Patch Readme – Linux and Windows

Cloud Service Automation

Software version: CSA 4.50.0003 Patch
Publication Date: May 25, 2016

Contents

Introduction

This ReadMe provides lists of CSA Fixed Issues and Know Issues, includes a What's New section, and explains how to Install the Patch and Uninstall the Patch. The cumulative patch updates CSA server to 04.50.0003.

Note: See the CSA 4.x Documentation Library on the HP Software Support Online portal for links to all product documentation.

What's New

Fixed issues

This release resolves numerous CSA issues. See the Fixed Issues section.

TLS support

To restrict support to TLS 1.2 only (optional), modify the following files:

File	Modification
`<CSA_HOME>\jboss-as\standalone\configuration\standalone.xml` file (for standalone servers) and `<CSA_HOME>\jboss-as\standalone\configuration\standalone.full.ha.xml` (for clusters)	Insert the yellow-highlighted information shown below: `<https-listener name="https" socket-binding="https" security-realm="SSLRealm" enabled-protocols="TLSv1.2" enabled-cipher-suites="TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,..."/>`

`<CSA_HOME>\portal\conf\mpp.conf`	Insert the yellow-highlighted information shown below:
	`"provider": {`
	`"url": "https://<LB node>:<lb csa port>",`
	`"contextPath": "/csa/api/mpp",`
	`"strictSSL": true,`
	`"TLSVersions": "1.2",`
	`"ca": "C:/Program Files/HPE/CSA/jboss-as/standalone/configuration/apache_csa.crt"`
	`},`
	`"idmProvider": {`
	`"url": "https://<LB node>:<lb csa port>",`
	`"returnUrl": "https://<LB node>:<lb mpp port>",`
	`"contextPath": "/idm-service",`
	`"username": "idmTransportUser",`

	"password": "ENC(F9za+OiGOCl1PmTgef2EUQ\u003d\u003d)",
	"strictSSL": true,
	"TLSVersions": "1.2",
	"ca": "C:/Program Files/HPE/CSA/jboss-as/standalone/configuration/apache_csa.crt"
	},
	"https": {
	"enabled": true,
	"options": {
	"pfx": "../conf/.mpp_keystore",
	"passphrase": "ENC(Rp1mUoWYO5TdgwAGofCRiw\u003d\u003d)",
	"TLSVersions": "1.2"
	}
	},
	Note: You must make sure that your integrated products also support TLS 1.2.

Apache v2.4 support

To enable CSA support for Apache 2.4, add these parameters and corresponding values to the `<path_to>\Apache2.2\conf\extra\mpp.conf` file after the entry `SSLProxyEngine`:

- `SSLProxyEngine` **on**
- `SSLProxyVerify` **none**
- `SSLProxyCheckPeerCN` **off**
- `SSLProxyCheckPeerName` **off**

Note: CSA 4.50.0003 has been verified on clusters using Apache 2.4 and BIG-IP F5 11.5.1 LB. Support for TLS 1.1 only and TLS 1.2 only has been verified with CSA 4.50.0003 and OO 10.51.

Fixed Issues

Issues fixed in 4.50.0003 patch

Issue	Description
QCCR1D224435	**Symptom:** When custom regular expression are mentioned for option properties and left empty, validation fails for the default value and throws blue screen. **Resolution:** Corrected the behavior in the product.
QCCR1D212892	**Symptom:** MPP does not retain expected order of option properties, and the order in Service Offering UI changes after loading offering in MPP **Resolution:** Corrected the behavior in the product.
QCCR1D208821	**Symptom:** Parent property not present on same option model throws blue screen **Resolution:** Corrected the behavior in the product.
QCCR1D213229	**Symptom:** Modifying a subscription that has 2-level option sets does not work as expected when setting Initial Order Only=ON for the parent option **Resolution:** The fix is to allow Consumers to modify the Child Options if Child `Optionset initialOrderOnly` is set Off, while the parent `Optionset's IntialOrderOnly` is set ON.
QCCR1D217168	**Symptom:** We should be able to get a list of service offerings associated to a selected Service Design. **Resolution:** The list of service offerings will get displayed in the designer page.
QCCR1D217514	**Symptom:** Provide refresh button on subscription list page on mpp. **Resolution:** Provided Refresh button to reload the data once gray button appears.
QCCR1D217838	**Symptom:** Elasticsearch/Search Guard plugin needs to be configurable for TLS 1.2 only or TLS 1.2 and 1.1 only.

Issue	Description
	Resolution: Now supported.
QCCR1D218397	**Symptom:** Confirmation message modification needed to alert users when a subscription is canceled. **Resolution:** Modified the message to alert the user during subscription cancelation.
QCCR1D218526	**Symptom:** Canceled/Expired failed subscriptions should show retry button. **Resolution:** Provided retry button for cancel/expire failed subscriptions.
QCCR1D218668	**Symptom:** Provide a way to mark Subscription name as a required input to prevent creation of multiple services with the same name. **Resolution:** Now supported.
QCCR1D218877	**Symptom:** Subscription modify fails with 'timeout' status while OO flow finishes without error. **Resolution:** The List Data type found in property type of Topology Component property will be removed. Topology Component property now only supports 'String', 'Boolean', 'integer' only.
QCCR1D218936	**Symptom:** The value of Customer Regular Expression could not be seen after reopening. **Resolution:** Now supported.
QCCR1D219686	**Symptom:** Modify Subscription Do not Pass value to Component property. **Resolution:** Now supported.
QCCR1D220515	**Symptom:** While reordering using a reordered request, the selection options are ignored when the request is submitted. **Resolution:** Subscriber options are now filled first.
QCCR1D222574	**Symptom:** Need procedure to delete duplicate usernames from database.

<table>
<tr><th>Issue</th><th>Description</th></tr>
<tr><td></td><td>Resolution:
Now supported.</td></tr>
<tr><td>QCCR1D224014</td><td>
Symptom:
Group Owned Subscription is not returned through Global Search.
Resolution/Workaround:
Group-owned subscription access is turned off by default.
Use the following steps to enable access for all members of the group:
Note: Make sure the CSA jar files are already loaded.

Run the following command to create new ES indexes to store user-group information:

a. Windows:
<code>CSA\csa-search-service\bin>..\..\node.js\node.exe create-usergroup-index-mapping.js</code>
b. Linux:
<code>csa/csa-search-service/bin>..\..\node.js\node</code>

create-usergroup-index-mapping.jsAdd new search-based mapping:
<table>
<tr><th>In this Location</th><th>Add This</th></tr>
<tr><td>csa.properties file</td><td>enableSearchForGroupOwned=true</td></tr>
<tr><td>CSA\csa-search-service\app.json
Under msvc-basic-search</td><td>enableSearchForGroupOwned: true

For example:
"msvc-basic-search": {
"searchEngineURL": "https://localhost:9201",
"searchEngineUser": "admin",
...
"strictSSL": false,

"enableSearchForGroupOwned": true,
"rejectUnauthorized": false,
...
"maxFile": 10
}</td></tr>
</table>

Note: Run the create-usergroup-index-mapping.js script successfully before you set the enableSearchForGroupOwned property to true in either the csa.properties or the app.json file.
</td></tr>
</table>

Issue	Description
	If the `enableSearchForGroupOwned` property is set to `true`, the Global Search will only work for the subscriptions created after the property is set. 3. Restart CSA, Marketplace Portal, Search, and Elasticsearch 1.5.2 (elasticsearch-service-x64).

Issues fixed in 4.50.0002 patch

Issue	Description
QCCR1D189960	**Symptom:** When assigning a group to the CSA subscription, Groups like "Remote Desktop Users" where the user is not a member is shown. **Resolution:** Only the groups defined in CSA for access will be displayed in the drop down list for Group Ownership.
QCCR1D193127	**Symptom:** Unable to view the value shown in the drop-down lists while expanding the details in View Request Details, and Review Request Details. **Resolution:** Corrected the behavior in the product.
QCCR1D212278	**Symptom:** Approval pop-ups are shown each time an action is being started on a service component even when no approval is set for the specific action. **Resolution:** Corrected the behavior in the product.
QCCR1D212537	**Symptom:** Admin UI wrongly checks the input values for Offerings. It request for Display name + version to be unique, which is not correct. **Resolution:** Allows creating a service offering that has the same display name and offering version as set for another service offering.
QCCR1D212811	**Symptom:** Service Modification form should have "Show More Details" enabled (ON) by default.

Issue	Description
	Resolution: Show Details is enabled in Subscription Modification screen by default.
QCCR1D213328	**Symptom:** When the subscription is in paused state and the subscription has an approval for cancellation, then the subscription is stuck in the pending state forever. **Resolution:** Subscription will not be stuck in pending state under any conditions.
QCCR1D213369	**Symptom:** Request Subscription API calls, which works for CSA 3.2 are not working on CSA 4.5. **Resolution:** Upgraded the undertow jars.
QCCR1D214030	**Symptom:** Subscription creation/edit is ignoring subscriber's input for a property that is unlocked but is under locked Option **Resolution:** Subscriber input given to a property of a locked Option will be set.
QCCR1D214086	**Symptom:** It was not possible to integrate to CSA using ccue-consumption REST API. **Resolution:** Now we are providing 2(GET and POST) integration APIs in CSA to use the ccue-consumption REST API.
QCCR1D214172	**Symptom:** Dynamic option JSP is not running in some cases - cached results are presented. **Resolution:** Option value cache timeout reduced to one second, instant cached results are presented.
QCCR1D214834	**Symptom:** API is not returning the correct date format in the XML. If the milliseconds portion of the timestamp is .000, then the API is strips the value and causes the OO date parser to fail. **Resolution:** Added 10 millisecond delay when time has 000 millisecond value.
QCCR1D215129	**Symptom:** Unable to receive emails when subscription processing is paused due to provisioning failure.

Issue	Description
	Resolution: Emails should be sent when subscription provisioning fails and pause on failure is enabled.
QCCR1D215378	**Symptom:** While migrating design from CloudOS to HOS without saving the design, the correct HOS tag is not arrived. **Resolution:** Fixed.
QCCR1D217040	**Symptom:** Option icons on service offering options are not displayed in the MPP. **Resolution:** Fixed.
QCCR1D217430	**Symptom:** Database Error Occurs when we request User Identifier Through Legacy API. **Resolution:** Fixed.
QCCR1D217755	**Symptom:** DB error occurs when executing 2 API calls at the same time, as it doesn't allow two update queries on the same table at the same time. **Resolution:** Parallel submit of request will not result in an exception and the subscriptions will be created successfully.
QCCR1D218298	**Symptom:** The user options are arranged in a random way for some offerings. **Resolution:** The Option property sorting is now based on the natural order defined in the Design.
QCCR1D218404	**Symptom:** CSA Category Filter is only showing "Platform Services". "Database Services" and "Network Services" not displaying in the drop-down list. **Resolution:** Fixed.
QCCR1D218711	**Symptom:**

Issue	Description
	Some JSPs that are loading dynamic subscription options are shown as invalid when the default option is empty. **Resolution:** Fixed.
QCCR1D219387	**Symptom:** If a display name of a Topology design contains multi-byte characters, a name of the corresponding OO content pack is corrupted. **Resolution:** Fixed.
Issues fixed in 4.50.0001 patch	
QCCR1D170695	**Symptom:** The internal action - 'Build Resource Provider and Pool List' fails to select a valid Resource Pool when used with multiple resource providers. **Resolution:** Fixed.
QCCR1D190452	**Symptom:** Service Offering with a wide Optionsets takes long time to load in the MPP. **Resolution:** Loading time improved.
QCCR1D194880	**Symptom:** In CSA 4.10, the selected background image for the "Dashboard Widgets" is ignored and the background remains white in MPP. **Resolution:** The requested change will not be addressed within the product.
QCCR1D194983	**Symptom:** If the Subscriber Option properties that are set to invisible in the Service Design they will reappear after the visibility of the overlaying option in the Service Offering changed. **Resolution:** The visibility of the options in the portal are now consistent with their settings in the Offering UI.
QCCR1D208427	**Symptom:** Show properties of a canceled subscription. **Resolution:**

Issue	Description
	Component properties of a canceled subscription now shown on the services page.
QCCR1D208611	**Symptom:** Too many logs accumulate after old subscriptions are deleted from MPP and CSM. **Resolution:** Fixed.
QCCR1D208830	**Symptom:** Subscriber Option values from dynamic JSP pages are not loading when propertyName string used **Resolution:** Fixed.

QCCR1D209136	**Symptom:**
	When the following API call is executed, there is a subscription count 1:
	`https://***.***.***.***:8444/csa/rest/user/mysubscription?userIdentifier=20f6509a49a978fe0149c8629a3e5163&requestor=pvrbican_m&returnRetired=true&creationStartDate=2015-03-11T23:59:59`
	After adding the creationEndDate parameter, execution of the call using the same startDateParameter yields a subscription count 87:
	`https://***.***.***.***:8444/csa/rest/user/mysubscription?userIdentifier=20f6509a49a978fe0149c8629a3e5163&requestor=pvrbican_m&returnRetired=true&creationStartDate=2015-03-11T23:59:59&creationEndDate=2015-03-17T23:59:59`
	Resolution:
	Fixed.

QCCR1D209782	**Symptom:** In CSA 3.2, the Cancel Subscription button is still available to the end-user. If the user clicks 'Cancel Subscription' twice, CSA continues the provisioning lifecycle. This option is not available in CSA 4.2. **Resolution:** Cancel Subscription button should be enabled in MPP UI if a subscription cancellation fails.

Known Issues

The following table describes the remaining known issues in this patch.

Issue	Description

QCCR1D220470	**Symptom:**
	Cluster environment fails after installation if CSA is configured in high-availability mode.
	Resolution:
	Replace this:
	`<!--START HA Mode Configuration-->`
	`<!--  <jee:jndi-lookup id="channelGroup" jndi-name="java:jboss/clustering/group/server" expected-type="org.wildfly.clustering.group.Group"/> à`
	`<!--END HA Mode Configuration-->`
	With this:
	`<!--START HA Mode Configuration-->`
	`<jee:jndi-lookup id="channelGroup" jndi-name="java:jboss/clustering/group/server" expected-type="org.wildfly.clustering.group.Group"/>`
	`<!--END HA Mode Configuration-->`
	
	Restart CSA, Marketplace Portal, Search, and Elasticsearch 1.5.2 (elasticsearch-service-x64).
	
	`<jee:jndi-lookup id="channelGroup" jndi-name="java:jboss/clustering/group/server" expected-type="org.wildfly.clustering.group.Group"/>`
	`<!--END HA Mode Configuration-->`

QCCR1D210391	**Symptom:** Elastic Search does not work after installation if CSA 4.5 is configured in high-availability mode. **Resolution:** See Configuring Elasticsearch in Cluster Environments.
QCCR1D210453	**Symptom:** Modifying token values in Option Model property editor causes problems when retrieving property values from Marketplace Portal during service creation. **Resolution:** Do not edit token value after selecting a token.
QCCR1D210590	**Symptom:** Various issues are seen when using Google Chrome version 44 to browse Service Management Console and Marketplace Portal when CSA is setup with self-signed certificates. **Resolution:** Use earlier versions of Google Chrome, or another browser, such as Internet Explorer or Mozilla Firefox. Alternatively, in Google Chrome v. 44, add the certificate to 'Trusted Root Certificate Authorities'.

Issue	Description
QCCR1D211195	**Symptom:** In Internet Explorer 11, service topology view of a service subscription from Marketplace Portal does not show the state of a service component when users hover over the icon. **Resolution:** Use another browser or browser version.
QCCR1D211202	**Symptom:** Webpage becomes unresponsive when you open a service offering based on OpenStack service designs. **Resolution:** Log out of Marketplace Portal and log back in.

QCCR1D207419	**Symptom:**
	Audit logging does not occur when IDM creates an SSO cookie.
	Resolution:
	Add the `<property name="auditAppender" ref="auditAppender"/>` property to any un-commented SSOFilter bean in the `/idm-service.war/WEB-INF/spring/applicationContext-security.xml` file:
	Make the change highlighted in yellow:
	`<bean id="ssoFilter" class="com.hp.ccue.identity.filter.sso.SSOFilter">`
	`<property name="generateTokenUtil" ref="generateTokenUtil" />`
	`<property name="tokenFactory" ref="tokenFactory" />`
	`<property name="loginRedirectionHandler" ref="loginRedirectionHandler" />`
	`<property name="auditAppender" ref="auditAppender"/>`
	`</bean>`

Enhancements

The following table describes the enhancements available in this patch.

Change Request	Description
QCCR1D201403	**Symptom:** CSA currently uses the out-of-the-box, Spring- provided CAC filter, which provides a regex to parse the Subject field. **Resolution:** CSA now supports subjectDN and subjectAltName attributes (rfc822Name and OtherName for UPN) of X.509 certificate.
QCCR1D208162	**Symptom:** Service Request does not track the subscription completion.

Change Request	Description
	Resolution: The service request state/status and completedOn timestamp updated to include order, modify, and cancel.
QCCR1D209226	**Symptom:** Emails rejecting end-user requests do not include a reason. **Resolution:** Fixed.
Enhancements for 4.50.0001 patch	
QCCR1D188066	**Symptom:** Inability to read the catalog ID in the dynamic query JSPs, by adding the SVC_CATALOG_ID token to the list of available tokens in the dynamic query http body. **Resolution:** The catalog ID - [PORTAL: CATALOG_ID] is now available.
QCCR1D209730	**Symptom:** Logged-in user Id incorrect. **Resolution:** Fixed.

QCCR1D210180	**Symptom:**
	Consumer admin is able to create service offerings from MPP and potentially set zero pricing.
	Resolution:
	Follow these steps to remove the Offering Management tile, which enables the Tenant Admin to turn off the Offering Management widget:
	1. In `<CSA_Installation_Folder>/portal/conf/dashboard.json`, in the `MANAGE_OFFERINGS` entry, delete the yellow-highlighted object labeled `common.items.MANAGE_OFFERINGS:`
	`{`
	`"label": "common.items.MANAGE_OFFERINGS",`
	`"icon": {`
	`  "className": "icon-services"`
	`},`
	`"className": "orange",`
	`"link": {`
	`  "url" : "consumption/offerings/ ",`
	`  "target": "_blank"}`
	`}`
	2. In `<CSA_Installation_Folder>/portal/conf/mpp.json`, in the `enableOfferingAdministration` parameter, set the `consumption.enableOfferingAdministration` property to FALSE.
	7. Restart MPP service.

Change Request	Description
QCCR1D210054	**Symptom:** Need the ability to disable security-warning banner. **Resolution:** Change the value of the following parameters to FALSE: 1. MPP: **Parameter:** `header.securityWarning.enable` **Location:** `CSA_HOME/portal/conf/dashboard.json` 2. MPP Tenant Admin: **Parameter:** `enableSecurityWarning` **Location:** `CSA_HOME/portal/node_modules/mpp-consumption/dist/offerings/config.js` 3. SCM: **Parameter:** `enableSecurityWarning` **Location:** `CSA_HOME/jboss-as/standalone/deployments/csa.war/offerings/config.json`

Install the patch

This section describes how to install the patch.

Check preinstallation requirements

Make sure you fulfill these prerequisites before installing:

1. Check minimum hardware requirements:
   - CPU: 4 CPU, 3.0 GHz
   - RAM: 8 GB
   - Hard Drive: 20 GB
2. Check the CSA 4.60 Support Matrix to verify operating-system requirements:
3. Check minimum software requirements:
   - CSA version 4.50.0000
4. **Windows:** Set the CSA_HOME environment variable to the following (remote MPP node):

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

   Linux: Set the CSA_HOME environment variable for the remote MPP node to the CSA folder default location:
   `/usr/local/hp/csa`
5. Back up your CSA environment.
6. Stop new subscription creation and subscription modification.

   Warning: If you do not stop creation and modification, the installation might fail and CSA might be left in an unstable state.

7. Stop the following CSA services: CSA Provider Console and Marketplace Portal, Search, Elasticsearch 1.5.2

   Important: You must stop these services on each node in a cluster.

Install the patch

Use the following procedure to install the patch in a standalone configuration or on *each* node of a cluster:

1. Download the CSA patch file:

   Linux:
   https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/LID/CSA_00033

   Windows:
   https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/LID/CSA_00034

2. For **Linux**:
   a. Extract the downloaded file: `HP_CSA_Patch_04.50.0003.bin` file from the patch tar file.
   b. Make sure that the `csauser` user is the owner, and has full privileges to, the `HP_CSA_Patch_04.50.0003.bin` file.
   c. Log in as `csauser` and run `HP_CSA_Patch_04.50.0003.bin` to open the CSA Patch Installer console mode.
   d. Enter `./HP_CSA_Patch_04.50.0003.bin` to run the patch installer.
   e. Select **Enter** in the introduction, warnings, and prerequisites screens.
   f. In the environment dialog screen, select **Standalone** or **Cluster** environment, then click **Enter**.
   g. In the set-up screen, select your set-up option:
      - CSA and MPP are installed
      - Only MPP is installed

      Note: If you select **Only MPP**, perform the same steps to install the patch, but ignore the configurations that are specific to JBoss and `csa.war`.
   h. Click **Enter**.
   i. Enter the CSA database password for the CSA user and click **Enter**.
   j. In the pre-installation summary dialog screen, click **Enter**.

      The patch installer begins the installation.
   k. When prompted, click **Enter** to exit the installation.

3. For **Windows**:
   a. Extract the `HP_CSA_Patch_04.50.0003.exe` file from the patch zip file.
   b. Run `HP_CSA_Patch_04.50.0003.exe` to launch the installation wizard.

c. Click **Next** to open the CSA Environment Selection wizard.

d. Select **Standalone** or **Cluster** environment, then click **Next**.

e. Select your set-up option:

- CSA and MPP are installed
- Only MPP is installed

  Note: If you select **Only MPP**, perform the same steps to install the patch, but ignore the configurations that are specific to JBoss and `csa.war`.

f. Enter the CSA database user password and click **Next**.

g. Click **Install** to run the patch installation.

h. When prompted, click **Done** to exit the installation.

Verify the installation

The verification steps apply to both standalone and clustered environments. For clustered environments, complete these steps on each node after completing the installation on each node.

1. Check for errors in the log files:

   Windows: `<CSA_HOME>\_CSA_4_50_3_installation\Logs`
   Linux: `$CSA_HOME/_CSA_4_50_3_installation/Logs`
   Log files include `csa_install.log`, `csa_InstallPatch.log`, `msvc_*.log`, `upgrade_idm.log`, and `upgrade_search_service.log`.

   Note: If there are errors, create a backup of the log files, restore the backup of the CSA_HOME directory, and contact HP Support.

2. Clear the browser cache.

3. Make sure the CSA, Marketplace Portal, HP Search, and Elasticsearch services are running:

   Windows: Installer automatically starts these services.

   Linux: Start the services manually. In a cluster environment, manually start the services on all nodes.

4. Launch the CSA Console, log in, and check for the updated version.

Windows Configurations

This section describes further configurations required for Windows.

Configuring Elasticsearch in Cluster Environments

Installing the patch on an HA cluster environment disables Elasticsearch. Use the steps in this section to re-enable Elasticsearch and also enable strictSSL support.

1. Follow the instructions in Chapter 7 of the *CSA 4.50 Configuration Guide* to enable Elasticsearch.
2. Replace the values of the following entries with the local node's fully qualified domain name (FQDN):

File Name	Entry
`csa.properties`	`csa.provider.msvc.hostname`
`csa-search-service/app.json`	`ccue-basic-server.host`
`csa-search-service/app.json`	`msvc-basic-search.searchEngineURL`

3. Complete the following certificate set-up steps for your environment:

Step	Directions

If the cluster setup is using the default CSA (self-signed) certificates:	Change the following settings to `false`:
	`csa-search-service/app.json msvc-basic-search.strictSSL/rejectUnauthorized: false`
	`elasticsearch/config/elasticsearch.yml searchguard.ssl.transport.http.enforce_clientauth: false`
	Note: These 2 settings do not need to be modified if the cluster runs valid certificates signed by a common CA.

Modify the following HA configurations in `csa-search-service/app.json`:	`idmURL` - point to the load balancer
	For example:
	`idmURL: https://http-loadbalancer.csapcoe.hp.com:8443/idm-service`
	Where `Port 8443` is the load-balancer port that you configured manually during the CSA 4.50 installation.
	`Cert` - point to the load-balancer cert
	For example:
	`ca: C:/Program Files/Hewlett-Packard/CSA/jboss-as/standalone/configuration/apache_csa.crt`
	Note: You *must* change the default `*.crt` file name (`jboss.crt`).

For more information on setting up certificates, see the following CSA 4.50 documents:

Document	Link to CSA 4.50 document on the SSO
FIPS 140-2 Compliance Statement	https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01691504
FIPS Compliance Configuration Guide	https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01702243

Configuring an CSA Linux Cluster for High Availability Using an Apache Web Server	https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01737522
Configuring an CSA Windows Cluster for High Availability Using an Apache Web Server	https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01737523

FIPS Compliance

Follow these steps if you manually reconfigured a CSA 4.50 installation to FIPS mode.

Important: If you have not reconfigured CSA to function in FIPS *before* installing this patch, do not follow the steps below. If you plan to reconfigure CSA to function in FIPS mode *after* installing this patch, use nodejs-fips-ssl1.0.2d-windows-0.10.33.zip from the patch zip instead of the patch on CSA 4.50 installation media.

The FIPS mode support matrix and configuration steps are documented in separate FIPS documentation.

Installing FIPS Compliant nodejs on standalone CSA servers or node js on clustered CSA servers

1. Back up the CSA environment.
2. Download the patch file.
3. Stop new subscription creation and subscription modification.

   Important: If you do not stop creation and modification, the uninstall might fail and CSA might be left in an unstable state.

   a. Sign out of all open instances of the CSA Provider Console and Marketplace Portal.

   b. Stop the following CSA services: CSA, Marketplace Portal, Search, and Elasticsearch 1.5.2.

   Note: For clustered CSA servers, stop the services on all nodes.
4. Extract `nodejs-fips-ssl1.0.2d-windows-0.10.33.zip` from the patch zip.
5. Extract files from `nodejs-fips-ssl1.0.2d-windows-0.10.33.zip` and place them in the `<CSA_HOME>\node.js` folder (`<CSA>/node.js` for clustered servers), replacing the existing files that are already in that folder.
6. Clear the browser cache.
7. Start the following services: CSA, Marketplace Portal, Search, and Elasticsearch 1.5.2.

   Note: For clustered CSA servers, start the services on all nodes.

Configure CSA with CAC for SAN

You can configure both the subjectDN and CAC for SAN (subjectAlternativeName) SAN x.509 attributes,

Configure CSA with CAC for SAN (SubjectAlternativeName)/SubjectDN based authentication

Before you configure CSA to support the attributes:

1. Make sure CAC is enabled. See the *CSA Configuration Guide* for more information.
2. Stop CSA, Marketplace Portal service, OO, and global search.

To configure the CSA console:

1. Back up the `csa.properties` file.
2. Modify the file:

Property Name	Modification
`csa.cac.x509Attribute`	Certificate user name. Allowed attributes: 1. `subjectDN` (default attribute) 2. `san` 3. `subjectDN`, `san` or `san`, `subjectDN` (both attributes) Syntax example: **`csa.cac.x509Attribute=san`** **Note:** If you set the property to both attributes, and the `san` attribute is not present in the certificate, CSA reports an authentication failure, and uses the default attribute (`subjectDN`).
`csa.cac.regex`	`subjectDN` X.509 attribute. Allowed attributes: CN=`(.*?)`, Syntax example: **#csa.cac.regex=CN=(.*?),** **Note:** Do not set this property if the `csa.cac.x509Attribute` is set to `san`.
`csa.cac.san.type`	Subject alternative name. Allowed types: `othername` and `rfc822name` **Note:** otherName only supports the OID for UPN (1.3.6.1.4.1.311.20.2.3). Syntax example: **csa.cac.san.type=otherName** Default: `othername` **Note:** Do not set this property if the `csa.cac.x509Attribute` is set to `subjectDN`.

3. Make a back-up copy of `$CSA_HOME\jboss-as\standalone\deployments\csa.war\WEB-INF\applicationContext-security.xml`.
4. Modify the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/applicationContext-security.xml` file:
   a. Uncomment the line highlighted in yellow, which occurs below this line:

      `<!-- Pre-authentication for CAC -->`:

```
    <!-- Pre-authentication for CAC -->
   <security:authentication-provider
ref="customX509AttrPreAuthAuthProvider"/>
```

   b. Remove both of these lines:

```
“x509 and custom filter config for CAC “
```

      And

```
<x509 subject-principal-regex="CN=(.*?)," user-
serviceref="cacUserDetailsService" />
```

c. Uncomment both occurrences of the following line.

```
<custom-filter position="LAST" ref="cacFilter" />
```

d. Uncomment the following line:

```
<custom-filter position="X509_FILTER"
ref="cacX509AuthenticationFilter" />
```

e. Locate the following lines.

```
<beans:bean id="cacUserDetailsService"
class="com.hp.csa.authn.impl.CACUserDetailsServiceImpl">
        <beans:property name="restRole" value="ROLE_REST" />
    </beans:bean>
    <beans:bean id="cacFilter"
class="com.hp.csa.security.CACFilter" />
```

Uncomment the content below these lines (see highlighted section below showing the uncommented lines):

```
<!--  Bean definitions for CAC -->
<beans:bean id="cacUserDetailsService"
class="com.hp.csa.authn.impl.CACUserDetailsServiceImpl">
        <beans:property name="restRole" value="ROLE_REST" />
    </beans:bean>
<beans:bean id="cacX509AuthenticationFilter"
class="org.springframework.security.web.authentication.preauth.x50
9.X509AuthenticationFilter">
              <beans:property name="authenticationManager"
ref="authenticationManager" />
              <beans:property name="principalExtractor"
ref="customX509Extractor" />
    </beans:bean>

   <beans:bean id="customX509AttrPreAuthAuthProvider"
class="org.springframework.security.web.authentication.preauth.Pre
AuthenticatedAuthenticationProvider">
        <beans:property name="preAuthenticatedUserDetailsService"
ref="customAuthenticationUserDetailsService" />
   </beans:bean>

   <beans:bean id="customAuthenticationUserDetailsService"
class="org.springframework.security.core.userdetails.UserDetailsBy
NameServiceWrapper">
        <beans:property name="userDetailsService"
ref="cacUserDetailsService" />
   </beans:bean>

   <beans:bean id="customX509Extractor"
class="com.hp.csa.security.CustomX509PrincipalExtractor">
        <beans:property name="x509Attribute"
value="${csa.cac.x509Attribute:subjectDN}"/>
        <beans:property name="regex"
value="${csa.cac.regex:CN=(.*?),}"/>
        <beans:property name="sanType"
value="${csa.cac.san.type:otherName}"/>
    </beans:bean>
```

f. Save the file.

Integrate the Marketplace Portal with CAC

To integrate the Marketplace Portal with CAC:

1. Back up `$CSA_HOME\jboss-as\standalone\deployments\idm-service.war\WEB-INF\spring\applicationContext.properties`.
2. Modify the file

Property Name	Modification
`idm.cac.x509Attribute`	Certificate user name. Allowed attributes: 1. `subjectDN` (default attribute) 2. san 3. subjectDN,san or san,subjectDN (both attributes) Syntax example: **csa.cac.x509Attribute=san** **Note:** If you set the property to both attributes, and the `san` attribute is not present in the certificate, the system uses the default attribute (`subjectDN`).
`idm.cac.regex`	`subjectDN` X.509 attribute. Allowed attributes: `CN=(.*?)`, Syntax example: **#csa.cac.regex=CN=(.*?),** **Note:** Do not set this property if the `csa.cac.x509Attribute` is set to `san`.
`idm.cac.san.type`	Subject alternative name. Allowed types: `othername` and `rfc822name` Syntax example: **csa.cac.san.type=otherName** Default: `otherName` **Note:** Do not set this property if the `csa.cac.x509Attribute` is set to `subjectDN`.

3. If SSO is configured for the Marketplace Portal, see *Configure Marketplace Portal for CAC authentication based on SAN when SSO is enabled*.
4. Make a back-up copy of `$CSA_HOME\jboss-as\standalone\deployments\idm-service.war\WEB-INF\spring\applicationContext-security.xml`.

5. Modify the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/applicationContext-security.xml` file:

   a. Uncomment the section `<!-- START Certificate Authentication Configuration -->` (or, if you are not using SSO, the `<!-- START without SSO support -->` section). For example:

```
<!-- START without SSO support -->
    <!--
    <security:http pattern="/idm/v0/login" use-expressions="true"
auto-config="false">
        <security:http-basic />
        <security:custom-filter ref="requestTokenCompositeFilter"
position="FIRST"/>
        <security:x509 subject-principal-regex="CN=(.*?)," user-
service-ref="cacUserDetailsService" />
        <security:custom-filter position="LAST" ref="cacFilter" />
    </security:http>

    <bean id="cacFilter"
class="com.hp.ccue.identity.filter.certificate.CertificateFilter">
        <property name="generateTokenUtil" ref="generateTokenUtil"
/>
        <property name="tokenFactory" ref="tokenFactory"/>
        <property name="loginRedirectionHandler"
ref="loginRedirectionHandler"/>
        <property name="authenticationProvider"
ref="cacLdapAuthProvider"/>
    </bean>-->
```

   b. Uncomment the content below this line: `<!-- START Certificate Authentication Configuration with subjectAlternativeName authentication --><!-- (without SSO support) -->`. For example:

```
    <!-- START Certificate Authentication Configuration with
subjectAlternativeName authentication -->
    <!-- (without SSO support) -->
    <security:http pattern="/idm/v0/login" use-expressions="true"
auto-config="false">
        <security:http-basic />
        <security:custom-filter ref="requestTokenCompositeFilter"
position="FIRST"/>
        <security:custom-filter position="LAST" ref="cacFilter" />
        <security:custom-filter position="X509_FILTER"
ref="cacX509AuthenticationFilter" />
    </security:http>

    <bean id="cacFilter"
class="com.hp.ccue.identity.filter.certificate.CertificateFilter">
        <property name="generateTokenUtil" ref="generateTokenUtil"
/>
        <property name="tokenFactory" ref="tokenFactory"/>
```

```
        <property name="loginRedirectionHandler"
ref="loginRedirectionHandler"/>
        <property name="authenticationProvider"
ref="cacLdapAuthProvider"/>
    </bean>
    <!-- END Certificate Authentication Configuration with
subjectAlternativeName authentication -->
```

c. Uncomment this section `<!-- START Certificate Authentication (beans) -->`. For example:

```
    <!-- START Certificate Authentication (beans) -->
    <bean id="cacX509AuthenticationFilter"
class="org.springframework.security.web.authentication.preauth.x50
9.X509AuthenticationFilter">
        <property name="authenticationManager" ref="authManager"
/>
        <property name="principalExtractor"
ref="customX509Extractor" />
    </bean>

   <bean id="customX509AttrPreAuthAuthProvider"
class="org.springframework.security.web.authentication.preauth.Pre
AuthenticatedAuthenticationProvider">
        <property name="preAuthenticatedUserDetailsService"
ref="customAuthenticationUserDetailsService" />
   </bean>

   <bean id="customAuthenticationUserDetailsService"
class="org.springframework.security.core.userdetails.UserDetailsBy
NameServiceWrapper">
        <property name="userDetailsService"
ref="cacUserDetailsService" />
   </bean>

   <bean id="customX509Extractor"
class="com.hp.ccue.identity.filter.certificate.CustomX509Principal
Extractor">
        <property name="x509Attribute"
value="${idm.cac.x509Attribute:subjectDN}" />
        <property name="regex" value="${idm.cac.regex:CN=(.*?),}"
/>
        <property name="sanType"
value="${idm.cac.san.type:OtherName}" />
        <property name="UPNResolver"
ref="userPrincipalNameResolver" />
    </bean>

    <bean id="userPrincipalNameResolver"
class="com.hp.ccue.identity.filter.certificate.CsaBouncyCastleUpnE
xtractor" />

   <!-- END Certificate Authentication (beans) -->
```

d. Uncomment the following line: `<!--Pre authentication provider for CAC with subjectAlternativeName authentication -->`. For example:

```
<!--Pre authentication provider for CAC with
subjectAlternativeName authentication -->
<security:authentication-provider
ref="customX509AttrPreAuthAuthProvider" />
```

6. Save the file and exit.

Configure the Marketplace Portal for CAC authentication based on SAN when SSO is enabled

To configure the Marketplace Portal:

1. Make a back-up copy of `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/ applicationContext-security.xml`.
2. In the file, add comment symbols for the content that comes after the lines `-- START Certificate Authentication Configuration -->` and `<!-- START with SSO support -->`, so that it appears as follows:

```
<!--
    <security:http pattern="/idm/v0/login" use-expressions="true"
auto-config="false">
        <security:http-basic />
        <security:custom-filter ref="hpssoProvidedFilter"
before="PRE_AUTH_FILTER" />
        <security:custom-filter ref="hpssoIntegrationFilter"
after="PRE_AUTH_FILTER" />
        <security:custom-filter ref="requestTokenCompositeFilter"
position="FIRST"/>
        <security:x509 subject-principal-regex="CN=(.*?)," user-
service-ref="cacUserDetailsService" />
        <security:custom-filter position="LAST" ref="cacFilter" />

    </security:http>

    <bean id="cacFilter"
class="com.hp.ccue.identity.filter.certificate.CertificateFilter">
        <property name="generateTokenUtil" ref="generateTokenUtil"
/>
        <property name="tokenFactory" ref="tokenFactory"/>
        <property name="tokenWriter" ref="hpssoTokenWriter" />
        <property name="loginRedirectionHandler"
ref="loginRedirectionHandler"/>
        <property name="authenticationProvider"
ref="cacLdapAuthProvider"/>
        <property name="auditAppender" ref="auditAppender"/>
    </bean>
-->
```

a. Uncomment the content below the line `<START Certificate Authentication Configuration with subjectAlternativeName authentication (with SSO support).` For example:

```
   <!-- START Certificate Authentication Configuration with
subjectAlternativeName authentication -->
    <!-- (with SSO support -->
    <security:http pattern="/idm/v0/login" use-expressions="true"
auto-config="false">
        <security:http-basic />
        <security:custom-filter ref="hpssoProvidedFilter"
before="PRE_AUTH_FILTER" />
        <security:custom-filter ref="hpssoIntegrationFilter"
after="PRE_AUTH_FILTER" />
        <security:custom-filter ref="requestTokenCompositeFilter"
position="FIRST"/>
        <security:custom-filter position="LAST" ref="cacFilter" />
        <security:custom-filter position="X509_FILTER"
ref="cacX509AuthenticationFilter" />
    </security:http>

    <bean id="cacFilter"
class="com.hp.ccue.identity.filter.certificate.CertificateFilter">
        <property name="generateTokenUtil" ref="generateTokenUtil"
/>
        <property name="tokenFactory" ref="tokenFactory"/>
        <property name="tokenWriter" ref="hpssoTokenWriter" />
        <property name="loginRedirectionHandler"
ref="loginRedirectionHandler"/>
        <property name="authenticationProvider"
ref="cacLdapAuthProvider"/>
        <property name="auditAppender" ref="auditAppender"/>
    </bean>

    <!-- END Certificate Authentication Configuration with
subjectAlternativeName authentication -->
```

b. Below the line `<!-- START Certificate Authentication (beans) -->`

uncomment the content:

```
    <!-- START Certificate Authentication (beans) -->
    <bean id="cacX509AuthenticationFilter"
class="org.springframework.security.web.authentication.preauth.x50
9.X509AuthenticationFilter">
        <property name="authenticationManager" ref="authManager"
/>
        <property name="principalExtractor"
ref="customX509Extractor" />
    </bean>

   <bean id="customX509AttrPreAuthAuthProvider"
class="org.springframework.security.web.authentication.preauth.Pre
AuthenticatedAuthenticationProvider">
```

```
        <property name="preAuthenticatedUserDetailsService"
ref="customAuthenticationUserDetailsService" />
   </bean>

   <bean id="customAuthenticationUserDetailsService"
class="org.springframework.security.core.userdetails.UserDetailsBy
NameServiceWrapper">
        <property name="userDetailsService"
ref="cacUserDetailsService" />
   </bean>

   <bean id="customX509Extractor"
class="com.hp.ccue.identity.filter.certificate.CustomX509Principal
Extractor">
        <property name="x509Attribute"
value="${idm.cac.x509Attribute:subjectDN}" />
        <property name="regex" value="${idm.cac.regex:CN=(.*?),}"
/>
        <property name="sanType"
value="${idm.cac.san.type:OtherName}" />
        <property name="UPNResolver"
ref="userPrincipalNameResolver" />
    </bean>

    <bean id="userPrincipalNameResolver"
class="com.hp.ccue.identity.filter.certificate.CsaBouncyCastleUpnE
xtractor" />

   <!-- END Certificate Authentication (beans) -->
```

e. Uncomment the line below `<!--Pre authentication provider for CAC with subjectAlternativeName authentication -->`:

```
<security:authentication-provider
ref="customX509AttrPreAuthAuthProvider" />
```

f. Within the `<!-- START Certificate Authentication Configuration -->` section, uncomment the content after the `START without SSO support` line. For example:

```
<!--
<security:http pattern="/idm/v0/login" use-expressions="true"
auto-config="false">
        <security:http-basic />
        <security:custom-filter ref="requestTokenCompositeFilter"
position="FIRST"/>
        <security:x509 subject-principal-regex="CN=(.*?)," user-
service-ref="cacUserDetailsService" />
        <security:custom-filter position="LAST" ref="cacFilter" />

    </security:http>

    <bean id="cacFilter"
class="com.hp.ccue.identity.filter.certificate.CertificateFilter">
```

```
        <property name="generateTokenUtil" ref="generateTokenUtil"
/>
        <property name="tokenFactory" ref="tokenFactory"/>
        <property name="loginRedirectionHandler"
ref="loginRedirectionHandler"/>
        <property name="authenticationProvider"
ref="cacLdapAuthProvider"/>
    </bean>
      -->
```

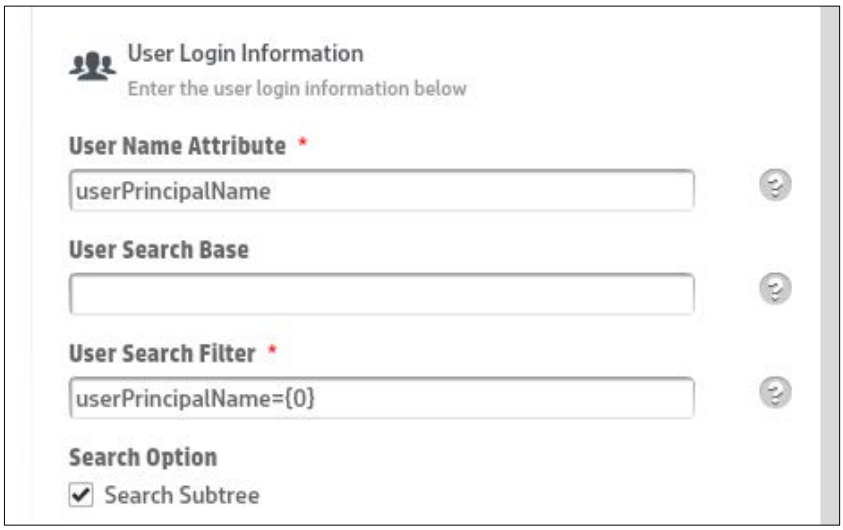
g. Save the file.

h. Restart CSA, the Marketplace Portal, Search, and Elasticsearch.

LDAP server configuration for CAC authentication based on UPN

In the LDAP server login information screen enter the following:

1. User Name Attribute: `userPrincipleName`.
2. User Search Filter: `userPrincipalName={0`
3. Choose the Search Option `Search Subtree`.



Note: If SSO is enabled for CAC authentication based on UPN on other products (such as OO), you must make these changes for those products too.

Linux - Uninstall the patch

This section explains how to prepare to uninstall, how to uninstall, and how to verify patch uninstall.
Note: Uninstallation of the patch will not revert the database-indexing changes made during patch installation.

Uninstall Preparation

To prepare for the uninstall:

1. Backup the CSA environment.
2. Stop new subscription creation and subscription modification.

   Warning: If you do not stop creation and modification, the uninstall might fail and CSA might be left in an unstable state.
3. Sign out of all open instances of the CSA Provider Console and Marketplace Portal.
4. Stop the following CSA services: CSA Provider Console and Marketplace Portal, HP search, and

   Elasticsearch 1.5.2

   Important: You must stop these services on each node in a cluster.

Uninstall the patch on standalone and cluster CSA servers

To uninstall the patch:

1. Navigate to `$CSA_HOME/_CSA_4_50_3_installation/Uninstaller`.
2. Run `./Uninstall HP Cloud Service Automation Patch` to start the uninstaller console mode.
3. Click **Enter** for the introductory and warning screens.
4. Click **Enter** to run the patch uninstaller.
5. Click **Enter** to exit the uninstall.

Windows – Uninstalling the patch

This section describes how to uninstall the patch in both standalone and clustered environments.

Uninstalling the patch on standalone and clustered environments

You can uninstall the patch in a standalone environment using either of the following methods:

- Using the Control Panel
- Using the Uninstall Cloud Service Automation Patch wizard

Note: Perform the steps on each node of the cluster after stopping the services on all nodes.
To uninstall the patch using the Control Panel:

1. In the Control Panel choose **Uninstall a program**.
2. Select **Cloud Service Automation Patch** and click **Uninstall**.
3. Follow the instructions on the uninstall wizard to uninstall the patch.

To uninstall the patch using the Uninstall Cloud Service Automation Patch wizard:

1. Navigate to `<CSA_HOME>\_CSA_4_50_3_installation\Uninstaller`.

2. Execute `Uninstall HP Cloud Service Automation Patch.exe` to open the Uninstall Cloud Service Automation Patch wizard.
3. Click **Uninstall** to uninstall the patch.
4. Click **Done** to exit the uninstall wizard.

Verify the uninstall

The verification steps apply to both standalone and clustered environments. For clustered environments, complete these steps on each node.

1. Check for errors in the log files:

   Windows: `<CSA_HOME>\_CSA_4_50_3_installation\Logs`
   Linux: `$CSA_HOME/_CSA_4_50_3_installation/Logs`
   Log files include `csa_install.log`, and `csa_InstallPatch.log`.
   Note: If there are errors, create a backup of the log files, restore the backup of the CSA_HOME directory, and contact HP Support.

2. Clear the browser cache.
3. Make sure the CSA, Marketplace Portal, HP Search, and Elasticsearch services are running:

   Windows: The installer automatically starts these services.
   Linux: Start the services manually. In a cluster environment, manually start the services on all nodes.

CSA modified files

```
<CSA_HOME>\jboss-as\standalone\deployments\csa.war\*
<CSA_HOME>\jboss-as\standalone\deployments\idm-service.war\*
<CSA_HOME>\portal\*
<CSA_HOME>\jboss-as\standalone\configuration\standalone.xml
<CSA_HOME>\jboss-as\standalone\configuration\standalone-full-ha.xml
<CSA_HOME>\jboss-
as\modules\system\layers\base\io\undertow\core\main\module.xml
<CSA_HOME>\jboss-
as\modules\system\layers\base\io\undertow\core\main\undertow-core-
1.1.0.Final.jar
<CSA_HOME>\jboss-
as\modules\system\layers\base\io\undertow\servlet\main\module.xml
<CSA_HOME>\jboss-
as\modules\system\layers\base\io\undertow\servlet\main\undertow-
servlet-1.1.0.Final.jar
<CSA_HOME>\jboss-
as\modules\system\layers\base\io\undertow\websocket\main\module.xml
<CSA_HOME>\jboss-
as\modules\system\layers\base\io\undertow\websocket\main\undertow-
websockets-jsr-1.1.0.Final.jar
<CSA_HOME>\jboss-
as\modules\system\layers\base\org\apache\commons\collections\main\com
mons-collections-3.2.1.jar
```

```
<CSA_HOME>\jboss-
as\modules\system\layers\base\org\apache\commons\collections\main\mod
ule.xml
<CSA_HOME>\elasticsearch-1.5.2\config\*
<CSA_HOME>\openjre\*
<CSA_HOME>\CSAKit-4.5\OO Flow Content\10X\EXISTING-INFRASTRUCTURE-
WINDOWS-cp-1.50.0000.jar
<CSA_HOME>\CSAKit-4.5\OO Flow Content\10X\oo10-csa-cp-4.50.0000.jar
<CSA_HOME>\CSAKit-4.5\OO Flow Content\10X\oo10-csa-integrations-cp-
4.50.0000.jar
<CSA_HOME>\CSAKit-4.5\OO Flow Content\10X\oo10.50-csa-integrations-
cp-4.50.0001.jar
<CSA_HOME>\CSAKit-4.5\OO Flow Content\9X\CSA-4_10-
ContentInstaller.jar
<CSA_HOME>\Tools\ComponentTool\*
<CSA_HOME>\Tools\ContentArchiveTool\CODAR_BP_EXISTING_WINDOWS_SERVER_
COMPONENT_v1.50.00.zip
<CSA_HOME>\Tools\ContentArchiveTool\content-archive-tool.jar
<CSA_HOME>\Tools\DBPurgeTool\db-purge-tool.jar
<CSA_HOME>\Tools\PasswordUtil\passwordUtil-standalone.jar
<CSA_HOME>\Tools\ProcessDefinitionTool\process-defn-tool.jar
<CSA_HOME>\Tools\ProviderTool\provider-tool.jar
<CSA_HOME>\Tools\SchemaInstallationTool\*
<CSA_HOME>\Tools\SupportTool\support-tool.jar
```

Errata

In the *CSA Cluster Configuration using Apache Server* white paper, make the following changes to the section that discusses generating the certificate and private key:

Replace the following text in yellow highlight:

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

With this text in yellow highlight:

```
  "<path_to>\Apache2.2\openssl" req -x509 -days 365 –sha256 -
newkey rsa:2048 -nodes
  -keyout <path_to>\Apache2.2\conf\apache_csa.key
  -out <path_to>\Apache2.2\conf\apache_csa.crt
  -config <path_to>\Apache2.2\conf\openssl.cnf
  -subj /O=HP/OU=HP/CN=[APACHE_LOAD_BALANCER_HOSTNAME]”
```

Send documentation feedback

If you have comments about this document, you can send them to clouddocs@hpe.com.

Legal notices

Warranty

The only warranties for Hewlett Packard 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. Hewlett Packard 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 Hewlett Packard required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright notice

Trademark notices

Adobe® is a trademark of Adobe Systems Incorporated.
Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.
Oracle and Java are registered trademarks of Oracle and/or its affiliates.
UNIX® is a registered trademark of The Open Group.
RED HAT READY™ Logo and RED HAT CERTIFIED PARTNER™ Logo are trademarks of Red Hat, Inc.
The OpenStack word mark and the Square O Design, together or apart, are trademarks or registered trademarks of OpenStack Foundation in the United States and other countries, and are used with the OpenStack Foundation's permission.

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 HP Software Support and sign-in or register.
Select Manuals from the Dashboard menu to view all available documentation. Use the search and filter functions to find documentation, whitepapers, and other information sources.
You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your Hewlett Packard sales representative for details.

Support

For product support, go to HP Software Support online support.