Hewlett Packard Enterprise

Cloud Service Automation

Software version: 4.80.0002
For Microsoft Windows® and Linux operating systems

Patch Readme

Document release date : October 2018
Software release date : October 2017

Contents

Introduction

This readme describes the fixed issues and known issues in this patch and provides instructions for installing and configuring the patch on a Linux or Windows HPE Cloud Service Automation (CSA) server. The cumulative patch updates the CSA server to 04.80.0002.

What's new with this Patch?

- **ATTN:** It is important to take a backup of IdM database before you proceed with this patch installation and ensure that it is preserved for a later time. If you choose to uninstall this patch at a later time, CSA services will not come up till you revert back the IdM database to the older copy which was backed up prior to the patch installation

- **MPP provide users an option to renew a subscription before it expires.**

  This patch provides the ability to perpetually renew a particular subscription with restriction on the max term period. Please refer to the online help for further details.

- **Ability to set Subscription Start Time**

  With this patch we will be able to specify the Subscription Start Time, along with the Start Date.

- **New API for Request Handling**

  This API is used to submit a service request for creating a subscription, modifying a subscription, Issuing user actions on a subscription, cancelling a subscription, resubmitting a request based on an existing request.

  Please refer to **Appendix A** of the **Patch Read Me** file for further details.

- **Display the properties associated with public actions as part of the Service Request.**

  With this patch we will be able to view the properties which are changed as part of the public action in Service Request page as well as Review Request page (approver context)

- **It is now possible for a user to assign a group to which a user belongs to, but which has not been explicitly added to the access control of the organization.**

  For group ownership, the users could only select the groups which has been added to the access control of the organization. With this patch, there has a been a configurable parameter added by which it is now possible for a user to assign a group to which a user belongs to, but which has not been explicitly added to the access control of the organization.

  Please refer to **Appendix B** of the **Patch Read Me** file for further details.

- We have included a Tool named **Hotfix Deployer Tool**, to simplify the Deployment of hotfixes in this patch. The tool is available at %CSA_HOME%/hotfixes/hotfixDeployer directory.

  Please refer to **Appendix C** of the **Patch Read Me** file for further details.

- **Enhanced import mechanism, for service component template, enables to consume some of latest content capsules that were released post CSA 4.8 release.**

  This includes updates to vCenter, Amazon, Azure and Docker integrations.
  Please browse ITOM market place portal directly or through content store to see the full list with capsule specific version info.
  Please refer to individual capsule documentation for prerequisites, deployment instructions and use case details.

- **SAML Configuration steps are different from what is mentioned in CSA 4.8 Config guide.**

  Please refer to **Appendix D** for details.

  NOTE: If SAML is already configured in your system, you would need to do a couple of additional steps as part of SAML configuration after the patch installation.

Fixed Issues

The issues fixed with this patch are described in the table below.

Issue ID	Description
QCCR1D180247	Show properties on approval request
QCCR1D217764	“IdM Dependency (113302) - “ CSA does not accept LW-SSO tokens from other products
QCCR1D232619	Provide users an option to renew subscription before it expires
QCCR1D232984	CSA MPP API: need improvement on how to submit new request from MPP API
QCCR1D233226	Users are not able to select the group they are belong in Market place portal
QCCR1D233486	User is able to delete a service offering based on which there are active service instances and thus break the upgrade chain.
QCCR1D234559	MPP Regex validation passes on Modify page but fails during checkout.
QCCR1D234919	Email notifications display subscriber.userId where subscriber.name is used
QCCR1D235113	Ability to set Subscription Start Time
QCCR1D236020	[Idm dependency 237278] User is not able to login to admin/mpp portal after upgrading CSA to 4.7
QCCR1D236631	E-Mail Address RegEx does not allow TLDs with more than 2-4 chars (eg. energy)

QCCR1D236949	Fail to upgrade Service offering
QCCR1D237111	Check of permissions which user is having by groupmembership missing in 4.70
QCCR1D237221	State of the service instance is sometimes shown as deploying when service health is enabled
QCCR1D237393	CSA api/mpp/mpp-subscription - response - changes between CSA4.2 and CSA4.7
QCCR1D237824	Semantic validation is not working for user action
QCCR1D237993	[Idm dependency 115537] User is not able to login to MPP when secondary authentication is enabled
QCCR1D238038	Field Issue Regression -- Capability component Requirement is not working
QCCR1D238228	MPP API for get request gives a NPE for requests created for test deployments

Issue ID	Description
QCCR1D238260	Semantic Validation for null value does not throw the error message in the first attempt
QCCR1D238529	In CSA 4.8 MPP Portal, the subscription name is showing twice - see QCCR1D227772
QCCR1D238737	CSA Actions Stuck in Pending Deploying and Pending Transitioning States
QCCR1D239248	user/mycomponents API for a particular user returns the subscriptions details of other organization that the user does not belong to
QCCR1D239814	LDAP user unable to login after SAML Enabled.
QCCR1D239836	API call returning different information used for Group Ownership with 4.8
QCCR1D239935	Pause on error - notifications Receiving null values from propel
QCCR1D240122	MPP Cart is not working as expected
QCCR1D240196	JSPs with spaces in the name not laoding while ordering a subscription.
QCCR1D240506	CSA 4.70 - modifyable flag doesn't change anything for child option sets
QCCR1D240603	Data Integrity Violation exception thrown by OO Flow Execution Observer when the value of OO output parameter is more than 4000 characters

QCCR1D240633	Defect : maxFile option in mpp.json is not working
QCCR1D241223	Multiple attempts to update process instance exception seen with old style designs in 4.8
QCCR1D242441	CSA cluster duplicate events problem

Known issues

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

Issues	Description
QCCR1D234930	Problem : Cloud Optimizer is not able to get CSA Organization LDAP details after fixing existing security vulnerability in HPE CSA Cause : Code fix is completed to close the security vulnerability. Please ensure to pass the userIdenttifier to all the API calls as mentioned in CSA REST API Guide. Workaround : Hotfix available. Please contact support.
QCCR1D228812	Problem : The privacy statement does appear to show up on 4.8MR bits on the initial MPP login screen at /org/<ORG_NAME>. However, the next IDM screen you are navigated to when clicking **Log in** is where the issue lies. The screen apparently should, but does not show the privacy statement. Cause : Code defect. Workaround : The user could always manually go to the privacy link they have configured for the organizations privacy statement. This link is available in the **Organizations** > **Organization Name** > **General** **Settings** area. Or, the user could simply return back to the main portal login page to view the privacy link.
QCCR1D235507	Problem : Resuming a failed upgrade is failing on Oracle PCoE Environment because of the created_by and updated_by references in the scripts. Cause : Resuming a failed upgrade is failing and `csa\_CSA_4_80_0_installation\Logs\install.log` contains error message that `UPDATED_BY_ID` columns is missing For example error message from Oracle database: `PL/SQL: ORA-00904: "UPDATED_BY_ID": invalid identifier` Workaround : Restore the database from backup taken prior upgrade and resume the upgrade again.
QCCR1D227860	Problem : Exception in log file, csa.log Cause : A bug in NodeJS. See https://github.com/nodejs/node/issues/712 Workaround : A bug in NodeJS. See https://github.com/nodejs/node/issues/712
QCCR1D229293	Problem : Operation Orchestration displays: 403 Error when trying to use direct link from HPE CSA using menu Workflows -> Orchestration in case that LDAP Users does not Exist in OO.

Issues	Description
	Cause : Caused by defect QCCR8C32250 in product HPE Operation Orchestration Workaround : Modify URL of HPE Operation Orchestration to end with /oo/login/login-form or use seeded user admin for login to HPE CSA.
QCCR1D232747	Problem : When CSA is configured with HPSSO which is a default in 4.8 (documentation contains steps how to disable it for FIPS mode), it will fail to logout user from CSA when the user performs logout action in other integrated product like HPE OO followed by login as different user in HPE OO. HPSSO does not have central server to handle logout. Programs using HPSSO do not need to know each other as long as shared secret used for encryption and validation of cookie is same. Cause : In CSA the Management Console in csa.war uses IdM tokens as means to authenticate users. HPSSO tokens are recognized only by Identity Management (IdM) component, but not by CSA Management Console. When there is no session with Management console, the csa.war will redirect user to IdM which will validate and consume HPSSO cookie to produce IdM token for Management Console.CSA Management Console will perform logout when it is accessed while the HPSSO cookie is missing (due to logout in other product which deletes the cookie). But if CSA Management Console is accessed after logout followed by login in other product, then it will not detect the logout (it does not inspect cookie contents, it cannot decrypt it, in CSA only IdM component can decrypt it) and keep session established with original user identified by IdM token. Sessions are still limited by token expiration. IdM tokens expire after 30 minutes by default, though there is process to extend their lifetime if done within these 30 minutes. Workaround : Multiple options: • Turn off HPSSO if its functionality is not desirable. • Perform logout in CSA, not in HPE OO. • After performing logout in HPE OO, access HPE CSA so HPE CSA notices the cookie got deleted and it will perform logout, before continuing in to login as different user in HPE OO.
QCCR1D235119	Problem : upgrade fails with "Read timed out" during processing "`csa_remove_createdby_updatedby.plsql`" file on SQL Server (check `CSA\_CSA_4_80_0_installation\Logs\install.log` to ensure it) Cause : `csa_remove_createdby_updatedby.plsql` contains ALTER TABLE ... REBUILD statements that goes through all rows in table. So the REBUILD operation could timeout on huge databases. Workaround : 1. Edit CSA\scripts\mssql\csa_remove_createdby_updatedby.plsql and comment out all "

Issues	Description
	ALTER TABLE ... REBUILD" statements at the end of the file. You can comment it out by enclosing all REBUILD statements to /* and */ (SQL comments). Save the file. 2. Restart the upgrade process. It should end successfully. 3. After upgrade it is recommended to apply the commented REBUILD statements manually, For example, using Microsoft SQL Server Management Studio. **Note:** It could take several hours on big databases with millions of artifacts.
QCCR1D235209	Problem : If [CLIENT:<prop>] token is used as parameter value of semantic validation parameters, then test (validation) fails with following error message: Option property with the name <prop> is not found. If this refers to a new property, ensure that it is saved. Test fails even if the [CLIENT:<prop>] is used on property <prop> and user filled "Input Validation" input fields. **Note:** it is test issue only. In runtime tokens are resolved correctly. Cause : 1. If token [CLIENT:<prop>] is used as parameter value of validation parameter on user operation parameter <prop> and user filled Input Validation field input • It is caused by UI, which does not replaces the [CLIENT:<prop>] token with string entered to Input Validation input field. 2. If token [CLIENT:<prop>] refers to another parameter of user operation • It is caused by backend, which does not resolve tokens pointing to parameters of user operation when test is requested 3. If token [CLIENT:<prop>] refers option model property • Such token cannot be resolved because a. User operation does not have access to option model (e.g., user operation is on resource offering), b. Option model can define more than one property of the name, so it is not possible to identify the property Workaround : For all causes 1), 2), and 3) the workaround is * enter value instead of token [CLIENT:<prop>] used as user operation parameter value - once tested, change parameter value back to the token.
QCCR1D234010	Problem : The increment and decrement quantity field in Marketplace Portal shopping cart does not show increment/decrement buttons in Internet Explorer. Cause : Standard UI widget for number input type does not include increment/decrement buttons in Internet Explorer. Workaround : Enter quantity manually.
QCCR1D235356	Problem : CSA 4.8 Content Store, after installing the content from file system, if we try installing the same content through HPLN, it does not prompt for re-install dialog box in the first attempt. Cause : Product Limitation.

Issues	Description
	Workaround : 1. Install the content from file system. 2. Install the same content from the HPLN site (it will fail for the first time). 3. Re-attempt because all subsequent attempts to install the same content from HPLN site will succeed and the re-install dialog box will appear. Refresh the browser after every attempt in case the browser is slow or lagging.
QCCR1D235590	Problem : Import Preview fails while previewing the import of a design from an upgraded CSA instance into a fresh CSA 4.8 instance. Cause : A constraint violation is indicated in the Preview Workaround : Result of Import Preview can be ignored, and the design can be imported by clicking on Import
QCCR1D234938	Problem : CO URL in csa.war/dashboard/config.json file has changed to default value after Upgrade to CSA 4.8. Cause : Structural changes to the config.json file that is the New Dashboard changes Workaround : If you have made customizations to the config.json for the CSA launchpad/dashboard you will need to manually re-apply those after upgrade due to structural changes to the config.json file with the addition of the new interactive dashboard.
QCCR1D234038	Problem : SAML configuration is lost after upgrade to CSA 4.8 from CSA 4.7 Cause : Process Limitation Workaround : If SAML is configured in CSA 4.7 and you have upgraded to CSA 4.8, you need to configure SAML again.
QCCR1D225958	Problem : Missing data points when VM is powered OFF or Suspended. Cause : Unable to plot the graph for missing data points. Workaround : No workaround available.
QCCR1D228220	Problem : Health status is not updated for servers deployed on Helion Openstack (HOS) provider. Cause : CSA is unable to retrieve the health status since Cloud Optimizer (CO) is not supporting HOS 3.0. Workaround : It is a product limitation. No workaround available.
QCCR1D228619	Problem : Global search from MPP portal does not work in a Linux CSA installation. Cause : CSA Search service fails to update the Elasticsearch indices as a result of which Global search from MPP returns nothing Workaround : After CSA installation is complete, or after a CSA restart, stop the CSA Search service and restart it manually by following the steps below: If CSA was installed in a location other than /usr/local/hp/csa, adjust the path accordingly.

QCCR1D234418	Problem : Upgrade from 4.6 to 4.8 is failing for windows with MS-SQL database
	Cause : Snapshot Isolation not enabled for idm
	Workaround : For Microsoft SQL Server, it is mandatory to enable the snapshot isolation for Identity management database which can be achieved through following two database statements:
	`ALTER DATABASE idmdb SET ALLOW_SNAPSHOT_ISOLATION ON;`
	`ALTER DATABASE idmdb SET READ_COMMITTED_SNAPSHOT ON;`

Issues	Description
QCCR1D218883	Problem : Custom changes in Elasticsearch configuration may be discarded during an HA upgrade installation. Cause : Product defect. Workaround : Custom changes from upgraded installation are stored in a backup folder in /elasticsearch/config/. Transfer custom changes from the older installation file into the upgraded file.
QCCR1D227598	Problem : The SAML Authorization does not work if the access control is configured with the LDAP sub tree. Cause : CSA does not support the LDAP sub tree for Access Control (ACL) when SAML is enabled. Workaround : None
QCCR1D235063	Problem : "**Subscription Status**", "**Service Instance Status**", and "**Upgradable To**" fields go out of focus and get shifted to the bottom of the **Operations Overview** page. Cause : This is a Chrome browser issue in version 52 through version 55. Workaround : Use Chrome 56 and above version to avoid this problem.

QCCR1D234562	Problem : SMC login fails if we disable HP SSO configuration manually on CSA 4.8 HA
	Cause : Product limitation
	Workaround : Open the file $CSA-HOME\jboss-as\standalone\deployments\csa.war\WEB-INF\ applicationContext-security.xml and set checkSSOCookie value to false in the below mentioned
	section of bean and restart CSA service.
	`<beans:bean id="tokenValidityFilter"class="com.hp.csa.security. TokenValidityFilter">`
	`<beans:property name="checkSSOCookie" value="true"/>`
	`</beans:bean>`

QCCR1D230155	Problem : SMC portal does not get logged out upon HP SSO timeout. Cause : Product limitation. Workaround : No workaround currently available.
QCCR1D230605	Problem : Manage User Subscriptions under Administration of MPP lists few users unauthorized to access the MPP. Cause : Product limitation. Workaround : No workaround currently available.
QCCR1D235314	Problem : Even if the undeploy/unreserving actions fails during cancellation, the subscription will go offline. However the resources may not be completely deallocated. Cause : This is because of a limitation in the architecture that does not allow to pause/resume the failed actions during cancellation. Workaround : No workaround available.
QCCR1D232661	Problem : Currently we do not support hybrid Cloud Slang-AFL flows in any combination. Cause : It is a product limitation. Workaround : The procedure on 'Creating a topology Design with CloudSlang' is available in the Topology Components Guide (Whitepaper). Refer to this guide for a workaround information.
QCCR1D186068	Problem : When importing an Operations Orchestration flow in the Designs / Topology / Components area

Issues	Description
	of the Cloud Service Management Console, if that flow contains an Input property with Type value of List of Values and From value of Prompt User from List – Selection List, the resulting component imported into CSA will have a property value of type String for this Input property. Instead of a list of values from which one or more can be selected, a single text input will be presented to the user for this property in both the Components and Designer areas. Cause : The Designs / Topology / Components and Designs / Topology / Designer areas of the Cloud Service Management Console do not have graceful support for multi-select properties such as these. Workaround : In the text input for such a property, encode the property values using the appropriate delimiter, which is determined by the method the flow uses to parse the Input property. If the flow uses the Selection List Iterate operation that is provided with the Base content pack in Operations Orchestration, the delimiter (separator) is configurable and has a default of '|'. For example, the values 'red', 'green', and 'blue' would be specified as 'red|green|blue' (unquoted) if using the Selection List Iterate operation with the default separator value.
QCCR1D187711	Problem : Topology components imported from Chef include an attributes parameter in their deploy operation, allowing customization of the provisioning of the Chef recipe. Properties passed in the attributes parameter are automatically converted to Strings. For example, an Integer component property of 3306 will be converted to "3306", and a Boolean component property of true will be converted to "true". If the Chef recipe is written to expect an Integer or Boolean input and not a String, the provisioning of the component will fail. Cause : Product limitation. Workaround : The Chef recipe should be written or modified to expect String inputs.
CR1D226494	Problem : The Featured Category list is empty for a newly created organization. Cause : The organization data synchronization is not complete after a new organization is created in IDM tables. Workaround : After the synchronization is completed, the catalogs and featured category list will appear. (~30 seconds)
QCCR1D233354	Problem : In MPP Service checkout page for an offering, the group list shows only the DNs that are added in the access control of the organization, it does not list all the groups to which the user belongs in LDAP.

Issues	Description
	Cause : This behavior is currently unsupported in CSA. In order to show the group in group list, all the groups need to be explicitly mentioned in the organization access control. Workaround : None.
QCCR1D234644	Problem : Misleading icon displayed in MPP. If an organization is set to Pause Subscriptions on Provisioning error and a subscription fails, MPP shows right status as Paused but the icon is wrong. Spinner is displayed in MPP instead of Pause icon. Cause : Wrong HTML in MPP code base. Workaround : No workaround is required. Inappropriate icon is displayed.
QCCR1D228672	Problem : Cannot launch the show performance page using SSO from MPP. Cause : SSO token is not passed correctly. Workaround : User can login to Cloud Optimizer manually by entering username and password.

Patch Installation

This section describes how to install the patch.

Note: If there are any customized configurations/folders present, ensure you take a backup of those files/directories and restore them back after installing the patch.

Check Pre-installation Requirements

Ensure the below prerequisites are fulfilled before installing:

1. Check minimum hardware requirements:
    - CPU: 4 CPU, 3.0 GHz
    - RAM: 8 GB
    - Hard Drive: 20 GB
2. Check the **CSA 4.80 Support Matrix** to verify operating-system requirements.
3. Check minimum software requirements:
    - CSA version 4.80.0000
4. Set the CSA_HOME environment variable:

    In case of remote MPP installation, please ensure that CSA_HOME environment variable is set.
    - Windows: Set the CSA_HOME environment variable to point to the CSA installed location.
      Eg: C:\Program Files\HPE\CSA
    - Linux: Set the CSA_HOME environment variable to point to the CSA installed location
      Eg: /usr/local/hpe/csa

5. **Back up your CSA environment.**

    Please make sure to take backup of CSA and IdM databases. There are some schema changes in the IdM database because of which patch uninstallation will not bring the system back to the previous state.

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: HPE Cloud Service Automation, HPE Marketplace Portal, HPE Search Service and Elasticsearch 1.6.1 (elasticsearch-service-x64).

   Important: You must stop these services on each node in a cluster.
   Note: If you do not stop these services manually, the following folders will not be cleared and will cause UI issues after installing the patch:

   Windows: `<CSA_HOME>\jboss-as\standalone\tmp`
   Clustered environment: `<CSA_HOME>\jboss-as\domain\tmp`
   Linux: `/usr/local/hpe/csa/jboss-as/standalone/tmp`

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_00049
   - **Windows**: https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/LID/CSA_00050

2. Connect to your respective IdM database, and create the procedure mentioned below and execute the same.
   - Oracle
   - PostgreSQL
   - SQL

Oracle:

```
--------------------------------------------------------------------------------------------------------------------------------
--Create Produce IDM_SP_REMOVE_DUPLICATE_USER which will remove all the duplicate users in IdM
--------------------------------------------------------------------------------------------------------------------------------
create or replace PROCEDURE IDM_SP_REMOVE_DUPLICATE_USER
AS
  v_user_id VARCHAR2(32);
  v_user_name_key VARCHAR2(2000);
  TYPE USER_ARRAY IS TABLE OF VARCHAR2(2000) INDEX BY VARCHAR(2000);
  v_user_name_list USER_ARRAY;
BEGIN
 DBMS_OUTPUT.enable(20000);
  FOR u IN (
   SELECT u1.organization org_id, u1.uuid user_id, u1.DELETED, u1.name user_name FROM abstract_user u1, (
      SELECT organization, name, DELETED FROM abstract_user GROUP BY organization, name, DELETED HAVING
count(*) > 1
   ) u2
   WHERE u1.organization=u2.organization AND u1.name=u2.name AND nvl(u1.deleted, 'NULL') = nvl(u2.deleted, 'NULL')
ORDER BY CREATED_DATE DESC
  ) LOOP
  DBMS_OUTPUT.put_line(u.org_id||', user='||u.user_name);
    v_user_name_key := u.org_id || '#' || u.user_name;
  IF v_user_name_list.EXISTS(v_user_name_key)
   THEN

     dbms_output.put_line('Deleting Duplicat user: ' || u.org_id || ', user_id=' || u.user_id || ', user_name=' ||
u.user_name );

      DELETE FROM ABSTRACT_USER_METADATA WHERE uuid = u.user_id;
      DELETE FROM ABSTRACT_USER_REPRESENTATION WHERE USER_FK = u.user_id;
      DELETE FROM ABSTRACT_USER_PROFILE WHERE user_id = u.user_id;
      DELETE FROM USER_GROUP_DATABASE_REP WHERE user_id = u.user_id;
      DELETE FROM USER_GROUP_REP WHERE user_id = u.user_id;
      DELETE FROM ABSTRACT_USER WHERE uuid = u.user_id;
```

```
   ELSE
      dbms_output.put_line('Skipping');
      v_user_name_list(v_user_name_key) := v_user_name_key;
   END IF;
  END LOOP;
END;
```

PostgreSQL:

```
CREATE OR REPLACE FUNCTION IDM_SP_REMOVE_DUPLICATE_USER()
RETURNS integer AS $$
DECLARE
  v_user_id VARCHAR(32);
  v_user_name_key VARCHAR(2000);
  v_user_name_list VARCHAR(2000)[];
  u record;
  delete_count int;
BEGIN
 delete_count:=0;
 FOR u IN (
  SELECT u1.organization org_id, u1.uuid user_id, u1.DELETED, u1.name user_name FROM abstract_user u1, (
     SELECT organization, name, DELETED FROM abstract_user GROUP BY organization, name, DELETED HAVING
count(*) > 1
  ) u2
  WHERE u1.organization=u2.organization AND u1.name=u2.name AND u1.deleted is NULL and u2.deleted is NULL
ORDER BY CREATED_DATE DESC
 ) LOOP
      v_user_name_key := u.org_id || '#' || u.user_name;

  IF v_user_name_key=any(v_user_name_list)
  THEN
     DELETE FROM ABSTRACT_USER_METADATA WHERE uuid = u.user_id;
     DELETE FROM ABSTRACT_USER_REPRESENTATION WHERE USER_FK = u.user_id;
     DELETE FROM ABSTRACT_USER_PROFILE WHERE user_id = u.user_id;
     DELETE FROM USER_GROUP_DATABASE_REP WHERE user_id = u.user_id;
     DELETE FROM USER_GROUP_REP WHERE user_id = u.user_id;
     DELETE FROM ABSTRACT_USER WHERE uuid = u.user_id;
                  delete_count:=delete_count+1;
  ELSE
     v_user_name_list:=v_user_name_list ||v_user_name_key;
  END IF;
 END LOOP;
 return delete_count;
END; $$
LANGUAGE 'plpgsql';
select IDM_SP_REMOVE_DUPLICATE_USER();
DROP FUNCTION IF EXISTS IDM_SP_REMOVE_DUPLICATE_USER;
```

SQL:

```
create PROCEDURE  IDM_SP_REMOVE_DUPLICATE_USER
AS
```

```
 DECLARE
  @v_first BIT,
  @v_prv_username NVARCHAR(1024),
  @v_username NVARCHAR(1024),
 @v_user_id NVARCHAR(1024)
 DECLARE
  v_cur_fk CURSOR FOR
  SELECT u1.name user_name, u1.uuid user_id FROM abstract_user u1, (
      SELECT organization, name, DELETED FROM abstract_user GROUP BY organization, name, DELETED HAVING
count(*) > 1
    ) u2
    WHERE u1.organization=u2.organization AND u1.name=u2.name AND ISNULL(u1.deleted, 'NULL') =
ISNULL(u2.deleted, 'NULL') ORDER BY u1.name, CREATED_DATE ASC
BEGIN
 SET @v_first = 1;
 OPEN v_cur_fk;
 FETCH NEXT FROM v_cur_fk INTO @v_username, @v_user_id;
 WHILE @@FETCH_STATUS = 0
 BEGIN
  IF @v_prv_username IS NULL
  BEGIN
   SET @v_prv_username = @v_username;
  END

  IF @v_prv_username != @v_username
  BEGIN
   SET @v_first = 1
  END

  IF @v_first=1
  BEGIN
   SET @v_first = 0
  END
  ELSE
  BEGIN

    print 'Remove user: '+ @v_username +', '+ @v_user_id;

    DELETE FROM ABSTRACT_USER_METADATA WHERE uuid = @v_user_id;
    DELETE FROM ABSTRACT_USER_REPRESENTATION WHERE USER_FK = @v_user_id;
    DELETE FROM ABSTRACT_USER_PROFILE WHERE user_id = @v_user_id;
    DELETE FROM USER_GROUP_DATABASE_REP WHERE user_id = @v_user_id;
    DELETE FROM USER_GROUP_REP WHERE user_id = @v_user_id;
    DELETE FROM ABSTRACT_USER WHERE uuid = @v_user_id;
  END;--Cleanup user

  SET @v_prv_username = @v_username;
  FETCH NEXT FROM v_cur_fk INTO @v_username, @v_user_id;
 END ---END LOPP
 CLOSE v_cur_fk;
 DEALLOCATE v_cur_fk;
END
```

```
go
exec IDM_SP_REMOVE_DUPLICATE_USER
go
drop procedure  IDM_SP_REMOVE_DUPLICATE_USER
go
```

For Linux:

Note: For clusters, perform all steps on each node in a cluster.

a. Extract the downloaded file: `HPE_CSA_Patch_04.80.0002.bin` file from the patch file.

b. Ensure that the `csauser` user is the owner of the file and has full privileges.

c. Log in as `csauser` and run `HPE_CSA_Patch_04.80.0002.bin` to open the CSA patch installer console mode.

d. Enter `./HPE_CSA_Patch_04.80.0002.bin` to run the patch installer and respond to the warning message on backing up the installation folder.

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. The installer will prompt for the password of CSA Database user.

j. A second prompt will appear to ensure that the IdM Database has been backed up. In case the user uninstall the patch, it is required to import back the older IdM DB for CSA to be functional.

k. In the pre-installation summary dialog screen, click **Enter**.

The patch installer begins the installation.

l. When prompted, click **Enter** to exit the installation.

m. (Optional) If you want to install the new CI Type-based capsules from ITOM Marketplace, perform this step: The patch installer will deploy a zip file named CC-HPE-CSA-CIType-Palette.zip in the following path: `<CSA_HOME>\_CSA_4_80_2_installation\Backup\Tools\CSLContentInstaller\`. Run the capsule installer `csl-content-installer.jar` from the above path in silent mode and point to this jar file to import/install the same to central. Refer the *Capsule Installer Guide* for help.

After completing step 'm', you can proceed with installation of capsules.

For Windows:

a. Extract the `HP_CSA_Patch_04.80.0002.exe` file from the patch zip file.

b. Run `HP_CSA_Patch_04.80.0002.exe` to launch the installation wizard and respond to the warning message on backing up the installation folder.

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. The installer will prompt for the password of CSA Database user.

g. A second prompt will appear to ensure that the IdM database has been backed up. In case the user uninstall the patch it is important to bring back the older IdM DB for CSA to be functional.

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

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

j. (Optional) If you want to install the new CI Type-based capsules from ITOM Marketplace, perform this step: The patch installer will deploy a zip file named CC-HPE-CSA-CIType-Palette.zip in the following path: `<CSA_HOME>\_CSA_4_80_2_installation\Backup\Tools\CSLContentInstaller\`. Run the capsule installer `csl-content-installer.jar` from the above path in silent mode and point to this jar file to import/install the same to central. Refer the *Capsule Installer Guide* for help.

After completing step 'j', you can proceed with installation of capsules.

Verify the Patch 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_80_2_installation\Logs`
   - **Linux:** `$CSA_HOME/_CSA_4_80_2_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 HPE Support.
2. Clear the browser cache.
3. Ensure the HPE Cloud Service Automation, Marketplace Portal, HPE Search, and Elasticsearch services 1.6.1 (elasticsearch-service-x64) 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.

Patch Removal - Linux

This section provides the steps to uninstall the patch on a Linux server in both standalone and clustered environments.

Note: Uninstallation of the patch will not revert the database-indexing changes made during patch installation.

As a result after the patch uninstallation, users will not be able to login to CSA or MPP portals till we manually import the IdM database which we had backed up before patch installation.

Before Uninstalling the Patch

Complete the following preparation steps before you uninstall the patch:

1. Backup the CSA environment.

2. Stop new subscription creation and subscription modification.

   Warning: If you do not stop creation and modification, uninstallation 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: HPE Cloud Service Automation, HPE Marketplace Portal, HPE Search Service, and Elasticsearch 1.6.1 (elasticsearch-service-x64).

   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_80_2_installation/Uninstaller`.
2. Run `./Uninstall HPE Cloud Service Automation Patch` to start the uninstaller console mode.
3. A prompt will appear to enforce the need to import the IdM database which was backed up before the patch installation, for CSA to be functional.
4. Click **Enter** for the introductory and warning screens.
5. Click **Enter** to run the patch uninstaller.
6. When the patch uninstallation is complete, click **Enter** to exit the uninstallation process.
7. **Manually import the IdM database which we had backed up earlier before the patch installation.**

Patch Removal - Windows

This section provides the steps to uninstall the patch on a Windows server in both standalone and clustered environments.

Note: Uninstallation of the patch will not revert the database-indexing changes made during patch installation.

As a result after the patch uninstallation, users will not be able to login to CSA or MPP portals till we manually import the IdM database which we had backed up before patch installation.

Before Uninstalling the Patch

Complete the following preparation steps before you uninstall the patch:

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

   Warning: If you do not stop creation and modification, the uninstallation 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: HPE Cloud Service Automation, HPE Marketplace Portal, HPE Search Service, and Elasticsearch 1.6.1 (elasticsearch-service-x64).

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

Uninstalling the Patch on Standalone and Clustered Environments

You can uninstall the patch using either of the following methods:

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

Note: For clustered environments, 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_80_2_installation\Uninstaller`.
2. Execute `Uninstall HPE Cloud Service Automation Patch.exe` to open the Uninstall Cloud Service Automation Patch wizard.
3. A prompt will appear to enforce the need to import the IdM database which was backed up before the patch installation
4. Click **Uninstall** to uninstall the patch.
5. Click **Done** to exit the uninstall wizard.
5. **Manually import the IdM database which we had backed up earlier before the patch installation.**

Patch Removal Verification

After uninstalling the patch, perform the following steps to verify the patch was removed. These verification steps apply to both standalone and clustered environments.

Note: For clustered environments, complete these steps on each node.

1. Check for errors in the log files:
    - **Windows:** `<CSA_HOME>\_CSA_4_80_2_installation\Logs`
    - **Linux:** `$CSA_HOME/_CSA_4_80_2_installation/Logs`
      Log files include `csa_uninstall.log`, and `csa_unInstallPatch.log`.

    Note: If there are errors, create a backup of the log files, restore the backup of the `CSA_HOME` directory, and contact HPE Support.
2. Clear the browser cache.
3. Ensure the HPE Cloud Service Automation, Marketplace Portal, HPE Search, and Elasticsearch 1.6.1 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>/CSAKit-4.7/Content Archives/topology/Jenkins plugin/HPE_Codar.hpi
<CSA_HOME>/Tools/CSLContentInstaller/existing-infra.zip
<CSA_HOME>/Tools/CSLContentInstaller/CC-HPE-CSA-CIType-Palette.zip
<CSA_HOME>/Tools/CSLContentInstaller/csl-content-installer.jar
<CSA_HOME>/Tools/SupportabilityTools/*
<CSA_HOME>/ Tools/OGUpdateTool/*
<CSA_HOME>/Tools/lib/CLI-lib.jar
<CSA_HOME>/Hotfixes/*
<Deployments_home>/csa-codar-provider-help.war/en_US/*
<Deployments_home>/csa-provider-help.war/en_US/*
<Deployments_home>/codar-provider-help.war/en_US/*
<CSA_HOME>/portal/node_modules/mpp-ui/dist/ccue-marketplaceportal-help/help/en_US/*

Appendix A

Simplified API

Simplified APIs are a new set of user friendly REST APIs.

Service Request API

Service Request API is a simplified API for handling requests. You can use this API to:

- Submit a service request to create, modify or cancel a subscription.
- Issue user actions on a subscription,
- Resubmit a modify request that has failed
- Submit a request based on an existing request.

Features

Service Request API has the following features:

- To make the API portable across different environment, you can reference the Option Sets, Options and Properties by their display names instead of IDs.
- Inputs are specified in the following hierarchy: Option Set -> Option -> Property.
- For child Option Sets nested within an Option Property, it is not necessary to maintain the hierarchy. The Option Sets are flat array regardless of whether the Option Set is at the top level or nested.
- You can reference the Option Sets, Options and Properties by their display names.
- Instead of passing all option properties to the request body, you can pass only the options that are selected and the properties that have values different form the default value.
- The API has thorough error handling capabilities with clear error codes. A detailed message about the problem is provided so that the caller can take corrective action.
- The API thoroughly validates the request body input and sends errors with details.
- APIs are versioned according to the semantic versioning scheme.

NOTE: Please refer to the CSA API Guide for more details.

Appendix B

For group ownership, the users could only select the groups which has been added to the access control of the organization. With this patch, there has a been a configurable parameter added by which it is now possible for a user to assign a group to which a user belongs to, but which has not been explicitly added to the access control of the organization.

e.g. Consider a user is part of cn=devGroup,dc=myorg,dc=com, cn=demoGroup,dc=myorg,dc=com and cn=innoGroup,dc=myorg,dc=com

If the access has been provided only to cn=devGroup,dc=myorg, the subscriber will not see the groups demoGroup, innoGroup while selecting the groups for group owned subscription as per the earlier behaviour.

With this patch, the subscribers will be able to see all the 3 groups while creating a group owned subscription. Other subscribers, who have access to CSA and is also part of any of the selected group, will be able to access the subscription.

If you are not already using "group ownership" feature, you need to follow the below steps to enable this feature:

For customers with no group owned subscriptions,

- The following configuration needs to be added to the csa.properties.
  listAllUserLDAPGroups=true.

- Clear the CSA_USER_GROUP table in the CSA database.

- After Subsequent login, the group ownership drop down option will list all the groups the user belongs to.

If you are are already using "group ownership" feature, please follow the below steps to enable this new behaviour.

- Convert the existing data by executing a tool which will convert the canonical name of the group to the "Distinguished Name" of the group as listed below:

  [CSA_HOME] \Tools\OGUpdateTool> java –jar og-update-tool.jar –c config.properties [-j (driver).jar]

  The details required to configure the parameters in the config file can be referred here.

- To enable this feature, the following configuration needs to be added to the csa.properties file.
  listAllUserLDAPGroups=true

- Clear the CSA_USER_GROUP table in the CSA database.

- After Subsequent login, the group ownership drop down option will list all the groups that the user belongs to.

Once the configuration is changed, the OWNER_GROUP field in the CSA_SERVICE_SUBSCR table will now store the group name as distinguished name (In earlier releases, it was stored as canonical name).

NOTE: If you wish to exclude groups from being listed in the group ownership drop down option, the following property needs to be added to csa.properties file.

userLDAPGroupExclusionList= [{dn of the group}, {dn of the group}]

For example:
userLDAPGroupExclusionList=[{cn=group1,ou=myou,dc=myorg,dc=com},{ cn=group2,cn=mygroups,dc=myorg,dc=com }]

Appendix C

How to Use the HotfixDeployer tool

Windows:

a) Place the hotfixes zip files inside %CSA_HOME% /hotfixes folder.
b) Open a command prompt to the %CSA_HOME% /hotfixes/hotfixDeployer directory.

To deploy a fix :
../../node.js/node hotfixManger.js -deploy "hotfixName.zip"

e.g. C:\Program Files\HPE\CSA\hotfixes\hotfixDeployer>../../node.js/node hotfixManger.js –deploy QCCR1D23451.zip >> <QCCR ID>.zip

To undeploy the fix :

../../node.js/node hotfixManger.js -undeploy "hotfixName"

e.g. C:\Program Files\HPE\CSA\hotfixes\hotfixDeployer>../../node.js/node hotfixManger.js -undeploy QCCR1D23451 >> <QCCR ID>

List the hotfixes deployed:

../../node.js/node hotfixManger.js –list

List all the hotfixes – deployed and undeployed

../../node.js/node hotfixManger.js -listAll

Help - Displays the list of commands supported and their syntax
../../node.js/node hotfixManger.js -help

Linux:

a) Place the hotfixes zip files inside %CSA_HOME% /hotfixes folder.
b) Open a command prompt to the %CSA_HOME% /hotfixes/hotfixDeployer directory.

To deploy a fix :

../../node.js/bin/node hotfixManger.js -deploy "hotfixName.tar" >> hotfiName.zip

e.g. $../../node.js/bin/node hotfixManger.js -deploy QCCR1D23451.tar >> <QCCR ID>.zip

To undeploy the fix :
../../node.js/node hotfixManger.js -undeploy "hotfixName"
e.g. $../../node.js/node hotfixManger.js -undeploy QCCR1D23451 >> <QCCR ID>

List the hotfixes deployed:
../../node.js/bin/node hotfixManger.js -list

List all the hotfixes – deployed and undeployed
../../node.js/bin/node hotfixManger.js -listAll

Help - Displays the list of commands supported and their syntax
../../node.js/bin/node hotfixManger.js -help

Appendix D

SAML Configuration steps are different from what is mentioned in CSA 4.8 Configuration guide.

If SAML is already configured in your system, you can skip other steps and need to follow **Step 3** alone.

For fresh configuration of SAML, please follow the below steps:

Step 1) Follow the steps mentioned in **CSA 4.8 Configuration guide** and configure SAML. We can exclude Step 5 and Step 6 of the Configuration Guide under the heading **SAML Configuration on a CSA Fresh Install** since it is already taken care from IDM.

Step 2) Make sure that the certificate of your Identity Provider is **imported** in IDM as mentioned in the **CSA 4.8 Configuration guide** under the heading **Exporting the ADFS Certificate and Importingthe Certificate in Identity Management component.**

Step 3) There are two ways by which we can update SAML related system properties.

Method 1: Using json file to update the idm.auth.flow property for missing organizations.

Method 2: Using REST API to update the idm.auth.flow property for missing organizations

Method 1: Update SAML related system properties using JSON File:

- Copy sample json file (com.hpe.tenant1__1.2.0.1__Update_Metadata.json.template) from "{CSA install DIR}\jboss-as\standalone\deployments\idm-service.war\WEB-INF\classes\seeded\samples" to "{CSA install DIR} \jboss-as\standalone\deployments\idm-service.war\WEB-INF\classes\seeded" directory.
- Rename the copied file to "com.hpe.tenant1__1.2.0.1__Update_Metadata.json".

- Open the json file in an editor.
- Remove the entire content of the file and add the below content inside the file:

```
[
{
"operation":"ADD_OR_UPDATE",
"type":"organizationMetadata",
"names":{
"organizationName":"CUSTOM ORG1"
},
"attributes":{
"key":"idm.auth.flow",
"value":"seeded,database_user,ldap,ad,jaas,saml",
"public":true
}
}
]
```

- Restart CSA services.
- After successful restart of CSA services, under organization->**selected_org->ldap**, configure ldap details for your AD.
- In access control add the groups.

When you access the organization portal, you will be directed to an ADFS login page. Use valid user credentials to log on to your consumer portal.

Method 2: Update SAML related system properties using REST API:

After the patch installation, we need to execute the following PUT API call to add the idm.auth.flow property for the existing and new organizations.

Property Name	Type of REST API	URL	Request/Response Body

idm.auth.flow	PUT	https://sen_winsql2012.csacloud.local:8444/idm-service//api/scim/organizations/8a828ea15ad63008015ad64a36c0000f/metadata/idm.auth.flow	{
			"key": "idm.auth.flow",
			"value": "seeded,database_user,ldap,ad,jaas,saml",
			"public": true
			}
			Output of the REST Call should be(Ex: Below):
			{
			"key": "idm.auth.flow",
			"value": "seeded,database_user,ldap,ad,jaas,saml",
			"public": true,
			"id":

Property Name	Type of REST API	URL	Request/Response Body
			"8a828dad5f1430c9015f145aa8c90059" }

After successful execution of the above query,

- Restart CSA services for SAML to work.
- After successful restart of CSA services, under organization->**selected_org->ldap**, configure ldap details for your AD.
- In access control add the groups.

When you access the organization portal, you will be directed to an ADFS login page. Use valid user credentials to log on to your consumer portal.

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 Enterprise 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 Enterprise 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 Enterprise 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 the following URL and sign-in or register:
https://softwaresupport.hpe.com.
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 Enterprise sales representative for details.

Support

Visit the Hewlett Packard Enterprise Software Support Online web site at https://softwaresupport.hpe.com.