aws

Implementation Guide

# Centralized Logging on AWS

# Centralized Logging on AWS: Implementation Guide

# Table of Contents

# Centralized Logging on AWS

**Important**

Centralized Logging on AWS has been superseded by the Centralized Logging with OpenSearch solution, which helps you quickly build a centralized log analytics platform. We recommend migrating to this new solution if all of the following are true:

- You currently use the Centralized Logging on AWS solution
- You aren't using AWS GovCloud (US) Region deployments
- You aren't using cross-Region logging features

To migrate to the new solution, follow the steps outlined under Migrate to the Centralized Logging with OpenSearch solution.

# Migrate to the Centralized Logging with OpenSearch solution

**Time to migrate**: Approximately 60 minutes

In March 2023, a new AWS Solution, Centralized Logging with OpenSearch (referred to as the new solution), was released to make it easy for customers to build centralized log analytic platform with Amazon OpenSearch Service on AWS. If you are an existing user of the Centralized Logging on AWS solution (referred to as the legacy solution), we recommend that you consider migrating to the new solution because it offers more features than the legacy solution. For more information, refer to Comparison between the two solutions.

This migration guide outlines steps to reuse the Amazon OpenSearch Service domain provisioned by the legacy solution in the new solution, so you do not lose historical log data. If you do not need the historical log data, consider deleting all resources provisioned by the legacy solution, and use the implementation guide to launch the new solution.

> **Note**
>
> Don't upgrade to the new solution if you want to deploy in AWS GovCloud (US) Regions. Instead, continue using the legacy solution.

## Comparison between the two solutions

| Features | Supported by new solution? | Supported by legacy solution? |
|---|---|---|
| **Management** | | |
| Web Console | Yes | No |
| **Log source (AWS service logs)** | | |
| Amazon CloudTrail logs | Yes | Yes |
| VPC Flow Logs | Yes | Yes |

| Features | Supported by new solution? | Supported by legacy solution? |
|---|---|---|
| Amazon S3 access logs | Yes | No |
| AWS Config logs | Yes | No |
| Amazon CloudFront standard logs | Yes | No |
| Amazon CloudFront real-time logs | Yes | No |
| Application Load Balancer logs | Yes | No |
| AWS WAF logs | Yes | No |
| Amazon RDS Aurora/MySQL logs | Yes | No |
| AWS Lambda logs | Yes | No |
| **Log source (application logs)** | | |
| EC2 application logs | Yes | No |
| EKS pod logs | Yes | No |
| Syslog | Yes | No |
| **Log processor** | | |
| Predefined log parser - Apache | Yes | Yes |
| Predefined log parser - Nginx | Yes | No |
| Predefined log parser - Spring Boot | Yes | No |

| Features | Supported by new solution? | Supported by legacy solution? |
|---|---|---|
| Predefined pog parser - JSON | Yes | No |
| Predefined log parser - Regex (Single line and multiple lines) | No | No |
| Log enrichment - Geo to IP | Yes | No |
| Log enrichment - User agent parser | Yes | No |
| **Log agent** | | |
| Amazon CloudWatch Logs agent | No | Yes |
| FluentBit log agent | Yes | No |
| Automatic installation and monitoring | Yes | No |
| Automatic configuration | Yes | No |
| **Built-in OpenSearch dashboards** | | |
| Amazon CloudTrail logs | Yes | Yes |
| VPC Flow Logs | Yes | Yes |
| Amazon S3 access logs | Yes | No |
| AWS Config logs | Yes | No |
| Amazon CloudFront standard logs | Yes | No |
| Amazon CloudFront real-time logs | Yes | No |

| Features | Supported by new solution? | Supported by legacy solution? |
|---|---|---|
| Application Load Balancer logs | Yes | No |
| AWS WAF logs | Yes | No |
| Amazon RDS Aurora/MySQL logs | Yes | No |
| AWS Lambda logs | Yes | No |
| Nginx access logs | Yes | No |
| Apache HTTP Server access logs | Yes | No |
| **OpenSearch domain management** | | |
| Provision domain | No | Yes |
| Import existing domain | Yes | No |
| CloudWatch Alarms for domains | Yes | No |
| Index lifecycle management | Yes | No |
| Proxy stack (Nginx) | Yes | No |
| Jumpbox server (Windows) | No | Yes |
| **Supported AWS Regions** | | |
| AWS Standard Regions | Yes | Yes |
| AWS China Regions | Yes | No |
| GovCloud Region | No | Yes |

| Features | Supported by new solution? | Supported by legacy solution? |
|---|---|---|
| **Cross account and cross Region** | | |
| Cross-account log ingestion | Yes | Yes |
| Cross-Region log ingestion | Yes | Yes |
| **Authentication option** | | |
| Amazon Cognito user pool | Yes | Yes |
| OpenID Connect | Yes | No |
| **Network option** | | |
| Launch with new VPC | Yes | Yes |
| Launch with existing VPC | Yes | No |

# Migration overview

Both the new solution and legacy solution use OpenSearch Service as the log analytics engine. To migrate to the new solution, follow these steps:

- Step 1: Deploy the new solution
- Step 2: Upgrade the existing OpenSearch Service domains
- Step 3: Import the existing Amazon OpenSearch Service domain into the new solution
- Step 4: Create new log analytics pipelines using new solution
- Step 5 (Optional): Delete provisioned resources by the legacy solution

# Step 1: Deploy the new solution

Follow the Automated deployment steps to deploy the Centralized Logging with OpenSearch solution. You can choose deployment with Amazon Cognito user pools or OpenID Connect either in an existing VPC or in a new VPC.

## Step 2. Upgrade the existing OpenSearch Service domains

The legacy solution provisioned an OpenSearch Service domain with engine version Elasticsearch 7.7. To work with the new solution, upgrade the OpenSearch Service domain to OpenSearch 1.0 and above. The upgrade process takes about 30 minutes.

1. Sign in to the Amazon OpenSearch Service console.
2. Under **Domains**, select the `centralizedlogging` OpenSearch Service domain.

> **Note**
>
> `centralizedlogging` is the fixed name of the OpenSearch Service domain provisioned by the legacy solution.

3. Choose **Actions** on the top right corner, and select **Upgrade**.
4. Select **OpenSearch 1.3 (latest)** from the list.
5. Type **upgrade** in the text field, and choose **Upgrade**.

## Step 3: Import the existing OpenSearch Service domain into the new solution

After the domain has completed upgrading in step 2, you can import it into the new solution.

1. Go to the AWS CloudFormation console, and select the stack provisioned in Step 1: Deploy the new solution.
2. Choose the **Outputs** tab, and then select the value for **WebConsoleUrl**. The URL opens in your web browser.
3. Input the credentials, and choose **Sign In**. The email is the one you used when provisioning the new solution, and a temporary password will be sent to the email address. When you sign in to the system for the first time, you will be asked to set a new password.
4. After signing in to the Centralized Logging with OpenSearch console, select **Import OpenSearch Domain** in the left navigation bar.
5. Follow the steps to Import an Amazon OpenSearch Service domain.

## Step 4: Create new log analytics pipelines using the new solution

Use the new solution's web console to ingest either AWS service logs or application logs. Follow the steps in the AWS Services Logs and Application Logs sections to start creating new log pipelines.

The new log analytic pipelines create and use new indices in the OpenSearch Service domain. You cannot migrate the existing data with the new pipelines. However, you can choose to retain existing data by keeping the corresponding indices as needed.

## Step 5 (Optional): Delete provisioned resources by the legacy solution

The new solution can reuse the domains provisioned by the legacy solution. If you no longer need the legacy log analytic pipelines, go to CloudFormation console and delete the old stack. The OpenSearch Service domain and VPC will be retained after you delete the old stacks.

## FAQ

**Question: Can I migrate the existing data in Elasticsearch domain to work with the new pipeline?**

**Answer:** No. This is not supported. You can keep your existing data (index) in your Elasticsearch domain.

**Question: Do I have to delete the legacy solution from my AWS account when migrating to the new solution?**

**Answer:** You can delete the stack of the legacy solution from the CloudFormation console if you no longer need old log analytics pipelines. Note that the Elasticsearch domain and VPC will be retained after you delete the old stacks and can be used in the new solution.

**Question: Do I have to delete the Jumpbox server created in the legacy solution?**

**Answer:** It depends. In the legacy solution, you can choose to deploy a Jumpbox server to access the Kibana dashboard within the VPC. In the new version, we have introduced the Nginx proxy stack, which is a new way to access OpenSearch Dashboards. The new way requires that you have a custom domain name and the SSL certificate.

**Question: Can I reuse the Amazon Cognito user pool for OpenSearch Service to access the web console?**

**Answer:** The Amazon Cognito user pool in the legacy solution is used to access OpenSearch Dashboards. In the new solution, we also provision an Amazon Cognito user pool for authentication and authorization for the frontend web console and backend APIs by default. If you want to use the existing user pool, you can launch the new solution with OpenID Connect.

**Question: Can I deploy the new solution with the existing VPC created in the legacy solution?**

**Answer:** You can deploy the new solution with either a new VPC or using the existing VPC. VPC peering is required if you want to access the Elasticsearch domain in the existing VPC. The new solution requires at least two private subnets with NAT gateway. By default, the VPC created by the old solution doesn't have them, you might need to add NAT gateway to the VPC yourself.

**Question: I have already used CloudWatch Logs agent to collect logs from Amazon EC2, do I need to migrate?**

**Answer:** The new version uses Fluent Bit as the log agent to collect logs from Amazon EC2 instances, and it offers a web console to install, monitor, and configure log agents. If you want to ingest logs from Amazon EC2 with the new solution, follow the steps in the Application Logs section.

**Question: The new application log pipeline creates new Amazon Kinesis data streams, can I use the one created in the legacy solution?**

**Answer:** No. In the legacy solution, we use Firehose to consume the messages from Kinesis Data Streams. However, in the new solution, we have replaced the Firehose with an AWS Lambda based custom log processor. You must create new pipelines from the web console, but to avoid additional cost, you should delete the old Kinesis data streams if they are no longer used.

**Question: I already use the legacy solution to analyze VPC Flow Logs or AWS CloudTrail logs, do I need to migrate?**

**Answer:** We recommend that you migrate to the new solution, which supports both VPC Flow Logs and CloudTrail logs from Amazon Simple Storage Service (Amazon S3) and CloudWatch Logs. You must create new log analytics pipelines from the web console of the new solution. When the new pipelines are created, you can delete the legacy solution to avoid additional cost.

**Question: How can I consume CloudWatch custom logs using the new solution?**

**Answer:** You can use Firehose to subscribe CloudWatch Logs and transfer logs into Amazon S3. Complete the following steps to use the new solution to ingest logs from Amazon S3 to OpenSearch:

1. Create subscription filters with Firehose by following the instructions in Cross-account log data sharing using Kinesis Data Firehose.
2. Transfer your logs to Amazon S3 by following the instructions in Creating an Amazon Kinesis Data Firehose Delivery Stream.