HP Cloud Service Automation

For the Windows ® operating system

Software Version: 4.10

Configuring an HP CSA Cluster for High Availability Using an Apache Web Server as a Proxy

Document Release Date: August 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.

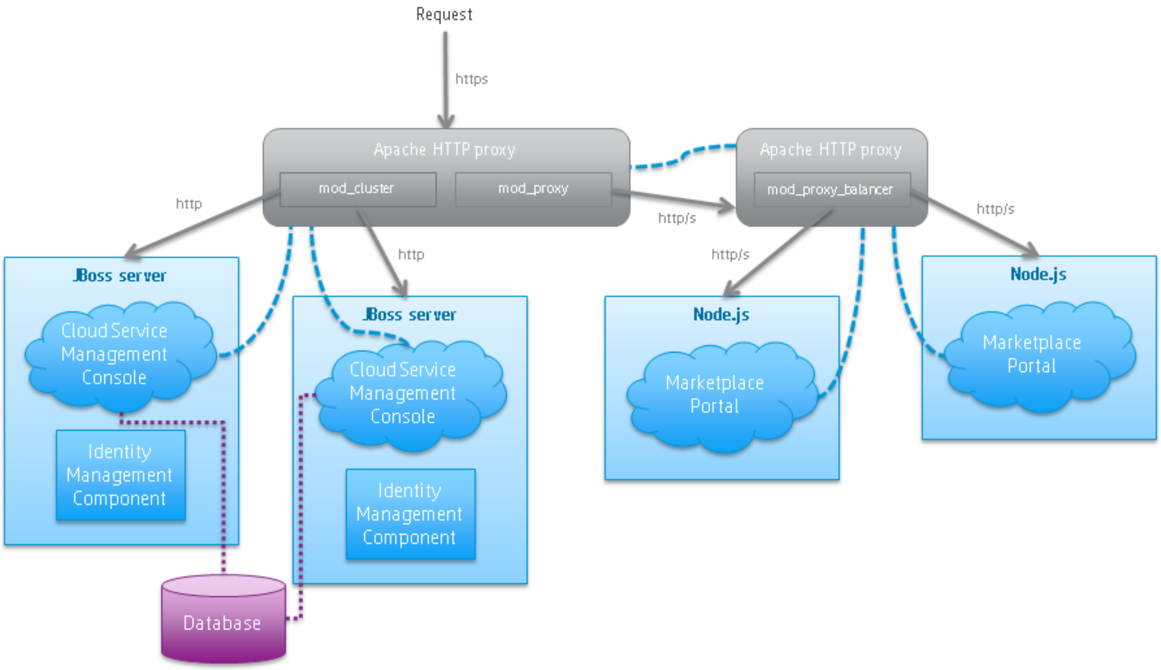
Because clustering distributes the workload across different nodes, if any node fails, HP CSA remains accessible through other nodes in the cluster. You can continue to improve user request throughput by simply adding nodes to the cluster. If a node shuts down, activities such as email notifications 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 this document, a cluster configuration consists of six different physical (or virtual) hosts: two hosts are running HP CSA in domain mode, one host is running an Apache Web server with the mod_cluster module (a software load balancer that is available out-of-the-box from JBoss 7.1.1 and is configured on an Apache HTTP server so that web requests can be proxied into the HP CSA/JBoss cluster), one host is running an Apache Web server with the mod_proxy_balancer module (a software load balancer that is available out-of-the-box from JBoss 7.1.1 and is configured on an Apache HTTP server so that web requests can be proxied into a Node.js cluster for the Marketplace Portal), and two hosts are running the Marketplace Portal. This document does not cover the load balancing features of the mod_cluster or mod_proxy_balancer modules.

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.



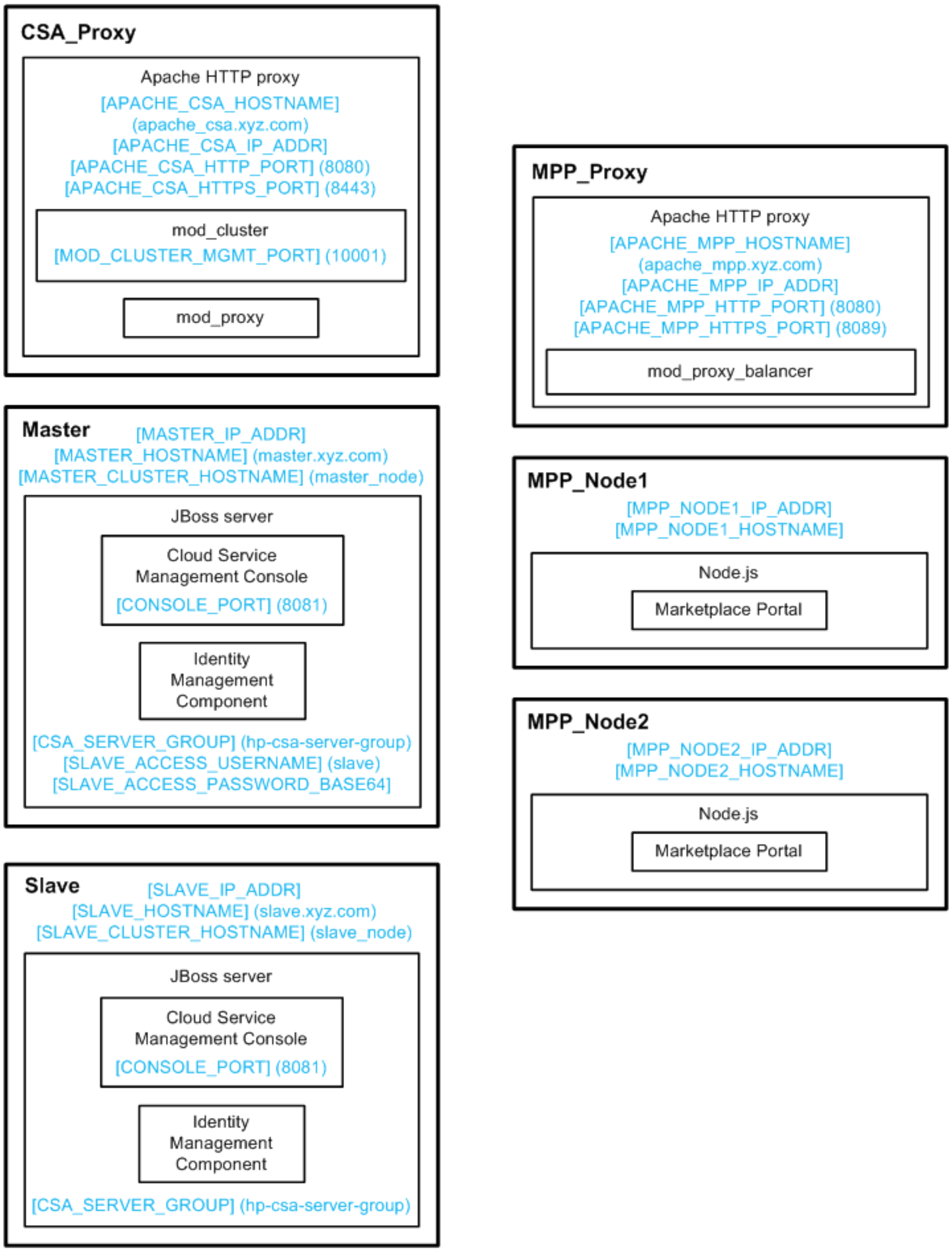
The cluster uses a Web server to distribute requests among any number of nodes and can be useful to an organization that already uses a standard Web server within its network infrastructure. The Web server (internal or external) listens for HTTPS requests from standard interface clients. Nodes are transparent to users and users access only the URL to the Web server. The Web server forwards HTTP requests to one of the other nodes.

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

- **Master node**: hosts HP CSA
- **Slave node**: hosts HP CSA
- **CSA_Proxy node**: the domain controller and hosts the Apache Web server with the mod_cluster module (the master/slave nodes and the CSA_Proxy node communicate using the mod_cluster module)
- **MPP_Node1 node**: hosts the Marketplace Portal
- **MPP_Node2 node**: hosts the Marketplace Portal
- **MPP_Proxy node**: hosts the Apache Web server with the mod_proxy_balancer module (the MPP_Node1/MPP_Node2 nodes and the MPP_Proxy node communicate using the mod_proxy_balancer module)

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).


CSA_Proxy
Apache HTTP proxy
[APACHE_CSA_HOSTNAME]
(apache_csa.xyz.com)
[APACHE_CSA_IP_ADDR]
[APACHE_CSA_HTTP_PORT] (8080)
[APACHE_CSA_HTTPS_PORT] (8443)
mod_cluster
[MOD_CLUSTER_MGMT_PORT] (10001)
mod_proxy
MPP_Proxy
Apache HTTP proxy
[APACHE_MPP_HOSTNAME]
(apache_mpp.xyz.com)
[APACHE_MPP_IP_ADDR]
[APACHE_MPP_HTTP_PORT] (8080)
[APACHE_MPP_HTTPS_PORT] (8089)
mod_proxy_balancer
Master
[MASTER_IP_ADDR]
[MASTER_HOSTNAME] (master.xyz.com)
[MASTER_CLUSTER_HOSTNAME] (master_node)
JBoss server
Cloud Service Management Console
[CONSOLE_PORT] (8081)
Identity Management Component
[CSA_SERVER_GROUP] (hp-csa-server-group)
[SLAVE_ACCESS_USERNAME] (slave)
[SLAVE_ACCESS_PASSWORD_BASE64]
MPP_Node1
[MPP_NODE1_IP_ADDR]
[MPP_NODE1_HOSTNAME]
Node.js
Marketplace Portal
MPP_Node2
[MPP_NODE2_IP_ADDR]
[MPP_NODE2_HOSTNAME]
Node.js
Marketplace Portal
Slave
[SLAVE_IP_ADDR]
[SLAVE_HOSTNAME] (slave.xyz.com)
[SLAVE_CLUSTER_HOSTNAME] (slave_node)
JBoss server
Cloud Service Management Console
[CONSOLE_PORT] (8081)
Identity Management Component
[CSA_SERVER_GROUP] (hp-csa-server-group)

The user who sets up the nodes should have knowledge of or work with someone who has knowledge of HP CSA, HP Operations Orchestration, Apache HTTP server, 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).
- 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.
- If you run the Configuration tool more than once on the CSA_Proxy or MPP_Proxy node, verify that the port settings and virtual host definitions have not been replaced with different ports in the `<path_to>\Apache2.2\conf\httpd.conf` or `<path_to>\Apache2.2\conf\httpds.conf` files and that the ports are defined in the appropriate file.
- When using HP CSA to configure an organization, if you are using the Apache Web server as a load balancer in a clustered environment (as described in this document), do not use a semicolon (;) or plus sign (+) in the organization's name. If one of these characters is present in the organization's name, you may not be able to log in to the Marketplace Portal.

Chapter 2: Install HP CSA on the Master Node

Complete the tasks in the following sections to install HP CSA on the master node (you will configure HP CSA at a later time). If you do not intend to use the Configuration tool to configure the CSA_Proxy and MPP_Proxy nodes, you can install and configure HP CSA on the master node at a later time.

Install HP CSA

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 node.

- 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 you configure HP Operations Orchestration, during the configuration of the **CSA_REST_URI** System Property setting, set the **Property Value** to https://*[APACHE_CSA_HOSTNAME]*:*[APACHE_CSA_HTTPS_PORT]*/csa/rest.

- When you configure HP Operations Orchestration, you must configure SSL between HP Operations Orchestration and the master and slave nodes.

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).

Copy the Configuration Tool to the CSA_Proxy and MPP_Proxy Nodes

If you want to use the Configuration tool to configure the CSA_Proxy or MPP_Proxy node, you must copy the tool to the appropriate node.

Copy the following file to the CSA_Proxy and MPP_Proxy nodes:

```
%CSA_HOME%\Tools\ConfigurationTool\configuration-tool.jar
```

Chapter 3: Configure the CSA_Proxy Node

This section describes how to install and configure the applications needed to set up the CSA_Proxy node in an HP CSA cluster configured for high availability. The CSA_Proxy node proxies web requests into the HP CSA cluster. You can configure the CSA_Proxy node using the Configuration tool or manually.

The CSA_Proxy node consists of:

- Apache HTTP Web server configured as a proxy
- mod_cluster module

Configure the Apache HTTP Web Server Using the Configuration Tool

Complete the tasks in the following sections to install and configure the Apache HTTP Web server on the CSA_Proxy node.

Install the Apache HTTP Web Server and mod_cluster Module

Install the Apache HTTP Web server and mod_cluster module on the CSA_Proxy node. To install the Apache HTTP Web server and mod_cluster module:

1. Download and install the Apache HTTP Server (including SSL) from apache.org (http://httpd.apache.org/download.cgi). The names in the directory path in which the Apache HTTP Server is installed must not contain any spaces.

2. Download the mod_cluster module from JBoss.org (http://www.jboss.org/mod_cluster/downloads). The 32-bit Windows binary is available from http://downloads.jboss.org/mod_cluster//1.2.0.Final/mod_cluster-1.2.0.Final-windows-x86-ssl.zip.

3. Copy the following modules from the mod_cluster module into the *<path_to>*\Apache2.2\modules directory:

   ```
   mod_advertise.so
   mod_manager.so
   mod_proxy_cluster.so
   mod_slotmem.so
   ```

4. Verify that the following modules exist in the *<path_to>*\Apache2.2\modules directory:

   ```
   mod_proxy.so
   mod_proxy_ajp.so
   ```

```
mod_proxy_connect.so
mod_proxy_http.so
```

Run the Configuration Tool on the CSA_Proxy Node

Set up the CSA_Proxy node in the cluster by running the Configuration tool. The Configuration tool allows you to set up the Apache Web server from an interface rather than manually editing configuration files.

The examples in this section show running the Configuration tool in an interface or "swing" mode. Examples on how to run the Configuration tool in other modes are not provided.

To set up the CSA_Proxy node by configuring the Apache Web server as a proxy for HP CSA, do the following:

1. If you have not done so already, install HP CSA on the master and copy the `%CSA_HOME%\Tools\ConfigurationTool\configuration-tool.jar` file to this node.

   > **Note:** The Configuration tool requires that a supported JRE version is installed on the system and that JRE is configured in the system registry or the path to the JRE binaries (`<jre_installation>\bin`) is defined in the system path variable. For a list of supported JRE versions, refer to the *HP Cloud Service Automation System and Software Support Matrix*, available on the HP Software Support Web site at http://h20230.www2.hp.com/selfsolve/manuals/ (this site requires that you register with HP Passport).

2. On the CSA_Proxy node, launch the Configuration tool:

   a. From a command prompt, navigate to where you copied the `configuration-tool.jar` file.

   b. Type `"<jre_installation>\bin\java" -jar configuration-tool.jar -i swing`

3. Select **Configure the Apache Web Server** and **Configure for HP CSA**, and click **Next**.

4. Configure an Apache Web server as a proxy for HP CSA.

a. Enter the following information:

Field	Description
Apache Home Directory	Required. Choose the absolute directory path to the location where the Apache Web server is installed.
IP Address or Hostname	Required. The IP address or fully-qualified domain name of the Apache Web server instance (for example, apache_csa.xyz.com or *[APACHE_CSA_HOSTNAME]* or *[APACHE_CSA_IP_ADDR]*).
HTTP Port	Required. The port used by the Apache Web server (for example, 8080 or *[APACHE_CSA_HTTP_PORT]*). **Note:** If the Apache Web server is configured to use HTTP, the mod_proxy module will also use HTTP.
Mod Cluster Port	Required. The port used as the mod_cluster management port (for example, 10001 or *[MOD_CLUSTER_MGMT_PORT]*).
Allowed IP Addresses or Hostnames	Optional. The IP addresses or fully-qualified domain names of the master and slave nodes (for example, *[MASTER_HOSTNAME]* or *[MASTER_IP_ADDR]* and *[SLAVE_HOSTNAME]* or *[SLAVE_IP_ADDR]*). The IP addresses or hostnames must be separated by a comma.
Configure SSL	Optional. Select this option if you want the Apache Web server to communicate with HP CSA over SSL.
HTTPS Port	The port used by the Apache Web server when SSL is enabled (for example, 8443 or *[APACHE_CSA_HTTPS_PORT]*). **Note:** If the Apache Web server is configured to use HTTPS, the mod_proxy module will also use HTTPS.

Field		Description
	Create a self-signed certificate	Select this option to generate a self-signed certificate and key for the Apache Web server to use for outbound communication. Typically, a self-signed certificate is only used in a test environment. An SSL certificate file named `apache.crt` and a private key named `apache.key` are created in the `<path_to>\Apache2.2\conf` directory. Copy these files to the master, slave, MPP_Node1, and MPP_Node2 nodes and rename them to `apache_csa.crt` and `apache_csa.key`.
	Import key/certificate files	Select this option if you are using an existing certificate for the Apache Web Server to use for outbound communication. For example, select this option if you already generated a Certificate Authority-signed certificate for the Apache Web Server. Click **Import** to select the key/certificate file(s) to use for outbound communication. Copy this certificate to the master, slave, MPP_Node1, and MPP_Node2 nodes. For detailed instructions on how to create SSL certificates, refer to the Apache documentation (http://httpd.apache.org/docs/2.2/ssl/ssl_faq.html#aboutcerts).
Marketplace Portal Apache Proxy		Optional. Select this option if you have set up another Apache Web server as a proxy for the Marketplace Portal (in the example used in this guide, select this option). These fields configure the communication between the two Apache Web servers.
	IP Address or Hostname	The IP address or fully-qualified domain name of the MPP_Proxy node (for example, apache_mpp.xyz.com or *[APACHE_MPP_HOSTNAME]* or *[APACHE_MPP_IP_ADDRESS]*).
	Port	The port used by the MPP_Proxy node (for example, 8089 or *[APACHE_MPP_HTTPS_PORT]*).
	Configured with SSL	Select this option if the MPP_Proxy node is configured with SSL (in the example used in this guide, select this option).

b. Click **Next**.

5. Verify the information you just configured. If you need to update any information, use the **Back** button to return to the appropriate dialog to re-enter the information. If the information is correct, click **Finish**.

> **Note:** If you run the Configuration tool more than once, verify that the port settings and virtual host definitions have not been replaced with different ports in the `<path_to>\Apache2.2\conf\httpd.conf` or `<path_to>\Apache2.2\conf\httpds.conf` files and that the ports are defined in the appropriate file.

Verify the httpd.conf File on the CSA_Proxy Node

In the `<path_to>\Apache2.2\conf\httpd.conf` file, verify that the mod_proxy_balancer module is disabled. The CSA_Proxy node must run the mod_cluster module only. The mod_cluster and mod_proxy_balancer modules cannot be run on the same Apache Web server.

The following line should either not be present or should be commented out in the `httpd.conf` file:

```
LoadModule proxy_balancer_module modules\mod_proxy_balancer.so
```

Start the Apache HTTP Web Server on the CSA_Proxy Node

To start the Apache HTTP Web server, do the following:

1. Navigate to the Services screen (**Control Panel > Administrative Tools > Services**).

2. Right-click on the **Apache2.2** service and select **Start**.

Configure the CSA_Proxy Node Manually

This section describes how to install and manually configure the applications needed to set up the CSA_Proxy node in an HP CSA cluster configured for high availability (how to configure the applications without using the Configuration tool).

Install the Apache HTTP Web Server and mod_cluster Module on the CSA_Proxy Node

Install the Apache HTTP Web server and mod_cluster module on the CSA_Proxy node. To install the Apache HTTP Web server and mod_cluster module:

1. Download and install the Apache HTTP Server (including SSL) from apache.org (http://httpd.apache.org/download.cgi). The names in the directory path in which the Apache HTTP Server is installed must not contain any spaces.

2. Download the mod_cluster module from JBoss.org (http://www.jboss.org/mod_cluster/downloads). The 32-bit Windows binary is available from http://downloads.jboss.org/mod_cluster//1.2.0.Final/mod_cluster-1.2.0.Final-windows-x86-ssl.zip.

3. Copy the following modules from the mod_cluster module into the *<path_*

to>\Apache2.2\modules directory:

```
mod_advertise.so
mod_manager.so
mod_proxy_cluster.so
mod_slotmem.so
```

4. Verify that the following modules exist in the *<path_to>*\Apache2.2\modules directory:

```
mod_proxy.so
mod_proxy_ajp.so
mod_proxy_connect.so
mod_proxy_http.so
```

Configure the Apache HTTP Web Server as a Proxy on the CSA_Proxy Node

Complete the tasks in the following sections to configure the Apache HTTP Web server as a proxy on the CSA_Proxy node.

Configure the Apache HTTP Web Server and mod_cluster Module on the CSA_Proxy Node

Configure the Apache HTTP Server and mod_cluster module on the CSA_Proxy node. Complete the following tasks to configure the Apache HTTP Server and mod_cluster module.

1. Edit the *<path_to>*\Apache2.2\conf\httpd.conf file:

   a. Enable the default port and port 8089. Add the following port entries:

   ```
   Listen [APACHE_CSA_HTTP_PORT]
   ServerName [APACHE_CSA_HOSTNAME]:[APACHE_CSA_HTTP_PORT]
   Listen 8089
   ServerName *:8089
   ```

   For example, if you want to change the default port to 8080, update the port entries to the following:

   ```
   Listen 8080
   ServerName apache_csa.xyz.com:8080
   Listen 8089
   ServerName *:8089
   ```

   Note: If the Apache Web server is configured to use HTTP, the mod_proxy module

> will also use HTTP.

b. Add or update the list of modules that are loaded to include the following comments and modules:

```
# Disable mod_proxy_balancer.so
# LoadModule proxy_balancer_module modules\mod_proxy_balancer.so
# The mod_proxy.so and mod_proxy_ajp.so modules should already be
configured in apache2.conf
LoadModule proxy_module modules\mod_proxy.so
LoadModule proxy_ajp_module modules\mod_proxy_ajp.so
# Additionally load the following modules
LoadModule advertise_module modules\mod_advertise.so
LoadModule manager_module modules\mod_manager.so
LoadModule proxy_cluster_module modules\mod_proxy_cluster.so
LoadModule proxy_connect_module modules\mod_proxy_connect.so
LoadModule proxy_http_module modules\mod_proxy_http.so
LoadModule slotmem_module modules\mod_slotmem.so
```

c. Set up a virtual host for mod_cluster:

```
Listen [APACHE_CSA_IP_ADDR]:[MOD_CLUSTER_MGMT_PORT]
<VirtualHost [APACHE_CSA_IP_ADDR]:[MOD_CLUSTER_MGMT_PORT]>
   <Directory>
      Order deny,allow
      Deny from all
      Allow from [MASTER_IP_ADDR]
      Allow from [SLAVE_IP_ADDR]
   </Directory>
   <Location /mod_cluster-manager>
      SetHandler mod_cluster-manager
      Order deny,allow
      Deny from all
      Allow from [MASTER_IP_ADDR]
      Allow from [SLAVE_IP_ADDR]
   </Location>
   EnableMCPMReceive
   KeepAliveTimeout 60
   MaxKeepAliveRequests 0
   ManagerBalancerName [CSA_SERVER_GROUP]
   AdvertiseFrequency 5
</VirtualHost>
```

where:

- *[MOD_CLUSTER_MGMT_PORT]* is any free port that can be used as the mod_cluster management port (for example, 10001).

- *[CSA_SERVER_GROUP]* is the JBoss server group name specified in `%CSA_HOME%\jboss-as-7.1.1.Final\domain\configuration\domain.xml`.

Configure SSL on the CSA_Proxy Node

Configure SSL on the Apache HTTP Web server for outbound communication.

1. Generate the SSL certificate and private key. For a test environment, you can create a self-signed SSL certificate and key using the following command:

   ```
   openssl req -new -x509 -days 365 -sha1 -newkey rsa:2048 -nodes
   -keyout <path_to>\Apache2.2\conf\apache_csa.key
   -out <path_to>\Apache2.2\conf\apache_csa.crt
   -config <path_to>\Apache2.2\conf\openssl.cnf
   -subj /O=HP/OU=HP/CN=[MASTER_HOSTNAME]
   ```

   For detailed instructions on how to create SSL certificates, refer to the Apache documentation (http://httpd.apache.org/docs/2.2/ssl/ssl_faq.html#aboutcerts).

2. Copy the SSL certificate (`apache_csa.crt`) to the master, slave, MPP_Node1, and MPP_Node2 nodes.

3. Load the SSL module:

   a. Edit `<path_to>\Apache2.2\conf\httpd.conf` to include the SSL configuration and load the SSL module.

   ```
   Include conf\extra\httpd-ssl.conf
   LoadModule ssl_module modules\mod_ssl.so
   ```

   b. Place the certificate (`apache_csa.crt`) and the private key (`apache_csa.key`) in the `<path_to>\Apache2.2\conf` directory. Verify that their location is correctly specified in the `<path_to>\Apache2.2\conf\extra\httpd-ssl.conf` file.

   ```
   SSLCertificateFile <path_to>\Apache2.2\conf\apache_csa.crt
   SSLCertificateKeyFile <path_to>\Apache2.2\conf\apache_csa.key
   ```

   c. If needed, change the port in `<path_to>\Apache2.2\conf\extra\httpd-ssl.conf` (for example, use port 8443 instead of the default port).

   ```
   Listen 8443
   <VirtualHost _default_:8443>
   ServerName [APACHE_CSA_HOSTNAME]:8443
   ```

4. Edit the `<path_to>\Apache2.2\conf\extra\httpd-ssl.conf` file. Set up a virtual host for the MPP_Proxy node:

```
<VirtualHost _default_:8089>
   ErrorLog <path_to>\Apache2.2\logs\mpp_proxy_error.log
   TransferLog <path_to>\Apache2.2\logs\mpp_proxy_access.log
```

```
   LogLevel warn
   SSLProtocol all -SSLv2
   SSLEngine on
   SSLCertificateFile <path_to>\Apache2.2\conf\apache_csa.crt
   SSLCertificateKeyFile <path_to>\Apache2.2\conf\apache_csa.key
   SSLProxyEngine On
   ProxyRequests Off
   ProxyPreserveHost On
   ProxyPass /https://[APACHE_MPP_HOSTNAME]:8089/
   ProxyPassReverse /https://[APACHE_MPP_HOSTNAME]:8089/
</VirtualHost>
```

Start the Apache HTTP Web Server on the CSA_Proxy Node

To start the Apache HTTP Web server, do the following:

1. Navigate to the Services screen (**Control Panel > Administrative Tools > Services**).

2. Right-click on the **Apache2.2** service and select **Start**.

Chapter 4: Configure the MPP_Proxy Node

This section describes how to install and configure the applications needed to set up the MPP_Proxy node in an HP CSA cluster configured for high availability. The MPP_Proxy node proxies web requests into the Marketplace Portal cluster. You can configure the MPP_Proxy node using the Configuration tool or manually.

The MPP_Proxy node consists of:

- Apache HTTP Web server configured as a load balancer

Configure the MPP_Proxy Node Using the Configuration Tool

This section describes how to configure the applications on the MPP_Proxy node using the Configuration tool.

Install the Apache HTTP Web Server on the MPP_Proxy Node

To install the Apache HTTP Web server on the MPP_Proxy node, do the following:

1. Download and install the Apache HTTP Server (including SSL) from apache.org (http://httpd.apache.org/download.cgi). The names in the directory path in which the Apache HTTP Server is installed must not contain any spaces.

2. Verify that the following modules exist in the `<path_to>\Apache2.2\modules` directory:

   ```
   mod_proxy.so
   mod_proxy_ajp.so
   mod_proxy_balancer.so
   mod_proxy_connect.so
   mod_proxy_http.so
   ```

Run the Configuration Tool on the MPP_Proxy Node

Set up the Apache Web server on the MPP_Proxy node in the cluster by running the Configuration tool. The Configuration tool allows you to configure the Apache Web server as a load balancer from an interface rather than manually editing configuration files.

The examples in this guide show how to configure the Apache Web server as a load balancer for the Marketplace Portal on the MPP_Proxy node (based on the diagram in the overview of this guide).

The examples in this section also show running the Configuration tool in an interface or "swing" mode. Examples on how to run the Configuration tool in other modes are not provided.

To set up the MPP_Proxy node by configuring the Apache Web server as a load balancer for the Marketplace Portal, do the following:

1. If you have not done so already, install HP CSA on the master and copy the `%CSA_HOME%\Tools\ConfigurationTool\configuration-tool.jar` file to this node.

   > **Note:** The Configuration tool requires that a supported JRE version is installed on the system and that JRE is configured in the system registry or the path to the JRE binaries (`<jre_installation>\bin`) is defined in the system path variable. For a list of supported JRE versions, refer to the *HP Cloud Service Automation System and Software Support Matrix*, available on the HP Software Support Web site at http://h20230.www2.hp.com/selfsolve/manuals/ (this site requires that you register with HP Passport).

2. On the MPP_Proxy node, launch the Configuration tool:

   a. From a command prompt, navigate to where you copied the `configuration-tool.jar` file.

   b. Type `"<jre_installation>\bin\java" -jar configuration-tool.jar -i swing`

3. Select **Configure the Apache Web server** and **Configure for the Marketplace Portal** and click **Next**.

4. Configure an Apache Web server as a proxy for Marketplace Portal.

a. Enter the following information:

Field		Description
Apache Home Directory		Required. Choose the absolute directory path to the location where the Apache Web server is installed.
IP Address or Hostname		Required. The IP address or fully-qualified domain name of the Apache Web server instance (for example, apache_mpp.xyz.com or *[APACHE_MPP_HOSTNAME]* or *[APACHE_MPP_IP_ADDR]*).
HTTP Port		Required. The port used by the Apache Web server (for example, 8080 or *[APACHE_MPP_HTTP_PORT]*). **Note:** If the Apache Web server is configured to use HTTP, the mod_proxy_balancer module will also use HTTP.
Allowed IP Addresses or Hostnames		Optional. The IP addresses or fully-qualified domain names of the master and slave nodes. The IP addresses or hostnames must be separated by a comma (for example, *[MASTER_HOSTNAME]* or *[MASTER_IP_ADDR]* and *[SLAVE_HOSTNAME]* or *[SLAVE_IP_ADDR]*).
Configure SSL		Optional. Select this option if you want the Apache Web server to communicate with Marketplace Portal over SSL.
	HTTPS Port	The port used by the Apache Web server when SSL is enabled (for example, 8089 or *[APACHE_MPP_HTTPS_PORT]*). **Note:** If the Apache Web server is configured to use HTTPS, the mod_proxy_balancer module will also use HTTPS.
	Create a self-signed certificate	Select this option to generate a self-signed certificate and key for the Apache Web server. Typically, a self-signed certificate is only used in a test environment. An SSL certificate file named `apache.crt` and a private key named `apache.key` are created in the `<path_to>\Apache2.2\conf` directory. Copy the certificate file to the MPP_Node1 and MPP_Node2 nodes and rename it to `apache_mpp.crt`.

Field		Description
	Import key/certificate files	Select this option to use the Apache Web server's Certificate Authority-signed certificate. Click **Import** to select the key/certificate file(s) to import into the Marketplace Portal's truststore. For detailed instructions on how to create SSL certificates, refer to the Apache documentation (http://httpd.apache.org/docs/2.2/ssl/ssl_faq.html#aboutcerts).

b. Click **Next**.

5. Verify the information you just configured. If you need to update any information, use the **Back** button to return to the appropriate dialog to re-enter the information. If the information is correct, click **Finish**.

> **Note:** If you run the Configuration tool more than once, verify that the port settings and virtual host definitions have not been replaced with different ports in the `<path_to>\Apache2.2\conf\httpd.conf` or `<path_to>\Apache2.2\conf\httpds.conf` files and that the ports are defined in the appropriate file.

Configure Session Persistence with the Marketplace Portal

On the MPP_Proxy node, enable the load balancer (mod_proxy_balancer module) stickyness. Refer to http://httpd.apache.org/docs/2.2/mod/mod_proxy_balancer.html for more information.

Start the Apache HTTP Web Server on the MPP_Proxy Node

To start the Apache HTTP Web server, do the following:

1. Navigate to the Services screen (**Control Panel > Administrative Tools > Services**).

2. Right-click on the **Apache2.2** service and select **Start**.

Configure the MPP_Proxy Node Manually

This section describes how to install and manually configure the applications needed to set up the MPP_Proxy node in an HP CSA cluster configured for high availability (how to configure the applications without using the Configuration tool).

Install the Apache HTTP Web Server on the MPP_Proxy Node

To install the Apache HTTP Web server on the MPP_Proxy node, do the following:

1. Download and install the Apache HTTP Server (including SSL) from apache.org (http://httpd.apache.org/download.cgi). The names in the directory path in which the Apache HTTP Server is installed must not contain any spaces.

2. Verify that the following modules exist in the `<path_to>\Apache2.2\modules` directory:

   ```
   mod_proxy.so
   mod_proxy_ajp.so
   mod_proxy_balancer.so
   mod_proxy_connect.so
   mod_proxy_http.so
   ```

Configure the Apache HTTP Web Server as a Load Balancer on the MPP_Proxy Proxy Node

Complete the tasks in the following sections to configure the Apache HTTP Web server as a load balancer on the MPP_Proxy node.

Configure SSL on the MPP_Proxy Node

Configure SSL on the Apache HTTP Web server for outbound communication.

1. Generate the SSL certificate and private key. For a test environment, you can create a self-signed SSL certificate and key using the following command:

   ```
   openssl req -new -x509 -days 365 -sha1 -newkey rsa:2048 -nodes
   -keyout <path_to>\Apache2.2\conf\apache_mpp.key
   -out <path_to>\Apache2.2\conf\apache_mpp.crt
   -config <path_to>\Apache2.2\conf\openssl.cnf
   -subj /O=HP/OU=HP/CN=[MASTER_HOSTNAME]
   ```

   For detailed instructions on how to create SSL certificates, refer to the Apache documentation (http://httpd.apache.org/docs/2.2/ssl/ssl_faq.html#aboutcerts).

2. Copy the certificate file (`apache_mpp.crt`) to the MPP_Node1 and MPP_Node2 nodes.

3. Load the SSL module:

   a. Edit `<path_to>\Apache2.2\conf\httpd.conf` to include the SSL configuration and load the SSL module.

      ```
      Include conf\extra\httpd-ssl.conf
      LoadModule ssl_module modules\mod_ssl.so
      ```

b. Place the certificate (`apache_mpp.crt`) and the private key (`apache_mpp.key`) in the *<path_to>*`\Apache2.2\conf` directory.

Configure the Apache HTTP Web Server on the MPP_Proxy Node

1. Edit the *<path_to>*`\Apache2.2\conf\httpd.conf` file:

   a. Enable port 8089. Add the following port entries:

   ```
   Listen 8089
   ServerName *:8089
   ```

   > **Note:** If the Apache Web server is configured to use HTTPS, the mod_proxy_balancer module will also use HTTPS.

   b. Add or update the list of modules that are loaded to include the following comments and modules:

   ```
   # Disable mod_proxy_balancer.so
   # LoadModule proxy_balancer_module modules\mod_proxy_balancer.so
   # The mod_proxy.so and mod_proxy_ajp.so modules should already be
   configured in apache2.conf
   LoadModule proxy_module modules\mod_proxy.so
   LoadModule proxy_ajp_module modules\mod_proxy_ajp.so
   # Additionally load the following modules
   LoadModule proxy_balancer_module modules\mod_proxy_balancer.so
   LoadModule proxy_connect_module modules\mod_proxy_connect.so
   LoadModule proxy_http_module modules\mod_proxy_http.so
   LoadModule proxy_connect_module modules\mod_headers.so
   LoadModule proxy_connect_module modules\mod_ssl.so
   ```

2. Edit the *<path_to>*`\Apache2.2\conf\extra\httpd-ssl.conf` file. Set up a virtual host:

   ```
   <VirtualHost _default_:8089>
      ErrorLog <path_to>\Apache2.2\logs\mpp_proxy_error.log
      TransferLog <path_to>\Apache2.2\logs\mpp_proxy_access.log
      LogLevel warn
      SSLProtocol all -SSLv2
      SSLProxyEngine On
      SSLEngine on
      SSLCertificateFile <path_to>\Apache2.2\conf\apache_mpp.crt
      SSLCertificateKeyFile <path_to>\Apache2.2\conf\apache_mpp.key
      <Proxy *>
         Order deny,allow
         Allow from all
   ```

```
   </Proxy>
   <Proxy balancer://mycluster/>
      BalancerMember https://[MASTER_HOSTNAME]:8089
      BalancerMember https://[SLAVE_HOSTNAME]:8089
      ProxySet lbmethod=byrequests
      ProxySet stickysession=ROUTEID
   </Proxy>
   ProxyPass / balancer://mycluster/
   ProxyPassReverse / balancer://mycluster/
</VirtualHost>
```

3. On the MPP_Proxy node, enable the load balancer (mod_proxy_balancer module) stickyness. Refer to http://httpd.apache.org/docs/2.2/mod/mod_proxy_balancer.html for more information.

Start the Apache HTTP Web Server on the MPP_Proxy Node

To start the Apache HTTP Web server, do the following:

1. Navigate to the Services screen (**Control Panel > Administrative Tools > Services**).

2. Right-click on the **Apache2.2** service and select **Start**.

Chapter 5: Configure the Master Node

This chapter describes how to configure the master node in an HP CSA cluster configured for high availability. You can install and configure the master node using the Configuration tool or manually.

Configure the Master Node Using the Configuration Tool

The master node consists of:

- HP CSA

- Identity Management component

Configure HP CSA on the Master Node

The following are tasks to configure HP CSA:

- **Request a Software License** - Required. Request and add a software license.

- **Share Filesystem Resources** - Optional. Configure HP CSA to share filesystem resources to free up disk space.

- **Rename Servers** - Optional. Rename the HP CSA server node.

- **Configure Multiple Network Interfaces** - Optional. Configure the management interface to use multiple network interfaces.

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 4.00 licenses are valid and are automatically added.

> **Note:** HP CSA version 4.10 licenses are not compatible with HP CSA version 4.00. That is, you cannot add HP CSA version 4.10 licenses to HP CSA version 4.00.

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 CSA_Proxy server

([APACHE_CSA_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. Map the shared location as a network drive. For example, map `S:\CSA` on the master node to the shared location.

3. Move the `%CSA_HOME%\jboss-as-7.1.1.Final\domain\servers\hp-cloud\deployments\csa.war\images` directory to the shared location (for example, `S:\CSA\images`).

   Ensure that the mapped `images` directory is readable and writeable.

4. Delete the `%CSA_HOME%\jboss-as-7.1.1.Final\domain\servers\hp-cloud\deployments\csa.war\images` directory from the master and slave nodes.

5. Create a symbolic link to the mapped `images` directory. For example, from a command prompt, type the following commands:

   ```
   cd %CSA_HOME%\jboss-as-7.1.1.Final\domain\servers\hp-cloud\
   deployments\csa.war
   mklink /d images "S:\CSA\images"
   ```

Rename Servers

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

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).

Run the Configuration Tool on the Master Node

Set up the master node in the cluster by running the Configuration tool. The Configuration tool allows you to configure the master node from an interface rather than manually editing configuration files.

The examples in this section also show running the Configuration tool in an interface or "swing" mode. Examples on how to run the Configuration tool in other modes are not provided.

To set up the master node, do the following:

1. On the master node, launch the Configuration tool:

   a. From a command prompt, navigate to `%CSA_HOME%\Tools\ConfigurationTool\`.

   b. Type `"<csa_jre>\bin\java" -jar configuration-tool.jar -i swing`

2. Select **Set up an HP CSA clustered node**, **Master**, **Apache Web Server as a proxy**, and **Use an existing Apache Web server as a proxy**, and click **Next**.

3. Use an existing Apache Web server as a proxy for HP CSA.

a. Enter the following information:

Field		Description
IP Address or Hostname		Required. The IP address or fully-qualified domain name of the CSA_Proxy node (for example, apache_csa.xyz.com or *[APACHE_CSA_HOSTNAME]* or *[APACHE_CSA_IP_ADDR]*).
HTTP Port		Required. The port used by the CSA_Proxy node (for example, 8080 or *[APACHE_CSA_HTTP_PORT]*).
Marketplace Portal Proxy HTTP Port		Required. The port used by the MPP_Proxy node (for example, 8080 or *[APACHE_MPP_HTTP_PORT]*).
Mod Cluster Port		Required. The port used as the mod_cluster management port (for example, 10001 or *[MOD_CLUSTER_MGMT_PORT]*).
Configured with SSL		Optional. Select this option if the CSA_Proxy and MPP_Proxy nodes communicate with HP CSA over SSL.
	HTTPS Port	The port used by the CSA_Proxy node when SSL is enabled (for example, 8443 or *[APACHE_CSA_HTTPS_PORT]*).
	Marketplace Portal Proxy HTTPS Port	The port used by the MPP_Proxy node when SSL is enabled (for example, 8089 or *[APACHE_MPP_HTTPS_PORT]*).
	Import Certificate	Click **Import Certificate** to select the Apache Web server key/certificate files from the CSA_Proxy node to import into HP CSA's truststore. You should have copied this file to the master node when you configured the CSA_Proxy node. For detailed instructions on how to create SSL certificates for the Apache Web server, refer to the Apache documentation (http://httpd.apache.org/docs/2.2/ssl/ssl_faq.html#aboutcerts).

b. Click **Next**.

4. Configure the master node.

a. Enter the following information:

Field	Description
IP Address	Required. The IP address of the master node (for example, *[MASTER_IP_ADDR]*).
Cluster Hostname	Required. A unique name that identifies this node in the cluster (for example, master_node or *[MASTER_CLUSTER_HOSTNAME]*).
Add JBoss Management Users	Required. Click **Add** to create Management Users in the ManagementRealm of JBoss. You must create at least one user who can connect to the master node for each slave node (this user's name and password are needed when configuring the slave node). Optionally, create another user who can access the JBoss Management Web interface to validate the JBoss cluster configuration. For example, create a user called *[SLAVE_ACCESS_USERNAME]* that is used by the slave node to connect to the master node. Create another user called `csaadmin` who can access the JBoss Management Web interface.

b. Click **Next**.

5. Verify the information you just configured. If you need to update any information, use the **Back** button to return to the appropriate dialog to re-enter the information. If the information is correct, click **Finish**.

Configure the HP CSA Truststore Properties

You must configure information about the HP CSA's keystore. Do the following:

1. 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.

2. 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).

3. 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.

4. Save and exit the file.

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. Stop the `HP Cloud Service Automation` service:

   a. Navigate to the Services screen (**Control Panel > Administrative Tools > Services**).

   b. Right-click on the **HP Cloud Service Automation** service and select **Stop**.

2. Delete the existing HP CSA service:

   a. Open a command prompt.

   b. Run the following command:

      execute sc delete CSA

3. Edit the `%CSA_HOME%\jboss-as-7.1.1.Final\bin\service.bat` file:

   a. Locate the two occurrences of `standalone.bat` and replace them with `domain.bat`.

   b. 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).

4. From a command prompt, do the following:

   a. Change to the `%CSA_HOME%\jboss-as-7.1.1.Final\bin` directory.

   b. Run the following command:

      service.bat install /c

5. Start the `HP Cloud Service Automation` service in domain mode:

   a. Navigate to the Services screen (**Control Panel > Administrative Tools > Services**).

   b. Right-click on the **HP Cloud Service Automation** service and select **Start**.

Configure the Master Node Manually

This section describes how to install and manually configure the applications needed to set up the master node in an HP CSA cluster configured for high availability (how to configure the applications without using the Configuration tool).

The master node consists of:

- HP CSA
- Identity Management component

Install HP CSA on the Master Node

If you have not done so already, complete the tasks in the following section to install HP CSA on the master node.

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 node.
- 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 you configure HP Operations Orchestration, during the configuration of the **CSA_REST_URI** System Property setting, set the **Property Value** to https://*[APACHE_CSA_*

HOSTNAME]:*[APACHE_CSA_HTTPS_PORT]*/csa/rest.

- When you configure HP Operations Orchestration, you must configure SSL between HP Operations Orchestration and the master and slave nodes.

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 proxy and set the mode in which HP CSA is running:

   ```
   csa.provider.hostname=[APACHE_CSA_HOSTNAME]
   csa.provider.port=[APACHE_CSA_HTTPS_PORT]
   csa.provider.rest.protocol=https
   deploymentMode=clustered
   ```

   For example:

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

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. In a later section you will configure SSL on the Apache HTTP Web server (CSA_Proxy node) for outbound communication.

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.bat` 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 4.00 licenses are valid and are automatically added.

> **Note:** HP CSA version 4.10 licenses are not compatible with HP CSA version 4.00. That is, you cannot add HP CSA version 4.10 licenses to HP CSA version 4.00.

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 CSA_Proxy server ([APACHE_CSA_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. Map the shared location as a network drive. For example, map `S:\CSA` on the master node to the shared location.

3. Move the `%CSA_HOME%\jboss-as-7.1.1.Final\domain\servers\hp-cloud\deployments\csa.war\images` directory to the shared location (for example, `S:\CSA\images`).

   Ensure that the mapped `images` directory is readable and writeable.

4. Delete the `%CSA_HOME%\jboss-as-7.1.1.Final\domain\servers\hp-cloud\deployments\csa.war\images` directory from the master and slave nodes.

5. Create a symbolic link to the mapped `images` directory. For example, from a command prompt,

type the following commands:

```
cd %CSA_HOME%\jboss-as-7.1.1.Final\domain\servers\hp-cloud\
deployments\csa.war
mklink /d images "S:\CSA\images"
```

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 the `%CSA_HOME%\jboss-as-7.1.1.Final\domain\configuration\domain.xml` file in an editor.

2. Verify that mod_cluster already exists as a subsystem and that the `proxy-list` attribute is configured as follows:

```
<subsystem xmlns="urn:jboss:domain:modcluster:1.0">
   <mod-cluster-config advertise-socket="modcluster" proxy-list="[APACHE_CSA_
IP_ADDR]:[MOD_CLUSTER_MGMT_PORT]">
      <dynamic-load-provider>
         <load-metric type="busyness"/>
      </dynamic-load-provider>
   </mod-cluster-config>
</subsystem>
```

3. 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="ajp" protocol="AJP/1.3" scheme="http" socket-
binding="ajp"/>
   <virtual-server name="default-host" enable-welcome-root="true">
      <alias name="localhost"/>
      <alias name="example.com"/>
   </virtual-server>
</subsystem>
```

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 (`apache_csa.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:

   ```
   keytool.sh -importcert -file %CSA_HOME%\jboss-as-
   7.1.1.Final\domain\configuration\apache_csa.crt -alias apache_csa -keystore
   <csa_jre>\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 = [APACHE_CSA_HOSTNAME]
   idm.csa.port = [APACHE_CSA_HTTPS_PORT]
   ```

   For example:

   ```
   idm.csa.hostname = apache_csa.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 *[APACHE_CSA_HOSTNAME]* and `port` to *[APACHE_CSA_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="~~localhost~~apache_csa.xyz.com"/>
   <beans:property name="port" value="~~8444~~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>
```

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. Stop the `HP Cloud Service Automation` service:

   a. Navigate to the Services screen (**Control Panel > Administrative Tools > Services**).

   b. Right-click on the **HP Cloud Service Automation** service and select **Stop**.

2. Delete the existing HP CSA service:

   a. Open a command prompt.

   b. Run the following command:

      execute sc delete CSA

3. Edit the `%CSA_HOME%\jboss-as-7.1.1.Final\bin\service.bat` file:

   a. Locate the two occurrences of `standalone.bat` and replace them with `domain.bat`.

   b. 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).

4. From a command prompt, do the following:

   a. Change to the `%CSA_HOME%\jboss-as-7.1.1.Final\bin` directory.

   b. Run the following command:

      service.bat install /c

5. Start the `HP Cloud Service Automation` service in domain mode:

   a. Navigate to the Services screen (**Control Panel > Administrative Tools > Services**).

   b. Right-click on the **HP Cloud Service Automation** service and select **Start**.

Chapter 6: Configure the Slave Node

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

Configure the Slave Node Using the Configuration Tool

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 you configure HP Operations Orchestration, during the configuration of the **CSA_REST_URI** System Property setting, set the **Property Value** to https://*[APACHE_CSA_HOSTNAME]*:*[APACHE_CSA_HTTPS_PORT]*/csa/rest.
- When you configure HP Operations Orchestration, you must configure SSL between HP Operations Orchestration and the master and slave nodes.

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

The following are tasks to configure HP CSA:

- **Share Filesystem Resources** - Optional. Configure HP CSA to share filesystem resources to free up disk space.
- **Rename Servers** - Optional. Rename the HP CSA server node.
- **Configure Multiple Network Interfaces** - Optional. Configure the management interface to use multiple network interfaces.

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. Map the shared location as a network drive. For example, map `S:\CSA` on the slave node to the shared location.
2. Delete the `%CSA_HOME%\jboss-as-7.1.1.Final\domain\servers\hp-cloud\deployments\csa.war\images` directory.
3. Create a symbolic link to the mapped `images` directory. For example, from a command prompt, type the following commands:

```
cd %CSA_HOME%\jboss-as-7.1.1.Final\domain\servers\hp-cloud\
deployments\csa.war
mklink /d images "S:\CSA\images"
```

Rename Servers

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

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 the `%CSA_HOME%\jboss-as-7.1.1.Final\domain\configuration\domain.xml` file in an editor.

2. Verify that mod_cluster already exists as a subsystem and that the `proxy-list` attribute is configured as follows:

```
<subsystem xmlns="urn:jboss:domain:modcluster:1.0">
   <mod-cluster-config advertise-socket="modcluster" proxy-list="[APACHE_CSA_
IP_ADDR]:[MOD_CLUSTER_MGMT_PORT]">
      <dynamic-load-provider>
```

```
         <load-metric type="busyness"/>
      </dynamic-load-provider>
   </mod-cluster-config>
</subsystem>
```

3. 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="ajp" protocol="AJP/1.3" scheme="http" socket-
binding="ajp"/>
   <virtual-server name="default-host" enable-welcome-root="true">
      <alias name="localhost"/>
      <alias name="example.com"/>
   </virtual-server>
</subsystem>
```

Import the SSL Certificate on the Slave Node

Import the Apache HTTP Web server SSL certificate into the JVM truststore.

1. If you have not already done so, copy the SSL certificate (`apache_csa.crt`) that you generated on the master 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\apache_csa.crt -alias apache_csa -keystore
<csa_jre>\lib\security\cacerts
```

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

Run the Configuration Tool on the Slave Node

Set up the slave node in the cluster by running the Configuration tool. The Configuration tool allows you to configure the slave node from an interface rather than manually editing configuration files.

The example in this section shows how to configure the slave node in a clustered configuration with a master node that also hosts the Apache Web server as a proxy for HP CSA (based on the diagram in the overview of this guide). You may also configure the Apache Web server as a proxy for HP CSA on the slave node or on a remote system instead. However, examples for these configurations are not provided.

The example in this section also shows running the Configuration tool in an interface or "swing" mode. Examples on how to run the Configuration tool in other modes are not provided.

To set up the slave node, do the following:

1. On the slave node, launch the Configuration tool:

   a. From a command prompt, navigate to `%CSA_HOME%\Tools\ConfigurationTool\`.

   b. Type `"<csa_jre>\bin\java" -jar configuration-tool.jar -i swing`

2. Select **Set up an HP CSA clustered node** and **Slave**, **Apache Web Server as a proxy**, **Use an existing Apache Web server as a proxy**, and click **Next**.

3. Configure the existing Apache Web server as a proxy for HP CSA.

   Enter the following information:

Field		Description
IP Address or Hostname		Required. The IP address or fully-qualified domain name of the Apache Web server instance.
HTTP Port		Required. The port used by the Apache Web server (for example, 8080).
Mod Cluster Port		Required. The port used as the mod_cluster management port (for example, 10001).
Configured with SSL		Optional. Select this option if the Apache Web server communicates with HP CSA over SSL.
	HTTPS Port	The port used by the Apache Web server when SSL is enabled (for example, 8443).
	Import Certificate	Select this option to use the Apache Web server's Certificate Authority-signed certificate. Click **Import** to select the key/certificate file(s) to import into HP CSA's truststore. For detailed instructions on how to create SSL certificates, refer to the Apache documentation (http://httpd.apache.org/docs/2.2/ssl/ssl_faq.html#aboutcerts).

4. Click **Next**.

5. Configure the slave node.

a. Enter the following information:

Field	Description
IP Address or Hostname	Required. The IP address or fully-qualified domain name of the slave node.
Master IP Address or Hostname	Required. The IP address or fully-qualified domain name of the master node.
Cluster Nodename	Required. The name of the JBoss Management User who connects to the master node. This is the same JBoss Management User you added when you configured the master node using this tool (for example, *[SLAVE_ACCESS_USERNAME]*).
Slave Password (Base64)	Required. The password (encoded in base64 format) of the JBoss Management User who connects to the master node (this is the same JBoss Management User you added when you configured the master node using this tool; for example, *[SLAVE_ACCESS_PASSWORD_BASE64]*).

b. Click **Next**.

6. Verify the information you just configured. If you need to update any information, use the **Back** button to return to the appropriate dialog to re-enter the information. If the information is correct, click **Finish**.

Configure the HP CSA Truststore Properties

You must configure information about the HP CSA's keystore. Do the following:

1. 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.

2. 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).

3. 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*.

4. Save and exit the file.

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. Stop the `HP Cloud Service Automation` service:

   a. Navigate to the Services screen (**Control Panel > Administrative Tools > Services**).

   b. Right-click on the **HP Cloud Service Automation** service and select **Stop**.

2. Delete the existing HP CSA service:

   a. Open a command prompt.

   b. Run the following command:

      execute sc delete CSA

3. Edit the `%CSA_HOME%\jboss-as-7.1.1.Final\bin\service.bat` file:

   a. Locate the two occurrences of `standalone.bat` and replace them with `domain.bat`.

   b. 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).

4. From a command prompt, do the following:

   a. Change to the `%CSA_HOME%\jboss-as-7.1.1.Final\bin` directory.

   b. Run the following command:

      service.bat install /c

5. Start the `HP Cloud Service Automation` service in domain mode:

a. Navigate to the Services screen (**Control Panel > Administrative Tools > Services**).

b. Right-click on the **HP Cloud Service Automation** service and select **Start**.

Configure the Slave Node Manually

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 (how to configure the applications without using the Configuration tool).

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 you configure HP Operations Orchestration, during the configuration of the **CSA_REST_URI** System Property setting, set the **Property Value** to https://*[APACHE_CSA_HOSTNAME]*:*[APACHE_CSA_HTTPS_PORT]*/csa/rest.

- When you configure HP Operations Orchestration, you must configure SSL between HP Operations Orchestration and the master and slave nodes.

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 proxy and set the mode in which HP CSA is running:

   ```
   csa.provider.hostname=[APACHE_CSA_HOSTNAME]
   csa.provider.port=[APACHE_CSA_HTTPS_PORT]
   csa.provider.rest.protocol=https
   deploymentMode=clustered
   ```

   For example:

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

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. In a later section you will configure SSL on the Apache HTTP Web server (CSA_Proxy node) for outbound communication.

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" 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. Map the shared location as a network drive. For example, map `S:\CSA` on the slave node to the shared location.

2. Delete the `%CSA_HOME%\jboss-as-7.1.1.Final\domain\servers\hp-cloud\deployments\csa.war\images` directory.

3. Create a symbolic link to the mapped `images` directory. For example, from a command prompt, type the following commands:

   ```
   cd %CSA_HOME%\jboss-as-7.1.1.Final\domain\servers\hp-cloud\
   deployments\csa.war
   mklink /d images "S:\CSA\images"
   ```

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 the `%CSA_HOME%\jboss-as-7.1.1.Final\domain\configuration\domain.xml` file in an editor.

2. Verify that mod_cluster already exists as a subsystem and that the `proxy-list` attribute is configured as follows:

   ```
   <subsystem xmlns="urn:jboss:domain:modcluster:1.0">
      <mod-cluster-config advertise-socket="modcluster" proxy-list="[APACHE_CSA_
   IP_ADDR]:[MOD_CLUSTER_MGMT_PORT]">
         <dynamic-load-provider>
            <load-metric type="busyness"/>
         </dynamic-load-provider>
      </mod-cluster-config>
   </subsystem>
   ```

3. 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="ajp" protocol="AJP/1.3" scheme="http" socket-
   binding="ajp"/>
      <virtual-server name="default-host" enable-welcome-root="true">
         <alias name="localhost"/>
         <alias name="example.com"/>
   ```

```
    </virtual-server>
</subsystem>
```

Import the SSL Certificate on the Slave Node

Import the Apache HTTP Web server SSL certificate into the JVM truststore.

1. If you have not already done so, copy the SSL certificate (`apache_csa.crt`) that you generated on the master 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\apache_csa.crt -alias apache_csa -keystore
   <csa_jre>\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 = [APACHE_CSA_HOSTNAME]
   idm.csa.port = [APACHE_CSA_HTTPS_PORT]
   ```

   For example:

   ```
   idm.csa.hostname = apache_csa.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 *[APACHE_CSA_HOSTNAME]* and `port` to *[APACHE_CSA_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="~~localhost~~apache_csa.xyz.com"/>
   <beans:property name="port" value="~~8444~~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>
```

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. Stop the `HP Cloud Service Automation` service:

   a. Navigate to the Services screen (**Control Panel > Administrative Tools > Services**).

   b. Right-click on the **HP Cloud Service Automation** service and select **Stop**.

2. Delete the existing HP CSA service:

   a. Open a command prompt.

   b. Run the following command:

execute sc delete CSA

3. Edit the `%CSA_HOME%\jboss-as-7.1.1.Final\bin\service.bat` file:

   a. Locate the two occurrences of `standalone.bat` and replace them with `domain.bat`.

   b. 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).

4. From a command prompt, do the following:

   a. Change to the `%CSA_HOME%\jboss-as-7.1.1.Final\bin` directory.

   b. Run the following command:

      service.bat install /c

5. Start the `HP Cloud Service Automation` service in domain mode:

   a. Navigate to the Services screen (**Control Panel > Administrative Tools > Services**).

   b. Right-click on the **HP Cloud Service Automation** service and select **Start**.

Chapter 7: 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). You must configure the Marketplace Portal node manually.

The Marketplace Portal node consists of:

- The Marketplace Portal

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 Apache HTTP proxy server installed on the CSA_Proxy node (for example, apache_csa.xyz.com or *[APACHE_CSA_HOSTNAME]*).
- When configuring the HP CSA Port, use the port of the Apache HTTP proxy server installed on the CSA_Proxy node (for example, 8443 or *[APACHE_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).

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 Apache Web server from the CSA_Proxy node (for example, apache_csa.crt) to the `%CSA_HOME%\portal\conf\jboss-as-7.1.1.Final\$CSA_HOME/jboss-as-7.1.1.Final/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 *[APACHE_CSA_HOSTNAME]* and *[APACHE_CSA_HTTPS_PORT]*. For example:

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

- For the idmProvider, update the values of the `url` attribute to use *[APACHE_CSA_HOSTNAME]* and *[APACHE_CSA_HTTPS_PORT]*, and `returnUrl` to use *[APACHE_MPP_HOSTNAME]*, and `ca` to use the location of the SSL certificate of the Apache Web server as a proxy for HP CSA. For example:

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

3. Restart the Marketplace Portal service:

   a. Navigate to the Services screen (**Control Panel > Administrative Tools > Services**).

   b. Right-click on the **Marketplace Portal** service and select **Restart**.

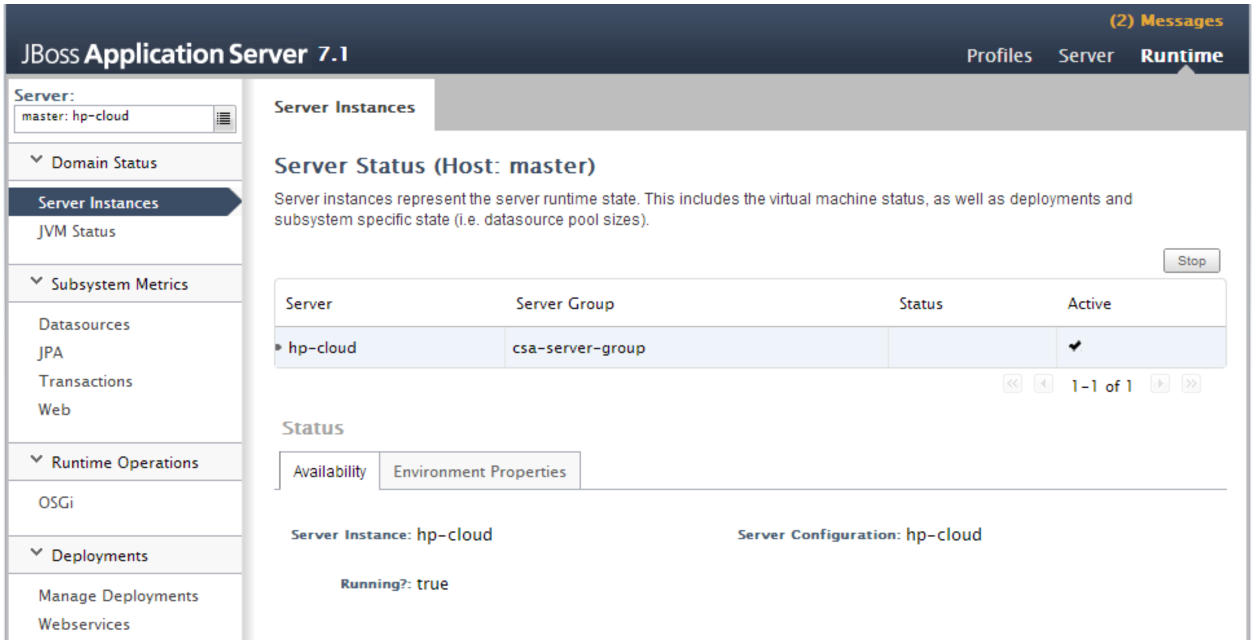
Chapter 8: Validate the JBoss Cluster Configuration

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.



Server: master: hp-cloud

Server Status (Host: master)

Server instances represent the server runtime state. This includes the virtual machine status, as well as deployments and subsystem specific state (i.e. datasource pool sizes).

Server	Server Group	Status	Active
hp-cloud	csa-server-group		✓

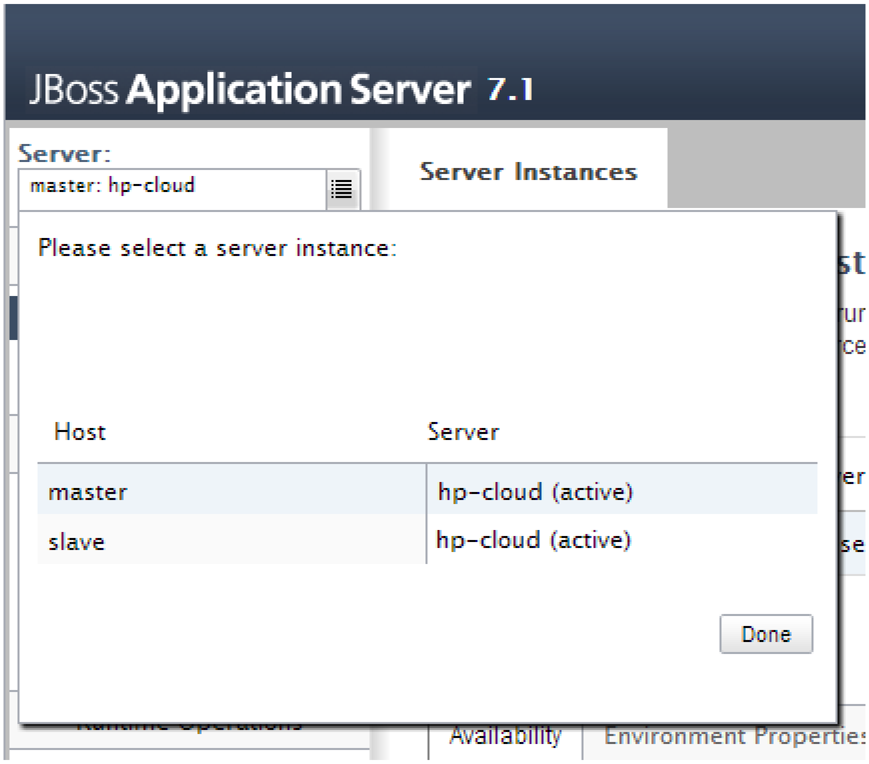
Server Instance: hp-cloud

Server Configuration: hp-cloud

Running?: true

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.



Please select a server instance:

Host	Server
master	hp-cloud (active)
slave	hp-cloud (active)

Chapter 9: 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:

1. On the server that hosts HP CSA, navigate to **Control Panel** > **Administrative Tools** > **Services**.
2. Right-click on the HP Cloud Service Automation service and select **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:

1. On the server that hosts HP Cloud Service Automation, navigate to **Control Panel** > **Administrative Tools** > **Services**.

2. Right-click on the HP Cloud Service Automation service and select **Stop**.

Start the Marketplace Portal

To start the Marketplace Portal service, do the following:

1. Navigate to the Services screen (**Control Panel > Administrative Tools > Services**).

2. Right-click on the **Marketplace Portal** service and select **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`.

Start the Apache HTTP Web server

To start the Apache HTTP Web server, do the following:

1. Navigate to the Services screen (**Control Panel > Administrative Tools > Services**).

2. Right-click on the **Apache2.2** service and select **Start**.

Stop the Apache HTTP Web server

To stop the Apache HTTP Web server, do the following:

1. Navigate to the Services screen (**Control Panel > Administrative Tools > Services**).

2. Right-click on the **Apache2.2** service and select **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://`*`[APACHE_CSA_HOSTNAME]`*`:`*`[APACHE_CSA_HTTP_PORT]`*`/csa`
  For example, `http://apache_csa.xyz.com:8080/csa`

- `https://`*`[APACHE_CSA_HOSTNAME]`*`:`*`[APACHE_CSA_HTTPS_PORT]`*`/csa`
  For example, `https://apache_csa.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://`*`[APACHE_CSA_HOSTNAME]`*`:8444/mpp`
  For example, `http://apache_csa.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://`*`[APACHE_CSA_HOSTNAME]`*`:`*`[APACHE_CSA_HTTP_PORT]`*`/org/`*`<organization_identifier>`*
  For example, `http://apache_csa.xyz.com:8080/org/ORGANIZATION_A`

- `https://`*`[APACHE_CSA_HOSTNAME]`*`:`*`[APACHE_CSA_HTTPS_PORT]`*`/org/`*`<organization_identifier>`*
  For example, `http://apache_csa.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 (for use with HP CSA configuration only; see "Encrypt a Marketplace Portal Password" below for information on how to encrypt a Marketplace Portal password):

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

   ```
   C:\Program Files\Hewlett-Packard\CSA\scripts
   ```

2. Run the following command:

   ```
   "<csa_jre>\bin\java" -jar passwordUtil.jar encrypt <myPassword>
   ```

Encrypt a Marketplace Portal Password

To encrypt a password used by the Marketplace Portal:

1. Open a command prompt and change to the `%CSA_HOME%\portal\bin` directory. For example:

   ```
   C:\Program Files\Hewlett-Packard\CSA\portal\bin
   ```

2. Run the following command:

   ```
   ..\..\node.js\node passwordUtil --keyfilePath <keyfile> --password
   <myPassword>
   ```

   where <keyfile> is the path to (absolute or relative to the bin directory) and name of the file that contains the Marketplace Portal's encrypted symmetric key (if the file does not exist, it will create the file) and <myPassword> is the password to be encrypted.

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 66 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 66 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.

Appendix A: The Configuration Tool Modes and Options

This appendix gives a high-level overview of the modes in which the Configuration tool can be run and the options required to run it.

The Configuration Tool Modes

The mode of the Configuration tool determines how you interact with the tool, the information that is configured using the tool, and the information that must be configure manually. The mode is specified as an option when running the tool.

The Configuration tool can be run in the following different modes:

- **swing** - Run the tool from a graphical user interface. In this mode, all tasks that are required to configure an HP CSA cluster (set up a master or slave node, configure HP CSA, configure JBoss, and configure the Apache Web server) can be completed. You can also configure HP CSA and JBoss properties in a standalone environment.

  The steps to use this mode are documented in this guide.

- **console** - Run the tool from the command line. In this mode, you can only set up the master or slave node. All other tasks must be manually completed (configure HP CSA, configure JBoss, and configure the Apache Web server).

Configuration tool Modes and Covered Tasks

	swing	console
Set up a master or slave node for HP CSA	✔	✔
Set up a clustered node for Marketplace Portal	✔	✔
Configure HP CSA	✔	
Configure JBoss	✔	
Configure Apache Web server	✔	

The Configuration Tool Options

The options of the Configuration tool determine the mode in which you interact with the tool.

The following options are available in the Configuration tool:

Option	Description
-i	Required. The mode in which you interact with the tool: swing or console. Refer to "The Configuration Tool Modes" on the previous page for more information.
-f	Optional. The name and location of the properties file used to configure responses to the tool such that no interaction is necessary when running the tool. Refer to the `%CSA_HOME%\Tools\ConfigurationTool\response.properties` file for an example of a properties file and for information on the properties to configure.

To run the Configuration tool, run the following command:

```
"<csa_jre>\bin\java"  -jar configuration-tool.jar -i <mode>
-f <properties_file>
```

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

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 an Apache Web Server as a Proxy (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.

hp

Java™
COMPATIBLE