Centralized Logging

AWS Implementation Guide

Garvit Singh

November 2016

Last updated: December 2019 (see revisions)

Contents

About This Guide

This implementation guide discusses architectural considerations and configuration steps for deploying a centralized logging solution on the Amazon Web Services (AWS) Cloud. It includes links to AWS CloudFormation templates that launch, configure, and run the AWS compute, network, storage, and other services required to deploy this solution on AWS, using AWS best practices for security and availability.

The guide is intended for IT infrastructure architects, administrators, and DevOps professionals who have practical experience architecting on the AWS Cloud.

Overview

Amazon Web Services (AWS) provides service-specific operational metrics and log files to give customers insight into how the service is operating. Many AWS services also generate security log data, including audit logs for access, configuration changes, and billing events. In addition to AWS log data, web servers, applications, and operating systems generate log files in different formats, and in a disorganized and distributed fashion. Effectively consolidating, managing, and analyzing these different log types is a challenge for almost every company, which is why many AWS customers choose to implement a centralized logging solution.

The AWS Cloud provides a suite of infrastructure services that enable you to deploy a centralized logging solution in an available and affordable way. This guide provides infrastructure and configuration information for deploying a centralized logging solution that collects, analyzes, and displays logs on AWS across multiple accounts and AWS Regions. The solution uses Amazon Elasticsearch Service (Amazon ES), a managed service that simplifies the deployment, operation, and scaling of Elasticsearch clusters in the AWS Cloud, as well as Kibana, an analytics and visualization platform that is integrated with Amazon ES. In combination with other AWS managed services, this solution provides customers with a turnkey environment to begin logging and analyzing their AWS environment and applications.

The information in this guide assumes basic knowledge of web, application, and operating system log formats. It is also helpful to have working knowledge of Amazon ES and Kibana for creating and customizing your own dashboards and visualizations.

Cost

You are responsible for the cost of the AWS services used while running this reference deployment. As of the date of publication, the cost for running a centralized logging solution with this solution's default settings in the US East (N. Virginia) Region is as shown in the table below. This includes charges for Amazon Elasticsearch Service instance hours.

Cluster Size	Total Cost/Hour
Small	$1.44
Medium	$6.43
Large	$12.43

This cost estimate does not reflect variable, usage-driven charges incurred from Amazon CloudWatch, AWS CloudTrail, AWS Lambda, or the cost for sample logs. For full details, see the pricing webpage for each AWS service you will be using in this solution.

Architecture Overview

Deploying this solution builds the following environment in the AWS Cloud.

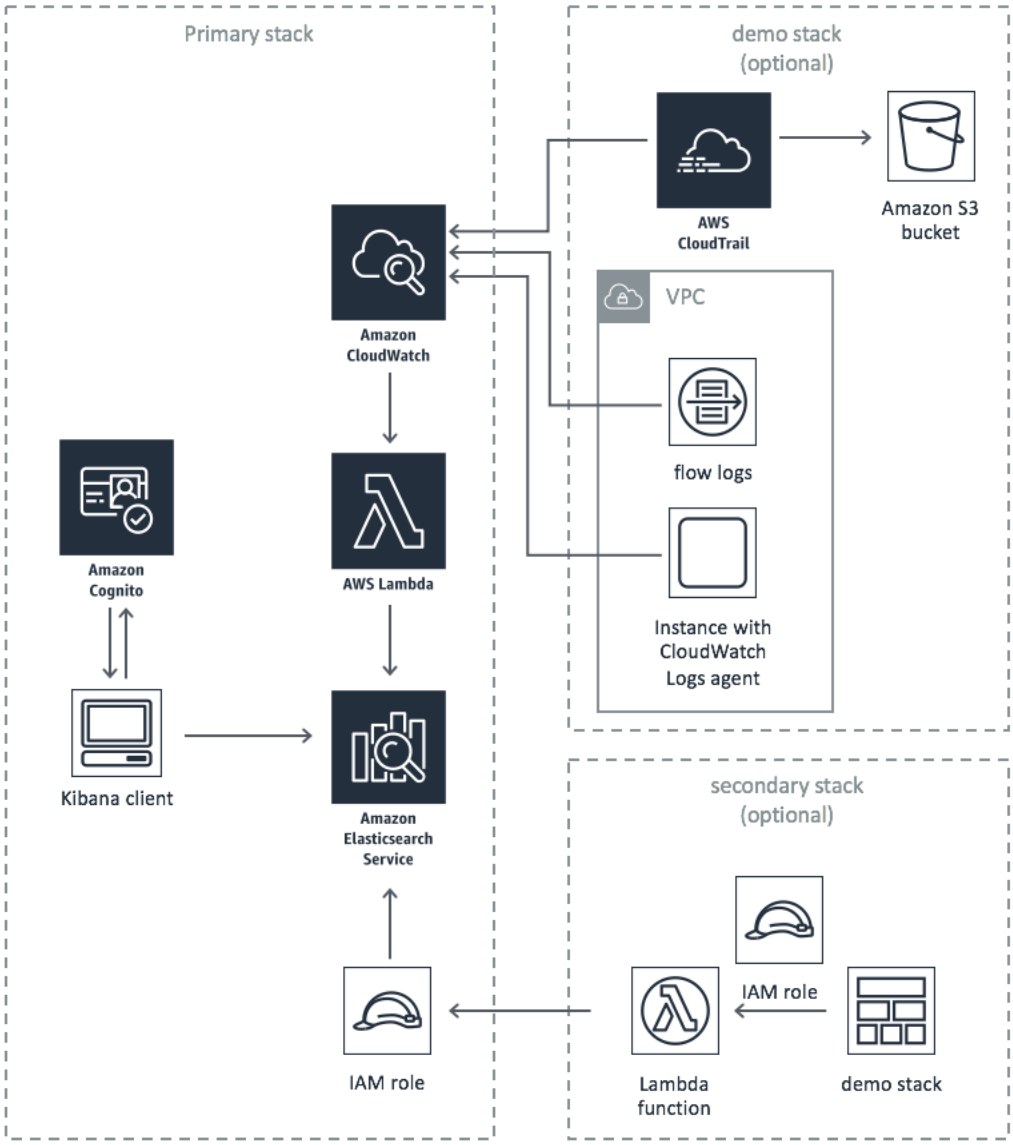

Figure 1: Centralized logging solution architecture on AWS

This solution includes an AWS CloudFormation template that you deploy in the primary account. This template launches an Amazon Elasticsearch Service (Amazon ES) domain, which is the hardware, software, and data exposed by Amazon ES endpoints. During initial configuration of the solution's primary template, users choose from one of three solution sizes to determine the number and type of data nodes (Amazon ES instances) in the cluster: small, medium, or large. The primary template also provisions an Amazon Cognito user pool for Kibana dashboard user authentication.

The solution also includes a secondary template that you can deploy in secondary accounts and other AWS Regions. This template launches an AWS Lambda function that indexes logs from the secondary account or region on the Amazon ES domain in the primary account or region. During configuration of this template, you specify the Amazon ES domain endpoint and the Amazon Resource Name (ARN) of the primary AWS Identity and Access Management (IAM) role that the Lambda function will assume.

The centralized logging solution is designed to allow you to centralize the management of your own logs, but it also includes sample logs you can deploy for testing purposes. For more information, see Appendix A.

Design Considerations

Custom Sizing

Choose from three preset Amazon ES cluster sizes to support your anticipated log traffic:

Small:
- 3 dedicated master nodes; c4.large.elasticsearch instance type
- 4 data nodes; i3.large.elasticsearch instance type

Medium:
- 3 dedicated master nodes; c4.large.elasticsearch instance type
- 6 data nodes; i3.2xlarge.elasticsearch instance type

Large:
- 3 dedicated master nodes; c4.large.elasticsearch instance type
- 6 data nodes; i3.4xlarge.elasticsearch instance type

Scalability

Modify your cluster's instance count and type directly in Amazon ES to accommodate your changing environment and requirements, without having to reconfigure the solution architecture or manage backend resources. As a best practice, we recommend that you monitor your cluster's performance metrics.

Kibana Dashboard

Take advantage of Kibana features to create, save, and share custom visualizations and customer views. This solution includes a configuration file to get you started with some popular dashboard views.

Logging Across Accounts and Regions

The Amazon ES domain that this solution creates can accept log data from other AWS accounts and AWS Regions. Customers can launch the spoke template in secondary

accounts and other regions to use this solution to index logs across accounts and regions.

During initial configuration, enter the secondary account IDs in the **Spoke Accounts** parameter before you deploy the spoke template in those accounts to ensure that the secondary accounts can assume the master IAM role. To add accounts after you launch the primary template, update the **Spoke Accounts** parameter in the primary stack with the secondary account IDs. Then, update the primary stack and deploy the spoke template in the secondary accounts. You can remove an account at any time by removing its ID from the **Spoke Accounts** parameter.

Solution Updates

Centralized Logging version 3.2 uses the most up-to-date Node.js runtime. Version 2.2 uses the Node.js 8.10 runtime, which reaches end-of-life on December 31, 2019. In January, AWS Lambda will block the create operation and, in February, Lambda will block the update operation. For more information, see Runtime Support Policy in the *AWS Lambda Developer Guide*.

To continue using this solution with the latest features and improvements, you can update the stack.

Regional Deployments

This solution uses Amazon Cognito which is available in specific AWS Regions only. Therefore, you must launch this solution's primary template in a region that supports Amazon Cognito.[1] The solution's spoke template can be deployed in any region in secondary accounts. Once deployed, the solution will monitor logs for all regions in applicable accounts.

AWS CloudFormation Templates

This solution uses AWS CloudFormation to automate the deployment of a centralized logging solution on the AWS Cloud. It includes the following AWS CloudFormation template, which you can download before deployment:

View template **centralized-logging-primary.template:** Use this template to launch the centralized logging solution and all associated components. The default configuration deploys an Amazon Elasticsearch Service domain.

[1] For the most current service availability by region, see https://aws.amazon.com/about-aws/global-infrastructure/regional-product-services/.

The solution offers three deployment size options based on logging requirements, but you can also customize the template based on your specific needs.

View template **centralized-logging-spoke.template:** Use this template to configure permissions for managing logs in secondary accounts. This template launches an AWS Lambda function that assumes the AWS Identity and Access Management (IAM) master role from the primary account to index logs on the Amazon ES domain.

If you set the **Sample Logs** template parameter in these templates to `Yes`, the templates launch the following nested stack:

- **centralized-logging-demo.template:** This template deploys sample logs you can use for testing purposes. The default configuration deploys an Amazon EC2 instance with a reference Apache server in an Amazon VPC, an Amazon Simple Storage Service (Amazon S3) bucket, an Amazon CloudTrail trail, and VPC flow logs.

Automated Deployment

Before you launch the automated deployment, please review the architecture, configuration, and other information discussed in this guide. Follow the step-by-step instructions in this section to configure and deploy a centralized logging solution into your account.

Time to deploy: Approximately 30 minutes

What We'll Cover

The procedure for deploying this architecture on AWS consists of the following steps. For detailed instructions, follow the links for each step.

Step 1. Launch the Primary Stack

- Launch the AWS CloudFormation template into your AWS account.
- Enter values for required parameters: **Stack Name, Cognito Admin Email, Domain Admin Email**
- Review the other template parameters, and adjust if necessary.

Step 2. Launch the Spoke Stack (Optional)

- Launch the AWS CloudFormation template into secondary AWS accounts and AWS Regions.
- Review the template parameters, and adjust if necessary.

Step 3. Configure the Kibana Dashboard (Optional)

- Import the sample Kibana dashboard to test the solution

Step 1. Launch the Primary Stack

This automated AWS CloudFormation template deploys the centralized logging solution in your primary AWS account.

> **Note**: You are responsible for the cost of the AWS services used while running this solution. See the Cost section for more details. For full details, see the pricing webpage for each AWS service you will be using in this solution.

1. Sign in to the AWS Management Console and click the button to the right to launch the `centralized-logging-primary` AWS CloudFormation template. You can also download the template as a starting point for your own implementation.

2. The template is launched in the US East (N. Virginia) Region by default. To launch the centralized logging solution in a different AWS Region, use the region selector in the console navigation bar.
3. On the **Select Template** page, verify that you selected the correct template and choose **Next**.
4. On the **Specify Details** page, assign a name to your centralized logging solution stack.
5. Under **Parameters**, review the parameters for the template and modify them as necessary. This solution uses the following default values.

Parameter	Default	Description
Domain Name	`centralized-logging`	The name of the Amazon ES domain that this template will create. **Note:** Amazon ES domain names must start with a lowercase letter and must be between 3 and 28 characters. Valid characters are a-z (lowercase only), 0-9, and – (hyphen).
Cluster Size	`Small`	A drop-down box with three Amazon ES cluster sizes: `Small`, `Medium`, `Large`
Spoke Accounts	<Optional input>	Comma delimited list of account IDs for log indexing. Enter the secondary account IDs in this parameter before you deploy the spoke template in secondary accounts. To add accounts after you launch the primary template, update the

Parameter	Default	Description
		Spoke Accounts parameter in the primary stack with the secondary account IDs. Then, update the primary stack and deploy the spoke template in the secondary accounts. **Note:** For cross-region log indexing in the primary account, enter the primary account ID. For cross-account indexing, enter secondary (spoke) account IDs. For both, enter primary and secondary account IDs.
Cognito Admin Email	*<Requires input>*	Email address of the Kibana dashboard administrator
Domain Admin Email	*<Requires input>*	Email address of the Amazon ES domain administrator
Sample Logs	`No`	Choose whether to deploy the demo template
VPC CIDR for Sample Sources	`10.250.0.0/16`	CIDR block for the sample logs VPC. You can modify the address range to avoid overlapping with existing networks. **Note:** Use this parameter only if you choose `Yes` for **Sample Logs**.
Subnet for Sample Web Server	`10.250.250.0/24`	CIDR block for the sample web server. You can modify the address range to avoid overlapping with existing networks. **Note:** Use this parameter only if you choose `Yes` for **Sample Logs**.

6. Choose **Next**.
7. On the **Options** page, choose **Next**.
8. On the **Review** page, review and confirm the settings. Be sure to check the box acknowledging that the template will create AWS Identity and Access Management (IAM) resources.
9. Choose **Create** to deploy the stack.

   You can view the status of the stack in the AWS CloudFormation console in the **Status** column. You should see a status of CREATE_COMPLETE in approximately 30 minutes.
10. To see details for the stack resources, choose the **Outputs** tab. The following table describes some of these outputs in more detail.

Key	Description
KibanaURL	URL for front-end access to the Kibana 4 dashboard
DomainEndpoint	URL for the Amazon ES domain endpoint

Key	Description
MasterRole	Master IAM role for log indexing on the Amazon ES domain

Note: This solution deploys an AWS Lambda function, `solution-helper`, which runs only during initial configuration or when resources are updated or deleted. You will see the `solution-helper` function in the AWS Lambda console, which is necessary to manage associated resources for as long as the solution is running.

Step 2. Launch the Spoke Stack (Optional)

Use this procedure to launch the components necessary to manage logs in secondary accounts. You must enter the secondary account IDs in the **Spoke Accounts** parameter of the primary template before you launch this template in secondary accounts.

Note: You are responsible for the cost of the AWS services used while running this solution. See the Cost section for more details. For full details, see the pricing webpage for each AWS service you will be using in this solution.

1. Sign in to the AWS Management Console and click the button to the right to launch the `centralized-logging-spoke` AWS CloudFormation template.
   You can also download the template as a starting point for your own implementation.

   Launch Spoke Template

2. The template is launched in the US East (N. Virginia) Region by default. To launch the centralized logging solution in a different AWS Region, use the region selector in the console navigation bar.
3. On the **Select Template** page, verify that you selected the correct template and choose **Next**.
4. On the **Specify Details** page, assign a name to your centralized logging solution stack.
5. Under **Parameters**, review the parameters for the template and modify them as necessary. This solution uses the following default values.

Parameter	Default	Description
Elasticsearch Endpoint	*<Requires input>*	Amazon Elasticsearch Service (Amazon ES) domain endpoint **Note:** You can find the endpoint in the primary AWS CloudFormation stack **Outputs** tab. The

		endpoint is the value of the **DomainEndpoint** key. Do not enter `https://`.
Master Account Role	*<Requires input>*	AWS IAM role for cross-account indexing **Note:** You can find the master role in the primary AWS CloudFormation stack **Outputs** tab. The role is the value of the **MasterRole** key.
Cluster Size	`Small`	A drop-down box with three Amazon ES cluster sizes: `Small`, `Medium`, `Large` **Note:** Select the same cluster size you chose for the primary stack. You can find the cluster size in the primary AWS CloudFormation stack **Outputs** tab. The name of the cluster size is the value of the **ClusterSize** key.
Sample Logs	`No`	Choose whether to deploy the demo template
VPC CIDR for Sample Sources	`10.250.0.0/16`	CIDR block for the sample logs VPC. You can modify the address range to avoid overlapping with existing networks. **Note:** Use this parameter only if you choose `Yes` for **Sample Logs**.
Subnet for Sample Web Server	`10.250.250.0/24`	CIDR block for the sample web server. You can modify the address range to avoid overlapping with existing networks. **Note:** Use this parameter only if you choose `Yes` for **Sample Logs**.

6. Choose **Next**.
7. On the **Options** page, choose **Next**.
8. On the **Review** page, review and confirm the settings. Be sure to check the box acknowledging that the template will create AWS Identity and Access Management (IAM) resources.
9. Choose **Create** to deploy the stack.

   You can view the status of the stack in the AWS CloudFormation console in the **Status** column. You should see a status of CREATE_COMPLETE in roughly five minutes.

Step 3. Configure the Kibana Dashboard (Optional)

A Kibana dashboard displays a group of visualizations that you can modify, save, and share. If you choose to deploy the sample logs, the visualizations for this solution combine data from VPC flow logs, the Apache web server, and AWS CloudTrail to create a

centralized view of an application and its supporting resources. Note that you must set the **Sample Logs** AWS CloudFormation parameter to `Yes` before you configure the dashboard.

After the centralized logging solution stack launch completes, you will receive a verification email with a user name and password you use to access the Kibana dashboard and begin importing sample log data. Use the following steps to log in to Kibana, add an Amazon ES index, and import the solution's preconfigured dashboard settings.

1. Download dashboard configuration file (`basic-dashboard.json`) from the centralized logging solution Amazon S3 bucket. You will use this later in the procedure to configure your first dashboard.
2. Go to the AWS CloudFormation console, and in the **Outputs** tab, open the **KibanaURL** link to go to the Kibana dashboard.
3. When prompted, log in to the dashboard with the user name and password from the verification email. Note that you will be prompted to change the password when you log in for the first time.
4. In the left menu bar, choose **Management**.
5. Under **Configure an index pattern**, set the **Index name or pattern** field to `cwl-*`.
   You should see the message box underneath change from red to green, confirming that there are matching indices and aliases.
6. Under **Time Filter field name**, choose **@timestamp**.
7. Choose **Create**. You will see a list of every field in the index.
8. On the **Saved Objects** tab, choose **Import** and select the `basic-dashboard.json` file you downloaded in Step 1 of this procedure. If prompted, choose **Yes, overwrite all.**

   Note: If this causes an error message, choose **Go Back**. Delete the `cwl-*` index you just created. Wait at least 10 minutes for the indices to populate. Then, repeat steps 4-8.

9. In the **Saved Objects** tab under **Dashboards**, you should see a **Basic** dashboard. Choose the eye icon next to the dashboard to view it.
10. The solution's default dashboard will load. In the upper-right corner, you can adjust the data time period (clock icon). You can also adjust interval for the webpage refresh rate (**Auto-refresh**).

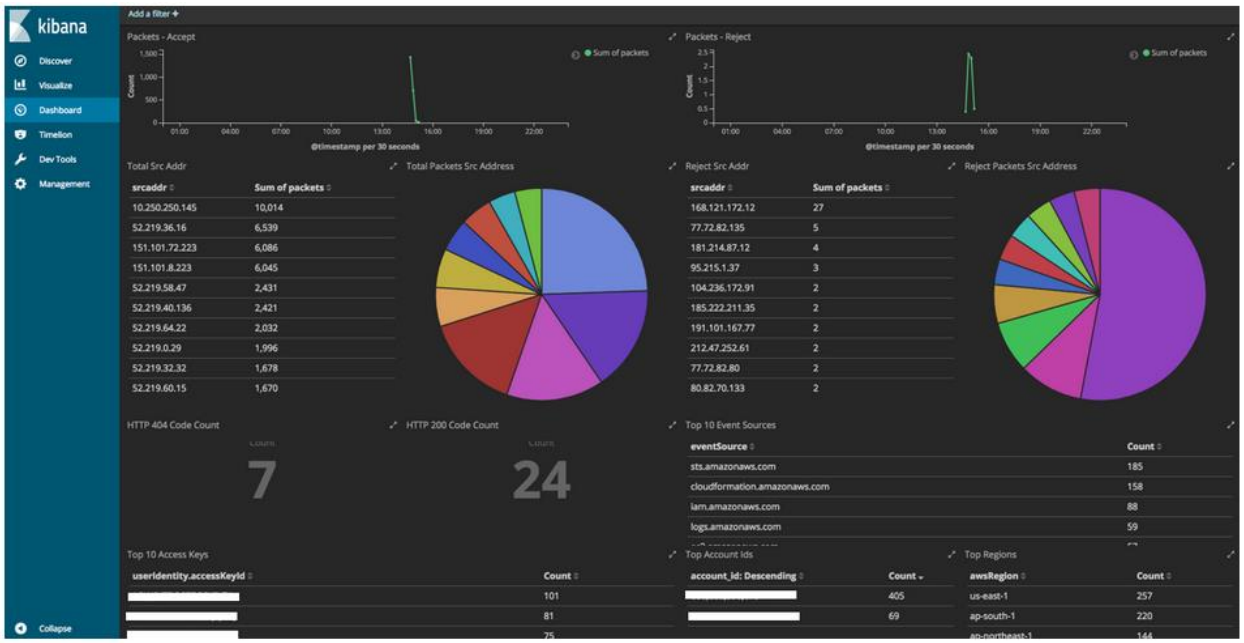

Figure 2: Sample Kibana dashboard

Explore and experiment with the dashboard settings. You can interact with the Apache server to see the events passed to the dashboard metrics, for example, request a webpage that doesn't exist to see the 404 error count increase. The VPC visualizations show you information such as the top 10 rejected source IP addresses.

You can create and save additional visualizations based on the data that is relevant to your application. For more information, go to the Kibana User Guide.

Security

When you build systems on AWS infrastructure, security responsibilities are shared between you and AWS. This shared model can reduce your operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. For more information about security on AWS, visit the AWS Security Center.

Amazon Cognito

Amazon Elasticsearch Service uses Amazon Cognito to offer user name and password protection for Kibana. This authentication feature is optional and available only for domains using Elasticsearch 5.1 or later. If you don't configure Amazon Cognito authentication, you can still protect Kibana using an IP-based access policy and a proxy server.

Access Policy

The centralized logging solution features an access policy that restricts access to the Amazon ES domain to two roles: the solution's master AWS Identity and Access Management (IAM) role for cross-account and cross-region indexing and the `CognitoAuthorizedUser` role for access to the Kibana dashboard. Any secondary accounts you specify in the **Spoke Accounts** parameter will assume the master role. To mitigate the risk of unauthorized access to the permissions granted by the solution's master IAM role, AWS recommends that you deploy the solution in an isolated and tightly controlled management account, and limit access to that account.

Sample Logs Apache Server

Note that the sample logs Apache web server this solution deploys is publicly accessible on port 80. If you modify this sample logs web server for production use, we recommend that you use HTTPS by enabling Transport Layer Security (TLS) and add authentication.

Additional Resources

AWS services

- AWS CloudFormation
- Amazon Elasticsearch Service
- Kibana User Guide
- AWS Lambda

  AWS Lambda
- Amazon CognitoAmazon S3
- Amazon CloudWatch
- IAM

Appendix A: Sample Logs

The centralized logging solution includes an AWS CloudFormation template that deploys sample logs you can use for testing purposes. This template launches an Amazon Elastic Compute Cloud (Amazon EC2) instance with a reference Apache server that hosts a simple web application in an Amazon Virtual Private Cloud (Amazon VPC). During initial launch, the Amazon CloudWatch Logs agent is automatically installed on the instance, which is used to direct raw log data to Amazon CloudWatch.

VPC Flow Logs are enabled in the VPC to capture information about IP traffic to, from, and within the network. Customers can use this example to enable VPC Flow Logs in other VPCs; this data is automatically published to a log group in Amazon CloudWatch Logs.

The demo template turns on AWS CloudTrail and creates a trail for the account, and also creates an Amazon Simple Storage Service (Amazon S3) bucket to store CloudTrail logs, which are automatically delivered to Amazon CloudWatch.

An Amazon CloudWatch event triggers the solution's custom AWS Lambda function, which uploads any new log data (VPC flow logs, CloudTrail logs, and Apache logs) from Amazon CloudWatch to Amazon ES for analysis and visualization.

The primary solution template includes a parameter you can use to automatically deploy the demo template in the primary account. The secondary template also includes a parameter you can use to automatically deploy the demo template in secondary accounts.

Appendix B: Adding Custom CloudWatch Logs

The centralized logging solution enables you to add custom Amazon CloudWatch log sources and log groups to the solution's Amazon Elasticsearch Service (Amazon ES) domain. Use the following procedure to add custom log sources and groups.

1. Navigate to the Amazon CloudWatch console and select **Logs**.
2. Choose the applicable Log Group.
3. In the **Actions** drop-down menu, choose **Stream to AWS Lambda**.
4. In the **Lambda Function** drop-down menu, select **LogStreamer**. Then, choose **Next**.
5. In the **Log Format** drop-down menu, select the applicable log format.
6. Under **Select Log Data to Test**, choose **Test Pattern**.
7. Verify that the **Results** section shows at least one match.
8. Choose **Next**. For more information, see Real-time Processing of Log Data with Subscriptions.
9. Choose **Start Streaming**.

To verify that your logs are being indexed on the Amazon ES domain, navigate to the Amazon ES dashboard. Under the **Indices** section of the dashboard, check **Mappings** for indexed fields from the sample logs.

Appendix C: Migrating to the New Version

If you use an earlier version of the centralized logging solution and you want to move to the new version of the solution, you must migrate data from your existing Amazon

Elasticsearch Service (Amazon ES) domain to the newly provisioned Amazon ES domain to avoid losing data from your existing domain. **Do not update the solution stack.** If you update the stack, your Amazon ES domain will be deleted and replaced by a new one, causing you to lose indexed data on your existing domain.

To migrate your data, complete the following task:

1. Deploy the new version of the primary AWS CloudFormation template in the same account and AWS Region as your current primary stack.
2. Use a snapshot to migrate the indexed data on your Amazon ES domain.
3. After the migration is complete, delete the old AWS CloudFormation stack to stop incurring charges.

Note that the new version of the template includes a retention policy for the Amazon ES domain so the domain will not be deleted with future stack updates.

Appendix D: Troubleshooting

The centralized logging solution logs error, warning, informational, and debugging messages for the solution's AWS Lambda functions. To choose the type of messages to log, find the applicable function in the Lambda console and change the **LOG_LEVEL** environment variable to the applicable type of message.

Level	Description
ERROR	Logs will include information on anything that causes an operation to fail.
WARNING	Logs will include information on anything that can potentially cause inconsistencies in the function but might not necessarily cause the operation to fail. Logs will also include ERROR messages.
INFO	Logs will include high-level information about how the function is operating. Logs will also include ERROR and WARN messages.
DEBUG	Logs will include information that might be helpful when debugging a problem with the function. Logs will also include ERROR, WARNING, and INFO messages.

Common Errors

AWS CloudFormation Primary Template Validation Error

If before you deploy the primary stack, you receive a **Template validation error**, verify that you are deploying the stack in an AWS Region that supports Amazon Cognito.

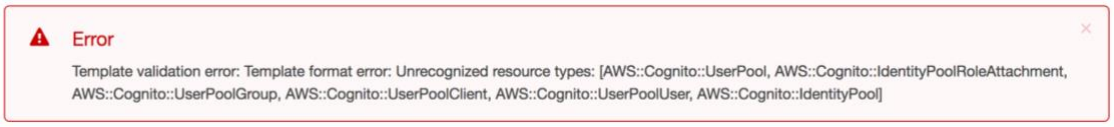

Figure 3: Template validation error

Resolution

To deploy the primary stack in a region that supports Amazon Cognito, complete the following task:

1. In the primary account, navigate to the AWS Management Console.
2. In the console navigation bar, use the region selector to choose an AWS Region that supports Amazon Cognito.

> **Note:** For the most current service availability by region, see AWS service offerings by region.

3. Launch the stack.

AWS CloudFormation Stack Deletion Error

If you receive a `Cannot unsubscribe a subscription that is pending confirmation` message when you attempt to delete the solution's AWS CloudFormation stack, retain the Amazon Simple Notification Service (Amazon SNS) subscription. Amazon SNS subscriptions in a pending state will be automatically deleted after three days.

Figure 4: Stack deletion error

Resolution

After you receive the stack deletion error, complete the following task:

1. Navigate to the AWS CloudFormation console.
2. Select the applicable stack.
3. For **Action**, choose **Delete Stack**.
4. In the **Delete Stack** window, verify the checkbox next to the Amazon SNS subscription is selected.

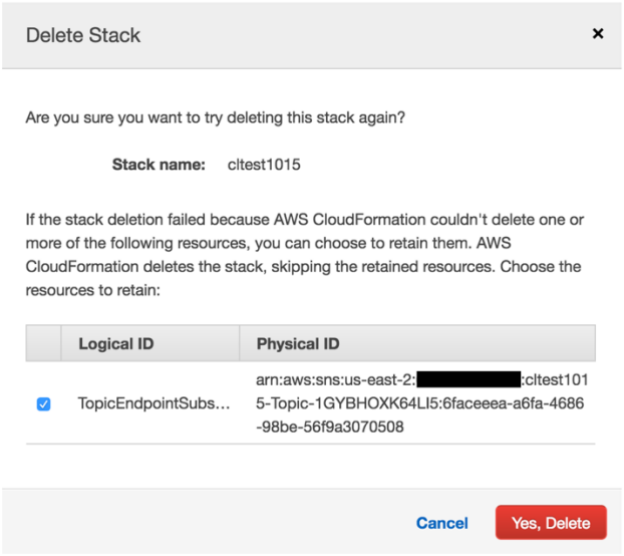

Figure 5: Delete stack window

5. Select **Yes, Delete**.

LogStreamer AWS Lambda Function Permission Error

If the solution's AWS Lambda function (`LogStreamer`) generates permission errors, verify that you granted the secondary account the appropriate permissions to index logs on the Amazon ES domain in the primary account by including the account IDs in the **Spoke Accounts** AWS CloudFormation parameter.

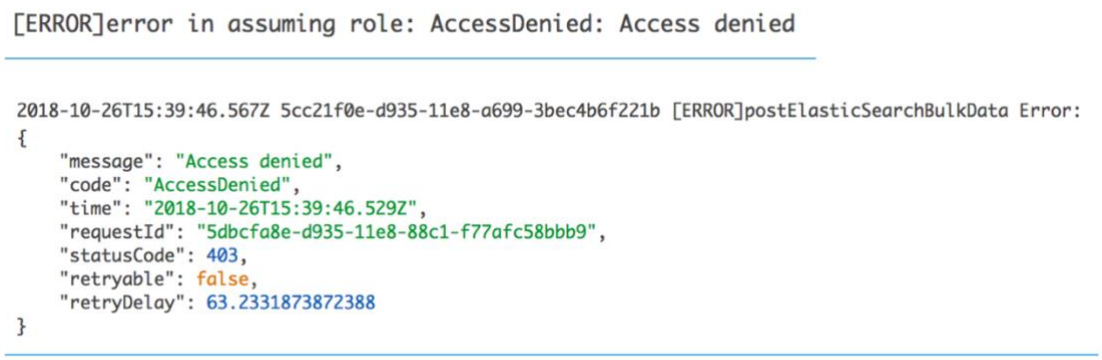

Figure 6: Permission error

Resolution

Complete the following task:

1. In the primary account, navigate to the AWS CloudFormation console.
2. Select the applicable stack.

3. For **Action**, choose **Update Stack**.
4. Select **Next**.
5. For **Spoke Accounts**, enter the applicable secondary account IDs and select **Next**. Note that the format is comma separated (for more than one value).
6. Select **Next**.
7. On the **Review** page, review and confirm the settings. Be sure to check the box acknowledging that the template will create AWS Identity and Access Management (IAM) resources.
8. Choose **Update** to update the stack.
9. After the stack is updated, verify that the Lambda function does not show the permission errors.

Amazon ES Bulk Data Error

If you receive a `postElasticSearchBulkData` error, check to make sure that you provided the correct Amazon ES endpoint in the **Elasticsearch Endpoint** AWS CloudFormation parameter.

Figure 7: postElasticSearchBulkData error

Resolution

Complete the following task:

1. In the applicable secondary account, navigate to the AWS CloudFormation console.
2. Select the applicable spoke stack.
3. For **Action**, choose **Update Stack**.

4. Select **Next**.
5. For **Elasticsearch Endpoint**, verify that you entered the correct endpoint. Make sure that the endpoint does not include `https://`. Then, select **Next**.
6. Select **Next**.
7. On the **Review** page, review and confirm the settings. Be sure to check the box acknowledging that the template will create AWS Identity and Access Management (IAM) resources.
8. Choose **Update** to update the stack.

AWS CloudFormation Stack Update Error

If you receive an **UPDATE_FAILED** message when you try to update the stack to the new version, migrate to the new version instead of updating the stack.

Resolution

Follow the migration steps in Appendix C.

Appendix E: Collection of Operational Metrics

This solution includes an option to send anonymous operational metrics to AWS. We use this data to better understand how customers use this solution to improve the services and products that we offer. When enabled, the following information is collected and sent to AWS each time the AWS Lambda function (`LogStreamer`) is invoked:

- **Solution ID:** The AWS solution identifier
- **Unique ID (UUID):** Randomly generated, unique identifier for each centralized logging solution deployment
- **Timestamp:** Data-collection timestamp
- **Cluster Size:** Size of the Amazon Elasticsearch Service cluster the solution will deploy
- **Items Indexed:** The number of items indexed successfully
- **Total Item Size:** The total size (in bytes) of the items indexed, including failures

Note that AWS will own the data gathered via this survey. Data collection will be subject to the AWS Privacy Policy. To opt out of this feature, modify the AWS CloudFormation template mapping section as follows:

```
Mappings:
  InstanceMap:
    send-data: {"SendAnonymousData": "Yes"},
```

to

```
Mappings:
  InstanceMap:
    send-data: {"SendAnonymousData": "No"},
```

Source Code

You can visit our GitHub repository to download the templates and scripts for this solution, and to share your customizations with others.

Document Revisions

Date	Change
November 2016	Initial publication
February 2018	Added cross-account and cross-region functionality and upgraded Amazon Elasticsearch Service version to 6.0
November 2018	Added Amazon Cognito for Kibana dashboard user authentication, changed custom sizing of the Elasticsearch cluster, and added information on troubleshooting
December 2019	Added information on support for Node.js update

Notices

This document is provided for informational purposes only. It represents AWS current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

The Centralized Logging solution is licensed under the terms of the Apache License Version 2.0 available at https://www.apache.org/licenses/LICENSE-2.0.