

Monitoring Amazon Web Services

Amazon Web Services PowerPack version 110

Table of Contents

Introduction	. 4
What is AWS?	. 5
What is an AWS Region?	. 5
What is an AWS Zone?	. 5
What Does the Amazon Web Services PowerPack Monitor?	. 6
Installing the Amazon Web Services PowerPack	. 8
Monitoring Consolidated Billing Accounts	. 9
ScienceLogic Events and AWS Alarms	. 9
Configuring AWS Monitoring	10
Configuring Amazon Web Services for Monitoring	11
Configuring AWS for Region-Specific Monitoring	15
Example 1: One Region	16
Example 2: Multiple Regions	.16
Configuring AWS to Report Billing Metrics	17
Creating an AWS Credential	.19
Testing the AWS Credential	20
Creating an AWS Virtual Device	22
Understanding the AWS Dynamic Applications	23
AWS Account Discovery	23
Configuring "AWS Lambda Service Discovery"	24
Configuring "AWS Lambda Function Qualified Discovery"	27
Discovering the AWS Account	.31
Viewing AWS Component Devices	32
Relationships Between Component Devices	34
Configuring the AWS Dashboards	35
Amazon API Throttling Events	36
Configuring Inbound CloudWatch Alarms	38
CloudWatch Alarm Event Policies	.38
Creating Custom CloudWatch Metrics	40
Configuring CloudWatch to Send Alarms for a Metric	.42
Enabling Custom Metrics Collection in the ScienceLogic Platform	.45
Configuring the "AWS CloudWatch Alarms Performance" Dynamic Application	45
Enabling CloudWatch Alarm Events in the ScienceLogic Platform	47
AWS Reports	.49
AWS Billing Report	.50
AWS Inventory Report	.52
AWS Running Config Report	54
AWS Dashboards	.56
Installing the Amazon Web Services: Dashboards PowerPack	56
AWS Account Billing Dashboard	58
AWS Health Status Dashboard	59
AWS Service Instance Performance Dashboards	59
AWS Run Book Actions and Automations	61
About the Kun Book Actions and Automations	62
Disabling EC2 and EBS Instances by EC2 ag	.63
Modifying the Parameters of the Automation Actions	64
Enabling the Component Device Record Created Event Policy	64
Enabling the Automation Policies	.64
Preserving Automation Changes	65
Discovering EC2 Instances by Public or Private IP Address	65

Modifying the Parameters of the Automation Actions	
Enabling the Component Device Record Created Event Policy	
Enabling the Device Record Created Event Policy	69
Enabling the Automation Policies	69
Preserving Automation Changes	69
Vanishing Terminated or Terminating EC2 Instances	70
Enabling the Automation Policies	71
Preserving Automation Changes	71

Chapter

Introduction

Overview

This manual describes how to monitor Amazon Web Services (AWS) in the ScienceLogic platform using the *Amazon Web Services* PowerPack. It also describes the reports you can generate and the dashboards you can view after you collect data from AWS, as well as the Run Book Action and Automation policies you can use to automate certain aspects of monitoring AWS.

The following sections provide an overview of Amazon Web Services and the Amazon Web Services PowerPack:

What is AWS?	5
What is an AWS Region?	5
What is an AWS Zone?	5
What Does the Amazon Web Services PowerPack Monitor?	6
Installing the Amazon Web Services PowerPack	8
Monitoring Consolidated Billing Accounts	9
ScienceLogic Events and AWS Alarms	9

NOTE: For more information about setting up a ScienceLogic appliance on an Amazon Web Services EC2 instance, see the *Installation and Initial Configuration* manual.

NOTE: For more information about setting up an AWS Elasticsearch, Logstash, and Kibana (ELK) stack, see the *Monitoring AWS ELK Stacks* 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 AWS?

Amazon Web Services is Amazon's "Infrastructure As A Service" offering. AWS includes multiple products (called **Services**) including virtual servers, DNS, private cloud, content delivery, storage, and database products.

What is an AWS Region?

An AWS region is an individual data center located in a specific geographic locale. Regions have a canonical naming scheme of:

country/continent-direction-number

For example, the 'us-east-1' region is located in the United States, on the east coast, and it is the #1 data center in that region.

AWS regions are also commonly referred to by the city or state in which the data center is located. For example, us-west-2 is commonly referred to as "Oregon", ap-northeast-1 is commonly referred to as "Tokyo", etc.

The Dynamic Applications in the Amazon Web Services PowerPack create a "region" component device for each discovered region. The component devices for regions include both the region name and city/state description. For example, the Dynamic Applications might discover a component device called "Oregon: us-west-2". Component devices that represent AWS services reside under the appropriate "region" component device and appropriate "zone" component device.

What is an AWS Zone?

All instances of an AWS service reside in one or more Zones. A zone is a physical network and power partition (airgap firewall) within a regional data center. Some AWS instances, like EC2 instances, are in a single zone. Other AWS instances, like an SNS queue, exist in all zones simultaneously.

The AWS naming convention for a zone is:

region[a-z]

For example, zone 'a' for the region 'us-east-1' is named 'us-east-1a'.

When a user deploys a service instance, the user can specify a "zone preference", but the final zone for that service instance is decided by AWS, not the user.

The Dynamic Applications in the Amazon Web Services PowerPack create a "zone" component device for each discovered zone.

AWS services with a specific zone affinity reside under the appropriate zone component device. For example, the Dynamic Applications in the PowerPack might discover the zone "us-west-1b" and create a component device called ""us-west-1b".

AWS services reside under the appropriate "region" component device and appropriate "zone" component device. The Dynamic Applications in the PowerPack create a "multi-zoned" component device for services that are inherently zone agnostic such as the Simple Queue Service (SQS).

Component devices that represent Zones are a named container with no associated performance metrics.

What Does the Amazon Web Services PowerPack Monitor?

To collect data from Amazon Web Services, the ScienceLogic Data Collector or All-In-One Appliance connects via HTTPS to the URLs listed in the following AWS document: http://docs.aws.amazon.com/general/latest/gr/rande.html.

The Amazon Web Services PowerPack includes Dynamic Applications that can monitor performance metrics and collect configuration data for the following AWS Services and components:

- API Gateways
- AutoScale
- CloudFront
- CloudTrail
- CloudWatch
- Direct Connect
- DynamoDB (DDB)
- ElastiCache
- Elastic Beanstalk
- Elastic Block Store (EBS)
- Elastic Compute Cloud (EC2)
- Elastic Load Balancers (ELB)
- Elastic Map Reduce (EMR)
- Glacier
- Lambda
- Lightsail
- OpsWorks

- RedShift
- Relational Data Store (RDS)
- Route53
- Security Groups
- Simple Notification Service (SNS)
- Simple Queue Service (SQS)
- Simple Storage Service (S3)
- Storage Gateways (ASG)
- Storage Gateway Volumes
- Virtual Private Cloud Service (VPC)
- Virtual Private Networks (VPN)

NOTE: The following services are not monitored for GovCloud accounts:

- API Gateway private integrations
- CloudFront
- Replica Lambda functions

NOTE: To monitor performance metrics for an AutoScale group, you must activate detailed instance monitoring for that group. For instructions on how to perform this task, see http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/as-instance-monitoring.html.

NOTE: To monitor Lambda services, you must first configure some of the Dynamic Applications in the Amazon Web Services PowerPack prior to discovery. For more information, see the Configuring "AWS Lambda Service Discovery" and Configuring "AWS Lambda Function Qualified Discovery" sections.

The Dynamic Applications in the PowerPack also monitor:

- The general health of each AWS service
- Current billing metrics for each service aligned with the account
- Custom, application-specific performance metrics configured on the account
- The state of any AWS Alarms set on metrics in Cloudwatch

In addition to Dynamic Applications, the PowerPack includes the following features:

• Event Policies and corresponding alerts that are triggered when AWS component devices meet certain status criteria

- 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

NOTE: To view Amazon Web Services dashboards, you must first install the Amazon Web Services: Dashboards PowerPack. For more information, see the AWS Dashboards chapter.

Installing the Amazon Web Services PowerPack

Before completing the steps in this manual, you must import and install the latest version of the Amazon Web Services PowerPack.

NOTE:	If you are upgrading	from an earlier ve	rsion of the Pov	verPack, see the	<u>Release Notes</u> f	or the version
	you are installing for	upgrade instructic	ons.			

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.)

To download and install a PowerPack:

- 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:

Impo	ort PowerPack™	×
	Browse for file Browse License: Import	

- 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*.

Monitoring Consolidated Billing Accounts

Consolidated billing is an option provided by Amazon that allows multiple AWS accounts to be billed under a single account. For more information about consolidated billing, see http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html.

If a consolidated billing account is monitored by the ScienceLogic platform, the billing metrics associated with that account include only the consolidated amounts, per service. If you use consolidated billing and want to collect billing metrics per-account, you must discover each account separately. To monitor only the billing metrics for an AWS account, you can create credentials that include only billing permissions.

ScienceLogic Events and AWS Alarms

In addition to the ScienceLogic platform collecting metrics for AWS instances, you can configure CloudWatch to send alarm information to the platform via API. The platform can then generate an event for each alarm.

For instructions on how configure CloudWatch and the platform to generate events based on CloudWatch alarms, see the **Configuring Inbound CloudWatch Alarms** section.

Chapter

2

Configuring AWS Monitoring

Overview

The following sections describe how to configure and discover Amazon Web Services and component devices for monitoring by the ScienceLogic platform using the *Amazon Web Services* PowerPack:

Configuring Amazon Web Services for Monitoring	11
Configuring AWS for Region-Specific Monitoring	
Example 1: One Region	
Example 2: Multiple Regions	
Configuring AWS to Report Billing Metrics	
Creating an AWS Credential	
Testing the AWS Credential	
Creating an AWS Virtual Device	
Understanding the AWS Dynamic Applications	23
AWS Account Discovery	
Configuring "AWS Lambda Service Discovery"	
Configuring "AWS Lambda Function Qualified Discovery"	
Discovering the AWS Account	
Viewing AWS Component Devices	
Relationships Between Component Devices	
Configuring the AWS Dashboards	
Amazon API Throttling Events	36

Configuring Amazon Web Services for Monitoring

To use the AWS Dynamic Applications, you must configure a credential that allows the ScienceLogic platform to connect to the AWS REST API. The *Amazon Web Services* PowerPack includes three credential templates.

To use the credential templates included in the PowerPack, you must download the security credentials for a user associated with your AWS account. The user must meet the following requirements:

- The Dynamic Applications in the Amazon Web Services PowerPack require, at minimum, the actions that are
 in the ReadOnlyAccess AWS Managed policy. To set this user policy, see
 https://console.aws.amazon.com/iam/home?region=us-east1#/policies/arn:aws:iam::aws:policy/ReadOnlyAccesss serviceLevelSummary?section=policy_versions.
- You can use the Dynamic Applications in the Amazon Web Services PowerPack to discover and monitor only specific regions and services. To do so, you must create a JSON permissions policy that uses the NotAction, Allow, and Deny policy elements to specify which regions and services you want to monitor or not monitor and select that policy for your AWS user. For more information, see the Configuring AWS for Region-Specific Monitoring section.
- To collect billing metrics, the user must have read permission in the us-east-1 zone. For instructions on how to configure your AWS account to report billing metrics, see the **Configuring AWS to Report Billing Metrics** section.
- If you are using multiple users to monitor AWS, each instance of a service must be visible to only one of those users. If an instance is visible to multiple users that are used to monitor AWS in the ScienceLogic platform, the device record for that instance will repeatedly switch between the component trees of the accounts that have visibility to that instance.

To create a read-only user account, perform the following steps:

1. Open a browser session and go to <u>aws.amazon.com</u>.

2. Click [My Account] and then select AWS Management Console. If you are not currently logged in to the AWS site, you will be prompted to log in:



- 3. In the AWS Management Console, under the Security & Identity heading, click [Identity & Access Management].
- 4. After logging in, the Identity & Access Management Dashboard page appears:

ashboard	Welcome to Identity and Access Managemen	nt	Feature Spotlight
Details	IAM users sign-in link:		Introduction to AWS IAM < ()
iroups	https://642636115777.signin.aws.amazon.com/console	Customize Copy Link	
lsers	IAM Resources		
oles	Users: 6	Roles: 0	
olicies	Groups: 0	Identity Providers: 0	● (i) 0:00 / 2:16 [™]
lentity Providers	Customer Managed Policies: 1		
ccount Settings	Security Status	2 out of 5 comple	te. 🔇 🔹 🔹 🖒
redential Report	Delete your root access keys	*	Additional Information
	Activate MFA on your root account	*	IAM documentation
ncryption Keys	Create individual IAM users	~	Policy Simulator
	▲ Use groups to assign permissions	×	Videos, IAM release history and additional
	Apply an IAM password policy	~	

5. To create a user account for the ScienceLogic platform, click **[Users]** on the Dashboard menu.

etalis oups outs outs outs outs outs outs outs out		Create New Users Use	er Actions 👻				C 0
Ups User Name \$ Groups Password Password Last Used \$ Access Keys Creation Time \$ lels EM7 0 NA 1 active 2015-06-28 15:55 ED1 lelse EM7-RW 0 NA 1 active 2015-06-28 15:55 ED1 antily Providers em7admin 0 NA 1 active 2015-06-08 15:16 ED1 count Settings useast1 0 NA 1 active 2015-06-28 17:47 ED1 uswest1 0 NA 1 active 2015-06-08 15:16 ED1 uswest1 0 NA 1 active 2015-06-24 17:47 ED1	tails	Q Search					Showing 6 re
Interse EM7 0 NA 1 active 2015-05-28 15:55 EDT Interse EM7-RW 0 NA 1 active 2015-06-09 13:15 EDT Interse em7admin 0 NA 1 active 2015-06-09 13:15 EDT count Settings em7admin 0 NA 1 active 2015-06-08 15:16 EDT count Settings useast1 0 NA 1 active 2015-08-24 17:47 EDT edential Report usewst1 0 NA 1 active 2015-08-24 17:47 EDT	ers	User Name \$	Groups	Password	Password Last Used \$	Access Keys	Creation Time \$
Ibles EM7-RW 0 NA 1 active 2015-06-09 13:15 EDT entity Providers em7admin 0 NA 1 active 2015-06-09 13:15 EDT count Settings useast1 0 NA 1 active 2015-06-09 15:16 EDT edential Report useast1 0 NA 1 active 2015-08-24 17:47 EDT useast1 0 NIA 1 active 2015-08-24 17:47 EDT	les	EM7	0		N/A	1 active	2015-05-28 15:55 EDT
mtty Providers em/?admin 0 NA 1 active 2015-06-08 15:16 EDT count Settings useast1 0 N/A 1 active 2015-06-08 15:16 EDT edential Report uswest1 0 N/A 1 active 2015-08-24 17:47 EDT uswest1 0 N/A 1 active 2015-08-24 17:47 EDT	icies	EM7-RW	0		N/A	1 active	2015-06-09 13:15 EDT
count Settings useast1 0 N/A 1 active 2015-08-24 17:47 EDT edential Report uswest1 0 N/A 1 active 2015-08-24 17:47 EDT uswest1 0 N/A 1 active 2015-08-24 17:47 EDT uswest1 0 N/A 1 active 2015-08-24 17:47 EDT	ntity Providers	em7admin	0		N/A	1 active	2015-06-08 15:16 EDT
Image: second	count Settings	useast1	0		N/A	1 active	2015-08-24 17:47 EDT
Upwart2 0 N/A 1 active 2045 09 24 17 47 EDT	edential Report	uswest1	0		N/A	1 active	2015-08-24 17:47 EDT
		uswest2	0		N/A	1 active	2015-08-24 17:47 EDT

- 6. Click the [Create New Users] button.
- 7. Enter a username for the new user, e.g. "EM7", and make sure the **Generate an access key for each user** checkbox is selected.

8. Click the [Create] button to generate your user account. The Create User page appears:

🎁 AWS 🗸 S	ervices 🗸 Edit 🗸	ScienceLogic Training	▼ Global ▼ Support ▼
Create User	 Your 1 User(s) have been created successfully. This is the last time these User security credentials will be You can manage and recreate these credentials any time. Show User Security Credentials 	e available for download.	
		Close	Download Credentials

- 9. Click the **[Download Credentials]** button to save your Access Key ID and Secret Key as a CSV (commaseparated value) text file, and then click **[Close]**.
- 10. After creating a user, you must assign it a set of permissions policies. Click the username of the user account you created. The user's account information appears:

🎁 AWS 🗸 Services	s 🕶 Edit 👻		ScienceLogic Training 🗸	Global 🗸	Support +
Dashboard	IAM > Users > EM7-BA				<u>^</u>
• Deteile	 Summary 				
Details	User ARN:	arn:aws:lam::642636115777:user/EM7-BA			
Groups	Has Password:	No			
Users	Groups (for this user):	0			
Roles	Path:	1			
Policies	Creation Time:	2015-09-02 11:32 EDT			
Identity Providers					
Account Settings	- Groups				
Account octangs	This user does not belong to any	arouns			
Credential Report	Add User to Groups	ar o al par			
	And ober to oroups				
Encryption Keys	Barrelania				
	 Permissions 				
	Managed Policies				^
	There are no managed policies a	tached to this user.			
	Attach Policy				
	Inline Policies				^
	There are no inline policies to she	w To create one. click here.			
Feedback Senglish			is. All rights reserved. Prin	racy Policy	Terms of Use

11. Under the Permissions heading, click the [Attach Policy] button. The Attach Policy page appears:

Attach Policy Select one or more policies to attach. Each user can have up to 10 policies attached. Filter: Policy Type • @ Search Policy Name • Attached Entities • Creation Time • Ediled Time • @ 01/00 Access 5 2015-02-06 13.39 EST 2015-00-16 13.61 @ 1 ReadOnlyAccess 1 2016-02-06 13.39 EST 2015-00-06 13.30 @ 1 AmazonAPR/GatewayAdministrator 0 2015-07-09 13.36 EDT 2015-02-06 13.40 @ 1 AmazonAppStreamFulAccess 0 2015-02-06 13.40 EST 2015-02-06 13.40 @ 1 AmazonAppStreamFulAccess 0 2015-02-06 13.40 EST 2015-02-06 13.40 @ 1 AmazonAppStreamFulAccess 0 2015-02-06 13.40 EST 2015-02-06 13.40 @ 1 AmazonAppStreamFulAccess 0 2015-03-04 13.22 EDT 2015-03-04 13.22 @ 1 AmazonAppStreamFulAccess 0 2015-03-04 13.22 EDT 2015-03-04 13.22 @ 1 AmazonCognitoDeveloperAuthentizate 0 2015-03-04 13.02 EDT 2015-03-04 13.02 @ 1 AmazonCognitoDeveloperAuthentizate 0 <th>S 🗸 Services 🖌 Edit 🗸</th> <th></th> <th></th> <th></th> <th></th> <th>ScienceLogic Training + Global + Su</th>	S 🗸 Services 🖌 Edit 🗸					ScienceLogic Training + Global + Su
Select one or more policies to attach. Each user can have up to 10 policies attached. Fitter: Policy Type • @ Search Policy Name • Attached Entities • Creation Time • Edited Time • Policy Name • Attached Entities • Creation Time • Edited Time • Policy Name • Attached Entities • Creation Time • Edited Time • Policy Name • Attached Entities • Creation Time • Edited Time • Image: Policy Type • @ Search Standard Access 5 2015-0266 13.39 EST 2015-06.15 Bit 1 Image: Policy Type • @ Search Image: Policy Time • Administrator/Access 1 2015-0266 13.39 EST 2015-0266 13.3 Image: Policy Time • @ AmazonAplicatewayAdministrator 0 2015-07-09 13.3 EDT 2015-07-09 13.3 Image: Policy Time • @ AmazonAppStreamFulAccess 0 2015-0266 13.40 EST 2015-0266 13.40 Image: Policy Time • @ AmazonAppStreamFulAccess 0 2015-0266 13.40 EST 2015-0324 13.24 Image: Policy Time • @ AmazonAppStreamFulAccess 0 2015-0324 13.24 EDT 2015-0324 13.24 Image: Policy Time • @ AmazonAppStreamFulAccess 0 2015-0324 13.24 EDT 2015-0324 13.24 Image: Policy Time • @ AmazonAppSt	blicy	Attach P	olicy			
Filter: Policy Type • < Search Policy Name * Attached Entities * Creation Time * Edited Time * Image: Search Search Search Edited Time * Edited Time * Image: Search Search Search Creation Time * Edited Time * Image: Search Search Search Creation Time * Edited Time * Image: Search Search Search Corestion Time * Edited Time * Image: Search Search Search Corestion Time * Edited Time * Image: Search Search Search Corestion Time * Edited Time * Image: Search AmazonAPIGatewayAdministrator 0 2015-0206 13.3 EDT 2015-0206 13.4 Image: AmazonAPIGatewayInvokeFullAccess 0 2015-0206 13.40 EST 2015-0206 13.4 Image: AmazonAppStreamFullAccess 0 2015-0206 13.40 EST 2015-0324 13.2 Image: AmazonCognitoDeveloperAuthentizate 0 2015-0324 13.22 EDT 2015-0324 13.2 Image: AmazonCognitoDeveloperAuthentizate 0 2015-0324 13.06 EDT 2015-0324 13.2		Select one or	more policies to attach. Each user can have	up to 10 policies attached.		
Filter: Policy Type Q Soarch Policy Name * Attached Entities * Creation Time * Edited Time * Image: Comparison of the co						
Policy Name * Attached Entities * Creation Time * Edited Time * Image: Control of the state of the stat		Filter: Po	licy Type - Q Search			Showing 150
Image: ReadOnlyAccess 5 2015-02-06 13.39 EST 2015-02-09 13.34 EDT 2015-02-06 13.40 EST 2015-02-06 13.40			Policy Name \$	Attached Entities \$	Creation Time \$	Edited Time ¢
iii AdministratorAccess 1 2015-02-06 13.39 EST 2015-02-06 13.34 iiii AmazonAPIGatewayAdministrator 0 2015-07-09 13.34 EDT 2015-07-09 13.34 iiiii AmazonAPIGatewayAdministrator 0 2015-07-09 13.34 EDT 2015-07-09 13.34 iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii		Image:	ReadOnlyAccess	5	2015-02-06 13:39 EST	2015-06-15 18:16 EDT
Image: AmagenAPIGatewayAdministrator 0 2015-07-09 13.34 EDT 2015-07-09 13.34 Image: AmagenAPIGatewayAmvinkeFullAccess 0 2015-07-09 13.36 EDT 2015-07-09 13.36 Image: AmagenAPIGatewayInvokeFullAccess 0 2015-07-09 13.36 EDT 2015-07-09 13.36 Image: AmagenAPIGatewayInvokeFullAccess 0 2015-07-09 13.36 EDT 2015-02-06 13.40 Image: AmagenApiGatewayInvokeFullAccess 0 2015-02-06 13.40 EST 2015-02-06 13.40 Image: AmagenCognitoDeveloperAuthenticate 0 2015-03-24 13.22 EDT 2015-03-24 13.22 Image: AmagenCognitoDeveloperAuthenticate 0 2015-03-24 13.24 2015-03-24 13.24 ImagenCognitoDeadOnly 0 2015-03-24 13.24 2015-03-24 13.24 2015-03-24 13.24 ImagenDynamoDBFUIAccess 0 2015-03-26 13.40 EST 2015-02-06 13.40 2015-02-06 13.40 EST <		0	AdministratorAccess	1	2015-02-06 13:39 EST	2015-02-06 13:39 EST
Image: AmagenAPIGatewayInvokeFullAccess 0 2015-07-09 13:36 EDT 2015-07-09 13:36 Image: AmagenApiGatewayInvokeFullAccess 0 2015-02-06 13:40 EST 2015-02-06 13:40 Image: AmagenApiGatewayInvokeFullAccess 0 2015-02-06 13:40 EST 2015-02-06 13:40 Image: AmagenApiGatewayInvokeFullAccess 0 2015-02-06 13:40 EST 2015-02-06 13:40 Image: AmagenApiGatewayInvokeFullAccess 0 2015-02-06 13:40 EST 2015-03-24 13:22 Image: AmagenCognitoDeveloperAuthenticate 0 2015-03-24 13:22 EDT 2015-03-24 13:22 Image: AmagenCognitoDeveloperAuthenticate 0 2015-03-24 13:22 2015-03-24 13:22 Image: AmagenCognitoDeveloperAuthenticate 0 2015-03-24 13:22 2015-03-24 13:22 Image: AmagenCognitoDeveloperAuthenticate 0 201		0 👔	AmazonAPIGatewayAdministrator	0	2015-07-09 13:34 EDT	2015-07-09 13:34 EDT
Image: AmagenAppStreamFullAccess 0 2015-02-06 13:40 EST 2015-03-24 13:22 EDT 2015-03-24 13:22 EDT 2015-03-24 13:22 EDT 2015-03-24 13:21 EDT 2015-0		0 📋	AmazonAPIGatewayInvokeFullAccess	0	2015-07-09 13:36 EDT	2015-07-09 13:36 EDT
Image: Amage:		0 👔	AmazonAppStreamFullAccess	0	2015-02-06 13:40 EST	2015-02-06 13:40 EST
Image: AmagenCognitoDeveloperAuthenticate 0 2015-0324 13:22 EDT 2015-0324 13:22 Image: AmagenCognitoDeveloperAuthenticate 0 2015-0324 13:22 EDT 2015-0324 13:24 Image: AmagenCognitoDeveloperAuthenticate 0 2015-0324 13:22 EDT 2015-0324 13:24 Image: AmagenCognitoDeveloperAuthenticate 0 2015-0324 13:26 EDT 2015-0324 13:26 Image: AmagenCognitoDeveloperAuthenticate 0 2015-02-06 13:40 EST 2015-02-06 13:40 EST		0 📋	AmazonAppStreamReadOnlyAccess	0	2015-02-06 13:40 EST	2015-02-06 13:40 EST
iii AmazonCognitoPowerUser 0 2015-03-24 13:14 EDT 2015-03-24 13:14 EDT 2015-03-24 13:06 EDT 2015-03-06 13:40 EDT 2015-		0 📦	AmazonCognitoDeveloperAuthenticate	0	2015-03-24 13:22 EDT	2015-03-24 13:22 EDT
Image: AmagenCognitoReadOnly 0 2015-03-24 13.06 EDT 2015-03-26 13.40 EST 2015-03-26 EST <t< td=""><td></td><td>0 🧃</td><td>AmazonCognitoPowerUser</td><td>0</td><td>2015-03-24 13:14 EDT</td><td>2015-03-24 13:14 EDT</td></t<>		0 🧃	AmazonCognitoPowerUser	0	2015-03-24 13:14 EDT	2015-03-24 13:14 EDT
iii AmazonDRSVPCManagement 0 2015-09-01 20.09 EDT 2015-09-01 20.09 EDT iii AmazonDynamoDBFulAccess 0 2015-02-06 13.40 EST 2015-02-06 13.40 EST iii AmazonDynamoDBFulAccesswithDat 0 2015-02-06 13.40 EST 2015-02-06 13.40 EST		0 📦	AmazonCognitoReadOnly	0	2015-03-24 13:06 EDT	2015-03-24 13:06 EDT
Image: Provide and the system of th		0 🔋	AmazonDRSVPCManagement	0	2015-09-01 20:09 EDT	2015-09-01 20:09 EDT
AmazonDynamoDBFullAccesswithDat 0 2015-02-06 13:40 EST 2015-02-06 13:40		0 🔋	AmazonDynamoDBFullAccess	0	2015-02-06 13:40 EST	2015-02-06 13:40 EST
		0 🚺	AmazonDynamoDBFullAccesswithDat	0	2015-02-06 13:40 EST	2015-02-06 13:40 EST
4		•				

- 12. Select the checkbox for *Read Only* Access or select the policy based on the definition supplied by ScienceLogic.
- 13. Click the **[Attach Policy]** button.

Configuring AWS for Region-Specific Monitoring

You can use the Dynamic Applications in the Amazon Web Services PowerPack to discover and monitor only the specific regions and services for which your AWS user has IAM policy permissions.

To monitor specific regions and services, you must create a JSON policy in the AWS Management Console that uses the NotAction, Allow, and Deny policy elements to specify the regions and services you want to monitor as well as which regions and services you **do not** want to monitor. You must then attach this permissions policy to the AWS user account you created.

NOTE: You must have at least Read-Only JSON policy permissions for the regions you want to monitor. 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.

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.

NOTE: For more information about the NotAction, Allow, and Deny policy elements, see https://docs.aws.amazon.com/IAM/latest/UserGuide/reference policies elements notaction.html.

The following sections provide two examples of region-specific JSON policies.

Example 1: One Region

This JSON Policy will deny any service that is not in the us-east-1 region. As a result, the ScienceLogic Platform will discover only components in the us-east-1 region.

NOTE: In addition to the code below, you would need to specify the other resource permissions you want to allow in the policy.

```
"Version": "2012-10-17",
  "Statement": [
    {
       "Sid": "DenyAllOutsideUSEast1",
       "Effect": "Deny",
       "NotAction": [
         "iam:*",
         "organizations:*",
         "support:*",
         "aws-portal:*",
         "s3:ListAllMyBuckets"
       ],
       "Resource": "*",
       "Condition": {
         "StringNotEquals": {
            "aws:RequestedRegion": "us-east-1"
         }
       }
    }
  ]
}
```

Example 2: Multiple Regions

This JSON Policy will deny any service that is not in the us-east-1, us-west-2, and ap-northeast-1 regions. As a result, the ScienceLogic Platform will discover only components in the us-east-1, us-west-2, and ap-northeast-1 regions.

NOTE: In addition to the code below, you would need to specify the other resource permissions you want to allow in the policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
       "Sid": "DenyAllOutsideUSWest2USEast1APNortheast1",
       "Effect": "Deny",
       "NotAction": [
         "iam:*",
         "organizations:*",
         "support:*",
         "aws-portal:*",
         "s3:ListAllMyBuckets"
       ],
       "Resource": "*",
       "Condition": {
         "StringNotEquals": {
           "aws:RequestedRegion": ["us-east-1", "us-west-2", "ap-northeast-1"]
         }
       }
    }
  ]
}
```

Configuring AWS to Report Billing Metrics

To use the "AWS Billing Performance Percent" Dynamic Application, your AWS account must meet the following requirements:

- The user account you supplied in the AWS credential must have permission to view the us-east-1 zone.
- Your AWS account must be configured to export billing metrics to the CloudWatch service.

If your AWS account is not configured to export billing metrics to the CloudWatch service, the "AWS Billing Performance Percent" Dynamic Application will generate the following event:

No billing metrics can be retrieved. Your AWS account is not configured to export billing metrics into CloudWatch.

To configure your AWS account to export billing metrics to the CloudWatch service, perform the following steps:

1. Open a browser session and go to aws.amazon.com.

2. Click [My Account] and then select Billing & Cost Management. If you are not currently logged in to the AWS site, you will be prompted to log in:

web services	
Sign In or Create an AWS Account What is your e-mail or mobile number? E-mail or mobile number: • I am a new user. • I am a returning user and my password is: Sign In using our secure server Strong tyour password?	Now Available Amazon Aurora Enterprise-class database at 1/10th the cost
Learn more about <u>AWS Identity and Access Management</u> and <u>AW</u> additional security for your AWS Account. View full <u>AWS Free Us</u>	<u>S Multi-Factor Authentication</u> , features that provide age <u>Tier</u> offer terms.
About Amazon.com Sign In Amazon Web Services uses information from your Amazon.com account of this site is governed by our Terms of Use and Privacy Policy linked be	to identify you and allow access to Amazon Web Services. Your use ow.
<u>Terms of Use Privacy Policy</u> © 1996-2015 An amazon .com	, Amazon.com, Inc. or its affiliates

3. After logging in, the **Billing & Cost Management Dashboard** page appears. In the left navigation bar, click **[Preferences]**. The **Preferences** page appears:



4. Select the **Receive Billing Alerts** checkbox.

CAUTION: If you enable this option, this option cannot be disabled.

5. Click the [Save Preferences] button.

Creating an AWS Credential

To use the Dynamic Applications in the Amazon Web Services PowerPack, you must first define an AWS credential in the ScienceLogic platform. The PowerPack includes the following sample credentials you can use as templates for creating SOAP/XML credentials for AWS:

- AWS Credential Proxy, for users who connect to AWS through a third-party proxy server
- AWS Credential Specific Region, for users who connect to a GovCloud account or the Beijing region
- AWS Credential, for users who do not use a proxy server nor connect to a specific AWS region

To define an AWS credential:

- 1. Go to the **Credential Management** page (System > Manage > Credentials).
- 2. Locate the AWS Credential, AWS Credential Proxy, or AWS Credential Specific Region credential and click its wrench icon (*P*). The Credential Editor modal page appears:

Credential Editor [77]	×
Edit SOAP/XML Credential #77	New Reset
Basic Settings Profile Name Content Encoding Method HTTP Version AWS Credential [text/xml] [POST] [HTTP/1.1] URL [https://Host:Port/Path %D = Aligned Device Address %N = Aligned Device Host Name] Inttp://example.com/ [http://example.com/ [http://example.com/	Soap Options Embedded Password [%P] Embed Value [%1] Embed Value [%2]
HTTP Auth User HTTP Auth Password Timeout (seconds) [AWS Account Access Key] 2	Embed Value [%3] Embed Value [%4]
Proxy Settings Hostname/IP Port User Password 0	HTTP Headers + Add a header
CURL Options CAINFO CAPATH CLOSEPOLICY CONNECTTIMEOUT COOKIES COOKIESTR COOKIESTR COOKIELST CRLF CUSTOMREQUEST DNSCACHETIMEOUT	
Save Save As	

3. Enter values in the following fields:

Basic Settings

- Profile Name. Type a new name for your AWS credential.
- HTTP Auth User. Type your Access Key ID.
- HTTP Auth Password. Type your Secret Access Key. The characters appear as asterisks to protect your password privacy.

Proxy Settings

NOTE: The *Proxy Settings* fields are required only if you are discovering AWS services through a proxy server. Otherwise, leave these fields blank.

- Hostname/IP. Type the host name or IP address of the proxy server.
- **Port**. Type the port on the proxy server to which you will connect.
- User. Type the username used to access the proxy server.
- Password. Type the password used to access the proxy server.

CAUTION: If you are creating a credential from the AWS Credential - Proxy example and the proxy server does not require a username and password, then the User and Password fields must both be blank. In that scenario, if you leave the "<Proxy_User>" text in the User field, the ScienceLogic platform cannot properly discover your AWS services.

SOAP Options

- **Embed Value [%1]**. To monitor a GovCloud account, type "us-gov-west-1". To monitor the Beijing region, type "cn-north-1". Otherwise, leave this field blank.
- 4. Click the [Save As] button, and then click [OK].

Testing the AWS Credential

The ScienceLogic platform includes a Credential Test for Amazon Web Services. Credential Tests define a series of steps that the platform can execute on demand to validate whether a credential works as expected.

The AWS Credential Test can be used to test a SOAP/XML credential for monitoring AWS using the Dynamic Applications in the Amazon Web Services PowerPack. The AWS Credential Test performs the following steps:

• Test Reachability. Performs an ICMP ping request to the URL for the EC2 service in the region specified in the credential. If a region is not specified in the credential, the us-east-1 region is used.

- Test Port Availability. Performs an NMAP request to TCP port 443 on the URL for the EC2 service in the region specified in the credential. If a region is not specified in the credential, the us-east-1 region is used.
- **Test Name Resolution**. Performs an nslookup request on the URL for the EC2 service in the region specified in the credential. If a region is not specified in the credential, the us-east-1 region is used.
- Make connection to AWS account. Attempts to connect to the AWS service using the account specified in the credential.
- Scan AWS services. Verifies that the account specified in the credential has access to the ec2, iam, and s3 services.

NOTE: The AWS Credential Test does not support the testing of credentials that connect to AWS through a proxy server.

To test the AWS credential:

- 1. Go to the **Credential Test Management** page (System > Customize > Credential Tests).
- 2. Locate the **AWS Credential Test** and click its lightning bolt icon (*****). The **Credential Tester** modal page appears:

Credential Tester [[BETA] ×
Test Type	[AWS Credential Test]
Credential	Amazon Web Services Credential
Hostname/IP	
Collector	[RS-DCU-69]
	Run Test

- 3. Supply values in the following fields:
 - Test Type. This field is pre-populated with the credential test you selected.
 - **Credential**. Select the credential to test. This drop-down list includes only credentials that you have access to that can be tested using the selected credential test.
 - Hostname/IP. Leave this field blank.
 - Collector. Select the All-In-One Appliance or Data Collector that will run the test.
- 4. Click the [Run Test] button to run the credential test. The Test Credential window appears:

Step	Description	Log Message	Status	
Test Reachability	Check to see if the EC2 service is reachable using ICMP	The EC2 service is reachable using ICMP. The average response time is 3.400ms	Passed	
2 Test Port Availability	Check to see if the EC2 HTTPS port is open	Port 443 is open	Passed	
8 Test Name Resolution	Check to see if nslookup can resolve the EC2 Service	Name resolution succeeded: Forward returned 1 result	Passed	
Make connection to AWS ad	ccount Check to see if an AWS account can be connected to and querier	d. AWS connection succeeded	Passed	
Scan AWS Services	Verify services are available to specified account.	AWS service scan succeeded	Passed	

2

The **Test Credential** window displays a log entry for each step in the credential test. The steps performed are different for each credential test. The log entry for each step includes the following information:

- **Step**. The name of the step.
- **Description**. A description of the action performed during the step.
- Log Message. The result of the step for this credential test.
- **Status**. Whether the result of this step indicates the credential or the network environment is configured correctly (Passed) or incorrectly (Failed).
- Step Tip. Mouse over the question mark icon () to display the tip text. The tip text recommends what to do to change the credential or the network environment if the step has a status of "Failed".

Creating an AWS Virtual Device

Because the Amazon Web Service does not have a specific IP address, you cannot discover an AWS device using discovery. Instead, you must create a **virtual device** that represents the Amazon Web Service. A virtual device is a user-defined container that represents a device or service that cannot be discovered by the ScienceLogic platform. You can use the virtual device to store information gathered by policies or Dynamic Applications.

To create a virtual device that represents your Amazon service:

- 1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
- 2. Click the [Actions] button, then select Create Virtual Device. The Virtual Device modal page appears:

Virtual Device		×
Create Virtual Device		Reset
Device Name	Amazon Cloud	
Organization	System	•
Device Class	Service AWS Service	•
Collector	CUG	T
	Add	

- 3. Enter values in the following fields:
 - **Device Name**. Enter a name for the device. For example, you could enter "Amazon Cloud" in this field.
 - Organization. Select the organization for this device. The organization the device is associated with limits the users that will be able to view and edit the device.
 - Device Class. Select Service | AWS Service.
 - Collector Group. Select the collector group that will monitor the device.

4. Click the **[Add]** button to create the virtual device.

Understanding the AWS Dynamic Applications

The Dynamic Applications in the Amazon Web Services PowerPack are divided in to four types:

- **Discovery**. These Dynamic Applications poll AWS for new instances of services or changes to existing instances of services.
- **Instance**. These Dynamic Applications retrieve configuration information about each service instance and retrieve any changes to that configuration information.
- Performance. These Dynamic Applications poll AWS for performance metrics.
- *Health*. These Dynamic Applications collect the RSS status update messages from the Amazon Health Status page (http://status.aws.amazon.com/).

Service Discovery Dynamic Applications are responsible for searching the AWS cloud for instances of specific service. Typically, a Service Discovery Dynamic Application will then align Discovery Dynamic Applications for each AWS service it discovers, Performance Dynamic Applications for each discovered service, and Configuration Dynamic Applications for each discovered service.

For example, the Dynamic Application "AWS EC2 Service Discovery" will create a component device for the EC2 service and align the Dynamic Applications "EC2 Service Performance", "EC2 Service Health", and "EC2 Instance Discovery" to that component device.

The Dynamic Application "EC2 Instance Discovery" will create component devices for each EC2 instance and align the Dynamic Applications "EC2 Instance" (a Configuration Dynamic Application), "EC2 Instance Performance", and "EBS Discovery" to that component device.

The general Dynamic Application hierarchy is:

- Account Discovery
 - Region Discovery
 - Zone Discovery
 - Service Discovery
 - Service Performance
 - Service Health
 - Instance Discovery
 - Instance Config
 - Instance Performance

AWS Account Discovery

The Dynamic Application "AWS Account Discovery" is the root Dynamic Application that retrieves the user's account permissions. The "Account" component device uses the full user ID as the device name.

The "AWS Account Discovery" Dynamic Application aligns the Dynamic Applications "AWS Region Discovery" and "AWS Region Instance" to the account component device. These Dynamic Applications discover the AWS Regions that contain services for the user.

The "AWS Account Discovery" Dynamic Application retrieves account-specific performance statistics such as total number of API calls and custom (application-specific) performance metrics.

Configuring "AWS Lambda Service Discovery"

By default, the "AWS Lambda Service Discovery" Dynamic Application is configured to discover only regular Lambda functions, not replica 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.

To configure the "AWS Lambda Service Discovery" Dynamic Application to discover both regular and replica Lambda functions:

- 1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
- 2. Locate the "AWS Lambda Service Discovery" Dynamic Application and click its wrench icon (*P*). The **Dynamic Applications Properties Editor** page appears.
- 3. In the **Operational State** field, select *Disabled*, and then click **[Save]**. This disables the Dynamic Application from collecting data.

Close <u>P</u> roperties	<u>C</u> ollections	<u>S</u> nippets	Threshold	ds	Alerts	Comp	onent	Subso	cribers	
Dynamic Applications [1438] Properties	Editor								Guide	Reset
Application Name [AWS Lambda Service Discovery Application Type [[Snippet Configuration] Caching	€	Version Nur [Version 1.0] Operational Disabled	mber	[Default]	Abandon Cor Null Rov	Collection Itext	•		Disable Rol	lup of Data it Mapping
[No caching] Device Dashboard None	▼ €	Poll Freque	ency ⊧s]▼ 😯	[Hide rov	v] Null Colur s]	nn Option	• •		Save	re e As
Description										
Release Notes & Change Log										
₿ - ♪ B I <u>U</u> S	A- TI- 0-	¶ - %-		12 3 ⊟ i≡	⊞	<u>୧</u> ତ୍ତ 🎦	<u>_</u> <	/>		
Version 1.0: 1. Initial Version of the AWS L Copyright (c) 2003-2018 Scien	ambda Service	Discovery dynar	nic application	1.						A
This software is the copyrighter Use of the Software is governe agreement, which accompanie ("License Agreement"). An end that is accompanied by or inclu	d work of Scienc d by the terms of s or is included v user is not perm des a License A	eLogic, Inc. f the software lic vith the Software nitted to install a greement, unles	ense ∋ ny Software s he or she							
first agrees to the License Agre	ement terms.									•

- 4. Click the [Snippets] tab. The Dynamic Applications Snippet Editor & Registry page appears.
- 5. In the **Snippet Registry** pane, click the wrench icon (*P*) for the "aws_lambda_service_discovery" snippet.
- 6. In the Active State field, select Disabled, and then click [Save]. This disables the "aws_lambda_service_ discovery" snippet.

Close <u>P</u> roperties <u>C</u> ollections	<u>S</u> nippets <u>T</u> hresholds	<u>A</u> lerts C	Component Subscribers	6
Dynamic Applications [1438] Snippet Editor & Registry Editing S	nippet [1782]			Guide Reset
Snippet Name aws_lambda_service_discovery from content import content_errors, conten from silo_aws import AwsLambdaServiceDiscovery' with content_errors.ErrorManager(self): with content_logger.LogManager(self) a replica_discovery = False AwsLambdaServiceDiscovery(self, sn	Active State Disabled Snipper Code t_logger very s logger: ippet_id, replica_discovery)	•	Required [Required - Stop Collection]	
	Save Save As			
Snippet Registry Snip Aws_lambda_service_discovery aws_lambda_service_orscovery_snow_replicas	pet Name		State Required ID Enabled Required snip_1782 Enabled Required snip_1783	Date Edit 2 2018-07-09 09:58:21 3 2018-07-10 07:51:04 4

- 7. In the **Snippet Registry** pane, click the wrench icon (*P*) for the "aws_lambda_service_discovery_show_ replicas" snippet.
- 8. In the Active State field, select Enabled, and then click [Save]. This enables the "aws_lambda_service_ discovery_show_replicas" snippet.
- 9. Click the [Collections] tab. The Dynamic Applications | Collections Objects page appears.

 Click the wrench icon (P) for the first Collection Object listed in the Collection Object Registry pane, select aws_lambda_service_discovery_show_replicas in the Snippet field for that Collection Object, and then click [Save].

Close	<u>P</u> roperties	<u>C</u> ollections	<u>S</u> nippet:	s <u>T</u> hres	holds	<u>A</u> lerts		Compon	ent	Subs	scriber	S	
Dynamic Applications	[1438] Collection Obj	ects										Guide R	eset
Object Name	Availability								Descr	iption			
Snippet Arguments	exists					Availability	of the s	service co	nponer	nt.			
Class Type	[10 Config Character]												
String Type	[Standard]	•											
Custom Attribute	[None]	T											
Snippet	[aws_lambda_service	_discovery_sho	ow_replicas]	•									11
Group / Usage Type	[Group 1]	▼ [St	andard]	V		Component	Identifiers	,					
Asset / Form Link	[None]	▼ [No	one]	•		Availability	ruentinera	, 			Form	iuia	
Inventory Link	[Disabled]	•				Class Identifier	1						
Change Alerting	[Disabled]			T		GUID (%G)	2						
Table Alignment	[Left]	•				MAC Address		_					
Hide Object	v					Organization		•					
				Save	Sa	ve As				🗆 Disa	ible Obj	ect Maintenance	
Collection Object R	egistry				_								
	Object Name			Class	Class	Snippet Argumen	ts Group	ID	Asset Link	Change Alerting	Align	Edit Date	
1. 🥜 Availability			Con	fig Character	10	exists	1	o_16713		Disabled	Left	2018-07-10 07:51:5	2
2. PDistinguished	Vame		Con	fig Character	10	arn	1	o_16717		Disabled	Left	2018-07-10 07:51:1	7
3. <i>P</i> Id			Con	fig Character	10	id	1	o_16714		Disabled	Left	2018-07-10 07:51:2	3
4. Allamo			Labe	el (Config Group)	108	nomo	1	0_16/16		Disabled	Left	2018-07-10 07:51:2	8
5. privalne			Con	lig Character	10	name		0_10/15		Disabled	Leit	2010-07-10 07.51.5	4
						[5	Select Actio	on]				•	Go

- 11. Repeat step 10 for all of the remaining Collection Objects listed in the Collection Object Registry pane.
- 12. Click the **[Properties]** tab.
- 13. In the **Operational State** field, select *Enabled*, and then click **[Save]**. This re-enables data collection for the Dynamic Application.

NOTE: If you configure the "AWS Lambda Service Discovery" Dynamic Application to discover both regular and replica Lambda functions, then when you run discovery, the Dynamic Applications in the Amazon Web Services PowerPack will create <u>parent/child relationships</u> between replica Lambda functions and their corresponding master Lambda functions. In this scenario, the <u>Device View and other</u> <u>device component maps</u> will display the relationship in this order: Lambda Function Service > Lambda Replica Function > Master Lambda Function. The replica appears as the parent to the master Lambda function because the replica could be in the same or a different region than the master Lambda function.

Configuring "AWS Lambda Function Qualified Discovery"

By default, the "AWS Lambda Function Qualified Discovery" Dynamic Application is configured to discover and model all Lambda alias components. An **alias** is a qualifier inside an AWS Lambda function that enables the user to control which versions of the Lambda function are executable—for instance, a production version and a test version.

When the "AWS Lambda Function Qualified Discovery" Dynamic Application is configured to discover alias components, the ScienceLogic platform collects data only for the Lambda function versions specified in the alias.

Depending on your needs, you can optionally configure the Dynamic Application to instead do one of the following:

- Discover and model all Lambda version components. If you select this configuration, the ScienceLogic platform collects data for all existing versions of the Lambda function.
- Discover and model only Lambda version components with AWS configurations filtered by a trigger. If you select this configuration, the ScienceLogic platform collects data only for versions of the Lambda function that have triggers or are specified in an alias.

NOTE: If you have configured the "AWS Lambda Service Discovery" Dynamic Application to discover both regular and replica Lambda functions and you want the ScienceLogic platform to create dynamic component map relationships between replica Lambda functions and their parent Lambda function versions, you must follow these instructions to configure the "AWS Lambda Function Qualified Discovery" Dynamic Application to discover and model all Lambda version components.

To configure the "AWS Lambda Function Qualified Discovery" Dynamic Application:

- 1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
- Locate the "AWS Lambda Function Qualified Discovery" Dynamic Application and click its wrench icon (*P*). The Dynamic Applications Properties Editor page appears.

3. In the **Operational State** field, select *Disabled*, and then click **[Save]**. This disables the Dynamic Application from collecting data.

	<u>P</u> ropertie	s <u>C</u>	ollection	s	<u>S</u> ni	ippets	Thre	sholds		Alerts			Comp	onent	t	Subsc	ribers		
Dynamic Applications	[1442] Proj	perties Edito	or														Guide		Reset
AWS Lambda F [[Snippet Config [[No caching]]	Application N unction Quali Application T juration] Caching Device Dasht	lame ified Discover Type board	ry @ ▼ @ ▼ @ ▼ @		V [Versio Disable [Every	Version N n 1.0] peration ed Poll Free 15 Minu	lumber v e al State v e juency ites] v e	ſ	efault] lide rov - values	Aba N V] Nul 3]	Cor ull Rov	Colle ntext w Op mn O	tion ption				Disab Com	le Rollup () ponent Ma)) Save Save Save As	of Data apping
Description																			
Release Notes & Char	nge Log						vice.												/j
B. A. D.	I II .	S 1 -	Tt-	A -	a .	×	=. 7=		:=	m .	_	Q			1				
		5 A	11.		11			1	:=	HH .		· · · · · · · · · · · · · · · · · · ·			~//				_
Version 1.0: 1. Initial Versio Copyright (c) 20	את of the A 03-2018 כ	WS Lamb	da Func gic, Inc.	ction C	Qualifie	ed Diso	covery dyna	amic appli	cation	I.									_
This software is Use of the Softw agreement, whi	the copyri vare is gov ch accomp	ighted wor verned by panies or i	rk of Sci the term s include	encel ns of t ed wit	Logic, I the soft th the S	lnc. tware Softwa	license ire												

- 4. Click the [Snippets] tab. The Dynamic Applications Snippet Editor & Registry page appears. The Snippet Registry pane includes the following snippets:
 - aws_lambda_function_aliases_discovery. When this snippet is enabled, the Dynamic Application discovers all Lambda alias components.
 - aws_lambda_function_all_versions_discovery. When this snippet is enabled, the Dynamic Application discovers all Lambda version components.
 - aws_lambda_function_versions_by_triggers_discovery. When this snippet is enabled, the Dynamic Application discovers Lambda version components with AWS configurations containing a trigger or those with an alias.

5. One at a time, click the wrench icon (*P*) for each of the snippets, select *Enabled* or *Disabled* in the **Active State** field, and then click **[Save]** to enable the appropriate snippet and disable the others.

Close <u>P</u> roperties	<u>C</u> ollections	<u>S</u> nippets	<u>T</u> hresholds	<u>A</u> lerts	Component	Subscribers	
Dynamic Applications [1442] Snippet I	ditor & Registry Editing S	Snippet [1787]					Guide Reset
Snippet Nam aws_lambda_function_aliases_c	e iscovery	[Disabled]	Active State Snippet Code		[Required - S	Required Stop Collection]	T
<pre>from content import con from silo_aws import Aw</pre>	tent_errors, conter sLambdaFunctionAlia	nt_logger asDiscovery					
<pre>app_name = 'AwsLambdaFu with content_errors.Err with content_logger AwsLambdaFuncti</pre>	nctionAliasDiscover orManager(self): LogManager(self) a onAliasDiscovery(se	y' 15 logger: 1f, snippet_	id).process()				
			Save Save As				
Snippet Registry							
1 ws_lambda_function_aliases	Snip _discovery ns_discovery by triggers_discovery	ppet Name			State Reg Disabled Reg Enabled Reg	quired ID puired snip_1787 puired snip_1788 puired snip_1789	Date Edit 2018-07-09 11:29:35
	,						

NOTE: You can enable only one of these snippets at a time.

6. Click the [Collections] tab. The Dynamic Applications | Collections Objects page appears.

7. Click the wrench icon (*P*) for the first Collection Object listed in the **Collection Object Registry** pane, select the snippet you enabled in step 5 in the **Snippet** field for that Collection Object, and then click **[Save]**.

Close	<u>P</u> roperties	<u>C</u> ollectio	ns <u>S</u> ni	ppets	Thresh	olds	Alerts		Compone	ent	Subs	cribers	6	
Dynamic Applications	[1442] Collection Ob	jects											Guide	Reset
Object Name	Availability									Descri	otion			
Snippet Arguments	exists						Availability of	the s	ervice com	ponen	t.			
Class Ture		1			11									
String Type	[10 Config Character]				•									
Custom Attribute	[Standard]	•												
Sninnet	Laws lambda functio	on all version	ns. discovery 1		•									
Group / Usage Type	[[aws_lamoua_luncut	JII_all_version	IStandardi											
Asset / Form Link	[None]		[None]		•		Component Id	entifiers				Form	ula	
Inventory Link	[Disabled]		[]				Class Identifier 2		A					
Change Alerting	[Disabled]				T		GUID (%G)							
Table Alignment	[Left]	•					Organization							
Hide Object	 Image: A start of the start of						Previous Unique I	Ds	•					13
	_				0 X	0	- 4-				_			
					Save	Sav	e As				Disa	ble Obje	ect Maintenance	•
Collection Object R	egistry													
	Object Nam	ie			Class	Class	Snippet Arguments	Group	ID	Asset	Change	Alian	Edit Date	
1 Au vailability				Config	Type Character	10	exists	1	o 16772	Link	Alerting	Left 2	018-07-09 11:3	0:08
2. Class Identifier	1			Config C	haracter	10	classIdentifier1	1	o 16778		Disabled	Left 2	2018-07-09 11:3	0:22
3. ADistinguished I	Name			Config C	haracter	10	arn	1	o_16776		Disabled	Left 2	2018-07-09 11:3	0:29
4. 🥜Id				Config C	haracter	10	id	1	o_16773		Disabled	Left 2	2018-07-09 11:3	0:35
5. 🥜 Lambda Functi	ion Qualifieds			Label (C	onfig Group)	108		1	o_16775		Disabled	Left 2	2018-07-09 11:3	0:43
6. 🥜 Name				Config C	Character	10	name	1	o_16774		Disabled	Left 2	2018-07-09 11:3	0:51
7. 🥜 Qualifier				Config C	Character	10	qualifier	1	o_16777		Disabled	Left 2	2018-07-09 11:3	0:58
							[Sele	ect Actio	on]					Go

- 8. Repeat step 7 for all of the remaining Collection Objects listed in the Collection Object Registry pane.
- 9. Click the [Properties] tab.
- 10. In the Operational State field, select Enabled, and then click [Save]. This re-enables data collection for the Dynamic Application. The next time discovery is run, new component devices might be discovered and some previously discovered components might become unavailable, depending on how you configured the Dynamic Application.
- **NOTE:** If you configure the "AWS Lambda Function Qualified Discovery" Dynamic Application to discover Lambda alias or version components and your AWS service includes an API Gateway that triggers a Lambda Function, then the Dynamic Applications in the Amazon Web Services PowerPack will create a device relationship between that Lambda Function and its corresponding Lambda alias or version component device.

Discovering the AWS Account

To discover your AWS account, you must manually align the following Dynamic Applications with the AWS virtual device:

- AWS Health
- AWS Account Discovery

After you manually align these Dynamic Applications, the other Dynamic Applications in the Amazon Web Services PowerPack will automatically align to discover and monitor all of the components in your AWS account.

TIP: If your AWS account includes API Gateways or Lambda services to be monitored and you want the ScienceLogic platform to put those component devices in a "vanished" state if the platform cannot retrieve data about them for a specified period of time, ScienceLogic recommends setting the Component Vanish Timeout Mins. field to at least 120 minutes. For more information, see the chapter on "Vanishing and Purging Devices" in the Device Management manual.

To align the Dynamic Applications to your virtual device:

- 1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
- 2. Click the wrench icon (🎤) for your virtual device.

3. In the **Device Administration** panel, click the **[Collections]** tab. The **Dynamic Application Collections** page appears:

Close	<u>P</u> roperties	T <u>h</u> resholds	<u>C</u> ollections	<u>M</u> onitors			
<u>S</u> chedule	Logs	T <u>o</u> olbox	Interfaces	<u>R</u> el ations hips	Tickets	Redirects	<u>N</u> otes
					101 10 1		
Device Name	Amazon Cloud			Managed Ty	pe Virtual Device		
Ches	1001 Convice			Sub Cla	AVANS Service		
Organization	Sustem			Linti	AVV3 Service		Contine
Organization	System			Group / Collec	tor CLIG Lem7 ao		Service
					coorenn_ao		🚣 🐸 📶 🖶 🥜
Device Hostname							Amazon Cloud
				_			
Dynamic Applica	tion [™] Collections	Application Added				Expand	Actions Reset Guide
		Dynamic Application		<u>ID</u>	Poll Frequency	Type	Credential
+ AWS Account	Discovery			32	5 mins	Snippet Configuration	Amazon Web Services Credential 🥖 🗌
+ AWS Health				137	30 mins	Snippet Configuration	Amazon Web Services Credential 📝 📃
						[Select Action]	▼ Go
					_		
				Sav	2		

- 4. Click the [Actions] button, and then select Add Dynamic Application from the menu.
- 5. In the **Dynamic Application Alignment** modal page, select AWS Health in the **Dynamic Applications** field.
- 6. In the Credentials field, select the credential you created for your AWS service.
- 7. Click the [Save] button to align the Dynamic Application.
- 8. Repeat steps 4-7 for the "AWS Account Discovery" Dynamic Application.

Viewing AWS Component Devices

When the ScienceLogic platform performs collection for the AWS virtual device, the platform will create component devices that represent each element in your AWS infrastructure and align other Dynamic Applications to those component devices. Some of the Dynamic Applications aligned to the component devices will also be used to create additional component devices. All component devices appear in the **Device Manager** page (Registry > Devices > Device Manager).

In addition to the **Device Manager** page, you can view the AWS service and all associated component devices in the following places in the user interface:

• The **Device View** page displays a map of a particular device and all of the devices with which it has parentchild relationships. Double-clicking any of the devices listed reloads the page to make the selected device the primary device:



• The **Device Components** page (Registry > Devices > Device Components) displays a list of all root devices and component devices discovered by the ScienceLogic platform in an indented view, so you can easily view the hierarchy and relationships between child devices, parent devices, and root devices. To view the component devices associated with an AWS service, find the AWS virtual device and click its plus icon (+):

[Device Name •	IP Address	Device Category	Device Class Sub-class		Organization	Current State >=Health ▼	Collection Group	Collection State	
AWS_CC	DM_04_QALS-RO	- "	Service	AWS Service	260	AWS_COM_04	🛦 Healthy	CUG_Automatio	n User-Disabled	🖶 👯 🗞 🖉
	Device Name •	IP Address	Device Category	Device Class Sub-class		Organization	Current State	Collection Group	Collection State	
. — 🥜 📶 AID	DAJXNRL3TG5ESLKGCP6	· ·	Account	AWS Account	261	AWS_COM_04	🛕 Healthy	CUG_Automatio	r User-Disabled	🖶 🎗 🗞 🛲
	Device Name •	IP Addre	<u>Devi</u> 255 <u>Categ</u>	re pry. Device Class Sub-class		Organization	Current State >=Health ▼	Collection Group	Collection State)
1. – 🥕	Central: ca-central-1		Region	AWS Region Canada (Central	l) 276	AWS_COM_04	🛦 Healthy	CUG_Automatio	User-Disabled	🖶 🏹 🗞 🚠
	Device Name •		ddress <u>Ca</u>	evice tegory Device Class Sub-cla	iss D	D Organization	Current State >=Healthr ▼	Collection Group	Collection State	
1. +	🤌 📶 ca-central-1 API Gatewa	ay Service 💆	Servi	ce AWS API Gateway Service	133	0 AWS_COM_04	🛦 Healthy	CUG_Automatic	User-Disabled	1 × 1
2. +	🤌 🎢 ca-central-1 CloudTrail S	Service 🖤	Servi	ce AWS CloudTrail Service	346	AWS_COM_04	🛦 Healthy	CUG_Automatic	User-Disabled	🖷 🎝 🗞 😹
3.	🤌 📶 ca-central-1 CloudWatcl	h Service 🖉	Servi	ce AWS CloudWatch Service	307	AWS_COM_04	🛦 Healthy	CUG_Automatic	User-Disabled	🖶 🏷 🗞 😹
4. +	ntral-1 S3 Service		Servi	ce AWS S3 Service	366	AWS_COM_04	🛦 Healthy	CUG_Automatic	User-Disabled	🖷 👯 🗞 😹
5. +	ntral-1 Security		Netw	ork AWS Security	338	AWS_COM_04	🛦 Healthy	CUG_Automatic	User-Disabled	n 🏹 🗞 😹
6. +	nt ca-central-1 VPC Servic	xe 💌	Servi	ce AWS VPC Service	297	AWS_COM_04	🛦 Healthy	CUG_Automatic	User-Disabled	🖶 🖏 🖏 📠
7.			Avail	abilityZor AWS Availability Zone - Cer	ntral 985	AWS_COM_04	A Healthy	CUG_Automatic	User-Disabled	19 1 19 19 19 19 19 19 19 19 19 19
8.	🤌 📶 ca-central-1b	•	Avail	abilityZor AWS Availability Zone - Cer	ntral 980	AWS_COM_04	A Healthy	CUG_Automatic	User-Disabled	H 🕄 🗞 🧟
2. + 🥕	CloudFront Service	•	Service	AWS CloudFront Service	264	AWS_COM_04	A Healthy	CUG_Automatic	User-Disabled	📾 👯 🗞 🙈
3. + 🥠	I Frankfurt: eu-central-1	۳	Region	AWS Region EU (Frankfurt)	277	AWS COM 04	A Healthy	CUG Automatio	User-Disabled	📾 💢 🗞 者

The Component Map page (Views > Device Maps > Components) allows you to view devices by root
node and view the relationships between root nodes, parent components, and child components in a map.
This makes it easy to visualize and manage root nodes and their components. The ScienceLogic platform
automatically updates the Component Map as new component devices are discovered. The platform also
updates each map with the latest status and event information. To view the map for an AWS service, go to
Views > Device Maps > Components, and select the map from the list in the left NavBar. To learn more
about the Component Map page, see the Views manual.



Relationships Between Component Devices

In addition to the parent/child relationships between component devices, relationships are automatically created by the Dynamic Applications in the Amazon Web Services PowerPack between the following component devices:

- AWS API Gateway Services and AWS Network Load Balancers
- AWS API Instances and AWS Lambda Functions
- AWS Application ELBs and AWS Availability Zones
- AWS Application ELBs and AWS Security Groups
- AWS Application ELBs and AWS VPC Instances
- AWS Auto Scale Groups and AWS Auto Scale Launch Configurations
- AWS EC2 Instances and AWS Auto Scale Groups
- AWS EC2 Instances and AWS EBS Volumes
- AWS EC2 Instances and AWS Elastic Beanstalk Applications
- AWS EC2 Instances and AWS ELB Instances
- AWS EC2 Instances and AWS EMR Instances
- AWS EC2 Instances and AWS OpsWorks Instances
- AWS EC2 Instances and AWS Security Groups

- AWS EC2 Instances and AWS VPC Instances
- AWS EC2 Instances and AWS VPC Subnets
- AWS EC2 Instances and the Cisco Cloud Center application
- 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
- AWS Route Tables and AWS Subnets
- AWS Route Tables and AWS Virtual Private Gateways
- AWS S3 Instances and AWS CloudTrail Instances
- AWS Security Groups and AWS VPC Instances
- AWS SNS Instances and AWS CloudTrail Instances
- AWS SNS Instances and AWS Glacier Instances
- AWS VPC Instances and other intra-account AWS VPC Instances

Configuring the AWS Dashboards

The AWS Account Billing and AWS Health Status dashboards must have their (base) Custom Table widgets manually configured to filter only AWS service-specific events. To do this:

- 1. Go to Dashboards > AWS Account Billing.
- 2. Click the down-arrow in the upper-right of the AWS Events widget, and then select *Configure* from the **Options** menu. The **Widget Configuration** modal page appears.

3. In the **Device Class** filter, enter "AWS" to show only AWS device classes:

Dashboards						
[AWS Account Billing]						
SH GH	Widget Configuration				Close / Esc	
Estimated Billion (Last 12 hours)	Editing: (base) Custom Table				Reset	
Contrator of Contrational	Widget Na	me		Widget Refresh Ra	te	
	AWS Events		Widget default (1 minute)			
200 no data						
11 No data was found for	Options				-	
	Entity Type					
	- can be Contextually Driven					
	Page Results					
	Prive Context					
	Contextually Driven (if applicable)				1	
	- Date Basse					
	last 12 [Hours]					
	Lise Timespan' context					
	always 👻					
	Field for 'Timespan' context					
	[Last Detected]					
	Disabled Columns	Event Severity	Device Class	Device Group / IT Service		
	et en	AWS				
		All Severities AWS Acc	count AWS Account	All Groups		
AWS Events		Notice AWS Aut	5 Scale Group AWS Auto :	EM7 (IT Service) Example Map		
	Acknowledged	Minor AWS Aut	o Scale Service AWS Auto	FS To Disable		
	C licket D	Major AWS Ava Critical AWS Clo	udFront Behavior I AWS Clo	KVM (II Service) Some Devices		
Idata local: File system usage exceeded	C External Ticket	+ AWS Close	JdFront Error Page AWS C +	VMware Health (IT Service) +		
T Service State Major: Windows	Date Acknowledged	Event Policy	Device Category	Organization	-	
Nameserver not responding to DNS			Save		Create Template	
Physical Memory has exceeded th				ANA ING. FLAGRE		
Swap Memory has exceeded three						

- 4. Control-click on the following items in the **Device Class** field:
 - AWS DDB Service
 - AWS EC2 Service
 - AWS ELB Service
 - AWS EMR Service
 - AWS RDS Service
 - AWS SNS Service
 - AWS SQS Service
 - AWS Storage Gateway Service
- 5. Click the **[Save]** button.
- 6. Repeat steps 1 5 for the AWS Health Status dashboard.

Amazon API Throttling Events

By default, the ScienceLogic platform will use the Collector Group aligned with the root AWS virtual device to retrieve data from AWS devices and services.

If the platform must collect data from a large set of AWS devices and services, the platform might generate Notify events with a message ending in the text "Retry #1-10 Sleeping: ... seconds". The platform generates these events when the Amazon API throttles collection in response to a large number of requests to the API. Even though the platform is generating Notify "Retry" events, the platform is still collecting data from AWS. This issue commonly occurs when a specific Amazon data center edge is close to capacity.
If the ScienceLogic platform generates the Minor event "Collection missed on <device> on 5 minute poll", this indicates that the platform was unable to retrieve that specific datum from the Amazon cloud during the most recent five-minute polling cycle. If you frequently see the "Collection missed" event across your cloud, you must contact Amazon support to whitelist the IP address of your Data Collector. This will prevent further throttling from occurring.

Chapter

3

Overview

The following sections describe the CloudWatch alarm Event Policies that are included in the Amazon Web Services PowerPack and information about configuring CloudWatch and the platform to generate events based on CloudWatch alarms:

Configuring Inbound CloudWatch Alarms

CloudWatch Alarm Event Policies	. 38
Creating Custom CloudWatch Metrics	.40
Configuring CloudWatch to Send Alarms for a Metric	. 42
Enabling Custom Metrics Collection in the ScienceLogic Platform	.45
Configuring the "AWS CloudWatch Alarms Performance" Dynamic Application	. 45
Enabling CloudWatch Alarm Events in the ScienceLogic Platform	47

CloudWatch Alarm Event Policies

Amazon CloudWatch is a service that allows you to monitor your AWS resources and applications in near realtime. You can use CloudWatch to collect and track metrics, and use CloudWatch alarms to send notifications or automatically trigger changes to the resources being monitored based on rules that you define.

In addition to the ScienceLogic platform collecting metrics for AWS instances, you can configure CloudWatch to send alarm information to the platform via API. The platform can then generate an event for each alarm.

The Amazon Web Services PowerPack includes an "AWS CloudWatch Alarms Performance" Dynamic Application. This Dynamic application monitors CloudWatch alarms and associates the alarms with the appropriate AWS component devices, if applicable. If an appropriate component device does not exist in the ScienceLogic Platform or cannot be determined, the alarm is instead associated with the component device for the AWS account. **CAUTION:** The performance data collected by the "AWS CloudWatch Alarms Performance" Dynamic Application is metadata intended to give general insight into the alarm activity the Dynamic Application is processing. This metadata can help identify overall trends, but users should be cautioned that the data presented can be imprecise in certain scenarios, such as when the Dynamic Application is being run in debug mode while data is still being collected.

Event Policy Name	Description	Event Source	Severity
AWS: CloudWatchAlarm_Action_Failed	An Amazon CloudWatch alarm action has failed.	API	Major
AWS: CloudWatchAlarm_Action_ InProgress	An Amazon CloudWatch alarm action is in progress.	API	Notice
AWS: CloudWatchAlarm_Action_ Succeeded	An Amazon CloudWatch alarm action has succeeded.	API	Notice
AWS: CloudWatchAlarm_ ConfigurationUpdate	A ConfigurationUpdate alarm type is received.	API	Notice
AWS: CloudWatchAlarm_StateUpdate_ Alarm	A CloudWatch alarm transitions to an "Alarm" state.	API	Major
AWS: CloudWatchAlarm_StateUpdate_ InsufficientData	A CloudWatch alarm transitions to an "Insufficient Data" state.	API	Notice
AWS: CloudWatchAlarm_StateUpdate_ OK	A CloudWatch alarm transitions to an "OK" state.	API	Healthy

The Amazon Web Services PowerPack also includes several pre-defined event policies for CloudWatch alarms:

These events are aligned to AWS Account component devices in the following way:

- If the CloudWatch alarm is configured on a device that is discovered in the ScienceLogic platform, then the event in the platform will be aligned with the component device for that instance.
- If the CloudWatch alarm is configured on a device that is either not discovered or not supported by CloudWatch, or if the ScienceLogic platform cannot determine a correct component device, then that alarm will be aligned to the Account component device.

The "AWS CloudWatch Alarms Performance" Dynamic Application and related Event Policies are disabled by default. If you want the platform to monitor CloudWatch alarms and generate events about them, you must enable the Dynamic Application and Event Policies. You must also configure the Dynamic Application to specify which types of alarms you want to monitor.

For more information about enabling and configuring the "AWS CloudWatch Alarms Performance" Dynamic Application, see the Configuring the "AWS CloudWatch Alarms Performance" Dynamic Application section. For more information about enabling the CloudWatch alarms Event Policies, see the Enabling CloudWatch Alarm Events in the ScienceLogic Platform section.

NOTE: Because the AWS services make new data points available at varying time intervals, there might be a difference in the data points collected by the ScienceLogic platform when compared to data presented in CloudWatch at a given time. The difference between the ScienceLogic platform and CloudWatch is typically less than 1%.

NOTE: If an event expires and the CloudWatch alarm in AWS is still in an "Alarm" state, the ScienceLogic Platform will not generate any additional CloudWatch events unless that CloudWatch alarm changes states in AWS.

Creating Custom CloudWatch Metrics

A CloudWatch alarm watches a single metric and performs one or more actions based on the value of the metric relative to a threshold over a number of time periods. A CloudWatch metric consists of the following elements:

- A namespace, such as AWS/EC2
- A metric name, such as CPUUtilization
- A value, such as 42.006
- A *dimension* that identifies a particular resource instance, such as {'Name': 'InstanceId', 'Value': 'i-0a6a989bb8d57b074'}

NOTE: For a complete list of supported CloudWatch Metrics and Dimensions, see <u>https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CW_Support_For_AWS.html</u>.

The Amazon Web Services PowerPack uses the metric dimensions identified in an alarm to associate the alarm message to a particular ScienceLogic component device. The following table lists the services that are currently supported and the dimensions used to associate an alarm to a component device:

AWS Service	Dimension
API Gateway	'ApiName', 'ApiName, Stage' NOTE : ScienceLogic recommends that you create API Gateways with unique names within the same region.
ApplicationELB	'LoadBalancer'

AWS Service	Dimension
CloudFront	'DistributionId'
DynamoDB	'TableName'
EBS	'Volumeld'
EC2	'InstanceId' 'AutoScalingGroupName'
ElasticBeanstalk	'EnvironmentName'
ElastiCache	'CacheClusterld' NOTE : Alarms for this service will be associated with the component device for the AWS account.
ElasticMapReduce	'JobFlowId'
ELB	'LoadBalancerName'
Glacier	'VaultId' NOTE : This service is not supported by CloudWatch. You must define a custom metric and publish the metric to the CloudWatch service using an agent toolkit or the AWS command- line interface.
Lambda	'FunctionName', 'Resource', 'Version', 'Alias', 'Executed Version' NOTE : Alarms "across all functions" for this service will be associated with the component device for the AWS account. Alarms "by function name" will be aligned to a specific Lambda function.
OpsWorks	'StackId', 'InstanceId'
RDS	'DBInstanceIdentifier' NOTE : Alarms for this service will be associated with the component device for the AWS account.
Redshift	'ClusterIdentifier' NOTE : Alarms for this service will be associated with the component device for the AWS account.
Route53	'HealthCheckId'
SNS	'TopicName'
SQS	'QueueName'
StorageGateway	'Gatewayld' & 'Volumeld'
\$3	'BucketName'

AWS enables users to create custom metrics for these services and then publish those metrics to CloudWatch using the AWS command-line interface (CLI) or an application programming interface (API). The Dynamic Applications in the *Amazon Web Services* PowerPack can then collect data for these custom AWS metrics (which are not in the "AWS" cloud namespace).

NOTE: For the Amazon Web Services PowerPack to collect data for these custom metrics, you must enable certain Dynamic Applications that are disabled by default. For more information, see the *Enabling Custom Metrics Collection in the ScienceLogic Platform* section.

When creating a custom metric, it is important that the metric is correctly formed. For the ScienceLogic platform to align a custom metric to a particular ScienceLogic component device, the following must be true:

• The metric namespace must include the service being tracked.

For example, *MyVendorName/EC2* would be a valid namespace that the *Amazon* Web Services PowerPack could use to identify the EC2 service for a tracked metric.

• The dimension must include one or more of the dimensions listed in the preceding table. The dimension enables the ScienceLogic platform to identify which device to associate with the alarm.

For example, if the dimension included {'Name': 'InstanceId', 'Value': 'i-0a6a989bb8d57b074'}, this would identify the EC2 component. Other dimensions are permitted, but 'InstanceId' is necessary to locate the EC2 instance.

If the component device was an AutoScaleGroup component that is also under the EC2 service, then the dimension might look like this: {'Name': 'AutoScalingGroupName', 'Value': 'Y1Z55ZJ390UP'}.

NOTE: If the CloudWatch event cannot align to a particular ScienceLogic component device, it will instead align to the component device for the AWS account.

Configuring CloudWatch to Send Alarms for a Metric

To configure CloudWatch to send alarms to the ScienceLogic platform for a metric, perform the following steps:

1. Open a browser session and go to <u>aws.amazon.com</u>.

2. Click **[My Account]** and then select AWS Management Console. If you are not currently logged in to the AWS site, you will be prompted to log in:

Sign In or Create an AWS Account What is your e-mail or mobile number? -mail or mobile number:	
I am a returning user	Now Available
and my password is:	Amazon Aurora
Sign in using our secure server	Enterprise-class database at 1/10th the cost
Forgot your password?	Learn more
Learn more about <u>AWS Identity and Access Management</u> and <u>AN</u>	<u>VS Multi-Factor Authentication</u> , features that provide
additional security for your AWS Account. View full <u>AWS Free U</u>	<u>sage Tier</u> offer terms.
oout Amazon.com Sign In nazon Web Services uses information from your Amazon.com account	to identify you and allow access to Amazon Web Services. Your

- 3. In the AWS Management Console, under the Management Tools heading, click [CloudWatch].
- 4. Click the [Browse Metrics] button.
- 5. Select the metric for which you want CloudWatch to send alarms.
- 6. Select the instances for which you want CloudWatch to send alarms for this metric.

7. Click the [Create Alarm] button. The Create Alarm page is displayed:

1. Select Metric 2. Define Alarm	
Alarm Threshold	Alarm Preview
rovide the details and threshold for your alarm. Use the graph on the right to help set the opropriate threshold.	This alarm will trigger when the blue line goes up to or above the red line for a duration of 5 minutes
Name: Description:	CPUUtilization >= 0 30 25
Whenever: CPUUtilization is: >= v 0 for: 1 consecutive period(s)	20 15 10 5 0 9/03 9/03 9/03 9/03 11:00 12:00 13:00 14:00
ACTIONS efine what actions are taken when your alarm changes state.	Namespace: AWS/EC2 Instanceld: i-51c892a6
Notification Delete	Metric Name: CPUUtilization
Whenever this alarm: State is ALARM Send notification to: Select a notification list New list Enter list	Period: 5 Minutes ▼ Statistic: Average ▼
+ Notification + AutoScaling Action + EC2 Action	

- 8. Specify a Name and Description for the alarm.
- 9. If you have previously configured an alarm for the ScienceLogic platform, select the notification list for the platform in the Send notification to field. Otherwise, select the [New list] link to the right of the Send notification to field and supply values in the following fields:
 - Send notification to. Enter a name for the new notification list. If you add additional alarms, you can select the name you enter in this field instead of re-entering the email address.
 - Email list. Enter the email alias you configured for the ScienceLogic platform email address.
- 10. Supply values in the other fields in this page as desired.
- 11. Click the [Create Alarm] button.
- 12. Log in to the email account you configured to receive email from the email alias.
- 13. Open the confirmation email from Amazon and click the [Confirm subscription] link.

Enabling Custom Metrics Collection in the ScienceLogic Platform

AWS enables users to publish their own custom metrics to CloudWatch using the AWS command-line interface (CLI) or an application programming interface (API). The *Amazon Web Services* PowerPack includes Dynamic Applications that collect data for custom AWS metrics (which are not in the "AWS" cloud namespace). However, these Dynamic Applications are disabled by default and must be enabled for use.

To enable these Dynamic Applications:

- 1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
- 2. Click the wrench icon (*P*) for the "AWS Custom Metrics" Dynamic Application. The **Dynamic Applications Properties Editor** page appears.
- 3. In the **Operational State** field, select Enabled.
- 4. Click the **[Save]** button.
- 5. Repeat steps 1 4 for the "AWS Custom Metrics Cache" Dynamic Application.

Configuring the "AWS CloudWatch Alarms Performance" Dynamic Application

The Amazon Web Services PowerPack includes an "AWS CloudWatch Alarms Performance" Dynamic Application that monitors CloudWatch alarms and associates the alarms with the appropriate AWS component devices, if applicable. This Dynamic Application must be enabled if you want the platform to generate CloudWatch alarm events.

NOTE: If an appropriate component device does not exist in the ScienceLogic platform or cannot be determined, the alarm is instead associated with the "Account" component device.

To enable the "AWS CloudWatch Alarms Performance" Dynamic Application:

1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).

 Locate the "AWS CloudWatch Alarms Performance" Dynamic Application and then click its wrench icon (*P*). The Dynamic Applications Properties Editor page appears.

Close	<u>P</u> roperties	<u>C</u> ollections	Presentations	<u>S</u> nippets	Thresholds	Alerts	Subscribers
Dynamic Applicati	ons [1438] Properti	es Editor					Guide Reset
AWS Cloud [Snippet Pr [No cachir None	Application Name Watch Alarms Perform Application Type arformance] Caching 19] Device Dashboard	nance d	Version Numb [[Version 1.0] Operational St Enabled Poll Frequent [[Every 1 Minute]	er • • • • • • • • • • • • • • • • • • •	Abando [Default] C [values] Null Co [values]	n Collection	Disable Rollup of Data Component Mapping Save Save As
Description This dynamic ap	plication monitors ,	Amazon Web Servic	e Cloudwatch Alarms	s performance inf	ormation.		
Release Notes & C	hange Log						
🖹 - 🎽 B	। <u> </u>	A - TI- 6	• ¶ • ≫• ≣		≡ ;≡ ⊞	• % 🖬 🗷	
Version 1.0: 1. Initial Ver Copyright (c) This software Use of the So agreement, v ("License Agi that is accom- first agrees to	sion 2003-2018 Scie : is the copyright oftware is govern /hich accompani reement"). An en panied by or inc o the License Ag	nceLogic, Inc. ed work of Scienc ed by the terms c es or is included \ d user is not perm ludes a License A reement terms.	eLogic, Inc. If the software licer with the Software nitted to install any greement, unless	nse r Software he or she			

- 3. In the **Operational State** field, select Enabled.
- 4. Click [Save].

By default, the "AWS CloudWatch Alarms Performance" Dynamic Application monitors only the "StateUpdate" type of CloudWatch alarms. If you want the Dynamic Application to also monitor "Action" and "ConfigurationUpdate" alarm types, you must configure the Dynamic Application to do so.

To configure the "AWS CloudWatch Alarms Performance" Dynamic Application to monitor all CloudWatch alarm types:

- 1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
- 2. Locate the "AWS CloudWatch Alarms Performance" Dynamic Application and then click its wrench icon (*P*). The **Dynamic Applications Properties Editor** page appears.
- 3. Click the [Collections] tab. The Collection Objects page appears.

4. On the **Collection Objects** page, locate the "CloudWatch Alarms Collection Success" collection object and then click its wrench icon (*P*).

Close P	roperties	<u>C</u> ollections	Presentations	<u>S</u> nippets]	[hresholds	<u>A</u> lerts		Subscrib	ers	
Dynamic Applications [1429] Collection Ob	jects								Guide	Reset
Object Name Snippet Arguments Class Type Snippet Group / Usage Type Enable Deviation Alerting:	CloudWatch Alar alarms_succes [4 Performance. [cloudwatch_al [No Group] max weeks	ms Collection Succe s Gaunel arms_performance } ▼ [[5 s data: [0] min	Standard] weeks data:	* * *	Indic histo encou espec be mc (<u>Conf</u> <u>cloue</u> <u>State</u> cloue	ates the succe ry collection inters an unexy isly importan intored. 1 igurationUpdat watch alarms p watch alarms p	Dess ss (1) or failur snippet. Failure ected error. Nu for determinir. . To collect all . <u>StateUpdats</u> , erformance. 2 ypes, select the erformance Stats For	cription re (0) (0) DTE: 1 DTE: 1 Action Action Action Action Close Action A) of the g occurs in This coll. ich <u>Cloud</u> udWatch a on), sele collect oppet te only.	<u>CloudWatch</u> alarms f the snippet section object is witch alarms are larm types t the snippet only <u>CloudWatch</u>	to
				Save Sav	re As]			Disable C	bject Maintenance	
Collection Object Registr	y Obj	ect Name		Class	Cla	ss Snippe	t Arguments	Group	D ID	Edit Date	
PCloudWatch Action PCloudWatch Action PCloudWatch Action PCloudWatch Alarms PCloudWatch Alarms PCloudWatch Alarms PCloudWatch StateU PCloudWatch StateU PCloudWatch StateU PCloudWatch StateU PCloudWatch StateU	(Failed) Alarms Alarms is Collection Suc arationOpdate Ala Jarms pdate (ALARM) A pdate (INSUFFIC Adate (OK) Alarm larms	irms Jams IENT_DATA) Alarms IS	8	Performance Ga Performance Ga Performance G Performance Ga Performance Ga Performance Ga Performance Ga Performance Ga	uge 4 uge 4 auge 4 uge 4 uge 4 uge 4 uge 4 uge 4 uge 4 uge 4	action_type_cc action_type_cc total_alarm_cc alarms_succc config_type_cc state_type_co state_type_co state_alarm_type state_insufficie state_ok_type aggregate_ala	type_count unt unt sss sunt unt inf_info_type_count rm_count		o_16663 o_16663 o_16667 o_16664 o_16665 o_16665 o_16660 o_16661 o_16662 o_16668	2018-04-19 13:55: 2018-04-19 13:55: 2018-04-19 13:55: 2018-04-19 13:55: 2018-04-19 13:55: 2018-04-19 13:55: 2018-04-19 13:55: 2018-04-19 13:55: 2018-04-19 13:55:	166 1 166 1 173 1 166 1 166 1 166 1 166 1 166 1 166 1 166 1 166 1 166 1 166 1 166 1 166 1
						[Select Ad	tion]			•	Go

5. In the **Snippet** field, select cloudwatch alarms performance.

NOTE: If you want to revert back to monitoring only the "StateUpdate" CloudWatch alarms, then select cloudwatch_alarms_performance_StateUpdate_only in the **Snippet** field.

6. Click [Save].

Enabling CloudWatch Alarm Events in the ScienceLogic Platform

The Amazon Web Services PowerPack also includes several pre-defined event policies for CloudWatch alarms. These Event Policies must be enabled if you want the platform to generate CloudWatch alarm events.

To enable the CloudWatch alarms Event Policies:

1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager).

2. In the *Event Policy Name* filter-while-you-type field, type "CloudWatch".

											Create	Reset	Guid
Event Policy Name •	Type	State	P-Pack	Severity	Weight		Expiry	Time	Thresh	Edited By	Last Edited	External ID	Ext. Categor
Advarding Share Strength Strengt Strength Strength Strength Strength Strength Streng	API	Enabled	Yes	Major	0	4234	90 Min.	0 Min.	0	em7admin	2018-04-17 09:56:26		
A SAWS: CloudWatchAlarm Action InProgress	API	Enabled	Yes	Notice	0	4236	30 Min.	0 Min.	0	em7admin	2018-04-17 09:56:26		
AWS: CloudWatchAlarm_Action_Succeeded	API	Enabled	Yes	Notice	0	4233	30 Min.	0 Min.	0	em7admin	2018-04-17 09:56:26		
AWS: CloudWatchAlarm_ConfigurationUpdate	API	Enabled	Yes	Notice	0	4235	30 Min.	0 Min.	0	em7admin	2018-04-17 09:56:26		
AWS: CloudWatchAlarm_StateUpdate_Alarm	API	Enabled	Yes	Major	0	4230	90 Min.	0 Min.	0	em7admin	2018-04-17 09:56:26		
AWS: CloudWatchAlarm_StateUpdate_InsufficientData	API	Enabled	Yes	Notice	0	4231	30 Min.	0 Min.	0	em7admin	2018-04-17 09:56:27		
AWS: CloudWatchAlarm_StateUpdate_OK	API	Enabled	Yes	Healthy	0	4232	15 Min.	0 Min.	0	em7admin	2018-04-17 09:56:27		

- 3. Select the check boxes for the events you want to enable.
- 4. In the **Select Action** drop-down field, select ENABLE these Event Policies.
- 5. Click **[Go]**.

Chapter

AWS Reports

Overview

The following sections describe the reports that are included in the Amazon Web Services PowerPack:

AWS Billing Report	50
AWS Inventory Report	52
AWS Running Config Report	54

AWS Billing Report

This report displays service costs for Amazon Web Services. The report includes Total, Monthly, Quarterly, and Annual costs.

i. Science	Logic	
WS Billing Report – Total S	Service Costs	
port Start Date: 2014/04		
ort Duration: To present		
ning data may be inaccorate due to missed poils.		
Accoun	t: (none)	
Service	# Instances	Total Cost
	0	\$0.00
Total for Account: (none)	0	\$0.00
Account: AIDAJ5CRUC	DWAW7CRUTMS [14	4115]
Service	# Instances	Total Cost
sqs	2	\$0.00
EC2	72	\$0.00
SNS	15	\$0.00
Total for Account: AIDAJ5CRUCDWAW7	89	\$0.00
Overall Tatala	89	\$0.00

Science	Logic						Monthly Cos	8					
						Account: (none)							
Region	Service	Apr 2014	May 2014	Jun 2014	Jul 2014	Aug 2014	Sep 2014	Oct 2014	Nov 2014	Dec 2014	Jan 2015	Feb 2015	Mar 2015
		\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	90.00	\$0.00	\$0.00	\$0.00
Total for Account: (none)		\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
					Account: Al	DAJ5CRUCDWAW7C	RUTMS [14115]						
Region	Service	Apr 2014	May 2014	Jun 2014	Jul 2014	Aug 2014	Sep 2014	Oct 2014	Nov 2014	Dec 2014	Jan 2015	Feb 2015	Mar 2015
Frankfurt: eu-central-1 [14444]	sqs	\$0.00	\$0.00	\$0.00	\$0.00	90.00	\$0.00	\$0.00	\$0.00	50.00	\$0.00	\$0.00	\$0.00
Frankfurt: eu-central-1 [14444]	EC2	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
	SNS	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	90.00	\$0.00	\$0.00	\$0.00
Total for Account: AIDAJ5CRUCDWAW	7CRUTMS [14115]	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Overall Totals:		\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
					Gene	rated on: 2015/04/17	07:46:56						

....ScienceLogic

AWS Billing Report – Quarterly Costs

Account: (none)										
Region	Service	Q2 2014	Q3 2014	Q4 2014	Q1 2015					
		\$0.00	\$0.00	\$0.00	\$0.00					
Total for Account: (none)		\$0.00	\$0.00	\$0.00	\$0.00					
Account: AIDAJ5CRUCDWAW7CRUTMS [14115]										
Region	Service	Q2 2014	Q3 2014	Q4 2014	Q1 2015					
Frankfurt: eu-central-1 [14444]	SQS	\$0.00	\$0.00	\$0.00	\$0.00					
Frankfurt: eu-central-1 [14444]	EC2	\$0.00	\$0.00 \$0.00 \$0.00		\$0.00					
	SNS	\$0.00	\$0.00	\$0.00	\$0.00					
Total for Account: AIDAJ5CRUCDWAW	7CRUTMS [14115]	\$0.00	\$0.00	\$0.00	\$0.00					
Overall Totals:		\$0.00	\$0.00	\$0.00	\$0.00					
	Gene	rated on: 2015/04/17 (07:46:56							

....ScienceLogic

AWS Billing Report – Annual Costs

Account: (none)									
Region	Service	2014	2015						
		\$0.00	\$0.00						
Total for Account: (none)	\$0.00	\$0.00							
Account	RUTMS [14115]								
Region	Service	2014	2015						
Frankfurt: eu-central-1 [14444]	\$0.00	\$0.00							
Frankfurt: eu-central-1 [14444]	EC2	\$0.00	\$0.00						
	SNS	\$0.00	\$0.00						
Total for Account: AIDAJ5CRUCDWAW	7CRUTMS [14115]	\$0.00	\$0.00						
	\$0.00	\$0.00							

AWS Billing Report - Control								
Description:	AWS Billing							
Report Version:	1.1							
Generated On:	2015/04/17 07:46:56							
AWS Accounts:	All							
Start Date:	2014/04							
Duration:	To present							
Generated on: 2015/04/17 07:46:56								

The following input options are available when generating the report:

- AWS Accounts. Select the AWS Account(s) for which you want to generate the report. The All Accounts checkbox is selected by default. De-selecting this checkbox allows you to select one or more specific accounts for which to generate a report.
- **Report Span**. Select a span from one to 36 months for the report, or specify a specific starting date for the report.

This description covers the latest version of this report as shipped by ScienceLogic. This report might have been modified on your ScienceLogic system.

AWS Inventory Report

This report displays an inventory of AWS instance counts. The report includes the number of each kind of instance in every zone associated with the chosen accounts. It also includes a count of each EC2 instance size in each zone.

....ScienceLogic

AWS Inventory	Report -	Instance	Counts
Aws inventory	Report -	mstance	Counts

						Organizat	tion: Pitte	ck [193]									
					Account	: AIDAJ5CR	UCDWAY	V7CRUTMS	14115]								
7	Clasics	Laurah Car		Mich Diet	L	evel1: Cloud	Front Se	rvice [14120	CNIC	500	000	2 Uselik Ch	C United To	60	605	500	1/00
Zone	Glacier	Launch Con	AS Group	Web Dist	sudFront Or	i Cloud I rail	ELB	Subnet	SNS	EC2	RDS	3 Health Ch	63 Hosted Zo	53	sqs	EBS	VPC
11210K6q0(264.cl0001r0nt.net [14150]	U	U	0	1	1	U	U	U	U	U	0	0	U	0	U	U	U
Totals for Level1: CloudFront Service [14120]	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0
					Lev	el1: Frankfu	irt: eu-ce	ntral-1 [1444	4]								
Zone	Glacier	Launch Con	AS Group	Web Dist	audFront Or	i CloudTrail	ELB	Subnet	SNS	EC2	RDS	3 Health Ch	63 Hosted Zo	S3	SQS	EBS	VPC
u-central-1 Glacier Service [14467]	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
eu-central-1 VPC Service [14447]	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	1
eu-central-1a [14446]	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
Totals for Level1: Frankfurt: eu-central-1 [14444]	1	0	0	0	0	0	0	2	0	1	0	0	0	0	0	1	1
[]					L	evel1: Irelar	nd: eu-we	st-1 [14117]									
Zone	Glacier	Launch Con	AS Group	Web Dist	audFront Or	i CloudTrail	ELB	Subnet	SNS	EC2	RDS	3 Health Ch	43 Hosted Zo	S 3	SQS	EBS	VPC
eu-west-1 Glacier Service [14129]	1	0	0	0	0	0	0	0	0	0	0	0	0	1	Ő	8	0
u-west-1 CloudTrail Service [14346]	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
eu-west-1 ELB Service [14124]	0	0	0	0	0	0	1	0	0	7	0	0	0	0	0	0	0
eu-west-1 SNS Service [14123]	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
eu-west-1 VPC Service [14130]	0	0	0	0	0	0	0	9	0	0	0	0	0	0	0	0	2
Totals for Level1: Ireland: eu-west-1 [14117]	1	0	0	0	0	1	1	9	1	7	0	0	0	1	0	8	2
					Le	vel1: N. Virg	inia: us-	ast-1 [14118]								
Zone	Glacier	Launch Con	AS Group	Web Dist	oudFront Or	i CloudTrail	ELB	Subnet	SNS	EC2	RDS	3 Health Ch	63 Hosted Zo	S3	SQS	EBS	VPC
is-east-1 Auto Scale Service [14138]	0	2	1	0	0	0	2	0	0	38	0	0	0	0	0	0	0
is-east-1 CloudTrail Service [14139]	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
is-east-1b [14133]	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0
is-standard S3 Service [14137]	0	0	0	0	0	0	0	0	0	0	0	0	0	5	0	41	0
is-east-1 SQS Service [14340]	0	0	0	0	0	0	0	0	8	0	0	0	0	0	1	0	0
us-east-1 VPC Service [14141]	0	0	0	0	0	0	0	8	0	0	0	0	0	0	0	0	6
Totals for Level1: N. Virginia: us-east-1 [14118]	0	2	1	0	0	1	2	8	8	38	3	0	0	5	1	41	6
					L	evel1: Orego	on: us-w	st-2 [14119]									
Zone	Glacier	Launch Con	AS Group	Web Dist	oudFront Or	i CloudTrail	ELB	Subnet	SNS	EC2	RDS	3 Health Ch	63 Hosted Zo	S3	sqs	EBS	VPC
Is-west-2 Auto Scale Service [14147]	0	1	1	0	0	0	0	0	0	9	0	0	0	0	0	0	0
JS-West-2 Cloud Frail Service [14148]	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
JS-West-2 S3 Service [14146]	0	0	0	0	0	0	0	0		0	0	0	0	3	0	6	
IS-West-2 SQS Service [14336]	0	0	0	0	0	0	0	0	4		0		8	8	1	0	1
Is-west-2 VPC Service [14149]	0	0		0	0		0	3	0	0	0	0	0	0	0	0	1
Totals for Level1: Oregon: us-west-2 [14119]	0	1	1	U	0	Level1: Rout	e 53 Sen	3 /ice [14116]	4	9	U	U	U	3	1	0	1
Zone	Glacier	Launch Con	AS Group	Web Dist	JudFront Or	i CloudTrail	ELB	Subnet	SNS	EC2	RDS	3 Health Ch	63 Hosted Zo	S 3	SQS	EBS	VPC
napmycloud.net [14121]	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0
Totals for Level1: Route 53 Service [14116]	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0
Totals for Account:	2	3	2	1	1	3	3	22	13	55	3	1	1	9	2	56	10
Totals for Organization: Dittock [193]	2	3	2	1	1	3	3	22	13	55	3	1	1	9	2	56	10
Charal Totalo	2	3	2	1	1	3	3	22	13	55	3	1	1		2	56	10
		3		1	-							-			4		10

Organizat								
Organizat								
	tion: Pittocl	k [193]						
nt: AIDAJ5CR	UCDWAW7	CRUTMS [1	4115]					
vel1: Frankfu	irt: eu-cent	ral-1 [14444]					
M1.small	M3.large	T1.micro	T2.small	T2.micro	C3.large	M3.xlarge	M3.medium	M1.medium
0	0	0	0	1	0	0	0	0
0	0	0	0	1	0	0	0	0
Level1: Irelar	na: eu-west	-1 [14117]						
MLSmall	M3.large	11_micro	12.small	12.micro	C3.large	M3.xtarge	M3.medium	M1.medium
0	0	2	0	0	0	0	0	0
0	0	2	8	8	0	0	8	0
0	1	2	0	0	0	0	0	0
evel1: N. Vire	inia: ue.ea	et-1 [1/119]			v			v
M1 small	M3 Jarne	T1 micro	T2 small	T2 micro	C3 large	M3 viarge	M3 medium	M1 medium
4	4	3	11	1	0	0	0	0
ó	Ó	õ	0	3	ō	1	ō	ō
1	ō	4	ō	ō	ō	ō	ō	1
2	ō	2	ō	ō	1	ō	ō	ō
7	4	9	11	4	1	1	0	1
Level1: Orego	on: us-west	-2 [14119]						
M1.small	M3.large	T1.micro	T2.small	T2.micro	C3.large	M3.xlarge	M3.medium	M1.medium
0	0	4	0	0	0	0	1	0
0	0	3	0	0	0	0	0	0
0	0	0	0	0	0	0	1	0
0	0	7	0	0	0	0	2	0
7	5	22	11	5	1	1	2	1
7	5	22	11	5	1	1	2	1
7	5	22	11	5	1	1	2	1
	terit: Frankt, Mt.small 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Velt. Frankfurf. success MLsmall MLlarge 0 0 0 0 Levell: Ireland MLsmall MLlarge 0 0 0 1 0 0 evel1: Nelarge MLsmall MLlarge MLsmall Nelarge 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 <td< td=""><td>Vell: Frankfurf: Eucentral: [1.44x] HLamal Milarge TLmicro MLamal Milarge TLmicro 0 0 0 0 Leveli: Ireland: Eulerski [1.4117] MLamal Milarge TLmicro 0 0 2 0 0 2 0 2 <t< td=""><td>Volt. Frankfurt: suc-central: I [1444] ML.small Marge Tumbor T2.moil ML.small Marge Tumbor T2.moil Leveli: treland: su-west-1 [14117] MLsmall MLsmall MLsmall ML.small Malarge Tumbor T2.moil 0 0 0 0 0 0 1 2 0 0 0 2 0 0 0 2 0 0 0 2 0 0 0 2 0 0 0 2 0 0 0 2 0 0 0 2 0 11 0 4 0 11 0 4 0 1 0 4 0 1 0 4 0 1 0 4 0 0 0 4 0 0<!--</td--><td>Will: Frankfurt: esi-central-I [J4449] '''' MLamal MJarge TLamiro TZ_micro 0 0 0 10 1 0 0 0 0 1 Leveli: treland: eu-west-1 [J4117] Ittic Ittic Ittic MLamal MSlarge TLintro TZ_micro 0 0 1 0 0 2 0</td><td>Mill Frankfurt esc-entraid [J.444] Milamal Milarge Til.com T2.smail T2.micro C3.large Milamal Milarge Til.com T2.smail T2.micro C3.large 0 0 0 0 1 0 0 0 0 1 0 Leveli: Ireland: Eurore T2.micro C3.large 0 1 2 0 0 0 0 0 1 2 0<!--</td--><td>Mill Frankhrit eur-entryis / J (2444) Tarmetro Callarge Tarmetro Callarge Mill and Mill and Mill ange Till control Tarmetro Callarge Mill ange Mill and Mill ange Till control Tarmetro Callarge Mill ange Mill and Mill ange Till control Tarmetro Callarge Mill ange Mill and Mill ange Till contro Tarmetro Callarge Mill ange Mill and Mill ange Till contro Tarmetro Callarge Mill ange 0 0 2 0 0 0 0 0 1 2 0 0 0 0 0 0 2 0 0 0 0 0 1 1 1 1 1 1 Mill ange 1 1 1 1 1 1 1 0 4 0 0 0 0 0 <td>Mill Argani Mill Alarge Timero Timero Timero Callarge Mill Amedium Mill Amail Millarge Timero Timero O 0</td></td></td></td></t<></td></td<>	Vell: Frankfurf: Eucentral: [1.44x] HLamal Milarge TLmicro MLamal Milarge TLmicro 0 0 0 0 Leveli: Ireland: Eulerski [1.4117] MLamal Milarge TLmicro 0 0 2 0 0 2 0 2 <t< td=""><td>Volt. Frankfurt: suc-central: I [1444] ML.small Marge Tumbor T2.moil ML.small Marge Tumbor T2.moil Leveli: treland: su-west-1 [14117] MLsmall MLsmall MLsmall ML.small Malarge Tumbor T2.moil 0 0 0 0 0 0 1 2 0 0 0 2 0 0 0 2 0 0 0 2 0 0 0 2 0 0 0 2 0 0 0 2 0 0 0 2 0 11 0 4 0 11 0 4 0 1 0 4 0 1 0 4 0 1 0 4 0 0 0 4 0 0<!--</td--><td>Will: Frankfurt: esi-central-I [J4449] '''' MLamal MJarge TLamiro TZ_micro 0 0 0 10 1 0 0 0 0 1 Leveli: treland: eu-west-1 [J4117] Ittic Ittic Ittic MLamal MSlarge TLintro TZ_micro 0 0 1 0 0 2 0</td><td>Mill Frankfurt esc-entraid [J.444] Milamal Milarge Til.com T2.smail T2.micro C3.large Milamal Milarge Til.com T2.smail T2.micro C3.large 0 0 0 0 1 0 0 0 0 1 0 Leveli: Ireland: Eurore T2.micro C3.large 0 1 2 0 0 0 0 0 1 2 0<!--</td--><td>Mill Frankhrit eur-entryis / J (2444) Tarmetro Callarge Tarmetro Callarge Mill and Mill and Mill ange Till control Tarmetro Callarge Mill ange Mill and Mill ange Till control Tarmetro Callarge Mill ange Mill and Mill ange Till control Tarmetro Callarge Mill ange Mill and Mill ange Till contro Tarmetro Callarge Mill ange Mill and Mill ange Till contro Tarmetro Callarge Mill ange 0 0 2 0 0 0 0 0 1 2 0 0 0 0 0 0 2 0 0 0 0 0 1 1 1 1 1 1 Mill ange 1 1 1 1 1 1 1 0 4 0 0 0 0 0 <td>Mill Argani Mill Alarge Timero Timero Timero Callarge Mill Amedium Mill Amail Millarge Timero Timero O 0</td></td></td></td></t<>	Volt. Frankfurt: suc-central: I [1444] ML.small Marge Tumbor T2.moil ML.small Marge Tumbor T2.moil Leveli: treland: su-west-1 [14117] MLsmall MLsmall MLsmall ML.small Malarge Tumbor T2.moil 0 0 0 0 0 0 1 2 0 0 0 2 0 0 0 2 0 0 0 2 0 0 0 2 0 0 0 2 0 0 0 2 0 0 0 2 0 11 0 4 0 11 0 4 0 1 0 4 0 1 0 4 0 1 0 4 0 0 0 4 0 0 </td <td>Will: Frankfurt: esi-central-I [J4449] '''' MLamal MJarge TLamiro TZ_micro 0 0 0 10 1 0 0 0 0 1 Leveli: treland: eu-west-1 [J4117] Ittic Ittic Ittic MLamal MSlarge TLintro TZ_micro 0 0 1 0 0 2 0</td> <td>Mill Frankfurt esc-entraid [J.444] Milamal Milarge Til.com T2.smail T2.micro C3.large Milamal Milarge Til.com T2.smail T2.micro C3.large 0 0 0 0 1 0 0 0 0 1 0 Leveli: Ireland: Eurore T2.micro C3.large 0 1 2 0 0 0 0 0 1 2 0<!--</td--><td>Mill Frankhrit eur-entryis / J (2444) Tarmetro Callarge Tarmetro Callarge Mill and Mill and Mill ange Till control Tarmetro Callarge Mill ange Mill and Mill ange Till control Tarmetro Callarge Mill ange Mill and Mill ange Till control Tarmetro Callarge Mill ange Mill and Mill ange Till contro Tarmetro Callarge Mill ange Mill and Mill ange Till contro Tarmetro Callarge Mill ange 0 0 2 0 0 0 0 0 1 2 0 0 0 0 0 0 2 0 0 0 0 0 1 1 1 1 1 1 Mill ange 1 1 1 1 1 1 1 0 4 0 0 0 0 0 <td>Mill Argani Mill Alarge Timero Timero Timero Callarge Mill Amedium Mill Amail Millarge Timero Timero O 0</td></td></td>	Will: Frankfurt: esi-central-I [J4449] '''' MLamal MJarge TLamiro TZ_micro 0 0 0 10 1 0 0 0 0 1 Leveli: treland: eu-west-1 [J4117] Ittic Ittic Ittic MLamal MSlarge TLintro TZ_micro 0 0 1 0 0 2 0	Mill Frankfurt esc-entraid [J.444] Milamal Milarge Til.com T2.smail T2.micro C3.large Milamal Milarge Til.com T2.smail T2.micro C3.large 0 0 0 0 1 0 0 0 0 1 0 Leveli: Ireland: Eurore T2.micro C3.large 0 1 2 0 0 0 0 0 1 2 0 </td <td>Mill Frankhrit eur-entryis / J (2444) Tarmetro Callarge Tarmetro Callarge Mill and Mill and Mill ange Till control Tarmetro Callarge Mill ange Mill and Mill ange Till control Tarmetro Callarge Mill ange Mill and Mill ange Till control Tarmetro Callarge Mill ange Mill and Mill ange Till contro Tarmetro Callarge Mill ange Mill and Mill ange Till contro Tarmetro Callarge Mill ange 0 0 2 0 0 0 0 0 1 2 0 0 0 0 0 0 2 0 0 0 0 0 1 1 1 1 1 1 Mill ange 1 1 1 1 1 1 1 0 4 0 0 0 0 0 <td>Mill Argani Mill Alarge Timero Timero Timero Callarge Mill Amedium Mill Amail Millarge Timero Timero O 0</td></td>	Mill Frankhrit eur-entryis / J (2444) Tarmetro Callarge Tarmetro Callarge Mill and Mill and Mill ange Till control Tarmetro Callarge Mill ange Mill and Mill ange Till control Tarmetro Callarge Mill ange Mill and Mill ange Till control Tarmetro Callarge Mill ange Mill and Mill ange Till contro Tarmetro Callarge Mill ange Mill and Mill ange Till contro Tarmetro Callarge Mill ange 0 0 2 0 0 0 0 0 1 2 0 0 0 0 0 0 2 0 0 0 0 0 1 1 1 1 1 1 Mill ange 1 1 1 1 1 1 1 0 4 0 0 0 0 0 <td>Mill Argani Mill Alarge Timero Timero Timero Callarge Mill Amedium Mill Amail Millarge Timero Timero O 0</td>	Mill Argani Mill Alarge Timero Timero Timero Callarge Mill Amedium Mill Amail Millarge Timero Timero O 0

The following input options are available when generating the report:

• **Organizations**. Select the organization for which you want to generate the report. The All Organizations checkbox is selected by default. De-selecting this checkbox allows you to select one or more specific organizations for which to generate a report.

- AWS Accounts. Select the AWS Account(s) for which you want to generate the report. The All Accounts checkbox is selected by default. De-selecting this checkbox allows you to select one or more specific accounts for which to generate a report.
- *Filter on EC2 Instance Config Data*. Select the EC2 instances that will be included in the report based on the configuration data reported for each EC2 instance:
 - Choose up to four configuration parameters for EC2 instances.
 - For each selected configuration parameter, enter a value to match against and select how that value should be matched.
 - In the **Comparison Operator** field, select whether an EC2 instance must match all configuration parameters (*and*) or only one configuration parameter (or) to be included on the report.
- **Report Options**. Select the Include Terminated Instances checkbox to include all terminated instances.

This description covers the latest version of this report as shipped by ScienceLogic. This report might have been modified on your ScienceLogic system.

AWS Running Config Report

This report displays the running config of all AWS instances for one to all organizations across a number of AWS billing accounts.

	Awa Kuming Comg
Junociencelogic	
0	
AWS Running Config Report	
AIDAJ5CRU	CDWAW7CRUTMS [14115]
Clo	udFront Service [14120]
d12tib	k6qbt264.cloudfront.net [14150]
Key	/ Value *** AWS CloudFront Origin Discovery ***
Distinguished Name:	am:avs:cloudfront::789135808643:distribution/E1KPRUBCK0YU3E
Exists:	1
ld:	cloudiront E1KPRUBCK0YU3E/silocloudtrail.s3.amazonaws.com
***** Application *****	*** AWS CloudFront Web Distribution ***
Trusted Signers:	
ld:	doudfront E1KPRUBCK0YU3E
State:	True am see doubteet - 700125000642-detrautionE1K/DDI IBCX (V/I I2E
Comment	antara.countent.res155000/45.05000004E1KFRUBUKUTUSE
Delivery Method:	Web
Price Class:	Not Available
Name:	d12bbk6qbt264.cloudfront.net
Chames:	2014/09/18/103:23:03:7772
Status:	Deployed
***** Application *****	*** AWS CloudFront Restriction Discovery ***
Exists:	1 Mar All C. Claud Event Event Directory att
Application ***** Application *****	AWS Goud-ront Error Hage Discovery ***
***** Application *****	*** AWS CloudFront Behavior Discovery ***
Exists:	1

The following input options are available when generating the report:

- Organizations. Select one, multiple, or all organizations to include in the report.
 - All Organizations. This checkbox is selected by default. De-selecting this checkbox allows you to select one or more specific organizations for the report.
 - Organizations. If you unchecked the **All Organizations** checkbox, select one or more organizations to include in the report.
- AWS Accounts. Select one, multiple, or all AWS Accounts to include in the report.
 - All Accounts. This checkbox is selected by default. De-selecting this checkbox allows you to select one or more specific AWS accounts for the report.
 - Accounts. If you unchecked the **All Accounts** checkbox, select one or more AWS Accounts to include in the report.
- *Filter on EC2 Instance Config Data*. Select the EC2 instances that will be included on the report based on the configuration data reported for each EC2 instance:
 - Choose up to four configuration parameters for EC2 instances.
 - For each selected configuration parameter, enter a value to match against and select how that value should be matched.
 - In the **Comparison Operator** field, select whether an EC2 instance must match all configuration parameters (*and*) or only one configuration parameter (or) to be included in the report.
- **Report Options**. Select the Include Terminated Instances checkbox to include all terminated instances.

This description covers the latest version of this report as shipped by ScienceLogic. This report might have been modified on your ScienceLogic system.

Chapter

AWS Dashboards

Overview

The following sections describe how to install the Amazon Web Services: Dashboards PowerPack and a description of each dashboard that is included in the PowerPack:

Installing the Amazon Web Services: Dashboards PowerPack	56
AWS Account Billing Dashboard	.58
AWS Health Status Dashboard	59
AWS Service Instance Performance Dashboards	

Installing the Amazon Web Services: Dashboards PowerPack

To view the Amazon Web Services dashboards in the ScienceLogic platform, you must first install the Amazon Web Services: Dashboards PowerPack.

NOTE: The AWS dashboards have a default **Access Control** setting of "Private", which means they can be viewed only by an administrator. For more information about dashboard access settings, see the **Dashboards** manual.

To install the PowerPack:

- 1. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
- 2. Click the [Actions] button, then select Install PowerPack. The Imported PowerPacks modal page appears.

 Use the search filter in the PowerPack Name column heading to locate the PowerPack you want to install. To do so, enter text to match, including special characters, and the Imported PowerPacks modal page displays only PowerPacks that have a matching name.

Power	Pack Installer			
Imp	orted PowerPacks™ PowerPack	Files F	ound	[298] Reset
			Revisio	
1	PowerPack Name	Version	<u>n</u>	GUID Last Edited Imported •
1.	Event Association Test	1	1	DED1884762194566B70BCD4DF3A742 2015-12-16 09:43:07 2015-12-16 09:43:0()
2	Event Suppression Test	1	1	EC64565DCA55E155135F91F81F44D8-2015-12-09 07:44:172015-12-09 07:44:12 //
3.	SLPSD: Onboarding	0.20000	287	E121312B60972ED35BEDA19E88D195 2015-11-12 12:14:05 2015-11-12 12:13:50 🖌 📃
4.	SL_PS Cisco 3rd Party Device Support	1.39999	151	8B78EDB3A373B2D187ECEAE2545744 2015-11-05 12:17:39 2015-11-05 12:16:54 🖉 📃
5.	NetApp Base Pack	7.7.0	6873	8014D5DAD2B8C9AC3E1DD84CC227E 2015-10-21 13:31:47 2015-10-29 14:56:55 🏏 📃
6.	Cisco: Contact Center Enterprise *BETA*	0.5	1119	7CC6AD933EFB4FF5D840EFEA40F85C 2015-12-14 13:50:5(2015-10-29 14:56:54 🖋 🗌
7.	EM7 Standard Device Categories	7.7.0	255	7A7322AA30F189B42943C082EFD7121 2015-06-02 18:30:5€ 2015-10-29 14:56:54 🏏 🧾
8.	BL Test	1	2	74F7E816CF0FC9153700D2AF0982C2; 2015-10-29 10:56:112015-10-29 10:56:06 🖋 🗌
9.	BL Test	1	1	74F7E816CF0FC9153700D2AF0982C2 2015-10-29 10:56:112015-10-29 10:54:15 🏏 🧾
10.	Microsoft: Office 365 *BETA*	0.5	138	8FA30F7D1FAC9162DD8C717D9EF778 2015-10-20 16:44:37 🖋 📃
11.	NetApp Base Pack	7.7.0	6838	8014D5DAD2B8C9AC3E1DD84CC227E 2015-10-21 13:31:47 2015-10-20 16:44:37 🏏 🧾
12	Cisco: Contact Center Enterprise *BETA*	0.5	1109	7CC6AD933EFB4FF5D840EFEA40F85C 2015-12-14 13:50:50 2015-10-20 16:44:30 🖋 🔲
13.	EM7 Default Internal Events	7.7.0	316	BE1F363DB4BA9A10F5C6BC28931F0B 2015-10-28 13:26:25 2015-10-20 16:44:36 🖋 🧾
14.	F5 BIG-IP *BETA*	7.7.0	3242	BFA4E6B316FD2302D913EF38FE7FF822015-10-2813:26:272015-10-2016:44:30 🥖 🔲
15.	Microsoft: Office 365 *BETA*	0.5	136	8FA30F7D1FAC9162DD8C717D9EF778 2015-10-14 15:12:24 🖋 厂
16.	Cisco: Contact Center Enterprise *BETA*	0.5	1022	7CC6AD933EFB4FF5D840EFEA40F85C 2015-12-14 13:50:5C 2015-10-14 15:12:2: 🥖 🔲
17.	Microsoft Base Pack	7.7.0	868	97469E96E98B5DAB516F3CCC8747CE 2015-10-28 13:26:26 2015-10-13 12:47:54 🖋 🗾
18.	EM7 Default Internal Events	7.7.0	315	BE1F363DB4BA9A10F5C6BC28931F0B 2015-10-28 13:26:25 2015-10-13 12:47:54 🖋 🥅
19.	NetApp Base Pack	7.7.0	6792	8014D5DAD2B8C9AC3E1DD84CC227E 2015-10-21 13:31:47 2015-10-13 12:47:54 📝 🗐 🔤
	55 BIO ID			

- 4. Click the lightning-bolt icon (\checkmark) for the PowerPack that you want to install.
- 5. The Install PowerPack modal page appears. To install the PowerPack, click [Install].

Install Power-Pack™ .kate:	s_test_pp_3 Versi	ion 1				Reset
Package Information Created: 2015-07	GUID: 9F7ECF5CI 7-28 14:10:53	BC81D713AD94AF704FBA136C Updated: 2015-07-28 14:10:53	Revision: 2 Compi	Expor led: 201	ted From: 7.6.0.beta 15-07-28 14:12:21	
Package Content						
		Theme Name			GUID	Action
1. kates_test_theme_3	3			A6	D9EA56C5FAE1F35E6F0411BD79AD0	update
kates_test_theme_	4			AD	0A02B6763C3CCA014FBB00A9A21A64	update
Installation hBGC6W	n Key: /ETV3SH8Epeyp7	cpySyuEak0FeBpD/IYENPd0oBSc) Insta	KOJmVT4Z1ZfC)molbNF	RR/6MJw6aZOvgFY()	

6. The PowerPack now appears in the **PowerPack Manager** page. The contents of the PowerPack are automatically installed in your ScienceLogic system.

AWS Account Billing Dashboard

The AWS Account Billing Dashboard displays:

🕙 हस <mark>12H 24</mark> H मे	0	14D		300	90D	No Org	anizations Selected	ŝ	Aganizations Selector •		2 V
Estimated Billing (Last 12 hours)	• Total (\$) (La	ist 12 hours)									
Elestic MapReduce -											
Storage Galeway	479.75										
	479.68\$										
	479.66\$										
	479.64\$										
	479.625										
	479.65										
	07	00 08 [:] 00	0 09:00	10:00	11:00	12:00	13:00	14:00	15:00 16:00	17:00	18:00
AWS Events											•
Message •						Element		Severity	Last Detected		
WISNoBillingEvent: No billing metrics can be retrieved. Your AWS account is not configured to export billing metrics can be retrieved. Your AWS account is not configured to export billing metrics.	trics into Cloud	Watch.			1)143308194941 1)443629253563		Minor		27/10/2013 06:01:01 pm 27/10/2013 06:01:02 pm		
AWSNoBillingEvent: No billing metrics can be retrieved. Your AWS account is not configured to export billing me	trics into Cloud	Watch.			1233364061881		Minor		27/10/2013 06:01:00 pm		
Device Failed Availability Check: Your AWS account keys are invalid or your account does not have sufficient pri	tleges.				AWS test		Major		27/10/2013 06:25:10 pm		

- A pie chart that shows the estimated billing amount for each service over the selected time period.
- A performance graph that shows the estimated billing amount for the selected service, over time. To select a service, click on the pie-chart segment for that service.
- A table that shows the currently active AWS events.
- A time span selector that controls the amount of data shown in the pie chart and the performance graph.
- An organization selector that limits the data in the pie chart and performance graph to include only instances associated with the selected organizations.

AWS Health Status Dashboard

The AWS Health Status Dashboard displays:

No Organizations Selected	Organizations Selec	to: •	No Device G	oups Selected	Device Groups Sele	dar •			Ø					
AWS Services (all types)	 Selected Device Details 		 Selected Service Health 	· Selected Service Health										
eu-west-1a EC2 Service	^ DID	26688	Republic Restriction											
eu-west-1c EC2 Service	Device Name	Ameu-west-1a EC2 Service	2013-07-09 10:22:35 Service is operating normally. [RESOLVED] Increased API error rates											
sa-east-1 EMR Service	IP Address		2013-08-01 04:44:10	44:10 Informational message: Small number of instances unavailable in a single availability zone										
sa-east-1 SNS Service	Device Class Sub-class	AWS EC2 Service AWS EC2 Service	2013-08-01 05:23:51	Informational message: Small number	r of instances unavailable in a single :	availability zone								
sa-east-1 SQS Service	Organization	💕 Bosozoku Org	2013-08-01 05:49:30	Service is operating normally: Small n	umber of instances unavailable in a si	ingle availability zone								
sa-east-1a EC2 Service	Current State	Healthy	2013-08-09 07:21:54	Informational message: Network Con	nectivity									
sa-east-1a EC2 Service	Last Poll		2013-08-09 07:54:09	Service is operating normally: Network	Connectivity									
sa-east-1a EC2 Service	Group/Collector	CUG_20212	2013-08-09 10:43:35	Informational message: Network Con	nectivity									
us-east-1 DDB Service			2013-08-09 11:30:11	Informational message: Network Con	nectivity									
us-east-1 DDB Service			2013-08-09 12:23:55	Informational message: [RESOLVED]	Network Connectivity									
us-east-1 DDB Service			2013-08-16 11:11:58	Informational message: Increased Au	to Scaling Error Rates									
us-east-1 ELB Service			2013-08-16 11:25:48	Service is operating normally: [RESOL	VED] Increased Auto Scaling Error Ra	tes								
us-east-1 EMR Service			2013-09-21 17:52:46	Informational message: Increased La	unch Latencies and Error Rates									
us-east-1 SNS Service			2013-09-21 18:32:15	Service is operating normally. [RESOL	VED] Increased Launch Latencies and	d Error Rates								
us-east-1 SNS Service			2013-09-30 09:28:13	Informational message: [RESOLVED]	DNS Resolution Issues									
us-east-1 SNS Service			2013-10-24 09:05:37	Informational message: [RESOLVED]	Increased API Error Rates									
us-east-1 SNS Service														
us-east-1 SQS Service	1													
us-east-1 Storage Gateway Service														
us-east-1a EC2 Service	AWS Service-related EM7 E	vents: Last Detected (Last 12 hours)												
us-east-1a EC2 Service														
us-east-1a RDS Service		Managa •		Stganization	Element	Deverthy	Admoniedged	Ticket ID	Last Detected					
us-east-1b EC2 Service														
us-east-1b EC2 Service														
us-east-1b EC2 Service														
us-east-1b RDS Service				No results to display.										
us-east-1b RDS Service														
us-east-1c EC2 Service														
us-east-1c RDS Service														
us-east-1c RDS Service														
us-east-1d RDS Service														
us-west-1 ELB Service														
us-west-1 SNS Service														
us-west-1 SQS Service														
us-west-1a EC2 Service														
us-west-1a RDS Service														
us-west-1b EC2 Service														
us-west-1b RDS Service														
us-west-1c EC2 Service														
us-west-1c RDS Service	-													

- A traffic light widget that displays a list of AWS services. To populate the other widgets in this dashboard, select a service.
- A tear-sheet widget that displays information and links for the selected service.
- A service health widget, that displays log messages about the health of the service.
- A table that displays currently active events for the service.
- An organization selector and a device group selector that control which services are shown in the traffic light widget.

AWS Service Instance Performance Dashboards

The Amazon Web Services: Dashboards PowerPack includes a dashboard for each service type. Each dashboard displays performance metrics for instances of an AWS service. The following dashboards are included:

- AWS DDB Performance
- AWS EBS Performance
- AWS EC2 Performance
- AWS ELB Performance
- AWS EMR Performance
- AWS RDS Performance
- AWS SQS Performance
- AWS Storage Gateway Performance

Each performance dashboard includes:

SH 12H	241	70	14D 30D	900	No Organizations	Selected	Organizati	iona Selector •	V No De	vice Groups Selected	Device Groups Selector		<. 7
EC2 Instances	CPU	Utilization % (Last 12 hours)			0		Disk Ops I	Read & Write (Last 12 hours)					
eu-west-1a t1.micro: i-43464e0c													
eu-west-1c ScienceLogic-Proxy: t1.micro: i-3895						~							
sa-east-1a m1.small: i-815b139e	5%						0.05IOPS						
sa-east-1a m1.small: i-e1c5f3fe													
sa-east-1a m1.small: i-f95b13e6													
sa-east-1a SA-Samba - aether: t1.micro: i-b1d7c	**						0.025IOPS						
sa-east-1a SA-Samba - demeter: t1.micro: i-b86													
sa-east-1a SA-Samba - hemera: t1.micro: i-b767	3%												
sa-east-1a SA-Samba - hermes: t1.micro: i-bbd/=							0IOPS						
sa-east-1a SA-Samba - kronos: t1.micro: i-220s													
sa-east- la SA-Samba - nyx: t1.micro: 1-bod/d2a	2%												
sa-east-la SA-Samba - oceanus: t1 micro: 1-040							-0.03IOPS						
as east to SA Samba - themis: 11 micro: 1000	15												
sareast 1a SA-Samba - trentis, t1 micro, i-2 lob													
es.ast.1s Sciencel onic.Provu: 11 micro: i.5sft		~~~~~~	h		~~~~~)	-0.05IOPS						
sa east 1a Sciencel oric Provy: 11 micro: i-5c06	0%	08:00	10:00 12:00	14:00	16:00	18:00	1	00.00	10:00	12:00	14:00	16:00	18:00
aa-east-1a Sciencel ogic-Proxy: t1 micro: i-5f1dc		ſ											
a-east-1a ScienceLogic-Proxy: t1.micro: i-609d			 eu-west-1a t1.micro: i-43464e0c: 0 	CPU Utilization (%)				- eu-west-1a t1.mic	ro: i-43464e0c: Disk Rea	d Ops — eu-west-	1a t1.micro: i-43464e0	2 Disk Write Ops	
sa-east-1a ScienceLogic-Proxy: t1.micro: i-620#	Neta	ork In & Network Out (Last 12 hours)					Disk Rear	1.8 Write Butes (Last 12 hours)					
sa-east-1a ScienceLogic-Proxy: t1.micro: i-621a	-					-	0.0.0.000						
sa-east-1a ScienceLogic-Proxy: t1.micro: i-76f3e						_							
sa-east-1a ScienceLogic-Proxy: t1.micro: i-7da6	6048												
sa-east-1a ScienceLogic-Proxy: t1.micro: i-b6a8							50m8						
sa-east-1a ScienceLogic-Proxy: t1.micro: i-c467	5018					_							
sa-east-1a ScienceLogic-Proxy: t1.micro: i-c667													
sa-east-1a ScienceLogic-Proxy: t1.micro: i-e014	4018					-	25mB						
sa-east-1a ScienceLogic-Proxy: t1.micro: i-e42a													
us-east-1a AWS_EM7_GNMSOE: t1.micro: i-dd													
us-east-1a AWS_EM7_Rox: t1.micro: i-a2da69c	3048						0m8 =						
us-east-1a AWS_Kizuna: t1.micro: i-1d495d7d													
us-east-1a AWS_Nombe: t1.micro: i-1c7f5777	2048												
us-east-1a AWS_not_empty: t1.micro: i-527f573							-25mB						
us-east-1a AWS_Tokidoki: t1.micro: i-f5376b98	1018					-							
us-east-1a East 1a Instance: t1.micro: i-b6/03ed													
us-east-1a m1.small: i-59a86821	0.0		<u> </u>				-S0mB						
us-east- ia mi.smaii: i-5ba86623													
us-east- ia mi.smail: i-/3661a14		08:00	10:00 12:00	14:00	16:00	18:00		08.00	10:00	12:00	14:00	16:00	18:00
us east 1a m1 small i 9fa969a7		- eu-west-1a t1.micro:	i-43464e0c Network In (B) - eu-we	est-1a t1.micro: i-43464e0	c: Network Out (B)			- eu-west-1a t1.micro: i-4	3464e0c: Disk Read Brt	es (B) - eu-west-	1a t1.micro: i-43464e0	Disk Write Bytes (B)	
wareaatria mitaman, i-31800087	1												-

- A traffic light widget that shows the status of all instances for the service.
- Four performance graphs that show applicable metrics when you select an instance from the traffic light widget.
- A time span selector that controls the amount of data shown in the performance graphs.
- An organization selector and device group selector that control which instances are shown in the traffic light widget.

Chapter

AWS Run Book Actions and Automations

Overview

The following sections describe the Run Book Action and Automation policies that are included in the Amazon Web Services PowerPack and how to use them:

About the Run Book Actions and Automations	62
Disabling EC2 and EBS Instances by EC2 Tag	63
Modifying the Parameters of the Automation Actions	64
Enabling the Component Device Record Created Event Policy	64
Enabling the Automation Policies	64
Preserving Automation Changes	65
Discovering EC2 Instances by Public or Private IP Address	65
Modifying the Parameters of the Automation Actions	66
Enabling the Component Device Record Created Event Policy	68
Enabling the Device Record Created Event Policy	69
Enabling the Automation Policies	69
Preserving Automation Changes	69
Vanishing Terminated or Terminating EC2 Instances	70
Enabling the Automation Policies	71
Preserving Automation Changes	71

About the Run Book Actions and Automations

The Amazon Web Services PowerPack includes Run Book Action and Automation policies that can be used to:

- Automatically disable EC2 and EBS devices based on EC2 tags collected from AWS
- Automatically create and start a discovery session for the public or private IP address of an EC2 instance after a component and physical device are merged
- Automatically move an EC2 instance to a vanished state if the EC2 instance is in a terminating or terminated state

The following table describes the automation policies and what they do:

Policy Name	Result					
AWS: Disable EBS Instances by EC2 Tag	If a component device belongs to the AWS EBS Volumes device group and has an EC2 tag, the ScienceLogic platform disables the device.					
AWS: Disable EC2 and EBS Instances by EC2 Tag	If a component device belongs to either the AWS EBS Volumes or AWS EC2 Instances device group and has an EC2 tag, the platform disables the device.					
AWS: Disable or Discover EC2 Instances	The platform automatically discovers EC2 instances by public or private IP address. Additionally, if a component device belongs to the AWS EC2 Instances device group and has an EC2 tag, the platform disables the device.					
AWS: Discover EC2 Instances	The platform automatically discovers EC2 instances by public or private IP address.					
AWS: Merge with EC2	If the platform determines that the IP address of a physical device matches a custom attribute added to an EC2 Instance component device, the platform merges the devices.					
AWS: Vanish Terminated EC2 Instances	If a device belongs to the AWS EC2 Instances device group and is in a terminated or terminating state, the platform un-merges the EC2 Instance and physical device (if applicable), clears the device's associated events, and then moves the device to a vanished state.					

NOTE: The automation policies in the *Amazon Web Services* PowerPack are disabled by default. To use these automations, you must enable the automation policies and optionally modify the parameters in the automation actions.

NOTE: To use the automation policies in the Amazon Web Services PowerPack, the AWS EBS Volumes and AWS EC2 Instances device groups must already be created and populated.

Disabling EC2 and EBS Instances by EC2 Tag

The automation for disabling EC2 and EBS instances includes two automation actions that are executed in the following order:

- AWS: Get EC2 Instance Configuration. This action requests information from the AWS API about the EC2 instance that triggered the automation action or the EC2 instance associated with the EBS instance that triggered the automation action. Information about the EC2 instance associated with an EBS instance is returned only if one EC2 instance is associated with the EBS instance.
- AWS: Disable Instance By Tag. This action compares the information collected by the AWS: Get EC2 Instance Configuration automation action with a pre-defined list of key/value pairs. If an AWS tag matches a key/value pair, the triggering device is disabled.

The Amazon Web Services PowerPack includes three automation policies that trigger these actions:

- AWS: Disable EC2 and EBS Instances by EC2 Tag. If enabled, this automation policy can trigger for any device with which the "AWS EC2 Instance" or the "AWS EBS Instance" Dynamic Applications are aligned (the members of the AWS EC2 Instances and AWS EBS Volumes device groups). The automation policy triggers when the "Component Device Record Created" event is active on the matching devices, immediately after the devices are discovered in the system. Enable this automation policy if you want to disable EC2 and EBS instances by EC2 tag, but do not want to enable automated discovery of EC2 instances by public or private IP address.
- AWS: Disable or Discover EC2 Instances. If enabled, this automation policy can trigger for any device with which the "AWS EC2 Instance" Dynamic Application is aligned (the members of the AWS EC2 Instances). The automation policy triggers when the "Component Device Record Created" event is active on the matching devices, immediately after the devices are discovered in the system. Enable this automation policy if you want to disable EC2 instances by EC2 tag and want to enable automated discovery of EC2 instances by public or private IP address. This automation policy is configured to run both processes in the correct order for EC2 instances. If you enable this automation policy and want to automatically disable associated EBS instances, you must also enable the AWS: Disable EBS Instances by EC2 Tag automation policy.
- AWS: Disable EBS Instances by EC2 Tag. If enabled, this automation policy can trigger for any device with which the "AWS EC2 Instance" Dynamic Application is aligned (the members of the AWS EC2 Instances). The automation policy triggers when the "Component Device Record Created" event is active on the matching devices, immediately after the devices are discovered in the system. Enable this automation policy if you want to disable EC2 instances by EC2 tag, want to enable automated discovery of EC2 instances by public or private IP address, and want to disable EBS instances by EC2 tag.

To use this automation, you must:

- Modify the parameters of the automation actions (optional)
- Enable the Component Device Record Created event policy
- Enable the automation policies
- Configure your system to preserve these changes

Modifying the Parameters of the Automation Actions

The snippet for the **AWS**: **Disable EBS Instances by EC2 Tag** automation action includes the pre-defined list of key/value pairs with which the tags collected from the AWS API are compared. You must modify this list to include the key/value pairs that you want to use to disable EC2 instances.

To modify the parameters for the AWS: Disable EBS Instances by EC2 Tag automation action:

- 1. Go to the **Action Policy Manager** page (Registry > Run Book > Actions).
- 2. Click the wrench icon (*P*) for the AWS: Disable Instance By Tag automation action.
- 3. In the **Snippet Code** field, locate and edit the following line:

```
DISABLE_TAGS = [('ExampleKey', 'ExampleValue')]
```

The line must be in the following format, with each key and each value inside single-quotes and each key/value pair comma-separated inside parentheses, with commas separating each key/value pair.

DISABLE_TAGS [('Key', 'Value'), ('Key', 'Value'), ..., ('Key', 'Value')]

For example, suppose you want to disable an EC2 instance where the "Environment" key is either "dev" or "test" or the "Owner" key is "Sales". You would update the line so it looks like this:

```
DISABLE_TAGS [('Environment', 'dev'), ('Environment', 'test'), ('Owner', 'Sales')]
```

4. Click the [Save] button.

Enabling the Component Device Record Created Event Policy

To enable the "Component Device Record Created" event policy:

- 1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager).
- 2. Click the wrench icon (🌮) for the "Component Device Record Created" event policy.
- 3. In the **Operational State** field, select Enabled.
- 4. Click [Save].

To prevent this change from being overwritten when the PowerPacks installed on the system are updated, you can enable the **Selective PowerPack Field Protection** option. To enable this option:

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

Enabling the Automation Policies

To enable one or more automation policies in the Amazon Web Services PowerPack:

1. Go to the Automation Policy Manager page (Registry > Run Book > Automation).

- 2. Click the wrench icon (\checkmark) for the automation policy you want to enable.
- 3. In the **Policy State** field, select Enabled.
- 4. Click [Save].

Preserving Automation Changes

If you have modified automation actions and policies that are included in the Amazon Web Services PowerPack, those changes will be overwritten when the PowerPack is updated in your system. If you have modified automation actions and policies that are included in the PowerPack, you can:

- Re-implement those changes after each update of the Amazon Web Services PowerPack.
- Remove the content from the PowerPack on your system. When the Amazon Web Services PowerPack is updated in your system, updated versions of this content will not be installed on your system and your local changes will be preserved.

To remove automation actions or automation policies content from the Amazon Web Services PowerPack on your system:

- 1. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
- 2. Click the wrench icon (*P*) for the Amazon Web Services PowerPack. The **Editing PowerPack** page appears.
- 3. In the left NavBar of the Editing PowerPack page, select the type of content you want to remove:
 - To remove an automation action, click **Run Book Actions**. The **Embedded Run Book Actions** and **Available Run Book Actions** panes appear.
 - To remove an automation policy, click **Run Book Policies**. The **Embedded Run Book Policies** and **Available Run Book Policies** panes appear.
- 4. In the upper pane, click the bomb icon () for each automation action or automation policy that you want to remove from the Amazon Web Services PowerPack on your system.

6

Discovering EC2 Instances by Public or Private IP Address

The automation for discovering EC2 instances by public or private IP addresses includes three automation actions that are executed in the following order:

- AWS: Get EC2 Instance Configuration. This action requests information from the AWS API about the EC2 instance that triggered the automation action.
- AWS: Discover from EC2 IP. This action uses the IP address and port information in the response from the AWS API to create and run a discovery session. This action also adds a custom attribute to the EC2 component device record that can be used to match a newly discovered device to the EC2 instance.
- AWS: Merge Physical with Component. This action matches the IP address of a physical device with the custom attribute added to EC2 component devices by the AWS: Discover from EC2 IP automation action. If a match is found, the matching EC2 component device is merged with the physical device.

The Amazon Web Services PowerPack includes three automation policies that trigger these actions:

- AWS: Discover EC2 Instances. If enabled, this automation policy can trigger for any device with which the "AWS EC2 Instance" Dynamic Application is aligned (the members of the AWS EC2 Instances). The automation policy triggers when the "Component Device Record Created" event is active on the matching devices, immediately after the devices are discovered in the system. Enable this automation policy if you want to enable automated discovery of EC2 instances by public or private IP address but do not want disable EC2 and EBS instances by EC2 tag.
- AWS: Disable or Discover EC2 Instances. If enabled, this automation policy can trigger for any device with which the "AWS EC2 Instance" Dynamic Application is aligned (the members of the AWS EC2 Instances). The automation policy triggers when the "Component Device Record Created" event is active on the matching devices, immediately after the devices are discovered in the system. Enable this automation policy if you want to disable EC2 instances by EC2 tag **and** want to enable automated discovery of EC2 instances by public or private IP address. This automation policy is configured to run both in the correct order for EC2 instances.
- AWS: Merge with EC2. If enabled, this automation policy can trigger for any device. The automation policy triggers when the "Device Record Created" event is active on the matching devices, immediately after the devices are discovered in the system. Enable this automation policy if you want to enable automated discovery of EC2 instances by public or private IP address.

To use this automation, you must:

- Modify the parameters of the automation actions (optional)
- Enable the Component Device Record Created event policy
- Enable the Device Record Created event policy
- Enable the automation policies
- Configure your system to preserve these changes

Modifying the Parameters of the Automation Actions

The snippet for the AWS: Discover from EC2 IP automation action includes parameters that define how the automation action creates discovery sessions. You can edit the following lines in the Snippet Code field of the AWS: Discover from EC2 IP automation action to change these parameters:

• EC2_IP_ATTRIBUTE = 'PrivateIpAddress'

The attribute returned by the AWS API for EC2 instances that contains the IP address to use in the discovery session. By default, the private IP address is used. To use the public IP address of the EC2 instance, change this line to:

EC2_IP_ATTRIBUTE = 'PublicIpAddress'

• EXTRA SCAN PORTS = ["21","22","23","25","80","443","5985","5986"]

The list of TCP ports used in the discovery session includes any TCP ports that are specified explicitly in the security group associated with the EC2 instance, plus any TCP ports included in the EXTRA_SCAN_PORTS parameter. You can add or remove ports from this default list. For example, if you wanted to remove TCP port 21 from this list and add TCP port 53, you would change this line to:

EXTRA_SCAN_PORTS = ["22","23","25","53","80","443","5985","5986"]

NOTE: The EXTRA_SCAN_PORTS parameter must be populated if there are no rules for specific ports in the security group associated with the EC2 instance.

• AUTO_INCLUDE_CREDS = True

If the AUTO_INCLUDE_CREDS parameter is "True", the automation will automatically add credentials to the discovery session. A credential will be added automatically if it meets one of the following requirements:

- The credential is an SNMP credential, the Security Group associated with the EC2 instance includes a rule that allows access to UDP port 161, and the credential is explicitly aligned within the organization of the EC2 instance.
- The credential is an SNMP credential, the Security Group associated with the EC2 instance includes a rule that allows access to UDP port 161, the credential is associated with all organizations in the system, and the INCLUDE_ALL_ORG_CREDS parameter is "True".
- The credential is not an SNMP credential or an LDAP/AD credential, the TCP port used by the credential is included in the list of TCP ports for the discovery session (the credential is specified explicitly in the security group associated with the EC2 instance or is included in the EXTRA_SCAN_ PORTS parameter), and the credential is explicitly aligned with in the organization of the EC2 instance.
- The credential is not an SNMP credential or an LDAP/AD credential, the TCP port used by the credential is included in the list of TCP ports for the discovery session (the credential is specified explicitly in the security group associated with the EC2 instance or is included in the EXTRA_SCAN_ PORTS parameter), and the INCLUDE ALL ORG CREDS parameter is "True".

To disable the automatic alignment of credentials to the discovery session, change this line to:

AUTO_INCLUDE_CREDS = False

• INCLUDE_ALL_ORG_CREDS = True

If INCLUDE_ALL_ORG_CREDS is "True" and the AUTO_INCLUDE_CREDS parameter is "True", credentials that are aligned with all organizations (credentials that do not have an explicit organization alignment) are automatically included in the discovery session when that credential meets the other requirements for being automatically included in the discovery session.

• EXTRA_CREDS = ""

In addition to the credentials that are automatically included in the discovery sessions based on open ports, you can optionally specify a string of comma-separated credential IDs for credentials that will be included in every discovery session created by this automation. For example, if you wanted to include credentials with IDs 10 and 13 in every discovery session created by this automation, you would change this line to:

EXTRA_CREDS = "10,13"

• DISCOVER_NON_SNMP = "1"

If DISCOVER_NON_SNMP is set to "1", discovery sessions created by this automation will be configured to discover non-SNMP devices. If you want the discovery sessions created by this automation to discover only SNMP devices, change this line to:

DISCOVER NON SNMP = "0"

• TEMPLATE NAME = ""

If you specify a device template name in the TEMPLATE_NAME parameter, that device template will be automatically aligned with all discovery sessions created by this automation. For example, if you wanted to align a device template called "Standard Device Template" to every discovery session created by this automation, you would change this line to:

TEMPLATE_NAME = "Standard Device Template"

To modify the parameters for the AWS: Discover from EC2 IP automation action, perform the following steps:

- 1. Go to the Action Policy Manager page (Registry > Run Book > Actions).
- 2. Click the wrench icon (*P*) for the AWS: Discover from EC2 IP automation action.
- 3. In the **Snippet Code** field, locate and edit the line(s) for the parameter(s) you want to change:
- 4. Click the [Save] button.

If you modified the EC2_IP_ATTRIBUTE parameter in the AWS: Discover from EC2 IP automation action, you must perform the following steps to update the AWS: Merge Physical with Component automation action:

To modify the parameters for the AWS: Discover from EC2 IP automation action, perform the following steps:

- 1. Go to the Action Policy Manager page (Registry > Run Book > Actions).
- 2. Click the wrench icon (*P*) for the AWS: Discover from EC2 IP automation action.
- 3. In the **Snippet Code** field, locate and edit the following line:

IP_ATTRIBUTE = 'c-EC2_PrivateIpAddress'

If you changed the EC2_IP_ATTRIBUTE parameter in the **AWS**: **Discover from EC2 IP** automation action to 'PublicIpAddress', change this line to:

IP ATTRIBUTE = 'c-EC2 PublicIpAddress'

4. Click the [Save] button.

Enabling the Component Device Record Created Event Policy

To enable the "Component Device Record Created" event policy:

- 1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager).
- 2. Click the wrench icon (🎤) for the "Component Device Record Created" event policy.
- 3. In the **Operational State** field, select Enabled.
- 4. Click [Save].

To prevent this change from being overwritten when the PowerPacks installed on the system are updated, you can enable the **Selective PowerPack Field Protection** option. To enable this option:

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

Enabling the Device Record Created Event Policy

To enable the "Device Record Created" event policy:

- 1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager).
- 2. Click the wrench icon (🎤) for the "Device Record Created" event policy.
- 3. In the Operational State field, select Enabled.
- 4. Click [Save].

To prevent this change from being overwritten when the PowerPacks installed on the system are updated, you can enable the **Selective PowerPack Field Protection** option. To enable this option:

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

Enabling the Automation Policies

To enable one or more automation policies in the Amazon Web Services PowerPack:

- 1. Go to the Automation Policy Manager page (Registry > Run Book > Automation).
- 2. Click the wrench icon (🌮) for the automation policy you want to enable.
- 3. In the Policy State field, select Enabled.
- 4. Click [Save].

Preserving Automation Changes

If you have modified automation actions and policies that are included in the Amazon Web Services PowerPack, those changes will be overwritten when the PowerPack is updated in your system. If you have modified automation actions and policies that are included in the PowerPack, you can:

- Re-implement those changes after each update of the Amazon Web Services PowerPack.
- Remove the content from the PowerPack on your system. When the Amazon Web Services PowerPack is updated in your system, updated versions of this content will not be installed on your system and your local changes will be preserved.

To remove automation actions or automation policies content from the Amazon Web Services PowerPack on your system:

- 1. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
- 2. Click the wrench icon (*P*) for the Amazon Web Services PowerPack. The **Editing PowerPack** page appears.
- 3. In the left NavBar of the **Editing PowerPack** page, select the type of content you want to remove:
 - To remove an automation action, click **Run Book Actions**. The **Embedded Run Book Actions** and **Available Run Book Actions** panes appear.
 - To remove an automation policy, click **Run Book Policies**. The **Embedded Run Book Policies** and **Available Run Book Policies** panes appear.
- 4. In the upper pane, click the bomb icon () for each automation action or automation policy that you want to remove from the Amazon Web Services PowerPack on your system.

Vanishing Terminated or Terminating EC2 Instances

The automation for vanishing terminated EC2 instances includes one automation action:

- AWS: Vanish Terminated EC2 Instances. This action requests information from the AWS API about the EC2 instance that triggered the automation action. If the response from the AWS API indicates that the EC2 instance that triggered the automation action is in a terminated or terminating state, the action performs the following steps:
 - If the automation triggers for a physical device that is merged with an EC2 instance, the devices are un-merged.
 - If the automation triggers for a physical device that is merged with an EC2 instance, after being unmerged the physical device is moved to a virtual collector group.
 - If the automation triggers for a physical device that is merged with an EC2 instance, after being unmerged, all events associated with the physical device are cleared.
 - All events associated with the component device are cleared.
 - The component device is vanished.

The Amazon Web Services PowerPack includes an automation policy that triggers this action:

• AWS: Vanish Terminated EC2 Instances. If enabled, this automation policy can trigger for any device with which the "AWS EC2 Instance" Dynamic Application is aligned (the members of the AWS EC2 Instances). The automation policy triggers when the Availability Check Failed event is active on the matching devices.

To use this automation, you must:

- Enable the AWS: Vanish Terminated EC2 Instances automation policy
- Configure your system to preserve this change

Enabling the Automation Policies

To enable one or more automation policies in the Amazon Web Services PowerPack:

- 1. Go to the Automation Policy Manager page (Registry > Run Book > Automation).
- 2. Click the wrench icon (🎤) for the automation policy you want to enable.
- 3. In the **Policy State** field, select Enabled.
- 4. Click [Save].

Preserving Automation Changes

If you have modified automation actions and policies that are included in the Amazon Web Services PowerPack, those changes will be overwritten when the PowerPack is updated in your system. If you have modified automation actions and policies that are included in the PowerPack, you can:

- Re-implement those changes after each update of the Amazon Web Services PowerPack.
- Remove the content from the PowerPack on your system. When the Amazon Web Services PowerPack is updated in your system, updated versions of this content will not be installed on your system and your local changes will be preserved.

To remove automation actions or automation policies content from the Amazon Web Services PowerPack on your system:

- 1. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
- 2. Click the wrench icon (*P*) for the Amazon Web Services PowerPack. The **Editing PowerPack** page appears.
- 3. In the left NavBar of the **Editing PowerPack** page, select the type of content you want to remove:
 - To remove an automation action, click **Run Book Actions**. The **Embedded Run Book Actions** and **Available Run Book Actions** panes appear.
 - To remove an automation policy, click **Run Book Policies**. The **Embedded Run Book Policies** and **Available Run Book Policies** panes appear.
- 4. In the upper pane, click the bomb icon () for each automation action or automation policy that you want to remove from the Amazon Web Services PowerPack on your system.

© 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