

HP Cloud Service Automation

Software Version: 4.20
Linux operating system

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

Document Release Date: March 2016
Software Release Date: December 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

© Copyright 2010-2016 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

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/hpsupport>

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

- Document Change Notes 5
- Chapter 1: Overview 6
 - Request Flow 8
 - About the Examples 9
 - General Notes about Configuring a Clustered Environment 11
- Chapter 2: Configure the Load Balancer Node 12
 - Install and Configure the Load Balancer 12
 - Generate the Certificate 12
 - Start the Load Balancer 12
- Chapter 3: Configure the HP CSA Node 13
 - Install HP CSA 13
 - Upgrade HP CSA 14
 - Configure HP CSA 16
 - Edit Properties 16
 - Request a Software License 17
 - Configure Marketplace Portal Redirection 18
 - Configure JBoss 18
 - Configure a Secure Connection 20
 - Configure the Identity Management Component 21
 - Reconfigure the HP CSA Service 22
 - Configure the TCP Communication Channel on JGroups 23
 - Configure HP Single Sign-On 25
 - Identify the Node Running HP CSA Background Services 26
 - Share Filesystem Resources 26
- Chapter 4: Configure the Marketplace Portal Node 28
 - Install the Marketplace Portal 28
 - Upgrade the Marketplace Portal 28
 - Configure the Marketplace Portal 29
- Chapter 5: Common Tasks 31

Start HP CSA	31
Stop HP CSA	31
Start the Marketplace Portal	32
Stop the Marketplace Portal	32
Launch the Cloud Service Management Console	32
Launch the Marketplace Portal	32
Chapter 6: Troubleshoot the HP CSA Clustered Environment	34
Send Documentation Feedback	36

Document Change Notes

Description	Date
Initial release of this document with CSA 4.2 MR	December 2014
In the " Configure the TCP Communication Channel on JGroups " on page 23 section, added a new step 4.	February 2016
In the " Configure JBoss " on page 18 section, added new step f in step 2.	March 2016

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 standalone 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.

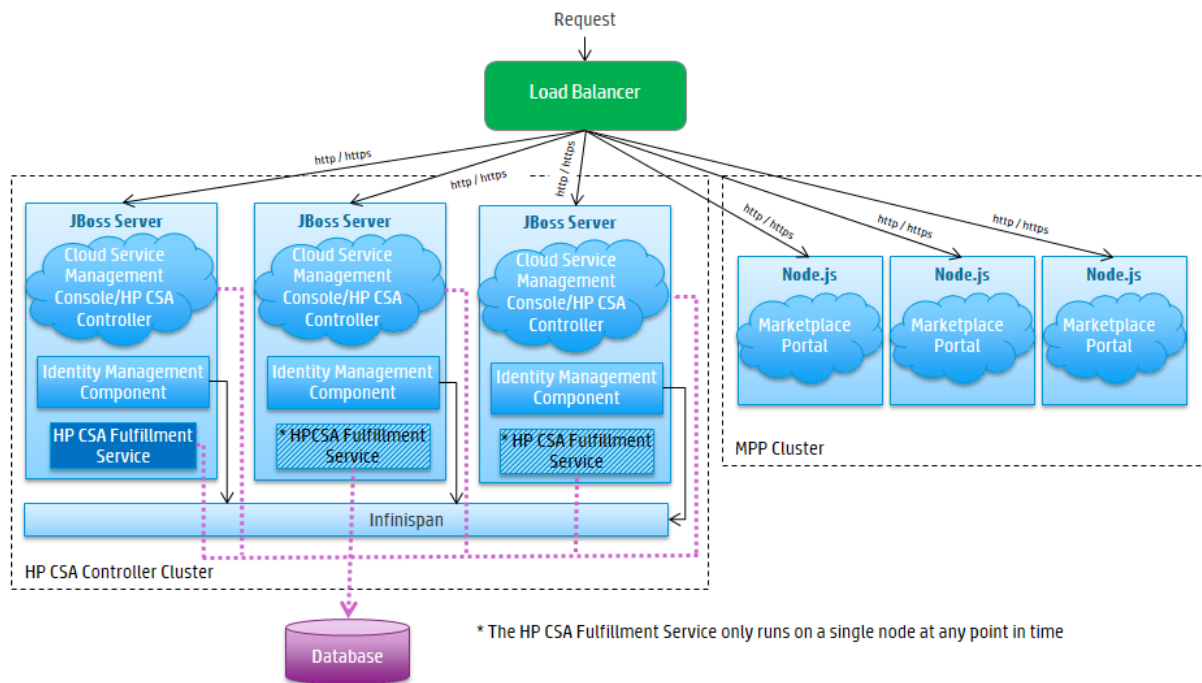


Figure 1-1. Example Cluster Configuration

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 and forwards them to one of the nodes. These nodes are transparent to users and users access only the URL to the load balancer.

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.

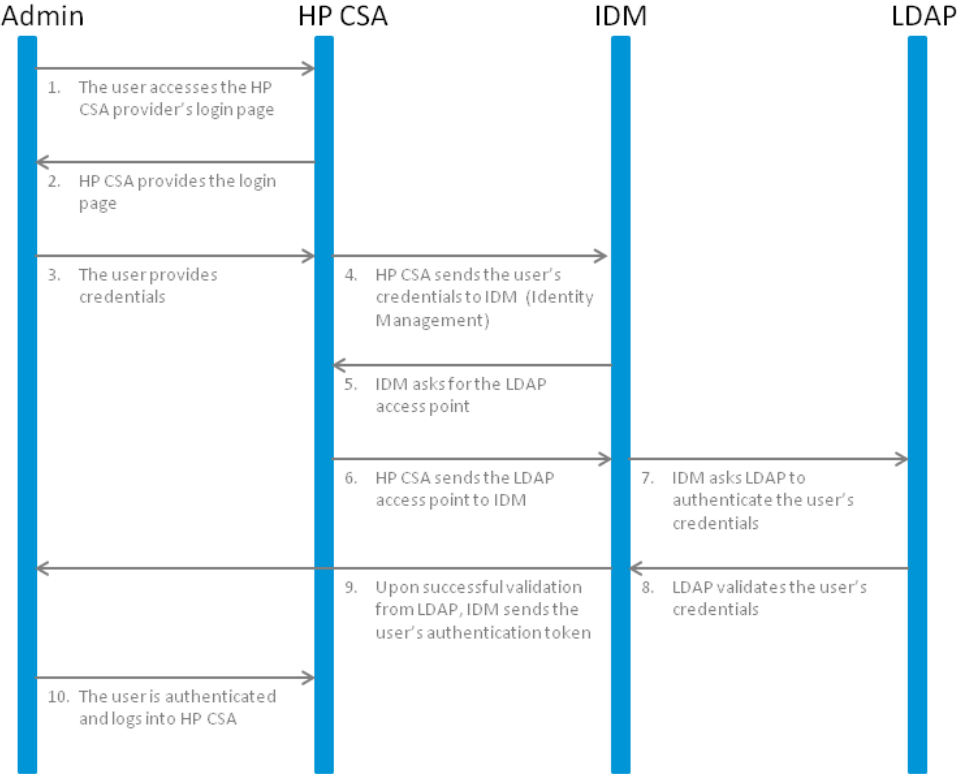


Figure 1-2. Cloud Service Management Console Request Flow

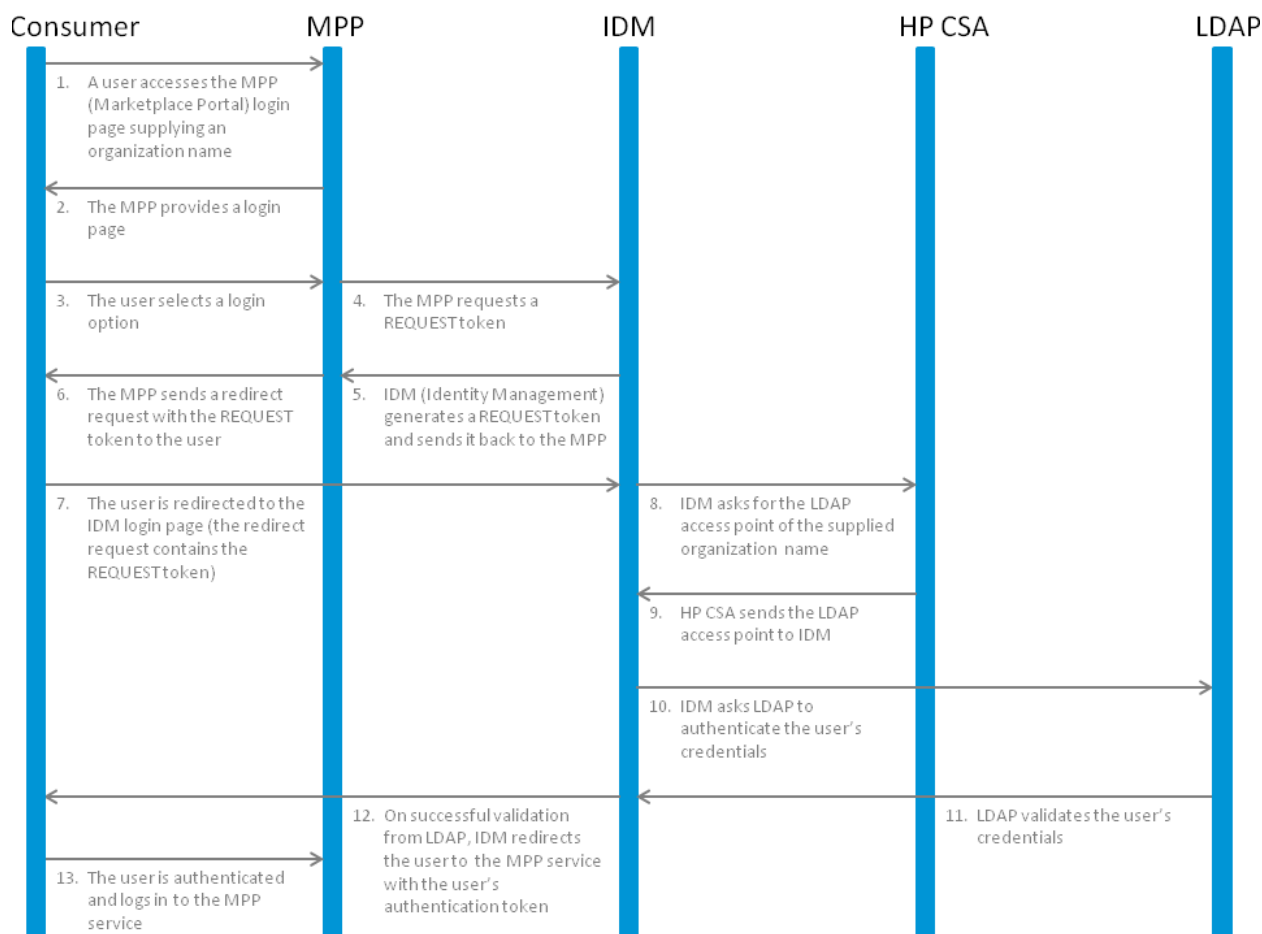


Figure 1-3. Marketplace Portal Request Flow

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
- **CSA_Node 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 "CSA_Node1" node is denoted as [CSA_NODE1_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).

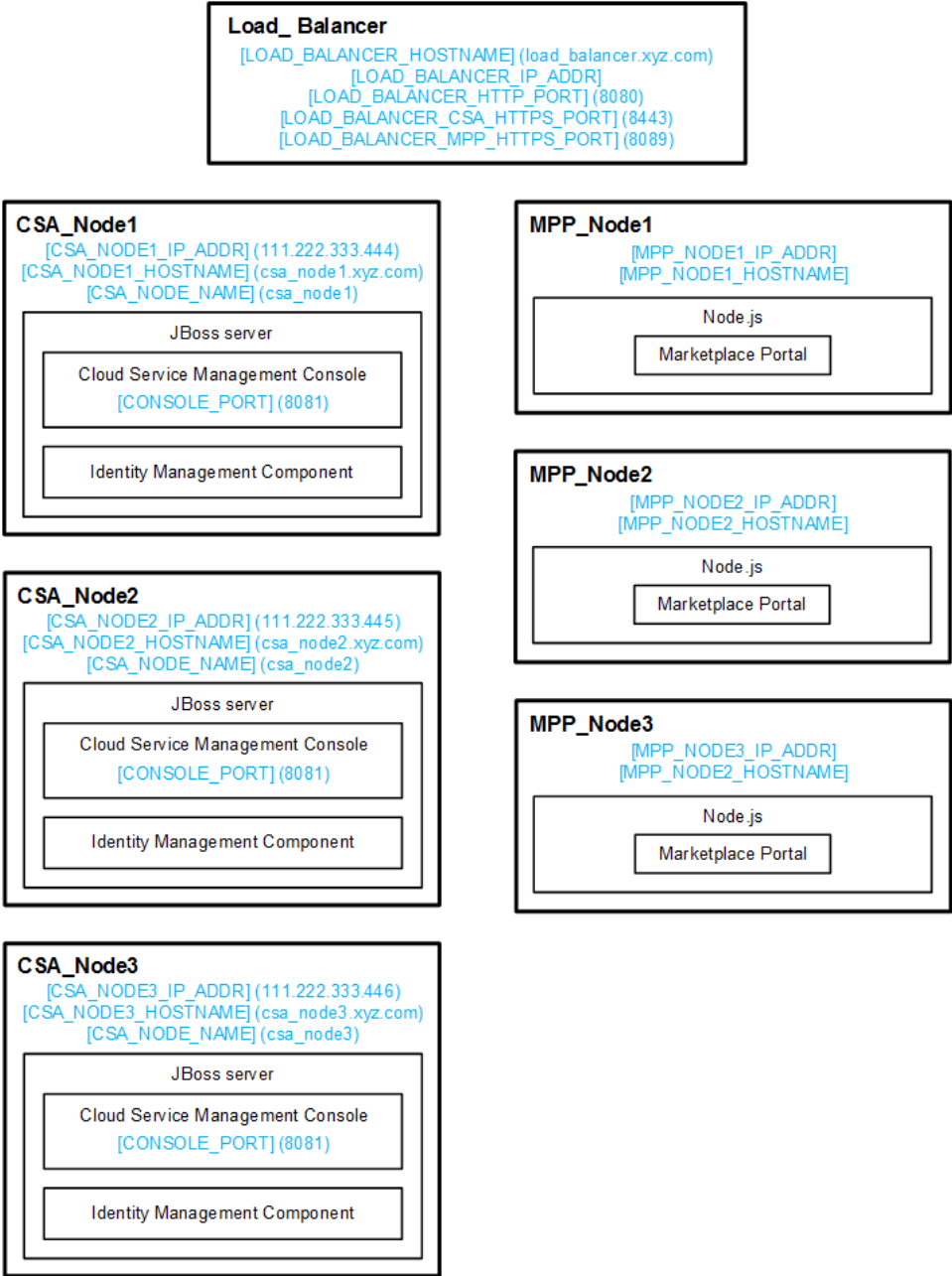


Figure 1-4. Example Values for Example Cluster Configuration

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 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 with the following exceptions:

- When configuring the load balancer, configure sticky sessions. Sticky sessions are required for session persistence between the load balancer and the Marketplace Portal in a clustered environment.
- HP CSA only supports secure connections over TLSv1. The load balancer should be configured for this connection protocol.

Generate the Certificate

If you will be configuring a secure connection (using a protocol such as TLS) to communicate from the load balancer to the HP CSA and Marketplace Portal nodes, you will need to generate the load balancer's certificate (in this document, it will be referred to as `load_balancer.crt`). Copy this certificate to the `$CSA_HOME/jboss-as/standalone/configuration` directory on the HP CSA nodes and to the `$CSA_HOME/portal/conf/` directory on the Marketplace Portal nodes.

Note: 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 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 HP CSA Node

This chapter describes how to install, upgrade, and configure an HP CSA node in an HP CSA cluster configured for high availability (for example, `csa_node1`, `csa_node2`, or `csa_node3`).

The CSA node consists of:

- HP CSA
- Identity Management component

To configure the CSA node, do the following:

- Install or upgrade the HP CSA
- Configure HP CSA

Install HP CSA

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

- You must install the same version of HP CSA on each node (including the Marketplace Portal nodes).
- Install HP CSA in the same location in which you installed or will be installing HP CSA on all CSA nodes.
- Install HP CSA database components and create the database schema for one and only one of the CSA nodes. HP recommends that you create the schema when you install HP CSA on the first CSA node. Then, you do not need to create the schema when you install HP CSA on the other nodes.

Note: All CSA nodes must connect to the same database schema. However, you only need to create the database schema once.

- Use an external (existing) instance of HP Operations Orchestration.

Note: You cannot configure HP CSA in a clustered environment using the embedded HP Operations Orchestration instance.

Note: HP recommends that you install HP Operations Orchestration in its own cluster configured for high availability. Refer to the HP Operations Orchestration documentation for more information.

- You must configure a secure protocol connection (such as TLS) between HP Operations Orchestration and all CSA nodes.
- If you are configuring HP Operations Orchestration for sequential designs, set the **Property Value** of the **CSA_REST_URI** System Property to `https://[LOAD_BALANCER_HOSTNAME]:[LOAD_BALANCER_CSA_HTTPS_PORT]/csa/rest`.

For example:

```
https://load_balancer.xyz.com:8443/csa/rest
```

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).

Upgrade HP CSA

To upgrade HP CSA, on each CSA node, do the following:

1. Upgrade HP CSA as described in the *HP Cloud Service Automation Upgrade Guide* with the following exceptions:
 - Install HP CSA database components and upgrade the database schema on one and only one of the CSA nodes. HP recommends that you upgrade the schema on the first CSA node that you upgrade. Then, you do not need to install HP CSA database components and upgrade the database schema when you upgrade HP CSA on the other CSA nodes.

Note: All CSA nodes must connect to the same database schema. However, you only need to install HP CSA database components and upgrade the database schema once.

- Any customizations you made to the `$CSA_HOME/jboss-as-7.1.1.Final/bin/domain.conf` file must be made to the `$CSA_HOME/jboss-as-7.1.1.Final/bin/standalone.conf` file before running the upgrade installer. The upgrade installer uses the `standalone.conf` file, not the `domain.conf` file.

For example, if you updated the path to the JRE in the `domain.conf` file, make the same changes in the `standalone.conf` file before running the upgrade installer. The upgrade installer will use the JRE defined in the `standalone.conf` file.

The *HP Cloud Service Automation Upgrade 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).

2. Follow the instructions below to configure HP CSA.
3. If you customized any files in the directory or subdirectories of `$CSA_HOME/jboss-as-7.1.1.Final/domain/`, you will need to manually restore these customizations to the equivalent file in the `$CSA_HOME/jboss-as/standalone/` directory.

All files in `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/<server_name>/deployments/*.war` are backed up to `$CSA_HOME/_CSA_4_20_0_installation/Backup/domain/*.war`.

Configure HP CSA

Complete the following tasks to configure HP CSA on each CSA node:

- ["Edit Properties" below](#) (required)
- ["Request a Software License" on the next page](#) (required)
- ["Configure Marketplace Portal Redirection" on page 18](#) (required)
- ["Configure JBoss" on page 18](#) (required)
- ["Configure a Secure Connection" on page 20](#) (required)
- ["Configure the Identity Management Component" on page 21](#) (required)
- ["Reconfigure the HP CSA Service" on page 22](#) (required)
- ["Configure the TCP Communication Channel on JGroups" on page 23](#) (required if multicast messaging is not supported)
- ["Configure HP Single Sign-On" on page 25](#) (required if using HP SSO)
- ["Configure the TCP Communication Channel on JGroups" on page 23](#) (optional)
- ["Share Filesystem Resources" on page 26](#) (optional)

Edit Properties

Update 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.

1. Edit the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/csa.properties`:
 - a. Set the following properties:

```
csa.provider.hostname=[LOAD_BALANCER_HOSTNAME]
csa.provider.port=[LOAD_BALANCER_CSA_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 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 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 certificate with the `Subject Alt Name` attribute set to the IP address of the system on which the load balancer is installed.

- b. Add and set the following property:

```
csa.provider.ip=[LOAD_BALANCER_IP_ADDR]
```

2. Edit the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/swagger.properties` and set the following property:

```
documentation.services.basePath=https://[LOAD_BALANCER_HOSTNAME]:[LOAD_BALANCER_CSA_HTTPS_PORT]/csa/rest
```

For example:

```
documentation.services.basePath=https://load_balancer.xyz.com:8443/csa/rest
```

Request a Software License

HP CSA version 4.20 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 4.20, 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.

When you request a software license, typically you supply the IP address of the system on which HP CSA is installed. However, 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.

Configure Marketplace Portal Redirection

One of the URLs that can be used to launch the Marketplace Portal (for example, `https://load_balancer.xyz.com:8443/mpp`) redirects the request from the JBoss server (the HP CSA controller) to the Node.js server (the Marketplace Portal). By default, the request is redirected to the same system on which HP CSA is installed. However, in a clustered environment, the request must be redirected to the load balancer.

To update the redirection, do the following:

1. Open the `$CSA_HOME/jboss-as/standalone/deployments/mpp.war/index.html` in a text editor.
2. Locate the following line:

```
<meta http-equiv="refresh" content="0;URL= https://[CSA_NODE_HOSTNAME]:[CSA_NODE_HTTPS_PORT]"/>
```

3. Replace `[CSA_NODE_HOSTNAME]` with `[LOAD_BALANCER_HOSTNAME]` and `[CSA_NODE_HTTPS_PORT]` with `[LOAD_BALANCER_MPP_HTTPS_PORT]`. For example:

```
<meta http-equiv="refresh" content="0;URL= https://[LOAD_BALANCER_HOSTNAME]:[LOAD_BALANCER_MPP_HTTPS_PORT]"/>
```

or

```
<meta http-equiv="refresh" content="0;URL= https://load_balancer.xyz.com:8089"/>
```

4. Save and exit the file.

Configure JBoss

Configure JBoss for use in an HP CSA clustered environment:

1. To configure a secure connection between the load balancer and JBoss, open a window and do the following:
 - a. Open the `$CSA_HOME/jboss-as/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 the Web subsystem property's connector named `https` (this content needs to

be added to the `standalone-full-ha.xml` file, which is described in the next step). 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/standalone/configuration/.keystore" verify-
client="false"/>
</connector>).
```

2. Open another window and do the following:

- a. Open the `$CSA_HOME/jboss-as/standalone/configuration/standalone-full-ha.xml` file in a text editor.
- b. If you are configuring a secure connection between the load balancer and JBoss, locate the Web subsystem property (for example, locate `<subsystem xmlns="urn:jboss:domain:web:1.2" default-virtual-server="default-host" native="false">`).
- c. To configure a secure connection between the load balancer and JBoss, 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:1.2" 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/standalone/configuration/.keystore" verify-
client="false"/>
  </connector>
  <connector name="ajp" protocol="AJP/1.3" scheme="http" socket-
binding="ajp"/>
  .
  .
  .
</subsystem>
```

- d. 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:1.2" 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/standalone/configuration/.keystore" verify-  
client="false"/>  
</connector>  
<connector name="ajp" protocol="AJP/1.3" scheme="http" socket-  
binding="ajp"/>  
.  
.  
.  
</subsystem>
```

- e. Locate the server property and configure a unique node name for the node. Locate

```
<server xmlns="urn:jboss:domain:1.3">
```

and set the name to `[CSA_NODE_NAME]`.

For example:

```
<server xmlns="urn:jboss:domain:1.3" name="csa_node1">
```

- f. Add the node's IP address to the public interface. Locate

```
<interface name="public">
```

and add the IP address `[CSA_NODE1_IP_ADDR]`. For example:

```
<interface name="public">  
  <inet-address value="111.222.333.444"/>  
</interface>
```

- g. Save your changes.

Configure a Secure Connection

Configure a secure connection (using a protocol such as TLS) on the CSA node for communication from the load balancer node.

1. If you have not already done so, copy the certificate from the load balancer node (`load_balancer.crt`) to the `$CSA_HOME/jboss-as/standalone/configuration` directory.
2. Import the certificate into the JVM on the CSA node using the following command:

```
$CSA_JRE_HOME/bin/keytool -importcert -file $CSA_HOME/jboss-as/  
standalone/configuration/load_balancer.crt -alias load_balancer_csa  
-keystore $CSA_JRE_HOME/lib/security/cacerts
```

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

Configure the Identity Management Component

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

1. Add the following content to the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/applicationContext.properties` file:

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

For example:

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

2. In the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/applicationContext-common.xml` file, enable clustering by removing the comment tags (`<!--` and `-->`) from the following content:

```
<!--
<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/standalone/deployments/csa.war/WEB-INF/applicationContext-security.xml` file. Update the values of `hostname` to `[LOAD_BALANCER_HOSTNAME]` and `port` to `[LOAD_BALANCER_CSA_HTTPS_PORT]`:

```
<beans:bean id="idmConfig"
class="com.hp.ccue.identity.rp.IdentityServiceConfig">
  <beans:property name="protocol" value="https"/>
  <beans:property name="hostname" value="[LOAD_BALANCER_HOSTNAME]"/>
  <beans:property name="port" value="[LOAD_BALANCER_CSA_HTTPS_PORT]"/>
  <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>
```

For example:

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

```
<beans:property name="hostname" value="load_balancer.xyz.com"/>
<beans:property name="port" value="8443"/>
<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>
```

4. Edit the following content in the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/applicationContext.properties` file. Update the values of `idm.csa.audit.hostname` to `[LOAD_BALANCER_HOSTNAME]` and `idm.csa.audit.port` to `[LOAD_BALANCER_HTTPS_PORT]`:

```
# Properties for CSA Auditing Server
.
.
.
idm.csa.audit.hostname = [LOAD_BALANCER_HOSTNAME]"/>
idm.csa.audit.port = [LOAD_BALANCER_HTTPS_PORT]"/>
```

For example:

```
# Properties for CSA Auditing Server
.
.
.
idm.csa.audit.hostname = load_balancer.xyz.com"/>
idm.csa.audit.port = 8443"/>
```

Reconfigure the HP CSA Service

Reconfigure the HP CSA service to start, restart, and stop HP CSA using the `standalone-full-ha.xml` configuration file.

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

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 `export CSA_DEPLOY_MODE=standalone.sh # Standalone Mode` line:

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

- c. Add the following line:

```
export CSA_DEPLOY_MODE="standalone.sh -c standalone-full-ha.xml  
-u [MULTICAST_ADDRESS]" # HA Mode
```

where `[MULTICAST_ADDRESS]` is the UDP multicast address used by the JGroups subsystem on JBoss for communication between nodes. The JGroups subsystem establishes the cluster and manages membership of nodes in the cluster. Multicast addresses fall in the range between 224.0.0.0 and 239.255.255.255 (for example, 230.0.0.4). All nodes in a cluster must use the same multicast address. If you are configuring more than one cluster in your domain, use a different multicast address for each cluster.

If the environment that you are using to set up the cluster does not support multicast messaging, the JGroups subsystem can be configured to use multiple TCP unicast messages. See ["Configure the TCP Communication Channel on JGroups"](#) below for more information. If you use multiple TCP unicast messages, do not specify the `-u [MULTICAST_ADDRESS]` option in the `csa_env.conf` file.

4. Start the HP Cloud Service Automation service. Run the following command:

```
service csa start
```

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, do the following:

1. Open the `$CSA_HOME/jboss-as/standalone/configuration/standalone-full-ha.xml` file in an editor.
2. Update the `jgroups` subsystem default stack from `udp` to `tcp`. Change

```
<subsystem xmlns="urn:jboss:domain:jgroups:1.1" default-stack="udp">
```

to

```
<subsystem xmlns="urn:jboss:domain:jgroups:1.1" default-stack="tcp">
```

3. Locate the tcp stack and replace

```
<protocol socket-binding="jgroups-mping" type="MPING"/>
```

with

```
<protocol type="TCPPING">  
  <property name="initial_hosts">[LIST_OF_INITIAL_HOSTS]</property>  
  <property name="num_initial_members">[NUMBER_OF_INITIAL_HOSTS]</property>  
  
  <property name="port_range">1</property>  
  <property name="timeout">2000</property>  
</protocol>
```

where:

- *[LIST_OF_INITIAL_HOSTS]* is a comma-separated list of nodes (IP address and port) that define the cluster. It is recommended that all known nodes in the HP CSA controller cluster are listed. Other nodes that are not listed may join the cluster and you may remove a node from the list at any time. However, at least one initial host (a node in the list of initial hosts) must be running in order for other nodes (that are not included in this list) to join the cluster. The more initial hosts listed means that there is a greater chance an initial host is running so that an unlisted node may join the cluster (if no initial hosts are running, no unlisted nodes may join the cluster). Once the cluster is running, if you update the list of initial hosts, all nodes in the cluster must be restarted. The following are examples of a list of three initial hosts: *[CSA_NODE1_IP_ADDR][7600], [CSA_NODE2_IP_ADDR][7600], [CSA_NODE3_IP_ADDR][7600]* or *111.222.333.444[7600], 111.222.333.445[7600], 111.222.333.446[7600]*
- *[NUMBER_OF_INITIAL_HOSTS]* is the number of initial hosts specified in the cluster.

For example:

```
<protocol type="TCPPING">  
  <property name="initial_hosts">111.222.333.444[7600], 111.222.333.445[7600],  
  111.222.333.446[7600]</property>  
  <property name="num_initial_members">3</property>  
  <property name="port_range">1</property>  
  <property name="timeout">2000</property>  
</protocol>
```

A TCP-based channel may be less efficient than its UDP counterpart as the size of the cluster increases beyond four to six nodes.

4. Add the node's IP address to the public interface. Locate:

```
<interface name="public">
```


and add the IP address [CSA_NODE1_IP_ADDR]. For example:

```
<interface name="public">  
    <inet-address value="{jboss.bind.address:<CSA_Node_ip_Address}"/>  
</interface>
```

5. Reconfigure the HP CSA service. In the \$CSA_HOME\scripts\csa_env.conf file:
 - a. Locate the Toggle below two lines to run CSA in HA mode comment.
 - b. Comment out export CSA_DEPLOY_MODE=standalone.sh # Standalone Mode.
 - c. Add export CSA_DEPLOY_MODE="standalone.sh -c standalone-full-ha.xml" # HA Mode.

Note: You do not need to specify the -u [MULTICAST_ADDRESS] option.

Configure HP Single Sign-On

If you have integrated HP Single Sign-On (HP SSO) between HP CSA and another application (such as HP Operations Orchestration), you must configure HP SSO on the CSA node.

1. Open the \$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/hpssoConfiguration.xml file in a text editor.
2. Locate the following content:

```
<onFailure>  
    .  
    .  
    .  
    <action name="redirectToAP">  
        <targetUrl>https://[CSA_NODE_HOSTNAME]:[CSA_NODE_PORT]  
/csa/login</targetUrl>  
    </action>
```

3. Replace [CSA_NODE_HOSTNAME] and [CSA_NODE_PORT] with the load balancer hostname (LOAD_BALANCER_HOSTNAME) and the virtual host port for the HP CSA nodes (LOAD_BALANCER_CSA_HTTPS_PORT). For example:

```
<onFailure>  
    .  
    .  
    .  
    <action name="redirectToAP">  
        <targetUrl>https://load_balancer.xyz.com:8443/csa/login</targetUrl>  
    </action>
```

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" on page 31](#) for more information.
2. Edit the `$CSA_HOME/jboss-as/standalone/configuration/standalone-full-ha.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" on page 31](#) for more information.

After you start individual nodes 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/standalone/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 ["Configure the TCP Communication Channel on JGroups" on page 23](#)). If the node that is selected as the provider goes down, you should immediately see this statement in another log file in the cluster.

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 or JSP files, 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/standalone/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. Move the contents of the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/images` directory to the shared location (for example, move the files to `//<SharedFilesystem>/CSAImages`).

2. On the CSA node, log in as root.
3. If it exists, delete the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/images` directory.
4. 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>
```

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

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

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

```
//<SharedFileSystem>/CSAImages $CSA_HOME/jboss-as/  
standalone/deployments/csa.war/images cifs credentials=  
/etc/.win-mnt-cred,icharset=utf8,file_mode=0777,dir_mode=0777,  
uid=csauser,gid=csagrps 0 0
```

7. Mount the shared filesystem:

```
mount -a
```

Chapter 4: Configure the Marketplace Portal Node

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

To configure the Marketplace Portal, do the following:

- Install or upgrade the Marketplace Portal
- Configure the Marketplace Portal

Install the Marketplace Portal

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

- You must install the same version of HP CSA on each node (including the CSA nodes).
- 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_CSA_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).

Upgrade the Marketplace Portal

Upgrade HP CSA (remote Marketplace Portal) on each Marketplace Portal node as described in the *HP Cloud Service Automation Upgrade Guide* with the following exception:

- Edit the `$CSA_HOME/portal/conf/mpp.json` file. Update the value of the `ha_enabled` property to disable the Marketplace Portal from using the Redis cache server for session persistence. The load balancer will use sticky sessions for session persistence. For example:

```
"ha": {  
  "enabled": false,  
  .
```

.
.

The *HP Cloud Service Automation Upgrade 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 each Marketplace Portal node, do the following:

1. If you have not done so already, copy the 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_CSA_HTTPS_PORT]` and `ca` to use the location of the certificate of the load balancer. For example:

```
"provider": {  
  "url": "https://[LOAD_BALANCER_HOSTNAME]:[LOAD_BALANCER_CSA_HTTPS_PORT]"  
  "ca": "$CSA_HOME/portal/conf/load_balancer.crt"  
  .  
  .  
  .  
},
```

or

```
"provider": {  
  "url": "https://load_balancer.xyz.com:8443"  
  "ca": "$CSA_HOME/portal/conf/load_balancer.crt"  
  .  
  .  
  .  
},
```

- For the `idmProvider`, update the values of the `url` attribute to use `[LOAD_BALANCER_HOSTNAME]` and `[LOAD_BALANCER_CSA_HTTPS_PORT]`, `returnUrl` to use `[LOAD_BALANCER_HOSTNAME]` and `[LOAD_BALANCER_MPP_HTTPS_PORT]`, and `ca` to use the location of the certificate of the load balancer. For example:

```
"idmProvider": {  
  "url": "https://[LOAD_BALANCER_HOSTNAME]:[LOAD_BALANCER_CSA_HTTPS_PORT]",  
  "returnUrl": "https://[LOAD_BALANCER_HOSTNAME]:[LOAD_BALANCER_MPP_HTTPS_
```

```
    PORT]",  
    "ca": "$CSA_HOME/portal/conf/load_balancer.crt"  
    .  
    .  
    .  
  },  
  or  
  "idmProvider": {  
    "url": "https://load_balancer.xyz.com:8443",  
    "returnUrl": "https://load_balancer.xyz.com:8089",  
    "ca": "$CSA_HOME/portal/conf/load_balancer.crt"  
    .  
    .  
    .  
  },
```

3. Restart the Marketplace Portal service:

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

Chapter 5: Common Tasks

This chapter provides information on how to perform common tasks.

Tasks include:

- ["Start HP CSA" below](#)
- ["Stop HP CSA" below](#)
- ["Start the Marketplace Portal" on the next page](#)
- ["Stop the Marketplace Portal" on the next page](#)
- ["Launch the Cloud Service Management Console" on the next page](#)
- ["Launch the Marketplace Portal" on the next page](#)
- ["Identify the Node Running HP CSA Background Services" on page 26](#)

Start HP CSA

Caution: If you have not already done so, [reconfigure the HP CSA service](#) to start and stop HP CSA using the `standalone-full-ha.xml` configuration file (you should have completed these steps when you configured the CSA node).

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

```
service csa start
```

Stop HP CSA

Caution: If you have not already done so, [reconfigure the HP CSA service](#) to start and stop HP CSA using the `standalone-full-ha.xml` configuration file (you should have completed these steps when you configured the CSA 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 Marketplace Portal, on the server that hosts Marketplace Portal, type `service mpp stop`.

Launch the Cloud Service Management Console

Launch the Cloud Service Management Console through the load balancer by opening 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_CSA_HTTPS_PORT]/csa`
For example, `https://load_balancer.xyz.com:8443/csa`

Launch the Marketplace Portal

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

- `https://[LOAD_BALANCER_HOSTNAME]:8443/mpp`
For example, `https://load_balancer.xyz.com:8443/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_MPP_HTTPS_PORT]
/org/<organization_identifier>`
For example, `https://load_balancer.xyz.com:8089/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.

Chapter 6: 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 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 TLS and the load balancer redirects HTTPS traffic to HTTP.

Workaround

Make the following changes on all CSA nodes:

In the `$CSA_HOME/jboss-as/standalone/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**.

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.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 reachable on the same multicast address

Workaround

Do one of the following:

- Use a different multicast address for each clustered environment.
- Configure the TCP communication channel on JGroups to define the nodes that belong to the cluster. Refer to "[Configure the TCP Communication Channel on JGroups](#)" on page 23 for more information.

Send Documentation 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 4.20)

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.

We appreciate your feedback!

