HP ServiceCenter and

Configuration Management Integration

Software Version: 1.0

User's Guide

May 2007

Legal Notices

Warranty

Hewlett-Packard makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices

Trademark Notices

[List here only relevant trademark notices that appear on the HP Legal Acknowledgment web page. Use appropriate symbols (®, ™) as indicated. Do not list any trademarks that are not listed on the Legal web page: http://legalweb.corp.hp.com/legal/files/tradeack.asp]

Acknowledgements

List here acknowledgements relevant to your product.

Support

Please visit the HP Software web site at:

http://www.managementsoftware.hp.com/

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

You can also go directly to the support web site at:

http://support.openview.hp.com/

HP 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 valuable support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter 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 log in. Many also require a support contract.

To find more information about access levels, go to:

http://support.openview.hp.com/access_level.jsp

To register for an HP Passport ID, go to:

https://passport2.hp.com/hpp/newuser.do

Contents

1 Introduction

The ServiceCenter (SC) and Configuration Management (CM) Integration solution allows for federation of data between both applications in order to automate the processes of Change and Incident Management with desired state management.

This document describes the value the integration provides and how to configure it. The document structure begins by providing an overview of the solution. Then it describes the pre-installation and configuration necessary before using the integration between SC and CM applications. It then finishes by outlining each feature of the integration.

Note: The integration described in this document should also apply to HP Service Manager. You may substitute references to ServiceCenter with Service Manager.

Intended Audience

This guide is intended to describe the features of the integration between SC and CM applications for all users that want to use the integration, and also the administrators that set up the solution.

Prerequisites

As this document refers to HP Configuration Management Solution, ServiceCenter and Connect-It features, the reader should be familiar with their mechanisms and the modules used in this integration. Moreover, the reader should be familiar with IT service management processes.

Related Documents

The following list of documentation is suggested in case additional learning is required. Please refer to each product's distribution to access the complete documentation.

SC/CM Integration documentation:

SC/CM Integration – Product Specifications

SC documentation:

HP ServiceCenter software – Installation Guide

HP ServiceCenter software – Database Conversion and RDBMS Support Guide

Internal help of HP ServiceCenter

CM documentation:

HP Using Radia software – Essentials Guide

HP Management Portal Using Radia software – Installation and Configuration Guide

HP Policy Server Using Radia software – Installation and Configuration Guide

HP Administrator Workstation Using Radia software – System Explorer Guide

Connect-It documentation:

HP Connect-It software – Connectors

HP Connect-It software – Programmer's Reference

HP Connect-It software – User's Guide

Status of the document

This is a draft version to be reviewed by all engineers that are working under project.

2 Overview

Before further describing the functioning of the integration solution, this chapter will introduce both the ServiceCenter and Configuration Management products with an overview of their application area, their capabilities and their features.

Architecture

The SC / CM integration uses the following global architecture:

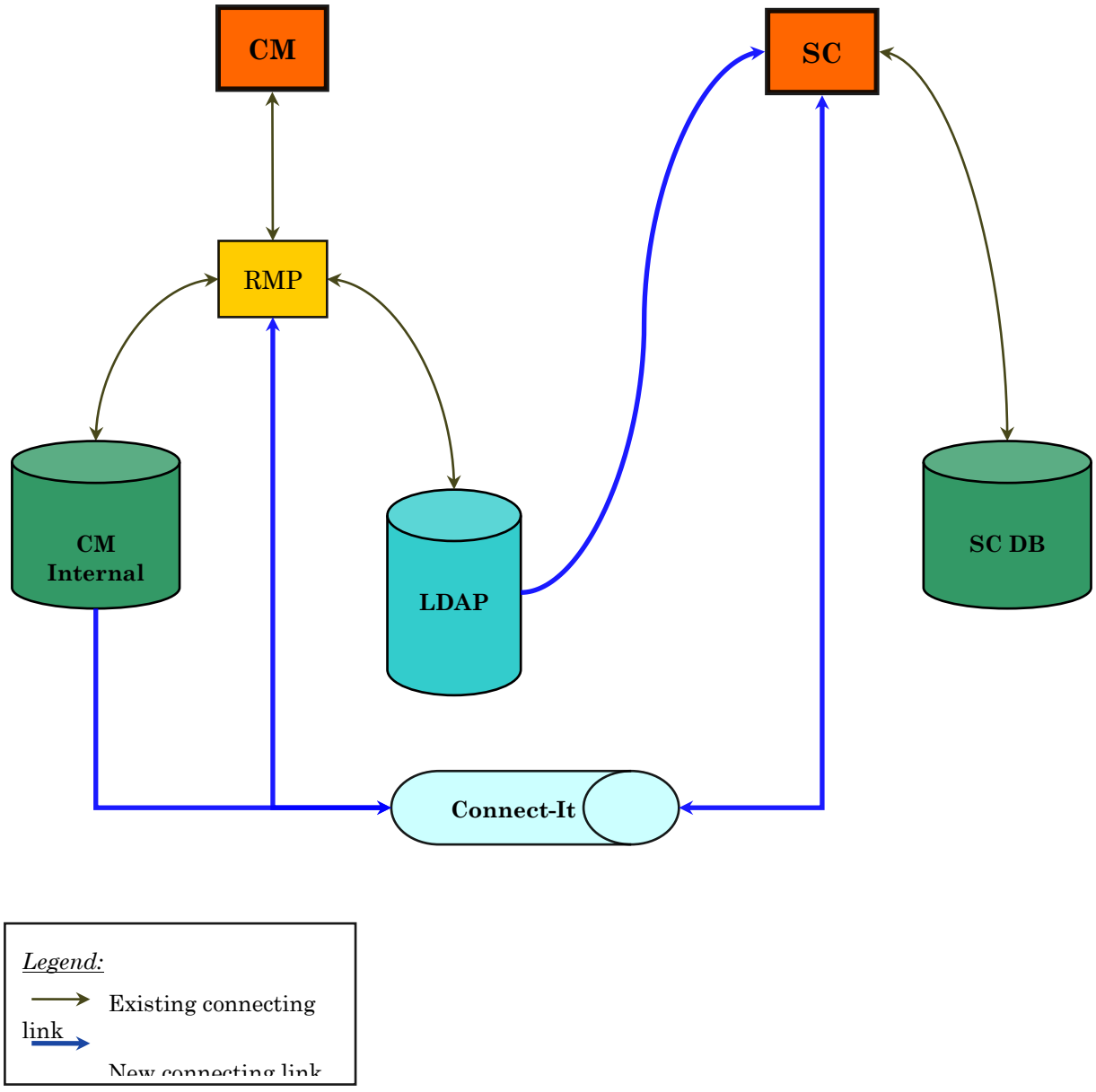

Figure 1: Global architecture of SC / CM Integration

Use Cases

The SC / CM integration enables four use cases:

1. *Use Case #1:* Software provisioning. According to the business needs, software provisioning can be requested by either granting or denying policy access. An existing policy access can also be revoked. Through ServiceCenter, a RFC is created to request the desired provisioning action. Once the RFC is created, the corresponding policy into Configuration Management solution is created or revoked.
2. *Use Case #2:* Reporting a software incident. If a user experiences a problem with a software installation, he can report an incident through the service desk. Then according to this incident, a repair action can be created into Configuration Management in order to repair the impacted software installation.
3. *Use Case #3:* Managing a non-compliance state. Configuration Management detects that a device is no longer in compliance with its policy definition and launches a repair action. If the repair action is successful, then a ServiceCenter incident is automatically created and closed. If the report action is unsuccessful, then a ServiceCenter incident is automatically opened and assigned so an agent can check what happened and take corrective actions as necessary.
4. *Use Case #4:* Managing a connectivity issue. Configuration Management detects that a device has not been connected to the network for a predetermined amount of time. A ServiceCenter incident is reported automatically. Consequently the agent can contact the user in order to have her/him connect to the network. Once the desired state has been enforced, the incident is automatically updated.

3 Installation and configuration

Required environment

The SC / CM integration was developed with the following product features:

- ServiceCenter v6.2.0.0. The product includes at least the following modules:
  - Configuration Management,
  - Service Desk,
  - Change Management,
  - Incident Management.
- Configuration Management version 4.2. The product includes at least the following components:
  - Management Portal,
  - Management Portal Web Services version 1.3
  - Integration Server,
  - Configuration Server,
  - Policy Manager,
  - Messaging Server.
- Connect-It v3.70 or higher. The product includes at least the following connectors:
  - HP Service Management connectors/ServiceCenter connectors/ServiceCenter (named “ServiceCenter connector” in the following sections),
  - HP Configuration Management connectors/Management Portal (named “Management Portal connector” in the following sections),
  - HP Configuration Management connectors/Service Events (named “Service Events connector” in the following sections).

Data are managed as follow:

- SC and CM use their own databases for their respective data,
- A Microsoft Active Directory LDAP server is used to store manageable entities.

All these components are required to be installed and configured correctly in the environment.

ServiceCenter configuration

Automatic import

The integration requires a ServiceCenter enhancement. To configure all the SC enhancements, a file should be imported into SC application. The UNL file is located under the following directory:

```
<Connect-It root directory>/datakit/sccm/sc62cm42/sc
```

This file permits to import data that should be integrated into SC in order to enable the whole functionalities of the SC / CM integration.

The following items list the data imported by this script:

- Structure of *cm3r*, *cm3t* and *probsummary* tables, with their associated links.
- Some specific data:
  - Change and Task objects:
    - New Change/Task category,
    - New Change phases,
    - New Change/Task fields.
  - Incident objects:
    - New product and problem types,
    - New Incident fields.
  - A user capability word to restrict the access to information.
- Some new forms to manage the new kinds of Change, Task and Incident objects, with their associated format controls and links objects.
- Some new events and event maps that are used by the integration scenarios to read and write data.
- The LDAP mapping configuration in order to access to LDAP data.

For further details on importing scripts into SC, please refer to the SC documentation.

Additional configuration

In addition to the above import phase, some points need to be configured by an administrator in SC database.

- A new user capability word "*CM Advanced*" allows users with a user profile including this privilege to overwrite the policy priority when he opens or update a Policy Change. This capability word is provided by the above import script, and it should be linked to existing operator profile(s) according to the access needs. The following steps describe how to perform this action:

1. In SC interface, go to `Utilities/Administration/Security/User Administration/User and Contact Utilities/Search for User Role` menu.
2. Search for the user role to be enhanced.
3. Go to `Startup` tab.
4. In `Capability Words` section, add at the end of the existing list the following line: `CM Advanced`
5. Save the record.

Operators having the enhanced user role may need to be updated in order to refresh their capabilities. To do this, the user role referenced in an operator must be cleared and filled again, then the operator record must be saved.

- In order to federate CM Services with SC devices to import CM DSL into SC, a device subtype should be added to the "*Business Service*" existing device type, following these steps:
  1. In SC interface, go to `Services/Configuration Management/Administration/CI Types` menu.
  2. Search for "*Business Service*" CI type.
  3. In `Sub Types` array, add at the end of the list the following line: `CM Service`
  4. Save the record.
- This integration creates Incidents with "*business applications*" category. In order to display all relevant information (such as the impacted CM service for instance), new forms are available: *IM.template.open.sccm, IM.template.update.sccm, IM.template.close.sccm*. By default, they are isolated and only available from the forms list of the SC Incident file. According to the existing customization before adding this integration, they can be linked to the "*business applications*" category, following these steps (this operation is supposed to be done for the rest of the documentation):
  1. Go to `Services/Incident Management/Security Files` menu.
  2. Click on `Search/Add` button for Categories.
  3. Search for the "*business applications*" category.
  4. Go to `Formats` tab.
  5. Enter the following information in the `Display Formats` section:
     a. Open = *IM.template.open.sccm*
     b. Update = *IM.template.update.sccm*
     c. Close = *IM.template.close.sccm*
  6. Save the category.
- The above import script contains the configuration to access to LDAP entities. Nonetheless, the connection to the LDAP server should be configured following these steps:
  1. In SC interface, go to `Utilities/Tools/LDAP Mapping` menu.
  2. In the "*ServiceCenter LDAP Mapping – System Level Specification*" form, enter the following information:

a. `LDAP Server`: the name of the server that hosts the LDAP server on which CM relies to manage entities.

b. `LDAP Port`: the port of the LDAP server

c. `LDAP Base Directory`: the Base Directory that contains all entities to manage

3. Then click on `Save` button.

4. The *File/Field Level Mapping* for the concerned entities is defined thanks to import script as defined above.

Connect-It scenarios configuration

The SC / CM integration is composed of seven Connect-It scenarios that enables the federation of data between the two products.

Next sections describe all scenarios used for this integration as well as the configuration needed for using them in your environment.

Integration scenarios

The integration contains the following scenarios (located in directory `<Connect-It root directory>/scenario/sccm/sc62cm42`):

- `cmsc_device.scn`: propagates the device entities from CM internal database to SC database
- `cmsc_group.scn`: propagates the group entities from CM internal database to SC database
- `cmsc_service.scn`: propagates the service objects from CM internal database to SC database
- `sccm_change_policy.scn`: creates the corresponding policy into CM from a SC Change created in the framework of a software access definition.
- `sccm_policy_incident.scn`: creates a CM repair action against a software installation on a targeted device for which a SC Incident was reported by the user. Then the SC Incident is updated according to the repair action result.
- `cmsc_policy_compliance.scn`: launches a Repair action against the software for which a compliance issue was detected. Then it creates and updates an incident into SC according the result of the CM Repair action.
- `cmsc_connectivity_incident.scn`: creates a SC Incident for each connectivity issue detected by CM. As soon as the issue is resolved, the Incident is updated.

Connectors' configuration

The following three connectors are used by the above scenarios:

- HP Service Management connectors/ServiceCenter connectors/ServiceCenter,
- HP Configuration Management connectors/Management Portal,

- HP Configuration Management connectors/Service Events.

Each connector should be configured to connect to the correct data source.

Please refer to the Connect-It Connectors guide for further details about the configuration of these connectors.

Scenarios scheduling

Each scenario execution should be scheduled to ensure periodical federation of the required data.

The scheduling of each scenario depends on business needs, and should be configured accordingly. A scheduler can be defined through Connect-It where the scheduling can then be configured.

Connect-It enables to associate a service (Windows) or daemon (Unix) to a scenario. This service or daemon allows your Connect-It server to start the data-processing procedure as a background task, depending on the scheduler associated to the scenario.

Please refer to the Connect-It User's Guide for more details about scenario scheduling.

Mapping tailoring

Some tailoring of the scenarios may be required based on your production environment's configuration:

- `cmsc_policy_compliance.scn`:
  - The conditions that trigger this scenario are based on the features of a policy compliance issue detected by CM. These condition can be tailored by modifying the where clause of the scenario mapping.
- `cmsc_connectivity_incident.scn`:
  - The condition to trigger the scenario is based on the predetermined amount of time that is defined on CM side from which a connection loss is considered as a connectivity issue. This variable is defined as a script constant for the scenario. It is called "*connection_delay_in_days*" and can be tailored according to the CM configuration. The unit of measure for connection delay is in days.

There are other tailoring options available depending on your business needs, for instance:

- Mapping tables (stored in `<Connect-It root directory>\scenario\sccm\mpt\sccm.mpt` file, and editable through the Connect-It interface),
- Constant string values (stored in `<Connect-It root directory>\scenario\sccm\strings\sccm.str` file, and editable through the Connect-It interface.

Please refer to the Connect-It User's Guide for further details on mapping, string tables, and script constants.

4 Federation of reference data

The SC / CM Integration solution starts with a data preparation phase consisting in:

- Common managed CIs for both SC and CM products.
- Federating CM services into SC repository.

Once the environment is set up for both SC and CM products, the four use cases described above can be run.

Each step of this phase is described in the next sections.

LDAP connection

CM relies on a LDAP server to store its manageable entities and its policy definition. As SC is equipped with a native LDAP connection, it is connected to the same LDAP server than CM is. Thanks to this connection and through the "*File/Field Level Specifications*" configuration (refer to the section *ServiceCenter configuration*

to have more details about LDAP configuration), the following mapping is defined:

LDAP entity	**SC file**
User	Contact
Computer	Computer
Group	Group
Organizational-Unit	Department
Organization	Company
Locality	Location

Table 1: Mapping of LDAP entities in SC files

By default, the *File/Field Level Specification* for each entity is configured to set LDAP as the primary data source. Consequently, the data in the internal SC DB linked to the above files are no longer displayed, only LDAP entities are now accessible. If SC local data requires to be accessible, the option '*LDAP is Primary Data Source*' must be unchecked from the respective file.

Federation of CM internal information

CM also uses an internal database in which Device and Group can be stored. These two entities can be federated to SC database, in Computer and Group files respectively.

Two Connect-It scenarios enable this federation:

- `cmsc_device.scn`, federates the CM Device entities to SC Computer file,
- `cmsc_group.scn`, federates the CM Group entities to SC Group file.

Once configured as described in the *Additional configuration*

In addition to the above import phase, some points need to be configured by an administrator in SC database.

- A new user capability word "*CM Advanced*" allows users with a user profile including this privilege to overwrite the policy priority when he opens or update a Policy Change. This capability word is provided by the above import script, and it should be linked to existing operator profile(s) according to the access needs. The following steps describe how to perform this action:

  5 In SC interface, go to `Utilities/Administration/Security/User Administration/User and Contact Utilities/Search for User Role` menu.

  6 Search for the user role to be enhanced.

  7 Go to `Startup` tab.

  8 In `Capability Words` section, add at the end of the existing list the following line: `CM Advanced`

  9 Save the record.

  

  Operators having the enhanced user role may need to be updated in order to refresh their capabilities. To do this, the user role referenced in an operator must be cleared and filled again, then the operator record must be saved.

- In order to federate CM Services with SC devices to import CM DSL into SC, a device subtype should be added to the "*Business Service*" existing device type, following these steps:

  10 In SC interface, go to `Services/Configuration Management/Administration/CI Types` menu.

  11 Search for "*Business Service*" CI type.

  12 In `Sub Types` array, add at the end of the list the following line: `CM Service`

  13 Save the record.

- This integration creates Incidents with "*business applications*" category. In order to display all relevant information (such as the impacted CM service for instance), new forms are available: *IM.template.open.sccm, IM.template.update.sccm, IM.template.close.sccm*. By default, they are isolated and only available from the forms list of the SC Incident file. According to the existing customization before adding this integration, they can be linked to the "*business applications*" category, following these steps (this operation is supposed to be done for the rest of the documentation):

  14 Go to `Services/Incident Management/Security Files` menu.

  15 Click on `Search/Add` button for Categories.

16 Search for the "*business applications*" category.

17 Go to `Formats` tab.

18 Enter the following information in the `Display Formats` section:

d Open = *IM.template.open.sccm*

e Update = *IM.template.update.sccm*

f Close = *IM.template.close.sccm*

19 Save the category.

- The above import script contains the configuration to access to LDAP entities. Nonetheless, the connection to the LDAP server should be configured following these steps:

20 In SC interface, go to `Utilities/Tools/LDAP Mapping` menu.

21 In the "*ServiceCenter LDAP Mapping – System Level Specification*" form, enter the following information:

d `LDAP Server`: the name of the server that hosts the LDAP server on which CM relies to manage entities.

e `LDAP Port`: the port of the LDAP server

f `LDAP Base Directory`: the Base Directory that contains all entities to manage

22 Then click on `Save` button.

23 The *File/Field Level Mapping* for the concerned entities is defined thanks to import script as defined above.

Connect-It scenarios configuration

section, these two scenarios should be executed periodically in order to federate the devices and groups from CM to SC. The membership between devices and groups is federates and updated.

Federation of services between SC and CM

CM manages Services in its DSL. These services are stored in the internal DB of CM and required to be federated to SC DB in order to have access to them.

This task is performed by the `cmsc_service.scn` scenario that retrieves correct information from CM and that transmits them into SC DB.

These services are federated to the SC Device file, and are defined as devices of "*Business Service*" type, with a "*CM Service*" subtype.

When they are available from CM, the corresponding SC devices have an "*Installed*" status. If a CM service is no longer available, the status of the corresponding SC device becomes "*Retired*".

To ensure up to date federation of CM services to SC, it is recommended to run periodically the scenario `cmsc_service.scn`. Please refer to section *Additional configuration*

In addition to the above import phase, some points need to be configured by an administrator in SC database.

- A new user capability word "*CM Advanced*" allows users with a user profile including this privilege to overwrite the policy priority when he opens or update a Policy Change. This capability word is provided by the above import script, and it should be linked to existing operator profile(s) according to the access needs. The following steps describe how to perform this action:

  24 In SC interface, go to `Utilities/Administration/Security/User Administration/User and Contact Utilities/Search for User Role` menu.

  25 Search for the user role to be enhanced.

  26 Go to `Startup` tab.

  27 In `Capability Words` section, add at the end of the existing list the following line: `CM Advanced`

  28 Save the record.

Operators having the enhanced user role may need to be updated in order to refresh their capabilities. To do this, the user role referenced in an operator must be cleared and filled again, then the operator record must be saved.

- In order to federate CM Services with SC devices to import CM DSL into SC, a device subtype should be added to the "*Business Service*" existing device type, following these steps:

  29 In SC interface, go to `Services/Configuration Management/Administration/CI Types` menu.

  30 Search for "*Business Service*" CI type.

  31 In `Sub Types` array, add at the end of the list the following line: `CM Service`

  32 Save the record.

- This integration creates Incidents with "*business applications*" category. In order to display all relevant information (such as the impacted CM service for instance), new forms are available: *IM.template.open.sccm, IM.template.update.sccm, IM.template.close.sccm*. By default, they are isolated and only available from the forms list of the SC Incident file. According to the existing customization before adding this integration, they can be linked to the "*business applications*" category, following these steps (this operation is supposed to be done for the rest of the documentation):

  33 Go to `Services/Incident Management/Security Files` menu.

  34 Click on `Search/Add` button for Categories.

  35 Search for the "*business applications*" category.

  36 Go to `Formats` tab.

  37 Enter the following information in the `Display Formats` section:

  g Open = *IM.template.open.sccm*

  h Update = *IM.template.update.sccm*

  i Close = *IM.template.close.sccm*

38 Save the category.

- The above import script contains the configuration to access to LDAP entities. Nonetheless, the connection to the LDAP server should be configured following these steps:

39 In SC interface, go to `Utilities/Tools/LDAP Mapping` menu.

40 In the "*ServiceCenter LDAP Mapping – System Level Specification*" form, enter the following information:

g `LDAP Server`: the name of the server that hosts the LDAP server on which CM relies to manage entities.

h `LDAP Port`: the port of the LDAP server

i `LDAP Base Directory`: the Base Directory that contains all entities to manage

41 Then click on `Save` button.

42 The *File/Field Level Mapping* for the concerned entities is defined thanks to import script as defined above.

Connect-It scenarios configuration

for more details about the Connect-It scenarios configuration.

5 Software provisioning

The first use case consists of a CM policy creation after a SC change was requested by a user that needs to dispose of a software solution.

The following next sections describe the features of this use case.

Context

This use case can be triggered by the following events:

- A user needs access to a new software application in order to fulfil his new job duties.
- Access to a specific software application needs to be restricted for a group of employees.
- A software permission needs to be revoked to free up a licence.

In all cases, a user creates a RFC from SC Change Management module in order to initiate the request.

RFC creation

The user that requests software provisioning can create either a Change or a Task within the SC Change Management module.

Change creation

First the user goes to `Services/Change Management` menu and selects the `Open New Change` action.

Among the list of available Change categories, he selects the "*Policy*" one.

Then a specific form is displayed. Except the classical information needed when creating a Change, the user has to specify the following information in the `Configuration Management Policy` tab:

- He first chooses the kind of entity for which the software access needs to be managed. He can choose between Computer, Person, Group, Company, Department or Location.
- According his choice, he must specify the targeted entity.
- Then he indicates the service to use among the proposed list of available services.
- The action should be chosen between: *Grant, Deny* and *Revoke*.
- If the action is *Grant* or *Deny*, and if he has an advanced role, he can choose the priority of the policy to be defined.
  - For a *Grant* action, the available priorities are: *May (+), Should (++), Must (+++).* The default one is *May (+).* This default priority is used if the user has a basic role.

  - For a *Deny* action, the available priorities are: *May Not (-), Should Not (--), Must Not (---).* The default one is *Must Not (---).* This default priority is used if the user has a basic role.
- If the action is *Grant* and if the targeted entity is a Computer, then he can choose between creating only a policy, or creating a policy and a deployment job.
- If he chooses to create both policy and job in a same time, then he should select the deployment method:
  - *Immediate*, to deploy immediately the specified software on the targeted device.
  - *Scheduled*, to specify the date and time at which the deployment should occur.
- Once all information is entered, the user saves this Change.
- The Change needs to be approved following the normal Change approval process.

Once approved, the Change is ready to be deployed in order to create the corresponding action on CM side.

Task creation

First the user goes to `Services/Change Management` menu and selects the `Open New Task` action.

Among the list of available Task categories, he selects the "*Policy*" one.

Then a specific form is displayed. Except the classical information needed when creating a Task, the user has to specify the following information in the `Configuration Management Policy` tab:

- He first chooses the kind of entity for which the software access needs to be managed. He can choose between Computer, Person, Group, Company, Department or Location.
- According his choice, he must specify the targeted entity.
- Then he indicates the service to use among the proposed list of available services.
- The action should be chosen between: *Grant, Deny* and *Revoke.*
- If the action is *Grant* or *Deny*, and if he has an advanced role, he can choose the priority of the policy to be defined.
  - For a *Grant* action, the available priorities are: *May (+), Should (++), Must (+++).* The default one is *May (+).* This default priority is used if the user has a basic role.
  - For a *Deny* action, the available priorities are: *May Not (-), Should Not (--), Must Not (---).* The default one is *Must Not (---).* This default priority is used if the user has a basic role.
- If the action is *Grant* and if the targeted entity is a Computer, then he can choose between creating only a policy, or creating a policy and a deployment job.
- If he chooses to create both policy and job in a same time, then he should select the deployment method:
  - *Immediate*, to deploy immediately the specified software on the targeted device.
  - *Scheduled*, to specify the date and time at which the deployment should occur.
- Once all information is entered, the user saves this Task.
- The Task needs to be approved following the normal Change approval process.

Once approved, the Task is ready to be deployed in order to create the corresponding action on CM side.

Deployment of SC Change/Task into CM

The Connect-It scenario named `sccm_change_policy.scn` deploys to CM all Changes and Tasks that are created into SC and that have relevant features (valid category, under implementation phase, not yet deployed). This leads to the creation of the corresponding CM action:

- If the user selected the *Grant* or *Deny* action, then a policy is created to define the access to the specified software for the targeted entity. Moreover, if the entity is a Computer and if the user wanted a deployment action, then a deployment job is also created to deploy the software on the computer, according to the deployment method.
- If the user selected the *Revoke* action, then the existing policy defined on the specified entity is unassigned. Moreover, in case the specified entity is a computer, the software application is automatically removed.

Notification of status between CM task and SC Change/Task

The same Connect-It scenario updates the initiating RFC status for tracking purposes.

- If only a policy was created or removed, then the status of the deployment creation is used to update the status of the initiating RFC.
- If a job was created in addition to the policy, then the RFC status depends on the job evolution.

The agent monitoring the Change Management request can review the RFC progression and can close it when all actions have been executed successfully and the desired state is reached.

6 Reporting a software incident

The second use case consists in a CM repair action execution after a SC incident about a software dysfunction was reported by a user.

The following next sections describe the features this use case.

Context

This use case concerns the users who experience an issue with a software installation that needs a resolution.

If a user has a problem with a software application that is installed on its workstation (deleted files, corrupted files …) then he can call the helpdesk in order to report this incident.

The agent that receives the call will create an Incident ticket through the SC service desk and initiate remediation procedures against the software installation.

Incident creation

The agent first goes to `Services/Service Desk` menu, and select `Register New Interaction` action.

- Except the classical information to be entered for a new interaction, he chooses the following kind of Incident:
  - *Category = business applications*
  - *Subcategory = client dependent*
  - *Product type = policy*
  - *Problem type = remediation*
- Then he registers the Incident clicking on `Create Incident` button.
- A new form appears with the information that he has just specified. He goes to the `Actions/Resolution` tab and selects the `Remote action` sub tab, in which he specifies the service to use in order to repair the software installation.
- Then he presses the `Remediate` button to prepare the Incident ticket to be deployed to CM.

Deployment of SC Incident to CM Repair task

The Connect-It scenario `sccm_policy_incident.scn` performs the deployment of Incident from SC to CM.

This leads to a CM Repair task creation, which tries to repair the specified software installation on the targeted computer.

The initiating incident ticket should be updated according to the transmission task status returned by the CM response. If the transmission is successful, then the status becomes "*Work in progress*" and an action is specified.

This way, the agent can check the Incident progression. If the application has successfully been repaired, the user should confirm this to the agent.

Consequently the agent can close the Incident ticket.

7 Managing a non-compliance state

The third use case consists in a SC incident report and a CM repair action execution after CM identifies that a policy is no longer in compliance with a client state.

The following next sections describe the features of this use case.

Context

CM can detect automatically that a device state is no longer in compliance with its policy definition. It logs this issue as an internal event.

This event is processed by the integration in order to report the incident to SC so that it can be verified by an agent.

Automatic Repair action and Incident creation

The Connect-It scenario `cmsc_policy_compliance.scn` detects the event logged by CM, and then launches a repair action to try to reach the desired state. This action is a CM Repair action against the impacted device and software.

Then, it creates the corresponding SC Incident ticket, with the following information:

- *Category = business applications*
- *Subcategory = client dependent*
- *Product type = policy*
- *Problem type = compliance*
- The impacted computer is provided, as well as the impacted software.
- If the Repair action is successful, then the resolution and the status of this Incident ticket are updated.

Closure of the SC Incident ticket

As the incident was reported to SC, an agent can analyze this new incident, and may make actions to close it. Three cases are possible:

1. The repair action was successful; the operator analyzes the resolution then closes the incident ticket.
2. The repair action has failed, and the agent decides no further action is required and closes the incident ticket.
3. The repair action has failed, and the agent decides a new policy is required to address this compliance issue:

a. The agent invokes the software provisioning process (use case #1, described in section *Software provisioning*

b.) to create a RFC to correct the compliance issue.

c. The operator can close the incident as soon as a resolution is applied.

8 Managing a connectivity issue

The fourth and last use case consists in a SC incident automatic report after CM detects a connectivity issue with a client.

The following next sections describe the features of this use case.

Context

CM can detect automatically that a device has been unreachable for a predetermined amount of time. It logs this issue as an internal event.

This event is processed by the integration in order to report the incident into SC so that it can be investigated by an agent.

Automatic Incident creation

The Connect-It scenario `cmsc_connectivity_incident.scn` detects the event logged by CM, and then creates the corresponding SC Incident ticket, with the following information:

- *Category = business applications*
- *Subcategory = client dependent*
- *Product type = policy*
- *Problem type = compliance*
- The impacted computer is specified.

Agent action

As the incident was reported to SC, an agent can analyze this new incident, and take actions to resolve this situation.

The agent can take one of two following actions:

1. Decide to do nothing and close the incident ticket.
2. Decide to contact the user of the concerned CI to reconnect to the network so the desired state policies can be enforced.

Resolution of the incident

The same Connect-It scenario should regularly checks if the device was reconnected to the network since the incident was reported.

In the case where the device has been reconnected to the network, this scenario can update the status and the resolution of the SC Incident ticket, so that the agent can verify that the incident is now resolved.

Once resolved, the agent can close the SC Incident ticket.

9 Implementation choices

Features mapping of a computer

For the non-compliance state and the connectivity issue use cases, some CM Inventory tables are used to check records and trigger the process.

These tables store the name of computers as identifier, no DN information is accessible from them. Consequently, when an incident is reported from a record in these tables, only the name of the computer is provided to perform a reconciliation with the computers accessible from SC.

From SC point of view, an incident references a computer through its `logical.name` field (in the `device` table).

This implies that the name of a computer is stored in the `logical.name` field and the DN of a computer mapped from LDAP is stored in the `machine.name` field.

Creation of a CM action specifying a computer

For the software provisioning and software incident report use cases (data from SC are used to create actions in CM), if a computer is targeted, then the following algorithm is applied:

- If the computer comes from LDAP and can be identified thanks to its DN, then this information is used to create the action and identify the targeted device.
- Otherwise,
  - if the computer disposes of an IP address, this information is used,
  - in addition to this, if it disposes of a Network name, this other information is also specified.

10 Glossary

Configuration Management Database (CMDB)

A CMDB is a unified or federated repository of information related to all the components of an information system. It helps an organization to understand the relationships between these components and track their configuration and their management. The CMDB is a fundamental component of the ITIL framework's Configuration Management process.

HP Configuration Management software (CM)

HP Configuration Management software automates the management of software such as operating systems, applications, patches, content, and configuration settings to ensure that each computing device is maintained in the right configuration.

HP Configuration Management Service

A service in CM defines the support that represents a software solution for which CM creates access rights through policy definition or software deployment task.

HP Connect-It software

Connect-It is an EAI (Enterprise Application Integration) type integration platform. An EAI solution enables a company to integrate the different applications from which it can obtain or to which it can provide internal data (Internal support, equipment management software, etc.) or external data (ERP, B2B, B2C).

HP Connect-It Connector

A connector in Connect-It represents an end point (a source or target product). Connectors communicate with the external applications and enable these applications to exchange data.

HP Connect-It Scenario

A scenario in Connect-It defines the integration logic that enables process and information to be passed between different external applications.

HP Inventory Manager (IM)

The Inventory Manager is a component of the CM suite used to discover configuration information on remote computers. It enables to centralize the discovery results maintaining the discovery information within a database.

HP ServiceCenter software (SC)

HP ServiceCenter is a comprehensive and fully integrated IT service management software suite that enables IT to improve service levels, balance resources and control costs. With embedded ITIL-based best practices, ServiceCenter lets people deploy consistent, integrated work processes across every part of the IT organization.

Incident

Any event which is not a part of the standard operation of a system that causes, or may cause, an interruption to, or a reduction in, the quality of service. It can be registered into a Service Desk that assigns an incident ticket in order to improve its traceability from its report to its resolution.

Request For Change (RFC)

A Request For Change is a mean of proposing a change to any component of an IT Infrastructure or any aspect of an IT Service. It is the initial point of the ITIL Change Management process.

Web Services (WS)

Web Services can be defined as a software system designed to support interoperable Machine to Machine interaction over a network.