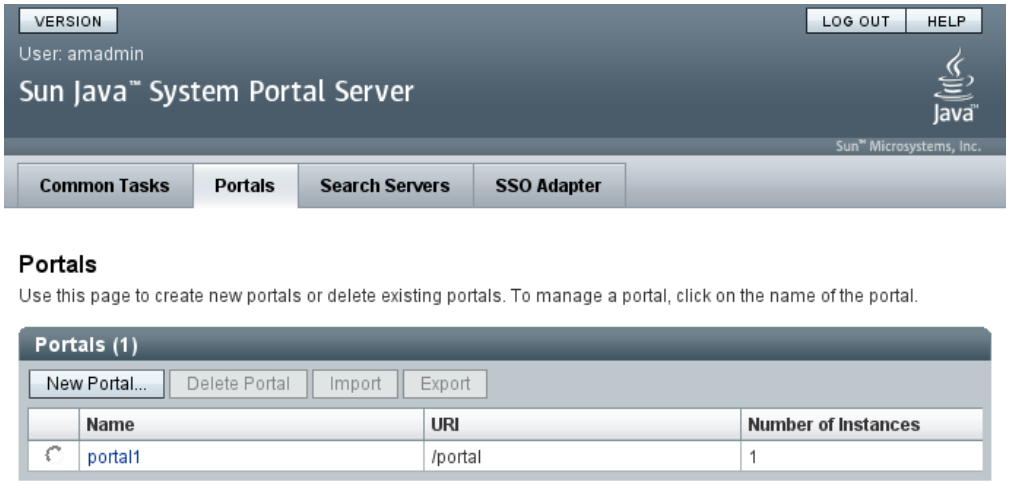
B. Create a Portal Server Instance on the New Application Server Instance

This section shows you how to use the Portal Server console to create a Portal Server instance on the new application server instance you created in the previous step.

1. Access the Portal Server console via the following URL:

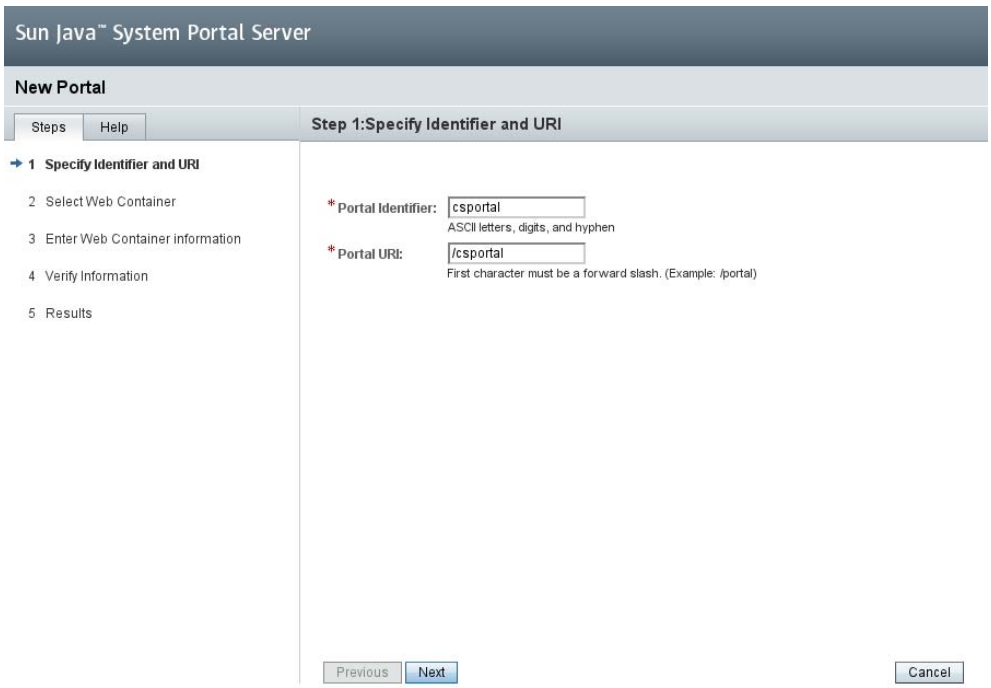
   `http://<server>:<port>/psconsole`

2. Select the **Portals** tab.

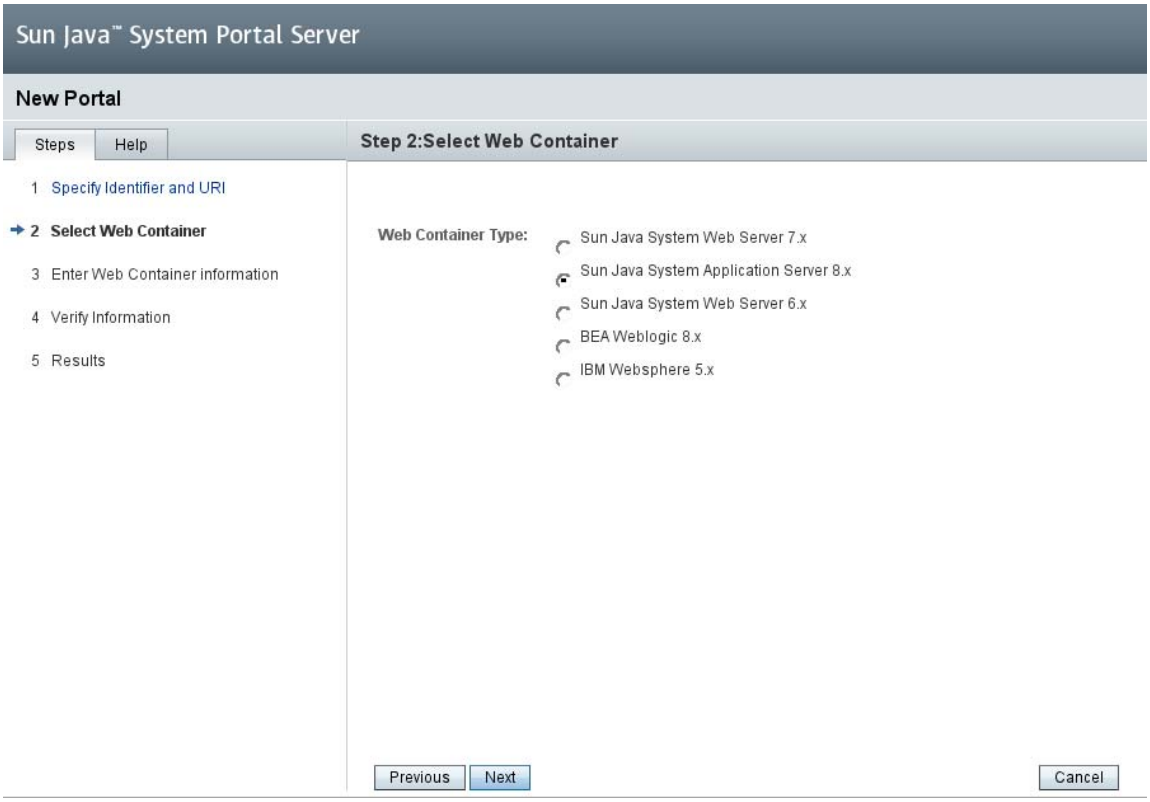


3. Click **New Portal**.

4. In the pop-up window that appears, enter a portal identifier and a portal URI. FatWire recommends using the same value for both. The portal URI must begin with a / (slash). When you are finished, click **Next**.



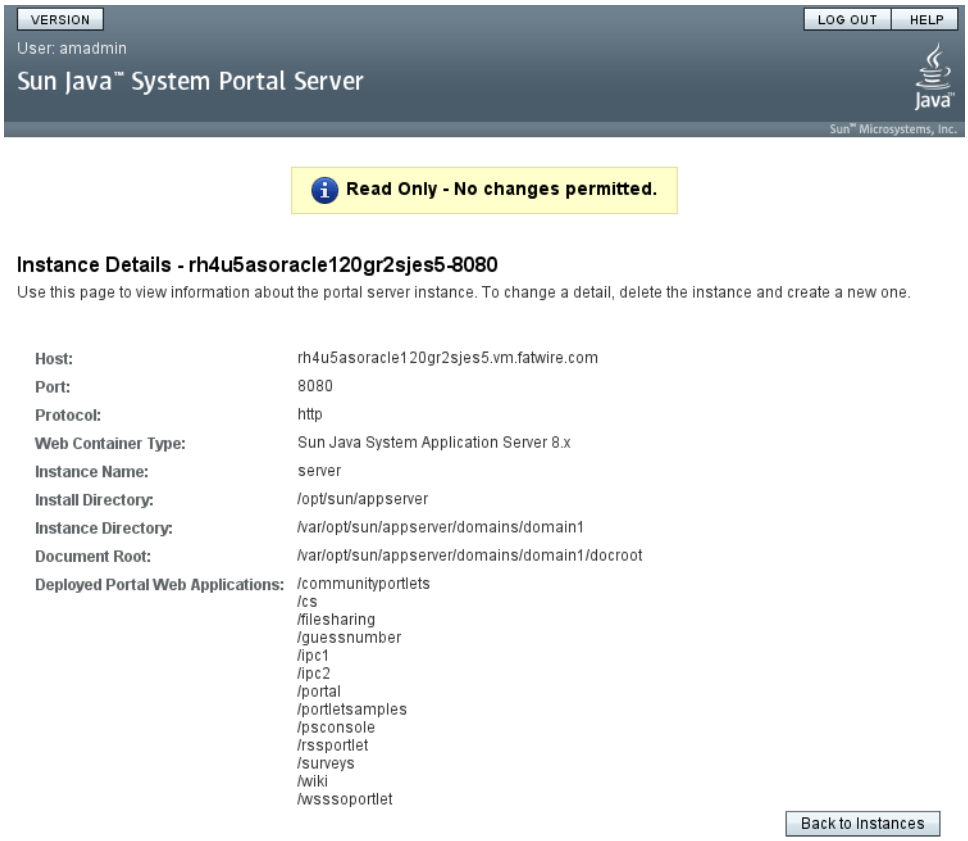
5. In the "Select Web Container" screen, select **Sun Java System Application Server 8.x** and click **Next**.



6. Obtain the values required for the next step from your existing Portal Server instance as follows:
   a. Open a new browser window and log in to the Portal Server console.
   b. In the console, select your existing Portal Server instance (**portal1** in our example).
   c. Select the **Server Instances** tab.

   d. In the tab, select your existing application server instance

e. In the “Instance Details” screen, make a record of all the displayed values. (You will need them to complete the next step.)



7. In the “Enter Web Container Information” screen, enter the following information (you obtained some of this information in the previous step):
   a. **Protocol:** `HTTP` (default)
   b. **Host:** name of the host on which the target application server instance resides
   c. **Port:** port on which the target application server instance is listening for connections
   d. **Install Directory:** the directory in which Sun Application Server is installed
   e. **Instance Name:** name of the target application server instance (that is, the instance under which the new Portal Server instance will reside
   f. **Instance Directory:** location of the domain under which this Portal Server instance will be deployed (that is, the domain under which the target application server instance has been deployed)
   g. **Document Root:** location of the document root directory of the domain under which this Portal Server instance will be deployed
   h. **Domain Name:** name of the domain under which this Portal Server instance will be deployed
   i. **Admin Protocol:** `HTTPS` (default)

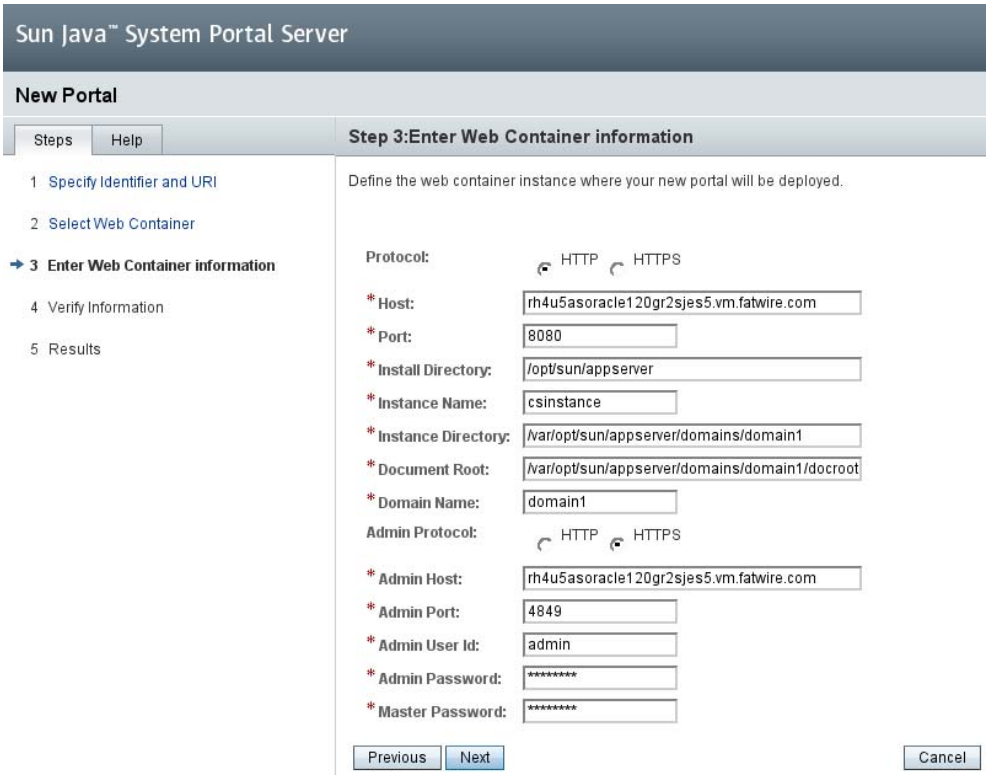
j. **Admin Host:** name of the host on which the admin instance resides (by default, this is the system on which the Portal Server instance will be deployed)

k. **Admin Port:** port on which the admin instance is listening for connections (by default, this is port `4849`)

l. **Admin User ID:** `admin` (unless you changed it during SJES installation)

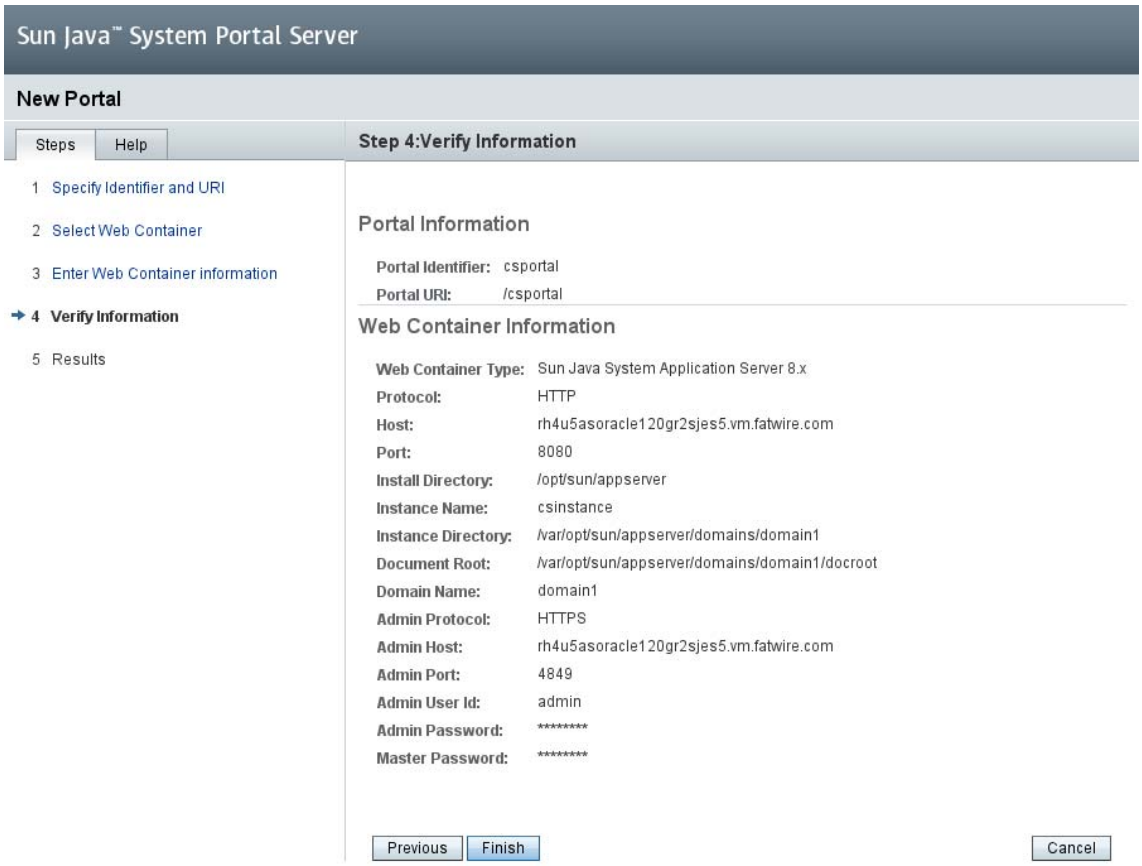
m. **Admin Password:** your admin password (set during SJES installation)

n. **Master Password:** your master password (set during SJES installation; typically, this is the same as your admin password).

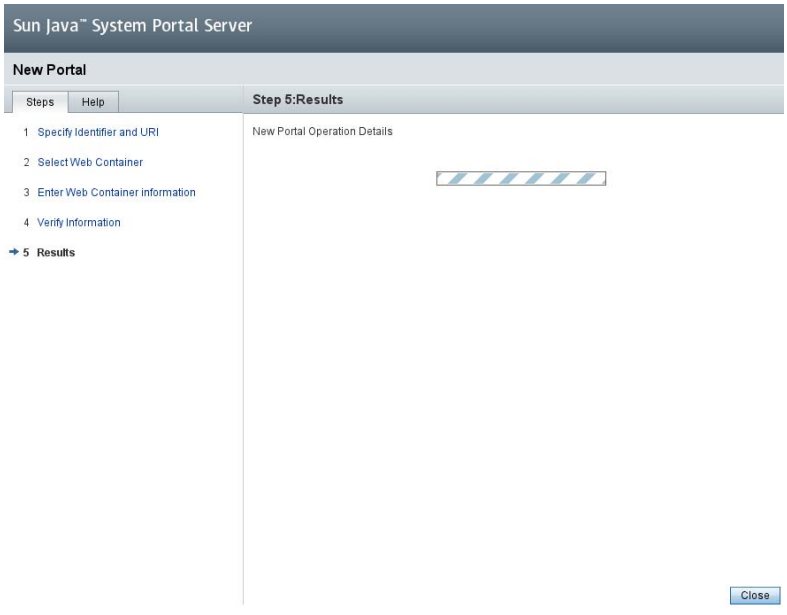


o. When you are finished, click **Next**.

8. In the "Verify Information" screen, verify the information you entered and click **Finish**.



9. Allow the portal creation process to complete – it may take a few minutes.



10. When the operation completes successfully, click **Close**.

C. Test the New Portal Server Instance

At this point, you should have a new node agent and application server instance. The new Portal Server instance should be running under the new application server instance.

Verify that the Portal Server instance is operational by accessing the following URL:

`http://<hostname>:<new_appserv_instance_port>/<new_portal_URI>`

D. Add the DeveloperSample Sample Portal to the New Portal Server Instance

In order to use the new Portal Server instance with Content Server, you must deploy the DeveloperSample portal.

1. Create a temporary directory on the SJES machine and change to that directory.
2. Copy the following files from `<jes_home>/portal/sample/portals/shared` to the temporary directory:
   - `password.properties`

     `cp /opt/sun/portal/samples/portals/shared/ password.properties.template password.properties`
   - `input.properties`

     `cp /opt/sun/portal/samples/portals/shared/ input.properties.template input.properties`
3. Make a backup copy of the `build.xml` file in case you need to undo the changes you will make in the next step:

   `cp /opt/sun/portal/samples/portals/developer/build.xml /opt/sun/portal/samples/portals/developer/build.xml.org`
4. Open your copy of `password.properties` and do the following:
   a. Locate the following section:

```
#
# Identifies the password for the super user for Sun Java
# System Access Manager
#
amadminPassword=%AMADMIN_PASSWORD%
#
# Identifies the password for the internal root user for Sun
# Java # System Access Manager
#
amldapuserPassword=%AMLDAPUSER_PASSWORD%
#
# Identifies the password for the Sun Java System User
# Management utility (commadmin)
#
userManagementPassword=%USER_MANAGEMENT_PASSWORD%
```

   b. For the `amadmin` and `amldapuser` users, replace the string inside the percent marks with the user's password. (If you have enabled user password management on your SJES installation, also set the user management password.)

   c. Save and close the file.

5. Open your copy of `input.properties` and do the following:
   a. Locate the following section:

```
#
# Portal configuration location
# example: /etc/opt/SUNWportal
ps.config.location=%PS_CONFIG_LOCATION%
#
# Portal identifier
# example: portal1
ps.portal.id=%PORTAL_ID%
#
# Portal access url
# example: http://siroe.com:80/portal
ps.access.url=%PORTAL_ACCESS_URL%
#
# Portal web application uri
# example: /portal
ps.webapp.uri=%PORTAL_WEBAPP_URI%
#
# Subscriptions profiler email address
# example: admin@siroe.com
ps.profiler.email=%PROFILER_EMAIL%
#
# Subscriptions profiler SMTP server
# example: siroe.com
ps.profiler.smtp.host=%PROFILER_SMTP_HOST%
#
# Search access url
# example: http://siroe.com:80/mySearch/search
search.access.url=%SEARCH_ACCESS_URL%
#
# Search server id
# example: mySearch
search.id=%SEARCH_ID%
#
# Access Manager admin dn
# example: uid=amAdmin,ou=People,dc=siroe,dc=com
am.admin.dn=%AM_ADMIN_DN%
#
# Access Manager default organization
# example: dc=siroe,dc=com
default.org.dn=%DEFAULT_ORG_DN%
```

b. For each parameter, replace the string inside the percent marks with the value that is correct for your installation.

In the example below, we assume that your hostname is `abc.fatwire.com` and that the additional Portal Server instance you created is named `csportal`.

```
#
# Portal configuration location
# example: /etc/opt/SUNWportal
ps.config.location=/opt/sun/portal
#
# Portal identifier
# example: portal1
ps.portal.id=csportal
#
# Portal access url
# example: http://siroe.com:80/portal
ps.access.url=http://abc.vm.fatwire.com:38080/csportal
#
# Portal web application uri
# example: /portal
ps.webapp.uri=/csportal
#
# Subscriptions profiler email address
# example: admin@siroe.com
ps.profiler.email=root@abc.vm.fatwire.com
#
# Subscriptions profiler SMTP server
# example: siroe.com
ps.profiler.smtp.host=abc.vm.fatwire.com
#
# Search access url
# example: http://siroe.com:80/mySearch/search
search.access.url=http://abc.vm.fatwire.com:8080/mySearch/
   search
#
# Search server id
# example: mySearch
search.id=mySearch
#
# Access Manager admin dn
# example: uid=amAdmin,ou=People,dc=siroe,dc=com
am.admin.dn=uid=amAdmin,ou=People,dc=vm,dc=fatwire,dc=com
#
# Access Manager default organization
# example: dc=siroe,dc=com
default.org.dn=dc=vm,dc=fatwire,dc=com
```

c. Save and close the file.

6. (Recommended) Delete obsolete `.par` files for portal interfaces:
   a. Change to the `/var/<jes_home>/portal/par` directory.
   b. Delete the following files:
      - `community_sample.par`
      - `developer_sample.par`
      - `enterprise_sample.par`

      For example:

      ```
      rm -f community_sample.par developer_sample.par
         enterprise_sample.par
      ```
7. Prepare your environment and execute the modified ant build script:
   a. Set your `JAVA_HOME` variable to point to the JDK used by JES:

      ```
      export JAVA_HOME=/opt/jdk1.5.0_11
      ```
   b. Set your `PATH` variable to include the Java binaries:

      ```
      export PATH=/opt/jdk1.5.0_11/bin:$PATH
      ```
   c. Prepare your portal environment using the `psEnv.sh` command (source it):

      ```
      . <jes_home>/portal/lib/psEnv.sh
      ```
   d. (Linux only) Link `/etc/<jes_home>/portal/PSConfig.properties` to `<jes_home>/portal/PSConfig.properties`:

      ```
      ln -s /etc/opt/sun/portal/PSConfig.properties
         /opt/sun/portal/PSConfig.properties
      ```
   e. Execute the ant build script:

      ```
      <jes_home>/bin/ant -buildfile <jes_home>/portal/samples/
         portals/developer/build.xml
      ```
   f. When prompted for the location of the configuration files, enter the path to the temporary directory you created in step 1 on page 41.

      Sample ant script output:

      ```
      ...
      cleanPassword:
      [delete]
      Deleting: /var/opt/sun/portal/tmp/password1969882429

      run:

      BUILD SUCCESSFUL
      Total time: 5 minutes 29 seconds
      ```

E. Test the DeveloperSample Sample Portal

Verify that the DeveloperSample sample portal is functioning by accessing your portal URL and appending the following string to it:

```
?desktop.suid=uid=devauthlessanonymous,ou=People,o=DeveloperSample
   ,dc=vm,dc=fatwire,dc=com
```

For example:

```
http://rh4u5asoracle120gr2sjes5.vm.fatwire.com:8080/portal/
   dt?desktop.suid=uid=devauthlessanonymous,ou=People,o=DeveloperS
   ample,dc=vm,dc=fatwire,dc=com
```

Setting Permissions for Content Server

This section shows you how to modify your `server.policy` file to add the permissions necessary to support Content Server. The permissions must be in place before the CS application is deployed.

1. Locate the `server.policy` file for your domain. For example:

   ```
   /var/opt/sun/appserver/domains/domain1/config/server.policy
   ```

2. Open the `server.policy` file in a text editor and locate the following section:

   ```
   // Basic set of required permissions granted to all remaining
      code
   grant {
   permission java.lang.RuntimePermission "loadLibrary.*";
   permission java.lang.RuntimePermission "queuePrintJob";
   permission java.net.SocketPermission "*", "connect";
   permission java.io.FilePermission "<<ALL FILES>>","read";
   ```

   a. Change the line highlighted in the previous step to the following (keep it as one line):

      ```
      permission java.io.FilePermission "<<ALL FILES>>",
         "read,write,delete";
      ```

   b. Locate the following line:

      ```
      permission java.util.PropertyPermission "*", "read";
      ```

      and change it to the following:

      ```
      permission java.util.PropertyPermission "*", "read,write";
      ```

   c. Add the following line after the line you just edited:

      ```
      permission java.lang.reflect.ReflectPermission "*",
         "read,write";
      ```

   d. Locate the following line,

      ```
      permission java.lang.RuntimePermission "queuePrintJob";
      ```

      and add the following lines after it:

      ```
      permission java.lang.RuntimePermission "createClassLoader";
      permission java.lang.RuntimePermission
         "setContextClassLoader";
      permission java.lang.RuntimePermission
         "getProtectionDomain";
      permission java.lang.RuntimePermission
         "reflectionFactoryAccess";
      permission java.lang.RuntimePermission  "modifyThread";
      permission java.lang.RuntimePermission "createClassLoader";
      permission java.lang.RuntimePermission "getClassLoader";
      permission java.io.SerializablePermission
         "enableSubclassImplementation";
      permission java.io.SerializablePermission
         "enableSubstitution";
      ```

When you have made the above changes, the section should look as follows (new and modified lines are highlighted in bold):

```
// Basic set of required permissions granted to all remaining
   code
grant {
permission java.lang.RuntimePermission "loadLibrary.*";
permission java.lang.RuntimePermission "queuePrintJob";
permission java.lang.RuntimePermission "createClassLoader";
permission java.lang.RuntimePermission "setContextClassLoader";
permission java.lang.RuntimePermission "getProtectionDomain";
permission java.lang.RuntimePermission
   "reflectionFactoryAccess";
permission java.lang.RuntimePermission  "modifyThread";
permission java.lang.RuntimePermission "createClassLoader";
permission java.lang.RuntimePermission "getClassLoader";
permission java.io.SerializablePermission
   "enableSubclassImplementation";
permission java.io.SerializablePermission "enableSubstitution";
permission java.net.SocketPermission "*", "connect";
permission java.io.FilePermission "<<ALL FILES>>",
   "read,write,delete";
// work-around for pointbase bug 4864405
permission java.io.FilePermission
   "${com.sun.aas.instanceRoot}${/}lib${/}databases${/}-",
   "delete";
permission java.io.FilePermission "${java.io.tmpdir}${/}-",
   "delete";
permission java.util.PropertyPermission "*", "read,write";
permission java.lang.reflect.ReflectPermission "*",
   "read,write";
permission java.lang.RuntimePermission "modifyThreadGroup";
};
```

3. At the very end of the file, add the following:

Note

Note the following:

- `ear` files are deployed to the `j2ee-apps` directory located in `/var/opt/<jes_home>/domains/<domain>/applications/`
- `war` files are deployed to the `j2ee-modules` directory located in `/var/opt/<jes_home>/domains/<domain>/applications/`

Depending on your installation type (web application or portal), modify the path in the code below as necessary.

```
grant codeBase "file:/var/opt/sun/appserver/domains/domain1/
   applications/j2ee-apps/ContentServer/cs_war/WEB-INF/lib/-"
   { permission java.security.AllPermission; };
```

4. Save and close the file.

5. If you are using node agents, repeat steps 2-4 for the corresponding node agent's `server.policy` file. For example:

   `<node_agent_name>/agent/config/server.policy`

Chapter 5

Working with the Data Source

This chapter provides instructions for creating a domain and data source for web and portal installations.

This chapter contains the following sections:

Modifying the Classpath of a Domain

The classpath of a domain must be modified to include database connection jars. The basic classpath affects only the domain and not any server instances.

To modify the classpath of a domain

1. Determine the pre_class_path for a server running on a given port:

   ```
   ./asadmin get --user admin --password demo4132 \
      --host localhost --port 4849 server.java-
      config.classpath_prefix
   ```

   Example response:

   ```
   server.java-config.classpath-prefix = /opt/SUNWam/lib/sax.jar:/
      opt/SUNWam/lib/dom.jar:/opt/SUNWam/lib/saaj-api.jar:/opt/
      SUNWam/lib/common-logging.jar:/opt/SUNWam/lib/saaj-
      impl.jar:/opt/SUNWam/lib/mail.jar:/opt/SUNWam/lib/
      activation.jar:
   ```

2. Add a new item to the classpath:

   ```
   ./asadmin set --user admin --password demo4132 \
      --host localhost \
      --port 4849 server.java-config.classpath_prefix={string
      return from get}:{path to classes12.zip}
   ```

   Example response:

   ```
   /opt/SUNWam/lib/sax.jar:/opt/SUNWam/lib/dom.jar:/opt/SUNWam/
      lib/saaj-api.jar:/opt/SUNWam/lib/common-logging.jar:/opt/
      SUNWam/lib/saaj-impl.jar:/opt/SUNWam/lib/mail.jar:/opt/
      SUNWam/lib/activation.jar:/u01/DB/Oracle/classes12.zip:/u01/
      DB/Oracle/ojdbc14.jar:/u01/DB/JTDS/jtds-1.1.jar:/u01/DB/DB2/
      db2jcc.jar:/u01/DB/DB2/db2jcc_license_cu.jar
   ```

3. Restart the affected domain.

Manually Modifying the Classpath of a Node Agent

This section shows you how to modify the classpath of a node agent, using the graphical interface and a file-based method.

Note

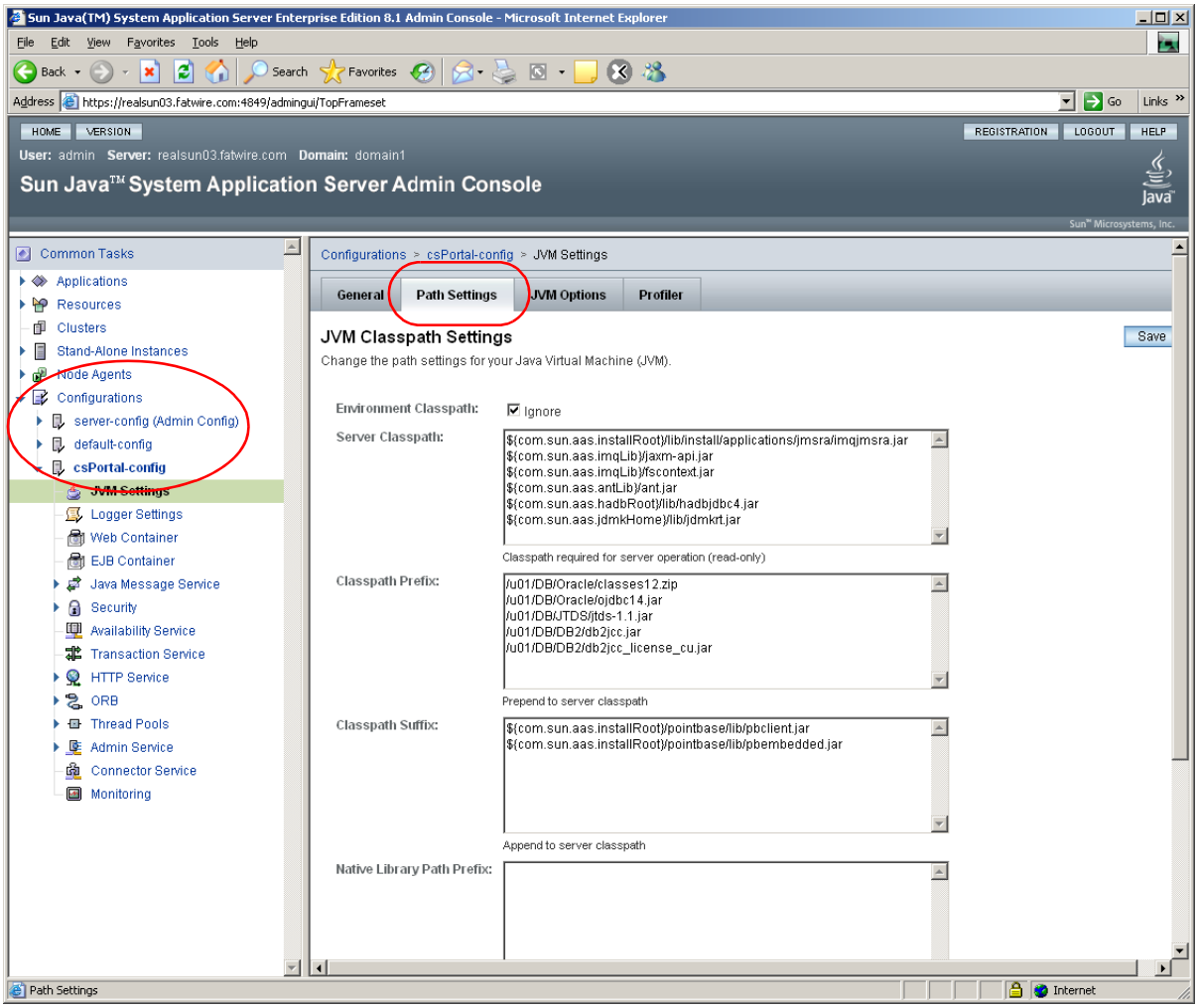
The graphical interface method is preferred. The file-based method is an advanced method for experienced users.

Graphical Method (preferred)

1. Open the admin console of the Sun JES Application Server and browse the left-hand tree to **Configurations** > ***instance_name*** > **JVM Settings**.
2. In the right-hand pane, select the **Path Settings** tab.

a. Add the correct paths to the list box “Classpath Prefix,” making sure to list one `jar` file per line.

b. Save the changes by clicking the **Save** button, then restart the instance.



File-based Method (advanced)

The file-based method for modifying the classpath of a node agent involves editing an XML file. In order to successfully edit the file, you must be especially careful to enter all characters correctly. Complete the following steps:

1. Make a backup of the `domain.xml` file located in `/var/opt/<jes_home>/domains/domain1/config/`
2. Using a text editor, open `domain.xml` located in `/var/opt/<jes_home>/domains/domain1/config/`
   a. Search for: `<instance name>-name`
   b. Search again for: `server-classpath`

c. Add a new section called: `classpath-prefix`

It has the following form:

```
classpath-prefix="/<path>/file.jar:
   ${path.separator}<path>/file.jar"
```

Example:

```
classpath-prefix="
  /u01/DB/Oracle/classes12.zip:
  ${path.separator}/u01/DB/Oracle/ojdbc14.jar:
  ${path.separator}/u01/DB/JTDS/jtds-1.1.jar:
  ${path.separator}/u01/DB/DB2/db2jcc.jar:
  ${path.separator}/u01/DB/DB2/db2jcc_license_cu.jar"
```

d. Save the changes.

3. Restart the domain.

Creating a New Data Source

Note

If you are using an Oracle database and require text attributes greater than 2000 characters, you will have to set `cc.bigtext` to `CLOB`. To support `CLOB`, use Oracle database 9.2.0.6 (or a higher supported version). Also use Oracle 10g drivers. (`CLOB` is not supported for lower database versions and for Oracle drivers 9x [thin, type 4].)

You will set `cc.bigtext` to `CLOB` when you run the Content Server installer (as explained in "Running the Installer," on page 123.)

1. List all currently created pools and all resources:

```
./asadmin list-jdbc-connection-pools --user admin \
   --password demo4132
```

```
./asadmin list-jdbc-resources --user admin --password demo4132
```

2. Create a new data pool for your database type:

- **For Oracle 9 and 10**:
  Include `ojdbc14.jar` and `classes12.zip` in the classpath

```
./asadmin create-jdbc-connection-pool --user admin \
   --password demo4132 --host localhost --port 4849 \
   --datasourceclassname oracle.jdbc.pool.OracleDataSource \
   --restype javax.sql.ConnectionPoolDataSource \
   --property User=JES3:Password=demo4132:URL=\
   "jdbc:oracle:thin:@10.120.16.55:1521:OraCS\
   " csPoolOracle
```

- **For SQL Server 2000**:
  Using the third-party JTDS driver, include `jtds-1.2.jar` in the classpath:

```
./asadmin create-jdbc-connection-pool --user admin \
   --password demo4132 --host localhost --port 4849 \
   --datasourceclassname net.sourceforge.jtds.jdbcx.
   JtdsDataSource --restype javax.sql.DataSource \
   --property User=csuser:Password=demo4132:
   SelectMethod=Cursor:DatabaseName=CS:serverName=\
   "win2k3db.fatwire.com\":portNumber=1433 csPoolJTDS
```

- **For DB2**:
  Using the third-party IBM DB2 drivers, include `db2jcc.jar` and `db2jcc_license_cu.jar`

```
./asadmin create-jdbc-connection-pool --user admin \
   --password demo4132 --host localhost --port 4849 \
   --datasourceclassname
   com.ibm.db2.jcc.DB2ConnectionPoolDataSource \
   --restype javax.sql.ConnectionPoolDataSource \
   --property User=csuser:Password=demo4132:URL=\"jdbc:db2:/
   /aixdb2.fatwire.com:50001/
   CS621JES\":driverType=4:serverName=aixdb2.fatwire.com:dat
   abaseName=CS:portNumber=50001 csPoolIBMDB2
```

Note

The data source command below automatically targets the default instance `server` to target another instance. Add the **`--target <instance name>`** option after **`--port <number>`**.

3. Create a new data source that connects to your pool above:

```
./asadmin create-jdbc-resource --user admin \
   --password demo4132 --host localhost --port 4849 \
   --connectionpoolid csPoolOracle jdbc/csDataSourceOracle
```

4. Restart the domain.
5. Test the pool:

```
./asadmin ping-connection-pool --user admin \
   --password demo4132 --host localhost \
   --port 4849 csPoolIBMDB2
```

Deleting a Data Source

1. List all currently created pools and all resources:

```
./asadmin list-jdbc-connection-pools --user admin \
   --password demo4132
```

```
./asadmin list-jdbc-resources --user admin --password demo4132
```

2. Delete the data pool:

```
./asadmin delete-jdbc-resource --user admin \
   --password demo4132 --host localhost --port 4849 jdbc/
   csDataSourceOracle
```

3. Delete the data source:

```
./asadmin delete-jdbc-connection-pool --user admin \
   --password demo4132 --host localhost --port 4849 csPoolDB2
```

Chapter 6

Deploying Applications

This chapter provides instructions for deploying Content Server as a web application and a portal.

This chapter contains the following sections:

Deploying Applications

This section provides instructions for completing the following operations:

- Deploying a Web Application
- Deploying a Portal Application (Portal Server 7.x on Application Server)
- Deploying a Portal Application (Portal Server 7.x on Web Server)

Deploying a Web Application

To deploy a web application on JES 2006Q4

1. List all currently deployed applications:

```
./asadmin list-application-refs --user admin --password
   <password> --host localhost --port 4848
```

2. Deploy Content Server:

```
./asadmin deploy --user admin --port 4848 --host localhost \
   --virtualservers server --contextroot servlet --upload \
   --name ContentServer –enabled=true \ <cs_application_path>
   /ContentServer.ear
```

3. List all currently deployed applications to confirm proper deployment:

```
./asadmin list-application-refs --user admin --password
   <password> --host localhost --port 4848
```

4. Restart the domain on which you deployed Content Server:
   a. Stop the domain: `./asadmin stop-domain <domain-name>`
   b. Start the domain: `./asadmin start-domain <domain-name>`

Deploying a Portal Application (Portal Server 7.*x* on Application Server)

Note

The commands in this section automatically target the default instance, `server`. To target another instance, add `--target <instance_name>` after `--port <number>`.

To deploy a portal application on Sun Portal Server 7.*x*

1. List all currently deployed applications:

```
/opt/sun/appserver/bin/asadmin list-application-refs --host
<hostname> --port 4849 --user admin server
```

2. Deploy the Spark portlet using the following command:

```
/opt/sun/portal/bin/psadmin deploy-portlet -u amadmin -f /opt/
sun/portal/bin/password -p portal1 -d
"o=DeveloperSample,dc=vm,dc=fatwire,dc=com" /u01/cs/
ominstallinfo/app/cs.war
```

3. List all currently deployed applications to confirm proper deployment:

```
/opt/sun/appserver/bin/asadmin list-application-refs --host
<hostname> --port 4849 --user admin server
```

4. Restart the instance on which you deployed Content Server (not required but strongly suggested):

```
./asadmin stop-instance --host localhost --port 4849 \
   --user admin --password demo4132 csPortal
```

```
./asadmin start-instance --host localhost --port 4849 \
   --user admin --password demo4132 csPortal
```

Deploying a Portal Application (Portal Server 7.x on Web Server)

Note

Before using the **wadm** command to complete the steps in this section, make sure you have created a password file for it. See "Before Using the wadm Command for the First Time," on page 72 for details.

1. List all currently deployed applications:

```
<jes_home>/webserver7/bin/wadm list-webapps --user=admin
   --port=8800 --password-file=/opt/sun/webserver7/bin/password
   --vs=<hostname> --config=<hostname> --no-ssl
```

2. If the target Web Server instance is not a brand new instance (that is, at least one application has been deployed to it at some point), re-deploy the instance's configuration from the config-store:

```
<jes_home>/webserver7/bin/wadm deploy-config --user=admin
   --port=8800 –password-file=<jes_home>/webserver7/bin/
   password --no-ssl --force <hostname>
```

3. Deploy the portal application using the following command:

```
<jes_home>/portal/bin/psadmin deploy-portlet -u amadmin –f
   <jes_home>/portal/bin/password -p portal1 -d
   "o=DeveloperSample,dc=vm,dc=fatwire,dc=com" <install_home>/
   ominstallinfo/app/cs.war
```

4. Restart the target Web Server instance. See "Web Server 7," on page 20 for the required commands.

5. List all currently deployed applications to confirm proper deployment:

```
<jes_home>/webserver7/bin/wadm list-webapps --user=admin
   --port=8800 --password-file=/opt/sun/webserver7/bin/password
   --vs=<hostname> --config=<hostname> --no-ssl
```

Undeploying Applications

This section provides instructions for completing the following operations:

- Undeploying a Web Application
- Undeploying a Portal Application (Portal Server 7.x on Application Server)
- Undeploying a Portal Application (Portal Server 7.x on Web Server)

Undeploying a Web Application

To undeploy a web application

Use the following command to undeploy a web application:

```
./opt/<jes_home>/sbin/asadmin undeploy --user admin --password
   demo4132 \ --host localhost --port 4849 --target csPortal cs
```

Undeploying a Portal Application (Portal Server 7.*x* on Application Server)

To undeploy a portal application

1. List all currently deployed applications:

```
/opt/sun/appserver/bin/asadmin list-application-refs --host
   <hostname> --port 4849 --user admin server
```

2. Use the following command to undeploy the portal application:

```
./opt/sun/portal/bin/psadmin undeploy-portlet -u amadmin -f \
    /opt/sun/portal/bin/password -p portal1 -d \
   "o=DeveloperSample,dc=vm,dc=fatwire,dc=com" cs
```

Undeploying a Portal Application (Portal Server 7.*x* on Web Server)

Note

Before using the **wadm** command to complete the steps in this section, make sure you have created a password file for it. See "Before Using the wadm Command for the First Time," on page 72 for details.

1. List all currently deployed applications:

```
<jes_home>/webserver7/bin/wadm list-webapps --user=admin
   --port=8800 --password-file=/opt/sun/webserver7/bin/password
   --vs=<hostname> --config=<hostname> --no-ssl
```

2.Re-deploy the Web Server instance configuration from the config-store:

```
<jes_home>/webserver7/bin/wadm deploy-config --user=admin
   --port=8800 -password-file=<jes_home>/webserver7/bin/
   password --no-ssl --force <hostname>
```

2. Undeploy the portal application using the following command:

```
<jes_home>/portal/bin/psadmin undeploy-portlet -u amadmin -f
   /opt/sun/portal/bin/password -p portal1
   -d "o=DeveloperSample,dc=vm,dc=fatwire,dc=com" cs
```

Chapter 7

Setting Up the Sun JES Application Server Load Balancing Plugin

If you plan to install a web server, you need to generate the load balancing plugin that comes with JES application server. This chapter provides instructions for generating the plugin.

This chapter contains the following sections:

Generating the JES Application Server Load Balancing Plugin

1. Create an `lb-config` file:

```
./asadmin create-http-lb-config  --host localhost --port 4849 \
   --user admin --password demo4132 --target csPortal
   lbconfig_csPortal
```

2. Run the following command for each instance, other than the first, that you want to be referenced in the `lb-config` file:

```
./asadmin create-http-lb-ref --host localhost --port 4849 \
   --user admin --password demo4132 --config lbconfig_csPortal
   csDB2
```

3. Enable the `http-lb-server` for each instance you included in the commands in steps 1 and 2:

```
./asadmin enable-http-lb-server --host localhost --port 4849 \
   --user admin --password demo4132 csPortal
```

4. Create a new health checker. Repeat this step for each instance you included in the commands in steps 1 and 2:

```
./asadmin create-http-health-checker --host localhost \
   --port 4849 --user admin --password demo4132 --config
   lbconfig_csPortal csPortal
```

5. Export the `lb-config` file to disk, then copy it to each web server that you will use:

```
./asadmin export-http-lb-config --host localhost --port 4849 \
   --user admin --password demo4132 --config lbconfig_csPortal
   /u01/lbconfig.xml
```

Deleting the JES Application Server Load Balancing Plugin

1. Delete the http health checker for each instance:

```
./asadmin create-http-health-checker --host localhost \
   --port 4849 --user admin --password demo4132 --config
   lbconfig_csPortal csPortal
```

2. Delete references to each instance you want to remove:

```
./asadmin delete-http-lb-ref  --host localhost --port 4849 \
   --user admin --password demo4132 --config lbconfig_csPortal
   csPortal
```

3. After all instances have been deleted, remove the `lb-config` file:

```
./asadmin delete-http-lb-config --host localhost --port 4849 \
   --user admin --password demo4132 lbconfig_csPortal
```

Part 3

Web Server

This part contains information related to the web servers that support Content Server web applications and portals. Note that installing a web server is optional.

This part contains the following chapters:

Chapter 8

Installing a Web Server

Content Server supports Sun Web Server 7 (portal installations only), and the Apache 2.x and Microsoft IIS web servers (web and portal installations).

For instructions on installing the web server, consult the following sources:

- If you are installing Sun Web Server 7, see “Installing JES,” on page 136.
- If you are installing an Apache web server on Linux or Solaris, consult our guide, *Configuring Third-Party Software* for instructions. If you are using an operating system other than Linux or Solaris, refer to the Apache documentation.
- If you are installing IIS on Windows, consult our guide, *Configuring Third-Party Software* for instructions. If you are using a different operating system, refer to the IIS documentation.

Chapter 9

Configuring the Web Server and JES Load Balancing Plugin

This chapter provides instructions for configuring the web server and the load balancing plugin for use with the web server.

This chapter contains the following sections:

Configuring Sun Web Server 7

This section shows you how to configure Sun Web Server 7 for use with Content Server.

Creating a Data Source in Sun Web Server 7

This section shows you how to create a data source that Sun Web Server 7 will use to communicate with the Content Server database.

1. Create a `lib` directory for the Web Server instance:

   ```
   mkdir /var/<jes_home>/webserver7/https-rho10wl.vm.fatwire.com/
      lib
   ```

2. Place the `.jar` files required by your configuration in the lib directory you created in step 1. (These `.jar` files will be included in the class path when the Web Server instance is restarted.) Refer to the table below for the names of `.jar` files applicable to your configuration.

Table 1: Data Source Information

Database Driver	Parameters	Values
JTDS (third-party driver)	DriverClass	`net.sourceforge.jtds.jdbcx.JtdsDataSource`
	Required `.jar` files	`jtds-1.2.jar`

	URL	`jdbc:jtds:sqlserver://<server>:<dbport>/<dbname>`
		Ex:
		`jdbc:jtds:sqlserver://10.120.14.22:1433/CS70`

DB2	DriverClass	`com.ibm.db2.jcc.DB2Driver`
	Required `.jar` files	`db2jcc.jar, db2cc_license_cu.jar`

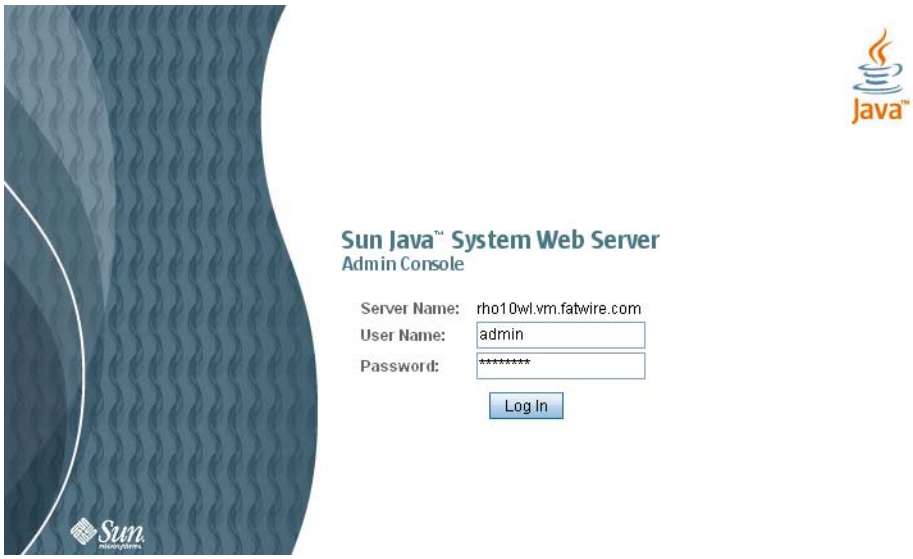
	URL	`jdbc:db2://<hostname>:<dbport>/<dbname>`
		Ex:
		`jdbc:db2://10.120.16.30:50001/WL814CS`

Oracle Thin driver	DriverClass	`oracle.jdbc.driver.OracleDriver`
	Required `.jar` files	`ojdbc14.jar`

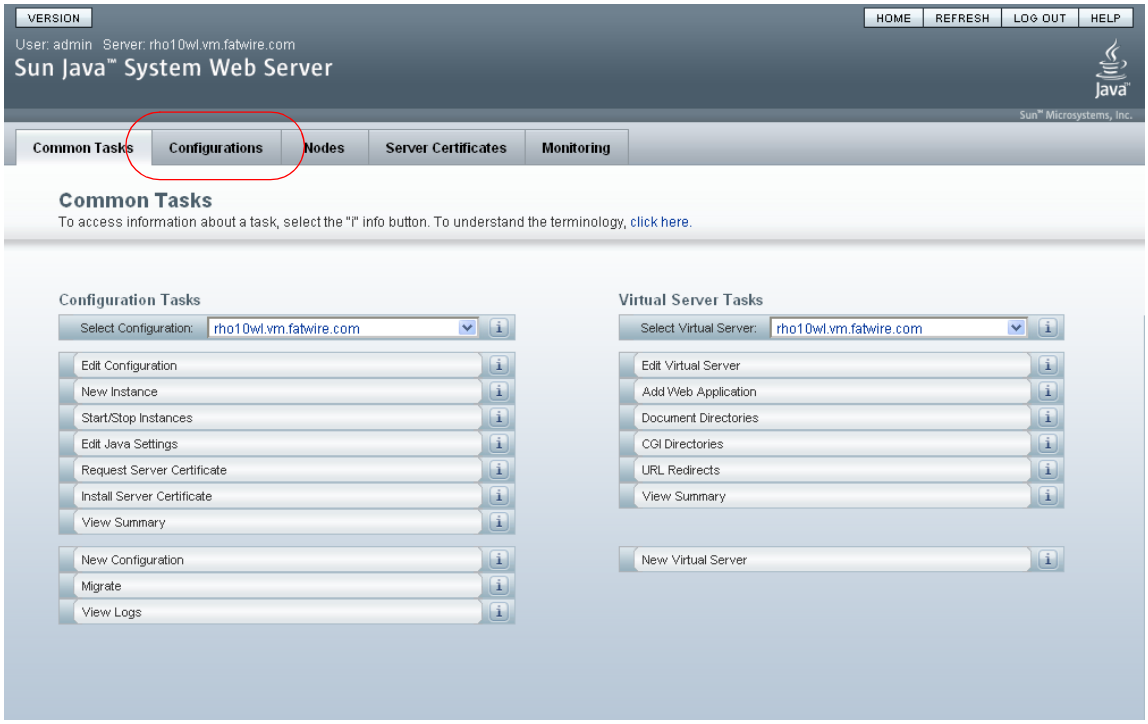
	URL	`jdbc:oracle:thin:@//<hostname>:1521/<dbname>`
		Ex:
		`jdbc:oracle:thin:@//godzilla.fatwire.com:1521/LINKSYS`

3. Restart the Web Server instance. See "Web Server 7," on page 20 for the appropriate start and stop commands.
4. Log in to the Web Server console as the `admin` user via the following URL:

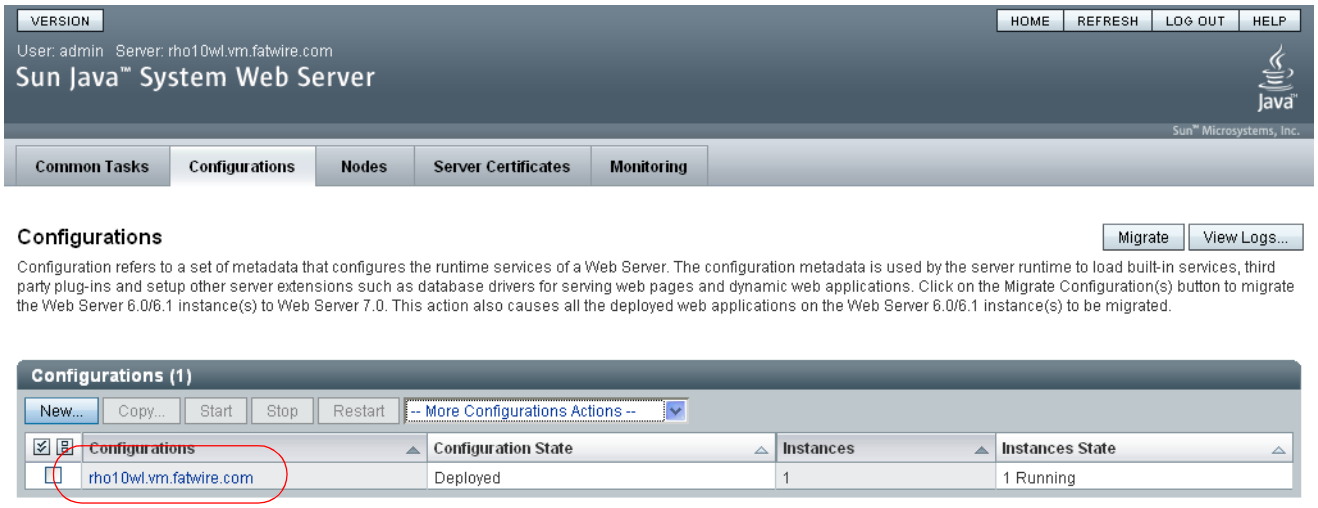
   `http://<host name>:8800`



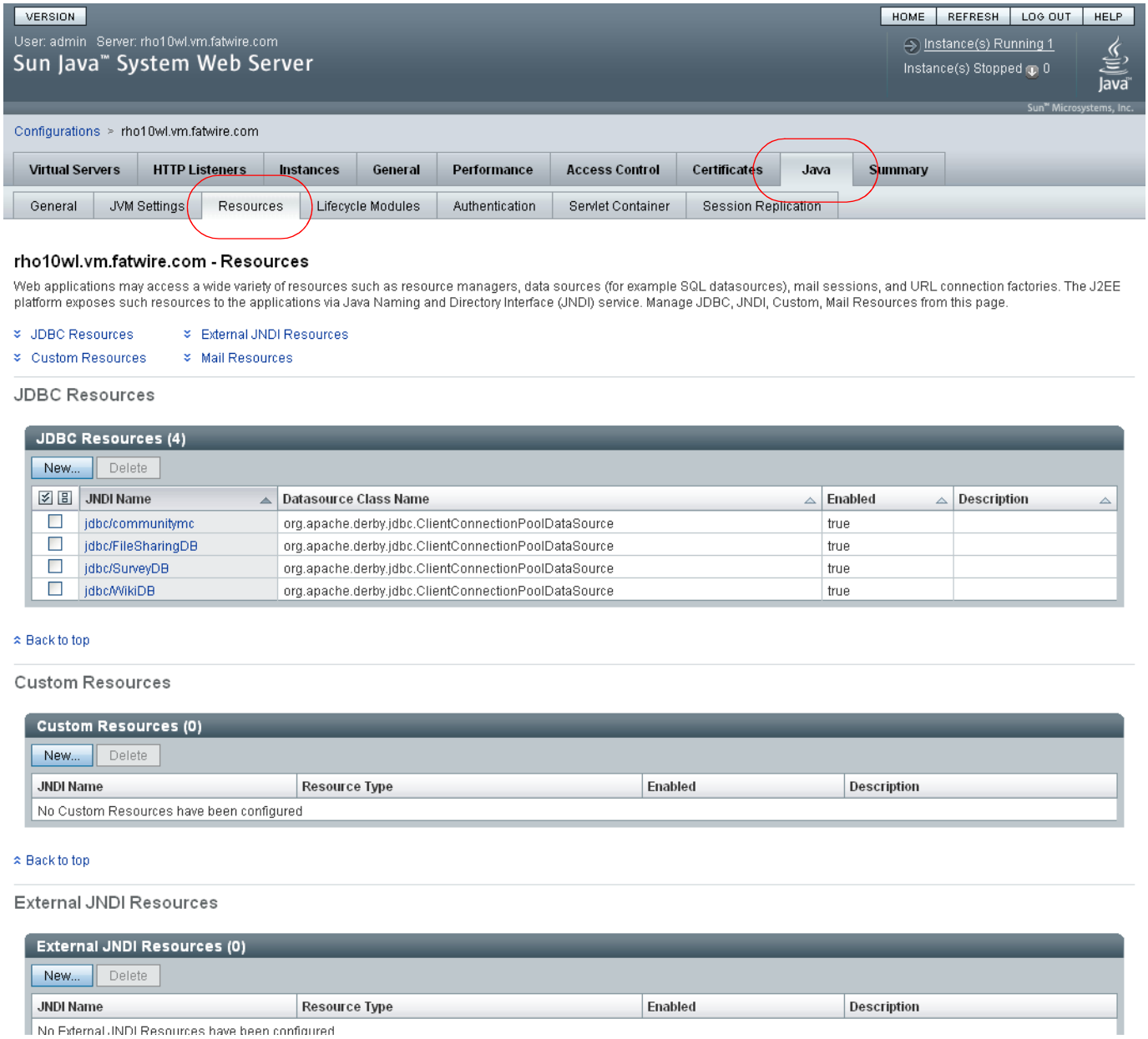
5. In the Web Server console, click the **Configurations** tab.



6. Click the configuration corresponding to the host on which JES is running.

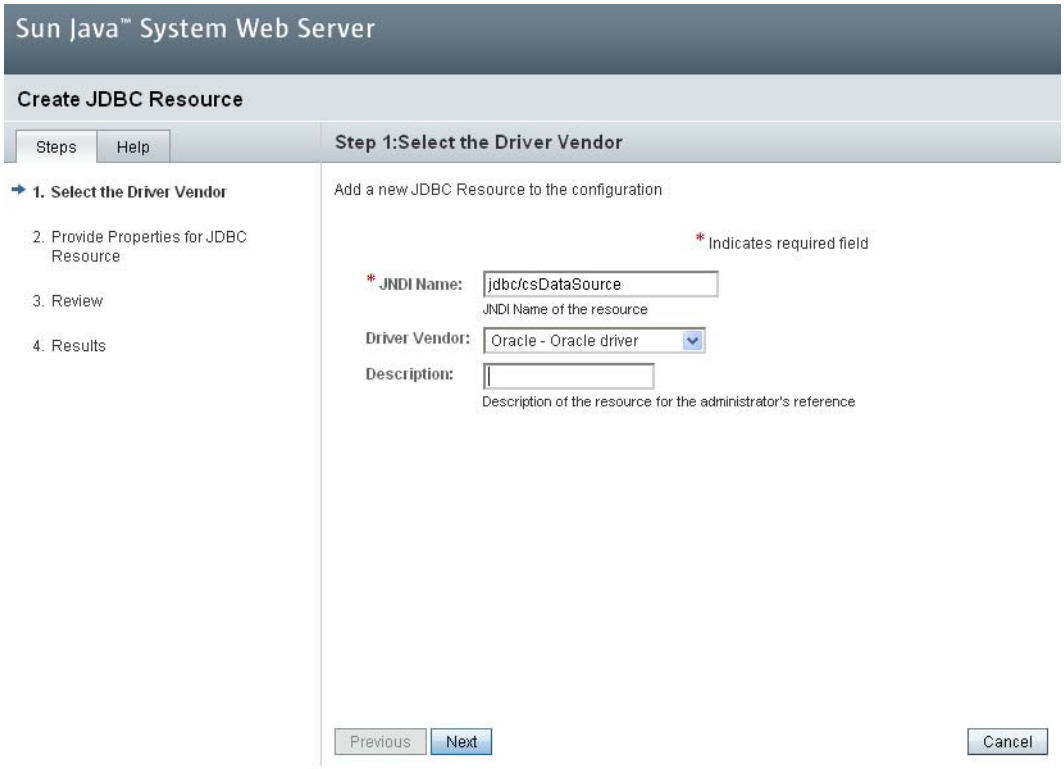


7. Click the **Java** tab, then the **Resources** sub-tab.



8. In the “JDBC Resources” section, click **New**.

9. In the pop-up window that appears, do the following:
   a. In the **JNDI Name** field, enter a name for the data source.
   b. In the "Driver Vendor" drop-down list, select the appropriate database driver vendor. Refer to Table 1, on page 66 for a list of supported drivers.
   c. Click **Next**.

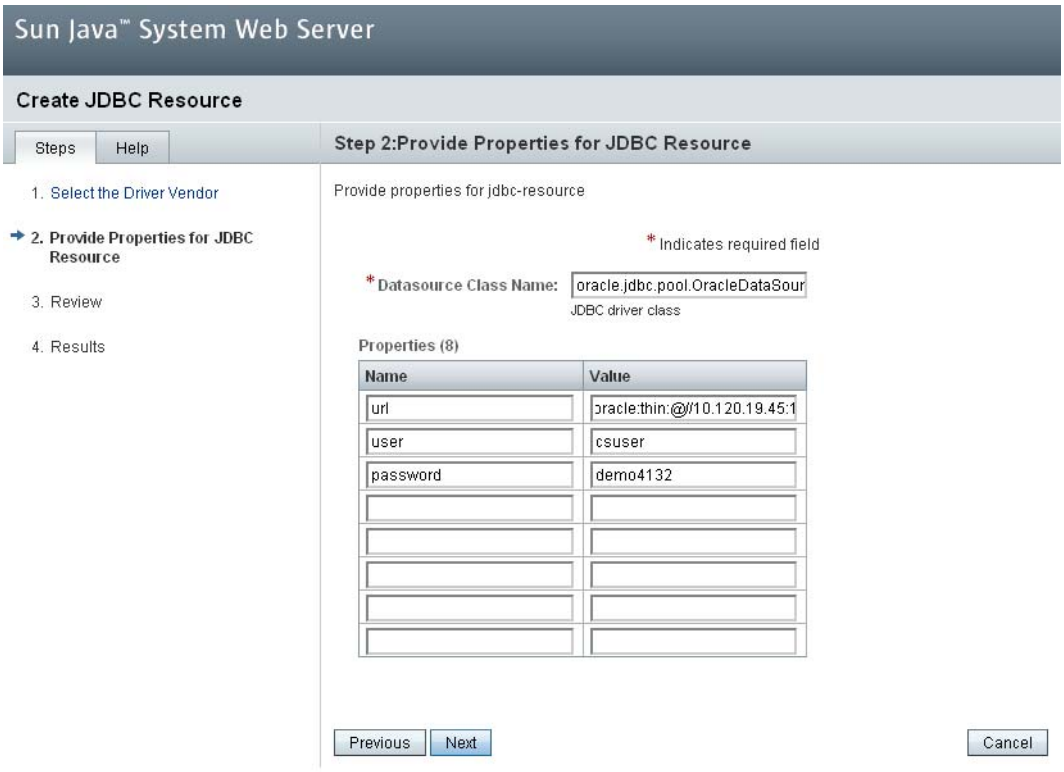


10. In the "Provide Properties for JDBC Resources" screen, do the following:

a. Enter the URL to your database. Refer to Table 1, on page 66 for the URL appropriate for your configuration.

b. Enter the user name and password of the database user used to connect to the CS database.

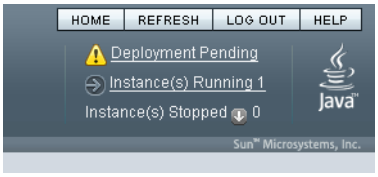
c. Click **Next**.



11. In the "Review" screen, review the information you entered, then click **Finish**.

12. In the "Results" screen, click **Close** to close the pop-up window.

The Portal Server console refreshes and a **Deployment Pending** link with a yellow exclamation mark icon appears at the top right of the console.



13. Click the **Deployment Pending** link.

14. In the pop-up window that appears, click **Deploy**.

When the deployment completes successfully, a confirmation message appears.

15. Click **Close** to close the pop-up window.

Synchronizing Web Server Instance Configurations

Sun JES stores the configuration of each Web Server instance present on your system in a configuration repository called the config-store. The config-store is located at `/var/<jes_home>/webserver7/admin-server/config-store`.

When working with Sun Web Server instances, you will use the **`wadm`** command for the following tasks:

- Synchronizing a Web Server Instance with the config-store. When you deploy an application to a Web Server instance, you must also deploy (or re-deploy) from the config-store the configuration of that instance. This ensures that the configurations are identical – if they are not, the Web Server instance will not function properly.
- Synchronizing the config-store with a Web Server Instance. When you make changes to the configuration of a Web Server instance already running an application, you must update the config-store's copy of that instance's configuration with the new version. Otherwise, your changes will be lost if you re-deploy the old configuration stored in the config-store.

Before Using the wadm Command for the First Time

Before you use the **`wadm`** command for the first time, you must create a password file (located in `<jes_home>/webserver7/bin/`) which will contain your JES admin password. This way, you do not need to enter the password each time you run the **`wadm`** command.

Create the password file as follows:

```
echo wadm_admin=<admin_password> > <jes_home>/webserver7/bin/
      password
```

Synchronizing a Web Server Instance with the config-store

Note

The admin server must be running before you can use the **wadm** command.

To re-deploy a configuration from the config-store to the target Web Server instance, use the following command:

```
<jes_home>/webserver7/bin/wadm deploy-config --user=admin
   --port=8800 -password-file=<jes_home>/webserver7/bin/password
   --no-ssl --force <hostname>
```

Synchronizing the config-store with a Web Server Instance

Note

The admin server must be running before you can use the **wadm** command.

To update the config-store with a new version of a Web Server instance configuration, use the following command:

```
<jes_home>/webserver7/bin/wadm pull-config --user=admin
   --port=8800 --password-file=<jes_home>/webserver7/bin/password
   --config=<hostname> --no-ssl <hostname>
```

Configuring the Apache and IIS Web Servers

Before you can use any external web server with the Sun JES application server, you must complete the steps required to create an lb-configuration. For instructions, see "Generating the JES Application Server Load Balancing Plugin," on page 60.

To configure the Apache or IIS web server, refer to the product documentation for instructions.

Configuring the Load Balancing Plugin for the Web Server

This section provides instructions for configuring the plugin that comes with and connects to Sun JES application server. The following configurations are covered:

- Configuring for Apache 2.x
- Configuring for IIS

Note

If you have not generated the load balancing plugin, do so now. For instructions, see "Generating the JES Application Server Load Balancing Plugin," on page 60.

Configuring for Apache 2.*x*

A. Configuration Requirements

- **Linux installations**: In order to use the Sun plugin with a Linux server, you must have a copy of the Sun Java Application Server installed before configuring Apache. See the *High Availability Administration Guide* (available from Sun) for the complete set of steps that are needed to install Apache as a front-end web server for Sun Java Application Server on Linux.
- **Solaris installations**: See the *High Availability Administration Guide* (available from Sun) for the complete set of steps that are needed to install Apache as a front-end web server for Sun Java Application Server on Solaris.
- `lbconfig.xml` refers to the file that was copied from the application server. Place `lbconfig.xml` in your `<apache install>/conf` directory.
- Copy from the application server to this server all the `.db` files that are associated with the domain you will be connecting to, and place the files into: `<apache install>/sec_db_files`
- Obtain the file `mod_loadbalancer.so` located in `/opt/<jes_home>/appserver/lib/webserver-plugin/<platform>/apache2/` for your given platform. Copy the file into the `<apache install>/libexec` directory.

B. Configuration Steps

1. Edit the `httpd.conf` file by adding the following lines:

```
LoadModule apachelbplugin_module libexec/mod_loadbalancer.so
#AddModule mod_apachelbplugin.cpp
<IfModule mod_apachelbplugin.cpp>
config-file <apache install>/conf/lbconfig.xml
locale en
</IfModule>
```

2. If Apache is located on Solaris, add the following line before the block of lines in step 1 above:

```
LoadFile /usr/lib/libCstd.so.1
```

3. Under `<apache install>`, create a new directory named: `sec_db_files`
4. Copy all the files from the directory `/var/opt/domains/domain1/config/*.db` on the application server to `<apache install>/sec_db_files`.
5. Modify the `apachectl` file located in `<apache install>/bin` by adding the following to the beginning of the `LIB_PATH` statement:

   Linux: `/opt/sun/private/lib`

   Solaris: `/usr/lib/mps/secv1`
6. Stop and restart Apache.

Configuring for IIS

> **Note**
>
> In order to use the Sun plugin with IIS, you must install a copy of the Sun JES application server locally.

1. Copy the file `lbconfig.xml` to the local machine and place it in: `wwroot\sun-passthrough`
2. Locate the file `sun-passthrough.dll` in the Sun JES application server. Install and copy the file to a directory under: `wwroot\sun-passthrough`
3. Open the **ISAPI Filters** tab and add a new filter:

   name: `lbpassthrough`

   executable: location of the file copied in step 1
4. Right-click on the website which will forward your request to Sun JES application server and select **New > Virtual Directory**.

   Alias: `sun-passthrough`

   Path: `wwwroot\sun-passthrough`

   Permissions: execute only
5. Add the location of the Sun JES application server `install/bin` directory to the system path.
6. Stop the web server instance that was edited.

7. Restart the server.
8. Start the web server instance that was edited.
9. Edit the file `sun-passthrough.properties` in `wwwroot\sun-passthrough` by modifying the property `lb-config-file` to point to the `lbconfig.xml file` that was copied in step 1.
10. Restart the web server.

Chapter 10

Configuring a Portal Installation

This chapter shows you how to configure a portal installation of Content Server.

This chapter contains the following sections:

Turn Off Parallel Portlet Render Mode

Go to `/var/opt/sun/portal/portals/<portal_name>/config/` and edit the `desktopconfig.properties` file by changing the following line:

from:

```
portletRenderModeParallel=true
```

to:

```
portletRenderModeParallel=false
```

Populating the Portal Interface

In this section, you will create portlet channels, select the portlets you wish to display, and create the container channels which will display the portlets.

Note

In this guide, “container channel” is also called “display page.”

This procedure consists of the following steps:

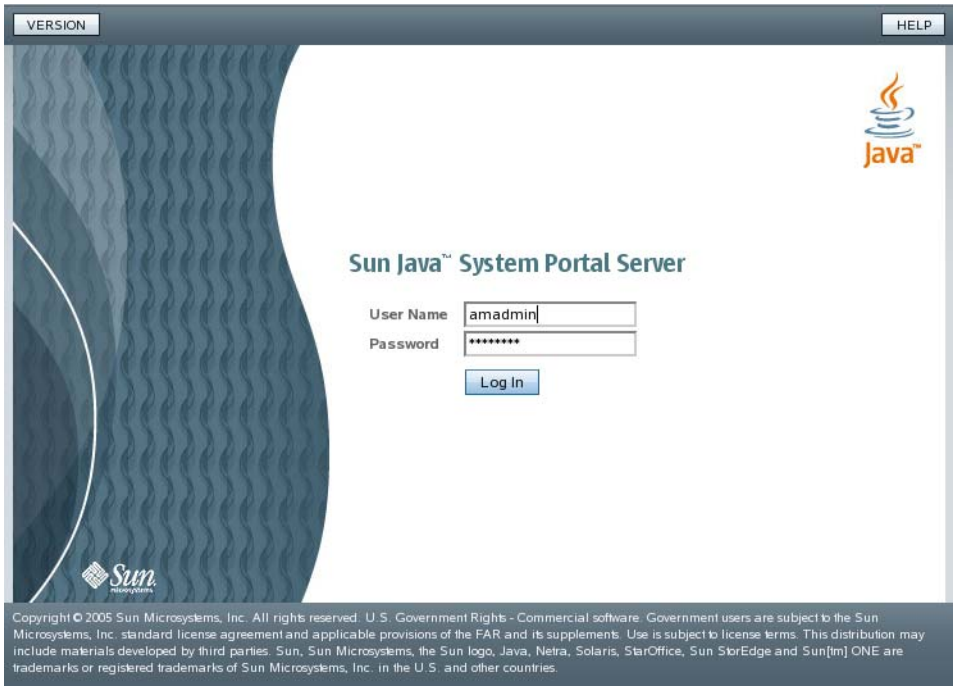
A. Create a New Portal Tab

B. Create Portlet Containers Under the New Tab Container

C. Add Portlets to Each Tab Container

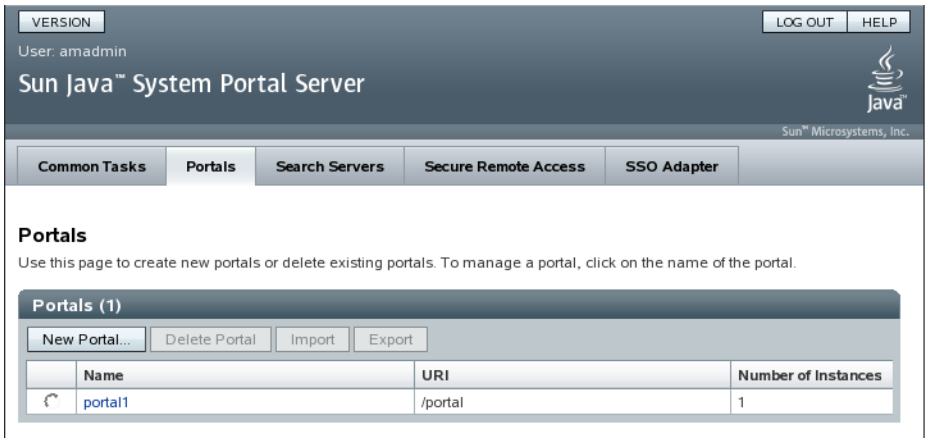
A. Create a New Portal Tab

1. Log in to the Portal Server console as the `amadmin` user via the following URL: `http://<servername>:8080/psconsole`.

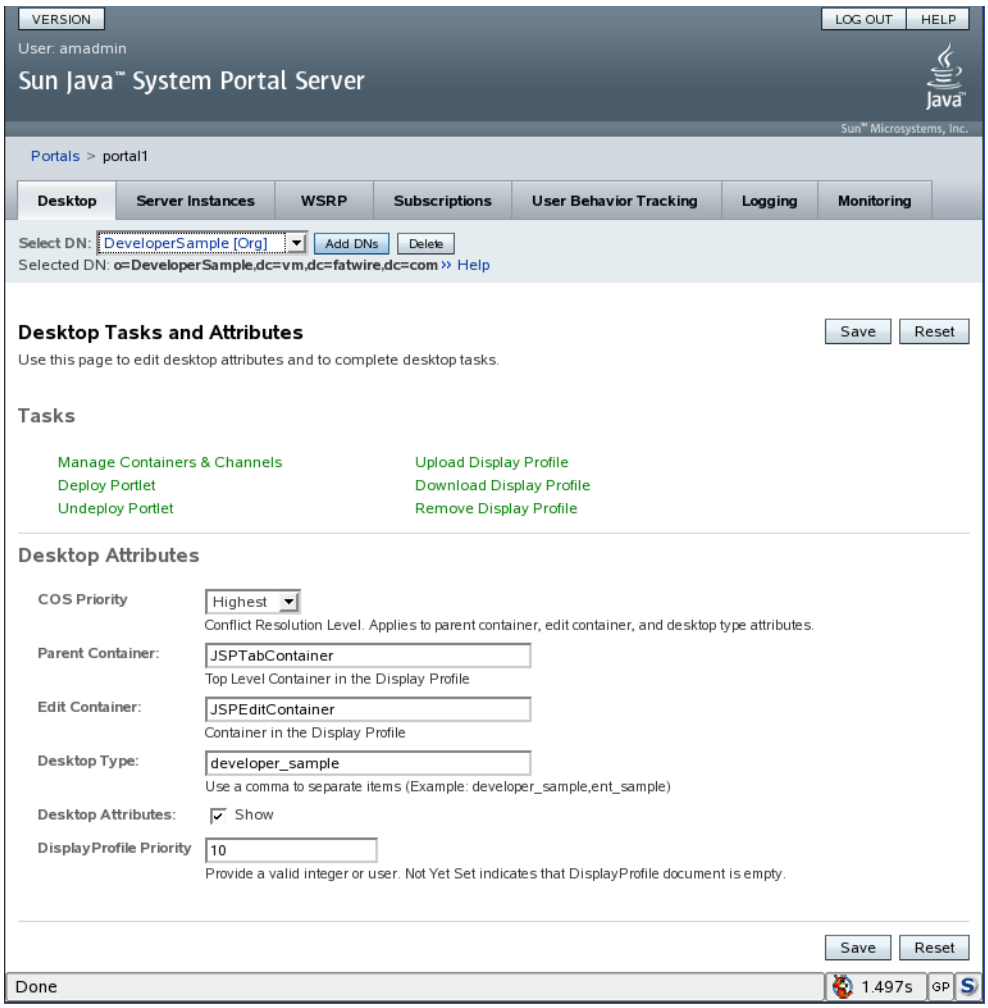


2. Select the **Portals** tab.

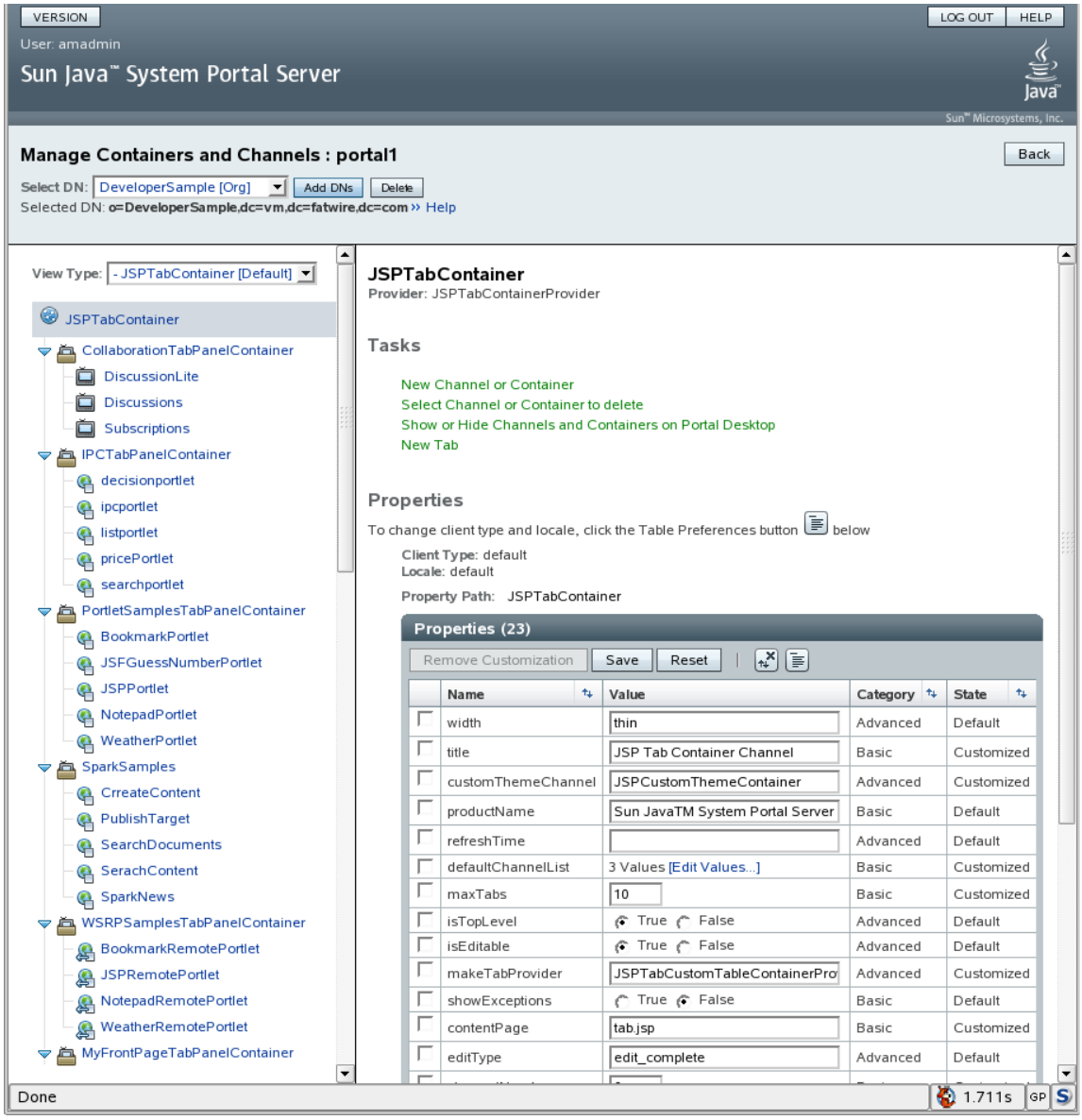
3. Select the portal on which Content Server is installed.



4. In the “Select DN:” drop-down list, select **DeveloperSample [Org]**.
5. In the “Tasks” area, click the **Manage Containers & Channels** link.

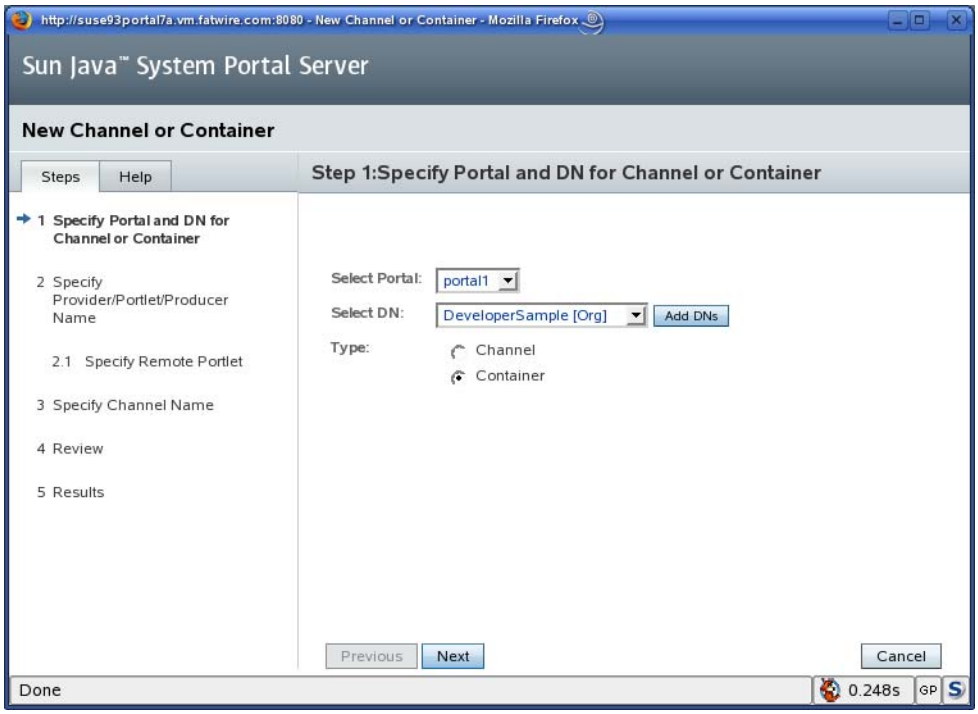


6. In the “View Type” drop-down list on the “Manage Containers and Channels” page, select **- JSPTabContainer [Default]**.

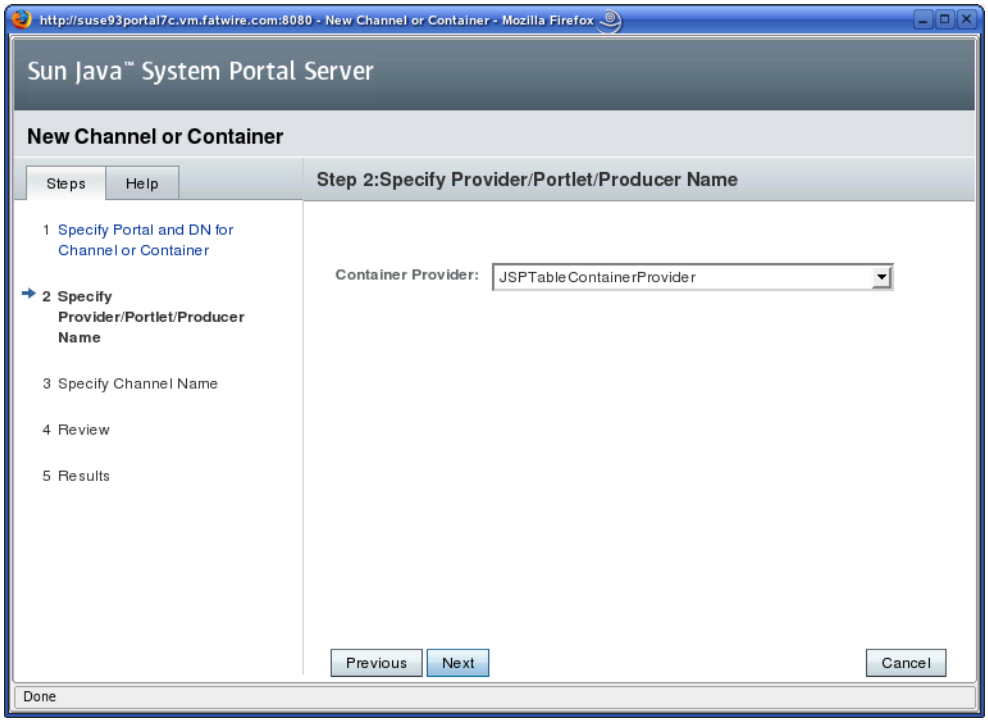


7. In the “Tasks” area, click the **New Channel or Container** link.

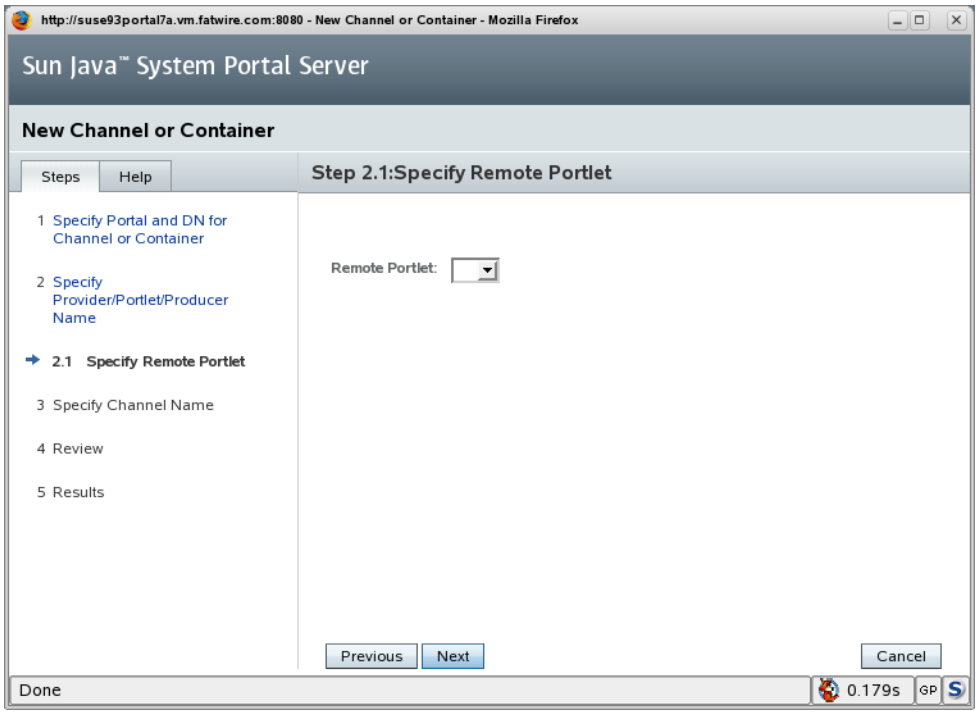
8. In the “New Channel or Container” pop-up window, select **Container** and click **Next**.



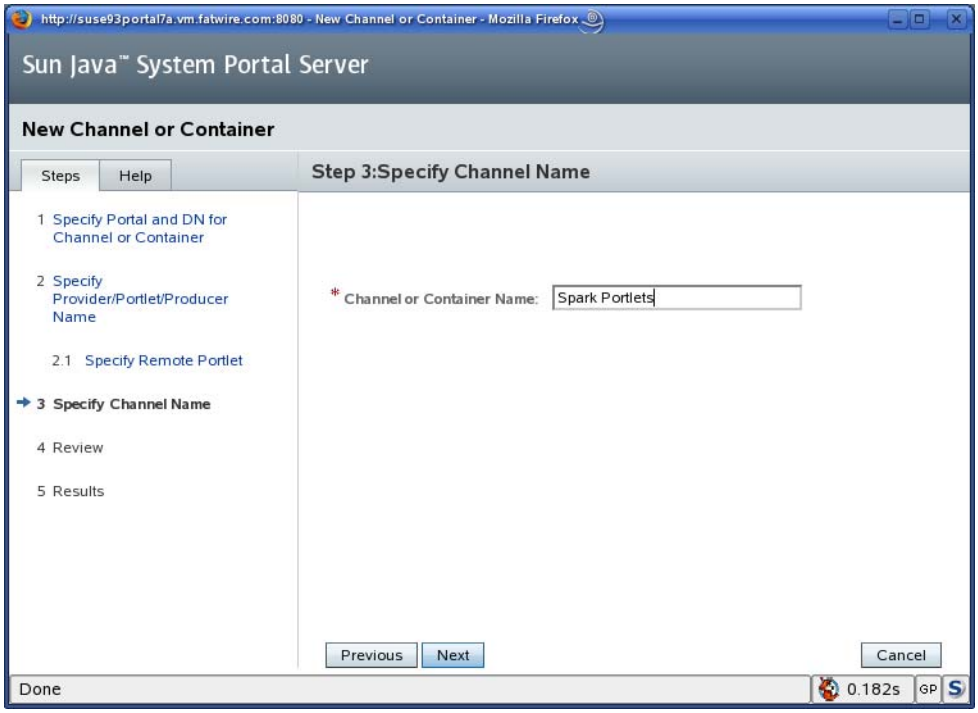
9. In the “Container Provider” drop-down list, select **JSPTabContainerProvider** and click **Next**.



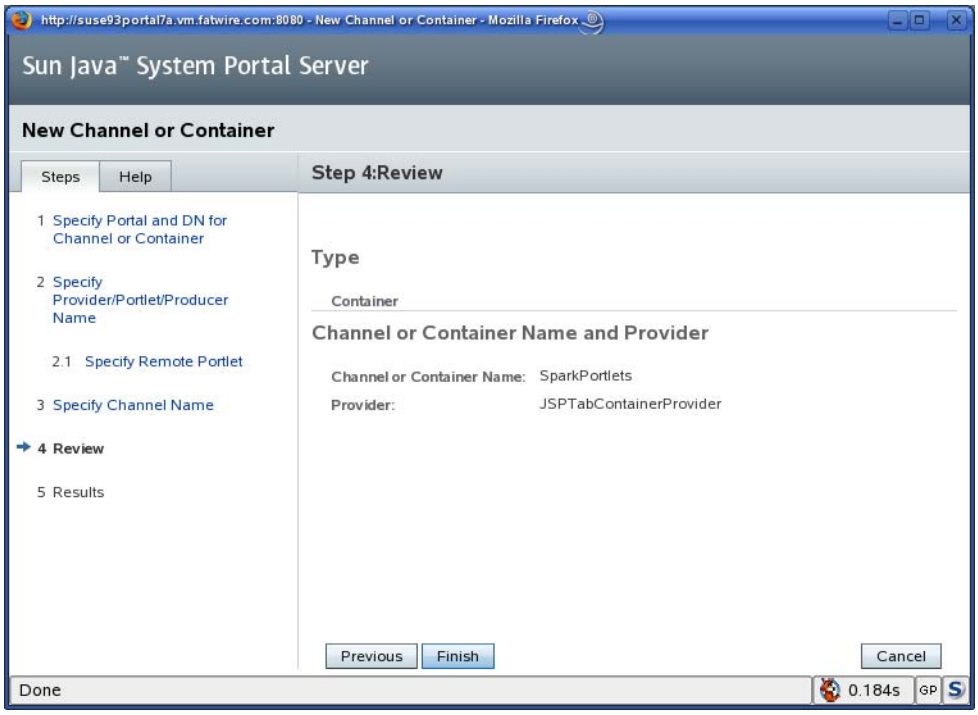
10. Do not select anything in the “Remote Portlet” drop-down list; click **Next**.



11. Enter a name for the new portal tab and click **Next**.

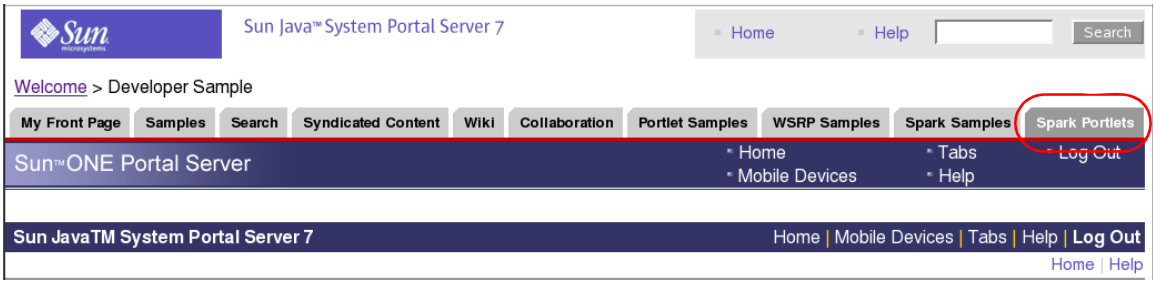


12. In the "Review" screen, click **Finish**.

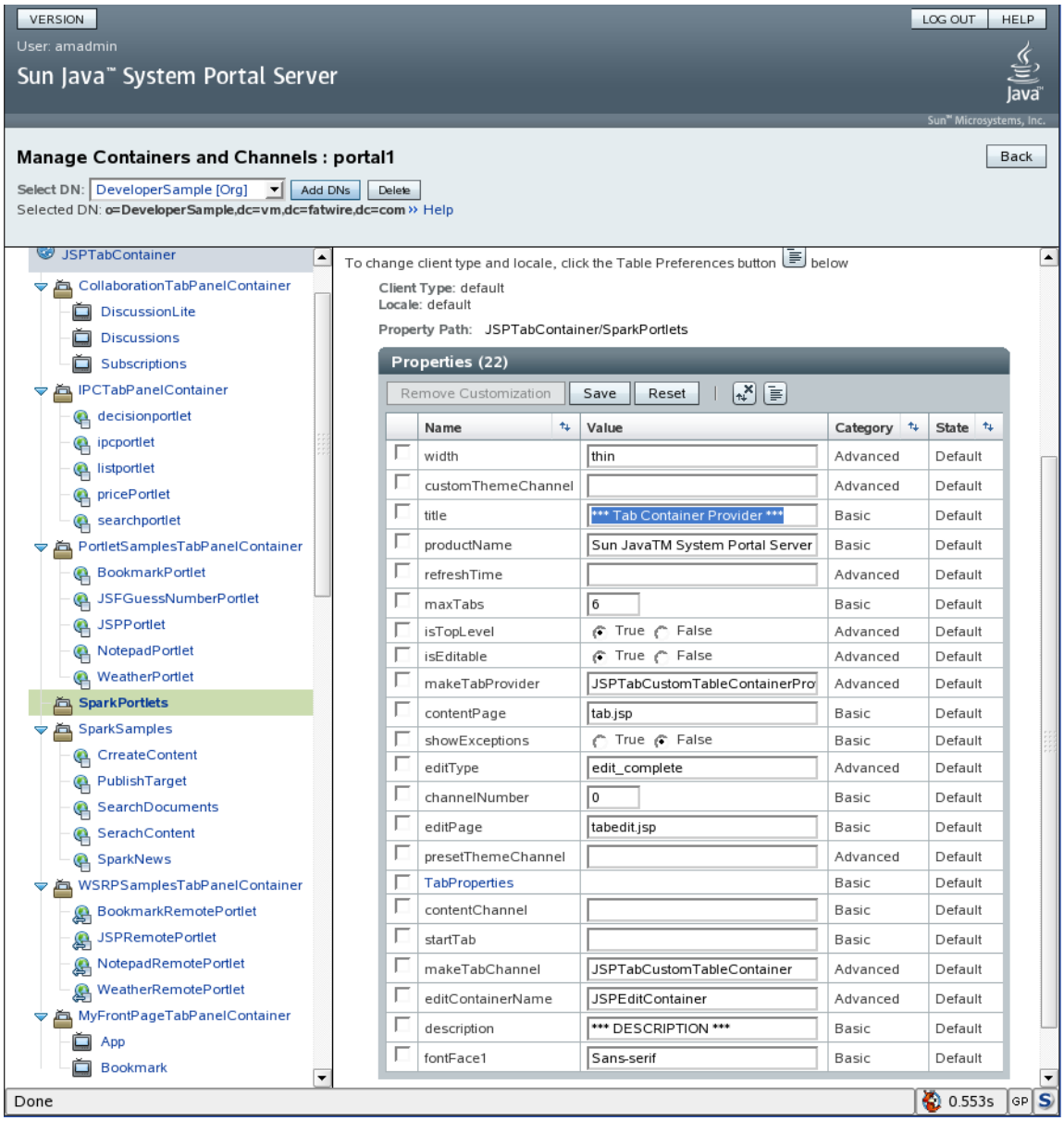


13. In the "Results" screen, click **Close**.

The new tab container appears in the left-hand pane; the tab it represents appears in your portal.

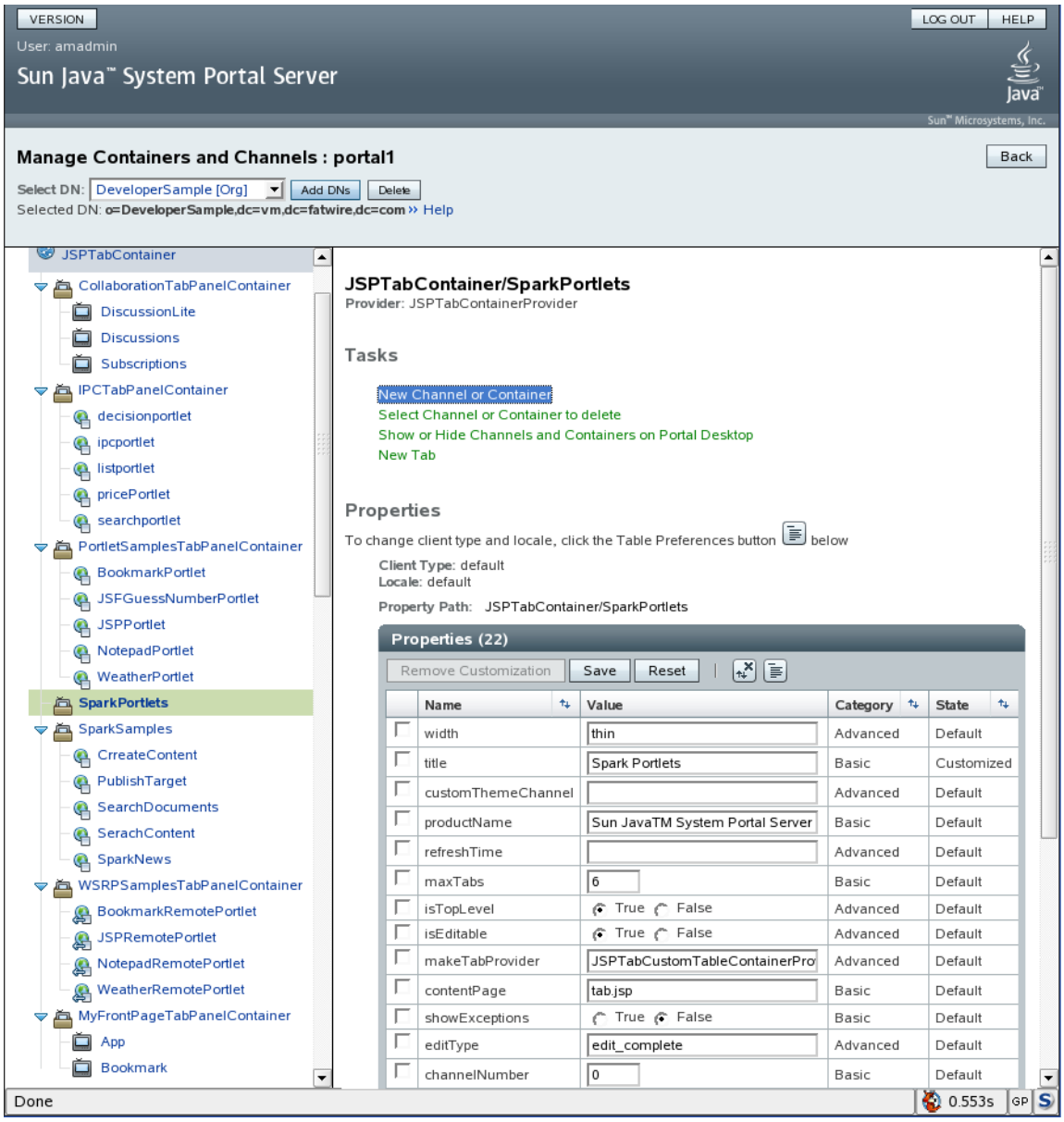


14. In the left-hand pane, select the tab container you just created and enter a descriptive value for the **title** property, then click **Save**.

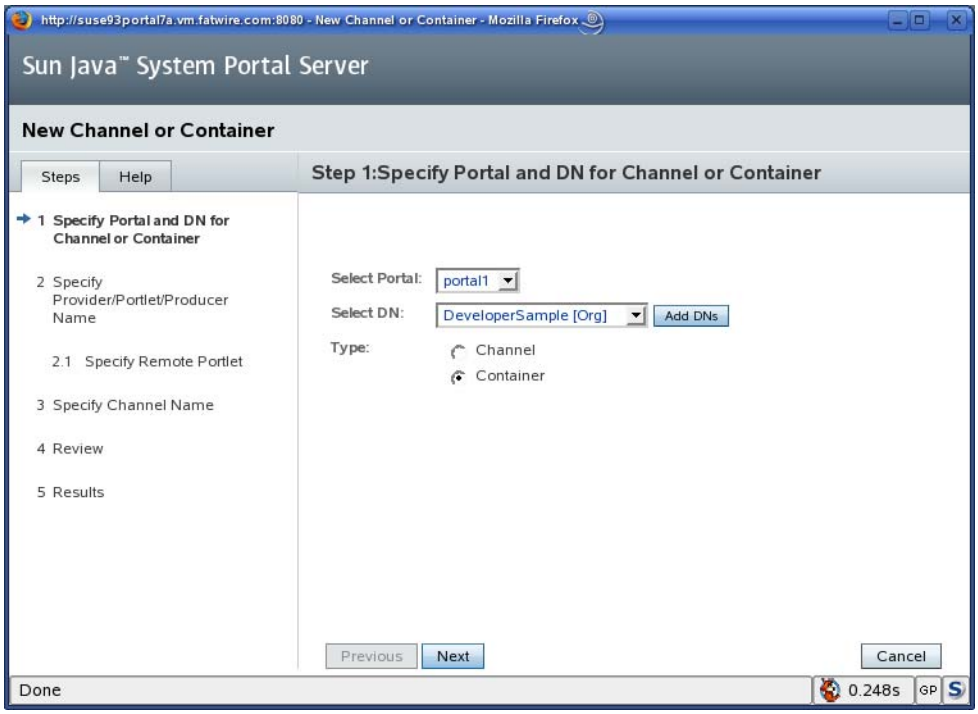


B. Create Portlet Containers Under the New Tab Container

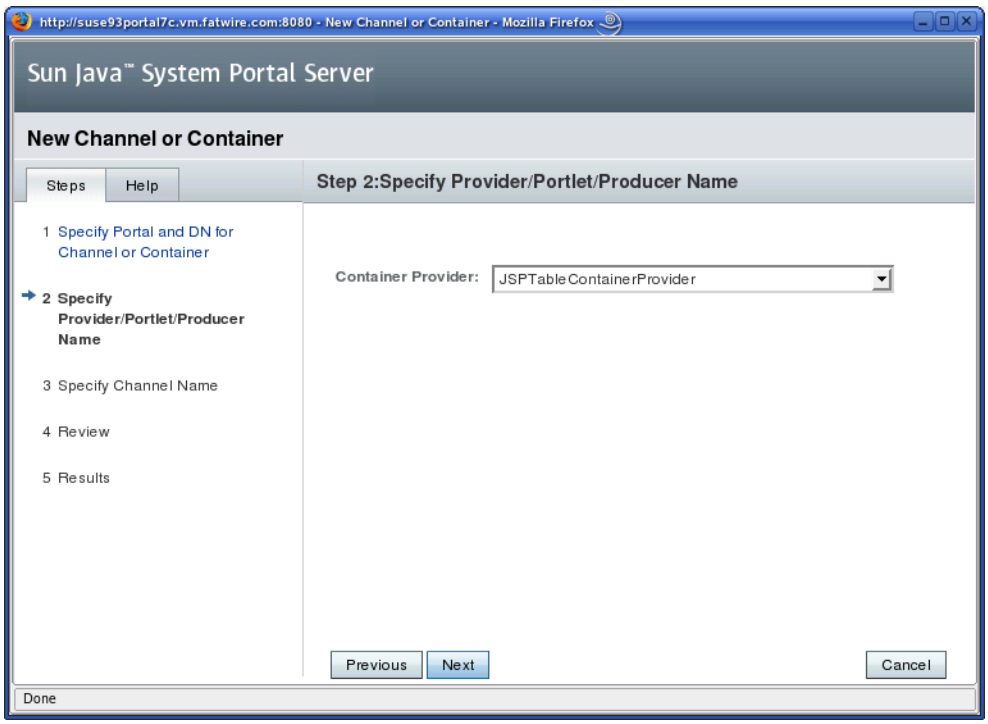
1. In the left-hand pane, select the tab you created in step A.
2. In the right-hand pane, click **New Channel or Container**.



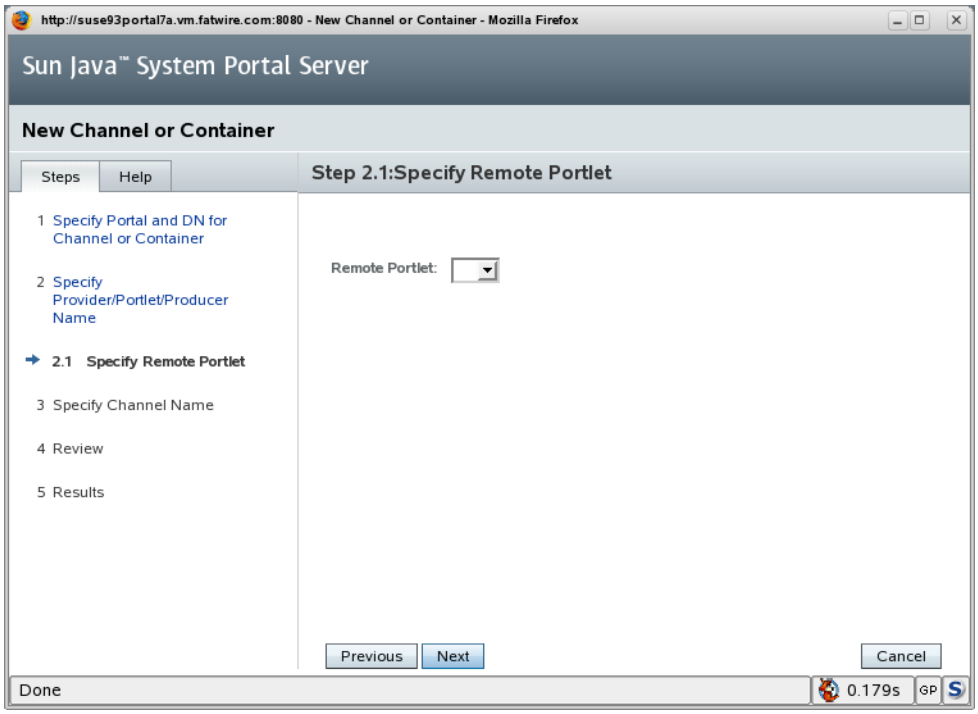
3. In the “New Channel or Container” pop-up window, select **Container** and click **Next**.



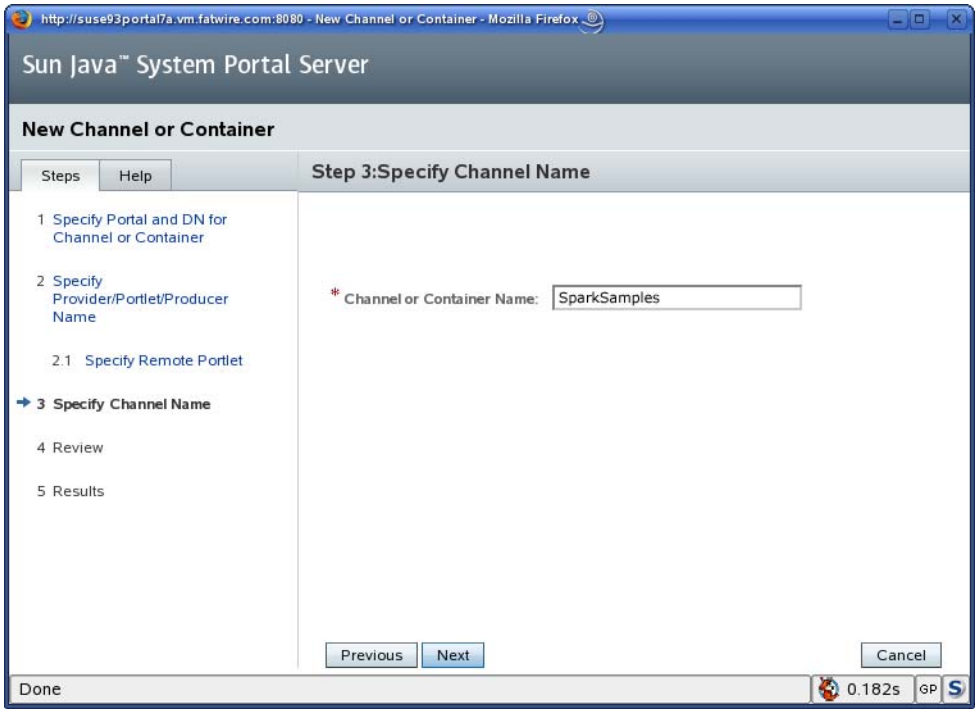
4. In the “Container Provider” drop-down list, select **JSPTableContainerProvider** and click **Next**.



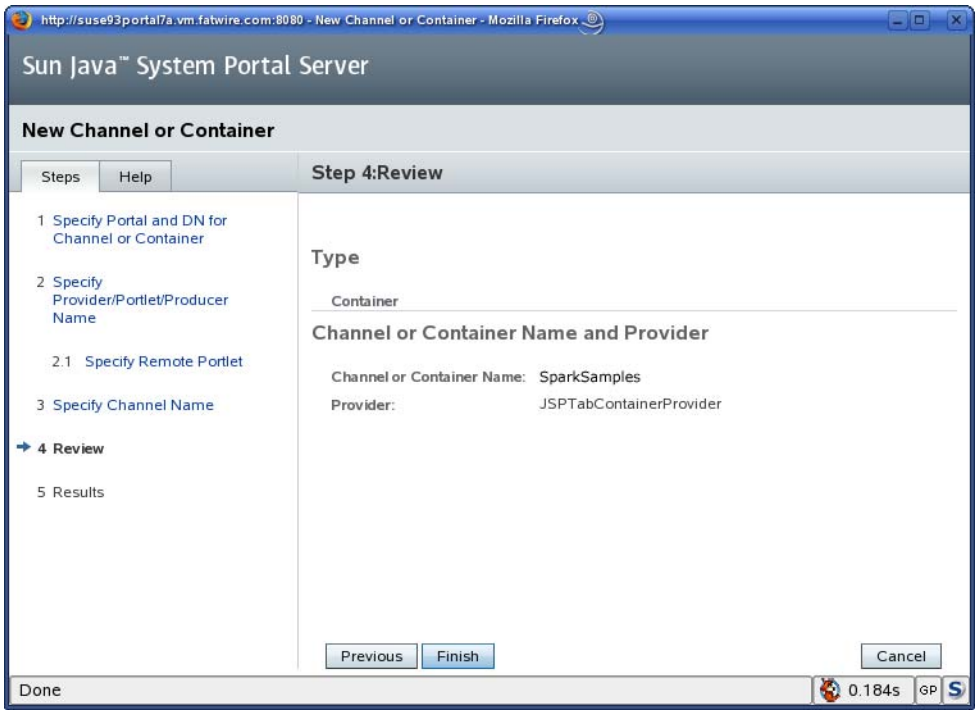
5. Do not select anything in the “Remote Portlet” drop-down list; click **Next**.



6. Enter a name for the new container and click **Next**.



7. In the “Review” screen, click **Finish**.

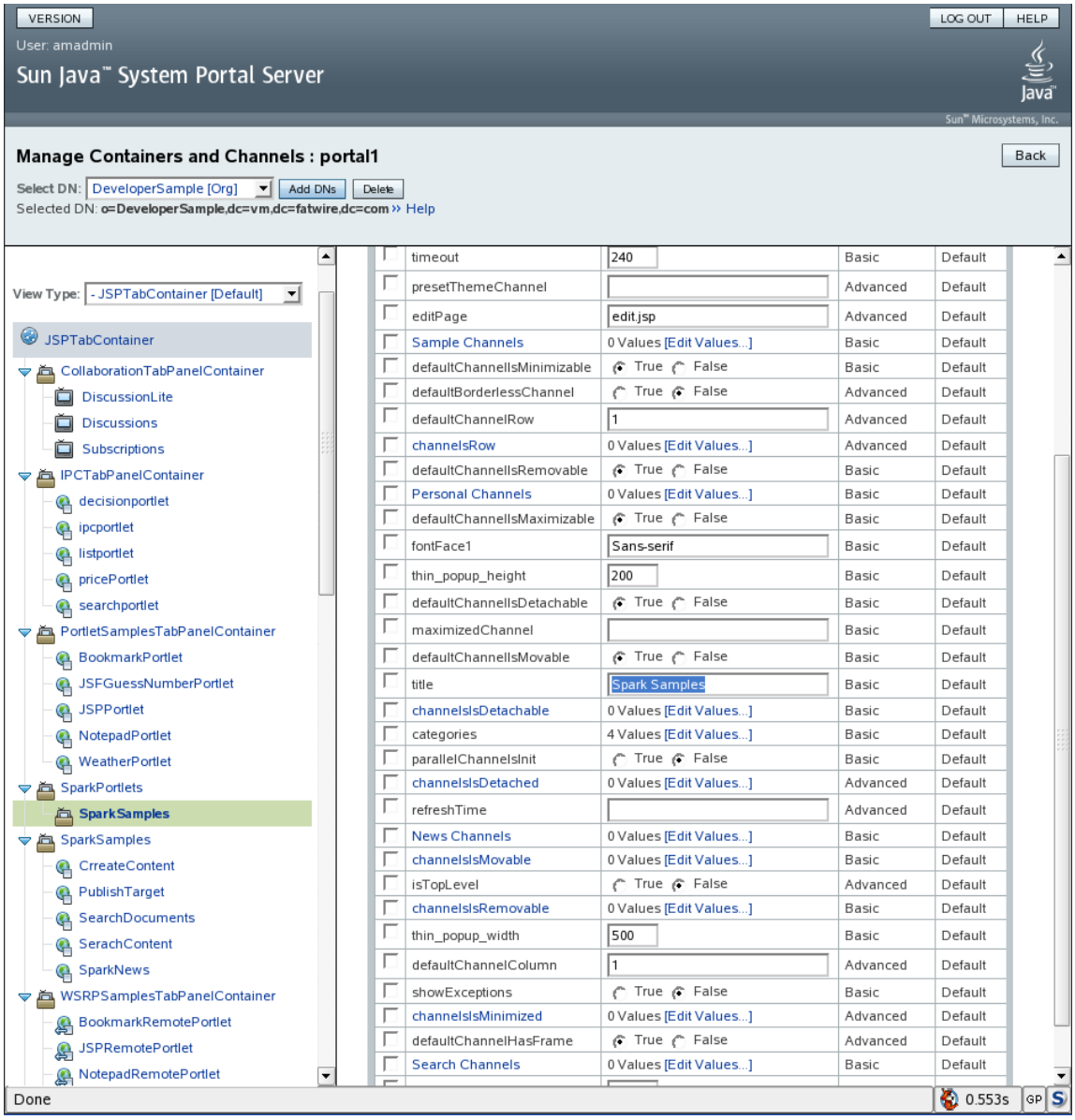


8. In the “Results” screen, click **Close**.

   The new container appears below the tab container you created in step A.

9. In the left pane, selected the newly created container and enter a descriptive value for the **title** property. Suggested container names are the following:
   - FatWire Spark
   - FatWire Content
   - FatWire Documents
   - FatWire Admin

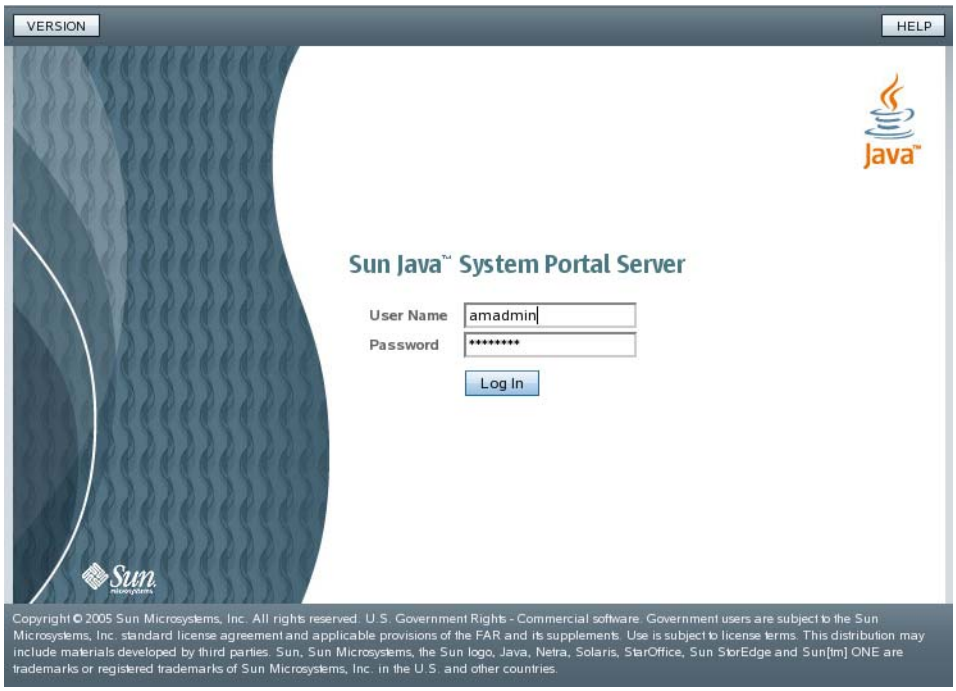
   When you are finished, click **Save**.



10. Repeat steps 1 – 9 to create additional containers.
11. When you are finished, log out of the Portal Server Admin Console to save your changes.

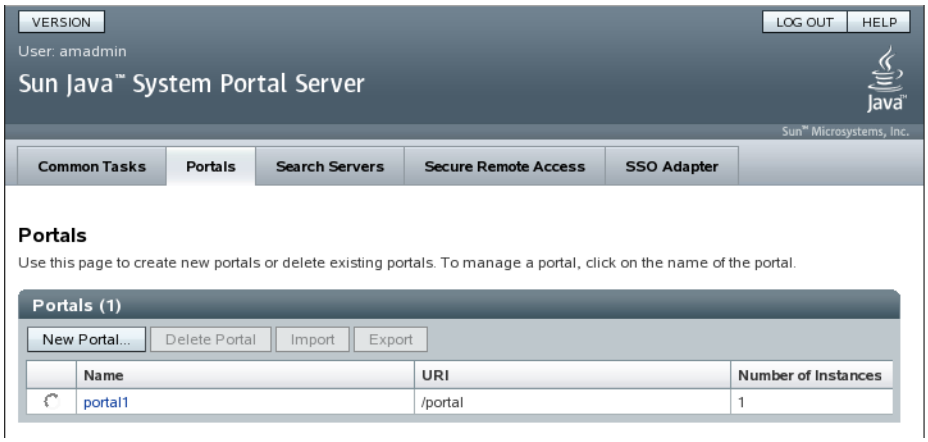
C. Add Portlets to Each Tab Container

1. Log in to the Portal Server console as the `amadmin` user via the following URL: `http://<servername>:8080/psconsole`

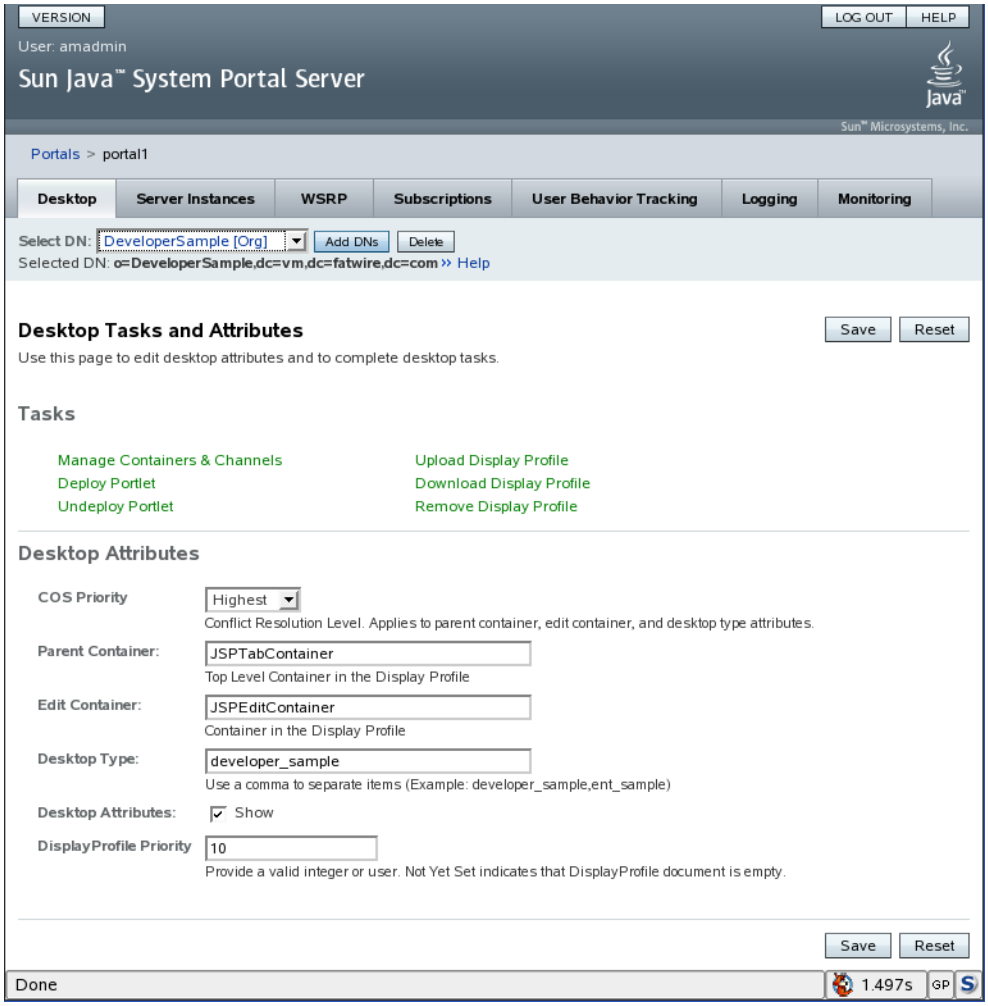


2. Select the **Portals** tab.

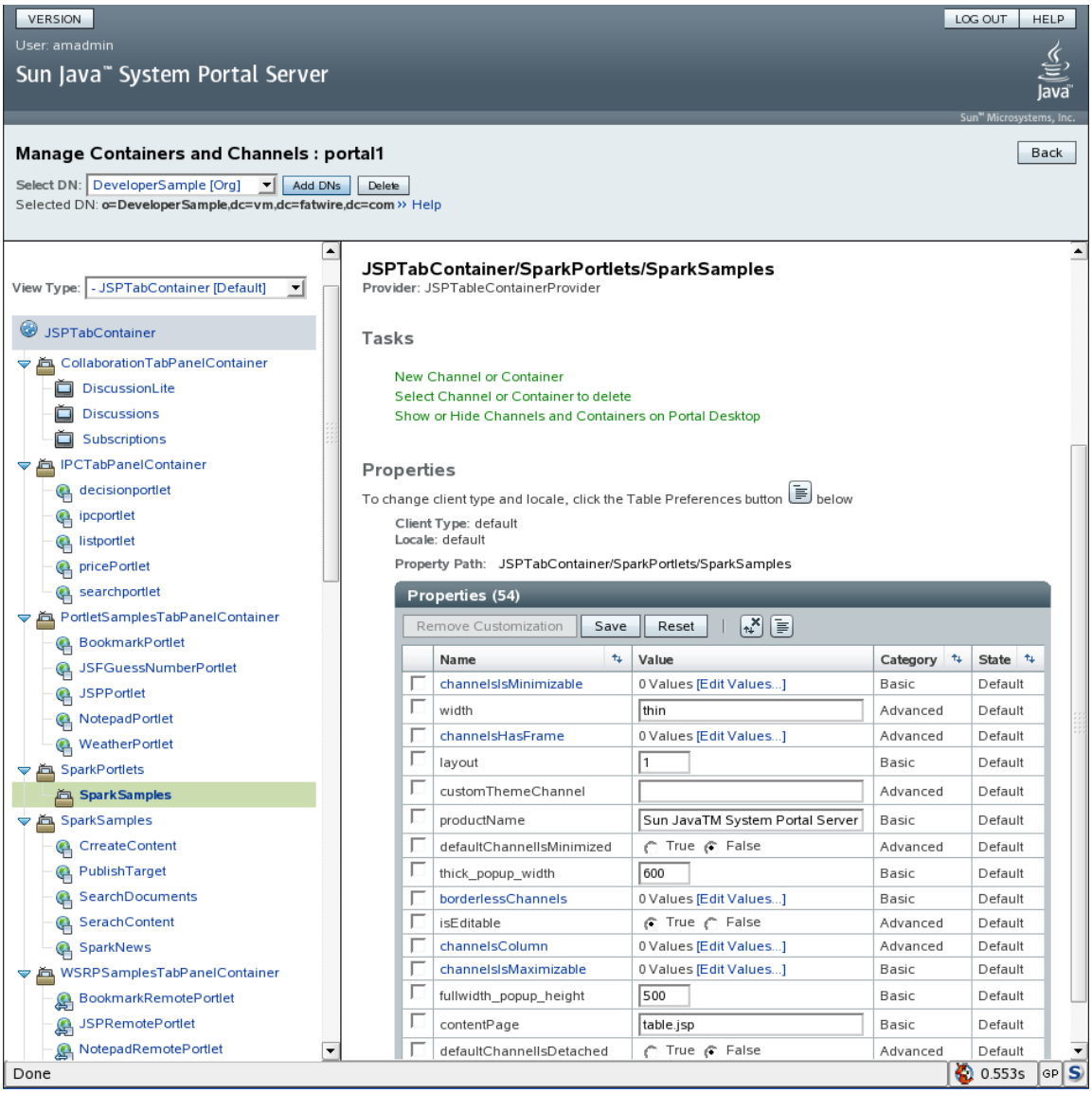
3. Select the portal on which Content Server is installed.



4. In the “Select DN:” drop down list, select **DeveloperSample [Org]**.
5. In the “Tasks” area, click the **Manage Containers & Channels** link.

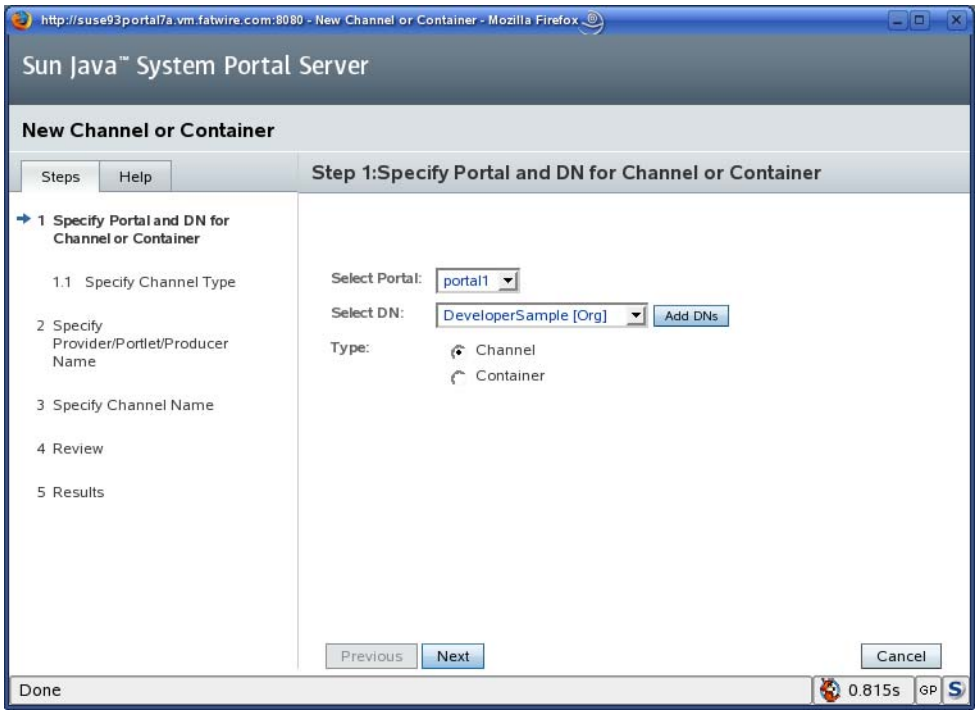


6. In the “View Type” drop-down list on the “Manage Containers & Channels” page, select **- JSPTabContainer [Default]**.

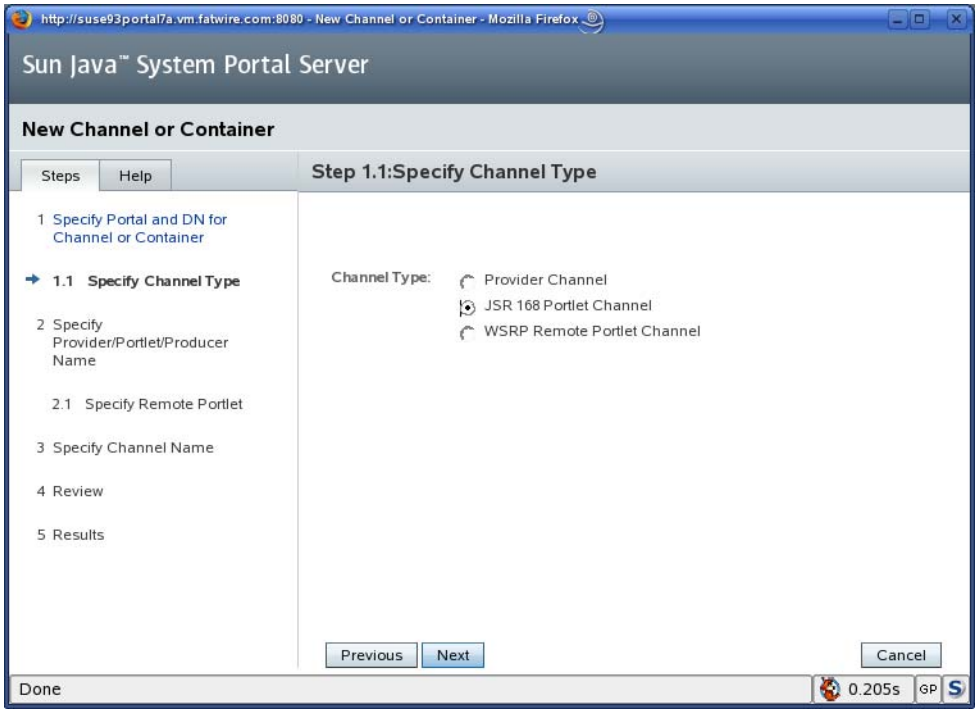


7. In the left-hand pane, select the container to which you want to add a portlet.
8. In the right-hand pane, click the **New Channel or Container** link.

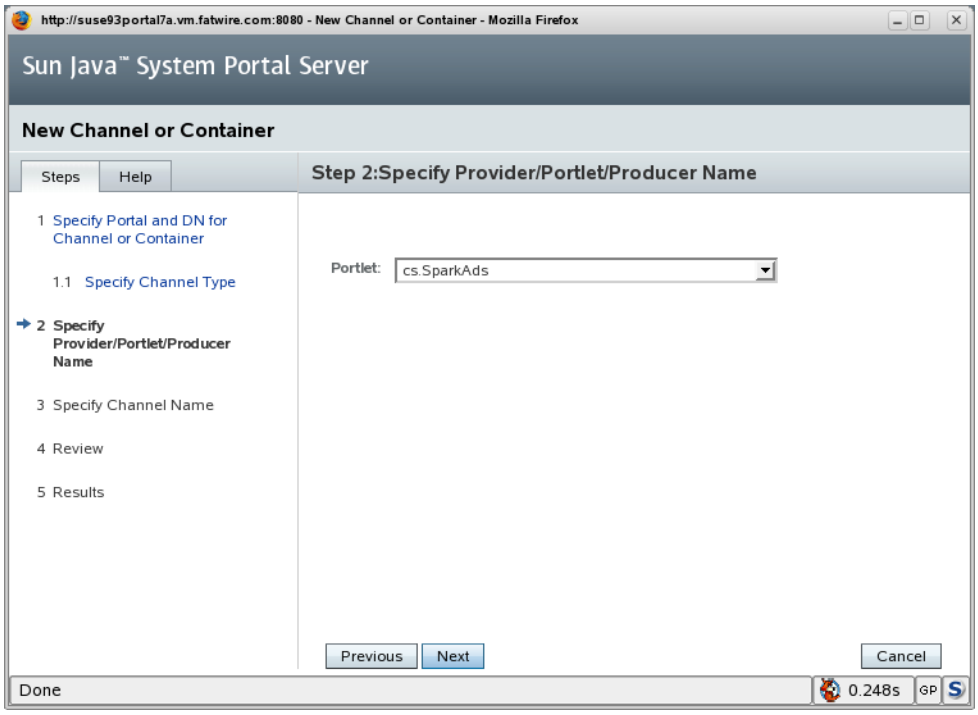
9. In the “New Channel or Container” pop-up window, select **Channel** and click **Next**.



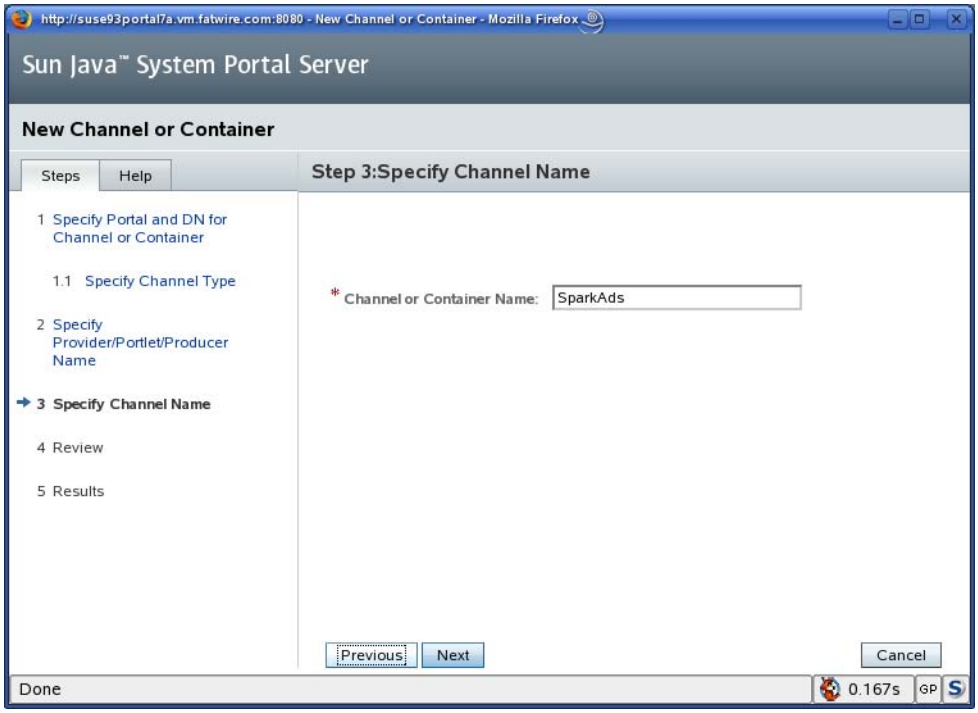
10. In the “Channel Type” drop-down list, select **JSP 168 Portlet Channel**.



11. Select the portlet you wish to add to the container (display page) and click **Next**.

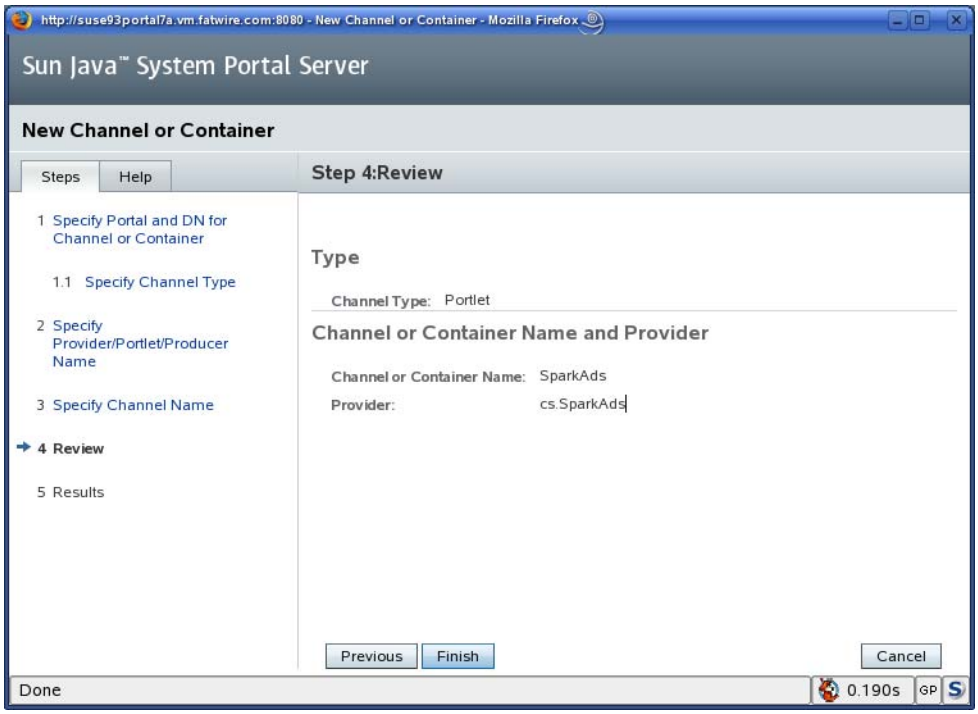


12. In the **Channel or Container Name** field, enter the name you wish the portlet to display when rendered on the page. For a list of portlet names, refer top the table below the figure. When you are finished, click **Next**.



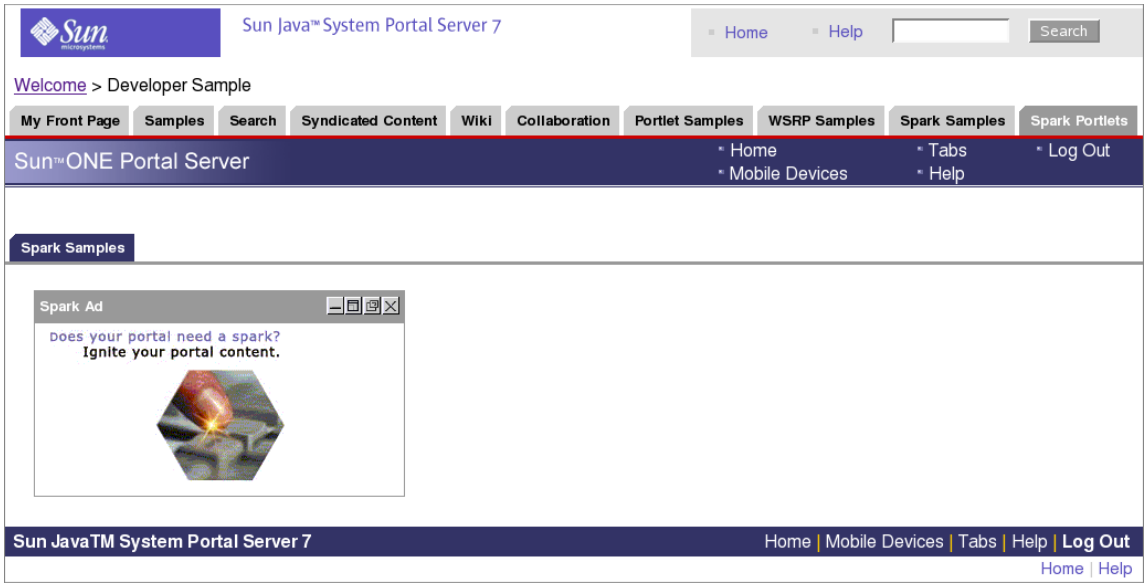
Default Portlet Names				Sample Portlet Names
Active Content	ClearCheckouts	Document Assignments	RolesAdmin	SparkAd
Active Documents	Content Assignments	Document History	Search Content	SparkDocuments
Checked Out Content	Content History	My Documents	Search Documents	SparkJobs
Checked Out Documents	ContentDefinition	Publish Console	Site Info	SparkNews
ClearAssignments	Create Content	PublishTarget		

13. In the "Review" screen, click **Finish**.

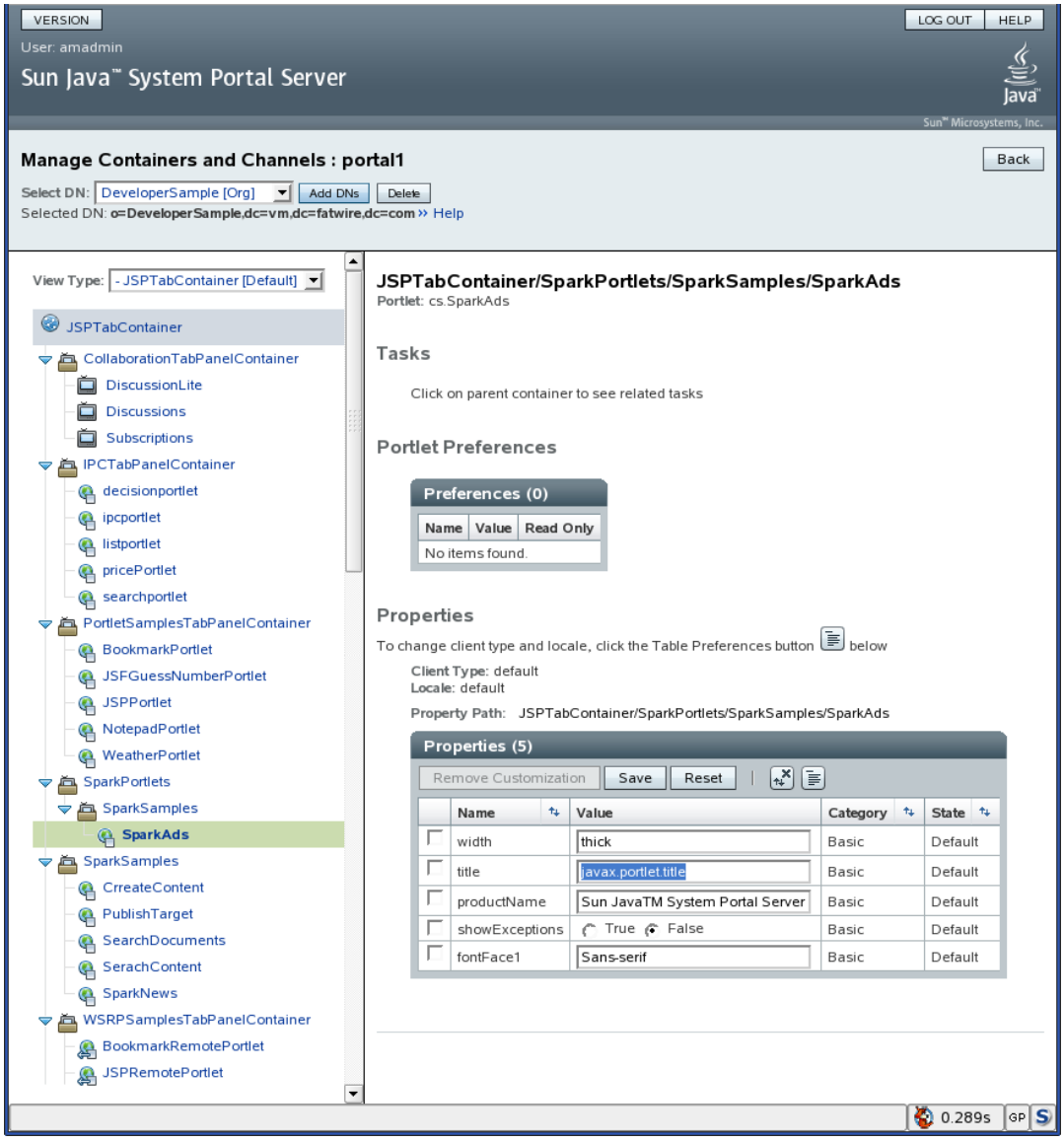


14. In the "Results" screen, click **Close**.

The new portlet channel appears in the left-hand pane, below the selected parent container; the portlet it represents appears in your portal, in the tab you created in step A.



15. In the left pane, select the portlet channel you created earlier in this step and enter a descriptive value for the **title** property. When you are finished, click **Save**.



16. Repeat steps 7 – 15 for each portlet you wish to add to a container. When you are finished, repeat this procedure for each container you have created in step B.

17. When you are finished, log out of the Portal Server Admin Console to save your changes.

Configuring Portal Tab Accessibility

This section shows you how to configure access to tabs on your portal, so that:

- When not logged in, Content Server users will only see the **Spark Samples** tab.
- When logged in, Content Server users will only see the **FatWire Content** and **FatWire Document** tabs. Users with administrative roles will also see the **Admin** tab.

Note

This procedure assumes that you have already created the desired tabs in your portal, as described in "Populating the Portal Interface," on page 78 (in other words, you have the **Spark Samples**, **FatWire Content**, **FatWire Document**, and **Admin** tabs in the **DeveloperSample** realm).

This procedure consists of the following steps:

A. Add New Roles to Sun Access Manager

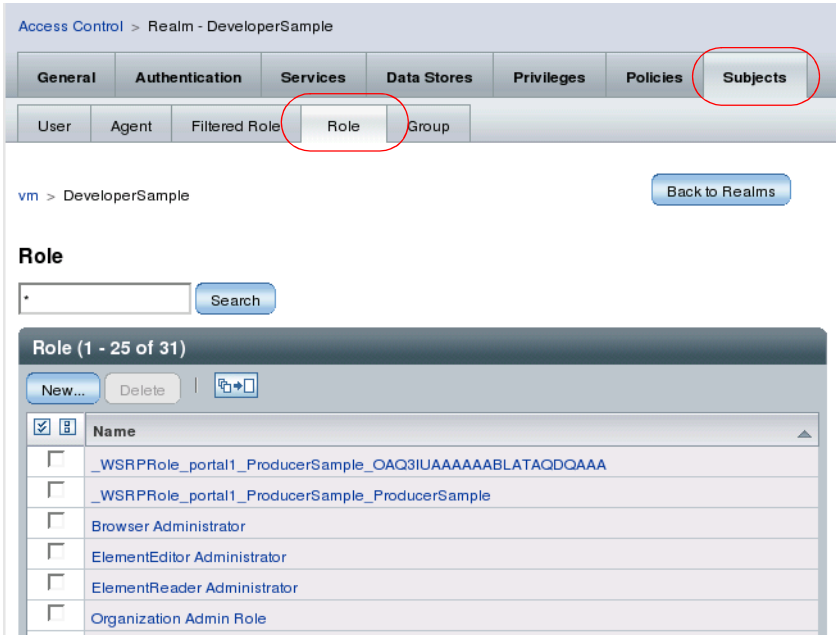
In this section, you will add two new roles, `FatWireSparkUser` and `FatWireSparkAdmin`, to Sun Access Manager under the DeveloperSample sample portal. These roles will be used to determine which users will see which tabs in the portal.

Note

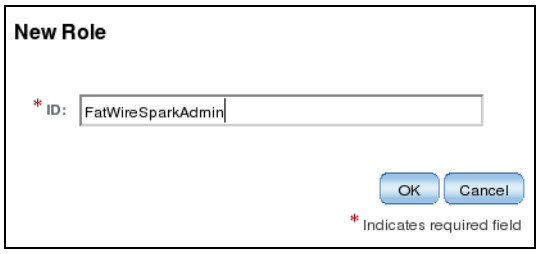
The steps that follow this section assume that the roles used to restrict tab accessibility are named `FatWireSparkUser` and `FatWireSparkAdmin`. If you decide to name the roles differently, you will have to substitute the appropriate names when prompted in the later sections.

1. Log in to the Sun Access Manager as the `amadmin` user.
2. Select the **DeveloperSample** realm.

3. Click the **Subjects** tab, then the **Role** sub-tab.



4. Click **New...**.
5. In the **New Role** field, enter `FatWireSparkAdmin`, then click **OK**.



6. Create the `FatWireSparkUser` role by repeating steps 4 and 5.
7. Continue to the next section, "B. Create the sparkuser Account."

B. Create the sparkuser Account

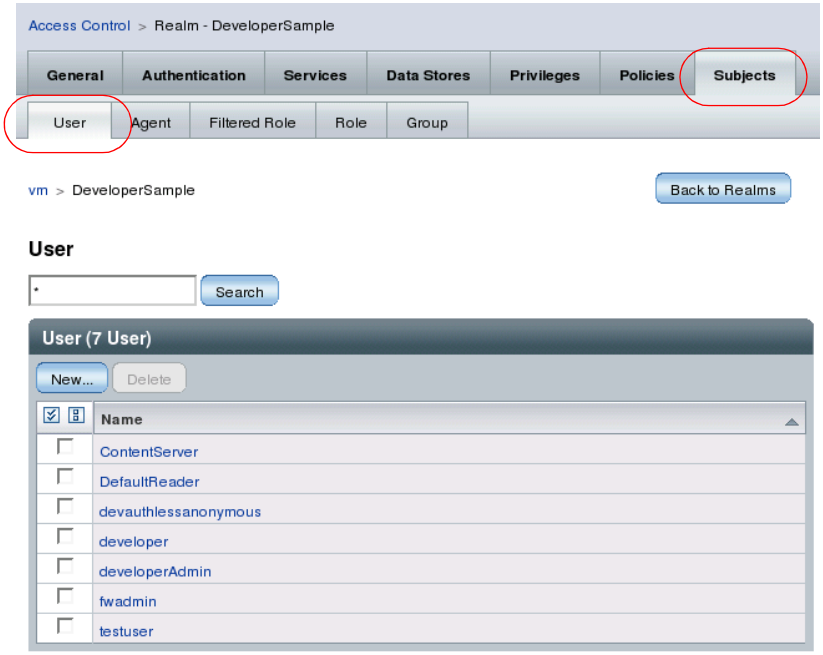
In this section, you will create a new user account, `sparkuser`, that will hold general (non-administrative) user privileges in the portal.

Note

If you have already created the `SparkContent` and `SparkDocument` users as part of your Content Server installation, you can choose to skip this section and use one of these existing accounts instead. In such case, substitute the alternate user name in place of the `sparkuser` user name in the sections that follow.

1. Complete the steps in the previous section, "A. Add New Roles to Sun Access Manager," if you have not already done so.

2. Click the **Subjects** tab, then the **Users** sub-tab.



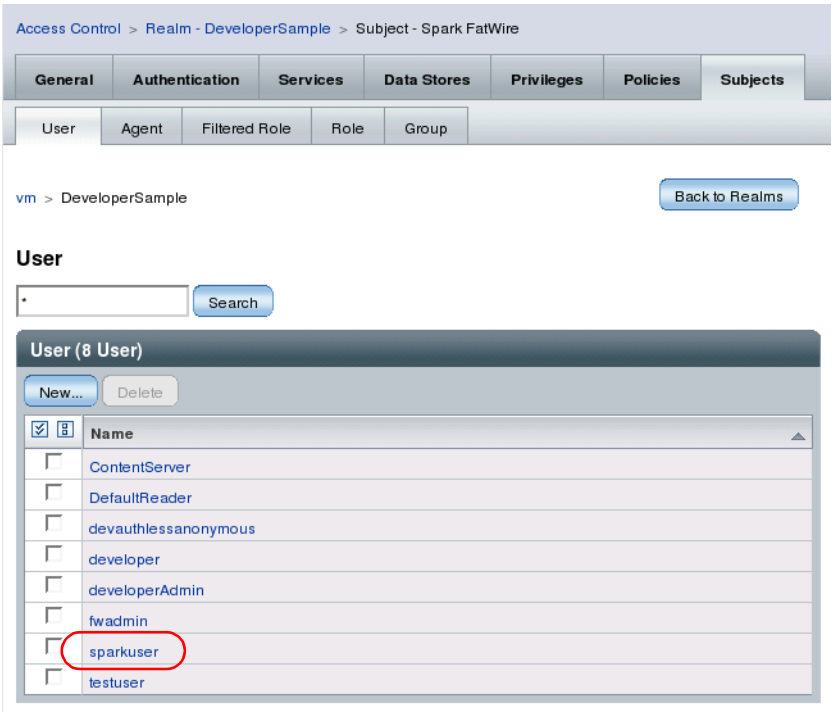
3. Click **New...**.
4. Fill out the form as follows, then click **OK**:
   - **ID:** `sparkuser`
   - **First Name:** `Spark`
   - **Last Name:** `FatWire`
   - **Full Name:** `sparkuser`
   - **Password:** `password`
   - **Password (confirm):** `password`
   - **User Status:** `Active` (this **must** be set to active for the portal to work)
5. Continue to the next section, "Assign the New Roles to the fwadmin and sparkuser Users."

C. Assign the New Roles to the fwadmin and sparkuser Users

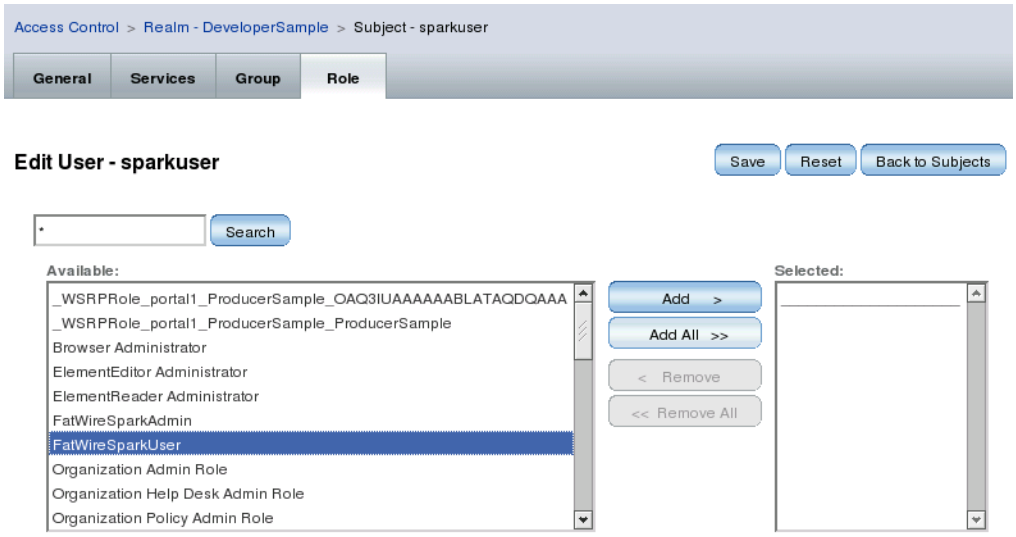
In this section you will assign the `FatWireSparkAdmin` and `FatWireSparkUser` roles you created earlier to the `fwadmin` and `sparkuser` users, respectively. (If you have additional users accessing the portal, assign the appropriate role(s) to their user names as well.)

1. Complete the steps in the previous section, "B. Create the sparkuser Account," on page 100, if you have not already done so.

2. Assign the appropriate roles to the newly created `sparkuser` account:
   a. In the list of users, click the newly created `sparkuser` account.

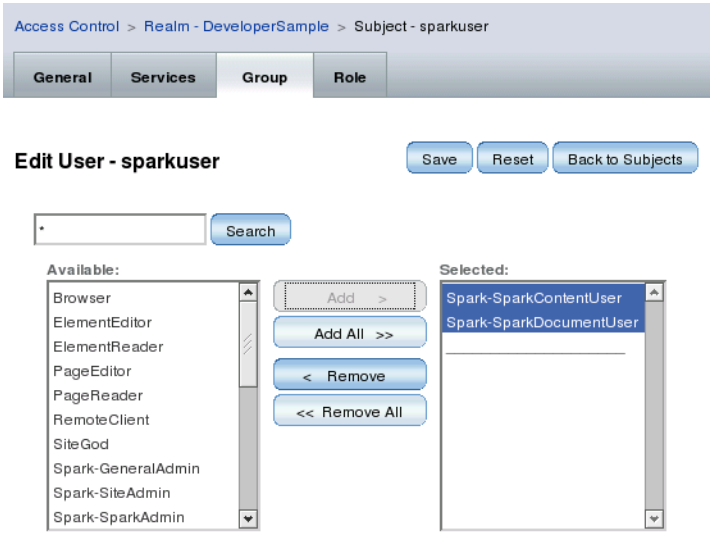


   b. Click the **Role** tab.
   c. In the "Available" list, select the `FatWireSparkUser` role and click **Add**.



3. Click **Save**. A confirmation message appears.

4. Assign the appropriate groups to the newly created `sparkuser` account:
   a. Click the **Group** tab.
   b. In the "Available" list, select the following groups:
      - **Spark-SparkContentUser**
      - **Spark-SparkDocumentUser**
      - **PageReader**
      - **ElementReader**
      - **Visitor**
      - **Browser**
      - **UserReader**
      - **xceleditor**
      - **Spark-GeneralAdmin**



   c. Click **Save**. A confirmation message appears.
5. Click **Back to Subjects**.
6. Assign the appropriate roles to the `fwadmin` user:
   a. In the list of users, click `fwadmin`.
   b. Click the **Role** tab.
   c. In the "Available" list, select the `FatWireSparkAdmin` role and click **Add**.
   d. Click **Save**.
7. Click **Back to Subjects**.

D. Test the Tab Access Rights

In this section you will verify that tab access rights have been configured properly.

1. Log in to the portal interface as the `sparkuser` user via the following URL:

   `http://<hostname>:<port>/<portal_URI>/dt`

2. Click the **Admin** tab.

   When you attempt to access the **Admin** tab, the portlets in that tab should show an error message indicating that administrative privileges are required to access them. The message indicates that the `sparkuser` user does not have administrative privileges, which is the desired behavior.

   If you do not see the error message, or if you see the message, "Please log in first," check the permissions granted to the `sparkuser` user and confirm that they match those listed in "Assign the New Roles to the fwadmin and sparkuser Users," on page 101.

3. Log out and log back in, this time as the `fwadmin` user. You should be able to access all portlets in all tabs. If you cannot access some of the portlets, check the permissions granted to the `fwadmin` user.

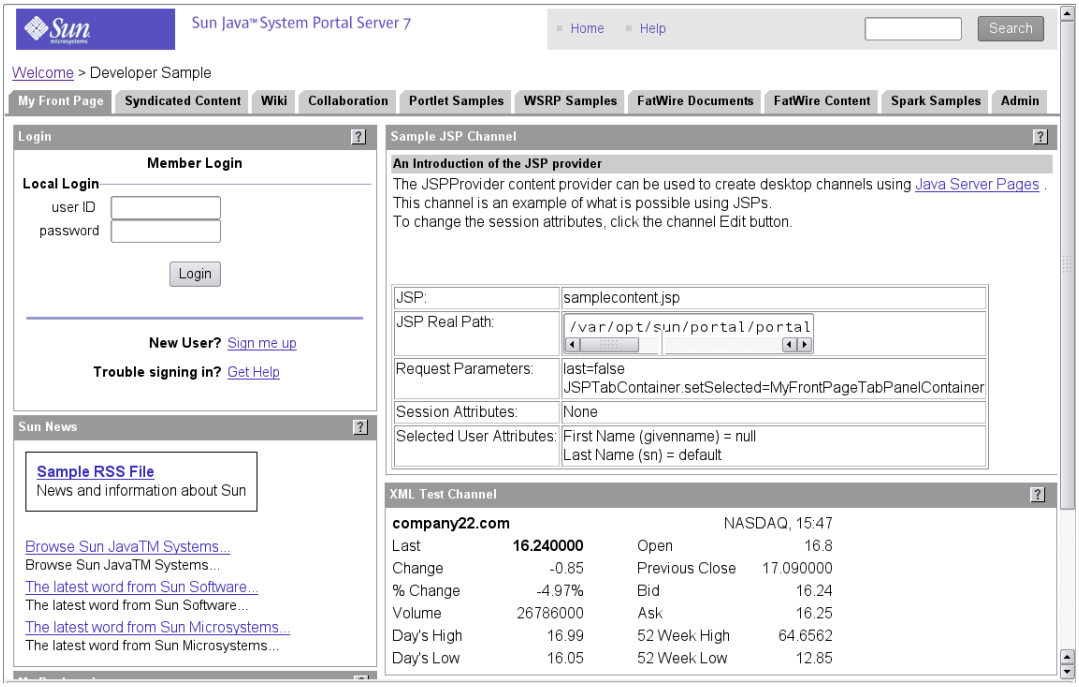
E. Clean Up the DeveloperSample Portal Desktop

In this section you will remove most of the default tabs from the portal interface, leaving only the login portlet, and any portlets that have been configured as part of the Content Server installation. Doing so will significantly reduce the clutter on the portal desktop.

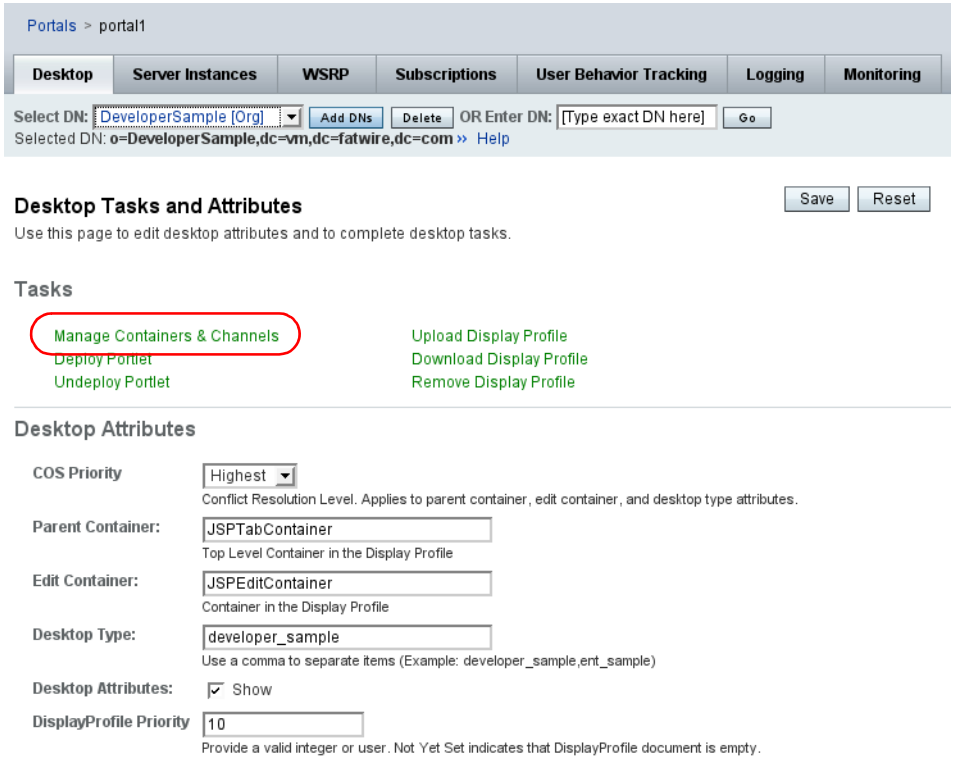
1. Access the portal interface via the following URL:

   `http://<hostname>:<port>/<portal_URI>/dt`

   The interface will look similar to the following:

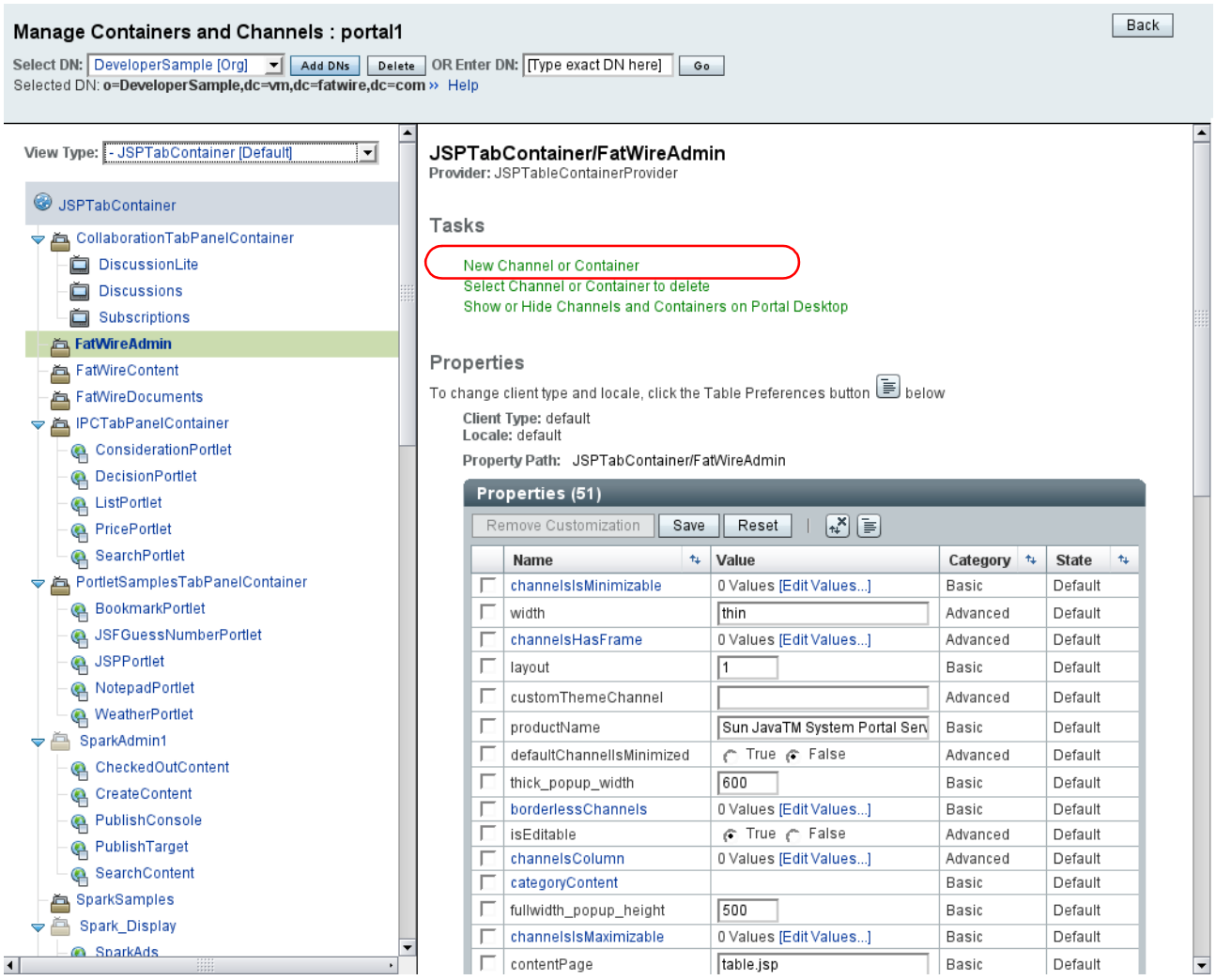


2. Log in to the Portal Server console as the `amadmin` user via the following URL:
   `http://<hostname>:<port>/psconsole`
3. Click the **Portals** tab.
4. Select the Portal Server instance on which you installed Content Server (the default instance is **portal1**).
5. Select **DeveloperSample [Org]** from the drop-down list.
6. Click **Manage Containers & Channels**.

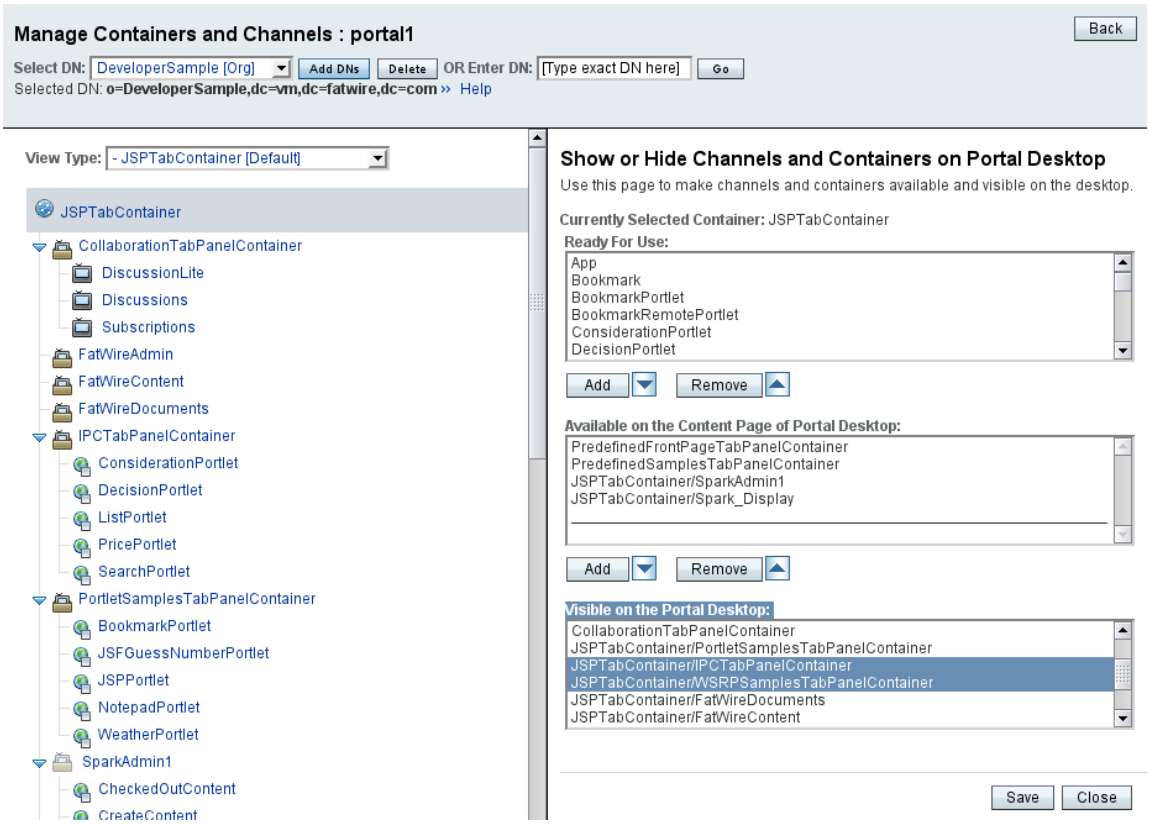


7. In “View Type” drop-down list in the upper left, select - **JSPTabContainer [Default]**

8. Click **Show or Hide Channels and Containers on Portal Desktop**.



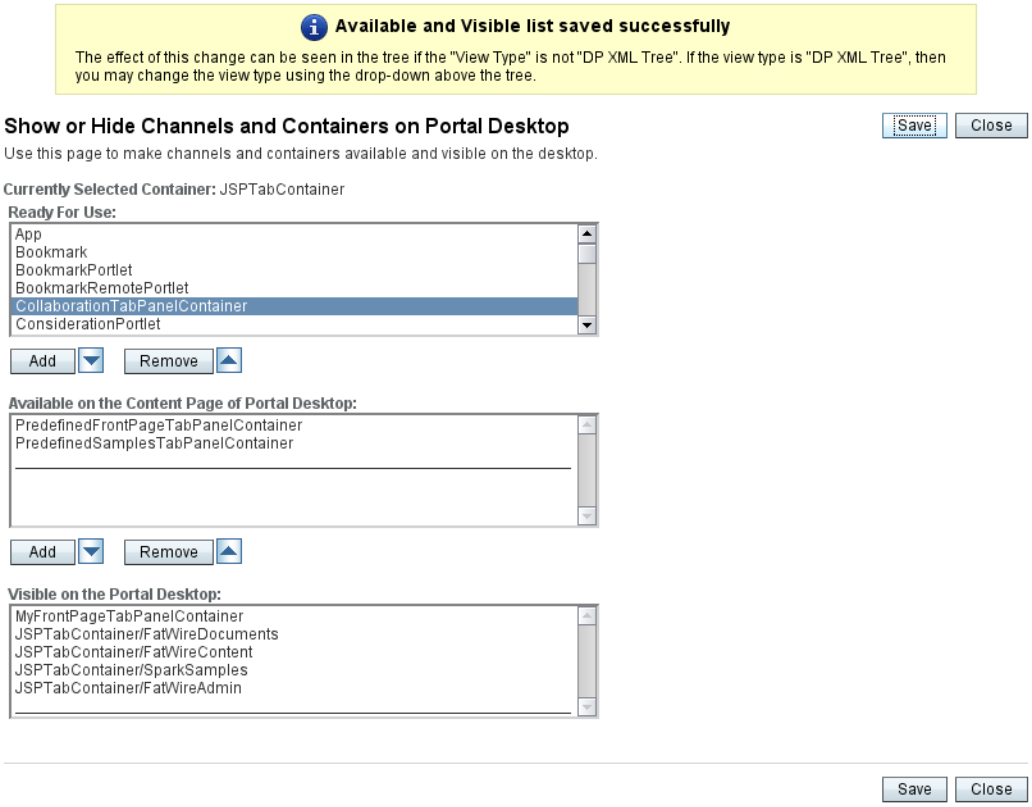
9. In the **Visible on the Portal Desktop** field, do the following:
   a. Select the following entries:
      - **JSPTabContainer/IPCTabPanelContainer**
      - **JSPTabContainer/WSRPSamplesTabPanelContainer**
      - **WikiTabPanelContainer**
      - **CollaborationTabPanelConatiner**
      - **SyndicatedContentTabPanelContainer**
      - **JSPTabContainer/PortletSamplesTabPanelConatiner**
      - **JSPTabContainer/SamplesTabConatiner**
      - **JSPTabContainer/SearchTabConatiner**
   b. Click **Remove**.



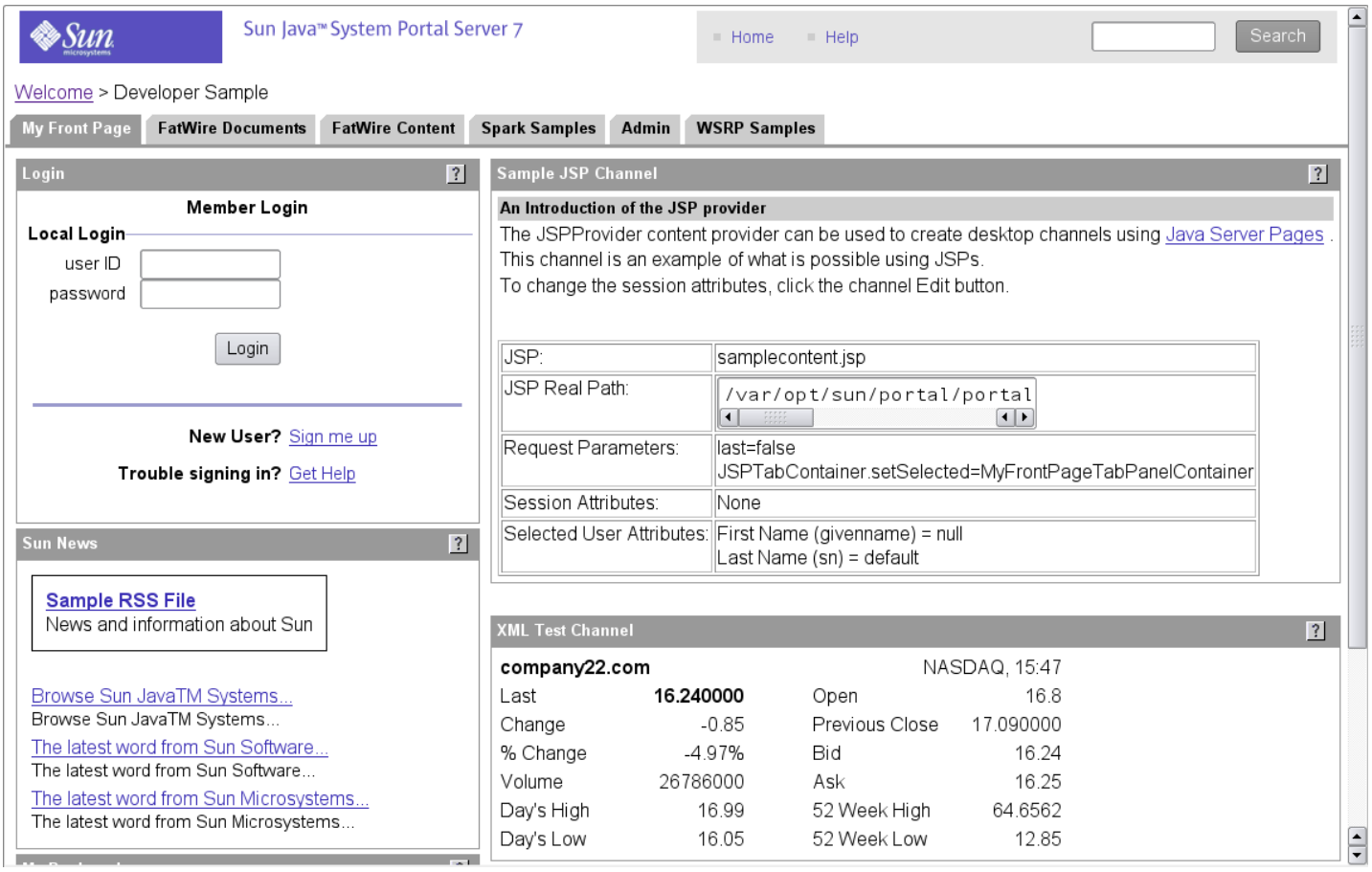
10. In the **Available on the Content Page of Portal Desktop** field, select the entries listed in step 9 and click **Remove**.

A confirmation message appears. The **Visible on the Portal Desktop** field should now contain only the following entries:

- **MyFrontPageTabPanelContainer**
- **JSPTabContainer/FatWireDocuments**
- **JSPTabContainer/FatWireContent**
- **JSPTabContainer/FatWireSamples**
- **JSPTabContainer/FatWireAdmin**



The portal interface should now looks as follows:



11. Click **Close** and continue to the next section, "F. Add the New Roles to the Portal Interface," on page 110.

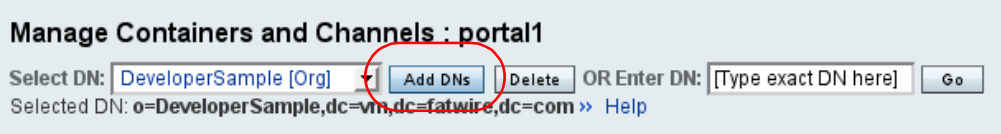
F. Add the New Roles to the Portal Interface

At this point you should have two users, `fwadmin` and `sparkuser`, each holding an appropriate role (`FatWireSparkAdmin` and `FatWireSparkUser`, respectively). In this section, you will add the roles held by these users to the portal. The roles will determine which users see which tabs and portlets in the portal interface. You add the roles by configuring the corresponding portal realms.

Note

If you have named the roles you have assigned to the `fwadmin` and `sparkuser` users differently from our example, substitute the correct names when performing the steps in this section.

1. Complete the steps in the previous section, "E. Clean Up the DeveloperSample Portal Desktop," on page 104, if you have not already done so.
2. Click **Add DNs** in the upper left of the Portal Server console.



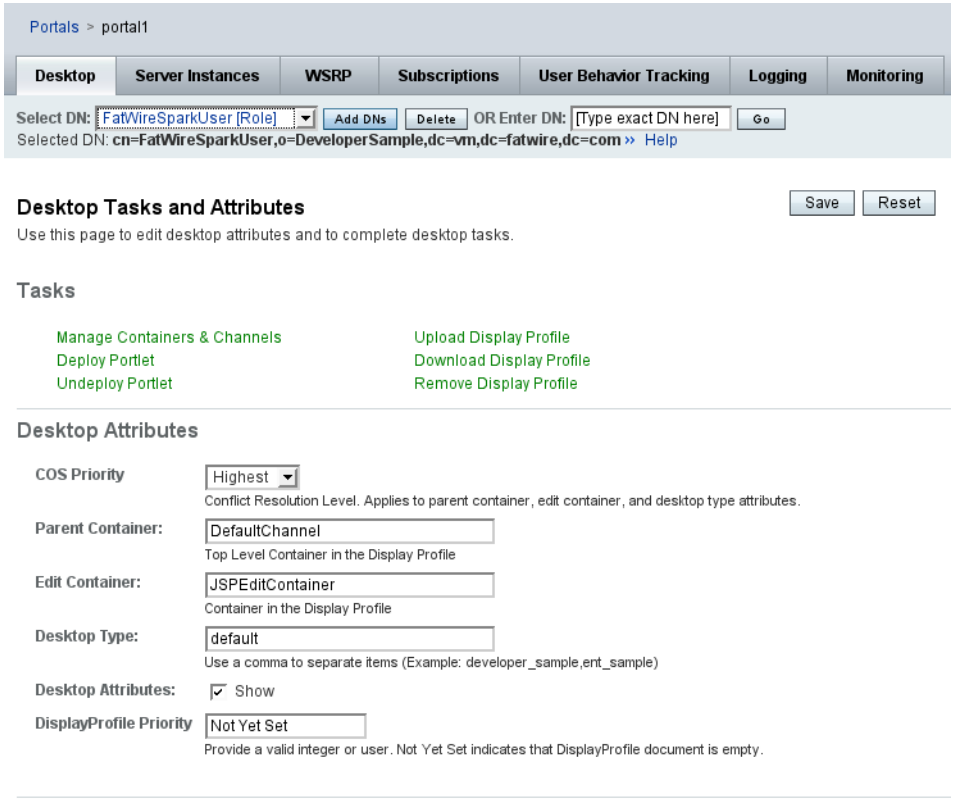
3. In the pop-up window that appears, do the following:
   a. In the "Search for:" drop-down list, select **Role**.
   b. In the field next to the list, enter `FatWireSparkUser`.
   c. Click **Search**.

   d. In the "Found" list, select the check box next to the `FatWireSparkUser` user name and click **Add**.
4. Repeat steps 2 and 3 for the `FatWireSparkAdmin` user.

5. Click **Back** in the upper right of the Portal Server console.

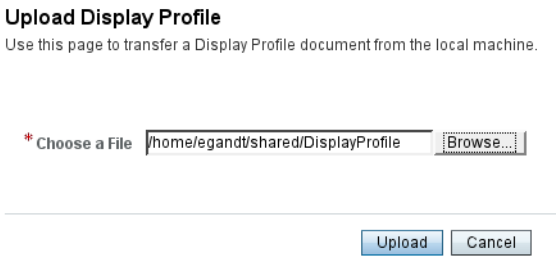
   The new realms corresponding to the `FatWireSparkUser` and `FatWireSparkAdmin` roles appear in the "Select DN:" drop-down list at the upper left of the Portal Server console now. At this point, any user assigned one of these roles will not be able to log in to the portal until you complete the remaining steps in this section.
6. In the "Select DN:" drop-down list, select **DeveloperSample [Org]**.
7. Click **Download Display Profile**.

   A "Save" dialog box appears, prompting you to save the display profile for the selected realm as a file on your local machine.
8. In the "Save" dialog box, enter the file name, `DisplaySample`, and click **Save**.
9. Click **Back** in the upper right of the Portal Server console.
10. In the "Select DN:" drop-down list, select **FatWireSparkUser [Org]**.
11. Click **Upload Display Profile**.



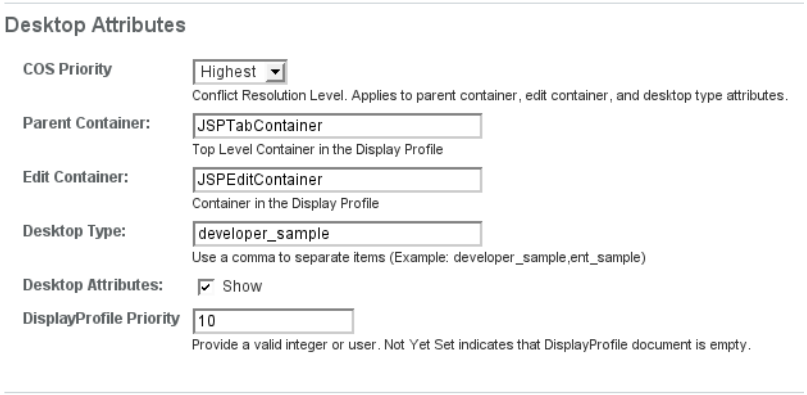
The "Upload Display Profile" pop-up window appears, prompting you to upload a file containing a portal realm display profile.

12. In the pop-up window, click **Browse** and select the `DisplayProfile` file you saved in step 8. When you have selected the file, click **Upload**.

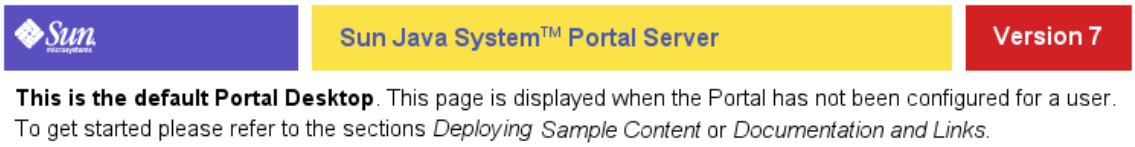


When the upload succeeds, a confirmation message appears.

13. Click **Cancel** to close the pop-up window and return to the Portal Server console.
14. Make sure that the **FatWireSparkUser [Org]** DN is still selected, then modify the values of the following properties:
    a. **Parent Container:** change from `DefaultChannel` to `JSPTabContainer`
    b. **Desktop Type:** change from `default` to `DeveloperSample`



15. Click **Save**. A confirmation message appears.
16. In the "Select DN:" drop-down list, select **DeveloperSample [Org]**.
17. Repeat steps 10–15 for the `FatWireSparkAdmin` role.
18. Test your configuration by logging in as the `sparkuser` and `fwadmin` users. If you receive the following error, review and repeat the steps for that role in this section.



19. Continue to the next section, "G. Disable "Admin" Tab Access for Non-Administrative Users," on page 113.

G. Disable “Admin” Tab Access for Non-Administrative Users

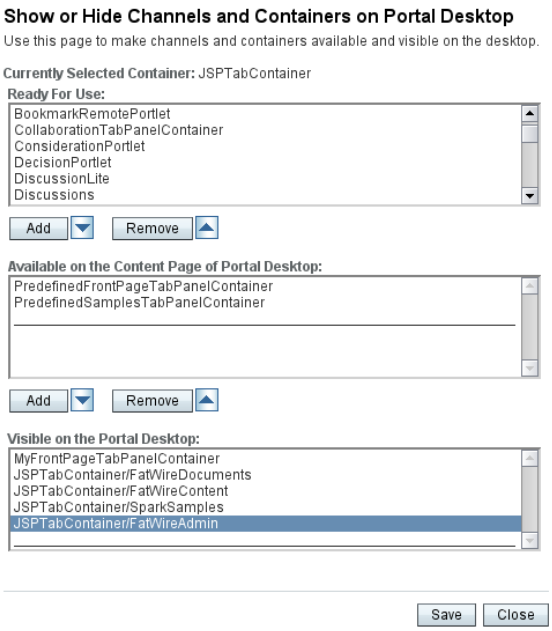
In this section you will disable access to the **Admin** tab for users who do not hold administrative roles. In our example, users holding the `FatWireSparkUser` role will not be permitted to access the **Admin** tab when they log in to the portal interface.

Note

You can reuse this procedure to enable or disable access to any tab within your portal.

1. Complete the steps in the previous section, “F. Add the New Roles to the Portal Interface,” on page 110, if you have not already done so.
2. In the “Select DN:” drop-down list, select **FatWireSparkUser [Org]**.
3. Click **Manage Containers and Channels**.
4. In the “View type:” drop-down list in the upper left of the Portal Server console, select **- JSPTabContainer [Default]**

5. In the tree on the left, click the **JSPTabContainer** header (a gray box).
6. In the main pane, click **Show or Hide Channels and Containers on Portal Desktop**.
7. Remove the **Admin** tab from view for the selected role:
   a. In the **Visible on the Portal Desktop** field, select **JSPTabContainer/FatWireAdmin** and click **Remove**.
   b. In the **Available on the Content Page of Portal Desktop** field, select **JSPTabContainer/FatWireAdmin** and click **Remove**.



8. Click **Save**.
9. Test your changes. Log in to the portal interface as the `sparkuser` user and make sure that the **Admin** tab is not visible.

   If the tab is still visible, review the changes you have made and retry this procedure.
10. Proceed to the next section, "H. Disable Access to Remaining FatWire Tabs for Guest Visitors."

H. Disable Access to Remaining FatWire Tabs for Guest Visitors

In this section you will disable access to the **FatWire Content**, **FatWire Documents**, and **Admin** tabs for guest visitors – users that have not logged in to the portal.

1. Complete the steps in "G. Disable "Admin" Tab Access for Non-Administrative Users," on page 113," if you have not already done so.
2. Click **Manage Containers and Channels**.
3. In the "View type:" drop-down list in the upper left of the Portal Server console, select **- JSPTabContainer [Default]**

4. In the tree on the left, click the **JSPTabContainer** header (a gray box).
5. In the main pane, click **Show or Hide Channels and Containers on Portal Desktop**.
6. Remove the **Admin** tab from view for the selected role:
   a. In the **Visible on the Portal Desktop** field, select the following entries:
      - **JSPTabContainer/FatWireDocuments**
      - **JSPTabContainer/FatWireContent**
      - **JSPTabContainer/FatWireAdmin**

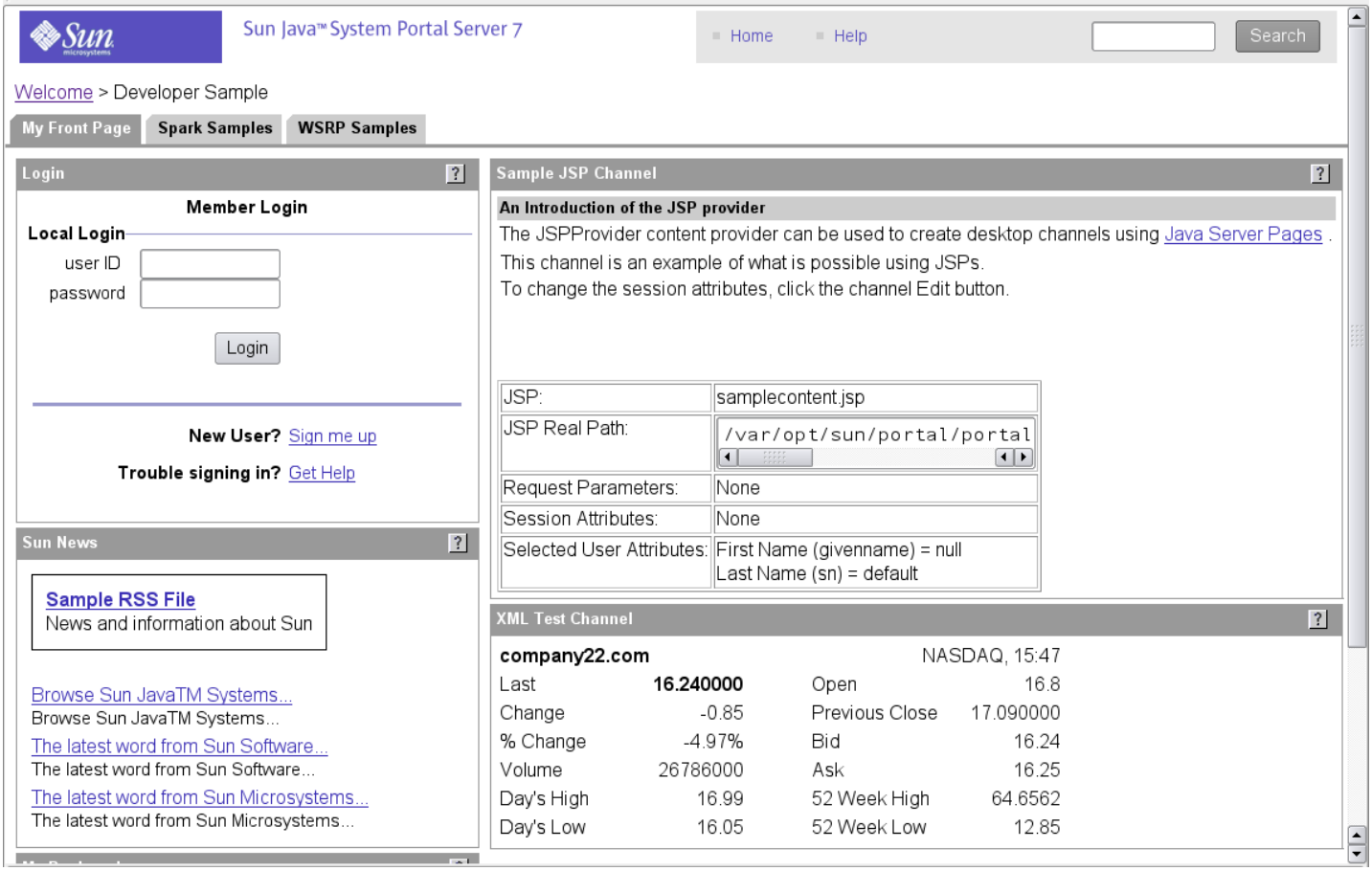
   b. Click **Remove**.
   c. In the **Available on the Content Page of Portal Desktop** field, remove the fields listed in step a and click **Remove**.

   The **Visible on the Portal Desktop** field should now contain only the following entries:
   - **MyFrontPageTabPanelContainer**
   - **JSPTabContainer/FatWireSamples**
7. Click **Save**.

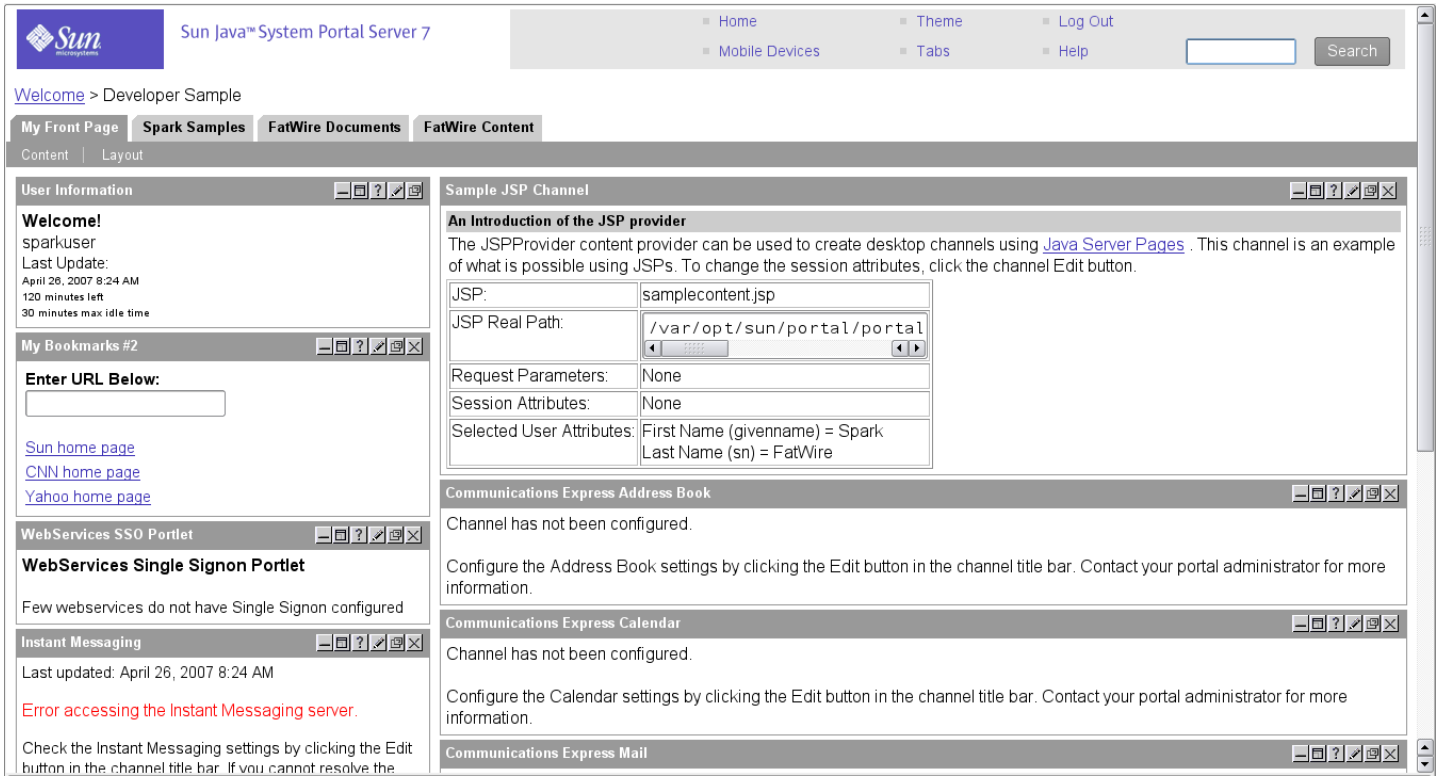
I. Test Your Configuration

After following the steps in this section, your portal interface should now look as follows:

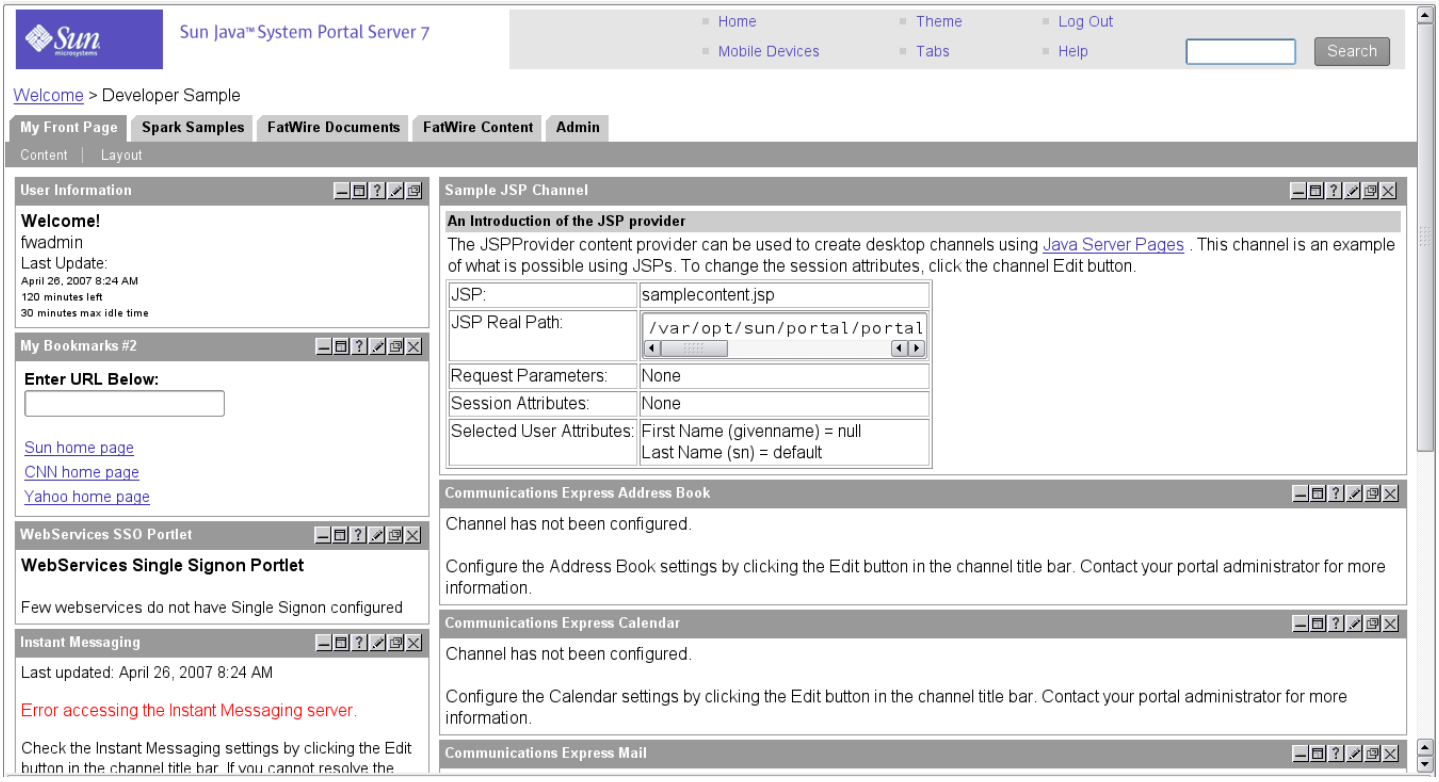
- When a user accesses the portal interface but does not log in:



- When a user holding the `FatWireSparkUser` role logs in to the portal interface:



- When a user holding the `FatWireSparkAdmin` role logs in to the portal interface:



Note

Click the **Admin** tab to test whether access to this tab has been configured properly. If you cannot access the **Admin** tab, review the steps in this section and check your configuration for possible errors.

Part 4

Content Server

This part shows you how to proceed through the installation of Content Server. It contains the following chapters:

- Chapter 11, “Installing and Configuring Content Server”

Chapter 11

Installing and Configuring Content Server

Content Server can be installed on any instance, but certain requirements must be met prior to the installation. This chapter covers the pre-installation requirements and provides instructions for installing Content Server as a web application and a portal.

This chapter contains the following sections:

Pre-Installation Steps

In this section you will turn off transactions. Transactions must be disabled in order for the installer to successfully complete its process. You will re-enable transactions after the installation is complete.

To disable transactions

1. Stop the application server:

   `/opt/<jes_home>/appserver/bin/asadmin stop-domain <domain_name>`

2. Modify `domain.xml` as follows:

   a. Open `/opt/<jes_home>/appserver/domains/<domain_name>/config/domain.xml` in a text editor.

   b. Search for `java-config` and add the following line:

   ```
   <jvm-options>-DrunTransCode=false</jvm-options>
   ```

   c. Save and exit the file.

3. Start the application server:

   `/opt/<jes_home>/appserver/bin/asadmin start-domain <domain_name>`

Installing Content Server

After completing Steps I – IV.1 in the "Installation Quick Reference," on page 9, you install Content Server using the provided installer. The installation process consists of two stages.

In the first stage, the installer gathers necessary configuration information, installs the file structure, and deploys the CS application. At the end of the first stage, the installer displays an "Installation Actions" window describing the steps you must perform before proceeding to the second stage of the installation. The first of those steps will be to deploy the CS application (for instructions, see Chapter 6, "Deploying Applications").

If you are using an Oracle database and require text attributes greater than 2000 characters, you must set the `cc.bigtext` property to `CLOB` after the CS application is deployed. (For instructions, see step 5 in the next section.)

If the first stage fails, the installer allows you to go back and modify your configuration options (except the database type), and retry the installation.

Note

If you need to change the type of database you have specified during the installation, you must delete the installed CS file structure and restart the installation.

In the second stage, the installer populates the database with the tables and data required for Content Server to function. If the second stage fails, the file structure and database tables must be deleted and the installation restarted from the beginning.

Running the Installer

To install Content Server

1. Make sure you have completed Steps I – IV.1 in the "Installation Quick Reference," on page 9.
2. Extract the Content Server installer archive into a temporary directory.
3. Change to the temporary directory containing the installer files.
4. Execute the installer script:
   - On Windows: **`csInstall.bat`**
   - On Unix: **`csInstall.sh`**

   The installer provides online help at each screen. Read the online help for detailed explanations of the options that are presented in each screen. If you encounter problems during the installation process, consult the online help for possible causes and solutions.
5. If you are using an Oracle database and require text attributes greater than 2000 characters, you must set the `cc.bigtext` property to `CLOB`. When the installer displays the "Installation Actions" pop-up window, complete step 1 displayed in the window, then do the following:
   a. Open the Property Editor by clicking the **Property Editor** button.
   b. In the Property Editor, open the `futuretense.ini` file.
   c. Click the **Database** tab.
   d. Locate the `cc.bigtext` property and set its value to `CLOB`.
   e. Save your changes and close the Property Editor.
   f. Continue to step 3 displayed in the "Installation Actions" window.
6. When the installation completes successfully, perform the post-installation steps in the next section as required for your installation.

Post-Installation Steps

When the installation process completes successfully, perform the following steps:

A. Turning on Transactions

B. Setting File Permissions (Unix Only)

C. Verifying the Installation

D. Configuring the Portal Installation (Portal Installations only)

E. Integrating with LDAP (Required for Portal Installations)

F. Setting Up a Content Server Cluster (Optional)

G. Setting Up Content Server for Its Business Purpose

A. Turning on Transactions

1. Stop the application server:

   `/opt/<jes_home>/appserver/bin/asadmin stop-domain <domain_name>`

2. Modify `domain.xml` as follows:
   a. Open `/opt/<jes_home>/appserver/domains/<domain_name>/config/domain.xml` in a text editor.
   b. Search for `java-config` and change the following line:

      from:

      ```
      <jvm-options>-DrunTransCode=false</jvm-options>
      ```

      to:

      ```
      <jvm-options>-DrunTransCode=true</jvm-options>
      ```
3. Save and exit the file.

B. Setting File Permissions (Unix Only)

If you installed Content Server on Unix, you must grant the "executable" permission to all files in the `<cs_install_dir>/bin` directory. To do so, perform the following steps:

1. Change to the `<cs_install_dir>/bin` directory.
2. Run the following command: **`chmod +x *`**
3. Restart the CS application.

C. Verifying the Installation

In this section, you will log in to your installation in order to verify that it functions. This section covers the following types of installations:

- Web Installations
- Portal Installations

Web Installations

If you installed Content Server as a web application, log in as the administrator to verify your installation.

Logging in to the Advanced Interface

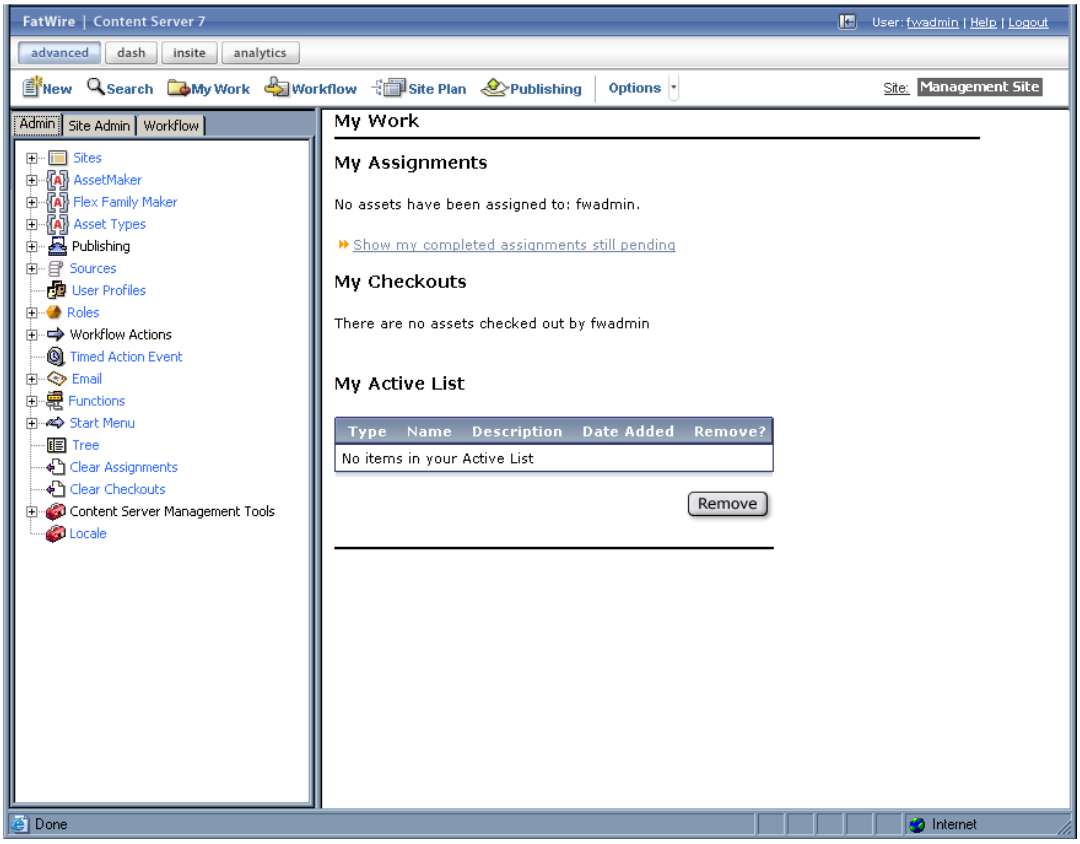
1. Point your browser to the following URL:

   `http://<hostname>:<port>/<context>/Xcelerate/LoginPage.html`

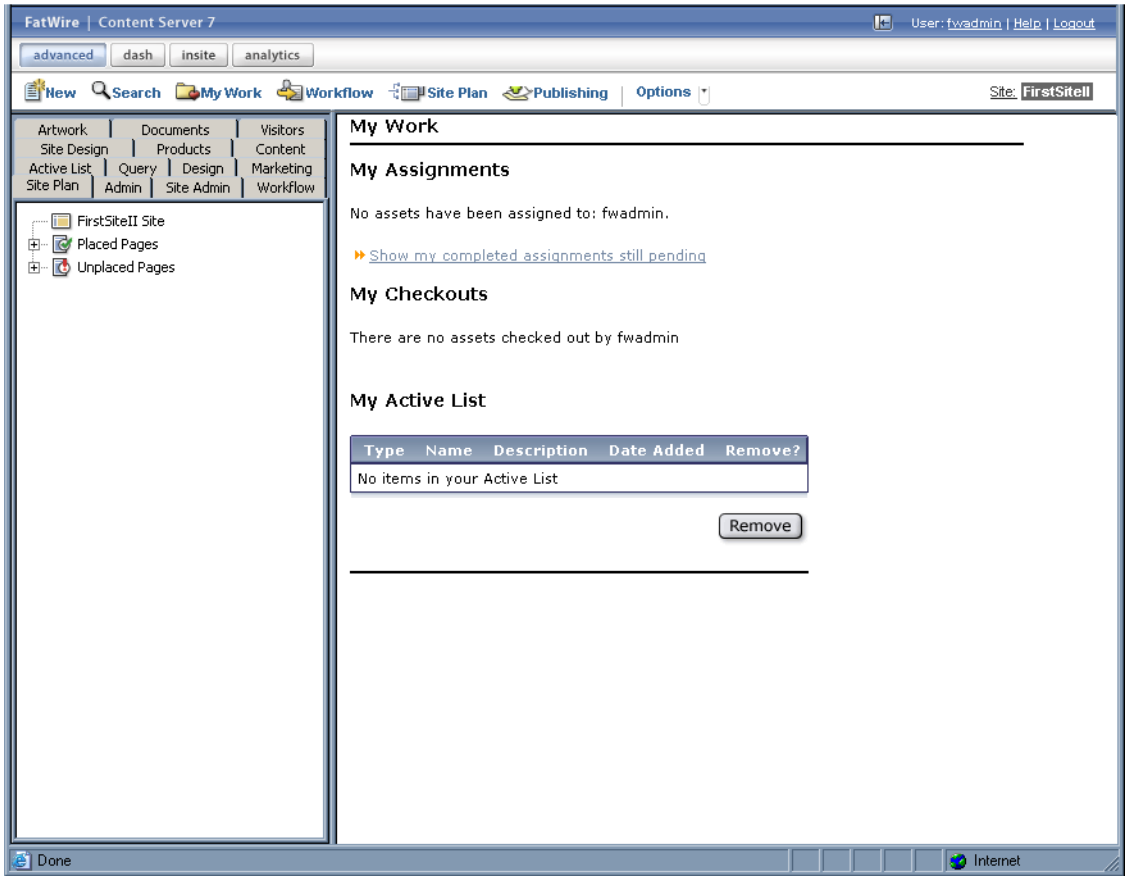
   Content Server displays the Advanced interface login page.

2. Enter the following credentials:
   - User name: **fwadmin**
   - Password: **xceladmin**
3. Click **Login**.

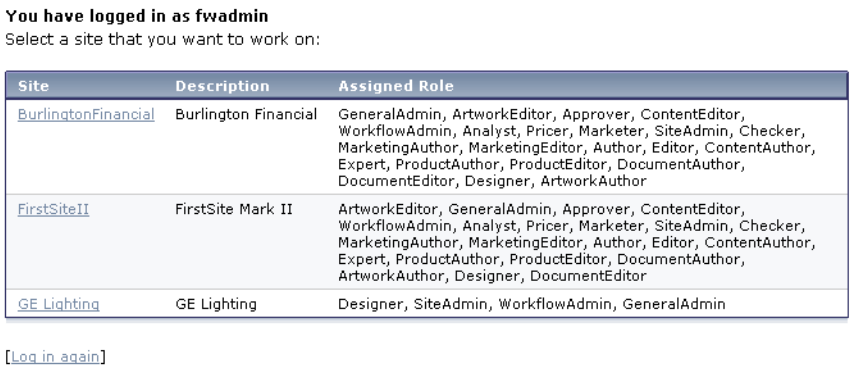
   Depending on whether you installed sample sites, one of the following happens:
   - If you did not install any sample sites, you are logged in to the built in Content Server management site. Only system administration functionality is available.



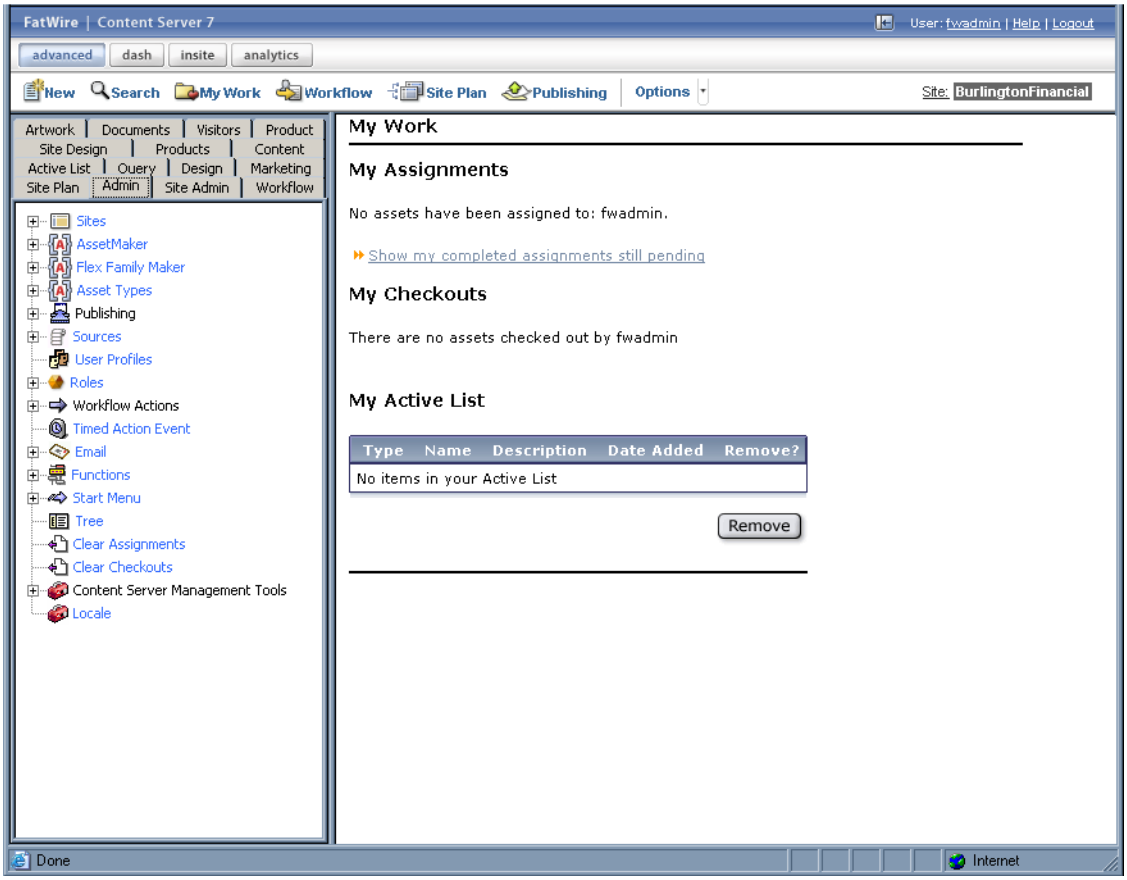
- If you installed one sample site, you are logged in to that site.



- If you installed more than one sample site, Content Server displays the "Select Site" screen. In such case, select the sample site you wish to log in to.



When you select a site, you are logged in to that site.



Logging in to the Dashboard Interface

1. Point your browser to the following URL:

   `http://<hostname>:<port>/<context>`

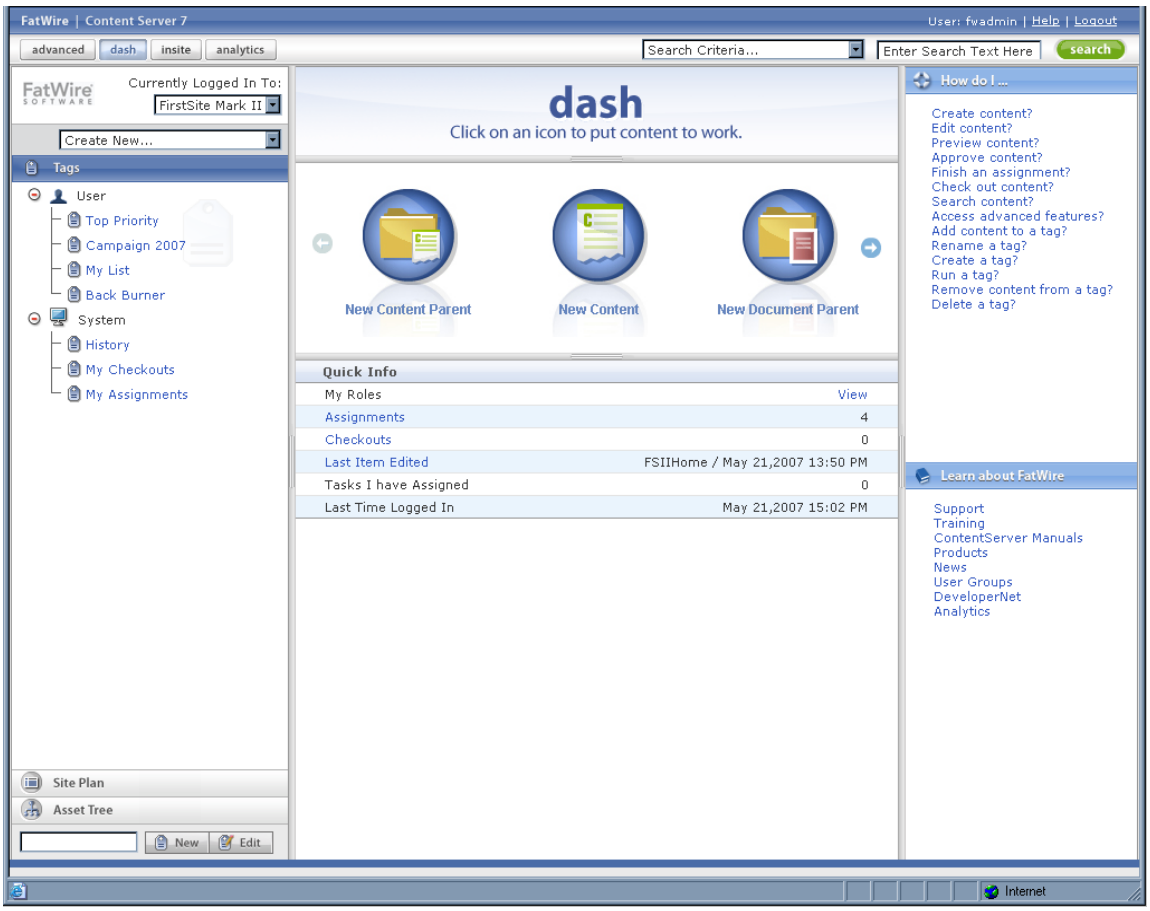
   Content Server displays the Dashboard interface login page.

2. Enter the following credentials:
   - User name: **fwadmin**
   - Password: **xceladmin**

3. Click **Login**.

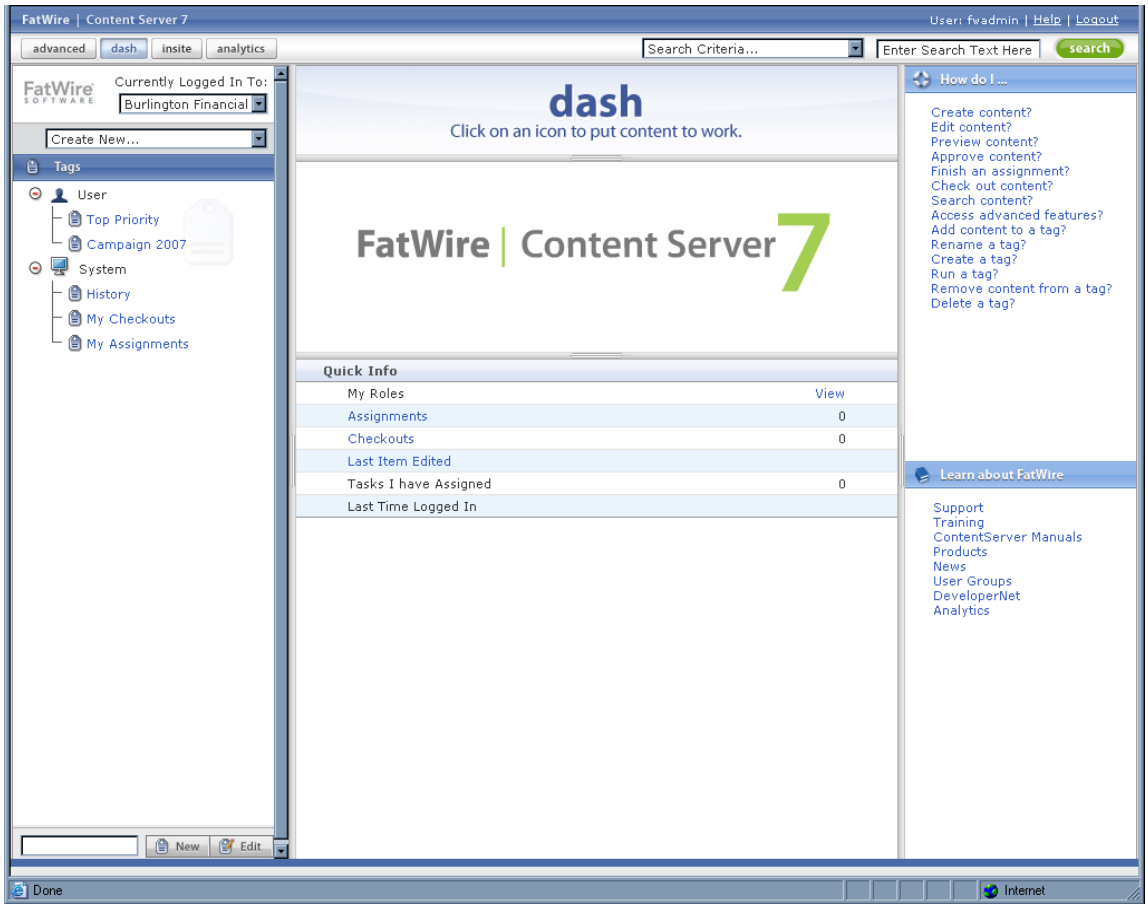
   Depending on whether you installed sample sites, one of the following happens:

   - If you did not install any sample sites, Content Server displays a message notifying you of that fact. You will not be able to log in to the Dashboard interface until at least one site exists on your system.
   - If you installed one sample site, you are logged in to that site.



   - If you installed more than one sample site, Content Server displays the “Select Site” screen. In such case, select the sample site you wish to log in to.

When you select a site, you are logged in to that site.



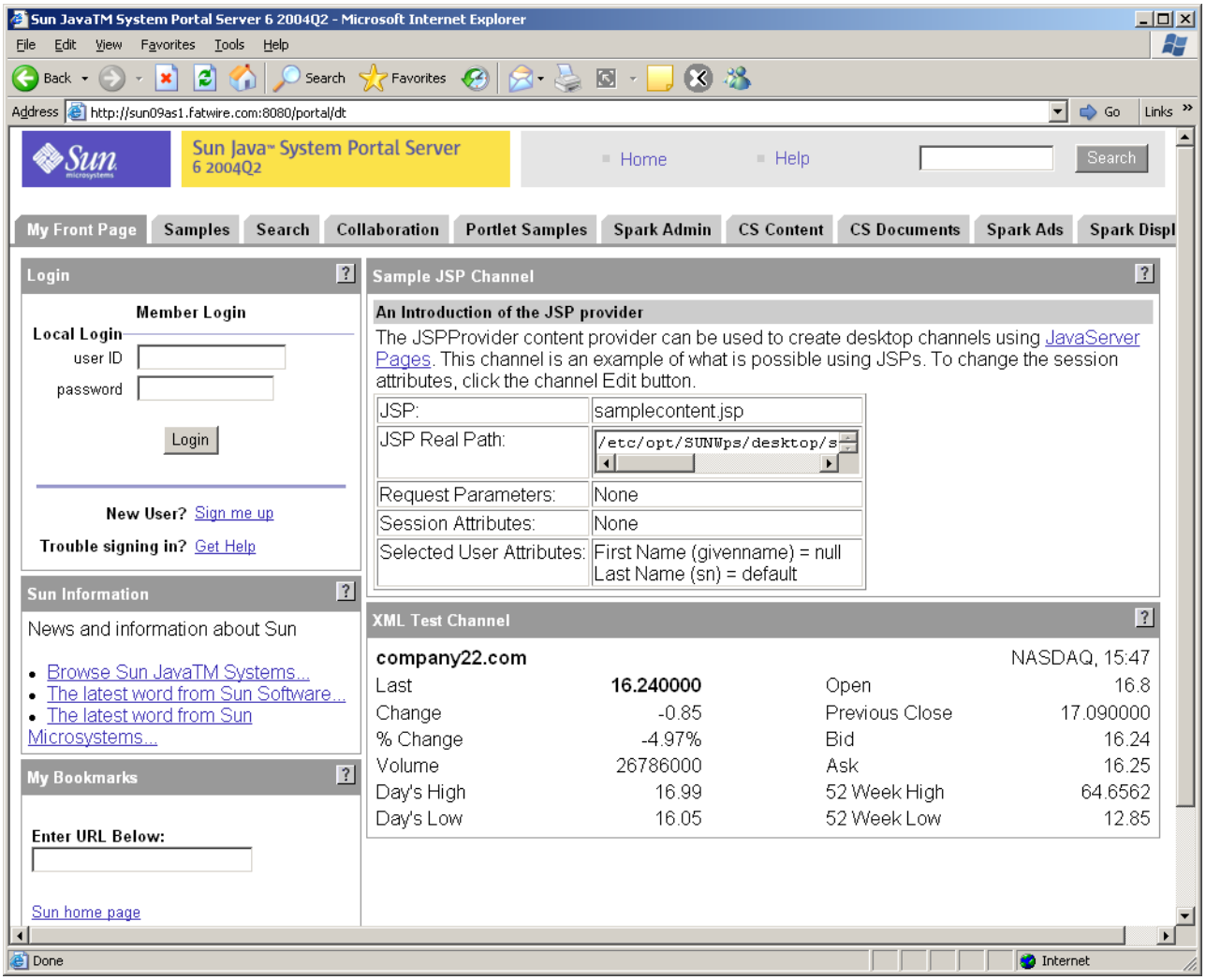
Content Server is now ready for configuration. Follow the steps in the rest of this chapter, starting with “E. Integrating with LDAP (Required for Portal Installations),” on page 131.

Portal Installations

If you installed a Content Server portal, log in to the portal interface by doing the following:

1. Point your web browser to the following URL:
   `http://<hostname>:<port>/<URI>/portal/dt`
2. Log in with the following credentials:
   - User name: **fwadmin**
   - Password: **xceladmin**

   The “Sun Java System Portal Server” page is displayed and the Content Server portal is now ready for configuration. Follow the steps in the rest of this chapter.



D. Configuring the Portal Installation (Portal Installations only)

If you installed Content Server as a portal, configure your portal installation now. For instructions, see Chapter 10, "Configuring a Portal Installation."

E. Integrating with LDAP (Required for Portal Installations)

LDAP integration is mandatory for portal installations, and optional for web installations. If you need to perform LDAP integration, you must do the following:

1. Set up a supported LDAP server of your choice. For instructions, see *Configuring Third-Party Software*.
2. Run the LDAP integration program included on the Content Server CD.

For more information, see the *LDAP Integration Guide*.

F. Setting Up a Content Server Cluster (Optional)

If you plan to create a Content Server cluster, see "Working with Clusters," on page 30 for instructions.

G. Setting Up Content Server for Its Business Purpose

Once you have completed your Content Server installation, you are ready to configure it for business use. For instructions, see the *Content Server Administrator's Guide* and the *Content Server Developer's Guide*. The guides explain how to create and enable a content management environment including the data model, content management sites, site users, publishing functions, and client interfaces.

Appendices

This section contains the following appendices:

- Appendix A, “Sample Procedure for Installing JES”
- Appendix B, “Sample Procedure for Uninstalling JES”

Appendix A

Sample Procedure for Installing JES

This appendix provides sample procedures for installing JES for use by Content Server. Use the procedures as a reference and a means of obtaining detailed information about the steps that apply to your own installation procedure.

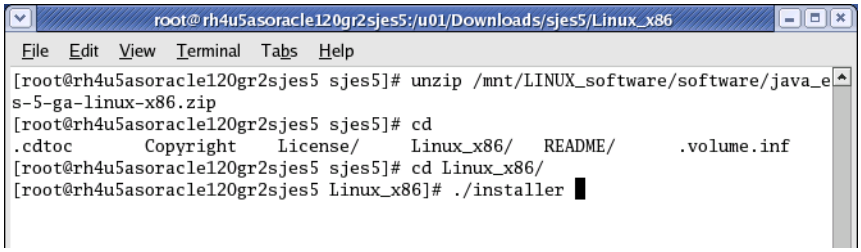
This chapter contains the following sections:

Installing JES

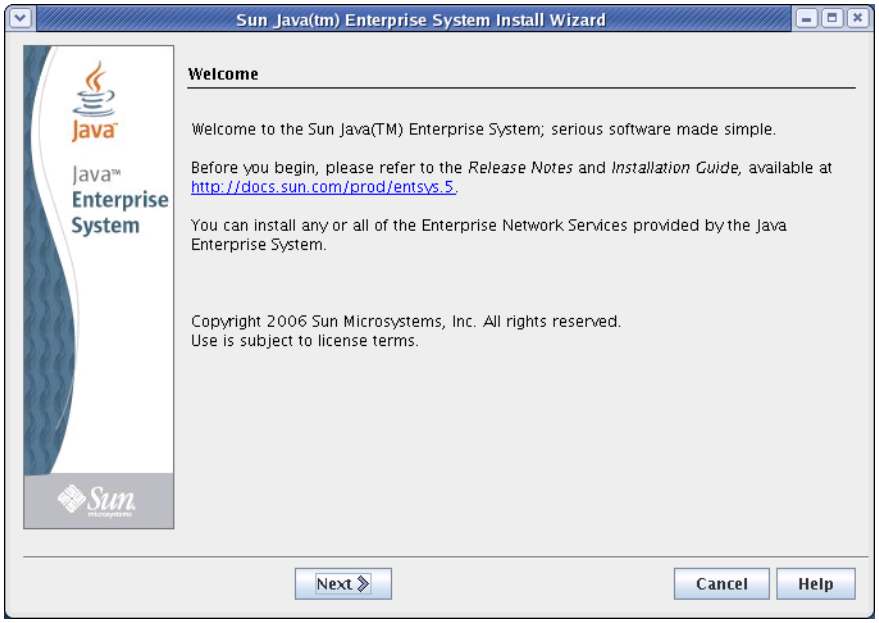
Note

Procedures for installing JES are environment specific. They depend on licensing terms and the JES version, among other factors. For instructions on installing JES on your environment, consult the JES documentation. Commands for starting and stopping JES components are given in “Start/Stop Commands,” on page 20.

1. Download JES packages from Sun’s web site and decompress them into a temporary directory.
2. Change to the temporary directory containing the installer.
3. Change to the directory corresponding to your platform and operating system.
4. Run the installer:
   a. Make sure you have at least 4GB of swap space available on your system.
   b. Start the installer: `./installer`

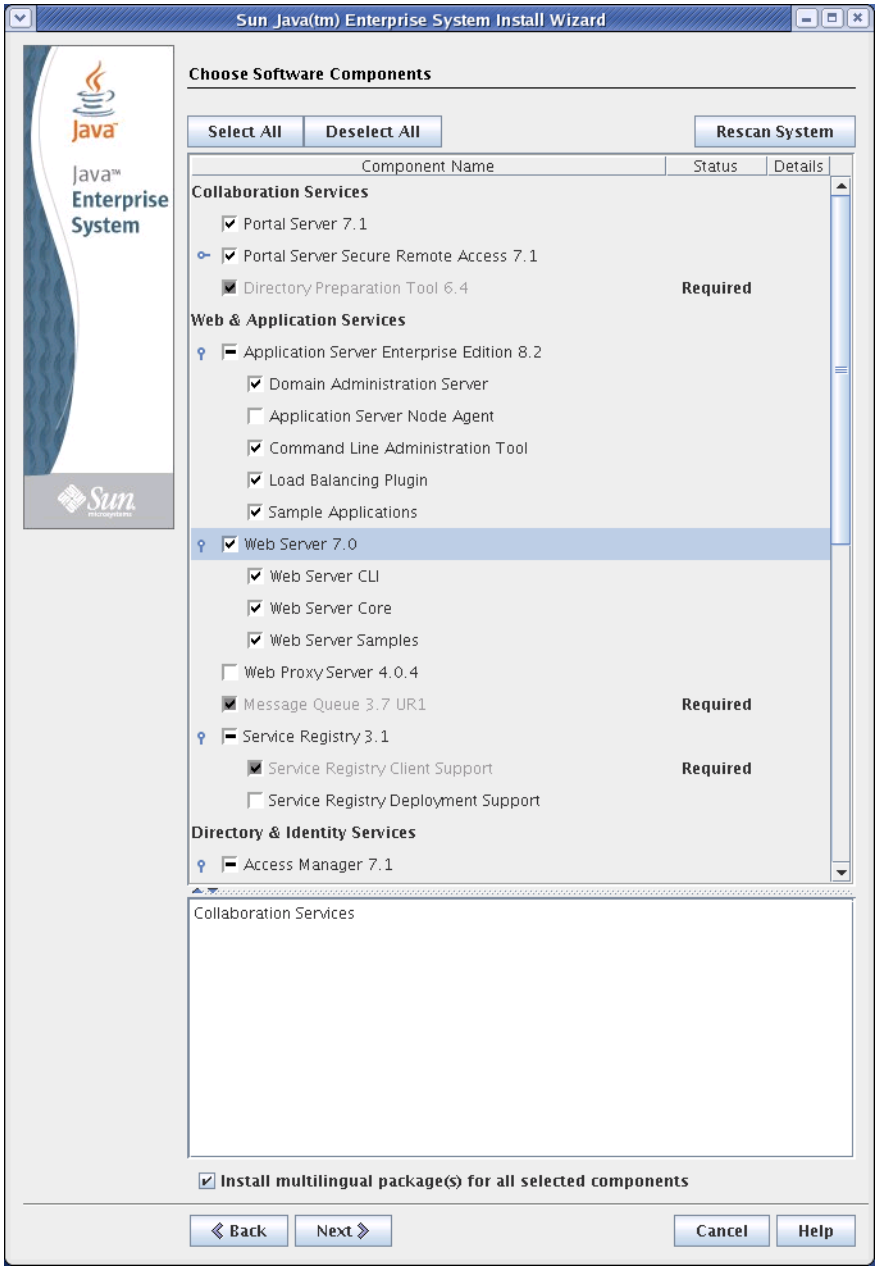


5. In the “Welcome” screen, click **Next**.



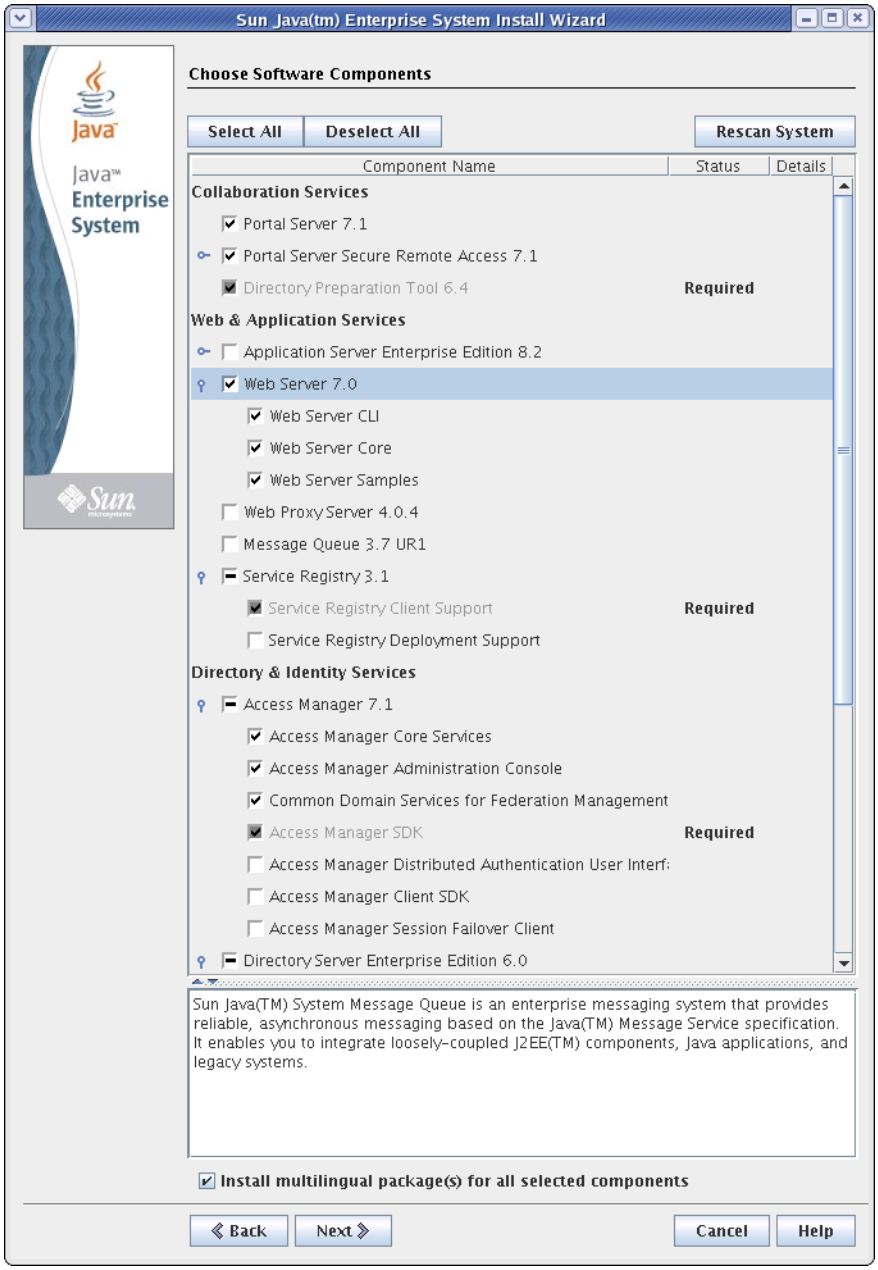
6. In the “Software License Agreement” screen, read the terms of the agreement and click **Yes, Accept License**.

7. Select the components you want to install:
   a. If you are installing Content Server on Sun Application Server, select the following components, then click **Next**:
      - **Portal Server 7.1**
      - **Portal Server Secure Remote Access 7.1**
      - **Application Server Enterprise Edition 8.2**
      - (Optional) **Web Server 7.0**
      - **Access Manager 7.1**
      - **Directory Server Enterprise Edition 6.0**

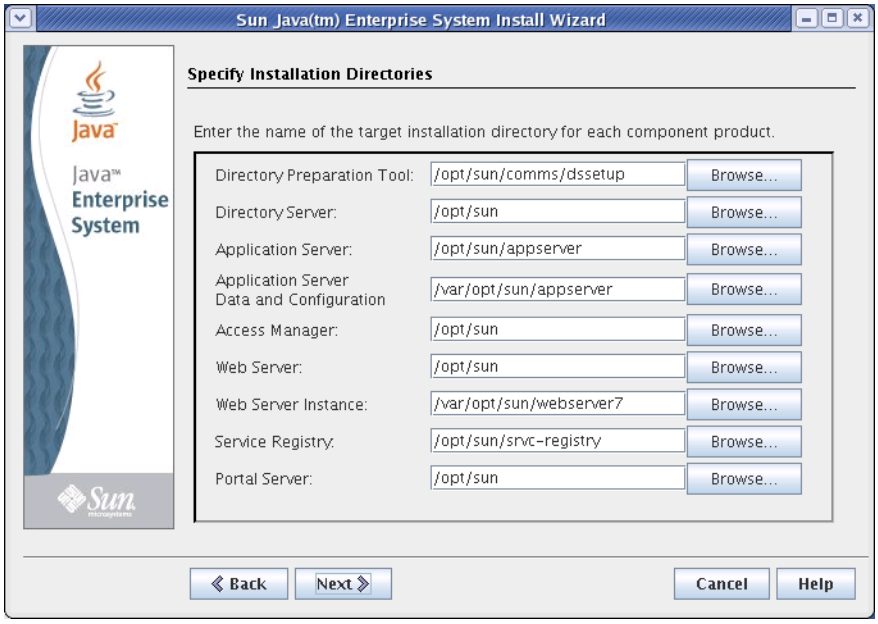


b. If you are installing Content Server on Sun Web Server, select the following components, then click **Next**:

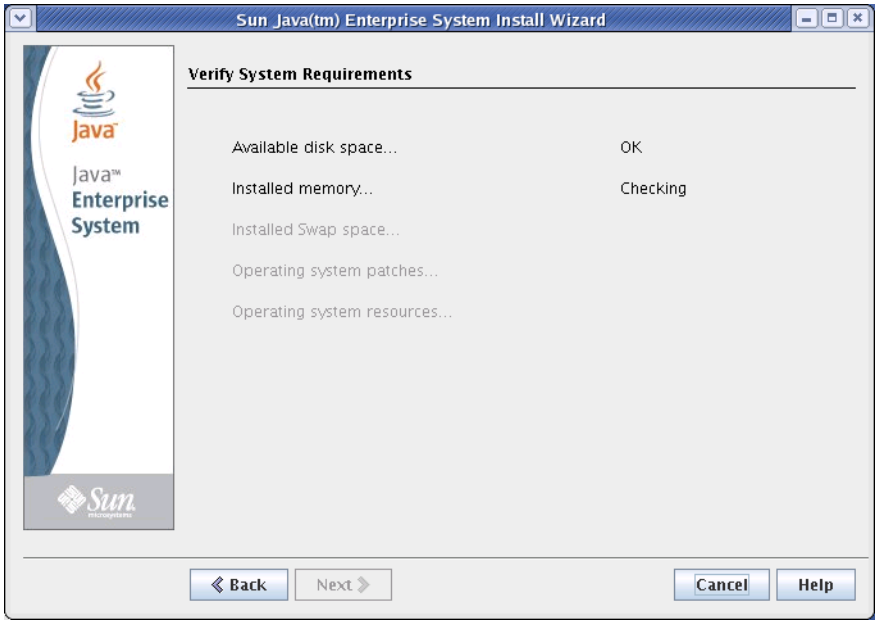
- **Portal Server 7.1**
- **Portal Server Secure Remote Access 7.1**
- **Web Server 7.0**
- **Access Manager 7.1**
- **Directory Server Enterprise Edition 6.0**



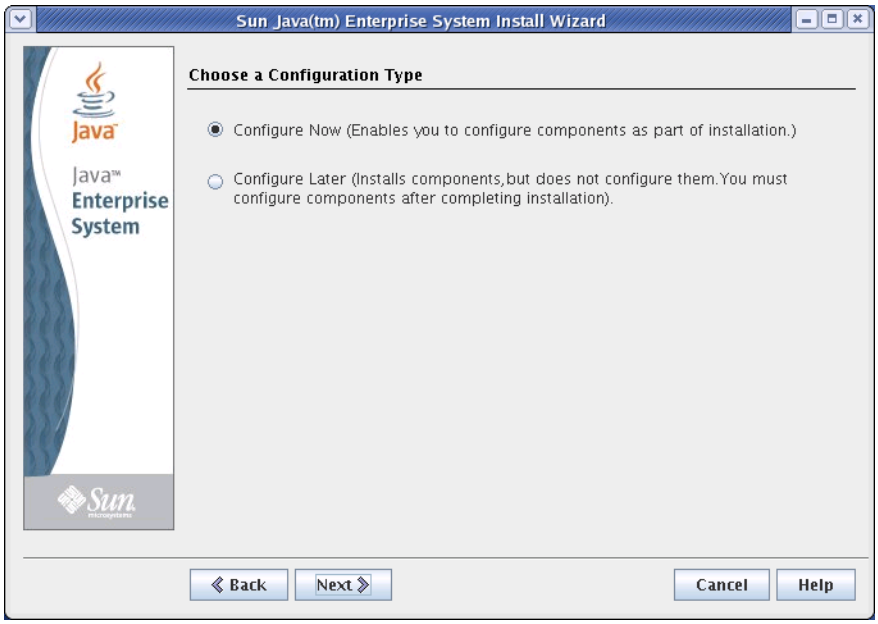
8. Specify the installation directories for the components you are installing. FatWire recommends using the default values. When you are finished, click **Next**.



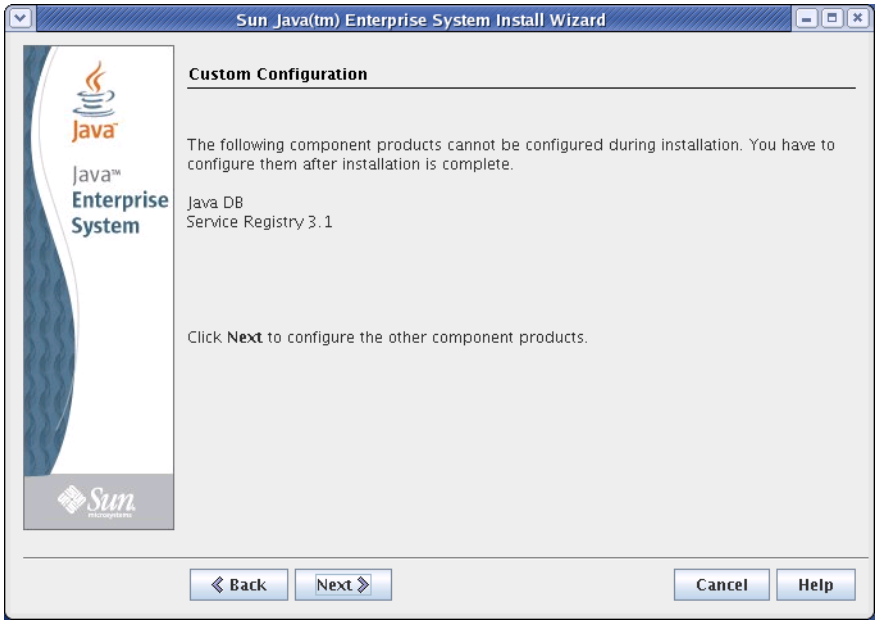
9. In the "Verify System Requirements" screen, click **Next**. If any of the checks fail, fix the reported problems before proceeding with the installation.



10. In the “Choose a Configuration Type” screen, select **Configure Now** and click **Next**.



11. In the “Custom Configuration” screen, click **Next**.

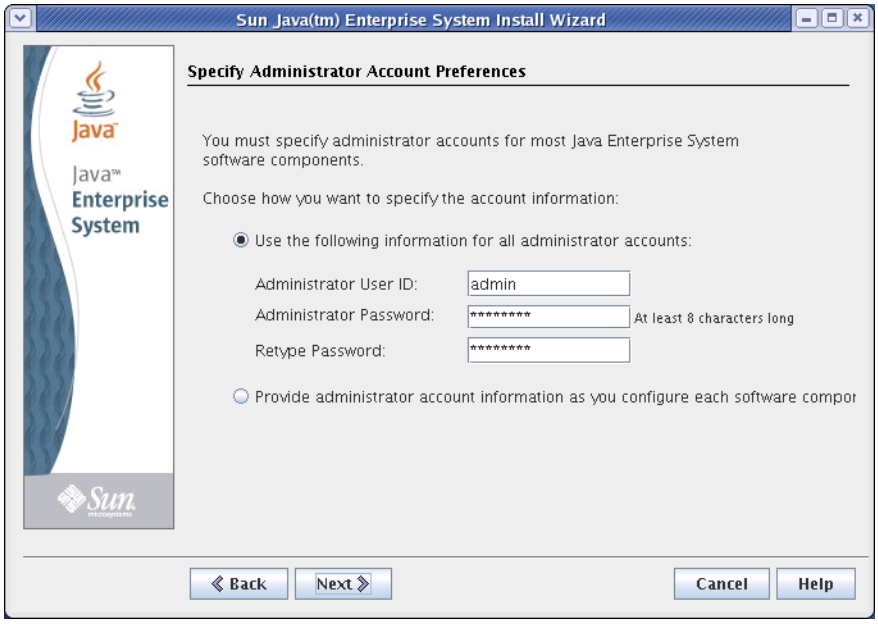


12. In the "Specify Administrator Account Preferences" screen, do the following:

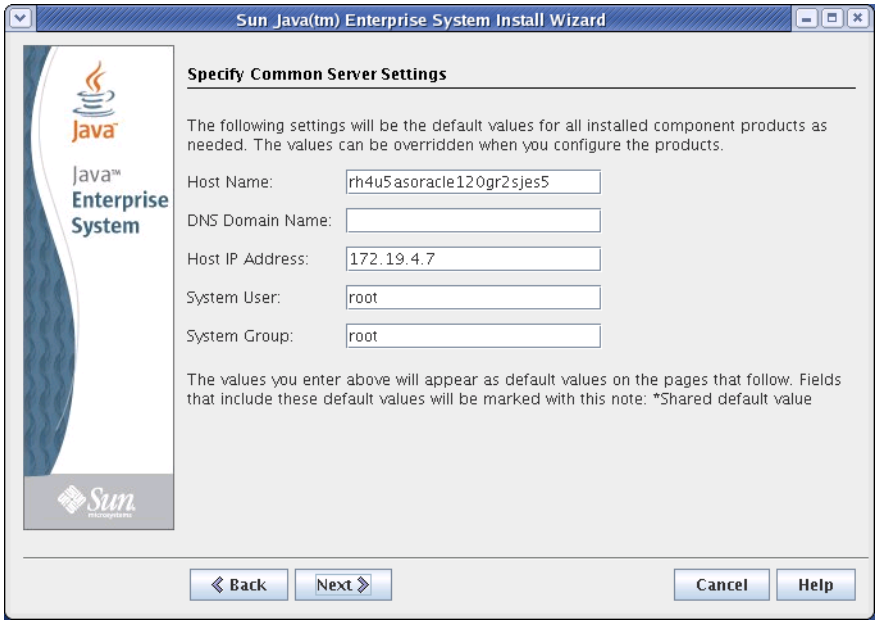
a. Enter and re-enter the Administrator User password.

b. Make a record of the Administrator User ID and password.

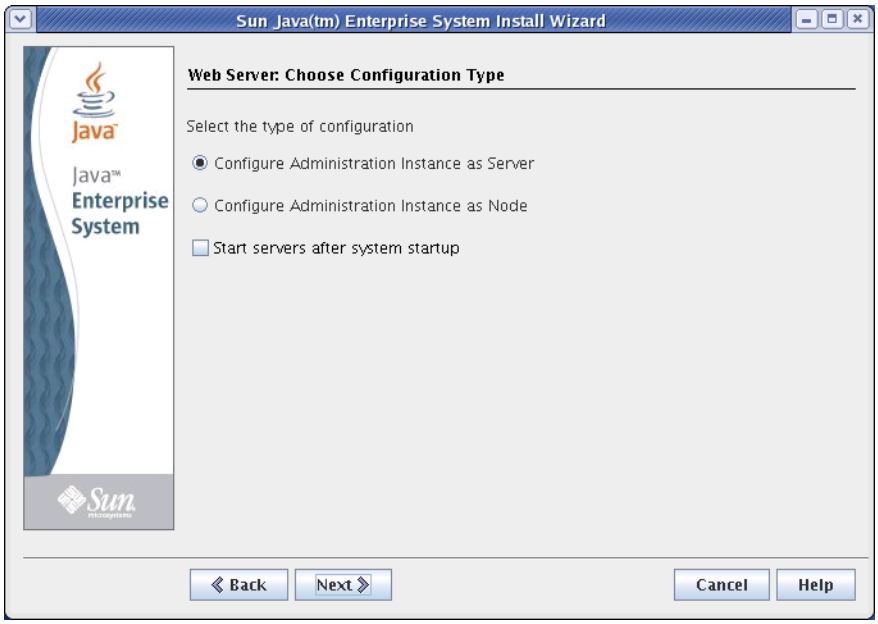
c. Click **Next**.



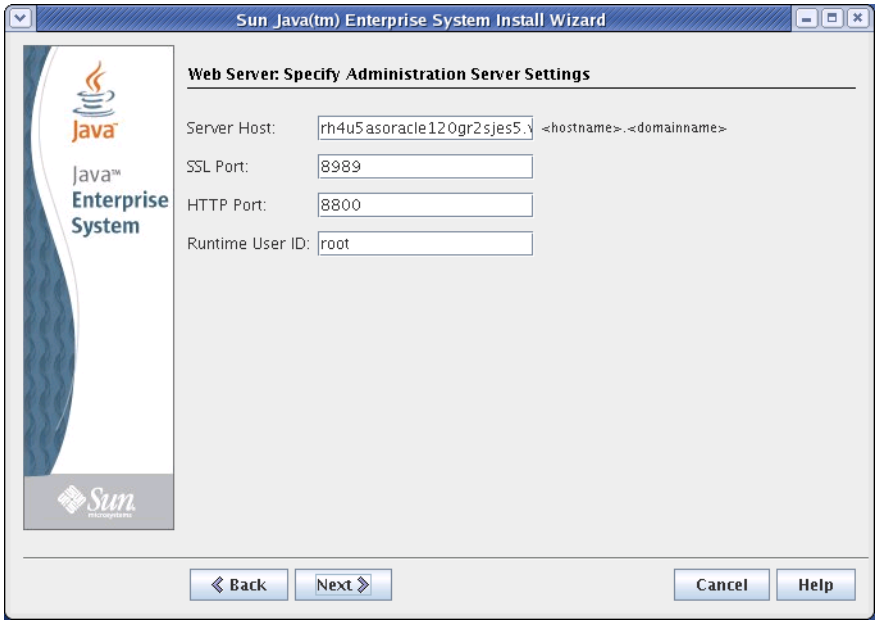
13. In the "Specify Common Server Settings" screen, enter your DNS domain name, make sure all displayed information is correct, and click **Next**.



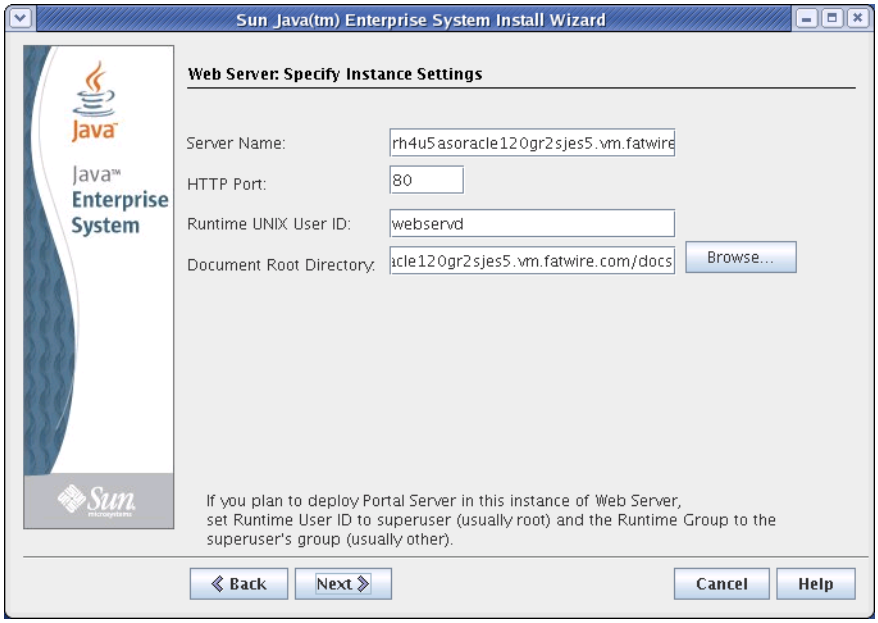
14. In the “Web Server: Choose Configuration Type” screen, click **Next**.



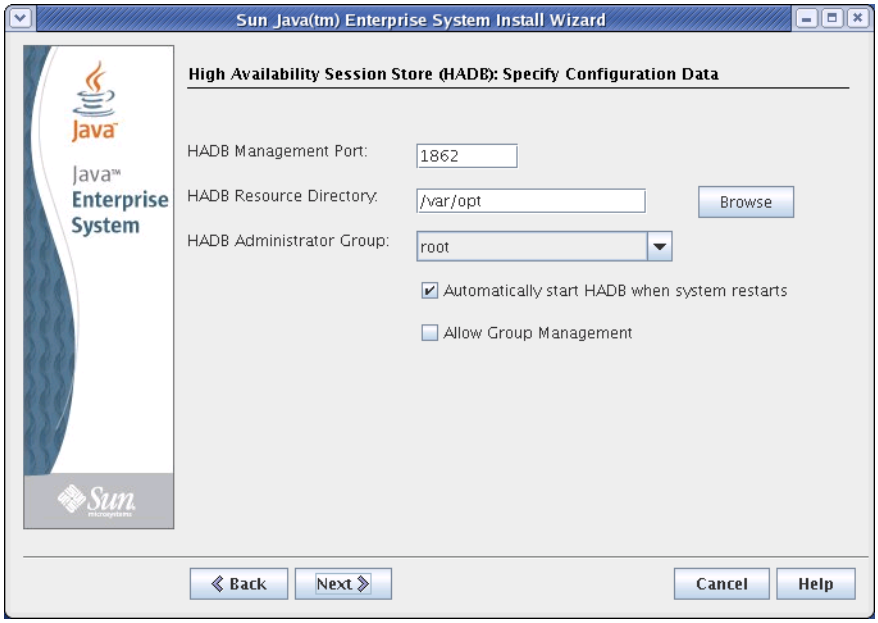
15. In the “Web Server: Specify Administration Server Settings” screen, make a record of the displayed port numbers, then click **Next**.



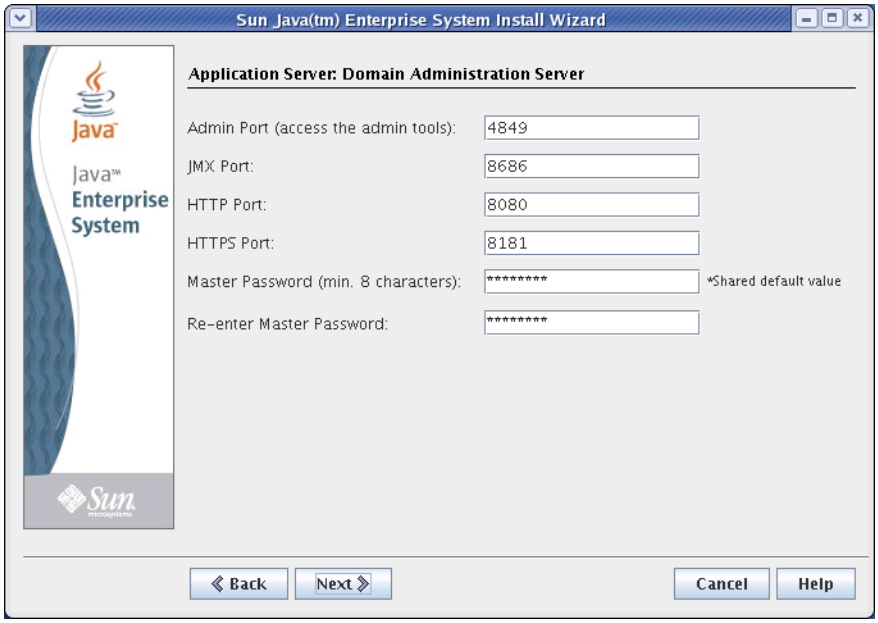
16. In the “Web Server: Specify Instance Settings” screen, do the following:
    a. Change the value of the **Runtime UNIX User ID** field to a valid user name.
    b. Verify all of the displayed information is correct.
    c. Click **Next**.



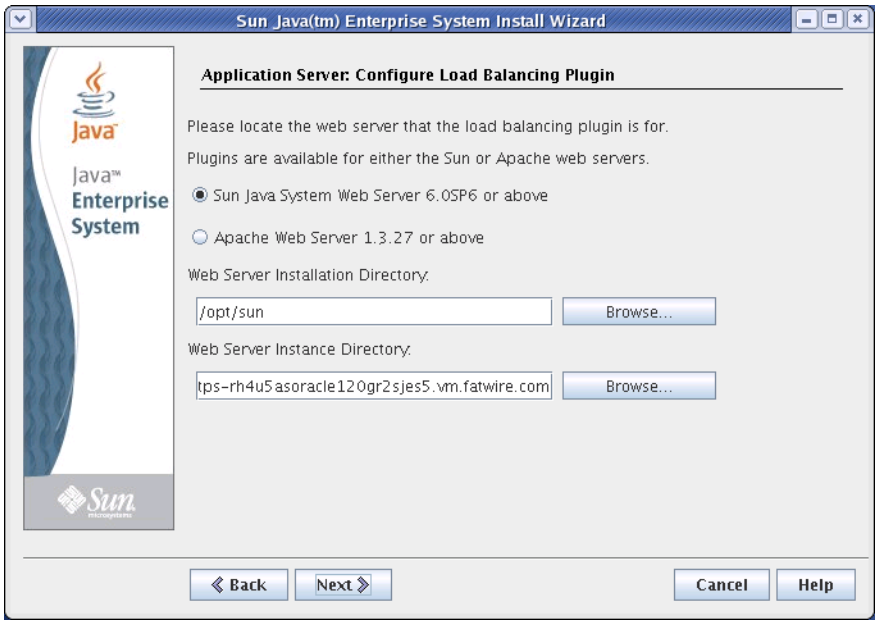
17. In the “HADB Specify Session Data” screen, click **Next**.



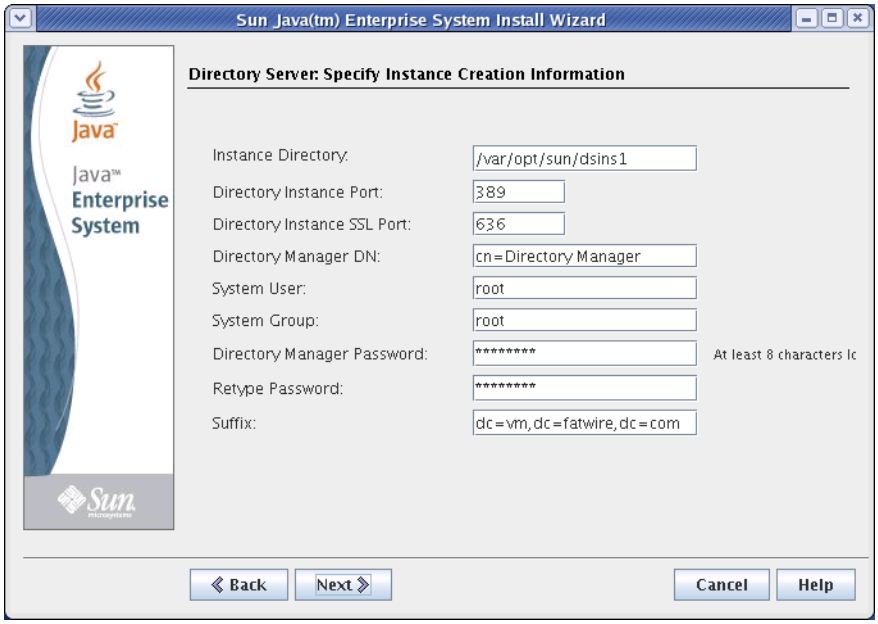
18. In the "Application Server: Domain Administration Server" screen, make a record of the Admin, HTTP, and HTTPS port numbers, then click **Next**. Do **not** change the master password.



19. In the "Application Server: Configure Load Balancing Plugin" screen, click **Next**.



20. In the "Directory Server: Specify Instance Creation Information" screen, make a record of the **Instance Directory**, **Directory Instance Port**, and **Directory Manager DN** field values, then click **Next**. Do **not** change the Directory Manager password.



21. In the "Access Manager: Specify Configuration Information" screen, do the following:

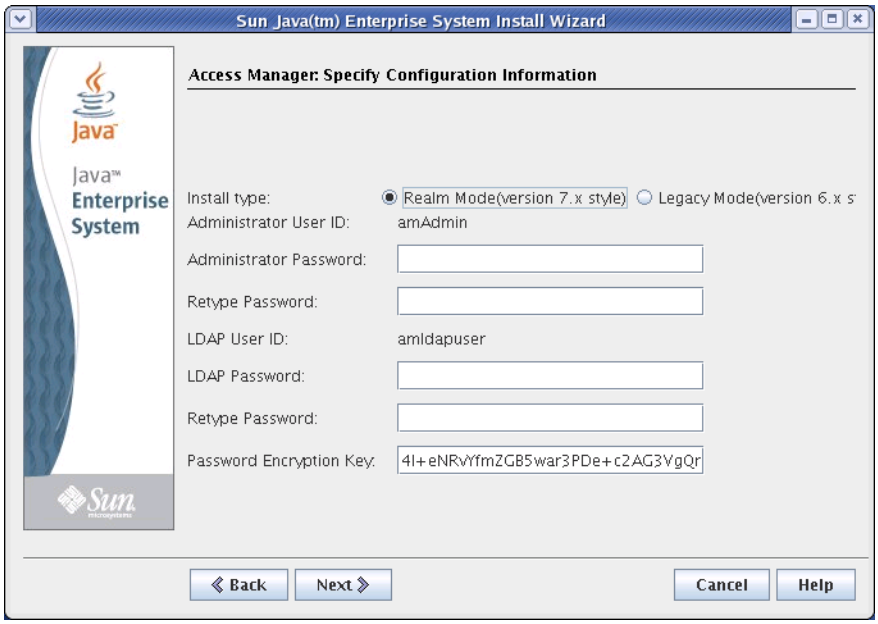
a. Select the **Realm (version 7.x style)** radio button.

b. Enter and re-enter the Access Manager Administrator User password.

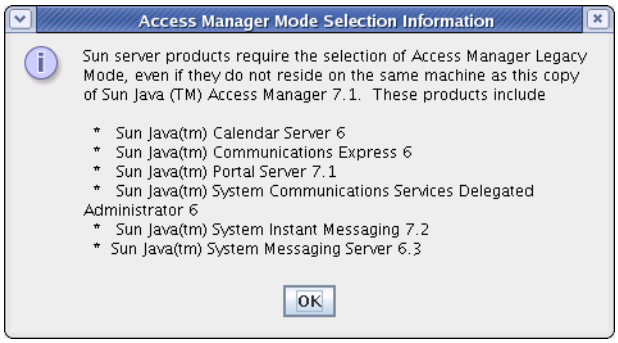
c. Enter and re-enter the Access Manager LDAP user password. This password must be different from the Access Manager Administrator User password.

d. Make a record of the passwords you entered, and the corresponding user names.

e. Click **Next**.



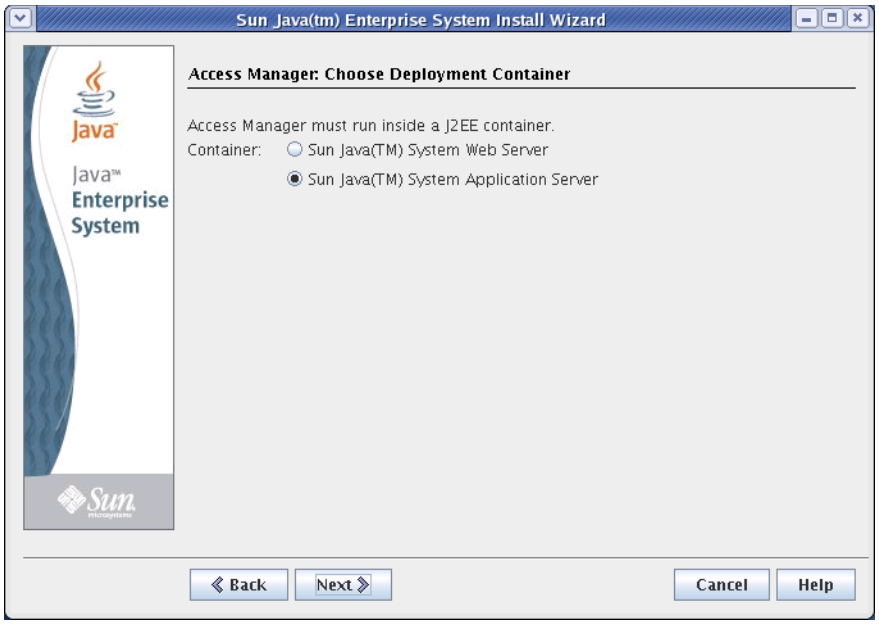
22. In the pop-up dialog box that appears, click **OK**.



23. In the "Access Manager: Choose Deployment Container" screen, do one of the following:

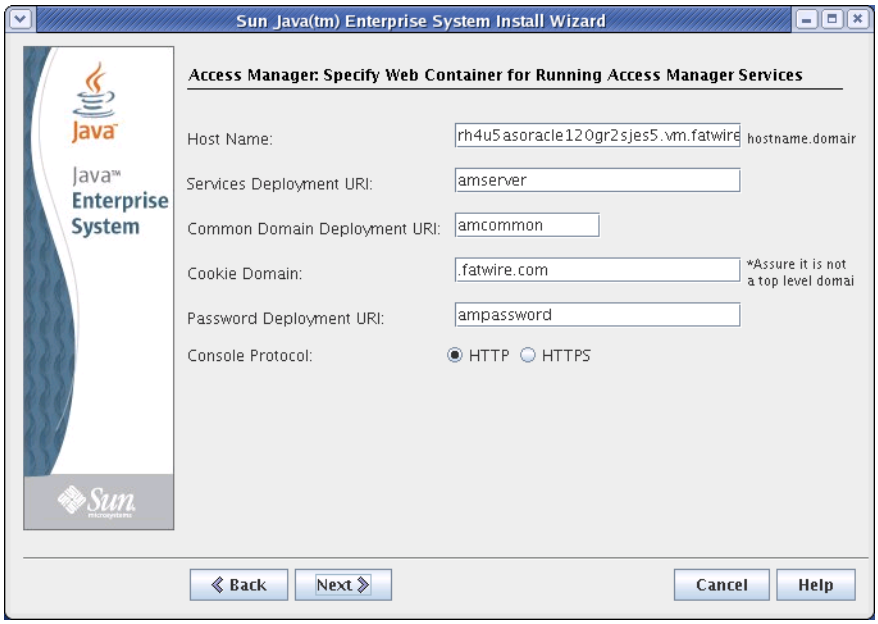
a. If you are installing Content Server on Sun Application Server, select the **Sun Java System Application Server** radio button, and click **Next**.

b. If you are installing Content Server on Sun Web Server, select the **Sun Java System Web Server** radio button, and click **Next**.

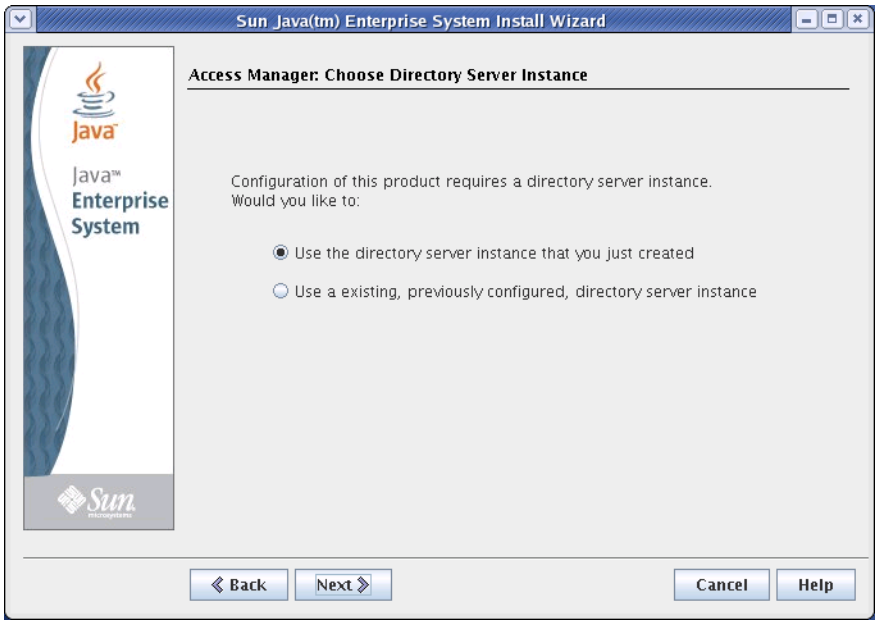


24. In the “Access Manager: Specify Sun Java System Application Server” screen, click **Next**.

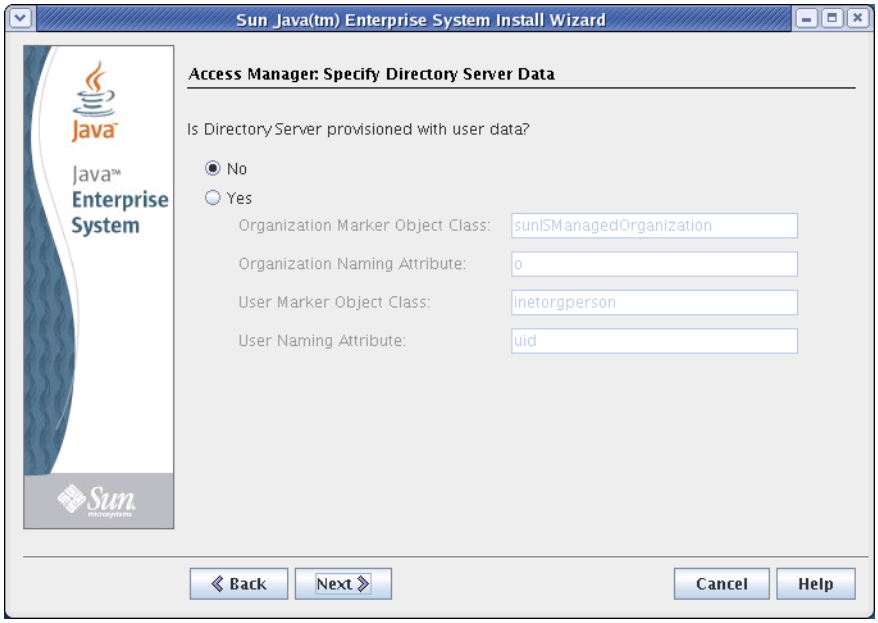
25. In the “Access Manager: Specify Web Container for Running Access Manager Services” screen, make sure that the **Hostname**, **Cookie Domain**, and **Console Protocol** field values are correct, then click **Next**.



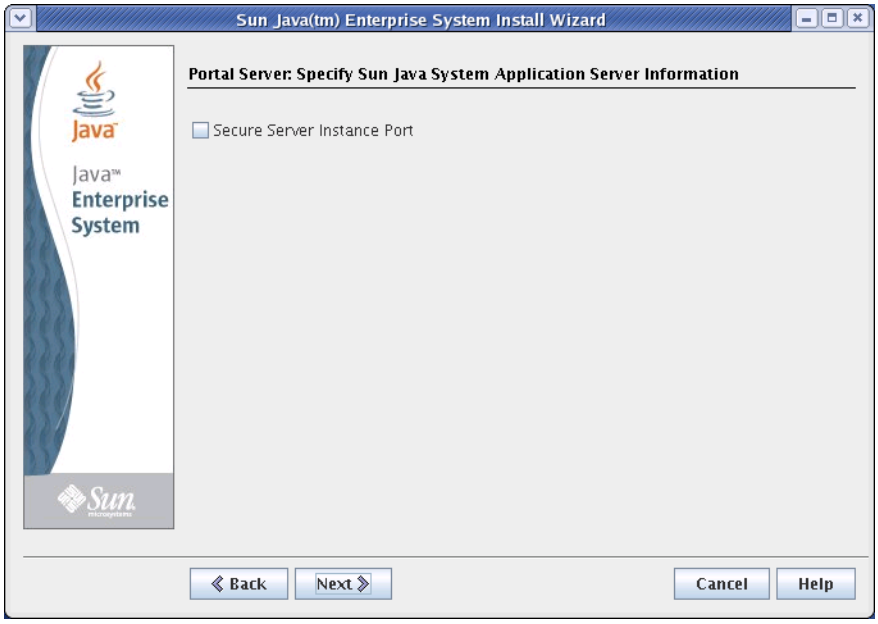
26. In the “Access Manager: Choose Directory Server Instance” screen, click **Next**.



27. In the “Access Manager: Specify Directory Server Data” screen, click **Next**.



28. In the "Portal Server: Specify Sun Java System Application Server Information" screen, click **Next**.

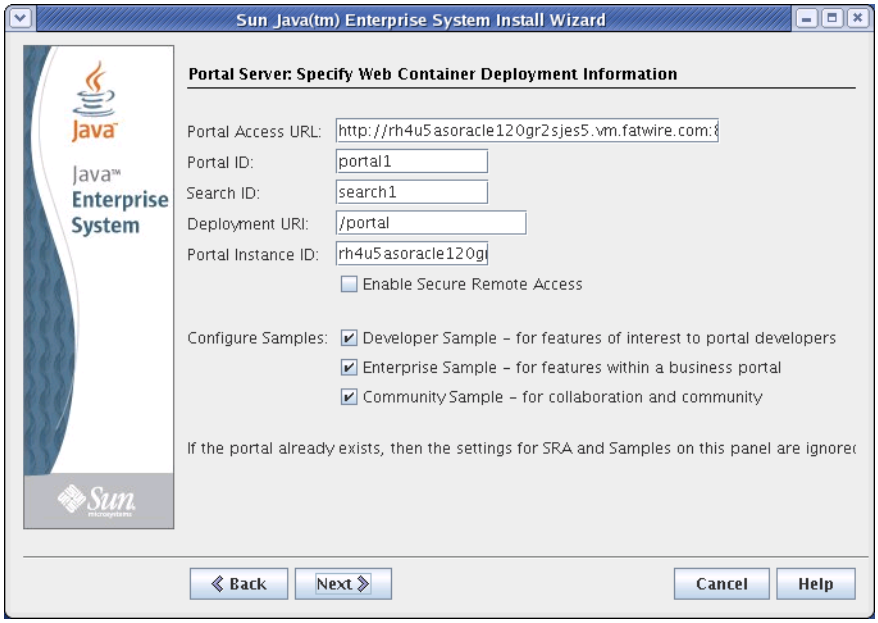


29. In the "Portal Server: Specify Web Container Deployment Information" screen, do the following:

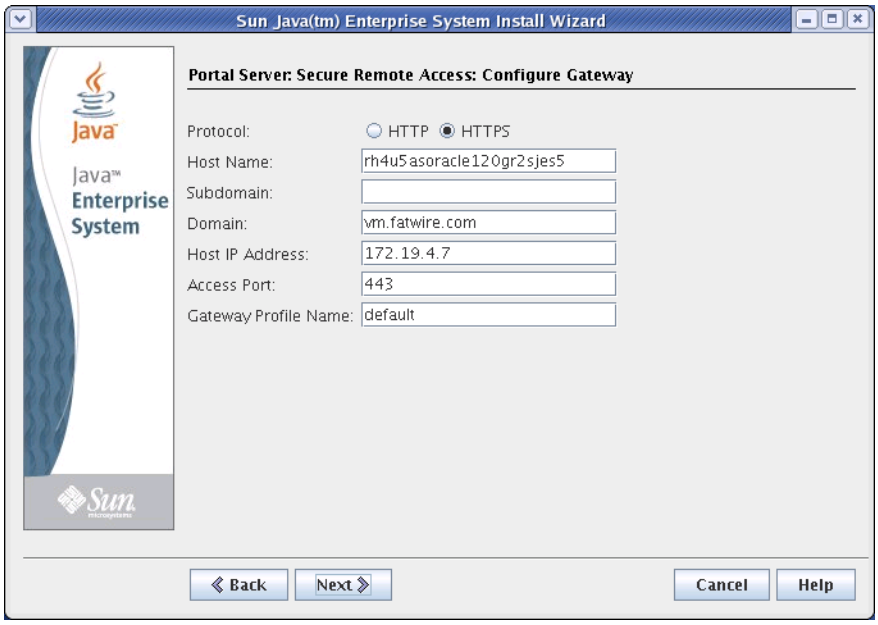
a. Confirm that the displayed information is correct.

b. Make a record of the **Portal ID** and **Deployment URI** field values.

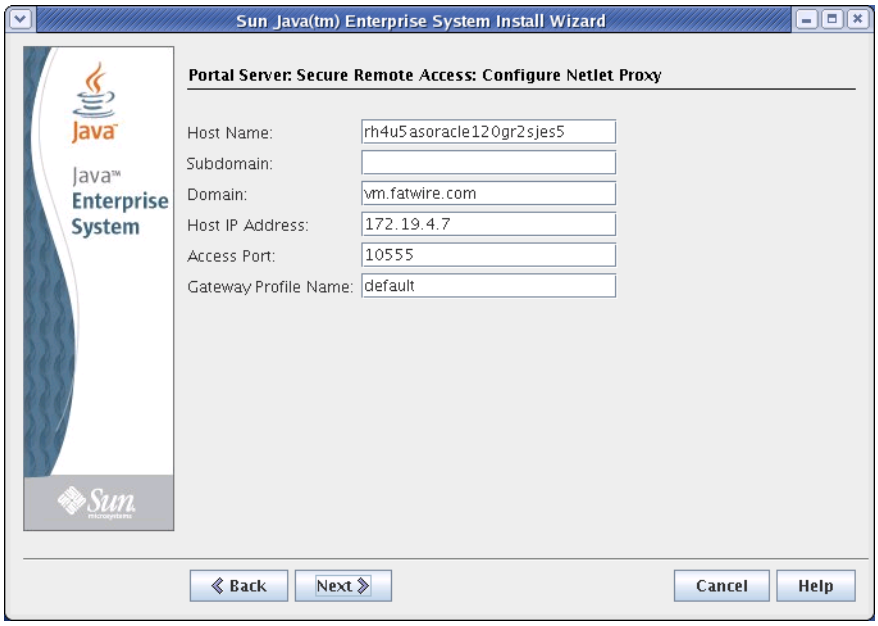
c. Click **Next**.



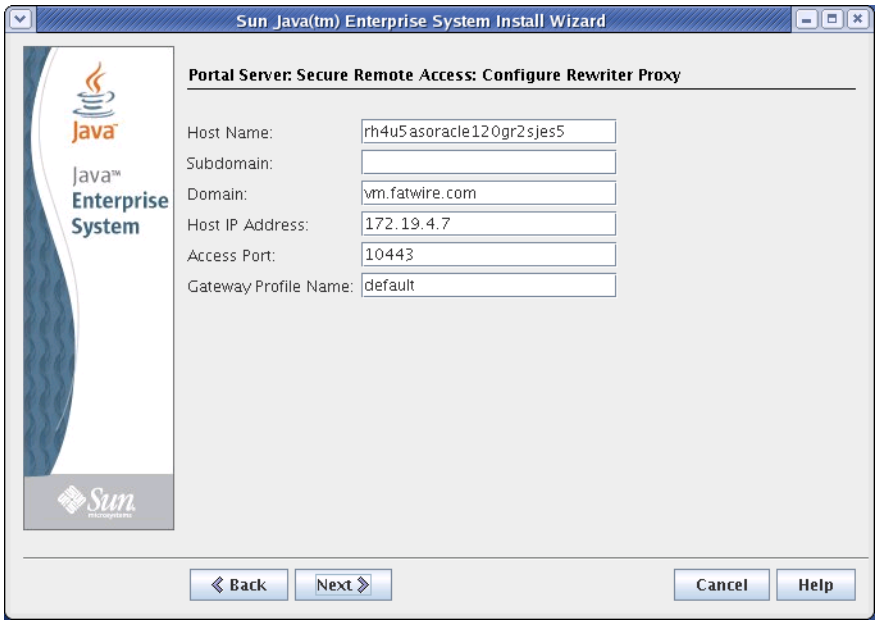
30. In the “Portal Server: Secure Remote Access: Configure Gateway” screen, click **Next**.



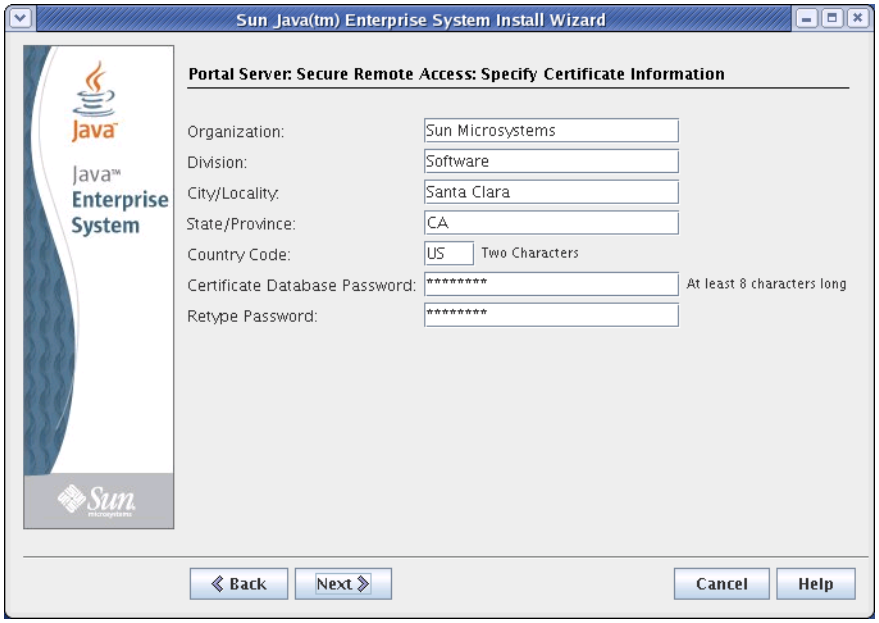
31. In the “Portal Server: Secure Remote Access: Netlet Proxy” screen, click **Next**.



32. In the “Portal Server: Secure Remote Access: Rewriter Proxy” screen, click **Next**.



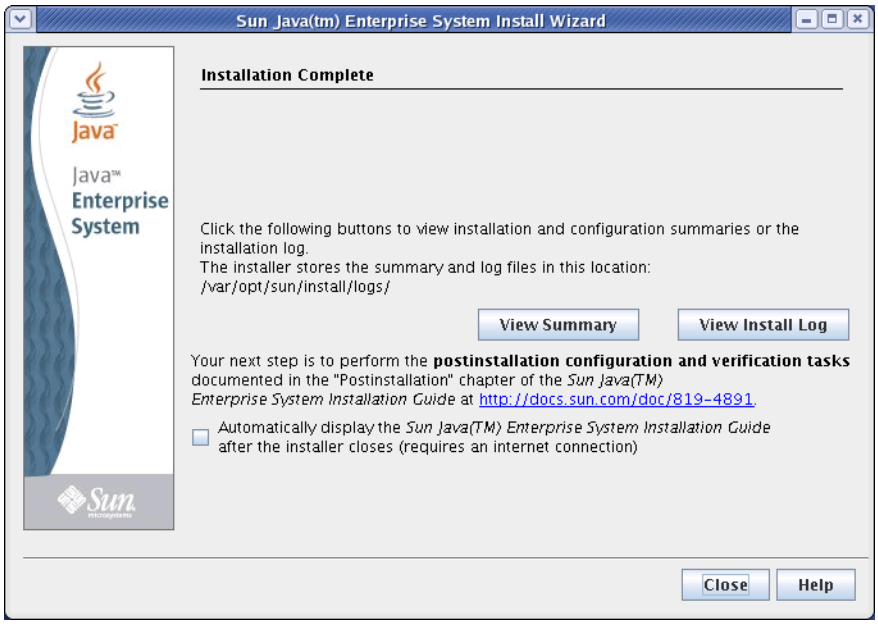
33. In the “Portal Server: Secure Remote Access: Specify Certificate Information” screen, replace the displayed information with information from your certificate, then click **Next**. (If you do not yet have a certificate click **Next**; you can change this information later.)



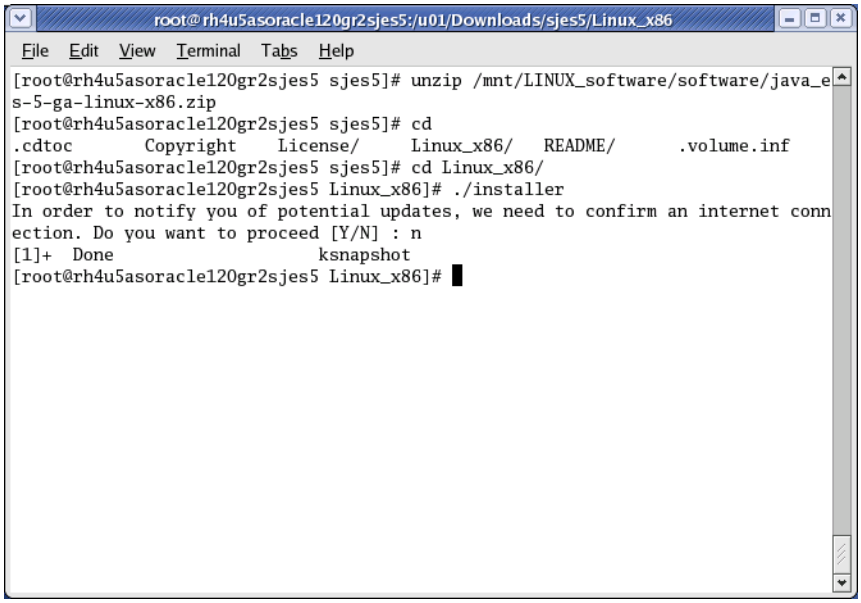
34. In the “Ready to Install” screen, review the choices you have made, then click **Install**.
35. Wait for the installation to complete.

36. In the “Installation Complete” screen, do the following:
    a. Click **View Summary** and review the displayed information.
    b. If no failures occurred during the installation, click **Close**.

       If any of the components failed to install, click **View Installation Log** and review the log for possible causes of failure, then retry the installation.



37. (Optional) If you want to check for the latest JES updates, press **Y** when prompted. Otherwise, press **N**.



Appendix B

Sample Procedure for Uninstalling JES

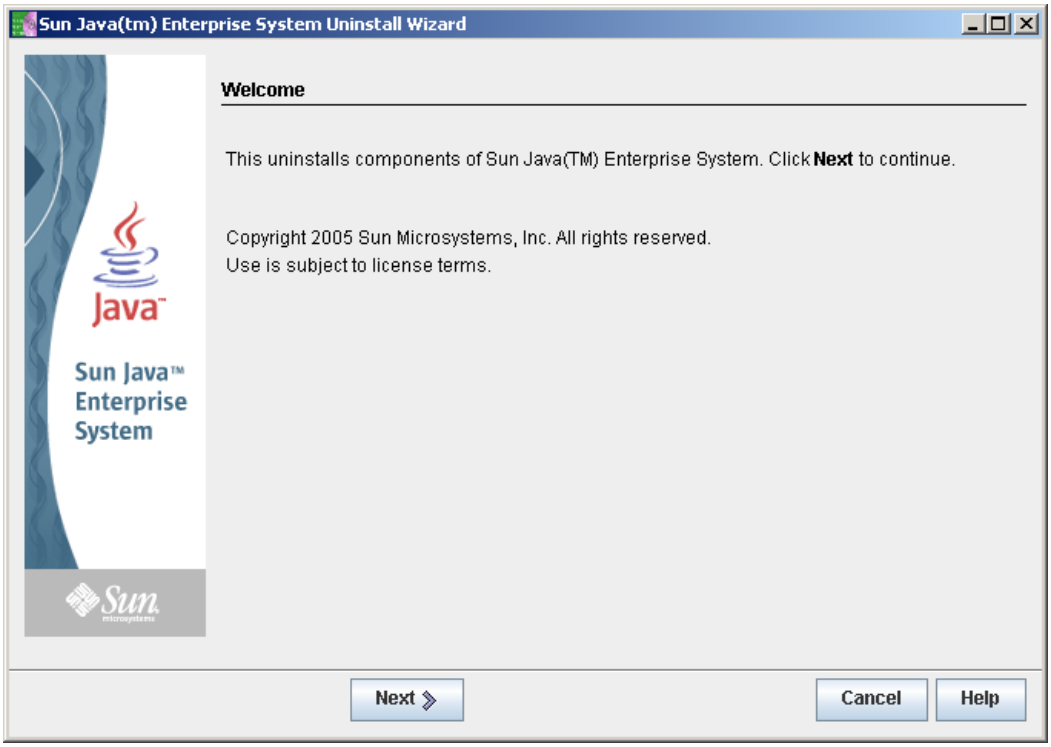
This appendix provides a sample procedure for uninstalling JES. The procedure is based on scripts provided by Sun Microsystems.

Uninstalling JES

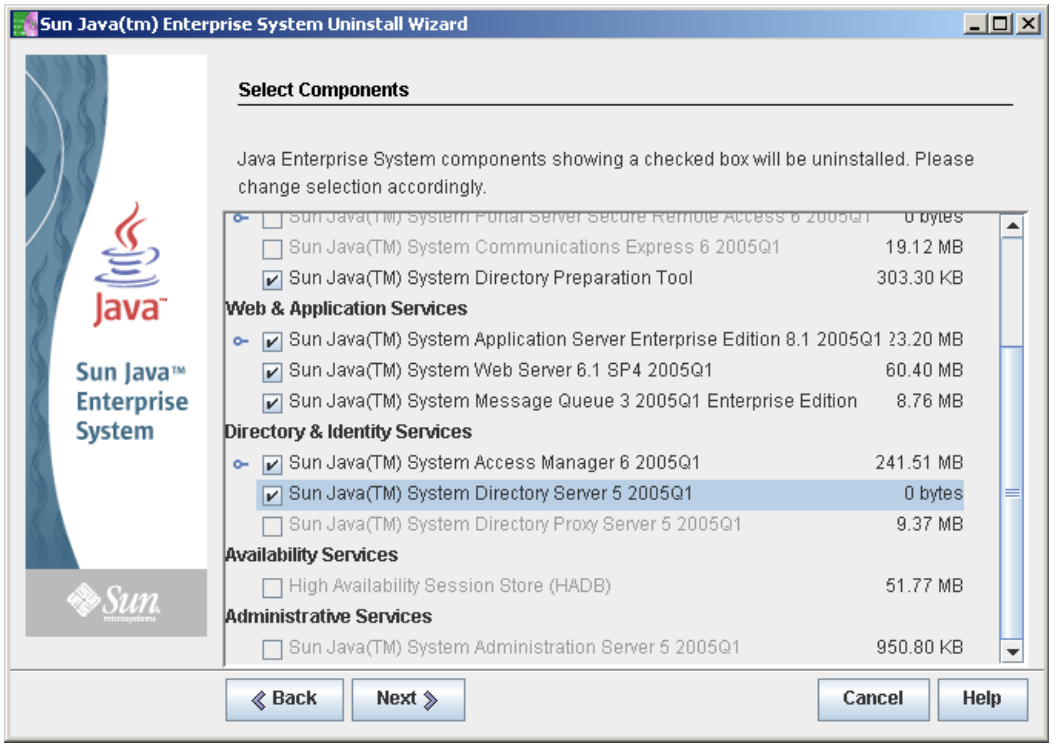
1. Execute the following command:

   `/var/scam/prod/entices/uninstall`

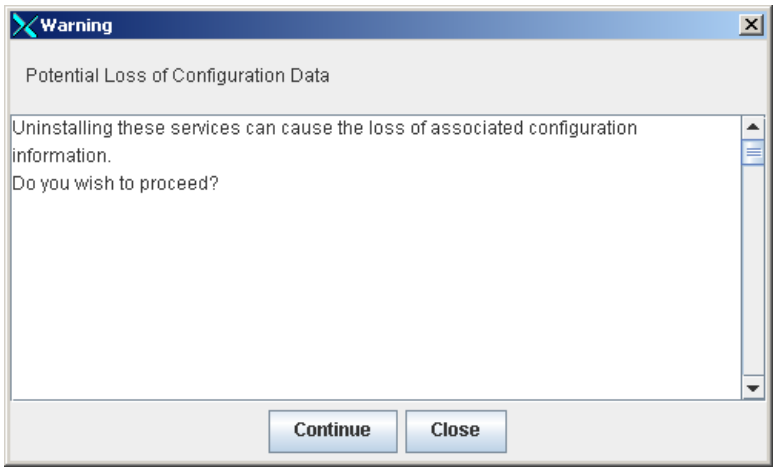
2. In the “Welcome” screen, click **Next**.



3. In the next screen, select all components. Click **Next**.

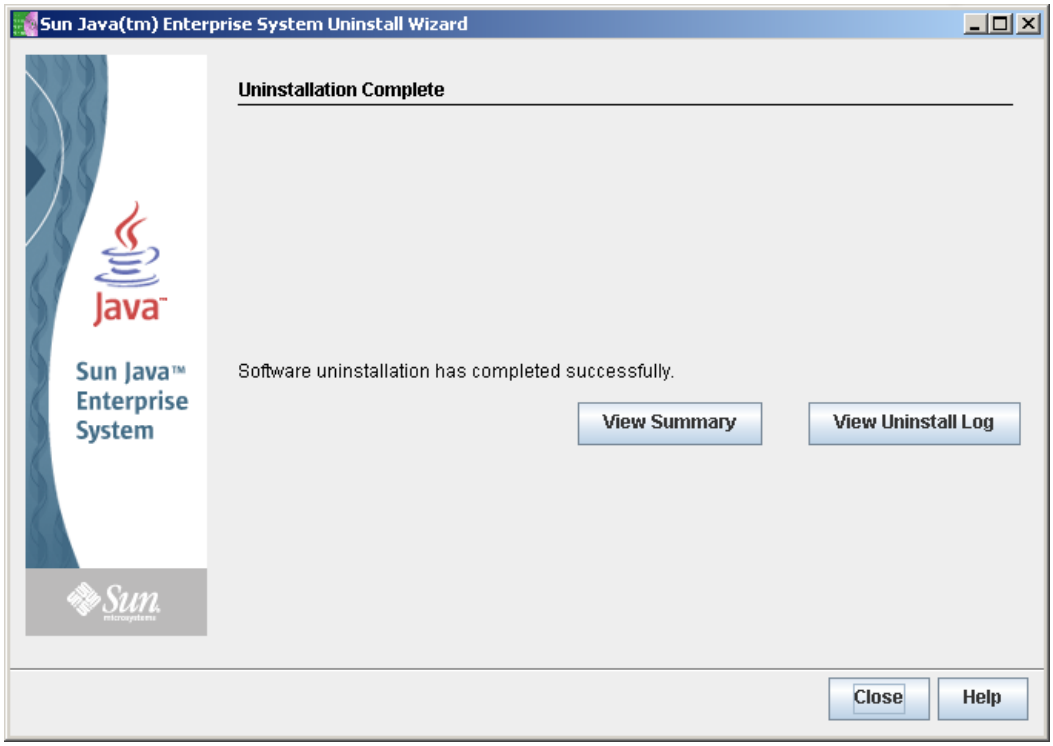


4. In the "Potential Loss of Configuration Data" window, click **Continue**.



5. Wait for the uninstallation process to complete.

6. Click **Close**.



7. Run `jesrm.sh` (this file can be found on the Sun site; it is not part of the FatWire distribution) and select option 8 from the menu.
8. Check that none of the following are running. If they are, stop them:

```
ps -ef|grep "appserver"
ps -ef|grep "webserv"
ps -ef|grep "dps"
ps -ef|grep "imq"
ps -ef|grep "slapd"
ps -ef|grep "admin"
```

9. Remove the following directories:

```
rm -rf /var/sadm/install/logs/Orion*
rm -rf /var/sadm/install/productregistry
rm -rf /var/sadm/install/.lockfile
rm -rf /var/sadm/install/.pkg.lock
rm -rf /var/sadm/install/logs/Administration_Server*
rm -rf /var/sadm/install/logs/Directory_Server*
rm -rf /var/sadm/prod/orion
rm -rf /usr/sunone/*
rm -rf /var/opt/SUNW*
rm -rf /etc/opt/SUNW*
rm -rf /opt/SUNWps
rm -rf /opt/SUNWam
rm -rf /opt/SUNWappserver
rm -rf /opt/SUNWwbsvr
```

10. Reboot the server.