

HP Operations Orchestration

For the Windows and Linux operating systems

Software Version: Content Pack 16

Amazon Security Token Service Integration Guide

Document Release Date: November 2014

Software Release Date: November 2014



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

© Copyright 2014 Hewlett-Packard Development Company, L.P.

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.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

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

Contents

| | |
|---|----|
| Amazon Security Token Service Integration Guide..... | 1 |
| Contents..... | 5 |
| Amazon Security Token Service Introduction..... | 6 |
| Overview of Amazon Security Token Service Integration..... | 6 |
| Supported Versions..... | 6 |
| Downloading OO Releases and Documents on HP Live Network..... | 6 |
| Getting Started with the Amazon Security Token Service Integration..... | 8 |
| Installing and Configuring the Integration..... | 8 |
| Amazon Security Token Service Use Cases..... | 8 |
| Amazon STS — OO Integration Architecture..... | 9 |
| Location of Security Token Service Integration Operations and Flows in OO Studio..... | 9 |
| Troubleshooting..... | 10 |
| Troubleshooting Overview..... | 10 |
| General Troubleshooting Procedures and Tools..... | 10 |
| Error Messages..... | 10 |
| Security..... | 12 |
| Tools..... | 13 |

Chapter 1

Amazon Security Token Service Introduction

This chapter includes:

| | |
|---|---|
| Overview of Amazon Security Token Service Integration..... | 6 |
| Supported Versions..... | 6 |
| Downloading OO Releases and Documents on HP Live Network..... | 6 |

Overview of Amazon Security Token Service Integration

This integration enables you to request temporary, limited-privilege credentials for AWS Identity and Access Management (IAM) users or for users that you authenticate (federated users).

Security Token Service (STS) integrates with Amazon EC2. To use this integration successfully, you should have knowledge of STS, EC2, and IAM technology. This means that someone with an AWS account or an IAM user can request temporary access credentials for another AWS account for an IAM user, or even for a user that does not have an AWS account (federated user).

The credentials include a temporary Access Key ID, a Secret Access Key and a generated security token. You can use these credentials to access the EC2 services and resources. When the request for credentials is made using Get Federation Token, you can set the permissions inline for these credentials. When Get Session Token is used, the permissions are transferred from the user making the request to the generated credentials.

This document explains how this integration has been implemented and how the operations included communicate between OO and Security Token Service (STS).

Supported Versions

| Operations Orchestration Version | Amazon Security Token Service Version |
|----------------------------------|---------------------------------------|
| OO Content Pack 16 | STS API Version 2011-06-15 |

Downloading OO Releases and Documents on HP Live Network

HP Live Network provides an Operations Orchestration Community page where you can find and download supported releases of OO and associated documents.

To download OO releases and documents, visit the following site:

<https://hpln.hp.com/>

Note: This site requires that you register for an HP Passport and sign-in.

To register for an HP Passport ID:

1. Go to: <http://h20229.www2.hp.com/passport-registration.html>

Or

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

2. On the HP Live Network page, click **Operations Orchestration Community**. The Operations Orchestration Community page contains links to announcements, discussions, downloads, documentation, help, and support.
3. On the left-hand side, click **Operations Orchestration Content Packs**.
4. In the **Operations Orchestration Content Packs** box, click **Content**. The HP Passport and sign-in page appears.
5. Enter your user ID and Password to access to continue.
6. Click **HP Operations Orchestration 9.00**.
7. Search for the required HP Operations Orchestration Content Pack.

Chapter 2

Getting Started with the Amazon Security Token Service Integration

This chapter includes:

| | |
|--|---|
| Installing and Configuring the Integration | 8 |
| Amazon Security Token Service Use Cases | 8 |
| Amazon STS — OO Integration Architecture | 9 |
| Location of Security Token Service Integration Operations and Flows in OO Studio | 9 |

Installing and Configuring the Integration

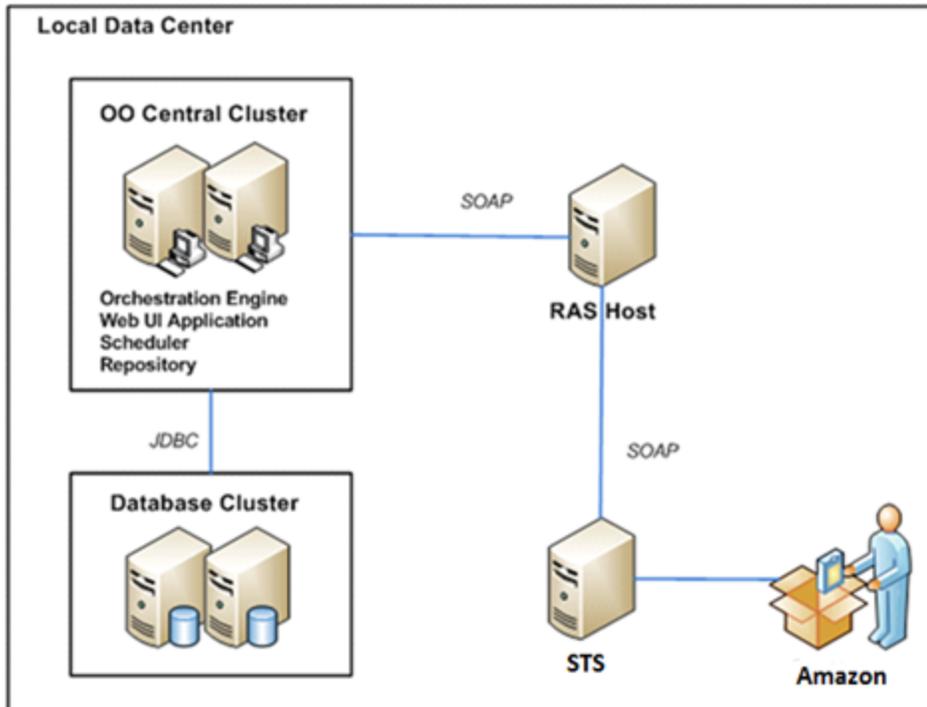
No special installation and configuration instructions are required for the Amazon Security Token Service integration. To use Amazon Security Token Service, you need to have an AWS account ID.

Amazon Security Token Service Use Cases

The following are the major use cases for the Amazon STS integration, and the operations that you can use to implement them.

1. Request temporary access credentials for AWS Identity or IAM user:
 - Get Session Token
2. Request temporary access credentials for non-AWS account (federated user):
 - Get Federation Token

Amazon STS — OO Integration Architecture



Location of Security Token Service Integration Operations and Flows in OO Studio

The Security Token Service integration includes the following operations in the **OO Studio Library/Integrations/Amazon/Security Token Service** folder.



Chapter 3

Troubleshooting

This chapter includes:

| | |
|---|----|
| Troubleshooting Overview..... | 10 |
| General Troubleshooting Procedures and Tools..... | 10 |
| Error Messages..... | 10 |

Troubleshooting Overview

This section provides troubleshooting procedures and tools you can use to solve problems you may encounter while using this integration. It also includes a list of the error messages you may receive while using the integration and offers descriptions and possible fixes for the errors.

General Troubleshooting Procedures and Tools

When troubleshooting issues related to the STS integration, verify the following:

1. The same operation works when it is performed through the STS console using the same parameters.
2. Your access key and proxy parameters are correct.
3. If the credentials used to request credentials for a federated user belong to an IAM user, check if this IAM user has permission to call the Get Federation Token service.
4. When these credentials are used to access an EC2 service or resource, check if the correct policy is attached to them.

Error Messages

This section lists the error messages you may receive while using this integration.

- The request signature does not conform to AWS standards. Error code: `IncompleteSignature`
- The request processing has failed due to some unknown error, exception or failure. Error code: `InternalFailure`
- The action or operation requested is invalid. Error code: `InvalidAction`
- The X.509 certificate or AWS Access Key ID provided does not exist

in our records. Error code: InvalidClientTokenId

- Parameters that must not be used together were used together. Error code : InvalidParameterCombination
- A bad or out-of-range value was supplied for the input parameter. Error code : InvalidParameterValue
- AWS query string is malformed, does not adhere to AWS standards. Error code: InvalidQueryParameter
- The query string is malformed. Error code: MalformedQueryString
- The request is missing an action or operation parameter. Error code: MissingAction
- Request must contain either a valid (registered) AWS Access Key ID or X.509 certificate. Error code: MissingAuthenticationToken
- An input parameter that is mandatory for processing the request is not supplied. Error code: MissingParameter
- The AWS Access Key ID needs a subscription for the service. Error code: OptInRequired
- Request is past expires date or the request date (either with 15 minute padding), or the request date occurs more than 15 minutes in the future. Error code: RequestExpired
- The request has failed due to a temporary failure of the server. Error code: ServiceUnavailable
- Request was denied due to request throttling. Error code: Throttling
- Failed to open HTTP connection
- The value for durationSeconds input should be between 3600 and 129600
- The value for durationSeconds should be an integer.
- AWS was not able to validate the provided access credentials. Error code: AuthFailure.

Chapter 4

Security

This section describes how security is handled by the Amazon STS integration.

The STS integration uses the Amazon STS Query API. To perform its task, each STS operation sends a query to Amazon. This query is sent over HTTPS and the Symphony Client library is used for sending the actual requests. Every STS operation has two inputs: **accessKey** and **accessKeyId**. These are provided by Amazon for every Amazon account.

According to Amazon, in addition to the name of the action and the list of parameters, you must include a signature in every query request. The signature is created by using the **accessKey** provided by the user. The steps for creating a signature are described on the Amazon Web site at http://docs.amazonwebservices.com/IAM/latest/UserGuide/IAM_UsingQueryAPI.html#query-authentication and are implemented by the operations.

The STS integration uses version 2 of the signature. For calculating an RFC 2104-compliant HMAC with the query string created by using the input parameters, the integration use the secret Access Key as the key, and SHA1 as the hash algorithm. You should not perform any special configurations; just provide the **accessKey** and **accessKeyId**.

Chapter 5

Tools

Following are OO tools that you can use with the Amazon STS integration:

- **RSFlowInvoke.exe** and **JRSFlowInvoke.jar**

RSFlowInvoke (**RSFlowInvoke.exe** or the Java version, **JRSFlowInvoke.jar**) is a command-line utility that allows you to start a flow without using Central (although the Central service must be running). RSFlowInvoke is useful when you want to start a flow from an external system, such as a monitoring application that can use a command line to start a flow.

- **Web Services Wizard (wswizard.exe)**

When you run the Web Services Wizard, you provide it with the WSDL for a given Web service. The WSDL string you provide as a pointer can be a file's location and name or a URL. The Web Services Wizard displays a list of the methods in the API of the Web service that you specify. When you run the wizard, pick the methods you want to use, and with one click for each method you have selected, the wizard creates an HP OO operation that can execute the method. This allows you to use the Web Services Wizard to create operations from your monitoring tool's API.

These tools are available in the Operations Orchestration home folder in **/Studio/tools/**.