Monitoring Amazon Web Services ELK Stacks

ELK: AWS CloudTrail PowerPack version 100

Table of Contents

Chapter 1

Introduction

Overview

This manual describes how to monitor Amazon Web Services (AWS) component devices that are part of an Elasticsearch, Logstash, and Kibana (ELK) stack in the ScienceLogic platform using the *ELK: AWS CloudTrail* PowerPack.

The following sections provide an overview of AWS ELK stacks and the *ELK: AWS CloudTrail* PowerPack:

NOTE: The *ELK: AWS CloudTrail* PowerPack is meant to be used in conjunction with the *Amazon Web Services* PowerPack. For more information about the *Amazon Web Services* PowerPack, including how to install the PowerPack and discover AWS devices, see the ***Monitoring Amazon Web Services*** manual.

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

What is an AWS ELK Stack?

An ELK stack is a centralized log management platform consisting of three open-source products:

- Elasticsearch, a storage solution with search and indexing capabilities
- Logstash, a server-side data collection engine
- Kibana, a web user interface used for visualizing stored data

In an ELK stack, Logstash collects data, Elasticsearch indexes and stores the data, and Kibana visually presents the data in a user-friendly manner.

You can install an ELK stack on an Amazon Web Services instance to collect, store, and visualize data about that instance.

What Does the ELK: AWS CloudTrail PowerPack Monitor?

The *ELK: AWS CloudTrail* PowerPack includes the following features:

- A sample Credential that you can use to create Basic/Snippet credentials to monitor AWS component devices in ELK stacks
- Dynamic Applications that align to AWS component devices in ELK stacks and then monitor CloudTrail logs and states changes on EC2 instances
- An Event Policy that notifies users when the ELK Dynamic Applications have aligned to AWS components
- Run Book Policies and Actions that align the ELK Dynamic Applications to AWS components and update the alignment status on the ScienceLogic Data Collector or All-In-One Appliance

Installing the ELK: AWS CloudTrail PowerPack

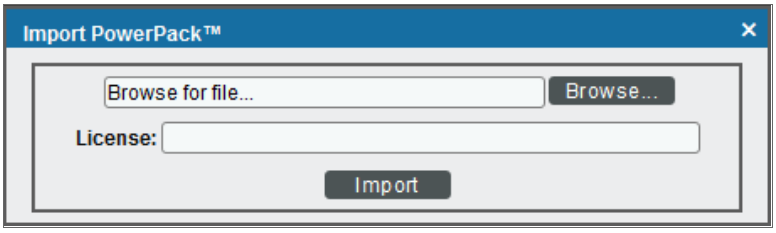
Before completing the steps in this manual, you must import and install the latest version of the *ELK: AWS CloudTrail* PowerPack.

To download and install a PowerPack:

> **TIP:** By default, installing a new version of a PowerPack overwrites 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 new PowerPacks from overwriting local changes for some commonly customized fields. (For more information, see the ***System Administration*** manual.)

1. Download the PowerPack from the ScienceLogic Customer Portal.
2. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
3. In the **PowerPack Manager** page, click the **[Actions]** button, then select *Import PowerPack*.

4. The **Import PowerPack** dialog box appears:



5. Click the **[Browse]** button and navigate to the PowerPack file.
6. When the **PowerPack Installer** modal page appears, click the **[Install]** button to install the PowerPack.

> NOTE: If you exit the **PowerPack Installer** modal page without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPack Manager** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal page. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

Chapter 2

Configuring AWS ELK Stack Monitoring

Overview

The following sections describe how to configure AWS component devices in ELK stacks for monitoring by the ScienceLogic platform using the *ELK: AWS CloudTrail* PowerPack:

Prerequisites for Monitoring AWS ELK Stacks

To configure the ScienceLogic platform to monitor AWS component devices in ELK stacks using the *ELK: AWS CloudTrail* PowerPack, you must first:

- Install the *Amazon Web Services* PowerPack.
- Create a virtual device in the ScienceLogic platform to represent your AWS service.
- Discover AWS component devices by manually aligning the "AWS Account Discovery" Dynamic Application to the virtual device.
- Ensure that your AWS CloudTrail bucket is properly configured for all read/write events.

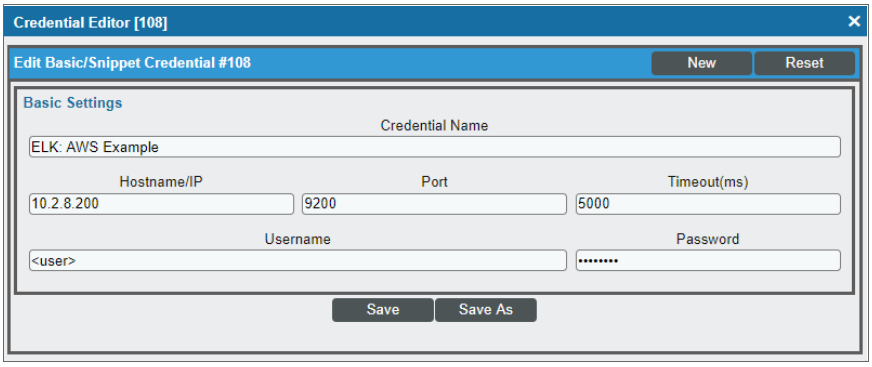
NOTE: For more information about the *Amazon Web Services* PowerPack, including how to install the PowerPack and discover AWS devices, see the ***Monitoring Amazon Web Services*** manual.

Creating an AWS ELK Credential

To use the Dynamic Applications in the *ELK: AWS CloudTrail* PowerPack, you must first define a credential in the ScienceLogic platform. This credential enables the Dynamic Applications in the *ELK: AWS CloudTrail* PowerPack to monitor your AWS component devices in ELK stacks. The PowerPack includes a sample Basic/Snippet credential (**ELK: AWS Example**) that you can use as a template.

To define an AWS ELK credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the wrench icon ( ) for the **ELK: AWS Example** credential. The **Credential Editor** modal page appears:



3. Enter values in the following fields:
   - ***Credential Name***. Type a new name for your AWS ELK credential.
   - ***Hostname/IP***. Type the IP address or hostname for the Logstash server that collects data for the AWS components in your ELK stack.
   - ***Port***. Type "9200".

   Use the default values for the remaining fields.

> **NOTE:** The Basic/Snippet credential requires values in the ***Username*** and ***Password*** fields, but the values themselves do not matter.

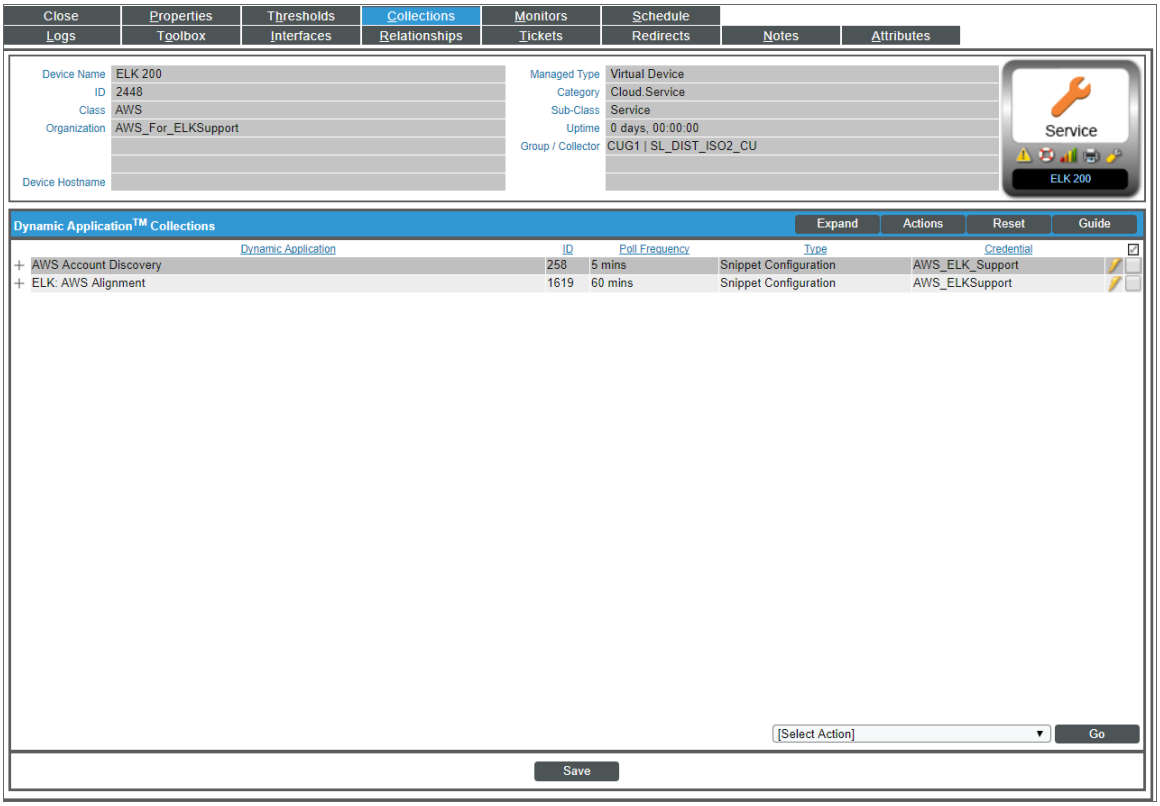
4. Click the **[Save As]** button, and then click **[OK]**.

Aligning the AWS ELK Dynamic Applications

To monitor your AWS component devices in ELK stacks, you must manually align the "ELK: AWS Alignment" Dynamic Application with the AWS virtual device. When you do so, the remaining Dynamic Applications from the *ELK: AWS CloudTrail* PowerPack automatically align to the appropriate AWS component devices.

To manually align the "ELK: AWS Alignment" Dynamic Application to your virtual device:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Locate your AWS virtual device and click its wrench icon ( ).
3. In the **Device Administration** panel, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.



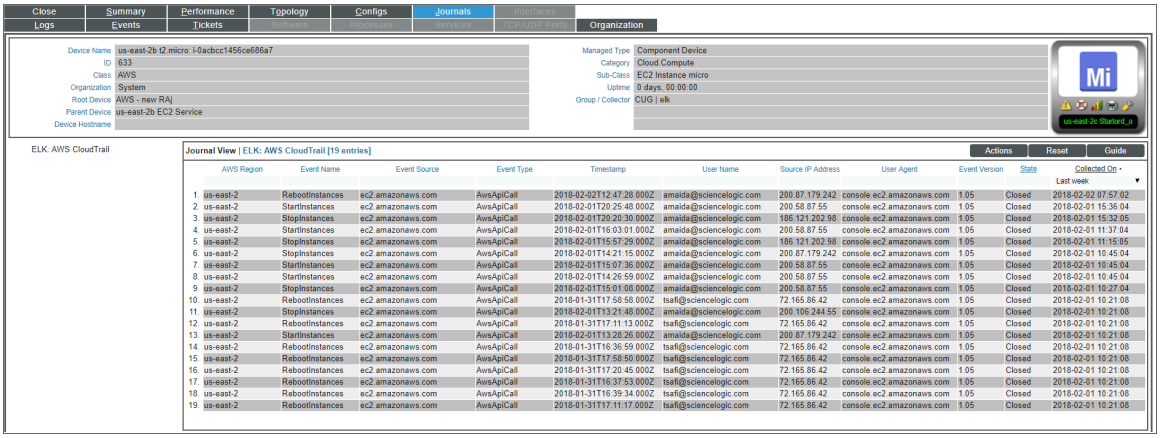
4. Click the **[Actions]** button, and then select *Add Dynamic Application* from the menu.
5. In the **Dynamic Application Alignment** modal page, select *ELK: AWS Alignment* in the ***Dynamic Applications*** field.
6. In the ***Credentials*** field, select the *credential you created for your AWS ELK components*.
7. Click **[Save]**.

NOTE: By default, the "ELK: AWS Alignment" Dynamic Application begins collecting data after 60 minutes. If you want to begin collecting data immediately, click the lightning bolt icon ( ) for the "ELK: AWS Alignment" Dynamic Application on the **Dynamic Application Collections** page.

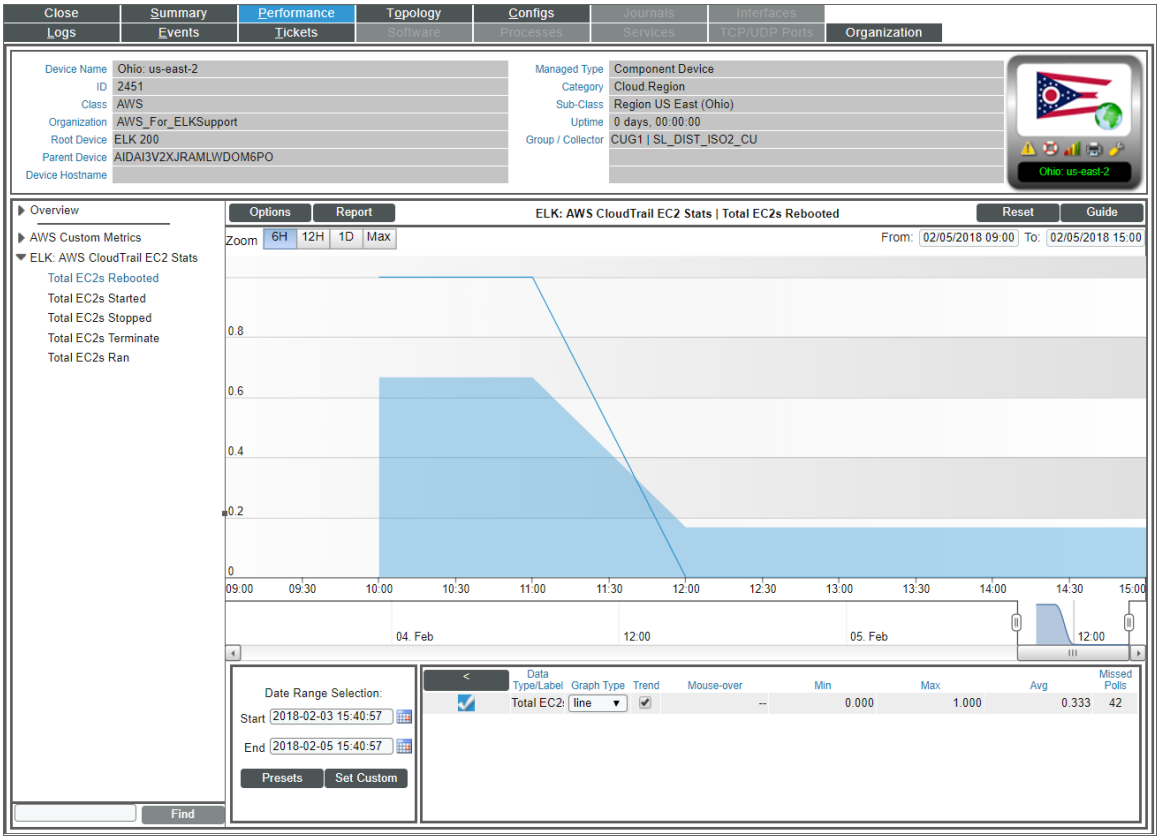
When you align the "ELK: AWS Alignment" Dynamic Application to the AWS root device, the platform then aligns the following Dynamic Application from the *ELK: AWS CloudTrail* PowerPack to the appropriate component devices:

- ELK: AWS CloudTrail
- ELK: AWS CloudTrail EC2 Stats

To view the data collected by the "ELK: AWS CloudTrail" Dynamic Application, navigate to the **Journal View** page (Registry > Devices > Device Manager > bar-graph icon > Journals) and click **ELK: AWS CloudTrail** on the left menu:



To view the data collected by the "ELK: AWS CloudTrail EC2 Stats" Dynamic Application, navigate to the **Device Performance** page (Registry > Devices > Device Manager > bar-graph icon > Performance) and click **ELK: AWS CloudTrail** on the left menu:



© 2003 - 2018, 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

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

International: +1-703-354-1010