Amazon Web Services PowerPack Release Notes

Version 110

Table of Contents

Overview

Amazon Web Services PowerPack version 110 adds the ability to limit discovery to only the regions specified in the user's IAM assigned policy. It also introduces the ability to discover and monitor AWS API Gateway and Lambda services.

- **Minimum Required Platform Version**: 8.8.0
- **Support Status**: GA

This document describes:

- *Pre-install or pre-upgrade information*
- *The upgrade process for systems running version 100 or later of the PowerPack*
- *The upgrade process for systems running version 8.1.0 or earlier of the PowerPack*
- *The features included in version 110*
- *The enhancements and issues addressed in version 110*
- *The known issues in version 110*

Before You Install or Upgrade

Ensure that you are running version 8.8.0 or later of the ScienceLogic platform before installing the *Amazon Web Services* PowerPack version 110. Additionally, the Data Collectors used to monitor the AWS account must be running the Oracle Linux 7.2 operating system.

If your system is not currently running version 8.8.0 or later, you must upgrade to 8.8.0 or later as part of the upgrade process for version 110 of the PowerPack.

NOTE: For details on upgrading the ScienceLogic platform, see the appropriate ScienceLogic Release Notes.

Upgrade Process from PowerPack version 100 or Later

This section describes the upgrade process when upgrading from version 100 or later of the *Amazon Web Services* PowerPack.

TIP: By default, installing a new version of a PowerPack will overwrite all content in that PowerPack that has already been installed on the target system. You can use the ***Enable Selective PowerPack Field Protection*** setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent local changes for some commonly customized fields from being overwritten.

To upgrade from version 100 or later of the *Amazon Web Services* PowerPack:

1. Familiarize yourself with the ***Known Issues*** for this release.
2. Disable collection for AWS devices. To do so, go to the **Device Components** page (Registry > Devices > Device Components) and then select the checkbox for all Amazon Web Services root devices. In the ***Select Actions*** drop-down list, select *Change Collection State: Disabled (recursive)*, and then click the **[Go]** button.
3. If you have not done so already, upgrade your system to the 8.8.0 or later release.

NOTE: For versions 8.6.0 and later of the ScienceLogic platform, the *Amazon Web Services* PowerPack content library will not update until you enable collection for your AWS devices.

4. If you are upgrading from a version of the *Amazon Web Services* PowerPack between versions 104 and 107, you must delete any LightSail Instances that were previously discovered by the "AWS LightSail EC2 Instance Discovery" Dynamic Application. To do so, go to the **Device Manager** page (Registry > Devices > Device Manager), type "LightSail EC2 Instance" in the ***Device Class | Sub-class*** column search field, and then select the checkboxes for all of the devices listed. In the ***Select Action*** drop-down list, select *DELETE Selected Devices*, and then click the **[Go]** button.

NOTE: Deleting these devices results in the loss of any historical data collected by the beta EC2 LightSail Dynamic Applications between versions 104 and 107.

5. Download version 110 of the *Amazon Web Services* PowerPack from the Customer Portal to a local computer.
6. Go to the **PowerPack Manager** page (System > Manage > PowerPacks). Click the **[Actions]** menu and choose *Import PowerPack*. When prompted, import version 110 of the *Amazon Web Services* PowerPack.
7. After importing the PowerPack, you will be prompted to install the PowerPack. Click the **[Install]** button to install the PowerPack.

Upgrade Process from PowerPack version 8.1.0 or Earlier

This section describes the upgrade process when upgrading from version 8.1.0 or earlier of the *Amazon Web Services* PowerPack to version 110.

To upgrade from version 8.1.0 or earlier, you must perform the following general steps:

1. *Disable collection for AWS devices*.
2. *Upgrade to the 8.8.0 or later release*.
3. If you have made changes to the AWS PowerPack, optionally *enable selective PowerPack field protection*.
4. *Install the AWS 110 PowerPack*.
5. If you enabled selective PowerPack field protection, *edit collection objects*.
6. *Clear the cache on all Data Collectors*.
7. *Unalign the AWS Custom Metrics Dynamic Application*.
8. *Enable collection for AWS devices*.
9. If you enabled selective PowerPack field protection, optionally *disable selective PowerPack field protection* after the installation.

Step 1: Disable Collection for AWS Devices

To disable collection for AWS devices:

1. Go to the **Device Components** page (Registry > Devices > Device Components).
2. Select the checkbox for all Amazon Web Services root devices.
3. In the ***Select Actions*** drop-down list, select *Change Collection State: Disabled (recursive)*.
4. Click the **[Go]** button.

Step 2: Upgrade to the 8.8.0 or Later Release

If you have not previously done so, upgrade or migrate your system to an 8.8.0 or later release using the documentation applicable to your current version:

- For systems running an 8.x release, see the 8.8.0 Release Notes.
- For systems running a 7.x release, see the 8.8.0 Migration Steps document.

NOTE: For versions 8.6.0 and later of the ScienceLogic platform, the *Amazon Web Services* PowerPack content library will not update until you enable collection for your AWS devices.

Step 3 (Optional): Enable Selective PowerPack Field Protection

If you have made changes to the *Amazon Web Service* PowerPack on your system, you can use the ***Enable Selective PowerPack Field Protection*** option to preserve changes to some fields. For a full list of fields that are preserved by this option, click the **[Guide]**button on the **Behavior Settings** page (System > Settings > Behavior). If you use the ***Enable Selective PowerPack Field Protection*** option, you must perform the steps listed in the *Step 5 (If Applicable): Edit Collection Objects* section after installing version 110 of the *Amazon Web Services* PowerPack.

To enable selective PowerPack field protection:

1. Go to the **Behavior Settings** page (System > Settings > Behavior).
2. Enable the ***Enable Selective PowerPack Field Protection*** checkbox.
3. Click the **[Save]** button.

Step 4: Install Version 110 of the Amazon Web Services PowerPack

To install the version 110 of the *Amazon Web Services* PowerPack:

1. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
2. Click the **[Actions]** button and select *Import PowerPack*. The **Import PowerPack** modal page appears.
3. Click the **[Browse]** button and select the PowerPack file in your file browser.
4. Click the **[Import]** button. A confirmation dialog appears.
5. Click the **[OK]** button. The **PowerPack Installer** modal page appears.
6. Click the **[Install]** button. A confirmation dialog appears.
7. Click the **[OK]** button.

Step 5 (If Applicable): Edit Collection Objects

If you performed the steps listed in the *Step 3 (Optional): Enable Selective PowerPack Field Protection* section, you must perform the following steps:

1. Go to the **Dynamic Applications Manager** page (System > Manage > Application).
2. Click the wrench icon () for the AWS CloudFront Origin Dynamic Application. The **Dynamic Applications Properties Editor** page appears.
3. Click the **[Collections]** tab.
4. Click the wrench icon () for the Distinguished Name collection object.
5. Select the ***Hide Object*** checkbox.
6. Click the **[Save]** button.

Step 6: Clear Data Collector Cache

To perform this step manually, perform the following steps for every Data Collector used to monitor an AWS account:

1. Log in to the command-line of the appliance as the em7admin user.
2. Ensure the content library version on the Data Collector matches the version from the new PowerPack installation:

   For ScienceLogic platform version 8.5.0 and below:

   ```
   $ cd /var/lib/em7/content/aws
   $ cat version.txt
   ```

   Ensure that the current content library version matches the version installed in the PowerPack.

   For ScienceLogic platform version 8.6.0 and above:

   ```
   $ cd /opt/em7/envs
   $ ls -ltr
   ```

   Locate the soft link "system" and change directories to the path, as in the example below:

   ```
   lrwxrwxrwx. 1 s-em7-core s-em7-core 40 Feb 5 21:40 system ->
   /opt/em7/envs/system-7666504203980756445

   $ cd /opt/em7/envs/system-7666504203980756445
   $ cd lib/python2.7/cl-packages/silo_aws
   $ cat version.txt
   ```

   Ensure that the current content library version matches the version installed in the PowerPack.

NOTE: For versions 8.6.0 and above of the ScienceLogic platform, the content library version listed in the version.txt file will not update until you *enable collection for your AWS devices*.

3. Execute the following command to open a MariaDB prompt:

   ```
   $ sudo bash
   [sudo] password for root:
   # silo_mysql
   ```

4. Execute the following command:

   ```
   DELETE FROM cache.dynamic_app WHERE `key` LIKE 'AWS_SELF_MONITOR_%';
   ```

Step 7: Unalign the AWS Custom Metrics Dynamic Application

A previous release of the *Amazon Web Services* PowerPack erroneously aligned the AWS Custom Metrics Dynamic Application to certain types of devices. To unalign the AWS Custom Metrics Dynamic Application from these devices:

1. Copy the provided aws_unalign_custom_metrics_app.py file to the home directory of the em7admin user on an appliance in your system:
    - If your system includes All-In-One Appliances, use the primary All-In-One Appliance.
    - If your system includes Database Servers where the user interface/API has not been disabled on the Database Servers, use the primary Database Server.
    - If your system includes Database Servers where the user interface/API has been disabled on the Database Servers, use an Administration Portal.

NOTE: The aws_unalign_custom_metrics_app.py file can be found by clicking the "Contrib Files" link for the most recent version of the Amazon Web Services PowerPack on the ScienceLogic customer portal.

2. Log in to the command-line of the appliance as the em7admin user.
3. Execute the following command:

```
sudo python aws_unalign_custom_metrics_app.py --base-url http://[IP address of appliance] --username [username of administrator user] --password [password of administrator user]
```

The output will show information about each device from which the AWS Custom Metrics Dynamic Application was unaligned.

Step 8: Enable Collection for AWS Devices

To enable collection for AWS devices:

1. Go to the **Device Components** page (Registry > Devices > Device Components).
2. Select the checkbox for all AWS Web Services root devices.
3. In the ***Select Actions*** drop-down list, select *Change Collection State: Enabled (recursive)*.
4. Click the **[Go]** button.

Step 9 (Optional): Disable Selective PowerPack Field Protection

If you performed the steps listed in the *Step 3 (Optional): Enable Selective PowerPack Field Protection* section and want to disable the option for future PowerPack updates, perform the following steps:

1. Go to the **Behavior Settings** page (System > Settings > Behavior).
2. Disable the ***Enable Selective PowerPack Field Protection*** checkbox.
3. Click the **[Save]** button.

Features

Amazon Web Services version 110 includes the following features:

- Dynamic Applications that discover, model, and collect data from AWS component devices
- Event Policies and corresponding alerts that are triggered when AWS component devices meet certain status criteria

NOTE: Many of the Event Policies included in the *Amazon Web Services* PowerPack are disabled by default. You must manually enable the Event Policies that you want to use. To do so, go to the **Event Policy Editor** page (Registry > Events > Event Manager > create or edit) and change the ***Operational State*** to *Enabled*.

- Device Classes for each of the AWS component devices monitored
- Sample credentials for discovering AWS component devices
- Reports and dashboards that display information about AWS instances and component devices
- Run Book Action and Automation policies that can automate certain AWS monitoring processes

Enhancements and Issues Addressed

Version 110 of the *Amazon Web Services* PowerPack includes the following enhancements and addressed issues:

- The ability to discover and monitor only the regions specified in the user's IAM permissions policy has been added to the *Amazon Web Services* PowerPack. To discover and monitor a specific region, the user must have at least ReadOnly permissions for that region.

NOTE: To discover specific regions, you must have at least Read-Only JSON policy permissions for those regions. You cannot discover regions for which you do not have policy permissions. At a minimum, you must at least have permissions for the us-east-1 (Virginia) region; without permissions for this region, you cannot discover general AWS services such as CloudFront, Route53, and OpsWorks. For more information, see the ***Monitoring Amazon Web Services*** manual.

TIP: When discovering resources in specific regions, you should ensure that any Global services or resources you want to monitor have the necessary access permissions.

- The *Amazon Web Services* PowerPack can now monitor AWS API Gateway services. The following Dynamic Applications were added to the PowerPack to discover and monitor AWS API Gateway services:
    - AWS API Gateway Service Discovery

- AWS API Gateway Service Health
- AWS API Gateway Service Configuration
- AWS API Instance Discovery
- AWS API Instance Configuration
- AWS API Instance Performance
- AWS API Stage Instance Discovery
- AWS API Stage Instance Configuration
- AWS API Stage Instance Performance

NOTE: AWS API Gateway private integrations are not supported in AWS GovCloud accounts. For a list of services that are supported in AWS GovCloud accounts, see https://docs.aws.amazon.com/govcloud-us/latest/UserGuide/supported-services.html. For more information about limitations for services that are supported by AWS GovCloud accounts, see https://docs.aws.amazon.com/govcloud-us/latest/UserGuide/using-services.html.

TIP: ScienceLogic recommends assigning unique names to all of the AWS API Gateways that you want to monitor, even if AWS allows you to have duplicate names.

NOTE: AWS API Gateway services are not included in the "AWS Health Status" dashboard by default. To include them, click **[Options]** in the **AWS Services** pane, select *Configure*, select *AWS | API Gateway Service* in the ***Device Classes*** field, and then click **[Save]**.

- The *Amazon Web Services* PowerPack can now monitor AWS Lambda services. The following Dynamic Applications were added to the PowerPack to discover and monitor Lambda services:
  - AWS Lambda Service Discovery
  - AWS Lambda Service Health
  - AWS Lambda Service Configuration
  - AWS Lambda Service Performance
  - AWS Lambda Function Discovery
  - AWS Lambda Function Configuration
  - AWS Lambda Function Performance
  - AWS Lambda Function Replica Discovery
  - AWS Lambda Function Replica Configuration
  - AWS Lambda Function Qualified Discovery
  - AWS Lambda Function Qualified Configuration
  - AWS Lambda Function Qualified Performance

NOTE: By default, the "AWS Lambda Service Discovery" Dynamic Application is configured to discover only regular Lambda functions. If you want to discover both regular and replica Lambda functions, then you must configure the "AWS Lambda Service Discovery" Dynamic Application to do so prior to discovering your Lambda service. For more information, see the ***Monitoring Amazon Web Services*** manual.

NOTE: By default, the "AWS Lambda Function Qualified Discovery" Dynamic Application is configured to discover and model all Lambda alias components. Depending on your needs, you can optionally configure the Dynamic Application to instead discover and model all Lambda version components or only Lambda version components with AWS configurations containing a trigger. For more information, see the ***Monitoring Amazon Web Services*** manual.

NOTE: Replica Lambda functions are not supported in AWS GovCloud accounts.

NOTE: AWS Lambda services are not included in the "AWS Health Status" dashboard by default. To include them, click **[Options]** in the **AWS Services** pane, select *Configure*, select *AWS | Lambda Service* in the ***Device Classes*** field, and then click **[Save]**.

- The "AWS CloudWatch Alarms Performance" Dynamic Application was updated to collect API Gateway Service and Lambda Function alarms from the CloudWatch API.
- The following Device Classes were added to the PowerPack to support API Gateway and Lambda service monitoring:
    - AWS API Gateway Service
    - AWS API Instance
    - AWS API Stage Instance
    - AWS Lambda Service
    - AWS Lambda Function
    - AWS Lambda Function Alias
    - AWS Lambda Function Version
    - AWS Lambda Function Replica
- The PowerPack was updated to create and model relationships between the following Device Classes:
    - AWS API Gateway Services and AWS Network Load Balancers
    - AWS API Instances and AWS Lambda Functions
    - AWS Lambda Functions and AWS Security Groups
    - AWS Lambda Functions and AWS Simple Notification Services (SNS)
    - AWS Lambda Functions and AWS Simple Queue Services (SQS)
    - AWS Lambda Functions and AWS Subnets

    - AWS Lambda Functions and AWS VPC Instances
    - AWS Lambda Function Qualified Services and AWS Security Groups
    - AWS Lambda Function Qualified Services and AWS Subnets
    - AWS Lambda Function Qualified Services and AWS VPC Instances
    - AWS Lambda Function Replicas and their parent AWS Lambda Function Versions
- New Region and Availability Zone Device Classes were added for European Union West (Paris).
- The following Device Classes were added to represent EC2 instances of different sizes:

Device Class	Description	Class ID
AWS	EC2 Instance	9xlarge
AWS	EC2 Instance	12xlarge
AWS	EC2 Instance	16xlarge
AWS	EC2 Instance	18xlarge
AWS	EC2 Instance	24xlarge
AWS	EC2 Instance	32xlarge
AWS	EC2 Instance	metal

- The connection pool was optimized for Bulk Performance type Dynamic Applications so that only connections relevant to the devices being collected have a session connection and that connection can be reopened as needed.

Known Issues and Workarounds

The following known issues affect version 110 of the *Amazon Web Services* PowerPack:

- Some disk-related alerts and events were removed from the "AWS LightSail Instance Performance" Dynamic Application as of *Amazon Web Services* PowerPack version 108. If you are upgrading from a version prior to version 108, then you must manually delete the thresholds relating to these removed alerts and events. To do so, go to the **Dynamic Applications Threshold Objects** page (System > Manage > Applications > wrench icon > Thresholds) for the "AWS LightSail Instance Performance" Dynamic Application, and then click the bomb icon () for the following thresholds:
    - AWS: LightSail Disk IOPS High
    - AWS: LightSail Disk GB Usage High
- AWS does not currently support IPv6 addresses for LightSail services. However, the "AWS LightSail Instance Configuration" Dynamic Application includes support for IPv6 addresses in the event that AWS adds support in the future.

- Because AWS Government accounts do not support all of the services supported by AWS Commercial accounts, some expected errors will appear when discovering AWS Government Accounts. For example:

```
HTTPSConnectionPool(host='lightsail.us-gov-west-1.amazonaws.com', port=443): Max
retries exceeded with url: / (Caused by ProxyError('Cannot connect to proxy.', error
('Tunnel connection failed: 503 Service Unavailable',)))

Unable to process AWS request: AID: 402, SID: 415, DID: 3, Class:
AwsOpsWorksServiceDisc UnrecognizedClientException The security token included in
the request is invalid.

Unable to process AWS request: AID: 279, SID: 275, DID: 84, Class:
AwsOpsWorksServiceDisc UnrecognizedClientException The security token included in
the request is invalid. Invalid credentials for billing metric retrieval.
```

  If you are discovering **only** an AWS Government account, then a simple workaround to these errors is to disable and delete the Dynamic Applications relating to services that are not supported by the AWS Government account.

NOTE: For more information about which services are supported by AWS Government account, see https://aws.amazon.com/about-aws/global-infrastructure/regional-product-services.

WARNING: If you are discovering both AWS Government and Commercial accounts, you should not disable or delete any AWS Dynamic Applications.

- SSL EOF error messages might appear in the system log when connecting to AWS through a proxy server. The error does not seem to prevent or cause issues with data collection.
- "Read operation timed out" and "Connection reset by peer" error messages might appear in the system log and device logs when upgrading the *Amazon Web Services* PowerPack from versions prior to 108.

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010