HP IT Operations Compliance

Software Version: 1.10

-

Integration Guide

Document Release Date: September 2015
Software Release Date: September 2015

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

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

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

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

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

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

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

Support

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

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

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

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

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

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

To find more information about access levels, go to:

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

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

Contents

Chapter 1: ITOC-SA Integration

This section discusses the use of HP IT Operations Compliance (ITOC) with HP Server Automation (SA). ITOC leverages SA agents and gateway for remote execution.

ITOC-SA Integration Overview

ITOC has a remote execution path that uses Salt agents to perform compliance scans on target servers. SA also has its own agents that perform remote execution on target managed devices. For customers who already have SA agents installed and want to use ITOC to apply compliance on the same managed devices, ITOC can delegate remote execution through SA agents instead of installing additional ITOC agents on the servers.

The ITOC Resource Manager Adapter delegates the responsibilities to SA to execute scripts remotely. The Resource Manager Adapter sends ITOC scanning and remediation jobs to SA and triggers Run Server Script jobs in SA.

Prerequisites

The following items are required to integrate ITOC with SA:

- Install ITOC version 1.10 using the **HP IT Operations Compliance Installation, User, and Setup Guide**. Install SA version 10.2 and later using the ***HP SA Installation Guide***.
- SA version 10.20 or later.
- Data Center Automation Appliance (DCAA) version 1.0 with SSH enabled.

The Resource Manager Adapter should match SA core server support and agent support.

Resource Manager Adapter Support Matrix

	SA 10.20 Core Server Support	ITOC 1.00 Server Support	ITOC 1.10 Agent Support	Adapter Support	DCAA 1.0 with SSH Enabled
RHEL 5	Yes	-	Yes	Yes	-
RHEL 6	Yes	Yes	Yes	Yes	-
RHEL 7	-	Yes	Yes	-	-
OEL 6	Yes	Yes	Yes	Yes	-
OEL 7	-	Yes	Yes	-	-

	SA 10.20 Core Server Support	ITOC 1.00 Server Support	ITOC 1.10 Agent Support	Adapter Support	DCAA 1.0 with SSH Enabled
CentOS 6.4	-	Yes	Yes	-	-
CentOS 6.5 x64	-	-	-	-	Yes
CentOS 7	-	Yes	Yes	-	-
SLES 11	Yes	-	-	Yes	-
Ubuntu 12.04	-	-	Yes	-	-
Ubuntu 14.04	-	-	Yes	-	-

Prerequisites for Installing the Resource Adapter

You must install an agent before you install the Resource Adapter. If you install the adapter before you install the agent, agent installation will fail.

For an SA core installed using non-root user, the ITOC agent and adapter need to be installed manually. For more information, see "Install Agents on Resources Manually" in the **HP IT Operations Compliance Installation, Setup, and Upgrade Guide** and Install the ITOC Agent and the Adapter to SA Using the adapter_easy_install.sh Script.

For information about installing an agent, see "Install an Agent on a Resource" in the **HP IT Operations Compliance User Guide** for instructions on how to install the agent through the UI.

Install the ITOC Agent and the Adapter to SA Using the adapter_easy_install.sh Script

1. From the ITOC server, locate the `adapter_easy_install.sh` script in the `<itoc_install_directory>/adapters/packages/sa` directory.
2. From the ITOC server, run the `adapter_easy_install.sh` script.
   Provide the SSH credential and SSH port of the SA Slice host.
3. The `adapter_easy_install.sh script` will complete the installation of the ITOC agent to SA Slice, register the ITOC agent, install the adapter to the SA slice, and generate the key for the adapter in phases.

Install the ITOC Agent and Adapter Manually to SA

1. Specify the SA hostname, SSH port, and SSH credential.
2. Copy the appropriate agent platform package from the `<itoc_install_directory>/salt/srv/salt` directory on the ITOC server to the SA Slice host where you plan to install the adapter.
3. Copy the `ITOC_SA_Lite-version_num` package from `<itoc_install_directory>/adapters/packages/sa` on the ITOC server to the SA Slice host.
4. On the SA Slice, create a directory; for example, `/opt/hp/itoc`. Ensure that the user who installs the agent in the next step has **Read**, **Write**, and **Execute** permissions on this directory.
5. From the SA Slice, install the agent:
   `./<platform>_minion-version -- -d <full_path> -f <itoc_server_FQDN>`
6. From the ITOC server, register the agent installed in step 5:
   `<itoc_install_directory>/scripts/minion_reg.sh -a <agent_key>`
7. From the SA Slice, `cd` to the directory to which the packages were copied. Run the following command to install the adapter:
   `./ITOC_SA_Lite<-ver_num> -- -d <agent_install_directory>/adapter -f <SA_Slice_Host_FQDN>`

   Note: A path relative to the agent install path must to be specified in the `-d` option.

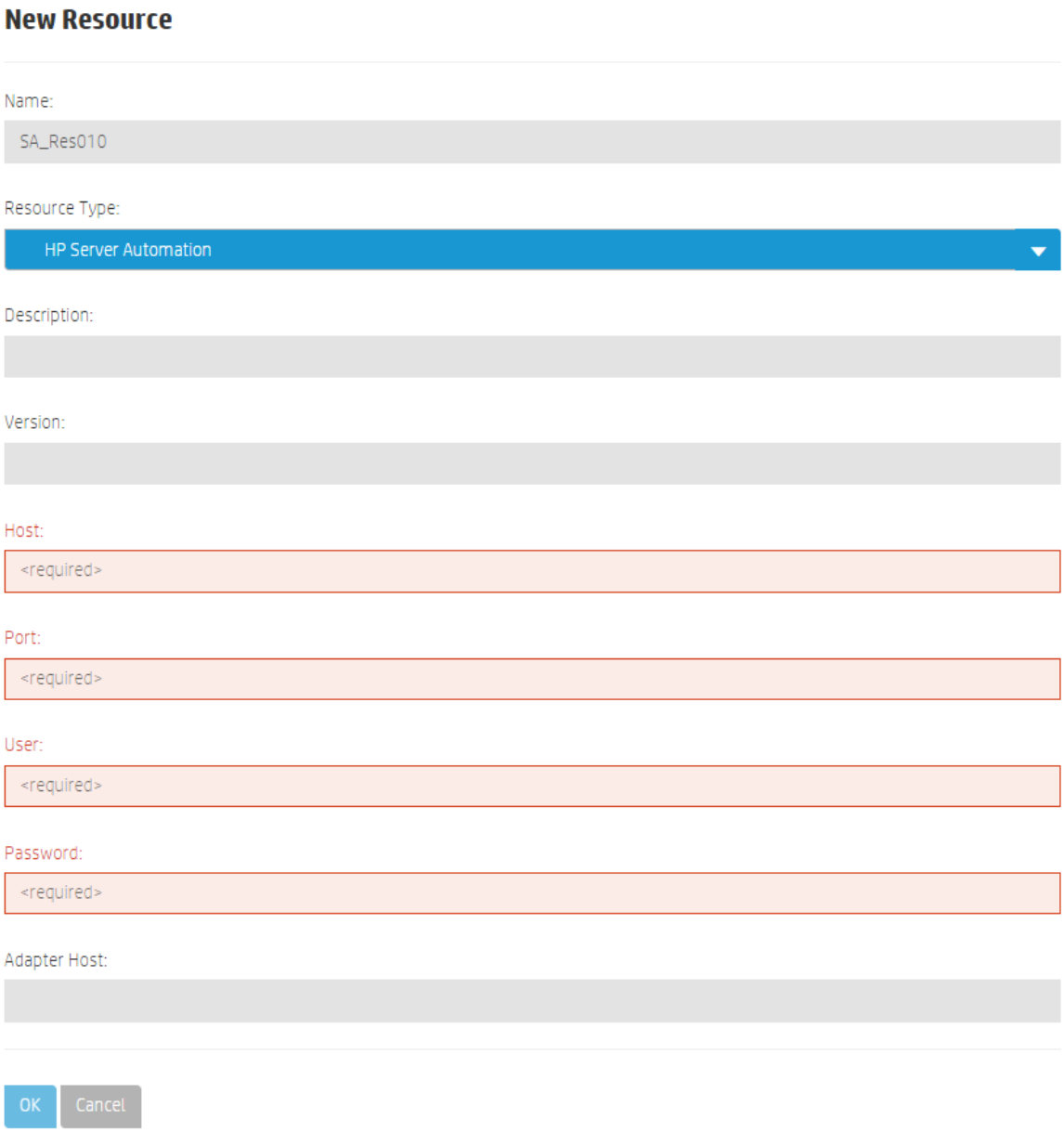
   Note: The end directory of adapter installation path must be `adapter`, as shown in step 7.
8. From the SA Slice, copy the public key in the `<SA_Slice Hostname>-public.pem` file from the `<agent_install_directory>/adapter` directory (as the file or copy the file content from `stdout`) to the ITOC server directory: `<itoc_install_directory>/adapters/keys`

Create a Resource Manager - SA

1. Log in to ITOC as a user with the Business Administrators role.
2. Navigate to the **Resource Managers** list under the Administration tab.
3. From **Actions**, select **New Resource Manager**.
4. The **New Resource Manager** dialog appears:

   Complete the following fields:

- **Name:** (required) - User-specified name.
- **Resource Type:** (required) - Select **HP Server Automation**. The following example shows the fields for an **HP Server Automation** resource:



Enter resource attribute information:

  - **Description:** (optional) - A detailed description of the SA core with which you are integrating.
  - **Version:** (optional) - The SA version being used.
  - **Host:** (required) - The hostname for the SA Core. This hostname matches the hostname registered with the Salt server.

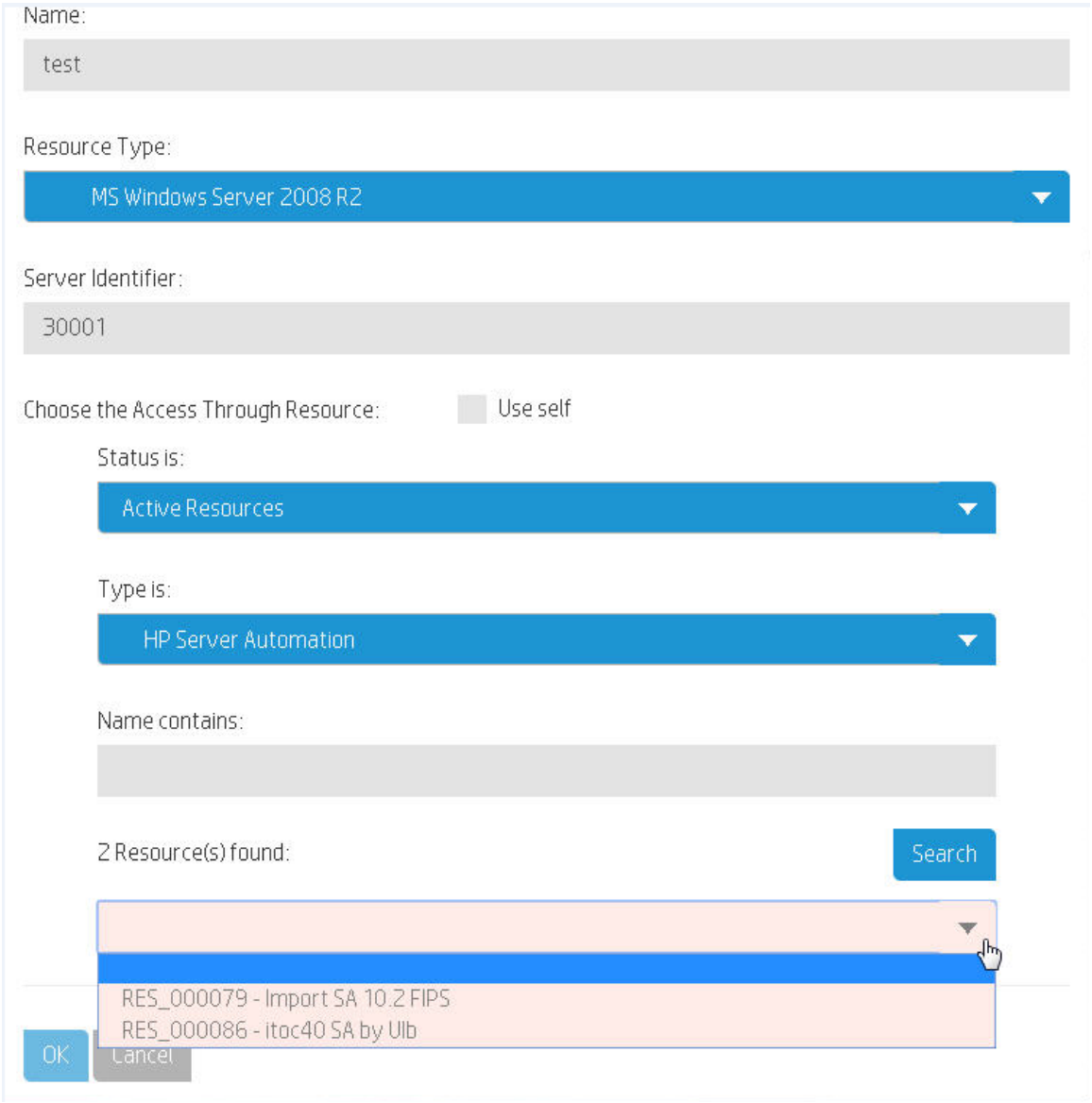
> **Note:** Make sure the value you enter in the Host field matches exactly to the value you specified for the Slice Hostname during adapter installation.

- **Port:** (required) - The port of the SA Slice's configuration gateway tunnel port. The default is 443.
- **User:** (required) - An SA Integration User with the following permissions:
  - Run Ad hoc scripts.
  - Run Ad hoc & Saved Server Scripts as Super User.
  - Managed Servers and Groups
  - Read and write permission on the resource (facility, customer, or device group) to which the managed server belongs.
- **Password:** (required) - SA user password.
- **Adapter Host:** (optional) - The host on which the adapter is installed. If this information is not provided, the default is the SA Core hostname provided above.

Create a Resource Managed by SA in ITOC

Create a resource for the server that is managed by SA in ITOC.

1. Navigate to the **Resources** list.
2. Click **Actions**, and select **New Resource**.
3. The **New Resource** dialog appears:
   - **Name** - Name of the server.
   - **Resource Type** - The OS platform of the SA managed server.
   - **Server Identifier** - The object ID of the managed server in SA.
   - **Choose the Access Through Resource:** - Uncheck the **Use self** box.
   - **Type is:** Choose **HP Server Automation**.
   - **Name contains:** Enter the full or partial name of the Resource Manager to use, and press **Search**. Select the resource manager you want to use.
4. Press **OK**.



For more information about creating resources in ITOC, see the **HP IT Operations Compliance User Guide**.

Uninstall the Resource Adapter

1. Locate the following scripts on the SA slice on which the adapter was installed. These scripts should be in the home directory of the UNIX user specified for adapter installation. If `root` was specified, these scripts will be in `/root`.
   `.uninstall_itoc_adapter.sh`

   `.uninstall_itoc_minion.sh`

2. Run the `.uninstall_itoc_adapter.sh` script.
3. Manually remove the following files. If the adapter installation was done using the `adapter_easy_install.sh` script, these files will be in the `/tmp` directory:
   - `ITOC_SA_Lite-<version>`
   - `minion_easy_install`
   - `<platform>_minion-<version>`
4. Uninstall the ITOC agent from the SA Slice. You must uninstall the adapter before you uninstall the ITOC agent. See "Uninstall an Agent" in the **HP IT Operations Compliance Installation, Setup, and Upgrade Guide**.
5. From the ITOC server, remove the adapter key in the `<itoc_install_directory>/adapters/keys` directory.
6. From the ITOC server, unregister the ITOC agent of the SA Slice host by running the following: `<itoc_install_directory>/scripts/minion_reg.sh -d <agent_key>`
7. From the ITOC UI, log in as `itocadmin`. Navigate to the **Resource Manager** list, and delete the SA resource manager instance.

Chapter 2: ITOC-CSA Integration

HP Cloud Service Automation (HP CSA) orchestrates the deployment of infrastructure to provide private cloud, public cloud, or hybrid cloud for end users. ITOC is a compliance management solution designed for ensuring business service compliance against corporate and regulatory policies, making your environment compliant and secure. This chapter discusses ITOC integration on the CSA platform.

ITOC-CSA Integration Overview

You can configure CSA and ITOC so that when a new service instance is instantiated in CSA, ITOC receives a notification (as an invocation of a rest API call) from CSA. This notification is delivered to the ITOC integration user (for example, "csauser" in a "public" organization) along with the CSA's Service Instance ID. The customer should have the correct LDAP and the same definition of organizations in ITOC as that of CSA in order for CSA integration to work.

When CSA notifies ITOC of a new service instance:

1. CSA looks up the `csa.properties` file to discover the ITOC endpoint and initiates a REST API call to ITOC using the ITOC username/password and tenant name configured in the `csa.properties` file. (For information about configuring the csa.properties file, see Configure CSA.)

2. This API call to ITOC initiates the search for a Resource Manager of type Cloud Service Automation. ITOC searches this list of resource managers for the one with the `serviceURL` that matches the CSA instance that initiated this API call. This Resource Manager provides the user, password, and tenant credentials to ITOC to communicate with the CSA service.

3. Once two-way communication between CSA and ITOC is established, ITOC examines the service instance reported by CSA and determines if the instance should be created, modified, or canceled (obsoleted) in ITOC.

    a. If no existing service definition is found, a new ITOC instance is created.

    b. If a previous definition is found, the ITOC instance is modified and updated.

    c. If CSA reports a canceled instance, ITOC searches for that instance and obsoletes the service and attached resources.

4. When steps 1, 2, and 3 are completed, the ITOC user receives an email notification detailing whether each instance was created, modified, or canceled.

The ITOC-CSA usage flow is as follows:

1. Configure CSA to send service instantiation, modification, and cancellation data (notifications) to an ITOC instance.

2. Configure ITOC to communicate with CSA on receipt of the CSA data.
3. Configure CSA service designs to provide necessary information for integration with ITOC.
4. CSA notifies ITOC by calling the ITOC REST API when a CSA service instance is instantiated, modified, or canceled.

Prerequisites

To integrate ITOC and CSA, you must have:

- CSA version 4.5 with one or more of the following two providers:

  Note: CSA-ITOC integration supports only the following in Release 1.10.

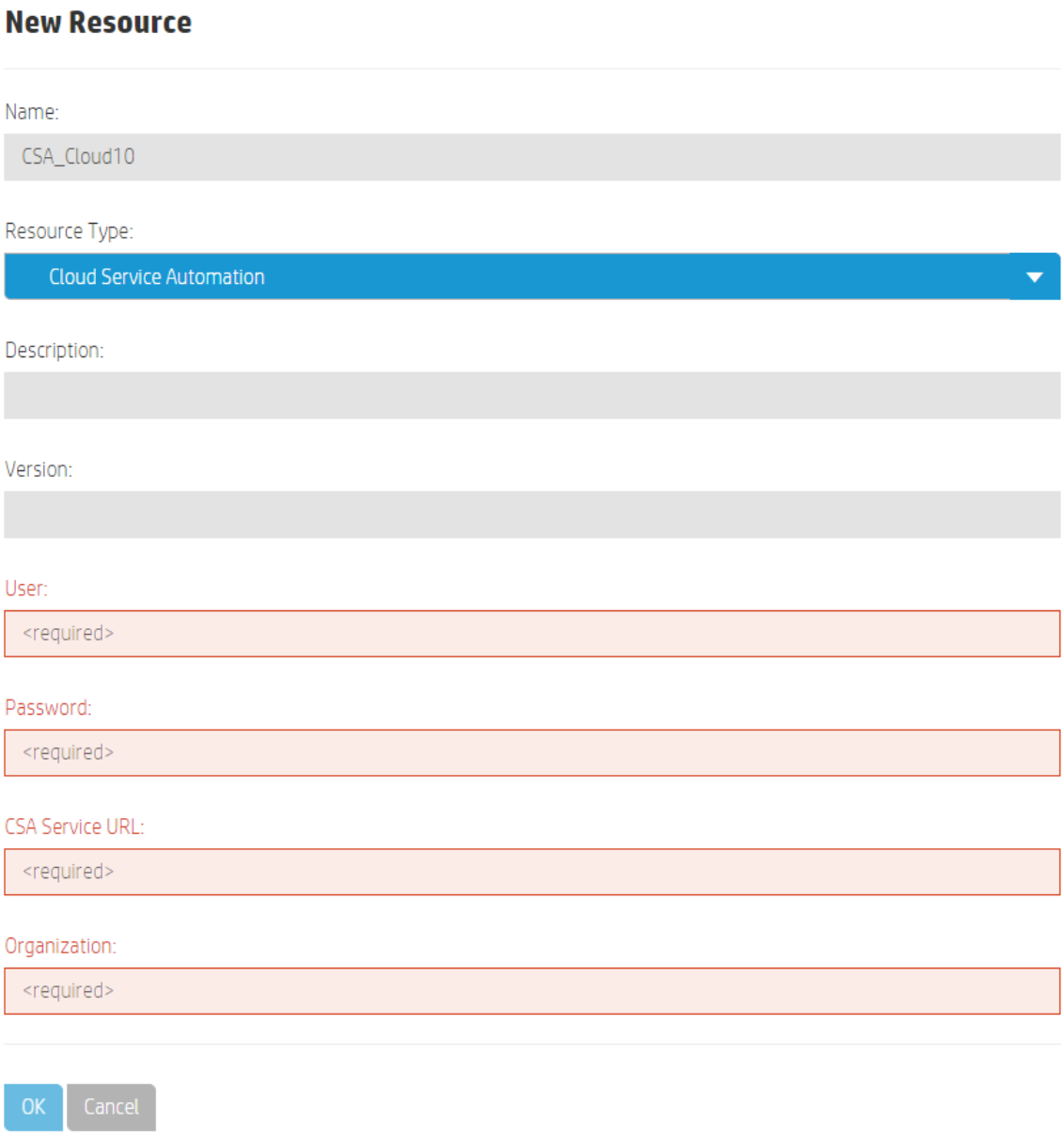
  - vCenter
  - OpenStack

Create a Resource Manager - CSA

1. Log in to ITOC as a user with the Business Administrators role.
2. Navigate to the **Resource Managers** list.
3. From **Actions**, select **New Resource Manager**.
4. The **New Resource Manager** dialog appears:

   Complete the following fields:

   - **Name:** (required) - User-specified name.
   - **Resource Type:** (required) - Select **Cloud Service Automation**. The following example shows the fields for an **Cloud Service Automation** resource:



Enter resource attribute information:

- **Description:** (optional) - A detailed description of the CSA core with which you are integrating.
- **Version:** (optional) - The CSA version being used.
- **User** (required) - The CSA user.
- **Password:** (required) - CSA user password.

- **CSA Service URL:** (required) - `https://<csaServer>:<csaPort>/csa/`
  Note: The Service URL must end with `/csa/`, as shown above.
- **Organization:** (required) - The organization of the user.
  Note: If you created the CSA instance using the defaults, this value would be **CSA-Provider**.

Configure CSA

An Admin user configures the ITOC integration endpoint that the CSA instance will contact.

1. Log in to the CSA server and navigate to the `<csaInstallDir>/csa/jboss-as/standalone/deployments/csa.war/WEBINF/classes/csa.properties` file.
2. Modify the `csa.properties` file with the following information:
   - `csa.ITOC.Integration.enabled=true`
   - `csa.ITOC.Notification.BaseUri=https://itocserver:itoc port/` - The `itocport` value typically is 7771 for default ITOC installs.
   - `csa.ITOC.Notification.username=csauser` - The `csauser` value is the ITOC user that will be used for integration and must belong to a special ITOC role called “INTEGRATION_USER”.
   - `csa.ITOC.Notification.password=hpitoc` - The `csauser`'s password.
   - `csa.ITOC.Notification.tenant=public` - The organization of the `csauser`.

     NOTE: This organization must match the corresponding organization in ITOC; otherwise, the import will fail.
3. Restart the CSA instance, and run:
   `/etc/init.d/csa restart`

Configure CSA Component for ITOC Resource

All applicable resource attributes for a resource type need to be defined on the CSA component used in a topology design to be instantiated and imported to ITOC in order for the imported ITOC resource to be successfully scanned or remediated.

To make a CSA component property available to ITOC, you can perform one of the following tasks:

- Ensure that the existing CSA component property name is the same as the ITOC resource attribute name.
  For example, if the CSA component has a property “Hostname,” then its value will be taken as the ITOC resource attribute "Hostname" value.

- Map the existing CSA component property name to the ITOC resource attribute name in the `resource.properties` file on the ITOC server (in the same folder as the `application.properties` file).
  For example, if the existing CSA resource property "serverName" has the value of the ITOC resource attribute "Hostname," configure the mapping in `resource.properties` file as follows:

  ```
  serverName=Hostname
  ```

  Where the CSA property name is the key in the mapping, and the ITOC resource attribute name is the value.

- Add the ITOC resource attribute to the CSA component property and prefix the attribute with "ITOC."
  You may define ITOCHostname in the CSA component property that has the value of ITOC resource attribute "Hostname."

Import the Server Certificate from CSA to ITOC

This section describes how to import a server certificate from CSA to ITOC for HTTPS communication.

Prerequisite

This process must be performed by a user with privileges to log in to both the CSA and ITOC servers and access the install location.

On the CSA Server

1. On the CSA server, verify the certificate is available in the keystore. Use the alias `csa` to narrow your choices:

```
# <csa_server>/csa/openjre/bin/keytool -list -alias csa -v -keystore
<csa_server>/csa/openjre/lib/security/cacerts
Enter keystore password:
Alias name: csa
Creation date: May 27, 2015
Entry type: trustedCertEntry

Owner: CN=csa.server.domain.net, OU=TEST, O=TEST, L=Palo Alto, ST=CA, C=US
Issuer: CN=csa.server.domain.net, OU=TEST, O=TEST, L=Palo Alto, ST=CA, C=US
Serial number: 7a8bdee
Valid from: Wed May 27 02:38:51 PDT 2015 until: Thu Sep 24 02:38:51 PDT 2015
Certificate fingerprints:
MD5: 1E:35:CB:E0:B6:93:B9:21:8C:17:BF:57:C5:61:B0:70
SHA1: 85:54:F8:E8:A3:D5:6C:7B:5A:5D:AF:AA:14:A9:03:E3:67:F9:2A:39
SHA256: 9B:AB:E7:77:4F:84:C7:54:D2:7D:F0:4B:2F:EE:37:30:56:1F:66:72:
A9:30:43:62:22:AF:7A:49:80:D1:94:5A
```

```
Signature algorithm name: SHA256withRSA
Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 40 41 77 C8 53 D2 F7 CB 6B 42 66 9F D7 3F 25 AA @Aw.S...kBf..?%.
0010: 9E 43 09 30 .C.0
]
]
#
```

2. Export the certificate to a file, using the default Java keystore password `changeit` when prompted.

```
 # <csa_server>/csa/openjre/bin/keytool -export -alias csa -file /tmp/csa.crt -
keystore
<csa_server>/csa/openjre/lib/security/cacerts
Enter keystore password:
Certificate stored in file </tmp/csa.crt>
#
```

3. On the ITOC server, copy the exported certificate file `csa.crt` from CSA server to ITOC server and import the certificate.
   - Use the default Java keystore password `changeit` when prompted.
   - Enter yes when prompted: `Trust this certificate?`

```
# <itoc_server>/openjre/bin/keytool -importcert -alias csa -file /tmp/csa.crt -
keystore <itoc_server>/wildfly-8.1.0.Final/standalone/configuration/selfcacerts
Enter keystore password:
Owner: CN=csa.server.domain.net, OU=TEST, O=TEST, L=Palo Alto, ST=CA, C=US
Issuer: CN=csa.server.domain.net, OU=TEST, O=TEST, L=Palo Alto, ST=CA, C=US
Serial number: 7a8bdee
Valid from: Wed May 27 02:38:51 PDT 2015 until: Thu Sep 24 02:38:51 PDT 2015
Certificate fingerprints:
MD5:
1E:35:CB:E0:B6:93:B9:21:8C:17:BF:57:C5:61:B0:70
SHA1: 85:54:F8:E8:A3:D5:6C:7B:5A:5D:AF:AA:14:A9:03:E3:67:F9:2A:39
SHA256: 9B:AB:E7:77:4F:84:C7:54:D2:7D:F0:4B:2F:EE:37:30:56:1F:
66:72:A9:30:43:62:22:AF:7A:49:80:D1:94:5A
Signature algorithm name: SHA256withRSA
Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
```

```
KeyIdentifier [
0000: 40 41 77 C8 53 D2 F7 CB 6B 42 66 9F D7 3F 25
AA @Aw.S...kBf..?%.
0010: 9E 43 09 30 .C.0
]
]
Trust this certificate? [no]: yes
Certificate was added to keystore
#

List the certificate to confirm

# <itoc_server>/openjre/bin/keytool -list -alias csa -v -keystore
/opt/hp/itoc/wildfly-8.1.0.Final/standalone/configuration/selfcacerts
Enter keystore password:
Alias name: csa
Creation date: Jul 28, 2015
Entry type: trustedCertEntry
Owner: CN=csa.server.domain.net, OU=TEST, O=TEST, L=Palo Alto, ST=CA, C=US
Issuer: CN=csa.server.domain.net, OU=TEST, O=TEST, L=Palo Alto, ST=CA, C=US
Serial number: 7a8bdee
Valid from: Wed May 27 02:38:51 PDT 2015 until: Thu Sep 24 02:38:51 PDT 2015
Certificate fingerprints:
MD5: 1E:35:CB:E0:B6:93:B9:21:8C:17:BF:57:C5:61:B0:70
SHA1: 85:54:F8:E8:A3:D5:6C:7B:5A:5D:AF:AA:14:A9:03:E3:67:F9:2A:39
SHA256: 9B:AB:E7:77:4F:84:C7:54:D2:7D:F0:4B:2F:EE:37:30:56:
1F:66:72:A9:30:43:62:22:AF:7A:49:80:D1:94:5A
Signature algorithm name: SHA256withRSA
Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 40 41 77 C8 53 D2 F7 CB 6B 42 66 9F D7 3F 25 AA @Aw.S...kBf..?%.
0010: 9E 43 09 30 .C.0
]
]
#
```

4. Restart the ITOC server.

Configure CSA Designs for Import Into ITOC

Configure CSA designs so that CSA instances can be imported into ITOC:

1. Ensure that every resource component that is part of the CSA service has following attribute set: `ITOCResourceType`
2. The value specified for `ITOCResourceType` must be of type String and have a valid 1:1 mapping to ITOC-supported resource types. If not specified, the resource type (when imported into ITOC) will be "Unknown."
3. All applicable properties for a given resource type in ITOC must be available on the CSA resource also and have the exact same name and value.
4. All CSA services to be imported into ITOC require a TAG attached to the CSA design in the following format:

   `ITOCPolicy_POL_ 0001:MW_12`

   in which `POL_0001` is the applicable business ID of the policy and `12` is the ID of the maintenance window that will run the jobs for this service. The user can include multiple Maintenance Windows in a tag as follows:

   `ITOCPolicy_POL_ 0001:MW_12:MW_14:MW_xx`

   If the policy or maintenance window names are missing, no statement is created.
5. ITOC supports the `ITOCDomainName` user-defined property in CSA services to specify the optional domain name for a resource.

ITOC Import

When ITOC successfully imports the CSA service and associated resource instances, it also automatically:

- Creates the corresponding Business Service and all associated resources.
- Promotes the business service to production.
- Ensures that the policy specified by the `ITOCPolicy_ tag` is available in the same org as the user that initiated the service in CSA and in production.
- Ensures the maintenance window is available and in the same org as the user that initiated the service in CSA.
- Creates and promotes to production a new statement that ties the newly imported service with the specified policy and maintenance window.

Send Documentation Feedback

If you have comments about HP ITOC or this document, contact HP. If an email client is configured on this system, click the link above to generate an email to the HP ITOC team. Just add your feedback to the email and click send.

If no email client is available, send your feedback to itopscompliance@hp.com. Please include the name and version of the document in your feedback memo.

We appreciate your feedback!