Centralized Logging

AWS Implementation Guide

*Chuan Chen April 2020*



Copyright (c) 2019 by Amazon.com, Inc or its affiliates.

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

# Overview

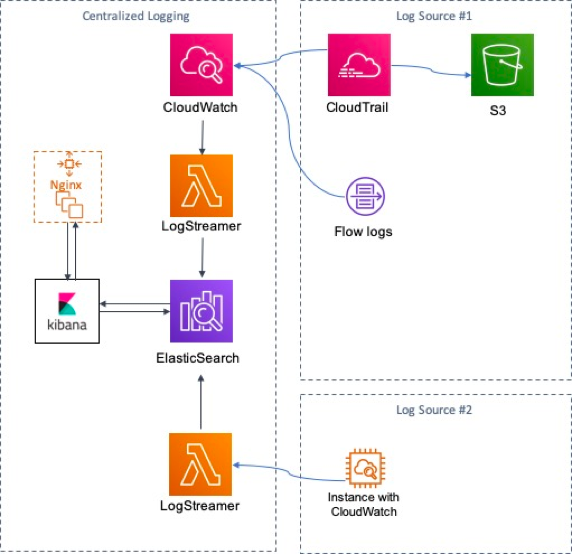
Amazon Web Services (AWS) provides service-specific operational metrics and log files to give customers insight into how the service is operating. Many AWS services also generate security log data, including audit logs for access, configuration changes, and billing events. In addition to AWS log data, 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.

## 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 Nginx reverse proxy 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.

# 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](https://aws.amazon.com/blogs/database/get-started-with-amazon-elasticsearch-service-set-cloudwatch-alarms-on-key-metrics/).

## Kibana Dashboard

Take advantage of [Kibana](https://www.elastic.co/guide/en/kibana/current/index.html) 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 1.1 uses the most up-to-date Node.js runtime. For more information, see [Runtime Support Policy](https://docs.aws.amazon.com/lambda/latest/dg/runtime-support-policy.html) in the *AWS Lambda Developer Guide*.

# 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:

[**centralized-logging-primary-china.template**](https://aws-solutions-reference.s3.cn-north-1.amazonaws.com.cn/aws-centralized-logging/v1.1/centralized-logging-primary-china.template): Use this template to launch the centralized logging solution and all associated components. The default configuration deploys an Amazon Elasticsearch Service domain.

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

[**centralized-logging-spoke-china.template**](https://aws-solutions-reference.s3.cn-north-1.amazonaws.com.cn/aws-centralized-logging/v1.1/centralized-logging-spoke-china.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-china.template**](https://aws-solutions-reference.s3.cn-north-1.amazonaws.com.cn/aws-centralized-logging/v1.1/centralized-logging-demo-china.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

## Step 1. Launch the Primary Stack

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

1. Sign in to the AWS Management Console and click the link to the right to launch the **[centralized- logging-primary-china](https://cn-northwest-1.console.amazonaws.cn/cloudformation/home?region=cn-northwest-1" \l "/stacks/new?&templateURL=https://aws-solutions-reference.s3.cn-north-1.amazonaws.com.cn/aws-centralized-logging/v1.1/centralized-logging-primary-china.template)** AWS CloudFormation template.
2. The template is launched in the China Ningxia (cn-northwest-1) 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. ‘Elasticsearch domain admin email’ and ‘Proxy Pass’ are user name and password for initial access to Kibana. ‘Key Pair’ is used to login into Nginx server for management, you should have at least one available key pair in launched region.
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.

1. To see details for the stack resources, choose the **Outputs** tab. The following table describes some of these outputs in more detail.

## 

## 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.

1. Sign in to the AWS Management Console and click the button to the right to launch the [**centralized-logging-spoke-china**](https://cn-northwest-1.console.amazonaws.cn/cloudformation/home?region=cn-northwest-1#/stacks/new?&templateURL=https://aws-solutions-reference.s3.cn-north-1.amazonaws.com.cn/aws-centralized-logging/v1.1/centralized-logging-spoke-china.template) AWS CloudFormation 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.
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 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.

1. When prompted, log in to the dashboard with the user name and password, which are input at Step 1.
2. In the left menu bar, choose **Management**.
3. Under **Configure an index pattern**, set the **Index name or pattern** field to cwl-

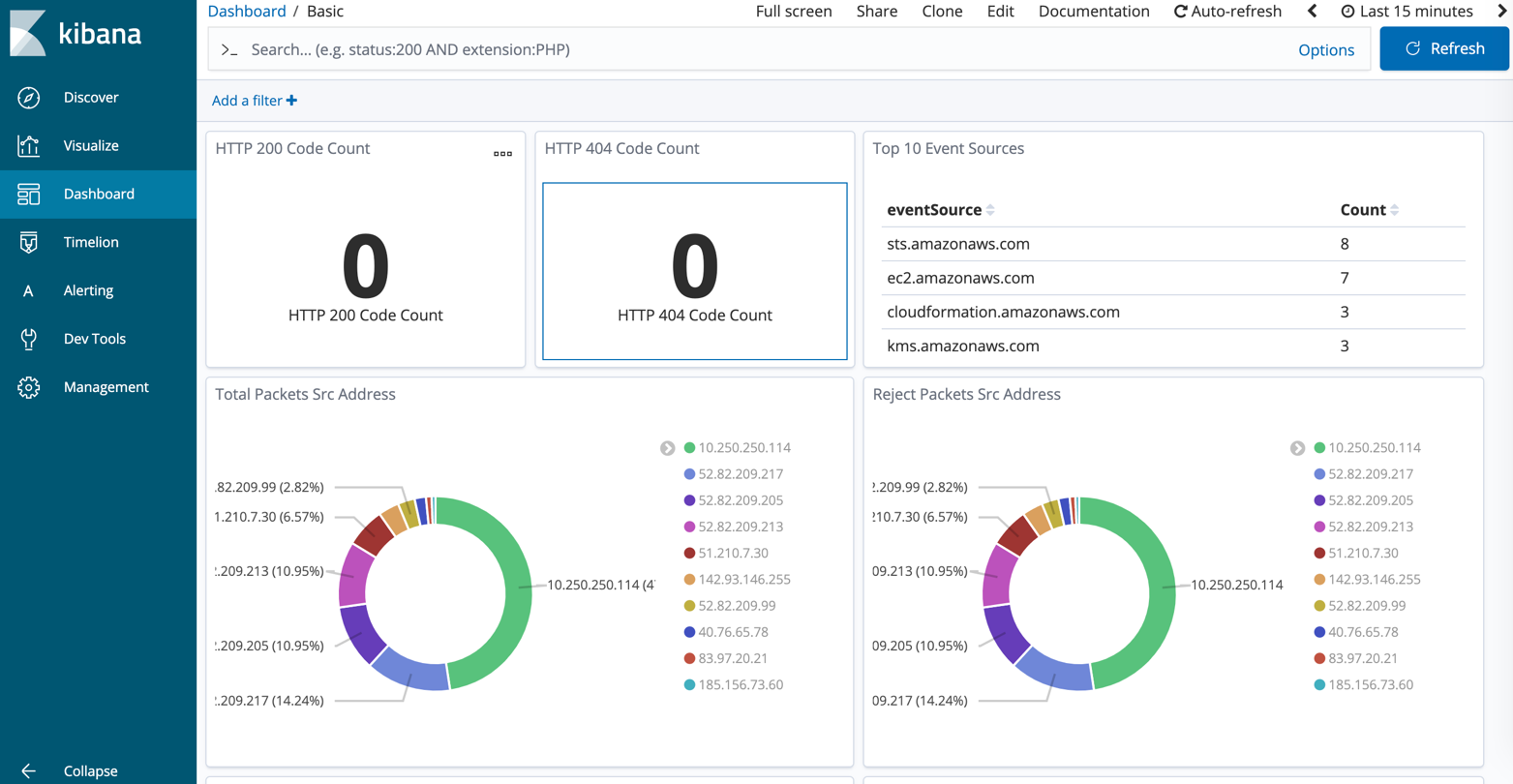
\*.

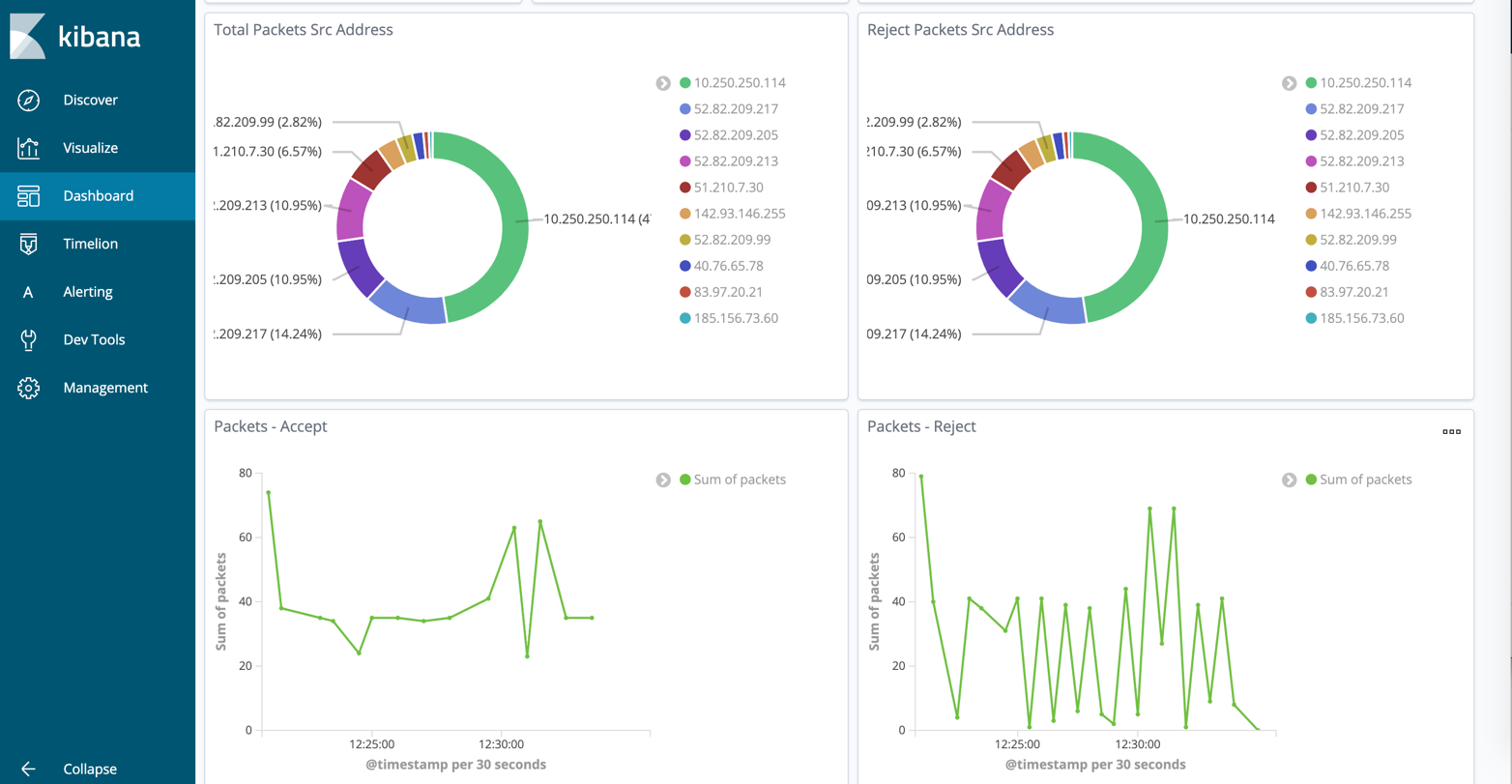
You should see the message box underneath change from red to green, confirming that there are matching indices and aliases.

1. Under **Time Filter field name**, choose **@timestamp**.
2. Choose **Create**. You will see a list of every field in the index.
3. 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.

1. In the **Saved Objects** tab under **Dashboards**, you should see a **Basic** dashboard. Choose the eye icon next to the dashboard to view it.
2. 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](https://www.elastic.co/guide/en/kibana/current/index.html).

# 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](http://aws.amazon.com/security/).

## 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.

# Document Revisions

|  |  |
| --- | --- |
| **Date** | **Change** |
| **April 2016** | Initial publication |

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

**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.](http://www.apache.org/licenses/LICENSE-2.0)