



Amazon Web Services PowerPack Release Notes

Version 100

Table of Contents

Overview	3
Upgrade Process	3
Step 1: Disable Collection for AWS Devices	4
Step 2: Upgrade to the 8.1.1 or Later Release	4
Step 3 (Optional): Enable Selective PowerPack Field Protection	4
Step 4: Install Version 100 of the Amazon Web Services PowerPack	5
Step 5 (If Applicable): Edit Collection Objects	5
Step 6: Verify Installation and Clear Data Collector Cache	5
Step 7: Unalign the AWS Custom Metrics Dynamic Application	6
Step 8: Enable Collection for AWS Devices	7
Step 9 (Optional): Disable Selective PowerPack Field Protection	7
Enhancements and Issues Addressed	7
Known Issues	8

Overview

Version 100 of the Amazon Web Services PowerPack adds support to the new Mumbai Region and addresses multiple known issues.

The minimum required platform version for version 100 of the Amazon Web Services PowerPack is 8.1.1. If your system is not currently running version 8.1.1 or later, you must upgrade to 8.1.1 as part of the upgrade process for version 100 of the Amazon Web Services PowerPack.

This document describes:

- [The upgrade process for version 100 of the PowerPack](#)
- [The enhancements and issues addressed in version 100](#)
- [The known issues that affect version 100](#)

Upgrade Process

This section describes the upgrade process for the version 100 of the Amazon Web Services PowerPack. The upgrade process for version 100 of the Amazon Web Services PowerPack includes executing a series of commands on every Data Collector monitoring an AWS account. There are two options for this step in the upgrade process:

- Execute the commands manually from the command-line of each Data Collector or All-In-One Appliance.
- If you are using a distributed system, use a Linux server running Ansible to execute the commands. This option is recommended if your system includes a large number of Data Collectors monitoring AWS accounts. For information on installing Ansible, see http://docs.ansible.com/ansible/intro_installation.html. The Ansible server must meet the following requirements:

- Ansible version 2.0 or later must be installed. To check the installed version, execute the following command:

```
ansible --version
```

- The `/etc/ansible/hosts` file must include an entry for each Data Collector used to monitor an AWS account and an entry for each Database Server in the following format:

```
[collectors_aws]
<Data Collector IP address>
<Data Collector IP address>
.
.
<Data Collector IP address>
[database]
<Database IP Address>
<Database IP Address>
<Database IP Address>
```

- The host fingerprint for each Data Collector and Database Server listed in the `/etc/ansible/hosts` file must be included in the `known_hosts` file.

- The server must be able to communicate with each Data Collector and Database Server listed in the `/etc/ansible/hosts` file. To test connectivity, execute the following command:


```
ansible all --ask-pass -m ping -u em7admin
```
- The `aws_pp_post_upgrade.yml` file must be saved on the local file system of the Ansible server.

To upgrade from a previous version of the Amazon Web Services PowerPack to version 100 of the Amazon Web Services PowerPack, you must perform the following general steps:

1. [Disable collection for AWS devices.](#)
2. [Upgrade to the 8.1.1 or later release.](#)
3. If you have made changes to the AWS PowerPack, optionally [enable selective PowerPack field protection](#).
4. [Install the AWS 100 PowerPack.](#)
5. If you enabled selective PowerPack field protection, [edit collection objects](#).
6. [Verify the installation and 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 8.1.1 or Later Release

If you have not previously done so, upgrade your system to an 8.1.1 or later release using the documentation applicable to your current version:

- For systems running an 8.0 or 8.1.0 release, see the [8.1.1.2 Release Notes](#).
- For systems running a 7.x release, see the [8.1.1 Migration Steps](#) document.

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 100 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 100 of the Amazon Web Services PowerPack

To install the version 100 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. Enable the **Hide Object** checkbox.
6. Click the Save button.

Step 6: Verify Installation and Clear Data Collector Cache

This step can be performed manually or using an Ansible server.

NOTE: It can take up to five minutes after the installation of a PowerPack for the update content library to install on a Data Collector.

To perform this step using an Ansible server:

1. Log in to the command-line of the Ansible server:
2. Execute the following command:

```
ansible-playbook --extra-vars "aws_ppcl_version=1.5.6" aws_pp_post_upgrade.yml -v -k
```

3. Validate that the output includes the following for every Data Collector used to monitor an AWS account:
 - The "Validate content library version" task did not fail
 - The "Remove Self-Monitoring Cache" task did not fail

It can take up to five minutes after the installation of a PowerPack for the update content library to install on a Data Collector. If the output indicates the "Validate content library version" task failed, wait five minutes and execute the command listed in step 2 again. If the "Validate content library version" task fails again, contact ScienceLogic Support.

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. Execute the following command:
- ```
watch cat /var/lib/em7/content/aws/version.txt
```
3. Within five minutes of the PowerPack installation, the command should return "1.5.6". If the command does not return "1.5.6", contact ScienceLogic Support.
  4. Enter "Ctrl + C" to exit the command.
  5. Execute the following command to open a MariaDB prompt:

```
silo_mysql
```

6. 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.
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.

---

## Enhancements and Issues Addressed

The following changes are included in version 100 of the Amazon Web Services PowerPack:

- The following new configuration Dynamic Applications have been added, which collect data for CloudFront Web Distribution component devices:
  - AWS CloudFront Behaviors
  - AWS CloudFront Error Page
  - AWS CloudFront Invalidations
  - AWS CloudFront Origins
  - AWS CloudFront Restriction
- Specific Device Classes have been added for the AWS Mumbai region.
- Performance improvements have been made to the collection of Redshift data.
- Performance improvements have been made to the collection of Storage Gateway data.
- Performance improvements have been made to the collection of Opsworks data.

- An issue has been addressed that caused gaps in performance data for EC2 and EBS component devices.
- The AWS Custom Metrics Dynamic Application no longer aligns with devices that do not support custom metrics collection.
- The event that occurs when the AWS PowerPack discovers an unsupported region is now human-readable.
- Request Limit Exceeded errors from the AWS API are now handled correctly by the request retry mechanism.
- The AWS Self-Monitoring and AWS Service Self-Monitoring Dynamic Applications have been deprecated.

---

## Known Issues

The following are known issues with version 100 of the Amazon Web Services PowerPack that will be addressed in a future release:

- An erroneous CloudFront RTMP Distribution is discovered by the PowerPack.
- During the upgrade process, a "FileNotFoundException" unhandled exception can occur.
- After upgrading to version 100 of the Amazon Web Services PowerPack, duplicate journal entries are collected by the AWS OpsWorks Service Health Dynamic Application.



© 2003 - 2016, ScienceLogic, Inc.

All rights reserved.

#### LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

#### 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](mailto:legal@sciencelogic.com)



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

International: +1-703-354-1010