HP Cloud Service Automation

For the Linux operating system

Software Version: 4.10

Configuring an HP CSA Cluster for High Availability Using a Load Balancer

Document Release Date: September 2014

Software Release Date: July 2014

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

The OpenStack® Word Mark and the Square O Design, together or apart, are trademarks or registered trademarks marks of OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

RED HAT READY™ Logo and RED HAT CERTIFIED PARTNER™ Logo are trademarks of Red Hat, Inc.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: **http://h20230.www2.hp.com/selfsolve/manuals**

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: **http://h20229.www2.hp.com/passport-registration.html**

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at: **http://www.hp.com/go/hpsoftwaresupport**

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

Contents

Chapter 1: Overview

HP Cloud Service Automation (HP CSA) uses JBoss clustering technology to enable you to configure an active/active (high-availability) cluster. Clustering enables you to run HP CSA on several parallel servers called *nodes*. Cluster configuration improves performance on systems that handle high transaction volumes or large numbers of concurrent users. In addition to handling higher user loads and providing greater scalability, the cluster configuration supports server failover features.

Web requests to the HP CSA Controller or Marketplace Portal are load balanced among the nodes in the cluster. Increasing the number of nodes in the cluster will improve web request transaction throughput. However, certain HP CSA background services, those that handle the fulfillment of subscription requests asynchronously, only run on a single node in the cluster. For those HP CSA background services, adding more nodes to the cluster will not increase the throughput of subscription fulfillment. Instead, for those HP CSA background services, a cluster deployment only allows failover capability for the background service.

Because clustering distributes the workload across different nodes, if any node fails, HP CSA remains accessible through other nodes in the cluster. You can continue to improve user request throughput by simply adding nodes to the cluster. If a node shuts down, activities such as email notifications that are scheduled to run on that node are automatically transferred to another available node. This server failover feature helps ensure that HP CSA remains operational.

Unsaved changes on a node that shuts down are lost and are not transferred to an available node. Users who log on to HP CSA after a node shuts down see only changes that were saved on that node.

In the following diagram, the example cluster configuration consists of seven different physical (or virtual) hosts: one host is running a load balancer that proxies web requests into the HP CSA/JBoss cluster or Node.js cluster (for the Marketplace Portal), three hosts are running HP CSA in domain mode, and three hosts are running the Marketplace Portal.

Note: Content on how to use a database cluster or Oracle RAC is beyond the scope of this document. However, configuring HP CSA to use a Microsoft SQL Server cluster is no different from configuring HP CSA to use a standalone Microsoft SQL Server. Install and configure the Microsoft SQL Server cluster according to the manufacturer's documentation and follow the instructions to install HP CSA using a Microsoft SQL Server in the *HP Cloud Service Automation Installation Guide*.

For information about configuring HP CSA with Oracle RAC, refer to the *Configuring HP CSA to Work with Oracle RAC* whitepaper.

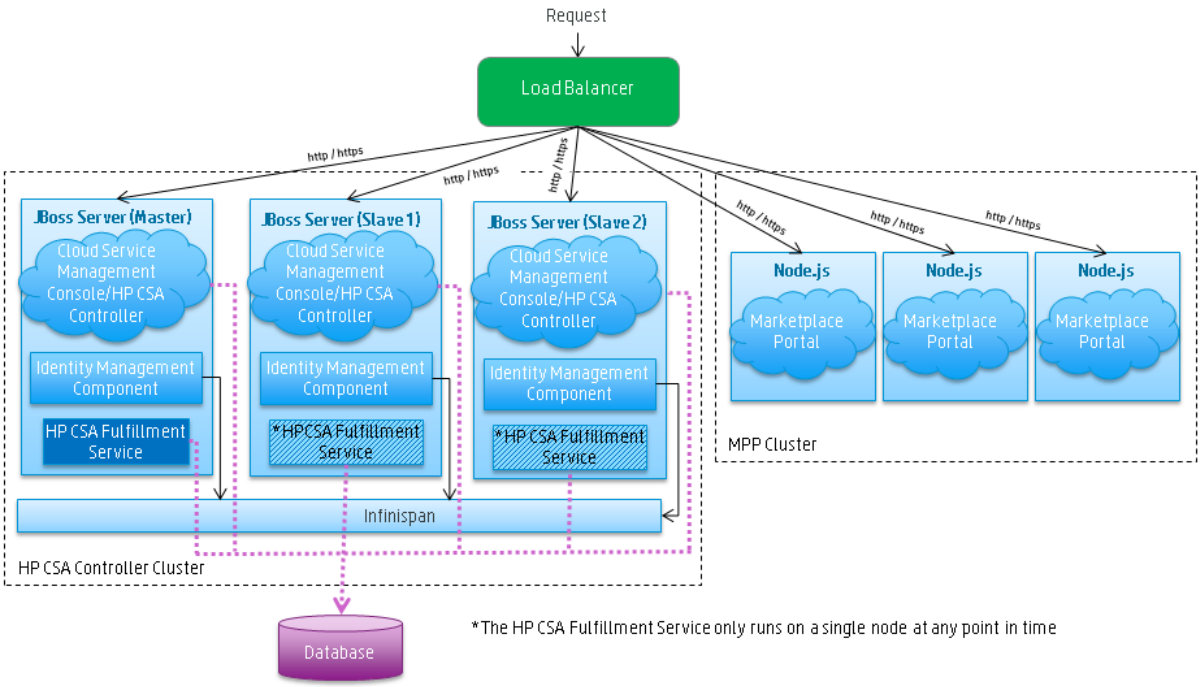


Figure 1-1. Example Cluster Configuration

The cluster uses a load balancer to distribute requests among any number of nodes. The load balancer (internal or external) listens for HTTP/S requests from standard interface clients. Nodes are transparent to users and users access only the URL to the load balancer. The load balancer forwards HTTP/S requests to one of the other nodes.

The Identity Management components communicate over an Infinispan data bus (a JBoss module) which replicates a user's authentication token across all nodes on which the Identity Management component is installed. If one node fails, another node will have the user's authentication token and can validate the user's requests.

Request Flow

The following diagrams show how a request (distributed from the load balancer) is processed in the clustered environment for the Cloud Service Management Console and Marketplace Portal.

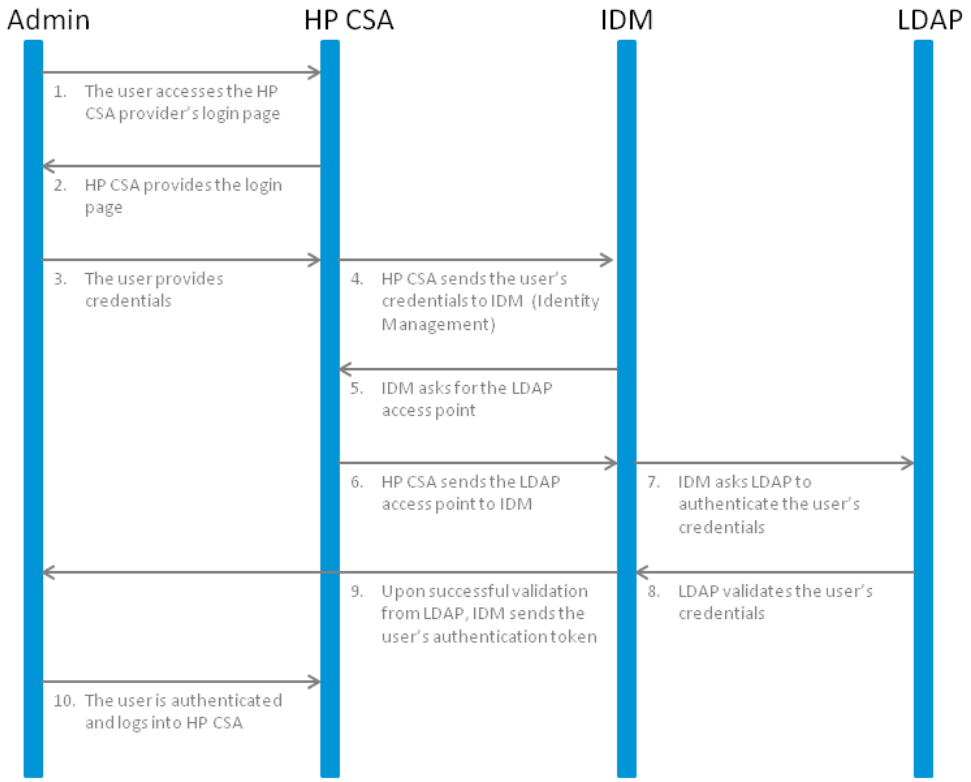


Figure 1-2. Cloud Service Management Console Request Flow

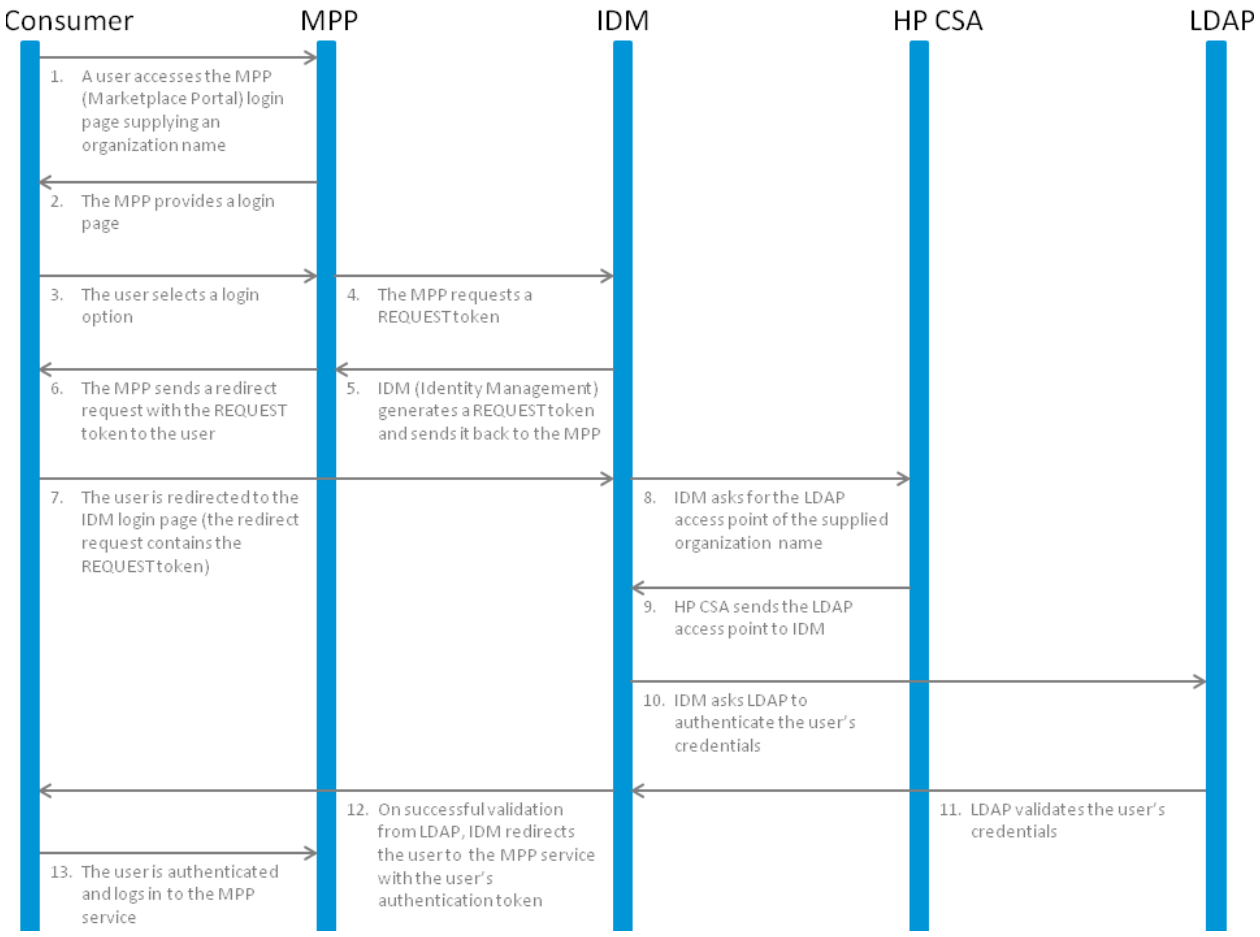


Figure 1-3. Marketplace Portal Request Flow

About the Examples

In this document, the following names are used to identify the hosts or nodes in the clustered environment:

- **Load_Balancer node**: the load balancer that distributes requests among the nodes in the clustered environment
- **Master node**: hosts HP CSA
- **Slave nodes**: hosts HP CSA
- **MPP_Node nodes**: hosts the Marketplace Portal

In this document, an item denoted in square brackets is a placeholder for the actual value that has been configured (for example, the hostname of the "master" node is denoted as [MASTER_HOSTNAME]).

In the following diagram, items in parentheses are default or example values used in this document (for example, the default port used by the Cloud Service Management Console is 8081).

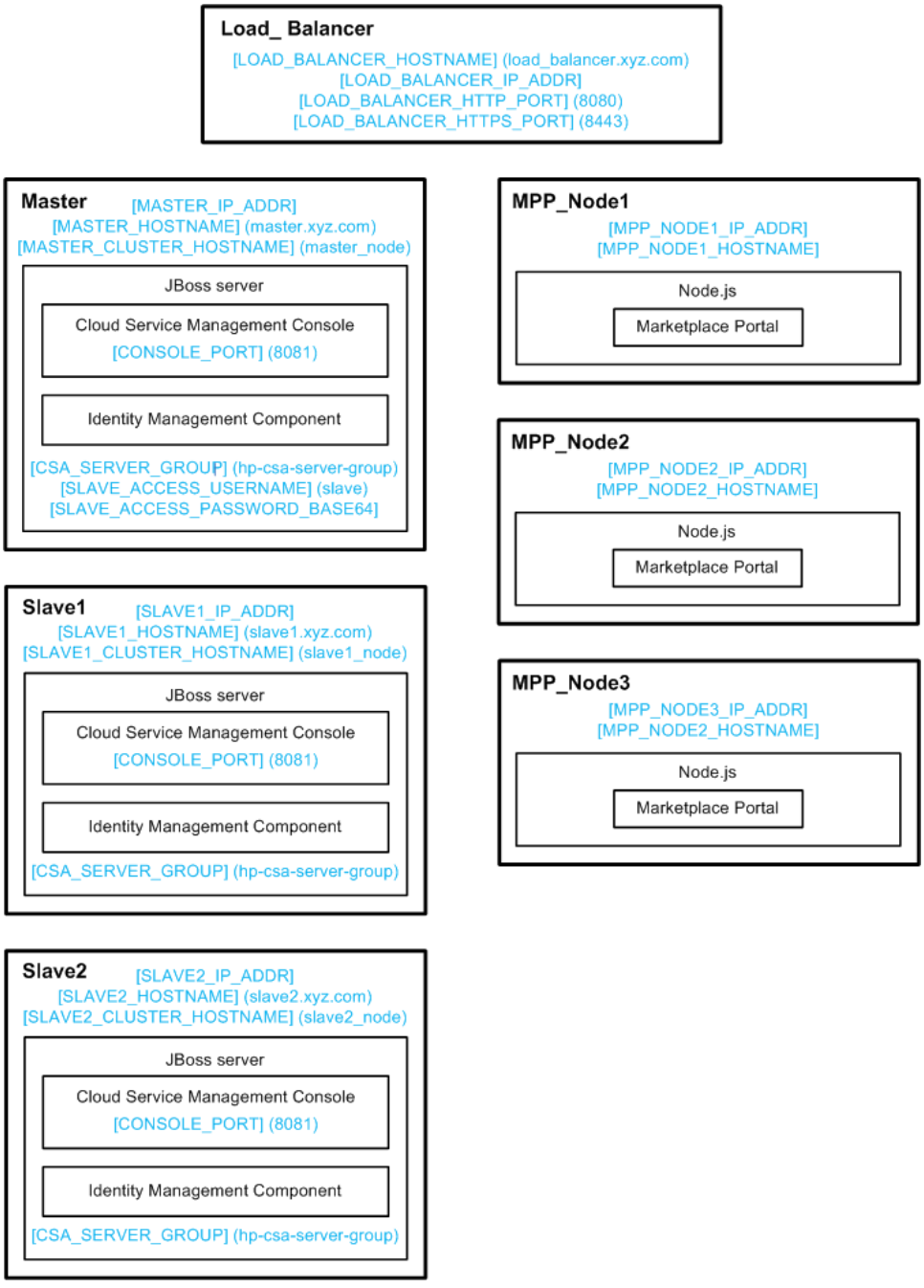


Figure 1-4. Example Values for Example Cluster Configuration

The user who sets up the nodes should have knowledge of or work with someone who has knowledge of HP CSA, HP Operations Orchestration, load balancers, JBoss, and resource providers that will be integrated with HP CSA.

General Notes about Configuring a Clustered Environment

The following information should be considered when configuring a clustered environment:

- It is recommended that you install and configure the nodes in the order presented in this guide. There are some tasks that are dependent on this order (such as generating SSL certificates and importing them).

  Install and configure the load balancer node first. Follow the manufacturer's recommendations to install and configure the load balancer.

- The system time among all nodes in the cluster must be synchronized. If the time is not synchronized, users may experience problems such as not being able to log in to the Marketplace Portal.

- HP CSA must be installed in the same directory on all nodes. Some file locations are hardcoded in configuration files and, if these file locations do not match among nodes, HP CSA fails to start.

Chapter 2: Configure the Load Balancer Node

Install and configure the load balancer on the load balancer node before setting up the HP CSA cluster configured for high availability.

Install and Configure the Load Balancer

Install and configure the load balancer following the manufacturer's recommendations. When configuring the load balancer, configure the sticky bit to enable sticky sessions. This is required for session persistence between the load balancer and the Marketplace Portal in a clustered environment.

Generate the SSL Certificate

If you will be using SSL to communicate between the load balancer and HP CSA or between the load balancer and Marketplace Portal, you will need to generate the load balancer's SSL certificate (in this document, it will be referred to as `load_balancer.crt`). Copy and import this SSL certificate into the keystore on each of the HP CSA and Marketplace Portal nodes.

When configuring HP CSA, if you intend to refer to the load balancer system by its IP address rather than its fully-qualified domain name, you must generate the SSL certificate with the `Subject Alt Name` attribute set to the IP address of the load balancer system.

Start the Load Balancer

You can start the load balancer now (following the manufacturer's recommendations) or after configuring the HP CSA cluster.

Chapter 3: Configure the Master Node

This chapter describes how to install HP CSA on and configure the master node in an HP CSA cluster configured for high availability.

The master node consists of:

- HP CSA
- Identity Management component

Install HP CSA on the Master Node

Install HP CSA as described in the *HP Cloud Service Automation Installation Guide* with the following exceptions:

- When selecting a location in which to install HP CSA on the master node, select the same location in which you installed or will be installing HP CSA on the slave nodes.
- When asked to install HP CSA database components and create the database schema, on the master node, click **Yes**.

  Note: Both the master and slave nodes must connect to the same database schema. Create the schema when you install HP CSA on the master node. Then, you do not need to create the schema when you install HP CSA on the slave node.

- When configuring HP Operations Orchestration, during the configuration of the **CSA_REST_URI** System Property setting, set the **Property Value** to https://*[LOAD_BALANCER_HOSTNAME]*:*[LOAD_BALANCER_HTTPS_PORT]*/csa/rest.
- When integrating with HP Operations Orchestration, you must configure SSL between HP Operations Orchestration and the master and slave nodes. Refer to the *HP Cloud Service Automation Configuration Guide* for complete information about integrating HP CSA with HP Operations Orchestration.

The *HP Cloud Service Automation Installation Guide* can be downloaded from the HP Software Support Web site at http://h20230.www2.hp.com/selfsolve/manuals/ (this site requires that you register with HP Passport).

Configure HP CSA on the Master Node

Complete the tasks in the following sections to configure HP CSA on the master node.

Edit csa.properties on the Master Node

Edit the `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/csa.war/WEB-INF/classes/csa.properties` file:

1. Update the following property values to route requests to the Cloud Service Management Console through the load balancer and set the mode in which HP CSA is running:

   ```
   csa.provider.hostname=[LOAD_BALANCER_HOSTNAME]
   csa.provider.port=[LOAD_BALANCER_HTTPS_PORT]
   csa.provider.rest.protocol=https
   deploymentMode=clustered
   ```

   For example:

   ```
   csa.provider.hostname=load_balancer.xyz.com
   csa.provider.port=8443
   csa.provider.rest.protocol=https
   deploymentMode=clustered
   ```

   Note: If you set the `csa.provider.hostname` attribute to the IP address of the system on which the load balancer is installed, the `Subject Alt Name` attribute of the load balancer's SSL certificate that has been imported into HP CSA's keystore must also be set to the IP address of the system on which the load balancer is installed. If the load balancer's SSL certificate does not contain the `Subject Alt Name` attribute or it is not set to the IP address of the system on which the load balancer is installed, you must regenerate and re-import the load balancer's SSL certificate with the `Subject Alt Name` attribute set to the IP address of the system on which the load balancer is installed.

2. Open the `$CSA_HOME/jboss-as-7.1.1.Final/standalone/deployments/csa.war/WEB-INF/classes/csa.properties` file in a text editor and locate the `csaTruststore` and `csaTruststorePassword` properties and values.

3. Open the `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/csa.war/WEB-INF/classes/csa.properties` file in a text editor and locate the `csaTruststore` and `csaTruststorePassword` properties (these properties are not configured).

4. Copy the values from the first file to the `csaTruststore` and `csaTruststorePassword` properties in the second file.

   For more information about these properties, refer to the *HP Cloud Service Automation Configuration Guide*.

5. Save and exit the file.

Remove the Security Restraint on the Master Node

Remove or comment out the following security constraint block from the `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/csa.war/WEB-INF/web.xml` file:

```
 <security-constraint>
  <web-resource-collection>
    ... ...
    ... ...
  </web-resource-collection>
  <user-data-constraint>
    ... ...
  </user-data-constraint>
</security-constraint>
```

This disables SSL communication between JBoss nodes.

Configure Hosts on the Master Node

Edit the `$CSA_HOME/jboss-as-7.1.1.Final/domain/configuration/host.xml` file and make the following changes:

1. Specify a name that uniquely identifies this host in the cluster.

   ```
   <host name="master_node" xmlns="urn:jboss:domain:1.2">
      ... ...
   </host>
   ```

2. Ensure that this host is configured as the domain controller.

   ```
   <domain-controller>
      <local/>
   </domain-controller>
   ```

3. Configure interfaces:

   ```
   <interfaces>
      <interface name="management">
         <inet-address value="${jboss.bind.address.management:[MASTER_IP_ADDR]}
   "/>
      </interface>
      <interface name="public">
         <inet-address value="${jboss.bind.address:[MASTER_IP_ADDR]}"/>
      </interface>
      <interface name="unsecure">
         <inet-address value="${jboss.bind.address.unsecure:[MASTER_IP_ADDR]}"/>

      </interface>
   </interfaces>
   ```

Refer to the JBoss AS 7 Admin Guide (https://docs.jboss.org/author/display/AS71/Management+tasks) for additional information about configuring interfaces. For example, if you have multiple network interfaces on your host, use the IPv4 wildcard address <any-ipv4-address/> in `host.xml` for the "management" interface as follows:

```
<interfaces>
   <interface name="management">
      <any-ipv4-address/>
   </interface>
   ... ...
</interfaces>
```

Configure Users on the Master Node

You must configure at least two users in the ManagementRealm of the JBoss server on the master node. For each slave node in the clustered environment, you must configure a unique user that allows the slave node to connect to the master node. You must also create a user who can access the JBoss Management Web interface.

To configure the users:

1. Navigate to `$CSA_HOME/jboss-as-7.1.1.Final/bin` and run the `add-user.sh` script.
2. When prompted, create a Management User in the ManagementRealm that uniquely identifies the slave node and is used by the slave node to join the cluster. This user is referred to as *[SLAVE_ACCESS_USERNAME]* in examples in this guide.
3. Specify a password for this user. After you've configured the user and password, encode the password in a base64 format. This password is referred to as *[SLAVE_ACCESS_PASSWORD_BASE64]* in examples in this guide.
4. For each additional slave node in the cluster, run the script to create a unique Management User and password for that node and encode the password in a base64 format.
5. Run the script again to create another Management User in the ManagementRealm named "admin" or "csaadmin". You can use this user to access the JBoss Management Web interface.

Request a Software License

HP CSA version 4.10 requires a software license. HP CSA licensing is based on the number of operating system instances (OSIs) being used in current, active subscriptions.

After initial installation of HP CSA version 4.10, when you log in to the Cloud Service Management Console, a temporary 90-day trial license is activated. Once the trial license expires, you are limited to 25 OSIs. If you created more than 25 OSIs during the trial period, you cannot create any additional OSIs. You can add more licenses at any time to increase your OSI capacity.

After upgrade to HP CSA version 4.10, when you log in to the Cloud Service Management Console, all HP CSA version 4.x licenses are valid and are automatically added.

Note: HP CSA version 4.10 licenses are not compatible with HP CSA version 4.x. That is, you cannot add HP CSA version 4.10 licenses to HP CSA version 4.x.

When you request a software license, you must supply the IP address of the system on which HP CSA is installed. In a clustered environment, use the IP address of the load balancer ([LOAD_BALANCER_IP_ADDR]) when requesting a software license. The license should be installed on only one node in the clustered environment.

For more information on managing software licenses, refer to the *HP Cloud Service Automation Configuration Guide*. For information on how to view, add, or delete a license, refer to the HP Cloud Service Management Console Help.

Share Filesystem Resources

Configure HP CSA to share filesystem resources to free up disk space (this task is optional). Static filesystem resources, such as images, can be stored on one system and shared by all nodes in the cluster. The following example shows how to share the `images` directory that is installed with each instance of HP CSA.

HP CSA provides images that are stored in an `images` directory (for example, `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/csa.war/images`). From the Cloud Service Management Console, you may also upload images which are saved to the same `images` directory. You can store these images on a shared filesystem on a network and the images on this single shared filesystem can be used by all nodes in the cluster.

To configure HP CSA to use a shared filesystem to store images, do the following:

1. Create a shared filesystem on the network. The master and slave nodes must be able to read and write to the shared location.
2. Move the contents of the `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/csa.war/images` directory to the shared location (for example, move the files to `//<SharedFilesystem>/CSAImages`).
3. On the master node, log in as root.
4. If it exists, delete the `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/csa.war/images` directory.
5. Create a credentials file to store the shared filesystem user login information. For example, create `/etc/.win-mnt-cred` and add the following lines:

   ```
   username=<SharedFilesystemUser>
   password=<SharedFilesystemPassword>
   ```

6. Change the permissions of the credentials file. Type the following:

   ```
   chmod 600 /etc/.win-mnt-cred
   ```

7. Edit `/etc/fstab` by adding the following line:

   ```
   //<SharedFilesystem>/CSAImages $CSA_HOME/jboss-as-7.1.1.Final/
   domain/servers/hp-cloud/deployments/csa.war/images cifs credentials=
   /etc/.win-mnt-cred,iocharset=utf8,file_mode=0777,dir_mode=0777,
   uid=csauser,gid=csagrp 0 0
   ```

8. Mount the shared filesystem:

   ```
   mount -a
   ```

Rename Servers on the Master Node

By default, the server installed as part of the setup is named "hp-cloud". Each host on which the application is installed will have this named server. For convenience, if you prefer renaming a server on any of your nodes, you may do so by following the steps listed below. Renaming a server is optional.

1. Edit the `$CSA_HOME/jboss-as-7.1.1.Final/domain/configuration/host.xml` file on the node and update the name attribute to the desired server name. For example:

   ```
   <servers>
      <server name="~~hp-cloud~~[DESIRED_SERVER_NAME]" group="hp-csa-server-group"
   />
      .
      .
      .
   <servers>
   ```

2. Edit the `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/csa.war/WEB-INF/web.xml` file:

   a. Locate the `The file below is used by the HP SSO Framework for the configurations required` comment.

   b. Below this comment, locate the parameter named `com.hp.sw.bto.ast.security.lwsso.conf.fileLocation`, and update the directory path value to use the desired server name. For example, `<param-value>`***[$CSA_HOME]*** `/jboss-as-7.1.1.Final/domain/servers/`~~`hp-cloud`~~***[DESIRED_SERVER_NAME]*** `/deployments/csa.war/WEB-INF/hpssoConfiguration.xml</param-value>`.

3. Rename the `hp-cloud` directory in `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud` to `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/`*`[DESIRED_SERVER_NAME]`*.

Configure Multiple Network Interfaces on the Master Node

Configure the management interface to use multiple network interfaces by using the IPv4 wildcard address. Edit the `$CSA_HOME/jboss-as-7.1.1.Final/domain/configuration/host.xml` file and specify the IPv4 wildcard address <any-ipv4-address/> in the management interface. For example:

```
<interfaces>
   <interface name="management">
      <any-ipv4-address/>
   </interface>
   .
   .
   .
</interfaces>
```

For additional information about configuring interfaces, refer to the JBoss AS 7 Admin Guide (https://docs.jboss.org/author/display/AS71/Management+tasks).

Configure JBoss on the Master Node

Configure JBoss for use in an HP CSA clustered environment by doing the following:

1. Open a window and do the following:

   a. Open the `$CSA_HOME/jboss-as-7.1.1.Final/standalone/configuration/standalone.xml` file in a text editor.

   b. Locate the Web subsystem property (for example, locate `<subsystem xmlns="urn:jboss:domain:web:1.1" default-virtual-server="default-host" native="false">`).

   c. Make a copy of its connector named https (for example, make a copy of `<connector name="https" protocol="HTTP/1.1" scheme="https" secure="true" socket-binding="https">
      <ssl name="ssl" key-alias="CSA" certificate-key-file= "/usr/local/hp/csa/jboss-as-7.1.1.Final/standalone/configuration/.keystore" verify-client="false"/>
   </connector>`).

   d. Note the name and location of the file referenced by the `certificate-key-file` attribute (for example, `/usr/local/hp/csa/jboss-as-7.1.1.Final/standalone/configuration/.keystore`).

2. Open another window and do the following:

   a. Copy the file referenced by the `certificate-key-file` attribute to the `$CSA_HOME/jboss-as-7.1.1.Final/domain/configuration/` directory.

For example, copy `/usr/local/hp/csa/jboss-as-7.1.1.Final/standalone/configuration/.keystore` to `/usr/local/hp/csa/jboss-as-7.1.1.Final/domain/configuration/.keystore`

b. Open the `$CSA_HOME/jboss-as-7.1.1.Final/domain/configuration/domain.xml` file in a text editor.

c. Locate the Web subsystem property (for example, locate `<subsystem xmlns="urn:jboss:domain:web:1.1" default-virtual-server="default-host" native="false">`).

d. Find the connector named http and after it, insert the connector named https that you copied from the `standalone.xml` file. For example:

```
<subsystem xmlns="urn:jboss:domain:web:1.1" default-virtual-
server="default-host" native="false">
   <connector name="http" protocol="HTTP/1.1" scheme="http" socket-
binding="http"/>
   <connector name="https" protocol="HTTP/1.1" scheme="https"
secure="true" socket-binding="https">
      <ssl name="ssl" key-alias="CSA" certificate-key-file=
"/usr/local/hp/csa/jboss-as-
7.1.1.Final/standalone/configuration/.keystore" verify-client="false"/>
   </connector>
   <connector name="ajp" protocol="AJP/1.3" scheme="http" socket-
binding="ajp"/>
. . .
</subsystem>
```

e. Update the content of the connector named https so that the `certificate-key-file` attribute references the file that you copied to the `$CSA_HOME/jboss-as-7.1.1.Final/domain/configuration/` directory in step 2a. For example:

```
<connector name="https" protocol="HTTP/1.1" scheme="https" secure="true" socket-
binding="https">
  <ssl name="ssl" key-alias="CSA" certificate-key-file="/usr/local/hp/csa/jboss-as-
7.1.1.Final/domain/configuration/.keystore" verify-client="false"/>
</connector>
```

f. Update the Web subsystem by adding the `instance-id` attribute to the Web subsystem, if it does not already exist. For example:

```
<subsystem xmlns="urn:jboss:domain:web:1.1" default-virtual-
server="default-host" instance-id="${jboss.node.name}" native="false">
   <connector name="http" protocol="HTTP/1.1" scheme="http" socket-
binding="http"/>
   <connector name="https" protocol="HTTP/1.1" scheme="https"
secure="true" socket-binding="https">
      <ssl name="ssl" key-alias="CSA" certificate-key-file=
"/usr/local/hp/csa/jboss-as-
```

```
7.1.1.Final/standalone/configuration/.keystore" verify-client="false"/>
   </connector>
   <connector name="ajp" protocol="AJP/1.3" scheme="http" socket-
binding="ajp"/>
. . .
</subsystem>
```

g. Save your changes.

Configure SSL on the Master Node

Configure SSL on the master node.

1. If you have not already done so, copy the SSL certificate from the CSA_Proxy node (`load_balancer.crt`) to the `$CSA_HOME/jboss-as-7.1.1.Final/domain/configuration` directory.

2. Import the certificate into the JVM on the master node using the following command:

   Red Hat Enterprise Linux

   ```
   keytool.sh -importcert -file $CSA_HOME/jboss-as-
   7.1.1.Final/domain/configuration/load_balancer.crt -alias load_balancer_csa -
   keystore $CSA_JRE_HOME/lib/security/cacerts
   ```

   Ubuntu Linux

   ```
   keytool.sh -importcert -file $CSA_HOME/jboss-as-
   7.1.1.Final/domain/configuration/load_balancer.crt -alias load_balancer_csa -
   keystore $CSA_JRE_HOME/lib/security/cacerts
   ```

   where *<csa_jre>* `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

Configure the Identity Management Component on the Master Node

Complete the tasks in this section to configure the Identity Management component on the master node.

1. Add the following content to the `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/idm-service.war/WEB-INF/spring/applicationContext.properties` file:

   ```
   idm.csa.hostname = [LOAD_BALANCER_HOSTNAME]
   idm.csa.port = [LOAD_BALANCER_HTTPS_PORT]
   ```

For example:

```
idm.csa.hostname = load_balancer.xyz.com
idm.csa.port = 8443
```

2. In the `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/idm-service.war/WEB-INF/spring/applicationContext-common.xml` file, uncomment or enable the following content:

```
<!--
<property name="clusterEnabled" value="true" />
-->
```

For example:

```
<!--
<property name="clusterEnabled" value="true" />
-->
```

If more detailed configuration is required, the `clusterConfigFile` or `configFile` properties may be set. Refer to the *HP Cloud Service Automation Configuration Guide* for more information about these properties.

3. Edit the following content in the `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/csa.war/WEB-INF/applicationContext-security.xml` file. Update the values of `hostname` to *[LOAD_BALANCER_HOSTNAME]* and `port` to *[LOAD_BALANCER_HTTPS_PORT]*. For example:

```
<beans:bean id="idmConfig"
class="com.hp.ccue.identity.rp.IdentityServiceConfig">
   <beans:property name="protocol" value="https"/>
   <beans:property name="hostname" value="localhostload_balancer.xyz.com"/>
   <beans:property name="port" value="8444448443"/>
   <beans:property name="servicePath" value="idm-service"/> <!-- or hpcloud-
idm-service if you don’t change the name of the WAR -->
   <beans:property name="integrationAcctUserName" value="idmTransportUser"/>
   <beans:property name="integrationAcctPassword"
value="${securityIdmTransportUserPassword}"/>
</beans:bean>
```

Reconfigure the HP CSA Service on the Master Node

By default, the HP CSA service is configured to start, restart, and stop HP CSA in standalone mode. This section shows how to reconfigure the HP CSA service to start, restart, and stop HP CSA in domain mode.

Caution: You must stop the HP CSA service before reconfiguring it.

To reconfigure the HP CSA service to start, restart, and stop HP CSA in domain mode, do the following:

1. Open a command prompt.
2. Stop the `HP Cloud Service Automation` service. Run the following command:

   service csa stop
3. Edit the `$CSA_HOME\scripts\csa_env.conf` file:
   a. Locate the `Toggle below two lines to run CSA in HA mode` comment.
   b. Below this comment, comment out the following line:

      ```
      export CSA_DEPLOOY_MODE=standalone.sh # Standalone Mode
      ```

   c. Uncomment the following line:

      ```
      export CSA_DEPLOY_MODE=domain.sh # HA Mode
      ```
4. Edit the `$CSA_HOME\jboss-as-7.1.1.Final\scripts\csa` file:

   Locate the two occurrences of `--connect command=:shutdown` and replace them with `--connect --controller=<system_hostname>:9999 /host=<unique_host_name>:shutdown`

   where *<system_hostname>* is the IP address or fully-qualified domain name used to identify this system on which HP CSA is running and *<unique_host_name>* is the name that uniquely identifies this host in the cluster and is defined in the `$CSA_HOME/jboss-as-7.1.1.Final/domain/configuration/host.xml` file (for example, master_node or slave_node).
5. Start the HP Cloud Service Automation service in domain mode. Run the following command:

   service csa start

Chapter 4: Configure the Slave Node

This section describes how to install and manually configure the applications needed to set up the slave node in an HP CSA cluster configured for high availability.

The slave node consists of:

- HP CSA
- Identity Management component

Install HP CSA on the Slave Node

Install HP CSA as described in the *HP Cloud Service Automation Installation Guide* with the following exceptions:

- When selecting a location in which to install HP CSA on the slave node, select the same location in which you installed or will be installing HP CSA on the master node.
- When asked to install HP CSA database components and create the database schema, on the slave node, click **No**.

  Note: Both the master and slave nodes must connect to the same database schema. Create the schema when you install HP CSA on the master node. Then, you do not need to create the schema when you install HP CSA on the slave node.

- When configuring HP Operations Orchestration, during the configuration of the **CSA_REST_URI** System Property setting, set the **Property Value** to https://*[LOAD_BALANCER_HOSTNAME]*:*[LOAD_BALANCER_HTTPS_PORT]*/csa/rest.
- When integrating with HP Operations Orchestration, you must configure SSL between HP Operations Orchestration and the master and slave nodes. Refer to the *HP Cloud Service Automation Configuration Guide* for complete information about integrating HP CSA with HP Operations Orchestration.

The *HP Cloud Service Automation Installation Guide* can be downloaded from the HP Software Support Web site at http://h20230.www2.hp.com/selfsolve/manuals/ (this site requires that you register with HP Passport).

Configure HP CSA on the Slave Node

Complete the tasks in the following sections to configure HP CSA on the slave node.

Edit csa.properties on the Slave Node

Edit the `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/csa.war/WEB-INF/classes/csa.properties` file:

1. Update the following property values to route requests to the Cloud Service Management Console through the load balancer and set the mode in which HP CSA is running:

   ```
   csa.provider.hostname=[LOAD_BALANCER_HOSTNAME]
   csa.provider.port=[LOAD_BALANCER_HTTPS_PORT]
   csa.provider.rest.protocol=https
   deploymentMode=clustered
   ```

   For example:

   ```
   csa.provider.hostname=load_balancer.xyz.com
   csa.provider.port=8443
   csa.provider.rest.protocol=https
   deploymentMode=clustered
   ```

   Note: If you set the `csa.provider.hostname` attribute to the IP address of the system on which the load balancer is installed, the `Subject Alt Name` attribute of the load balancer's SSL certificate that has been imported into HP CSA's keystore must also be set to the IP address of the system on which the load balancer is installed. If the load balancer's SSL certificate does not contain the `Subject Alt Name` attribute or it is not set to the IP address of the system on which the load balancer is installed, you must regenerate and re-import the load balancer's SSL certificate with the `Subject Alt Name` attribute set to the IP address of the system on which the load balancer is installed.

2. Open the `$CSA_HOME/jboss-as-7.1.1.Final/standalone/deployments/csa.war/WEB-INF/classes/csa.properties` file in a text editor and locate the `csaTruststore` and `csaTruststorePassword` properties and values.

3. Open the `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/csa.war/WEB-INF/classes/csa.properties` file in a text editor and locate the `csaTruststore` and `csaTruststorePassword` properties (these properties are not configured).

4. Copy the values from the first file to the `csaTruststore` and `csaTruststorePassword` properties in the second file.

   For more information about these properties, refer to the *HP Cloud Service Automation Configuration Guide*.

5. Save and exit the file.

Remove the Security Restraint on the Slave Node

Remove or comment out the following security constraint block from the `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/csa.war/WEB-INF/web.xml` file:

```
 <security-constraint>
  <web-resource-collection>
    ... ...
    ... ...
  </web-resource-collection>
  <user-data-constraint>
    ... ...
  </user-data-constraint>
</security-constraint>
```

This disables SSL communication between JBoss nodes.

Configure Hosts on the Slave Node

Edit the `$CSA_HOME/jboss-as-7.1.1.Final/domain/configuration/host.xml` file and make the following changes:

1. Specify a name that uniquely identifies this host in the cluster. Use one of the Management Users in the ManagementRealm that you created on the master node (for example, [SLAVE_ACCESS_USERNAME]). This name is used to connect the slave node to the master node (join the cluster).

   ```
   <host name="[SLAVE_ACCESS_USERNAME]" xmlns="urn:jboss:domain:1.2">
      ... ...
   </host>
   ```

2. Configure the master node as the domain controller.

   ```
   <domain-controller>
      <remote host="[MASTER_IP_ADDR]" port="9999" security-
   realm="ManagementRealm"/>
   </domain-controller>
   ```

3. Configure interfaces:

   ```
   <interfaces>
      <interface name="management">
         <inet-address value="${jboss.bind.address.management:[SLAVE_IP_ADDR]}
   "/>
      </interface>
      <interface name="public">
         <inet-address value="${jboss.bind.address:[SLAVE_IP_ADDR]}"/>
      </interface>
      <interface name="unsecure">
         <inet-address value="${jboss.bind.address.unsecure:[SLAVE_IP_ADDR]}"/>
   ```

```
      </interface>
   </interfaces>
```

Refer to the JBoss AS 7 Admin Guide (https://docs.jboss.org/author/display/AS71/Management+tasks) for additional information about configuring interfaces. For example, if you have multiple network interfaces on your host, use the IPv4 wildcard address <any-ipv4-address/> in `host.xml` for the "management" interface as follows:

```
<interfaces>
   <interface name="management">
      <any-ipv4-address/>
   </interface>
   ... ...
</interfaces>
```

Configure Authentication Credentials for [SLAVE_ACCESS_USERNAME] on the Slave Node

When configuring the master node, you configured a Management User in the ManagementRealm (for example, *[SLAVE_ACCESS_USERNAME]*) that allows the slave node to connect to the master node and is also used to uniquely identify the slave node (as configured in the previous section). You must also configure the authentication credentials of this user on the slave node so that the slave node can join the cluster.

Edit the `$CSA_HOME/jboss-as-7.1.1.Final/domain/configuration/host.xml` file and make the following changes:

1. Configure the base64 encoded password of the *[SLAVE_ACCESS_USERNAME]* user as the secret identifier:

   ```
   <security-realms>
      <security-realm name="ManagementRealm" >
         <server-identities>
            <secret value="[SLAVE_PASSWORD_BASE64]"/>
         </server-identities>
         <authentication>
            <properties path="mgmt-users.properties" relative-
   to="jboss.domain.config.dir"/>
         </authentication>
      </security-realm>
   </security-realms>
   ```

2. If it exists, comment out or remove the ApplicationRealm. For example:

   ```
   <!--
   <security-realm name="ApplicationRealm">
      <authentication>
         <properties path="application-users.properties" relative-
   ```

```
to="jboss.domain.config.dir" />
   </authentication>
</security-realm>
-->
```

Share Filesystem Resources

Configure HP CSA to share filesystem resources to free up disk space (this task is optional). If you have not done so already, configure a shared filesystem resource from the master node.

The following example configures the images directory as a shared filesystem, using the shared images directory that you set up when you configured the master node (`$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/csa.war/images`).

To configure HP CSA to use a shared filesystem to store images, do the following:

1. On the slave node, log in as root.
2. If it exists, delete the `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/csa.war/images` directory.
3. Create a credentials file to store the shared filesystem user login information. For example, create `/etc/.win-mnt-cred` and add the following lines:

   ```
   username=<SharedFilesystemUser>
   password=<SharedFilesystemPassword>
   ```

4. Change the permissions of the credentials file. Type the following:

   ```
   chmod 600 /etc/.win-mnt-cred
   ```

5. Edit `/etc/fstab` by adding the following line:

   ```
   //<SharedFilesystem>/CSAImages $CSA_HOME/jboss-as-7.1.1.Final/
   domain/servers/hp-cloud/deployments/csa.war/images cifs credentials=
   /etc/.win-mnt-cred,iocharset=utf8,file_mode=0777,dir_mode=0777,
   uid=csauser,gid=csagrp 0 0
   ```

6. Mount the shared filesystem:

   ```
   mount -a
   ```

Rename Servers on the Slave Node

By default, the server installed as part of the setup is named "hp-cloud". Each host on which the application is installed will have this named server. For convenience, if you prefer renaming a server on any of your nodes, you may do so by following the steps listed below. Renaming a server is optional.

1. Edit the `$CSA_HOME/jboss-as-7.1.1.Final/domain/configuration/host.xml` file on the node and update the name attribute to the desired server name. For example:

```
<servers>
   <server name="~~hp-cloud~~[DESIRED_SERVER_NAME]" group="hp-csa-server-group"
/>
   .
   .
   .
<servers>
```

2. Edit the `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/csa.war/WEB-INF/web.xml` file:

   a. Locate the `The file below is used by the HP SSO Framework for the configurations required` comment.

   b. Below this comment, locate the parameter named `com.hp.sw.bto.ast.security.lwsso.conf.fileLocation`, and update the directory path value to use the desired server name. For example, `<param-value>`***[$CSA_HOME]*** `/jboss-as-7.1.1.Final/domain/servers/`~~`hp-cloud`~~***[DESIRED_SERVER_NAME]*** `/deployments/csa.war/WEB-INF/hpssoConfiguration.xml</param-value>`.

3. Rename the `hp-cloud` directory in `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud` to `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/`*`[DESIRED_SERVER_NAME]`*.

Configure Multiple Network Interfaces on the Slave Node

Configure the management interface to use multiple network interfaces by using the IPv4 wildcard address. Edit the `$CSA_HOME/jboss-as-7.1.1.Final/domain/configuration/host.xml` file and specify the IPv4 wildcard address <any-ipv4-address/> in the management interface. For example:

```
<interfaces>
   <interface name="management">
      <any-ipv4-address/>
   </interface>
   .
   .
   .
</interfaces>
```

For additional information about configuring interfaces, refer to the JBoss AS 7 Admin Guide (https://docs.jboss.org/author/display/AS71/Management+tasks).

Configure JBoss on the Slave Node

Configure JBoss for use in an HP CSA clustered environment by doing the following:

1. Open a window and do the following:

   a. Open the `$CSA_HOME/jboss-as-7.1.1.Final/standalone/configuration/standalone.xml` file in a text editor.

   b. Locate the Web subsystem property (for example, locate `<subsystem xmlns="urn:jboss:domain:web:1.1" default-virtual-server="default-host" native="false">`).

   c. Make a copy of its connector named https (for example, make a copy of
   ```
   <connector name="https" protocol="HTTP/1.1" scheme="https" secure="true" socket-binding="https">
      <ssl name="ssl" key-alias="CSA" certificate-key-file="/usr/local/hp/csa/jboss-as-7.1.1.Final/standalone/configuration/.keystore" verify-client="false"/>
   </connector>
   ```
).

   d. Note the name and location of the file referenced by the `certificate-key-file` attribute (for example, `/usr/local/hp/csa/jboss-as-7.1.1.Final/standalone/configuration/.keystore`).

2. Open another window and do the following:

   a. Copy the file referenced by the `certificate-key-file` attribute to the `$CSA_HOME/jboss-as-7.1.1.Final/domain/configuration/` directory.

   For example, copy `/usr/local/hp/csa/jboss-as-7.1.1.Final/standalone/configuration/.keystore` to `/usr/local/hp/csa/jboss-as-7.1.1.Final/domain/configuration/.keystore`

   b. Open the `$CSA_HOME/jboss-as-7.1.1.Final/domain/configuration/domain.xml` file in a text editor.

   c. Locate the Web subsystem property (for example, locate `<subsystem xmlns="urn:jboss:domain:web:1.1" default-virtual-server="default-host" native="false">`).

   d. Find the connector named http and after it, insert the connector named https that you copied from the `standalone.xml` file. For example:

   ```
   <subsystem xmlns="urn:jboss:domain:web:1.1" default-virtual-server="default-host" native="false">
      <connector name="http" protocol="HTTP/1.1" scheme="http" socket-binding="http"/>
      <connector name="https" protocol="HTTP/1.1" scheme="https" secure="true" socket-binding="https">
         <ssl name="ssl" key-alias="CSA" certificate-key-file="/usr/local/hp/csa/jboss-as-7.1.1.Final/standalone/configuration/.keystore" verify-client="false"/>
      </connector>
   ```

```
   <connector name="ajp" protocol="AJP/1.3" scheme="http" socket-
binding="ajp"/>
. . .
</subsystem>
```

e. Update the content of the connector named https so that the `certificate-key-file` attribute references the file that you copied to the `$CSA_HOME/jboss-as-7.1.1.Final/domain/configuration/` directory in step 2a. For example:

```
<connector name="https" protocol="HTTP/1.1" scheme="https" secure="true" socket-
binding="https">
  <ssl name="ssl" key-alias="CSA" certificate-key-file="/usr/local/hp/csa/jboss-as-
7.1.1.Final/domain/configuration/.keystore" verify-client="false"/>
</connector>
```

f. Update the Web subsystem by adding the `instance-id` attribute to the Web subsystem, if it does not already exist. For example:

```
<subsystem xmlns="urn:jboss:domain:web:1.1" default-virtual-
server="default-host" instance-id="${jboss.node.name}" native="false">
   <connector name="http" protocol="HTTP/1.1" scheme="http" socket-
binding="http"/>
   <connector name="https" protocol="HTTP/1.1" scheme="https"
secure="true" socket-binding="https">
      <ssl name="ssl" key-alias="CSA" certificate-key-file=
"/usr/local/hp/csa/jboss-as-
7.1.1.Final/standalone/configuration/.keystore" verify-client="false"/>
   </connector>
   <connector name="ajp" protocol="AJP/1.3" scheme="http" socket-
binding="ajp"/>
. . .
</subsystem>
```

g. Save your changes.

Import the SSL Certificate on the Slave Node

Import the load balancer's SSL certificate into the JVM truststore.

1. If you have not already done so, copy the SSL certificate (`load_balancer.crt`) that you generated on the load balancer node to the `$CSA_HOME/jboss-as-7.1.1.Final/domain/configuration` directory on the slave node.

2. Import the certificate using the following command:

```
keytool.sh -importcert -file $CSA_HOME/jboss-as-
7.1.1.Final/domain/configuration/load_balancer.crt -alias load_balancer_csa -
keystore $CSA_JRE_HOME/lib/security/cacerts
```

where *<csa_jre>* `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

Configure the Identity Management Component on the Slave Node

Complete the tasks in this section to configure the Identity Management component on the slave node.

1. Add the following content to the `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/idm-service.war/WEB-INF/spring/applicationContext.properties` file:

   ```
   idm.csa.hostname = [LOAD_BALANCER_HOSTNAME]
   idm.csa.port = [LOAD_BALANCER_HTTPS_PORT]
   ```

   For example:

   ```
   idm.csa.hostname = load_balancer.xyz.com
   idm.csa.port = 8443
   ```

2. In the `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/idm-service.war/WEB-INF/spring/applicationContext-common.xml` file, uncomment or enable the following content:

   ```
   <!--
   <property name="clusterEnabled" value="true" />
   -->
   ```

   For example:

   ```
   <!--
   <property name="clusterEnabled" value="true" />
   -->
   ```

   If more detailed configuration is required, the `clusterConfigFile` or `configFile` properties may be set. Refer to the *HP Cloud Service Automation Configuration Guide* for more information about these properties.

3. Edit the following content in the `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/csa.war/WEB-INF/applicationContext-security.xml` file. Update the values of `hostname` to *[LOAD_BALANCER_HOSTNAME]* and `port` to *[LOAD_BALANCER_HTTPS_PORT]*. For example:

   ```
   <beans:bean id="idmConfig"
   class="com.hp.ccue.identity.rp.IdentityServiceConfig">
      <beans:property name="protocol" value="https"/>
      <beans:property name="hostname" value="localhostload_balancer.xyz.com"/>
      <beans:property name="port" value="84448443"/>
   ```

```
   <beans:property name="servicePath" value="idm-service"/> <!-- or hpcloud-
idm-service if you don't change the name of the WAR -->
   <beans:property name="integrationAcctUserName" value="idmTransportUser"/>
   <beans:property name="integrationAcctPassword"
value="${securityIdmTransportUserPassword}"/>
</beans:bean>
```

Reconfigure the HP CSA Service on the Slave Node

By default, the HP CSA service is configured to start, restart, and stop HP CSA in standalone mode. This section shows how to reconfigure the HP CSA service to start, restart, and stop HP CSA in domain mode.

Caution: You must stop the HP CSA service before reconfiguring it.

To reconfigure the HP CSA service to start, restart, and stop HP CSA in domain mode, do the following:

1. Open a command prompt.
2. Stop the `HP Cloud Service Automation` service. Run the following command:

   service csa stop
3. Edit the `$CSA_HOME\scripts\csa_env.conf` file:
   a. Locate the `Toggle below two lines to run CSA in HA mode` comment.
   b. Below this comment, comment out the following line:

      ```
      export CSA_DEPLOOY_MODE=standalone.sh # Standalone Mode
      ```

   c. Uncomment the following line:

      ```
      export CSA_DEPLOY_MODE=domain.sh # HA Mode
      ```
4. Edit the `$CSA_HOME\jboss-as-7.1.1.Final\scripts\csa` file:

   Locate the two occurrences of `--connect command=:shutdown` and replace them with `--connect --controller=<system_hostname>:9999 /host=<unique_host_name>:shutdown`

   where *<system_hostname>* is the IP address or fully-qualified domain name used to identify this system on which HP CSA is running and *<unique_host_name>* is the name that uniquely identifies this host in the cluster and is defined in the `$CSA_HOME/jboss-as-7.1.1.Final/domain/configuration/host.xml` file (for example, master_node or slave_node).

5. Start the HP Cloud Service Automation service in domain mode. Run the following command:

   service csa start

Chapter 5: Configure the Marketplace Portal Node

This section describes how to install and configure the Marketplace Portal node in an HP CSA cluster configured for high availability (for example, MPP_Node1 or MPP_Node2 or MPP_Node3).

To configure the Marketplace Portal, do the following:

- Install the Marketplace Portal
- Configure the Marketplace Portal

Install the Marketplace Portal

Install a remote instance of the Marketplace Portal, as described in the *HP Cloud Service Automation Installation Guide* with the following exceptions:

- When selecting a location in which to install the Marketplace Portal, select the same location for all Marketplace Portal nodes.
- When configuring the HP CSA Host, use the fully-qualified domain name of the Load_Balancer node (for example, load_balancer.xyz.com or *[LOAD_BALANCER_HOSTNAME]*).
- When configuring the HP CSA Port, use the port of the load balancer installed on the Load_ Balancer node (for example, 8443 or *[LOAD_BALANCER_HTTPS_PORT]*).

The *HP Cloud Service Automation Installation Guide* can be downloaded from the HP Software Support Web site at http://h20230.www2.hp.com/selfsolve/manuals/ (this site requires that you register with HP Passport).

Configure the Marketplace Portal

To configure the Marketplace Portal on the Marketplace Portal node, do the following:

1. If you have not done so already, copy the SSL certificate of the load balancer from the Load_ Balancer node (for example, load_balancer.crt) to the `$CSA_HOME/portal/conf/` directory on the Marketplace Portal node.
2. Edit the following content in the `$CSA_HOME/portal/conf/mpp.json` file:
   - For the provider, update the `url` attribute value to use *[LOAD_BALANCER_HOSTNAME]* and *[LOAD_BALANCER_HTTPS_PORT]*. For example:

     ```
     "url": "https://~~hostname:8444~~load_balancer.xyz.com:8443",
     ```

   - For the idmProvider, update the values of the `url` attribute to use *[LOAD_BALANCER_*

HOSTNAME] and *[LOAD_BALANCER_HTTPS_PORT]*, and `returnUrl` to use *[LOAD_BALANCER_HOSTNAME]*, and `ca` to use the location of the SSL certificate of the load balancer. For example:

```
"url": "https://~~hostname:8444~~load_balancer.xyz.com:8443",
"returnUrl": "https://~~hostname~~load_balancer.xyz.com:8089",
"ca": "~~$caPath$~~$CSA_HOME/portal/conf/load_balancer.crt"
```

3. Restart the Marketplace Portal service:

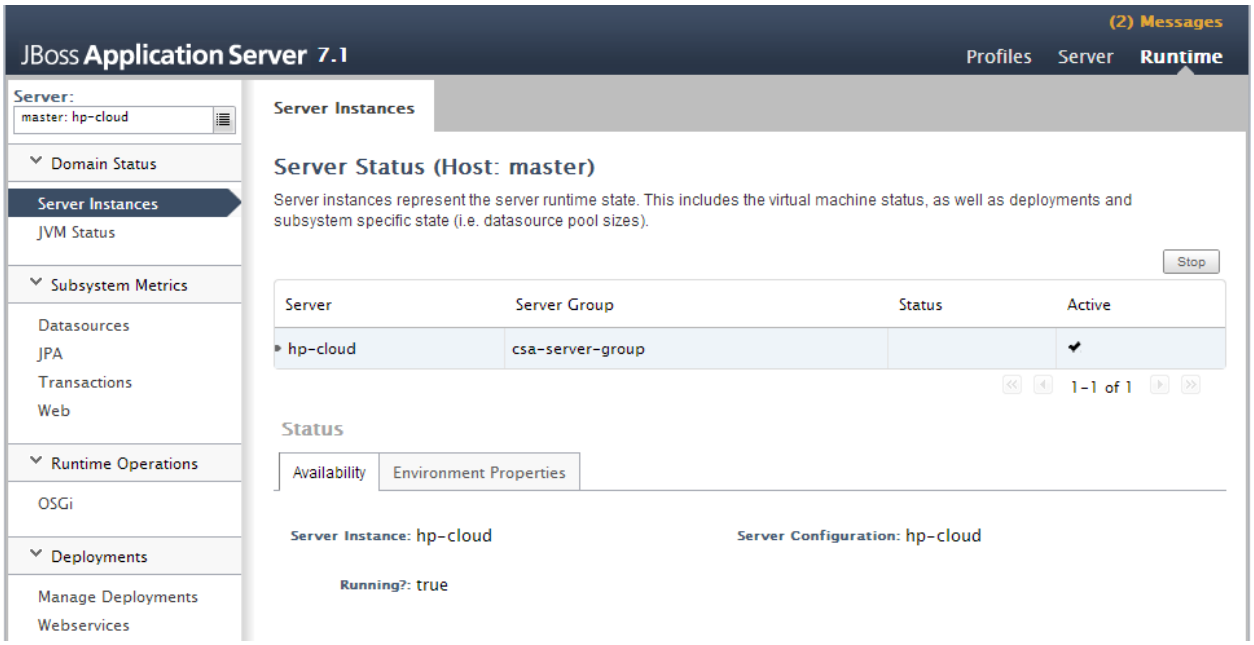
   Open a command prompt and type `service mpp restart`.

Chapter 6: Validate the JBoss Cluster Configuration

The JBoss Application Server provides many management clients, including the Web Management Interface which can be used as a visual tool to validate the cluster setup and if the servers have been deployed on each of the nodes (for more information about additional JBoss Application Server management clients, refer to https://docs.jboss.org/author/display/AS7/Management+Clients). Connect to the Web Management Interface to validate your JBoss cluster configuration.

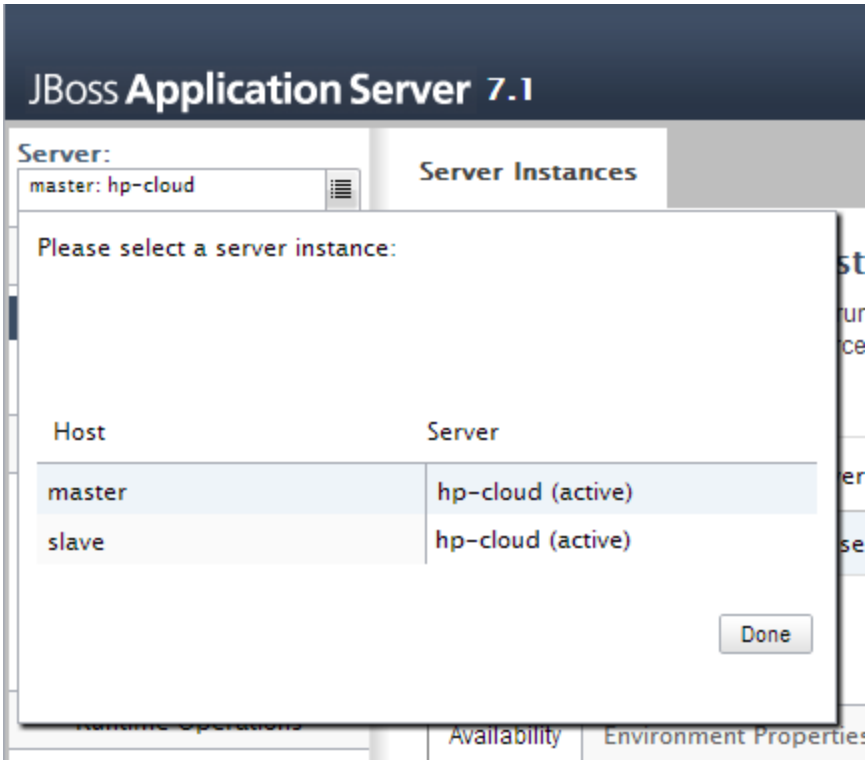
To connect to the Web Management Interface:

1. Open `http://[MASTER_HOSTNAME]:9990/` in a browser.
2. Log in using the JBoss Management Users credentials (username and password) that you created when you configured the master node using the Configuration tool.



3. Click the icon next to the **Server** name to display a list of server instances. Both the master

and slave nodes should be listed with the "hp-cloud" server active on each host.



Chapter 7: Common Tasks

This chapter provides information on how to perform common tasks.

Tasks include:

Start HP CSA in Domain Mode

Caution: If you have not already done so, reconfigure the HP CSA service to start and stop HP CSA in domain mode (you should have completed these steps when you configured the master/slave node). Otherwise, the service will start HP CSA in standalone mode.

To start HP CSA, on the server that hosts HP CSA, type the following:

```
service csa start
```

Stop HP CSA in Domain Mode

Caution: If you have not already done so, reconfigure the HP CSA service to start and stop HP CSA in domain mode (you should have completed these steps when you configured the master/slave node).

To stop HP CSA, on the server that hosts HP Cloud Service Automation, type the following:

```
service csa stop
```

Start the Marketplace Portal

To start Marketplace Portal, on the system that hosts HP CSA, open a command prompt and type `service mpp start`.

Stop the Marketplace Portal

To stop the Marketplace Portal service:

1. On the server that hosts Marketplace Portal, navigate to **Control Panel** > **Administrative Tools** > **Services**.
2. Right-click on the **Marketplace Portal** service and select **Stop**.

To stop Marketplace Portal, on the server that hosts Marketplace Portal, type `service mpp stop`.

Launch the Cloud Service Management Console

To launch the Cloud Service Management Console through the proxy, open one of the following URLs in a supported Web browser:

- `http://[LOAD_BALANCER_HOSTNAME]:[LOAD_BALANCER_HTTP_PORT]/csa`
  For example, `http://load_balancer.xyz.com:8080/csa`
- `https://[LOAD_BALANCER_HOSTNAME]:[LOAD_BALANCER_HTTPS_PORT]/csa`
  For example, `https://load_balancer.xyz.com:8443/csa`

To launch the Cloud Service Management Console directly from the master node, open the following URL in a supported Web browser:

- `http://[MASTER_HOSTNAME]:[CONSOLE_PORT]/csa`
  For example, `http://master.xyz.com:8081/csa`

To launch the Cloud Service Management Console directly from the slave node, open the following URL in a supported Web browser:

- `http://[SLAVE_HOSTNAME]:[CONSOLE_PORT]/csa`
  For example, `http://slave.xyz.com:8081/csa`

Launch the Marketplace Portal

To launch the default Marketplace Portal, open the following URL in a supported Web browser:

- `https://[LOAD_BALANCER_HOSTNAME]:8444/mpp`
  For example, `http://load_balancer.xyz.com:8444/mpp`

The organization associated with the default Marketplace Portal is defined in the `$CSA_HOME/portal/conf/mpp.json` file. By default, this is the sample organization that is installed with HP CSA (CSA_CONSUMER). To modify the organization associated with the default Marketplace Portal, modify the `defaultOrganizationName` property value by setting it to the *<organization_identifier>* of the desired organization, where *<organization_identifier>* is the unique name that HP Cloud Service Automation assigns to the organization, based on the organization display name

(the organization identifier can be found in the General Information section of the **Organizations** tile of the Cloud Service Management Console).

To launch an organization's Marketplace Portal, open one of the following URLs in a supported Web browser:

- `http://[LOAD_BALANCER_HOSTNAME]:[LOAD_BALANCER_HTTP_PORT]/org/<organization_identifier>`
  For example, `http://load_balancer.xyz.com:8080/org/ORGANIZATION_A`
- `https://[LOAD_BALANCER_HOSTNAME]:[LOAD_BALANCER_HTTPS_PORT]/org/<organization_identifier>`
  For example, `http://load_balancer.xyz.com:8443/org/ORGANIZATION_A`

where <*organization_identifier*> is the unique name that HP Cloud Service Automation assigns to the organization, based on the organization display name (the organization identifier can be found in the General Information section of the **Organizations** tile of the Cloud Service Management Console)

Caution: Do not launch more than one organization-specific Marketplace Portal from the same browser session. For example, if you launch ORGANIZATION_A's Marketplace Portal in a browser, do not open a tab or another window from that browser and launch ORGANIZATION_B's Marketplace Portal. Otherwise, the user who has logged in to the Marketplace Portal launched for ORGANIZATION_A will start to see data for ORGANIZATION_B.

Instead, start a new browser session to launch another organization's Marketplace Portal.

Encrypt an HP CSA Password

To encrypt a password:

1. Open a command prompt and change to the `$CSA_HOME/scripts` directory. For example:

   ```
   /usr/local/hp/csa/scripts
   ```

2. Run the following command:

   ```
   $CSA_JRE_HOME/bin/java -jar passwordUtil.jar encrypt <myPassword>
   ```

Identify the Node Running HP CSA Background Services

While Web requests can be serviced by any node in the cluster, HP CSA background services run on a single node in the cluster. The cluster automatically picks a provider for these services. The cluster also ensures that a new provider is selected if an existing one becomes unavailable (for example, when a node crashes).

To identify the provider for background services in the cluster, on each node:

1. Stop HP CSA. See "Stop HP CSA in Domain Mode" on page 38 for more information.
2. Edit the `$CSA_HOME/jboss-as-7.1.1.Final/domain/configuration/domain.xml` file. Add the following to enable INFO-level logging for `com.hp.csa.ha.CSAHASingletonService` in the logging subsystem:

   ```
   <logger category="com.hp.csa.ha.CSAHASingletonService">
      <level name="INFO"/>
   </logger>
   ```

3. Start HP CSA. See "Start HP CSA in Domain Mode" on page 38 for more information.

   After you start individual nodes in domain mode and they join the cluster, you should notice the message, `CSA HA Singleton Service started on this node`, in one (and only one) `$CSA_HOME/jboss-as-7.1.1.Final/domain/log/server.log`. The log file corresponding to the other nodes in the cluster should not display this message. If you notice this message in multiple log files, consider switching to the TCP channel for JGroups communication, as described in the next section. If the node that is selected as the provider goes down, you should immediately see this statement in another log file on the cluster.

Configure the TCP Communication Channel on JGroups

JBoss uses JGroups for communication between nodes in order to establish the cluster and manage membership of nodes in the cluster. By default, the JGroups subsystem on JBoss is configured to communicate through IP multicast messages using UDP. If the environment that you are using to set up the cluster does not support multicast messaging, the JGroups subsystem may alternatively be configured to use multiple TCP unicast messages.

To configure the TCP communication channel on JGroups, update the JGroups subsystem in `$CSA_HOME/jboss-as-7.1.1.Final/domain/configuration/domain.xml` as follows:

```
<subsystem xmlns="urn:jboss:domain:jgroups:1.1" default-stack="tcp">
<!-- change the default stack from udp to tcp -->
  <stack name="udp">
    ... ...
    ... ...
  </stack>
  <stack name="tcp">
    <transport type="TCP" socket-binding="jgroups-tcp" diagnostics-socket-
binding="jgroups-diagnostics"/>
    <!-- Replace MPING with TCPPING -->
    <protocol type="TCPPING">
      <property name="initial_hosts">[MASTER_IP_ADDR][7600],[SLAVE_IP_ADDR]
[7600]</property>
      <property name="port_range">0</property>
    </protocol>
  <!-- Retain the other entries: MERGE2, FD_SOCK through FRAG2 -->
  ... ...
  ... ...
```

```
  </stack>
</subsystem>
```

You should list all the nodes in the cluster using the **initial_hosts** property of TCPPING. Note that a TCP-based channel may be less efficient than its UDP counterpart as the size of the cluster increases beyond four to six nodes.

Chapter 8: Troubleshoot the HP CSA Clustered Environment

This section describes some of the common problems you may encounter while configuring your HP CSA clustered environment for high availability. Workarounds are provided, when available. Additional information may be found in the *HP Cloud Service Automation Release Notes*.

Problem

Accessing a Flex-based user interface (such as the Cloud Service Management Console or Marketplace Portal) may generate an error when running in a clustered environment with a load balancer. The following error may appear in the log file:

```
flex.messaging.security.SecurityException: Secure endpoint
'/messagebroker/amfsecure' must be contacted via a secure protocol
```

Cause

The client side traffic is configured as SSL and the load balancer redirects HTTPS traffic to HTTP.

Workaround

Make the following changes on both the master and slave nodes:

In the `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/csa.war/WEB-INF/flex/services-config.xml` file, update the endpoint class value for the `csa-secure-amf` channel to **flex.messaging.endpoints.AMFEndpoint**. If you have configured a load balancer in a standalone environment and have encountered this problem, update the `$CSA_HOME/jboss-as-7.1.1.Final/standalone/deployments/csa.war/WEB-INF/flex/services-config.xml` file.

For example, change the following from:

```
<channel-definition id="csa-secure-amf" class="mx.messaging.channels.SecureAMFChannel">
   <endpoint url="https://{server.name}:{server.port}/{context.root}/messagebroker/amfsecure"
class="flex.messaging.endpoints.SecureAMFEndpoint" />
   <properties>
      <add-no-cache-headers>false</add-no-cache-headers>
   </properties>
</channel-definition>
```

to

```
<channel-definition id="csa-secure-amf" class="mx.messaging.channels.SecureAMFChannel">
   <endpoint url="https://{server.name}:{server.port}/{context.root}/messagebroker/amfsecure"
class="~~flex.messaging.endpoints.SecureAMFEndpoint~~flex.messaging.endpoints.AMFEndpoint" />
      <properties>
         <add-no-cache-headers>false</add-no-cache-headers>
      </properties>
</channel-definition>
```

Problem

Nodes that do not belong to the HP CSA clustered environment attempt to join the cluster.

Cause

More than one HP CSA clustered environment is configured in the domain.

Workaround

1. Configure the TCP communication channel on JGroups to define the nodes that belong to the cluster. Refer to the *Configure the TCP Communication Channel on JGroups* section in "Identify the Node Running HP CSA Background Services" on page 40 for more information.

2. In the `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/idmservice.war/WEB-INF/spring/applicationContext-common.xml` file, uncomment or enable the following content:

   ```
   <--
   <name=" clusterConfigFile" value="jgroups.xml" />
   -->
   ```

   For example:

   ```
   <—
   <name=" clusterConfigFile" value="jgroups.xml" />
   —>
   ```

3. In `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/idmservice.war/WEB-INF/classes/`, create the `jgroups.xml` file. This file defines the cluster. Refer to "Example jgroups.xml File" on page 45 for an example of a `jgroups.xml` file.

Appendix A: Example jgroups.xml File

The following is an example of the `jgroups.xml` file, based on the example values shown in the *Overview* chapter. If you copy the content of this example file, you must update the highlighted content with the IP addresses of the nodes in your HP CSA cluster. If you have more than three nodes in your HP CSA cluster, additional content must be added for each node. If you have less than three nodes in your HP CSA cluster, you must remove extraneous content.

```
<config xmlns="urn:org:jgroups"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="urn:org:jgroups file:schema/JGroups-3.2.xsd">
   <TCP bind_addr="${jgroups.tcp.address:[MASTER_IP_ADDRESS]}"
        bind_port="${jgroups.tcp.port:7601}"
        loopback="true"
        port_range="30"
        recv_buf_size="20m"
        send_buf_size="640k"
        max_bundle_size="64k"
        use_send_queues="true"
        enable_diagnostics="false"
        bundler_type="new"
        thread_naming_pattern="pl"
        thread_pool.enabled="true"
        thread_pool.min_threads="2"
        thread_pool.max_threads="30"
        thread_pool.keep_alive_time="60000"
        thread_pool.queue_enabled="true"
        thread_pool.queue_max_size="100"
        thread_pool.rejection_policy="Discard"
        oob_thread_pool.enabled="true"
        oob_thread_pool.min_threads="2"
        oob_thread_pool.max_threads="30"
        oob_thread_pool.keep_alive_time="60000"
        oob_thread_pool.queue_enabled="false"
        oob_thread_pool.queue_max_size="100"
        oob_thread_pool.rejection_policy="Discard"/>

   <TCP bind_addr="${jgroups.tcp.address:[SLAVE1_IP_ADDR]}"
        bind_port="${jgroups.tcp.port:7601}"
        loopback="true"
         .
         .
         .
        oob_thread_pool.rejection_policy="Discard"/>
```

```
    <TCP bind_addr="${jgroups.tcp.address:[SLAVE2_IP_ADDR]}"
         bind_port="${jgroups.tcp.port:7601}"
         loopback="true"
          .
          .
          .
         oob_thread_pool.rejection_policy="Discard"/>

    <TCPPING timeout="3000" initial_hosts="[MASTER_IP_ADDRESS][7601],
             [SLAVE1_IP_ADDR][7601],[SLAVE2_IP_ADDR][7601]"
             port_range="0"
             num_initial_members="2"
             ergonomics="false"/>

    <MERGE2 max_interval="30000"
            min_interval="10000"/>
    <FD_SOCK/>
    <FD timeout="3000"
        max_tries="3"/>
    <VERIFY_SUSPECT timeout="1500"/>
    <pbcast.NAKACK2 use_mcast_xmit="false"
                    xmit_interval="1000"
                    xmit_table_num_rows="100"
                    xmit_table_msgs_per_row="10000"
                    xmit_table_max_compaction_time="10000"
                    max_msg_batch_size="100"/>
    <UNICAST2 stable_interval="5000"
              xmit_interval="500"
              max_bytes="1m"
              xmit_table_num_rows="20"
              xmit_table_msgs_per_row="10000"
              xmit_table_max_compaction_time="10000"
              max_msg_batch_size="100"
              conn_expiry_timeout="0"/>
    <pbcast.STABLE stability_delay="500"
                   desired_avg_gossip="5000"
                   max_bytes="1m"/>
    <pbcast.GMS print_local_addr="false"
                join_timeout="3000"
                view_bundling="true"/>
    <tom.TOA/> <!-- the TOA is only needed for total order transactions-->
    <UFC max_credits="200k"
         min_threshold="0.20"/>
    <MFC max_credits="200k"
         min_threshold="0.20"/>
    <FRAG2 frag_size="60000"/>
    <RSVP timeout="60000"
          resend_interval="500"
          ack_on_delivery="false" />
</config>
```

We appreciate your feedback!

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Configuring an HP CSA Cluster for High Availability Using a Load Balancer (Cloud Service Automation 4.10)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to CSAdocs@hp.com.


Java™
COMPATIBLE