AWS Data Provider for SAP

Installation and Operations Guide

AWS Data Provider Version 2.9

February 2018

Notices

Contents

Abstract

The Amazon Web Services (AWS) Data Provider for SAP is a tool that collects performance-related data from AWS services. It makes this data available to SAP applications to help monitor and improve the performance of business transactions. The AWS Data Provider for SAP uses operating system, network, and storage data that is most relevant to the operation of the SAP infrastructure. Its data sources include Amazon Elastic Compute Cloud (Amazon EC2) and Amazon CloudWatch. This guide provides installation, configuration, and troubleshooting information for the AWS Data Provider for SAP on both Linux and Windows.

Introduction

Many organizations of all sizes are choosing to host key SAP systems in the Amazon Web Services (AWS) Cloud. With AWS, you can quickly provision an SAP environment. Additionally, the elastic nature of the AWS Cloud enables you to scale computing resources up and down as needed. As a result, your business can dedicate more resources (both people and funds) to innovation.

Many SAP systems operate daily business transactions and are critical to business functions. As an SAP customer, you need the ability to track and troubleshoot the performance of these transactions. The AWS Data Provider for SAP is a tool that collects key performance data that SAP applications can use to monitor transactions built by SAP. The data is collected from a variety of sources within your AWS Cloud operating environment, including Amazon Elastic Compute Cloud (Amazon EC2) and Amazon CloudWatch. This data includes information about the operating system, network, and storage that is relevant to your SAP infrastructure. Data from the AWS Data Provider for SAP is read by the SAP Operating System Collector (SAPOSCOL) and the SAP CIM Provider.

Figure 1 provides a high-level illustration of the AWS Data Provider for SAP, its data sources, and its outputs.
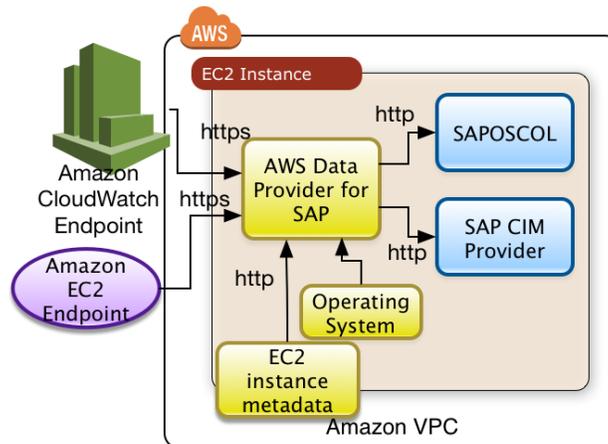
Figure 1: Data sources for the AWS Data Provider for SAP

The purpose of this guide is to help you:

- Understand the technical requirements and components necessary to install and operate the AWS Data Provider for SAP.

- Install the AWS Data Provider for SAP.

- Understand the update process for the AWS Data Provider for SAP.

- Troubleshoot installation issues.

Upgrading from Earlier Versions

The current version of the AWS Data Provider for SAP is version 2.9. For a list of changes in each version, see Appendix C. If you have an earlier version installed, we recommend that you uninstall it before installing the current version.

> **Note on versions 1.3 and 1.3.1**: If you've already installed and customized the AWS Data Provider for SAP version 1.3 or 1.3.1, save your proxy configuration from your custom proxy.properties file. Version 2.5 (or later) will look for these files in the same location as before.

Technical Requirements

Before creating an SAP instance, ensure that the following technical requirements are met.

Amazon VPC Network Topologies

You need to deploy SAP systems that receive information from the AWS Data Provider for SAP within an Amazon Virtual Private Cloud (Amazon VPC). You can use one of the following network topologies to enable routing to internet-based endpoints:

- The first topology configures routes and traffic directly to the AWS Cloud through an internet gateway within an Amazon VPC (see Figure 2). For more information about internet gateways, see the AWS documentation.[1]
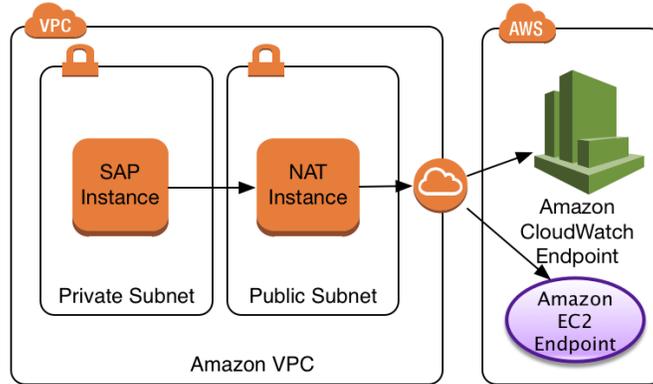
Figure 2: Connection to the AWS Cloud via an internet gateway

- A second topology routes traffic from the Amazon VPC, through your organization's on-premises data center, and back to the AWS Cloud (see Figure 3). For more information about this topology, see the AWS documentation.[2]
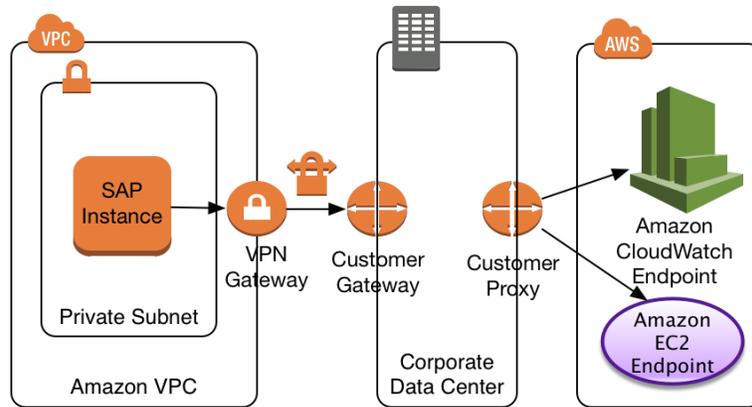
Figure 3: Connection to the AWS Cloud via an on-premises data center

IAM Roles

You need to grant the AWS Data Provider for SAP read-only access to the Amazon CloudWatch, Amazon S3, and Amazon EC2 services so that you can use their APIs. You can do this by creating an AWS Identity and Access Management (IAM) role for your EC2 instance and attaching a permissions policy.

To create an IAM role and grant permissions to your EC2 instance:

1. Sign in to the <u>AWS Management Console</u> and open the IAM console at <u>https://console.aws.amazon.com/iam/</u>.

2. In the navigation pane, choose **Roles**, and then choose **Create role**.

3. Choose the **AWS service** role type, and then choose **EC2**.
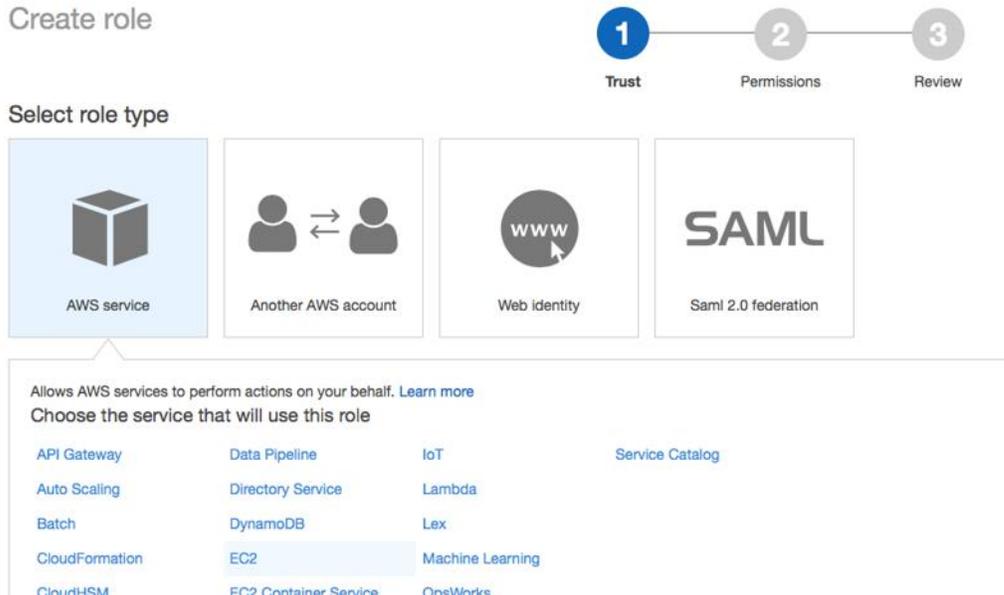
Figure 4: Creating a role for Amazon EC2

4. Choose **EC2** as the use case. Then choose **Next Permissions**.
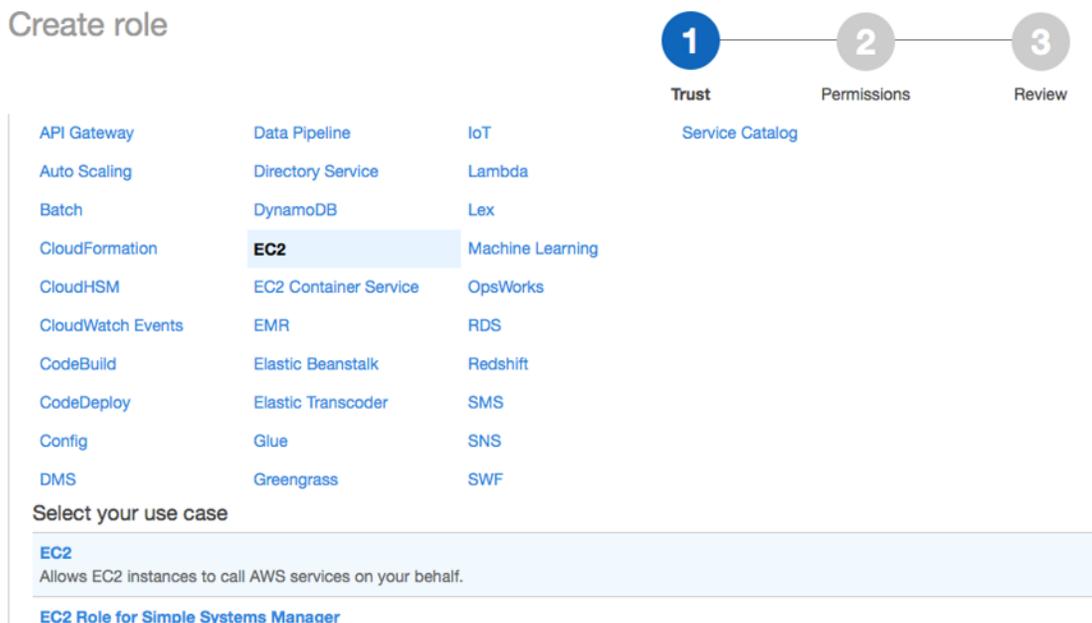
Figure 5: Select EC2 as your use case

5. Choose **Create policy**, and then choose **Create Your Own Policy**.
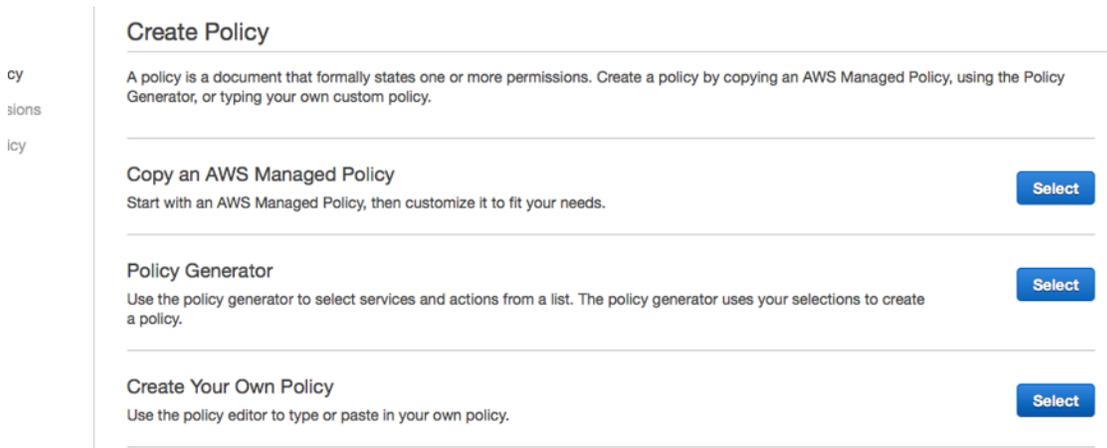
Figure 6: Create your own policy

6. For **Policy Name**, type a policy name. For **Description**, type a description for the new role. Next, copy and paste the following policy into the **Policy Document** box (see Figure 7).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "EC2:DescribeInstances",
        "EC2:DescribeVolumes"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "cloudwatch:GetMetricStatistics",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::aws-data-provider/config.properties"
    }
  ]
}
```

Review Policy

Customize permissions by editing the following policy document. For more information about the access policy language, see Overview of Policies in the *Using IAM* guide. To test the effects of this policy before applying your changes, use the IAM Policy Simulator.

Policy Name

DataProviderAccessPolicy

Description

This Policy Allows SAP systems to gather monitoring data from CloudWatch with the help of the AWS Data Provider for SAP

Policy Document

```
11        },
12 ▾      {
13          "Effect": "Allow",
14          "Action": "cloudwatch:GetMetricStatistics",
15          "Resource": "*"
16        },
17 ▾  {
18          "Effect": "Allow",
19          "Action": "s3:GetObject",
20          "Resource":
21          "arn:aws:s3:::aws-data-provider/config.properties"
22        }
23      ]
24  }
25
```

Figure 7: Customize permissions by editing the policy document

7. Choose **Create Policy**. The IAM console confirms the new policy with a message similar to the following.

✔ **DataProviderAccessPolicy** has been created.
You are now ready to attach your policy to users, groups, and roles.

Create policy   Policy actions ▾

Figure 8: Policy confirmation

8. Under **Policy actions**, choose **Attach** to attach the policy you just created in step 7 to your EC2 instance.

An alternative to the previous steps is to add the policy to a role, which gets assigned to a new EC2 instance.

Installing the AWS Data Provider for SAP

The AWS Data Provider for SAP is a daemon or service that automatically starts with your operating system and collects, aggregates, and exposes metrics to the SAP platform. Metrics are sourced from a variety of providers that pull metrics from the relevant areas of the platform. The AWS Data Provider for SAP is designed to continue operating, regardless of whether its providers have connectivity or permissions to access the AWS service metrics they are requesting. Providers that cannot reach the metrics they are harvesting return blank values.

For example, if your EC2 instance does not have an IAM role associated with it that grants explicit access to the CloudWatch **GetMetricStatistics** API, the CloudWatch provider will be unable to perform the GetMetricStatistics action on the EC2 instance and will return blank values.

The AWS Data Provider for SAP is designed to automatically update itself so that it can provide you with the most current metrics. When the AWS Data Provider for SAP starts up, a built-in update service retrieves the latest versions of its components and metric definitions. If the AWS Data Provider for SAP cannot access the update service, it will continue to run but won't be able to obtain updates.

Installing on Linux

Before installing the AWS Data Provider for SAP, install the "wget" and "bc" packages. The installation script needs these packages, and they are unlikely to be preinstalled on an Oracle Linux AMI.

To install the AWS Data Provider for SAP on SUSE Linux Enterprise Server (SLES) 11 or 12, Red Hat Linux, or Oracle Linux, with an IAM role assigned with the appropriate permissions to access CloudWatch and Amazon EC2, follow these steps:

1. Download the Linux installation script:
   https://s3.amazonaws.com/aws-data-provider/bin/aws-agent_install.sh

   Users in the China Region may use:
   https://s3.cn-north-1.amazonaws.com.cn/aws-data-provider/bin/aws-agent_install.sh

```
ls3115:~/test # wget https://s3.amazonaws.com/aws-data-provider/bin/aws-agent_install.sh
--2015-05-29 14:56:13--  https://s3.amazonaws.com/aws-data-provider/bin/aws-agent_install
.sh
Connecting to 147.204.6.19:8080... connected.
Proxy request sent, awaiting response... 200 OK
Length: 3499 (3.4K) [application/x-sh]
Saving to: `aws-agent_install.sh'

100%[====================================================>] 3,499        --.-K/s   in 0.001s

2015-05-29 14:56:14 (5.41 MB/s) - `aws-agent_install.sh' saved [3499/3499]
```

Figure 9: Downloading the Linux installation script

2. Make the script executable, and then run it.

```
ls3115:~/test # chmod +x aws-agent_install.sh
ls3115:~/test # ./aws-agent_install.sh █
```

Figure 10: Running the Linux installation script

If you don't have transparent HTTP/HTTPS access to the internet, start the script with the required information about the HTTP/HTTPS proxies, using the following syntax:

```
aws-agent_install.sh [proxy-host [proxy-port [ proxy-user-name
[proxy-user-password [domain]]]]]
```

where:

- *proxy-host* specifies the address of the HTTP proxy server (for example, 10.0.10.2).

- *proxy-port* specifies the port number of the HTTP proxy server (for example, 8080).

- *proxy-user-name, proxy-user-password,* and *domain* specify the credentials for the HTTP proxy server, if it requires authentication (these arguments are optional).

  You should see the script pulling down all the required files it needs, as shown.

```
Starting AWS agent installer.
16:53:10.564 I FFFFF **********************************************
                    *          AWS Data Collector         *
                    *          Library Update Service     *
                    **********************************************

16:53:11.467 I 0400B Updating file: jetty-server-7.6.5.v20120716/NOTICE.txt

16:53:11.539 I 0400B Updating file: sigar/libsigar-amd64-linux.so

16:53:11.687 I 0400B Updating file: commons-daemon-1.0.10/commons-daemon-1.0.10.jar

16:53:11.750 I 0400B Updating file: jackson-core-1.8.7/jackson-mapper-asl-1.8.7.jar

16:53:11.914 I 0400B Updating file: awsDataCollector.jar

16:53:11.997 I 0400B Updating file: wel4j-core/NOTICE.txt

16:53:12.048 I 0400B Updating file: wel4j-core/wel4j64.dll

16:53:12.103 I 0400B Updating file: velocity-1.7-dep/velocity-1.7-dep.jar

16:53:12.410 I 0400B Updating file: jetty-server-7.6.5.v20120716/LICENSE.txt
```

Figure 11: AWS Data Provider for SAP update service

At the very end, you will see the agent start as a daemon.

```
16:53:16.657 I 0400B Updating file: servlet-api-2.5.jar

16:53:16.717 I 0400C Updating local version manifest


*****
Starting the aws-agent service.
Starting aws-agent...                              Ok

Installer completed, exiting.
ip-10-32-59-140:~ #
```

Figure 12: Completing the installation on Linux

3. Verify that the service is running by calling `netstat -ant` to determine if the listener is running on localhost port 8888.

```
p-10-32-59-140:~ # netstat -ant
ctive Internet connections (servers and established)
roto Recv-Q Send-Q Local Address           Foreign Address         State
cp      0          0.0.0.0.22             0.0.0.0:*               LISTEN
cp      0      0 0.0.0.0:8888             0.0.0.0:*               LISTEN
cp      0      0 127.0.0.1:25             0.0.0.0:*               LISTEN
cp      0      0 0.0.0.0:111              0.0.0.0:*               LISTEN
cp      0     52 10.32.59.140:22          69.120.21.212:49759     ESTABLISHE
p-10-32-59-140:~ #
```

Figure 13: Verifying the installation on Linux

You should also view the log files at /var/log/aws-agent/messages to ensure the daemon has the appropriate connectivity and authorization to access the required metrics.

```
ip-10-32-59-140:~ # cat /var/log/aws-agent/messages
16:53:17.614 I 00001 ****** AWS SAP Data Collector Agent is Starting ******

16:53:17.621 I 00002 Software Version: 1.0.47 : Fri Sep 21 22:22:00 UTC 2012

16:53:17.622 I 0000C Agent log level has been set to INFO

16:53:17.624 I 08001  ** Running Diagnostics **

16:53:17.624 I 08002 Diagnostic : AWS Connectivity

16:53:18.353 I 08005 Diagnostic : Passed

16:53:18.353 I 08006 Diagnostic : Amazon CloudWatch Connectivity & Access

16:53:19.069 I 08009 Diagnostic : Passed

16:53:19.069 I 0800A Diagnostic : EC2 API Connectivity & Access

16:53:19.370 I 0800D Diagnostic : Passed

16:53:19.371 I 0800E ** Diagnostics Complete **

16:53:19.565 I 03002 vhostmd agent is listening on localhost

16:53:19.566 I 0000D Agent is starting the vhostmd provider

ip-10-32-59-140:~ #
```

Figure 14: Verifying connectivity and authorization on Linux

At startup, the monitoring agent runs three sets of diagnostics:

- The AWS connectivity diagnostic ensures network connectivity to Amazon S3 for obtaining automatic updates to the AWS Data Provider for SAP.

- The second diagnostic tests for authorization to access CloudWatch. This authorization requires assigning an IAM role to the EC2 instance you are running on with an IAM policy that allows access to CloudWatch. For details, see IAM Roles, earlier in this guide.

- The third diagnostic tests for authorization to access Amazon EC2, which also requires an IAM role associated with the EC2 instance.

The AWS Data Provider for SAP is designed to run with or without connectivity, but you can't obtain updates without connectivity. CloudWatch and Amazon

EC2 will return blank values if you don't have the proper authorizations in place.

You can also call the AWS Data Provider for SAP directly to view the metrics. Calling `wget http://localhost:8888/vhostmd` returns a file of metrics. You can look inside the file to see the metrics that were returned, as shown here.

```
ip-10-32-59-140:~ # wget http://localhost:8888/vhostmd
--2012-10-09 17:10:28--  http://localhost:8888/vhostmd
Resolving localhost... 127.0.0.1, ::1
Connecting to localhost|127.0.0.1|:8888... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/xml]
Saving to: `vhostmd'

    [ <=>                                                    ] 7,58

2012-10-09 17:10:31 (385 MB/s) - `vhostmd' saved [7589]

ip-10-32-59-140:~ # cat vhostmd
<?xml version="1.0" encoding="UTF-8"?>
  <metrics>
    <metric context="host" category="config" type="long" unit="posixtime"
      <name>Time Stamp</name>
      <value>1349802629284</value>
    </metric>
    <metric context="host" category="config" type="int64" unit="sec">
      <name>Refresh Interval</name>
      <value>60</value>
    </metric>
    <metric context="host" category="config" type="string" unit="none">
      <name>Cloud Provider</name>
      <value>Amazon Web Services</value>
    </metric>
    <metric context="host" category="config" type="string" unit="none">
      <name>Instance Type</name>
      <value>m1.large</value>
    </metric>
```

Figure 15: Viewing metrics on Linux

The AWS Data Provider for SAP now starts automatically each time the operating system starts. You can also manually stop and restart the AWS Data Provider for SAP with the following command, which depends on your operating system version:

- SLES 11, Oracle Linux 6, and Red Hat Linux 6:

```
service aws-agent [start|stop]
```

- SLES 12, Oracle Linux 7, and Red Hat Linux 7:

```
systemctl [start|stop] aws-agent
```

Installing on Windows

1. Open a web browser and download the installer from:
   https://s3.amazonaws.com/aws-data-provider/bin/aws-agent-installer-win-x64.exe

   Users in the China Region must use:
   https://s3.cn-north-1.amazonaws.com.cn/aws-data-provider/bin/aws-agent-installer-win-cn-x64.exe

2. Run the installer, and choose **Yes** when prompted. This installs and runs the AWS Data Provider for SAP as a Windows service.
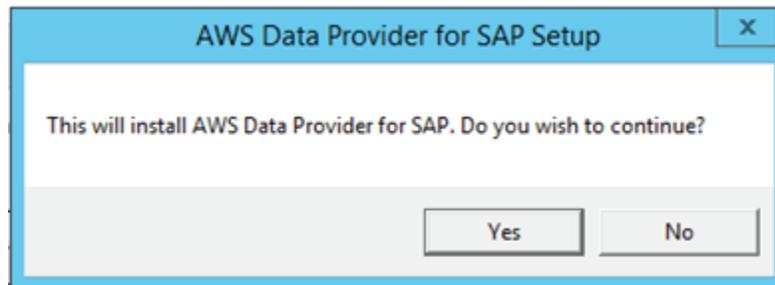
Figure 16: Running the Windows installation script

When the installation process is complete, you receive the following message.
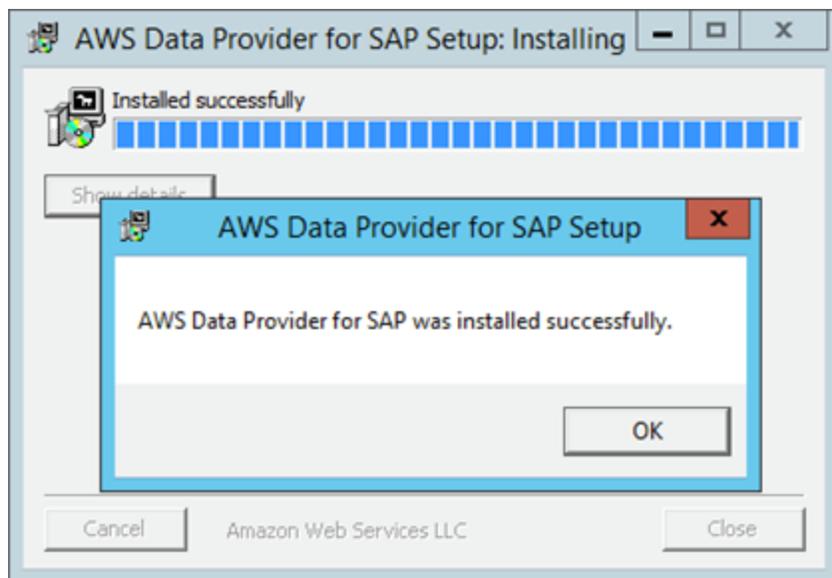
Figure 17: Completing the installation on Windows

3. Check the installation:

   - When the script has completed, the software is installed in the C:\Program Files\Amazon\DataProvider directory.

   - The installation also creates and starts a Windows service named **AWS Data Provider for SAP**.

   - To ensure that the service is running, you can open a web browser and type `http://localhost:8888/vhostmd`. If it's running, it returns pages of metrics from the AWS Data Provider for SAP.

4. Configure the AWS Data Provider for SAP to use proxies:

   - Stop the Windows service **AWS Data Provider for SAP**.

   - Enter the required proxy information into this file: C:\Program Files\Amazon\DataProvider\proxy.properties.

   - Restart the Windows service, **AWS Data Provider for SAP**.

   - When the service starts, it performs an update of the agent, and then works in standard mode.

5. Verify that the service is running by calling `netstat -ant` from a command window or from a Windows PowerShell script to determine if the listener is running on localhost port 8888.

Figure 18: Verifying the installation on Windows

6. Go to the Windows event log and look at the application log for startup events from the AWS Data Provider for SAP. In particular, you should look at the diagnostics.
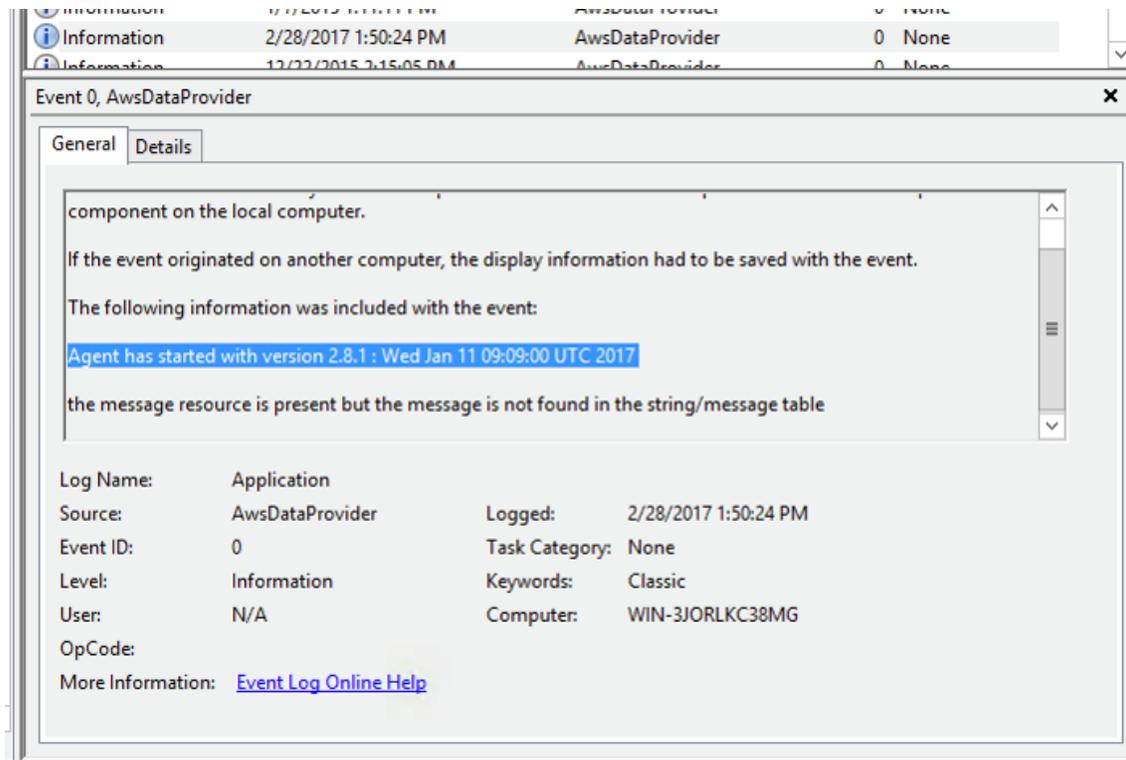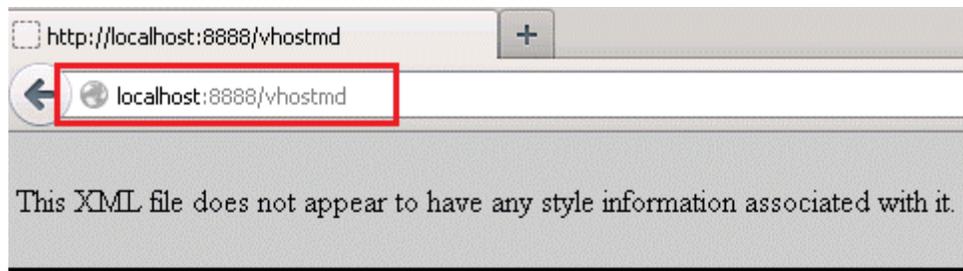

Figure 19: Checking diagnostics on Windows

At startup, the monitoring agent runs three sets of diagnostics:

- The AWS connectivity diagnostic ensures network connectivity to Amazon S3 for obtaining automatic updates to the AWS Data Provider for SAP.

- The second diagnostic tests for authorization to access CloudWatch, which requires assigning an IAM role to the EC2 instance you are running on with an IAM policy that allows access to CloudWatch. For details, see IAM Roles, earlier in this guide.

- The third diagnostic tests for authorization to access Amazon EC2, which also requires an IAM role associated with the EC2 instance.

The AWS Data Provider for SAP is designed to run with or without connectivity, but you can't obtain updates without connectivity. If you don't have the proper authorizations in place, CloudWatch and Amazon EC2 return blank values.

You can also call the AWS Data Provider for SAP directly from your web browser to view metrics, as shown in Figure 20.

```
http://localhost:8888/vhostmd          +

localhost:8888/vhostmd

This XML file does not appear to have any style information associated with it. T

— <metrics>
    — <metric context="host" category="config" type="long" unit="posixtime">
        <name>Time Stamp</name>
        <value>1349813196225</value>
      </metric>
    — <metric context="host" category="config" type="int64" unit="sec">
        <name>Refresh Interval</name>
        <value>60</value>
      </metric>
    — <metric context="host" category="config" type="string" unit="none">
        <name>Cloud Provider</name>
        <value>Amazon Web Services</value>
      </metric>
    — <metric context="host" category="config" type="string" unit="none">
        <name>Instance Type</name>
        <value>m1.xlarge</value>
      </metric>
```

Figure 20: Viewing metrics on Windows

The AWS Data Provider for SAP now starts automatically each time the operating system starts. You can also manually stop and restart the AWS Data Provider for SAP, just as you would stop and restart any other Windows service.
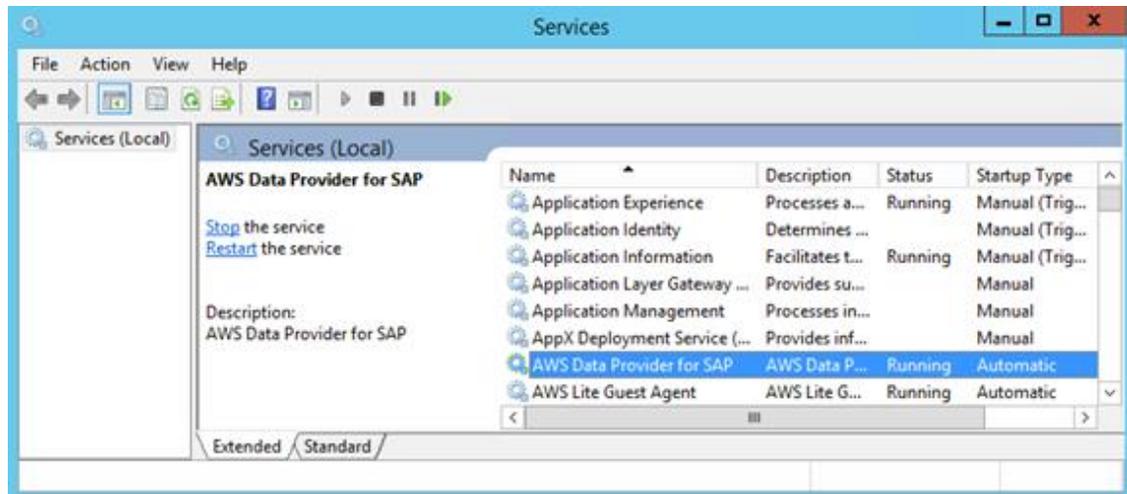
Figure 21: Stopping and restarting the AWS Data Provider for SAP on Windows

Updating the AWS Data Provider for SAP

AWS Data Provider for SAP version 1.2.2 and earlier cannot automatically update to version 2.9. To upgrade to AWS Data Provider for SAP version 2.9, uninstall the earlier version using the following instructions, and then install the latest version.

If you're using a proxy configuration, you should preserve the proxy.properties file by copying it into a safe location.

Uninstalling on Linux

1. Log in to Linux as a superuser.

2. Stop the service with the following command.

```
/usr/local/ec2/aws-agent/bin/aws-agent_uninstall
```

Uninstalling on Windows

1. Run the uninstaller.

```
C:\Program Files\AmazonA\DataProvider\uninstall.exe
```
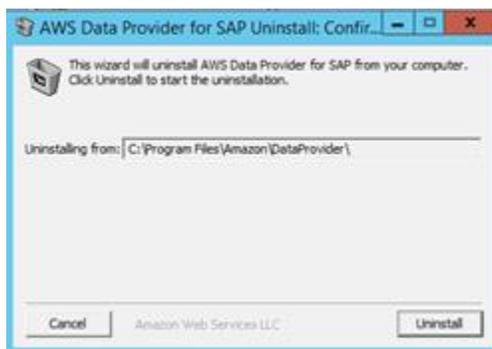
2. When prompted, choose **Uninstall**.

Figure 22: Uninstalling the AWS Data Provider for SAP on Windows

Troubleshooting

This section provides help to analyze installation problems.

Troubleshooting on Linux

Problem: The installation failed, and I'm not sure if my files are in a consistent state.

Check the /usr/local/ec2/aws-agent directory for the presence of a versions.mf file. If this file isn't present in the directory, rerun the installation script to reload the entire set of files for the AWS Data Provider for SAP from the update service. If the versions.mf file is present, delete it, and then rerun the installation script to reload the AWS Data Provider for SAP files.

Problem: The AWS Data Provider for SAP failed to start at the end of the installation process.

Check for the presence of the versions.mf file in the /usr/local/ec2/aws-agent directory. If the file is present, delete it, and then rerun the installation script to download the files again.

If reinstalling the AWS Data Provider for SAP doesn't solve the problem, you can gather debug information about the AWS Data Provider for SAP by going to the /etc/rc.d/ directory and editing the aws-agent file.

Figure 23: Debugging the installation on Linux

In the DAEMONOPTS section of the aws-agent file, make these changes:

- Add the `–debug` flag as the first option right before `–jvm`

- Change the `–LogLevel=INFO` option to `–LogLevel=FINE`

Lastly, you should copy the following.

```
exec='$DAEMON $DAEMONOPTS > /dev/null 2>&1
```

Then remove the last part of the line (`> /dev/null 2>&1`), which suppresses console output. You can comment out the original line so you can put it back later.

Now if you run **service aws-agent-start**, you get a lot of debugging output that might help you diagnose the root cause of the problem.

Figure 24: Debugging information on Linux

Problem: I want to reinstall the AWS Data Provider for SAP from scratch.

Log in to Linux as a superuser, and remove your current AWS Data Provider for SAP installation, as follows.

```
/usr/local/ec2/aws-agent/bin/aws-agent_uninstall
```

You can then get the latest version of the installation script from https://s3.amazonaws.com/aws-data-provider/bin/aws-agent_install.sh and rerun it. This downloads all prerequisites from scratch, and installs the latest software distribution.

Problem: When I looked at my logs I noticed that my installation failed all diagnostics.

```
14:32:15.862 I 08001  ** Running Diagnostics **

14:32:15.862 I 08002 Diagnostic : AWS Connectivity

14:33:19.362 W 08003 Diagnostic : Failed

14:33:19.362 I 08006 Diagnostic : Amazon CloudWatch Connectivity & Access

14:33:19.515 W 08007 Diagnostic : Failed

14:33:19.516 I 0800A Diagnostic : EC2 API Connectivity & Access

14:33:19.542 W 0800B Diagnostic : Failed

14:33:19.542 I 0800E ** Diagnostics Complete **
```

Figure 25: Symptoms of internet connectivity problems on Linux

Failing *all* diagnostics indicates that there's a problem with your outbound connection to the internet. You can confirm this by pinging a well-known internet location, like www.amazon.com. The most common cause of routing issues is in the VPC network configuration, which needs to have either an internet gateway in place or a VPN connection to your data center with a route to the internet. For details, see Internet Access, earlier in this guide.

Problem: When I looked at my logs I noticed that I don't have access to CloudWatch and Amazon EC2, but I did pass the first diagnostic for AWS connectivity.

```
14:38:57.467 I 08001  ** Running Diagnostics **

14:38:57.468 I 08002 Diagnostic : AWS Connectivity

14:38:58.182 I 08005 Diagnostic : Passed

14:38:58.182 I 08006 Diagnostic : Amazon CloudWatch Connectivity & Access

14:38:58.325 W 08007 Diagnostic : Failed

14:38:58.325 I 0800A Diagnostic : EC2 API Connectivity & Access

14:38:58.357 W 0800B Diagnostic : Failed

14:38:58.357 I 0800E ** Diagnostics Complete **
```

Figure 26: Symptoms of authorization issues on Linux

This is a clear indicator that you have an authorization issue when trying to access CloudWatch and Amazon EC2. The common cause for this problem is not having an IAM role associated with your instance that contains the IAM policy, as specified in IAM Roles, earlier in this guide. You can quickly diagnose this issue by looking at the EC2 instance in question in the Amazon EC2 console and verifying the IAM role.

Root Device Type:	ebs	Tenancy:	default
IAM Role:	-	Lifecycle:	normal
EBS Optimized:	false		
Block Devices:	sda1		
Network Interfaces:	eth0		
Public DNS:			
Private DNS:		Product Codes:	
Private IPs:	10.0.0.174		
Secondary Private IPs:			
Launch Time:	2012-10-09 14:18 EDT (less than an hour)		
State Transition Reason:	-		
Termination Protection:	Disabled		

Figure 27: Verifying the IAM role for an EC2 instance

If the IAM role doesn't exist, you have to launch a new instance from an AMI and assign it an IAM role. IAM roles can't currently be assigned to an instance that is already launched.

If you do have an IAM role assigned to the instance, go to the IAM console, select the IAM role name, and then expand the policy. Verify that you have the required policy that is specified in IAM Roles, earlier in this guide.
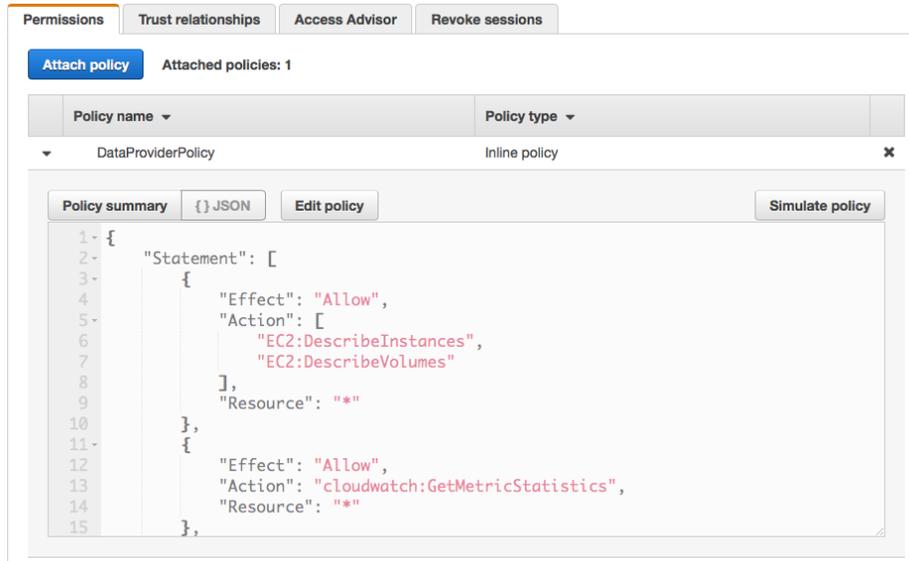
Figure 28: Verifying the policy for the IAM role

Troubleshooting on Windows

Problem: The installation failed, and I'm not sure if my files are in a consistent state.

Check the C:\Program Files\Amazon\DataProvider directory for the presence of a versions.mf file. If this file isn't present in the directory, rerun the installation script to reload the entire set of files for the AWS Data Provider for SAP from the update service. If the versions.mf file is present, delete it, and then rerun the installation script to reload the AWS Data Provider for SAP files.

Problem: The AWS Data Provider for SAP failed to start at the end of the installation process.

Check for the C:\Program Files\Amazon\DataProvider directory for the presence of the versions.mf file. If the versions.mf file is present, delete it, and then rerun the installation script to download the file again.

If reinstalling the AWS Data Provider for SAP doesn't solve the problem, you can gather debugging information about the AWS Data Provider for SAP by reviewing the log files in the C:\Program Files\Amazon\DataProvider directory.

These log files include an installation log, a log of the service installation, and the output of the AWS Data Provider for SAP itself.

```
       LastWriteTime          Length Name
       -------------          ------ ----
10/9/2012      4:20 PM               aws-agent
10/9/2012      4:26 PM           833 agentinstallog.txt
10/9/2012      4:26 PM          2203 awsagent-stdout.2012-10-09.log
10/9/2012      4:26 PM           201 AwsDataCollectorLibraryUpdateService.txt
10/9/2012      4:26 PM          1267 commons-daemon.2012-10-09.log
```

Figure 29: Log files on Windows

Problem: I want to reinstall the AWS Data Provider for SAP from scratch.

Remove the versions.mf file from the C:\Program Files\Amazon\DataProvider\ directory, and then rerun the installation script from https://s3.amazonaws.com/aws-data-provider/bin/aws-agent-installer-win-x64.exe. This downloads all prerequisites from scratch, and gives you the latest software distribution.

Problem: When I looked at my logs, I noticed that my installation failed all diagnostics.

```
14:32:15.862 I 08001  ** Running Diagnostics **

14:32:15.862 I 08002 Diagnostic : AWS Connectivity

14:33:19.362 W 08003 Diagnostic : Failed

14:33:19.362 I 08006 Diagnostic : Amazon CloudWatch Connectivity & Access

14:33:19.515 W 08007 Diagnostic : Failed

14:33:19.516 I 0800A Diagnostic : EC2 API Connectivity & Access

14:33:19.542 W 0800B Diagnostic : Failed

14:33:19.542 I 0800E ** Diagnostics Complete **
```

Figure 30: Symptoms of internet connectivity problems on Windows

Failing *all* diagnostics indicates that there's a problem with your outbound connection to the internet. You can confirm this by pinging a well-known internet location, like www.amazon.com. The most common cause of routing issues is in the VPC network configuration, which needs to have either an internet gateway in place or a VPN connection to your data center with a route to the internet.

Problem: When I looked at my logs, I noticed that I don't have access to CloudWatch and Amazon EC2, but I did pass the first diagnostic for AWS connectivity.


```
14:38:57.467 I 08001  ** Running Diagnostics **

14:38:57.468 I 08002 Diagnostic : AWS Connectivity

14:38:58.182 I 08005 Diagnostic : Passed

14:38:58.182 I 08006 Diagnostic : Amazon CloudWatch Connectivity & Access

14:38:58.325 W 08007 Diagnostic : Failed

14:38:58.325 I 0800A Diagnostic : EC2 API Connectivity & Access

14:38:58.357 W 0800B Diagnostic : Failed

14:38:58.357 I 0800E ** Diagnostics Complete **
```

Figure 31: Symptoms of authorization issues on Windows

This is a clear indicator that you have an authorization issue when trying to access CloudWatch and Amazon EC2. The common cause for this problem is not having an IAM role associated with your instance that contains the IAM policy, as specified in IAM Roles earlier in this guide. You can quickly diagnose this issue by looking at the specific EC2 instance in the Amazon EC2 console and verifying the IAM role.

Root Device Type:	ebs	**Tenancy:**	default
IAM Role:	-	**Lifecycle:**	normal
EBS Optimized:	false		
Block Devices:	sda1		
Network Interfaces:	eth0		
Public DNS:			
Private DNS:		**Product Codes:**	
Private IPs:	10.0.0.174		
Secondary Private IPs:			
Launch Time:	2012-10-09 14:18 EDT (less than an hour)		
State Transition Reason:	-		
Termination Protection:	Disabled		

Figure 32: Verifying the IAM role for an EC2 instance

If the IAM role doesn't exist, you have to launch a new instance from an AMI and assign it an IAM role. You cannot currently assign IAM roles to an instance that is already launched.

If you do have an IAM role assigned to the instance, go to the IAM console, select the IAM role name, and then choose **Show**. Verify that you have the required policy that is specified in IAM Roles.

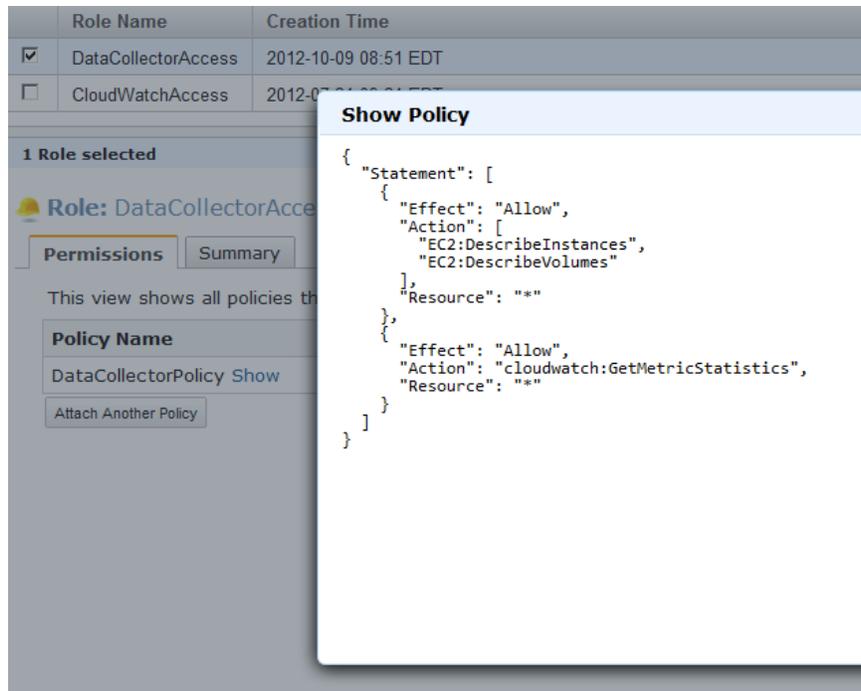**Figure 33: Verifying the policy for the IAM role**

Conclusion

This document helps SAP users to install and operate the AWS Data Provider for SAP. The AWS Data Provider for SAP allows SAP support to monitor SAP applications according to SAP standards.

Contributors

The following individuals contributed to this document:

- Stefan Schneider, Solutions Architect, Amazon Web Services

Document Revisions

Date	Description
September 2017	Update for software release 2.9
December 2015	Update for software release 2.0
January 2014	Initial release of documentation.

Appendix A: Customizing the AWS Data Provider for SAP

Some settings are hard coded in the AWS Data Provider for SAP. You can override existing settings or add new settings. For example, when AWS adds new instance types, you can add these to the AWS Data Provider for SAP configuration.

The AWS Data Provider for SAP creates a database by reading the configuration information from the following files, in this sequence:

- It reads the config.properties file from the JAR (Java Archive) file of the data provider application.

- It reads the file from https://s3.amazonaws.com/aws-data-provider/config.properties, which provides settings for EC2 instance types and Amazon Elastic Block Store (Amazon EBS) volume types. For example, when AWS releases new instance types, AWS updates this file. This file doesn't have to exist.

- It reads the file from the directory in which the proxy configuration file is located. This file is required only if a user wants to override or extend the current configuration. Default locations are:

  - On Linux: /usr/local/ec2/aws-agent/config.properties

  - On Windows: C:\Program Files\Amazon\DataProvider\config

Syntax Rules for Configuration Files

- The configuration files require a comma after the last value in every row.

- Spaces are not ignored in strings. The entire string between the commas, including any spaces, is accepted as the value.

- If there are multiple rows with the same instance type, the existing value for that type is overwritten.

- Capitalization in strings is case sensitive.

User-Configurable EC2 Instance Types

The AWS Data Provider for SAP maintains a database of all relevant EC2 instance types for SAP.

Entries for EC2 instance types must be in a comma-separated list, as follows:

ec2type,*i-type,cpu,core,threads,t-ecu,ecu,hthread,l-map,w-map,speed,p-ecu,*

For example:

```
ec2type,r3.8xlarge,2,16,2,32,1,thread,eth0,lan2,10000,true,
```

where the following applies:

Field name	Content	Example	Type	Description
keyword	ec2type	–	String	A token to identify a record with an EC2 instance description
i-type **(instance type)**	See list	r3.8xlarge	String	Instance type, which must match the EC2 instance metadata string
cpu **(CPUs)**	1 | 2	2	2	Number of sockets
core **(Cores)**	*integer*	16	Integer	Total number of processor cores
threads **(threads per core)**	1 | 2	2	Integer	Threads per core
t-ecu **(total ECU value)**	*integer*	32	Double	ECU value for previous-generation instance types that have ECU ratings; number of cores for post-ECU instance types

Field name	Content	Example	Type	Description
ecu **(ECU per core)**	*double*	1	Double	1 for all post-ECU instance types; total ECU divided by cores for previous-generation instance types that have ECU ratings
hthread **(hyperthreading)**	thread | core	thread	String	**thread** for hyperthreaded instance types; **core** for non-hyperthreaded instance types
l-map **(Linux NIC mapping)**	eth0	eth0	String	Linux mapping of network interface
w-map **(Windows NIC mapping)**	eth0	lan2	String	Windows mapping of network interface
speed **(network interface speed)**	1000 | 2000 | 10000	100000	Integer	Maximum speed of network interface, in KB
p-ecu **(post ECU)**	true | false	true	Boolean	**true** for modern instances that don't have ECU ratings

User-Configurable EBS Volume Types

The AWS Data Provider for SAP maintains a database of all relevant EBS volume types for SAP.

Entries for EBS volume types must be in a comma-separated list, as follows:

voltype,*ebs-type,sample-time,*

For example:

```
voltype,io1,60,
```

where the following applies:

Field name	Content	Example	Type	Description
keyword	voltype	–	String	A token to identify a record with an EBS volume description
ebs-type **(EBS type)**	io1|gp2|sc1|st1	Io1	String	EBS type, which must match the EBS volume metadata string
sample-time	60 | 300	60	Integer	CloudWatch sample time in seconds

> **Important:** The sample time is required to calibrate the EBS metrics to the SAP monitoring requirements. Changes in the sample time will lead to incorrect EBS metrics in the SAP monitoring system.

User-Configurable Support Status

To include optional entries for the support status, use a comma-separated list, as follows:

support,*status,*

For example:

```
support,production,
```

where the following applies:

Field name	Content	Example	Type	Comment
keyword	support	–	String	A token to identify the support status
status	production | anonymous | none	production	String	Choose **production** (default) to allow AWS to check whether the

Field name	Content	Example	Type	Comment
				instance meets prerequisites

The *status* field supports the following values:

- "production" (default): Allows AWS to check whether the instance meets the SAP required prerequisites for SAP support, from <u>SAP Note 1656250</u> (requires SAP support portal login).[3]

- "anonymous": Does not allow AWS to check whether the instance meets prerequisites.

- "none": Legacy mode for version 1.3.1 backward compatibility.

Appendix B: Verification of AWS Data Provider for SAP in SAP System Monitoring

The AWS Data Provider for SAP exposes AWS-specific metrics through an XML page at *http://localhost:8888/vhostmd* of the given system.

This section explains which metrics get exposed to the SAP system and how you can access them for SAP system monitoring.

Checking Metrics with the SAP Operating System Collector (SAPOSCOL)

The information provided by the AWS Data Provider for SAP is read by the SAP Operating System Collector ([SAPOSCOL]).[4] You can use the interactive mode of SAPOSCOL to verify that the two tools are working together correctly. The following example shows a lookup under Windows. A lookup under Linux is very similar.

1. Open a Windows command shell and direct the shell to the directory C:\Program Files\SAP\hostctrl\exe. Start `saposcol.exe` with the `-d` option.

<p align="center">**Figure 34: Starting SAPOSCOL**</p>

2. SAPOSCOL is now in interactive mode. Type `dump ccm` and press **Enter** to list all values gathered. SAPOSCOL will display a lengthy list of metrics, as shown here.

Figure 35: Metrics from SAPOSCOL

- The following two metrics indicate that SAPOSCOL is collaborating successfully with the AWS Data Provider for SAP:

  o Enhanced Monitoring Access   TRUE

  o Enhanced Monitoring Details   ACTIVE

- The AWS-specific metrics start with the following strings:

  o Virtualization_Configuration

  o CPU_Virtualization_Virtual_System

  o Memory_Virtualization_Virtual_System

  o System_Info_Virtualization_System

Figure 36: AWS-specific metrics

Checking Metrics with the SAP CCMS Transactions

SAPOSCOL hands the AWS-enhanced statistics with other operating system-specific metrics to the SAP system. You can also check the AWS-enhanced statistics in the SAP CCMS. You can enter the transaction *st06* (or */nst06*) in the upper-left transaction field of the SAP GUI for quick access to this data.

> **Note:** You will need the appropriate authorizations to look up this information.
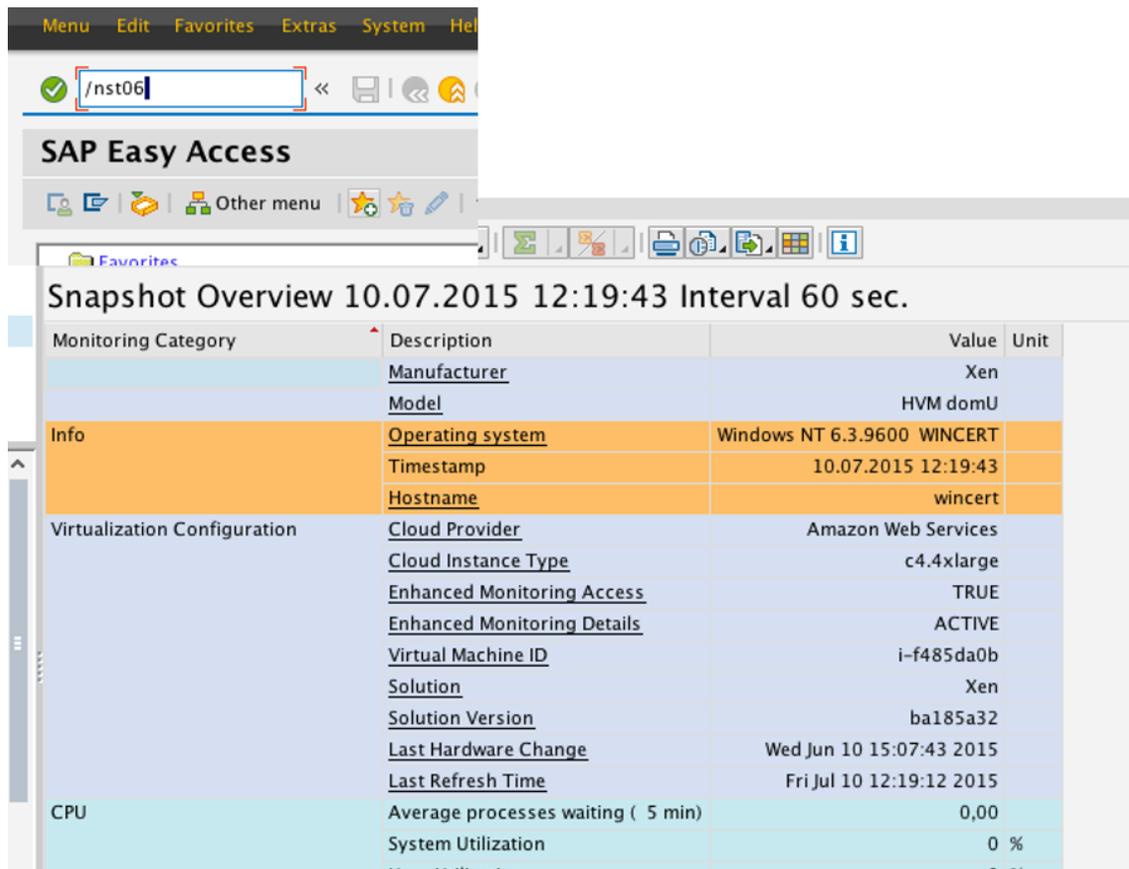

Figure 37: Statistics in the SAP CCMS (standard view)

On this screen, you can verify core AWS information such as:

- Cloud provider

- Instance type

- Status of enhanced monitoring access (must be TRUE)

- Status of enhanced monitoring details (must be ACTIVE)

- Virtual machine identifier

Important: The enhanced AWS metrics aren't shown in standard view.

To view enhanced AWS statistics, choose the **Standard View** button in the upper-left corner. It changes to **Expert View** and displays the enhanced AWS statistics. The list that appears is comprehensive. It shows the processor details.

CPU Virtualization Host	Overprovisioning	no	
	Processor	Intel(R) Xeon(R) @ 2900MHz	
	Number of Cores per Physical CPU	8	Core
	Number of Threads per Core	2	Thds
	Current Processor Frequency	2.900	MHz
	Maximum Processor Frequency	2.900	MHz
CPU Virtualization Virtual System	Physical Reference Compute Unit (CU)	Intel(R) Xeon(R) @ 2900MHz	
	CPU Physical Equivalent	thread @ 1CUs	
	Guaranteed Capacity	16,00	CPUs
	Capacity Consumed	0,00	CPUs
	Additional Capacity Available	16,00	CPUs
	Available Capacity	16,00	CPUs
	Available Capacity Consumed	0,0	%
	Capacity Maximum	16,00	CPUs

Figure 38: Enhanced AWS statistics (expert view)

It also shows details about the memory subsystem (main memory and disks) and network interfaces.

Memory Virtualization Host	Overprovisioning	no	
	Network Read Throughput	5	kB/s
	Network Write Throughput	4	kB/s
	Network TCP Retransmission Rate	0	/s
	lan2\Network Device Id	eni-8235b5d8	
	lan2\Minimum Network Bandwith	10.000	Mb...
	lan2\Maximum Network Bandwith	10.000	Mb...
	disk0\Volume Id	vol-f4b78f0c	
	disk0\Refresh Interval	300	s
	disk0\Volume Utilization	0,0	%
	disk0\Guaranteed Disk IOPS	3.000	
	disk0\Volume Queue Length	0	
	disk0\Volume Read Response Time	0	msec
	disk0\Volume Write Response Time	0	msec
	disk0\Volume Read Throughput	1	kB/s
	disk0\Volume Write Throughput	15	kB/s
	disk0\Volume Read Ops	0	/s
	disk0\Volume Write Ops	2	/s
	disk1\Volume Id	vol-89676771	
	disk1\Refresh Interval	300	s
	disk1\Volume Utilization	0,0	%
	disk1\Guaranteed Disk IOPS	300	
	disk1\Volume Queue Length	0	
	disk1\Volume Read Response Time	0	msec
	disk1\Volume Write Response Time	0	msec
	disk1\Volume Read Throughput	0	kB/s
	disk1\Volume Write Throughput	0	kB/s
	disk1\Volume Read Ops	0	/s
	disk1\Volume Write Ops	0	/s

Figure 39: Memory and networking statistics (expert view)

Note: The screen illustrations in Figures 37–39 were taken from SAP NetWeaver 7.4 SP08. This version shows the enhanced AWS statistics in the **Memory Virtualization** section. This problem has been fixed by SAP in later versions of NetWeaver.

Appendix C: Changes and Bug Fixes by Product Version

Version 1.2 (September 16, 2014)

- New: Support for the T2, R3, and C3 instance families.

- New: Support for post-ECU (EC2 Compute Unit) instance types:

  o New instance types no longer have ECU values.

  o The reference compute power for these instance types is a hardware thread of the given processor. The total CPU power is equal to the number of the vCPUs of a given instance type.

- New: Support for the new EBS GP2 volume type.

  o Every volume is now tagged with the EBS volume type.

- New: Report of EBS one-minute volume statistics.

  o EBS volumes now report their individual sample interval in a separate attribute.

- Bug fix: EBS volume mapping for Windows devices now reports the correct name.

- Bug fix: Installation, update, and operation through HTTP/HTTPS proxies has been fixed.

- New: JRE 8 support has been added on Linux.

Version 1.2.1 (September 29, 2014)

- Bug fix: EBS volumes now report correct attribute type ("string") for volume type.

Version 1.2.2 (October 1, 2014)

- Windows bug fix: Installer executable pulls installation from correct Amazon S3 bucket.

- Windows bug fix: AWS Data Provider for SAP now reports the correct disk mapping for Windows EBS volumes with the following names: xvd[a-z][a-z].

Version 1.3 (February 17, 2015)

- New: Support for new Amazon EC2 C4 instance family.

- Security fix: Upgraded Linux and Windows versions to JRE 8u31.

- Bug fix: Relative performance of c3.8xlarge instances is now reported correctly.

- New: CloudWatch and Amazon EC2 metrics access points:

  o Support for the EU (Frankfurt) Region was added.

  o Access points are user configurable. You can add information about new AWS Regions without having to install a new product version.

  o Access points are now updated from an internet-based database file. You can add new AWS Regions by updating a web-based configuration file and then restarting the daemon/service.

- New: Message log files with fixed disk space consumption are provided on Linux.

- New: User-configurable EC2 instance types are available.

- New: Web update support was added for future EC2 instance types without product updates.

- Bug fix: GP2 volumes now report the correct sample interval time.

- New: User-configurable sample times for new EBS volume types are now available.

- New: The AWS Data Provider for SAP now reports the virtualization type of the EC2 instance.

Version 1.3.1 (July 14, 2015)

- Bug fixes: Security fixes.

- New: Support for C4, D2, and M4 instance types. Users who migrate instances with installed 1.3 agents will automatically receive support for

the new instance types through an updated configuration database on the web.

Version 2.0 (December 22, 2015)

- New: Windows devices in the range sdb to sdzz get correct SCSI device IDs assigned.

- New: Java VM consumption is now limited to 64 MB maximum heap size.

Version 2.1 (January 20, 2016)

- Support for Asia Pacific (Seoul) Region.

- Bug fix: Version 2.0 pulled files from an incorrect S3 bucket for installation. Version 2.0 needs to be uninstalled before version 2.1 is installed.

Version 2.5 (May 2, 2016)

- Bug fixes: Security and stability fixes in versions 2.2-2.4.

- New: Support for new Amazon EBS volume types:

    o Throughput Optimized HDD (`st1`)

    o Cold HDD (`sc1`)

- New: Support for the Amazon EC2 X1 instance family.

Version 2.6 (September 1, 2016)

- Bug fixes: Installation script checks for existence of wget

- Support for Oracle Linux.

Version 2.7 (December 21, 2016)

- Support for Canada (Central), US East (Ohio), and EU (London) Regions.

- Default access point resolution for common AWS Regions is added.

Version 2.8 (March 1, 2017)

- SLES 12, Red Hat 7, and Oracle Linux 7 will now use SYSTEMD to manage the daemon.

- Support for SLES and SLES for SAP 12 SP2.

- SLES 12 SP1 systems will get migrated from Linux services to SYSTEMD when trying to install the AWS Data Provider without having it de-installed first.

- Minor changes in logging texts.

- Support for R4 and M4 instance types.

- Updated Windows installation verification.

Version 2.9 (August 30, 2017)

- Added support for China Regions.

- Added Linux uninstaller.

- Linux installer can be customized to install from a custom S3 bucket.

- Silent installer for Windows (does not require any input).

- Improvements in determination of access points.

- Support for X1E instance family.

Notes

[1]

   http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Internet_Gateway.html

[2] http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html

[3] http://service.sap.com/sap/support/notes/1656250

[4]

   https://help.sap.com/saphelp_nw70/helpdata/en/c4/3a6bff505211d1895500
   00e829fbbd/frameset.htm