HP Operations Orchestration

For the Windows and Linux operating systems

Software Version: Content Pack 16

Amazon Identity and Access Management 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

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

Chapter 1

Amazon Identity and Access Management Introduction

This chapter includes:

Purpose of the Amazon Identity and Access Management Integration (IAM)

With this integration, administrators can create HP Operations Orchestration (OO) flows that are integrated with Amazon Identity and Access Management (IAM).

AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users. IAM enables you to create and manage users in AWS, and it also enables you to grant access to AWS resources for users managed outside of AWS in your corporate directory. IAM offers greater security, flexibility, and control when using AWS. IAM enables identity federation between your corporate directory and AWS services. This enables you to use your existing corporate identities to grant secure and direct access to AWS resources, such as S3 buckets, without creating a new AWS identity for those users.We have implemented some basic operations for users, access credentials, and permissions management provided by the IAM API Version 2010-05-08.

To learn how to create OO flows, see the Studio Guide to Authoring Operations Orchestration Flows in the documentation set for the current OO release. The IAM integration uses the IAM Query API released on 2010/05/08 to integrate with OO. IAM integrates with EC2, VPC, Load Balancing, and Security Token Service Amazon Integrations.

Audience

This guide is intended for users who have an Amazon AWS account and wish to create and manage users in AWS.

Prerequisites

To use this integration successfully, you should have knowledge of the IAM technology.

Useful links and resources:

- AWS Identity and Access Management. For details, see http://aws.amazon.com/iam/.
- IAM API reference. For details, see, http://docs.amazonwebservices.com/IAM/latest/APIReference/API_Operations.html

Supported Versions

Operations Orchestration Version	Amazon Identity and Access Management
OO Content Pack 16	IAM API version 2010-05-08

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

This chapter includes:

Installing and Configuring the Integration

No special instalation and configuration instructions are required for IAM integration. To use IAM, you need to have an AWS account ID or credentials of an IAM user (that has permission to use IAM) belonging to an AWS account.

Use Cases

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

1. Manage user policies:
   - Delete User Policy
   - Get User Policy
   - List User Policy
   - Put User Policy
2. Manage security credentials:
   - Create Access Key
   - Delete Access Key
   - List Access Keys
   - Update Access Key
3. Manage user permissions:
   - Create User
   - Delete User
   - Get User
   - Update User

4. Create Administrator IAM user:
   a. Create an IAM user using the **Create User** operation.
   b. Apply IAM policy to enable full access to Amazon services and resources using the **Put Policy** operation and using this policy as input. The policy used is:

```
{
  Statement":[
    {
      "Effect":"Allow",
      "Action":"*"
      "Resource":"*"
    }
   ]
}
```

   c. Call the **Get User** operation using the newly created user credentials to check if the user is available and ready to use.
5. Enable an IAM user to manage his own credentials.
   a. Create an IAM user using the **Create User** operation.
   b. Get an ARN (Amazon Resource Name) using the **Get User** operation (one of the outputs of the **Get user** operation is called ARN).
   c. Use this ARN to create a policy document that allows the users to manage their own credentials and apply this policy using **Put Policy** operation. The policy used is:

```
{
   "Statement":[{
   "Effect":"Allow",
   "Action":["iam:*AccessKey*"],
   "Resource":"${arn}"
  }
 ]
}
```

   where ${arn} is the output of the Get User operation.
6. Enable an IAM user access to some EC2 services:

   Apply this policy to an IAM user:

```
{
   "Statement":[
   {
     "Action":[
     "ec2:RunInstances",
     "ec2:StopInstances",
     "ec2:StartInstances",
     "ec2:TerminateInstances",
     "ec2:DescribeInstances"
```

```
      "Effect": "Allow",
      "Resource": "*"
      }
    ]
}
```

As a result, this user has access to the RunInstances, StopInstances, StartInstances, TerminateInstances, and DescribeInstances EC2 services.

7. Provide perimeter control

   Add a policy to IAM user that denies an AWS request from a user if the originating IP address is outside the corporation network using the **Put Policy** operation. The policy used is:

```
{
   "Statement":[{
   "Effect":"Deny",
   "Effect":"Deny",
     "Action":
       [
        "ec2:RunInstances",
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstances"
       "iam:*"
       ]
     "Resource":"*",
     "Condition":{
       "NotIpAddress":{
         "aws:SourceIp":["15.0.0.0/8","16.0.0.0/8"]
       }
     }
   }
 ]
]
```

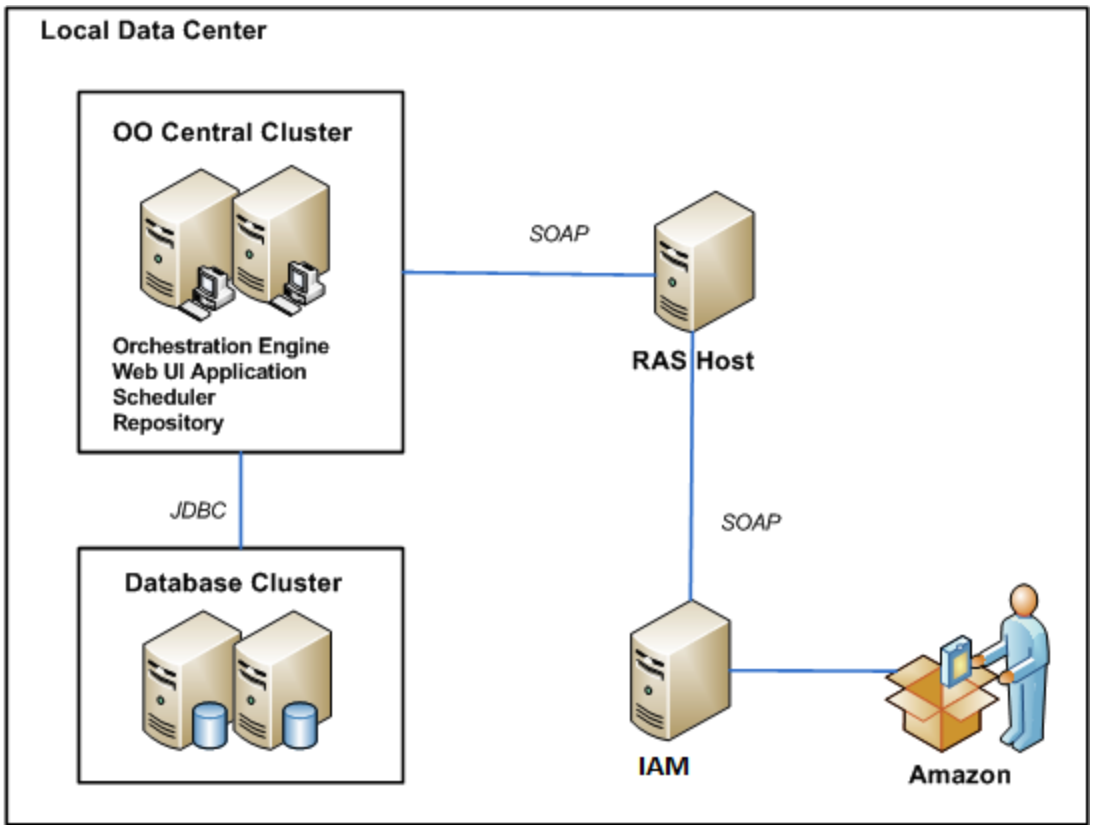
Using these use cases, the following end-to-end scenario can be created:

Initial setup of a company's IAM users:

- Using the AWS paying account credentials, first create an AWS Administrator (an IAM user with full access to all Amazon services and resources). (The subflow is located at **Library\Integrations\IAM\Samples\Create IAM Accounts\Create Administrator**.)
- Read a file with the user name and email address of the company's employees. (The subflow is located at **Library\Integrations\IAM\Samples\Create IAM Accounts\Get Employees Info**).
- The administrator creates an IAM account and sets permissions for every employee listed in the file. Therefore, every IAM user is able to manage his own credentials and access EC2 services as long as the source IP from which the administrator makes the AWS request, belongs to certain IP ranges. (The flow is located at **Library\Integrations\IAM\Samples \Create IAM Accounts\Create IAM Accounts**.)

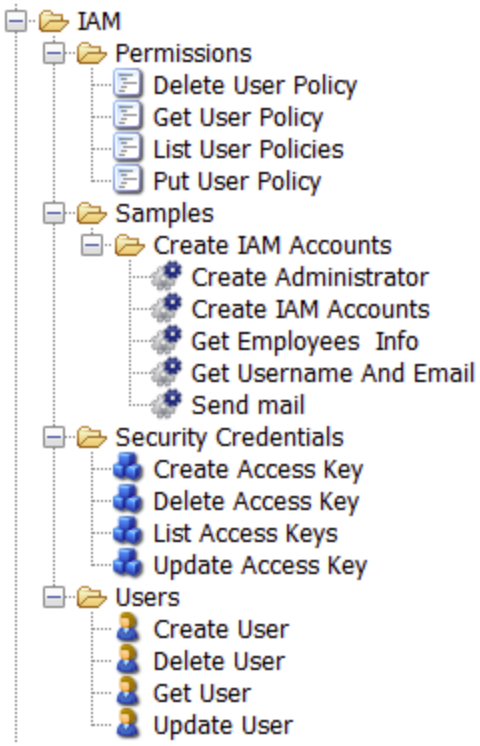
- After the account is created, every employee receives an email notification listing the employee's AWS credentials and permissions. (The subflow is located at **Library\Integrations\IAM\Samples\Create IAM Accounts\Send mail**.)

IAM - OO Integration Architecture



Location of IAM Integration Operations in OO Studio

The IAM integration includes the following operations in the OO Studio Library/Integrations/Amazon/IAM folder.


IAM
Permissions
Delete User Policy
Get User Policy
List User Policies
Put User Policy
Samples
Create IAM Accounts
Create Administrator
Create IAM Accounts
Get Employees Info
Get Username And Email
Send mail
Security Credentials
Create Access Key
Delete Access Key
List Access Keys
Update Access Key
Users
Create User
Delete User
Get User
Update User

Chapter 3

Troubleshooting

This chapter includes:

Troubleshooting Overview

This section provides troubleshooting procedures and tools that 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 IAM integration, verify that:

- The same operation works when it is performed through the IAM console using the same parameters.
- Your access key and proxy parameters are correct.
- When using Delete User, the user you want to delete does not have policies attached because a user that has policies attached cannot be deleted.
- When using Create User, you set the generate credentials input to **true** if you want this user to be able to authenticate itself when using other Amazon services provided by OO.
- If the credentials used for authentication when using these operations belong to an IAM user, this IAM user has permission to access the IAM services.
- The policy you want to attach to the user respects the IAM policy language.

Error Messages

This section lists the error messages you may receive while using this integration. Each error message includes possible causes and fixes for the error.

- `InvalidClientTokenId`

  The security token included in the request is invalid.

- `This user has policies attached. Please delete the policies first and then delete the user.`
- `IncompleteSignature`

  The request signature does not conform to AWS standards.
- `InternalFailure`

  The request processing has failed due to some unknown error, exception or failure.
- `InvalidAction`

  The action or operation requested is invalid.
- `InvalidParameterCombination`

  Parameters that must not be used together were used together.
- `InvalidParameterValue`

  A bad or out-of-range value was supplied for the input parameter.
- `InvalidQueryParameter`

  The query string is malformed, does not adhere to AWS standards.
- `MalformedQueryString`

  The query string is malformed
- `MissingAction`

  The request is missing an action or operation parameter.
- `MissingAuthenticationToken`

  The request must contain either a valid (registered) AWS Access Key ID or X.509 certificate.
- `MissingParameter`

  An input parameter that is mandatory for processing the request is not supplied.
- `OptInRequired`

  The AWS Access Key ID needs a subscription for the service.
- `RequestExpired`

  The request is past the expiry date or the request date (either with 15 minute padding), or the request date occurs more than 15 minutes in the future.
- `ServiceUnavailable`

  The request has failed due to a temporary failure of the server.
- `Throttling`

  The request was denied due to request throttling.

Chapter 4

Security

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

The IAM integration uses the IAM Query API. To perform its task, each IAM 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 IAM 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/AWSEC2/2009-04-04/DeveloperGuide/index.html?using-query-api.html, and are implemented by the operations.

The IAM 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 uses the Secret Access Key as the key, and SHA1 as the hash algorithm. You should not perform any special configuration other than providing the **accessKey** and **accessKeyId**.

Chapter 5

OO Tools You Can Use with the Amazon IAM – OO Integration

Following are OO tools that you can use with the Amazon IAM 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.

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