HP Cloud Service Automation

Release Notes

This document provides an overview of the changes made to HP Cloud Service Automation (HP CSA) for the 4.01 release. It contains important information not included in the manuals or in online help.

In This Version

HP Cloud Service Automation (HP CSA) provides software to integrate specific HP products for the purpose of delivering and managing automated services in a cloud computing environment. For more information about integrated products, see the *HP Cloud Service Automation Solution and Software Support Matrix*.

To ensure the performance and stability of the HP Cloud Service Automation environment, complete the following tasks before installation begins:

- Review supported hardware and software for each component product in order to meet the minimum installation requirements.

- Make sure the relevant patches and hot fixes to the patch releases are applied to the component products.

- Review the release notes for each component product to be aware of additional changes or restrictions.

Installation Requirements

Installation requirements are documented in the *HP Software Cloud Service Automation Solution and Software Support Matrix.*

Documentation

HP CSA documentation is located on HP Software Product Manuals website.

Contents

Installation Notes

Backing up the HP CSA 4.00 Installation
Follow these instructions before completing the steps in the *HP Cloud Service Automation Upgrade Guide*.

I. Back up the HP CSA 4.00 database.

Before installing CSA 4.01, please make a backup copy of CSA 4.0 database. This backup is necessary to restore the database to a known HP CSA 4.00 state in case of the necessity to roll back the HP CSA 4.01 installation.

II. Back up the HP CSA 4.00 installation.

Before installing HP CSA 4.01, stop the HP Cloud Service Automation service (this service is called 'csa' on Linux systems) and HP Marketplace Portal service (this service is called 'mpp' on Linux systems). Make a backup copy of the entire HP CSA 4.00 installation directory. This backup copy is necessary in case of the necessity to roll back the HP CSA 4.01 installation. If you have high availability (HA) installations in your environment, do the previous steps for all HA nodes.

Note: If HP CSA is installed on a virtual machine, a snapshot of the virtual machine should be taken and labeled 'CSA 4.0' before continuing with the HP CSA 4.01 installation. You can revert back to this snapshot in case of the necessity to roll back the HP CSA 4.01 installation.

III. Complete the steps in the *HP Cloud Service Automation Upgrade Guide*.

Rolling Back to the HP CSA 4.00 Installation
If it is necessary to roll back the HP CSA 4.01 installation to HP CSA 4.00, perform the following steps.

1. Restore the database from the backup of the CSA 4.00 database.
2. Uninstall HP CSA 4.01. This will remove the HP CSA installation entirely from the system.
3. After the successful uninstallation of HP CSA 4.01, install HP CSA 4.00.
    a. When installing HP CSA 4.00, select the database that has been restored in the steps above.
    b. Select **'no'** when prompted for the installation of database components.
4. After HP CSA 4.00 is installed, stop the HP Cloud Service Automation service (this service is called 'csa' on Linux systems) and the HP Marketplace Portal service (this service is called 'mpp' on Linux systems). Restore the following from the backup copy of the HP CSA 4.00 file system (taken prior to installing CSA 4.01):
    a. Any configuration files related to running command line tools, such as the Process Definition Tool, Content Archive Tool, DB Purge Tool, Provider Tool, and Configuration Tool. All these tools are present in the `<CSAInstallDir>/Tools` folder.
    b. `<CSAInstallDir>/jboss-as-7.1.1.Final/standalone/deployments/csa.war/images`
    c. `<CSAInstallDir>/jboss-as-7.1.1.Final/standalone/deployments/csa.war/propertysources`
    d. CSA trust store where certificates such as OO certificates were imported into. Usually this is `<JreForCSA>/lib/security/cacerts` file.
    e. Any FIPs and CAC configuration related files. Please follow the instructions from the 4.00 version of the *HP Cloud Service Automation Configuration Guide* regarding the files used for FIPs and CAC configuration.
5. Start the HP Cloud Service Automation and HP Marketplace Portal services.
6. If you have high availability (HA) installations in your environment, do the previous steps for all HA nodes.

Note: If HP CSA is installed on a virtual machine, restoring the virtual machine to the 'CSA 4.0' snapshot taken before CSA 4.01 installation will avoid steps 2-4 above.

Please contact [HP Software support](#) if you have questions about the roll back to HP CSA 4.00.

Fixes in this Release

HP Cloud Service Automation (HP CSA)

General

Attached documents of imported service offerings do not appear in the Marketplace Portal and Cloud Service Management Console

QCCR1D178143

Problem

When a service offering exported from HP CSA 3.20 is imported into HP CSA 4.00, any documents attached to the service offering will not be shown in the Marketplace Portal. The document names are also empty when viewed in the Cloud Service Management Console.

Cloud Service Management Console

Resource provider that was a candidate for resource utilization cannot be deleted

QCCR1D177145

Problem

If a resource provider was a candidate resource provider during provisioning of a sequenced design when the Build Resource Provider List or Build Resource Provider and Pool List actions were run, the resource provider cannot be deleted, even if the provider was not selected by the Select Resource Provider or Select Resource Provider and Pool actions.

Marketplace Portal does not display the cost of invisible options during checkout

QCCR1D177308

Problem

The Marketplace Portal does not display the cost of hidden options during checkout, but does account for them in the pricing summary. If subscribers add together the base price plus the prices for their selected options, it may not add up to the total price.

Error occurs when adding multiple documents or screenshots to a service offering

QCCR1D177456

Problem

If you try to add multiple documents or screenshots to a service offering in the Cloud Service Management Console using Internet Explorer 9 you can get the following error:

```
com.hp.ccue.consumption.svc.svc-exception$exception.svc.required.missing
```

Two CSA Internal process engines may be displayed when adding a lifecycle action

QCCR1D177579

Problem

When adding a lifecycle action in the Cloud Service Management Console, two process engines named 'CSA Internal' may be displayed.

Tag display name and/or description does not persist when using Internet Explorer

QCCR1D178165

Problem

When editing the **Display Name** or **Description** for a Tag in the Cloud Service Management Console using Internet Explorer, the **Display Name** and **Description** updates may not be persisted correctly when clicking **Save**. In particular, if you click in the **Display Name** or **Description** fields (rather than using the Tab key), and then type in a value and click **Save**, the updated value may not be persisted.

Fixes in this Release

Marketplace Portal

Errors in csa.log when Marketplace Portal loads dynamic values for topology design public actions

QCCR1D176876

Problem

When the dialog for the **Assign Floating IP Address** public action is displayed in the Marketplace Portal for services created from HP Cloud OS topology designs, errors will be written to the csa.log. For example:

```
ERROR  ActionParameterServiceImpl : Fetching dynamic values failed
java.lang.IllegalStateException: Expanded url
'http://10.10.10.10:21051/1/resource_pool_list/65/network_list/${network_ref}/floating_ip_list'
contains not expanded placeholders '[network_ref]'
```

Marketplace Portal service detail view does not show Volume Type correctly for services with Volume Group(s)

QCCR1D177646

Problem

The Marketplace Portal service detail view does not show **Volume Type** correctly for services with Volume Group(s) present. The internal HP Cloud OS id of the **Volume Type** is shown instead of a human readable name.

Cancel All shows a failure in Marketplace Portal

QCCR1D177900

Problem

When a Marketplace Portal user issues a **Cancel All** request, or when multiple HP Cloud OS-based subscriptions are otherwise canceled at the same time, some of the subscriptions may incorrectly show a status indicating that the cancel failed.

After "Access is Denied" message, clicking on **Return to Dashboard** takes you to the CSA Consumer login page

QCCR1D178075

Problem

If a user logs into the Marketplace Portal for an organization other than CSA Consumer organization and that user does not belong to the Service Consumer role for that organization, the user will see an "Access is Denied" page. If they click the **Return to Dashboard** button on that page, it will take them to the login page for the CSA Consumer organization, not the login page for the originally specified organization.

Subscription **End Date** is displayed as one day after the **Start Date**

QCCR1D178176

Problem

Recurring subscriptions created in the Marketplace Portal will display an **End Date** of one day after the **Start Date** when a user modifies the subscription. This can cause confusion for a subscriber, who may believe their subscription has expired.

Note that when upgrading from HP CSA 3.20 to CSA 4.00, subscriptions that had no end date configured in the 3.20 Cloud Subscriber Portal will become recurring subscriptions in the Marketplace Portal and exhibit the same behavior on subscription modification as discussed above.

Subscription end dates provided for selection are in the past

QCCR1D178181

Problem

When changing from a recurring subscription to a term subscription in the Marketplace Portal, it is possible the dates available for selection for the **End Date** are partially (or completely) in the past. The allowed values for **End Date** will depend on the **Start Date** for the subscription and the **Subscription End Date Period (months)** configured for the consumer organization in the Cloud Service Management Console's Organizations area.

Fixes in this Release

This issue will most commonly be encountered for subscriptions created in a prior version of CSA that was then upgraded to 4.0.

User cannot log in to Marketplace Portal after login screen token expires

QCCR1D 174988

Problem

If a Marketplace Portal user navigates to the login page, waits for a long duration, and then attempts to log in, the login will fail and a message will be displayed about an expired token. At that point, the user will be unable to refresh or otherwise navigate from the login page in order to obtain a new token.

HP CSA APIs

REST API login to a consumer organization returns large amount of data

QCCR178125

Problem

The data returned from a REST API login to a consumer organization (for example, `https://<csa_host>:8444/csa/rest/login/CSA_CONSUMER/consumer`) includes data for all Marketplace Portal dashboard widgets configured for the organization, increasing the size of the response and the total time for the request to complete.

Integrations with HP CSA

HP Cloud OS

After HP CSA is restarted, no topology designs can be created or provisioned using an SSL enabled HP Cloud OS resource provider

QCCR1D178194

Problem

If you configure an HP Cloud OS resource provider in the Resources area of the Cloud Service Management Console, and if that HP Cloud OS resource provider uses an HTTPS service access point, the provider validation will be successful, and you will be able to create topology based designs using that provider and you will be able to provision services using that provider. However, if the SSL certificate used by that Cloud OS resource provider is not trusted by HP CSA (that is, none of the signing certificates is trusted by a certificate in the cacerts truststore of the JRE used by HP CSA), and HP CSA is restarted, errors will be written to the log and no new topology designs can be created or provisioned using that provider.

Known Problems, Limitations and Workarounds

HP Cloud Service Automation (HP CSA)

General

In FIPS mode, HP CSA fails to start with NoSuchAlgorithmException in the log file
QCCR1D163384
Problem
Oracle JDBC Thin Driver (`ojdbc6.jar`) fails to connect to Oracle in SSL mode when a different crypto provider is specified in the `java.security` file.
Cause
Oracle JDBC Thin Driver (`ojdbc6.jar`) does not support SSL mode when a different crypto provider is specified in the `java.security` file. Detailed information can be found on the Oracle support site

(`https://support.oracle.com/`) where we raised a Sev2 service request for this issue. The SR number is Oracle.SR 3-6995008521.
Workaround
No workaround is available. The solution will be available once Oracle implements Enhancement Request (ER) 16794055 for their Oracle Thin JDBC driver. (For details please check SR 3-6995008521 at Oracle support home: `https://support.oracle.com/`).

In topology designs, a shared Volume Group is attached to only one Server Group after provisioning
QCCR1D176960
Problem
When a service instance is provisioned for a topology design that contains multiple Server Groups connected to a single Volume Group, the Volume Group will be attached to only one of the Server Groups after provisioning.
Cause
Product limitation
Workaround
Assign each Volume Group to a single, unique Server Group.

Problems in Cloud Service Management Console and Marketplace Portal after restarting CSA database
QCCR1D147907
Problem
Various problems occur in the Cloud Service Management Console and Marketplace Portal if the CSA database is restarted while the CSA service is still running**.** For example, the Marketplace Portal may display Service Unavailable error messages when attempting to log in well after th**e** database has been restarted. After successfully logging in, error messages may be displayed when navigating around the Marketplace Portal. The Management Console similarly will prevent login for a period after the database has been restarted and later display errors when navigating (such as 500 errors). The Management Console also may prevent subsequent logins after a logout.
Cause
A restart of the CSA database is not gracefully handled in the product.
Workaround
Restart the CSA service.

"Webpage not available" message displays when logging into Cloud Service Management Console or Marketplace Portal in a CAC-enabled environment
QCCR1D177398
Problem
When attempting to login to the Cloud Service Management Console or Marketplace Portal in a CAC-enabled environment, the user may be presented with a "Webpage not available" message This can occur if the card is not placed in the card reader but the associated certificates are already available in the browser. In such a scenario, the user will be prompted to insert the card and provide the PIN. After doing so, the UI should load, but the user may instead receive "Webpage not available."

Cause
This problem can occur if multiple browsers are concurrently attempting to access the Cloud Service Management Console or Marketplace Portal, which may result in timeouts because of multiple SSL connections.
Workaround
Reloading the browser page may resolve the issue; if not, locate running instances of the browser (In Task Manager, or similar), kill the browser processes, open a new browser, and try again to access the Cloud Service Management Console or Marketplace Portal.

Subscription requests involving the following flow fail: `Update SA Server Id on CSA OO`
QCCR1D177545
Problem
The `Update SA Server Id on CSA` OO flow, when run on HP OO 10.x, completes successfully, but HP CSA occasionally does not learn of its successful completion. This causes actions that call the flow to timeout after 1 hour, and subscription requests that involve this action to fail. The service design `VCENTER_COMPUTE_SA_SOFTWARE_POLICIES_3.20`, as well as any service design involving HP ADM or HP DMA, are susceptible to this problem.
Cause
Unknown. This issue is observed intermittently.
Workaround
No workaround is available.

Configuration of out-of-the-box users have been moved to the Identity Management component in HP CSA 4.01
QCCR1D182209
Problem
In the HP CSA Configuration Guide (4.00), the out-of-the-box users admin, csaReportingUser, cdaInboundUser, and ooInboundUser are shown to be configured in `applicationContext-security.xml` and `csa.properties`.
Cause
Out-of-the-Box users admin, csaReportingUser, cdaInboundUser, and ooInboundUser are configured in the Identity Management component in HP CSA 4.01.
Workaround
Configure these users in the `<CSA_HOME>\jboss-as-7.1.1.Final\standalone\deployments\idm-service.war\WEB-INF\classes\csa-provider-users.properties` file.

To disable the admin user:

Note: This property not only determines if the account is enabled, it also contains the password and the roles that control access to HP CSA. By default, the unencrypted value of the admin property is cloud,ROLE_REST,enabled

Edit the `<CSA_HOME>\jboss-as-7.1.1.Final\standalone\deployments\idm-service.war\WEB-INF\classes\csa-provider-users.properties` file.

Update the admin property to disable this user account. For example, set admin to the following value (this value should be encrypted): cloud,ROLE_REST,disabled

The csaReportingUser, cdaInboundUser, and ooInboundUser users should not be disabled.

To update the passwords:

Note: This property not only contains the password, but also the roles that control access to HP CSA and if the account is enabled. By default, the unencrypted value of each user is:

admin = cloud,ROLE_REST,enabled
csaReportingUser = cloud,ROLE_REST,ROLE_DYNAMIC,enabled
cdaInboundUser = CDA2CSAIntegration!,ROLE_REST,enabled
ooInboundUser = cloud,ROLE_REST,enabled

Edit the `<CSA_HOME>\jboss-as-7.1.1.Final\standalone\deployments\idm-service.war\WEB-INF\classes\csa-provider-users.properties` file and update the value of the desired property. Encrypt the entire value of the out-of-the-box user property, including the roles and account status.

The password for the cdaInboundUser shown in the HP CSA Configuration Guide (4.00) is incorrect

QCCR1D182210

Problem

The password for the cdaInboundUser in the HP CSA Configuration Guide (4.00) is listed as cloud.

Cause

The password was changed.

Workaround

The password is CDA2CSAIntegration!.

Installation, Initial Configuration, Upgrade, and Uninstallation

Cannot rename `setup.exe`

QCCR1D142364

Problem

HP CSA installer silently exits on Windows® prior to installing HP CSA when the install filename is not `setup.exe`.

Cause

Known InstallAnywhere defect in the version of InstallAnywhere used with HP CSA.

Workaround

Ensure the HP CSA Windows installer program is named `setup.exe` prior to invoking it. Note that certain browsers may automatically rename a file if a naming conflict exists, for example to `'setup (1).exe'`. The HP CSA installer must be renamed back to `setup.exe` prior to its invocation.

Uninstall process does not remove installation directory

QCCR1D174113

Problem

After uninstalling HP CSA on a Windows machine, the `<CSA_HOME>\_CSA_4_0_0_installation` directory may remain. This problem occurs when an Oracle JRE was selected during the HP CSA installation process.

Cause

Installation defect.

Workaround

Following uninstallation, manually delete any remaining folders in the `<CSA_HOME>` directory.

An upgrade to HP CSA 4.01 installed in a non-default location on Linux throws an exception

QCCR1D181314

Problem

When HP CSA 4.00 on Linux is installed in a non-default location, running the upgrade installer for HP CSA 4.01 results in the following exception:

```
1. java.io.FileNotFoundException: /usr/local/hp/csa/jboss-as-7.1.1.Final/bin/standalone.conf
(No such file or directory) at java.io.FileInputStream.open(Native Method)
```

Cause

The upgrade installer is using the default installation path for HP CSA on Linux even though HP CSA is installed in a non-default location. Therefore, the upgrade installer is not able to locate the `standalone.conf` file.

Workaround

The exception can be safely ignored. The location of the `standalone.conf` file is not needed to upgrade to HP CSA 4.01. The upgrade will complete successfully.

Known Problems, Limitations and Workarounds

Upgrade in a Linux environment fails if there is a mounted file system within the HP CSA installation

QCCR1D181403

Problem

If a file system is mounted within the HP CSA installation directory (for example, within $CSA_HOME) in a Linux environment, the upgrade will fail if the file system is not unmounted before the upgrade installer is run.

Cause

The upgrade will fail because the upgrade installer cannot remove the mounted file system during the upgrade.

Workaround

If you mounted a file system within the HP CSA installation directory (for example, within $CSA_HOME) in a Linux environment, you must unmount the file system before running the upgrade installer. After the upgrade installer has completed, remount the file system.

For instructions on how to upgrade to HP CSA 4.01, refer to the *HP CSA 4.01 Upgrade Guide*.

Upgrade fails if there is a file open from within the HP CSA installation

QCCR1D181588

Problem

If an HP CSA file is open during the upgrade, the upgrade will fail.

Cause

The upgrade will fail because the upgrade installer cannot remove the file that is open by another process.

Workaround

Before running the upgrade installer, do the following:

1   Back up HP CSA outside of `<CSA_HOME>`, the database, and the registry file (Windows: `C:\Program Files\Zero G Registry\com.zerog.registry.xml`; Linux: `/home/csauser/com.zerog.registry.xml` or `/var/com.zerog.registry.xml`).

2   Close all command prompts and exit all programs that are running on the system.

For instructions on how to upgrade to HP CSA 4.01, refer to the *HP CSA 4.01 Upgrade Guide*.

Linux installer accepts invalid responses for the installing the database components query

QCCR1D181784

Problem

When HP CSA 4.0x on Linux is installed, any non-standard response (a response that is not a "yes" or "no") to the `Do you want to install database components? (yes/no)` question is accepted. Any response that is not "yes" or "YES" is interpreted as a negative response and the database components are not installed.

Cause

The installer does not validate the response to this question.

Workaround

If the database components must be installed, carefully enter either "yes" or "YES" to the question `Do you want to install database components? (yes/no)` when running the installer on a Linux system.

Cloud Service Management Console

A blank page may display in Chrome

QCCR1D155822

Problem

A blank page may be displayed in certain areas of the Cloud Service Management Console in Chrome.

Cause

An issue exists with some versions of Flash Player bundled with Chrome.

Workaround

Type `chrome://plugins` into the URL field of Chrome. Click **Details** to display more information about each plugin. Multiple entries may exist under the Flash heading. Look for an entry for Chrome's Flash Player, which may include a path similar to `AppData\Local\Google\Chrome` in the **Location** field. Click **Disable** for this plugin.

Known Problems, Limitations and Workarounds

Download the latest Flash Player from

`http://download.macromedia.com/pub/flashplayer/current/support/install_flash_player.exe`

After installation, restart Chrome and type `chrome://plugins` into the URL field. Validate that Chrome's Flash Player is disabled and that the newly installed Flash Player is enabled.

In Chrome, the SWF contents of certain Management Console areas reload on every user navigation to the area

QCCR1D148227

Problem

When accessing the Cloud Service Management Console in Chrome, areas that involve a SWF file (including Organizations, Catalogs, Resources, and portions of Designs and Components) reload on every user navigation to the area.

Cause

Chrome will reload an SWF from an HTTPS web site if the SSL certificate configured for that site is not trusted by the browser.

Workaround

Configure a CA-signed certificate for use with HP CSA, as described in the HP CSA Installation and Configuration guides.

Problems logging into Cloud Service Management Console in multiple browser tabs

QCCR1D147470

Problem

Various problems can occur when a user logs in with different user credentials to the Cloud Service Management Console in multiple browser tabs.

If you log in as different HP CSA users in multiple tabs, the last user logged in determines the access rights of all currently open browser tabs. This can result in error messages being displayed when a user attempts to perform an action that the last logged in user does not have rights to perform.

Cause

Improper handling of multiple tabs.

Workaround

Use only one browser tab at a time to log in to the Cloud Service Management Console. If multiple tabs are used, ensure that the same user is logged in to each tab. To switch which user is logged in, first log out and then log back in as the different user.

Communication error in Firefox when "Use System Proxy Settings" is configured

QCCR1D143336

Problem

In certain network environments, you may receive a communication error in Firefox immediately after you log in to the Cloud Service Management Console. This is different from the normal and expected communication error that occurs when the Cloud Service Automation service is not running or is inaccessible.

Cause

In certain network environments, Firefox is unable to communicate with the Cloud Service Automation service when **Use System Proxy Settings** is configured.

Workaround

Configure Firefox network settings to use a method other than **Use System Proxy Settings**. For example, configure Firefox to use either a manual or automatic proxy configuration. In Firefox 14, these settings are configured in **Tools→ Options→ Advanced→Network→Settings**.

Performance is poor with update in place import process when large amounts of transactional data (Subscriptions) exist in the database

QCCR1D165072

Problem

Import (with the in place update option) for Service Offerings, Designs and Catalogs can have high response time if there are large amounts of transactional data (Subscriptions) in the database.

Cause

Large amounts of transactional data slow performance.

Workaround

Run the import updates during periods of low loads on the system to reduce the performance impact.

Cloud Service Management Console does not display or function properly when IE Enhanced Security Configuration (ESC) is enabled

QCCR1D165813

Problem

When viewing the Cloud Service Management Console in Internet Explorer on a system in which IE Enhanced Security Configuration is enabled, the Management Console may not display or function properly. In Internet Explorer 10 or 11, you may be presented with a blank screen when accessing the Management Console. In Internet Explorer 9, export functionality may not work properly.

Cause

IE Enhanced Security Configuration interferes with proper display of the Cloud Service Management Console.

Workaround

To access the Cloud Service Management Console using IE on a system in which IE Enhanced Security Configuration is enabled, select from one of the following options:

- Option 1: Add HP CSA as a Trusted site (in IE, select **Internet Options → Security → Trusted sites→ Sites**, and add `https://<csa_hostname>`).

- Option 2: Add HP CSA as a site in the Local intranet zone (in IE, select **Internet Options → Security → Local intranet → Sites**, and add `https://<csa_hostname>`).

- Option 3: Disable IE ESC (in Server Manager on Windows®, disable IE ESC).

Invalid URL values in Service Designer may be allowed

QCCR1D165628

Problem

Service Designer in the Cloud Service Management Console allows for validation of URL values when creating properties in an option model. However, the regular expression used for validating the URL values may allow creating some invalid URL values such as `'http:'`, `'http:/'`, `'http://'` or `'hhh:////'`

Cause

The regular expression that HP CSA uses to validate URL values validates a wide range of official IANA-registered schemes, which may not detect some invalid URL values.

Workaround

For more specific URL validation, create custom regular expressions from the Service Designer in the Cloud Service Management Console.

Add document to Service Offering does not open system find file dialog

QCCR1D176520

Problem

Trying to attach a document to a service offering (in the **Documents** tab of the Offerings area of the Cloud Service Management Console) is unsuccessful when using Firefox version 20.

Cause

This functionality does not work correctly in this version of Firefox.

Workaround

Please update to a later version of Firefox or use one of the other HP CSA supported browsers.

Changes to a topology design after a service offering is created do not get synchronized back to the offering

QCCR1D174068

Problem

Certain changes made to a topology design after a service offering is created from the design can result in inconsistencies between the two and lead to display errors in the Cloud Service Management Console as well as possible provisioning errors.

Cause

When a service offering is created from a topology design, certain aspects of the design, including the profiles and modifiable properties, are copied to the offering. Changes to these items (such as adding or removing profiles, or changing whether a property is modifiable) in the design after a service offering is created are not synchronized to existing service offerings.

Workaround

Avoid making changes to the profiles or modifiable properties in a topology design after a service offering has been created for the design. If such changes are required, first copy the design and make modifications to the copy.

Create new router option in a topology design causes provisioning to fail

QCCR1D176038

Problem

Topology designs with connected Network Segment and Router components that are configured to use an existing subnet but create a new router cannot be provisioned more than once.

Cause

Cloud OS does not support creating more than one router on a subnet

Workaround

Avoid reusing an existing subnet on a Network Segment in combination with the **Create new router** option on a Router in a topology design. Instead, use the **Create new subnet** option on the Network Segment in conjunction with the **Create new router** option.

Topology Designer does not provide option to configure action timeout

QCCR1D176668

Problem

The timeout for communicating with HP Cloud OS to provision a topology based subscription is set to sixty (60) minutes and cannot be changed. This is in contrast to actions for sequenced based designs, where each action has a configurable timeout.

Cause

Product limitation.

Workaround

No workaround is available.

Ubuntu browsers have trouble displaying non-English characters in some areas of the Cloud Service Management Console

QCCR1D177819

Problem

Certain areas of the Cloud Service Management Console may not display correctly in non-English locales with browsers running on Ubuntu.

Cause

Issue with non-English characters in Flash content on Ubuntu systems.

Workaround

Use a browser on a system other than Ubuntu, such as Windows.

Problems with duplicate Security Groups in topology designs

QCCR1D178056

Problem

When creating topology designs in the Cloud Service Management Console that contain a Network Segment and Server Group and a connection between the two, the designer is prompted to select a Security Group for the 'Network Interface to' connection. The values contained in the Security Group dropdown may contain duplicate entries for existing security groups if an identically named security group is present in multiple projects in Cloud OS. When trying to select one of these duplicate security groups, it is not possible to know which Cloud OS project the security group is associated with. If one selects a security group for a different project than the Cloud OS resource provider in HP CSA has been configured for (via the tenant property on the resource provider), deployment of the service will fail.

In addition, the Marketplace Portal allows selection of a security group in the Add Security Group public action. The Marketplace Portal will filter out duplicate security groups, but may filter out the incorrect duplicate (one for a different

project/tenant than the Cloud OS resource provider in CSA has been configured for). If a subscriber selects a security group for a different project/tenant than the Cloud OS resource provider in CSA has been configured for, the Add Security Group action will fail.

Cause

The list of security groups returned from Cloud OS includes all security groups for all projects in Cloud OS, instead of just the security groups applicable to the project the Cloud OS resource provider in CSA has been configured for. This list is not filtered by project in the Cloud Service Management Console or Marketplace Portal.

Workaround

Avoid using the security group named **default** in the topology designer of the Cloud Service Management Console and in the **Add Security Group** action in the Marketplace Portal. When creating security groups in Cloud OS, name security groups in a manner that avoids duplicates across other Cloud OS projects. Only select security groups known to exist in the appropriate Cloud OS project when setting the **Network Interface to** value in the Management Console and when specifying a security group in the **Add Security Group** action in the Marketplace Portal.

Cannot manage approval actions in the Catalogs area of the Cloud Service Management Console

QCCR1D178174

Problem

When publishing a service offering in the Cloud Service Management Console there are different levels of approval configuration in the Offerings area and the Catalogs area. In the Offerings area you can configure which actions, of **Order**, **Modify**, and **Cancel**, will require approval (if approval is configured). In the Catalogs area, this configuration is not available, and all offerings published from the Catalogs area, with approvals configured, will require approval for **Order** and **Modify** but not **Cancel**. In addition, in the Offerings area you can configure which public actions in the associated design require approval; this configuration is not available in the Catalogs area, and any public actions in a published offering from the Catalogs area will not require approval. The collection of actions that were selected for approval when publishing from the Offerings area are not visible or editable in the Catalogs area.

Cause

Product limitation.

Workaround

If you wish to override the default approval behavior (so that **Order** and **Modify** requests will require approval, but not **Cancel** requests), publish offerings from the Offerings area.

Service offerings that were published from the Offerings area, and whose approval policy has been changed to **No Approval**, still require approval

QCCR1D178192

Problem

If a catalog in the Cloud Service Management Console is configured to have an **Active** approval process and an approval policy, and if a user publishes a service offering to this catalog from the Offerings area and changes the approval policy to be **No Approval**, modify requests will still require approval.

Cause

Product defect.

Workaround

Publish service offerings from the Catalogs area if you need to override the default approval process and policy for a service offering.

Cannot delete component type that was used in a subscription that has been cancelled and deleted

QCCR1D180505

Problem

Custom service component types and component palettes cannot be deleted from the Cloud Service Management Console's Service Components tile under the following conditions:

1. Create a service design using service component templates derived from custom service component types. These custom service component types could be under an HP CSA component palette or a custom component palette.
2. Create service subscriptions to these service designs by publishing service designs as service offerings and by publishing service offerings into catalogs.
3. Cancel and delete the service subscriptions.
4. Unpublish the service offering using the service design created above from catalogs and delete the service offering.

5. Delete the service design.

Cause

Though the custom component types and custom component palettes could be deleted as there are no service designs referring to them, there are service component database records created for service subscriptions which are referring to these custom component types. This does not allow for the deletion of custom component types and custom component palettes.

Workaround

Deleted service subscriptions are stored in the HP CSA database in a 'Retired' state. In order to delete custom component types and custom component palettes, run the purge tool shipped with HP CSA in order to permanently delete subscriptions which are canceled, deleted or expired for certain number of days. After these subscriptions are permanently deleted, custom component types and custom component palettes can be deleted.

In the topology designer, the Modifiable checkbox for a dependent property can be unselected

QCCR1D180960

Problem

A user is able to unselect the **Modifiable** checkbox on dependent properties in topology designs. For example, when a user creates a topology design containing a Network Segment node, the user is able to select the **Modifiable** checkbox located by the **Network** property. If the user specifies the **Network** property with the **Modifiable** checkbox selected, then a new dependent property, **Select a subnet**, appears. The **Select a subnet** property has the **Modifiable** checkbox selected automatically. If the user unselects this checkbox, a subnet for the **Network** property cannot be selected in the Offerings of the Cloud Service Management Console or in the Marketplace Portal.

Cause

The topology designer allows the user to unselect the **Modifiable** checkbox of a dependent property.

Workaround

When creating topology designs, do not unselect a **Modifiable** checkbox of a dependent property if it has been automatically selected.

Error importing service offering archive

QCCR1D181093

Problem

When importing an offering of a sequenced design, if the sequenced design contains Delegated Topology components, you might encounter the following error: "The existing service design has active service offerings with an option model that is not equal to the option model being imported."

Cause

This issue can occur when the target system already contains the sequence design that need to be imported.

Workaround

Choose **Update** rather than **Import** when importing the offering of sequenced design with delegated topology components.

A service offering with a topology design that is imported using the content archive tool is not viewable in the Cloud Service Management Console

QCCR1D181337

Problem

When importing a service offering with a topology design using the –f or --updatePreserveExisting option of the content archive tool, the service offering cannot be viewed in the Cloud Service Management Console. Note that the topology design is imported successfully.

Cause

This issue can occur when an identical service offering cannot be found and updated.

Workaround

Create a new service offering with the imported topology design.

After viewing a topology design and returning to the list of designs, no designs are shown

QCCR1D181770

Problem

When returning to the list of topology designs after a tag is selected and a topology design is viewed, no designs are shown.

Cause

When returning to the list of topology designs, the focus is lost from the selected tag.

Workaround

Select a tag to view the designs.

"Internal server error contact your system administrator" message is logged every five minutes

QCCR1D182005

Problem

The following informational message is logged every five minutes which can fill the disk space:

```
WARN TopologyMetamodelProviderImpl : Internal server error contact your system administrator.
```

Cause

There is a problem with one of the configured resource providers.

Workaround

If disk space is not an issue and another resource provider can be used, the message can be ignored.

If disk space is an issue, correct the configuration of or remove the resource provider that is causing the problem.

Marketplace Portal

Marketplace Portal min/max messages are incorrect

QCCR1D177555

Problem

The Marketplace Portal performs validation on various inputs during checkout, service modification, and when performing service actions. Those validations can include checking for a min/max integer and min/max text length. If an input does not meet validation requirements (as configured in the service design), the messaging provided to the user is incorrect. For example, if the minimum value is 10, it might read:

```
"Must be greater than 10."
```

However, it should read:

```
"Must be greater than or equal to 10."
```

This applies to the min/max messages for integers and text lengths.

Cause

Incorrect text in the message catalogs.

Workaround

1. Instruct users to interpret the message as "greater than or equal".
2. Change the wording in the Marketplace Portal message catalogs. These can be found under:

```
<CSA_HOME>/portal/node_modules/mpp-ui/dist/locales
```

There are message catalogs for each supported language (e.g. "en") in a JSON format. The messages that need to be updated are found under `"common" > "validation"`. Replace the following incorrect messages:

```
    "minField": "Must be greater than {{min}}.",
    "maxField": "Must be less than {{max}}.",
    "minLengthField": "Must be longer than {{min}} characters.",
    "maxLengthField": "Must be shorter than {{max}} characters.",
```

With the following corrected messages:

```
    "minField": "Must be greater than or equal to {{min}}.",
    "maxField": "Must be less than or equal to {{max}}.",
    "minLengthField": "Must be longer than or equal to {{min}} characters.",
    "maxLengthField": "Must be shorter than or equal to {{max}} characters.",
```

The same type of change will need to be applied to any other languages that are used (for example, "zh").

Known Problems, Limitations and Workarounds

Marketplace Portal allows you to select security groups that are already added to the VM network interface

QCCR1D177361

Problem

For services created from Cloud OS topology designs, the **Add Security Group** action in the Marketplace Portal allows you to select security groups that are already added to the VM network interface. The dropdown should only display security groups that are not already assigned.

Cause

The list of security groups retrieved from HP Cloud OS is not properly filtered.

Workaround

No workaround is available.

Marketplace Portal allows you to remove security groups that are not assigned to the VM network interface

QCCR1D177360

Problem

For services created from Cloud OS topology designs, the **Remove Security Group** action in the Marketplace Portal allows you to select security groups that were not assigned to the VM network interface. The dropdown should only display security groups that were assigned to the VM network interface.

Cause

The list of security groups retrieved from HP Cloud OS is not properly filtered.

Workaround

No workaround is available.

Incorrect input property label for volume names in Marketplace Portal

QCCR1D176945

Problem

The Add Volume Group to Server Group public action visible in the Marketplace Portal for services created from Cloud OS topology designs has a misnamed input parameter that requests volume IDs to be provided instead of volume names.

Cause

An incorrect label for this input property is displayed for this action.

Workaround

The incorrect label does not affect the functionality of this action. The dropdown for this input will display volume names, and the action expects volume names as input.

Marketplace Portal is unresponsive after canceling subscriptions

QCCR1D177494

Problem

Canceling subscriptions for HP Cloud OS-based designs can cause the HP Cloud OS Administration Dashboard and/or Marketplace Portal to become unresponsive for a period of time. This behavior is most commonly experienced when multiple subscriptions are canceled concurrently.

Cause

Product defect.

Workaround

The UI will become responsive after a temporary delay.

The Marketplace Portal **Add Volume Group to Server Group** public action works only in limited situations

QCCR1D177615

Problem

The **Add Volume Group to Server Group** public action that is visible in the Marketplace Portal for services created from topology HP Cloud OS designs works only in very limited situations.

Cause

The number of servers in the server group must match the number of volumes being added when this action is called. However, the dropdown for **Volume IDs** does not allow a user to select multiple volumes. Therefore this

action can only work successfully if the number of servers in the server group is one (1). In addition, a volume must have already been created in HP Cloud OS that is not associated to a server group, as only such volumes will be available for user selection when running this action.

Workaround

No workaround available.

Marketplace Portal fails to start after installing HP CSA on Windows

QCCR1D172298

Problem

After installing HP CSA in a Windows environment, the Marketplace Portal may fail to start, preventing users from logging in to the Marketplace Portal.

Cause

The script used to start the Marketplace Portal service fails intermittently.

Workaround

Determine if the Marketplace Portal service is running by navigating to **Control Panel** > **Administrative Tools** > **Services**. If the HP Marketplace Portal service is not running, start the service. If it is running, but the Marketplace Portal is inaccessible to a web browser, restart the service.

Subscriber notifications are not localized in Marketplace Portal

QCCR1D177158

Problem

Notifications sent to subscribers in the Marketplace Portal are not localized to the client browser locale.

Cause

Product limitation.

Workaround

No workaround is available.

A **List** subscriber option property that is marked as not required in the Cloud Service Management Console appears as required in the Marketplace Portal

QCCR1D178237

Problem

When creating a **List** subscriber option property in the Cloud Service Management Console's Sequenced Designs area, if the **Value Entry Method** is **Dynamic Query**, **Multi-Select** is enabled, and the property is marked as **Not Required**, the property will still be required for subscribers in the Marketplace Portal.

Cause

Dynamic list properties are incorrectly always marked as required when properties are cloned from a service design to a service offering, and, hence, are required to subscribers in the Marketplace Portal.

Workaround

The script that produces the dynamic data can be updated to return a value such as **No Selection** that a subscriber can select to comply with the required property enforcement in the Marketplace Portal.

Properties that should not be visible to subscribers are displayed on the View Service Topology page

QCCR1D175828

Problem

In the Marketplace Portal, the **View Service Topology** link displays properties for topology based subscriptions that might not be appropriate to be visible to subscribers. In particular, properties such as `self`, `global_id`, and `resource_pool_ref` (among others) include the URL to the HP Cloud OS resource provider that performed the provisioning.

Cause

An exclusion list was created to hide these properties on the **My Service Details** page, but the same functionality was not added to the **View Service Topology** page.

Workaround

No workaround is available.

Known Problems, Limitations and Workarounds

When single sign-on is configured, credentials must be re-entered when accessing the Marketplace Portal page from a previous successful browser session
QCCR1D180630

Problem

At times, the single sign-on prompt might appear multiple times when trying to log in to the Marketplace Portal.

Cause

The issue can occur in situations where the domain name generated in the SiteMinder cookie (SMSESSION) does not match the address that is used to access the Marketplace Portal.

Workaround

Changes must be made to the values of the configuration parameters for the Marketplace Portal to use the fully-qualified domain name (FQDN) of the Web agent.

1   If the machine (from which the browser that accesses the Marketplace Portal is launched) is unable to recognize the FQDN, changes must be made to the machine configuration (for example, update the host file in Windows) to define an alias for the FQDN to the IP address of the Web agent.

2   On the system on which the Marketplace Portal is installed:

a   Update the following properties in the `%CSA_HOME%/portal/conf/mpp.json` file:
```
"idmProvider": {
.......
    " returnUrl ": " https://FQDN_OF_WEB_AGENT /mpp ",
    "redirectUrl": "https://FQDN_OF_WEB_AGENT ",
.......
}
```

b   Update the system configuration (for example, update the host file in Windows) to define an alias for the FQDN to the IP address of the Web agent.

c   Restart the system. Verify the Marketplace Portal service has restarted.

3   On the system on which HP CSA is installed:

a   Verify that the Organization URL for the consumer organization uses the FQDN (from the Cloud Service Management Console dashboard, select **Organizations > Customer Organization > General Information**). To update the Organization URL, set the csa.subscriber.portal.url property in `%CSA_HOME%\jboss-as-7.1.1.Final\standalone\deployments\csa.war\WEB-INF\classes\csa.properties` to use the FQDN.

b   Restart the HP Cloud Service Automation service.

When modifying a subscription, profiles are shown but not selectable
QCCR1D180705

Problem

When a sequenced design contains a Delegated Topology component, if a subscription is modified, the topology profiles will be shown. The topology profiles cannot be selected.

Cause

Modifying the topology subscription profiles is not supported through the Marketplace Portal. But, because the profiles originate through a sequenced design, they are shown in the Marketplace Portal.

Workaround

No workaround is available.

When logging in to the Marketplace Portal using single sign-on, the landing page should not be shown.
QCCR1D180818

Problem

When accessing the Marketplace Portal during a single sign-on session, the user would land on the landing page displaying a button to be clicked to get to the Marketplace Portal dashboard. By default the button is labeled with "Log In." This might cause confusion as the authentication has already been completed using a single sign-on login prompt. In order to avoid this confusion, the label of the button can be modified in the

`%CSA_HOME%/portal/node_modules/mpp-ui/dist/locales/{locale}/rb.json` file. The location of the file depends on the locale being used. For example, for English, the file is `%CSA_HOME%/portal/node_modules/mpp-ui/dist/locales/en/rb.json`.

Cause

The default value of the button has been defined as "Log in" in the `rb.json` file.

Workaround

1 Modify the value of the button in the rb.json file. For example, to change the label to "Click to continue," make the following modification:

```
"login": {
.......
    "login": "Click to continue",
.......
}
```

2 Restart the Marketplace Portal service.

The Marketplace Portal file system must be protected by the operating system.

QCCR1D181476

Problem

For security reasons, the Marketplace Portal file system must be protected by the operating system.

Cause

Some files should only be accessible by the owner of the application.

Workaround

After installing HP CSA, protect the Marketplace Portal file system:

Windows

1 Open an elevated command prompt (a command prompt that is run as the administrator). For example, navigate to **All Programs > Accessories**. Right-click on **Command Prompt** and select **Run as administrator**.

2 From the elevated command prompt, run the following command:

```
attrib +s +h "%CSA_HOME%\portal" /S /D /L
```

where %CSA_HOME% is the directory in which HP CSA is installed.

3 Restart the HP Cloud Service Automation and Marketplace Portal services. For example, navigate to **Control Panel > Administrative Tools > Services**. Right-click on the service and select **Restart**.

Linux

1 Log in as the root user.

2 Run the following commands:

```
chown –R csauser:csagrp $CSA_HOME/portal
chmod –R 700 $CSA_HOME/portal
```

where csauser and csagrp are the user and group you configured for HP CSA when you installed HP CSA and $CSA_HOME is the directory in which HP CSA is installed.

3 Log out as root and log in as csauser.

4 Restart the csa and mpp services by running the following commands:

```
service csa restart
service mpp restart
```

Known Problems, Limitations and Workarounds

Deleting a canceled subscription generates a cancel subscription request
QCCR1D181771

Problem

A duplicate cancel subscription request shows up under the **Requests** tile when a user deletes a canceled subscription.

Cause

When a user deletes a canceled subscription, a cancel subscription request is created.

Workaround

Ignore the duplicate cancel subscription request.

You can modify a subscription to include an empty value for single select list property even if the list property is a required field
QCCR1D181903

Problem

When modifying a subscription in the Marketplace Portal, a user can specify an empty value for a required field (when the field is a single select list property).

Cause

The Marketplace Portal does not detect empty single select list property values.

Workaround

Verify that required fields are filled with a valid value from the single select list before submitting a modification request.

Approval Request details page doesn't show a document that is attached from the shopping cart at order time
QCCR1D182016

Problem

Shopping Cart - Approval Request details page doesn't show a document that is attached from the shopping cart at order time.

Cause

The feature is not implemented.

Workaround

Submit a request directly (not via the shopping cart) to see the attachments.

A subscription submitted with an attached document that is larger than 5MB fails
QCCR1D182348

Problem

Submitting a subscription fails when the size of an attached document is larger than 5MB.

Cause

Only files up to 5MB can be submitted.

Workaround

Reduce the size of the attachment to less than 5MB before submitting the subscription.

Dynamic properties of a service whose configuration is being edited in the shopping cart are not properly set
QCCR1D182350

Problem

While editing a configuration of an order added to the shopping cart, previously selected dynamic properties values are not shown.

Cause

Dynamic property load handling is not implemented for the shopping cart.

Workaround

Reconfigure the service.

Known Problems, Limitations and Workarounds

Clustered Environment

The master node fails to start because HP CSA is installed in different paths on the master and slave nodes

QCCR1D180811

Problem

If HP CSA is installed in different paths on the master and slave nodes, the master node fails to start due to a mismatch in the ESAPI property file location.

Cause

The ESAPI property file location is hardcoded in the HP CSA configuration file.

Workaround

On the master and slave nodes, in the `%CSA_HOME%\jboss-as-7.1.1.Final\domain\configuration\domain.xml` file, locate the system-properties section and the property attribute whose name is set to org.owasp.esapi.resources. The value of this property is set to the name and location of the ESAPI file. For example, `<property name="org.owasp.esapi.resources" value="C:\Program Files\Hewlett-Packard\CSA/jboss-as-7.1.1.Final/domain/configuration/esapi"/>` where `C:\Program Files\Hewlett-Packard\CSA/jboss-as-7.1.1.Final/domain/configuration/esapi` is the name and location of the ESAPI file.

Replicate the absolute path of the ESAPI property file from master node to the slave nodes and vice-versa. This will make the ESAPI property file available in same location across all nodes, irrespective of the active node.

For example, in a clustered environment, the master node property is set to `C:\Program Files\Hewlett-Packard\CSA\jboss-as-7.1.1.Final\domain\configuration\esapi` and the slave node property is set to `C:\csa_slave\ jboss-as-7.1.1.Final\domain\configuration\esapi`. On the master node, create the `C:\csa_slave\ jboss-as-7.1.1.Final\domain\configuration\` directory and copy the `esapi` file to this directory. On the slave node, create the `C:\Program Files\Hewlett-Packard\CSA\jboss-as-7.1.1.Final\domain\configuration\` directory and copy the `esapi` file to this directory.

In the "Configuring an HP CSA Cluster for Server Failover" guide (version 4.00), the task to enable IdM when manually configuring the master node is missing

QCCR1D181045

Problem

Clustering is not enabled for the Identity Management component on the master node when following the instructions to manually configure a clustered environment in the *Configuring an HP CSA Cluster for Server Failover* guide (version 4.00). See pages 52-3 in the Windows guide and page 67 in the Linux guide.

Cause

The step to enable clustering for the Identity Management component on the master node is missing.

Workaround

Complete the following on the master node:

In the `%CSA_HOME%\jboss-as-7.1.1.Final\domain\servers\hp-cloud\deployments\idm-service.war\WEB-INF\spring\applicationContext-common.xml` file, uncomment or enable the following content:
```
<!--
<property name="clusterEnabled" value="true" />
-->
```

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

Known Problems, Limitations and Workarounds

In the "Configuring an HP CSA Cluster for Server Failover" guide, the file that should be edited on the slave node to enable clustering for IdM is not identified correctly in the appendix that documents the manual configuration of a clustered environment

QCCR1D181048

Problem

The file that should be edited on the slave node to enable clustering for the Identity Management component is not identified correctly in the appendix that documents the manual configuration of a clustered environment in the *Configuring an HP CSA Cluster for Server Failover* guide (version 4.00). See page 63 in the Windows guide and page 76 in the Linux guide.

Cause

The file that the guide says to edit is `%CSA_HOME%\jboss-as-7.1.1.Final\domain\servers\hp-cloud\deployments\idm-service.war\WEB-INF\spring\applicationContext.properties`.

Workaround

The file that should be edited is `%CSA_HOME%\jboss-as-7.1.1.Final\domain\servers\hp-cloud\deployments\idm-service.war\WEB-INF\spring\applicationContext-common.xml`.

In the "Configuring an HP CSA Cluster for Server Failover" guide, the MPP_Proxy node, CSA proxy, Identity Management component, and Redis data structure server are not configured on the slave node when following the instructions to configure a clustered environment

QCCR1D181049

Problem

The MPP_Proxy node, CSA proxy, Identity Management component, and Redis data structure server are not configured on the slave node when following the instructions to configure a clustered environment using the configuration tool from the *Configuring an HP CSA Cluster for Server Failover* guide (version 4.00).

Cause

The steps to configure the MPP_Proxy node, CSA proxy, Identity Management component, and Redis data structure server on the slave node using the configuration tool are missing from the *Configuring an HP CSA Cluster for Server Failover* guide (version 4.00).

Workaround

On the slave node, complete the following steps to configure the MPP_Proxy node, CSA proxy, Identity Management component, and Redis data structure server:

1   On the slave node, launch the Configuration tool:

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

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

3   Enter the following information:

Field	Description
IP Address or Hostname	Required. The IP address or hostname of the Apache Web server on the Marketplace Portal proxy node.
HTTP Port	Required. The port used by the Apache Web server on the Marketplace Portal proxy node (for example, 8080).
Configured with SSL	Optional. Select this option if you want the Apache Web server on the Marketplace Portal proxy node to communicate with the Marketplace Portal over SSL.
HTTPS Port	The port used by the Apache Web server on the Marketplace Portal proxy node (for example, 8089).

4   Click **Next**.

5   Enter the following information:

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

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

On upgrade in a clustered environment, the upgrade installer uses the JAVA_HOME variable defined in the configuration file for a standalone environment

QCCR1D181134

Problem

When upgrading HP CSA in a clustered environment, the upgrade installer uses the JRE defined in the configuration file for the standalone environment.

Cause

The upgrade installer does not detect if the HP CSA environment is standalone or clustered.

Workaround

Configure the JAVA_HOME variable in the configuration files for both a standalone and clustered environment. The location of the configuration files are:

Windows

- `<CSA_HOME>\jboss-as-7.1.1.Final\bin\standalone.conf.bat` (standalone)

- `<CSA_HOME>\jboss-as-7.1.1.Final\bin\domain.conf.bat` (clustered)

Linux

- `<CSA_HOME>/jboss-as-7.1.1.Final/bin/standalone.conf` (standalone)

- `<CSA_HOME>/jboss-as-7.1.1.Final/bin/domain.conf` (clustered)

Known Problems, Limitations and Workarounds

In the "Configuring an HP CSA Cluster for Server Failover" guide for Linux, the "Share Filesystem Resource" sections must be updated

QCCR1D181152

Problem

In a clustered environment on a Linux system, shared file system resources may not be visible in HP CSA.

Cause

The shared file system cannot be symbolically linked.

Workaround

Configure HP CSA to share file system resources using the following commands. The following example shows how to share the `images` directory that is installed with each instance of HP CSA.

1   Create a shared file system on the network. The master and slave nodes must be able to read and write to the shared location.

2   Move the contents of the `<CSA_HOME>/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/ csa.war/images` directory to the shared location (for example, move the files to `//<ShareSystem>/HAShare/CSAImages`).

3   On the master and slave nodes, log in as root.

4   If it exists, delete the `<CSA_HOME>/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/ csa.war/images` directory.

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

    username=<ShareSystemUser>
    password=<ShareSystemUserPassword>

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

    chmod 600 /etc/.win-mnt-cred

7   Edit `/etc/fstab` and add the following line:

    //<ShareSystem>/HAShare/CSAImages <CSA_HOME>/jboss-as-7.1.1.Final/domain/servers/hp-cloud/
    deployments/csa.war/images cifs credentials=/etc/.win-mnt-cred,iocharset=utf8,
    file_mode=0777,dir_mode=0777 0 0

8   Mount the shared file system:

    mount -a

On upgrade of a clustered environment on a Linux system, the upgraded web.xml file contains a ^M at the end of every line

QCCR1D181154

Problem

When upgrading HP CSA in a clustered environment on a Linux system, the `<CSA_HOME>/jboss-as-7.1.1.Final/ domain/servers/hp-cloud/deployments/csa.war/WEB-INF/web.xml` file contains a ^M at the end of every line.

Cause

The upgraded file contains a ^M at the end of every line.

Workaround

Note that the file functions properly with or without the ^M character appearing at the end of every line therefore no action is necessary.

To improve the readability of the file, update it by removing the ^M characters and saving the file.

Known Problems, Limitations and Workarounds

The configuration tool does not update the URL that redirects requests to the Marketplace Portal
QCCR1D181161

Problem

When you are running the configuration tool to configure an HP CSA master or slave node that uses the Apache HTTP proxy server as a load balancer, the tool does not update the Marketplace Portal URL in the `<CSA_HOME>/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/mpp.war/index.html` file. This file is used to redirect requests to the Marketplace Portal.

Cause

Not implemented.

Workaround

After running the configuration tool, edit the `<CSA_HOME>/jboss-as-7.1.1.Final/domain/servers/hp-cloud/deployments/mpp.war/index.html` file. Update the URL attribute value to the HP CSA Apache proxy server URL. The protocol and port should be based on the protocol and port that are configured to proxy requests from the HP CSA Apache proxy server to the Marketplace Portal (MPP) Apache proxy server.

For example, if the HP CSA Apache proxy server hostname is APACHE_MASTER_HOSTNAME and it proxies requests to the MPP Apache proxy server using HTTPS and port 8089, the URL attribute in the `index.html` file would be defined as follows:

```
<meta http-equiv="refresh" content="0;URL= https://APACHE_MASTER_HOSTNAME:8089/"/>
```

The configuration tool may not import the Apache HTTP proxy server certificate
QCCR1D181162

Problem

In a Linux environment, when you are running the configuration tool to configure an HP CSA master or slave node that uses the Apache HTTP proxy server as a load balancer, the tool may not import the Apache certificate into the HP CSA truststore.

Cause

The configuration tool does not import the Apache certificate into the HP CSA JRE truststore.

Workaround

After running the configuration tool, check if the Apache certificate is being imported into the HP CSA truststore by running following command on the master or slave node:

```
<CSA_JRE_HOME>/bin/keytool -list -alias apache -keystore <CSA_JRE_HOME>/lib/security/cacerts
```

If the alias `apache` is found, no action is required. The Apache certificate has been imported into the HP CSA truststore.

If the alias `apache` is not found in the HP CSA truststore, import the Apache certificate manually by running following command (if the Apache HTTP proxy server is located on a different system, copy the certificate to the master or slave node before running this command):

```
<CSA_JRE_HOME>/bin/keytool -importcert -file <path_to>/apache.crt -alias apache
-keystore <CSA_JRE_HOME>/lib/security/cacerts
```

Installation and Upgrade Guides

The generated PDFs have formatting problems

Problem

The PDFs generated from the Installation and Upgrade Guides have the following problems:
- In a table row that is split due to pagination, the first column of this row is merged with the first column of the next row in the table.
- Example text is truncated on the right margin.
- Text is awkwardly broken at the end of a line.
- Links to other sections in the document are broken.
- Icons embedded in the content may not be displayed.

Workaround
View the contents of the Installation and Upgrade Guides from a Web browser instead of printing them.

Online Help

Cloud Service Management Console Help is missing information about resource bindings and resource offerings when importing and exporting component palettes
QCCR1D177198
Problem
The Cloud Service Management Console Help is missing the following information:
- If component templates in a component palette have resource bindings on resource offerings, when the component palette is exported, resource offering XML files are included in the component palette archive.
- At component palette import, resource offerings are either created when a resource offering with same name does not exist on the system, or updated when a resource offering with the same name exists. This resource offering import behavior occurs because the import option for a component palette is always Update.

Cause
Missing information in the Cloud Service Management Console Help.
Workaround
Not Applicable.

HP CSA APIs

REST API login fails due to truncation of content
QCCR1D153699
Problem
If you use the user REST API lookup URL `https://<host>:<port>/csa/rest/login/<orgName>/<username>` without including a trailing "`/`" after `<username>`, the `<username>` may have trailing characters erroneously removed. For a username such as **john.smith@xyz.com**, the .**com** portion is removed from the username, resulting in an error.
Cause
Spring strips off the parts of the username after the final '.' if no trailing slash is included.
Workaround
There are 2 workarounds available
1) Add a trailing "`/`" to the REST API lookup call.
`https://<host>:<port>/csa/rest/login/<orgName>/<username>/`
For example,
`https://<host>:<port>/csa/rest/login/CSA-Provider/john.smith@xyz.com/`
2) For this type of username use the alternate lookup URL:
`https://<host>:<port>/csa/rest/login/<orgName>/userLookup?userName=<userName>`
For example:
`https://<host>:<port>/csa/rest/login/CSA-Provider/userLookup?userName=john.smith@xyz.com`

Primitive values reset to default if no value is provided
QCCR1D152913
Problem
When users make a PUT request from the REST API, if the users don't provide values for primitive properties, these properties are set to their default values.
Cause
Some properties of an artifact are modeled in Java using primitive types. This can cause certain issues when using the PUT requests via REST API. When a PUT request is sent to the HP CSA instance using a REST API, the data that represents an artifact or a part of an artifact is converted to a java object. All properties with primitive types in a Java object always need to have values. When users don't provide values for these properties, the default values are used to satisfy the requirement.

The following are the primitive types in Java:
- byte

- short
- int
- long
- float
- double
- char
- boolean

Workaround

Invoke a GET call first, and then modify only the necessary properties from the GET response. This modified response should be sent as part of the PUT request.

Artifact REST API returns error that detail=FULL is not supported

QCCR165193

Problem

When the Artifact GET REST API is called for an Organization artifact without specifying the detail parameter, an error is returned reporting that "detail=FULL is not supported for Organization Artifact".

Cause

The default value of detail parameter FULL has been disabled for the Organization artifact because the returned response can be very large due to many contained artifacts.

Workaround

Specify "detail=BASIC" as a query parameter.

Integrations with HP CSA

HP ArcSight Logger

HP CSA `server.log` integration with ArcSight Logger does not work correctly

QCCR1D156585

Problem

Integration of the `%CSA_HOME%\jboss-as-7.1.1.Final\standalone\log\server.log` with HP ArcSight Logger version 5.2 or 5.3 is not supported.

Cause

JBoss 7.1.1 integration with ArcSight Logger 5.2 or 5.3 requires an additional handler and is not currently supported by ArcSight Logger.

Workaround

No workaround is currently available. An enhancement request has been raised with the HP ArcSight Logger team for this handler and may be available after product release. Contact your HP support representative for more details on the status of this enhancement request.

HP ArcSight Logger configuration entries are not seen in `log4j.properties`

QCCR1D156785

Problem

If HP ArcSight Logger was configured with HP CSA prior to upgrade to 3.10, after upgrade to HP CSA 3.10, the ArcSight Logger integration no longer works as expected.

Cause

The upgrade to 3.10 does not properly update the `log4j.properties` file.

Workaround

After upgrading to HP CSA 3.1, open:
`%CSA_HOME%\jboss-as-7.1.1.Final\standalone\deployments\csa.war\WEB-INF\classes\log4j.properties`
and comment the following lines at the bottom of the file, as shown below:

```
#log4j.appender.cef1=com.hp.esp.arcsight.cef.appender.Log4jAppender
#log4j.appender.cef1.deviceVendor=HP
#log4j.appender.cef1.deviceProduct=CSA
#log4j.appender.cef1.deviceVersion=3.1
#log4j.appender.cef1.transportType=SYSLOG
```

```
#log4j.appender.cef1.hostName=192.x.x.x
#log4j.appender.cef1.port=515
#log4j.appender.cef1.layout=org.apache.log4j.PatternLayout
#log4j.appender.cef1.layout.ConversionPattern=%d{DATE} [%t] %-5p %x %C{1} : %m%n
#log4j.appender.cef1.appender.threshold=off
```

Cannot integrate HP ArcSight with HP Operations Orchestration (HP OO) 10.x

QCCR1D176942

Problem

HP OO 10.x integration with HP ArcSight is not supported or discussed in the HP CSA-ArcSight integration whitepaper.

Cause

Integration is not yet supported.

Workaround

HP OO 10.x integration with HP ArcSight will be available in a future release.

HP Cloud OS

Terminating an instance in HP Cloud OS 1.2 is not reflected in the HP CSA Marketplace Portal or Cloud Service Management Console

QCCR1D176653

Problem

Changes made to an already provisioned HP Cloud OS instance in the HP Cloud OS Administration Dashboard will not be reflected in the Cloud Service Management Console or the Marketplace Portal. For example, if you terminate an instance in HP Cloud OS via the HP Cloud OS Administration Dashboard, the subscription will still show as Active in the Marketplace Portal and the Operations area of the Cloud Service Management Console.

Cause

Changes made directly to active instances in HP Cloud OS are not synchronized to HP CSA.

Workaround

If you need to cancel or otherwise modify a subscription for a service that was provisioned by HP CSA, do so via the Marketplace Portal or the Operations area of the Cloud Service Management Console, not via the HP Cloud OS Administration Dashboard.

Maximum and minimum number of instances for a volume group in a deployed service do not display when using HP Cloud OS version 1.2

QCCR1D180635

Problem

The user will not see Maximum Instances and Minimum Instances for a volume group in a deployed service when using HP Cloud OS version 1.2.

Cause

HP Cloud OS 1.2 does not provide maximum and minimum number of instances for volume groups.

Workaround

No workaround is available for HP Cloud OS 1.2. To view the maximum and minimum number of instances for volume groups, upgrade to HP Cloud OS 2.0.

The HP Cloud OS resource pool can be unselected when a topology design is updated

QCCR1D181540

Problem

When creating a topology design that requires an HP Cloud OS resource pool, it is possible to save and publish the topology design after unselecting the HP Cloud OS resource pool. Subsequently, the resource pool cannot be selected in the Offerings of the Cloud Service Management Console or in the Marketplace Portal.

Cause

The topology designer allows the user to unselect the HP Cloud OS resource pool when updating a topology design.

Workaround

When updating topology designs, do not unselect the HP Cloud OS resource pool.

Known Problems, Limitations and Workarounds

The public action "Add Server to Server group" cannot be used
QCCR1D181733

Problem

The public action "Add Server to Server group" cannot be used when the HP Cloud OS provider instance is behind a proxy server with SSL enabled.

Cause

HP Cloud OS does not allow the public action "Add Server to Server group" to be used when behind a proxy server with SSL enabled.

Workaround

Disable SSL.

Import of service design fails with error "Error importing content archive. Import of topology 'My Service Design' contains critical error."
QCCR1D181764

Problem

If a service design named "My Service Design" is imported without the defaultCloudOSProvider or defaultResourcePool properties set, the following error is displayed:

```
Error importing content archive. Import of topology 'My Service Design' contains critical
error.
```

Cause

The defaultCloudOSProvider and defaultResourcePool properties must be configured when importing a service offering.

Workaround

To verify the cause of this error message, run a preview and select the "View Detailed Report" link. If the message `No enabled Cloud OS Provider could be found (for id COS 1.2 RC4).` is found, the defaultCloudOSProvider and defaultResourcePool properties have not been configured. Configure these properties before importing the service design.

Behavior of property values and resource pool in profiles of a topology design may not be as expected
QCCR1D181767

Problem

The property value or resource pool used in a topology design overrides the property value or resource pool used in the profile of a design. However, the property value or resource pool used in a profile does not override the property value or resource pool used in the design.

For example, if a topology design's resource pool value is changed, all profile's resource pool values are updated to match the design's value. But, if a profile's resource pool value is changed to a value different from the design's value, the values remain different (the design's value is not updated to match the profile's value).

Cause

This is the expected behavior.

Workaround

No workaround is available.

The following error messages are logged: "ERROR CloudOSPlugin: Failed to get the metamodel from Cloud OS Connection error, status code 401" or "WARN TopologyMetamodelProviderCache: Failed to refresh metamodel topology:design-hp_cloud_service-s-8a86183854fa7d2e0494fa7d8af100a"
QCCR1D182079

Problem

One or both of the following error messages appear in the log file:

```
ERROR CloudOSPlugin: Failed to get the metamodel from Cloud OS Connection error, status code
401
```

```
WARN TopologyMetamodelProviderCache: Failed to refresh metamodel topology:design-
hp_cloud_service-s-8a86183854fa7d2e0494fa7d8af100a.
```
Cause
The HP Cloud OS provider is not accessible.
Workaround
This is the expected behavior. The metamodel is required during design time. HP CSA needs the metamodel before creating topology designs. If the HP Cloud OS provider is not accessible, every attempt to open the designer will produce these error messages in the log files.

HP Matrix Operating Environment (HP MOE)

HP MOE Subscription fails with error "No server pools are available to user"
QCCR1D147531
Problem
When a subscription is requested for a MOE_COMPUTE_MT_3.20 or MOE_SCL_MT based service design, the following error is seen in the OO flow:

```
No server pools are available to user
```
Cause
HP Matrix Operating Environment has the following restriction: In v7.0, correct behavior of the API/CLI commands is only guaranteed if the user is the member of one organization.
Workaround
See the whitepaper *Multi-Tenancy in HP Matrix Operating Environment Infrastructure Orchestration 7.0* for more details.

HP Operations Orchestration (HP OO)

A subscription fails for an HP Cloud Service (HP CS) – OPENSTACK service and its status shows as **Pending**.
QCCR1D155141
Problem
When a subscription fails for an HP Cloud Service (HP CS) – OPENSTACK service, the subscription status in the Marketplace Portal may still show as **Pending** with a state of **Deploying**.
Cause
Invalid combination of inputs is selected when ordering the subscription. The HP Operations Orchestration (HP OO) – OPENSTACK integration flows do not return an error when an invalid combination of inputs is selected when ordering the subscription. They throw a runtime exception that terminates the flow. The process status is thus not updated in HP CSA, leaving the state as **Deploying** and the subscription status as **Pending**.
Workaround
No workaround is currently available. A defect has been submitted against the HP OO – HP CS integration, with ID QCCR1D155146.

HP OO error message occurs when running Resource Synchronization Action
QCCR1D178109
Problem
HP CSA includes a VMware vCenter Sync Resource Capacity OO flow that can be configured as a Resource Synchronization Action on a resource pool in the Resources area of the Cloud Service Management Console. This flow does not work correctly when using HP OO 10.02, and results in the following HP OO log error

```
2014-01-07 02:57:43,697 [WorkerExecutionThread-5_165674252] (PluginAdapterImpl.java:176)
ERROR - com.vmware.vim25.ManagedObjectNotFound at
Sun.reflect.NativeConstructorAccessorImpl.newInstance0(Native Method)
```
Cause
Defect in the flow.
Workaround
Manually update the capacities of the resources configured on resource pools in the Cloud Service Management Console.

Known Problems, Limitations and Workarounds

HP SiteScope (HP SiS)

Subscription for service design MOE_COMPUTE_SITESCOPE_UCMDB_3.20 is canceled and some HP SiteScope monitors are not removed when using HP Operations Orchestration

QCCR1D177099

Problem

When a subscription for the service design `MOE_COMPUTE_SITESCOPE_UCMDB_3.20` is cancelled, some of the monitors deployed on HP SiteScope may not be removed when using HP Operations Orchestration (HP OO) 10.x.

Cause

This is a defect in HP OO 10.01.001, which will be addressed in 10.10.

Workaround

Delete the monitors manually in HP SiteScope.

VMware vCenter

vCenter service design causes two lifecycle actions to run at the same time

QCCR1D165889

Problem

While one lifecycle transition is in progress, the lifecycle engine does not allow another lifecycle transition to begin. But, the Marketplace Portal allows this, which causes the lifecycle engine to behave unexpectedly. This issue occurs for vCenter-based subscriptions as part of Flex-in and Flex-out operations.

Cause

The `Add Server` public action on vCenter-based subscriptions has timed out. But the `Undeploy` action called by `Add Server` to perform cleanup is still running in the background. HP CSA is not aware of this process in the background and allows a subsequent `Add Server` action to be invoked.

Workaround

Increase the timeout for the vCenter Flex-in Server/vCenter Flex-out Server flows.

Follow the steps below for the Flex-in Server flows:

1. Open HP Operations Orchestration studio.
2. Open the `vCenter Flex-in Server` subflow found under
   `/Library/CSA/3.2/Providers/vCenter/vCenter Flex Server Count/Subflows/`.
3. Right click on the **Poll LCE** step and click on **Properties**.
4. Change the value of the `waitCounter` input to 120 (double the timeout minutes)
5. Save the flow changes.

Follow steps 3 through 5 above for `vCenter Flex-out Server` subflow found under
`/Library/CSA/3.2/Providers/vCenter/vCenter Flex Server Count/Subflows/`.

Legal Notices

Support

You can visit the HP Software support web site at:

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 software 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 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 an active support contract. To find more information about support access levels, go to the following URL:

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

To register for an HP Passport ID, go to the following URL:

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