HP Business Availability Center

for the Windows and Solaris operating systems

Software Version: 8.05

New Content in Business Availability Center 8.05

Document Release Date: September 2010
Software Release Date: September 2010

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 Notices

Trademark Notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Intel®, Pentium®, and Intel® Xeon™ are trademarks of Intel Corporation in the U.S. and other countries.

Java™ is a US trademark of Sun Microsystems, Inc.

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

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California.

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 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

Table of Contents

Service Level Management Web Services API

This chapter includes:

Concepts

Reference

Concepts

Introducing the SLM Web Services API

The SLM Web Services API is an integration tool for Service Level Management, enabling administration of agreements (SLAs) from an application either internal or external to Business Availability Center. The SLM Web services support the creation and management of agreements, including in an HP Software-as-a-Service deployment.

Prerequisite Knowledge

Users of the API should be familiar with Service Level Management administration and SOAP concepts.

Permissions

The administrator provides login credentials for connecting with the Web services. The credentials must be those of a user with Administrator permissions, or the agreement owner.

For details on setting permissions in the Permissions Manager, see "Permissions Overview" in *Platform Administration*.

Supported Operations

The following Web service operations are supported:

- Create SLA (with no CI)
- Get SLA general properties
- Update SLA general properties
- Delete SLA
- Add Service to SLA
- Delete Service from SLA
- Get Services that are included in the SLA

Using the SLM Web Services

The SLM Web Services API enables submitting a service request. The engine returns an error description if it cannot parse the statement or does not run successfully. If there is no error, the results of the request are returned.

The Web services are described in a SOAP WSDL file, located at:

http://<server>:8080/slm_ws/services/SlmServices?wsdl

The port specification is only necessary for non-standard installations. Consult your system administrator for the correct port number.

Developers can use a development environment to generate code from WSDL for calling the Web services. The WSDL describes the interface operations and operation parameters.

Reference

SLM Web Services' Operations

This section describes the operations for the SLM Web services.

createSLA

Creates a new agreement with the specified properties.

Operation signature:
String createSLA(String customerId, SlaPropertiesDTO properties)

Operation arguments:

Argument	Description
customerId	Typically 1 (apart from in an HP Software-as-a-Service environment).
properties	The properties used for initializing the new agreement, as follows: name,description,agreementDetails,type(OLA, SLA,UC), classification (internal, external); startDate,endDate,timeZoneId,customerId, providerId,trackingPeriods

Return-value: Returns the ID of the SLA in the CMDB.

Exception: Throws SlmWebServiceException if the user cannot create another agreement; for example, because the user does not have the necessary permissions to create the agreement, or if the number of allowed agreements has been reached.

updateSLA

Updates the agreement with the new properties.

Operation signature:
updateSLA(String customerId, String SLAId, SlaPropertiesDTO properties)

Operation arguments:

Argument	Description
customerId	Typically 1 (apart from in an HP Software-as-a-Service environment).
SLAId	The CMDB ID of the agreement to update.
properties	The properties to be updated.

Exceptions:

- Throws SlaDoesNotExistsException if an agreement with the given ID does not exist.
- Throws SlmWebServiceException if a system problem occurs that prevents the operation to execute successfully.

deleteSLA

Deletes the specified agreement.

Operation signature:
deleteSLA(String customerId, String SLAId)

Operation arguments:

Argument	Description
customerId	Typically 1 (apart from in an HP Software-as-a-Service environment).
SLAId	The CMDB ID of the agreement you want to delete.

Exception: Throws SlmWebServiceException when any type of error occurs.

getSLAProperties

Retrieves the properties of the specified agreement.

Operation signature:
SlaPropertiesDTO getSLAProperties(String customerId, String SLAId)

Operation arguments:

Argument	Description
customerId	Typically 1 (apart from in an HP Software-as-a-Service environment).
SLAId	The CMDB ID of the agreement with the properties you want to retrieve.

Exception: Throws SlmWebServiceException when any type of error occurs.

addServicesForSLA

Adds the specified Services and their impact sub-tree to the agreement. The matching service offering is used for each Service.

Operation signature:
String[] addServicesForSLA(String customerId, String slaId, serviceFullPath[] serviceFullPath)

Operation arguments:

Argument	Description
customerId	Typically 1 (apart from in an HP Software-as-a-Service environment).
SLAId	The CMDB ID of the agreement to which you want to add Services.
serviceFullPath	An array of services IDs according to their topology relation in the CMDB. For example, in order to add the hierarchy of services A --> B --> C, provide a **serviceFullPath** object with the services IDs from left to right.

Return-value: Returns an array of validation error messages (empty array if none).

Exception: Throws SlmWebServiceException if a system problem occurs that prevents the operation from executing successfully.

deleteServiceFromSLA

Removes the specified Services and their paths from the specified agreement.

Operation signature:
deleteServiceFromSLA(String customerId, String SLAId, Service[] services)

Operation arguments:

Argument	Description
customerId	Typically 1 (apart from in an HP Software-as-a-Service environment).
SLAId	The CMDB ID of the agreement from which you want to remove the Services.
services	The Services you want to remove from the agreement. Each Service includes: serviceId, serviceName If serviceId is missing, the server will try to obtain it using the serviceName.

Exceptions: Throws SlmWebServiceException when any type of error occurs.

getSLAServicesFullPath

Retrieves the Services of the specified agreement.

Operation signature:
ServiceFullPath[] getSLAServicesFullPath(String customerId, String SLAId)

Example: Example of SLA with Services 4, 5:

{id1, id2, id3, id4}
{id1, id2, id5}

Operation arguments:

Argument	Description
customerId	Typically 1 (apart from in an HP Software-as-a-Service environment).
SLAId	The CMDB ID of the agreement

Return-value: Returns the full paths of the Services in the agreement.

Exceptions: Throws SlmWebServiceException when any type of error occurs.

getServiceSLAs

Returns the agreements that include the specified Service.

Operation signature:
String[] getServiceSLAs(String customerId, String serviceId)

Operation arguments:

Argument	Description
customerId	Typically 1 (apart from in an HP Software-as-a-Service environment).
serviceId	The CMDB ID of the Service.

Return-value: Returns an array of agreement IDs that include the specified Service.

Exceptions: Throws SlmWebServiceException when any type of error occurs.

CMDB Connection Infrastructure Settings for Dashboard

Within the Dashboard application, the Console page includes the Changes & Incidents tab. By default, the Changes & Incidents tab displays data from the CMDB based on the following default connection settings: The port to connect to the CMDB is 8080, the protocol is http, and the CMDB host name is the host where the CMDB service is running.

However, in some environments these settings may be modified due to security needs. Three new infrastructure settings enable you to specify non-default CMDB connection settings, as follows:

- **CMDB machine host name.** Host name of the machine where CMDB is installed.
- **CMDB connection port.** Port number to use when connecting to CMDB.
- **CMDB connection protocol.** Protocol to use when connecting to CMDB (http/https).

To customize these connection settings, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**:

1. Select **Applications**.
2. Select **Dashboard Application**.
3. In the **Dashboard Application - Dashboard Layout Properties** area, modify the above settings.

Configure a Notification SNMP Trap for a CI Status Alert

This chapter includes:

Concepts

Tasks

Reference

Concepts

SNMP Traps

You can configure a Simple Network Management Protocol (SNMP) trap and attach it to an alert. The SNMP trap includes Object Identifiers (OIDs) and their values based on the alert's data.

The SNMP trap is sent when the alert criteria is met and the alert is triggered.

You can then view the alert notice with any SNMP management console. For detail on setting SNMP traps, see "How to Configure a Notification SNMP Trap" on page 21.

The MIB file, located at **<HPBSM root directory on the Data_processing Server>\HPBAC\SNMP_MIBS\CIAlerts.mib**, contains the mapping of Object Identifiers (OIDs) to alert-related data. The mapping is detailed in "Alerts MIB Varbinds" on page 23.

The alert type and its SNMP-specific code is detailed in "SNMP-Specific Codes" on page 23.

To configure SNMP traps, see "How to Configure a Notification SNMP Trap" on page 21.

The SNMP trap is sent when the alert criteria is met and the alert is triggered. You can view the alert notice with any SNMP management console in your organization.

Tasks

How to Configure a Notification SNMP Trap

You can configure an SNMP trap and attach it to an alert. This SNMP trap is sent when the alert criteria is met. The alert notice can be viewed with any SNMP management console in the organization.

This task includes the following steps:

- "Set up the appropriate administrative privileges" on page 21
- "Specify the host address of the SNMP trap" on page 22
- "Check the mapping of the OIDs to the alert data and configure the Alerts MIB – optional" on page 22

1 Set up the appropriate administrative privileges

You can set the appropriate administrative privileges to create a command that can be attached to an alert scheme and run when the alert it is attached to is triggered.

To set the appropriate administrative privileges:

a Select **Admin** > **Platform** > **Users and Permissions** > **User Management**.

b Select the appropriate user in the left column, and click the **Permissions** tab.

c Select the **Monitors** context, and under Active user, click **Alerts - Run executable file**.

d Click the **Operations** tab, and select the **Change** option.

2 Specify the host address of the SNMP trap

You specify the default host address of the SNMP trap in the Create New/ Edit SNMP Trap dialog box. For user interface details, see "Create New/ Edit SNMP Trap Dialog Box" in "CI Status Alerts" in *Alerts*.

You can also specify a global default host address in the Infrastructure Settings. For details, see the **Default SNMP Target Address/Default SNMP Port** in "Modify the alerts triggering defaults" in "How to Customize Alerts" in *Platform Administration*.

3 Check the mapping of the OIDs to the alert data and configure the Alerts MIB – optional

If you enabled alerts through SNMP traps in your alert schemes, it is recommended that you configure your SNMP management console to read the alerts MIB. This configuration enables you to see a name, rather than an Object ID (OID), when working in the management console.

Note: HP Business Service Management uses the AM alerts MIB 5.0 by default.

To configure the alerts MIB in your SNMP management console:

a Copy the **<HPBSM root directory on the Data_processing Server>\ HPBAC\SNMP_MIBS\CIAlerts.mib file** from the HP Business Service Management Documentation and Utilities DVD to your SNMP management console.

b To view the alerts varbinds, use your SNMP management console's MIB browser. For a list of varbinds and their descriptions, see "Alerts MIB Varbinds" on page 23.

c Using your SNMP management console's event configuration utility, configure the notification content and method for the various alert types. For a list of alert types and their corresponding SNMP-specific codes, see "SNMP-Specific Codes" on page 23.

Reference

SNMP-Specific Codes

The SNMP-specific code for a CI Status alert is **1**. Its type is: **CI Status Alert**.

Use this code when configuring CI Status alerts in your SNMP management console. For details, see "How to Configure a Notification SNMP Trap" on page 21.

Alerts MIB Varbinds

The tables list the varbinds used in the alerts MIB. For task details, see "How to Configure a Notification SNMP Trap" on page 21.

Object Identifier	MIB Label	Description
1.3.6.1.4.1.5233	HP	Company name
1.3.6.1.4.1.5233.6	ciAlerts	Subject
1.3.6.1.4.1.5233.6.1	alerted	Unique alert ID
1.3.6.1.4.1.5233.6.2	alertName	Alert name
1.3.6.1.4.1.5233.6.3	alertDescription	Alert description
1.3.6.1.4.1.5233.6.4	alertEventTime	Time when the event occurred. This is the event that triggered the alert.
1.3.6.1.4.1.5233.6.5	alertCIId	The ID of the CI whose status change triggered the alert
1.3.6.1.4.1.5233.6.6	alertCIName	The name of the CI whose status change triggered the alert

Object Identifier	MIB Label	Description
1.3.6.1.4.1.5233.6.7	alertKPIId	The ID of the KPI whose status change triggered the alert. The KPI is attached to the CI related to the alert.
1.3.6.1.4.1.5233.6.8	alertKPIName	The name of the KPI whose status change triggered the alert. The KPI is attached to the CI related to the alert.
1.3.6.1.4.1.5233.6.9	detailedDescription	The detailed description of the alert.
1.3.6.1.4.1.5233.6.10	alertPrevious Severity	Previous severity of the CI
1.3.6.1.4.1.5233.6.11	alertNextSeverity	Current severity of the CI (the change from previous severity to current severity is what triggered the alert).
1.3.6.1.4.1.5233.6.12	alertBACURL	The URL of the BSM Gateway server
1.3.6.1.4.1.5233.6.13	actualTime	When the triggering condition is related to time, this is the actual time when the CI has breached the condition. For other condition types, this value is N/A.
1.3.6.1.4.1.5233.6.14	conditionDescription	The description of the condition that triggered the alert.
1.3.6.1.4.1.5233.6.15	localImpactView	The name of the view when the CI that triggered the alert is part of the local impact view.