HP Cloud Service Automation

Software Version: 4.50
Linux operating system

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

Document Release Date: February 2016
Software Release Date: June 2015

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

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

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

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

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

Documentation Updates

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

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

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

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

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

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

Support

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

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

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

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

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

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

To find more information about access levels, go to:

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

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

Contents

Document Change Notes

Description	Date
Initial release of this document with CSA 4.5 MR	June 2015
In "Configure JBoss" on page 24, changed the public interface code in step 8: **from:** <inet-address value="111.222.333.444"/> **to:** <inet-address value="${jboss.bind.address:<CSA_Node_ip_Address>}"/>	February 2016
Added back the Configure the TCP Communication Channel on JGroups section that had been in the CSA 4.2 guide.	February 2016
In the Configure the TCP Communication Channel on JGroups section, added the changed step 8 in "Configure JBoss" on page 24, to be the new step 4.	February 2016

Chapter 1: Overview

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

Web requests to the HP CSA Controller or Marketplace Portal are load balanced among the nodes in the cluster. Increasing the number of nodes in the cluster will improve web request transaction throughput. Increasing the number of nodes in the cluster will also improve the response time by HP CSA fulfillment services to a high volume of concurrent deployment requests.

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 HP CSA throughput by simply adding nodes to the cluster. If a node shuts down, activities such as email notifications that are scheduled to run on that node are automatically transferred to another available node. This server failover feature helps ensure that HP CSA remains operational.

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

In this document, the example cluster configuration consists of seven different physical (or virtual) hosts: three hosts are running HP CSA in standalone mode, one host is running an Apache Web server with the mod_proxy_balancer module (a software load balancer that is available from Apache and is configured on an Apache HTTP server so that web requests can be proxied into the HP CSA/JBoss cluster and a Node.js cluster for the Marketplace Portal), and three hosts are running the Marketplace Portal.

Note: Content on how to use a database cluster or Oracle RAC is beyond the scope of this document.

However, configuring HP CSA to use a Microsoft SQL Server cluster is no different from configuring HP CSA to use a standalone Microsoft SQL Server. Install and configure the Microsoft SQL Server cluster according to the manufacturer's documentation and follow the instructions to install HP CSA using a Microsoft SQL Server in the *HP Cloud Service Automation Installation Guide*.

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

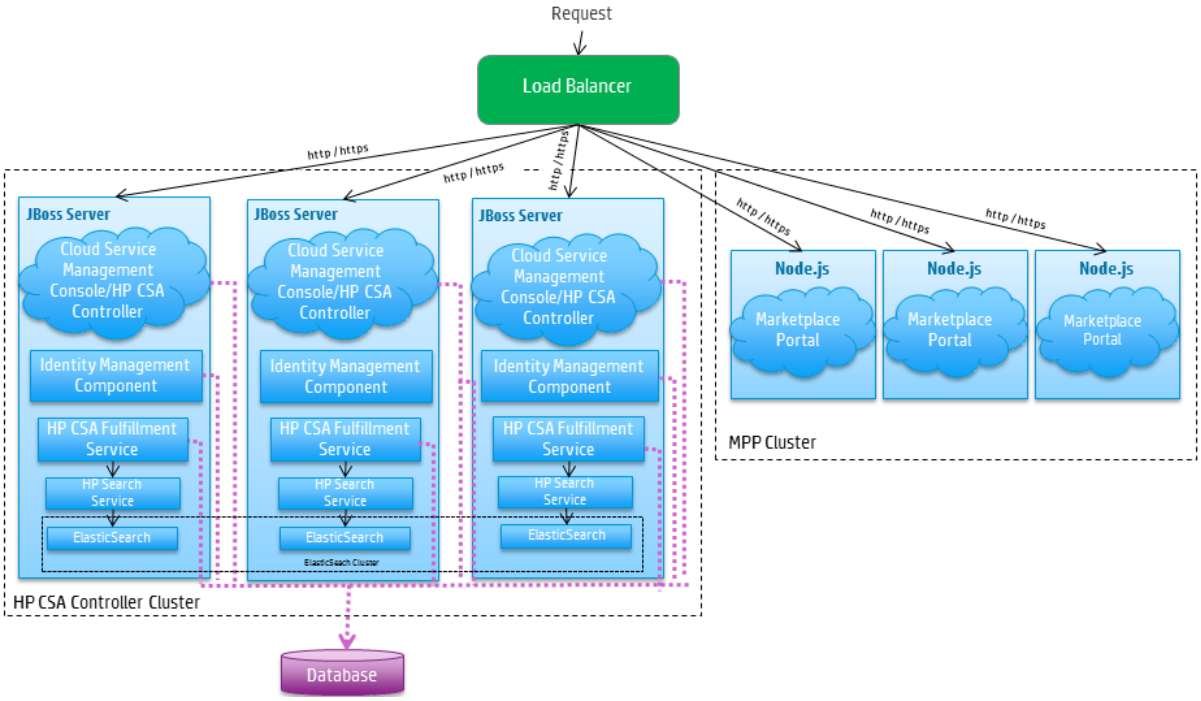

Figure 1-1. Example Cluster Configuration

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

Request Flow

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

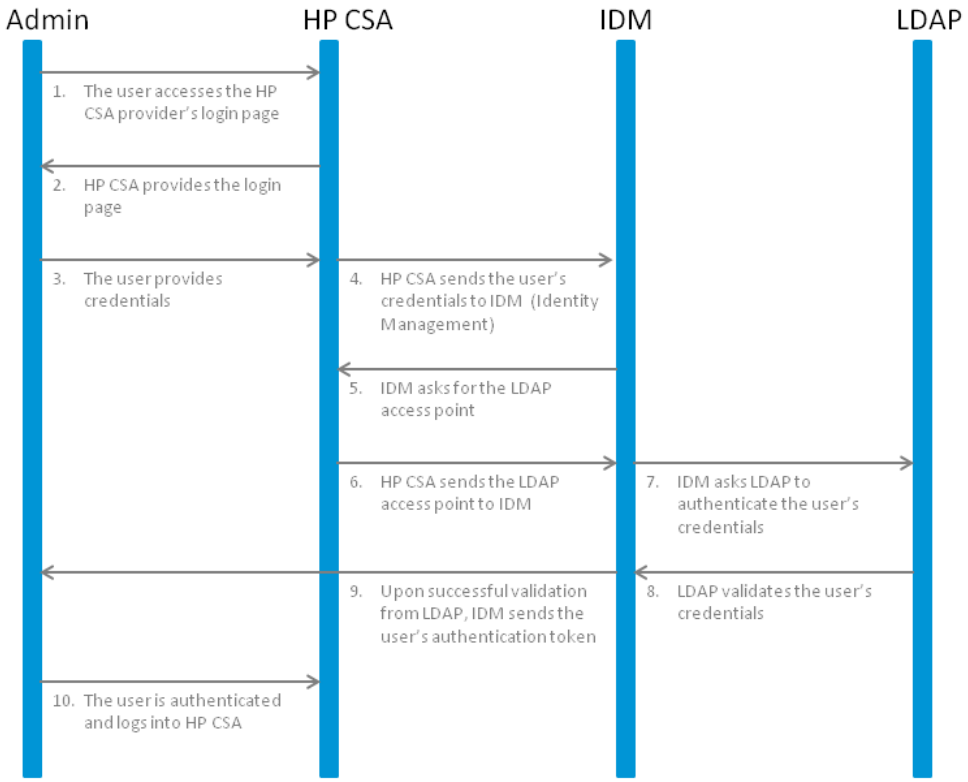

Figure 1-2. Cloud Service Management Console Request Flow

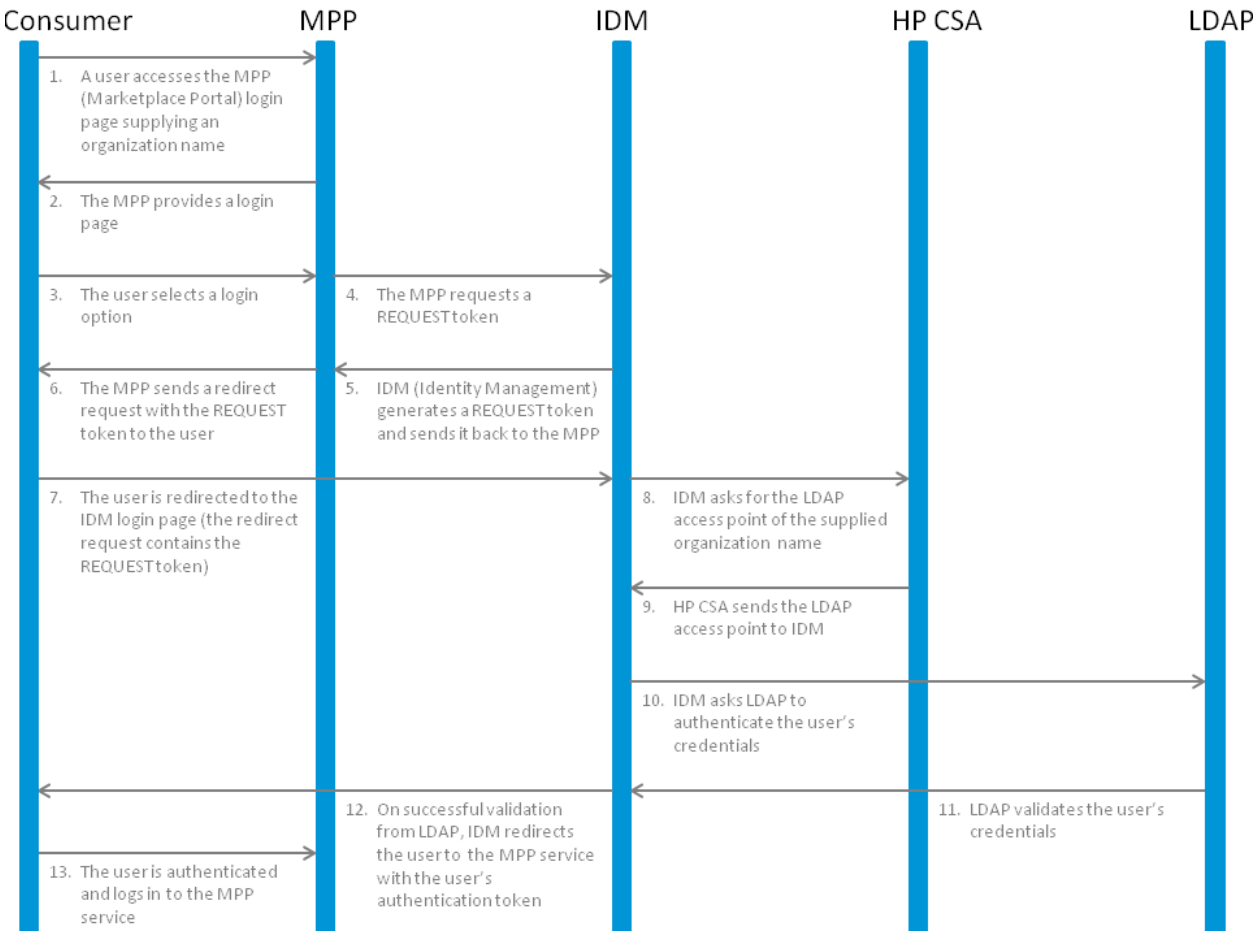

Figure 1-3. Marketplace Portal Request Flow

About the Examples

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

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

In this document, an item denoted in square brackets is a placeholder for the actual value that has been configured (for example, the hostname of the "CSA_Node1" node is denoted as [CSA_NODE1_HOSTNAME]).

In the following diagram, items in parentheses are default or example values used in this document (for example, the default port used by the Cloud Service Management Console is 8444).

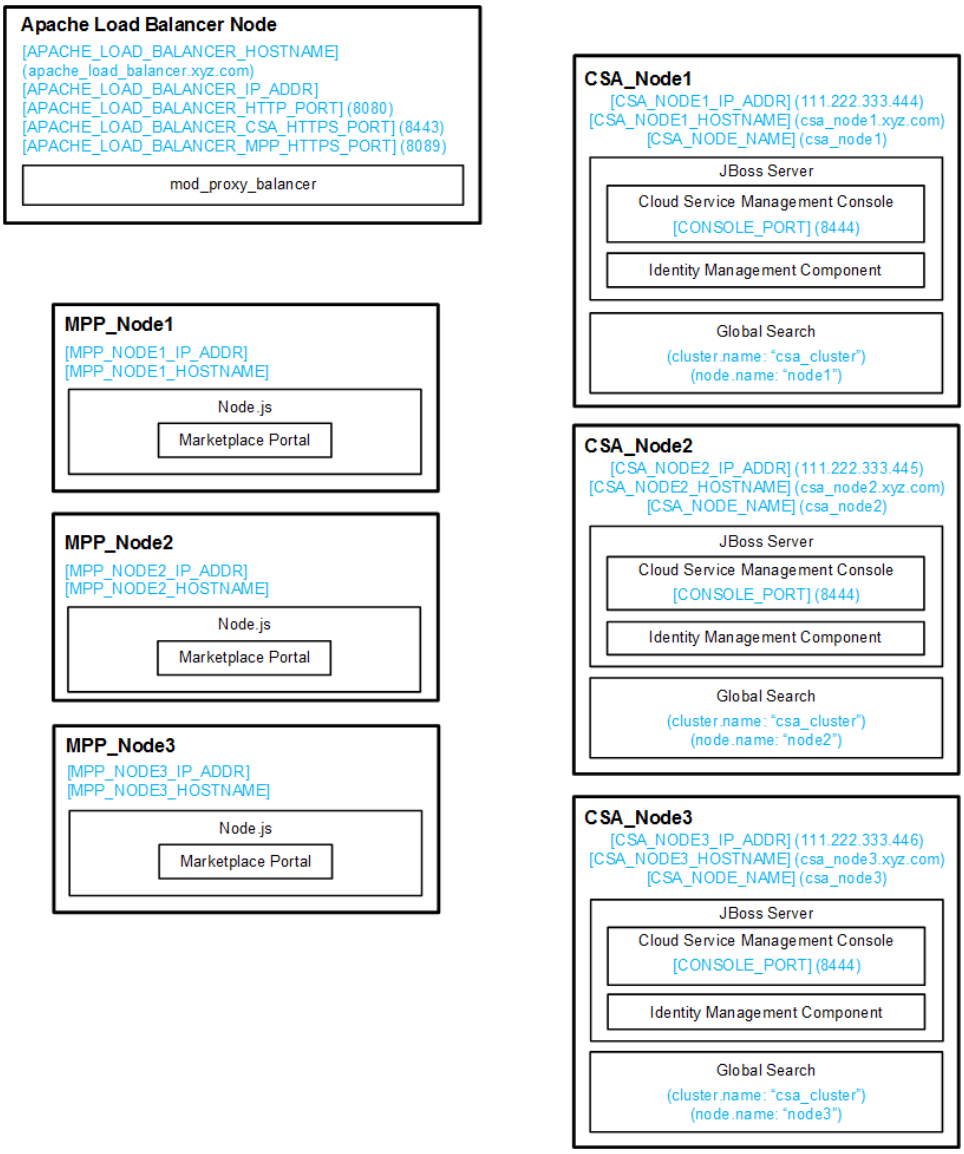

Figure 1-4. Example Values for Example Cluster Configuration

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

General Notes about Configuring a Clustered Environment

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

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

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

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

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

- When using HP CSA to configure an organization, if you are using the Apache Web server as a load balancer in a clustered environment (as described in this document), do not use a semicolon (;) or plus sign (+) in the organization's name. If one of these characters is present in the organization's name, you may not be able to log in to the Marketplace Portal.

Chapter 2: Configure the Apache Load Balancer Node

This section describes how to upgrade, install, configure, and start the applications needed to set up the Apache load balancer node in an HP CSA cluster configured for high availability. The Apache load balancer node proxies web requests into the HP CSA and Marketplace Portal cluster.

The Apache load balancer node consists of:

- Apache HTTP Web server configured as a load balancer

Upgrade the Apache Load Balancer Node

If you are upgrading from HP CSA 4.10, you must upgrade the Apache load balancer node. In HP CSA 4.10, the configuration uses two Apache load balancers, one for the CSA node (CSA_Proxy) and one for the Marketplace Portal node (MPP_Proxy). In this version of HP CSA, the configuration described in this document uses a single Apache load balancer node for both the CSA and Marketplace Portal nodes.

If you are upgrading from HP CSA 4.10, to upgrade the Apache load balancer node, do the following:

1. Stop the Apache load balancers on both the CSA_Proxy and MPP_Proxy nodes.
2. Uninstall the existing Apache applications from the CSA_Proxy node following the manufacturer's recommendations.
3. Follow the instructions below to install and configure the Apache load balancer node on the CSA_Proxy node. You are upgrading the CSA_Proxy node because this is the node which is associated with the HP CSA software license. You can continue to use this software license after the upgrade. If you choose to upgrade the MPP_Proxy node, you must request a software license for the MPP_Proxy node.

Install the Apache HTTP Web Server

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

1. Install the supported version of the Apache HTTP Server (including SSL) from apache.org (http://www.apache.org/).

   See the *HP Cloud Service Automation System and Software Support Matrix* for the supported version of the Apache HTTP Server. The *HP Cloud Service Automation System and Software Support Matrix* can be downloaded from the HP Software Support Web site at

http://h20230.www2.hp.com/selfsolve/manuals/ (this site requires that you register with HP Passport).

2. Verify that the following modules exist in the `/etc/httpd/modules` directory:

```
mod_authz_host.so
mod_headers.so
mod_log_config.so
mod_proxy.so
mod_proxy_balancer.so
mod_proxy_connect.so
mod_proxy_http.so
mod_rewrite.so
mod_ssl.so
```

Configure the Apache HTTP Web Server as a Load Balancer

Complete the tasks in the following sections to configure the Apache load balancer node.

Generate a Certificate

If you will be using a secure protocol such as TLS to communicate from the Apache load balancer node to the HP CSA and Marketplace Portal nodes, you will need to generate the Apache load balancer node's certificate (in this document, it will be referred to as `apache_csa.crt`).

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

```
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=[APACHE_LOAD_BALANCER_HOSTNAME]
```

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

2. Copy the certificate file (`apache_csa.crt`) to the `$CSA_HOME/jboss-as/standalone/configuration` directory on the CSA nodes and to the `$CSA_HOME/portal/conf/` directory on the Marketplace Portal nodes.

Configure the Apache HTTP Web Server

1. Create a virtual host file for the CSA nodes. In the `/etc/httpd/conf.d` directory, create a file named `csa.conf` that contains the following content:

```
Listen 8443
<VirtualHost _default_:8443>
ServerName [APACHE_LOAD_BALANCER_HOSTNAME]
   ErrorLog /etc/httpd/logs/csa_error.log
   TransferLog /etc/httpd/logs/csa_access.log
   SSLEngine on
   SSLProtocol all TLSv1
   SSLCertificateFile /etc/httpd/conf/apache_csa.crt
   SSLCertificateKeyFile /etc/httpd/conf/apache_csa.key
   <Proxy *>
      Order deny,allow
      Allow from all
   </Proxy>
   RewriteEngine On
   RewriteCond %{THE_REQUEST} \ (.*)//+(.*)\ [NC]
   RewriteRule .* %1/%2 [R=301,L]
   Header add Set-Cookie "CSA_ROUTEID=.%{BALANCER_WORKER_ROUTE}e; path=/"
env=BALANCER_ROUTE_CHANGED
   <Proxy balancer://csacluster/>
      BalancerMember http://[CSA_NODE1_HOSTNAME]:8444 route=csa1
      BalancerMember http://[CSA_NODE2_HOSTNAME]:8444 route=csa2
      BalancerMember http://[CSA_NODE3_HOSTNAME]:8444 route=csa3
      ProxySet stickysession=CSA_ROUTEID
   </Proxy>
   ProxyPass / balancer://csacluster/
   ProxyPassReverse / balancer://csacluster/
</VirtualHost>
```

2. Create a virtual host file for the Marketplace Portal nodes. In the `/etc/httpd/conf.d` directory, create a file named `mpp.conf` that contains the following content:

```
Listen 8089
<VirtualHost _default_:8089>
ServerName [APACHE_LOAD_BALANCER_HOSTNAME]
   ErrorLog /etc/httpd/logs/mpp_error.log
   TransferLog /etc/httpd/logs/mpp_access.log
   SSLEngine on
   SSLProtocol all -SSLv2
   SSLCertificateFile /etc/httpd/conf/apache_csa.crt
   SSLCertificateKeyFile /etc/httpd/conf/apache_csa.key
   SSLProxyEngine On
   ProxyRequests Off
```

```
   ProxyPreserveHost On
   <Proxy *>
      Order deny,allow
      Allow from all
   </Proxy>
   Header add Set-Cookie "MPP_ROUTEID=.%{BALANCER_WORKER_ROUTE}e; path=/"
env=BALANCER_ROUTE_CHANGED
   <Proxy balancer://mppcluster/>
      BalancerMember https://[MPP_NODE1_HOSTNAME]:8089 route=mpp1
      BalancerMember https://[MPP_NODE2_HOSTNAME]:8089 route=mpp2
      BalancerMember https://[MPP_NODE3_HOSTNAME]:8089 route=mpp3
      ProxySet stickysession=MPP_ROUTEID
   </Proxy>
   ProxyPass / balancer://mppcluster/
   ProxyPassReverse / balancer://mppcluster/
</VirtualHost>
```

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

   a. Add or update the list of modules that are loaded to include the following modules:

   ```
   LoadModule authz_host_module modules/mod_authz_host.so
   LoadModule headers_module modules/mod_headers.so
   LoadModule log_config_module modules/mod_log_config.so
   LoadModule proxy_module modules/mod_proxy.so
   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 rewrite_module modules/mod_rewrite.so
   LoadModule ssl_module modules/mod_ssl.so
   ```

   b. Add the following line:

   ```
   Include conf.d/*.conf
   ```

Start the Apache Load Balancer Node

To start the Apache load balancer node, open a command prompt and type `service httpd start`.

Chapter 3: Configure the HP CSA Node

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

The CSA node consists of:

- HP CSA
- Global search
- Identity Management component

To configure the CSA node, do the following:

- Install or upgrade the HP CSA node
- Configure HP CSA

Install HP CSA

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

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

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

- You can only use the installer to install sample content on the node on which database components have been installed and the database schema has been created. On the other nodes in the cluster, use the HP Cloud Content Capsule Installer to install the sample content after the database schema has been created. Refer to the *[[[Undefined variable CSAVariables.mnlCSLContentInstaller]]]* for more information.

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

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

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

- You must configure a secure protocol connection (such as TLS) between HP Operations Orchestration and all CSA nodes.

- If you are configuring HP Operations Orchestration for sequential designs, set the **Property Value** of the **CSA_REST_URI** System Property to `https://[APACHE_LOAD_BALANCER_HOSTNAME]:[APACHE_LOAD_BALANCER_CSA_HTTPS_PORT]/csa/rest`.

  For example:

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

- Do NOT start the Marketplace Portal service on the CSA nodes. The Marketplace Portal should be installed as a remote instance on a Marketplace Portal node in its own clustered environment. See "Configure the Marketplace Portal Node" on page 36 for more information.

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

Upgrade HP CSA

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

1. If you are using the JRE that is installed with HP CSA (OpenJRE), back up the truststore (`<csa_jre>/lib/security/cacerts`) and/or the load balancer certificate outside of `$CSA_HOME`. Because the JRE will be upgraded, the truststore is also upgraded. Any certificates you manually imported into the truststore will be lost unless you back up the truststore or the certificates. Do not re-use the truststore from the old version of the JRE (in case it contains public Certificate Authority certificates that are no longer trusted). Instead, you must export any root and/or self-signed certificates from the old truststore (certificates that you had manually imported into the old truststore) and import them into the new JRE truststore after running the upgrade installer.

2. Upgrade HP CSA as described in the *HP Cloud Service Automation Upgrade Guide* with the

following exceptions:

- Before running the upgrade installer, if you are upgrading from HP CSA version 4.10, any customizations you made to the `$CSA_HOME/jboss-as-7.1.1.Final/bin/domain.conf` file must be made to the `$CSA_HOME/jboss-as-7.1.1.Final/bin/standalone.conf` file. The upgrade installer uses the `standalone.conf` file, not the `domain.conf` file.

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

- When running the upgrade installer, install HP CSA database components and upgrade the database schema on one and only one of the CSA nodes. HP recommends that you upgrade the schema on the first CSA node that you upgrade. Then, you do not need to install HP CSA database components and upgrade the database schema when you upgrade HP CSA on the other CSA nodes.

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

- When running the upgrade installer, you must continue to use an external (existing) instance of HP Operations Orchestration. You cannot install or upgrade to use an embedded HP Operations Orchestration instance.

- When running the upgrade installer, you cannot install the additional sample content. You can deploy the content after the upgrade has completed. Refer to the *[[[Undefined variable CSAVariables.mnlCSLContentInstaller]]]* for information on how to manually deploy this content.

- After running the upgrade installer, any references to the `$CSA_HOME/jboss-as/standalone/configuration/standalone.xml` file in the *HP Cloud Service Automation Upgrade Guide* should be applied to the `$CSA_HOME/jboss-as/standalone/configuration/standalone-full-ha.xml` file instead.

  For example, in HP CSA version 4.20, if you customized the host or ports in the `standalone-full-ha.xml` file, when you follow the instructions in the *Recustomize Host and Ports* section of the *HP Cloud Service Automation Upgrade Guide*, instead of updating the `standalone.xml` file, you should update the `standalone-full-ha.xml` file. If you do not remember the customizations you made to the file, refer to the backed up copy, `$CSA_HOME/_CSA_4_50_0_installation/Backup/standalone/configuration/standalone-full-ha.xml`.

  In HP CSA version 4.10, if you customized the host or ports in the `domain.xml` file, when you follow the instructions in the *Recustomize Host and Ports* section of the *HP Cloud Service Automation Upgrade Guide*, instead of updating the `standalone.xml` file, you should update the `standalone-full-ha.xml` file. If you do not remember the customizations you made to the

file, refer to the backed up copy, `$CSA_HOME/_CSA_4_50_0_installation/Backup/domain/configuration/domain.xml`.

- After upgrade to HP CSA 4.50, if **Enable HP SSO** is selected during upgrade, and if the initString value in the `$CSA_HOME/jboss-as-7.1.1.Final/standalone/deployments/csa.war/WEB-INF/hpssoConfiguration.xml` (HP CSA 4.10) or `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/hpssoConfiguration.xml` (HP CSA 4.2x) file is detected to be the default value created during a previous installation of HP CSA, the initString value is regenerated as a security measure.

  If the external HP Operations Orchestration had not already been configured for HP SSO, the upgrade process will attempt to update the external HP Operations Orchestration's HP SSO configuration with the new initString value generated during installation.

  Any other products that you had configured for HP SSO with HP CSA will need to be updated to share a common initString with HP CSA. After upgrade to HP CSA 4.50, you should review and update, as needed, the HP SSO configuration in HP Operations Orchestration and other integrated products. For more information on configuring HP SSO between HP CSA and other products, refer to the *HP Cloud Service Automation Configuration Guide*.

The *HP Cloud Service Automation Upgrade Guide* and *HP Cloud Service Automation Configuration 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).

3. Follow the instructions in "Configure HP CSA" on the next page to configure HP CSA after running the upgrade installer. Do not copy back files from an earlier version of HP CSA unless you are instructed to do so. Many components of HP CSA, such as the JRE, JBoss, and Identity Management component, have been updated and therefore, the configuration files have also been updated. Some files may have retained the information you configured in the previous version. However, you should verify all information in the upgraded files.

   If you are upgrading from HP CSA version 4.10 and you customized any files in the directory or subdirectories of `$CSA_HOME/jboss-as-7.1.1.Final/domain/` that are not mentioned in the "Configure HP CSA" section, you will need to manually restore these customizations to the equivalent file in the `$CSA_HOME/jboss-as/standalone/` directory.

   All files in `$CSA_HOME/jboss-as-7.1.1.Final/domain/servers/<server_name>/deployments/*.war` are backed up to `$CSA_HOME/_CSA_4_50_0_installation/Backup/domain/*.war`. You can refer to these files if you do not remember the customizations that you made. However, do not copy these files back to the upgraded version of HP CSA.

Configure HP CSA

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

- "Edit Properties" below (required)
- "Enable JNDI" on the next page (required)
- "Request a Software License" on page 23 (required)
- "Configure Marketplace Portal Redirection" on page 23 (required)
- "Configure JBoss" on page 24 (required)
- "Configure a Secure Connection" on page 26 (required)
- "Configure the Identity Management Component" on page 27 (required)
- "Reconfigure the HP CSA Service" on page 28 (required)
- "Configure Global Search" on page 29 (required if using global search)
- "Configure HP Single Sign-On" on page 33 (required if using HP SSO)
- "Share Filesystem Resources" on page 34 (optional)

Edit Properties

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

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

   a. Set the following properties:

   ```
   csa.provider.hostname=[APACHE_LOAD_BALANCER_HOSTNAME]
   csa.provider.port=[APACHE_LOAD_BALANCER_CSA_HTTPS_PORT]
   csa.provider.rest.protocol=https
   deploymentMode=clustered
   ```

   For example:

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

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

b. Add and set the following property:

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

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

```
documentation.services.basePath=https://[APACHE_LOAD_BALANCER_HOSTNAME]:
[APACHE_LOAD_BALANCER_CSA_HTTPS_PORT]/csa/rest
```

For example:

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

Enable JNDI

Enable the Java Naming and Directory Interface (JNDI).

1. Open the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/applicationContext.xml` file in a text editor.
2. Locate the comment `START HA Mode Configuration` and uncomment following content:

```
<jee:jndi-lookup id="channelGroup"
jndi-name="java:jboss/clustering/group/server"
expected-type="org.wildfly.clustering.group.Group"/>
```

3. If you modified the channel group, update the value of the `jndi-name` attribute to the new group name.
4. Save and exit the file.

Request a Software License

HP CSA version 4.50 requires a software license. HP CSA licensing is based on the number of operating system instances (OSIs) being used in current, active subscriptions.

After initial installation of HP CSA version 4.50, when you log in to the Cloud Service Management Console, a temporary 90-day trial license is activated. Once the trial license expires, you are limited to 25 OSIs. If you created more than 25 OSIs during the trial period, you cannot create any additional OSIs. You can add more licenses at any time to increase your OSI capacity.

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

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

Configure Marketplace Portal Redirection

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

To update the redirection, do the following:

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

2. Locate the following line:

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

3. Replace [CSA_NODE_HOSTNAME] with [APACHE_LOAD_BALANCER_HOSTNAME] and [CSA_NODE_HTTPS_PORT] with [APACHE_LOAD_BALANCER_MPP_HTTPS_PORT]. For example:

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

   or

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

4. Save and exit the file.

Configure JBoss

Configure JBoss for use in an HP CSA clustered environment:

1. Open the `$CSA_HOME/jboss-as/standalone/configuration/standalone-full-ha.xml` file in a text editor.
2. Locate the server property and configure a unique node name for the node. Locate

   ```
   <server xmlns="urn:jboss:domain:2.2">
   ```

   and set the name to *[CSA_NODE_NAME]*.

   For example:

   ```
   <server xmlns="urn:jboss:domain:2.2" name="csa_node1">
   ```

3. Update the jgroups subsystem default stack from udp to tcp. Change

   ```
   <subsystem xmlns="urn:jboss:domain:jgroups:2.0" default-stack="udp">
   ```

   to

   ```
   <subsystem xmlns="urn:jboss:domain:jgroups:2.0" default-stack="tcp">
   ```

4. Locate the tcp stack and replace

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

   with

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

         <property name="port_range">1</property>
         <property name="timeout">2000</property>
   </protocol>
   ```

   where:

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

For example:

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

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

5. In the tcp stack and replace

```
<protocol type="pbcast.NAKACK2"/>
```

with

```
<protocol type="pbcast.NAKACK2">
   <property name="use_mcast_xmit">false</property>
   <property name="use_mcast_xmit_req">false</property>
</protocol>
```

6. Update the messaging subsystem password. Change

```
<cluster-password>${jboss.messaging.cluster.password:CHANGE ME!!}</cluster-
password>
```

to

```
<cluster-password>password</cluster-password>
```

7. Locate the transactions subsystem and configure the node identifier for the `<core-environment>`

property (set the node identifier to the unique node name you configured in step 2). Locate

```
<subsystem xmlns="urn:jboss:domain:transactions:2.0">
   <core-environment>
```

and add set the node identifier to *[CSA_NODE_NAME]*. For example:

```
<subsystem xmlns="urn:jboss:domain:transactions:2.0">
   <core-environment node-identifier="csa_node1">
```

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

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

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

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

Configure a Secure Connection

Configure a secure connection (using a protocol such as TLS) on the CSA node for communication from the Apache load balancer node and between each HP CSA node in the cluster.

1. To configure a secure connection between HP CSA and the Apache load balancer node:

   a. If you have not already done so, copy the certificate from the Apache load balancer node (`apache_csa.crt`) to the `$CSA_HOME/jboss-as/standalone/configuration` directory.

   b. Import the certificate into the JVM on the CSA node using the following command:

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

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

2. Copy and import the certificate of each HP CSA node to every other HP CSA node in the cluster:

   a. Copy the certificate of each HP CSA node to every other HP CSA node in the cluster. The certificate file on each HP CSA node is `$CSA_HOME/jboss-as/standalone/configuration/jboss.crt`.

      For example, copy the certificates from csa_node2 and csa_node3 to csa_node1 to the directory `/tmp/CSA-Certificates`. Rename the certificate files with unique names, such as `jboss-csa_node2.crt` and `jboss-csa_node3.crt`.

b. Import each certificate into the JVM of that HP CSA node.

For example, on csa_node1, run the following commands:

```
$CSA_JRE_HOME/bin/keytool -importcert -file /tmp/CSA-Certificates/jboss-csa_
node2.crt -alias csa_node2 -keystore $CSA_JRE_HOME/lib/security/cacerts

$CSA_JRE_HOME/bin/keytool -importcert -file /tmp/CSA-Certificates/jboss-csa_
node3.crt -alias csa_node3 -keystore $CSA_JRE_HOME/lib/security/cacerts
```

Configure the Identity Management Component

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

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

```
idm.csa.hostname = [APACHE_LOAD_BALANCER_HOSTNAME]
idm.csa.port = [APACHE_LOAD_BALANCER_CSA_HTTPS_PORT]
 .
 .
 .
# Properties for CSA Auditing Server
 .
 .
 .
idm.csa.audit.hostname = [APACHE_LOAD_BALANCER_HOSTNAME]"/>
idm.csa.audit.port = [APACHE_LOAD_BALANCER_HTTPS_PORT]"/>
```

For example:

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

2. Edit the following content in the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/applicationContext-security.xml` file. Update the values of `hostname` to *[APACHE_LOAD_BALANCER_HOSTNAME]* and `port` to *[APACHE_LOAD_BALANCER_CSA_HTTPS_PORT]*:

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

For example:

```
<beans:bean id="idmConfig"
class="com.hp.ccue.identity.rp.IdentityServiceConfig">
   <beans:property name="protocol" value="https"/>
   <beans:property name="hostname" value="apache_load_balancer.xyz.com"/>
   <beans:property name="port" value="8443"/>
   <beans:property name="servicePath" value="idm-service"/> <!-- or hpcloud-
idm-service if you don’t change the name of the WAR -->
   <beans:property name="integrationAcctUserName" value="idmTransportUser"/>
   <beans:property name="integrationAcctPassword"
value="${securityIdmTransportUserPassword}"/>
</beans:bean>
```

Reconfigure the HP CSA Service

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

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

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

   service csa stop

3. Edit the `$CSA_HOME/scripts/csa_env.conf` file:

a. Locate the `Toggle below two lines to run CSA in HA mode` comment.

b. Below this comment, comment out the `export CSA_DEPLOY_MODE=standalone.sh # Standalone Mode` line:

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

c. Uncomment the following line:

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

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

service csa start

Configure Global Search

Global search allows you to find a certain service offering, service instance, or subscription by a meaningful keyword from the Marketplace Portal. For service offerings, global search finds the keyword in the name, description, option sets, options, and properties. For service instances and subscriptions, global search finds the keyword in the name, description, and instance properties (name and value).

Global search must be enabled before being available on the Marketplace Portal. Refer to the *HP Cloud Service Automation Configuration Guide* for more information about enabling global search.

To configure global search, do the following:

1. Edit the `$CSA_HOME/[[[Undefined variable CSAVariables.dirElasticsearch]]]/config/elasticsearch.yml` file:

   a. Uncomment the `cluster.name` property and set it to a unique name that is shared by all the nodes in the cluster. That is, if you have more than one clustered environment on the same network, each clustered environment should have a unique cluster name. All the nodes in the single clustered environment will share the same cluster name.

   For example, `cluster.name: "csa_cluster"`

   b. Set the `node.name` property to a unique name. Each node in the cluster must have a unique node name.

   For example, `node.name: "node1"`

   c. Uncomment the `node.master` property and set it to **true** to make this node a master node. All nodes in the cluster should be a master node.

   For example, `node.master: true`

d. Optionally, uncomment and set the `node.data` property. Refer to the comments in the file for information of how to combine this and the `node.master` property settings to suit the requirements of the node.

e. Comment out the `node.local: true` property. When disabled, global search can find and communicate with other nodes on the network. If this property is left enabled, global search will not discover other nodes and will isolate itself from the network.

f. Set the `discovery.zen.ping.unicast.hosts` property to the IP addresses of the master nodes that perform discovery when new master or data nodes are started. Since all nodes in the cluster are master nodes, set this property to all IP addresses of the nodes in the cluster.

   For example, `discovery.zen.ping.unicast.hosts: ["111.222.333.444","111.222.333.445","111.222.333.446"]`

g. Locate the `Transport layer SSL` section and do the following:

   i. Verify that the following properties are set to these values (and if they are not set to these values, set them to these values):

   ```
   searchguard.ssl.transport.node.keystore_type: JKS
   searchguard.ssl.transport.node.keystore_password: changeit
   searchguard.ssl.transport.node.truststore_type: JKS
   searchguard.ssl.transport.node.truststore_password: changeit
   ```

   ii. Set the `searchguard.ssl.transport.node.keystore_filepath` property to the location of HP CSA's keystore. For example,

   ```
   searchguard.ssl.transport.node.keystore_filepath:
   /usr/local/hp/csa/jboss-as/standalone/configuration/.keystore
   ```

   iii. Set the `searchguard.ssl.transport.node.truststore_filepath` property to the location of HP CSA's truststore. For example,

   ```
   searchguard.ssl.transport.node.truststore_filepath:
   /usr/local/hp/csa/openjre/lib/security/cacerts
   ```

h. Locate the `REST layer SSL` section and do the following:

   i. Verify that the following properties are set to these values (and if they are not set to these values, set them to these values):

   ```
   searchguard.ssl.transport.http.keystore_type: JKS
   searchguard.ssl.transport.http.keystore_password: changeit
   searchguard.ssl.transport.http.truststore_type: JKS
   searchguard.ssl.transport.http.truststore_password: changeit
   ```

   ii. Set the `searchguard.ssl.transport.http.keystore_filepath:` property to the location of HP CSA's keystore. For example,

```
searchguard.ssl.transport.http.keystore_filepath:
/usr/local/hp/csa/jboss-as/standalone/configuration/.keystore
```

iii. Set the `searchguard.ssl.transport.http.truststore_filepath` property to the location of HP CSA's truststore. For example,

```
searchguard.ssl.transport.http.truststore_filepath:
/usr/local/hp/csa/openjre/lib/security/cacerts
```

i. Verify that the following properties are set to these values (and if they are not set to these values, set them to these values):

```
transport.tcp.port: 9300
http.port: 9201
http.enabled: true
discovery.zen.ping.timeout: 5s
```

j. Save and exit the file.

2. Create the security key on one node and copy it to the other nodes in the cluster. The security key is used to authenticate the communication between the nodes in the cluster when sharing the shards and replicas of the inventory index. The security key must be the same on all nodes in the cluster.

   a. On a CSA_Node (for example, csa_node1), restart HP CSA:

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

   b. After the service has restarted on csa_node1, copy the `$CSA_HOME/scripts/searchguard_node_key.key` file to the `$CSA_HOME/[[[Undefined variable CSAVariables.dirElasticsearch]]]/` directory and then copy the `$CSA_HOME/[[[Undefined variable CSAVariables.dirElasticsearch]]]/searchguard_node_key.key` file from csa_node1 to all other nodes in the cluster. Copy the file to the same directory (`$CSA_HOME/[[[Undefined variable CSAVariables.dirElasticsearch]]]/`) and use the same file name on the other nodes.

   c. On all nodes in the cluster except csa_node1, restart HP CSA:

      On all nodes in the cluster except csa_node1, open a command prompt and type `service csa restart`.

3. Configure the Identity Management component for global search.

   a. Edit the `$CSA_HOME/[[[Undefined variable CSAVariables.dirSearchService]]]/app.json` file. For msvc-basic-search, set the `idmURL` property to the URL of the load balancer and `/idm-service` proxy (*[APACHE_LOAD_BALANCER_HOSTNAME]:[APACHE_LOAD_BALANCER_CSA_HTTPS_PORT]/idm-service*).

      For example,

```
"msvc-basic-search": {
 .
 .
 .
"idmURL": "https://apache_load_balancer.xyz.com:8443/idm-service",
```

b. Edit the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/csa.properties` file. Set the `csa.provider.es.idmURL` property to the URL of the load balancer and `/idm-service` proxy (*[APACHE_LOAD_BALANCER_HOSTNAME]:[APACHE_LOAD_BALANCER_CSA_HTTPS_PORT]/idm-service*).

For example,

```
csa.provider.es.idmURL=https://apache_load_balancer.xyz.com:8443/idm-service
```

4. Restart HP CSA:

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

5. If you changed the `cluster.name`, you must create new indexes. Do the following:

Note: HP CSA must be running.

a. Open a command prompt and navigate to `$CSA_HOME/csa-search-service/bin/`.

b. Run the following command:

```
$CSA_HOME/node.js/node.exe create-index.js
```

If displayed, ignore the following errors:

```
ERROR: Error connecting to Elasticsearch server. Cannot create index
catalog. Error: DEPTH_ZERO_SELF_SIGNED_CERT
ERROR: Error connecting to Elasticsearch server. Cannot create index
inventory. Error: DEPTH_ZERO_SELF_SIGNED_CERT
```

It may take a few minutes for the first HP CSA artifact to be indexed.

6. You can verify the status of the global search cluster using the following commands from your web browser:

- **https://localhost:9201/_cluster/health?pretty=true** - Displays information about the global search cluster's health, such as the number of nodes in the cluster (`number_of_nodes`).
- **https://localhost:9201/_cluster/state** - Displays information about the state of the global search cluster, such as names of the nodes in the cluster.
- **https://localhost:9201/_cat/indices?v** - Displays information about the following required indexes: inventory, searchguard, and catalog. If you run this command immediately after

running the `create-index.js` script, you may only see the searchguard index. It may take a few minutes before the first HP CSA artifact is indexed and all three indexes will be displayed.

Refer to the Elasticsearch online documentation at https://www.elastic.co/guide/index.html for more information about these commands.

Configure HP Single Sign-On

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

1. Open the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/hpssoConfiguration.xml` file in a text editor.

2. Locate the following content:

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

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

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

4. Locate the `initString` value in the `crypto` element. The `initString` setting for HP CSA must be the same value for all nodes in the cluster and any applications (such as HP Operations Orchestration) that are integrated with HP Single Sign-On. The `initString` value represents a secret key and should be treated as such in your environment.

5. Copy the `initString` value to the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/hpssoConfiguration.xml` file on all other nodes in the cluster.

6. Copy the `initString` value to the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/hpssoConfig.xml` file on this and all other nodes in the cluster.

7. Configure this `initString` value in any applications that are integrated with HP CSA using HP Single Sign-On.

Share Filesystem Resources

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

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

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

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

2. On the CSA node, log in as root.

3. If it exists, delete the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/images` directory.

4. Create a credentials file to store the shared filesystem user login information. For example, create `/etc/.win-mnt-cred` and add the following lines:

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

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

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

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

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

7. Mount the shared filesystem:

```
mount -a
```

Chapter 4: Configure the Marketplace Portal Node

This chapter describes how to install, upgrade, and configure a remote Marketplace Portal instance on the Marketplace Portal node (for example, MPP_Node1, MPP_Node2, or MPP_Node3) in a cluster configured for high availability. The Marketplace Portal should be installed as a remote instance on a Marketplace Portal node in its own clustered environment.

To configure the Marketplace Portal, do the following:

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

Install the Remote Marketplace Portal Instance

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

- You must install the same version of HP CSA on each node (including the CSA nodes).
- When selecting a location in which to install the Marketplace Portal, select the same location for all Marketplace Portal nodes.
- When configuring the HP CSA Host, use the fully-qualified domain name of the Apache load balancer node (for example, apache_load_balancer.xyz.com or *[APACHE_LOAD_BALANCER_HOSTNAME]*).
- When configuring the HP CSA Port, use the port of the Apache server installed on the Apache load balancer node (for example, 8443 or *[APACHE_LOAD_BALANCER_CSA_HTTPS_PORT]*).

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

Upgrade the Remote Marketplace Portal Instance

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

- If you are upgrading from HP CSA version 4.10, edit the `$CSA_HOME/portal/conf/mpp.json` file. Update the value of the `ha enabled` property to disable the Marketplace Portal from using the Redis cache server for session persistence. The Apache load balancer will use sticky sessions for

session persistence. For example:

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

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

Configure the Remote Marketplace Portal Instance

To configure the remote Marketplace Portal instance on each Marketplace Portal node, do the following:

1. If you have not done so already, copy the certificate of the Apache server from the Apache load balancer node (for example, apache_csa.crt) to the `$CSA_HOME/portal/conf/` directory on the Marketplace Portal node.

2. Edit the following content in the `$CSA_HOME/portal/conf/mpp.json` file:

   - For the provider, update the `url` attribute value to use *[APACHE_LOAD_BALANCER_HOSTNAME]* and *[APACHE_LOAD_BALANCER_CSA_HTTPS_PORT]* (virtual host port) and `ca` to use the location of the certificate of the Apache load balancer node. For example:

     ```
     "provider": {
        "url": "https://[APACHE_LOAD_BALANCER_HOSTNAME]:[APACHE_LOAD_BALANCER_CSA_
     HTTPS_PORT]"
        "ca": "$CSA_HOME/portal/conf/apache_csa.crt"
         .
         .
         .
     },
     ```

     or

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

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

BALANCER_HOSTNAME] and *[APACHE_LOAD_BALANCER_CSA_HTTPS_PORT]* (virtual host port for the HP CSA nodes), `returnUrl` to use *[APACHE_LOAD_BALANCER_HOSTNAME]* and *[APACHE_LOAD_BALANCER_MPP_HTTPS_PORT]* (virtual host port for the Marketplace Portal nodes), and `ca` to use the location of the certificate of the Apache load balancer node. For example:

```
"idmProvider": {
   "url": "https://[APACHE_LOAD_BALANCER_HOSTNAME]:[APACHE_LOAD_BALANCER_CSA_
HTTPS_PORT]",
   "returnUrl": "https://[APACHE_LOAD_BALANCER_HOSTNAME]:[APACHE_LOAD_
BALANCER_MPP_HTTPS_PORT]",
   "ca": "$CSA_HOME/portal/conf/apache_csa.crt"
    .
    .
    .
},
```

or

```
"idmProvider": {
   "url": "https://apache_load_balancer.xyz.com:8443",
   "returnUrl": "https://apache_load_balancer.xyz.com:8089",
   "ca": "$CSA_HOME/portal/conf/apache_csa.crt"
    .
    .
    .
},
```

3. Restart the Marketplace Portal service:

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

Chapter 5: Common Tasks

This chapter provides information on how to perform common tasks.

Tasks include:

Start HP CSA

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

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

```
service csa start
```

Stop HP CSA

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

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

```
service csa stop
```

Start the Marketplace Portal

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

Stop the Marketplace Portal

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

Start the Apache Load Balancer Node

To start the Apache load balancer node, open a command prompt and type `service httpd start`.

Stop the Apache Load Balancer Node

To stop the Apache load balancer node, open a command prompt and type `service httpd stop`.

Launch the Cloud Service Management Console

Launch the Cloud Service Management Console through the Apache load balancer by opening one of the following URLs in a supported Web browser:

- `http://[APACHE_LOAD_BALANCER_HOSTNAME]:[APACHE_LOAD_BALANCER_HTTP_PORT]/csa`
  For example, `http://apache_load_balancer.xyz.com:8080/csa`
- `https://[APACHE_LOAD_BALANCER_HOSTNAME]:[APACHE_LOAD_BALANCER_CSA_HTTPS_PORT]/csa`
  For example, `https://apache_load_balancer.xyz.com:8443/csa`

Launch the Marketplace Portal

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

- `https://[APACHE_LOAD_BALANCER_HOSTNAME]:8443/mpp`
  For example, `https://apache_load_balancer.xyz.com:8443/mpp`

The organization associated with the default Marketplace Portal is defined in the `$CSA_HOME/portal/conf/mpp.json` file. By default, this is the sample organization that is installed with HP CSA (CSA_CONSUMER). To modify the organization associated with the default Marketplace

Portal, modify the `defaultOrganizationName` property value by setting it to the <*organization_identifier*> of the desired organization, where <*organization_identifier*> is the unique name that HP Cloud Service Automation assigns to the organization, based on the organization display name (the organization identifier can be found in the General Information section of the **Organizations** tile of the Cloud Service Management Console).

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

- `http://[APACHE_LOAD_BALANCER_HOSTNAME]:[APACHE_LOAD_BALANCER_HTTP_PORT]/org/<organization_identifier>`
  For example, `http://apache_load_balancer.xyz.com:8080/org/ORGANIZATION_A`
- `https://[APACHE_LOAD_BALANCER_HOSTNAME]:[APACHE_LOAD_BALANCER_MPP_HTTPS_PORT]/org/<organization_identifier>`
  For example, `https://apache_load_balancer.xyz.com:8089/org/ORGANIZATION_A`

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

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

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

Chapter 6: Troubleshoot the HP CSA Clustered Environment

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

Problem

Accessing the Cloud Service Management Console or Marketplace Portal may generate an error when running in a clustered environment with a load balancer. The following error may appear in the log file:

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

Cause

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

Workaround

Make the following changes on all CSA nodes:

In the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/flex/services-config.xml` file, update the endpoint class value for the `csa-secure-amf` channel to **flex.messaging.endpoints.AMFEndpoint**.

For example, change the following from:

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

to

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

Send Documentation Feedback

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

Feedback on Configuring an HP CSA Cluster for High Availability Using an Apache Web Server (Cloud Service Automation 4.50)

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 clouddocs@hp.com.

We appreciate your feedback!


Java™
COMPATIBLE