HP Cloud Service Automation

For the Linux operating system

Software Version: 4.00

Configuring an HP CSA Cluster for Server Failover

Document Release Date: January 2014

Software Release Date: January 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.

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

Contents

Chapter 1

Overview

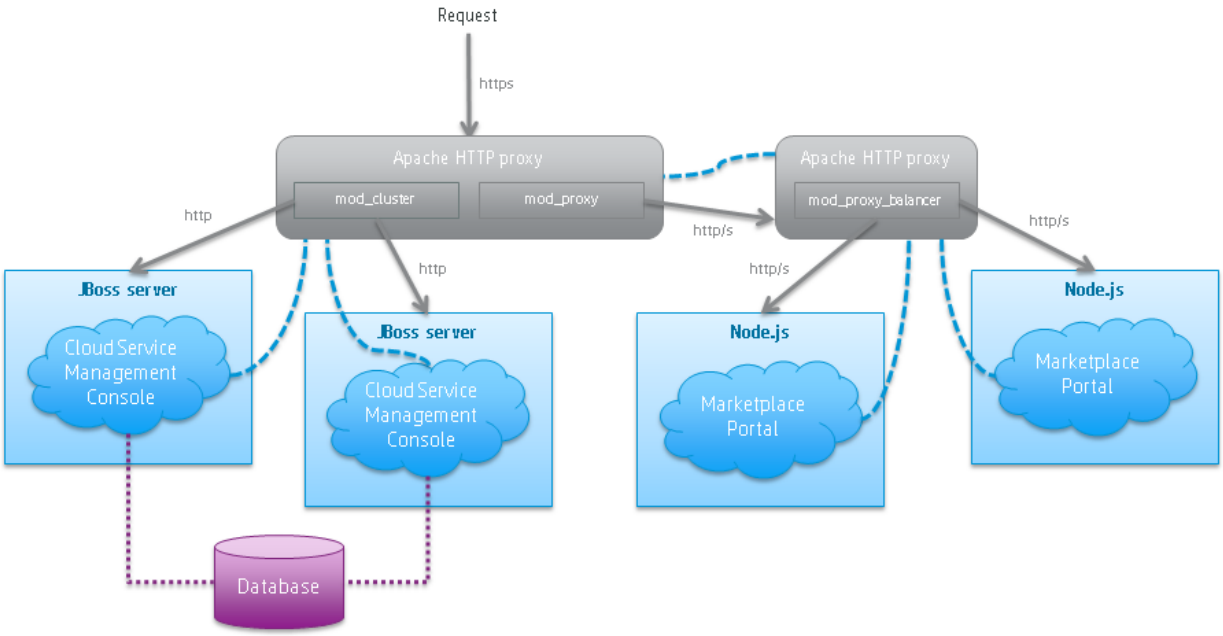
HP Cloud Service Automation (HP CSA) uses JBoss clustering technology to enable you to configure an active/active (high-availability) cluster. Clustering enables you to run HP CSA on several parallel servers called *nodes*. Cluster configurations improve performance on systems that handle high transaction 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.

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 system performance 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 three different physical (or virtual) hosts. One or more hosts may be running HP CSA in domain mode, a database, and an Apache Web server. The mod_cluster module, which is a software load balancer and is available out-of-the-box from JBoss 7.1.1, is configured on an Apache HTTP server so that web requests can be proxied into a JBoss cluster. The mod_proxy_balancer module, which is another software load balancer and is available out-of-the-box from JBoss 7.1.1, is configured on an Apache HTTP server so that web requests can be proxied into a Node.js cluster. This document, however, does not cover the load balancing features of the mod_cluster or mod_proxy_balancer modules.

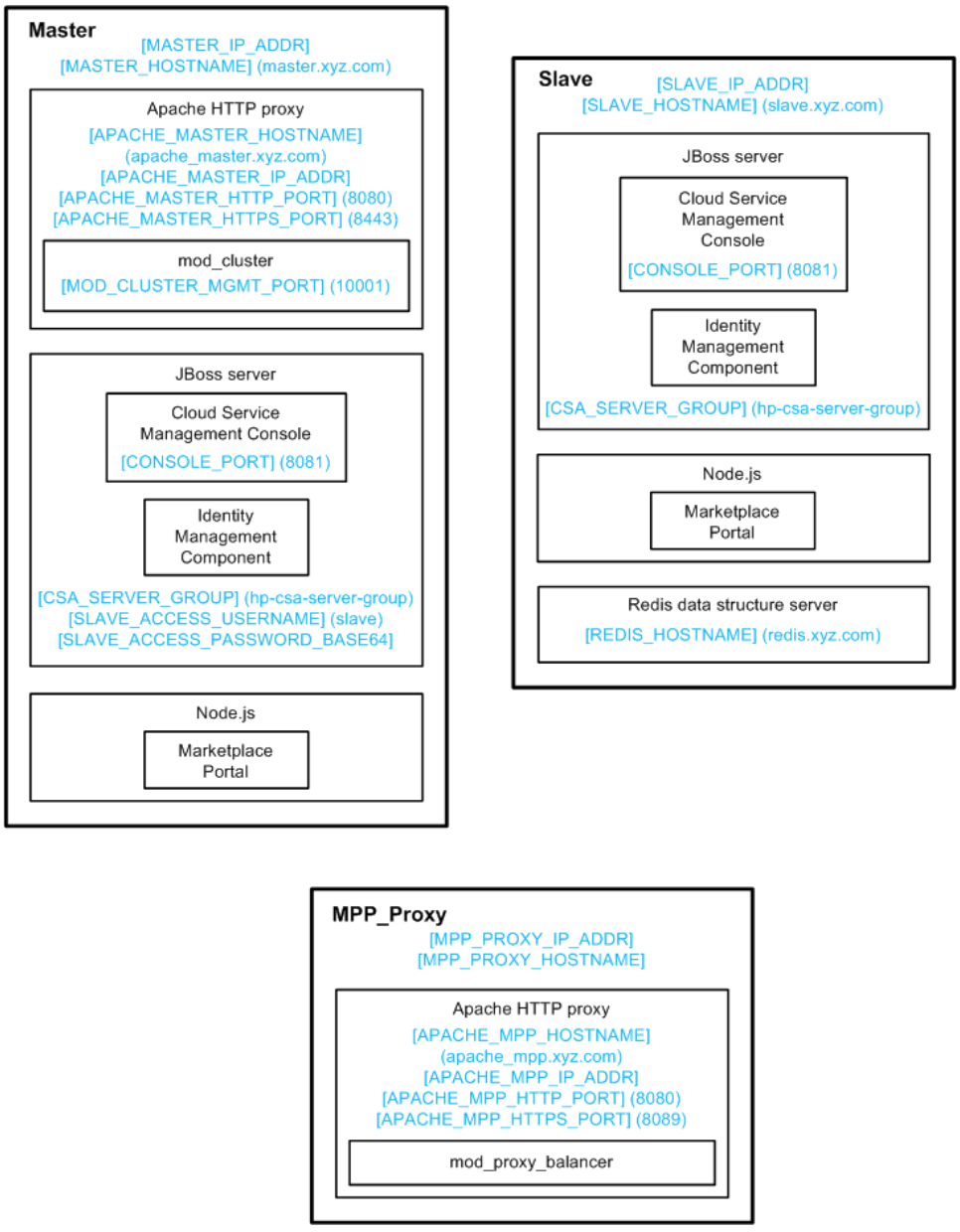
Note: Content on how to use a load balancer, database cluster, or Oracle RAC is beyond the scope of this document. For information about configuring HP CSA with Oracle RAC, refer to the *Configuring HP CSA to Work with Oracle RAC* whitepaper.



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, one node is identified as the master node, which is configured as the domain controller and hosts HP CSA and the Apache Web server with the mod_cluster module. The second node is identified as the slave node and hosts HP CSA and the Redis data structure server. The third node is identified as the MPP_Proxy node and hosts the Apache Web server with the mod_proxy_balancer module. HP CSA and the Apache Web server communicate using mod_cluster modules. Also 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).



Chapter 2

Configure the Cluster Nodes

This section describes how to install and configure the applications needed to set up nodes in a clustered environment.

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.

Configure the Marketplace Portal Proxy Node

This section describes how to install and manually configure the applications needed to set up the Marketplace Portal proxy node in an HP CSA cluster configured for server failover (how to configure the applications without using the Configuration tool).

The Marketplace Portal proxy node consists of:

- Apache HTTP Web server configured as a load balancer

Install the Apache HTTP Web Server on the Marketplace Portal Proxy Node

To install the Apache HTTP Web server on the Marketplace Portal 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.

   If you are installing the Apache HTTP server on a system running Ubuntu Linux, log in as csauser and run the following command: `sudo apt-get install apache2`

2. Verify that the following modules exist in the `/etc/httpd/modules` (Red Hat Enterprise Linux) or `/usr/lib/apache2/modules` (Ubuntu) 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 Marketplace Portal Proxy Node

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

Configure SSL on the Marketplace Portal 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:

   Red Hat Enterprise Linux

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

   Ubuntu Linux

   ```
   openssl req -new -x509 -days 365 -sha1 -newkey rsa:2048 -nodes
   -keyout /etc/apache2/cert/apache_mpp.key
   -out /etc/apache2/cert/apache_mpp.crt
   -config <path_to>/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. Load the SSL module:

   Red Hat Enterprise Linux

   a. Edit `/etc/httpd/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 `/etc/httpd/conf` directory.

Ubuntu Linux

a. Enable the SSL module. Verify the following files exist in `/etc/apache2/modules-enabled` (if they do not exist, copy them from `/etc/apache2/modules-available`):

```
ssl.conf
ssl.load
```

b. Update the SSL port used by the VirtualHost. Edit the `/etc/apache2/sites-available/default-ssl` file and update the following port entry:

```
<VirtualHost _default_:[APACHE_MPP_HTTPS_PORT]>
```

For example, if you want to change the SSL port to 8089, update the port entry to the following:

```
<VirtualHost _default_:8089>
```

c. Create a symbolic link to the `/etc/apache2/sites-available/default-ssl` directory from the `/etc/apache2/sites-enabled` directory. Run the following command:

```
ln -s /etc/apache2/sites-available/default-ssl /etc/apache2/sites-enabled/default-ssl
```

d. Start the Apache Web server:

```
sudo invoke-rc.d apache2 start
```

Configure the Apache HTTP Web Server on the Marketplace Portal Proxy Node

Red Hat Enterprise Linux

If you are running the Apache HTTP server on Red Hat Enterprise Linux, do the following:

1. Edit the `/etc/httpd/conf/httpd.conf` file:

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

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

   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 slotmem_module modules/mod_slotmem.so
```

2. Edit the `/etc/httpd/conf.d/ssl.conf` file. Set up a virtual host for the MPP_Proxy node:

```
<VirtualHost _default_:8089>
   ErrorLog /etc/httpd/logs/mpp_proxy_error.log
   TransferLog /etc/httpd/logs/mpp_proxy_access.log
   LogLevel warn
   SSLProtocol all -SSLv2
   SSLProxyEngine On
   SSLEngine on
   SSLCertificateFile /etc/httpd/conf/apache_mpp.crt
   SSLCertificateKeyFile /etc/httpd/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
   </Proxy>
   ProxyPass / balancer://mycluster/
   ProxyPassReverse / balancer://mycluster/
</VirtualHost>
```

Ubuntu Linux

If you are running the Apache HTTP server on Ubuntu Linux, do the following:

1. Log in to the system as csauser.

2. Add a port used by the Apache HTTP Server. Edit the `/etc/apache2/ports.conf` file. Change or add the following port entries:

```
NameVirutalHost *:8089
Listen 8089
```

3. In the `/usr/lib/apache2/mods-enabled` directory, create a file named `csa-ha.load` with the following contents:

```
LoadModule proxy_module /usr/lib/apache2/modules/mod_proxy.so
LoadModule proxy_ajp_module /usr/lib/apache2/modules/mod_proxy_ajp.so
LoadModule proxy_balancer_module /usr/lib/apache2/modules/mod_proxy_
```

```
balancer.so
LoadModule proxy_connect_module /usr/lib/apache2/modules/mod_proxy_connect.so

LoadModule proxy_http_module /usr/lib/apache2/modules/mod_proxy_http.so
```

4. Set up a virtual host. Add the following to the `/etc/apache2/sites-available/default-ssl.conf` file:

```
<VirtualHost _default_:8089>
   ErrorLog /etc/apache2/logs/mpp_proxy_error.log
   TransferLog /etc/apache2/logs/mpp_proxy_access.log
   LogLevel warn
   SSLProtocol all -SSLv2
   SSLProxyEngine On
   SSLEngine on
   SSLCertificateFile /etc/apache2/cert/apache_mpp.crt
   SSLCertificateKeyFile /etc/apache2/cert/apache_mpp.key
   <Proxy *>
      Order deny,allow
      Allow from all
   </Proxy>
   <Proxy balancer://mycluster/>
      BalancerMember https://[MASTER_HOSTNAME]:8089
      BalancerMember https://[SLAVE_HOSTNAME]:8089
   </Proxy>
   ProxyPass / balancer://mycluster/
   ProxyPassReverse / balancer://mycluster/
</VirtualHost>
```

Start the Apache HTTP Web Server on the Marketplace Portal Proxy Node

To start the Apache HTTP Web server, open a command prompt and type `service httpd start` (Red Hat Enterprise Linux) or `service apache2 start` (Ubuntu).

Configure the Master Node

This section describes how to install and configure the applications needed to set up the master node in an HP CSA cluster configured for server failover.

The master node consists of:

- HP CSA
- HP CSA database
- Apache HTTP Web server configured as a proxy

- mod_cluster module
- Identity Management component
- Marketplace Portal

Install HP CSA and the Apache HTTP Web Server on the Master Node

Complete the tasks in the following sections to install HP CSA and the Apache HTTP Web server on the master node.

Install HP CSA

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

- 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_MASTER_HOSTNAME]*:*[APACHE_MASTER_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).

Install the Apache HTTP Web Server and mod_cluster Module

Install the Apache HTTP Web server and mod_cluster module on the master 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.

If you are installing the Apache HTTP server on a system running Ubuntu Linux, log in as csauser and run the following command: `sudo apt-get install apache2`

2. Download the mod_cluster module from JBoss.org (http://www.jboss.org/mod_cluster/downloads).

3. Copy the following modules from the mod_cluster module into the `/etc/httpd/modules` (Red Hat Enterprise Linux) or `/usr/lib/apache2/modules` (Ubuntu) directory:

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

4. Verify that the following modules exist in the `/etc/httpd/modules` (Red Hat Enterprise Linux) or `/usr/lib/apache2/modules` (Ubuntu) directory:

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

Configure HP CSA

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 4.00 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 or upgrade to HP CSA version 4.00, when you log in to the Cloud Service Management Console, a temporary 90-day trial license is activated. Once the trial license expires, you are limited to 25 OSIs. If you created more than 25 OSIs during the trial period, you cannot create any additional OSIs. You can add more licenses at any time to increase your OSI capacity.

When you request a software license, 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 proxy server

([APACHE_MASTER_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. Mount the shared location. For example, mount the shared location to `/mnt/csa` by typing `mount -t cifs -o username=<user>, password=<pass> //sharedhost/CSA/ /mnt/csa`

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, `/mnt/csa/images`).

   Ensure that the mounted `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 mounted `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

   ln -s /mnt/csa/images images
   ```

6. Set the permissions and ownership for the `images` directory. Type the following:

   ```
   cd $CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/csa.war

   chmod 755 images
   chown csauser:csagrp 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 a given node and update the name attribute from:

```
<servers>
   <server name="hp-cloud" group="hp-csa-server-group" />
   .
   .
   .
<servers>
```

   to:

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

2. Additionally, you should rename the `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud` directory to *[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 the Apache HTTP Web Server as a Proxy

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

Configure the Apache HTTP Web Server and mod_cluster Module

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

Red Hat Enterprise Linux

If you are running the Apache HTTP server on Red Hat Enterprise Linux, do the following:

1. Edit the `/etc/httpd/conf/httpd.conf` file:

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

   ```
   Listen [APACHE_MASTER_HTTP_PORT]
   ServerName [APACHE_MASTER_HOSTNAME]:[APACHE_MASTER_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 master.xyz.com:8080
   Listen 8089
   ServerName *:8089
   ```

   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
   ```

2. Edit the `/etc/httpd/conf.d/ssl.conf` file:

   a. Set up a virtual host for the MPP_Proxy node:

```
<VirtualHost _default_:8089>
   ErrorLog /etc/httpd/logs/mpp_proxy_error.log
   TransferLog /etc/httpd/logs/mpp_proxy_access.log
   LogLevel warn
   SSLProtocol all -SSLv2
   SSLEngine on
   SSLCertificateFile /etc/httpd/conf/apache_csa.crt
   SSLCertificateKeyFile /etc/httpd/conf/apache_csa.key
   SSLProxyEngine On
   ProxyRequests Off
   ProxyPreserveHost On
   ProxyPass /https://[APACHE_MPP_HOSTNAME]:8089/
   ProxyPassReverse /https://[APACHE_MPP_HOSTNAME]:8089/
</VirtualHost>
```

   b. Set up a virtual host for mod_cluster:

```
Listen [APACHE_MASTER_IP_ADDR]:[MOD_CLUSTER_MGMT_PORT]
<VirtualHost [APACHE_MASTER_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`.

Ubuntu Linux

If you are running the Apache HTTP server on Ubuntu Linux, do the following:

1. Log in to the system as csauser.
2. Change the default port(s) used by the Apache HTTP Server. Edit the `/etc/apache2/ports.conf` file. Change or add the following port entries:

```
NameVirtualHost *:[APACHE_MASTER_HTTP_PORT]
Listen [APACHE_MASTER_HTTP_PORT]
NameVirutalHost *:[MOD_CLUSTER_MGMT_PORT]
Listen [MOD_CLUSTER_MGMT_PORT]
NameVirutalHost *:8089
Listen 8089
<IfModule mod_ssl.c>
   NameVirtualHost *:[APACHE_MASTER_HTTPS_PORT]
   Listen [APACHE_MASTER_HTTPS_PORT]
</IfModule>
<IfModule mod_gnutls.c>
   Listen [APACHE_MASTER_HTTPS_PORT]
</IfModule>
```

   For example, if you want to change the default port to 8080, the mod_cluster management port to 10001, and the SSL port to 8443, update the port entries to the following:

```
NameVirtualHost *:8080
Listen 8080
NameVirutalHost *:10001
Listen 10001
NameVirutalHost *:8089
Listen 8089
<IfModule mod_ssl.c>
   NameVirtualHost *:8443
   Listen 8443
</IfModule>
<IfModule mod_gnutls.c>
   Listen 8443
</IfModule>
```

3. In the `/usr/lib/apache2/mods-enabled` directory, create a file named `csa-ha.load` with the following contents:

```
LoadModule proxy_module /usr/lib/apache2/modules/mod_proxy.so
LoadModule proxy_ajp_module /usr/lib/apache2/modules/mod_proxy_ajp.so
LoadModule advertise_module /usr/lib/apache2/modules/mod_advertise.so
LoadModule manager_module /usr/lib/apache2/modules/mod_manager.so
```

```
LoadModule proxy_cluster_module /usr/lib/apache2/modules/mod_proxy_cluster.so
LoadModule proxy_connect_module /usr/lib/apache2/modules/mod_proxy_connect.so
LoadModule proxy_http_module /usr/lib/apache2/modules/mod_proxy_http.so
LoadModule slotmem_module /usr/lib/apache2/modules/mod_slotmem.so
```

4. Remove the following files from `/etc/apache2/modules-enabled` (if they exist):

```
proxy_ajp.load
proxy_balancer.load
proxy.load
```

5. Set up a virtual host for the MPP_Proxy node. Add the following to the `/etc/apache2/sites-enabled/default-ssl.conf` file:

```
<VirtualHost _default_:8089>
   ErrorLog /etc/apache2/logs/mpp_proxy_error.log
   TransferLog /etc/apache2/logs/mpp_proxy_access.log
   LogLevel warn
   SSLProtocol all -SSLv2
   SSLEngine on
   SSLCertificateFile /etc/apache2/cert/apache_csa.crt
   SSLCertificateKeyFile /etc/apache2/cert/apache_csa.key
   SSLProxyEngine On
   ProxyRequests Off
   ProxyPreserveHost On
   ProxyPass /https://[APACHE_MPP_HOSTNAME]:8089/
   ProxyPassReverse /https://[APACHE_MPP_HOSTNAME]:8089/
</VirtualHost>
```

6. Set up a virtual host for mod_cluster in the `/etc/apache2/sites-enabled` directory by creating a file named `001-default` with the following contents:

```
<VirtualHost [APACHE_MASTER_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

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:

   Red Hat Enterprise Linux

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

   Ubuntu Linux

   ```
   openssl req -new -x509 -days 365 -sha1 -newkey rsa:2048 -nodes
   -keyout /etc/apache2/cert/apache_csa.key
   -out /etc/apache2/cert/apache_csa.crt
   -config <path_to>/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 `$CSA_HOME/jboss-as-7.1.1.Final/domain/configuration` directory on the slave node.

3. Load the SSL module:

   Red Hat Enterprise Linux

   a. Edit `/etc/httpd/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 `/etc/httpd/conf` directory. Verify that their location is correctly specified in the `/etc/httpd/conf/extra/httpd-ssl.conf` file.

```
SSLCertificateFile /etc/httpd/conf/apache_csa.crt
SSLCertificateKeyFile /etc/httpd/conf/apache_csa.key
```

c. If needed, change the port in `/etc/httpd/conf/extra/httpd-ssl.conf` (for example, use port 8443 instead of the default port).

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

Ubuntu Linux

a. Enable the SSL module. Verify the following files exist in `/etc/apache2/modules-enabled` (if they do not exist, copy them from `/etc/apache2/modules-available`):

```
ssl.conf
ssl.load
```

b. Update the SSL port used by the VirtualHost. Edit the `/etc/apache2/sites-available/default-ssl` file and update the following port entry:

```
<VirtualHost _default_:[APACHE_MASTER_HTTPS_PORT]>
```

For example, if you want to change the SSL port to 8443, update the port entry to the following:

```
<VirtualHost _default_:8443>
```

c. Create a symbolic link to the `/etc/apache2/sites-available/default-ssl` directory from the `/etc/apache2/sites-enabled` directory. Run the following command:

```
ln -s /etc/apache2/sites-available/default-ssl /etc/apache2/sites-enabled/default-ssl
```

d. Start the Apache Web server:

```
sudo invoke-rc.d apache2 start
```

Run the Configuration tool

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 guide shows how to configure the Apache Web server as a proxy for HP CSA on the master node (based on the diagram in the overview of this guide) and configure the master

node. You may also configure the Apache Web server as a proxy on the slave node or on a remote system instead. However, examples for these configurations are not provided.

The examples in this section also show running the Configuration tool in console mode. Examples on how to run the Configuration tool in other modes are not provided.

To set up the master node by configuring 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_HOME/bin/java -jar configuration-tool.jar -i console`

2. Select a configuration option

   Set up an HP CSA clustered node. Select **1** and **enter**.

3. Verify your selection and select **enter** to continue.

4. Configure an HP CSA Cluster Node

   Configure the master node. Type **master** and select **enter**.

5. Use an Existing Apache Web Server as a Proxy for HP CSA

   Configure an Apache Web server as a proxy. Type **y** and select **enter**.

6. Verify your selections. You should have selected to configure a master node and an existing Apache Web server as a proxy on an HP CSA clustered node. If you made any errors in your selections, select **b** and **enter** to return to the Select a configuration option screen. To continue the configuration, select **enter**.

7. 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.
Mod Cluster Port		Required. The port used as the mod_cluster management port (for example, 10001).
Configured with SSL		Optional. Type **y** 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).

Field		Description
	Import Certificate	The file name and location of the certificate and key for the Apache Web server to be imported into HP CSA's truststore. You can specify a self-signed certificate (typically used in a test environment only) or Apache Web server's Certificate Authority-signed certificate. 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).
HTTP Port (if SSL not configured)		Required. The port used by the Apache Web server if the Apache Web server does not communicate with HP CSA over SSL (for example, 8080).

8. Select **enter** to continue configuring the master node. If you need to update any information, type **b** and select **enter** to return to the Configure an HP CSA Cluster Node screen to re-enter the information.

9. Configure the Master Node

   Enter the following information:

Field	Description
IP Address or Hostname	Required. The IP address or fully-qualified domain name of the master node.
Cluster Nodename	Required. A unique name that identifies this node in the cluster.

10. Add JBoss Management Users

    Add one or more JBoss Management users in the ManagementRealm of JBoss. At least one JBoss Management user must exist.

    If the Configuration tool detects a JBoss Management user, you will be prompted if you want to add another user. Type **y** to add another user or **n** to continue to the next screen.

    If no users are detected, enter the following information:

Field	Description
User Name	The name of a user who can access the JBoss Management Web interface. You must create at least one user who can connect to the master node from the 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` 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.
Password	The password of the JBoss Management User.

11. Create another JBoss Management User

    After you create a JBoss Management user, you may create another Management user. If you did not create a user, this screen does not display.

    Type **y** and select **enter** to add another JBoss Management User or type **n** and select **enter** if you do not want to add another user.

12. Select **enter** to display the information you just configured. Or, if you need to update any information, type **b** and select **enter** to return to the Use an Existing Apache Web Server as a Proxy for HP CSA screen to re-enter the information.

13. Verify the information you just configured. If you need to update any information, type **b** and select **enter** to return to the Configure the Master Node screen to re-enter the information. If the information is correct, select **enter**.

14. On the master node, re-launch the Configuration tool:

    Type `$CSA_JRE_HOME/bin/java -jar configuration-tool.jar -i console`

15. Select a configuration option

    Set up a Marketplace Portal clustered node. Select **2** and **enter**.

16. Use an Existing Apache Web Server as a Proxy

    Configure an Apache Web server as a proxy. Type **y** and select **enter**.

17. Verify your selection. You should have selected to set up a Marketplace Portal clustered node and an existing Apache Web server as a proxy on the HP CSA clustered node. If you made any errors in your selections, select **ctrl c** to exit the Configuration tool and start over. To continue the configuration, select **enter**.

18. Use an Existing Apache Web Server as a Proxy for Marketplace Portal

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.
Configured with SSL	Optional. Select **yes** if you want the Apache Web server on the Marketplace Portal proxy node to communicate with the Marketplace Portal over SSL or **no** if SSL is not required.
HTTP(S) Port	Required. The port used by the Apache Web server on the Marketplace Portal proxy node (for example, 8080 (HTTP) or 8089 (HTTPS)).
Import Certificate	Required. Import the SSL certificate for HP CSA. If HP CSA is in a clustered environment using the Apache Web server as a proxy, enter the SSL certificate of the Apache Web server as a proxy for the Marketplace Portal.

19. Select **enter** to continue configuring the slave node. If you need to update any information, type **b** and select **enter** to return to the Select a configuration option screen to re-enter the information.

20. Configure a Marketplace Portal Node

    Enter the following information:

Field	Description
Redis Data Structure Server	
IP Address or Hostname	Required. The IP address or fully-qualified domain name of the Redis data structure server.
Port	Required. The port used by the Redis data structure server.
CSA Provider	
IP Address or Hostname	Required. The IP address or fully-qualified domain name of the system that hosts HP CSA. If the HP CSA Provider in a clustered environment using the Apache Web server as a proxy, enter the IP address or fully-qualified domain name of the Apache Web server.
Port	Required. The port used by the system that hosts HP CSA. If the HP CSA Provider is in a clustered environment using the Apache Web server as a proxy, enter the port of the Apache Web server.
Identity Management Component	

Field	Description
IP Address or Hostname	Required. The IP address or fully-qualified domain name of the system that hosts HP CSA. If the Identity Management Component is in a clustered environment using the Apache Web server as a proxy, enter the IP address or fully-qualified domain name of the Apache Web server.
Port	Required. The port used by the system that hosts HP CSA. If the Identity Management Component is in a clustered environment using the Apache Web server as a proxy, enter the port of the Apache Web server.
Import HP CSA Certificate	
Import	Required. Import the SSL certificate for HP CSA. If HP CSA is in a clustered environment using the Apache Web server as a proxy, enter the SSL certificate of the Apache Web server as a proxy for HP CSA.

21. Select **enter** to display the information you just configured. Or, if you need to update any information, type **b** and select **enter** to return to the Select a configuration option screen to re-enter the information.

22. Verify the information you just configured. If you need to update any information, type **b** and select **enter** to return to the Configure a Marketplace Portal Node screen to re-enter the information. If the information is correct, select **enter**.

Stop and Start the Applications on the Master Node

Stop HP CSA

By default, HP CSA is automatically started in standalone mode. You must stop HP CSA that is running in standalone mode before you can start HP CSA in domain mode. To stop HP CSA, on the system that hosts HP CSA, open a command prompt and type `service csa stop`.

Start HP CSA

To start the HP CSA server in domain mode on the master node:

1. Open a command prompt and navigate to `$CSA_HOME/jboss-as-7.1.1.Final/bin`.

2. Type `./domain.sh`.

   JBoss will start and deploy the "hp-cloud" server. You should see the message `JBAS010919: Registering server hp-cloud` display on the console.

   If the following error message displays:

   ```
   JBAS012144: Could not connect to remote://<localhost>:9999. The connection timed out
   ```

verify that the "hp-cloud" server has been deployed by using the JBoss Web Management Interface or pointing a browser to `http://[APACHE_MASTER_HOSTNAME]:8081/csa`.

This is a known issue with JBoss on slow systems (see https://issues.jboss.org/browse/AS7-3524?page=com.atlassian.jirafisheyeplugin:fisheye-issuepanel&_sscc=t for more information).

Start Marketplace Portal

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

Start the Apache HTTP Web Server

To start the Apache HTTP Web server, open a command prompt and type `service httpd start` (Red Hat Enterprise Linux) or `service apache2 start` (Ubuntu).

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 server failover.

The slave node consists of:

- HP CSA
- Identity Management component
- Marketplace Portal
- Redis data structure server

Install HP CSA and the Redis Data Structure Server on the Slave Node

Complete the tasks in the following sections to install HP CSA and the Redis data structure server on the slave node.

Install HP CSA

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

- 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_MASTER_HOSTNAME]*:*[APACHE_MASTER_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).

Install the Redis Data Structure Server on the Slave Node

Install the Redis data structure server on the slave node only. To install the Redis data structure server:

Download and install the Redis data structure server from redis.io (http://download.redis.io/releases/redis-2.6.16.tar.gz).

Follow the instructions at http://redis.io/download to extract and compile the Redis data structure server.

Configure HP CSA

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. Mount the shared location. For example, mount the shared location to `/mnt/csa` by typing `mount -t cifs -o username=<user>, password=<pass> //sharedhost/CSA/ /mnt/csa`
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 mounted `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
   ln -s /mnt/csa/images images
   ```

4. Set the permissions and ownership for the `images` directory. Type the following:

   ```
   cd $CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/csa.war

   chmod 755 images
   chown csauser:csagrp 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 a given node and update the name attribute from:

   ```
   <servers>
      <server name="hp-cloud" group="hp-csa-server-group" />
      .
      .
      .
   <servers>
   ```

   to:

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

2. Additionally, you should rename the `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud` directory to *[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

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_
   MASTER_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

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_HOME/lib/security/cacerts
   ```

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

Run the Configuration tool

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 console 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_HOME/bin/java -jar configuration-tool.jar -i console`
2. Select a configuration option

   Set up an HP CSA clustered node. Select **1** and **enter**.
3. Verify your selection and select **enter** to continue.
4. Configure an HP CSA Cluster Node

Configure the slave node. Type **slave** and select **enter**.

5. Use an Existing Apache Web Server as a Proxy

   Configure the Apache Web server as a proxy. Type **y** and select **enter**.

6. Verify your selections. You should have selected to configure a slave node and an existing Apache Web server as a proxy on the HP CSA cluster node. If you made any errors in your selections, select **b** and **enter** to return to the Select a configuration option screen. To continue the configuration, select **enter**.

7. Use an 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.
Mod Cluster Port	Required. The port used as the mod_cluster management port (for example, 10001).
Configured with SSL	Optional. Select **yes** if you want the Apache Web server on the Marketplace Portal proxy node to communicate with the Marketplace Portal over SSL or **no** if SSL is not required.
HTTP(S) Port	Required. The port used by the Apache Web server on the Marketplace Portal proxy node (for example, 8080 (HTTP) or 8089 (HTTPS)).
Import HP CSA Certificate	
Import Certificate	Required. Import the SSL certificate for HP CSA. If HP CSA is in a clustered environment using the Apache Web server as a proxy, enter the SSL certificate of the Apache Web server as a proxy for HP CSA.

8. Select **enter** to continue configuring the slave node. If you need to update any information, type **b** and select **enter** to return to the Configure an HP CSA Cluster Node screen to re-enter the information.

9. Configure the Slave Node

   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. A unique name that identifies this node in the cluster.
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).

10. Select **enter** to continue configuring the slave node. If you need to update any information, type **b** and select **enter** to return to the Configure an HP CSA Cluster Node screen to re-enter the information.

11. Verify the information you just configured. If you need to update any information, type **b** and select **enter** to return to the Configure the Slave Node screen to re-enter the information. If the information is correct, select **enter**.

12. On the slave node, re-launch the Configuration tool:

    Type `$CSA_JRE_HOME/bin/java -jar configuration-tool.jar -i console`

13. Select a configuration option

    Set up a Marketplace Portal clustered node. Select **2** and **enter**.

14. Use an Existing Apache Web Server as a Proxy

    Configure an Apache Web server as a proxy. Type **y** and select **enter**.

15. Verify your selection. You should have selected to set up a Marketplace Portal clustered node and an existing Apache Web server as a proxy on the HP CSA clustered node. If you made any errors in your selections, select **ctrl c** to exit the Configuration tool and start over. To continue the configuration, select **enter**.

16. Use an Existing Apache Web Server as a Proxy for Marketplace Portal

    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.
Configured with SSL	Optional. Select **yes** if you want the Apache Web server on the Marketplace Portal proxy node to communicate with the Marketplace Portal over SSL or **no** if SSL is not required.
HTTP(S) Port	Required. The port used by the Apache Web server on the Marketplace Portal proxy node (for example, 8080 (HTTP) or 8089 (HTTPS)).
Import Certificate	Required. Import the SSL certificate for HP CSA. If HP CSA is in a clustered environment using the Apache Web server as a proxy, enter the SSL certificate of the Apache Web server as a proxy for the Marketplace Portal.

17. Select **enter** to continue configuring the slave node. If you need to update any information, type **b** and select **enter** to return to the Select a configuration option screen to re-enter the information.

18. Configure a Marketplace Portal Node

    Enter the following information:

Field	Description
Redis Data Structure Server	
IP Address or Hostname	Required. The IP address or fully-qualified domain name of the Redis data structure server.
Port	Required. The port used by the Redis data structure server.
CSA Provider	
IP Address or Hostname	Required. The IP address or fully-qualified domain name of the system that hosts HP CSA. If the HP CSA Provider in a clustered environment using the Apache Web server as a proxy, enter the IP address or fully-qualified domain name of the Apache Web server.
Port	Required. The port used by the system that hosts HP CSA. If the HP CSA Provider is in a clustered environment using the Apache Web server as a proxy, enter the port of the Apache Web server.

Field	Description
Identity Management Component	
IP Address or Hostname	Required. The IP address or fully-qualified domain name of the system that hosts HP CSA. If the Identity Management Component is in a clustered environment using the Apache Web server as a proxy, enter the IP address or fully-qualified domain name of the Apache Web server.
Port	Required. The port used by the system that hosts HP CSA. If the Identity Management Component is in a clustered environment using the Apache Web server as a proxy, enter the port of the Apache Web server.
Import HP CSA Certificate	
Import	Required. Import the SSL certificate for HP CSA. If HP CSA is in a clustered environment using the Apache Web server as a proxy, enter the SSL certificate of the Apache Web server as a proxy for HP CSA.

19. Select **enter** to display the information you just configured. Or, if you need to update any information, type **b** and select **enter** to return to the Select a configuration option screen to re-enter the information.

20. Verify the information you just configured. If you need to update any information, type **b** and select **enter** to return to the Configure a Marketplace Portal Node screen to re-enter the information. If the information is correct, select **enter**.

Stop and Start the Applications on the Slave Node

Stop HP CSA

By default, HP CSA is automatically started in standalone mode. You must stop HP CSA that is running in standalone mode before you can start HP CSA in domain mode. To stop HP CSA, on the system that hosts HP CSA, open a command prompt and type `service csa stop`.

Start HP CSA

To start the HP CSA server in domain mode on the slave node:

1. Open a command prompt and navigate to `$CSA_HOME/jboss-as-7.1.1.Final/bin`.

2. Type `./domain.sh`.

   On the console of the master node, you should see the following message when the slave node starts:

   ```
   JBAS010918: Registered remote slave host "slave"
   ```

   If a message similar to the following displays:

```
17:07:08,898 ERROR [org.jboss.as] (Controller Boot Thread) JBAS015875: JBoss
AS 7.1.1.Final "Brontes" started (with errors) in 8266ms - Started 149 of 276
services (4 services failed or missing dependencies, 122 services are passive
or on-demand)
```

you can safely ignore the message.

Start Marketplace Portal

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

Start the Redis Data Structure Server

To start the Redis data structure server, do the following:

1. Open a command prompt and navigate to `<path_to>/src/redis`.
2. Type **./redis-server &**.

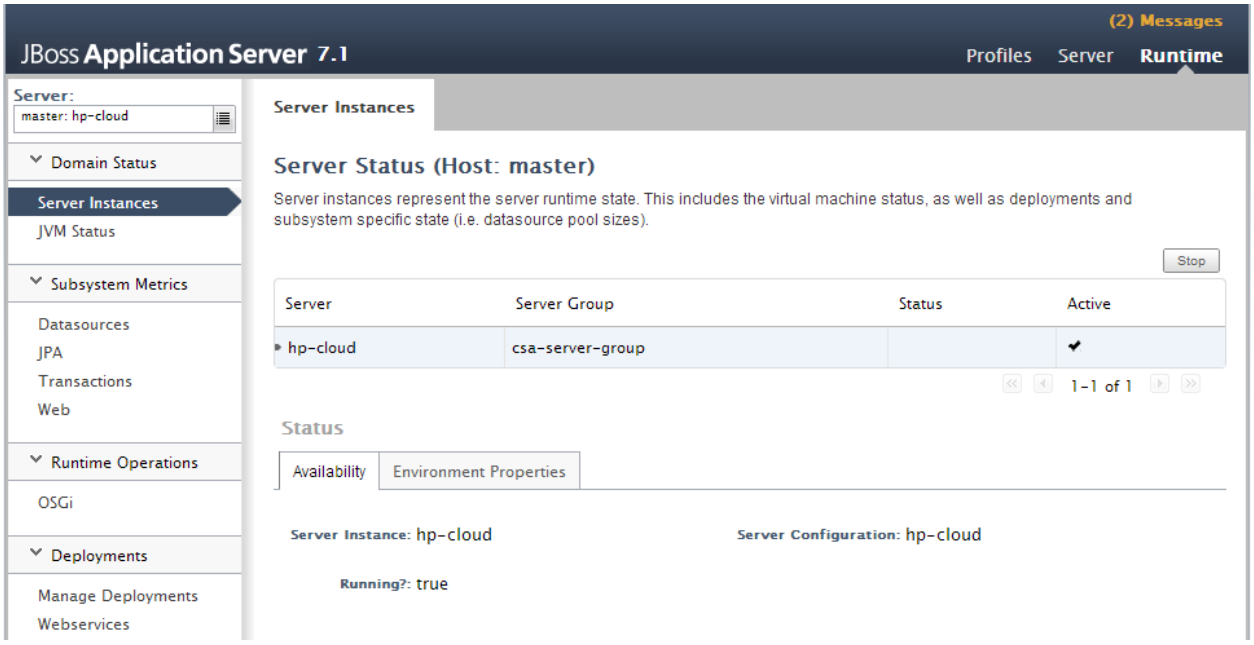
Chapter 3

Validate the JBoss Cluster Configuration

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

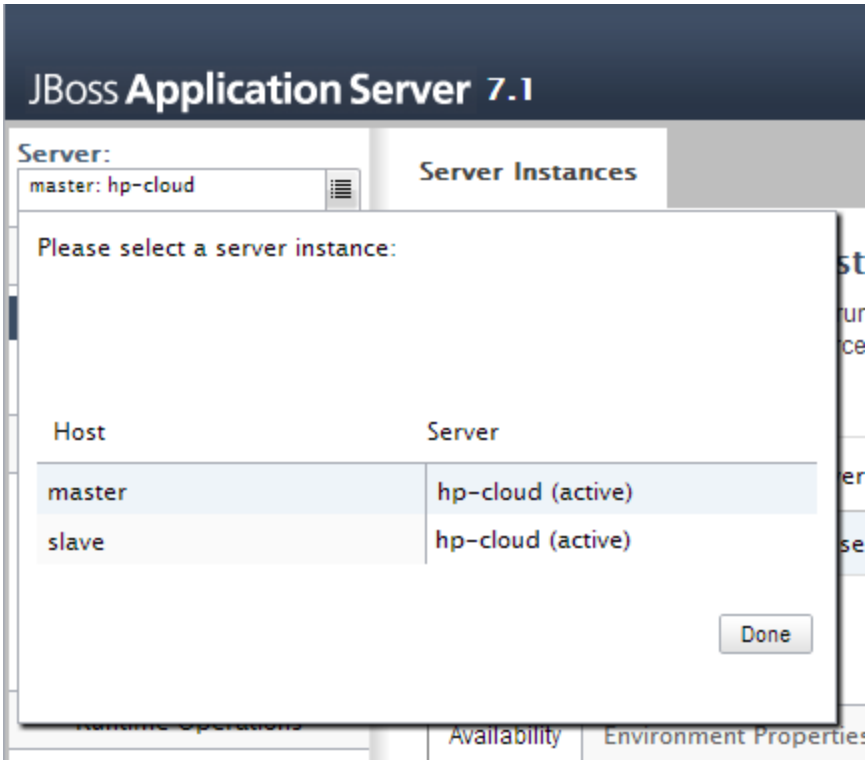
To connect to the Web Management Interface:

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



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

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



Chapter 4

Common Tasks

This chapter provides information on how to perform common tasks.

Tasks include:

Start HP CSA in Domain Mode

To start the HP CSA server in domain mode on the master node:

1. Open a command prompt and navigate to `$CSA_HOME/jboss-as-7.1.1.Final/bin`.
2. Type `./domain.sh`.

   JBoss will start and deploy the "hp-cloud" server. You should see the message `JBAS010919: Registering server hp-cloud` display on the console.

   If the following error message displays:

   ```
   JBAS012144: Could not connect to remote://<localhost>:9999. The connection timed out
   ```

   verify that the "hp-cloud" server has been deployed by using the JBoss Web Management Interface or pointing a browser to `http://[APACHE_MASTER_HOSTNAME]:8081/csa`.

   This is a known issue with JBoss on slow systems (see https://issues.jboss.org/browse/AS7-3524?page=com.atlassian.jirafisheyeplugin:fisheye-issuepanel&_sscc=t for more information).

To start the HP CSA server in domain mode on the slave node:

1. Open a command prompt and navigate to `$CSA_HOME/jboss-as-7.1.1.Final/bin`.
2. Type `./domain.sh`.

   On the console of the master node, you should see the following message when the slave node starts:

```
JBAS010918: Registered remote slave host "slave"
```

If a message similar to the following displays:

```
17:07:08,898 ERROR [org.jboss.as] (Controller Boot Thread) JBAS015875: JBoss
AS 7.1.1.Final "Brontes" started (with errors) in 8266ms - Started 149 of 276
services (4 services failed or missing dependencies, 122 services are passive
or on-demand)
```

you can safely ignore the message.

Stop HP CSA in Domain Mode

To stop HP CSA in domain mode:

1. From a command prompt, navigate to `$CSA_HOME/jboss-as-7.1.1.Final/bin/`.
2. Type `jboss-cli.sh --connect --command=:shutdown`

Start Marketplace Portal

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

Stop 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, open a command prompt and type `service httpd start` (Red Hat Enterprise Linux) or `service apache2 start` (Ubuntu).

Stop the Apache HTTP Web server

To stop the Apache HTTP Web server, open a command prompt and type `service httpd stop` (Red Hat Enterprise Linux) or `service apache2 stop` (Ubuntu).

Start the Redis data structure server

To start the Redis data structure server, do the following:

1. Open a command prompt and navigate to `<path_to>/src/redis`.
2. Type **./redis-server &**.

Launch the Cloud Service Management Console

To launch the Cloud Service Management Console through the proxy:

- Open `http://[APACHE_MASTER_HOSTNAME]:[APACHE_MASTER_HTTP_PORT]/csa` in a supported browser. For example, `http://apache_master.xyz.com:8080/csa`
- (SSL) Open `https://[APACHE_MASTER_HOSTNAME]:[APACHE_MASTER_HTTPS_PORT]/csa` in a supported browser. For example, `https://apache_master.xyz.com:8443/csa`

To launch the Cloud Service Management Console directly from the master node:

- Open `http://[MASTER_HOSTNAME]:[CONSOLE_PORT]/csa` in a supported browser. For example, `http://master.xyz.com:8081/csa`

To launch the Cloud Service Management Console directly from the slave node:

- Open `http://[SLAVE_HOSTNAME]:[CONSOLE_PORT]/csa` in a supported browser. For example, `http://slave.xyz.com:8081/csa`

Launch the Marketplace Portal

To launch the Marketplace Portal through the proxy:

- Open `http://[APACHE_MASTER_HOSTNAME]:8089` in a supported browser. For example, `http://apache_master.xyz.com:8089`
- (SSL) Open `https://[APACHE_MASTER_HOSTNAME]:[APACHE_MASTER_HTTPS_PORT]/mpp` in a supported browser. For example, `http://apache_master.xyz.com:8443/mpp`

To launch the Marketplace Portal directly from the master node:

- Open `https://[MASTER_HOSTNAME]:8089` in a supported browser. For example, `http://master.xyz.com:8089`

To launch the Marketplace Portal directly from the slave node:

- Open `http://[SLAVE_HOSTNAME]:8089` in a supported browser. For example, `http://slave.xyz.com:8089`

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 45 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 44 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

Manually Configure an HP CSA Cluster for Server Failover

This appendix describes how to install and manually configure the applications needed to set up the master, slave, and MPP_Proxy nodes in a clustered environment (configuring the applications without using the Configuration tool).

Complete the following:

1. "Configure the Master Node" on page 16
2. "Configure the Slave Node" on page 32
3. "Configure the Marketplace Portal Proxy Node" on page 12

Configure the Marketplace Portal Proxy Node

This section describes how to install and manually configure the applications needed to set up the Marketplace Portal proxy node in an HP CSA cluster configured for server failover (how to configure the applications without using the Configuration tool).

The Marketplace Portal proxy node consists of:

- Apache HTTP Web server configured as a load balancer

Install the Apache HTTP Web Server on the Marketplace Portal Proxy Node

To install the Apache HTTP Web server on the Marketplace Portal 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.

   If you are installing the Apache HTTP server on a system running Ubuntu Linux, log in as csauser and run the following command: `sudo apt-get install apache2`

2. Verify that the following modules exist in the `/etc/httpd/modules` (Red Hat Enterprise Linux) or `/usr/lib/apache2/modules` (Ubuntu) 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 Marketplace Portal Proxy Node

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

Configure SSL on the Marketplace Portal 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:

   Red Hat Enterprise Linux

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

   Ubuntu Linux

   ```
   openssl req -new -x509 -days 365 -sha1 -newkey rsa:2048 -nodes
   -keyout /etc/apache2/cert/apache_mpp.key
   -out /etc/apache2/cert/apache_mpp.crt
   -config <path_to>/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. Load the SSL module:

   Red Hat Enterprise Linux

   a. Edit `/etc/httpd/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 `/etc/httpd/conf` directory.

Ubuntu Linux

a. Enable the SSL module. Verify the following files exist in `/etc/apache2/modules-enabled` (if they do not exist, copy them from `/etc/apache2/modules-available`):

```
ssl.conf
ssl.load
```

b. Update the SSL port used by the VirtualHost. Edit the `/etc/apache2/sites-available/default-ssl` file and update the following port entry:

```
<VirtualHost _default_:[APACHE_MPP_HTTPS_PORT]>
```

For example, if you want to change the SSL port to 8089, update the port entry to the following:

```
<VirtualHost _default_:8089>
```

c. Create a symbolic link to the `/etc/apache2/sites-available/default-ssl` directory from the `/etc/apache2/sites-enabled` directory. Run the following command:

```
ln -s /etc/apache2/sites-available/default-ssl /etc/apache2/sites-enabled/default-ssl
```

d. Start the Apache Web server:

```
sudo invoke-rc.d apache2 start
```

Configure the Apache HTTP Web Server on the Marketplace Portal Proxy Node

Red Hat Enterprise Linux

If you are running the Apache HTTP server on Red Hat Enterprise Linux, do the following:

1. Edit the `/etc/httpd/conf/httpd.conf` file:

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

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

   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 slotmem_module modules/mod_slotmem.so
```

2. Edit the `/etc/httpd/conf.d/ssl.conf` file. Set up a virtual host for the MPP_Proxy node:

```
<VirtualHost _default_:8089>
   ErrorLog /etc/httpd/logs/mpp_proxy_error.log
   TransferLog /etc/httpd/logs/mpp_proxy_access.log
   LogLevel warn
   SSLProtocol all -SSLv2
   SSLProxyEngine On
   SSLEngine on
   SSLCertificateFile /etc/httpd/conf/apache_mpp.crt
   SSLCertificateKeyFile /etc/httpd/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
   </Proxy>
   ProxyPass / balancer://mycluster/
   ProxyPassReverse / balancer://mycluster/
</VirtualHost>
```

Ubuntu Linux

If you are running the Apache HTTP server on Ubuntu Linux, do the following:

1. Log in to the system as csauser.

2. Add a port used by the Apache HTTP Server. Edit the `/etc/apache2/ports.conf` file. Change or add the following port entries:

```
NameVirutalHost *:8089
Listen 8089
```

3. In the `/usr/lib/apache2/mods-enabled` directory, create a file named `csa-ha.load` with the following contents:

```
LoadModule proxy_module /usr/lib/apache2/modules/mod_proxy.so
LoadModule proxy_ajp_module /usr/lib/apache2/modules/mod_proxy_ajp.so
LoadModule proxy_balancer_module /usr/lib/apache2/modules/mod_proxy_
```

```
balancer.so
LoadModule proxy_connect_module /usr/lib/apache2/modules/mod_proxy_connect.so

LoadModule proxy_http_module /usr/lib/apache2/modules/mod_proxy_http.so
```

4. Set up a virtual host. Add the following to the `/etc/apache2/sites-available/default-ssl.conf` file:

```
<VirtualHost _default_:8089>
   ErrorLog /etc/apache2/logs/mpp_proxy_error.log
   TransferLog /etc/apache2/logs/mpp_proxy_access.log
   LogLevel warn
   SSLProtocol all -SSLv2
   SSLProxyEngine On
   SSLEngine on
   SSLCertificateFile /etc/apache2/cert/apache_mpp.crt
   SSLCertificateKeyFile /etc/apache2/cert/apache_mpp.key
   <Proxy *>
      Order deny,allow
      Allow from all
   </Proxy>
   <Proxy balancer://mycluster/>
      BalancerMember https://[MASTER_HOSTNAME]:8089
      BalancerMember https://[SLAVE_HOSTNAME]:8089
   </Proxy>
   ProxyPass / balancer://mycluster/
   ProxyPassReverse / balancer://mycluster/
</VirtualHost>
```

Start the Apache HTTP Web Server on the Marketplace Portal Proxy Node

To start the Apache HTTP Web server, open a command prompt and type `service httpd start` (Red Hat Enterprise Linux) or `service apache2 start` (Ubuntu).

Configure the Master Node

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

The master node consists of:

- HP CSA
- HP CSA database
- Apache HTTP Web server configured as a proxy

- mod_cluster module
- Identity Management component
- Marketplace Portal

Install HP CSA and the Apache HTTP Web Server on the Master Node

Complete the tasks in the following sections to install HP CSA and the Apache HTTP Web server 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 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_MASTER_HOSTNAME]*:*[APACHE_MASTER_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).

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

Install the Apache HTTP Web server and mod_cluster module on the master 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.

If you are installing the Apache HTTP server on a system running Ubuntu Linux, log in as csauser and run the following command: `sudo apt-get install apache2`

2. Download the mod_cluster module from JBoss.org (http://www.jboss.org/mod_cluster/downloads).

3. Copy the following modules from the mod_cluster module into the `/etc/httpd/modules` (Red Hat Enterprise Linux) or `/usr/lib/apache2/modules` (Ubuntu) directory:

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

4. Verify that the following modules exist in the `/etc/httpd/modules` (Red Hat Enterprise Linux) or `/usr/lib/apache2/modules` (Ubuntu) directory:

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

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.

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_MASTER_HOSTNAME]
csa.provider.port=[APACHE_MASTER_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
```

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 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" 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 two users in the ManagementRealm of the JBoss server on the master node. One user allows the slave node to connect to the master node. The second user is used to access the JBoss Management Web interface.

To configure the users:

1. Navigate to `$CSA_HOME/jboss-as-7.1.1.Final/bin` and run the `add-user.sh` script.
2. When prompted, create a Management User in the ManagementRealm named "slave". This user may also be referred to as *[SLAVE_ACCESS_USERNAME]* in examples in this guide.
3. Specify a password for this user. After you've created the user, encode the password in a base64 format. This password may be referred to as *[SLAVE_ACCESS_PASSWORD_BASE64]* in examples in this guide.
4. Create another Management User in the ManagementRealm named "admin" or "csaadmin".
5. Specify a password. You can use this user to access the JBoss Management Web interface.

Request a Software License

HP CSA version 4.00 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 or upgrade to HP CSA version 4.00, when you log in to the Cloud Service Management Console, a temporary 90-day trial license is activated. Once the trial license expires, you are limited to 25 OSIs. If you created more than 25 OSIs during the trial period, you cannot create any additional OSIs. You can add more licenses at any time to increase your OSI capacity.

When you request a software license, 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 proxy server

([APACHE_MASTER_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. Mount the shared location. For example, mount the shared location to `/mnt/csa` by typing `mount -t cifs -o username=<user>, password=<pass> //sharedhost/CSA/ /mnt/csa`

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, `/mnt/csa/images`).

   Ensure that the mounted `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 mounted `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

   ln -s /mnt/csa/images images
   ```

6. Set the permissions and ownership for the `images` directory. Type the following:

   ```
   cd $CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/csa.war

   chmod 755 images
   chown csauser:csagrp 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 a given node and update the name attribute from:

```
<servers>
   <server name="hp-cloud" group="hp-csa-server-group" />
   .
   .
   .
<servers>
```

   to:

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

2. Additionally, you should rename the `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud` directory to *[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 the Apache HTTP Web Server as a Proxy on the Master Node

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

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

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

Red Hat Enterprise Linux

If you are running the Apache HTTP server on Red Hat Enterprise Linux, do the following:

1. Edit the `/etc/httpd/conf/httpd.conf` file:

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

   ```
   Listen [APACHE_MASTER_HTTP_PORT]
   ServerName [APACHE_MASTER_HOSTNAME]:[APACHE_MASTER_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 master.xyz.com:8080
   Listen 8089
   ServerName *:8089
   ```

   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
```

2. Edit the `/etc/httpd/conf.d/ssl.conf` file:

   a. Set up a virtual host for the MPP_Proxy node:

```
<VirtualHost _default_:8089>
   ErrorLog /etc/httpd/logs/mpp_proxy_error.log
   TransferLog /etc/httpd/logs/mpp_proxy_access.log
   LogLevel warn
   SSLProtocol all -SSLv2
   SSLEngine on
   SSLCertificateFile /etc/httpd/conf/apache_csa.crt
   SSLCertificateKeyFile /etc/httpd/conf/apache_csa.key
   SSLProxyEngine On
   ProxyRequests Off
   ProxyPreserveHost On
   ProxyPass /https://[APACHE_MPP_HOSTNAME]:8089/
   ProxyPassReverse /https://[APACHE_MPP_HOSTNAME]:8089/
</VirtualHost>
```

   b. Set up a virtual host for mod_cluster:

```
Listen [APACHE_MASTER_IP_ADDR]:[MOD_CLUSTER_MGMT_PORT]
<VirtualHost [APACHE_MASTER_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`.

Ubuntu Linux

If you are running the Apache HTTP server on Ubuntu Linux, do the following:

1. Log in to the system as csauser.
2. Change the default port(s) used by the Apache HTTP Server. Edit the `/etc/apache2/ports.conf` file. Change or add the following port entries:

```
NameVirtualHost *:[APACHE_MASTER_HTTP_PORT]
Listen [APACHE_MASTER_HTTP_PORT]
NameVirutalHost *:[MOD_CLUSTER_MGMT_PORT]
Listen [MOD_CLUSTER_MGMT_PORT]
NameVirutalHost *:8089
Listen 8089
<IfModule mod_ssl.c>
   NameVirtualHost *:[APACHE_MASTER_HTTPS_PORT]
   Listen [APACHE_MASTER_HTTPS_PORT]
</IfModule>
<IfModule mod_gnutls.c>
   Listen [APACHE_MASTER_HTTPS_PORT]
</IfModule>
```

   For example, if you want to change the default port to 8080, the mod_cluster management port to 10001, and the SSL port to 8443, update the port entries to the following:

```
NameVirtualHost *:8080
Listen 8080
NameVirutalHost *:10001
Listen 10001
NameVirutalHost *:8089
Listen 8089
<IfModule mod_ssl.c>
   NameVirtualHost *:8443
   Listen 8443
</IfModule>
<IfModule mod_gnutls.c>
   Listen 8443
</IfModule>
```

3. In the `/usr/lib/apache2/mods-enabled` directory, create a file named `csa-ha.load` with the following contents:

```
LoadModule proxy_module /usr/lib/apache2/modules/mod_proxy.so
LoadModule proxy_ajp_module /usr/lib/apache2/modules/mod_proxy_ajp.so
LoadModule advertise_module /usr/lib/apache2/modules/mod_advertise.so
LoadModule manager_module /usr/lib/apache2/modules/mod_manager.so
LoadModule proxy_cluster_module /usr/lib/apache2/modules/mod_proxy_cluster.so
LoadModule proxy_connect_module /usr/lib/apache2/modules/mod_proxy_connect.so
LoadModule proxy_http_module /usr/lib/apache2/modules/mod_proxy_http.so
LoadModule slotmem_module /usr/lib/apache2/modules/mod_slotmem.so
```

4. Remove the following files from `/etc/apache2/modules-enabled` (if they exist):

```
proxy_ajp.load
proxy_balancer.load
proxy.load
```

5. Set up a virtual host for the MPP_Proxy node. Add the following to the `/etc/apache2/sites-enabled/default-ssl.conf` file:

```
<VirtualHost _default_:8089>
   ErrorLog /etc/apache2/logs/mpp_proxy_error.log
   TransferLog /etc/apache2/logs/mpp_proxy_access.log
   LogLevel warn
   SSLProtocol all -SSLv2
   SSLEngine on
   SSLCertificateFile /etc/apache2/cert/apache_csa.crt
   SSLCertificateKeyFile /etc/apache2/cert/apache_csa.key
   SSLProxyEngine On
   ProxyRequests Off
   ProxyPreserveHost On
   ProxyPass /https://[APACHE_MPP_HOSTNAME]:8089/
   ProxyPassReverse /https://[APACHE_MPP_HOSTNAME]:8089/
</VirtualHost>
```

6. Set up a virtual host for mod_cluster in the `/etc/apache2/sites-enabled` directory by creating a file named `001-default` with the following contents:

```
<VirtualHost [APACHE_MASTER_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 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_
MASTER_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 Apache HTTP Web server for outbound communication.

1. When you installed HP CSA, if you specified an IP address instead of a fully-qualified domain name as the hostname, you must generate the SSL certificate using the IP address. Open the *<path_to>*/Apache2.2/conf/openssl.cnf in a text editor and add the following in the [proxy_cert_ext] section:

   ```
   subjectAltName=ip:[APACHE_MASTER_IP_ADDR]
   ```

2. 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:

   Red Hat Enterprise Linux

   ```
   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]
   ```

   Ubuntu Linux

   ```
   openssl req -new -x509 -days 365 -sha1 -newkey rsa:2048 -nodes
   -keyout /etc/apache2/cert/apache_csa.key
   -out /etc/apache2/cert/apache_csa.crt
   -config <path_to>/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).

3. Copy the SSL certificate (apache_csa.crt) to the $CSA_HOME/jboss-as-7.1.1.Final/domain/configuration directory on the slave node.

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

   Red Hat Enterprise Linux

   ```
   keytool.sh -importcert -file <path_to>/apache2.2/conf/apache_csa.crt -alias
   apache_csa -keystore $CSA_JRE_HOME/lib/security/cacerts
   ```

   Ubuntu Linux

   ```
   keytool.sh -importcert -file /etc/apache2/cert/apache_csa.crt -alias apache_
   csa -keystore $CSA_JRE_HOME/lib/security/cacerts
   ```

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

5. Load the SSL module:

   Red Hat Enterprise Linux

   a. Edit `/etc/apache2/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 `apache2.2\conf` directory. Verify that their location is correctly specified in the `/etc/apache2/conf/extra/httpd-ssl.conf` file.

      ```
      SSLCertificateFile /etc/apache2/conf/apache_csa.crt
      SSLCertificateKeyFile /etc/apache2/conf/apache_csa.key
      ```

   c. If needed, change the port in `/etc/apache2/conf/extra/httpd-ssl.conf` (for example, use port 8443 instead of the default port).

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

   Ubuntu Linux

   a. Enable the SSL module. Verify the following files exist in `/etc/apache2/modules-enabled` (if they do not exist, copy them from `/etc/apache2/modules-available`):

      ```
      ssl.conf
      ssl.load
      ```

   b. Update the SSL port used by the VirtualHost. Edit the `/etc/apache2/sites-available/default-ssl` file and update the following port entry:

      ```
      <VirtualHost _default_:[APACHE_MASTER_HTTPS_PORT]>
      ```

      For example, if you want to change the SSL port to 8443, update the port entry to the following:

      ```
      <VirtualHost _default_:8443>
      ```

   c. Create a symbolic link to the `/etc/apache2/sites-available/default-ssl` directory from the `/etc/apache2/sites-enabled` directory. Run the following command:

      ```
      ln -s /etc/apache2/sites-available/default-ssl /etc/apache2/sites-enabled/default-ssl
      ```

d. Start the Apache Web server:

```
sudo invoke-rc.d apache2 start
```

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_MASTER_HOSTNAME]
   idm.csa.port = [APACHE_MASTER_HTTPS_PORT]
   ```

   For example:

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

2. 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_MASTER_HOSTNAME]* and `port` to *[APACHE_MASTER_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_master.xyz.com"/>
      <beans:property name="port" value="~~84~~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>
   ```

Configure the Marketplace Portal on the Master Node

Complete the tasks in this section to configure the Marketplace Portal on the master node.

1. Update the hostname in the Marketplace Portal redirection URL in the `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/mpp.war/index.html` file to *[APACHE_MASTER_HOSTNAME]*. For example:

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

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_MASTER_HOSTNAME]* and *[APACHE_MASTER_HTTPS_PORT]*. For example:

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

   - For the idmProvider, update the values of the `url` attribute to use *[APACHE_MASTER_HOSTNAME]* and *[APACHE_MASTER_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_master.xyz.com:8443",
     "returnUrl": "https://~~hostname~~apache_mpp.xyz.com:8089",
     "ca": "~~$caPath$~~/etc/apache2/cert/apache_csa.crt"
     ```

     On the slave node, if you followed the instructions in the previous sections, the SSL certificate of the Apache Web server as a proxy for HP CSA is located in `$CSA_HOME/jboss-as-7.1.1.Final/domain/configuration/apache_csa.crt`.

   - Update the values of the `ha enabled` to enable high-availability and `ha host` to use *[REDIS_HOSTNAME]*. For example:

     ```
     "enabled": ~~false~~true",
     "host": "~~hostname~~redis.xyz.com:8089",
     ```

Stop and Start the Applications on the Master Node

Stop HP CSA

By default, HP CSA is automatically started in standalone mode. You must stop HP CSA that is running in standalone mode before you can start HP CSA in domain mode. To stop HP CSA, on the system that hosts HP CSA, open a command prompt and type `service csa stop`.

Start HP CSA

To start the HP CSA server in domain mode on the master node:

1. Open a command prompt and navigate to `$CSA_HOME/jboss-as-7.1.1.Final/bin`.
2. Type `./domain.sh`.

   JBoss will start and deploy the "hp-cloud" server. You should see the message `JBAS010919: Registering server hp-cloud` display on the console.

   If the following error message displays:

```
JBAS012144: Could not connect to remote://<localhost>:9999. The connection
timed out
```

verify that the "hp-cloud" server has been deployed by using the JBoss Web Management Interface or pointing a browser to `http://[APACHE_MASTER_HOSTNAME]:8081/csa`.

This is a known issue with JBoss on slow systems (see https://issues.jboss.org/browse/AS7-3524?page=com.atlassian.jirafisheyeplugin:fisheye-issuepanel&_sscc=t for more information).

Start Marketplace Portal

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

Start the Apache HTTP Web Server

To start the Apache HTTP Web server, open a command prompt and type `service httpd start` (Red Hat Enterprise Linux) or `service apache2 start` (Ubuntu).

Configure the Slave Node

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

The slave node consists of:

- HP CSA
- Identity Management component
- Marketplace Portal
- Redis data structure server

Install HP CSA and the Redis Data Structure Server on the Slave Node

Complete the tasks in the following sections to install HP CSA and the Redis data structure server on the slave node.

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 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_MASTER_HOSTNAME]*:*[APACHE_MASTER_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).

Install the Redis Data Structure Server on the Slave Node

Install the Redis data structure server on the slave node only. To install the Redis data structure server:

Download and install the Redis data structure server from redis.io (http://download.redis.io/releases/redis-2.6.16.tar.gz).

Follow the instructions at http://redis.io/download to extract and compile the Redis data structure server.

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.

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_MASTER_HOSTNAME]
csa.provider.port=[APACHE_MASTER_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
```

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 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.

   ```
   <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 user (slave or *[SLAVE_ACCESS_USERNAME]*) that would allow the slave node to connect to the master node. You must configure the authentication credentials of this user 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. 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. Mount the shared location. For example, mount the shared location to `/mnt/csa` by typing `mount -t cifs -o username=<user>, password=<pass> //sharedhost/CSA/ /mnt/csa`
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 mounted `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
   ln -s /mnt/csa/images images
   ```

4. Set the permissions and ownership for the `images` directory. Type the following:

   ```
   cd $CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/csa.war

   chmod 755 images
   chown csauser:csagrp 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 a given node and update the name attribute from:

   ```
   <servers>
      <server name="hp-cloud" group="hp-csa-server-group" />
      .
      .
   ```

```
   .
<servers>
```

to:

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

2. Additionally, you should rename the `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud` directory to *[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_
MASTER_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_HOME/lib/security/cacerts
```

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

Configure the Identity Management Component on the Slave Node

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

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

```
idm.csa.hostname = [APACHE_MASTER_HOSTNAME]
idm.csa.port = [APACHE_MASTER_HTTPS_PORT]
```

For example:

```
idm.csa.hostname = apache_master.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.properties` file, uncomment or enable the following content:

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

For example:

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

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_MASTER_HOSTNAME]* and `port` to *[APACHE_MASTER_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="localhostapache_master.xyz.com"/>
   <beans:property name="port" value="84448443"/>
   <beans:property name="servicePath" value="idm-service"/> <!-- or hpcloud-
idm-service if you don't change the name of the WAR -->
   <beans:property name="integrationAcctUserName" value="idmTransportUser"/>
   <beans:property name="integrationAcctPassword"
value="${securityIdmTransportUserPassword}"/>
</beans:bean>
```

Configure the Marketplace Portal on the Slave Node

Complete the tasks in this section to configure the Marketplace Portal on the slave node.

1. Update the hostname in the Marketplace Portal redirection URL in the `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/mpp.war/index.html` file to *[APACHE_MASTER_HOSTNAME]*. For example:

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

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_MASTER_HOSTNAME]* and *[APACHE_MASTER_HTTPS_PORT]*. For example:

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

- For the idmProvider, update the values of the `url` attribute to use *[APACHE_MASTER_HOSTNAME]* and *[APACHE_MASTER_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_master.xyz.com:8443",
  "returnUrl": "https://~~hostname~~apache_mpp.xyz.com:8089",
  "ca": "~~$caPath$~~/etc/apache2/cert/apache_csa.crt"
  ```

  On the slave node, if you followed the instructions in the previous sections, the SSL certificate of the Apache Web server as a proxy for HP CSA is located in `$CSA_HOME/jboss-as-7.1.1.Final/domain/configuration/apache_csa.crt`.

- Update the values of the `ha enabled` to enable high-availability and `ha host` to use *[REDIS_HOSTNAME]*. For example:

  ```
  "enabled": ~~false~~true",
  "host": "~~hostname~~redis.xyz.com:8089",
  ```

Stop and Start the Applications on the Slave Node

Stop HP CSA

By default, HP CSA is automatically started in standalone mode. You must stop HP CSA that is running in standalone mode before you can start HP CSA in domain mode. To stop HP CSA, on the system that hosts HP CSA, open a command prompt and type `service csa stop`.

Start HP CSA

To start the HP CSA server in domain mode on the slave node:

1. Open a command prompt and navigate to `$CSA_HOME/jboss-as-7.1.1.Final/bin`.
2. Type `./domain.sh`.

   On the console of the master node, you should see the following message when the slave node starts:

   ```
   JBAS010918: Registered remote slave host "slave"
   ```

   If a message similar to the following displays:

   ```
   17:07:08,898 ERROR [org.jboss.as] (Controller Boot Thread) JBAS015875: JBoss
   AS 7.1.1.Final "Brontes" started (with errors) in 8266ms - Started 149 of 276
   ```

```
services (4 services failed or missing dependencies, 122 services are passive
or on-demand)
```

you can safely ignore the message.

Start Marketplace Portal

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

Start the Redis Data Structure Server

To start the Redis data structure server, do the following:

1. Open a command prompt and navigate to `<path_to>/src/redis`.
2. Type **./redis-server &**.

Appendix B

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, you can complete most tasks that are required to configure an HP CSA cluster (set up a master or slave node, configure HP CSA, and configure JBoss). You must manually configure the Apache Web server. You can also configure HP CSA and JBoss properties in a standalone environment.

- **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).

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

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_HOME/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 Cloud Service Automation, 4.00 Configuring an HP CSA Cluster for Server Failover

Just add your feedback to the email and click send.

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


Java™
COMPATIBLE