HP Codar

Software Version: 1.50
Windows ® and Linux operating systems

High Availability Guide

Document Release Date: May 2015
Software Release Date: May 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.

UNIX® is a registered trademark of The Open Group.

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

Acknowledgements

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes code licensed from RSA Data Security.

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

Overview

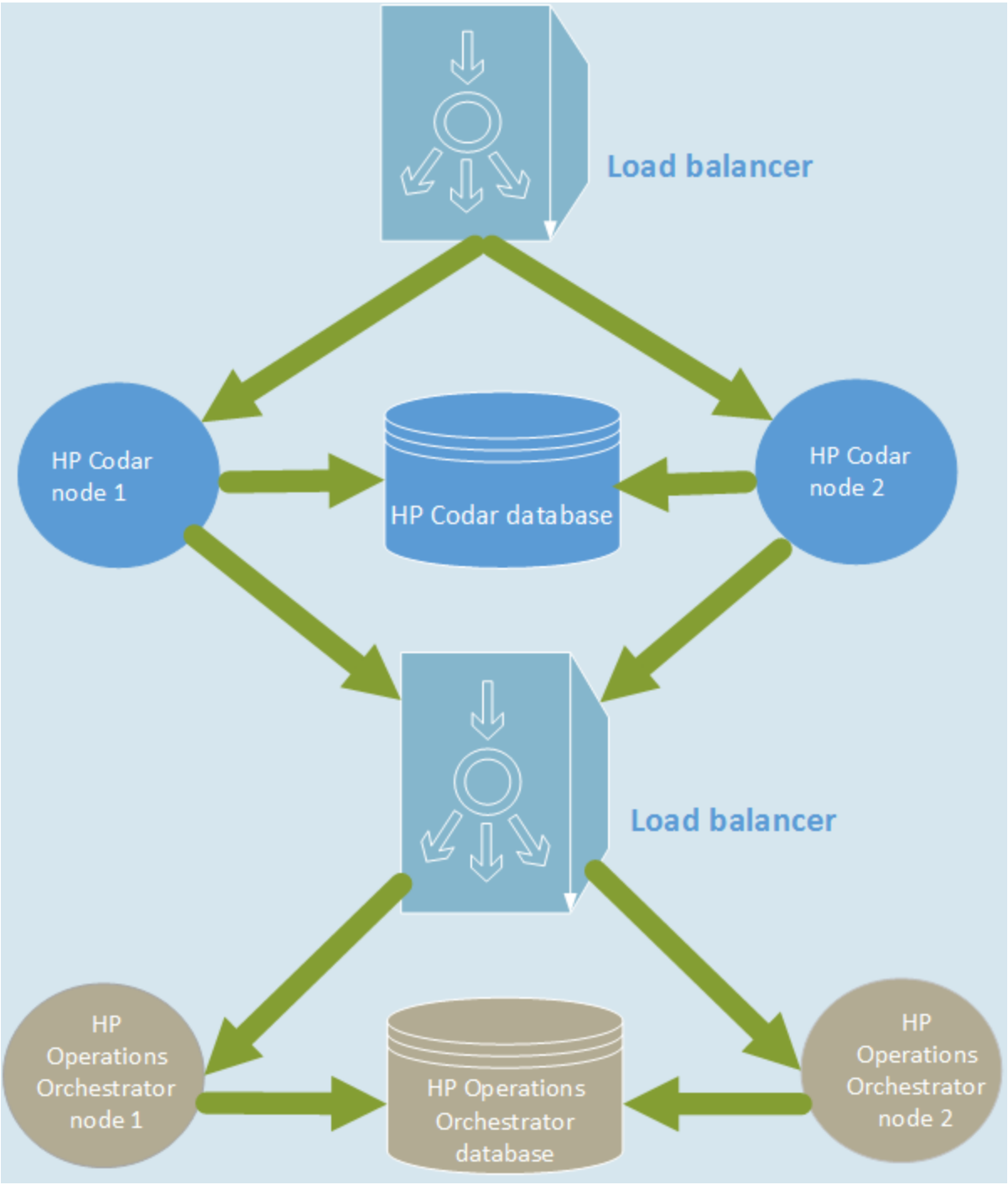
High availability (HA) refers to the process of keeping a computer system up and running continuously over a long period of time so that irrespective of the outside environment, the computer system continues to run without any disruptions.

HP Codar uses JBoss clustering technology to enable you to configure an active/active (high-availability) cluster. Clustering enables you to run HP Codar 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 HP Codar are load balanced among the nodes in the cluster. Increasing the number of nodes in the cluster improves web request transaction throughput. Increasing the number of nodes in the cluster also improves the response time by HP Codar fulfillment services to a high volume of concurrent deployment requests.

Because clustering distributes the workload across different nodes, if any node fails, HP Codar remains accessible through other nodes in the cluster. You can continue to improve HP 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 Codar 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 Codar after a node shuts down see only changes that were saved on that node.

HP Codar 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. Nodes are transparent to users and users access only the URL to the load balancer.



Guidelines for configuring in a clustered environment

The following guidelines must 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 HP Codar.

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

Configuring the load balancer node

Install and configure the load balancer on the load balancer node before setting up the HP Codar cluster configured for HA.

1. Install the load balancer
2. Configure the load balancer
3. Generate the SSL certificate required on the HP Codar node
4. Start the load balancer node

Installing the load balancer

Install and configure the load balancer following the manufacturer's recommendations. Refer to the manufacturer's documentation for more information.

Configuring the load balancer

The load balancer must be configured to balance the workload among the nodes in the HP Codar/JBoss cluster.

Configure the load balancer following the manufacturer's recommendations (refer to the manufacturer's documentation for more information) with the following exceptions:

- HP Codar only supports secure connections over TLSv1. Configure the load balancer for this connection protocol.

Generating the certificate

If you are configuring a secure connection (using a protocol such as TLS) to communicate from the load balancer to the HP Codar nodes, you need to generate the load balancer's certificate (referred to as `load_balancer.crt`). Copy this certificate to the `<codar_home>\jboss-as\standalone\configuration` (for Windows) or the `<codar_home>/jboss-as/standalone/configuration` (for Linux) directory on the HP Codar nodes.

Note: When configuring HP Codar, if you want to refer to the load balancer system by its IP address instead of its fully-qualified domain name (FQDN), you must generate the certificate with the `Subject Alt` attribute set to the IP address of the load balancer system.

Starting the load balancer

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

Configuring 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 Codar cluster configured for high availability. The Apache load balancer node comprises the Apache HTTP Web Server configured as a load balancer. It proxies web requests into the HP Codar cluster.

If you are using a load balancer other than Apache, see "Configuring the load balancer node" on page 8.

Upgrading the Apache load balancer node

To upgrade the Apache load balancer node, perform the following steps:

1. Stop the Apache load balancer on the HP Codar node.
2. Uninstall existing Apache applications from the HP Codar node following the manufacturer's recommendations.
3. Follow the instructions below to install and configure the Apache load balancer node on the HP Codar node. You are upgrading the HP Codar node because this is the node that is associated with the HP Codar software license. You can continue to use this software license after the upgrade.

Installing the Apache HTTP Web Server

To install the Apache HTTP 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/).

   For Microsoft Windows systems, after navigating to the mirror site, the 32-bit Windows installer is available in the `httpd/binaries/win32` directory.

   See the *HP Codar Support Matrix* for the supported version of the Apache HTTP Server. The *HP Codar 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 `<codar_home>\Apache2.2\modules` directory (for Microsoft Windows) or the `/etc/httpd/modules` directory (for Linux):

   - 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

Configuring the Apache HTTP Server as a load balancer

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

1. "Generate a certificate" on the next page
2. "Configure the Apache HTTP Server" on page 13

Start the Apache load balancer node

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

To start the Apache load balancer node on Microsoft Windows systems, do the following:

1. Navigate to the Services screen (**Control Panel** > **Administrative Tools** > **Services**).
2. Right-click the Apache2.2 service and select **Start**.

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 Codar node, you 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:

   For Microsoft Windows:

   ```
   "<codar_home>\Apache2.2\openssl" req -x509 -days 365 -newkey rsa:2048 -nodes -
   keyout <codar_home>\Apache2.2\conf\apache_csa.key -out <codar_
   home>\Apache2.2\conf\apache_csa.crt -config <codar_
   home>\Apache2.2\conf\openssl.cnf -subj /O=HP/OU=HP/CN=<apache_load_balancer_
   host_name>
   ```

   For 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=<apache_load_balancer_host_
   name>
   ```

   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 `<codar_home>\jbossas\standalone\configuration` directory (for Microsoft Windows) or the `<codar_home>/jbossas/standalone/configuration` directory (for Linux) on the HP Codar nodes.

Configure the Apache HTTP Server

1. Create a virtual host file for the HP Codar nodes. In the `<codar_home>\Apache2.2\conf\extra` directory (for Microsoft Windows) or the `/etc/httpd/conf.d` directory (for Linux), 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]:8081 route=csa1
BalancerMember http://[CSA_NODE2_HOSTNAME]:8081 route=csa2
BalancerMember http://[CSA_NODE3_HOSTNAME]:8081 route=csa3
ProxySet stickysession=CSA_ROUTEID
</Proxy>
ProxyPass / balancer://csacluster/
ProxyPassReverse / balancer://csacluster/
</VirtualHost>
```

2. Edit the `<codar_home>\Apache2.2\conf\httpd.conf` (for Microsoft Windows) `/etc/httpd/conf/httpd.conf` file (for Linux systems):

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

Microsoft Windows	Linux
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	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:

For Microsoft Windows:

```
Include conf\extra\csa.conf
```

For Linux:

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

Configuring the HP Codar node

This chapter describes how to install, upgrade, and configure an HP Codar node in an HP Codar cluster configured for HA (for example, codar_node1, codar_node2, or codar_node3).

The HP Codar node consists of:

- HP Codar
- Identity Management component

To configure the HP Codar node, do the following:

1. Install HP Codar
2. Configure HP Codar

Installing HP Codar

Install HP Codar on each HP Codar node as described in the *HP Codar Installation Guide* with the following exceptions:

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

  Note: All HP Codar 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 *HP Cloud Service Automation Content Installation Guide* for more information.
- If you are installing an external (existing) standalone instance of HP Operations Orchestration, HP recommends that you install HP Operations Orchestration in its own cluster configured for HA. Refer to the HP Operations Orchestration documentation for more information.

When installing HP Codar, if you have selected to install an embedded version of HP Operations Orchestration, perform the steps in the "Installing and configuring HP Operations Orchestration" on page 30 chapter.

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

Configuring HP Codar

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

1. "Edit properties" on the next page
2. "Enable JNDI" on page 18
3. "Request for a software license" on page 19
4. "Configure JBoss" on page 20
5. "Configure a secure connection" on page 22
6. "Configure the Identity Management component" on page 24
7. "Reconfigure the HP Codar service" on page 26
8. "Configure HP Single Sign-On" on page 27
9. "Share filesystem resources" on page 28

Edit properties

Update property values to route requests to the HP Codar node through the load balancer node and set the mode in which HP Codar is running as follows:

1. Edit the `<codar_home>\jboss-as\standalone\deployments\csa.war\WEB-INF\classes\csa.properties` (in Windows) or `<codar_home>/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/csa.properties` (in Linux) file as follows:

   a. Set the following properties:

   ```
   csa.provider.hostname=<load_balancer_host_name>
   csa.provider.port=<load_balancer_codar_port>
   csa.provider.rest.protocol=https
   deploymentMode=clustered
   ```

   For example:

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

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

   b. ssss

2. Edit the `<codar_home>/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/swagger.properties` (for Linux) or `<codar_home>\jboss-as\standalone\deployments\csa.war\WEB-INF\classes\swagger.properties` and set the following property:

   ```
   documentation.services.basePath=https://<load_balancer_host_name>:[load_
   balancer_port]/csa/rest
   ```

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

Enable JNDI

Enable the Java Naming and Directory Interface (JNDI):

1. Open the `<codar_home>\jboss-as\standalone\deployments\csa.war\WEBINF\applicationContext.xml` (for Microsoft Windows) or `<codar_home>/jboss-as/standalone/deployments/csa.war/WEBINF/applicationContext.xml` (for Linux) file in a text editor.

2. Locate the `START HA Mode Configuration` comment 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 close the file.

Request for a software license

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

After the initial installation, 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 Codar is installed. However, in a clustered environment, use the IP address of the load balancer when requesting a software license. Install the license on only one node in the clustered environment. For more information on managing software licenses, refer to the HP Codar Configuration Guide. For information on how to view, add, or delete a license, refer to the HP Codar online Help.

Configure JBoss

Configure JBoss for use in an HP Codar clustered environment:

1. Open the `<codar_home>/jboss-as/standalone/configuration/standalone-full-ha.xml` (for Linux) or `<codar_home>\jboss-as\standalone\configuration\standalone-full-ha.xml` (for Windows) file in a text editor.

2. Locate the `<server xmlns="urn:jboss:domain:2.2">` property and configure a unique name for the node. For example, <server xmlns="urn:jboss:domain:2.2" name="codar_node1">

3. Update the JGroups subsystem default stack from `udp` to `tcp`:

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

   For example,

   ```
   <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 controller cluster are listed. Other nodes that are not listed may join the cluster and you can 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 the 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, you must restart all nodes in the cluster. The following are examples of a list of three initial hosts: `[codar_node1_ip_address][7600],[codar_node2_ip_address][7600],[codar_node3_ip_address][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, 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 <*codar_node_name*>. For example:

   ```
   <subsystem xmlns="urn:jboss:domain:transactions:2.0">
      <core-environment node-identifier="codar_node1">
   ```

8. Add the node's IP address to the public interface. Locate `<interface name="public">` and add the IP address of the HP Codar node.For example:

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

Configure a secure connection

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

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

   a. If you have not already done so, copy the certificate from the load balancer node (load_balancer.crt) to the `<codar_home>/jboss-as/standalone/configuration` directory.

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

      For Linux:

      ```
      <codar_jre_home>/bin/keytool -importcert -file <codar_home>/jboss-as/
      standalone/configuration/load_balancer.crt -alias load_balancer_codar
      -keystore <codar_jre_home>/lib/security/cacerts
      ```

      For Windows:

      ```
      <codar_jre_home>\bin\keytool -importcert -file <codar_home>\jboss-as\
      standalone\configuration\load_balancer.crt -alias load_balancer_codar
      -keystore <codar_jre_home>\lib\security\cacerts
      ```

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

   a. Copy the certificate of each HP Codar node to every other HP Codar node in the cluster. The certificate file on each HP Codar node is `<codar_home>\jbossas\standalone\configuration\jboss.crt` (in Microsoft Windows) or `<codar_home>/jbossas/standalone/configuration/jboss.crt` (in Linux).

      For example, copy the certificates from codar_node2 and codar_node3 to codar_node1 to the directory `C:\Codar-Certificates`. Rename the certificate files with unique names, such as `jboss-codar_node2.crt` and `jboss-codar_node3.crt`.

   b. Import each certificate into the JVM of that HP Codar node. For example, on codar_node1, run the following commands:

      For Linux:

      ```
      <codar_jre_home>/bin/keytool -importcert -file /tmp/Codar-
      Certificates/jboss-codar_ node2.crt -alias codar_node2 -keystore <codar_jre_
      home>/lib/security/cacerts

      <codar_jre_home>/bin/keytool -importcert -file /tmp/Codar-
      Certificates/jboss-codar_ node3.crt -alias codar_node3 -keystore <codar_jre_
      home>/lib/security/cacerts
      ```

      For Windows:

```
"<codar_jre>\bin\keytool" -importcert -file C:\Codar-Certificates\jboss-
codar_ node2.crt -alias codar_node2 -keystore "<codar_
jre>\lib\security\cacerts"

"<codar_jre>\bin\keytool" -importcert -file C:\Codar-Certificates\jboss-
codar_ node3.crt -alias codar_node3 -keystore "<codar_
jre>\lib\security\cacerts"
```

Configure the Identity Management component

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

1. Add the following content in the `<codar_home>/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/applicationContext.properties` (in Linux) or the `<codar_home>\/jboss-as\standalone\deployments\idm-service.war\WEB-INF\spring\applicationContext.properties` (in Windows) file:

   ```
   idm.csa.hostname = <load_balancer_host_name>

   idm.csa.port = <load_balancer_codar_port_number>

   .

   .

   .

   # Properties for CSA Auditing Server

   .

   .

   .

   idm.csa.audit.hostname = <load_balancer_host_name>"/>

   idm.csa.audit.port = <load_balancer_codar_port_number>"/>
   ```

   For example:

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

   idm.csa.port = 8443

   .

   .

   .

   # Properties for CSA Auditing Server

   .

   .

   .

   idm.csa.audit.hostname = load_balancer.xyz.com"/>

   idm.csa.audit.port = 8443"/>
   ```

2. Update the values of the host name and port to the `[LOAD_BALANCER_HOSTNAME]` and `[LOAD_`

BALANCER_Codar_HTTPS_PORT] in the applicationContext-security.xml file:

```
<beans:bean id="idmConfig"
class="com.hp.ccue.identity.rp.IdentityServiceConfig">

<beans:property name="protocol" value="https"/>

<beans:property name="hostname" value="[LOAD_BALANCER_HOSTNAME]"/>

<beans:property name="port" value="[LOAD_BALANCER_Codar_HTTPS_PORT]"/>

<beans:property name="servicePath" value="idm-service"/> <!-- or hpcloudidm-
service if you don’t change the name of the WAR -->

<beans:property name="integrationAcctUserName" value="idmTransportUser"/>

<beans:property name="integrationAcctPassword"

value="${securityIdmTransportUserPassword}"/>

</beans:bean>
```

For example:

```
<beans:bean id="idmConfig"

class="com.hp.ccue.identity.rp.IdentityServiceConfig">

<beans:property name="protocol" value="https"/>

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

<beans:property name="port" value="8443"/>

<beans:property name="servicePath" value="idm-service"/> <!-- or hpcloudidm-
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>
```

3. Uncomment the following line in the <codar_home>\jboss-as\standalone\deployments\csa.war\WEB-INF\applicationContext.xml (for Windows) or <codar_home>/jboss-as/standalone/deployments/csa.war/WEB-INF/applicationContext.xml (for Linux) file:

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

Reconfigure the HP Codar service

Reconfigure the HP Codar service to start, restart, and stop HP Codar using the `standalone-fullha.xml` configuration file.

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

1. Open a command prompt.
2. Stop the HP Codar service by running the `service codar stop` command.
3. Edit the `<codar_home>/scripts/csa_env.conf` (for Linux) or the `<codar_home>\bin\service.bat` (for Windows) file:

   For Linux:

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

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

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

   For Windows:

   a. Locate the two occurrences of `standalone.bat`.

   b. Insert the `-c standalone-full-ha.xml` command line option into the `call standalone.bat > .r.lock >> run.log 2>&1` command line.

4. Start the HP Codar service by running the `service codar start` command.

Configure HP Single Sign-On

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

1. Open the `<codar_home>/jboss-as/standalone/deployments/csa.war/WEBINF/hpssoConfiguration.xml` (for Linux) or `<codar_home>/jboss-as/standalone/deployments/csa.war/WEBINF/hpssoConfiguration.xml` (for Windows) file in a text editor.

2. Locate the following content:

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

3. Replace [CSA_NODE_HOSTNAME] and [CSA_NODE_PORT] with the load balancer host name and the virtual host port for the HP Codar nodes. For example:

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

4. Locate the `initString` value in the `crypto` element. The `initString` setting for HP Codar 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. Copy the `initString` value to the other nodes in the cluster and configure any applications that are integrated with HP Single Sign-On. The `initString` value represents a secret key and must be treated as such in your environment.

Share filesystem resources

Configure HP Codar 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 Codar.

HP Codar provides images that are stored in an images directory (for example,`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.

Configuring HP Codar to use a shared filesystem to store images on Linux

To configure HP Codar to use a shared filesystem to store images on Linux systems, perform the following steps:

1. Move the contents of the `csa.war/images` directory to the shared location. For example, move the files to //<SharedFilesystem>/Codar/Images
2. On the HP Codar node, log in as root.
3. Delete the `<codar_home>/jboss-as/standalone/deployments/csa.war/images` directory if it exists.
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 by typing `chmod 600 /etc/.win-mnt-cred`.
6. Edit `/etc/fstab` by adding the following line:

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

7. Mount the shared filesystem by typing `mount -a`.

Configuring HP Codar to use a shared filesystem to store images on Microsoft Windows

To configure HP Codar to use a shared filesystem to store images on Windows systems, perform the following steps:

1. HP recommends that you run the HP Codar service as a non-administrative user. If you run the HP Codar service as a non-administrator user, the examples in this section assume that you have created the CodarUser.

2. On a remote system, create a directory or folder that will contain the shared files and share the folder. For example, if you create a folder named `C:\Codar\images` on the remote system, in a command prompt on the remote system, type `net share Codar_images=C:\Codar\images`.

3. Copy the `<codar_home>\jboss-as\standalone\deployments\csa.war\images` directory from one of the Codar nodes to the shared folder on the remote system.

4. Delete the `\csa.war\images` directory from each HP Codar node.

5. On each HP Codar node, create a symbolic link to the shared folder. For example, from a command prompt, type the following commands:

   ```
   mklink /d <codar_home>\jboss-as\standalone\deployments\csa.war\images
   \\<SharedFilesystem>\Codar_images
   ```

   Note: If you configured a non-administrator user to start and stop the HP Codar service (for example, CodarUser), you must create the symbolic link as this user.

6. On each node, do the following:
   a. Navigate to **Control Panel** > **Administrative Tools** > **Services**.

   b. Right-click on the HP Codar service and select **Properties**.

   c. Click the **Log On** tab.

   d. Select **This account**, enter the user who starts and stops the HP Codar service (for example, if you are running the HP Codar service as a non-administrator user such as CSAUser, enter `.\CSAUser`; if you are running the service as an administrator, enter `.\Administrator`), and enter the user's password.

   e. Click **OK**.

Installing and configuring HP Operations Orchestration

Install and configure HP Operations Orchestration as described in the *HP Codar Installation Guide* with the following exceptions. The *HP Codar Installation Guide* can be downloaded from the HP Software Support website (this site requires that you register with HP Passport).

1. HP recommends that you install HP Operations Orchestration in its own cluster configured for HA.
2. Configure SSL between HP Operations Orchestration and all HP Codar nodes.

Note: When you install HP Codar, HP Operations Orchestration is not available out-of-the-box in a cluster setup. Perform the steps in this chapter to configure HP Operations Orchestration in a cluster.

Configuring HP Codar in HA mode using an embedded instance of HP Operations Orchestration

When installing HP Codar, if you have selected to install an embedded version of HP Operations Orchestration, perform the following steps to configure HP Codar in HA mode using the embedded instance of HP Operations Orchestration:

Point all HP Operations Orchestration instances to a single database

Every HP Codar installation has an instance of HP Operations Orchestration installed and all these HP Operations Orchestration instances point to different databases. To enable HA we have to make all of the HP Operations Orchestration instances point to a single database manually by performing the following steps:

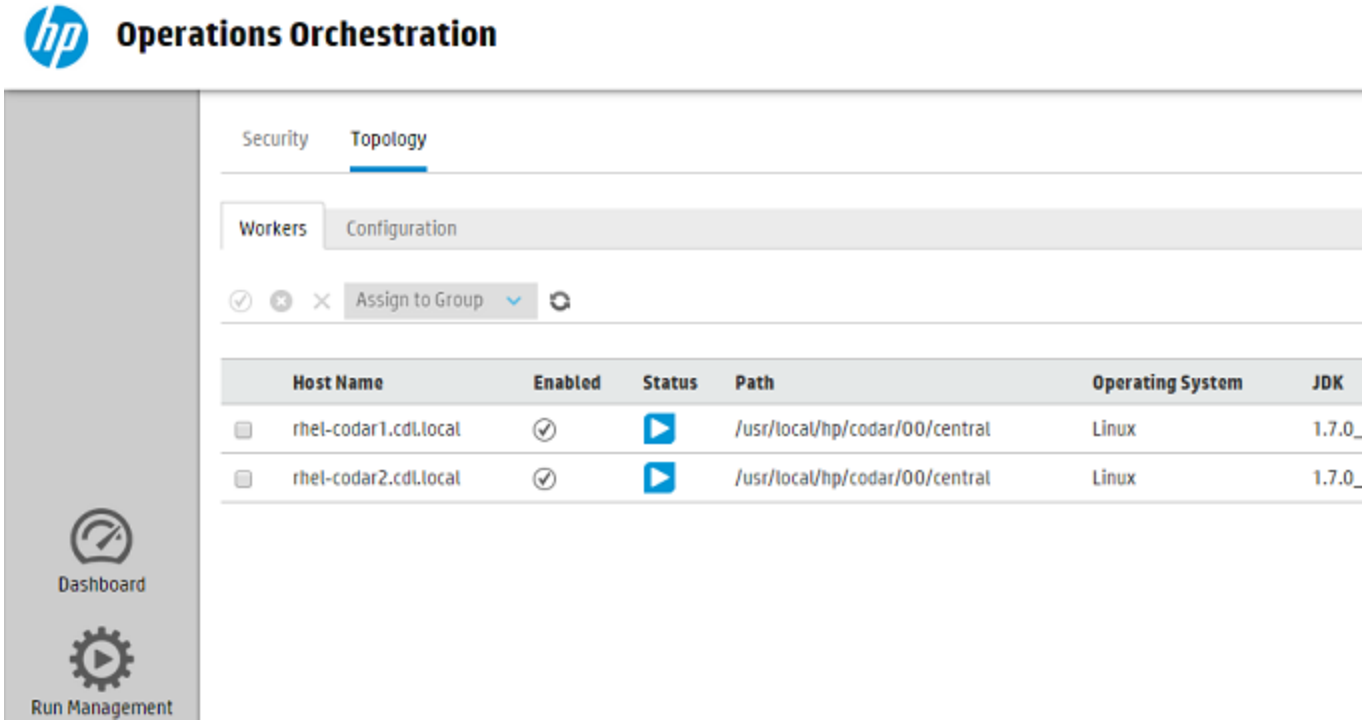
1. Copy the following files from one of the HP Operations Orchestration instances to all the other instances:

Microsoft Windows	Linux
■ <installation_directory>\HP Operations Orchestration\central\conf\database.properties ■ <installation_directory>\HP Operations Orchestration\central\var\security\encryption.properties ■ <installation_directory>\HP Operations Orchestration\central\var\security\encryption_repository ■ <installation_directory>\HP Operations Orchestration\central\var\security\key.store	■ <installation_directory>/HP Operations Orchestration/central/conf/database.properties ■ <installation_directory>/HP Operations Orchestration/central/var/security/encryption.properties ■ <installation_directory>/HP Operations Orchestration/central/var/security/encryption_repository ■ <installation_directory>/HP Operations Orchestration/central/var/security/key.store

2. Delete the `credentials.store` file from the `<installation dir>\HP Operations Orchestration\central\var\security` directory (in Microsoft Windows) or the `<installation dir>/HP Operations Orchestration/central/var/security` directory (in Linux)for all HP Operations Orchestration instances except the instance from which the files were copied in step 1.

3. Restart the HP Operations Orchestration service for all the instances.

Each of the HP Operations Orchestration instances now display all the hosts with active status as shown in the following figure. In this figure, two nodes have active status.



Configure HP Operations Orchestration in the HA environment

After ensuring that all HP Operations Orchestration instances point to a single database, configure them in the HA environment by performing the following steps:

> **Note:** Skip steps 1 to 5 if you are using the same load balancer for both HP Codar and HP Operations Orchestration.
>
> The steps below outline the configuration for the Apache load balancer, You can use any load balancer that you want.

1. Install the Apache server and generate an SSL certificate using the following command :

   ```
   openssl req -x509 -days 365 -newkey rsa:2048 -nodes -keyout <apache_
   home>\Apache<version>\conf\apache_csa.key -out <apache_
   home>\Apache<version>\conf\apache_csa.crt -config <apache_
   home>\Apache<version>\conf\openssl.cnf -subj /O=HP/OU=HP/CN=<apache_load_
   balancer_host_name>
   ```

2. Copy `apache_csa.crt` from `<apache_home>\Apache<version>\conf` to the `<codar_home>\jboss-as\standalone\configuration` directory.

3. Apply the SSL certificate on all the HP Codar nodes using the following command:

```
keytool -importcert -file "<codar_home>\jboss-
as\standalone\configuration\apache_csa.crt" -alias apache_csa -keystore
"<codar_home>/openjre/lib/security/cacert
```

4. Update the `httpd.conf` file with the following modifications:
   a. Verify that the following modules exist:
      - `<apache_home>\Apache<version>\modules\mod_authz_host.so`
      - `<apache_home>\Apache<version>\modules\mod_headers.so`
      - `<apache_home>\Apache<version>\modules\mod_log_config.so`
      - `<apache_home>\Apache<version>\modules\mod_proxy.so`
      - `<apache_home>\Apache<version>\modules\mod_proxy_balancer.so`
      - `<apache_home>\Apache<version>\modules\mod_proxy_connect.so`
      - `<apache_home>\Apache<version>\modules\mod_proxy_http.so`
      - `<apache_home>\Apache<version>\modules\mod_rewrite.so`
      - `<apache_home>\Apache<version>\modules\mod_ssl.so`
   b. Add or update the list of modules 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`
   c. Add the `Include conf/extra/OO.conf` and `Timeout 90000` lines.
5. Update the `<Engine defaultHost="localhost" name="Catalina" >` line to include the JVM route addition: `<Engine defaultHost="localhost" name="Catalina" jvmRoute="node1">`

The `jvmRoute` node number must match the node number used when configuring the Apache load balancer.

6. Create a virtual host file for the HP Operations Orchestration nodes by creating a file named `OO.conf` in the `<apache_home>\Apache<version>\conf\extra` directory. The file must contain the following content:

```
Listen 8585
<VirtualHost *:8585>
ProxyRequests off
ServerName [APACHE_LOAD_BALANCER_HOSTNAME]
ServerAlias [APACHE_LOAD_BALANCER_HOSTNAME]
<Proxy balancer://mycluster>
BalancerMember http:// [OO_NODE1_HOSTNAME]:8082 route=node1
BalancerMember http:// [OO_NODE2_HOSTNAME]:8082 route=node2
Order Deny,Allow
Deny from none
Allow from all
ProxySet stickysession=JSESSIONID|jsessionid scolonpathdelim=On
</Proxy>
<Location /balancer-manager>
SetHandler balancer-manager
Order deny,allow
Allow from all
</Location>
ProxyPass /balancer-manager!
ProxyPass / balancer://mycluster/ stickysession=JSESSIONID|jsessionid
scolonpathdelim=On
ProxyPassReverse / balancer://mycluster
SSLEngine On
SSLProxyEngine On
SSLProxyVerify none
SSLProxyCheckPeerCN off
SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
SSLCertificateFile <apache_home\Apache<version>\conf\apache_csa.crt
SSLCertificateKeyFile <apache_home\Apache<version>\conf\apache_csa.key
</VirtualHost>
```

7. Update the `OOS_URL` property of the `<codar_home>\jboss-as\standalone\deployments\codar.war\WEB-INF\classes\codar.properties` file with the URL of the load balancer for all of the HP Codar nodes. For example, `OOS_URL=https://<apache_load_balancer_host_name>:8585`

8. Specify the URL of the HP Operations Orchestration load balancer on the Configuration tab in one of the HP Operations Orchestration instances and save it. This URL gets reflected in the other instances.

9. Restart the HP Operations Orchestration central service, HP Codar service, and the Apache service.

Configure common tasks

This chapter provides information on how to perform common tasks pertaining to HP Codar.

Starting HP Codar

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

Starting HP Codar on Linux systems

To start HP Codar, on the server that hosts HP Codar, type `service codar start`.

Starting HP Codar on Windows systems

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

Stopping HP Codar

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

Stopping HP Codar on Linux systems

To stop HP Codar, on the server that hosts HP Codar, type `service codar stop`.

Stopping HP Codar on Windows systems

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

Start the Apache load balancer node

If you are using Apache as the load balancer, to start the Apache load balancer node, perform the following steps:

1. Navigate to the Services screen (**Control Panel** > **Administrative Tools** > **Services**).
2. Right-click on the **Apache<*version_number*>** service and select **Start**.

Stop the Apache load balancer node

To start the Apache load balancer node, perform the following steps:

1. Navigate to the Services screen (**Control Panel** > **Administrative Tools** > **Services**).
2. Right-click on the **Apache<*version_number*>** service and select **Stop**.

Launch HP Codar

Launch the HP Codar console through the load balancer by opening one of the following URLs in a supported Web browser:

- `http://<load_balancer_host_name>:<load_balancer_http_port>/csa`

  For example, http://load_balancer.xyz.com:8080/csa

- `https://<load_balancer_host_name>:<load_balancer_http_port>/csa`

  For example, https://load_balancer.xyz.com:8080/csa

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:

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!