ELK: AWS CloudTrail PowerPack Release Notes

Version 100

Table of Contents

Overview

Version 100 is the initial version of the *ELK: AWS CloudTrail* PowerPack, which provides additional data for Amazon Web Services (AWS) component devices that are part of an Elasticsearch, Logstash, and Kibana (ELK) stack. Version 100 includes Dynamic Applications, an Event Policy, a sample Credential, and Run Book Policies/Actions that enable you to monitor and align AWS CloudTrail data from Logstash.

- **Minimum Required Platform Version**: 8.4.3
- **Support Status**: Beta

This document describes:

- *Pre-install information*
- *The installation and upgrade process for the PowerPack*
- *The features included in version 100*

Before You Install

Ensure that you are running version 8.4.3 or later of the ScienceLogic platform before installing the *ELK: AWS CloudTrail* PowerPack version 100. You must also ensure that your AWS CloudTrail bucket is properly configured for all read/write events.

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

Installing ELK: AWS CloudTrail PowerPack version 100

To install the *ELK: AWS CloudTrail* PowerPack for the first time, perform the following steps:

1. See the *Before You Install or Upgrade* section. If you have not done so already, upgrade your system to the 8.4.3 or later release.
2. Download version 100 of the *ELK: AWS CloudTrail* PowerPack from the Customer Portal to a local computer.
3. Go to the **PowerPack Manager** page (System > Manage > PowerPacks). Click the **[Actions]** menu and choose *Import PowerPack*. When prompted, import version 100 of the *ELK: AWS CloudTrail* PowerPack.
4. After importing the PowerPack, you will be prompted to install the PowerPack. Click the **[Install]** button to install the PowerPack.
5. See the manual ***Monitoring AWS ELK Stacks*** for instructions on using the new PowerPack.

Included Features

ELK: AWS CloudTrail PowerPack version 100 includes the following features:

- Three Dynamic Applications that align to AWS component devices in ELK stacks and then monitor CloudTrail logs and states changes on EC2 instances:
    - ELK: AWS Alignment
    - ELK: AWS CloudTrail
    - ELK: AWS CloudTrail EC2 Stats
- An Event Policy that notifies users when the ELK Dynamic Applications have aligned to AWS components
- A sample Credential that you can use to create Basic/Snippet credentials to monitor AWS ELK stacks.
- Run Book Policies/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.

© 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