# Table of Contents

- What is Amazon Elasticsearch Service? .......................................................... 1
  - Features of Amazon Elasticsearch Service .................................................. 1
  - Supported Elasticsearch versions ............................................................... 2
  - Pricing for Amazon ES .................................................................................. 3
  - Getting started with Amazon Elasticsearch Service ..................................... 3
  - Related services ........................................................................................... 3

- Getting started ................................................................................................ 5
  - Step 1: Create a domain ................................................................................ 5
  - Step 2: Upload data for indexing ................................................................. 6
    - Option 1: Upload a single document ......................................................... 6
    - Option 2: Upload multiple documents ...................................................... 6
  - Step 3: Search documents .......................................................................... 7
    - Search documents from the command line .............................................. 7
    - Search documents using Kibana ............................................................. 7
  - Step 4: Delete a domain .............................................................................. 8
  - Next steps .................................................................................................... 8

- Creating and managing domains ................................................................... 9
  - Creating Amazon ES domains ..................................................................... 9
    - Creating Amazon ES domains (console) ................................................. 9
    - Creating Amazon ES domains (AWS CLI) .............................................. 12
    - Creating Amazon ES domains (AWS SDKs) .......................................... 13
  - Configuring access policies ....................................................................... 13
  - Advanced options ....................................................................................... 13
  - Configuration changes .............................................................................. 14
    - Changes that cause blue/green deployments ....................................... 14
    - Changes that don't cause blue/green deployments .............................. 14
    - Initiating a configuration change ......................................................... 15
    - Charges for configuration changes ....................................................... 15

- Service software updates .......................................................................... 16
  - Notifications ............................................................................................... 17
    - Getting started with notifications ......................................................... 17
    - Notification types .................................................................................... 18
    - Notification severities .......................................................................... 18
    - Sample EventBridge event ..................................................................... 18
  - Configuring a multi-AZ domain ................................................................. 19
    - Shard distribution ................................................................................... 19
    - Dedicated master node distribution ....................................................... 21
    - Availability zone disruptions ............................................................... 21

- VPC support ................................................................................................. 22
  - Limitations .................................................................................................. 25
  - About access policies on VPC domains .................................................... 25
  - Testing VPC domains ................................................................................ 26
  - Prerequisites ............................................................................................... 27
  - Reserving IP addresses in a VPC subnet .................................................... 27
  - Service-linked role for VPC access ........................................................... 28
  - Migrating from public access to VPC access ............................................ 28

- Monitoring cluster metrics .......................................................................... 28
  - Interpreting health dashboards ................................................................. 28
  - Cluster metrics .......................................................................................... 30
  - Dedicated master node metrics ............................................................... 32
  - EBS volume metrics .................................................................................. 33
  - Instance metrics ....................................................................................... 34
  - UltraWarm metrics .................................................................................... 39
  - Cold storage metrics ................................................................................ 40
Take and upload the snapshot ................................................................. 307
Create a domain .................................................................................. 308
Provide permissions to the S3 bucket .................................................. 309
Restore the snapshot ........................................................................... 310
Creating a search application ............................................................... 312
Step 1: Index sample data ................................................................. 312
Step 2: Create the API in API Gateway ............................................. 313
Step 3: Create and deploy the Lambda function .............................. 314
Step 4: Modify the domain access policy ......................................... 316
Step 5: Test the web application ....................................................... 316
Next steps .......................................................................................... 318
Visualizing support calls .................................................................... 318
Step 1: Configure prerequisites ......................................................... 319
Step 2: Copy sample code ................................................................. 319
(Optional) Step 3: Index sample data ............................................... 322
Step 4: Analyze and visualize your data ............................................ 323
Step 5: Clean up resources and next steps ....................................... 327
Troubleshooting ................................................................................ 328
Can't access Kibana ............................................................................ 328
Can't access VPC domain ................................................................. 328
Cluster in read-only state ................................................................. 328
Red cluster status ............................................................................. 329
  Recovering from a continuous heavy processing load .................. 330
Yellow cluster status ......................................................................... 331
ClusterBlockException ....................................................................... 331
  Lack of available storage space .................................................... 331
  Blocked disks due to low memory .................................................. 332
JVM OutOfMemoryError .................................................................... 332
Failed cluster nodes .......................................................................... 332
Exceeded maximum shard limit ....................................................... 333
Can't enable audit logs ........................................................................ 333
Can't close index ............................................................................... 333
Mapper parsing exception while indexing ...................................... 334
Client license checks .......................................................................... 334
Request throttling ............................................................................. 334
Can't SSH into node .......................................................................... 334
"Not Valid for the Object's Storage Class" snapshot error .......... 335
Invalid host header ........................................................................... 335
Invalid M3 instance type ................................................................. 335
Hot queries stop working after enabling UltraWarm .................... 335
Can't downgrade after upgrade ......................................................... 336
Need summary of domains for all regions ..................................... 336
Browser error when using Kibana ..................................................... 336
Unauthorized operation after selecting VPC access ..................... 337
Stuck at loading after creating VPC domain ................................. 337
Can't connect from Alpine Linux .................................................... 337
Certificate error when using SDK ..................................................... 337
Configuration API reference ............................................................. 339
Actions ............................................................................................. 339
  AcceptInboundCrossClusterSearchConnection .............................. 341
  AddTags ....................................................................................... 341
  AssociatePackage ....................................................................... 342
  CreateElasticsearchDomain ....................................................... 342
  CreateOutboundCrossClusterSearchConnection ........................... 346
  CreatePackage .......................................................................... 347
  DeleteElasticsearchDomain ....................................................... 348
  DeleteElasticsearchServiceRole .................................................. 348
What is Amazon Elasticsearch Service?

Amazon Elasticsearch Service (Amazon ES) is a managed service that makes it easy to deploy, operate, and scale Elasticsearch clusters in the AWS Cloud. Elasticsearch is a popular open-source search and analytics engine for use cases such as log analytics, real-time application monitoring, and clickstream analysis. With Amazon ES, you get direct access to the Elasticsearch APIs; existing code and applications work seamlessly with the service.

Amazon ES provisions all the resources for your Elasticsearch cluster and launches it. It also automatically detects and replaces failed Elasticsearch nodes, reducing the overhead associated with self-managed infrastructures. You can scale your cluster with a single API call or a few clicks in the console.

To get started using Amazon ES, you create a domain. An Amazon ES domain is synonymous with an Elasticsearch cluster. Domains are clusters with the settings, instance types, instance counts, and storage resources that you specify. Each instance acts as one Elasticsearch node.

You can use the Amazon ES console to set up and configure a domain in minutes. If you prefer programmatic access, you can use the AWS CLI or the AWS SDKs.

Topics

• Features of Amazon Elasticsearch Service (p. 1)
• Supported Elasticsearch versions (p. 2)
• Pricing for Amazon Elasticsearch Service (p. 3)
• Getting started with Amazon Elasticsearch Service (p. 3)
• Related services (p. 3)

Features of Amazon Elasticsearch Service

Amazon ES includes the following features:

Scale

• Numerous configurations of CPU, memory, and storage capacity known as instance types, including cost-effective Graviton instances
• Up to 3 PB of attached storage
• Cost-effective UltraWarm (p. 222) storage for read-only data
• Cold storage (p. 231) for infrequently accessed data

Security

• AWS Identity and Access Management (IAM) access control
• Easy integration with Amazon VPC and VPC security groups
• Encryption of data at rest and node-to-node encryption
• Amazon Cognito, HTTP basic, or SAML authentication for Kibana
- Index-level, document-level, and field-level security
- Audit logs
- Kibana multi-tenancy

**Stability**
- Numerous geographical locations for your resources, known as *Regions* and *Availability Zones*
- Node allocation across two or three Availability Zones in the same AWS Region, known as *Multi-AZ*
- Dedicated master nodes to offload cluster management tasks
- Automated snapshots to back up and restore Amazon ES domains

**Flexibility**
- SQL support for integration with business intelligence (BI) applications
- Custom packages to improve search results

**Integration with Popular Services**
- Data visualization using Kibana
- Integration with Amazon CloudWatch for monitoring Amazon ES domain metrics and setting alarms
- Integration with AWS CloudTrail for auditing configuration API calls to Amazon ES domains
- Integration with Amazon S3, Amazon Kinesis, and Amazon DynamoDB for loading streaming data into Amazon ES
- Alerts from Amazon SNS when your data exceeds certain thresholds

---

**Supported Elasticsearch versions**

Amazon ES currently supports the following Elasticsearch versions:

- 7.10, 7.9, 7.8, 7.7, 7.4, 7.1
- 6.8, 6.7, 6.5, 6.4, 6.3, 6.2, 6.0
- 5.6, 5.5, 5.3, 5.1
- 2.3
- 1.5

Compared to earlier versions of Elasticsearch, the 7.x and 6.x versions offer powerful features that make them faster, more secure, and easier to use. Here are a few highlights:

- **Higher indexing performance** – Newer versions of Elasticsearch provide superior indexing capabilities that significantly increase the throughput of data updates.
- **Better safeguards** – Newer versions of Elasticsearch help prevent overly broad or complex queries from negatively affecting the performance and stability of the cluster.
- **Vega visualizations** – Kibana 6.2 and later versions support the *Vega* visualization language, which lets you make context-aware Elasticsearch queries, combine multiple data sources into a single graph, add user interactivity to graphs, and much more.
- **Java high-level REST client** – Compared to the low-level client, this client offers a simplified development experience and supports most Elasticsearch APIs. For a code example, see Signing HTTP Requests (p. 143).
For more information, see the section called “Supported Elasticsearch operations” (p. 277), the section called “Features by Elasticsearch version” (p. 273), and the section called “Plugins by Elasticsearch version” (p. 275).

If you start a new Elasticsearch project, we strongly recommend that you choose the latest supported Elasticsearch version. If you have an existing domain that uses an older Elasticsearch version, you can choose to keep the domain or migrate your data. For more information, see the section called “Upgrading Elasticsearch” (p. 61).

Pricing for Amazon Elasticsearch Service

For Amazon ES, you pay for each hour of use of an EC2 instance and for the cumulative size of any EBS storage volumes attached to your instances. Standard AWS data transfer charges also apply.

However, some notable data transfer exceptions exist. If a domain uses multiple Availability Zones (p. 19), Amazon ES does not bill for traffic between the Availability Zones. Significant data transfer occurs within a domain during shard allocation and rebalancing. Amazon ES neither meters nor bills for this traffic. Similarly, Amazon ES does not bill for data transfer between UltraWarm (p. 222)/cold (p. 231) nodes and Amazon S3.

For full pricing details, see Amazon Elasticsearch Service Pricing. For information about charges incurred during configuration changes, see the section called “Charges for configuration changes” (p. 15).

Getting started with Amazon Elasticsearch Service

To get started, sign up for an AWS account if you don’t already have one. After you are set up with an account, complete the Getting Started (p. 5) tutorial for Amazon Elasticsearch Service. Consult the following introductory topics if you need more information while learning about the service:

- Create a domain (p. 9)
- Size the domain (p. 263) appropriately for your workload
- Control access to your domain using a domain access policy (p. 77) or fine-grained access control (p. 90)
- Index data manually (p. 158) or from other AWS services (p. 160)
- Use Kibana (p. 216) to search your data and create visualizations

For information on migrating to Amazon ES from a self-managed Elasticsearch cluster, see the section called “Migrating to Amazon ES” (p. 307).

Related services

Amazon ES commonly is used with the following services:

Amazon CloudWatch

Amazon ES domains automatically send metrics to CloudWatch so that you can monitor domain health and performance. For more information, see Monitoring Amazon Elasticsearch Service cluster metrics with Amazon CloudWatch (p. 28).

CloudWatch Logs can also go the other direction. You might configure CloudWatch Logs to stream data to Amazon ES for analysis. To learn more, see the section called “Loading streaming data from Amazon CloudWatch” (p. 170).
AWS CloudTrail

Use AWS CloudTrail to get a history of the Amazon ES configuration API calls and related events for your account. For more information, see Monitoring Amazon Elasticsearch Service configuration API activity (p. 119).

Amazon Kinesis

Kinesis is a managed service for real-time processing of streaming data at a massive scale. For more information, see the section called “Loading streaming data from Amazon Kinesis Data Streams” (p. 165) and the section called “Loading streaming data from Amazon Kinesis Data Firehose” (p. 170).

Amazon S3

Amazon Simple Storage Service (Amazon S3) provides storage for the internet. This guide provides Lambda sample code for integration with Amazon S3. For more information, see the section called “Loading streaming data from Amazon S3” (p. 160).

AWS IAM

AWS Identity and Access Management (IAM) is a web service that you can use to manage access to your Amazon ES domains. For more information, see the section called “Identity and Access Management” (p. 77).

AWS Lambda

AWS Lambda is a compute service that lets you run code without provisioning or managing servers. This guide provides Lambda sample code to stream data from DynamoDB, Amazon S3, and Kinesis. For more information, see the section called “Loading streaming data into Amazon ES” (p. 160).

Amazon DynamoDB

Amazon DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. To learn more about streaming data to Amazon ES, see the section called “Loading streaming data from Amazon DynamoDB” (p. 167).

Amazon QuickSight

You can visualize data from Amazon ES using Amazon QuickSight dashboards. For more information, see Using Amazon Elasticsearch Service with Amazon QuickSight in the Amazon QuickSight User Guide.
Getting started with Amazon Elasticsearch Service

This tutorial shows you how to use Amazon Elasticsearch Service (Amazon ES) to create and configure a test domain. An Amazon ES domain is synonymous with an Elasticsearch cluster. Domains are clusters with the settings, instance types, instance counts, and storage resources that you specify.

This tutorial walks you through the basic steps to get an Amazon ES domain up and running quickly. For more detailed information, see Creating and managing domains (p. 9) and the other topics within this guide. For information on migrating to Amazon ES from a self-managed Elasticsearch cluster, see the section called “Migrating to Amazon ES” (p. 307).

You can complete the following steps by using the Amazon ES console, the AWS CLI, or the AWS SDK:

1. Create a domain (p. 5)
2. Upload data for indexing (p. 6)
3. Search documents (p. 7)
4. Delete a domain (p. 8)

For information about installing and setting up the AWS CLI, see the AWS Command Line Interface User Guide.

Step 1: Create an Amazon ES domain

Important
This is a concise tutorial for configuring a test Amazon Elasticsearch Service (Amazon ES) domain. Do not use this process to create production domains. For a comprehensive version of the same process, see Creating and managing domains (p. 9).

An Amazon ES domain is synonymous with an Elasticsearch cluster. Domains are clusters with the settings, instance types, instance counts, and storage resources that you specify. You can create an Amazon ES domain by using the console, the AWS CLI, or the AWS SDKs.

To create an Amazon ES domain using the console

1. Go to https://aws.amazon.com and choose Sign In to the Console.
2. Under Analytics, choose Elasticsearch Service.
3. Choose Create a new domain.
4. For the deployment type, choose Development and testing.
5. For Elasticsearch version, choose the latest version and then choose Next.
6. Provide a name for the domain. The examples in this tutorial use the name movies.
7. Ignore the Custom endpoint setting.
8. Under Data nodes, choose the t3.small.elasticsearch instance type with the default value of one node.
9. Ignore the rest of the settings for now and choose Next.
10. For simplicity in this tutorial, use a public access domain. Under Network configuration, choose Public access.
11. For **Fine-grained access control**, choose **Create master user**. Provide a user name and password.
12. For now, ignore the **SAML authentication** and **Amazon Cognito authentication** sections.
13. For **Domain access policy**, choose **Allow open access to the domain**. In this tutorial, fine-grained access control handles authentication, not the domain access policy.
14. Keep the encryption settings at their default values and choose **Next**.
15. Ignore the tags option and choose **Next**.
16. Confirm your domain configuration and choose **Confirm**. New domains typically take 15–30 minutes to initialize, but can take longer depending on the configuration. After your domain initializes, make note of its endpoint.

**Next:** Upload data to an Amazon ES domain for indexing (p. 6)

### Step 2: Upload data to Amazon ES for indexing

**Important**
This is a concise tutorial for uploading a small amount of test data to Amazon Elasticsearch Service (Amazon ES). For more about uploading data in a production domain, see Indexing data (p. 158).

You can upload data to an Amazon ES domain using the command line or most programming languages.

The following example requests use curl (a common HTTP client) for brevity and convenience. Clients like curl can’t perform the request signing that’s required if your access policies specify IAM users or roles. To successfully complete this process, you must use fine-grained access control with a primary user name and password like you configured in Step 1 (p. 5).

You can install curl on Windows and use it from the command prompt, but we recommend a tool like Cygwin or the Windows Subsystem for Linux. macOS and most Linux distributions come with curl preinstalled.

#### Option 1: Upload a single document

Run the following command to add a single document to the *movies* domain:

```bash
```

For a detailed explanation of this command and how to make signed requests to Amazon ES, see Indexing data (p. 158).

#### Option 2: Upload multiple documents

To upload a JSON file that contains multiple documents to an Amazon ES domain

1. Create a file called *bulk_movies.json*. Paste the following content into the file and add a trailing newline:

```json
{
   "index": {
      "_index": "movies", "_id": "2"
   }
```

API Version 2015-01-01
To search documents in an Amazon Elasticsearch Service (Amazon ES) domain, use the Elasticsearch search API. Alternatively, you can use Kibana (p. 216) to search documents in the domain.

**Search documents from the command line**

Run the following command to search the *movies* domain for the word *mars*:

```
curl -XGET -u 'master-user:master-user-password' 'domain-endpoint/movies/_search?q=mars&pretty=true'
```

If you used the bulk data on the previous page, try searching for *rebel* instead.

**Search documents using Kibana**

Kibana is a popular open source visualization tool designed to work with Elasticsearch. It provides a helpful user interface for you to search and monitor your indices.

To search documents from an Amazon ES domain using Kibana

1. Point your browser to the Kibana plugin for your Amazon ES domain. You can find the Kibana endpoint on your domain dashboard on the Amazon ES console. The URL follows this format:

   `domain-endpoint/_plugin/kibana/

2. Log in using your primary user name and password.
3. To use Kibana, you need to configure at least one index pattern. Kibana uses these patterns to identify which indices you want to analyze. Open the Kibana main menu, choose Stack
Step 4: Delete a domain

Management, choose Index Patterns, and then choose Create index pattern. For this tutorial, enter movies.

4. Choose Next step and then choose Create index pattern. After the index is created, you can view the various document fields such as actor and director.

5. To begin searching your data, open the main menu again and choose Discover.

6. In the search bar, enter mars if you uploaded a single document, or rebel if you uploaded multiple documents, and then press Enter. Note how the similarity score (_score) increases if you search for a more specific phrase such as mars attacks.

Next: Delete a domain  (p. 8)

Step 4: Delete an Amazon ES domain

Because the movies domain from this tutorial is for test purposes, make sure to delete it when you’re done experimenting to avoid incurring charges.

To delete an Amazon ES domain from the console

1. Sign in to the Amazon Elasticsearch Service console.
2. Under My domains in the navigation pane, select the movies domain.
3. Choose Actions and then choose Delete domain.
4. Choose Delete the domain and then choose Delete.

Next steps

Now that you know how to create a domain and index data, you might want to try some of the following exercises:

- Learn about more advanced options for creating a domain. For more information, see Creating and managing Amazon Elasticsearch Service domains (p. 9).
- Discover how to manage the indices in your domain. For more information, see Managing indices in Amazon Elasticsearch Service (p. 222).
- Try out one of the tutorials for working with Amazon Elasticsearch Service. For more information, see Amazon Elasticsearch service tutorials (p. 307).
Creating and managing Amazon Elasticsearch Service domains

This chapter describes how to create and manage Amazon Elasticsearch Service (Amazon ES) domains. An Amazon ES domain is synonymous with an Elasticsearch cluster. Domains are clusters with the settings, instance types, instance counts, and storage resources that you specify.

Unlike the brief instructions in the Getting Started (p. 5) tutorial, this chapter describes all options and provides relevant reference information. You can complete each procedure by using instructions for the Amazon ES console, the AWS Command Line Interface (AWS CLI), or the AWS SDKs.

Creating Amazon ES domains

This section describes how to create Amazon ES domains by using the Amazon ES console or by using the AWS CLI with the `create-elasticsearch-domain` command.

Creating Amazon ES domains (console)

Use the following procedure to create an Amazon ES domain by using the console.

**To create an Amazon ES domain (console)**

1. Go to https://aws.amazon.com, and then choose Sign In to the Console.
2. Under Analytics, choose Elasticsearch Service.
3. Choose Create a new domain.
4. For Choose deployment type, choose the option that best matches the purpose of your domain:
   - **Production** domains use Multi-AZ and dedicated master nodes for higher availability.
   - **Development and testing** domains use a single Availability Zone.
   - **Custom** domains let you choose from all configuration options.

   **Important**
   Different deployment types present different options on subsequent pages. These steps include all options (the Custom deployment type).

5. For Elasticsearch version, we recommend that you choose the latest version. For more information, see the section called “Supported Elasticsearch versions” (p. 2).
6. Choose Next.
7. For Elasticsearch domain name, enter a domain name. The name must meet the following criteria:
   - Unique to your account and Region
   - Starts with a lowercase letter
   - Contains between 3 and 28 characters
   - Contains only lowercase letters a-z, the numbers 0-9, and the hyphen (-)
8. If you want to use a custom endpoint rather than the standard one of https://search-mydomain-1a2a3a4a5a6a7a8a9a0a9a8a7a.us-east-1.es.amazonaws.com, choose Enable custom endpoint. Then provide a name and certificate. For more information, see the section called “Creating a custom endpoint” (p. 66).
9. For **Availability Zones**, choose 1-AZ, 2-AZ, or 3-AZ. For more information, see the section called “Configuring a multi-AZ domain” (p. 19).

10. For **Instance type**, choose an instance type for the data nodes. For more information, see Supported instance types in Amazon Elasticsearch Service (p. 272).

    **Note**
    Not all Availability Zones support all instance types. If you choose 3-AZ, we recommend choosing current-generation instance types such as R5 or I3.

11. For **Number of nodes**, choose the number of data nodes.

    For maximum values, see the section called “Cluster and instance limits” (p. 295). Single-node clusters are fine for development and testing, but should not be used for production workloads. For more guidance, see the section called “Sizing domains” (p. 263) and the section called “Configuring a multi-AZ domain” (p. 19).

12. For **Data nodes storage type**, choose either **Instance** (default) or **EBS**.

    For guidance on creating especially large domains, see Petabyte Scale (p. 267). If you choose **EBS**, the following options appear:

    a. For **EBS volume type**, choose an EBS volume type.

        If you choose **Provisioned IOPS (SSD)** for the EBS volume type, for **Provisioned IOPS**, enter the baseline IOPS performance that you want. For more information, see Amazon EBS volumes in the Amazon EC2 documentation.

    b. For **EBS storage size per node**, enter the size of the EBS volume that you want to attach to each data node.

        **EBS volume size** is per node. You can calculate the total cluster size for the Amazon ES domain by multiplying the number of data nodes by the EBS volume size. The minimum and maximum size of an EBS volume depends on both the specified EBS volume type and the instance type that it's attached to. To learn more, see EBS Volume Size Limits (p. 296).

13. (Optional) Enable or disable dedicated master nodes (p. 268). Dedicated master nodes increase cluster stability and are required for domains that have instance counts greater than 10. We recommend three dedicated master nodes for production domains.

    **Note**
    You can choose different instance types for your dedicated master nodes and data nodes. For example, you might select general purpose or storage-optimized instances for your data nodes, but compute-optimized instances for your dedicated master nodes.

14. (Optional) To enable UltraWarm storage (p. 222), choose **Enable UltraWarm data nodes**. Each instance type has a maximum amount of storage (p. 296) that it can address. Multiply that amount by the number of warm data nodes for the total addressable warm storage.

15. (Optional) To enable cold storage (p. 231), choose **Enable cold storage**. You must enable UltraWarm to enable cold storage.

16. (Optional) For domains running Elasticsearch 5.3 and later, **Automated snapshot start hour** has no effect. For more information about automated snapshots, see the section called “Creating index snapshots” (p. 51).

17. (Optional) Choose **Optional Elasticsearch cluster settings**. For a summary of these options, see the section called “Advanced options” (p. 13).

18. Choose **Next**.

19. In the **Network configuration** section, choose either **VPC access** or **Public access**. If you choose **Public access**, skip to the next step. If you choose **VPC access**, ensure that you have met the prerequisites (p. 27), and then do the following:

    a. For **VPC**, choose the ID of the VPC that you want to use.
Creating Amazon ES domains (console)

Note
The VPC and domain must be in the same AWS Region, and you must select a VPC with tenancy set to Default. Amazon ES does not yet support VPCs that use dedicated tenancy.

b. For Subnet, choose a subnet. If you enabled Multi-AZ, you must choose two or three subnets. Amazon ES will place a VPC endpoint and elastic network interfaces in the subnets.

Note
You must reserve sufficient IP addresses for the network interfaces in the subnet (or subnets). For more information, see Reserving IP addresses in a VPC subnet (p. 27).

c. For Security groups, choose the VPC security groups that need access to the Amazon ES domain. For more information, see the section called “VPC support” (p. 22).

d. For IAM role, keep the default role. Amazon ES uses this predefined role (also known as a service-linked role) to access your VPC and to place a VPC endpoint and network interfaces in the subnet of the VPC. For more information, see Service-linked role for VPC access (p. 28).

20. In the Fine-grained access control section, enable or disable fine-grained access control:

- If you want to use IAM for user management, choose Set IAM role as master user and specify the ARN for an IAM role.
- If you want to use the internal user database, choose Create a master user and specify a user name and password.

Whichever option you choose, the master user can access all indices in the cluster and all Elasticsearch APIs. For guidance on which option to choose, see the section called “Key concepts” (p. 95).

If you disable fine-grained access control, you can still control access to your domain by placing it within a VPC, applying a restrictive access policy, or both. You must enable node-to-node encryption and encryption at rest to use fine-grained access control.

Note
We strongly recommend enabling fine-grained access control to protect the data on your domain. Fine-grained access control provides security at the cluster, index, document, and field levels.

21. (Optional) If you want to use SAML authentication for Kibana, choose Prepare SAML authentication. After the domain is available, see the section called “SAML authentication for Kibana” (p. 123) for additional steps.

22. (Optional) If you want to use Amazon Cognito authentication for Kibana, choose Enable Amazon Cognito authentication.

- Choose the Amazon Cognito user pool and identity pool that you want to use for Kibana authentication. For guidance on creating these resources, see the section called “Amazon Cognito authentication for Kibana” (p. 128).

23. For Domain access policy, add the ARNs or IP addresses that you want or choose a preconfigured policy from the dropdown list. For more information, see the section called “Identity and Access Management” (p. 77) and the section called “About access policies on VPC domains” (p. 25).

Note
If you chose VPC access in step 18, IP-based policies are prohibited. Instead, you can use security groups to control which IP addresses can access the domain. For more information, see the section called “About access policies on VPC domains” (p. 25).

24. (Optional) To require that all requests to the domain arrive over HTTPS, select the Require HTTPS for all traffic to the domain check box.

25. (Optional) To enable node-to-node encryption, select the Node-to-node encryption check box. For more information, see the section called “Node-to-node encryption” (p. 76).
26. (Optional) To enable encryption of data at rest, select the **Enable encryption of data at rest** check box.

Select *(Default) aws/es* to have Amazon ES create a KMS encryption key on your behalf (or use the one that it already created). Otherwise, choose your own KMS encryption key from the **KMS master key** menu. For more information, see the section called “Encryption at rest” (p. 74).

27. Choose **Next**.

28. On the **Review** page, review your domain configuration, and then choose **Confirm**.

### Creating Amazon ES domains (AWS CLI)

Instead of creating an Amazon ES domain by using the console, you can use the AWS CLI. For syntax, see Amazon Elasticsearch Service in the **AWS CLI command reference**.

#### Example commands

This first example demonstrates the following Amazon ES domain configuration:

- Creates an Amazon ES domain named *mylogs* with Elasticsearch version 7.10
- Populates the domain with two instances of the *r6g.large.elasticsearch* instance type
- Uses a 100 GiB General Purpose (SSD) EBS volume for storage for each data node
- Allows anonymous access, but only from a single IP address: 192.0.2.0/32

```bash
aws es create-elasticsearch-domain --domain-name mylogs --elasticsearch-version 7.10 --elasticsearch-cluster-config "InstanceType=r6g.large.elasticsearch,InstanceCount=2 --ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=100 --access-policies '{"Version": "2012-10-17", "Statement": [{"Action": "es:*", "Principal": "+", "Effect": "Allow", "Condition": {"IpAddress": ["192.0.2.0/32"]}}]}'
```

The next example demonstrates the following Amazon ES domain configuration:

- Creates an Amazon ES domain named *mylogs* with Elasticsearch version 7.10
- Populates the domain with six instances of the *r6g.large.elasticsearch* instance type
- Uses a 100 GiB General Purpose (SSD) EBS volume for storage for each data node
- Restricts access to the service to a single user, identified by the user’s AWS account ID: 555555555555
- Distributes instances across three Availability Zones

```bash
```

The next example demonstrates the following Amazon ES domain configuration:

- Creates an Amazon ES domain named *mylogs* with Elasticsearch version 7.10
- Populates the domain with ten instances of the *r6g.xlarge.elasticsearch* instance type
- Populates the domain with three instances of the *r6g.large.elasticsearch* instance type to serve as dedicated master nodes

```bash
```
• Uses a 100 GiB Provisioned IOPS EBS volume for storage, configured with a baseline performance of 1000 IOPS for each data node
• Restricts access to a single user and to a single subresource, the `_search` API

```
aws es create-elasticsearch-domain --domain-name mylogs --
elasticsearch-version 7.10 --elasticsearch-cluster-config
  InstanceType=r6g.xlarge.elasticsearch,InstanceCount=10,DedicatedMasterEnabled=true,DedicatedMasterType=r6g.large.elasticsearch,DedicatedMasterCount=3
  --ebs-options EBSEnabled=true,VolumeType=io1,VolumeSize=100,Iops=1000 --access-policies
  '{"Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS":
  east-1:555555555555:domain/mylogs/_search" } ] }'
```

**Note**
If you attempt to create an Amazon ES domain and a domain with the same name already exists, the CLI does not report an error. Instead, it returns details for the existing domain.

Creating Amazon ES domains (AWS SDKs)

The AWS SDKs (except the Android and iOS SDKs) support all the actions defined in the Amazon ES configuration API reference (p. 339), including `CreateElasticsearchDomain`. For sample code, see the section called "Using the AWS SDKs" (p. 153). For more information about installing and using the AWS SDKs, see AWS Software Development Kits.

Configuring access policies

Amazon Elasticsearch Service offers several ways to configure access to your Amazon ES domains. For more information, see the section called "Identity and Access Management" (p. 77) and the section called "Fine-grained access control" (p. 90).

The console provides preconfigured access policies that you can customize for the specific needs of your domain. You also can import access policies from other Amazon ES domains. For information about how these access policies interact with VPC access, see the section called "About access policies on VPC domains" (p. 25).

**To configure access policies (console)**

1. Go to [https://aws.amazon.com](https://aws.amazon.com), and then choose **Sign In to the Console**.
2. Under **Analytics**, choose **Elasticsearch Service**.
3. In the navigation pane, under **My domains**, choose the domain that you want to update.
4. Choose **Actions** and **Modify access policy**.
5. Edit the access policy JSON, or use the dropdown list to choose a preconfigured option.
6. Choose **Submit**.

Advanced options

Use advanced options to configure the following:

`rest.action.multi.allow_explicit_index`

Specifies whether explicit references to indices are allowed inside the body of HTTP requests. Setting this property to `false` prevents users from bypassing access control for subresources. By
default, the value is true. For more information, see the section called “Advanced options and API considerations” (p. 88).

**indices.fielddata.cache.size**

Specifies the percentage of Java heap space that is allocated to field data. By default, this setting is 20% of the JVM heap.

**Note**

Many customers query rotating daily indices. We recommend that you begin benchmark testing with `indices.fielddata.cache.size` configured to 40% of the JVM heap for most of these use cases. For very large indices, you might need a large field data cache.

**indices.query.bool.max_clause_count**

Specifies the maximum number of clauses allowed in a Lucene boolean query. The default is 1,024. Queries with more than the permitted number of clauses result in a `TooManyClauses` error. For more information, see the Lucene documentation.

### Making configuration changes in Amazon ES

Amazon ES uses a blue/green deployment process when updating domains. Blue/green typically refers to the practice of running two production environments, one live and one idle, and switching the two as you make software changes. In the case of Amazon ES, it refers to the practice of creating a new environment for domain updates and routing users to the new environment after those updates are complete. The practice minimizes downtime and maintains the original environment in the event that deployment to the new environment is unsuccessful.

#### Changes that cause blue/green deployments

The following operations cause blue/green deployments:

- Changing instance type
- If your domain doesn't have dedicated master nodes, changing data instance count
- Enabling or disabling dedicated master nodes
- Changing dedicated master node count
- Enabling or disabling Multi-AZ
- Changing storage type, volume type, or volume size
- Choosing different VPC subnets
- Adding or removing VPC security groups
- Enabling or disabling Amazon Cognito authentication for Kibana
- Choosing a different Amazon Cognito user pool or identity pool
- Modifying advanced settings
- Enabling or disabling the publication of error logs, audit logs, or slow logs to CloudWatch
- Upgrading to a new Elasticsearch version
- Enabling or disabling Require HTTPS
- Enabling encryption of data at rest or node-to-node encryption
- Enabling or disabling UltraWarm or cold storage
- Disabling auto-tune and rolling back its changes

#### Changes that don't cause blue/green deployments

In most cases, the following operations do not cause blue/green deployments:
• Changing access policy
• Changing the automated snapshot hour
• Enabling auto-tune or disabling it without rolling back its changes
• If your domain has dedicated master nodes, changing data node or UltraWarm node count

There are some exceptions. For example, if you haven’t reconfigured your domain since the launch of three Availability Zone support, Amazon ES might perform a one-time blue/green deployment to redistribute your dedicated master nodes across Availability Zones.

### Initiating a configuration change

When you initiate a configuration change, the domain state changes to **Processing** while Amazon ES creates a new environment with the latest service software (p. 16). During certain service software updates, the state remains **Active**. In both cases, you can review the cluster health and Amazon CloudWatch metrics and see that the number of nodes in the cluster temporarily increases—often doubling—while the domain update occurs. In the following illustration, you can see the number of nodes doubling from 11 to 22 during a configuration change and returning to 11 when the update is complete.

This temporary increase can strain the cluster’s dedicated master nodes (p. 268), which suddenly might have many more nodes to manage. It’s important to maintain sufficient capacity on dedicated master nodes to handle the overhead that is associated with these blue/green deployments.

**Important**

You do **not** incur any additional charges during configuration changes and service maintenance. You are billed only for the number of nodes that you request for your cluster. For specifics, see the section called “Charges for configuration changes” (p. 15).

To prevent overloading dedicated master nodes, you can monitor usage with the Amazon CloudWatch metrics (p. 28). For recommended maximum values, see the section called “Recommended CloudWatch alarms” (p. 270).

### Charges for configuration changes

If you change the configuration for a domain, Amazon ES creates a new cluster as described in the section called “Configuration changes” (p. 14). During the migration of old to new, you incur the following charges:

• If you change the instance type, you’re charged for both clusters for the first hour. After the first hour, you’re only charged for the new cluster. EBS volumes aren’t charged twice because they’re part of your cluster, so their billing follows instance billing.

  **Example:** You change the configuration from three `m3.xlarge` instances to four `m4.large` instances. For the first hour, you are charged for both clusters `(3 * m3.xlarge + 4 * m4.large)`. After the first hour, you are charged only for the new cluster `(4 * m4.large)`.

• If you don’t change the instance type, you are charged only for the largest cluster for the first hour. After the first hour, you are charged only for the new cluster.
**Example:** You change the configuration from six m3.xlarge instances to three m3.xlarge instances. For the first hour, you are charged for the largest cluster (6 * m3.xlarge). After the first hour, you are charged only for the new cluster (3 * m3.xlarge).

### Service software updates in Amazon Elasticsearch Service

*Note*  
Service software updates differ from Elasticsearch version upgrades. For information about upgrading to a later version of Elasticsearch, see the section called “Upgrading Elasticsearch” (p. 61).

Amazon Elasticsearch Service (Amazon ES) regularly releases system software updates that add features or otherwise improve your domains. The **Notifications** panel in the console is the easiest way to see if an update is available or check the status of an update. For more information about notifications, see the section called “Notifications” (p. 17). You can also receive these notifications through Amazon EventBridge.

Each notification includes details about the service software update. The notification severity is **Informational** if the update is optional and **High** if it's required. Consider the following when deciding whether to update your domain:

- If you take no action on required updates, Amazon ES still updates your domain service software automatically after a certain timeframe (typically two weeks). In this situation, Amazon ES sends notifications when it starts the update and when the update is complete.
- If you start an update manually, Amazon ES doesn't send a notification when it starts the update, only when the update is complete.

Manually updating your domain lets you take advantage of new features more quickly. When you choose **Update**, Amazon ES places the request in a queue and begins the update when it has time (typically within minutes). Consider updating your domain at a low traffic time. Your domain is ineligible for a service software update if it's in any of the following states:

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain in processing</td>
<td>The domain is in the middle of a configuration change. Check update eligibility after the operation completes.</td>
</tr>
<tr>
<td>Red cluster status</td>
<td>One or more indices in the cluster is red. For troubleshooting steps, see the section called “Red cluster status” (p. 329).</td>
</tr>
<tr>
<td>High error rate</td>
<td>The Elasticsearch cluster is returning a large number of 5xx errors when attempting to process requests. This problem is usually the result of too many simultaneous read or write requests. Consider reducing traffic to the cluster or scaling your domain.</td>
</tr>
<tr>
<td>Split brain</td>
<td><strong>Split brain</strong> means your Elasticsearch cluster has more than one master node and has split into two clusters that never will rejoin on their own. You can avoid split brain by using the recommended number of dedicated master nodes (p. 268). For help recovering from split brain, contact AWS Support.</td>
</tr>
<tr>
<td>Amazon Cognito integration issue</td>
<td>Your domain uses authentication for Kibana (p. 128), and Amazon ES can't find one or more Amazon Cognito resources. This problem usually occurs if</td>
</tr>
</tbody>
</table>
### Notifications

Notifications in Amazon Elasticsearch Service (Amazon ES) currently contain information about available software updates and Auto-Tune events for your domains. In the future, they might also include performance optimization recommendations such as moving to the correct instance type for a domain or rebalancing shards to reduce performance bottlenecks.

You can view notifications in the Notifications panel of the Amazon ES console or in Amazon EventBridge, but not in the AWS Personal Health Dashboard. They're available for all versions of Elasticsearch, with some minor exceptions.

#### Getting started with notifications

Notifications are enabled automatically when you create a domain. Go to the Notifications panel of the Amazon ES console to monitor and acknowledge notifications. Each notification includes information such as the time it was posted, the domain it relates to, a severity and status level, and a brief explanation. You can view historical notifications for up to 90 days in the console.

---

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Cognito user pool is missing</td>
<td>To correct the issue, recreate the missing resource and configure the Amazon ES domain to use it.</td>
</tr>
<tr>
<td>Other Amazon ES service issue</td>
<td>Issues with Amazon ES itself might cause your domain to display as ineligible for an update. If none of the previous conditions apply to your domain and the problem persists for more than a day, contact AWS Support.</td>
</tr>
</tbody>
</table>

---

### To request a service software update (console)

1. Go to [https://aws.amazon.com](https://aws.amazon.com) and choose **Sign In to the Console**.
2. Under **Analytics**, choose **Elasticsearch Service**.
3. In the navigation pane, under **My domains**, choose the domain you want to update.
4. For **Service software release**, follow the documentation link to compare your current version to the latest version. Then choose **Update**.

### To request a service software update (AWS CLI and AWS SDKs)

You can use the following commands to see if an update is available, check upgrade eligibility, and request an update:

- `describe-elasticsearch-domain` (**DescribeElasticsearchDomain**)
- `start-elasticsearch-service-software-update` (**StartElasticsearchServiceSoftwareUpdate**)

For more information, see the [AWS CLI Command Reference](https://docs.aws.amazon.com/cli/latest/reference/elasticsearch-domain/) and [Configuration API reference](https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/awscfg-api.html) (p. 339).

**Tip**

After requesting an update, you might have a narrow window of time in which you can cancel it. The duration of this `PENDING_UPDATE` state can vary greatly and depends on your AWS region and the number of concurrent updates Amazon ES is performing. To cancel, use the console or `stop-elasticsearch-service-software-update` (**StopElasticsearchServiceSoftwareUpdate**) command.
Notification types

At this time, all notifications in Amazon ES are informational, which relate to any action you’ve already taken or the operations of your domain. In the future, Amazon ES might also include actionable notifications, which will require you to take specific actions such as applying a mandatory security patch.

Notification severities

Each notification has a severity associated with it. Currently, all available notifications have a severity of Informational, while future ones might be Low, Medium, High, or Critical. See the following table for a summary of notification severities:

<table>
<thead>
<tr>
<th>Severity</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
</table>
| Informational | Information related to the operation of your domain.                     | • Service software update available  
|             |                                                                          | • Auto-Tune event                                  |
| Low        | A recommended action, but has no adverse impact on domain availability or performance if no action is taken. | N/A                                               |
| Medium     | There might be an impact if the recommended action is not taken, but comes with an extended time window for the action to be taken. | N/A                                               |
| High       | Urgent action is required to avoid adverse impact.                        | N/A                                               |
| Critical   | Immediate action is required to avoid adverse impact, or to recover from it. | N/A                                               |

Sample EventBridge event

The following example shows an Amazon ES notification event sent to Amazon EventBridge. The corresponding notification has a severity of Informational because the update is optional:

```json
{
    "version": "7.9",
    "id": "01234567-0123-0123-0123-012345678901",
    "detail-type": "Service Updates",
    "source": "aws.es",
    "account": "123456789012",
    "time": "2016-11-01T13:12:22Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:es:us-east-1:123456789012:domain/test-domain"
    ],
    "detail": {
        "event": "service_software_update",
        "status": "optional",
        "Severity": "informational",
```

API Version 2015-01-01
Configuring a multi-AZ domain in Amazon Elasticsearch Service

To prevent data loss and minimize Amazon Elasticsearch Service (Amazon ES) cluster downtime in the event of a service disruption, you can distribute nodes across two or three Availability Zones in the same Region, a configuration known as Multi-AZ. Availability Zones are isolated locations within each AWS Region.

For domains that run production workloads, we recommend the following configuration:

- Choose a Region that supports three Availability Zones with Amazon ES.
- Deploy the domain across three zones.
- Choose current-generation instance types for dedicated master nodes and data nodes.
- Use three dedicated master nodes and at least three data nodes.
- Create at least one replica for each index in your cluster.

The rest of this section provides explanations for and context around these recommendations.

**Shard distribution**

If you enable Multi-AZ, you should create at least one replica for each index in your cluster. Without replicas, Amazon ES can't distribute copies of your data to other Availability Zones, which largely defeats the purpose of Multi-AZ. Fortunately, the default configuration for any index is a replica count of 1. As the following diagram shows, Amazon ES makes a best effort to distribute primary shards and their corresponding replica shards to different zones.
In addition to distributing shards by Availability Zone, Amazon ES distributes them by node. Still, certain domain configurations can result in imbalanced shard counts. Consider the following domain:

- 5 data nodes
- 5 primary shards
- 2 replicas
- 3 Availability Zones

In this situation, Amazon ES has to overload one node in order to distribute the primary and replica shards across the zones, as shown in the following diagram.

To avoid these kinds of situations, which can strain individual nodes and hurt performance, we recommend that you choose an instance count that is a multiple of three if you plan to have two or more replicas per index.
Dedicated master node distribution

Even if you select two Availability Zones when configuring your domain, Amazon ES automatically distributes dedicated master nodes (p. 268) across three Availability Zones. This distribution helps prevent cluster downtime if a zone experiences a service disruption. If you use the recommended three dedicated master nodes and one Availability Zone goes down, your cluster still has a quorum (2) of dedicated master nodes and can elect a new master. The following diagram demonstrates this configuration.

This automatic distribution has some notable exceptions:

- If you choose an older-generation instance type that is not available in three Availability Zones, the following scenarios apply:
  - If you chose three Availability Zones for the domain, Amazon ES throws an error. Choose a different instance type, and try again.
  - If you chose two Availability Zones for the domain, Amazon ES distributes the dedicated master nodes across two zones.
- Not all AWS Regions have three Availability Zones. In these Regions, you can only configure a domain to use two zones (and Amazon ES can only distribute dedicated master nodes across two zones).

Availability zone disruptions

Availability Zone disruptions are rare, but do occur. The following table lists different Multi-AZ configurations and behaviors during a disruption.

<table>
<thead>
<tr>
<th>Number of Availability Zones in a Region</th>
<th>Number of Availability Zones That You Chose</th>
<th>Number of Dedicated Master Nodes</th>
<th>Behavior if One Availability Zone Experiences a Disruption</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 or more</td>
<td>2</td>
<td>0</td>
<td>Downtime. Your cluster loses half of its data nodes and must replace at least one in the</td>
</tr>
</tbody>
</table>
### Number of Availability Zones in a Region

<table>
<thead>
<tr>
<th>Number of Availability Zones in a Region</th>
<th>Number of Availability Zones That You Chose</th>
<th>Number of Dedicated Master Nodes</th>
<th>Behavior if One Availability Zone Experiences a Disruption</th>
</tr>
</thead>
</table>
| 2                                       | 2                                         | 3                               | 50/50 chance of downtime. Amazon ES distributes two dedicated master nodes into one Availability Zone and one into the other:  
  • If the Availability Zone with one dedicated master node experiences a disruption, the two dedicated master nodes in the remaining Availability Zone can elect a master.  
  • If the Availability Zone with two dedicated master nodes experiences a disruption, the cluster is unavailable until the remaining Availability Zone can add a dedicated master node and elect a master. |
| 3 or more                               | 2                                         | 3                               | No downtime. Amazon ES automatically distributes the dedicated master nodes across three Availability Zones, so the remaining two dedicated master nodes can elect a master. |
| 3 or more                               | 3                                         | 0                               | No downtime. Roughly two-thirds of your data nodes are still available to elect a master. |
| 3 or more                               | 3                                         | 3                               | No downtime. The remaining two dedicated master nodes can elect a master. |

In all configurations, regardless of the cause, node failures can cause the cluster's remaining data nodes to experience a period of increased load while Amazon ES automatically configures new nodes to replace the now-missing ones.

For example, in the event of an Availability Zone disruption in a three-zone configuration, two-thirds as many data nodes have to process just as many requests to the cluster. As they process these requests, the remaining nodes are also replicating shards onto new nodes as they come online, which can further impact performance. If availability is critical to your workload, consider adding resources to your cluster to alleviate this concern.

**Note**

Amazon ES manages Multi-AZ domains transparently, so you can't manually simulate Availability Zone disruptions.

---

### Launching your Amazon Elasticsearch Service domains using a VPC

You can launch AWS resources, such as Amazon Elasticsearch Service (Amazon ES) domains, into a virtual private cloud (VPC). A VPC is a virtual network that's dedicated to your AWS account. It's logically isolated from other virtual networks in the AWS Cloud.
Placing an Amazon ES domain within a VPC enables secure communication between Amazon ES and other services within the VPC without the need for an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within a VPC have an extra layer of security when compared to domains that use public endpoints.

To support VPCs, Amazon ES places an endpoint into one, two, or three subnets of your VPC. If you enable multiple Availability Zones (p. 19) for your domain, each subnet must be in a different Availability Zone in the same region. If you only use one Availability Zone, Amazon ES places an endpoint into only one subnet.

The following illustration shows the VPC architecture for one Availability Zone.

The following illustration shows the VPC architecture for two Availability Zones.
Amazon ES also places an *elastic network interface* (ENI) in the VPC for each of your data nodes. Amazon ES assigns each ENI a private IP address from the IPv4 address range of your subnet. The service also assigns a public DNS hostname (which is the domain endpoint) for the IP addresses. You must use a public DNS service to resolve the endpoint (which is a DNS hostname) to the appropriate IP addresses for the data nodes:

- If your VPC uses the Amazon-provided DNS server by setting the `enableDnsSupport` option to `true` (the default value), resolution for the Amazon ES endpoint will succeed.
- If your VPC uses a private DNS server and the server can reach the public authoritative DNS servers to resolve DNS hostnames, resolution for the Amazon ES endpoint will also succeed.

Because the IP addresses might change, you should resolve the domain endpoint periodically so that you can always access the correct data nodes. We recommend that you set the DNS resolution interval to one minute. If you’re using a client, you should also ensure that the DNS cache in the client is cleared.

**Note**
Amazon ES doesn't support IPv6 addresses with a VPC. You can use a VPC that has IPv6 enabled, but the domain will use IPv4 addresses.

**Topics**
- Limitations (p. 25)
- About access policies on VPC domains (p. 25)
- Testing VPC domains (p. 26)
- Before you begin: prerequisites for VPC access (p. 27)
Limitations

Currently, operating an Amazon ES domain within a VPC has the following limitations:

- You can either launch your domain within a VPC or use a public endpoint, but you can't do both. You must choose one or the other when you create your domain.
- If you launch a new domain within a VPC, you can't later switch it to use a public endpoint. The reverse is also true: If you create a domain with a public endpoint, you can't later place it within a VPC. Instead, you must create a new domain and migrate your data.
- You can't launch your domain within a VPC that uses dedicated tenancy. You must use a VPC with tenancy set to Default.
- After you place a domain within a VPC, you can't move it to a different VPC. However, you can change the subnets and security group settings.
- Compared to public domains, VPC domains display less information in the Amazon ES console. Specifically, the Cluster health tab does not include shard information, and the Indices tab is not present at all.
- To access the default installation of Kibana for a domain that resides within a VPC, users must have access to the VPC. This process varies by network configuration, but likely involves connecting to a VPN or managed network or using a proxy server or transit gateway. To learn more, see the section called “About access policies on VPC domains” (p. 25), the Amazon VPC User Guide, and the section called “Controlling access to Kibana” (p. 216).

About access policies on VPC domains

Placing your Amazon ES domain within a VPC provides an inherent, strong layer of security. When you create a domain with public access, the endpoint takes the following form:

https://search-domain-name-identifier.region.es.amazonaws.com

As the "public" label suggests, this endpoint is accessible from any internet-connected device, though you can (and should) control access to it (p. 77). If you access the endpoint in a web browser, you might receive a Not Authorized message, but the request reaches the domain.

When you create a domain with VPC access, the endpoint looks similar to a public endpoint:

https://vpc-domain-name-identifier.region.es.amazonaws.com

If you try to access the endpoint in a web browser, however, you might find that the request times out. To perform even basic GET requests, your computer must be able to connect to the VPC. This connection often takes the form of a VPN, transit gateway, managed network, or proxy server. For details on the various forms it can take, see Scenarios and Examples in the Amazon VPC User Guide. For a development-focused example, see the section called “Testing VPC domains” (p. 26).

In addition to this connectivity requirement, VPCs let you manage access to the domain through security groups. For many use cases, this combination of security features is sufficient, and you might feel comfortable applying an open access policy to the domain.
Operating with an open access policy does not mean that anyone on the internet can access the Amazon ES domain. Rather, it means that if a request reaches the Amazon ES domain and the associated security groups permit it, the domain accepts the request without further security checks.

For an additional layer of security, we recommend using fine-grained access control or an access policy that specifies IAM users or roles. In these situations, for the domain to accept a request, the security groups must permit it and it must be signed with valid credentials.

**Note**
Because security groups already enforce IP-based access policies, you can't apply IP-based access policies to Amazon ES domains that reside within a VPC. If you use public access, IP-based policies are still available.

### Testing VPC domains

The enhanced security of a VPC can make connecting to your domain and running basic tests a real challenge. If you already have an Amazon ES VPC domain and would rather not create a VPN server, try the following process:

1. For your domain's access policy, choose **Allow open access to the domain**. You can always update this setting after you finish testing.
2. Create an Amazon Linux Amazon EC2 instance in the same VPC, subnet, and security group as your Amazon ES domain.

   Because this instance is for testing purposes and needs to do very little work, choose an inexpensive instance type like `t2.micro`. Assign the instance a public IP address and either create a new key pair or choose an existing one. If you create a new key, download it to your `~/.ssh` directory.

   To learn more about creating instances, see [Getting Started with Amazon EC2 Linux Instances](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/).  
3. Add an internet gateway to your VPC.
4. In the route table for your VPC, add a new route. For **Destination**, specify a CIDR block that contains your computer's public IP address. For **Target**, specify the internet gateway you just created.

   For example, you might specify `123.123.123.123/32` for just your computer or `123.123.123.0/24` for a range of computers.

5. For the security group, specify two inbound rules:

<table>
<thead>
<tr>
<th>Type</th>
<th>Protocol</th>
<th>Port Range</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH (22)</td>
<td>TCP (6)</td>
<td>22</td>
<td><code>your-cidr-block</code></td>
</tr>
<tr>
<td>HTTPS (443)</td>
<td>TCP (6)</td>
<td>443</td>
<td><code>your-security-group-id</code></td>
</tr>
</tbody>
</table>

   The first rule lets you SSH into your EC2 instance. The second allows the EC2 instance to communicate with the Amazon ES domain over HTTPS.

6. From the terminal, run the following command:

   ```bash
   ssh -i ~/.ssh/your-key.pem ec2-user@your-ec2-instance-public-ip -N -L 9200:vpc-your-amazon-es-domain.region.es.amazonaws.com:443
   ```

   This command creates an SSH tunnel that forwards requests to `https://localhost:9200` to your Amazon ES domain through the EC2 instance. By default, Elasticsearch listens for traffic on port 9200. Specifying this port simulates a local Elasticsearch install, but use whichever port you'd like.
The command provides no feedback and runs indefinitely. To stop it, press Ctrl + C.


Alternately, you can send requests to https://localhost:9200 using curl, Postman, or your favorite programming language.

**Tip**
If you encounter curl errors due to a certificate mismatch, try the `--insecure` flag.

**Before you begin: prerequisites for VPC access**

Before you can enable a connection between a VPC and your new Amazon ES domain, you must do the following:

- **Create a VPC**
  
  To create your VPC, you can use the Amazon VPC console, the AWS CLI, or one of the AWS SDKs. For more information, see Working with VPCs in the Amazon VPC User Guide. If you already have a VPC, you can skip this step.

- **Reserve IP addresses**
  
  Amazon ES enables the connection of a VPC to a domain by placing network interfaces in a subnet of the VPC. Each network interface is associated with an IP address. You must reserve a sufficient number of IP addresses in the subnet for the network interfaces. For more information, see Reserving IP addresses in a VPC subnet (p. 27).

**Reserving IP addresses in a VPC subnet**

Amazon ES connects a domain to a VPC by placing network interfaces in a subnet of the VPC (or multiple subnets of the VPC if you enable multiple Availability Zones (p. 19)). Each network interface is associated with an IP address. Before you create your Amazon ES domain, you must have a sufficient number of IP addresses available in the VPC subnet to accommodate the network interfaces.

The number of IP addresses that Amazon ES requires depends on the following:

- Number of data nodes in your domain. (Master nodes are not included in the number.)
- Number of Availability Zones. If you enable two or three Availability Zones, you need only half or one-third the number of IP addresses per subnet that you need for one Availability Zone.

Here is the basic formula: The number of IP addresses reserved in each subnet is three times the number of nodes, divided by the number of Availability Zones.

**Examples**

- If a domain has 10 data nodes and two Availability Zones, the IP count is $10 / 2 \times 3 = 15$.
- If a domain has 10 data nodes and one Availability Zone, the IP count is $10 \times 3 = 30$.

When you create the domain, Amazon ES reserves the IP addresses, uses some for the domain, and reserves the rest for blue/green deployments (p. 14). You can see the network interfaces and their associated IP addresses in the **Network Interfaces** section of the Amazon EC2 console. The **Description** column shows which Amazon ES domain the network interface is associated with.
Tip
We recommend that you create dedicated subnets for the Amazon ES reserved IP addresses. By using dedicated subnets, you avoid overlap with other applications and services and ensure that you can reserve additional IP addresses if you need to scale your cluster in the future. To learn more, see Creating a subnet in your VPC.

Service-linked role for VPC access

A service-linked role is a unique type of IAM role that delegates permissions to a service so that it can create and manage resources on your behalf. Amazon ES requires a service-linked role to access your VPC, create the domain endpoint, and place network interfaces in a subnet of your VPC.

Amazon ES automatically creates the role when you use the Amazon ES console to create a domain within a VPC. For this automatic creation to succeed, you must have permissions for the es:CreateElasticsearchServiceRole and iam:CreateServiceLinkedRole actions. To learn more, see Service-Linked Role Permissions in the IAM User Guide.

After Amazon ES creates the role, you can view it (AWSServiceRoleForAmazonElasticsearchService) using the IAM console.

Note
If you create a domain that uses a public endpoint, Amazon ES doesn't need the service-linked role and doesn't create it.

For full information on this role's permissions and how to delete it, see the section called “Service-linked roles” (p. 141).

Migrating from public access to VPC access

When you create a domain, you specify whether it should have a public endpoint or reside within a VPC. Once created, you cannot switch from one to the other. Instead, you must create a new domain and either manually reindex or migrate your data. Snapshots offer a convenient means of migrating data. For information about taking and restoring snapshots, see the section called “Creating index snapshots” (p. 51).

Monitoring Amazon Elasticsearch Service cluster metrics with Amazon CloudWatch

Interpreting health dashboards

The Instance health tab in the Amazon ES console uses box charts to provide at-a-glance visibility into the health of each Elasticsearch node.
Each colored box shows the range of values for the node over the specified time period.

- Blue boxes represent values that are consistent with other nodes. Red boxes represent outliers.
- The white line within each box shows the node's current value.
- The “whiskers” on either side of each box show the minimum and maximum values for all nodes over the time period.

Amazon ES domains send performance metrics to Amazon CloudWatch every minute. If you use General Purpose or Magnetic EBS volumes, the EBS volume metrics update only every five minutes. To view these metrics, use the **Cluster health** and **Instance health** tabs in the Amazon Elasticsearch Service console. The metrics are provided at no extra charge.

If you make configuration changes to your domain, the list of individual instances in the **Cluster health** and **Instance health** tabs often double in size for a brief period before returning to the correct number. For an explanation of this behavior, see the section called “Configuration changes” (p. 14).

All metrics are in the AWS/ES namespace. Metrics for individual nodes are in the `ClientId, DomainName, NodeId` dimension. Cluster metrics are in the `Per-Domain, Per-Client Metrics` dimension. Some node metrics are aggregated at the cluster level and thus included in both dimensions. Shard metrics are in the `ClientId, DomainName, NodeId, ShardRole` dimension. The service archives metrics for two weeks before discarding them.

- the section called “Cluster metrics” (p. 30)
- the section called “Dedicated master node metrics” (p. 32)
- the section called “EBS volume metrics” (p. 33)
- the section called “Instance metrics” (p. 34)
- the section called “UltraWarm metrics” (p. 39)
- the section called “Cold storage metrics” (p. 40)
- the section called “Alerting metrics” (p. 41)
- the section called “Anomaly detection metrics” (p. 42)
- the section called “Asynchronous search metrics” (p. 43)
- the section called “SQL metrics” (p. 44)
- the section called “k-NN metrics” (p. 45)
- the section called “Cross-cluster search metrics” (p. 47)
# Cluster metrics

Amazon Elasticsearch Service provides the following metrics for clusters.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
<th>Relevant statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>ClusterStatus.green</td>
<td>A value of 1 indicates that all index shards are allocated to nodes in the cluster.</td>
<td>Maximum</td>
</tr>
<tr>
<td>ClusterStatus.yellow</td>
<td>A value of 1 indicates that the primary shards for all indices are allocated to nodes in the cluster, but replica shards for at least one index are not. For more information, see the section called “Yellow cluster status” (p. 331).</td>
<td>Maximum</td>
</tr>
<tr>
<td>ClusterStatus.red</td>
<td>A value of 1 indicates that the primary and replica shards for at least one index are not allocated to nodes in the cluster. For more information, see the section called “Red cluster status” (p. 329).</td>
<td>Maximum</td>
</tr>
<tr>
<td>Nodes</td>
<td>The number of nodes in the Amazon ES cluster, including dedicated master nodes and UltraWarm nodes. For more information, see the section called “Configuration changes” (p. 14).</td>
<td>Maximum</td>
</tr>
<tr>
<td>SearchableDocuments</td>
<td>The total number of searchable documents across all data nodes in the cluster.</td>
<td>Minimum, Maximum, Average</td>
</tr>
<tr>
<td>DeletedDocuments</td>
<td>The total number of documents marked for deletion across all data nodes in the cluster. These documents no longer appear in search results, but Elasticsearch only removes deleted documents from disk during segment merges. This metric increases after delete requests and decreases after segment merges.</td>
<td>Minimum, Maximum, Average</td>
</tr>
<tr>
<td>CPUUtilization</td>
<td>The percentage of CPU usage for data nodes in the cluster. Maximum shows the node with the highest CPU usage. Average represents all nodes in the cluster. This metric is also available for individual nodes.</td>
<td>Maximum, Average</td>
</tr>
<tr>
<td>FreeStorageSpace</td>
<td>The free space for data nodes in the cluster. Sum shows total free space for the cluster, but you must leave the period at one minute to get an accurate value. Minimum and Maximum show the nodes with the least and most free space, respectively. This metric is also available for individual nodes. Amazon ES throws a ClusterBlockException when this metric reaches 0. To recover, you must either delete indices, add larger instances, or add EBS-based storage to existing instances. To learn more, see the section called “Lack of available storage space” (p. 331).</td>
<td>Maximum, Average</td>
</tr>
</tbody>
</table>
### Cluster metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Metric</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>FreeStorageSpace</td>
<td>The Amazon ES console displays this value in GiB. The Amazon CloudWatch console displays it in MiB.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>FreeStorageSpace will always be lower than the value that the Elasticsearch _cluster/stats API provides. Amazon ES reserves a percentage of the storage space on each instance for internal operations.</td>
</tr>
<tr>
<td></td>
<td>Relevant statistics: Minimum, Maximum, Average, Sum</td>
</tr>
<tr>
<td>ClusterUsedSpace</td>
<td>The total used space for the cluster. You must leave the period at one minute to get an accurate value.</td>
</tr>
<tr>
<td></td>
<td>The Amazon ES console displays this value in GiB. The Amazon CloudWatch console displays it in MiB.</td>
</tr>
<tr>
<td></td>
<td>Relevant statistics: Minimum, Maximum</td>
</tr>
<tr>
<td>ClusterIndexWritesBlocked</td>
<td>Indicates whether your cluster is accepting or blocking incoming write requests. A value of 0 means that the cluster is accepting requests. A value of 1 means that it is blocking requests.</td>
</tr>
<tr>
<td></td>
<td>Some common factors include the following: FreeStorageSpace is too low or JVMMemoryPressure is too high. To alleviate this issue, consider adding more disk space or scaling your cluster.</td>
</tr>
<tr>
<td></td>
<td>Relevant statistics: Maximum</td>
</tr>
<tr>
<td>JVMMemoryPressure</td>
<td>The maximum percentage of the Java heap used for all data nodes in the cluster. Amazon ES uses half of an instance's RAM for the Java heap, up to a heap size of 32 GiB. You can scale instances vertically up to 64 GiB of RAM, at which point you can scale horizontally by adding instances. See the section called “Recommended CloudWatch alarms” (p. 270).</td>
</tr>
<tr>
<td></td>
<td>Relevant statistics: Maximum</td>
</tr>
<tr>
<td>AutomatedSnapshotFailure</td>
<td>The number of failed automated snapshots for the cluster. A value of 1 indicates that no automated snapshot was taken for the domain in the previous 36 hours.</td>
</tr>
<tr>
<td></td>
<td>Relevant statistics: Minimum, Maximum</td>
</tr>
<tr>
<td>CPUCreditBalance</td>
<td>The remaining CPU credits available for data nodes in the cluster. A CPU credit provides the performance of a full CPU core for one minute. For more information, see CPU credits in the Amazon EC2 Developer Guide. This metric is available only for the T2 instance types.</td>
</tr>
<tr>
<td></td>
<td>Relevant statistics: Minimum</td>
</tr>
<tr>
<td>KibanaHealthyNodes</td>
<td>A health check for Kibana. If the minimum, maximum, and average are all equal to 1, Kibana is behaving normally. If you have 10 nodes with a maximum of 1, minimum of 0, and average of 0.7, this means 7 nodes (70%) are healthy and 3 nodes (30%) are unhealthy.</td>
</tr>
<tr>
<td></td>
<td>Relevant statistics: Minimum, Maximum, Average</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>KMSKeyError</td>
<td>A value of 1 indicates that the KMS customer master key used to encrypt data at rest has been disabled. To restore the domain to normal operations, re-enable the key. The console displays this metric only for domains that encrypt data at rest. Relevant statistics: Minimum, Maximum</td>
</tr>
<tr>
<td>KMSKeyInaccessible</td>
<td>A value of 1 indicates that the KMS customer master key used to encrypt data at rest has been deleted or revoked its grants to Amazon ES. You can't recover domains that are in this state. If you have a manual snapshot, though, you can use it to migrate the domain's data to a new domain. The console displays this metric only for domains that encrypt data at rest. Relevant statistics: Minimum, Maximum</td>
</tr>
<tr>
<td>InvalidHostHeaderRequests</td>
<td>The number of HTTP requests made to the Elasticsearch cluster that included an invalid (or missing) host header. Valid requests include the domain hostname as the host header value. Amazon ES rejects invalid requests for public access domains that don't have a restrictive access policy. We recommend applying a restrictive access policy to all domains. If you see large values for this metric, confirm that your Elasticsearch clients include the domain hostname (and not, for example, its IP address) in their requests. Relevant statistics: Sum</td>
</tr>
<tr>
<td>ElasticsearchRequests</td>
<td>The number of requests made to the Elasticsearch cluster. Relevant statistics: Sum</td>
</tr>
<tr>
<td>2xx, 3xx, 4xx, 5xx</td>
<td>The number of requests to the domain that resulted in the given HTTP response code (2xx, 3xx, 4xx, 5xx). Relevant statistics: Sum</td>
</tr>
</tbody>
</table>

### Dedicated master node metrics

Amazon Elasticsearch Service provides the following metrics for dedicated master nodes (p. 268).

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MasterCPUUtilization</td>
<td>The maximum percentage of CPU resources used by the dedicated master nodes. We recommend increasing the size of the instance type when this metric reaches 60 percent. Relevant statistics: Average</td>
</tr>
<tr>
<td>MasterFreeStorageSpace</td>
<td>This metric is not relevant and can be ignored. The service does not use master nodes as data nodes.</td>
</tr>
</tbody>
</table>

API Version 2015-01-01
### EBS volume metrics

Amazon Elasticsearch Service provides the following metrics for EBS volumes.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReadLatency</td>
<td>The latency, in seconds, for read operations on EBS volumes.</td>
</tr>
<tr>
<td>WriteLatency</td>
<td>The latency, in seconds, for write operations on EBS volumes.</td>
</tr>
<tr>
<td>ReadThroughput</td>
<td>The throughput, in bytes per second, for read operations on EBS volumes.</td>
</tr>
<tr>
<td>WriteThroughput</td>
<td>The throughput, in bytes per second, for write operations on EBS volumes.</td>
</tr>
<tr>
<td>DiskQueueDepth</td>
<td>The number of pending input and output (I/O) requests for an EBS volume.</td>
</tr>
<tr>
<td>ReadIOPS</td>
<td>The number of input and output (I/O) operations per second for read operations on EBS volumes.</td>
</tr>
</tbody>
</table>
Instance metrics

Amazon Elasticsearch Service provides the following metrics for each instance in a domain. Amazon ES also aggregates these instance metrics to provide insight into overall cluster health. You can verify this behavior using the Sample Count statistic in the console. Note that each metric in the following table has relevant statistics for the node and the cluster.

Important
Different versions of Elasticsearch use different thread pools to process calls to the _index API. Elasticsearch 1.5 and 2.3 use the index thread pool. Elasticsearch 5.x, 6.0, and 6.2 use the bulk thread pool. 6.3 and later use the write thread pool. Currently, the Amazon ES console doesn’t include a graph for the bulk thread pool. Use GET _cluster/settings?include_defaults=true to check thread pool and queue sizes for your cluster.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WriteIOPS</td>
<td>The number of input and output (I/O) operations per second for write operations on EBS volumes.</td>
</tr>
<tr>
<td></td>
<td>Relevant statistics: Minimum, Maximum, Average</td>
</tr>
</tbody>
</table>

### Metric

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IndexingLatency</td>
<td>The average time, in milliseconds, that it takes a shard to complete an indexing operation.</td>
</tr>
<tr>
<td></td>
<td>Relevant node statistics: Average</td>
</tr>
<tr>
<td></td>
<td>Relevant cluster statistics: Average, Maximum</td>
</tr>
<tr>
<td>IndexingRate</td>
<td>The number of indexing operations per minute. A single call to the _bulk API that adds two documents and updates two counts as four operations, which might be spread across one or more nodes. If that index has one or more replicas, other nodes in the cluster also record a total of four indexing operations. Document deletions do not count towards this metric.</td>
</tr>
<tr>
<td></td>
<td>Relevant node statistics: Average</td>
</tr>
<tr>
<td></td>
<td>Relevant cluster statistics: Average, Maximum, Sum</td>
</tr>
<tr>
<td>SearchLatency</td>
<td>The average time, in milliseconds, that it takes a shard on a data node to complete a search operation.</td>
</tr>
<tr>
<td></td>
<td>Relevant node statistics: Average</td>
</tr>
<tr>
<td></td>
<td>Relevant cluster statistics: Average, Maximum</td>
</tr>
<tr>
<td>SearchRate</td>
<td>The total number of search requests per minute for all shards on a data node. A single call to the _search API might return results from many different shards. If five of these shards are on one node, the node would report 5 for this metric, even though the client only made one request.</td>
</tr>
<tr>
<td></td>
<td>Relevant node statistics: Average</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SysMemoryUtilization</td>
<td>The percentage of the instance's memory that is in use. High values for this metric are normal and usually do not represent a problem with your cluster. For a better indicator of potential performance and stability issues, see the JVMMemoryPressure metric. Relevance: Relevant node statistics: Minimum, Maximum, Average. Relevant cluster statistics: Minimum, Maximum, Average.</td>
</tr>
<tr>
<td>JVMGCYoungCollectionCount</td>
<td>The number of times that &quot;young generation&quot; garbage collection has run. A large, ever-growing number of runs is a normal part of cluster operations. Relevance: Relevant node statistics: Maximum. Relevant cluster statistics: Sum, Maximum, Average.</td>
</tr>
<tr>
<td>JVMGCYoungCollectionTime</td>
<td>The amount of time, in milliseconds, that the cluster has spent performing &quot;young generation&quot; garbage collection. Relevance: Relevant node statistics: Maximum. Relevant cluster statistics: Sum, Maximum, Average.</td>
</tr>
<tr>
<td>JVMGCOldCollectionCount</td>
<td>The number of times that &quot;old generation&quot; garbage collection has run. In a cluster with sufficient resources, this number should remain small and grow infrequently. Relevance: Relevant node statistics: Maximum. Relevant cluster statistics: Sum, Maximum, Average.</td>
</tr>
<tr>
<td>JVMGCOldCollectionTime</td>
<td>The amount of time, in milliseconds, that the cluster has spent performing &quot;old generation&quot; garbage collection. Relevance: Relevant node statistics: Maximum. Relevant cluster statistics: Sum, Maximum, Average.</td>
</tr>
<tr>
<td>KibanaConcurrentConnections</td>
<td>The number of active concurrent connections to Kibana. If this number is consistently high, consider scaling your cluster. Relevance: Relevant node statistics: Maximum. Relevant cluster statistics: Sum, Maximum, Average.</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>KibanaHeapTotal</td>
<td>The amount of heap memory allocated to Kibana in MiB. Different EC2 instance types can impact the exact memory allocation.</td>
</tr>
<tr>
<td></td>
<td>Relevant node statistics: Maximum</td>
</tr>
<tr>
<td></td>
<td>Relevant cluster statistics: Sum, Maximum, Average</td>
</tr>
<tr>
<td>KibanaHeapUsed</td>
<td>The absolute amount of heap memory used by Kibana in MiB.</td>
</tr>
<tr>
<td></td>
<td>Relevant node statistics: Maximum</td>
</tr>
<tr>
<td></td>
<td>Relevant cluster statistics: Sum, Maximum, Average</td>
</tr>
<tr>
<td>KibanaHeapUtilization</td>
<td>The maximum percentage of available heap memory used by Kibana. If this value increases above 80%, consider scaling your cluster.</td>
</tr>
<tr>
<td></td>
<td>Relevant node statistics: Maximum</td>
</tr>
<tr>
<td></td>
<td>Relevant cluster statistics: Minimum, Maximum, Average</td>
</tr>
<tr>
<td>KibanaOS1MinuteLoad</td>
<td>The one-minute CPU load average for Kibana. The CPU load should ideally stay below 1.00. While temporary spikes are fine, we recommend increasing the size of the instance type if this metric is consistently above 1.00.</td>
</tr>
<tr>
<td></td>
<td>Relevant node statistics: Average</td>
</tr>
<tr>
<td></td>
<td>Relevant cluster statistics: Average, Maximum</td>
</tr>
<tr>
<td>KibanaRequestTotal</td>
<td>The total count of HTTP requests made to Kibana. If your system is slow or you see high numbers of Kibana requests, consider increasing the size of the instance type.</td>
</tr>
<tr>
<td></td>
<td>Relevant node statistics: Sum</td>
</tr>
<tr>
<td></td>
<td>Relevant cluster statistics: Sum</td>
</tr>
<tr>
<td>KibanaResponseTimesMaxInMillis</td>
<td>The maximum amount of time, in milliseconds, that it takes for Kibana to respond to a request. If requests consistently take a long time to return results, consider increasing the size of the instance type.</td>
</tr>
<tr>
<td></td>
<td>Relevant node statistics: Maximum</td>
</tr>
<tr>
<td></td>
<td>Relevant cluster statistics: Maximum, Average</td>
</tr>
<tr>
<td>ThreadPoolForce_mergeQueue</td>
<td>The number of queued tasks in the force merge thread pool. If the queue size is consistently high, consider scaling your cluster.</td>
</tr>
<tr>
<td></td>
<td>Relevant node statistics: Maximum</td>
</tr>
<tr>
<td></td>
<td>Relevant cluster statistics: Sum, Maximum, Average</td>
</tr>
<tr>
<td>ThreadPoolForce_mergeRejected</td>
<td>The number of rejected tasks in the force merge thread pool. If this number continually grows, consider scaling your cluster.</td>
</tr>
<tr>
<td></td>
<td>Relevant node statistics: Maximum</td>
</tr>
<tr>
<td></td>
<td>Relevant cluster statistics: Sum</td>
</tr>
</tbody>
</table>

API Version 2015-01-01

36
<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
<th>Relevant node statistics</th>
<th>Relevant cluster statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>ThreadpoolForce_mergeThreads</td>
<td>The size of the force merge thread pool.</td>
<td>Maximum</td>
<td>Average, Sum</td>
</tr>
<tr>
<td>ThreadpoolIndexQueue</td>
<td>The number of queued tasks in the index thread pool. If the queue size is consistently high, consider scaling your cluster. The maximum index queue size is 200.</td>
<td>Maximum</td>
<td>Sum, Maximum, Average</td>
</tr>
<tr>
<td>ThreadpoolIndexRejected</td>
<td>The number of rejected tasks in the index thread pool. If this number continually grows, consider scaling your cluster.</td>
<td>Maximum</td>
<td>Sum</td>
</tr>
<tr>
<td>ThreadpoolIndexThreads</td>
<td>The size of the index thread pool.</td>
<td>Maximum</td>
<td>Average, Sum</td>
</tr>
<tr>
<td>ThreadpoolSearchQueue</td>
<td>The number of queued tasks in the search thread pool. If the queue size is consistently high, consider scaling your cluster. The maximum search queue size is 1,000.</td>
<td>Maximum</td>
<td>Sum, Maximum, Average</td>
</tr>
<tr>
<td>ThreadpoolSearchRejected</td>
<td>The number of rejected tasks in the search thread pool. If this number continually grows, consider scaling your cluster.</td>
<td>Maximum</td>
<td>Sum</td>
</tr>
<tr>
<td>ThreadpoolSearchThreads</td>
<td>The size of the search thread pool.</td>
<td>Maximum</td>
<td>Average, Sum</td>
</tr>
<tr>
<td>ThreadpoolBulkQueue</td>
<td>The number of queued tasks in the bulk thread pool. If the queue size is consistently high, consider scaling your cluster.</td>
<td>Maximum</td>
<td>Sum, Maximum, Average</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ThreadpoolBulkRejected</td>
<td>The number of rejected tasks in the bulk thread pool. If this number continually grows, consider scaling your cluster.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Relevant node statistics: Maximum</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Relevant cluster statistics: Sum</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ThreadpoolBulkThreads</td>
<td>The size of the bulk thread pool.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Relevant node statistics: Maximum</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Relevant cluster statistics: Average, Sum</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ThreadpoolWriteThreads</td>
<td>The size of the write thread pool.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Relevant node statistics: Maximum</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Relevant cluster statistics: Average, Sum</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ThreadpoolWriteQueue</td>
<td>The number of queued tasks in the write thread pool.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Relevant node statistics: Maximum</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Relevant cluster statistics: Average, Sum</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ThreadpoolWriteRejected</td>
<td>The number of rejected tasks in the write thread pool.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Relevant node statistics: Maximum</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Relevant cluster statistics: Average, Sum</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Because the default write queue size was increased from 200 to 10000 in version 7.9, this metric is no longer the only indicator of rejections from Amazon ES. Use the CoordinatingWriteRejected, PrimaryWriteRejected, and ReplicaWriteRejected metrics to monitor rejections in versions 7.9 and later.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CoordinatingWriteRejected</td>
<td>The total number of rejections happened on the coordinating node due to indexing pressure since the last Amazon ES process startup.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Relevant node statistics: Maximum</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Relevant cluster statistics: Average, Sum</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This metric is available in version 7.9 and above.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PrimaryWriteRejected</td>
<td>The total number of rejections happened on the primary shards due to indexing pressure since the last Amazon ES process startup.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Relevant node statistics: Maximum</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Relevant cluster statistics: Average, Sum</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This metric is available in version 7.9 and above.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### UltraWarm metrics

Amazon Elasticsearch Service provides the following metrics for UltraWarm (p. 222) nodes.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReplicaWriteRejected</td>
<td>The total number of rejections happened on the replica shards due to indexing pressure since the last Amazon ES process startup. Relevant node statistics: Maximum. Relevant cluster statistics: Average, Sum. This metric is available in version 7.9 and above.</td>
</tr>
<tr>
<td>WarmCPUUtilization</td>
<td>The percentage of CPU usage for UltraWarm nodes in the cluster. Maximum shows the node with the highest CPU usage. Average represents all UltraWarm nodes in the cluster. This metric is also available for individual UltraWarm nodes. Relevant statistics: Maximum, Average.</td>
</tr>
<tr>
<td>WarmFreeStorageSpace</td>
<td>The amount of free warm storage space in MiB. Because UltraWarm uses Amazon S3 rather than attached disks, Sum is the only relevant statistic. You must leave the period at one minute to get an accurate value. Relevant statistics: Sum.</td>
</tr>
<tr>
<td>WarmJVMMemoryPressure</td>
<td>The maximum percentage of the Java heap used for the UltraWarm nodes. Relevant statistics: Maximum.</td>
</tr>
<tr>
<td>WarmSearchableDocuments</td>
<td>The total number of searchable documents across all warm indices in the cluster. You must leave the period at one minute to get an accurate value. Relevant statistics: Sum.</td>
</tr>
<tr>
<td>WarmSearchLatency</td>
<td>The average time, in milliseconds, that it takes a shard on an UltraWarm node to complete a search operation. Relevant node statistics: Average. Relevant cluster statistics: Average, Maximum.</td>
</tr>
<tr>
<td>WarmSearchRate</td>
<td>The total number of search requests per minute for all shards on an UltraWarm node. A single call to the _search API might return results from many different shards. If five of these shards are on one node, the node would report 5 for this metric, even though the client only made one request. Relevant node statistics: Average. Relevant cluster statistics: Average, Maximum, Sum.</td>
</tr>
<tr>
<td>WarmStorageSpaceUtilization</td>
<td>The total amount of warm storage space, in MiB, that the cluster is using.</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>HotStorageSpaceUtilization</td>
<td>The total amount of hot storage space that the cluster is using.</td>
</tr>
<tr>
<td>WarmSysMemoryUtilization</td>
<td>The percentage of the warm node's memory that is in use.</td>
</tr>
<tr>
<td>HotToWarmMigrationQueueSize</td>
<td>The number of indices currently waiting to migrate from hot to warm storage.</td>
</tr>
<tr>
<td>WarmToHotMigrationQueueSize</td>
<td>The number of indices currently waiting to migrate from warm to hot storage.</td>
</tr>
<tr>
<td>HotToWarmMigrationFailure</td>
<td>The total number of failed hot to warm migrations.</td>
</tr>
<tr>
<td>HotToWarmMigrationForceMergeLatency</td>
<td>The average latency of the force merge stage of the migration process. If this stage consistently takes too long, consider increasing index.ultrawarm.migration.force_merge.max_num_segments.</td>
</tr>
<tr>
<td>HotToWarmMigrationSnapshotLatency</td>
<td>The average latency of the snapshot stage of the migration process. If this stage consistently takes too long, ensure that your shards are appropriately sized and distributed throughout the cluster.</td>
</tr>
<tr>
<td>HotToWarmMigrationProcessingLatency</td>
<td>The average latency of successful hot to warm migrations, not including time spent in the queue. This value is the sum of the amount of time it takes to complete the force merge, snapshot, and shard relocation stages of the migration process.</td>
</tr>
<tr>
<td>HotToWarmMigrationSuccess</td>
<td>The total number of successful hot to warm migrations.</td>
</tr>
<tr>
<td>HotToWarmMigrationSuccessLatency</td>
<td>The average latency of successful hot to warm migrations, including time spent in the queue.</td>
</tr>
</tbody>
</table>

## Cold storage metrics

Amazon Elasticsearch Service provides the following metrics for cold storage (p. 231).
Alerting metrics

Amazon Elasticsearch Service provides the following metrics for alerting (p. 253).

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AlertingDegraded</td>
<td>A value of 1 means that either the alerting index is red or one or more nodes is not on schedule. A value of 0 indicates normal behavior. Relevant statistics: Maximum</td>
</tr>
<tr>
<td>AlertingIndexExists</td>
<td>A value of 1 means the .opendistro-alerting-config index exists. A value of 0 means it does not. Until you use the alerting feature for the first time, this value remains 0.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ColdStorageSpaceUtilization</td>
<td>The total amount of cold storage space, in MiB, that the cluster is using. Relevant statistics: Max</td>
</tr>
<tr>
<td>ColdToWarmMigrationFailureCount</td>
<td>The total number of failed cold to warm migrations. Relevant statistics: Sum</td>
</tr>
<tr>
<td>ColdToWarmMigrationLatency</td>
<td>The amount of time for successful cold to warm migrations to complete. Relevant statistics: Average</td>
</tr>
<tr>
<td>ColdToWarmMigrationQueueSize</td>
<td>The number of indices currently waiting to migrate from cold to warm storage. Relevant statistics: Maximum</td>
</tr>
<tr>
<td>ColdToWarmMigrationSuccessCount</td>
<td>The total number of successful cold to warm migrations. Relevant statistics: Sum</td>
</tr>
<tr>
<td>WarmToColdMigrationFailureCount</td>
<td>The total number of failed warm to cold migrations. Relevant statistics: Sum</td>
</tr>
<tr>
<td>WarmToColdMigrationLatency</td>
<td>The amount of time for successful warm to cold migrations to complete. Relevant statistics: Average</td>
</tr>
<tr>
<td>WarmToColdMigrationQueueSize</td>
<td>The number of indices currently waiting to migrate from warm to cold storage. Relevant statistics: Maximum</td>
</tr>
<tr>
<td>WarmToColdMigrationSuccessCount</td>
<td>The total number of successful warm to cold migrations. Relevant statistics: Sum</td>
</tr>
</tbody>
</table>
### Anomaly detection metrics

Amazon Elasticsearch Service provides the following metrics for anomaly detection (p. 255).

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnomalyDetectionPluginUnhealthy</td>
<td>A value of 1 means that the anomaly detection plugin is not functioning properly, either because of a high number of failures or because one of the indices that it uses is red. A value of 0 indicates the plugin is working as expected.</td>
</tr>
<tr>
<td>AnomalyDetectionRequestCount</td>
<td>The number of requests to detect anomalies.</td>
</tr>
<tr>
<td>AnomalyDetectionFailureCount</td>
<td>The number of failed requests to detect anomalies.</td>
</tr>
</tbody>
</table>

---
Asynchronous search metrics

Amazon Elasticsearch Service provides the following metrics for asynchronous search (p. 212).

**Asynchronous search coordinator node statistics (per coordinator node)**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AsynchronousSearchSubmissionRate</td>
<td>The number of asynchronous searches submitted in the last minute.</td>
</tr>
<tr>
<td>AsynchronousSearchInitializedRate</td>
<td>The number of asynchronous searches initialized in the last minute.</td>
</tr>
<tr>
<td>AsynchronousSearchCompletionRate</td>
<td>The number of asynchronous searches successfully completed in the last minute.</td>
</tr>
<tr>
<td>AsynchronousSearchFailureRate</td>
<td>The number of asynchronous searches that completed and failed in the last minute.</td>
</tr>
<tr>
<td>AsynchronousSearchPersistRate</td>
<td>The number of asynchronous searches that persisted in the last minute.</td>
</tr>
</tbody>
</table>
### SQL metrics

Amazon Elasticsearch Service provides the following metrics for **SQL support (p. 183)**.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQLFailedRequestCount</td>
<td>The number of requests to the <code>_opendistro/_sql</code> API that failed due to a client issue. For example, a request might return HTTP status code 400 due to an <code>IndexNotFoundException</code>. Relevant statistics: Sum</td>
</tr>
<tr>
<td>SQLFailedRequestCount</td>
<td>The number of requests to the <code>_opendistro/_sql</code> API that failed due to a server problem or feature limitation. For example, a request might return HTTP status code 503 due to a <code>VerificationException</code>. Relevant statistics: Sum</td>
</tr>
<tr>
<td>SQLRequestCount</td>
<td>The number of requests to the <code>_opendistro/_sql</code> API. Relevant statistics: Sum</td>
</tr>
<tr>
<td>SQLDefaultCursorRequestCount</td>
<td>Similar to <code>SQLRequestCount</code> but only counts pagination requests. Relevant statistics: Sum</td>
</tr>
<tr>
<td>SQLUnhealthy</td>
<td>A value of 1 indicates that, in response to certain requests, the SQL plugin is returning 5xx response codes or passing invalid query DSL to Elasticsearch. Other requests should continue to succeed. A value of 0 indicates no recent failures. If you see a sustained value of 1, troubleshoot the requests your clients are making to the plugin.</td>
</tr>
</tbody>
</table>
Amazon Elasticsearch Service includes the following metrics for the k-nearest neighbor (k-NN) plugin.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KNNCacheCapacityReached</td>
<td>Per-node metric for whether cache capacity has been reached. This metric is only relevant to approximate k-NN search. Relevant statistics: Maximum</td>
</tr>
<tr>
<td>KNNCircuitBreakerTriggered</td>
<td>Per-cluster metric for whether the circuit breaker is triggered. If any nodes return a value of 1 for KNNCacheCapacityReached, this value will also return 1. This metric is only relevant to approximate k-NN search. Relevant statistics: Maximum</td>
</tr>
<tr>
<td>KNNEvictionCount</td>
<td>Per-node metric for the number of graphs that have been evicted from the cache due to memory constraints or idle time. Explicit evictions that occur because of index deletion are not counted. This metric is only relevant to approximate k-NN search. Relevant statistics: Sum</td>
</tr>
<tr>
<td>KNNGraphIndexErrors</td>
<td>Per-node metric for the number of requests to add the knn_vector field of a document to a graph that produced an error. Relevant statistics: Sum</td>
</tr>
<tr>
<td>KNNGraphIndexRequests</td>
<td>Per-node metric for the number of requests to add the knn_vector field of a document to a graph. Relevant statistics: Sum</td>
</tr>
<tr>
<td>KNNGraphMemoryUsage</td>
<td>Per-node metric for the current cache size (total size of all graphs in memory) in kilobytes. This metric is only relevant to approximate k-NN search. Relevant statistics: Average</td>
</tr>
<tr>
<td>KNNGraphQueryErrors</td>
<td>Per-node metric for the number of graph queries that produced an error. Relevant statistics: Sum</td>
</tr>
<tr>
<td>KNNGraphQueryRequests</td>
<td>Per-node metric for the number of graph queries. Relevant statistics: Sum</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>KNNHitCount</td>
<td>Per-node metric for the number of cache hits. A cache hit occurs when a user queries a graph that is already loaded into memory. This metric is only relevant to approximate k-NN search.</td>
</tr>
<tr>
<td>KNNLoadExceptionCount</td>
<td>Per-node metric for the number of times an exception occurred while trying to load a graph into the cache. This metric is only relevant to approximate k-NN search.</td>
</tr>
<tr>
<td>KNNLoadSuccessCount</td>
<td>Per-node metric for the number of times the plugin successfully loaded a graph into the cache. This metric is only relevant to approximate k-NN search.</td>
</tr>
<tr>
<td>KNNMissCount</td>
<td>Per-node metric for the number of cache misses. A cache miss occurs when a user queries a graph that is not yet loaded into memory. This metric is only relevant to approximate k-NN search.</td>
</tr>
<tr>
<td>KNNQueryRequests</td>
<td>Per-node metric for the number of query requests the k-NN plugin received.</td>
</tr>
<tr>
<td>KNNScriptCompilationErrors</td>
<td>Per-node metric for the number of errors during script compilation. This statistic is only relevant to k-NN score script search.</td>
</tr>
<tr>
<td>KNNScriptCompilations</td>
<td>Per-node metric for the number of times the k-NN script has been compiled. This value should usually be 1 or 0, but if the cache containing the compiled scripts is filled, the k-NN script might be recompiled. This statistic is only relevant to k-NN score script search.</td>
</tr>
<tr>
<td>KNNScriptQueryErrors</td>
<td>Per-node metric for the number of errors during script queries. This statistic is only relevant to k-NN score script search.</td>
</tr>
<tr>
<td>KNNScriptQueryRequests</td>
<td>Per-node metric for the total number of script queries. This statistic is only relevant to k-NN score script search.</td>
</tr>
<tr>
<td>KNNTotalLoadTime</td>
<td>The time in nanoseconds that k-NN has taken to load graphs into the cache. This metric is only relevant to approximate k-NN search.</td>
</tr>
</tbody>
</table>
Cross-cluster search metrics

Amazon Elasticsearch Service provides the following metrics for cross-cluster search (p. 189).

Source domain metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Dimension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CrossClusterOutboundConnections</td>
<td>ConnectionId</td>
<td>Number of connected nodes. If your response includes one or more skipped domains, use this metric to trace any unhealthy connections. If this number drops to 0, then the connection is unhealthy.</td>
</tr>
<tr>
<td>CrossClusterOutboundRequests</td>
<td>ConnectionId</td>
<td>Number of search requests sent to the destination domain. Use to check if the load of cross-cluster search requests are overwhelming your domain, correlate any spike in this metric with any JVM/CPU spike.</td>
</tr>
</tbody>
</table>

Destination domain metric

<table>
<thead>
<tr>
<th>Metric</th>
<th>Dimension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CrossClusterInboundRequests</td>
<td>ConnectionId</td>
<td>Number of incoming connection requests received from the source domain.</td>
</tr>
</tbody>
</table>

Add a CloudWatch alarm in the event that you lose a connection unexpectedly. For steps to create an alarm, see Create a CloudWatch Alarm Based on a Static Threshold.

Learning to Rank metrics

Amazon Elasticsearch Service provides the following metrics for Learning to Rank (p. 195).

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LTRRequestTotalCount</td>
<td>Total count of ranking requests.</td>
</tr>
<tr>
<td>LTRRequestErrorCount</td>
<td>Total count of unsuccessful requests.</td>
</tr>
<tr>
<td>LTRStoreIndexIsRed</td>
<td>Tracks if one of the indices needed to run the plugin is red.</td>
</tr>
<tr>
<td>LTRMemoryUsage</td>
<td>Total memory used by the plugin.</td>
</tr>
</tbody>
</table>

Configuring logs in Amazon Elasticsearch Service

Amazon Elasticsearch Service (Amazon ES) exposes the following Elasticsearch logs through Amazon CloudWatch Logs:

- Error logs
- Search slow logs
- Index slow logs
- Audit logs (p. 109)
Search slow logs, index slow logs, and error logs are useful for troubleshooting performance and stability issues. Audit logs track user activity for compliance purposes. All the logs are disabled by default. If enabled, standard CloudWatch pricing applies.

Note
Error logs are available only for Elasticsearch versions 5.1 and greater. Slow logs are available for all Elasticsearch versions.

For its logs, Elasticsearch uses Apache Log4j 2 and its built-in log levels (from least to most severe) of TRACE, DEBUG, INFO, WARN, ERROR, and FATAL.

If you enable error logs, Amazon ES publishes log lines of WARN, ERROR, and FATAL to CloudWatch. Amazon ES also publishes several exceptions from the DEBUG level, including the following:

- org.elasticsearch.index.mapper.MapperParsingException
- org.elasticsearch.index.query.QueryShardException
- org.elasticsearch.action.search.SearchPhaseExecutionException
- org.elasticsearch.action.search.OutOfModuleExecutionException
- org.elasticsearch.common.util.concurrent.EsRejectedExecutionException
- java.lang.IllegalArgumentException

Error logs can help with troubleshooting in many situations, including the following:

- Painless script compilation issues
- Invalid queries
- Indexing issues
- Snapshot failures

Enabling log publishing (console)

The Amazon ES console is the simplest way to enable the publishing of logs to CloudWatch.

To enable log publishing to CloudWatch (console)

1. Go to https://aws.amazon.com, and then choose Sign In to the Console.
2. Under Analytics, choose Elasticsearch Service.
3. In the navigation pane, under My domains, choose the domain you want to update.
4. On the Logs tab, choose Setup for the log you want.
5. Create a CloudWatch log group, or choose an existing one.

   Note
   If you plan to enable multiple logs, we recommend publishing each to its own log group.
   This separation makes the logs easier to scan.

6. Choose an access policy that contains the appropriate permissions, or create a policy using the JSON that the console provides:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "es.amazonaws.com"
            },
            "Action": [
```
Important

CloudWatch Logs supports 10 resource policies per Region. If you plan to enable logs for several Amazon ES domains, you should create and reuse a broader policy that includes multiple log groups to avoid reaching this limit. For steps on updating your policy, see the section called "Enabling log publishing (AWS CLI)" (p. 49).

7. Choose Enable.

The status of your domain changes from Active to Processing. The status must return to Active before log publishing is enabled. This change typically takes 30 minutes, but can take longer depending on your domain configuration.

If you enabled one of the slow logs, see the section called “Setting Elasticsearch logging thresholds for slow logs” (p. 51). If you enabled audit logs, see the section called “Configuring audit logs in Kibana” (p. 111). If you enabled only error logs, you don’t need to perform any additional configuration steps.

Enabling log publishing (AWS CLI)

Before you can enable log publishing, you need a CloudWatch log group. If you don’t already have one, you can create one using the following command:

```bash
aws logs create-log-group --log-group-name my-log-group
```

Enter the next command to find the log group’s ARN, and then **make a note of it**:

```bash
aws logs describe-log-groups --log-group-name my-log-group
```

Now you can give Amazon ES permissions to write to the log group. You must provide the log group’s ARN near the end of the command:

```bash
```

Important

CloudWatch Logs supports 10 resource policies per Region. If you plan to enable slow logs for several Amazon ES domains, you should create and reuse a broader policy that includes multiple log groups to avoid reaching this limit.

If you need to review this policy at a later time, use the `aws logs describe-resource-policies` command. To update the policy, issue the same `aws logs put-resource-policy` command with a new policy document.

Finally, you can use the --log-publishing-options option to enable publishing. The syntax for the option is the same for both the `create-elasticsearch-domain` and `update-elasticsearch-domain-config` commands.
Enabling log publishing (AWS SDKs)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Valid Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>--log-publishing-options</td>
<td>SEARCH_SLOW_LOGS={CloudWatchLogsLogGroupArn=cw_log_group_arn,Enabled=true}</td>
</tr>
<tr>
<td></td>
<td>INDEX_SLOW_LOGS={CloudWatchLogsLogGroupArn=cw_log_group_arn,Enabled=true}</td>
</tr>
<tr>
<td></td>
<td>ES_APPLICATION_LOGS={CloudWatchLogsLogGroupArn=cw_log_group_arn,Enabled=true}</td>
</tr>
<tr>
<td></td>
<td>AUDIT_LOGS={CloudWatchLogsLogGroupArn=cw_log_group_arn,Enabled=true}</td>
</tr>
</tbody>
</table>

**Note**
If you plan to enable multiple logs, we recommend publishing each to its own log group. This separation makes the logs easier to scan.

**Example**

The following example enables the publishing of search and index slow logs for the specified domain:

```
```

To disable publishing to CloudWatch, run the same command with `Enabled=false`.

If you enabled one of the slow logs, see the section called “Setting Elasticsearch logging thresholds for slow logs” (p. 51). If you enabled audit logs, see the section called “Configuring audit logs in Kibana” (p. 111). If you enabled only error logs, you don't need to perform any additional configuration steps.

**Enabling log publishing (AWS SDKs)**

Before you can enable log publishing, you must first create a CloudWatch log group, get its ARN, and give Amazon ES permissions to write to it. The relevant operations are documented in the Amazon CloudWatch Logs API Reference:

- CreateLogGroup
- DescribeLogGroup
- PutResourcePolicy

You can access these operations using the AWS SDKs.

The AWS SDKs (except the Android and iOS SDKs) support all the operations that are defined in *Configuration API reference* (p. 339), including the --log-publishing-options option for CreateElasticsearchDomain and UpdateElasticsearchDomainConfig.

If you enabled one of the slow logs, see the section called “Setting Elasticsearch logging thresholds for slow logs” (p. 51). If you enabled only error logs, you don't need to perform any additional configuration steps.
Setting Elasticsearch logging thresholds for slow logs

Elasticsearch disables slow logs by default. After you enable the publishing of slow logs to CloudWatch, you still must specify logging thresholds for each Elasticsearch index. These thresholds define precisely what should be logged and at which log level.

You specify these settings through the Elasticsearch REST API:

```
PUT elasticsearch_domain_endpoint/index/_settings
{
  "index.search.slowlog.threshold.query.warn": "5s",
  "index.search.slowlog.threshold.query.info": "2s"
}
```

To test that slow logs are publishing successfully, consider starting with very low values to verify that logs appear in CloudWatch, and then increase the thresholds to more useful levels.

If the logs don't appear, check the following:

- Does the CloudWatch log group exist? Check the CloudWatch console.
- Does Amazon ES have permissions to write to the log group? Check the Amazon ES console.
- Is the Amazon ES domain configured to publish to the log group? Check the Amazon ES console, use the AWS CLI describe-elasticsearch-domain-config option, or call DescribeElasticsearchDomainConfig using one of the SDKs.
- Are the Elasticsearch logging thresholds low enough that your requests are exceeding them? To review your thresholds for an index, use the following command:

```
GET elasticsearch_domain_endpoint/index/_settings?pretty
```

If you want to disable slow logs for an index, return any thresholds that you changed to their default values of -1.

Disabling publishing to CloudWatch using the Amazon ES console or AWS CLI does not stop Elasticsearch from generating logs; it only stops the publishing of those logs. Be sure to check your index settings if you no longer need the slow logs.

Viewing logs

Viewing the application and slow logs in CloudWatch is just like viewing any other CloudWatch log. For more information, see View Log Data in the Amazon CloudWatch Logs User Guide.

Here are some considerations for viewing the logs:

- Amazon ES publishes only the first 255,000 characters of each line to CloudWatch. Any remaining content is truncated. For audit logs, it's 10,000 characters per message.
- In CloudWatch, the log stream names have suffixes of -index-slow-logs, -search-slow-logs, -es-application-logs, and -audit-logs to help identify their contents.

Creating index snapshots in Amazon Elasticsearch Service

Snapshots in Amazon Elasticsearch Service (Amazon ES) are backups of a cluster's indices and state. State includes cluster settings, node information, index settings, and shard allocation.
Amazon ES snapshots come in the following forms:

- **Automated snapshots** are only for cluster recovery. You can use them to restore your domain in the event of red cluster status or data loss. For more information, see Restoring snapshots (p. 59) below. Amazon ES stores automated snapshots in a preconfigured Amazon S3 bucket at no additional charge.

- **Manual snapshots** are for cluster recovery or for moving data from one cluster to another. You have to initiate manual snapshots. These snapshots are stored in your own Amazon S3 bucket and standard S3 charges apply. If you have a snapshot from a self-managed Elasticsearch cluster, you can use that snapshot to migrate to an Amazon ES domain. For more information, see Migrating to Amazon Elasticsearch Service (p. 307).

All Amazon ES domains take automated snapshots, but the frequency differs in the following ways:

- For domains running Elasticsearch 5.3 and later, Amazon ES takes hourly automated snapshots and retains up to 336 of them for 14 days.
- For domains running Elasticsearch 5.1 and earlier, Amazon ES takes daily automated snapshots during the hour you specify, retains up to 14 of them, and doesn't retain any snapshot data for more than 30 days.

If your cluster enters red status, all automated snapshots fail while the cluster status persists. If you don't correct the problem within two weeks, you can permanently lose the data in your cluster. For troubleshooting steps, see the section called “Red cluster status” (p. 329).

**Topics**

- Prerequisites (p. 52)
- Registering a manual snapshot repository (p. 55)
- Taking manual snapshots (p. 58)
- Restoring snapshots (p. 59)
- Deleting manual snapshots (p. 60)
- Automating snapshots with Index State Management (p. 61)
- Using Curator for snapshots (p. 61)

## Prerequisites

To create snapshots manually, you need to work with IAM and Amazon S3. Make sure you meet the following prerequisites before you attempt to take a snapshot:

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S3 bucket</td>
<td>Create an S3 bucket to store manual snapshots for your Amazon ES domain. For instructions, see Create a Bucket in the Amazon Simple Storage Service Getting Started Guide. Remember the name of the bucket to use it in the following places:</td>
</tr>
<tr>
<td></td>
<td>• The Resource statement of the IAM policy attached to your IAM role</td>
</tr>
<tr>
<td></td>
<td>• The Python client used to register a snapshot repository (if you use this method)</td>
</tr>
</tbody>
</table>
### Prerequisites

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Important</strong></td>
<td>Do not apply an S3 Glacier lifecycle rule to this bucket. Manual snapshots don't support the S3 Glacier storage class.</td>
</tr>
<tr>
<td>Prerequisite</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>IAM role</td>
<td>Create an IAM role to delegate permissions to Amazon ES. For instructions, see Creating an IAM role (console) in the IAM User Guide. The rest of this chapter refers to this role as TheSnapshotRole.</td>
</tr>
</tbody>
</table>

**Attach an IAM policy**

Attach the following policy to TheSnapshotRole to allow access to the S3 bucket:

```json
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": [
            "s3:ListBucket"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::s3-bucket-name"
        ]
    },
    {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::s3-bucket-name/*"
        ]
    }
}
```

For instructions to attach a policy to a role, see Adding IAM Identity Permissions in the IAM User Guide.

**Edit the trust relationship**

Edit the trust relationship of TheSnapshotRole to specify Amazon ES in the Principal statement as shown in the following example:

```json
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "",
        "Effect": "Allow",
        "Principal": {
            "Service": "es.amazonaws.com"
        },
        "Action": "sts:AssumeRole"
    }
}
```

For instructions to edit the trust relationship, see Modifying a role trust policy in the IAM User Guide.
Registering a manual snapshot repository

You need to register a snapshot repository with Amazon ES before you can take manual index snapshots. This one-time operation requires that you sign your AWS request with credentials that are allowed to access `TheSnapshotRole`, as described in the section called “Prerequisites” (p. 52).

**Step 1: Map the manage_snapshots role (if using fine-grained access control)**

Fine-grained access control introduces an additional step when registering a repository. Even if you use HTTP basic authentication for all other purposes, you need to map the `manage_snapshots` role to your IAM role that has `iam:PassRole` permissions to pass `TheSnapshotRole`.

1. Navigate to the Kibana plugin for your Amazon ES domain. You can find the Kibana endpoint on your domain dashboard on the Amazon ES console.
2. From the main menu choose Security and then Roles.
3. Search for and select the `manage_snapshots` role.
4. Go to the Mapped users tab and choose Manage mapping.
5. Under Backend roles, add the domain ARN of the role that has permissions to pass `TheSnapshotRole`. The ARN has the following format:

```
arn:aws:iam::<your_account_id>:role/role-name
```
6. Select Map and confirm the role shows up under Mapped users.

**Step 2: Register a repository**

To register a snapshot repository, send a PUT request to the Amazon ES domain endpoint. You can't use `curl` to perform this operation because it doesn't support AWS request signing. Instead, use the sample Python client (p. 57), Postman, or some other method to send a signed request (p. 143) to register the snapshot repository.

The request takes the following format:

```plaintext
PUT elasticsearch-domain-endpoint/_snapshot/my-snapshot-repo-name
{
  "type": "s3",
  "settings": {
    "bucket": "s3-bucket-name",
    "region": "region",
    "role_arn": "arn:aws:iam::123456789012:role/TheSnapshotRole"
  }
}
```

If your domain resides within a virtual private cloud (VPC), your computer must be connected to the VPC for the request to successfully register the snapshot repository. Accessing a VPC varies by network configuration, but likely involves connecting to a VPN or corporate network. To check that you can reach the Amazon ES domain, navigate to `https://your-vpc-domain.region.es.amazonaws.com` in a web browser and verify that you receive the default JSON response.

**Encrypting snapshot repositories**

You currently can't use Key Management Service (KMS) master keys to encrypt manual snapshots, but you can protect them using server-side encryption (SSE).

To enable SSE with S3-managed keys for the bucket you use as a snapshot repository, add "server_side_encryption": true to the "settings" block of the PUT request. For more information, see Protecting data using server-side encryption with Amazon S3-managed encryption keys in the Amazon Simple Storage Service User Guide.

Alternatively, you can use customer master keys (CMKs) for server-side encryption on the S3 bucket you use as a snapshot repository.

**Migrating data to a different domain**

Registering a snapshot repository is a one-time operation. However, to migrate from one domain to another, you have to register the same snapshot repository on the old domain and the new domain. The repository name is arbitrary.

Consider the following guidelines when migrating to a new domain or registering the same repository with multiple domains for another reason:

- When registering the repository on the new domain, add "readonly": true to the "settings" block of the PUT request. This setting prevents you from accidentally overwriting data from the old domain.
- If you're migrating data to a domain in a different region, (for example, from an old domain and bucket located in us-east-2 to a new domain in us-west-2), you might see this 500 error when sending the PUT request:

  ```plaintext
  The bucket is in this region: us-east-2. Please use this region to retry the request.
  ```
If you encounter this error, try replacing "region": "us-east-2" with "endpoint": "s3.amazonaws.com" in the PUT statement and retry the request.

Using the sample Python client

The Python client is easier to automate than a simple HTTP request and has better reusability. If you choose to use this method to register a snapshot repository, save the following sample Python code as a Python file, such as register-repo.py. The client requires the AWS SDK for Python (Boto3), requests and requests-aws4auth packages. The client contains commented-out examples for other snapshot operations.

Tip
A Java-based code sample is available in Signing HTTP Requests (p. 143).

Update the following variables in the sample code: host, region, path, and payload.

```python
import boto3
import requests
from requests_aws4auth import AWS4Auth

host = '' # include https:// and trailing /
region = '' # e.g. us-west-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
                   session_token=credentials.token)

# Register repository
path = '_snapshot/my-snapshot-repo-name' # the Elasticsearch API endpoint
url = host + path

payload = {
    "type": "s3",
    "settings": {
        "bucket": "s3-bucket-name",
        "region": "us-west-1",
        "role_arn": "arn:aws:iam::123456789012:role/TheSnapshotRole"
    }
}

headers = {"Content-Type": "application/json"}

r = requests.put(url, auth=awsauth, json=payload, headers=headers)

print(r.status_code)
print(r.text)
```

# # Take snapshot
# # path = '_snapshot/my-snapshot-repo/my-snapshot'
# # url = host + path
# # r = requests.put(url, auth=awsauth)
# # print(r.text)
# # # Delete index
# # path = 'my-index'
# # url = host + path
# #
Taking manual snapshots

Snapshots are not instantaneous. They take time to complete and don't represent perfect point-in-time views of the cluster. While a snapshot is in progress, you can still index documents and make other requests to the cluster, but new documents and updates to existing documents generally aren't included in the snapshot. The snapshot includes primary shards as they existed when Elasticsearch initiated the snapshot. Depending on the size of your snapshot thread pool, different shards might be included in the snapshot at slightly different times.

Snapshot storage and performance

Elasticsearch snapshots are incremental, meaning they only store data that changed since the last successful snapshot. This incremental nature means the difference in disk usage between frequent and infrequent snapshots is often minimal. In other words, taking hourly snapshots for a week (for a total of 168 snapshots) might not use much more disk space than taking a single snapshot at the end of the week. Also, the more frequently you take snapshots, the less time they take to complete. Some Elasticsearch users take snapshots as often as every half hour.

Create a snapshot

You specify the following information when you create a snapshot:

- The name of your snapshot repository
- A name for the snapshot

The examples in this chapter use curl, a common HTTP client, for convenience and brevity. However, if your access policies specify IAM users or roles, however, you must sign your snapshot requests. You can
use the commented-out examples in the sample Python client (p. 57) to make signed HTTP requests to the same endpoints that the curl commands use.

To take a manual snapshot, perform the following steps:

1. You can't take a snapshot if one is currently in progress. To check, run the following command:

   ```bash
curl -XGET 'elasticsearch-domain-endpoint/_snapshot/_status'
   ```

2. Run the following command to take a manual snapshot:

   ```bash
curl -XPUT 'elasticsearch-domain-endpoint/_snapshot/repository-name/snapshot-name'
   ```

   **Note**
   The time required to take a snapshot increases with the size of the Amazon ES domain. Long-running snapshot operations sometimes encounter the following error: 504 GATEWAY_TIMEOUT. You can typically ignore these errors and wait for the operation to complete successfully. Run the following command to verify the state of all snapshots of your domain:

   ```bash
curl -XGET 'elasticsearch-domain-endpoint/_snapshot/repository-name/_all?pretty'
   ```

### Restoring snapshots

**Warning**
If you use index aliases, cease write requests to an alias, or switch the alias to another index, prior to deleting its index. Halting write requests helps avoid the following scenario:

1. You delete an index, which also deletes its alias.
2. An errant write request to the now-deleted alias creates a new index with the same name as the alias.
3. You can no longer use the alias due to a naming conflict with the new index.

If you switched the alias to another index, specify "include_aliases": false when you restore from a snapshot.

To restore a snapshot, perform the following steps:

1. Identify the snapshot you want to restore. To see all snapshot repositories, run the following command:

   ```bash
curl -XGET 'elasticsearch-domain-endpoint/_snapshot?pretty'
   ```

   After you identify the repository, run the following command to see all snapshots:

   ```bash
curl -XGET 'elasticsearch-domain-endpoint/_snapshot/repository-name/_all?pretty'
   ```

   **Note**
   Most automated snapshots are stored in the cs-automated repository. If your domain encrypts data at rest, they're stored in the cs-automated-enc repository. If you don't see the manual snapshot repository you're looking for, make sure you registered it (p. 55) to the domain.
2. (Optional) Delete or rename one or more indices in the Amazon ES domain if you have naming conflicts between indices on the cluster and indices in the snapshot. You can't restore a snapshot of your indices to an Elasticsearch cluster that already contains indices with the same names.

You have the following options if you have index naming conflicts:

- Delete the indices on the existing Amazon ES domain and then restore the snapshot.
- Rename the indices as you restore them from the snapshot (p. 333) and reindex them later.
- Restore the snapshot to a different Amazon ES domain (only possible with manual snapshots).

The following command deletes all existing indices in a domain:

```
curl -XDELETE 'elasticsearch-domain-endpoint/_all'
```

However, if you don't plan to restore all indices, you can just delete one:

```
curl -XDELETE 'elasticsearch-domain-endpoint/index-name'
```

3. To restore a snapshot, run the following command:

```
curl -XPOST 'elasticsearch-domain-endpoint/_snapshot/repository-name/snapshot-name/_restore'
```

Due to special permissions on the Kibana and fine-grained access control indices, attempts to restore all indices might fail, especially if you try to restore from an automated snapshot. The following example restores just one index, my-index, from 2020-snapshot in the cs-automated snapshot repository:

```
curl -XPOST 'elasticsearch-domain-endpoint/_snapshot/cs-automated/2020-snapshot/_restore' -d '{"indices": "my-index"}' -H 'Content-Type: application/json'
```

Alternately, you might want to restore all indices except the Kibana and fine-grained access control indices:

```
curl -XPOST 'elasticsearch-domain-endpoint/_snapshot/cs-automated/2020-snapshot/_restore' -d '{"indices": ".kibana*,.opendistro_security"}' -H 'Content-Type: application/json'
```

**Note**

If not all primary shards were available for the indices involved, a snapshot might have a state of PARTIAL. This value indicates that data from at least one shard wasn't stored successfully. You can still restore from a partial snapshot, but you might need to use older snapshots to restore any missing indices.

**Deleting manual snapshots**

To delete a manual snapshot, run the following command:

```
DELETE _snapshot/repository-name/snapshot-name
```
Automating snapshots with Index State Management

You can use the Index State Management (ISM) snapshot operation to automatically trigger snapshots of indices based on changes in their age, size, or number of documents. For an example ISM policy using the snapshot operation, see Sample Policies (p. 239).

Using Curator for snapshots

Some users find tools like Curator convenient for index and snapshot management. Use pip to install Curator:

```
    pip install elasticsearch-curator
```

Curator offers advanced filtering functionality that can help simplify management tasks on complex clusters. Amazon ES supports Curator on domains running Elasticsearch version 5.1 and above. You can use Curator as a command line interface (CLI) or Python API. If you use the CLI, export your credentials at the command line and configure `curator.yml` as follows:

```
client:
    hosts: search-my-domain.us-west-1.es.amazonaws.com
    port: 443
    use_ssl: True
    aws_region: us-west-1
    aws_sign_request: True
    ssl_no_validate: False
    timeout: 60

logging:
    loglevel: INFO
```

For sample Lambda functions that use the Python API, see the section called "Using Curator to rotate data" (p. 244).

Upgrading Elasticsearch

**Note**

Elasticsearch version upgrades differ from service software updates. For information on updating the service software for your Amazon ES domain, see the section called “Service software updates” (p. 16).

Amazon Elasticsearch Service (Amazon ES) offers in-place Elasticsearch upgrades for domains that run versions 5.1 and later. If you use services like Amazon Kinesis Data Firehose or Amazon CloudWatch Logs to stream data to Amazon ES, check that these services support the newer version of Elasticsearch before migrating.

Currently, Amazon ES supports the following upgrade paths:

<table>
<thead>
<tr>
<th>From Version</th>
<th>To Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.x</td>
<td>7.x</td>
</tr>
</tbody>
</table>

**Important**

Elasticsearch 7.10 introduces a breaking change with regard to dynamic templates. For more information, see the section called "Mapper parsing exception while indexing" (p. 334).
Troubleshooting an upgrade

The upgrade process consists of three steps:

1. **Pre-upgrade checks** – Amazon ES performs a series of checks for issues that can block an upgrade and doesn't proceed to the next step unless these checks succeed.

2. **Snapshot** – Amazon ES takes a snapshot of the Elasticsearch cluster and doesn't proceed to the next step unless the snapshot succeeds. If the upgrade fails, Amazon ES uses this snapshot to restore the cluster to its original state. For more information about this snapshot, see the section called "Can't downgrade after upgrade" (p. 336).

3. **Upgrade** – Amazon ES starts the upgrade, which can take from 15 minutes to several hours to complete. Kibana might be unavailable during some or all of the upgrade.

## Troubleshooting an upgrade

In-place Elasticsearch upgrades require healthy domains. Your domain might be ineligible for an upgrade or fail to upgrade for a wide variety of reasons. The following table shows the most common issues.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Too many shards per node</td>
<td>The 7.x versions of Elasticsearch have a default setting of no more than 1,000 shards per node. If a node in your current cluster exceeds this setting, Amazon ES doesn't allow you to upgrade. See the section called &quot;Exceeded maximum shard limit&quot; (p. 333) for troubleshooting options.</td>
</tr>
<tr>
<td>Domain in processing</td>
<td>The domain is in the middle of a configuration change. Check upgrade eligibility after the operation completes.</td>
</tr>
<tr>
<td>Issue</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Red cluster status</td>
<td>One or more indices in the cluster is red. For troubleshooting steps, see the section called “Red cluster status” (p. 329).</td>
</tr>
<tr>
<td>High error rate</td>
<td>The Elasticsearch cluster is returning a large number of 5xx errors when attempting to process requests. This problem is usually the result of too many simultaneous read or write requests. Consider reducing traffic to the cluster or scaling your domain.</td>
</tr>
<tr>
<td>Split brain</td>
<td>Split brain means that your Elasticsearch cluster has more than one master node and has split into two clusters that never will rejoin on their own. You can avoid split brain by using the recommended number of dedicated master nodes (p. 268). For help recovering from split brain, contact AWS Support.</td>
</tr>
<tr>
<td>Master node not found</td>
<td>Amazon ES can't find the cluster's master node. If your domain uses multi-AZ (p. 19), an Availability Zone failure might have caused the cluster to lose quorum and be unable to elect a new master node (p. 268). If the issue does not self-resolve, contact AWS Support.</td>
</tr>
<tr>
<td>Too many pending tasks</td>
<td>The master node is under heavy load and has many pending tasks. Consider reducing traffic to the cluster or scaling your domain.</td>
</tr>
<tr>
<td>Impaired storage volume</td>
<td>The disk volume of one or more nodes isn't functioning properly. This issue often occurs alongside other issues, like a high error rate or too many pending tasks. If it occurs in isolation and doesn't self-resolve, contact AWS Support.</td>
</tr>
<tr>
<td>KMS key issue</td>
<td>The KMS key that is used to encrypt the domain is either inaccessible or missing. For more information, see the section called “Monitoring domains that encrypt data at rest” (p. 76).</td>
</tr>
<tr>
<td>Snapshot in progress</td>
<td>The domain is currently taking a snapshot. Check upgrade eligibility after the snapshot finishes. Also check that you can list manual snapshot repositories, list snapshots within those repositories, and take manual snapshots. If Amazon ES is unable to check whether a snapshot is in progress, upgrades can fail.</td>
</tr>
<tr>
<td>Snapshot timeout or failure</td>
<td>The pre-upgrade snapshot took too long to complete or failed. Check cluster health, and try again. If the problem persists, contact AWS Support.</td>
</tr>
<tr>
<td>Incompatible indices</td>
<td>One or more indices is incompatible with the target Elasticsearch version. This problem can occur if you migrated the indices from an older version of Elasticsearch, like 2.3. Reindex the indices, and try again.</td>
</tr>
<tr>
<td>High disk usage</td>
<td>Disk usage for the cluster is above 90%. Delete data or scale the domain, and try again.</td>
</tr>
<tr>
<td>High JVM usage</td>
<td>JVM memory pressure is above 75%. Reduce traffic to the cluster or scale the domain, and try again.</td>
</tr>
<tr>
<td>Kibana alias problem</td>
<td>.kibana is already configured as an alias and maps to an incompatible index, likely one from an earlier version of Kibana. Reindex, and try again.</td>
</tr>
<tr>
<td>Red Kibana status</td>
<td>Kibana status is red. Try using Kibana when the upgrade completes. If the red status persists, resolve it manually, and try again.</td>
</tr>
</tbody>
</table>
### Issue | Description
---|---
Cross-cluster compatibility | You can only upgrade if cross-cluster compatibility is maintained between the source and destination domains post the upgrade. During the upgrade process, any incompatible connections are identified. To proceed with the upgrade, delete the incompatible connections.

Other Amazon ES service issue | Issues with Amazon ES itself might cause your domain to display as ineligible for an upgrade. If none of the preceding conditions apply to your domain and the problem persists for more than a day, contact [AWS Support](mailto:aws-support@amazon.com).

---

**Starting an upgrade**

The upgrade process is irreversible and can't be paused or canceled. During an upgrade, you can't make configuration changes to the domain. Before starting an upgrade, double-check that you want to proceed. You can use these same steps to perform the pre-upgrade check without actually starting an upgrade.

If the cluster has dedicated master nodes, upgrades complete without downtime. Otherwise, the cluster might be unresponsive for several seconds post-upgrade while it elects a master node.

**To upgrade a domain to a later version of Elasticsearch (console)**

1. Take a manual snapshot (p. 51) of your domain. This snapshot serves as a backup that you can restore on a new domain (p. 59) if you want to return to using the prior Elasticsearch version.
2. Go to [https://aws.amazon.com](https://aws.amazon.com), and then choose Sign In to the Console.
4. In the navigation pane, under My domains, choose the domain that you want to upgrade.
5. Choose Actions and Upgrade domain.
6. For Operation, choose Upgrade, Submit, and Continue.
7. Return to the Overview tab and choose Upgrade status to monitor the state of the upgrade.

**To upgrade a domain to a later version of Elasticsearch (AWS CLI and SDK)**

You can use the following operations to identify the right Elasticsearch version for your domain, start an in-place upgrade, perform the pre-upgrade check, and view progress:

- `get-compatible-elasticsearch-versions` (GetCompatibleElasticsearchVersions)
- `upgrade-elasticsearch-domain` (UpgradeElasticsearchDomain)
- `get-upgrade-status` (GetUpgradeStatus)
- `get-upgrade-history` (GetUpgradeHistory)

For more information, see the [AWS CLI Command Reference](https://docs.aws.amazon.com/cli/latest/reference/es/) and [Configuration API reference](https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/)

**Using a snapshot to migrate data**

In-place upgrades are the easier, faster, and more reliable way to upgrade a domain to a later Elasticsearch version. Snapshots are a good option if you need to migrate from a pre-5.1 version of Elasticsearch or want to migrate to an entirely new cluster.

The following table shows how to use snapshots to migrate data to a domain that uses a different Elasticsearch version. For more information about taking and restoring snapshots, see the section called “Creating index snapshots” (p. 51).
<table>
<thead>
<tr>
<th>From Version</th>
<th>To Version</th>
<th>Migration Process</th>
</tr>
</thead>
</table>
| 6.x          | 7.x        | 1. Review breaking changes for 7.0 to see if you need to make adjustments to your indices or applications. For other considerations, see the table in the section called “Upgrading Elasticsearch” (p. 61).  
2. Create a manual snapshot of the 6.x domain.  
3. Create a 7.x domain.  
4. Restore the snapshot from the original domain to the 7.x domain. During the operation, you likely need to restore the .kibana index under a new name: 

```json
POST _snapshot/<repository-name>/<snapshot-name>/_restore
{
  "indices": "*",
  "ignore_unavailable": true,
  "rename_pattern": ".kibana",
  "rename_replacement": ".backup-kibana"
}
```

Then you can reindex .backup-kibana on the new domain and alias it to .kibana.  
5. If you no longer need your original domain, delete it. Otherwise, you continue to incur charges for the domain. |
| 6.x          | 6.8        | 1. Create a manual snapshot of the 6.x domain.  
2. Create a 6.8 domain.  
3. Restore the snapshot from the original domain to the 6.8 domain.  
4. If you no longer need your original domain, delete it. Otherwise, you continue to incur charges for the domain. |
| 5.x          | 6.x        | 1. Review breaking changes for 6.0 to see if you need to make adjustments to your indices or applications. For other considerations, see the table in the section called “Upgrading Elasticsearch” (p. 61).  
2. Create a manual snapshot of the 5.x domain.  
3. Create a 6.x domain.  
4. Restore the snapshot from the original domain to the 6.x domain.  
5. If you no longer need your 5.x domain, delete it. Otherwise, you continue to incur charges for the domain. |
| 5.x          | 5.6        | 1. Create a manual snapshot of the 5.x domain.  
2. Create a 5.6 domain.  
3. Restore the snapshot from the original domain to the 5.6 domain.  
4. If you no longer need your original domain, delete it. Otherwise, you continue to incur charges for the domain. |
| 2.3          | 6.x        | Elasticsearch 2.3 snapshots are not compatible with 6.x. To migrate your data directly from 2.3 to 6.x, you must manually recreate your indices in the new domain. |
### Creating a custom endpoint for Amazon Elasticsearch Service

Creating a custom endpoint for your Amazon Elasticsearch Service (Amazon ES) domain makes it easier for you to refer to your Elasticsearch and Kibana URLs. You can include your company's branding or just use a shorter, easier-to-remember endpoint than the standard one.

If you ever need to switch to a new domain, just update your DNS to point to the new URL and continue using the same endpoint as before.

<table>
<thead>
<tr>
<th>From Version</th>
<th>To Version</th>
<th>Migration Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3</td>
<td>5.x</td>
<td>Alternately, you can follow the 2.3 to 5.x steps in this table, perform _reindex operations in the new 5.x domain to convert your 2.3 indices to 5.x indices, and then follow the 5.x to 6.x steps.</td>
</tr>
<tr>
<td>1.5</td>
<td>5.x</td>
<td>Elasticsearch 1.5 snapshots are not compatible with 5.x. To migrate your data from 1.5 to 5.x, you must manually recreate your indices in the new domain. <strong>Important</strong> 1.5 snapshots are compatible with 2.3, but Amazon ES 2.3 domains do not support the _reindex operation. Because you cannot reindex them, indices that originated in a 1.5 domain still fail to restore from 2.3 snapshots to 5.x domains.</td>
</tr>
</tbody>
</table>
| 1.5          | 2.3        | 1. Use the migration plugin to find out if you can directly upgrade to version 2.3. You might need to make changes to your data before migration.  
b. Choose **Run checks now**.  
c. Review the results and, if needed, follow the instructions to make changes to your data. |

---

Creating a custom endpoint for Amazon Elasticsearch Service

Creating a custom endpoint for your Amazon Elasticsearch Service (Amazon ES) domain makes it easier for you to refer to your Elasticsearch and Kibana URLs. You can include your company's branding or just use a shorter, easier-to-remember endpoint than the standard one.

If you ever need to switch to a new domain, just update your DNS to point to the new URL and continue using the same endpoint as before.

### From Version | To Version | Migration Process
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3</td>
<td>5.x</td>
<td>Alternately, you can follow the 2.3 to 5.x steps in this table, perform _reindex operations in the new 5.x domain to convert your 2.3 indices to 5.x indices, and then follow the 5.x to 6.x steps.</td>
</tr>
<tr>
<td>1.5</td>
<td>5.x</td>
<td>Elasticsearch 1.5 snapshots are not compatible with 5.x. To migrate your data from 1.5 to 5.x, you must manually recreate your indices in the new domain. <strong>Important</strong> 1.5 snapshots are compatible with 2.3, but Amazon ES 2.3 domains do not support the _reindex operation. Because you cannot reindex them, indices that originated in a 1.5 domain still fail to restore from 2.3 snapshots to 5.x domains.</td>
</tr>
</tbody>
</table>
| 1.5            | 2.3        | 1. Use the migration plugin to find out if you can directly upgrade to version 2.3. You might need to make changes to your data before migration.  
b. Choose **Run checks now**.  
c. Review the results and, if needed, follow the instructions to make changes to your data. |
You secure custom endpoints by either generating a certificate in AWS Certificate Manager (ACM) or importing one of your own.

Custom endpoints for new domains

You can enable a custom endpoint for a new Amazon ES domain using the Amazon ES console, AWS CLI, or configuration API.

To customize your endpoint (console)

1. From the Amazon ES, choose Create a new domain.
2. Select a deployment type and version and choose Next.
3. Provide a domain name.
4. Under Custom endpoint, select Enable custom endpoint.
5. For Custom hostname, enter your preferred custom endpoint hostname. The hostname should be a fully qualified domain name (FQDN), such as www.yourdomain.com or example.yourdomain.com.

   Note
   If you don't have a wildcard certificate you must obtain a new certificate for your custom endpoint's subdomains.

   6. For AWS certificate, choose the SSL certificate to use for your domain. If no certificates are available, you can import one into ACM or use ACM to provision one. For more information, see Issuing and Managing Certificates in the AWS Certificate Manager User Guide.

      Note
      The certificate must have the custom endpoint name and be in the same account as your Amazon ES domain.

      • Follow the rest of the steps to create your domain and choose Confirm.
      • Select the domain when it's finished processing to view your custom endpoint.

To use the CLI or configuration API, use the CreateElasticsearchDomain and UpdateElasticsearchDomainConfig operations. For more information, see the AWS CLI Command Reference and Configuration API reference (p. 339).

Custom endpoints for existing domains

To add a custom endpoint to an existing Amazon ES domain, choose Edit domain and perform steps 4–6 above.

Next steps

After you enable a custom endpoint for your Amazon ES domain, you must create a CNAME mapping in Amazon Route 53 (or your preferred DNS service provider) to route traffic to the custom endpoint and its subdomains. Without this mapping, your custom endpoint won't work. For steps to create this mapping in Route 53, see Configuring DNS routing for a new domain and Creating a hosted zone for a subdomain. For other providers, consult their documentation.

If you use SAML authentication for Kibana (p. 123), you must update your IdP with the new SSO URL.

Auto-Tune for Amazon Elasticsearch Service

Auto-Tune in Amazon Elasticsearch Service (Amazon ES) uses performance and usage metrics from your Elasticsearch cluster to suggest changes to the Java virtual machine (JVM) settings on your nodes. These optional changes improve cluster speed and stability.
Some changes deploy immediately, while others require you to schedule a maintenance window. You can revert to the default Amazon ES settings at any time.

As Auto-Tune gathers and analyzes performance metrics for your domain, view its recommendations in the Amazon ES console on the Notifications page.

Auto-Tune is available in commercial Regions on domains running Elasticsearch 6.7 or later with a supported instance type (p. 272).

**Enabling or disabling Auto-Tune**

Amazon ES enables Auto-Tune by default on new domains. To enable or disable Auto-Tune on existing domains, we recommend using the console, which greatly simplifies the process. In the console, choose your domain and **Edit domain**, then configure the settings in the **Auto-Tune** section.

**AWS CLI**

To use the AWS CLI, configure the `auto-tune-options` parameters. The following sample command enables Auto-Tune on an existing domain with a maintenance schedule that repeats every day at 12:00pm UTC:

```bash
aws es update-elasticsearch-domain-config --domain-name mylogs --auto-tune-options '{"DesiredState": "ENABLED","MaintenanceSchedules": [{"StartAt": "2021-12-19","Duration": {"Value": 2,"Unit": "HOURS"},"CronExpressionForRecurrence": "cron(0 12 * * ? *)"}]}'
```

**Configuration API**

To use the configuration API (p. 339), configure the `AutoTuneOptions` settings:

```json
POST https://es.us-east-1.amazonaws.com/2015-01-01/es/domain/domain-name/config
{
    "AutoTuneOptions": {
        "DesiredState": "ENABLED",
        "MaintenanceSchedules": [
            {
                "StartAt": 4104152288000,
                "Duration": {
                    "Value": 2,
                    "Unit": "HOURS"
                },
                "CronExpressionForRecurrence": "cron(0 12 * * ? *)"
            }
        ]
    }
}
```

Auto-Tune has two broad categories of changes:

- Nondisruptive changes that it applies as the cluster runs
- Changes that require a blue/green deployment (p. 14)

If you enable Auto-Tune without setting a maintenance window, Auto-Tune only applies nondisruptive changes. The performance benefits over time are generally smaller, but you avoid the overhead associated with blue/green deployments.

For guidance on configuring maintenance windows, see the section called “Scheduling changes” (p. 69).
Scheduling changes

To apply changes that require a blue/green deployment, you schedule a maintenance window for your domain—for example, between 6:00 and 9:00 AM on a Friday morning. We recommend scheduling maintenance windows for low-traffic times.

- To review all changes before deploying them, wait for Auto-Tune to notify you of a suggested optimization. Then schedule a one-time maintenance window to deploy the changes.
- For a more automated experience, set a weekly maintenance window, such as every Saturday at 2:00 AM, or use a custom Cron expression (p. 69) for more complex schedules.

To schedule changes in the console, choose your domain, choose the Auto-Tune tab, choose Modify, and then choose Submit. This tab also shows your current maintenance window and whether Auto-Tune will make any changes during the next window.

Cron expressions

Cron expressions for Auto-Tune use the same six-field syntax as Amazon CloudWatch Events:

<table>
<thead>
<tr>
<th>Field</th>
<th>Valid Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minute</td>
<td>0–59</td>
</tr>
<tr>
<td>Hour</td>
<td>0–23</td>
</tr>
<tr>
<td>Day of month</td>
<td>1–31</td>
</tr>
<tr>
<td>Month</td>
<td>1–12 or JAN, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP, OCT, NOV, DEC</td>
</tr>
<tr>
<td>Day of week</td>
<td>1–7 or SUN, MON, TUE, WED, THU, FRI, SAT</td>
</tr>
<tr>
<td>Year</td>
<td>1970–2199</td>
</tr>
</tbody>
</table>

Day of month and day of week overlap, so you can specify one, but not both. You must mark the other as ?. For a full summary of wildcard options, see the Amazon CloudWatch Events User Guide.

Types of changes

Based on your domain's performance metrics, Auto-Tune can suggest adjustments to the following settings.

<table>
<thead>
<tr>
<th>Change Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>JVM heap size</td>
<td>By default, Amazon ES uses 50% of an instance's RAM for the JVM heap, up to a heap size of 32 GiB.</td>
</tr>
</tbody>
</table>
Tagging Amazon Elasticsearch Service domains

Tags let you assign arbitrary information to an Amazon Elasticsearch Service (Amazon ES) domain so you can categorize and filter on that information. A tag is a key-value pair that you define and associate with an Amazon ES domain. You can use these tags to track costs by grouping expenses for similarly tagged resources. AWS doesn't apply any semantic meaning to your tags. Tags are interpreted strictly as character strings. All tags have the following elements:

<table>
<thead>
<tr>
<th>Tag Element</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag key</td>
<td>The tag key is the name of the tag. Key must be unique to the Amazon ES domain to which they're attached. For a list of basic restrictions on tag keys and values, see User-Defined Tag Restrictions.</td>
<td>Yes</td>
</tr>
<tr>
<td>Tag value</td>
<td>The tag value is the string value of the tag. Tag values can be null and don't have to be unique in a tag set. For example, you can have a key-value pair in a tag set of project/Trinity and cost-center/Trinity. For a list of basic restrictions on tag keys and values, see User-Defined Tag Restrictions.</td>
<td>No</td>
</tr>
</tbody>
</table>

Each Amazon ES domain has a tag set, which contains all the tags assigned to that Amazon ES domain. AWS doesn't automatically assign any tags to Amazon ES domains. A tag set can contain between 0 and 50 tags. If you add a tag to a domain with the same key as an existing tag, the new value overwrites the old value.

Tagging examples

You can use a key to define a category, and the value could be an item in that category. For example, you could define a tag key of project and a tag value of Salix, indicating that the Amazon ES domain is assigned to the Salix project. You could also use tags to designate Amazon ES domains as being used for test or production by using a key such as environment=test or environment=production. Try to use a consistent set of tag keys to make it easier to track metadata that is associated with Amazon ES domains.

You also can use tags to organize your AWS bill to reflect your own cost structure. To do this, sign up to get your AWS account bill with tag key values included. Then, organize your billing information according to resources with the same tag key values to see the cost of combined resources. For example, you can tag several Amazon ES domains with key-value pairs, and then organize your billing information to see the total cost for each domain across several services. For more information, see Using Cost Allocation Tags in the AWS Billing and Cost Management documentation.

Note

Tags are cached for authorization purposes. Because of this, additions and updates to tags on Amazon ES domains might take several minutes before they're available.
Working with tags (console)

The console is the simplest way to tag a domain.

To create a tag (console)

1. Go to https://aws.amazon.com, and then choose Sign In to the Console.
2. Under Analytics, choose Elasticsearch Service.
3. In the navigation pane, choose your Amazon ES domain.
4. On the domain dashboard, choose Manage tags.
5. In the Key column, enter a tag key.
6. (Optional) In the Value column, enter a tag value.
7. Choose Submit.

To delete a tag (console)

Use the following procedure to delete a resource tag.

1. Go to https://aws.amazon.com, and then choose Sign In to the Console.
2. Under Analytics, choose Elasticsearch Service.
3. In the navigation pane, choose your Amazon ES domain.
4. On the domain dashboard, choose Manage tags.
5. Next to the tag that you want to delete, choose Remove.
6. Choose Submit.

For more information about using the console to work with tags, see Working with Tag Editor in the AWS Management Console Getting Started Guide.

Working with tags (AWS CLI)

You can create resource tags using the AWS CLI with the --add-tags command.

Syntax

```
add-tags --arn=<domain_arn> --tag-list Key=<key>,Value=<value>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--arn</td>
<td>Amazon resource name for the Amazon ES domain to which the tag is attached.</td>
</tr>
<tr>
<td>--tag-list</td>
<td>Set of space-separated key-value pairs in the following format: Key=&lt;key&gt;,Value=&lt;value&gt;</td>
</tr>
</tbody>
</table>

Example

The following example creates two tags for the logs domain:

```
aws es add-tags --arn arn:aws:es:us-east-1:379931976431:domain/logs --tag-list Key=service,Value=Elasticsearch Key=instances,Value=m3.2xlarge
```
You can remove tags from an Amazon ES domain using the `remove-tags` command.

**Syntax**

```
remove-tags --arn=<domain_arn> --tag-keys Key=<key>,Value=<value>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--arn</td>
<td>Amazon Resource Name (ARN) for the Amazon ES domain to which the tag is attached.</td>
</tr>
<tr>
<td>--tag-keys</td>
<td>Set of space-separated key-value pairs that you want to remove from the Amazon ES domain.</td>
</tr>
</tbody>
</table>

**Example**

The following example removes two tags from the `logs` domain that were created in the preceding example:

```
```

You can view the existing tags for an Amazon ES domain with the `list-tags` command:

**Syntax**

```
list-tags --arn=<domain_arn>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--arn</td>
<td>Amazon Resource Name (ARN) for the Amazon ES domain to which the tags are attached.</td>
</tr>
</tbody>
</table>

**Example**

The following example lists all resource tags for the `logs` domain:

```
aws es list-tags --arn arn:aws:es:us-east-1:379931976431:domain/logs
```

**Working with tags (AWS SDKs)**

The AWS SDKs (except the Android and iOS SDKs) support all the actions defined in the Amazon ES configuration API reference (p. 339), including the `AddTags`, `ListTags`, and `RemoveTags` operations. For more information about installing and using the AWS SDKs, see AWS Software Development Kits.
Security in Amazon Elasticsearch Service

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that is built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The shared responsibility model describes this as security of the cloud and security in the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS compliance programs. To learn about the compliance programs that apply to Amazon Elasticsearch Service, see AWS Services in Scope by Compliance Program.

- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company’s requirements, and applicable IAWS and regulations.

This documentation helps you understand how to apply the shared responsibility model when using Amazon ES. The following topics show you how to configure Amazon ES to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your Amazon ES resources.

**Topics**

- [Data protection in Amazon Elasticsearch Service](p. 73)
- [Identity and Access Management in Amazon Elasticsearch Service](p. 77)
- [Fine-grained access control in Amazon Elasticsearch Service](p. 90)
- [Managing audit logs in Amazon Elasticsearch Service](p. 109)
- [Monitoring Amazon Elasticsearch Service configuration API activity](p. 119)
- [Compliance validation for Amazon Elasticsearch Service](p. 121)
- [Resilience in Amazon Elasticsearch Service](p. 122)
- [Infrastructure security in Amazon Elasticsearch Service](p. 122)
- [SAML authentication for Kibana](p. 123)
- [Configuring Amazon Cognito authentication for Kibana](p. 128)
- [Using service-linked roles to provide Amazon Elasticsearch Service access to resources](p. 141)

Data protection in Amazon Elasticsearch Service

The AWS shared responsibility model applies to data protection in Amazon Elasticsearch Service. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. This content includes the security configuration and management tasks for the
AWS services that you use. For more information about data privacy, see the [Data Privacy FAQ](#). For information about data protection in Europe, see the [AWS Shared Responsibility Model and GDPR](#) blog post on the [AWS Security Blog](#).

For data protection purposes, we recommend that you protect AWS account credentials and set up individual user accounts with AWS Identity and Access Management (IAM). That way each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. We recommend TLS 1.2 or later.
- Set up API and user activity logging with AWS CloudTrail.
- Use AWS encryption solutions, along with all default security controls within AWS services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing personal data that is stored in Amazon S3.
- If you require FIPS 140-2 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see [Federal Information Processing Standard (FIPS) 140-2](#).

We strongly recommend that you never put sensitive identifying information, such as your customers' account numbers, into free-form fields such as a Name field. This includes when you work with Amazon ES or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into Amazon ES or other services might get picked up for inclusion in diagnostic logs. When you provide a URL to an external server, don't include credentials information in the URL to validate your request to that server.

## Encryption of data at rest for Amazon Elasticsearch Service

Amazon ES domains offer encryption of data at rest, a security feature that helps prevent unauthorized access to your data. The feature uses AWS Key Management Service (AWS KMS) to store and manage your encryption keys and the Advanced Encryption Standard algorithm with 256-bit keys (AES-256) to perform the encryption. If enabled, the feature encrypts the following aspects of a domain:

- All indices (including those in UltraWarm storage)
- Elasticsearch logs
- Swap files
- All other data in the application directory
- Automated snapshots

The following are not encrypted when you enable encryption of data at rest, but you can take additional steps to protect them:

- Manual snapshots: You currently can't use KMS master keys to encrypt manual snapshots. You can, however, use server-side encryption with S3-managed keys or customer master keys (CMKs) to encrypt the bucket you use as a snapshot repository. For instructions, see the section called “Registering a manual snapshot repository” (p. 55).
- Slow logs and error logs: If you publish logs (p. 47) and want to encrypt them, you can encrypt their CloudWatch Logs log group using the same AWS KMS master key as the Amazon ES domain. For more information, see [Encrypt Log Data in CloudWatch Logs Using AWS KMS](#) in the [Amazon CloudWatch Logs User Guide](#).
Amazon ES supports only symmetric customer master keys, not asymmetric ones. To learn how to create symmetric customer master keys, see Creating Keys in the AWS Key Management Service Developer Guide.

Regardless of whether encryption at rest is enabled, all domains automatically encrypt custom packages (p. 177) using AES-256 and Amazon ES-managed keys.

**Enabling encryption of data at rest**

Encryption of data at rest on new domains requires Elasticsearch 5.1 or later. Enabling the feature on existing domains requires Elasticsearch 6.7 or later. Choose the existing domain in the AWS console, Actions, and Modify encryption.

To use the Amazon ES console to configure encryption of data at rest, you must have read permissions to AWS KMS, such as the following identity-based policy:

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "kms:List*",
            "kms:Describe*"
         ],
         "Resource": "*"
      }
   ]
}
```

If you want to use a master key other than (Default) aws/es, you must also have permissions to create grants for the key. These permissions typically take the form of a resource-based policy that you specify when you create the key.

If you want to keep your key exclusive to Amazon ES, you can add the `kms:ViaService` condition to that key policy:

```json
"Condition": {
   "StringEquals": {
      "kms:ViaService": "es.us-west-1.amazonaws.com"
   },
   "Bool": {          
      "kms:GrantIsForAWSResource": "true"
   }
}
```

For more information, see Using Key Policies in AWS KMS in the AWS Key Management Service Developer Guide.

**Warning**

If you delete the key that you used to encrypt a domain, the domain becomes inaccessible. The Amazon ES team can't help you recover your data. AWS KMS deletes master keys only after a waiting period of at least seven days, so the Amazon ES team might contact you if they detect that your domain is at risk.

**Disabling encryption of data at rest**

After you configure a domain to encrypt data at rest, you can't disable the setting. Instead, you can take a manual snapshot (p. 51) of the existing domain, create another domain (p. 9), migrate your data, and delete the old domain.
Monitoring domains that encrypt data at rest

Domains that encrypt data at rest have two additional metrics: `KMSKeyError` and `KMSKeyInaccessible`. These metrics appear only if the domain encounters a problem with your encryption key. For full descriptions of these metrics, see the section called “Cluster metrics” (p. 30). You can view them using either the Amazon ES console or the Amazon CloudWatch console.

Tip
Each metric represents a significant problem for a domain, so we recommend that you create CloudWatch alarms for both. For more information, see the section called “Recommended CloudWatch alarms” (p. 270).

Other considerations

- Automatic key rotation preserves the properties of your AWS KMS master keys, so the rotation has no effect on your ability to access your Elasticsearch data. Encrypted Amazon ES domains don't support manual key rotation, which involves creating a new master key and updating any references to the old key. To learn more, see Rotating Customer Master Keys in the AWS Key Management Service Developer Guide.

- Certain instance types don't support encryption of data at rest. For details, see the section called “Supported instance types” (p. 272).

- Domains that encrypt data at rest use a different repository name for their automated snapshots. For more information, see the section called “Restoring snapshots” (p. 59).

- Encrypting an Amazon ES domain requires a grant, and each encryption key has a limit of 500 grants per principal. This limit means that the maximum number of Amazon ES domains that you can encrypt using a single key is 500. Currently, Amazon ES supports a maximum of 100 domains per account (per Region), so this grant limit is of no consequence. If the domain limit per account increases, however, the grant limit might become relevant.

If you need to encrypt more than 500 domains at that time, you can create additional keys. Keys are regional, not global, so if you operate in more than one AWS Region, you already need multiple keys.

Node-to-node encryption for Amazon Elasticsearch Service

Node-to-node encryption provides an additional layer of security on top of the default features of Amazon ES.

Each Amazon ES domain—regardless of whether the domain uses VPC access—resides within its own, dedicated VPC. This architecture prevents potential attackers from intercepting traffic between Elasticsearch nodes and keeps the cluster secure. By default, however, traffic within the VPC is unencrypted. Node-to-node encryption enables TLS 1.2 encryption for all communications within the VPC.

If you send data to Amazon ES over HTTPS, node-to-node encryption helps ensure that your data remains encrypted as Elasticsearch distributes (and redistributes) it throughout the cluster. If data arrives unencrypted over HTTP, Amazon ES encrypts it after it reaches the cluster. You can require that all traffic to the domain arrive over HTTPS using the console, AWS CLI, or configuration API.

Enabling node-to-node encryption

Node-to-node encryption on new domains requires Elasticsearch 6.0 or later. Enabling the feature on existing domains requires Elasticsearch 6.7 or later. Choose the existing domain in the AWS console, Actions, and Modify encryption.
Alternatively, you can use the AWS CLI or configuration API. For more information, see the AWS CLI Command Reference and Configuration API reference (p. 339).

Disabling node-to-node encryption

After you configure a domain to use node-to-node encryption, you can't disable the setting. Instead, you can take a manual snapshot (p. 51) of the encrypted domain, create another domain (p. 9), migrate your data, and delete the old domain.

Identity and Access Management in Amazon Elasticsearch Service

Amazon Elasticsearch Service (Amazon ES) offers several ways to control access to your domains. This topic covers the various policy types, how they interact with each other, and how to create your own custom policies.

Important

VPC support introduces some additional considerations to Amazon ES access control. For more information, see the section called “About access policies on VPC domains” (p. 25).

Types of policies

Amazon ES supports three types of access policies:

- the section called “Resource-based policies” (p. 77)
- the section called “Identity-based policies” (p. 79)
- the section called “IP-based policies” (p. 80)

Resource-based policies

You add a resource-based policy, often called the domain access policy, when you create a domain. These policies specify which actions a principal can perform on the domain’s subresources. Subresources include Elasticsearch indices and APIs.

The Principal element specifies the accounts, users, or roles that are allowed access. The Resource element specifies which subresources these principals can access. The following resource-based policy grants test-user full access (es:* ) to the subresources on test-domain:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iamb:123456789012:user/test-user"
        ],
      },
      "Action": ["es:*"],
    }
  ]
}
```
Two important considerations apply to this policy:

- These privileges apply only to this domain. Unless you create similar policies on other domains, test-user can only access test-domain.
- The trailing */ in the Resource element is significant and indicates that resource-based policies only apply to the domain's subresources, not the domain itself. In resource-based policies, the es:* action is equivalent to es:ESHttp*.

For example, test-user can make requests against an index (GET https://search-test-domain.us-west-1.es.amazonaws.com/test-index), but can't update the domain's configuration (POST https://es.us-west-1.amazonaws.com/2015-01-01/es/domain/test-domain/config). Note the difference between the two endpoints. Accessing the configuration API (p. 339) requires an identity-based policy (p. 79).

To further restrict test-user, you can apply the following policy:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": ["arn:aws:iam::123456789012:user/test-user"],
      },
      "Action": ["es:ESHttpGet"],
    }
  ]
}
```

Now test-user can perform only one operation: searches against test-index. All other indices within the domain are inaccessible, and without permissions to use the es:ESHttpPut or es:ESHttpPost actions, test-user can't add or modify documents.

Next, you might decide to configure a role for power users. This policy gives power-user-role access to the HTTP GET and PUT methods for all URIs in the index:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": ["arn:aws:iam::123456789012:role/power-user-role"],
      },
      "Action": ["es:ESHttpGet", "es:ESHttpPut"],
    }
  ]
}
```
If your domain is in a VPC or uses fine-grained access control, you can use an open domain access policy. Otherwise, your domain access policy must contain some restriction, either by principal or IP address.

For information about all available actions, see the section called “Policy element reference” (p. 83). For far more granular control over your data, use an open domain access policy with fine-grained access control (p. 90).

1. **Identity-based policies**

Unlike resource-based policies, which are a part of each Amazon ES domain, you attach identity-based policies to users or roles using the AWS Identity and Access Management (IAM) service. Just like resource-based policies (p. 77), identity-based policies specify who can access a service, which actions they can perform, and if applicable, the resources on which they can perform those actions.

While they certainly don't have to be, identity-based policies tend to be more generic. They often govern only the configuration API actions a user can perform. After you have these policies in place, you can use resource-based policies (or fine-grained access control (p. 90)) in Amazon ES to offer users access to Elasticsearch indices and APIs.

**Note**

Users with the AWS managed AmazonESReadOnlyAccess policy can't see cluster health status on the console. To allow them to see cluster health status (and other Elasticsearch data), add the es:ESHttpGet action to an access policy and attach it to their accounts or roles.

Because identity-based policies attach to users or roles (principals), the JSON doesn't specify a principal. The following policy grants access to actions that begin with Describe and List. This combination of actions provides read-only access to domain configurations, but not to the data stored in the domain itself:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "es:Describe*",
        "es:List*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

An administrator might have full access to Amazon ES and all data stored on all domains:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "es:*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```
Identity-based policies let you use tags to control access to the configuration API (not the Elasticsearch APIs). The following policy, for example, lets attached principals view and update a domain's configuration if the domain has the `team:devops` tag:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:ResourceTag/team": ["devops"
        ]
      }
    }
  ]
}
```

Similarly, Amazon ES supports the `RequestTag` and `TagKeys` global condition keys for the configuration API. These conditions only apply to API calls that include tags within the request, such as `CreateElasticsearchDomain`, `AddTags`, and `RemoveTags`. The following policy lets attached principals create domains, but only if they include the `team:it` tag in the request:

```json
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": ["es:CreateElasticsearchDomain", "es:AddTags"],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:RequestTag/team": ["it"
      ]
    }
  }
}
```

For more details on using tags for access control and the differences between resource-based and identity-based policies, see the IAM User Guide.

**IP-based policies**

IP-based policies restrict access to a domain to one or more IP addresses or CIDR blocks. Technically, IP-based policies are not a distinct type of policy. Instead, they are just resource-based policies that specify an anonymous principal and include a special `Condition` element.
The primary appeal of IP-based policies is that they allow unsigned requests to an Amazon ES domain, which lets you use clients like `curl` and Kibana (p. 216) or access the domain through a proxy server. To learn more, see the section called “Using a proxy to access Amazon ES from Kibana” (p. 216).

**Note**

If you enabled VPC access for your domain, you can't configure an IP-based policy. Instead, you can use security groups to control which IP addresses can access the domain. For more information, see the section called “About access policies on VPC domains” (p. 25).

The following policy grants all HTTP requests that originate from the specified IP range access to test-domain:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "es:ESHttp*
      ],
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": [
            "192.0.2.0/24"
          ]
        }
      },
    }
  ]
}
```

If your domain has a public endpoint and doesn't use fine-grained access control (p. 90), we recommend combining IAM principals and IP addresses. This policy grants test-user HTTP access only if the request originates from the specified IP range:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "arn:aws:iam::987654321098:user/test-user"
      ]
    },
    "Action": [
      "es:ESHttp*"
    ],
    "Condition": {
      "IpAddress": {
        "aws:SourceIp": [
          "192.0.2.0/24"
        ]
      }
    },
  }
}
```
Making and signing Amazon ES requests

Even if you configure a completely open resource-based access policy, all requests to the Amazon ES configuration API must be signed. If your policies specify IAM users or roles, requests to the Elasticsearch APIs also must be signed using AWS Signature Version 4. The signing method differs by API:

- To make calls to the Amazon ES configuration API, we recommend that you use one of the AWS SDKs. The SDKs greatly simplify the process and can save you a significant amount of time compared to creating and signing your own requests. The configuration API endpoints use the following format:

  `es.region.amazonaws.com/2015-01-01/`

  For example, the following request makes a configuration change to the `movies` domain, but you have to sign it yourself (not recommended):

  ```
  POST https://es.us-east-1.amazonaws.com/2015-01-01/es/domain/movies/config
  {
    "ElasticsearchClusterConfig": {
      "InstanceType": "c5.xlarge.elasticsearch"
    }
  }
  ```

  If you use one of the SDKs, such as Boto 3, the SDK automatically handles the request signing:

  ```
  import boto3
  client = boto3.client('es')
  response = client.update_elasticsearch_domain_config(
    DomainName='movies',
    ElasticsearchClusterConfig={
      'InstanceType': 'c5.xlarge.elasticsearch'
    }
  )
  ```

  For a Java code sample, see the section called "Using the AWS SDKs" (p. 153).

- To make calls to the Elasticsearch APIs, you must sign your own requests. For sample code in a variety of languages, see the section called "Signing HTTP requests" (p. 143). The Elasticsearch APIs use the following format:

  `domain-id.region.es.amazonaws.com`

  For example, the following request searches the `movies` index for `thor`:

  ```
  GET https://my-domain.us-east-1.es.amazonaws.com/movies/_search?q=thor
  ```

  **Note**
  The service ignores parameters passed in URLs for HTTP POST requests that are signed with Signature Version 4.

When policies collide

Complexities arise when policies disagree or make no explicit mention of a user. Understanding How IAM Works in the IAM User Guide provides a concise summary of policy evaluation logic:
• By default, all requests are denied.
• An explicit allow overrides this default.
• An explicit deny overrides any allows.

For example, if a resource-based policy grants you access to a domain subresource (an Elasticsearch index or API), but an identity-based policy denies you access, you are denied access. If an identity-based policy grants access and a resource-based policy does not specify whether or not you should have access, you are allowed access. See the following table of intersecting policies for a full summary of outcomes for domain subresources.

<table>
<thead>
<tr>
<th>Allowed in Identity-based Policy</th>
<th>Denied in Resource-based Policy</th>
<th>Neither Allowed nor Denied in Resource-based Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>Deny</td>
<td>Allow</td>
</tr>
<tr>
<td>Deny</td>
<td>Deny</td>
<td>Deny</td>
</tr>
<tr>
<td>Allow</td>
<td>Deny</td>
<td>Deny</td>
</tr>
</tbody>
</table>

**Policy element reference**

Amazon ES supports most policy elements in the IAM Policy Elements Reference, with the exception of NotPrincipal. The following table shows the most common elements.

<table>
<thead>
<tr>
<th>JSON Policy Element</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>The current version of the policy language is 2012-10-17. All access policies should specify this value.</td>
</tr>
<tr>
<td>Effect</td>
<td>This element specifies whether the statement allows or denies access to the specified actions. Valid values are Allow or Deny.</td>
</tr>
<tr>
<td>Principal</td>
<td>This element specifies the AWS account or IAM user or role that is allowed or denied access to a resource and can take several forms:</td>
</tr>
<tr>
<td></td>
<td>• <strong>AWS accounts:</strong> &quot;Principal&quot;:{&quot;AWS&quot;: [&quot;123456789012&quot;]} or &quot;Principal&quot;:{&quot;AWS&quot;: [&quot;arn:aws:iam::123456789012:root&quot;]}</td>
</tr>
<tr>
<td></td>
<td>• <strong>IAM users:</strong> &quot;Principal&quot;:{&quot;AWS&quot;: [&quot;arn:aws:iam::123456789012:user/test-user&quot;]}</td>
</tr>
<tr>
<td></td>
<td>• <strong>IAM roles:</strong> &quot;Principal&quot;:{&quot;AWS&quot;: [&quot;arn:aws:iam::123456789012:role/test-role&quot;]}</td>
</tr>
<tr>
<td>Action</td>
<td>Amazon ES uses the following actions for HTTP methods:</td>
</tr>
<tr>
<td></td>
<td>• es:ESHttpDelete</td>
</tr>
</tbody>
</table>

Specifying the * wildcard enables anonymous access to the domain, which we don't recommend unless you add an IP-based condition (p. 80), use VPC support (p. 22), or enable fine-grained access control (p. 90).
Amazon Elasticsearch Service Developer Guide
Policy element reference

<table>
<thead>
<tr>
<th>JSON Policy Element</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>es:ESHttpGet</td>
<td></td>
</tr>
<tr>
<td>es:ESHttpHead</td>
<td></td>
</tr>
<tr>
<td>es:ESHttpPost</td>
<td></td>
</tr>
<tr>
<td>es:ESHttpPut</td>
<td></td>
</tr>
<tr>
<td>es:ESHttpPatch</td>
<td></td>
</tr>
</tbody>
</table>

Amazon ES uses the following actions for the configuration API (p. 339):

- es:AddTags
- es:AssociatePackage
- es:CreateElasticsearchDomain
- es:CreateElasticsearchServiceRole
- es:CreatePackage
- es:DeleteElasticsearchDomain
- es:DeleteElasticsearchServiceRole
- es:DeletePackage
- es:DescribeElasticsearchDomain
- es:DescribeElasticsearchDomainConfig
- es:DescribeElasticsearchDomains
- es:DescribeElasticsearchInstanceTypeLimits
- es:DescribeReservedElasticsearchInstanceOfferings
- es:DescribeReservedElasticsearchInstances
- es:DissociatePackage
- es:ESCrossClusterGet
- es:GetCompatibleElasticsearchVersions
- es:ListDomainNames
- es:ListElasticsearchInstanceTypeDetails
- es:ListElasticsearchInstanceTypes
- es:ListElasticsearchVersions
- es:ListTags
- es:PurchaseReservedElasticsearchInstanceOffering
- es:RemoveTags
- es:UpdateElasticsearchDomainConfig

**Tip**

You can use wildcards to specify a subset of actions, such as "Action": "es:*" or "Action": "es:Describe*".

Certain `es:` actions support resource-level permissions. For example, you can give a user permissions to delete one particular domain without giving that user permissions to delete any domain. Other actions apply only to the service itself. For example, `es:ListDomainNames` makes no sense in the context of a single domain and thus requires a wildcard.

**Important**

Resource-based policies differ from resource-level permissions. Resource-based policies (p. 77) are full JSON policies that attach to domains. Resource-level permissions let you restrict actions to
particular domains or subresources. In practice, you can think of resource-level permissions as an optional part of a resource- or identity-based policy.

The following identity-based policy (p. 79) lists all es: actions and groups them according to whether they apply to the domain subresources (test-domain/*), to the domain configuration (test-domain), or only to the service (*):

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "es:ESHttpDelete",
        "es:ESHttpGet",
        "es:ESHttpHead",
        "es:ESHttpPost",
        "es:ESHttpPut",
        "es:ESHttpPatch"
      ],
    },
    {
      "Effect": "Allow",
      "Action": [
        "es:AssociatePackage",
        "es:CreateElasticsearchDomain",
        "es:DeleteElasticsearchDomain",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomainConfig",
        "es:DescribeElasticsearchDomains",
        "es:DissociatePackage",
        "es:ESCrossClusterGet",
        "es:GetCompatibleElasticsearchVersions",
        "es:UpdateElasticsearchDomainConfig"
      ],
    },
    {
      "Effect": "Allow",
      "Action": [
        "es:AddTags",
        "es:CreateElasticsearchServiceRole",
        "es:CreatePackage",
        "es:DeleteElasticsearchServiceRole",
        "es:DeletePackage",
        "es:DescribeElasticsearchInstanceTypeLimits",
        "es:DescribeReservedElasticsearchInstanceOfferings",
        "es:DescribeReservedElasticsearchInstances",
        "es:ESCrossClusterGet",
        "es:ListDomainNames",
        "es:ListElasticsearchInstanceTypeDetails",
        "es:ListElasticsearchInstanceTypes",
        "es:ListElasticsearchVersions",
        "es:ListTags",
        "es:PurchaseReservedElasticsearchInstanceOffering",
        "es:RemoveTags"
      ]
    }
  ]
}
```
<table>
<thead>
<tr>
<th>JSON Policy Element</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Resource&quot;: &quot;*&quot;</td>
<td>[ ]</td>
</tr>
</tbody>
</table>

**Note**  
While resource-level permissions for `es:CreateElasticsearchDomain` might seem unintuitive —after all, why give a user permissions to create a domain that already exists?—the use of a wildcard lets you enforce a simple naming scheme for your domains, such as "Resource": "arn:aws:es:us-west-1:987654321098:domain/my-team-name-*".  

Of course, nothing prevents you from including actions alongside less restrictive resource elements, such as the following:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "es:ESHttpGet",
                "es:DescribeElasticsearchDomain"
            ],
            "Resource": "*"
        }
    ]
}
```

To learn more about pairing actions and resources, see the Resource element in this table.

### Condition

Amazon ES supports most conditions that are described in [Available Global Condition Keys](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_condition keys.html) in the *IAM User Guide*. Notable exceptions include the `aws:SecureTransport` and `aws:PrincipalTag` keys, which Amazon ES does not support.

When configuring an IP-based policy (p. 80), you specify the IP addresses or CIDR block as a condition, such as the following:

```
"Condition": {
    "IpAddress": {
        "aws:SourceIp": [
            "192.0.2.0/32"
        ]
    }
}
```

As noted in the section called "Identity-based policies" (p. 79), the `aws:ResourceTag`, `aws:RequestTag`, and `aws:TagKeys` condition keys only apply to the configuration API, not the Elasticsearch APIs.
## JSON Policy Element

<table>
<thead>
<tr>
<th>Resource</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon ES uses Resource elements in three basic ways:</td>
<td></td>
</tr>
<tr>
<td>• For actions that apply to Amazon ES itself, like es:ListDomainNames, or to allow full access, use the following syntax:</td>
<td></td>
</tr>
<tr>
<td>&quot;Resource&quot;: &quot;*&quot;</td>
<td></td>
</tr>
<tr>
<td>• For actions that involve a domain's configuration, like es:DescribeElasticsearchDomain, you can use the following syntax:</td>
<td></td>
</tr>
<tr>
<td>• For actions that apply to a domain's subresources, like es:ESHttpGet, you can use the following syntax:</td>
<td></td>
</tr>
</tbody>
</table>

You don't have to use a wildcard. Amazon ES lets you define a different access policy for each Elasticsearch index or API. For example, you might limit a user's permissions to the test-index index:


Instead of full access to test-index, you might prefer to limit the policy to just the search API:


You can even control access to individual documents:

"Resource": "arn:aws:es:region:aws-account-id:domain/domain-name/test-index/test-type/1"

Essentially, if Elasticsearch expresses the subresource as a URI, you can control access to it using an access policy. For even more control over which resources a user can access, see the section called “Fine-grained access control” (p. 90).

For details about which actions support resource-level permissions, see the Action element in this table.

---

## AWS-managed policies

Amazon ES has three AWS-managed, identity-based IAM policies. See the section called “Service-linked role for VPC access” (p. 28) for a summary of the service-linked role (AWSServiceRoleForAmazonElasticsearchService) that Amazon ES uses to place domains within VPCs.
### AWS-Managed Policy

<table>
<thead>
<tr>
<th>AWS-Managed Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AmazonESFullAccess</td>
<td>Provides full access to the Amazon ES configuration API and all HTTP methods for the Elasticsearch APIs. Fine-grained access control (p. 90) and resource-based policies (p. 77) can still restrict access.</td>
</tr>
<tr>
<td>AmazonESReadOnlyAccess</td>
<td>Provides read-only access to the Amazon ES configuration API (es:Describe*, es:List*, and es:Get*) and no access to the HTTP methods for the Elasticsearch APIs.</td>
</tr>
<tr>
<td>AmazonESCognitoAccess</td>
<td>Provides the minimum Amazon Cognito permissions necessary to enable the section called “Amazon Cognito authentication for Kibana” (p. 128).</td>
</tr>
</tbody>
</table>

### Advanced options and API considerations

Amazon ES has several advanced options, one of which has access control implications: `rest.action.multi.allow_explicit_index`. At its default setting of true, it allows users to bypass subresource permissions under certain circumstances.

For example, consider the following resource-based policy:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::123456789012:user/test-user"
                ]
            },
            "Action": [
                "es:ESHttp*"
            ],
            "Resource": [
                "arn:aws:es:us-west-1:987654321098:domain/test-domain/_bulk"
            ]
        },
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::123456789012:user/test-user"
                ]
            },
            "Action": [
                "es:ESHttpGet"
            ],
        }
    ]
}
```
This policy grants test-user full access to test-index and the Elasticsearch bulk API. It also allows GET requests to restricted-index.

The following indexing request, as you might expect, fails due to a permissions error:

```
PUT https://search-test-domain.us-west-1.es.amazonaws.com/restricted-index/movie/1
{
  "title": "Your Name",
  "director": "Makoto Shinkai",
  "year": "2016"
}
```

Unlike the index API, the bulk API lets you create, update, and delete many documents in a single call. You often specify these operations in the request body, however, rather than in the request URL. Because Amazon ES uses URLs to control access to domain subresources, test-user can, in fact, use the bulk API to make changes to restricted-index. Even though the user lacks POST permissions on the index, the following request succeeds:

```
POST https://search-test-domain.us-west-1.es.amazonaws.com/_bulk
{
  "index": { 
    "_index": "restricted-index",
    "_type": "movie",
    "_id": "1"
  }   
  "title": "Your Name",
  "director": "Makoto Shinkai",
  "year": "2016"
}
```

In this situation, the access policy fails to fulfill its intent. To prevent users from bypassing these kinds of restrictions, you can change rest.action.multi.allow_explicit_index to false. If this value is false, all calls to the bulk, mget, and msearch APIs that specify index names in the request body stop working. In other words, calls to _bulk no longer work, but calls to test-index/_bulk do. This second endpoint contains an index name, so you don't need to specify one in the request body.

Kibana (p. 216) relies heavily on mget and msearch, so it is unlikely to work properly after this change. For partial remediation, you can leave rest.action.multi.allow_explicit_index as true and deny certain users access to one or more of these APIs.

For information about changing this setting, see the section called "Advanced options" (p. 13).

Similarly, the following resource-based policy contains two subtle issues:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/test-user"
      },
      "Action": "es:ESHttp*",
    },
    {
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/test-user"
      },
      "Action": "es:ESHttp*",
    }
  ]
}
```

- Despite the explicit deny, test-user can still make calls such as GET https://search-test-domain.us-west-1.es.amazonaws.com/_all/_search and GET https://search-test-domain.us-west-1.es.amazonaws.com/restricted-index/_search.
domain.us-west-1.es.amazonaws.com/*//_search to access the documents in restricted-index.

- Because the Resource element references restricted-index/*, test-user doesn't have permissions to directly access the index's documents. The user does, however, have permissions to delete the entire index. To prevent access and deletion, the policy instead must specify restricted-index*.

Rather than mixing broad allows and focused denies, the safest approach is to follow the principle of least privilege and grant only the permissions that are required to perform a task. For more information about controlling access to individual indices or Elasticsearch operations, see the section called "Fine-grained access control" (p. 90).

Configuring access policies

- For instructions on creating or modifying resource- and IP-based policies in Amazon ES, see the section called “Configuring access policies” (p. 13).
- For instructions on creating or modifying identity-based policies in IAM, see Creating IAM Policies in the IAM User Guide.

Additional sample policies

Although this chapter includes many sample policies, AWS access control is a complex subject that is best understood through examples. For more, see Example Policies in the IAM User Guide.

Fine-grained access control in Amazon Elasticsearch Service

Fine-grained access control offers additional ways of controlling access to your data on Amazon Elasticsearch Service (Amazon ES). For example, depending on who makes the request, you might want a search to return results from only one index. You might want to hide certain fields in your documents or exclude certain documents altogether. Fine-grained access control offers the following benefits:

- Role-based access control
- Security at the index, document, and field level
- Kibana multi-tenancy
- HTTP basic authentication for Elasticsearch and Kibana

Topics

- The bigger picture: fine-grained access control and Amazon ES security (p. 91)
- Key concepts (p. 95)
- Enabling fine-grained access control (p. 95)
- Accessing Kibana as the master user (p. 95)
- Managing permissions (p. 96)
- Recommended configurations (p. 100)
- Tutorial: IAM master user and Amazon Cognito (p. 101)
- Tutorial: Internal user database and HTTP basic authentication (p. 103)
- Limitations (p. 105)
The bigger picture: fine-grained access control and Amazon ES security

Amazon Elasticsearch Service security has three main layers:

**Network**

The first security layer is the network, which determines whether requests reach an Amazon ES domain. If you choose **Public access** when you create a domain, requests from any internet-connected client can reach the domain endpoint. If you choose **VPC access**, clients must connect to the VPC (and the associated security groups must permit it) for a request to reach the endpoint. For more information, see the section called “VPC support” (p. 22).

**Domain access policy**

The second security layer is the domain access policy. After a request reaches a domain endpoint, the **resource-based access policy** (p. 77) allows or denies the request access to a given URI. The access policy accepts or rejects requests at the “edge” of the domain, before they reach Elasticsearch itself.

**Fine-grained access control**

The third and final security layer is fine-grained access control. After a resource-based access policy allows a request to reach a domain endpoint, fine-grained access control evaluates the user credentials and either authenticates the user or denies the request. If fine-grained access control authenticates the user, it fetches all roles mapped to that user and uses the complete set of permissions to determine how to handle the request.

**Note**

If a resource-based access policy contains IAM users or roles, clients must send signed requests using AWS Signature Version 4. As such, access policies can conflict with fine-grained access control, especially if you use the internal user database and HTTP basic authentication. You can't sign a request with a user name and password and IAM credentials. In general, if you enable fine-grained access control, we recommend using a domain access policy that doesn't require signed requests.

This first diagram illustrates a common configuration: a VPC access domain with fine-grained access control enabled, an IAM-based access policy, and an IAM master user.
This second diagram illustrates another common configuration: a public access domain with fine-grained access control enabled, an access policy that doesn't use IAM principals, and a master user in the internal user database.
Example

Consider a GET request to `movies/_search?q=thor`. Does the user have permissions to search the `movies` index? If so, does the user have permissions to see all documents within it? Should the response omit or anonymize any fields? For the master user, the response might look like this:

```json
{
    "hits": {
        "total": 7,
        "max_score": 8.772789,
        "hits": [
            {
                "_index": "movies",
                "_type": "_doc",
                "_id": "tt0800369",
                "_score": 8.772789,
                "_source": {
                    "directors": [
                        "Kenneth Branagh",
                        "Joss Whedon"
                    ],
                    "release_date": "2011-04-21T00:00:00Z",
                    "genres": [
                        "Action",
                        "Adventure"
                    ]
                }
            }
        ]
    }
}
```
"Fantasy",

"plot": "The powerful but arrogant god Thor is cast out of Asgard to live amongst humans in Midgard (Earth), where he soon becomes one of their finest defenders. ",
"title": "Thor",
"actors": [
  "Chris Hemsworth",
  "Anthony Hopkins",
  "Natalie Portman"
],
"year": 2011
}

The response has fewer hits and fewer fields for each hit. Also, the release_date field is anonymized. If a user with no permissions makes the same request, the cluster returns an error:

```
{
  "error": {
    "root_cause": [ {
      "type": "security_exception",
      "reason": "no permissions for [indices:data/read/search] and User [name=limited-user, roles=[], requestedTenant=null]"
    } ],
    "type": "security_exception",
    "reason": "no permissions for [indices:data/read/search] and User [name=limited-user, roles=[], requestedTenant=null]",
    "status": 403
  }
}
```

If a user provides invalid credentials, the cluster returns an Unauthorized exception.
Key concepts

Roles are the core way of using fine-grained access control. In this case, roles are distinct from IAM roles. Roles contain any combination of permissions: cluster-wide, index-specific, document level, and field level.

After configuring a role, you map it to one or more users. For example, you might map three roles to a single user: one role that provides access to Kibana, one that provides read-only access to index1, and one that provides write access to index2. Or you could include all of those permissions in a single role.

Users are people or applications that make requests to the Elasticsearch cluster. Users have credentials—either IAM access keys or a user name and password—that they specify when they make requests. With fine-grained access control on Amazon Elasticsearch Service, you choose one or the other for your master user when you configure your domain. The master user has full permissions to the cluster and manages roles and role mappings.

- If you choose IAM for your master user, all requests to the cluster must be signed using AWS Signature Version 4. For sample code, see the section called “Signing HTTP requests” (p. 143).

We recommend IAM if you want to use the same users on multiple clusters, if you want to use Amazon Cognito to access Kibana, or if you have Elasticsearch clients that support Signature Version 4 signing.

- If you choose the internal user database, you can use HTTP basic authentication (as well as IAM credentials) to make requests to the cluster. Most clients support basic authentication, including curl. The internal user database is stored in an Elasticsearch index, so you can't share it with other clusters.

We recommend the internal user database if you don't need to reuse users across multiple clusters, if you want to use HTTP basic authentication to access Kibana (rather than Amazon Cognito), or if you have clients that only support basic authentication. The internal user database is the simplest way to get started with Amazon ES.

Enabling fine-grained access control

Enable fine-grained access control using the console, AWS CLI, or configuration API. The console offers the simplest experience. For steps, see Creating and managing domains (p. 9). Here are the requirements for enabling fine-grained access control:

- Elasticsearch 6.7 or later
- Encryption of data at rest (p. 74) and node-to-node encryption (p. 76) enabled
- Require HTTPS for all traffic to the domain enabled

You can't enable fine-grained access control on existing domains, only new ones. After you enable fine-grained access control, you can't disable it.

Accessing Kibana as the master user

Fine-grained access control has a Kibana plugin that simplifies management tasks. You can use Kibana to manage users, roles, mappings, action groups, and tenants. The Kibana sign-in page and underlying authentication method differs, however, depending on how you manage users and configured your domain.

- If you want to use IAM for user management, use the section called “Amazon Cognito authentication for Kibana” (p. 128) to access Kibana. Otherwise, Kibana shows a nonfunctional sign-in page. See the section called “Limitations” (p. 105).
With Amazon Cognito authentication, one of the assumed roles from the identity pool must match the IAM role that you specified for the master user. For more information about this configuration, see the section called “(Optional) Configuring granular access“ (p. 135) and the section called “Tutorial: IAM master user and Amazon Cognito“ (p. 101).

- If you choose to use the internal user database, you can sign in to Kibana with your master user name and password. You must access Kibana over HTTPS. Amazon Cognito and SAML authentication for Kibana both replace this login screen.

For more information about this configuration, see the section called “Tutorial: Internal user database and HTTP basic authentication“ (p. 103).

- If you choose to use SAML authentication, you can sign in using credentials from an external identity provider. For more information, see the section called “SAML authentication for Kibana“ (p. 123).

**Managing permissions**

As noted in the section called “Key concepts“ (p. 95), you manage fine-grained access control permissions using roles, users, and mappings. This section describes how to create and apply those resources. We recommend that you sign in to Kibana as the master user (p. 95) to perform these operations.
Creating roles

You can create new roles for fine-grained access control using Kibana or the _opendistro/_security operation in the REST API. For more information, see the Open Distro for Elasticsearch documentation.

Fine-grained access control also includes a number of predefined roles. Clients such as Kibana and Logstash make a wide variety of requests to Elasticsearch, which can make it hard to manually create roles with the minimum set of permissions. For example, the *kibana_user* role includes the permissions that a user needs to work with index patterns, visualizations, dashboards, and tenants. We recommend mapping it (p. 98) to any user or backend role that accesses Kibana, along with additional roles that allow access to other indices.

Cluster-level security

Cluster-level permissions include the ability to make broad requests such as _mget, _msearch, and _bulk, monitor health, take snapshots, and more. Manage these permissions using the **Cluster Permissions** section when creating a role. For a list of cluster-level action groups, see the Open Distro for Elasticsearch documentation.

Index-level security

Index-level permissions include the ability to create new indices, search indices, read and write documents, delete documents, manage aliases, and more. Manage these permissions using the **Index Permissions** section when creating a role. For a list of index-level action groups, see the Open Distro for Elasticsearch documentation.

Document-level security

Document-level security lets you restrict which documents in an index a user can see. When creating a role, specify an index pattern and an Elasticsearch query. Any users that you map to that role can see only the documents that match the query. Document-level security affects the number of hits that you receive when you search (p. 93).

For more information, see the Open Distro for Elasticsearch documentation.

Field-level security

Field-level security lets you control which document fields a user can see. When creating a role, add a list of fields to either include or exclude. If you include fields, any users you map to that role can see only
those fields. If you exclude fields, they can see all fields except the excluded ones. Field-level security affects the number of fields included in hits when you search (p. 93).

For more information, see the Open Distro for Elasticsearch documentation.

Field masking

Field masking is an alternative to field-level security that lets you anonymize the data in a field rather than remove it altogether. When creating a role, add a list of fields to mask. Field masking affects whether you can see the contents of a field when you search (p. 93).

Tip

If you apply the standard masking to a field, Amazon ES uses a secure, random hash that can cause inaccurate aggregation results. To perform aggregations on masked fields, use pattern-based masking instead.

Creating users

If you enabled the internal user database, you can create users using Kibana or the _opendistro/_security operation in the REST API. For more information, see the Open Distro for Elasticsearch documentation.

If you chose IAM for your master user, ignore this portion of Kibana. Create IAM users and IAM roles instead. For more information, see the IAM User Guide.

Mapping roles to users

Role mapping is the most critical aspect of fine-grained access control. Fine-grained access control has some predefined roles to help you get started, but unless you map roles to users, every request to the cluster ends in a permissions error.

Backend roles, also called external identities, offer another way of mapping roles to users. Rather than mapping the same role to dozens of different users, you can map the role to a single backend role, and then make sure that all users have that backend role. Backend roles can be IAM roles or arbitrary strings.

- Specify users, IAM user ARNs, and Amazon Cognito user strings in the Users section. Cognito user strings take the form of Cognito/user-pool-id/username.
- Specify backend roles and IAM role ARNs in the External identities section.
Managing permissions

You can map roles to users using Kibana or the _opendistro/_security operation in the REST API. For more information, see the Open Distro for Elasticsearch documentation.

Creating action groups

Action groups are sets of permissions that you can reuse across different resources. You can create new action groups using Kibana or the _opendistro/_security operation in the REST API, although the default action groups suffice for most use cases. For more information about the default action groups, see the Open Distro for Elasticsearch documentation.

Kibana multi-tenancy

Tenants are spaces for saving index patterns, visualizations, dashboards, and other Kibana objects. Kibana multi-tenancy lets you safely share your work with other Kibana users (or keep it private). You can control which roles have access to a tenant and whether those roles have read or write access. To learn more, see the Open Distro for Elasticsearch documentation.

To view your current tenant or change tenants

1. Navigate to Kibana and sign in.
2. In the upper-right, choose your user icon.
3. Choose Switch tenants.
4. Verify your tenant before creating visualizations or dashboards. If you want to share your work with all other Kibana users, choose Global. To share your work with a subset of Kibana users, choose a different shared tenant. Otherwise, choose Private.
**Recommended configurations**

Due to how fine-grained access control interacts with other security features (p. 91), we recommend several fine-grained access control configurations that work well for most use cases.

<table>
<thead>
<tr>
<th>Description</th>
<th>Master User</th>
<th>Domain Access Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use IAM credentials for calls to the Elasticsearch APIs, and use SAML authentication (p. 123) to access Kibana. Manage fine-grained access control roles using Kibana or the REST API.</td>
<td>IAM user or role</td>
<td><code>{ &quot;Version&quot;: &quot;2012-10-17&quot;, &quot;Statement&quot;: [ { &quot;Effect&quot;: &quot;Allow&quot;, &quot;Principal&quot;: { &quot;AWS&quot;: &quot;*&quot; }, &quot;Action&quot;: &quot;es:ESHttp*&quot;, &quot;Resource&quot;: &quot;domain-arn/*&quot; } ] }</code></td>
</tr>
<tr>
<td>Use IAM credentials or basic authentication for calls to the Elasticsearch APIs. Manage fine-grained access control roles using Kibana or the REST API. This configuration offers a lot of flexibility, especially if you have Elasticsearch clients that only support basic authentication. If you have an existing identity provider, use SAML authentication (p. 123) to access Kibana. Otherwise, manage Kibana users in the internal user database.</td>
<td>User name and password</td>
<td><code>{ &quot;Version&quot;: &quot;2012-10-17&quot;, &quot;Statement&quot;: [ { &quot;Effect&quot;: &quot;Allow&quot;, &quot;Principal&quot;: { &quot;AWS&quot;: &quot;*&quot; }, &quot;Action&quot;: &quot;es:ESHttp*&quot;, &quot;Resource&quot;: &quot;domain-arn/*&quot; } ] }</code></td>
</tr>
<tr>
<td>Use IAM credentials for calls to the Elasticsearch APIs, and use Amazon Cognito to access Kibana. Manage fine-grained access control roles using Kibana or the REST API.</td>
<td>IAM user or role</td>
<td><code>{ &quot;Version&quot;: &quot;2012-10-17&quot;, &quot;Statement&quot;: [ { &quot;Effect&quot;: &quot;Allow&quot;, &quot;Principal&quot;: { &quot;AWS&quot;: &quot;*&quot; }, &quot;Action&quot;: &quot;es:ESHttp*&quot;, &quot;Resource&quot;: &quot;domain-arn/*&quot; } ] }</code></td>
</tr>
<tr>
<td>Use IAM credentials for calls to the Elasticsearch APIs.</td>
<td>IAM user or role</td>
<td><code>{ &quot;Version&quot;: &quot;2012-10-17&quot;, </code>}</td>
</tr>
</tbody>
</table>
APIs, and block most access to Kibana. Manage fine-grained access control roles using the REST API.

```
"Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:ESHttp*",
    },
    {
      "Effect": "Deny",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:ESHttp*",
    }
]
```

Tutorial: IAM master user and Amazon Cognito

This tutorial covers a popular use case: an IAM master user with Amazon Cognito authentication for Kibana. Although these steps use the Amazon Cognito user pool for authentication, this same basic process works for any Cognito authentication provider that lets you assign different IAM roles to different users.

**Note**

This tutorial assumes you have two existing IAM roles, one for the master user and one for more limited users. If you don’t have two roles, create them.

To get started with fine-grained access control

1. Create a domain (p. 9) with the following settings:

   - Elasticsearch 7.8
   - Public access
   - Fine-grained access control enabled with an IAM role as the master user (IAMMasterUserRole for the rest of this tutorial)
   - Amazon Cognito authentication for Kibana (p. 128) enabled
   - The following access policy:

     ```
     {
       "Version": "2012-10-17",
       "Statement": [
         {
           "Effect": "Allow",
           "Principal": {
             "AWS": "*"
           },
           "Action": "es:ESHttp*",
         }
       ]
     }
     ```
• HTTPS required for all traffic to the domain
• Node-to-node encryption
• Encryption of data at rest

2. Navigate to the IAM console, and then choose Roles.
3. Choose IAMMasterUserRole, and then choose the Trust relationships tab.
4. Choose Edit trust relationship, and ensure that the Amazon Cognito identity pool can assume the role. You should see the following statement:

```json
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "Federated": "cognito-identity.amazonaws.com"
    },
    "Action": "sts:AssumeRoleWithWebIdentity",
    "Condition": {
      "StringEquals": {
        "cognito-identity.amazonaws.com:aud": "identity-pool-id"
      },
      "ForAnyValue:StringLike": {
        "cognito-identity.amazonaws.com:amr": "authenticated"
      }
    }
  }]
}
```

5. Choose Update Trust Policy.
6. Add the same trust policy to a second IAM role (IAMLimitedUserRole for the rest of this tutorial).
7. Navigate to the Amazon Cognito console, and then choose Manage User Pools.
8. Choose your user pool, and then choose Users and groups.
9. Choose Create user, specify a user name of master-user and a password, and then choose Create user.
10. Create another user named limited-user.
11. Choose the Groups tab, and then choose Create group.
12. Name the group master-user-group, choose IAMMasterUserRole in the IAM role dropdown list, and then choose Create group.
13. Create another group named limited-user-group that uses IAMLimitedUserRole.
14. Choose master-user-group, choose Add users, and then add master-user.
15. Choose limited-user-group, choose Add users, and then add limited-user.
16. Choose App client settings and note the app client ID for your domain.
17. Choose Federated Identities, choose your identity pool, and then choose Edit identity pool.
18. Expand Authentication providers, find your user pool ID and the app client ID for your domain, and then change Use default role to Choose role from token.
19. For Role resolution, choose DENY. With this setting, users must be in a group to receive an IAM role after authenticating.
20. Choose Save Changes.
21. Navigate to Kibana.
22. Sign in with master-user.
23. Choose Try our sample data.
24. Add the sample flight data.
26. Name the role new-role.
27. For index permissions, specify kibana_sample_data_fli* for the index pattern.
28. For the action group, choose read.
29. For Document Level Security Query, specify the following query:

```json
{
  "match": {
    "FlightDelay": true
  }
}
```
30. For field-level security, choose Exclude fields and specify FlightNum.
31. For Anonymize fields, specify Dest.
32. Choose Create.
33. Choose Mapped users, Manage mapping. Then add the ARN for IAMLimitedUserRole as an external identity and choose Map.
34. Return to the list of roles and choose kibana_user. Choose Mapped users, Manage mapping. Then add the ARN for IAMLimitedUserRole as an external identity and choose Map.
35. In a new, private browser window, navigate to Kibana, sign in using limited-user, and then choose Explore on my own.
36. Choose Dev Tools, and then run the default search:

```json
GET _search
{
  "query": {
    "match_all": {}
  }
}
```

Note the permissions error. limited-user doesn’t have permissions to run cluster-wide searches.
37. Run another search:

```json
GET kibana_sample_data_flights/_search
{
  "query": {
    "match_all": {}
  }
}
```

Note that all matching documents have a FlightDelay field of true, an anonymized Dest field, and no FlightNum field.
38. In your original browser window, signed in as master-user, choose Dev Tools, and then perform the same searches. Note the difference in permissions, number of hits, matching documents, and included fields.

Tutorial: Internal user database and HTTP basic authentication

This tutorial covers another popular use case: a master user in the internal user database and HTTP basic authentication for Kibana.
To get started with fine-grained access control

1. Create a domain (p. 9) with the following settings:
   - Elasticsearch 7.9
   - Public access
   - Fine-grained access control with a master user in the internal user database (TheMasterUser for the rest of this tutorial)
   - Amazon Cognito authentication for Kibana disabled
   - The following access policy:

   ```json
   {   
     "Version": "2012-10-17",
     "Statement": [
       {   
         "Effect": "Allow",
         "Principal": {   
           "AWS": [   
             "*"
           ]
         },
         "Action": [   
           "es:ESHttp*"
         ],
       }
     ]
   }
   ```

   - HTTPS required for all traffic to the domain
   - Node-to-node encryption
   - Encryption of data at rest

2. Navigate to Kibana.
4. Choose Try our sample data.
5. Add the sample flight data.
7. Name the user new-user and specify a password. Then choose Create.
8. Choose Roles, Create role.
9. Name the role new-role.
10. For index permissions, specify kibana_sample_data_fli* for the index pattern.
11. For the action group, choose read.
12. For Document Level Security Query, specify the following query:

   ```json
   {
     "match": {
       "FlightDelay": true
     }
   }
   ```

13. For field-level security, choose Exclude fields and specify FlightNum.
14. For Anonymize fields, specify Dest.
15. Choose Create.
16. Choose Mapped users, Manage mapping. Then add new-user to Users and choose Map.
17. Return to the list of roles and choose kibana_user. Choose Mapped users, Manage mapping. Then add new-user to Users and choose Map.

18. In a new, private browser window, navigate to Kibana, sign in using new-user, and then choose Explore on my own.

19. Choose Dev Tools and run the default search:

```json
GET _search
{
  "query": {
    "match_all": {}
  }
}
```

Note the permissions error. new-user doesn't have permissions to run cluster-wide searches.

20. Run another search:

```json
GET kibana_sample_data_flights/_search
{
  "query": {
    "match_all": {}
  }
}
```

Note that all matching documents have a FlightDelay field of true, an anonymized Dest field, and no FlightNum field.

21. In your original browser window, signed in as TheMasterUser, choose Dev Tools and perform the same searches. Note the difference in permissions, number of hits, matching documents, and included fields.

**Limitations**

Fine-grained access control has several important limitations:

- The hosts aspect of role mappings, which maps roles to hostnames or IP addresses, doesn't work if the domain is within a VPC. You can still map roles to users and backend roles.

- Users in the internal user database can't change their own passwords. Master users (or users with equivalent permissions) must change their passwords for them.

- If you choose IAM for the master user and don't enable Amazon Cognito or SAML authentication, Kibana displays a nonfunctional sign-in page.

- If you choose IAM for the master user, you can still create users in the internal user database. Because HTTP basic authentication is not enabled under this configuration, however, any requests signed with those user credentials are rejected.

- If you use SQL (p. 183) to query an index that you don't have access to, you receive a "no permissions" error. If the index doesn't exist, you receive a "no such index" error. This difference in error messages means that you can confirm the existence of an index if you happen to guess its name.

To minimize the issue, don't include sensitive information in index names (p. 158). To deny all access to SQL, add the following element to your domain access policy:

```json
{
  "Effect": "Deny",
  "Principal": {
    "AWS": [ "*"
  ]
}
```
Modifying the master user

If you forget the details of the master user, you can reconfigure it using the console, AWS CLI, or configuration API.

To modify the master user (console)

1. Go to https://aws.amazon.com, and then choose Sign In to the Console.
2. Under Analytics, choose Elasticsearch Service.
3. Choose your domain.
4. Choose Actions, Modify authentication.
5. Choose either Set IAM role as master user or Create new master user.

   • If you previously used an IAM master user, fine-grained access control re-maps the all_access role to the new IAM ARN that you specify.
   • If you previously used the internal user database, fine-grained access control creates a new master user. You can use the new master user to delete the old one.
   • Switching from the internal user database to an IAM master user does not delete any users from the internal user database. Instead, it just disables HTTP basic authentication. Manually delete users from the internal user database, or keep them in case you ever need to re-enable HTTP basic authentication.

6. Choose Submit.

Additional master users

You designate a master user when you create a domain, but if you want, you can use this master user to create additional master users. You have two options: Kibana or the REST API.

• In Kibana, choose Security, Role Mappings, and then map the new master user to the all_access and security_manager roles.
To use the REST API, send the following requests:

```json
PUT `/security/api/rolesmapping/all_access`
{
  "backend_roles": [
    "arn:aws:iam::123456789012:role/fourth-master-user"
  ],
  "hosts": [],
  "users": [
    "master-user",
    "second-master-user",
    "arn:aws:iam::123456789012:user/third-master-user"
  ]
}
```

```json
PUT `/security/api/rolesmapping/security_manager`
{
  "backend_roles": [
    "arn:aws:iam::123456789012:role/fourth-master-user"
  ],
  "hosts": [],
  "users": [
    "master-user",
    "second-master-user",
    "arn:aws:iam::123456789012:user/third-master-user"
  ]
}
```

These requests replace the current role mappings, so perform GET requests first so that you can include all current roles in the PUT requests. The REST API is especially useful if you can't access Kibana and want to map an IAM role from Amazon Cognito to the all_access role.
Manual snapshots

Fine-grained access control introduces some additional complications with taking manual snapshots. To register a snapshot repository—even if you use HTTP basic authentication for all other purposes—you must map the manage_snapshots role to an IAM role that has `iam:PassRole` permissions to assume TheSnapshotRole, as defined in the section called “Prerequisites” (p. 52).

Then use that IAM role to send a signed request to the domain, as outlined in the section called "Registering a manual snapshot repository" (p. 55).

Integrations

If you use other AWS services (p. 160) with Amazon ES, you must provide the IAM roles for those services with appropriate permissions. For example, Kinesis Data Firehose delivery streams often use an IAM role called `firehose_delivery_role`. In Kibana, create a role for fine-grained access control (p. 97), and map the IAM role to it (p. 98). In this case, the new role needs the following permissions:

```json
{
    "cluster_permissions": [
        "cluster_composite_ops",
        "cluster_monitor"
    ],
    "index_permissions": [{
        "index_patterns": [
            "firehose-index*"
        ],
        "allowed_actions": [
            "create_index",
            "manage",
            "crud"
        ]
    }]
}
```

Permissions vary based on the actions each service performs. An AWS IoT rule or AWS Lambda function that indexes data likely needs similar permissions to Kinesis Data Firehose, while a Lambda function that only performs searches can use a more limited set.

REST API differences

The fine-grained access control REST API differs slightly depending on your Elasticsearch version. Prior to making a `PUT` request, make a `GET` request to verify the expected request body. For example, a `GET` request to `_opendistro/_security/api/user` returns all users, which you can then modify and use to make valid `PUT` requests.

On Elasticsearch 6.x, requests to create users look like this:

```bash
PUT _opendistro/_security/api/user/new-user
{
    "password": "some-password",
    "roles": ["new-backend-role"]
}
```

On Elasticsearch 7.x, requests look like this:

```bash
PUT _opendistro/_security/api/user/new-user
{
}
```
Further, tenants are properties of roles in Elasticsearch 6.x:

```json
GET _opendistro/_security/api/roles/all_access
{
  "all_access": {
    "cluster": ["UNLIMITED"],
    "tenants": {
      "admin_tenant": "RW"
    },
    "indices": {
      "*": {
        "*": ["UNLIMITED"]
      }
    },
    "readonly": "true"
  }
}
```

In Elasticsearch 7.x, they are objects with their own URI:

```json
GET _opendistro/_security/api/tenants
{
  "global_tenant": {
    "reserved": true,
    "hidden": false,
    "description": "Global tenant",
    "static": false
  }
}
```

For documentation on the 7.x REST API, see the [Open Distro for Elasticsearch documentation](https://opendistro.github.io/).  

**Tip**

If you use the internal user database, you can use curl to make requests and test your domain. Try the following sample commands:

```bash
curl -X GET -u 'master-user:master-user-password' 'domain-endpoint/_search'
curl -X GET -u 'master-user:master-user-password' 'domain-endpoint/_opendistro/_security/api/user'
```

## Managing audit logs in Amazon Elasticsearch Service

If your Amazon Elasticsearch Service (Amazon ES) domain uses fine-grained access control, you can enable audit logs for your data. Audit logs are highly customizable and let you track user activity on your Elasticsearch clusters, including authentication success and failures, requests to Elasticsearch, index changes, and incoming search queries. The default configuration tracks a popular set of user actions, but we recommend tailoring the settings to your exact needs.

Just like Elasticsearch application logs and slow logs (p. 47), Amazon ES publishes audit logs to CloudWatch Logs. If enabled, standard CloudWatch pricing applies.
Note
To enable audit logs, your user role must be mapped to the `security_manager` role, which gives you access to the `_opendistro/_security` REST API. To learn more, see the section called “Modifying the master user” (p. 106).

Limitations

Audit logs have the following limitations:

- Audit logs don't include cross-cluster search requests that were rejected by the destination's domain access policy.
- The maximum size of each audit log message is 10,000 characters. The audit log message is truncated if it exceeds this limit.

Enabling audit logs

Enabling audit logs is a two-step process. First, you must configure your domain to publish audit logs to CloudWatch Logs using the console, AWS CLI, or configuration API. Then you can tune audit log settings using Kibana or the fine-grained access control REST API.

Important
If you encounter an error while following these steps, see the section called “Can't enable audit logs” (p. 333) for troubleshooting information.

To enable audit logs for an Amazon ES domain (console)

1. Choose the domain and then the Logs tab.
2. Under Set up audit logs, choose Setup.
3. Create a CloudWatch log group, or choose an existing one.
4. Choose an access policy that contains the appropriate permissions, or create a policy using the JSON that the console provides:

   ```json
   {
   "Version": "2012-10-17",
   "Statement": [
   {
   "Effect": "Allow",
   "Principal": {
   "Service": "es.amazonaws.com"
   },
   "Action": [
   "logs:PutLogEvents",
   "logs:CreateLogStream"
   ],
   "Resource": "cw_log_group_arn"
   }
   ]
   }
   ```
5. Choose Enable.

Sample CLI command

The following AWS CLI command enables audit logs on an existing domain:
You can also enable audit logs when you create a domain. For detailed information, see the AWS CLI Command Reference.

**Sample configuration API request**

The following request to the configuration API enables audit logs on an existing domain:

```json
POST https://es.us-east-1.amazonaws.com/2015-01-01/es/domain/my-domain/config
{
    "LogPublishingOptions": {
        "AUDIT_LOGS": {
            "Enabled": true|false
        }
    }
}
```

For detailed information, see *Configuration API reference* (p. 339).

**Configuring audit logs in Kibana**

After you enable audit logs, configure them to match your needs.

1. Open Kibana, and choose **Security**.
2. Choose **Audit logs**.
3. Choose **Enable audit logging**.
Audit logging

### Storage location
Amazon Elasticsearch Service publishes audit logs to CloudWatch Logs, where you can monitor and search them. Set up the CloudWatch Logs log group in the Logs section of the Amazon Elasticsearch Service console for this domain. [Learn more](#)

### Enable audit logging
Enabled

---

## General settings

### Layer settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>REST layer</th>
<th>REST disabled categories</th>
<th>Transport layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>REST layer</td>
<td>Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>REST disabled categories</td>
<td>AUTHENTICATED, GRANTED_PRIVILEGES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transport layer</td>
<td></td>
<td></td>
<td>Disabled</td>
</tr>
<tr>
<td>Transport disabled categories</td>
<td>AUTHENTICATED, GRANTED_PRIVILEGES</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Attribute settings

#### Bulk requests
- Enabled

### Ignore settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Ignored users</th>
<th>Ignored requests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignored users</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Ignored requests</td>
<td>--</td>
<td>--</td>
</tr>
</tbody>
</table>

### Compliance settings

### Compliance logging
- Enabled

### Read

<table>
<thead>
<tr>
<th>Setting</th>
<th>Ignored users</th>
<th>Watched fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read metadata</td>
<td>--</td>
<td>{ &quot;<em>&quot; : [ &quot;</em>&quot; ] }</td>
</tr>
</tbody>
</table>

### Write

<table>
<thead>
<tr>
<th>Setting</th>
<th>Log diffs</th>
<th>Ignored users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Write metadata</td>
<td>Disabled</td>
<td>--</td>
</tr>
</tbody>
</table>

The Kibana UI offers full control of audit log settings under **General settings** and **Compliance settings**. For a description of all configuration options, see [Audit Log Settings](#) (p. 114).
Audit log layers and categories

Cluster communication occurs over two separate layers: the REST layer and the transport layer.

- The REST layer covers communication with HTTP clients such as curl, Logstash, Kibana, the Java high-level REST client (p. 143), the Python Requests library—all HTTP requests that arrive at the cluster.
- The transport layer covers communication between nodes. For example, after a search request arrives at the cluster (over the REST layer), the coordinating node serving the request sends the query to other nodes, receives their responses, gathers the necessary documents, and collates them into the final response. Operations such as shard allocation and rebalancing also occur over the transport layer.

You can enable or disable audit logs for entire layers, as well as individual audit categories for a layer. The following table contains a summary of audit categories and the layers for which they are available.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Available for REST</th>
<th>Available for Transport</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAILED_LOGIN</td>
<td>A request contained invalid credentials, and authentication failed.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MISSING_PRIVILEGES</td>
<td>A user did not have the privileges to make the request.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>GRANTED_PRIVILEGES</td>
<td>A user had the privileges to make the request.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>OPENDISTRO_SECURITY_INDEX_ATTEMPT</td>
<td>A request tried to modify the .opendistro_security index.</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>AUTHENTICATED</td>
<td>A request contained valid credentials, and authentication succeeded.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>INDEX_EVENT</td>
<td>A request performed an administrative operation on an index, such as creating one, setting an alias, or performing a force merge. The full list of indices:admin/actions that this category includes are available in the Open Distro for Elasticsearch documentation.</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

In addition to these standard categories, fine-grained access control offers several additional categories designed to meet data compliance requirements.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMPLIANCE_DOC_READ</td>
<td>A request performed a read event on a document in an index.</td>
</tr>
</tbody>
</table>
Audit log settings

Audit logs have numerous configuration options.

**General settings**

General settings let you enable or disable individual categories or entire layers. We highly recommend leaving GRANTED_PRIVILEGES and AUTHENTICATED as excluded categories. Otherwise, these categories are logged for every valid request to the cluster.

<table>
<thead>
<tr>
<th>Name</th>
<th>Backend Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>REST layer</td>
<td>enable_rest</td>
<td>Enable or disable events that occur on the REST layer.</td>
</tr>
<tr>
<td>REST disabled categories</td>
<td>disabled_rest_categories</td>
<td>Specify audit categories to ignore on the REST layer. Modifying these categories can dramatically increase the size of the audit logs.</td>
</tr>
<tr>
<td>Transport layer</td>
<td>enable_transport</td>
<td>Enable or disable events that happen on the transport layer.</td>
</tr>
<tr>
<td>Transport disabled categories</td>
<td>disabled_transport_categories</td>
<td>Specify audit categories which must be ignored on the transport layer. Modifying these categories can dramatically increase the size of the audit logs.</td>
</tr>
</tbody>
</table>

Attribute settings let you customize the amount of detail in each log line.

<table>
<thead>
<tr>
<th>Name</th>
<th>Backend Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bulk requests</td>
<td>resolve_bulk_requests</td>
<td>Enabling this setting generates a log for each document in a bulk request, which can dramatically increase the size of the audit logs.</td>
</tr>
<tr>
<td>Request body</td>
<td>log_request_body</td>
<td>Include the request body of the requests.</td>
</tr>
<tr>
<td>Resolve indices</td>
<td>resolve_indices</td>
<td>Resolve aliases to indices.</td>
</tr>
</tbody>
</table>

Use ignore settings to exclude a set of users or API paths:
Audit log settings

<table>
<thead>
<tr>
<th>Name</th>
<th>Backend Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignored users</td>
<td>ignore_users</td>
<td>Specify users that you want to exclude.</td>
</tr>
<tr>
<td>Ignored requests</td>
<td>ignore_requests</td>
<td>Specify request patterns that you want to exclude.</td>
</tr>
</tbody>
</table>

Compliance settings

Compliance settings let you tune for index, document, or field-level access.

<table>
<thead>
<tr>
<th>Name</th>
<th>Backend Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance logging</td>
<td>enable_compliance</td>
<td>Enable or disable compliance logging.</td>
</tr>
</tbody>
</table>

You can specify the following settings for read events.

<table>
<thead>
<tr>
<th>Name</th>
<th>Backend Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read metadata</td>
<td>read_metadata_only</td>
<td>Include only metadata for read events. Do not include any document fields.</td>
</tr>
<tr>
<td>Ignored users</td>
<td>read_ignore_users</td>
<td>Do not include certain users for read events.</td>
</tr>
<tr>
<td>Watched fields</td>
<td>read_watched_fields</td>
<td>Specify the indices and fields to watch for read events. Adding watched</td>
</tr>
<tr>
<td></td>
<td></td>
<td>fields generates one log per document access, which can dramatically</td>
</tr>
<tr>
<td></td>
<td></td>
<td>increase the size of the audit logs. Watched fields support index</td>
</tr>
<tr>
<td></td>
<td></td>
<td>patterns and field patterns:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;index-name-pattern&quot;: [</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;field-name-pattern&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>],</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;logs*&quot;: [</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;message&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>],</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;twitter&quot;: [</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;id&quot;,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;user*&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>]</td>
</tr>
</tbody>
</table>

You can specify the following settings for write events.

<table>
<thead>
<tr>
<th>Name</th>
<th>Backend Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Write metadata</td>
<td>write_metadata_only</td>
<td>Include only metadata for write events. Do not include any document fields.</td>
</tr>
<tr>
<td>Log diffs</td>
<td>write_log_diffs</td>
<td>If write_metadata_only is false, include only the differences between</td>
</tr>
<tr>
<td></td>
<td></td>
<td>write events.</td>
</tr>
<tr>
<td>Ignored users</td>
<td>write_ignore_users</td>
<td>Do not include certain users for write events.</td>
</tr>
</tbody>
</table>
Audit log example

This section includes an example configuration, search request, and the resulting audit log for all read and write events of an index.

**Step 1: Configure audit logs**

After you enable the publishing of audit logs to a CloudWatch Logs group, navigate to the Kibana audit logging page and choose **Enable audit logging**.

1. In **General Settings**, choose **Configure** and make sure that the **REST layer** is enabled.
2. In **Compliance Settings**, choose **Configure**.
3. Under **Write**, in **Watched Fields**, add accounts for all write events to this index.
4. Under **Read**, in **Watched Fields**, add ssn and id- fields of the accounts index:

   ```json
   { 
     "accounts-": [ 
       "ssn",
       "id-"
     ]
   }
   ```

**Step 2: Perform read and write events**

1. Navigate to Kibana, choose **Dev Tools** and index a sample document:

   ```javascript
   PUT accounts/_doc/0
   { 
     "ssn": "123",
     "id-": "456"
   }
   ```

2. To test a read event, send the following request:

   ```javascript
   GET accounts/_search
   { 
     "query": { 
       "match_all": {}
     }
   }
   ```

**Step 3: Observe the logs**

2. In the navigation pane, choose **Log groups**.
3. Choose the log group that you specified while enabling audit logs. Within the log group, Amazon ES creates a log stream for each node in your domain.

4. In Log streams, choose Search all.

5. For the read and write events, see the corresponding logs. You can expect a delay of 5 seconds before the log appears.

**Sample write audit log**

```json
{
  "audit_compliance_operation": "CREATE",
  "audit_cluster_name": "824471164578:audit-test",
  "audit_node_name": "be217225a0b77c2bd76147d3ed3ff83c",
  "audit_category": "COMPLIANCE_DOC_WRITE",
  "audit_request_origin": "REST",
  "audit_compliance_doc_version": 1,
  "audit_node_id": "3xNJhm4XS_yTzEgDwCGRjA",
  "@timestamp": "2020-08-23T05:28:02.285+00:00",
  "audit_format_version": 4,
  "audit_request_remote_address": "3.236.145.227",
  "audit_trace_doc_id": "lxnJGXQBqZSlDB91r_uZ",
  "audit_request_effective_user": "admin",
  "audit_trace_shard_id": 8,
  "audit_trace_indices": [
    "accounts"
  ],
  "audit_trace_resolved_indices": [
    "accounts"
  ]
}
```

**Sample read audit log**

```json
{
  "audit_cluster_name": "824471164578:audit-docs",
  "audit_node_name": "806f6050cb45437e2401b07534a1452f",
  "audit_category": "COMPLIANCE_DOC_READ",
  "audit_request_origin": "REST",
  "audit_node_id": "saSevm9ASte0-pjAtYi2UA",
  "@timestamp": "2020-08-31T17:57:05.015+00:00",
  "audit_format_version": 4,
  "audit_request_remote_address": "54.240.197.228",
  "audit_trace_doc_id": "config:7.7.0",
  "audit_request_effective_user": "admin",
  "audit_trace_shard_id": 0,
  "audit_trace_indices": [
    "accounts"
  ],
  "audit_trace_resolved_indices": [
    "accounts"
  ]
}
```

To include the request body, return to Compliance settings in Kibana and disable Write metadata. To exclude events by a specific user, add the user to Ignored Users.

For a description of each audit log field, see Audit log field reference. For information on searching and analyzing your audit log data, see Analyzing Log Data with CloudWatch Logs Insights in the Amazon CloudWatch Logs User Guide.
Configuring audit logs using the REST API

We recommend using Kibana to configure audit logs, but you can also use the fine-grained access control REST API. This section contains a sample request. Full documentation on the REST API is available in the Open Distro for Elasticsearch documentation.

```
PUT _opendistro/security/api/audit/config
{
  "enabled": true,
  "audit": {
    "enable_rest": true,
    "disabled_rest_categories": [
      "GRANTED_PRIVILEGES",
      "AUTHENTICATED"
    ],
    "enable_transport": true,
    "disabled_transport_categories": [
      "GRANTED_PRIVILEGES",
      "AUTHENTICATED"
    ],
    "resolve_bulk_requests": true,
    "log_request_body": true,
    "resolve_indices": true,
    "exclude_sensitive_headers": true,
    "ignore_users": ["kibanaserver"],
    "ignore_requests": ["SearchRequest", "indices:data/read/*", "/_cluster/health"
  ]
  },
  "compliance": {
    "enabled": true,
    "internal_config": true,
    "external_config": false,
    "read_metadata_only": true,
    "read_watched_fields": {
      "read-index-1": ["field-1", "field-2"],
      "read-index-2": ["field-3"
    ]
  },
  "readIgnoreUsers": ["read-ignore-1"],
  "writeMetadataOnly": true,
  "writeLogDiffs": false,
  "write_watched_indices": [
    "write-index-1",
    "write-index-2",
    "log-*",
    "*"
  ],
  "writeIgnoreUsers": ["write-ignore-1"
  ]
}
```
Monitoring Amazon Elasticsearch Service configuration API activity

Amazon Elasticsearch Service (Amazon ES) integrates with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Amazon ES. CloudTrail captures all configuration API calls for Amazon ES as events.

**Note**
CloudTrail only captures calls to the configuration API (p. 339), such as CreateElasticsearchDomain and GetUpgradeStatus. CloudTrail doesn't capture calls to the Elasticsearch APIs (p. 277), such as _search and _bulk. For these calls, see the section called “Audit logs” (p. 109).

The captured calls include calls from the Amazon ES console, AWS CLI, or an AWS SDK. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Amazon ES. If you don't configure a trail, you can still view the most recent events on the CloudTrail console in Event history. Using the information collected by CloudTrail, you can determine the request that was made to Amazon ES, the IP address from which the request was made, who made the request, when it was made, and additional details.

To learn more about CloudTrail, see the AWS CloudTrail User Guide.

**Amazon Elasticsearch Service information in CloudTrail**

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in Amazon ES, that activity is recorded in a CloudTrail event along with other AWS service events in Event history. You can view, search, and download recent events in your AWS account. For more information, see Viewing Events with CloudTrail Event History.

For an ongoing record of events in your AWS account, including events for Amazon ES, create a trail. A trail enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS Regions. The trail logs events from all Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following:

- Overview for Creating a Trail
- CloudTrail Supported Services and Integrations
- Configuring Amazon SNS Notifications for CloudTrail
- Receiving CloudTrail Log Files from Multiple Regions and Receiving CloudTrail Log Files from Multiple Accounts

All Amazon ES configuration API actions are logged by CloudTrail and are documented in the Configuration API reference (p. 339).

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or AWS Identity and Access Management (IAM) user credentials
- Whether the request was made with temporary security credentials for a role or federated user
Understanding Amazon Elasticsearch Service log file entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the CreateElasticsearchDomain operation:

```json
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/test-user",
        "accountId": "123456789012",
        "accessKeyId": "access-key",
        "userName": "test-user",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-08-21T21:59:11Z"
            }
        },
        "invokedBy": "signin.amazonaws.com"
    },
    "eventTime": "2018-08-21T22:00:05Z",
    "eventSource": "es.amazonaws.com",
    "eventName": "CreateElasticsearchDomain",
    "awsRegion": "us-west-1",
    "sourceIPAddress": "123.123.123.123",
    "userAgent": "signin.amazonaws.com",
    "requestParameters": {
        "elasticsearchVersion": "6.3",
        "elasticsearchClusterConfig": {
            "instanceType": "m4.large.elasticsearch",
            "instanceCount": 1
        },
        "snapshotOptions": {
            "automatedSnapshotStartHour": 0
        },
        "domainName": "test-domain",
        "encryptionAtRestOptions": {},
        "eBSOptions": {
            "eBSEnabled": true,
            "volumeSize": 10,
            "volumeType": "gp2"
        },
        "accessPolicies": {
            "Version": "2012-10-17",
            "Statement": [{
                "Effect": "Allow",
                "Principal": {
                    "AWS": ["123456789012"]
                },
                "Action": ["es:*"],
            ]
        },
        "advancedOptions": {
            "rest.action.multi.allow_explicit_index": "true"
        }
    }
}
```
Compliance validation for Amazon Elasticsearch Service

Third-party auditors assess the security and compliance of Amazon Elasticsearch Service (Amazon ES) as part of multiple AWS compliance programs. These programs include SOC, PCI, and HIPAA.

For a list of AWS services in scope of specific compliance programs, see AWS Services in Scope by Compliance Program. For general information, see AWS Compliance Programs.

You can download third-party audit reports using AWS Artifact. For more information, see Downloading Reports in AWS Artifact.

Your compliance responsibility when using Amazon ES is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

Compliance validation
• **Security and Compliance Quick Start Guides** – These deployment guides discuss architectural considerations and provide steps for deploying security- and compliance-focused baseline environments on AWS.

• **Architecting for HIPAA Security and Compliance Whitepaper** – This whitepaper describes how companies can use AWS to create HIPAA-compliant applications.

• **AWS Compliance Resources** – This collection of workbooks and guides might apply to your industry and location.

• **AWS Config** – This AWS service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.

• **AWS Security Hub** – This AWS service provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices.

### Resilience in Amazon Elasticsearch Service

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between Availability Zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see AWS Global Infrastructure.

In addition to the AWS global infrastructure, Amazon ES offers several features to help support your data resiliency and backup needs:

- Multi-AZ domains and replica shards (p. 19)
- Automated and manual snapshots (p. 51)

### Infrastructure security in Amazon Elasticsearch Service

As a managed service, Amazon Elasticsearch Service (Amazon ES) is protected by the AWS global network security procedures that are described in the Amazon Web Services: Overview of Security Processes whitepaper.

You use AWS published API calls to access the Amazon ES configuration API through the network. Clients must support Transport Layer Security (TLS) 1.0 or later. We recommend TLS 1.2 or later. To configure the minimum required TLS version to accept, specify the `TLSSecurityPolicy` value in the domain endpoint options. For details, see the AWS CLI Command Reference.

Clients must also support cipher suites with perfect forward secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Most modern systems such as Java 7 and later support these modes.

Additionally, requests to the configuration API must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the AWS Security Token Service (AWS STS) to generate temporary security credentials to sign requests.

Depending on your domain configuration, you might also need to sign requests to the Elasticsearch APIs. For more information, see the section called “Making and signing Amazon ES requests” (p. 82).

Amazon ES supports public access domains, which can receive requests from any internet-connected device, and VPC access domains (p. 22), which are isolated from the public internet.
SAML authentication for Kibana

SAML authentication for Kibana lets you use your existing identity provider to offer single sign-on (SSO) for Kibana on Amazon Elasticsearch Service (Amazon ES) domains running Elasticsearch 6.7 or later. To use SAML authentication, you must enable fine-grained access control (p. 90).

Rather than authenticating through Amazon Cognito (p. 128) or the internal user database (p. 95), SAML authentication for Kibana lets you use third-party identity providers to log in to Kibana, manage fine-grained access control, search your data, and build visualizations. Amazon ES supports providers that use the SAML 2.0 standard, such as Okta, Keycloak, Active Directory Federation Services (ADFS), and Auth0. Requests from Amazon ES to third-party providers aren't explicitly encrypted with a service provider certificate.

SAML authentication for Kibana is only for accessing Kibana through a web browser. Your SAML credentials do not let you make direct HTTP requests to the Elasticsearch or Kibana APIs.

SAML configuration overview

This page assumes you have an existing identity provider and some familiarity with it. We can't provide detailed configuration steps for your exact provider, only for your Amazon ES domain.

The Kibana login flow can take one of two forms:

- **Service provider (SP) initiated**: You navigate to Kibana (for example, https://my-domain.us-east-1.es.amazonaws.com/_plugin/kibana), which redirects you to the login screen. After you log in, the identity provider redirects you to Kibana.
- **Identity provider (IdP) initiated**: You navigate to your identity provider, log in, and choose Kibana from an application directory.

Amazon ES provides two single sign-on URLs, SP-initiated and IdP-initiated, but you only need the one that matches your desired Kibana login flow. If you want to configure both SP- and IdP-initiated authentication, you must do so through your identity provider. For example, in Okta you can enable Allow this app to request other SSO URLs and add one or more IdP-initiated SSO URLs.

Regardless of which authentication type you use, the goal is to log in through your identity provider and receive a SAML assertion that contains your username (required) and any backend roles (p. 95) (optional, but recommended). This information allows fine-grained access control (p. 90) to assign permissions to SAML users. In external identity providers, backend roles are typically called "roles" or "groups."

**Note**

You can't change the SSO URL, so SAML authentication for Kibana does not support proxy servers.

Enabling SAML authentication

You can only enable SAML authentication for Kibana on existing domains, not during the creation of new ones. Due to the size of the IdP metadata file, we highly recommend using the AWS console.

Domains only support one Kibana authentication method at a time. If you have Amazon Cognito authentication for Kibana (p. 128) enabled, you must disable it before you can enable SAML.

**To enable SAML authentication for Kibana (console)**

1. Choose the domain, Actions, and Modify authentication.
2. Check Enable SAML authentication.
3. Note the service provider entity ID and the two SSO URLs. You only need one of the SSO URLs. For guidance, see the section called “SAML configuration overview” (p. 123).

Tip
These URLs change if you later enable a custom endpoint (p. 66) for your domain. In that situation, you must update your IdP.

4. Use these values to configure your identity provider. This is the most complex part of the process, and unfortunately, terminology and steps vary wildly by provider. Consult your provider's documentation.

In Okta, for example, you create a "SAML 2.0 web application." For Single sign on URL, specify the SSO URL that you chose in step 3. For Audience URI (SP Entity ID), specify the SP entity ID.

Rather than users and backend roles, Okta has users and groups. For Group Attribute Statements, we recommend adding role to the Name field and the regular expression .+ to the Filter field. This statement tells the Okta identity provider to include all user groups under the role field of the SAML assertion after a user authenticates.

In Auth0, you create a "regular web application" and then enable the SAML 2.0 add-on. In Keycloak, you create a "client."

5. After you configure your identity provider, it generates an IdP metadata file. This XML file contains information on the provider, such as a TLS certificate, single sign-on endpoints, and the identity provider's entity ID.

Copy and paste the contents of the IdP metadata file into the Metadata from IdP field in the AWS console. Alternately, upload the metadata file using the Import from XML file button. The metadata file should look something like this:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="entity-id"
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
  </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

6. Copy and paste the contents of the entityID property from your metadata file into the IdP entity ID field in the AWS console. Many identity providers also display this value as part of a post-configuration summary. Some providers call it the "issuer."

7. Provide a SAML master username and/or a SAML master backend role. This username and/or backend role receives full permissions to the cluster, equivalent to a new master user (p. 106), but can only use those permissions within Kibana.

In Okta, for example, you might have a user jdoe who belongs to the group admins. If you add jdoe to the SAML master username field, only that user receives full permissions. If you add
admins to the **SAML master backend role** field, any user who belongs to the `admins` group receives full permissions.

The contents of the SAML assertion must exactly match the strings that you use for the SAML master username and/or SAML master role. Some identity providers add a prefix before their usernames, which can cause a hard-to-diagnose mismatch. In the identity provider user interface, you might see `jdoe`, but the SAML assertion might contain `auth0|jdoe`. Always use the string from the SAML assertion.

Many identity providers let you view a sample assertion during the configuration process, and tools like **SAML-tracer** can help you examine and troubleshoot the contents of real assertions. Assertions look something like this:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion ID="id6729229929925925351343340162" IssueInstant="2020-09-22T22:03:08.633Z" Version="2.0"
 xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml2:Subject>
    <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">username</saml2:NameID>
    <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      <saml2:SubjectConfirmationData NotOnOrAfter="2020-09-22T22:08:08.816Z" Recipient="domain-endpoint/_plugin/kibana/_opendistro/_security/saml/acs"/>
    </saml2:SubjectConfirmation>
  </saml2:Subject>
  <saml2:Conditions NotBefore="2020-09-22T21:58:08.816Z" NotOnOrAfter="2020-09-22T22:08:08.816Z">
    <saml2:AudienceRestriction>
      <saml2:Audience>domain-endpoint</saml2:Audience>
    </saml2:AudienceRestriction>
  </saml2:Conditions>
  </saml2:AuthnStatement>
  <saml2:AttributeStatement>
    <saml2:Attribute Name="role" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
    </saml2:Attribute>
  </saml2:AttributeStatement>
</saml2:Assertion>
```

8. **Expand the Optional SAML settings** section.

9. Leave the **Subject key** field empty to use the **NameID** element of the SAML assertion for the username. If your assertion doesn't use this standard element and instead includes the username as a custom attribute, specify that attribute here.

   If you want to use backend roles (recommended), specify an attribute from the assertion in the **Role key** field, such as role or group. This is another situation in which tools like **SAML-tracer** can help.

10. By default, Kibana logs users out after 60 minutes. You can increase this value up to 1,440 (24 hours) using the **Session time to live** field.
11. Choose **Submit**. The domain enters a processing state for approximately one minute, during which time Kibana is unavailable.

12. After the domain finishes processing, open Kibana.
   - If you chose the SP-initiated URL, navigate to `domain-endpoint/_plugin/kibana/`.
   - If you chose the IdP-initiated URL, navigate to your identity provider's application directory.

In both cases, log in as either the SAML master user or a user who belongs to the SAML master backend role. To continue the example from step 7, log in as either `jdoe` or a member of the `admins` group.

13. After Kibana loads, choose **Security** and **Roles**.

14. **Map roles (p. 98)** to allow other users to access Kibana.
   
   For example, you might map your trusted colleague `jroe` to the `all_access` and `security_manager` roles. You might also map the backend role `analysts` to the `readall` and `kibana_user` roles.

   If you prefer to use the API rather than Kibana, see the following sample request:

   ```json
   PATCH _opendistro/_security/api/rolesmapping
   [   {   "op": "add", "path": "/security_manager", "value": { "users": ["master-user", "jdoe", "jroe"], "backend_roles": ["admins"] }   },
   {   "op": "add", "path": "/all_access", "value": { "users": ["master-user", "jdoe", "jroe"], "backend_roles": ["admins"] }   },
   {   "op": "add", "path": "/readall", "value": { "backend_roles": ["analysts"] }   },
   {   "op": "add", "path": "/kibanauser", "value": { "backend_roles": ["analysts"] }   }   ]
   ```

### Sample CLI command

The following AWS CLI command enables SAML authentication for Kibana on an existing domain:

```bash
aws es update-elasticsearch-domain-config --domain-name my-domain --advanced-security-options '{"SAMLOptions":{"Enabled":true,"MasterUserName":"my-idp-user","MasterBackendRole":"my-idp-group-or-role","Idp":{"EntityId":"entity-id","MetadataContent":"metadata-content-with-quotes-escaped"},"RolesKey":"optional-roles-key","SessionTimeoutMinutes":180,"SubjectKey":"optional-subject-key"}}'
```

You must escape all quotes and newline characters in the metadata XML. For example, use `<KeyDescriptor use="signing"/>
` instead of `<KeyDescriptor use="signing">` and a line break. For detailed information about using the AWS CLI, see the [AWS CLI Command Reference](https://docs.aws.amazon.com/cli/latest/reference/es/update-elasticsearch-domain-config.html).

### Sample configuration API request

The following request to the configuration API enables SAML authentication for Kibana on an existing domain:
POST https://es.us-east-1.amazonaws.com/2015-01-01/es/domain/my-domain/config
{
  "AdvancedSecurityOptions": {
    "SAMLOptions": {
      "Enabled": true,
      "MasterUserName": "my-idp-user",
      "MasterBackendRole": "my-idp-group-or-role",
      "Idp": {
        "EntityId": "entity-id",
        "MetadataContent": "metadata-content-with-quotes-escaped"
      },
      "RolesKey": "optional-roles-key",
      "SessionTimeoutMinutes": 180,
      "SubjectKey": "optional-subject-key"
    }
  }
}

You must escape all quotes and newline characters in the metadata XML. For example, use
<KeyDescriptor use="signing">
\n instead of <KeyDescriptor use="signing">
 and a line break. For detailed information about using the configuration API, see Configuration API reference (p. 339).

SAML troubleshooting

<table>
<thead>
<tr>
<th>Error</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your request: '/some/path' is not allowed.</td>
<td>Verify that you provided the correct SSO URL (p. 123) (step 3) to your identity provider.</td>
</tr>
<tr>
<td>Please provide valid identity provider metadata document to enable SAML.</td>
<td>Your IdP metadata file does not conform to the SAML 2.0 standard. Check for errors using a validation tool.</td>
</tr>
<tr>
<td>SAML configuration options aren't visible in the console.</td>
<td>Update to the latest service software (p. 16).</td>
</tr>
</tbody>
</table>
| SAML configuration error: Something went wrong while retrieving the SAML configuration, please check your settings. | This generic error can occur for many reasons. 
- Check that you provided your identity provider with the correct SP entity ID and SSO URL. 
- Regenerate the IdP metadata file, and verify the IdP entity ID. Add any updated metadata in the AWS console. 
- Verify that your domain access policy allows access to Kibana and _opendistro/_security/*. In general, we recommend an open access policy for domains that use fine-grained access control. 
- Consult your identity provider’s documentation for steps on configuring SAML. |
| Missing role: No roles available for this user, please contact your system administrator. | You successfully authenticated, but the username and any backend roles from the SAML assertion are not mapped to any roles and thus have no permissions. These mappings are case-sensitive. 
Verify the contents of your SAML assertion using a tool like SAML-tracer and your role mapping using the following call: |
Disabling SAML authentication

To disable SAML authentication for Kibana (console)

1. Choose the domain, Actions, and Modify authentication.
2. Uncheck Enable SAML authentication.
3. Choose Submit.
4. After the domain finishes processing, verify the fine-grained access control role mapping using the following call:

   ```
   GET _opendistro/_security/api/rolesmapping
   ```

Disabling SAML authentication for Kibana does not remove the mappings for the SAML master username and/or the SAML master backend role. If you want to remove these mappings, log in to Kibana using the internal user database (if enabled), or use the API to remove them:

```
PUT _opendistro/_security/api/rolesmapping/all_access
{
   "users": [
      "master-user"
   ]
}
```

Configuring Amazon Cognito authentication for Kibana

You can authenticate and protect your Amazon Elasticsearch Service (Amazon ES) default installation of Kibana using Amazon Cognito. Amazon Cognito authentication 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 (p. 80) and a proxy server (p. 216), HTTP basic authentication, or SAML (p. 123).

Much of the authentication process occurs in Amazon Cognito, but this section offers guidelines and requirements for configuring Amazon Cognito resources to work with Amazon ES domains. Standard pricing applies to all Amazon Cognito resources.
Tip
The first time that you configure a domain to use Amazon Cognito authentication for Kibana, we recommend using the console. Amazon Cognito resources are extremely customizable, and the console can help you identify and understand the features that matter to you.

Prerequisites
Before you can configure Amazon Cognito authentication for Kibana, you must fulfill several prerequisites. The Amazon ES console helps streamline the creation of these resources, but understanding the purpose of each resource helps with configuration and troubleshooting. Amazon Cognito authentication for Kibana requires the following resources:

- Amazon Cognito user pool
- Amazon Cognito identity pool
- IAM role that has the AmazonESCognitoAccess policy attached (CognitoAccessForAmazonES)

Note
The user pool and identity pool must be in the same AWS Region. You can use the same user pool, identity pool, and IAM role to add Amazon Cognito authentication for Kibana to multiple Amazon ES domains. To learn more, see the section called “Limits” (p. 137).

About the user pool
User pools have two main features: create and manage a directory of users, and let users sign up and log in. For instructions about creating a user pool, see Create a User Pool in the Amazon Cognito Developer Guide.

When you create a user pool to use with Amazon ES, consider the following:

- Your Amazon Cognito user pool must have a domain name. Amazon ES uses this domain name to redirect users to a login page for accessing Kibana. Other than a domain name, the user pool doesn't require any non-default configuration.
- You must specify the pool's required standard attributes—attributes like name, birth date, email address, and phone number. You can't change these attributes after you create the user pool, so choose the ones that matter to you at this time.
• While creating your user pool, choose whether users can create their own accounts, the minimum password strength for accounts, and whether to enable multi-factor authentication. If you plan to use an external identity provider, these settings are inconsequential. Technically, you can enable the user pool as an identity provider and enable an external identity provider, but most people prefer one or the other.

User pool IDs take the form of \textit{region\_ID}. If you plan to use the AWS CLI or an AWS SDK to configure Amazon ES, make note of the ID.

**About the identity pool**

Identity pools let you assign temporary, limited-privilege roles to users after they log in. For instructions about creating an identity pool, see Identity Pools in the Amazon Cognito Developer Guide. When you create an identity pool to use with Amazon ES, consider the following:

• If you use the Amazon Cognito console, you must select the **Enable access to unauthenticated identities** check box to create the identity pool. After you create the identity pool and configure the Amazon ES domain (p. 131), Amazon Cognito disables this setting.

• You don't need to add external identity providers to the identity pool. When you configure Amazon ES to use Amazon Cognito authentication, it configures the identity pool to use the user pool that you just created.

• After you create the identity pool, you must choose unauthenticated and authenticated IAM roles. These roles specify the access policies that users have before and after they log in. If you use the Amazon Cognito console, it can create these roles for you. After you create the authenticated role, make note of the ARN, which takes the form of \texttt{arn:aws:iam::123456789012:role/Cognito\_IdentityPoolAuth\_Role}.

Identity pool IDs take the form of \textit{region:ID-ID-ID-ID-ID}. If you plan to use the AWS CLI or an AWS SDK to configure Amazon ES, make note of the ID.

**About the CognitoAccessForAmazonES role**

Amazon ES needs permissions to configure the Amazon Cognito user and identity pools and use them for authentication. You can use \texttt{AmazonESCognitoAccess}, which is an AWS managed policy, for this purpose. If you use the console to create or configure your Amazon ES domain, it creates an IAM role for you and attaches this policy to the role. The default name for this role is \texttt{CognitoAccessForAmazonES}.

If you use the AWS CLI or one of the AWS SDKs, you must create your own role, attach the policy, and specify the ARN for this role when you configure your Amazon ES domain. The role must have the following trust relationship:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "es.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

For instructions, see Creating a Role to Delegate Permissions to an AWS Service and Attaching and Detaching IAM Policies in the IAM User Guide.
Configuring an Amazon ES domain

After you complete the prerequisites, you can configure an Amazon ES domain to use Amazon Cognito for Kibana.

**Note**
Amazon Cognito is not available in all AWS Regions. For a list of supported regions, see [AWS Regions and Endpoints](#). You don't need to use the same Region for Amazon Cognito that you use for Amazon ES.

Configuring Amazon Cognito authentication (console)

Because it creates the [CognitoAccessForAmazonES (p. 130)](#) role for you, the console offers the simplest configuration experience. In addition to the standard Amazon ES permissions, you need the following set of permissions to use the console to create a domain that uses Amazon Cognito authentication for Kibana:

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "iam:GetRole",
            "iam:PassRole",
            "iam:CreateRole",
            "iam:AttachRolePolicy",
            "ec2:DescribeVpcs",
            "cognito-identity:ListIdentityPools",
            "cognito-idp:ListUserPools"
         ],
         "Resource": "*"
      }
   ]
}
```

If [CognitoAccessForAmazonES (p. 130)](#) already exists, you need fewer permissions:

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "ec2:DescribeVpcs",
            "cognito-identity:ListIdentityPools",
            "cognito-idp:ListUserPools"
         ],
         "Resource": "*"
      },
      {
         "Effect": "Allow",
         "Action": [
            "iam:GetRole",
            "iam:PassRole"
         ],
         "Resource": "arn:aws:iam::123456789012:role/CognitoAccessForAmazonES"
      }
   ]
}
```
To configure Amazon Cognito authentication for Kibana (console)

1. Go to https://aws.amazon.com, and then choose Sign In to the Console.
2. Under Analytics, choose Elasticsearch Service.
3. In the navigation pane, under My domains, choose the domain that you want to configure.
4. Choose Actions, Modify authentication.
5. For Amazon Cognito authentication, choose Enable Amazon Cognito authentication.
6. For Region, select the Region that contains your Amazon Cognito user pool and identity pool.
7. For Cognito User Pool, select a user pool or create one. For guidance, see the section called “About the user pool” (p. 129).
8. For Cognito Identity Pool, select an identity pool or create one. For guidance, see the section called “About the identity pool” (p. 130).

   Note
   The Create new user pool and Create new identity pool links direct you to the Amazon Cognito console and require you to create these resources manually. The process is not automatic. To learn more, see the section called “Prerequisites” (p. 129).

9. For IAM Role, use the default value of CognitoAccessForAmazonES (recommended) or enter a new name. To learn more about the purpose of this role, see the section called “About the CognitoAccessForAmazonES role” (p. 130).
10. Choose Submit.

After your domain finishes processing, see the section called “Allowing the authenticated role” (p. 133) and the section called “Configuring identity providers” (p. 133) for additional configuration steps.

Configuring Amazon Cognito authentication (AWS CLI)

Use the --cognito-options parameter to configure your Amazon ES domain. The following syntax is used by both the create-elasticsearch-domain and update-elasticsearch-domain-config commands:

```bash
--cognito-options Enabled=true,UserPoolId="user-pool-id",IdentityPoolId="identity-pool-id",RoleArn="arn:aws:iam::123456789012:role/CognitoAccessForAmazonES"
```

Example

The following example creates a domain in the us-east-1 Region that enables Amazon Cognito authentication for Kibana using the CognitoAccessForAmazonES role and provides domain access to Cognito_Auth_Role:

```bash
```

After your domain finishes processing, see the section called “Allowing the authenticated role” (p. 133) and the section called “Configuring identity providers” (p. 133) for additional configuration steps.
Configuring Amazon Cognito Authentication (AWS SDKs)

The AWS SDKs (except the Android and iOS SDKs) support all the operations that are defined in the Configuration API reference (p. 339), including the CognitoOptions parameter for the CreateElasticsearchDomain and UpdateElasticsearchDomainConfig operations. For more information about installing and using the AWS SDKs, see AWS Software Development Kits.

After your domain finishes processing, see the section called “Allowing the authenticated role” (p. 133) and the section called “Configuring identity providers” (p. 133) for additional configuration steps.

Allowing the authenticated role

By default, the authenticated IAM role that you configured by following the guidelines in the section called “About the identity pool” (p. 130) does not have the necessary privileges to access Kibana. You must provide the role with additional permissions.

**Important**

If you configured fine-grained access control (p. 90) and use an "open" or IP-based access policy, you can skip this step.

You can include these permissions in an identity-based (p. 79) policy, but unless you want authenticated users to have access to all Amazon ES domains, a resource-based (p. 77) policy attached to a single domain is the better approach:

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "AWS": [
              "arn:aws:iam::123456789012:role/Cognito_identitypoolAuth_Role"
            ],
            "Action": [
              "es:ESHttp*"
            ],
          }
      }
   ]
}
```

For instructions about adding a resource-based policy to an Amazon ES domain, see the section called “Configuring access policies” (p. 13).

Configuring identity providers

When you configure a domain to use Amazon Cognito authentication for Kibana, Amazon ES adds an app client to the user pool and adds the user pool to the identity pool as an authentication provider. The following screenshot shows the App client settings page in the Amazon Cognito console.
Warning
Don’t rename or delete the app client.

Depending on how you configured your user pool, you might need to create user accounts manually, or users might be able to create their own. If these settings are acceptable, you don’t need to take further action. Many people, however, prefer to use external identity providers.

To enable a SAML 2.0 identity provider, you must provide a SAML metadata document. To enable social identity providers like Login with Amazon, Facebook, and Google, you must have an app ID and app secret from those providers. You can enable any combination of identity providers. The sign-in page adds options as you add providers, as shown in the following screenshot.

The easiest way to configure your user pool is to use the Amazon Cognito console. Use the Identity Providers page to add external identity providers and the App client settings page to enable and disable identity providers for the Amazon ES domain’s app client. For example, you might want to enable your own SAML identity provider and disable Cognito User Pool as an identity provider.
(Optional) Configuring granular access

You might have noticed that the default identity pool settings assign every user who logs in the same IAM role (Cognito_identitypoolAuth_Role), which means that every user can access the same AWS resources. If you want to use fine-grained access control (p. 90) with Amazon Cognito—for example, if you want your organization's analysts to have read-only access to several indices, but developers to have write access to all indices—you have two options:

- Create user groups and configure your identity provider to choose the IAM role based on the user's authentication token (recommended).
- Configure your identity provider to choose the IAM role based on one or more rules.

You configure these options using the Edit identity pool page of the Amazon Cognito console, as shown in the following screenshot. For a walkthrough that includes fine-grained access control, see the section called "Tutorial: IAM master user and Amazon Cognito" (p. 101).
(Optional) Configuring granular access

Authentication providers

Amazon Cognito supports the following authentication methods with Amazon Cognito Sign-In or any public provider. If you allow your users to authenticate using any of these public providers, you can specify your application identifiers here. Warning: Changing the application ID that your identity pool is linked to will prevent existing users from authenticating using Amazon Cognito. Learn more about public identity providers.

Important
Just like the default role, Amazon Cognito must be part of each additional role's trust relationship. For details, see Creating Roles for Role Mapping in the Amazon Cognito Developer Guide.
User groups and tokens

When you create a user group, you choose an IAM role for members of the group. For information about creating groups, see User Groups in the Amazon Cognito Developer Guide.

After you create one or more user groups, you can configure your authentication provider to assign users their groups’ roles rather than the identity pool’s default role. Choose the Choose role from token option. Then choose either Use default Authenticated role or DENY to specify how the identity pool should handle users who are not part of a group.

Rules

Rules are essentially a series of if statements that Amazon Cognito evaluates sequentially. For example, if a user’s email address contains @corporate, Amazon Cognito assigns that user Role_A. If a user’s email address contains @subsidiary, it assigns that user Role_B. Otherwise, it assigns the user the default authenticated role.

To learn more, see Using Rule-Based Mapping to Assign Roles to Users in the Amazon Cognito Developer Guide.

(Optional) Customizing the sign-in page

The UI customization page of the Amazon Cognito console lets you upload a custom logo and make CSS changes to the sign-in page. For instructions and a full list of CSS properties, see Specifying App UI Customization Settings for Your User Pool in the Amazon Cognito Developer Guide.

(Optional) Configuring advanced security

Amazon Cognito user pools support advanced security features like multi-factor authentication, compromised credential checking, and adaptive authentication. To learn more, see Managing Security in the Amazon Cognito Developer Guide.

Testing

After you are satisfied with your configuration, verify that the user experience meets your expectations.

To access Kibana

2. Sign in using your preferred credentials.
3. After Kibana loads, configure at least one index pattern. Kibana uses these patterns to identity which indices that you want to analyze. Enter *, choose Next step, and then choose Create index pattern.
4. To search or explore your data, choose Discover.

If any step of this process fails, see the section called “Common configuration issues” (p. 138) for troubleshooting information.

Limits

Amazon Cognito has soft limits on many of its resources. If you want to enable Kibana authentication for a large number of Amazon ES domains, review Limits in Amazon Cognito and request limit increases as necessary.
Each Amazon ES domain adds an app client to the user pool, which adds an authentication provider to the identity pool. If you enable Kibana authentication for more than 10 domains, you might encounter the "maximum Amazon Cognito user pool providers per identity pool" limit. If you exceed a limit, any Amazon ES domains that you try to configure to use Amazon Cognito authentication for Kibana can get stuck in a configuration state of Processing.

Common configuration issues

The following tables list common configuration issues and solutions.

### Configuring Amazon ES

<table>
<thead>
<tr>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon ES can't create the role (console)</td>
<td>You don't have the correct IAM permissions. Add the permissions specified in the section called “Configuring Amazon Cognito authentication (console)” (p. 131).</td>
</tr>
<tr>
<td>User is not authorized to perform: iam:PassRole on resource</td>
<td>You don't have iam:PassRole permissions for the CognitoAccessForAmazonES (p. 130) role. Attach the following policy to your account:</td>
</tr>
<tr>
<td>CognitoAccessForAmazonES (console)</td>
<td><img src="https://example.com/policy_code" alt="Policy Code" /></td>
</tr>
<tr>
<td></td>
<td>Alternately, you can attach the IAMFullAccess policy.</td>
</tr>
<tr>
<td>User is not authorized to perform: cognito-identity:ListIdentityPools</td>
<td>You don't have read permissions for Amazon Cognito. Attach the AmazonCognitoReadOnly policy to your account.</td>
</tr>
<tr>
<td>on resource</td>
<td></td>
</tr>
<tr>
<td>An error occurred (ValidationException) when calling the</td>
<td>Amazon ES isn't specified in the trust relationship of the CognitoAccessForAmazonES role. Check that your role uses the trust relationship that is specified in the section called &quot;About the CognitoAccessForAmazonES role&quot; (p. 130). Alternately, use the console to configure Amazon Cognito authentication. The console creates a role for you.</td>
</tr>
<tr>
<td>CreateElasticsearchDomain operation: Amazon Elasticsearch must be</td>
<td></td>
</tr>
<tr>
<td>allowed to use the passed role</td>
<td></td>
</tr>
<tr>
<td>An error occurred (ValidationException) when calling the</td>
<td>The role specified in --cognito-options does not have permissions to access Amazon Cognito. Check that the role has the AWS managed AmazonESCognitoAccess policy attached. Alternately, use the console to configure Amazon Cognito authentication. The console creates a role for you.</td>
</tr>
<tr>
<td>CreateElasticsearchDomain operation: User is not authorized to</td>
<td></td>
</tr>
<tr>
<td>perform: cognito-idp:action on resource: user pool</td>
<td></td>
</tr>
</tbody>
</table>
### Issue | Solution
--- | ---
An error occurred (ValidationException) when calling the CreateElasticsearchDomain operation: User pool does not exist | Amazon ES can’t find the user pool. Confirm that you created one and have the correct ID. To find the ID, you can use the Amazon Cognito console or the following AWS CLI command:
```
aws cognito-idp list-user-pools --max-results 60 --region region
```

An error occurred (ValidationException) when calling the CreateElasticsearchDomain operation: IdentityPool not found | Amazon ES can’t find the identity pool. Confirm that you created one and have the correct ID. To find the ID, you can use the Amazon Cognito console or the following AWS CLI command:
```
aws cognito-identity list-identity-pools --max-results 60 --region region
```

An error occurred (ValidationException) when calling the CreateElasticsearchDomain operation: Domain needs to be specified for user pool | The user pool does not have a domain name. You can configure one using the Amazon Cognito console or the following AWS CLI command:
```
aws cognito-idp create-user-pool-domain --domain name --user-pool-id id
```

### Accessing Kibana

| Issue | Solution |
--- | --- |
The login page doesn’t show my preferred identity providers. | Check that you enabled the identity provider for the Amazon ES app client as specified in the section called “Configuring identity providers” (p. 133). |

The login page doesn’t look as if it’s associated with my organization. | See the section called “(Optional) Customizing the sign-in page” (p. 137). |

My login credentials don’t work. | Check that you have configured the identity provider as specified in the section called “Configuring identity providers” (p. 133). |

If you use the user pool as your identity provider, check that the account exists and is confirmed on the User and groups page of the Amazon Cognito console. |

Kibana either doesn’t load at all or doesn’t work properly. | The Amazon Cognito authenticated role needs **es:ESHttp* permissions for the domain / to access and use Kibana. Check that you added an access policy as specified in the section called “Allowing the authenticated role” (p. 133). |

Invalid identity pool configuration. Check assigned IAM roles for this pool. | Amazon Cognito doesn’t have permissions to assume the IAM role on behalf of the authenticated user. Modify the trust relationship for the role to include: |

```json
{
  "Version": "2012-10-17",
  "Statement": [
```
Disabling Amazon Cognito authentication for Kibana

Use the following procedure to disable Amazon Cognito authentication for Kibana.

**To disable Amazon Cognito authentication for Kibana (console)**

1. Go to [https://aws.amazon.com](https://aws.amazon.com), and then choose **Sign In to the Console**.
2. Under **Analytics**, choose **Elasticsearch Service**.
3. In the navigation pane, under **My domains**, choose the domain that you want to configure.
4. Choose **Actions, Modify authentication**.
5. For **Amazon Cognito authentication**, clear the **Enable Amazon Cognito authentication** check box.
6. Choose **Submit**.

**Important**

If you no longer need the Amazon Cognito user pool and identity pool, delete them. Otherwise, you can continue to incur charges.

Deleting domains that use Amazon Cognito authentication for Kibana

To prevent domains that use Amazon Cognito authentication for Kibana from becoming stuck in a configuration state of **Processing**, delete Amazon ES domains before deleting their associated Amazon Cognito user pools and identity pools.
Using service-linked roles to provide Amazon Elasticsearch Service access to resources

Provide Amazon Elasticsearch Service (Amazon ES) access to resources in your AWS account using service-linked roles. A service-linked role is a unique type of AWS Identity and Access Management (IAM) role that's linked directly to Amazon ES. Service-linked roles are predefined by Amazon ES and include all the permissions the service requires to call other AWS services on your behalf.

A service-linked role makes setting up Amazon ES easier because you don't have to manually add the necessary permissions. Amazon ES defines the permissions of its service-linked roles, and unless defined otherwise, only Amazon ES can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

You can delete a service-linked role only after first deleting its related resources. This protects your Amazon ES resources because you can't inadvertently remove permission to access the resources.

For a list of all services that support service-linked roles, see AWS Services That Work with IAM and look for the services that have Yes in the Service-Linked Role column.

Permissions

Amazon ES uses the service-linked role named AWSServiceRoleForAmazonElasticsearchService.

The AWSServiceRoleForAmazonElasticsearchService service-linked role trusts the following services to assume the role:

- es.amazonaws.com

The role permissions policy allows Amazon ES to complete the following actions on the specified resources:

- Action: ec2:CreateNetworkInterface on *
- Action: ec2:DeleteNetworkInterface on *
- Action: ec2:DescribeNetworkInterfaces on *
- Action: ec2:ModifyNetworkInterfaceAttribute on *
- Action: ec2:DescribeSecurityGroups on *
- Action: ec2:DescribeSubnets on *
- Action: ec2:DescribeVpcs on *
- Action: elasticloadbalancing:AddListenerCertificates on *
- Action: elasticloadbalancing:RemoveListenerCertificates on *

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-Linked Role Permissions in the IAM User Guide.

Creating a service-linked role

You don't need to manually create a service-linked role. When you create a VPC access domain using the AWS Management Console, Amazon ES creates the service-linked role for you. In order for this automatic creation to succeed, you must have permissions for the es:CreateElasticsearchServiceRole and iam:CreateServiceLinkedRole actions.
If you delete this service-linked role and then need to create it again, you can use the same process to recreate the role in your account.

You can also use the IAM console, the IAM CLI, or the IAM API to create a service-linked role manually. For more information, see Creating a Service-Linked Role in the IAM User Guide.

**Editing a service-linked role**

Amazon ES doesn't let you edit the AWSServiceRoleForAmazonElasticsearchService service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a Service-Linked Role in the IAM User Guide.

**Deleting a service-linked role**

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don't have an unused entity that is not actively monitored or maintained. However, you must clean up your service-linked role before you can manually delete it.

**Cleaning up a service-linked role**

Before you can use IAM to delete a service-linked role, you must first confirm that the role has no active sessions and remove any resources used by the role.

To check whether the service-linked role has an active session in the IAM console

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane of the IAM console, choose Roles. Then choose the name (not the check box) of the AWSServiceRoleForAmazonElasticsearchService role.
3. On the Summary page for the selected role, choose the Access Advisor tab.
4. On the Access Advisor tab, review recent activity for the service-linked role.

**Note**

If you are unsure whether Amazon ES is using the AWSServiceRoleForAmazonElasticsearchService role, you can try to delete the role. If the service is using the role, then the deletion fails and you can view the regions where the role is being used. If the role is being used, then you must wait for the session to end before you can delete the role. You cannot revoke the session for a service-linked role.

To remove Amazon ES resources used by the AWSServiceRoleForAmazonElasticsearchService

1. Sign in to the AWS Management Console and open the Amazon ES console.
2. Delete any domains that list VPC under the Endpoint column.

**Manually deleting a service-linked role**

Use the Amazon ES configuration API to delete the AWSServiceRoleForAmazonElasticsearchService service-linked role. For more information, see the section called “DeleteElasticsearchServiceRole” (p. 348).
Sample code for Amazon Elasticsearch Service

This chapter contains common sample code for working with Amazon Elasticsearch Service: HTTP request signing in a variety of programming languages, compressing HTTP request bodies, and using the AWS SDKs to create domains.

Topics
- Signing HTTP requests to Amazon Elasticsearch Service (p. 143)
- Compressing HTTP requests in Amazon Elasticsearch Service (p. 151)
- Using the AWS SDKs to interact with Amazon Elasticsearch Service (p. 153)

Signing HTTP requests to Amazon Elasticsearch Service

This section includes examples of how to send signed HTTP requests to Amazon Elasticsearch Service using Elasticsearch clients and other common libraries. These code samples are for interacting with the Elasticsearch APIs, such as `_index`, `_bulk`, and `_snapshot`. If your domain access policy includes IAM users or roles (or you use an IAM master user with fine-grained access control (p. 90)), you must sign requests to the Elasticsearch APIs with your IAM credentials.

Important
For examples of how to interact with the configuration API, including operations like creating, updating, and deleting Amazon ES domains, see the section called "Using the AWS SDKs" (p. 153).

Topics
- Java (p. 143)
- Python (p. 146)
- Ruby (p. 148)
- Node (p. 149)
- Go (p. 150)

Java

The easiest way of sending a signed request is to use the Amazon Web Services Request Signing Interceptor. The repository contains some samples to help you get started, or you can download a sample project for Amazon ES on GitHub.

The following example uses the Elasticsearch low-level Java REST client to perform two unrelated actions: registering a snapshot repository and indexing a document. You must provide values for region and host.

```java
import org.apache.http.HttpHost;
```
import org.apache.http.HttpRequestInterceptor;
import org.apache.http.entity.ContentType;
import org.apache.http.nio.entity.NStringEntity;
import org.elasticsearch.client.Request;
import org.elasticsearch.client.Response;
import org.elasticsearch.client.RestClient;
import com.amazonaws.auth.AWS4Signer;
import com.amazonaws.auth.AWSCredentialsProvider;
import com.amazonaws.auth.DefaultAWSCredentialsProviderChain;
import com.amazonaws.http.AWSRequestSigningApacheInterceptor;
import java.io.IOException;
public class AmazonElasticsearchServiceSample {
    private static String serviceName = "es";
    private static String region = "us-west-1";
    private static String aesEndpoint = "https://domain.us-west-1.es.amazonaws.com";

    private static String payload = 
                "{ 
                    "type": "s3", 
                    "settings": 
                    { 
                        "bucket": "your-bucket", 
                        "region": "us-west-1", 
                        "role_arn": "arn:aws:iam::123456789012:role/TheServiceRole" 
                    }
                }";
    private static String snapshotPath = "/_snapshot/my-snapshot-repo";

    private static String sampleDocument = "{" + ""title":"Walk the Line"," + ""director":"James Mangold"," + ""year":2005"};
    private static String indexingPath = "/my-index/_doc";

    static final AWSCredentialsProvider credentialsProvider = new DefaultAWSCredentialsProviderChain();
    public static void main(String[] args) throws IOException {
        RestClient esClient = esClient(serviceName, region);

        // Register a snapshot repository
        HttpEntity entity = new NStringEntity(payload, ContentType.APPLICATION_JSON);
        Request request = new Request("PUT", snapshotPath);
        request.setEntity(entity);
        // request.addParameter(name, value); // optional parameters
        Response response = esClient.performRequest(request);
        System.out.println(response.toString());

        // Index a document
        String id = "1";
        request = new Request("PUT", indexingPath + "/" + id);
        request.setEntity(entity);

        // Using a String instead of an HttpEntity sets Content-Type to application/json automatically.
        // request.setJsonEntity(sampleDocument);

        response = esClient.performRequest(request);
        System.out.println(response.toString());
    }

    // Adds the interceptor to the ES REST client
    public static RestClient esClient(String serviceName, String region) {
        AWS4Signer signer = new AWS4Signer();
        signer.setServiceName(serviceName);
        signer.setRegionName(region);
        HttpRequestInterceptor interceptor = new AWSRequestSigningApacheInterceptor(serviceName, signer, credentialsProvider);
        return RestClient.builder(HttpHost.create(aesEndpoint)).setHttpClientConfigCallback(hacb -> hacb.addInterceptorLast(interceptor)).build();
    }
}
If you prefer the high-level REST client, which offers most of the same features and simpler code, try the following sample, which also uses the Amazon Web Services Request Signing Interceptor:

```java
import org.apache.http.HttpHost;
import org.apache.http.HttpRequestInterceptor;
import org.elasticsearch.action.index.IndexRequest;
import org.elasticsearch.action.index.IndexResponse;
import org.elasticsearch.client.RequestOptions;
import org.elasticsearch.client.RestClient;
import org.elasticsearch.client.RestHighLevelClient;
import com.amazonaws.auth.AWS4Signer;
import com.amazonaws.auth.AWSCredentialsProvider;
import com.amazonaws.auth.DefaultAWSCredentialsProviderChain;
import com.amazonaws.http.AWSRequestSigningApacheInterceptor;
import java.io.IOException;
import java.util.HashMap;
import java.util.Map;

public class AmazonElasticsearchServiceSample {
    private static String serviceName = "es";
    private static String region = "us-west-1";
    private static String aesEndpoint = ""; // e.g. https://search-mydomain.us-west-1.es.amazonaws.com
    private static String index = "my-index";
    private static String type = "_doc";
    private static String id = "1";
    static final AWSCredentialsProvider credentialsProvider = new DefaultAWSCredentialsProviderChain();

    public static void main(String[] args) throws IOException {
        RestHighLevelClient esClient = esClient(serviceName, region);

        // Create the document as a hash map
        Map<String, Object> document = new HashMap<>();
        document.put("title", "Walk the Line");
        document.put("director", "James Mangold");
        document.put("year", "2005");

        // Form the indexing request, send it, and print the response
        IndexRequest request = new IndexRequest(index, type, id).source(document);
        IndexResponse response = esClient.index(request, RequestOptions.DEFAULT);
        System.out.println(response.toString());
    }

    public static RestHighLevelClient esClient(String serviceName, String region) {
        AWS4Signer signer = new AWS4Signer();
        signer.setServiceName(serviceName);
        signer.setRegionName(region);
        HttpRequestInterceptor interceptor = new AWSRequestSigningApacheInterceptor(serviceName, signer, credentialsProvider);
        return new RestHighLevelClient(RestClient.builder(HttpHost.create(aesEndpoint)).setHttpClientConfigCallback(hacb -> hacb.addInterceptorLast(interceptor)));
    }
}
```

**Tip**
Both signed samples use the default credential chain. Run `aws configure` using the AWS CLI to set your credentials.
Python

You can install elasticsearch-py, an Elasticsearch client for Python, using pip. Instead of the client, you might prefer requests. The requests-aws4auth and SDK for Python (Boto3) packages simplify the authentication process, but are not strictly required. From the terminal, run the following commands:

```
pip install boto3
pip install elasticsearch
pip install requests
pip install requests-aws4auth
```

The following sample code establishes a secure connection to the specified Amazon ES domain and indexes a single document. You must provide values for `region` and `host`.

```
from elasticsearch import Elasticsearch, RequestsHttpConnection
from requests_aws4auth import AWS4Auth
import boto3

host = '' # For example, my-test-domain.us-east-1.es.amazonaws.com
region = '' # e.g. us-west-1

service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
session_token=credentials.token)

es = Elasticsearch(
    hosts = [{'host': host, 'port': 443}],
    http_auth = awsauth,
    use_ssl = True,
    verify_certs = True,
    connection_class = RequestsHttpConnection
)

document = {
    "title": "Moneyball",
    "director": "Bennett Miller",
    "year": "2011"
}

es.index(index="movies", doc_type="_doc", id="5", body=document)

print(es.get(index="movies", doc_type="_doc", id="5"))
```

If you don't want to use elasticsearch-py, you can just make standard HTTP requests. This sample creates a new index with seven shards and two replicas:

```
from requests_aws4auth import AWS4Auth
import boto3
import requests

host = '' # The domain with https:// and trailing slash. For example, https://my-test-domain.us-east-1.es.amazonaws.com/
path = 'my-index' # the Elasticsearch API endpoint
region = '' # For example, us-west-1

service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
session_token=credentials.token)

url = f'https://{host}{path}'

headers = {'Content-Type': 'application/json'}
document = {
    "title": "Moneyball",
    "director": "Bennett Miller",
    "year": "2011"
}

response = requests.put(url, headers=headers, json=document)
```
url = host + path

# The JSON body to accompany the request (if necessary)
payload = {
    "settings": {
        "number_of_shards": 7,
        "number_of_replicas": 2
    }
}

r = requests.put(url, auth=awsauth, json=payload)  # requests.get, post, and delete have similar syntax
print(r.text)

This next example uses the Beautiful Soup library to help build a bulk file from a local directory of HTML files. Using the same client as the first example, you can send the file to the _bulk API for indexing. You could use this code as the basis for adding search functionality to a website:

```python
from bs4 import BeautifulSoup
from elasticsearch import Elasticsearch, RequestsHttpConnection
from requests_aws4auth import AWS4Auth
import boto3
import glob
import json

bulk_file = ''

id = 1

# This loop iterates through all HTML files in the current directory and indexes two things: the contents of the first h1 tag and all other text.
for html_file in glob.glob('*.htm'):
    with open(html_file) as f:
        soup = BeautifulSoup(f, 'html.parser')

        title = soup.h1.string
        body = soup.get_text(" ", strip=True)
        # If get_text() is too noisy, you can do further processing on the string.

        index = { 'title': title, 'body': body, 'link': html_file }
        # If running this script on a website, you probably need to prepend the URL and path to html_file.

        # The action_and_metadata portion of the bulk file
        bulk_file += '{ "index" : { "_index" : "site", "_type" : "_doc", "_id" : "{}" + str(id) + '" } }\n'

        # The optional_document portion of the bulk file
        bulk_file += json.dumps(index) + '\n'

        id += 1

host = ''  # For example, my-test-domain.us-east-1.es.amazonaws.com
region = ''  # e.g. us-west-1

service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service)
es = Elasticsearch(
    hosts = [{'host': host, 'port': 443}],
    http_auth = awsauth,
    connection_class = RequestsHttpConnection)
```
Ruby

This first example uses the Elasticsearch Ruby client and Faraday middleware to perform the request signing. From the terminal, run the following commands:

```ruby
gem install elasticsearch
gem install faraday_middleware-aws-sigv4
```

This sample code creates a new Elasticsearch client, configures Faraday middleware to sign requests, and indexes a single document. You must provide values for `full_url_and_port` and `region`.

```ruby
require 'elasticsearch'
require 'faraday_middleware/aws_sigv4'

full_url_and_port = '' # e.g. https://my-domain.region.es.amazonaws.com:443
index = 'ruby-index'
type = '_doc'
id = '1'
document = {
  year: 2007,
  title: '5 Centimeters per Second',
  info: {
    plot: 'Told in three interconnected segments, we follow a young man named Takaki through his life.',
    rating: 7.7
  }
}

region = '' # e.g. us-west-1
service = 'es'

client = Elasticsearch::Client.new(url: full_url_and_port) do |f|
  f.request :aws_sigv4,
  service: service,
  region: region,
  access_key_id: ENV['AWS_ACCESS_KEY_ID'],
  secret_access_key: ENV['AWS_SECRET_ACCESS_KEY'],
  session_token: ENV['AWS_SESSION_TOKEN'] # optional
end

puts client.index(index: index, type: type, id: id, body: document)
```

If your credentials don't work, export them at the terminal using the following commands:

```bash
export AWS_ACCESS_KEY_ID="your-access-key"
export AWS_SECRET_ACCESS_KEY="your-secret-key"
export AWS_SESSION_TOKEN="your-session-token"
```

This next example uses the AWS SDK for Ruby and standard Ruby libraries to send a signed HTTP request. Like the first example, it indexes a single document. You must provide values for `host` and `region`.

```ruby
require 'elasticsearch'
require 'faraday_middleware/aws_sigv4'

host = 'my-domain.region.es.amazonaws.com'
region = 'us-west-1'

client = Elasticsearch::Client.new(url: host, region: region) do |f|
  f.request :aws_sigv4,
  host: host,
  service: 'es',
  region: region,
  access_key_id: ENV['AWS_ACCESS_KEY_ID'],
  secret_access_key: ENV['AWS_SECRET_ACCESS_KEY'],
  session_token: ENV['AWS_SESSION_TOKEN'] # optional
end

puts client.index(index: index, type: type, id: id, body: document)
```
require 'aws-sdk-elasticsearchservice'

host = '' # e.g. https://my-domain.region.es.amazonaws.com
index = 'ruby-index'
type = '_doc'
id = '2'
document = {
  year: 2007,
title: '5 Centimeters per Second',
  info: {
    plot: 'Told in three interconnected segments, we follow a young man named Takaki through his life.',
    rating: 7.7
  }
}

service = 'es'
region = '' # e.g. us-west-1

signer = Aws::Sigv4::Signer.new(
  service: service,
  region: region,
  access_key_id: ENV['AWS_ACCESS_KEY_ID'],
  secret_access_key: ENV['AWS_SECRET_ACCESS_KEY'],
  session_token: ENV['AWS_SESSION_TOKEN']
)

signature = signer.sign_request(
  http_method: 'PUT',
  url: host + '/' + index + '/' + type + '/' + id,
  body: document.to_json
)

uri = URI(host + '/' + index + '/' + type + '/' + id)

Net::HTTP.start(uri.host, uri.port, :use_ssl => true) do |http|
  request = Net::HTTP::Put.new uri
  request.body = document.to_json
  request['Host'] = signature.headers['host']
  request['X-Amz-Date'] = signature.headers['x-amz-date']
  request['X-Amz-Security-Token'] = signature.headers['x-amz-security-token']
  request['X-Amz-Content-Sha256'] = signature.headers['x-amz-content-sha256']
  request['Authorization'] = signature.headers['authorization']
  request['Content-Type'] = 'application/json'
  response = http.request request
  puts response.body
end

## Node

This example uses the [SDK for JavaScript in Node.js](https://github.com/aws/aws-sdk-js). From the terminal, run the following commands:

```
npm install aws-sdk
```

This sample code indexes a single document. You must provide values for `region` and `domain`.

```javascript
var AWS = require('aws-sdk');

var region = ''; // e.g. us-west-1
var domain = ''; // e.g. search-domain.region.es.amazonaws.com
var index = 'node-test';
```
var type = '_doc';
var id = '1';
var json = {
    "title": "Moneyball",
    "director": "Bennett Miller",
    "year": "2011"
}
indexDocument(json);

function indexDocument(document) {
    var endpoint = new AWS.Endpoint(domain);
    var request = new AWS.HttpRequest(endpoint, region);

    request.method = 'PUT';
    request.path += index + '/' + type + '/' + id;
    request.body = JSON.stringify(document);
    request.headers['host'] = domain;
    request.headers['Content-Type'] = 'application/json';
    // Content-Length is only needed for DELETE requests that include a request body, but including it for all requests doesn't seem to hurt anything.
    request.headers['Content-Length'] = Buffer.byteLength(request.body);

    var credentials = new AWS.EnvironmentCredentials('AWS');
    var signer = new AWS.Signers.V4(request, 'es');
    signer.addAuthorization(credentials, new Date());

    var client = new AWS.HttpClient();
    client.handleRequest(request, null, function(response) {
        console.log(response.statusCode + ' ' + response.statusMessage);
        var responseBody = '';
        response.on('data', function (chunk) {
            responseBody += chunk;
        });
        response.on('end', function (chunk) {
            console.log('Response body: ' + responseBody);
        });
        }, function(error) {
            console.log('Error: ' + error);
        });
}

If your credentials don't work, export them at the terminal using the following commands:

export AWS_ACCESS_KEY_ID="your-access-key"
export AWS_SECRET_ACCESS_KEY="your-secret-key"
export AWS_SESSION_TOKEN="your-session-token"

**Go**

This example uses the AWS SDK for Go and indexes a single document. You must provide values for domain and region.

```
package main

import (
    "fmt"
    "net/http"
    "strings"
    "time"
    "github.com/aws/aws-sdk-go/aws/credentials"
    "github.com/aws/aws-sdk-go/aws/signer/v4"
)
func main() {
    // Basic information for the Amazon Elasticsearch Service domain
    domain := "" // e.g. https://my-domain.region.es.amazonaws.com
    index := "my-index"
    id := "1"
    endpoint := domain + "/" + index + "/" + "_doc" + "/" + id
    region := "" // e.g. us-east-1
    service := "es"

    // Sample JSON document to be included as the request body
    json := `
      "title": "Thor: Ragnarok",
      "director": "Taika Waititi",
      "year": "2017"
    `
    body := strings.NewReader(json)

    // Get credentials from environment variables and create the Signature Version 4 signer
    credentials := credentials.NewEnvCredentials()
    signer := v4.NewSigner(credentials)

    // An HTTP client for sending the request
    client := &http.Client{}

    // Form the HTTP request
    if err != nil {
        fmt.Print(err)
    }

    // You can probably infer Content-Type programmatically, but here, we just say that it's
    // JSON
    req.Header.Add("Content-Type", "application/json")

    // Sign the request, send it, and print the response
    resp, err := client.Do(req)
    if err != nil {
        fmt.Print(err)
    }
    fmt.Println(resp.Status + 
}

If your credentials don't work, export them at the terminal using the following commands:

export AWS_ACCESS_KEY_ID="your-access-key"
export AWS_SECRET_ACCESS_KEY="your-secret-key"
export AWS_SESSION_TOKEN="your-session-token"

Compressing HTTP requests in Amazon Elasticsearch Service

You can compress HTTP requests and responses in Amazon Elasticsearch Service (Amazon ES) domains using gzip compression. Gzip compression can help you reduce the size of your documents and lower bandwidth utilization and latency, thereby leading to improved transfer speeds.

Gzip compression is supported for all domains running Elasticsearch 6.0 or later. Some Elasticsearch clients have built-in support for gzip compression, and many programming languages have libraries that simplify the process.
Enabling gzip compression

Not to be confused with similar Elasticsearch settings, `http_compression.enabled` is specific to Amazon ES and enables or disables gzip compression on a domain. Domains running Elasticsearch 7.x have the feature enabled by default, whereas domains running 6.x have it disabled by default.

To enable gzip compression, send the following request:

```json
PUT _cluster/settings
{
  "persistent": {
    "http_compression.enabled": true
  }
}
```

Requests to `_cluster/settings` must be uncompressed, so you might need to use a separate client or standard HTTP request to update cluster settings.

Required headers

When including a gzip-compressed request body, keep the standard `Content-Type: application/json` header, and add the `Content-Encoding: gzip` header. To accept a gzip-compressed response, add the `Accept-Encoding: gzip` header, as well. If an Elasticsearch client supports gzip compression, it likely includes these headers automatically.

Sample code (Python 3)

The following sample uses `elasticsearch-py` to perform the compression and send the request. This code signs the request using your IAM credentials.

```python
from elasticsearch import Elasticsearch, RequestsHttpConnection
from requests_aws4auth import AWS4Auth
import boto3

host = '' # e.g. my-test-domain.us-east-1.es.amazonaws.com
region = '' # e.g. us-west-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
                   session_token=credentials.token)

# Create the client.
es = Elasticsearch(
    hosts = [{'host': host, 'port': 443}],
    http_auth = awsauth,
    use_ssl = True,
    verify_certs = True,
    http_compress = True, # enables gzip compression for request bodies
    connection_class = RequestsHttpConnection)

document = {
    "title": "Moneyball",
    "director": "Bennett Miller",
    "year": "2011"
}

# Send the request.
print(es.index(index='movies', id='1', body=document, refresh=True))
```
Using the AWS SDKs to interact with Amazon Elasticsearch Service

This section includes examples of how to use the AWS SDKs to interact with the Amazon Elasticsearch Service (Amazon ES) configuration API. These code samples show how to create, update, and delete Amazon ES domains.

Important
For examples of how to interact with the Elasticsearch APIs, such as _index, _bulk, _search, and _snapshot, see the section called "Signing HTTP requests" (p. 143).

Java

This example uses the AWS SDK for Java to create a domain, update its configuration, and delete it. Uncomment the calls to waitForDomainProcessing (and comment the call to deleteDomain) to allow the domain to come online and be useable.

```java
package com.amazonaws.samples;
import java.util.concurrent.TimeUnit;

API Version 2015-01-01
153
```
import com.amazonaws.auth.DefaultAWSCredentialsProviderChain;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.elasticsearch.AWS Elasticsearch;
import com.amazonaws.services.elasticsearch.AWSElasticsearchClientBuilder;
import com.amazonaws.services.elasticsearch.model.CreateElasticsearchDomainRequest;
import com.amazonaws.services.elasticsearch.model.CreateElasticsearchDomainResult;
import com.amazonaws.services.elasticsearch.model.DeleteElasticsearchDomainRequest;
import com.amazonaws.services.elasticsearch.model.DeleteElasticsearchDomainResult;
import com.amazonaws.services.elasticsearch.model.DescribeElasticsearchDomainRequest;
import com.amazonaws.services.elasticsearch.model.DescribeElasticsearchDomainResult;
import com.amazonaws.services.elasticsearch.model.EBSOptions;
import com.amazonaws.services.elasticsearch.model.ElasticsearchClusterConfig;
import com.amazonaws.services.elasticsearch.model.NodeToNodeEncryptionOptions;
import com.amazonaws.services.elasticsearch.model.ResourceNotFoundException;
import com.amazonaws.services.elasticsearch.model.SnapshotOptions;
import com.amazonaws.services.elasticsearch.model.UpdateElasticsearchDomainConfigRequest;
import com.amazonaws.services.elasticsearch.model.UpdateElasticsearchDomainConfigResult;
import com.amazonaws.services.elasticsearch.model.VolumeType;

/**
 * Sample class demonstrating how to use the Amazon Web Services SDK for Java to create,
 * update,
 * and delete Amazon Elasticsearch Service domains.
 */

public class AESSample {

    public static void main(String[] args) {

        final String domainName = "my-test-domain";
        // Build the client using the default credentials chain.
        // You can use the CLI and run `aws configure` to set access key, secret
        // key, and default region.
        final AWSElasticsearch client = AWSElasticsearchClientBuilder
            .standard()
            // Unnecessary, but lets you use a region different than your default.
            .withRegion(Regions.US_WEST_2)
            // Unnecessary, but if desired, you can use a different provider chain.
            .withCredentials(new DefaultAWSCredentialsProviderChain())
            .build();

        // Create a new domain, update its configuration, and delete it.
        createDomain(client, domainName);
        // waitForDomainProcessing(client, domainName);
        updateDomain(client, domainName);
        // waitForDomainProcessing(client, domainName);
        deleteDomain(client, domainName);
    }

    /**
     * Creates an Amazon Elasticsearch Service domain with the specified options.
     * Some options require other Amazon Web Services resources, such as an Amazon Cognito
     * user pool
     * and identity pool, whereas others require just an instance type or instance
     * count.
     * *
     * @param client
     * The client to use for the requests to Amazon
     * Elasticsearch Service
     * @param domainName
     * The name of the domain you want to create
     */
    private static void createDomain(final AWSElasticsearch client, final String
        domainName) {
// Create the request and set the desired configuration options
CreateElasticsearchDomainRequest createRequest = new
CreateElasticsearchDomainRequest()
    .withDomainName(domainName)
    .withElasticsearchVersion("6.3")
    .withElasticsearchClusterConfig(new ElasticsearchClusterConfig()
        .withDedicatedMasterEnabled(true)
        .withDedicatedMasterCount(3)
        // Small, inexpensive instance types for testing. Not recommended
        // for production
        .withDedicatedMasterType("t2.small.elasticsearch")
        .withInstanceType("t2.small.elasticsearch")
        .withInstanceCount(5))
    // Many instance types require EBS storage.
    .withEBSOptions(new EBSOptions()
        .withEBSEnabled(true)
        .withVolumeSize(10)
        .withVolumeType(VolumeType.Gp2))
    // You can uncomment this line and add your account ID, a user name, and
    // domain name to add an access policy.
    // .withAccessPolicies("{"Version":"2012-10-17","Statement":
    // [{"Effect":"Allow","Principal":{"AWS":["arn:aws:iam::123456789012:user/user-name
    // "],"Action":["es:*"],"Resource":"arn:aws:es:region:123456789012:domain/domain-
    // name/*"]})
    .withNodeToNodeEncryptionOptions(new NodeToNodeEncryptionOptions()
        .withEnabled(true));

    // Make the request.
    System.out.println("Sending domain creation request...");
    CreateElasticsearchDomainResult createResponse =
    client.createElasticsearchDomain(createRequest);
    System.out.println("Domain creation response from Amazon Elasticsearch Service: ");
    System.out.println(createResponse.getDomainStatus().toString());
}
/**
 * Updates the configuration of an Amazon Elasticsearch Service domain with the
 * specified options. Some options require other Amazon Web Services resources, such as
 * Amazon Cognito user pool and identity pool, whereas others require just an
 * instance type or instance count.
 * @param client
 * The client to use for the requests to Amazon
 * Elasticsearch Service
 * @param domainName
 * The name of the domain to update
 */
private static void updateDomain(final AWSElasticsearch client, final String
domainName) {
    try {
        System.out.println("Sending domain creation request... ");
        CreateElasticsearchDomainResult createResponse =
        client.createElasticsearchDomain(createRequest);
        System.out.println("Domain creation response from Amazon Elasticsearch Service: ");
        System.out.println(createResponse.getDomainStatus().toString());
    }
withInstanceCount(3));

System.out.println("Sending domain update request...");
final UpdateElasticsearchDomainConfigResult updateResponse = client
.updateElasticsearchDomainConfig(updateRequest);
System.out.println("Domain update response from Amazon Elasticsearch
Service:");
System.out.println(updateResponse.toString());
} catch (ResourceNotFoundException e) {
    System.out.println("Domain not found. Please check the domain name.");
}
}

/**
 * Deletes an Amazon Elasticsearch Service domain. Deleting a domain can take
 * several minutes.
 * @param client          The client to use for the requests to Amazon
 * @param domainName      The name of the domain that you want to delete
 */
private static void deleteDomain(final AWSElasticsearch client, final String domainName) {
    try {
        final DeleteElasticsearchDomainRequest deleteRequest = new
DeleteElasticsearchDomainRequest()
            .withDomainName(domainName);

        System.out.println("Sending domain deletion request...");
        final DeleteElasticsearchDomainResult deleteResponse = client.deleteElasticsearchDomain(deleteRequest);
        System.out.println("Domain deletion response from Amazon Elasticsearch
Service:");
        System.out.println(deleteResponse.toString());
    } catch (ResourceNotFoundException e) {
        System.out.println("Domain not found. Please check the domain name.");
    }
}

/**
 * Waits for the domain to finish processing changes. New domains typically take 15-30
 * minutes to initialize, but can take longer depending on the configuration. Most updates to
 * existing domains take a similar amount of time. This method checks every 15 seconds and finishes only when
 * the domain's processing status changes to false.
 * @param client          The client to use for the requests to Amazon
 * @param domainName      The name of the domain that you want to check
 */
private static void waitForDomainProcessing(final AWSElasticsearch client, final String domainName) {
    // Create a new request to check the domain status.
    final DescribeElasticsearchDomainRequest describeRequest = new
DescribeElasticsearchDomainRequest()
        .withDomainName(domainName);

    // Every 15 seconds, check whether the domain is processing.
    DescribeElasticsearchDomainResult describeResponse = client.describeElasticsearchDomain(describeRequest);

    while (describeResponse.getProcessing().equals("true")) {
        // Wait 15 seconds before checking again.
        try {
            Thread.sleep(15000);
        } catch (InterruptedException e) {
            Thread.currentThread().interrupt();
        }
        describeResponse = client.describeElasticsearchDomain(describeRequest);
    }
}
while (describeResponse.getDomainStatus().isProcessing()) {
    try {
        System.out.println("Domain still processing..." volley); // move to next line
        TimeUnit.SECONDS.sleep(15); // move to next line
        describeResponse = client.describeElasticsearchDomain(describeRequest); // move to next line
    } catch (InterruptedException e) {
        e.printStackTrace();
    }
}

// Once we exit that loop, the domain is available
System.out.println("Amazon Elasticsearch Service has finished processing changes for your domain.");
System.out.println("Domain description response from Amazon Elasticsearch Service:");
System.out.println(describeResponse.toString());
}
Indexing data in Amazon Elasticsearch Service

Because Amazon Elasticsearch Service (Amazon ES) uses a REST API, numerous methods exist for indexing documents. You can use standard clients like curl or any programming language that can send HTTP requests. To further simplify the process of interacting with it, Amazon ES has clients for many programming languages. Advanced users can skip directly to the section called “Signing HTTP requests” (p. 143) or the section called “Loading streaming data into Amazon ES” (p. 160).

For an introduction to indexing, see the Open Distro for Elasticsearch documentation.

Naming restrictions for indices

Amazon ES indices have the following naming restrictions:

- All letters must be lowercase.
- Index names cannot begin with _ or -.
- Index names can't contain spaces, commas, ;, *, +, /, \, |, ?, #, >, or <.

Don't include sensitive information in index, type, or document ID names. Amazon ES uses these names in its Uniform Resource Identifiers (URIs). Servers and applications often log HTTP requests, which can lead to unnecessary data exposure if URIs contain sensitive information:

```
```

Even if you don't have permissions (p. 77) to view the associated JSON document, you could infer from this fake log line that one of Dr. Doe's patients with a phone number of 202-555-0100 had the flu in 2018.

Reducing response size

Responses from the _index and _bulk APIs contain quite a bit of information. This information can be useful for troubleshooting requests or for implementing retry logic, but can use considerable bandwidth. In this example, indexing a 32 byte document results in a 339 byte response (including headers):

```
PUT elasticsearch_domain/more-movies/_doc/1
{"title": "Back to the Future"}
```

Response

```
{
  "_index": "more-movies",
```
Amazon Elasticsearch Service Developer Guide
Reducing response size

}

"_type": "_doc",
"_id": "1",
"_version": 4,
"result": "updated",
"_shards": {
"total": 2,
"successful": 2,
"failed": 0
},
"_seq_no": 3,
"_primary_term": 1

This response size might seem minimal, but if you index 1,000,000 documents per day—approximately
11.5 documents per second—339 bytes per response works out to 10.17 GB of download traﬃc per
month.
If data transfer costs are a concern, use the filter_path parameter to reduce the size of the Amazon
ES response, but be careful not to ﬁlter out ﬁelds that you need in order to identify or retry failed
requests. These ﬁelds vary by client. The filter_path parameter works for all Amazon ES REST APIs,
but is especially useful with APIs that you call frequently, such as the _index and _bulk APIs:
PUT elasticsearch_domain/more-movies/_doc/1?filter_path=result,_shards.total
{"title": "Back to the Future"}

Response
{

}

"result": "updated",
"_shards": {
"total": 2
}

Instead of including ﬁelds, you can exclude ﬁelds with a - preﬁx. filter_path also supports wildcards:
POST elasticsearch_domain/_bulk?filter_path=-took,-items.index._*
{ "index": { "_index": "more-movies", "_id": "1" } }
{"title": "Back to the Future"}
{ "index": { "_index": "more-movies", "_id": "2" } }
{"title": "Spirited Away"}

Response
{

"errors": false,
"items": [
{
"index": {
"result": "updated",
"status": 200
}
},
{
"index": {
"result": "updated",
"status": 200
}
}
]

API Version 2015-01-01
159


Loading streaming data into Amazon Elasticsearch Service

You can load streaming data into your Amazon Elasticsearch Service (Amazon ES) domain from many different sources. Some sources, like Amazon Kinesis Data Firehose and Amazon CloudWatch Logs, have built-in support for Amazon ES. Others, like Amazon S3, Amazon Kinesis Data Streams, and Amazon DynamoDB, use AWS Lambda functions as event handlers. The Lambda functions respond to new data by processing it and streaming it to your domain.

**Note**
Lambda supports several popular programming languages and is available in most AWS Regions. For more information, see Building Lambda Functions in the *AWS Lambda Developer Guide* and AWS Lambda Regions in the *AWS General Reference*.

**Topics**
- Loading streaming data from Amazon S3 (p. 160)  
- Loading streaming data from Amazon Kinesis Data Streams (p. 165)  
- Loading streaming data from Amazon DynamoDB (p. 167)  
- Loading streaming data from Amazon Kinesis Data Firehose (p. 170)  
- Loading streaming data from Amazon CloudWatch (p. 170)  
- Loading streaming data from AWS IoT (p. 170)

### Loading streaming data from Amazon S3

You can use Lambda to send data to your Amazon ES domain from Amazon S3. New data that arrives in an S3 bucket triggers an event notification to Lambda, which then runs your custom code to perform the indexing.

This method of streaming data is extremely flexible. You can index object metadata, or if the object is plaintext, parse and index some elements of the object body. This section includes some unsophisticated Python sample code that uses regular expressions to parse a log file and index the matches.

**Tip**
For more robust code in Node.js, see [amazon-elasticsearch-lambda-samples](https://github.com/aws-samples/amazon-elasticsearch-lambda-samples) on GitHub. Some Lambda blueprints also contain useful parsing examples.

### Prerequisites

Before proceeding, you must have the following resources.

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon S3 Bucket</td>
<td>For more information, see <a href="https://docs.aws.amazon.com/AmazonS3/latest/userguide/creating-a-bucket.html">Creating a Bucket</a> in the <em>Amazon Simple Storage Service Getting Started Guide</em>. The bucket must reside in the same region as your Amazon ES domain.</td>
</tr>
<tr>
<td>Amazon ES Domain</td>
<td>The destination for data after your Lambda function processes it. For more information, see <a href="https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-domains.html#es-domains-create">Creating Amazon ES Domains</a> (p. 9).</td>
</tr>
</tbody>
</table>
Create the Lambda deployment package

Deployment packages are ZIP or JAR files that contain your code and its dependencies. This section includes Python sample code. For other programming languages, see Creating a Deployment Package in the AWS Lambda Developer Guide.

1. Create a directory. In this sample, we use the name `s3-to-es`.
2. Create a file in the directory named `sample.py`:

   ```python
   import boto3
   import re
   import requests
   from requests_aws4auth import AWS4Auth

   region = '' # e.g. us-west-1
   service = 'es'
   credentials = boto3.Session().get_credentials()
   awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
                      session_token=credentials.token)

   host = '' # the Amazon ES domain, including https://
   index = 'lambda-s3-index'
   type = '_doc'
   url = host + '/' + index + '/' + type
   headers = { "Content-Type": "application/json" }

   s3 = boto3.client('s3')

   # Regular expressions used to parse some simple log lines
   ip_pattern = re.compile('((d+\.\d+\./\d+))')
   time_pattern = re.compile('((d+\/)\w\w\w/\d\d\d\d:\d\d:\d\d:\d\d)')
   message_pattern = re.compile('"(.+)"

   # Lambda execution starts here
   def handler(event, context):
       for record in event['Records']:
           # Get the bucket name and key for the new file
           bucket = record['s3']['bucket']['name']
           key = record['s3']['object']['key']

           # Get, read, and split the file into lines
           obj = s3.get_object(Bucket=bucket, Key=key)
           body = obj['Body'].read()
           lines = body.splitlines()

           # Match the regular expressions to each line and index the JSON
           for line in lines:
               ip = ip_pattern.search(line).group(1)
               timestamp = time_pattern.search(line).group(1)
               message = message_pattern.search(line).group(1)

               document = { "ip": ip, "timestamp": timestamp, "message": message }
               r = requests.post(url, auth=awsauth, json=document, headers=headers)

   Edit the variables for region and host.

3. Install dependencies:

   ```bash
   cd s3-to-es
   pip install requests -t .
   ```
All Lambda execution environments have Boto3 installed, so you don't need to include it in your deployment package.

**Tip**
If you use macOS, these commands might not work properly. As a workaround, add a file named `setup.cfg` to the `s3-to-es` directory:

```
[install]
prefix=
```

4. Package the application code and dependencies:

```
zip -r lambda.zip *
```

**Create the Lambda function**

After you create the deployment package, you can create the Lambda function. When you create a function, choose a name, runtime (for example, Python 2.7), and IAM role. The IAM role defines the permissions for your function. For detailed instructions, see Create a Simple Lambda Function in the AWS Lambda Developer Guide.

This example assumes you're using the console. Choose Python 2.7 and a role that has S3 read permissions and Amazon ES write permissions, as shown in the following screenshot:
After you create the function, you must add a trigger. For this example, we want the code to run whenever a log file arrives in an S3 bucket:

1. Choose S3.
2. Choose your bucket.
3. For **Event type**, choose **PUT**.
4. For **Prefix**, type **logs/**.
5. For **Filter pattern**, type **.log**.
6. Select **Enable trigger**.
7. Choose **Add**.
Finally, you can upload your deployment package:

1. For Handler, type sample.handler. This setting tells Lambda the file (sample.py) and method (handler) that it should run after a trigger.
2. For Code entry type, choose Upload a .ZIP file, and then follow the prompts to upload your deployment package.
3. Choose Save.

At this point, you have a complete set of resources: a bucket for log files, a function that runs whenever a log file is added to the bucket, code that performs the parsing and indexing, and an Amazon ES domain for searching and visualization.

Testing the Lambda Function

After you create the function, you can test it by uploading a file to the Amazon S3 bucket. Create a file named sample.log using following sample log lines:

<table>
<thead>
<tr>
<th>Log Level</th>
<th>Timestamp</th>
<th>Message</th>
</tr>
</thead>
</table>

Upload the file to the logs folder of your S3 bucket. For instructions, see Add an Object to a Bucket in the Amazon Simple Storage Service Getting Started Guide.

Then use the Amazon ES console or Kibana to verify that the lambda-s3-index index contains two documents. You can also make a standard search request:

```json
GET https://es-domain/lambda-index/_search?pretty
{
    "hits" : {
        "total" : 2,
        "max_score" : 1.0,
        "hits" : [
            {
                "_index" : "lambda-s3-index",
                "_type" : "_doc",
                "_id" : "vTYxMIBJWV_TTkESDg",
                "_score" : 1.0,
                "_source" : {
                    "ip" : "12.345.678.91",
                    "message" : "GET /some-file.jpg",
                }
            },
            {
                "_index" : "lambda-s3-index",
                "_type" : "_doc",
                "_id" : "vjYmAHBIJWV_TTkEdCAB",
                "_score" : 1.0,
                "_source" : {
                    "ip" : "12.345.678.90",
                    "message" : "PUT /some-file.jpg",
                }
            }
        ]
    }
}```
Loading streaming data from Amazon Kinesis Data Streams

You can load streaming data from Kinesis Data Streams to Amazon ES. New data that arrives in the data stream triggers an event notification to Lambda, which then runs your custom code to perform the indexing. This section includes some unsophisticated Python sample code. For more robust code in Node.js, see amazon-elasticsearch-lambda-samples on GitHub.

Prerequisites

Before proceeding, you must have the following resources.

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Kinesis Data Stream</td>
<td>The event source for your Lambda function. To learn more, see Kinesis Data Streams.</td>
</tr>
<tr>
<td>Amazon ES Domain</td>
<td>The destination for data after your Lambda function processes it. For more information, see Creating Amazon ES Domains.</td>
</tr>
<tr>
<td>IAM Role</td>
<td>This role must have basic Amazon ES, Kinesis, and Lambda permissions, such as the following:</td>
</tr>
</tbody>
</table>

```json
{
  "Version": "2012-10-17",
  "Statement": [ 
    { 
      "Effect": "Allow",
      "Action": [ 
        "es:ESHttpPost",
        "es:ESHttpPut",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "kinesis:GetShardIterator",
        "kinesis:GetRecords",
        "kinesis:DescribeStream",
        "kinesis:ListStreams"
      ],
      "Resource": "*"
    }
  ]
}
```

The role must have the following trust relationship:

```json
{
  "Version": "2012-10-17",
  "Statement": [ 
    { 
      "Effect": "Allow",
      "Principal": { 
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```
Create the Lambda function

Follow the instructions in the section called “Create the Lambda deployment package” (p. 161), but create a directory named kinesis-to-es and use the following code for sample.py:

```python
import base64
import boto3
import json
import requests
from requests_aws4auth import AWS4Auth

region = '' # e.g. us-west-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
    session_token=credentials.token)

host = '' # the Amazon ES domain, including https://
index = 'lambda-kine-index'
type = '_doc'
url = host + '/' + index + '/' + type + '/'
headers = { "Content-Type": "application/json" }

def handler(event, context):
    count = 0
    for record in event['Records']:
        id = record['eventID']
        timestamp = record['kinesis']['approximateArrivalTimestamp']

        # Kinesis data is base64-encoded, so decode here
        message = base64.b64decode(record['kinesis']['data'])

        document = { "id": id, "timestamp": timestamp, "message": message }

        # Index the document
        r = requests.put(url + id, auth=awsauth, json=document, headers=headers)
        count += 1

    return 'Processed ' + str(count) + ' items.'
```

Edit the variables for region and host.

Use the following commands to install your dependencies:

```bash
cd kinesis-to-es
pip install requests -t .
pip install requests_aws4auth -t .
```

Then follow the instructions in the section called “Create the Lambda function” (p. 162), but specify the IAM role from the section called “Prerequisites” (p. 165) and the following settings for the trigger:

- **Kinesis stream**: your Kinesis stream
- **Batch size**: 100
- **Starting position**: Trim horizon
To learn more, see Working with Amazon Kinesis Data Streams in the Amazon Kinesis Data Streams Developer Guide.

At this point, you have a complete set of resources: a Kinesis data stream, a function that runs after the stream receives new data and indexes that data, and an Amazon ES domain for searching and visualization.

**Test the Lambda Function**

After you create the function, you can test it by adding a new record to the data stream using the AWS CLI:

```
aws kinesis put-record --stream-name es-test --data "My test data." --partition-key partitionKey1 --region us-west-1
```

Then use the Amazon ES console or Kibana to verify that `lambda-kine-index` contains a document. You can also use the following request:

```
GET https://es-domain/lambda-kine-index/_search
{
  "hits" : [
    {
      "_index": "lambda-kine-index",
      "_type": "_doc",
      "_id": "shardId-000000000000:49583511615762699495012960821421456686529436680496087042",
      "_score": 1,
      "_source": {
        "timestamp": 1523648740.051,
        "message": "My test data."
      }
    }
  ]
}
```

**Loading streaming data from Amazon DynamoDB**

You can use AWS Lambda to send data to your Amazon ES domain from Amazon DynamoDB. New data that arrives in the database table triggers an event notification to Lambda, which then runs your custom code to perform the indexing.

**Prerequisites**

Before proceeding, you must have the following resources.

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DynamoDB Table</td>
<td>The table contains your source data. For more information, see <a href="https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/">Basic Operations for Tables</a> in the <em>Amazon DynamoDB Developer Guide</em>. The table must reside in the same region as your Amazon ES domain and have a stream set to New image. To learn more, see <a href="https://docs.aws.amazon.com/amazonses/latest/developerguide/">Enabling a Stream</a>.</td>
</tr>
<tr>
<td>Amazon ES Domain</td>
<td>The destination for data after your Lambda function processes it. For more information, see <a href="https://docs.aws.amazon.com/amazonses/latest/developerguide/">Creating Amazon ES Domains</a> (p. 9).</td>
</tr>
</tbody>
</table>
Loading streaming data from Amazon DynamoDB

Prerequisite | Description
---|---
IAM Role | This role must have basic Amazon ES, DynamoDB, and Lambda execution permissions, such as the following:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "es:ESHttpPost",
                "es:ESHttpPut",
                "dynamodb:DescribeStream",
                "dynamodb:GetRecords",
                "dynamodb:GetShardIterator",
                "dynamodb:ListStreams",
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "*"
        }
    ]
}
```

The role must have the following trust relationship:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "lambda.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

To learn more, see Creating IAM Roles in the IAM User Guide.

Create the Lambda function

Follow the instructions in the section called "Create the Lambda deployment package" (p. 161), but create a directory named `ddb-to-es` and use the following code for `sample.py`:

```python
import boto3
import requests
from requests_aws4auth import AWS4Auth

region = '' # e.g. us-east-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
                    session_token=credentials.token)

host = '' # the Amazon ES domain, with https://
```
index = 'lambda-index'
type = '_doc'
url = host + '/' + index + '/' + type + '/'
headers = { "Content-Type": "application/json" }

def handler(event, context):
    count = 0
    for record in event['Records']:
        # Get the primary key for use as the Elasticsearch ID
        id = record['dynamodb']['Keys']['id']['S']
        if record['eventName'] == 'REMOVE':
            r = requests.delete(url + id, auth=awsauth)
        else:
            document = record['dynamodb']['NewImage']
            r = requests.put(url + id, auth=awsauth, json=document, headers=headers)
            count += 1
    return str(count) + ' records processed.'

Edit the variables for region and host.

Use the following commands to install your dependencies:

cd ddb-to-es
pip install requests -t .
pip install requests_aws4auth -t .

Then follow the instructions in the section called "Create the Lambda function" (p. 162), but specify the IAM role from the section called "Prerequisites" (p. 167) and the following settings for the trigger:

- **Table**: your DynamoDB table
- **Batch size**: 100
- **Starting position**: Trim horizon

To learn more, see Processing New Items in a DynamoDB Table in the Amazon DynamoDB Developer Guide.

At this point, you have a complete set of resources: a DynamoDB table for your source data, a DynamoDB stream of changes to the table, a function that runs after your source data changes and indexes those changes, and an Amazon ES domain for searching and visualization.

**Test the Lambda function**

After you create the function, you can test it by adding a new item to the DynamoDB table using the AWS CLI:

```bash
aws dynamodb put-item --table-name es-test --item '{"director": {"S": "Kevin Costner"},"id": {"S": "00001"},"title": {"S": "The Postman"}}' --region us-west-1
```

Then use the Amazon ES console or Kibana to verify that `lambda-index` contains a document. You can also use the following request:

```csharp
GET https://es-domain/lambda-index/_doc/00001 {
   "_index": "lambda-index",
   "_type": "_doc",
   "_id": "00001",
```

API Version 2015-01-01

169
Loading streaming data from Amazon Kinesis Data Firehose

Kinesis Data Firehose supports Amazon ES as a delivery destination. For instructions about how to load streaming data into Amazon ES, see Creating a Kinesis Data Firehose Delivery Stream and Choose Amazon ES for Your Destination in the Amazon Kinesis Data Firehose Developer Guide.

Before you load data into Amazon ES, you might need to perform transforms on the data. To learn more about using Lambda functions to perform this task, see Data Transformation in the same guide.

As you configure a delivery stream, Kinesis Data Firehose features a "one-click" IAM role that gives it the resource access it needs to send data to Amazon ES, back up data on Amazon S3, and transform data using Lambda. Because of the complexity involved in creating such a role manually, we recommend using the provided role.

Loading streaming data from Amazon CloudWatch

You can load streaming data from CloudWatch Logs to your Amazon ES domain by using a CloudWatch Logs subscription. For information about Amazon CloudWatch subscriptions, see Real-time Processing of Log Data with Subscriptions. For configuration information, see Streaming CloudWatch Logs Data to Amazon Elasticsearch Service in the Amazon CloudWatch Developer Guide.

Loading streaming data from AWS IoT

You can send data from AWS IoT using rules. To learn more, see Amazon ES Action in the AWS IoT Developer Guide.

Loading data into Amazon Elasticsearch Service with Logstash

The open source version of Logstash (Logstash OSS) provides a convenient way to use the bulk API to upload data into your Amazon Elasticsearch Service (Amazon ES) domain. The service supports all standard Logstash input plugins, including the Amazon S3 input plugin. Amazon ES supports two Logstash output plugins: the standard Elasticsearch plugin and the logstash-output-amazon-es plugin, which uses IAM credentials to sign and export Logstash events to Amazon ES.

If your Amazon ES domain uses fine-grained access control (p. 90) with HTTP basic authentication, configuration is similar to any other Elasticsearch cluster. This example configuration file takes its input from the open source version of Filebeat (Filebeat OSS).
Loading data with Logstash

```json
input {
  beats {
    port => 5044
  }
}

output {
  elasticsearch {
    hosts => ["https://domain-endpoint:443"]
    ssl => true
    index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"
    user => "some-user"
    password => "some-user-password"
    ilm_enabled => false
  }
}
```

Configuration varies by Beats application and use case, but your Filebeat OSS configuration might look like this:

```json
filebeat.inputs:
  - type: log
    enabled: true
    paths:
      - /path/to/logs/dir/*.log

filebeat.config.modules:
  path: ${path.config}/modules.d/*.yml
  reload.enabled: false
  setup.ilm.enabled: false
  setup.ilm.check_exists: false
  setup.template.settings:
    index.number_of_shards: 1

output.logstash:
  hosts: ["logstash-host:5044"]
```

If your domain uses an IAM-based domain access policy or fine-grained access control with an IAM master user, you must sign all requests to Amazon ES using IAM credentials. In this case, the simplest solution to sign requests from Logstash OSS is to use the `logstash-output-amazon-es` plugin. First, install the plugin.

```bash
bin/logstash-plugin install logstash-output-amazon_es
```

Then export your IAM credentials (or run `aws configure`).

```bash
export AWS_ACCESS_KEY_ID="your-access-key"
export AWS_SECRET_ACCESS_KEY="your-secret-key"
export AWS_SESSION_TOKEN="your-session-token"
```

Finally, change your configuration file to use the plugin for its output. This example configuration file takes its input from files in an S3 bucket.

```json
input {
  s3 {
    bucket => "my-s3-bucket"
    region => "us-east-1"
  }
}

output {
```

API Version 2015-01-01
171
```ruby
amazon_es {
  hosts => ["domain-endpoint"]
  ssl => true
  region => "us-east-1"
  index => "production-logs-%{+YYYY.MM.dd}"
}
```

If your Amazon ES domain is in a VPC, the Logstash OSS machine must be able to connect to the VPC and have access to the domain through the VPC security groups. For more information, see the section called "About access policies on VPC domains" (p. 25).
Searching data in Amazon Elasticsearch Service

There are several common methods for searching documents in Amazon Elasticsearch Service (Amazon ES), including URI searches and request body searches. Amazon ES offers additional functionality that improves the search experience, such as custom packages, SQL support, and asynchronous search. For a comprehensive Elasticsearch search API reference, see the Open Distro for Elasticsearch documentation.

**Note**
The following sample requests work with the Elasticsearch 6.x and 7.x APIs. Some requests might not work with older Elasticsearch versions.

**Topics**
- URI searches (p. 173)
- Request body searches (p. 174)
- Custom packages for Amazon Elasticsearch Service (p. 177)
- Querying your Amazon Elasticsearch Service data with SQL (p. 183)
- Querying Amazon Elasticsearch Service data using Piped Processing Language (p. 185)
- k-Nearest Neighbor (k-NN) search in Amazon Elasticsearch Service (p. 186)
- Cross-cluster search for Amazon Elasticsearch Service (p. 189)
- Learning to Rank for Amazon Elasticsearch Service (p. 195)
- Asynchronous search for Amazon Elasticsearch Service (p. 212)

## URI searches

Universal Resource Identifier (URI) searches are the simplest form of search. In a URI search, you specify the query as an HTTP request parameter:

```
GET https://search-my-domain.us-west-1.es.amazonaws.com/_search?q=house
```

A sample response might look like the following:

```
{
  "took": 25,
  "timed_out": false,
  "_shards": {
    "total": 10,
    "successful": 10,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": 85,
    "max_score": 6.6137657,
    "hits": [
      {
        "_index": "movies",
        "_type": "movie",
```

API Version 2015-01-01
173
By default, this query searches all fields of all indices for the term house. To narrow the search, specify an index (movies) and a document field (title) in the URI:

```
GET https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search?q=title:house
```

You can include additional parameters in the request, but the supported parameters provide only a small subset of the Elasticsearch search options. The following request returns 20 results (instead of the default of 10) and sorts by year (rather than by _score):

```
```

### Request body searches

To perform more complex searches, use the HTTP request body and the Elasticsearch domain-specific language (DSL) for queries. The query DSL lets you specify the full range of Elasticsearch search options. The following match query is similar to the final URI search (p. 173) example:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "size": 20,
  "sort": {
    "year": {
      "order": "desc"
    }
  }
}
```
"query": {
  "query_string": {
    "default_field": "title",
    "query": "house"
  }
}

**Note**
The _search API accepts HTTP GET and POST for request body searches, but not all HTTP clients support adding a request body to a GET request. POST is the more universal choice.

In many cases, you might want to search several fields, but not all fields. Use the multi_match query:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "size": 20,
  "query": {
    "multi_match": {
      "query": "house",
      "fields": ["title", "plot", "actors", "directors"]
    }
  }
}
```

### Boosting fields

You can improve search relevancy by "boosting" certain fields. Boosts are multipliers that weigh matches in one field more heavily than matches in other fields. In the following example, a match for *john* in the title field influences _score twice as much as a match in the plot field and four times as much as a match in the actors or directors fields. The result is that films like *John Wick* and *John Carter* are near the top of the search results, and films starring John Travolta are near the bottom.

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "size": 20,
  "query": {
    "multi_match": {
      "query": "john",
      "fields": ["title^4", "plot^2", "actors", "directors"]
    }
  }
}
```

### Paginating search results

If you need to display a large number of search results, you can implement pagination using the `from` parameter. The following request returns results 20–39 of the zero-indexed list of search results:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "from": 20,
  "size": 20,
  "query": {
    "multi_match": {
      "query": "house",
      "fields": ["title^4", "plot^2", "actors", "directors"]
    }
  }
}
```
Search result highlighting

The `highlight` option tells Elasticsearch to return an additional object inside of the `hits` array if the query matched one or more fields:

```json
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "size": 20,
  "query": {
    "multi_match": {
      "query": "house",
      "fields": ["title^4", "plot^2", "actors", "directors"]
    }
  },
  "highlight": {
    "fields": {
      "plot": {}
    }
  }
}
```

If the query matched the content of the `plot` field, a hit might look like the following:

```json
{
  "_index": "movies",
  "_type": "movie",
  "_id": "tt0091541",
  "_score": 11.276199,
  "_source": {
    "directors": [
      "Richard Benjamin"
    ],
    "release_date": "1986-03-26T00:00:00Z",
    "rating": 6,
    "genres": [
      "Comedy",
      "Music"
    ],
    "image_url": "http://ia.media-imdb.com/images/M/MV5BMTIzODEzODE2OF5BMl5BanBnXkFtZTcwNjQ3ODcyMQ@@._V1_SX400_.jpg",
    "plot": "A young couple struggles to repair a hopelessly dilapidated house.",
    "title": "The Money Pit",
    "rank": 4095,
    "running_time_secs": 5460,
    "actors": [
      "Tom Hanks",
      "Shelley Long",
      "Alexander Godunov"
    ],
    "year": 1986,
    "id": "tt0091541"
  },
  "highlight": {
    "plot": [
      "A young couple struggles to repair a hopelessly dilapidated <em>house</em>.
    ]
  }
}
```
By default, Elasticsearch wraps the matching string in `<em>` tags, provides up to 100 characters of context around the match, and breaks content into sentences by identifying punctuation marks, spaces, tabs, and line breaks. All of these settings are customizable:

```json
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
    "size": 20,
    "query": {
        "multi_match": {
            "query": "house",
            "fields": ["title^4", "plot^2", "actors", "directors"]
        }
    },
    "highlight": {
        "fields": {
            "plot": {}
        },
        "pre_tags": "<strong>",
        "post_tags": "</strong>",
        "fragment_size": 200,
        "boundary_chars": ".,!? "
    }
}
```

### Count API

If you're not interested in the contents of your documents and just want to know the number of matches, you can use the `_count` API instead of the `_search` API. The following request uses the `query_string` query to identify romantic comedies:

```json
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_count
{
    "query": {
        "query_string": {
            "default_field": "genres",
            "query": "romance AND comedy"
        }
    }
}
```

A sample response might look like the following:

```json
{
    "count": 564,
    "_shards": {
        "total": 5,
        "successful": 5,
        "skipped": 0,
        "failed": 0
    }
}
```

### Custom packages for Amazon Elasticsearch Service

Amazon Elasticsearch Service (Amazon ES) lets you upload custom dictionary files, such as stop words and synonyms, for use with your cluster. The generic term for these types of files is packages. Dictionary files improve your search results by telling Elasticsearch to ignore certain high-frequency words or
to treat terms like "frozen custard," "gelato," and "ice cream" as equivalent. They can also improve stemming, such as in the Japanese (kuromoji) Analysis plugin.

Topics
- Package permissions requirements (p. 178)
- Uploading packages to Amazon S3 (p. 178)
- Importing and associating packages (p. 178)
- Using custom packages with Elasticsearch (p. 179)
- Updating custom packages (p. 181)
- Dissociating and removing packages (p. 183)

Package permissions requirements

Users without administrator access require certain AWS Identity and Access Management (IAM) actions in order to manage packages:

- es:CreatePackage - create a package in an Amazon ES region
- es:DeletePackage - delete a package from an Amazon ES region
- es:AssociatePackage - associate a package to a domain
- es:DissociatePackage - dissociate a package from a domain

You also need permissions on the Amazon S3 bucket path or object where the custom package resides. Grant all permission within IAM, not in the domain access policy. For more information, see the section called "Identity and Access Management" (p. 77).

Uploading packages to Amazon S3

Before you can associate a package with your domain, you must upload it to an Amazon S3 bucket. For instructions, see Uploading S3 Objects in the Amazon Simple Storage Service Getting Started Guide.

If your package contains sensitive information, specify server-side encryption with S3-managed keys when you upload it. Amazon ES can't access files on S3 that you protect using an AWS KMS master key.

After you upload the file, make note of its S3 path. The path format is s3://bucket-name/file-path/file-name.

You can use the following synonyms file for testing purposes. Save it as synonyms.txt.

danish, croissant, pastry
ice cream, gelato, frozen custard
sneaker, tennis shoe, running shoe
basketball shoe, hightop

Certain dictionaries, such as Hunspell dictionaries, use multiple files and require their own directories on the file system. At this time, Amazon ES only supports single-file dictionaries.

Importing and associating packages

The console is the simplest way to import a package into Amazon ES and associate the package with a domain. When you import a package from Amazon S3, Amazon ES stores its own copy of the package and automatically encrypts that copy using AES-256 with Amazon ES-managed keys.
To import and associate a package with a domain (console)

1. In the Amazon Elasticsearch Service console, choose Packages.
2. Choose Import.
3. Give the package a descriptive name.
4. Provide the S3 path to the file, and then choose Import.
5. Return to the Packages screen.
6. When the package status is Available, select it. Then choose Associate to a domain.
7. Choose a domain, and then choose Associate.
8. In the navigation pane, choose your domain, and then choose the Packages tab.
9. When the package status is Available, note its ID. Use analyzers/id as the file path in requests to Elasticsearch (p. 179).

Alternately, use the AWS CLI, SDKs, or configuration API to import and associate packages. For more information, see the AWS CLI Command Reference and Configuration API reference (p. 339).

Using custom packages with Elasticsearch

After you associate a file with a domain, you can use it in parameters such as synonyms_path, stopwords_path, and user_dictionary when you create tokenizers and token filters. The exact parameter varies by object. Several objects support synonyms_path and stopwords_path, but user_dictionary is exclusive to the kuromoji plugin. The following example adds a synonyms file to a new index:

```json
PUT my-index
{
  "settings": {
    "index": {
      "analysis": {
        "analyzer": {
          "my_analyzer": {
            "type": "custom",
            "tokenizer": "standard",
            "filter": ["my_filter"]
          }
        },
        "filter": {
          "my_filter": {
            "type": "synonym",
            "synonyms_path": "analyzers/F11111111",
            "updateable": true
          }
        }
      }
    }
  },
  "mappings": {
    "properties": {
      "description": {
        "type": "text",
        "analyzer": "standard",
        "search_analyzer": "my_analyzer"
      }
    }
  }
}
```
This request creates a custom analyzer for the index that uses the standard tokenizer and a synonym token filter.

- Tokenizers break streams of characters into tokens (typically words) based on some set of rules. The simplest example is the whitespace tokenizer, which breaks the preceding characters into a token each time it encounters a whitespace character. A more complex example is the standard tokenizer, which uses a set of grammar-based rules to work across many languages.

- Token filters add, modify, or delete tokens. For example, a synonym token filter adds tokens when it finds a word in the synonyms list. The stop token filter removes tokens when it finds a word in the stop words list.

This request also adds a text field (description) to the mapping and tells Elasticsearch to use the new analyzer as its search analyzer. You can see that it still uses the standard analyzer as its index analyzer.

Finally, note the line "updateable": true in the token filter. This field only applies to search analyzers, not index analyzers, and is critical if you later want to update the search analyzer (p. 181) automatically.

For testing purposes, add some documents to the index:

```
POST _bulk
{
  "index": { "_index": "my-index", "_id": "1" }
  { "description": "ice cream" }
  { "index": { "_index": "my-index", "_id": "2" }
  { "description": "croissant" }
  { "index": { "_index": "my-index", "_id": "3" }
  { "description": "tennis shoe" }
  { "index": { "_index": "my-index", "_id": "4" }
  { "description": "hightop" }
}
```

Then search them using a synonym:

```
GET my-index/_search
{
  "query": {
    "match": {
      "description": "gelato"
    }
  }
}
```

In this case, Elasticsearch returns the following response:

```
{
  "hits": {
    "total": { "value": 1, "relation": "eq" },
    "max_score": 0.99463606,
    "hits": [{
      "_index": "my-index",
      "_type": "_doc",
      "_id": "1",
      "_score": 0.99463606,
      "_source": {
        "description": "ice cream"
      }
    }]
  }
}
```
Tip
Dictionary files use Java heap space proportional to their size. For example, a 2 GiB dictionary file might consume 2 GiB of heap space on a node. If you use large files, ensure that your nodes have enough heap space to accommodate them. Monitor (p. 30) the JVMMemoryPressure metric, and scale your cluster as necessary.

Updating custom packages

Uploading a new version of a package to Amazon S3 does not automatically update the package on Amazon Elasticsearch Service. Amazon ES stores its own copy of the file, so if you upload a new version to S3, you must manually update it.

Each of your associated domains stores its own copy of the file, as well. To keep search behavior predictable, domains continue to use their current package version until you explicitly update them.

To update a package (console)

1. In the Amazon Elasticsearch Service console, choose Packages.
2. Choose a package and Update package.
3. Provide the S3 path to the file, and then choose Update package.
4. Return to the Packages screen.
5. When the package status changes to Available, select it. Then choose one or more associated domains, Apply update, and confirm. Wait for the association status to change to Active.
6. The next steps vary depending on how you configured your indices:
   - If your domains runs Elasticsearch 7.8 or later and only uses search analyzers with the updateable (p. 179) field set to true, you don't need to take any further action. Amazon ES automatically updates your indices using the _opendistro/_refresh_search_analyzers API.
   - If your domain runs an earlier version of Elasticsearch, uses index analyzers, or doesn't use the updateable field, see the section called “Manual index updates” (p. 181).

Although the console is the simplest method, you can also use the AWS CLI, SDKs, or configuration API to update Amazon ES packages. For more information, see the AWS CLI Command Reference and Configuration API reference (p. 339).

Manual index updates

To use an updated package, you must manually update your indices if you meet any of the following conditions:

- Your domain runs Elasticsearch 7.7. or earlier.
- You use custom packages as index analyzers.
- You use custom packages as search analyzers, but don't include the updateable (p. 179) field.

To update analyzers with the new package files, you have two options:

- Close and open any indices that you want to update:

  POST my-index/_close
POST *my-index*/_open

- Reindex the indices. First, create an index that uses the updated synonyms file (or an entirely new file):

```json
PUT *my-new-index*
{
  "settings": {
    "analysis": {
      "analyzer": {
        "synonym_analyzer": {
          "type": "custom",
          "tokenizer": "standard",
          "filter": ["synonym_filter"]
        }
      },
      "filter": {
        "synonym_filter": {
          "type": "synonym",
          "synonyms_path": "analyzers/F222222222"
        }
      }
    }
  },
  "mappings": {
    "properties": {
      "description": {
        "type": "text",
        "analyzer": "synonym_analyzer"
      }
    }
  }
}
```

Then **reindex** the old index to that new index:

```json
POST _reindex
{
  "source": {
    "index": "my-index"
  },
  "dest": {
    "index": "my-new-index"
  }
}
```

If you frequently update index analyzers, use **index aliases** to maintain a consistent path to the latest index:

```json
POST _aliases
{
  "actions": [
    { "remove": { "index": "my-index", "alias": "latest-index" } },
    { "add": { "index": "my-new-index", ...
```
Dissociating and removing packages

Dissociating a package from a domain means that you can no longer use that file when you create new indices. Any indices that already use the file can continue using it.

The console is the simplest way to dissociate a package from a domain and remove it from Amazon ES. Removing a package from Amazon ES does not remove it from its original location on Amazon S3.

To dissociate a package from a domain and remove it from Amazon ES (console)

1. Go to https://aws.amazon.com, and then choose Sign In to the Console.
2. Under Analytics, choose Elasticsearch Service.
3. In the navigation pane, choose your domain, and then choose the Packages tab.
4. Choose a package, Actions, and then choose Dissociate. Confirm your choice.
5. Wait for the package to disappear from the list. You might need to refresh your browser.
6. If you want to use the package with other domains, stop here. To continue with removing the package, choose Packages in the navigation pane.
7. Select the package and choose Delete.

Alternately, use the AWS CLI, SDKs, or configuration API to dissociate and remove packages. For more information, see the AWS CLI Command Reference and Configuration API reference (p. 339).

Querying your Amazon Elasticsearch Service data with SQL

You can use SQL to query your Amazon Elasticsearch Service (Amazon ES), rather than using the JSON-based Elasticsearch query DSL. Querying with SQL is useful if you’re already familiar with the language or want to integrate your domain with an application that uses it.

Use the following table to find the version of the SQL plugin that’s supported by each Elasticsearch version. Each SQL plugin version corresponds to an Open Distro for Elasticsearch version.

<table>
<thead>
<tr>
<th>Elasticsearch version</th>
<th>SQL plugin version</th>
<th>Notable features</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1</td>
<td>1.1.0</td>
<td></td>
</tr>
<tr>
<td>7.3</td>
<td>1.3.0</td>
<td>CAST function, multiple string and number operators</td>
</tr>
<tr>
<td>7.4</td>
<td>1.4.0</td>
<td>Add additional date/time functions, support IF, IFNULL, and ISNULL functions</td>
</tr>
</tbody>
</table>
### Sample call

To query your data with SQL, send HTTP requests to `_opendistro/_sql` using the following format:

```json
POST elasticsearch_domain/_opendistro/_sql
{
  "query": "SELECT * FROM my-index LIMIT 50"
}
```

### Notes and differences

Calls to `_opendistro/_sql` include index names in the request body, so they have the same access policy considerations (p. 88) as the bulk, mget, and msearch operations. As always, follow the principle of least privilege when you grant permissions to API operations.

For security considerations related to using SQL with fine-grained access control, see Fine-Grained Access Control in Amazon Elasticsearch Service (p. 105).

The Open Distro for Elasticsearch SQL plugin includes many tuneable settings, but on Amazon ES, use the `_opendistro/_sql/settings` path rather than the standard `_cluster/settings` path:

```json
PUT _opendistro/_sql/settings
{
  "persistent": {
    "opendistro.sql.cursor.enabled": true
  }
}
```

### SQL Workbench

The SQL Workbench is a Kibana user interface that lets you run on-demand SQL queries, translate SQL into its REST equivalent, and view and save results as text, JSON, JDBC, or CSV. For more information, see Workbench.

### SQL CLI

The SQL CLI is a standalone Python application that you can launch with the `odfesql` command. For steps to install, configure, and use, see SQL CLI.
JDBC driver

The Java Database Connectivity (JDBC) driver lets you integrate Amazon ES domains with your favorite business intelligence (BI) applications. To get started, see the GitHub repository. The following table summarizes version compatibility for the driver.

<table>
<thead>
<tr>
<th>Elasticsearch Version</th>
<th>JDBC Driver Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.10</td>
<td>1.13.0</td>
</tr>
<tr>
<td>7.9</td>
<td>1.11.0</td>
</tr>
<tr>
<td>7.8</td>
<td>1.9.0</td>
</tr>
<tr>
<td>7.7</td>
<td>1.8.0</td>
</tr>
<tr>
<td>7.4</td>
<td>1.4.0</td>
</tr>
<tr>
<td>7.1</td>
<td>1.0.0</td>
</tr>
<tr>
<td>6.8</td>
<td>0.9.0</td>
</tr>
<tr>
<td>6.7</td>
<td>0.9.0</td>
</tr>
<tr>
<td>6.5</td>
<td>0.9.0</td>
</tr>
</tbody>
</table>

ODBC driver

The Open Database Connectivity (ODBC) driver is a read-only ODBC driver for Windows and macOS that lets you connect business intelligence and data visualization applications like Tableau, Microsoft Excel, and Power BI to the SQL plugin. For information on downloading and using the JAR file, see the SQL repository on GitHub.

Querying Amazon Elasticsearch Service data using Piped Processing Language

Piped Processing Language (PPL) is a query language that lets you use pipe (|) syntax to query data stored in Amazon Elasticsearch Service (Amazon ES).

The PPL syntax consists of commands delimited by a pipe character (|) where data flows from left to right through each pipeline. For example, the PPL syntax to find the number of hosts with HTTP 403 or 503 errors, aggregate them per host, and sort them in the order of impact is as follows:

```plaintext
source = kibana_sample_data_logs | 
where response='403' or response='503' | 
stats count(request) as request_count by host, response | 
sort -request_count
```

PPL requires Elasticsearch 7.9 or later. Full documentation for the feature, including detailed steps and command descriptions, is available in the Open Distro for Elasticsearch documentation.

To get started, choose Query Workbench in Kibana and select PPL. Use the bulk operation to index some sample data:
The following example returns firstname and lastname fields for documents in an accounts index with age greater than 18:

```
search source=accounts | where age > 18 | fields firstname, lastname
```

<table>
<thead>
<tr>
<th>id</th>
<th>firstname</th>
<th>lastname</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Amber</td>
<td>Duke</td>
</tr>
<tr>
<td>1</td>
<td>Hattie</td>
<td>Bond</td>
</tr>
<tr>
<td>2</td>
<td>Nanette</td>
<td>Bates</td>
</tr>
<tr>
<td>3</td>
<td>Dale</td>
<td>Adams</td>
</tr>
</tbody>
</table>

You can use a complete set of read-only commands like search, where, fields, rename, dedup, stats, sort, eval, head, top, and rare. For descriptions and examples of each command, see Commands.

The PPL plugin supports all SQL functions, including mathematical, trigonometric, date-time, string, aggregate, and advanced operators and expressions. To learn more, see SQL Functions.

### k-Nearest Neighbor (k-NN) search in Amazon Elasticsearch Service

Short for its associated k-nearest neighbors algorithm, k-NN for Amazon Elasticsearch Service (Amazon ES) lets you search for points in a vector space and find the "nearest neighbors" for those points by Euclidean distance or cosine similarity. Use cases include recommendations (for example, an "other songs you might like" feature in a music application), image recognition, and fraud detection.

Use the following table to find the version of the k-NN plugin running on your Amazon Elasticsearch Service domain. Each k-NN plugin version corresponds to an Open Distro for Elasticsearch version.
Getting started with k-NN

To use k-NN, you must create an index with the `index.knn` setting and add one or more fields of the `knn_vector` data type.

```
PUT my-index
{
  "settings": {
    "index.knn": true
  },
  "mappings": {
    "properties": {
      "my_vector1": {
        "type": "knn_vector",
        "dimension": 2
      },
      "my_vector2": {
        "type": "knn_vector",
        "dimension": 4
      }
    }
  }
}
```

The `knn_vector` data type supports a single list of up to 10,000 floats, with the number of floats defined by the required `dimension` parameter. After you create the index, add some data to it.

```
POST _bulk
{
  "index": {
    "_index": "my-index", "_id": "1" }
  "my_vector1": [1.5, 2.5], "price": 12.2 }
  "index": {
    "_index": "my-index", "_id": "2" }
  "my_vector1": [2.5, 3.5], "price": 7.1 }
  "index": {
    "_index": "my-index", "_id": "3" }
  "my_vector1": [3.5, 4.5], "price": 12.9 }
  "index": {
    "_index": "my-index", "_id": "4" }
  "my_vector1": [5.5, 6.5], "price": 1.2 }
  "index": {
    "_index": "my-index", "_id": "5" }
  "my_vector1": [4.5, 5.5], "price": 3.7 }
  "index": {
    "_index": "my-index", "_id": "6" }
  "my_vector2": [1.5, 5.5, 4.5, 6.4], "price": 10.3 }
  "index": {
    "_index": "my-index", "_id": "7" }
  "my_vector2": [2.5, 3.5, 5.6, 6.7], "price": 5.5 }
```
Then you can search the data using the \texttt{knn} query type.

\begin{verbatim}
GET my-index/_search
{
  "size": 2,
  "query": {
    "knn": {
      "my_vector2": {
        "vector": [2, 3, 5, 6],
        "k": 2
      }
    }
  }
}
\end{verbatim}

In this case, $k$ is the number of neighbors you want the query to return, but you must also include the \texttt{size} option. Otherwise, you get $k$ results for each shard (and each segment) rather than $k$ results for the entire query. k-NN supports a maximum $k$ value of 10,000.

If you mix the \texttt{knn} query with other clauses, you might receive fewer than $k$ results. In this example, the \texttt{post_filter} clause reduces the number of results from 2 to 1.

\begin{verbatim}
GET my-index/_search
{
  "size": 2,
  "query": {
    "knn": {
      "my_vector2": {
        "vector": [2, 3, 5, 6],
        "k": 2
      }
    }
  },
  "post_filter": {
    "range": {
      "price": {
        "gte": 6,
        "lte": 10
      }
    }
  }
}
\end{verbatim}

\section*{k-NN differences and tuning}

Open Distro for Elasticsearch lets you modify all k-NN settings using the \texttt{_cluster/settings} API. On Amazon ES, you can change all settings except \texttt{knn.memory.circuit_breaker.enabled} and \texttt{knn.circuit_breaker.triggered}. k-NN statistics are included as Amazon CloudWatch metrics (p. 28).

In particular, check the \texttt{KNNGraphMemoryUsage} metric on each data node against the \texttt{knn.memory.circuit_breaker.limit} statistic and the available RAM for the instance type. Amazon ES uses half of an instance's RAM for the Java heap (up to a heap size of 32 GiB). By default, k-NN uses up to 50\% of the remaining half, so an instance type with 32 GiB of RAM can accommodate 8 GiB of graphs (32 * 0.5 * 0.5). Performance can suffer if graph memory usage exceeds this value.
Cross-cluster search for Amazon Elasticsearch Service

Cross-cluster search in Amazon Elasticsearch Service (Amazon ES) lets you perform queries and aggregations across multiple connected domains. It often makes more sense to use multiple smaller domains instead of a single large domain, especially when you're running different types of workloads.

Workload-specific domains enable you to perform the following tasks:

- Optimize each domain by choosing instance types for specific workloads.
- Establish fault-isolation boundaries across workloads. This means that if one of your workloads fails, the fault is contained within that specific domain and doesn't impact your other workloads.
- Scale more easily across domains.

Cross-cluster search supports Kibana, so you can create visualizations and dashboards across all your domains.

Topics

- Limitations (p. 189)
- Cross-cluster search prerequisites (p. 189)
- Cross-cluster search pricing (p. 190)
- Setting up a connection (p. 190)
- Removing a connection (p. 191)
- Setting up security and sample walkthrough (p. 191)
- Kibana (p. 195)

Limitations

Cross-cluster search has several important limitations:

- You can only implement cross-cluster search on domains created on or after June 3rd, 2020.
- You can't connect to self-managed Elasticsearch clusters.
- You can't connect to domains in different AWS Regions.
- A domain can have a maximum of 20 outgoing connections. Similarly, a domain can have a maximum of 20 incoming connections. In other words, one domain can connect to a maximum of 20 other domains.
- Domains must either share the same major version, or be on the final minor version and the next major version (for example, 6.8 and 7.x are compatible).
- You can't use custom dictionaries or SQL with cross-cluster search.
- You can't use AWS CloudFormation to connect domains.
- You can't use cross-cluster search on M3 and T2 instances.

Cross-cluster search prerequisites

Before you set up cross-cluster search, make sure that your domains meet the following requirements:

- Elasticsearch version 6.7 or later
- Fine-grained access control enabled
• Node-to-node encryption enabled

**Cross-cluster search pricing**

There is no additional charge for searching across domains.

**Setting up a connection**

The "source" domain refers to the domain that a cross-cluster search request originates from. In other words, the source domain is the one that you send the initial search request to.

The "destination" domain is the domain that the source domain queries.

A cross-cluster connection is unidirectional from the source to the destination domain. This means that the destination domain can’t query the source domain. However, you can set up another connection in the opposite direction.

1. On your domain dashboard, choose a domain, and choose the **Cross-cluster search connections** tab.
2. In the **Outbound cluster connections** section, choose **Connect**.
3. On the **Connect clusters** page, in **Connection alias**, enter a name for your connection.
4. Choose between connecting a domain in your AWS account or in another account.
   - To connect to a domain in your AWS account, from the dropdown list, choose the domain that you want to connect to and choose **Submit**.
   - To connect to a domain in another AWS account, specify the ARN of the remote domain and choose **Submit**.
5. Cross-cluster search first validates the connection request to make sure that the prerequisites are met to ensure compatibility. If the domains are found to be incompatible, the connection request enters the “Validation failed” state.
6. After the connection request is validated successfully, it is sent to the destination domain, where it needs to be approved. Until this approval happens, the connection remains in a “Pending acceptance” state. When the connection request is accepted at the destination domain, the state changes to “Active” and the destination domain becomes available for queries.
   - The domain page shows you the overall domain health and instance health details of your destination domain. Only domain owners have the flexibility to create, view, remove, and monitor connections to or from their domains.

After the connection is established, any traffic that flows between the nodes of the connected domains is encrypted. If you connect a VPC domain to a non-VPC domain and the non-VPC domain is a public...
Removing a connection

Removing a connection stops any cross-cluster operation on its indices.

1. On your domain dashboard, choose the Cross-cluster search connections tab.
2. Select the domain connections that you want to remove and choose Remove.
3. To confirm deletion, choose Remove in the pop-up box.

You could perform these steps on either the source or destination domain to remove the connection. After the connection is removed, it's still visible with a "Deleted" status for a period of 15 days.

You can't delete a domain with active cross-cluster connections. To delete a domain, first remove all incoming and outgoing connections from that domain. This is to make sure you take into account the cross-cluster domain users before deleting the domain.

Setting up security and sample walkthrough

1. You send a cross-cluster search request to the source domain.
2. The source domain evaluates that request against its domain access policy. Because cross-cluster search requires fine-grained access control, we recommend an open access policy on the source domain.

Note

The domain resource policy evaluates the URI literally, so if you include remote indices in the path, use arn:aws:es:us-east-1:123456789012:domain/my-domain/local_index,dst%3Aremote_index rather than arn:aws:es:us-east-1:123456789012:domain/my-domain/local_index,dst:remote_index.

If you choose to use a restrictive access policy in addition to fine-grained access control, your policy must allow access to es:ESHttpGet at a minimum.

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "AWS": ["*"]
         },
         "Action": ["es:ESHttp*"],
      }
   ]
}
```

Note

The domain resource policy evaluates the URI literally, so if you include remote indices in the path, use arn:aws:es:us-east-1:123456789012:domain/my-domain/local_index,dst%3Aremote_index rather than arn:aws:es:us-east-1:123456789012:domain/my-domain/local_index,dst:remote_index.

If you choose to use a restrictive access policy in addition to fine-grained access control, your policy must allow access to es:ESHttpGet at a minimum.

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "AWS": ["*"]
         },
         "Action": ["es:ESHttpGet"],
      }
   ]
}
```
3. **Fine-grained access control (p. 90)** on the source domain evaluates the request:
   - Is the request signed with valid IAM or HTTP basic credentials?
   - If so, does the user have permission to perform the search and access the data?

If the request only searches data on the destination domain (for example, dest-alias:dest-index/_search), you only need permissions on the destination domain.

If the request searches data on both domains (for example, source-index,dest-alias:dest-index/_search), you need permissions on both domains.

In fine-grained access control, users must have the `indices:admin/shards/search_shards` permission in addition to standard read or search permissions for the relevant indices.

4. The source domain passes the request to the destination domain. The destination domain evaluates this request against its domain access policy. You must include the `es:ESCrossClusterGet` permission on the destination domain:

   ```json
   {  
   "Version": "2012-10-17",
   "Statement": [  
   {  
   "Effect": "Allow",
   "Principal": {  
   "AWS": "*"
   },
   "Action": "es:ESCrossClusterGet",
   }  
   ]  
   }
   ```

Make sure that the `es:ESCrossClusterGet` permission is applied for `/dst-domain` and not `/dst-domain/*`.

However, this minimum policy only allows cross-cluster searches. To perform other operations, such as indexing documents and performing standard searches, you need additional permissions. We recommend the following policy on the destination domain:

```json
{  
   "Version": "2012-10-17",
   "Statement": [  
   {  
   "Effect": "Allow",
   "Principal": {  
   "AWS": [  
   "*"
   ]
   },
   "Action": [  
   API Version 2015-01-01
192
```
"es:ESHttp**
],
},
{
"Effect": "Allow",
"Principal": {
"AWS": "*"
},
"Action": "es:ESCrossClusterGet",
}
]}

**Note**
All cross-cluster search requests between domains are encrypted in transit by default as part of node-to-node encryption.

5. The destination domain performs the search and returns the results to the source domain.
6. The source domain combines its own results (if any) with the results from the destination domain and returns them to you.
7. We recommend Postman for testing requests:
   - On the destination domain, index a document:

```plaintext
POST https://dst-domain.us-east-1.es.amazonaws.com/books/_doc/1
{
  "Dracula": "Bram Stoker"
}
```

   - To query this index from the source domain, include the connection alias of the destination domain within the query:

```plaintext
GET https://src-domain.us-east-1.es.amazonaws.com/<connection_alias>:books/_search
{
  ...
  "hits": [
   {
      "_index": "source-destination:books",
      "_type": "_doc",
      "_id": "1",
      "_score": 1,
      "_source": {
        "Dracula": "Bram Stoker"
      }
   }
  ]
}
```

You can find the connection alias on the **Cross-cluster search connections** tab on your domain dashboard.

- If you set up a connection between domain-a -> domain-b with connection alias cluster_b and domain-a -> domain-c with connection alias cluster_c, search domain-a, domain-b, and domain-c as follows:

```plaintext
GET https://src-domain.us-east-1.es.amazonaws.com/local_index,cluster_b:b_index,cluster_c:c_index/_search
```
{
  "query": {
    "match": {
      "user": "domino"
    }
  }
}

Response

{
  "took": 150,
  "timed_out": false,
  "_shards": {
    "total": 3,
    "successful": 3,
    "failed": 0,
    "skipped": 0
  },
  "_clusters": {
    "total": 3,
    "successful": 3,
    "skipped": 0
  },
  "hits": {
    "total": 3,
    "max_score": 1,
    "hits": [
      {
        "_index": "local_index",
        "_type": "_doc",
        "_id": "0",
        "_score": 1,
        "_source": {
          "user": "domino",
          "message": "Lets unite the new mutants",
          "likes": 0
        }
      },
      {
        "_index": "cluster_b:b_index",
        "_type": "_doc",
        "_id": "0",
        "_score": 2,
        "_source": {
          "user": "domino",
          "message": "I'm different",
          "likes": 0
        }
      },
      {
        "_index": "cluster_c:c_index",
        "_type": "_doc",
        "_id": "0",
        "_score": 3,
        "_source": {
          "user": "domino",
          "message": "So am I",
          "likes": 0
        }
      }
    ]
  }
}
All destination clusters that you search need to be available for your search request to run successfully. Otherwise, the whole request fails—even if one of the domains is not available, no search results are returned.

**Kibana**

You can visualize data from multiple connected domains in the same way as from a single domain, except that you must access the remote indices using `connection-alias:index`. So, your index pattern must match `connection-alias:index`.

**Learning to Rank for Amazon Elasticsearch Service**

Elasticsearch uses a probabilistic ranking framework called BM-25 to calculate relevance scores. If a distinctive keyword appears more frequently in a document, BM-25 assigns a higher relevance score to that document. This framework, however, doesn't take into account user behavior like click-through data, which can further improve relevance.

Learning to Rank is an open-source Elasticsearch plugin that lets you use machine learning and behavioral data to tune the relevance of documents. The plugin uses models from the XGBoost and Ranklib libraries to rescore the search results.

Learning to Rank requires Elasticsearch 7.7 or later. Full documentation for the feature, including detailed steps and API descriptions, is available in the Learning to Rank documentation.

**Note**

To use the Learning to Rank plugin, you must have full admin permissions. To learn more, see the section called “Modifying the master user” (p. 106).

**Topics**

- Getting started with Learning to Rank (p. 195)
- Learning to Rank API (p. 208)

**Getting started with Learning to Rank**

You need to provide a judgment list, prepare a training dataset, and train the model outside of Amazon Elasticsearch Service (Amazon ES). The parts in blue occur outside of Amazon ES:
Step 1: Initialize the plugin

To initialize the Learning to Rank plugin, send the following request to your Amazon Elasticsearch Service domain:

```json
PUT _ltr
{
  "acknowledged" : true,
  "shards_acknowledged" : true,
  "index" : ".ltrstore"
}
```

This command creates a hidden .ltrstore index that stores metadata information such as feature sets and models.

Step 2: Create a judgment list

**Note**
You must perform this step outside of Amazon Elasticsearch Service.

A judgment list is a collection of examples that a machine learning model learns from. Your judgment list should include keywords that are important to you and a set of graded documents for each keyword.

In this example, we have a judgment list for a movie dataset. A grade of 4 indicates a perfect match. A grade of 0 indicates the worst match.

<table>
<thead>
<tr>
<th>Grade</th>
<th>Keyword</th>
<th>Doc ID</th>
<th>Movie Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>rambo</td>
<td>7555</td>
<td>Rambo</td>
</tr>
<tr>
<td>3</td>
<td>rambo</td>
<td>1370</td>
<td>Rambo III</td>
</tr>
<tr>
<td>3</td>
<td>rambo</td>
<td>1369</td>
<td>Rambo: First Blood Part II</td>
</tr>
<tr>
<td>3</td>
<td>rambo</td>
<td>1368</td>
<td>First Blood</td>
</tr>
</tbody>
</table>

Prepare your judgment list in the following format:

```
4 qid:1 # 7555 Rambo
3 qid:1 # 1370 Rambo III
3 qid:1 # 1369 Rambo: First Blood Part II
3 qid:1 # 1368 First Blood
```

where qid:1 represents "rambo"

For a more complete example of a judgment list, see [movie judgments](#).

You can create this judgment list manually with the help of human annotators or infer it programmatically from analytics data.

Step 3: Build a feature set

A feature is a field that corresponds to the relevance of a document—for example, title, overview, popularity score (number of views), and so on.
Build a feature set with a Mustache template for each feature. For more information about features, see Working with Features.

In this example, we build a movie_features feature set with the title and overview fields:

```json
POST _ltr/_featureset/movie_features
{
  "featureset": {
    "name": "movie_features",
    "features": [
      {
        "name": "1",
        "params": ["keywords"],
        "template_language": "mustache",
        "template": {
          "match": {
            "title": "{{keywords}}"
          }
        }
      },
      {
        "name": "2",
        "params": ["keywords"],
        "template_language": "mustache",
        "template": {
          "match": {
            "overview": "{{keywords}}"
          }
        }
      }
    ]
  }
}
```

If you query the original .ltrstore index, you get back your feature set:

```sh
GET _ltr/_featureset
```

**Step 4: Log the feature values**

The feature values are the relevance scores calculated by BM-25 for each feature.

Combine the feature set and judgment list to log the feature values. For more information about logging features, see Logging Feature Scores.

In this example, the bool query retrieves the graded documents with the filter, and then selects the feature set with the sltr query. The ltr_log query combines the documents and the features to log the corresponding feature values:

```json
POST tmdb/_search
{
  "_source": {
    "includes": [
      "title",
      "overview"
    ]
  },
  "query": {
```
A sample response might look like the following:

```
{
  "took" : 7,
  "timed_out" : false,
  "shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 4,
      "relation" : "eq"
    },
    "max_score" : 0.0,
    "hits" : [
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1368",
        "_score" : 0.0,
        "_source" : {
          "overview" : "When former Green Beret John Rambo is harassed by local law enforcement and arrested for vagrancy, the Vietnam vet snaps, runs for the hills and rat-a-tat-tats his way into the action-movie hall of fame. Hounded by a relentless sheriff, Rambo employs heavy-handed guerilla tactics to shake the cops off his tail.",
          "title" : "First Blood"
        }
      },
      "fields" : {
```
"_ltrlog" : [
    {
      "log_entry1" : [ 
        {
          "name" : "1"
        },
        {
          "name" : "2",
          "value" : 10.558305
        }
      ]
    },
    "matched_queries" : [ 
      "logged_featureset"
    ],
    {
      "_index" : "tmdb",
      "_type" : "movie",
      "_id" : "7555",
      "_score" : 0.0,
      "_source" : {
        "overview" : "When governments fail to act on behalf of captive missionaries, ex-Green Beret John James Rambo sets aside his peaceful existence along the Salween River in a war-torn region of Thailand to take action. Although he's still haunted by violent memories of his time as a U.S. soldier during the Vietnam War, Rambo can hardly turn his back on the aid workers who so desperately need his help.",
        "title" : "Rambo"
      },
      "fields" : {
        "_ltrlog" : [
          {
            "log_entry1" : [ 
              {
                "name" : "1",
                "value" : 11.2569065
              },
              {
                "name" : "2",
                "value" : 9.936821
              }
            ]
          },
          "matched_queries" : [ 
            "logged_featureset"
          ],
          {
            "_index" : "tmdb",
            "_type" : "movie",
            "_id" : "1369",
            "_score" : 0.0,
            "_source" : {
              "overview" : "Col. Troutman recruits ex-Green Beret John Rambo for a highly secret and dangerous mission. Teamed with Co Bao, Rambo goes deep into Vietnam to rescue POWs. Deserted by his own team, he's left in a hostile jungle to fight for his life, avenge the death of a woman and bring corrupt officials to justice.",
              "title" : "Rambo: First Blood Part II"
            },
            "fields" : {
              "_ltrlog" : [
                
      API Version 2015-01-01
      199
"log_entry1" : [
    {
        "name" : "1",
        "value" : 6.334839
    },
    {
        "name" : "2",
        "value" : 10.558305
    }
],
"matched_queries" : [
    "logged_featureset"
],
{  
    "_index" : "tmdb",
    "_type" : "movie",
    "_id" : "1370",
    "_score" : 0.0,
    "_source" : {
        "overview" : "Combat has taken its toll on Rambo, but he's finally begun to find inner peace in a monastery. When Rambo's friend and mentor Col. Trautman asks for his help on a top secret mission to Afghanistan, Rambo declines but must reconsider when Trautman is captured.",
        "title" : "Rambo III"
    },
    "fields" : {
        "_ltrlog" : [
            {
                "log_entry1" : [  
                    {
                        "name" : "1",
                        "value" : 9.425955
                    },
                    {
                        "name" : "2",
                        "value" : 11.262714
                    }
            ]
        },
        "matched_queries" : [  
            "logged_featureset"
        ]
    }
}

In the previous example, the first feature doesn't have a feature value because the keyword "rambo" doesn't appear in the title field of the document with an ID equal to 1368. This is a missing feature value in the training data.

**Step 5: Create a training dataset**

**Note**

You must perform this step outside of Amazon Elasticsearch Service.

The next step is to combine the judgment list and feature values to create a training dataset. If your original judgment list looks like this:

```
API Version 2015-01-01
200
```
Convert it into the final training dataset, which looks like this:

4 qid:1 # 7555 Rambo
3 qid:1 # 1370 Rambo III
3 qid:1 # 1369 Rambo: First Blood Part II
3 qid:1 # 1368 First Blood

You can perform this step manually or write a program to automate it.

**Step 6: Choose an algorithm and build the model**

Note
You must perform this step outside of Amazon Elasticsearch Service.

With the training dataset in place, the next step is to use XGBoost or Ranklib libraries to build a model. XGBoost and Ranklib libraries let you build popular models such as LambdaMART, Random Forests, and so on.

For steps to use XGBoost and Ranklib to build the model, see the XGBoost and RankLib documentation, respectively. To use Amazon SageMaker to build the XGBoost model, see XGBoost Algorithm.

**Step 7: Deploy the model**

After you have built the model, deploy it into the Learning to Rank plugin. For more information about deploying a model, see Uploading A Trained Model.

In this example, we build a `my_ranklib_model` model using the Ranklib library:

```
```
To see the model, send the following request:

```
GET _ltr/_model/my_ranklib_model
```

**Step 8: Search with learning to rank**

After you deploy the model, you’re ready to search.
Perform the `sltr` query with the features that you're using and the name of the model that you want to execute:

```json
POST tmdb/_search
{
    "source": {
        "includes": ["title", "overview"]
    },
    "query": {
        "multi_match": {
            "query": "rambo",
            "fields": ["title", "overview"]
        }
    },
    "rescore": {
        "query": {
            "rescore_query": {
                "sltr": {
                    "params": {
                        "keywords": "rambo"
                    },
                    "model": "my_ranklib_model"
                }
            }
        }
    }
}
```

With Learning to Rank, you see “Rambo” as the first result because we have assigned it the highest grade in the judgment list:

```json
{
    "took" : 12,
    "timed_out" : false,
    "_shards" : {
        "total" : 1,
        "successful" : 1,
        "skipped" : 0,
        "failed" : 0
    },
    "hits" : {
        "total" : {
            "value" : 7,
            "relation" : "eq"
        },
        "max_score" : 13.096414,
        "hits" : [
            {
                "_index" : "tmdb",
                "_type" : "movie",
                "_id" : "7555",
                "_score" : 13.096414,
                "_source" : {
                    "overview" : "When governments fail to act on behalf of captive missionaries, ex-Green Beret John James Rambo sets aside his peaceful existence along the Salween River in a war-torn region of Thailand to take action. Although he's still haunted by violent memories of his time as a U.S. soldier during the Vietnam War, Rambo can hardly turn his back on the aid workers who so desperately need his help.",
                    "title" : "Rambo"
                }
            },
            {
                "_index" : "tmdb",
                "_type" : "movie",
```
"_id" : "1370",
"_score" : 11.17245,
"_source" : {
  "overview" : "Combat has taken its toll on Rambo, but he's finally begun to find inner peace in a monastery. When Rambo's friend and mentor Col. Trautman asks for his help on a top secret mission to Afghanistan, Rambo declines but must reconsider when Trautman is captured.",
  "title" : "Rambo III"
}
},
{
  "_id" : "1368",
  "_score" : 10.442155,
  "_source" : {
    "overview" : "When former Green Beret John Rambo is harassed by local law enforcement and arrested for vagrancy, the Vietnam vet snaps, runs for the hills and rat-a-tat-tats his way into the action-movie hall of fame. Hounded by a relentless sheriff, Rambo employs heavy-handed guerilla tactics to shake the cops off his tail.",
    "title" : "First Blood"
  }
},
{
  "_id" : "1369",
  "_score" : 10.442155,
  "_source" : {
    "overview" : "Col. Troutman recruits ex-Green Beret John Rambo for a highly secret and dangerous mission. Teamed with Co Bao, Rambo goes deep into Vietnam to rescue POWs. Deserted by his own team, he's left in a hostile jungle to fight for his life, avenge the death of a woman and bring corrupt officials to justice.",
    "title" : "Rambo: First Blood Part II"
  }
},
{
  "_id" : "31362",
  "_score" : 7.424202,
  "_source" : {
    "overview" : "It is 1985, and a small, tranquil Florida town is being rocked by a wave of vicious serial murders and bank robberies. Particularly sickening to the authorities is the gratuitous use of violence by two "Rambo" like killers who dress themselves in military garb. Based on actual events taken from FBI files, the movie depicts the Bureau's efforts to track down these renegades.",
    "title" : "In the Line of Duty: The F.B.I. Murders"
  }
},
{
  "_id" : "13258",
  "_score" : 6.43182,
  "_source" : {
    "overview" : "Will Proudfoot (Bill Milner) is looking for an escape from his family's stifling home life when he encounters Lee Carter (Will Poulter), the school bully. Armed with a video camera and a copy of "Rambo: First Blood", Lee plans to make cinematic history by filming his own action-packed video epic. Together, these two newfound friends—turned-budding-filmmakers quickly discover that their imaginative # and sometimes mishap-filled # cinematic adventure has begun to take on a life of its own!"
    "title" : "Son of Rambow"
  }
}
"_index" : "tmdb",
"_type" : "movie",
"_id" : "61410",
"_score" : 3.9719706,
"_source" : {
  "overview" : "It's South Africa 1990. Two major events are about to happen: The release of Nelson Mandela and, more importantly, it's Spud Milton's first year at an elite boys only private boarding school. John Milton is a boy from an ordinary background who wins a scholarship to a private school in KwaZulu-Natal, South Africa. Surrounded by boys with nicknames like Gecko, Rambo, Rain Man and Mad Dog, Spud has his hands full trying to adapt to his new home. Along the way Spud takes his first tentative steps along the path to manhood. (The path it seems could be a rather long road). Spud is an only child. He is cursed with parents from well beyond the lunatic fringe and a senile granny. His dad is a fervent anti-communist who is paranoid that the family domestic worker is running a shebeen from her room at the back of the family home. His mom is a free spirit and a teenager's worst nightmare, whether it's shopping for Spud's underwear in the local supermarket",
  "title" : "Spud"
}
}
]

If you search without using the Learning to Rank plugin, Elasticsearch returns different results:

POST tmdb/_search
{
  "source": {
    "includes": ["title", "overview"]
  },
  "query": {
    "multi_match": {
      "query": "Rambo",
      "fields": ["title", "overview"]
    }
  }
}

{
  "took" : 5,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 5,
      "relation" : "eq"
    },
    "max_score" : 11.262714,
    "hits" : [
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1370",
        "_score" : 11.262714,
        "_source" : {
          "overview" : "Combat has taken its toll on Rambo, but he’s finally begun to find inner peace in a monastery. When Rambo’s friend and mentor Col. Trautman asks for his help
"
on a top secret mission to Afghanistan, Rambo declines but must reconsider when Trautman is captured.

"title": "Rambo III"

},
{
"_index": "tmdb",
"_type": "movie",
"_id": "1368",
"_score": 10.558305,
"_source": {
"overview": "When former Green Beret John Rambo is harassed by local law enforcement and arrested for vagrancy, the Vietnam vet snaps, runs for the hills and rat-a-tat-tats his way into the action-movie hall of fame. Hounded by a relentless sheriff, Rambo employs heavy-handed guerilla tactics to shake the cops off his tail.",
"title": "First Blood"
}
},
{
"_index": "tmdb",
"_type": "movie",
"_id": "1369",
"_score": 10.558305,
"_source": {
"overview": "Col. Troutman recruits ex-Green Beret John Rambo for a highly secret and dangerous mission. Teamed with Co Bao, Rambo goes deep into Vietnam to rescue POWs. Deserted by his own team, he's left in a hostile jungle to fight for his life, avenge the death of a woman and bring corrupt officials to justice.",
"title": "Rambo: First Blood Part II"
}
},
{
"_index": "tmdb",
"_type": "movie",
"_id": "13258",
"_score": 6.4600153,
"_source": {
"overview": "Will Proudfoot (Bill Milner) is looking for an escape from his family's stifling home life when he encounters Lee Carter (Will Poulter), the school bully. Armed with a video camera and a copy of "Rambo: First Blood", Lee plans to make cinematic history by filming his own action-packed video epic. Together, these two newfound friends—turned-budding-filmmakers quickly discover that their imaginative # and sometimes mishap-filled # cinematic adventure has begun to take on a life of its own!"
"title": "Son of Rambow"
}
]}
}
Based on how well you think the model is performing, adjust the judgment list and features. Then, repeat steps 2–8 to improve the ranking results over time.

**Learning to Rank API**

Use the Learning to Rank operations to programmatically work with feature sets and models.

**Create store**

Creates a hidden `.ltrstore` index that stores metadata information such as feature sets and models.

```
PUT _ltr
```

**Delete store**

Deletes the hidden `.ltrstore` index and resets the plugin.

```
DELETE _ltr
```

**Create feature set**

Creates a feature set.

```
POST _ltr/_featureset/<name_of_features>
```

**Delete feature set**

Deletes a feature set.

```
DELETE _ltr/_featureset/<name_of_feature_set>
```

**Get feature set**

Retrieves a feature set.

```
GET _ltr/_featureset/<name_of_feature_set>
```

**Create model**

Creates a model.

```
POST _ltr/_featureset/<name_of_feature_set>/_createmodel
```

**Delete model**

Deletes a model.

```
DELETE _ltr/_model/<name_of_model>
```
Get Model

Retrieves a model.

```
GET _ltr/_model/<name_of_model>
```

Get stats

Provides information about how the plugin is behaving.

```
GET _ltr/_model/<name_of_model>
```

You can also filter by node and/or cluster:

```
GET _opendistro/_ltr/nodeID,nodeID,/stats/stat,stat

{
   "_nodes" : {
      "total" : 1,
      "successful" : 1,
      "failed" : 0
   },
   "cluster_name" : "873043598401:ltr-77",
   "stores" : {
      ".ltrstore" : {
         "model_count" : 1,
         "featureset_count" : 1,
         "feature_count" : 2,
         "status" : "green"
      }
   }
   },
   "status" : "green",
   "nodes" : {
      "DjelK-_ZSfyzstO5dhGGQA" : {
         "cache" : {
            "feature" : {
               "eviction_count" : 0,
               "miss_count" : 0,
               "entry_count" : 0,
               "memory_usage_in_bytes" : 0,
               "hit_count" : 0
            },
            "featureset" : {
               "eviction_count" : 2,
               "miss_count" : 2,
               "entry_count" : 0,
               "memory_usage_in_bytes" : 0,
               "hit_count" : 0
            },
            "model" : {
               "eviction_count" : 2,
               "miss_count" : 3,
               "entry_count" : 1,
               "memory_usage_in_bytes" : 3204,
               "hit_count" : 1
            }
         },
      }
   },
   "request_total_count" : 6,
   "request_error_count" : 0
}
```
The statistics are provided at two levels, node and cluster, as specified in the following tables:

### Node-level stats

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>request_total_count</td>
<td>Total count of ranking requests.</td>
</tr>
<tr>
<td>request_error_count</td>
<td>Total count of unsuccessful requests.</td>
</tr>
<tr>
<td>cache</td>
<td>Statistics across all caches (features, featuresets, models). A cache hit occurs when a user queries the plugin and the model is already loaded into memory.</td>
</tr>
<tr>
<td>cache.eviction_count</td>
<td>Number of cache evictions.</td>
</tr>
<tr>
<td>cache.hit_count</td>
<td>Number of cache hits.</td>
</tr>
<tr>
<td>cache.miss_count</td>
<td>Number of cache misses. A cache miss occurs when a user queries the plugin and the model has not yet been loaded into memory.</td>
</tr>
<tr>
<td>cache.entry_count</td>
<td>Number of entries in the cache.</td>
</tr>
<tr>
<td>cache.memory_usage_in_bytes</td>
<td>Total memory used in bytes.</td>
</tr>
<tr>
<td>cache.cache_capacity_reached</td>
<td>Indicates if the cache limit is reached.</td>
</tr>
</tbody>
</table>

### Cluster-level stats

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>stores</td>
<td>Indicates where the feature sets and model metadata are stored. (The default is &quot;.ltrstore&quot;. Otherwise, it's prefixed with &quot;.ltrstore_&quot;, with a user supplied name).</td>
</tr>
<tr>
<td>stores.status</td>
<td>Status of the index.</td>
</tr>
<tr>
<td>stores.feature_sets</td>
<td>Number of feature sets.</td>
</tr>
<tr>
<td>stores.features_count</td>
<td>Number of features.</td>
</tr>
<tr>
<td>stores.model_count</td>
<td>Number of models.</td>
</tr>
<tr>
<td>status</td>
<td>The plugin status based on the status of the feature store indices (red, yellow, or green) and circuit breaker state (open or closed).</td>
</tr>
<tr>
<td>cache.cache_capacity_reached</td>
<td>Indicates if the cache limit is reached.</td>
</tr>
</tbody>
</table>

### Get cache stats

Returns statistics about the cache and memory usage.

```
GET opendistro/_ltr/_cachestats
```
{
    "_nodes": {
        "total": 2,
        "successful": 2,
        "failed": 0
    },
    "cluster_name": "es-cluster",
    "all": {
        "total": {
            "ram": 612,
            "count": 1
        },
        "features": {
            "ram": 0,
            "count": 0
        },
        "featuresets": {
            "ram": 612,
            "count": 1
        },
        "models": {
            "ram": 0,
            "count": 0
        }
    },
    "stores": {
        ".ltrstore": {
            "total": {
                "ram": 612,
                "count": 1
            },
            "features": {
                "ram": 0,
                "count": 0
            },
            "featuresets": {
                "ram": 612,
                "count": 1
            },
            "models": {
                "ram": 0,
                "count": 0
            }
        }
    },
    "nodes": {
        "ejF6wutERF20wOFNOXB61A": {
            "name": "elasticsearch3",
            "hostname": "172.18.0.4",
            "stats": {
                "total": {
                    "ram": 612,
                    "count": 1
                },
                "features": {
                    "ram": 0,
                    "count": 0
                },
                "featuresets": {
                    "ram": 612,
                    "count": 1
                },
                "models": {
                    "ram": 0,
                    "count": 0
                }
            }
        }
    }
}
Asynchronous search requires Elasticsearch 7.10 or later. Full documentation for asynchronous search, including detailed steps and API descriptions, is available in the Open Distro for Elasticsearch documentation.

Sample search call

To perform an asynchronous search, send HTTP requests to \_opendistro\_asynchronous\_search using the following format:

\[
\text{POST } \text{elasticsearch\_domain}/\_opendistro/\_asynchronous\_search
\]

You can specify the following asynchronous search options:

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
<th>Default value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>_wait_for_complet...</td>
<td>Specifies the amount of time that you plan to wait for the results. You can see whatever results you get within this time just like in a normal search. You can poll the remaining results based on an ID. The maximum value is 300 seconds.</td>
<td>1 second</td>
<td>No</td>
</tr>
<tr>
<td>keep_on_completion</td>
<td>Specifies whether you want to save the results in the cluster after the search is complete. You can examine the stored results at a later time.</td>
<td>false</td>
<td>No</td>
</tr>
<tr>
<td>keep_alive</td>
<td>Specifies the amount of time that the result is saved in the cluster. For example, 2d means that</td>
<td>12 hours</td>
<td>No</td>
</tr>
</tbody>
</table>
Asynchronous search permissions

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
<th>Default value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>the results are stored in the cluster for 48 hours. The saved search results are deleted after this period or if the search is canceled. Note that this includes the query runtime. If the query overruns this time, the process cancels this query automatically.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Sample request

```
POST _opendistro/_asynchronous_search/?
pretty&size=10&wait_for_completion_timeout=1ms&keep_on_completion=true&request_cache=false
{
    "aggs": {
        "city": {
            "terms": {
                "field": "city",
                "size": 10
            }
        }
    }
}
```

**Note**

All request parameters that apply to a standard _search query are supported.

Asynchronous search permissions

The asynchronous search feature supports the section called “Fine-grained access control” (p. 90). For details on mixing and matching permissions to fit your use case, see Asynchronous search security.

For domains with fine-grained access control enabled, you need the following minimum permissions for a role:

```
# Allows users to use all asynchronous-search functionality
asynchronous_search_full_access:
    reserved: true
    cluster_permissions:
        - 'cluster:admin/opendistro/asynchronous-search/*'
    index_permissions:
        - index_patterns:
            - '*'
        allowed_actions:
            - 'indices:data/read/search*'

# Allows users to read stored asynchronous-search results
asynchronous_search_read_access:
    reserved: true
    cluster_permissions:
        - 'cluster:admin/opendistro/asynchronous-search/get'
```

For domains with fine-grained access control disabled, use your IAM access and secret key to sign all requests. You can access the results with the asynchronous search ID.

Asynchronous search settings

Open Distro for Elasticsearch lets you change all available asynchronous search settings using the _cluster/settings API. In Amazon ES, you can only change the following settings:
• opendistro.asynchronous_search.node_concurrent_running_searches
• opendistro.asynchronous_search.persist_search_failures

Cross-cluster search

You can perform an asynchronous search across clusters with the following minor limitations:

• You can run an asynchronous search only on the source domain.
• You can't minimize network round trips as part of a cross-cluster search query.

If you set up a connection between domain-a -> domain-b with connection alias cluster_b and domain-a -> domain-c with connection alias cluster_c, asynchronously search domain-a, domain-b, and domain-c as follows:

```
POST https://src-domain.us-east-1.es.amazonaws.com/local_index,cluster_b:b_index,cluster_c:c_index/_opendistro/_asynchronous_search/?pretty&size=10&wait_for_completion_timeout=500ms&keep_on_completion=true&request_cache=false
{
  "size": 0,
  "_source": {
    "excludes": []
  },
  "aggs": {
    "2": {
      "terms": {
        "field": "clientip",
        "size": 50,
        "order": {
          "_count": "desc"
        }
      }
    },
    "stored_fields": ["*"],
    "script_fields": {},
    "docvalue_fields": [
      "@timestamp"
    ],
    "query": {
      "bool": {
        "must": [
          {
            "query_string": {
              "query": "status:404",
              "analyze_wildcard": true,
              "default_field": "**"
            }
          },
          {
            "range": {
              "@timestamp": {
                "gte": 1483747200000,
                "lte": 1488326400000,
                "format": "epoch_millis"
              }
            }
          }
        ]
      }
    }
  }
}
```

API Version 2015-01-01
214
"should": [],
    "must_not": []
  }
}

Response

{
  "id": "Fm9pYmZjvVG91U19xb0HJcUJnMlJfBFEEAAAAAAAknghQ1OWVmczNzQjVEa2dMYTBXaTdBaAgAAAAAAAB",
  "state": "RUNNING",
  "start_time_in_millis": 1609329314796,
  "expiration_time_in_millis": 1609761314796
}

For more information, see the section called "Cross-cluster search" (p. 189).

UltraWarm

Asynchronous searches with UltraWarm indices continue to work. For more information, see the section called "UltraWarm storage" (p. 222).

Note
You can monitor asynchronous search statistics in CloudWatch. For a full list of metrics, see the section called "Asynchronous search metrics" (p. 43).
Using Kibana with Amazon Elasticsearch Service

Kibana is a popular open source visualization tool designed to work with Elasticsearch. Amazon Elasticsearch Service (Amazon ES) provides an installation of Kibana with every Amazon ES domain. You can find a link to Kibana on your domain dashboard on the Amazon ES console. The URL is `domain-endpoint/_plugin/kibana/`. Queries using this default Kibana installation have a 300-second timeout.

The following sections address some common Kibana use cases:

- the section called “Controlling access to Kibana” (p. 216)
- the section called “Configuring Kibana to use a WMS map server” (p. 219)
- the section called “Connecting a local Kibana server to Amazon ES” (p. 219)

Controlling access to Kibana

Kibana does not natively support IAM users and roles, but Amazon ES offers several solutions for controlling access to Kibana:

- Enable SAML authentication for Kibana (p. 123).
- Use fine-grained access control (p. 95) with HTTP basic authentication.
- Configure the section called “Amazon Cognito authentication for Kibana” (p. 128).
- For public access domains, configure an IP-based access policy (p. 80), with or without a proxy server (p. 216).
- For VPC access domains, use an open access policy, with or without a proxy server, and security groups to control access. To learn more, see the section called “About access policies on VPC domains” (p. 25).

Using a proxy to access Amazon ES from Kibana

Note
This process is only applicable if your domain uses public access and you don’t want to use the section called “Amazon Cognito authentication for Kibana” (p. 128). See the section called “Controlling access to Kibana” (p. 216).

Because Kibana is a JavaScript application, requests originate from the user's IP address. IP-based access control might be impractical due to the sheer number of IP addresses you would need to allow in order for each user to have access to Kibana. One workaround is to place a proxy server between Kibana and Amazon ES. Then you can add an IP-based access policy that allows requests from only one IP address, the proxy's. The following diagram shows this configuration.
1. This is your Amazon ES domain. IAM provides authorized access to this domain. An additional, IP-based access policy provides access to the proxy server.
2. This is the proxy server, running on an Amazon EC2 instance.
3. Other applications can use the Signature Version 4 signing process to send authenticated requests to Amazon ES.
4. Kibana clients connect to your Amazon ES domain through the proxy.

To enable this sort of configuration, you need a resource-based policy that specifies roles and IP addresses. Here's a sample policy:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Principal": {
        "AWS": "arn:aws:iam::111111111111:role/allowedrole1"
      },
      "Action": ["es:ESHttpGet"],
      "Effect": "Allow"
    }
  ]
}
```
We recommend that you configure the EC2 instance running the proxy server with an Elastic IP address. This way, you can replace the instance when necessary and still attach the same public IP address to it. To learn more, see Elastic IP Addresses in the Amazon EC2 User Guide for Linux Instances.

If you use a proxy server and the section called “Amazon Cognito authentication for Kibana” (p. 128), you might need to add settings for Kibana and Amazon Cognito to avoid redirect_mismatch errors. See the following nginx.conf example:

```
server {
    listen 443;
    server_name $host;
    rewrite ^/$ https://$host/_plugin/kibana redirect;

    ssl_certificate /etc/nginx/cert.crt;
    ssl_certificate_key /etc/nginx/cert.key;

    ssl on;
    ssl_session_cache builtin:1000 shared:SSL:10m;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_ciphers HIGH:!aNULL:!eNULL:!EXPORT:!CAMELLIA:!DES:!MD5:!PSK:!RC4;
    ssl_prefer_server_ciphers on;

    location /_plugin/kibana {
        # Forward requests to Kibana
        proxy_pass https://kibana_host/_plugin/kibana;

        # Handle redirects to Cognito
        proxy_redirect https://cognito_host https://$host;
        proxy_cookie_domain $kibana_host $host;
        proxy_cookie_path / _plugin/kibana/;

        # Response buffer settings
        proxy_buffer_size 128k;
        proxy_buffers 4 256k;
        proxy_busy_buffers_size 256k;
    }

    location ~(log|sign|fav|forgot|change|saml|oauth2) {
        # Forward requests to Cognito
        proxy_pass https://cognito_host;

        # Handle redirects to Kibana
        proxy_redirect https://kibana_host https://$host;
    }
}
```
Configuring Kibana to use a WMS map server

The default installation of Kibana for Amazon ES includes a map service, except for domains in the India and China regions. The map service supports up to 10 zoom levels.

Regardless of your region, you can configure Kibana to use a different Web Map Service (WMS) server for coordinate map visualizations. Region map visualizations only support the default map service.

To configure Kibana to use a WMS map server:

1. Open Kibana.
2. Choose Management.
3. Choose Advanced Settings.
5. Change `enabled` to `true` and `url` to the URL of a valid WMS map server:

```json
{
  "enabled": true,
  "url": "wms-server-url",
  "options": {
    "format": "image/png",
    "transparent": true
  }
}
```
6. Choose Save.

To apply the new default value to visualizations, you might need to reload Kibana. If you have saved visualizations, choose Options after opening the visualization. Verify that WMS map server is enabled and WMS url contains your preferred map server, and then choose Apply changes.

**Note**

Map services often have licensing fees or restrictions. You are responsible for all such considerations on any map server that you specify. You might find the map services from the U.S. Geological Survey useful for testing.

Connecting a local Kibana server to Amazon ES

If you have invested significant time into configuring your own Kibana instance, you can use it instead of (or in addition to) the default Kibana instance that Amazon ES provides.

To connect a local Kibana server to Amazon ES:

- Make the following changes to `config/kibana.yml`:

```yaml
kibana.index: ".kibanalocal"
# Use elasticsearch.url for versions older than 6.6
# elasticsearch.url: "https://domain-endpoint:443"
# Use elasticsearch.hosts for versions 6.6 and later
```
Managing indices in Kibana

The Kibana installation on your Amazon ES domain provides a useful UI for managing indices in different storage tiers on your domain. Choose Index Management from the Kibana main menu to view all indices in hot, UltraWarm (p. 222), and cold (p. 231) storage, as well as indices managed by Index State Management (ISM) policies. Use index management to move indices between warm and cold storage, and to monitor migrations between the three tiers.

**Index Management**

- Rollup jobs
- State management policies
- Indices
  - Hot Indices
  - Warm Indices
  - Cold Indices
  - Policy managed indices

**Cold indices**

Cold storage lets you further reduce storage costs.

Search index name or state

- [ ] Index
- [ ] my-index-3
- [ ] my-index-2
- [ ] my-index-1

**Additional features**

The default Kibana installation on each Amazon ES domain has some additional features compared to the open source version of Kibana:
• User interfaces for the various Open Distro for Elasticsearch plugins (p. 275)
• Tenants (p. 99)
• Reports

Use the Reporting menu to generate on-demand CSV reports from the Discover page and PDF or PNG reports of dashboards or visualizations. Amazon ES does not support scheduled reports.
• Gantt charts
• Notebooks (experimental)
Managing indices in Amazon Elasticsearch Service

After you add data to Amazon Elasticsearch Service (Amazon ES), you often need to reindex that data, work with index aliases, move an index to more cost-effective storage, or delete it altogether. This chapter covers UltraWarm storage and Index State Management. For information on the Elasticsearch index APIs, see the Open Distro for Elasticsearch documentation.

Topics
- UltraWarm storage for Amazon Elasticsearch Service (p. 222)
- Cold storage for Amazon Elasticsearch Service (p. 231)
- Index State Management in Amazon Elasticsearch Service (p. 238)
- Summarizing indices in Amazon Elasticsearch Service with index rollups (p. 243)
- Using Curator to rotate data in Amazon Elasticsearch Service (p. 244)
- Migrating Amazon Elasticsearch Service indices using remote reindex (p. 248)

UltraWarm storage for Amazon Elasticsearch Service

UltraWarm provides a cost-effective way to store large amounts of read-only data on Amazon Elasticsearch Service (Amazon ES). Standard data nodes use "hot" storage, which takes the form of instance stores or Amazon EBS volumes attached to each node. Hot storage provides the fastest possible performance for indexing and searching new data.

Rather than attached storage, UltraWarm nodes use Amazon S3 and a sophisticated caching solution to improve performance. For indices that you are not actively writing to, query less frequently, and don't need the same performance from, UltraWarm offers significantly lower costs per GiB of data. Because warm indices are read-only unless you return them to hot storage, UltraWarm is best-suited to immutable data, such as logs.

In Elasticsearch, warm indices behave just like any other index. You can query them using the same APIs or use them to create dashboards in Kibana.

Topics
- Prerequisites (p. 223)
- UltraWarm storage requirements and performance considerations (p. 224)
- UltraWarm pricing (p. 224)
- Enabling UltraWarm (p. 224)
- Migrating indices to UltraWarm storage (p. 226)
- Automating migrations (p. 228)
- Migration tuning (p. 228)
- Cancelling migrations (p. 229)
• Listing hot and warm indices (p. 229)
• Returning warm indices to hot storage (p. 229)
• Restoring warm indices from automated snapshots (p. 229)
• Manual snapshots of warm indices (p. 230)
• Migrating warm indices to cold storage (p. 231)
• Disabling UltraWarm (p. 231)

Prerequisites

UltraWarm has a few important prerequisites:

• UltraWarm requires Elasticsearch 6.8 or higher.
• To use warm storage, domains must have dedicated master nodes (p. 268).
• If your domain uses a T2 or T3 instance type for your data nodes, you can't use warm storage.
• If the domain uses fine-grained access control (p. 90), users must be mapped to the
  ultrawarm_manager role in Kibana to make UltraWarm API calls.

Note
The ultrawarm_manager role might not be defined on some preexisting Amazon ES domains.
If you don't see the role in Kibana, you need to manually create it (p. 223).

Configure permissions

If you enable UltraWarm on a preexisting Amazon ES domain, the ultrawarm_manager role might not be defined on the domain. Non-admin users must be mapped to this role in order to manage warm indices on domains using fine-grained access control. To manually create the ultrawarm_manager role, perform the following steps:

1. In Kibana, go to Security and choose Permissions.
2. Choose Create action group and configure the following groups:

<table>
<thead>
<tr>
<th>Group name</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ultrawarm_cluster</td>
<td>• cluster:admin/ultrawarm/migration/list</td>
</tr>
<tr>
<td></td>
<td>• cluster:monitor/nodes/stats</td>
</tr>
<tr>
<td>ultrawarm_index_read</td>
<td>• indices:admin/ultrawarm/migration/get</td>
</tr>
<tr>
<td></td>
<td>• indices:monitor/get</td>
</tr>
<tr>
<td>ultrawarm_index_write</td>
<td>• indices:admin/ultrawarm/migration/warm</td>
</tr>
<tr>
<td></td>
<td>• indices:monitor/stats</td>
</tr>
<tr>
<td></td>
<td>• indices:admin/ultrawarm/migration/cancel</td>
</tr>
</tbody>
</table>

3. Choose Roles and Create role.
4. Name the role ultrawarm_manager.
5. For Cluster permissions, select ultrawarm_cluster and cluster_monitor.
6. For Index, type *.
7. For Index permissions, select ultrawarm_index_read, ultrawarm_index_write, and indices_monitor.
8. Choose Create.
9. After you create the role, map it (p. 98) to any user or backend role that will manage UltraWarm indices.

UltraWarm storage requirements and performance considerations

As covered in the section called “Calculating storage requirements” (p. 264), data in hot storage incurs significant overhead: replicas, Linux reserved space, and Amazon ES reserved space. For example, a 20 GiB primary shard with one replica shard requires roughly 53 GiB of hot storage.

Because it uses Amazon S3, UltraWarm incurs none of this overhead. When calculating UltraWarm storage requirements, you consider only the size of the primary shards. The durability of data in S3 removes the need for replicas, and S3 abstracts away any operating system or service considerations. That same 20 GiB shard requires 20 GiB of warm storage. If you provision an ultrawarm1.large.elasticsearch instance, you can use all 20 TiB of its maximum storage for primary shards. See the section called “UltraWarm storage limits” (p. 296) for a summary of instance types and the maximum amount of storage that each can address.

With UltraWarm, we still recommend a maximum shard size of 50 GiB. The number of CPU cores and amount of RAM allocated to each UltraWarm instance type gives you an idea of the number of shards they can simultaneously search.

For example, each ultrawarm1.medium.elasticsearch instance has two CPU cores and can address up to 1.5 TiB of storage on S3. Two of these instances have a combined 3 TiB of storage, which works out to approximately 62 shards if each shard is 50 GiB. If a request to the cluster only searches four of these shards, performance might be excellent. If the request is broad and searches all 62 of them, the four CPU cores might struggle to perform the operation. Monitor the WarmCPUUtilization and WarmJVMMemoryPressure UltraWarm metrics (p. 39) to understand how the instances handle your workloads.

If your searches are broad or frequent, consider leaving the indices in hot storage. Just like any other Elasticsearch workload, the most important step to determining if UltraWarm meets your needs is to perform representative client testing using a realistic dataset.

UltraWarm pricing

With hot storage, you pay for what you provision. Some instances require an attached Amazon EBS volume, while others include an instance store. Whether that storage is empty or full, you pay the same price.

With UltraWarm storage, you pay for what you use. An ultrawarm1.large.elasticsearch instance can address up to 20 TiB of storage on S3, but if you store only 1 TiB of data, you’re only billed for 1 TiB of data. Like all other node types, you also pay an hourly rate for each UltraWarm node. For more information, see the section called “Pricing for Amazon ES” (p. 3).

Enabling UltraWarm

The console is the simplest way to create a domain that uses warm storage. While creating the domain, choose Enable UltraWarm data nodes and the number of warm nodes that you want. The same basic process works on existing domains, provided they meet the prerequisites (p. 223). Even after the domain state changes from Processing to Active, UltraWarm might not be available to use for several hours.
You can also use the AWS CLI or configuration API (p. 339) to enable UltraWarm, specifically the \n\nNote  
Domains support a maximum number of warm nodes. For details, see the section called "Limits" (p. 295).

Sample CLI command

The following AWS CLI command creates a domain with three data nodes, three dedicated master nodes, six warm nodes, and fine-grained access control enabled:

```bash
aws es create-elasticsearch-domain \
  --domain-name my-domain \
  --elasticsearch-version 7.10 \
  --elasticsearch-cluster-config InstanceCount=3,InstanceType=r6g.large.elasticsearch,DedicatedMasterEnabled=true,DedicatedMasterType=r6g.large.elasticsearch,DedicatedMasterCount=3,ZoneAwarenessEnabled=true,ZoneAwarenessConfig={AvailabilityZoneCount=3},WarmEnabled=true,WarmCount=6,WarmType=ultrawarm1.medium.elasticsearch \n  --ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=11 \n  --node-to-node-encryption-options Enabled=true \n  --encryption-at-rest-options Enabled=true \n  --domain-endpoint-options EnforceHTTPS=true,TLSSecurityPolicy=Policy-Min-TLS-1-2-2019-07 \n  --advanced-security-options Enabled=true,InternalUserDatabaseEnabled=true,MasterUserOptions='{"MasterUserName=master-user,Ma\n  --access-policies '{"Version":"2012-10-17","Statement":[]}"\n  --region us-east-1
```

For detailed information, see the AWS CLI Command Reference.

Sample configuration API request

The following request to the configuration API creates a domain with three data nodes, three dedicated master nodes, and six warm nodes with fine-grained access control enabled and a restrictive access policy:

```json
{
  "ElasticsearchClusterConfig": {
    "InstanceCount": 3,
    "InstanceType": "r6g.large.elasticsearch",
    "DedicatedMasterEnabled": true,
    "DedicatedMasterType": "r6g.large.elasticsearch",
    "DedicatedMasterCount": 3,
    "ZoneAwarenessEnabled": true,
    "ZoneAwarenessConfig": {
      "AvailabilityZoneCount": 3
    },
    "WarmEnabled": true,
    "WarmCount": 6,
    "WarmType": "ultrawarm1.medium.elasticsearch"
  },
  "EBSOptions": {
    "EBSEnabled": true,
    "VolumeType": "gp2",
    "VolumeSize": 11
  },
  "EncryptionAtRestOptions": {
```
Migrating indices to UltraWarm storage

If you finish writing to an index and no longer need the fastest possible search performance, migrate it from hot to warm:

```
POST _ultrawarm/migration/my-index/_warm
```

Then check the status of the migration:

```
GET _ultrawarm/migration/my-index/_status
```

```
{
  "migration_status": {
    "index": "my-index",
    "state": "RUNNING_SHARD_RELOCATION",
    "migration_type": "HOT_TO_WARM",
    "shard_level_status": {
      "running": 0,
      "total": 5,
      "pending": 3,
      "failed": 0,
      "succeeded": 2
    }
  }
}
```

Index health must be green to perform a migration. If you migrate several indices in quick succession, you can get a summary of all migrations in plaintext, similar to the `_cat` API:

```
GET _ultrawarm/migration/_status?v
```

```
index migration_type state
--- --- ----------------------------
my-index HOT_TO_WARM RUNNING_SHARD_RELOCATION
```
You can have up to 200 simultaneous migrations from hot to warm storage. To check the current number of migrations in the queue, monitor the `HotToWarmMigrationQueueSize` metric (p. 39). Indices remain available throughout the migration process—no downtime.

The migration process has the following states:

```
<table>
<thead>
<tr>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>PENDING_INCREMENTAL_SNAPSHOT</td>
</tr>
<tr>
<td>RUNNING_INCREMENTAL_SNAPSHOT</td>
</tr>
<tr>
<td>FAILED_INCREMENTAL_SNAPSHOT</td>
</tr>
<tr>
<td>PENDING_FORCE_MERGE</td>
</tr>
<tr>
<td>RUNNING_FORCE_MERGE</td>
</tr>
<tr>
<td>FAILED_FORCE_MERGE</td>
</tr>
<tr>
<td>PENDING_FULL_SNAPSHOT</td>
</tr>
<tr>
<td>RUNNING_FULL_SNAPSHOT</td>
</tr>
<tr>
<td>FAILED_FULL_SNAPSHOT</td>
</tr>
<tr>
<td>PENDING_SHARD_RELOCATION</td>
</tr>
<tr>
<td>RUNNING_SHARD_RELOCATION</td>
</tr>
<tr>
<td>FINISHED_SHARD_RELOCATION</td>
</tr>
</tbody>
</table>
```

As these states indicate, migrations might fail during snapshots, shard relocations, or force merges. Failures during snapshots or shard relocation are typically due to node failures or S3 connectivity issues. Lack of disk space is usually the underlying cause of force merge failures.

After a migration finishes, the same `_status` request returns an error. If you check the index at that time, you can see some settings that are unique to warm indices:

```
GET my-index/_settings

{
  "my-index": {
    "settings": {
      "index": {
        "refresh_interval": "-1",
        "auto_expand_replicas": "false",
        "provided_name": "my-index",
        "creation_date": "1599241458998",
        "unassigned": {
          "node_left": {
            "delayed_timeout": "5m"
          }
        },
        "number_of_replicas": "1",
        "uuid": "GswyCdR0RSq0SJYmzsIpiw",
        "version": {
          "created": "7070099"
        },
        "routing": {
          "allocation": {
            "require": {
              "box_type": "warm"
            }
          }
        },
        "number_of_shards": "5",
        "merge": {
          "policy": {
            "max_merge_at_once_explicit": "50"
          }
        }
      }
    }
  }
}
```
• `number_of_replicas`, in this case, is the number of passive replicas, which don't consume disk space.
• `routing.allocation.require.box_type` specifies that the index should use warm nodes rather than standard data nodes.
• `merge.policy.max_merge_at_once_explicit` specifies the number of segments to simultaneously merge during the migration.

Indices in warm storage are read-only unless you return them to hot storage (p. 229), which makes UltraWarm best-suited to immutable data, such as logs. You can query the indices and delete them, but you can't add, update, or delete individual documents. If you try, you might encounter the following error:

```json
{
  "error": {
    "root_cause": [{
      "type": "cluster_block_exception",
      "reason": "blocked by: [FORBIDDEN/12/index read-only / allow delete (api)];"
    }],
    "type": "cluster_block_exception",
    "reason": "blocked by: [FORBIDDEN/12/index read-only / allow delete (api)];"
  },
  "status": 403
}
```

## Automating migrations

We recommend using the section called "Index State Management" (p. 238) to automate the migration process after an index reaches a certain age or meets other conditions. The sample policy here (p. 239) demonstrates that workflow.

## Migration tuning

Index migrations to UltraWarm storage require a force merge. Each Elasticsearch index is composed of some number of shards, and each shard is composed of some number of Lucene segments. The force merge operation purges documents that were marked for deletion and conserves disk space. By default, UltraWarm merges indices into one segment.

You can change this value up to 1,000 segments using the `index.ultrawarm.migration.force_merge.max_num_segments` setting. Higher values speed up the migration process, but increase query latency for the warm index after the migration finishes. To change the setting, make the following request:

```json
PUT my-index/_settings
{
  "index": {
    "ultrawarm": {
      "migration": {
        "force_merge": {
          "max_num_segments": 1
        }
      }
    }
  }
}
```

To check how long this stage of the migration process takes, monitor the `HotToWarmMigrationForceMergeLatency` metric (p. 39).

API Version 2015-01-01

228
Cancelling migrations

UltraWarm handles migrations sequentially, in a queue. If a migration is in the queue, but has not yet started, you can remove it from the queue using the following request:

```
POST _ultrawarm/migration/_cancel/my-index
```

If your domain uses fine-grained access control, you must have the `indices:admin/ultrawarm/migration/cancel` permission to make this request.

Listing hot and warm indices

UltraWarm adds two additional options, similar to `_all`, to help manage hot and warm indices. For a list of all warm or hot indices, make the following requests:

```
GET _warm
GET _hot
```

You can use these options in other requests that specify indices, such as:

```
_cat/indices/_warm
_cluster/state/_all/_hot
```

Returning warm indices to hot storage

If you need to write to an index again, migrate it back to hot storage:

```
POST _ultrawarm/migration/my-index/_hot
```

You can have up to 10 simultaneous migrations from warm to hot storage. To check the current number, monitor the `WarmToHotMigrationQueueSize` metric (p. 39).

After the migration finishes, check the index settings to make sure they meet your needs. Indices return to hot storage with one replica.

Restoring warm indices from automated snapshots

In addition to the standard repository for automated snapshots, UltraWarm adds a second repository for warm indices, `cs-ultrawarm`. Each snapshot in this repository contains only one index. If you delete a warm index, its snapshot remains in the `cs-ultrawarm` repository for 14 days, just like any other automated snapshot.

When you restore a snapshot from `cs-ultrawarm`, it restores to warm storage, not hot storage. Snapshots in the `cs-automated` and `cs-automated-enc` repositories restore to hot storage.

**To restore an UltraWarm snapshot to warm storage**

1. Identify the latest snapshot that contains the index that you want to restore:

```
GET _snapshot/cs-ultrawarm/_all
```
Manual snapshots of warm indices

You can take manual snapshots of warm indices, but we don’t recommend it. The automated cs-ultrawarm repository already contains a snapshot for each warm index, taken during the migration, at no additional charge.

By default, Amazon ES does not include warm indices in manual snapshots. For example, the following call only includes hot indices:

```
PUT _snapshot/my-repository/my-snapshot
```

If you choose to take manual snapshots of warm indices, several important considerations apply.

- You can’t mix hot and warm indices. For example, the following request fails:

```
PUT _snapshot/my-repository/my-snapshot
{
  "indices": "warm-index-1,hot-index-1",
  "include_global_state": false
}
```

If they include a mix of hot and warm indices, wildcard (*) statements fail, as well.

- You can only include one warm index per snapshot. For example, the following request fails:

```
PUT _snapshot/my-repository/my-snapshot
{
  "indices": "warm-index-1,warm-index-2,other-warm-indices-*",
  "include_global_state": false
}
```

This request succeeds:

```
PUT _snapshot/my-repository/my-snapshot
```
Migrating warm indices to cold storage

If you have data in UltraWarm that you query infrequently, consider migrating it to cold storage. Cold storage is meant for data you only access occasionally or is no longer in active use. You can't read from or write to cold indices, but you can migrate them back to warm storage at no cost whenever you need to query them. For instructions, see the section called “Migrating indices to cold storage” (p. 234).

Disabling UltraWarm

The console is the simplest way to disable UltraWarm. Choose the domain, Edit domain, uncheck Enable UltraWarm data nodes, and Submit. You can also use the WarmEnabled option in the AWS CLI and configuration API.

Before you disable UltraWarm, you must either delete all warm indices or migrate them back to hot storage. After warm storage is empty, wait five minutes before attempting to disable the feature.

Cold storage for Amazon Elasticsearch Service

Cold storage lets you store any amount of infrequently accessed or historical data on your Amazon Elasticsearch Service (Amazon ES) domain and analyze it on demand, at a lower cost than other storage tiers. Cold storage is appropriate if you need to do periodic research or forensic analysis on your older data. Practical examples of data suitable for cold storage include infrequently accessed logs, data that must be preserved to meet compliance requirements, or logs that have historical value.

Similar to UltraWarm (p. 222) storage, cold storage is backed by Amazon S3. When you need to query cold data, you can selectively attach it to existing UltraWarm nodes. You can manage the migration and lifecycle of your cold data manually or with Index State Management policies.

Topics
- Prerequisites (p. 232)
- Cold storage requirements and performance considerations (p. 232)
- Cold storage pricing (p. 233)
- Enabling cold storage (p. 233)
- Managing cold indices in Kibana (p. 234)
- Migrating indices to cold storage (p. 234)
- Automating migrations to cold storage (p. 235)
- Canceling migrations to cold storage (p. 235)
- Listing cold indices (p. 236)
- Migrating cold indices to warm storage (p. 237)
- Canceling migrations from cold to warm storage (p. 237)
- Updating cold index metadata (p. 238)
- Deleting cold indices (p. 238)
- Disabling cold storage (p. 238)
Prerequisites

Cold storage has the following prerequisites:

- Cold storage requires Elasticsearch version 7.9 or later.
- To enable cold storage on an Amazon ES domain, you must also enable UltraWarm on the same domain.
- To use cold storage, domains must have dedicated master nodes (p. 268).
- If your domain uses a T2 or T3 instance type for your data nodes, you can't use cold storage.
- If the domain uses fine-grained access control (p. 90), non-admin users must be mapped (p. 98) to the cold_manager role in Kibana in order to manage cold indices.

**Note**

The cold_manager role might not exist on some preexisting Amazon ES domains. If you don't see the role in Kibana, you need to manually create it (p. 232).

Configure permissions

If you enable cold storage on a preexisting Amazon ES domain, the cold_manager role might not be defined on the domain. If the domain uses fine-grained access control (p. 90), non-admin users must be mapped to this role in order to manage cold indices. To manually create the cold_manager role, perform the following steps:

1. In Kibana, go to Security and choose Permissions.
2. Choose Create action group and configure the following groups:

<table>
<thead>
<tr>
<th>Group name</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>cold_cluster</td>
<td>• cluster:monitor/nodes/stats</td>
</tr>
<tr>
<td></td>
<td>• cluster:admin/ultrawarm*</td>
</tr>
<tr>
<td></td>
<td>• cluster:admin/cold/*</td>
</tr>
<tr>
<td>cold_index</td>
<td>• indices:monitor/stats</td>
</tr>
<tr>
<td></td>
<td>• indices:data/read/minmax</td>
</tr>
<tr>
<td></td>
<td>• indices:admin/ultrawarm/migration/get</td>
</tr>
<tr>
<td></td>
<td>• indices:admin/ultrawarm/migration/cancel</td>
</tr>
</tbody>
</table>

3. Choose Roles and Create role.
4. Name the role cold_manager.
5. For Cluster permissions, choose the cold_cluster group you created.
6. For Index, enter *.
7. For Index permissions, choose the cold_index group you created.
8. Choose Create.
9. After you create the role, map it (p. 98) to any user or backend role that manages cold indices.

Cold storage requirements and performance considerations

Because cold storage uses Amazon S3, it incurs none of the overhead of hot storage, such as replicas, Linux reserved space, and Amazon ES reserved space. Cold storage doesn't have specific instance types
because it doesn't have any compute capacity attached to it. You can store any amount of data in cold storage. Monitor the ColdStorageSpaceUtilization metric in Amazon CloudWatch to see how much cold storage space you're using.

### Cold storage pricing

Similar to UltraWarm storage, with cold storage you only pay for data storage. There's no compute cost for cold data and you won't get billed if there's no data in cold storage.

You don't incur any transfer charges when moving data between cold and warm storage. While indices are being migrated between warm and cold storage, you continue to pay for only one copy of the index. After the migration completes, the index is billed according to the storage tier it was migrated to. For more information about cold storage pricing, see the section called “Pricing for Amazon ES” (p. 3).

### Enabling cold storage

The console is the simplest way to create a domain that uses cold storage. While creating the domain, choose Enable cold storage. The same process works on existing domains as long as you meet the prerequisites (p. 223). Even after the domain state changes from Processing to Active, cold storage might not be available for several hours.

You can also use the AWS CLI or configuration API (p. 339) to enable cold storage.

### Sample CLI command

The following AWS CLI command creates a domain with three data nodes, three dedicated master nodes, cold storage enabled, and fine-grained access control enabled:

```bash
aws es create-elasticsearch-domain
  --domain-name my-domain
  --elasticsearch-version 7.10
  --elasticsearch-cluster-config ColdStorageOptions={Enabled=true},WarmEnabled=true,WarmCount=4,WarmType=ultrawarm1.medium.elasticsearch,DedicatedMasterEnabled=true,DedicatedMasterType=r6g.large.elasticsearch,DedicatedMasterCount=3,InstanceType=r6g.large.elasticsearch,InstanceCount=3
  --ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=11
  --node-to-node-encryption-options Enabled=true
  --encryption-at-rest-options Enabled=true
  --advanced-security-options Enabled=true,InternalUserDatabaseEnabled=true,MastUserOptions='{MasterUserName=master-user,MastUserPassword=master-password}'
  --region us-east-2
```

For detailed information, see the AWS CLI Command Reference.

### Sample configuration API request

The following request to the configuration API creates a domain with three data nodes, three dedicated master nodes, cold storage enabled, and fine-grained access control enabled:

```json
{  "ElasticsearchClusterConfig": {  "InstanceCount": 3,  "InstanceType": "r6g.large.elasticsearch",  "DedicatedMasterEnabled": true,  "DedicatedMasterType": "r6g.large.elasticsearch",  "DedicatedMasterCount": 3,  "ColdStorageOptions": {"Enabled": true},  "WarmOptions": {"Enabled": true, "WarmCount": 4, "WarmType": "ultrawarm1.medium.elasticsearch"},  "EbsOptions": {"Enabled": true, "VolumeType": "gp2", "VolumeSize": 11},  "NodeToNodeEncryptionOptions": {"Enabled": true},  "EncryptionAtRestOptions": {"Enabled": true},  "DomainEndpointOptions": {"EnforceHTTPS": true, "TLSSecurityPolicy": "Policy-Min-TLS-1-2-2019-07"},  "AdvancedSecurityOptions": {"Enabled": true, "InternalUserDatabaseEnabled": true, "MasterUserOptions": {"MasterUserName": "master-user", "MasterUserPassword": "master-password"}},  "Region": "us-east-2"}
```
Managing cold indices in Kibana

You can manage hot, warm and cold indices with the existing Kibana interface in your Amazon ES domain. Kibana enables you to migrate indices between warm and cold storage, and monitor index migration status, without using the CLI or configuration API. For more information, see Managing indices in Kibana (p. 220).

Migrating indices to cold storage

When you migrate indices to cold storage, you provide a time range for the data to make discovery easier. You can select a timestamp field based on the data in your index, manually provide a start and end timestamp, or choose to not specify one.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Supported value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>timestamp_field</td>
<td>The date/time field from the index mapping.</td>
<td>The minimum and maximum values of the provided field are computed and stored as the start_time and end_time metadata for the cold index.</td>
</tr>
</tbody>
</table>
Automating migrations to cold storage

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Supported value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>start_time and end_time</td>
<td>One of the following formats:</td>
<td>The provided values are stored as the start_time and end_time metadata for</td>
</tr>
<tr>
<td></td>
<td>• strict_date_optional_time. For example: yyyy-MM-dd'T'HH:mm:ss.SSSZ or yyyy-MM-dd</td>
<td>the cold index.</td>
</tr>
<tr>
<td></td>
<td>• Epoch time in milliseconds</td>
<td></td>
</tr>
</tbody>
</table>

If you don't want to specify a timestamp, add ?ignore=timestamp to the request instead.

The following request migrates a warm index to cold storage and provides start and end times for the data in that index:

```
POST _ultrawarm/migration/my-index/_cold
{
  "start_time": "2020-03-09",
  "end_time": "2020-03-09T23:00:00Z"
}
```

Then check the status of the migration:

```
GET _ultrawarm/migration/my-index/_status
```

You can migrate indices from warm to cold storage in batches of 10, with a maximum of 100 simultaneous requests. The migration process has the following states:

- ACCEPTED_COLD_MIGRATION - Migration request is accepted and queued.
- RUNNING_METADATA_MIGRATION - The migration request was selected for execution and metadata is migrating to cold storage.
- FAILED_METADATA_MIGRATION - The attempt to add index metadata has failed and all retries are exhausted.
- PENDING_INDEX_DETACH - Index metadata migration to cold storage is completed. Preparing to detach the warm index state from the local cluster.
- RUNNING_INDEX_DETACH - Local warm index state from the cluster is being removed. Upon success, the migration request will be completed.
- FAILED_INDEX_DETACH - The index detach process failed and all retries are exhausted.

### Automating migrations to cold storage

You can use Index State Management (p. 238) to automate the migration process after an index reaches a certain age or meets other conditions. See the sample policy (p. 240), which demonstrates how to automatically migrate indices from hot to UltraWarm to cold storage.

**Note**

An explicit timestamp_field is required in order to move indices to cold storage using an Index State Management policy.

### Canceling migrations to cold storage

If a migration to cold storage is queued or in a failed state, you can cancel the migration using the following request:

```
POST _ultrawarm/migration/_cancel/my-index
```
If your domain uses fine-grained access control, you need the indices:admin/ultrawarm/migration/cancel permission to make this request.

## Listing cold indices

Before querying, you can list the indices in cold storage to decide which ones to migrate to UltraWarm for further analysis. The following request lists all cold indices, sorted by index name:

```
GET _cold/indices/_search
```

### Filtering

You can filter cold indices based on a prefix-based index pattern and time range offsets.

The following request lists indices that match the prefix pattern of `event-*`:

```
GET _cold/indices/_search
{
    "filters":{
        "index_pattern": "event-***"
    }
}
```

The following request returns indices with `start_time` and `end_time` metadata fields between 2019-03-01 and 2020-03-01:

```
GET _cold/indices/_search
{
    "filters": {
        "time_range": {
            "start_time": "2019-03-01",
            "end_time": "2020-03-01"
        }
    }
}
```

### Sorting

You can sort cold indices by metadata fields such as index name or size. The following request lists all indices sorted by size in descending order:

```
GET _cold/indices/_search
{
    "sort_key": "size:desc"
}
```

Other valid sort keys are `start_time:asc/desc`, `end_time:asc/desc`, and `index_name:asc/desc`.

### Pagination

You can paginate a list of cold indices. Configure the number of indices to be returned per page with the `page_size` parameter (default is 10). Every `_search` request on your cold indices returns a pagination ID which you can use for subsequent calls.

The following request paginates the results of a `_search` request of your cold indices and displays the next 100 results:
Migrating cold indices to warm storage

After you narrow down your list of cold indices with the filtering criteria in the previous section, migrate them back to UltraWarm where you can query the data and use it to create visualizations.

The following request migrates two cold indices back to warm storage:

```
POST _cold/migration/_warm
{
    "indices": "my-index1,my-index2"
}
```

To check the status of the migration and retrieve the migration ID, send the following request:

```
GET _cold/migration/_status
```

To get index-specific migration information, include the index name:

```
GET _cold/migration/my-index/_status
```

Rather than specifying an index, you can list the indices by their current migration status. Valid values are _failed, _accepted, and _all.

The following command gets the status of all indices in a single migration request:

```
GET _cold/migration/_status?migration_id=my-migration-id
```

Retrieve the migration ID using the status request. For detailed migration information, add &verbose=true.

You can migrate indices from cold to warm storage in batches of 10, with a maximum of 100 simultaneous requests. The migration process has the following states:

- ACCEPTED_MIGRATION_REQUEST - Migration request is accepted and queued.
- RUNNING_INDEX_CREATION - Migration request is picked up for processing and will create warm indices in the cluster.
- PENDING_COLD_METADATA_CLEANUP - Warm index is created and the migration service will attempt to clean up cold metadata.
- RUNNING_COLD_METADATA_CLEANUP - Cleaning up cold metadata from the indices migrated to warm storage.
- FAILED_COLD_METADATA_CLEANUP - Failed to clean up metadata in the cold tier.
- FAILED_INDEX_CREATION - Failed to create an index in the warm tier.

Canceling migrations from cold to warm storage

If an index migration from cold to warm storage is queued or in a failed state, you can cancel it with the following request:

```
POST _cold/migration/my-index/_cancel
```
To cancel migration for a batch of indices (maximum of 10 at a time), specify the migration ID:

```
POST _cold/migration/_cancel?migration_id=my-migration-id
```

Retrieve the migration ID using the status request.

**Updating cold index metadata**

You can update the `start_time` and `end_time` fields for a cold index:

```
PATCH _cold/my-index
{
  "start_time": "2020-01-01",
  "end_time": "2020-02-01"
}
```

You can't update the `timestamp_field` of an index in cold storage.

**Note**

Kibana doesn't support the PATCH method. Use `curl`, Postman, or some other method to update cold metadata.

**Deleting cold indices**

If you're not using an ISM policy you can delete cold indices manually. The following request deletes a cold index:

```
DELETE _cold/my-index
```

**Disabling cold storage**

The Amazon ES console is the simplest way to disable cold storage. Select the domain and choose **Edit domain**, then deselect **Enable cold storage**.

To use the AWS CLI or configuration API, under **ColdStorageOptions**, set "Enabled"="false".

Before you disable cold storage, you must either delete all cold indices or migrate them back to warm storage, otherwise the disable action fails.

---

**Index State Management in Amazon Elasticsearch Service**

Index State Management (ISM) lets you define custom management policies to automate routine tasks and apply them to indices and index patterns in Amazon Elasticsearch Service (Amazon ES). You no longer need to set up and manage external processes to run your index operations.

A policy contains a default state and a list of states for the index to transition between. Within each state, you can define a list of actions to perform and conditions that trigger these transitions. A typical use case is to periodically delete old indices after a certain period of time. For example, you can define a policy that moves your index into a `read_only` state after 30 days and then ultimately deletes it after 90 days.
After you attach a policy to an index, ISM creates a job that runs every 30 to 48 minutes to perform policy actions, check conditions, and transition the index into different states. The base time for this job to run is every 30 minutes, plus a random 0-60% jitter is added to it to make sure you do not see a surge of activity from all your indices at the same time.

ISM requires Elasticsearch 6.8 or later. Full documentation for the feature is available in the Open Distro for Elasticsearch documentation.

**Important**
The `policy_id` setting for index templates is deprecated. You can no longer use index templates to apply ISM policies to newly created indices. You can continue to automatically manage newly created indices with the ISM template field. This update introduces a breaking change that affects existing CloudFormation templates using this setting.

**Sample policies**

The following sample policies demonstrate how to automate common ISM use cases.

**Hot to warm storage**

This sample policy moves an index from hot storage to UltraWarm (p. 222) storage after seven days and deletes the index after 90 days.

In this case, an index is initially in the **hot** state. After seven days, ISM moves it to the **warm** state. 83 days later, the service sends a notification to an Amazon Chime room that the index is being deleted and then permanently deletes it.

```json
{
  "policy": {
    "description": "Demonstrate a hot-warm-delete workflow.",
    "default_state": "hot",
    "schema_version": 1,
    "states": [
      {
        "name": "hot",
        "actions": [],
        "transitions": [
          {
            "state_name": "warm",
            "conditions": {
              "min_index_age": "7d"
            }
          }
        ]
      },
      {
        "name": "warm",
        "actions": [
          {
            "warm_migration": {},
            "timeout": "24h",
            "retry": {
              "count": 5,
              "delay": "1h"
            }
          }
        ],
        "transitions": [
          {
            "state_name": "delete",
            "conditions": {
              "min_index_age": "90d"
            }
          }
        ]
      },
      {
        "name": "delete",
        "actions": [
```
Hot to warm to cold storage

This sample policy moves an index from hot storage to UltraWarm, and eventually to cold storage (p. 231).

The index is initially in the hot state. After ten days, ISM moves it to the warm state. 80 days later, it moves the index to the cold state.

```json
{
    "policy": {
        "description": "Demonstrate a hot-warm-cold workflow.",
        "default_state": "hot",
        "schema_version": 1,
        "states": [{
            "name": "hot",
            "actions": [],
            "transitions": [{
                "state_name": "warm",
                "conditions": {
                    "min_index_age": "10d"
                }
            }]
        },
        {
            "name": "warm",
            "actions": [{
                "warm_migration": {},
                "retry": {
                    "count": 5,
                    "delay": "1h"
                }
            }],
            "transitions": [{
                "state_name": "cold",
                "conditions": {
                    "min_index_age": "90d"
                }
            }]
        },
        {
            "name": "cold",
            "actions": []
        }
    }
}
```
"cold_migration": {
    "timestamp_field": "@timestamp"
  }
}

Reduce replica count

This sample policy reduces replica count to zero after seven days to conserve disk space and then deletes the index after 21 days. This policy assumes your index is non-critical and no longer receiving write requests; having zero replicas carries some risk of data loss.

```json
{
  "policy": {
    "description": "Changes replica count and deletes.",
    "schema_version": 1,
    "default_state": "current",
    "states": [{
        "name": "current",
        "actions": [],
        "transitions": [{
            "state_name": "old",
            "conditions": {
                "min_index_age": "7d"
            }
        }]
    }, {
        "name": "old",
        "actions": [{
            "replica_count": {
                "number_of_replicas": 0
            }
        }],
        "transitions": [{
            "state_name": "delete",
            "conditions": {
                "min_index_age": "21d"
            }
        }]
    }, {
        "name": "delete",
        "actions": [{
            "delete": {}
        }],
        "transitions": []
    }]
  }
}
```

Take an index snapshot

This sample policy uses the `snapshot` operation to take a snapshot of an index as soon as it contains at least one document. `repository` is the name of the manual snapshot repository you registered in Amazon S3. `snapshot` is the name of the snapshot. For snapshot prerequisites and steps to register a repository, see the section called “Creating index snapshots” (p. 51).
Attach a policy to an index

After you create a policy, the next step is to attach it to an index or indices:

```json
POST _opendistro/_ism/add/my-index
{
  "policy_id": "my-policy-id"
}
```

Alternatively, select the index in Kibana and choose Apply policy.

**ISM templates**

You can set up an ism_template field in a policy so when you create an index that matches the template pattern, the policy is automatically attached to that index. In this example, any index you create with a name that begins with "log" is automatically matched to the ISM policy `my-policy-id`:

```json
PUT _opendistro/_ism/policies/my-policy-id
{
  "policy": {
    "description": "Example policy.",
    "default_state": "...",
    "states": [...],
    "ism_template": {
      "index_patterns": ["log*"],
      "priority": 100
    }
  }
}
```

For an example ISM template policy, see Sample policy with ISM template.
Differences

Compared to Open Distro for Elasticsearch, ISM for Amazon Elasticsearch Service has several differences.

ISM operations

- Amazon ES supports two unique ISM operations, `warm_migration` and `cold_migration`.

  If your domain has UltraWarm (p. 222) enabled, the `warm_migration` action transitions the index to warm storage. Even if the `warm_migration` action doesn't complete within the set timeout period, the migration to warm indices still continues.

  Setting an `error_notification` for the `warm_migration` action might notify you that the `warm_migration` action failed if it didn't complete within the timeout period. This failed notification is only for your own reference. The actual warm migration operation has no inherent timeout and continues to run until it eventually succeeds or fails.

- If your domain runs Elasticsearch 7.4 or later, Amazon ES supports the ISM `open` and `close` operations.

- If your domain runs Elasticsearch 7.7 or later, Amazon ES supports the ISM `snapshot` operation.

ISM settings

Open Distro for Elasticsearch lets you change all available ISM settings using the `_cluster/settings` API. On Amazon ES, you can only change the following settings:

- **Cluster-level settings:**
  - `enabled`
  - `history.enabled`

- **Index-level settings:**
  - `rollover_alias`

Summarizing indices in Amazon Elasticsearch Service with index rollups

Index rollups in Amazon Elasticsearch Service (Amazon ES) let you reduce storage costs by periodically rolling up old data into summarized indices.

You pick the fields that interest you and use an index rollup to create a new index with only those fields aggregated into coarser time buckets. You can store months or years of historical data at a fraction of the cost with the same query performance.

Index rollups requires Elasticsearch 7.9 or later. Full documentation for the feature is available in the Open Distro for Elasticsearch documentation.

Creating an index rollup job

To get started, choose **Index Management** in Kibana. Select **Rollup Jobs** and choose **Create rollup job**.
Step 1: Set up indices

Set up the source and target indices. The source index is the one that you want to roll up. The target index is where the index rollup results are saved.

After you create an index rollup job, you can't change your index selections.

Step 2: Define aggregations and metrics

Select the attributes with the aggregations (terms and histograms) and metrics (avg, sum, max, min, and value count) that you want to roll up. Make sure you don't add a lot of highly granular attributes, because you won't save much space.

Step 3: Specify schedules

Specify a schedule to roll up your indices as it's being ingested. The index rollup job is enabled by default.

Step 4: Review and create

Review your configuration and select Create.

Step 5: Search the target index

You can use the standard _search API to search the target index. You can't access the internal structure of the data in the target index because the plugin automatically rewrites the query in the background to suit the target index. This is to make sure you can use the same query for the source and target index.

To query the target index, set size to 0:

```json
GET target_index/_search
{
  "size": 0,
  "query": {
    "match_all": {}
  },
  "aggs": {
    "avg_cpu": {
      "avg": {
        "field": "cpu_usage"
      }
    }
  }
}
```

Using Curator to rotate data in Amazon Elasticsearch Service

This section contains sample code for using AWS Lambda and Curator to manage indices and snapshots in Amazon Elasticsearch Service (Amazon ES). Curator offers numerous filters to help you identify indices and snapshots that meet certain criteria, such as indices created more than 60 days ago or snapshots that failed to complete. Index State Management (p. 238) has some similar features and doesn't require Lambda or a separate EC2 instance. Depending on your use case, it might be a better choice.
Although Curator is often used as a command line interface (CLI), it also features a Python API, which means that you can use it within Lambda functions. For installation instructions, see the section called “Using Curator for snapshots” (p. 61).

For information about configuring Lambda functions and creating deployment packages, see the section called “Loading streaming data from Amazon S3” (p. 160). For even more information, see the AWS Lambda Developer Guide. This section contains only sample code, basic settings, triggers, and permissions.

Topics
• Sample code (p. 245)
• Basic settings (p. 247)
• Triggers (p. 248)
• Permissions (p. 248)

Sample code

The following sample code uses Curator and elasticsearch-py to delete any index whose name contains a time stamp indicating that the data is more than 30 days old. For example, if an index name is mylogs-2014.03.02, the index is deleted. Deletion occurs even if you create the index today, because this filter uses the name of the index to determine its age.

The code also contains some commented-out examples of other common filters, including one that determines age by creation date. The AWS SDK for Python (Boto3) and requests-aws4auth library sign the requests to Amazon ES.

Warning
Both code samples in this section delete data—potentially a lot of data. Modify and test each sample on a non-critical domain until you're satisfied with its behavior.

Index Deletion

```python
import boto3
from requests_aws4auth import AWS4Auth
from elasticsearch import Elasticsearch, RequestsHttpConnection
import curator

host = ''  # For example, search-my-domain.region.es.amazonaws.com
region = ''  # For example, us-west-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
session_token=credentials.token)

# Lambda execution starts here.
def lambda_handler(event, context):

    # Build the Elasticsearch client.
es = Elasticsearch(
        hosts = [{'host': host, 'port': 443}],
        http_auth = awsauth,
        use_ssl = True,
        verify_certs = True,
        connection_class = RequestsHttpConnection)

    # A test document.
document = {
        "title": "Moneyball",
        "director": "Bennett Miller",
    }
```
"year": "2011"
}

# Index the test document so that we have an index that matches the timestring pattern.
# You can delete this line and the test document if you already created some test indices.
es.index(index="movies-2017.01.31", doc_type="movie", id="1", body=document)

index_list = curator.IndexList(es)

# Filters by age, anything with a time stamp older than 30 days in the index name.
index_list.filter_by_age(source='name', direction='older', timestring='%Y.%m.%d',
unit='days', unit_count=30)

# Filters by naming prefix.
# index_list.filter_by_regex(kind='prefix', value='my-logs-2017')

# Filters by age, anything created more than one month ago.
# index_list.filter_by_age(source='creation_date', direction='older', unit='months',
#unit_count=1)

print("Found %s indices to delete" % len(index_list.indices))

if index_list.indices:
curator.DeleteIndices(index_list).do_action()

You must update the values for host and region.

The next code sample deletes any snapshot that is more than two weeks old. It also takes a new snapshot.

**Snapshot Deletion**

```python
import boto3
from datetime import datetime
from requests_aws4auth import AWS4Auth
from elasticsearch import Elasticsearch, RequestsHttpConnection
import logging
import curator

# Adding a logger isn't strictly required, but helps with understanding Curator's requests
# and debugging.
logger = logging.getLogger('curator')
logger.addHandler(logging.StreamHandler())
logger.setLevel(logging.INFO)

host = '' # For example, search-my-domain.region.es.amazonaws.com
region = '' # For example, us-west-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
session_token=credentials.token)
repository_name = 'my-repo'

# Lambda execution starts here.
def lambda_handler(event, context):
    now = datetime.now()
    date_string = '-'.join((str(now.year), str(now.month), str(now.day), str(now.hour), str(now.minute)))
    snapshot_name = 'my-snapshot-prefix-' + date_string
```
# Build the Elasticsearch client.
es = Elasticsearch(
    hosts = [{'host': host, 'port': 443}],
    http_auth = awsauth,
    use_ssl = True,
    verify_certs = True,
    connection_class = RequestsHttpConnection,
    timeout = 120  # Deleting snapshots can take a while, so keep the connection open
                 # for long enough to get a response.
)

try:
    # Get all snapshots in the repository.
    snapshot_list = curator.SnapshotList(es, repository=repository_name)

    # Filter by age, any snapshot older than two weeks.
    snapshot_list.filter_by_age(source='creation_date', direction='older',
                                unit='weeks', unit_count=2)

    # Delete the old snapshots.
    curator.DeleteSnapshots(snapshot_list, retry_interval=30,
                            retry_count=3).do_action()
    except (curator.exceptions.SnapshotInProgress, curator.exceptions.NoSnapshots,
            curator.exceptions.FailedExecution) as e:
        print(e)

    # Split into two try blocks. We still want to try and take a snapshot if deletion
    # failed.
    try:
        # Get the list of indices.
        # You can filter this list if you didn't want to snapshot all indices.
        index_list = curator.IndexList(es)

        # Take a new snapshot. This operation can take a while, so we don't want to wait
        # for it to complete.
        curator.Snapshot(index_list, repository=repository_name, name=snapshot_name,
                         wait_for_completion=False).do_action()
        except (curator.exceptions.SnapshotInProgress, curator.exceptions.FailedExecution) as e:
            print(e)

You must update the values for host, region, snapshot_name, and repository_name. If the output
is too verbose for your taste, you can change logging.INFO to logging.WARN.

Because taking and deleting snapshots can take a while, this code is more sensitive to connection
and Lambda timeouts—hence the extra logging code. In the Elasticsearch client, you can see that we set
the timeout to 120 seconds. If the DeleteSnapshots function takes longer to get a response from the
Amazon ES domain, you might need to increase this value. You must also increase the Lambda function
timeout from its default value of three seconds. For a recommended value, see the section called "Basic
settings" (p. 247).

## Basic settings

We recommend the following settings for these code samples.

<table>
<thead>
<tr>
<th>Sample Code</th>
<th>Memory</th>
<th>Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index Deletion</td>
<td>128 MB</td>
<td>10 seconds</td>
</tr>
<tr>
<td>Snapshot Deletion</td>
<td>128 MB</td>
<td>3 minutes</td>
</tr>
</tbody>
</table>
Triggers

Rather than reacting to some event (such as a file upload to Amazon S3), these functions are meant to be scheduled. You might prefer to run these functions more or less frequently.

<table>
<thead>
<tr>
<th>Sample Code</th>
<th>Service</th>
<th>Rule Type</th>
<th>Example Expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index Deletion</td>
<td>CloudWatch Events</td>
<td>Schedule expression</td>
<td>rate(1 day)</td>
</tr>
<tr>
<td>Snapshot Deletion</td>
<td>CloudWatch Events</td>
<td>Schedule expression</td>
<td>rate(4 hours)</td>
</tr>
</tbody>
</table>

Permissions

Both Lambda functions in this section need the basic logging permissions that all Lambda functions need, plus HTTP method permissions for the Amazon ES domain:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "logs:CreateLogGroup",
            "Resource": "arn:aws:logs:us-west-1:123456789012:*"
        },
        {
            "Effect": "Allow",
            "Action": ["logs:CreateLogStream", "logs:PutLogEvents"],
        },
        {
            "Effect": "Allow",
        }
    ]
}
```

Migrating Amazon Elasticsearch Service indices using remote reindex

Remote reindex lets you copy indices from a remote Amazon Elasticsearch Service (Amazon ES) cluster to a local one. You can migrate indices from any Amazon ES domains or self-managed Elasticsearch clusters.
Remote reindexing requires Elasticsearch 6.7 or later on the local domain. The remote domain must be lower or the same major version as the local domain. Within the same major version, the remote domain can be any minor version. For example, remote reindexing from 7.10.x to 7.9 is supported, but 7.x to 6.x isn’t supported.

Full documentation for the reindex operation, including detailed steps and supported options, is available in the Open Distro for Elasticsearch documentation.

Topics
- Prerequisites (p. 249)
- Reindex data between Amazon ES domains (p. 249)
- Reindex data between non-Amazon ES domains (p. 250)
- Reindex large datasets (p. 251)
- Remote reindex settings (p. 252)

Prerequisites
Remote reindex has the following requirements:

- The remote domain must be accessible from the local domain. For a remote domain that resides within a VPC, the local domain must have access to the VPC. This process varies by network configuration, but likely involves connecting to a VPN or managed network or using a proxy server. To learn more, see VPC Support (p. 22).
- The request must be authorized by the remote domain like any other REST request. If the remote domain is an FGAC-enabled Amazon ES domain, you must have permission to perform reindex on the local domain and read the index on the remote domain. For more security considerations, see Fine-Grained Access Control (p. 90).
- We recommend you create an index with the desired setting on your local domain before you start the reindex process.

Reindex data between Amazon ES domains
The most basic scenario is that the remote index is in the same region as your local domain with a publicly accessible endpoint and you have signed IAM credentials.

Specify the source index in the remote domain that you want to reindex from and the destination index on your local domain that you want to reindex to:

```
POST <local-domain-endpoint>/reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443"
    },
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```

You must add 443 at the end of the remote domain endpoint for a validation check.

To verify that the index is copied over to the local domain:
GET `<local-domain-endpoint>/local_index/_search`

If the remote index is in a region different from your local domain, pass in its region name, such as in this sample request:

```
POST <local-domain-endpoint>/_reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443",
      "region": "eu-west-1"
    },
    "index": "test_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```

In case of isolated regions like AWS GovCloud (US) or China regions, the endpoint might not be accessible because your IAM user is not recognized in those regions.

If the remote domain is secured with basic authorization, specify the username and password:

```
POST <local-domain-endpoint>/_reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443",
      "username": "username",
      "password": "password"
    },
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```

If the remote domain is hosted inside a VPC and it does not have VPC-level connectivity, configure a proxy with a publicly accessible endpoint. The proxy domain must have a certificate signed by a public certificate authority (CA). Self-signed or private CA-signed certificates are not supported.

**Reindex data between non-Amazon ES domains**

If the remote index is hosted outside of Amazon ES, like in a self-managed EC2 instance, specify `external` parameter as `true`:

```
POST <local-domain-endpoint>/_reindex
{
  "source": {
    "remote": {
      "host": "https://remote_endpoint:443",
      "username": "username",
      "password": "password",
      "external": true
    },
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```
Reindex large datasets

Remote reindex sends a scroll request to the remote domain with the following default values:

- Search context of 5 minutes
- Socket timeout of 30 seconds
- Batch size of 1,000

We recommend tuning these parameters to accommodate your data. For large documents, consider a smaller batch size and/or longer timeout. For more information, see Scroll search.

POST <local-domain-endpoint>/_reindex?pretty=true&scroll=10h&wait_for_completion=false
{
  "source": {
    "remote": {
      "host": "https://remote_endpoint:443",
      "socket_timeout": "60m"
    },
    "size": 100,
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}

We also recommend adding the following settings to the local index for better performance:

PUT local_index
{
  "settings": {
    "refresh_interval": -1,
    "number_of_replicas": 0
  }
}

After the reindex process is complete, you can set your desired replica count and remove the refresh interval setting.

To reindex only a subset of documents that you select through a query:

POST <local-domain-endpoint>/_reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443"
    },
    "index": "remote_index",
    "query": {
      "query": "query to select documents"
Remote reindex settings

In addition to the standard reindexing options, Amazon ES supports the following options:

<table>
<thead>
<tr>
<th>Options</th>
<th>Valid values</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>external</td>
<td>Boolean</td>
<td>If remote domain is not an Amazon ES domain, specify as true.</td>
<td>No</td>
</tr>
<tr>
<td>region</td>
<td>String</td>
<td>If remote domain is in a different region, specify the region name.</td>
<td>No</td>
</tr>
</tbody>
</table>
Monitoring data in Amazon Elasticsearch Service

Proactively monitor your data in Amazon Elasticsearch Service (Amazon ES) with alerting and anomaly detection. Set up alerts to receive notifications when your data exceeds certain thresholds. Anomaly detection uses machine learning to automatically detect any outliers in your streaming data. You can pair anomaly detection with alerting to ensure you're notified as soon as an anomaly is detected.

Topics
- Configuring alerts in Amazon Elasticsearch Service (p. 253)
- Anomaly detection in Amazon Elasticsearch Service (p. 255)
- Trace Analytics for Amazon Elasticsearch Service (p. 258)

Configuring alerts in Amazon Elasticsearch Service

Configure alerts in Amazon Elasticsearch Service (Amazon ES) to get notified when data from one or more indices meets certain conditions. For example, you might want to receive an email if your application logs more than five HTTP 503 errors in one hour, or you might want to page a developer if no new documents have been indexed in the last 20 minutes.

Alerting requires Elasticsearch version 6.2 or later. For full documentation, including API descriptions, see the Open Distro for Elasticsearch documentation. This topic highlights the differences in alerting in (Amazon ES) compared to the open-source version.

To get started with alerting
1. Choose Alerting from the Kibana main menu.
2. Set up a destination for the alert. Choose between Slack, Amazon Chime, a custom webhook, or Amazon SNS. As you might imagine, notifications require connectivity to the destination. For example, your Amazon ES domain must be able to connect to the internet to notify a Slack channel or send a custom webhook to a third-party server. The Amazon ES domain must have a public IP address to send alerts to a custom webhook.
3. Create a monitor in one of three ways: visually, using a query, or using an anomaly detector.
4. Define a condition to trigger the monitor.
5. (Optional) Add one or more actions to the monitor.

Tip
After an action successfully sends a message, securing access to that message (for example, access to a Slack channel) is your responsibility. If your domain contains sensitive data, consider using triggers without actions and periodically checking Kibana for alerts.

For detailed steps, see Monitors in the Open Distro for Elasticsearch documentation.

Differences

Compared to Open Distro for Elasticsearch, alerting in Amazon ES has some notable differences.
Amazon ES supports Amazon Simple Notification Service (Amazon SNS) for notifications. This integration means that in addition to standard destinations (Slack, custom webhooks, and Amazon Chime), you can also send emails, text messages, and even run AWS Lambda functions using SNS topics. For more information about Amazon SNS, see the Amazon Simple Notification Service Developer Guide.

**To add Amazon SNS as a destination**

1. Choose **Alerting** from the Kibana main menu.
2. Go to the **Destinations** tab and then choose **Add destination**.
3. Provide a unique name for the destination.
4. For **Type**, choose **Amazon SNS**.
5. Provide the SNS topic ARN.
6. Provide the ARN for an IAM role within your account that has the following trust relationship and permissions (at minimum):

   ```json
   {
     "Version": "2012-10-17",
     "Statement": [{
       "Effect": "Allow",
       "Principal": {
         "Service": "es.amazonaws.com"
       },
       "Action": "sts:AssumeRole"
     }]
   }
   
   {
     "Version": "2012-10-17",
     "Statement": [{
       "Effect": "Allow",
       "Action": "sns:Publish",
       "Resource": "sns-topic-arn"
     }]
   }
   
   For more information, see Adding IAM Identity Permissions in the IAM User Guide.
7. Choose **Create**.

**Alerting settings**

Amazon ES lets you modify the following alerting settings:

- `opendistro.scheduled_jobs.enabled`
- `opendistro.alerting.alert_history_enabled`
- `opendistro.alerting.alert_history_max_age`
- `opendistro.alerting.alert_history_max_docs`
- `opendistro.alerting.alert_history_retention_period`
- `opendistro.alerting.alert_history_rollover_period`
- `opendistro.alerting.filter_by_backend_roles`

All other settings use the default values which you can’t change.
To disable alerting, send the following request:

```json
PUT _cluster/settings
{
   "persistent" : {
      "opendistro.scheduled_jobs.enabled" : false
   }
}
```

The following request configures alerting to automatically delete history indices after seven days, rather than the default 30 days:

```json
PUT _cluster/settings
{
   "persistent": {
      "opendistro.alerting.alert_history_retention_period": "7d"
   }
}
```

If you previously created monitors and want to stop the creation of daily alerting indices, delete all alert history indices:

```bash
DELETE .opendistro-alerting-alert-history-*
```

To reduce shard count for history indices, create an index template. The following request sets history indices for both alerting and Index State Management (p. 238) to one shard and one replica:

```json
PUT _template/template-name
{
   "index_patterns": [".opendistro-alerting-alert-history-*", ".opendistro-ism-managed-index-history-*"],
   "template": {
      "settings": {
         "number_of_shards": 1,
         "number_of_replicas": 1
      }
   }
}
```

Depending on your tolerance for data loss, you might even consider using zero replicas. For more information about creating and managing index templates, see Index template in the Open Distro for Elasticsearch documentation.

### Alerting permissions

Alerting supports fine-grained access control (p. 90). For details on mixing and matching permissions to fit your use case, see Alerting security in the Open Distro for Elasticsearch documentation.

### Anomaly detection in Amazon Elasticsearch Service

Anomaly detection in Amazon Elasticsearch Service (Amazon ES) automatically detects anomalies in your Elasticsearch data in near-real time by using the Random Cut Forest (RCF) algorithm. RCF is an
unsupervised machine learning algorithm that models a sketch of your incoming data stream. The algorithm computes an anomaly grade and confidence score value for each incoming data point. Anomaly detection uses these values to differentiate an anomaly from normal variations in your data.

You can pair the anomaly detection plugin with the section called “Alerting” (p. 253) plugin to notify you as soon as an anomaly is detected.

Anomaly detection requires Elasticsearch 7.4 or later. All instance types support anomaly detection except for t2.micro and t2.small. Full documentation for anomaly detection, including detailed steps and API descriptions, is available in the Open Distro for Elasticsearch documentation.

Getting started with anomaly detection

To get started, choose Anomaly Detection in Kibana.

Step 1: Create a detector

A detector is an individual anomaly detection task. You can create multiple detectors, and all the detectors can run simultaneously, with each analyzing data from different sources.

Step 2: Add features to your detector

A feature is the field in your index that you check for anomalies. A detector can discover anomalies across one or more features. You must choose one of the following aggregations for each feature: average(), sum(), count(), min(), or max().

Note
The count() aggregation method is only available in Elasticsearch version 7.7 and later. For version 7.4, use a custom expression like the following:

```
{
   "aggregation_name": {
      "value_count": {
         "field": "field_name"
      }
   }
}
```

The aggregation method determines what constitutes an anomaly. For example, if you choose min(), the detector focuses on finding anomalies based on the minimum values of your feature. If you choose average(), the detector finds anomalies based on the average values of your feature. You can add a maximum of five features per detector.

You can configure the following optional settings (available in 7.7 and later):

- **Category field** - Categorize or slice your data with a dimension like IP address, product ID, country code, and so on.
- **Window size** - Set the number of aggregation intervals from your data stream to consider in a detection window.

After you set up your features, preview sample anomalies and adjust the feature settings if necessary.
Step 3: Observe the results

Anomaly detection / Detectors / cpu_ad

Live anomalies
View anomaly results during the last 60 intervals (60 minutes).

Anomaly history

Choose a filled rectangle in the heat map for a more detailed view.
• **Live anomalies** - displays the live anomaly results for the last 60 intervals. For example, if the interval is set to 10, it shows the results for the last 600 minutes. This chart refreshes every 30 seconds.

• **Anomaly history** - plots the anomaly grade with the corresponding measure of confidence.

• **Feature breakdown** - plots the features based on the aggregation method. You can vary the date-time range of the detector.

• **Anomaly occurrence** - shows the **Start time**, **End time**, **Data confidence**, and **Anomaly grade** for each anomaly detected.

If you set the category field, you see an additional **Heat map** chart that correlates results for anomalous entities. Choose a filled rectangle to see a more detailed view of the anomaly.

### Step 4: Set up alerts

To create a monitor to send you notifications when any anomalies are detected, choose **Set up alerts**. The plugin redirects you to the **Add monitor** page where you can configure an alert.

---

**Trace Analytics for Amazon Elasticsearch Service**

The default installation of Kibana for Amazon Elasticsearch Service (Amazon ES) includes the Trace Analytics plugin, which you can use to analyze trace data from distributed applications. The plugin requires Elasticsearch 7.9 or later.

In a distributed application, a single operation, such as a user clicking a button, can trigger an extended series of events. For example, the application front end might call a backend service, which calls another service, which queries a database, which processes the query and returns a result. Then the first backend service sends a confirmation to the front end, which updates the UI.

You can use Trace Analytics to help you visualize this flow of events and identify performance problems.
Prerequisites

Trace Analytics requires you to add instrumentation to your application and generate trace data using an OpenTelemetry-supported library such as Jaeger or Zipkin. This step occurs entirely outside of Amazon ES. The AWS Distro for OpenTelemetry documentation contains example applications for many programming languages that can help you get started, including Java, Python, Go, and JavaScript.

After you add instrumentation to your application, the OpenTelemetry Collector receives data from the application and formats it into OpenTelemetry data. See the list of receivers on GitHub. AWS Distro for OpenTelemetry includes a receiver for AWS X-Ray.

Finally, Data Prepper, an independent Open Distro for Elasticsearch component, formats that OpenTelemetry data for use with Elasticsearch. Data Prepper runs on a machine outside of the Amazon ES cluster, similar to Logstash.

For a Docker Compose file that demonstrates the end-to-end flow of data, see the Open Distro for Elasticsearch documentation.

OpenTelemetry Collector sample configuration

To use the OpenTelemetry Collector with Data Prepper, try the following sample configuration:

```yaml
receivers:
  jaeger:
    protocols:
      grpc:
  otlp:
    protocols:
      grpc:
  zipkin:

exporters:
  otlp/data-prepper:
    endpoint: data-prepper-host:21890
    insecure: true

service:
  pipelines:
    traces:
      receivers: [jaeger, otlp, zipkin]
      exporters: [otlp/data-prepper]
```

Data Prepper sample configuration

To send trace data to an Amazon ES domain, try the following sample configuration files.

data-prepper-config.yaml

```yaml
ssl: true
keyStoreFilePath: "/usr/share/data-prepper/keystore.jks" # required if ssl is true
keyStorePassword: "password" # optional, defaults to empty string
privateKeyPassword: "other_password" # optional, defaults to empty string
serverPort: 4900 # port for administrative endpoints, default is 4900
```

pipelines.yaml

```yaml
entry-pipeline:
```
# Workers is the number of application threads.  
# Try setting this value to the number of CPU cores on the machine.  
# We recommend the same number of workers for all pipelines.  
workers: 4  
delay: "100" # milliseconds  
source:  
  otel_trace_source:  
    ssl: true  
    sslKeyCertChainFile: "config/demo-data-prepper.crt"  
    sslKeyFile: "config/demo-data-prepper.key"  
buffer:  
  bounded_blocking:  
    # Buffer size is the number of export requests to hold in memory.  
    # We recommend the same value for all pipelines.  
    # Batch size is the maximum number of requests each worker thread processes within  
    the delay.  
    # Keep buffer size >= number of workers * batch size.  
    buffer_size: 1024  
    batch_size: 256  
sink:  
  - pipeline:  
      name: "raw-pipeline"  
  - pipeline:  
      name: "service-map-pipeline"  
raw-pipeline:  
  workers: 4  
  # We recommend the default delay for the raw pipeline.  
  delay: "3000"  
source:  
  pipeline:  
    name: "entry-pipeline"  
prepper:  
  - otel_trace_raw_prepper:  
buffer:  
  bounded_blocking:  
    buffer_size: 1024  
    batch_size: 256  
sink:  
  - elasticsearch:  
    hosts: ["https://domain-endpoint"]  
    # # Basic authentication  
    # username: "ta-user"  
    # password: "ta-password"  
    # IAM signing  
    aws_sigv4: true  
    aws_region: "us-east-1"  
    trace_analytics_raw: true  
service-map-pipeline:  
  workers: 4  
  delay: "100"  
source:  
  pipeline:  
    name: "entry-pipeline"  
prepper:  
  - service_map_stateful:  
buffer:  
  bounded_blocking:  
    buffer_size: 1024  
    batch_size: 256  
sink:  
  - elasticsearch:  
    hosts: ["https://domain-endpoint"]  
    # # Basic authentication  
    # username: "ta-user"  
    # password: "ta-password"  
    # IAM signing
For IAM signing, run `aws configure` using the AWS CLI to set your credentials.

If you use fine-grained access control (p. 90) with the internal user database, use the basic authentication lines instead.

If your domain uses fine-grained access control, you must map the Data Prepper user or role to the all_access role (p. 106).

If your domain doesn't use fine-grained access control, the Data Prepper user or role must have write permissions to several indices and templates, along with permissions to access an Index State Management (ISM) policy and retrieve cluster settings. The following policy shows the required permissions:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/data-prepper-sink-user"
            },
            "Action": "es:ESHttp*",
            "Resource": [
                "arn:aws:es:us-east-1:123456789012:domain/domain-name/otel-v1*",
                "arn:aws:es:us-east-1:123456789012:domain/domain-name/_template/otel-v1*",
                "arn:aws:es:us-east-1:123456789012:domain/domain-name/_alias/otel-v1*"
            ]
        },
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/data-prepper-sink-user"
            },
            "Action": "es:ESHttpGet",
            "Resource": "arn:aws:us-east-1:123456789012:domain/domain-name/_cluster/settings"
        }
    ]
}
```

Data Prepper uses port 21890 to receive data, and it must be able to connect to both the OpenTelemetry Collector and the Elasticsearch cluster. For performance tuning, adjust the worker count and buffer settings in your configuration file, along with the Java virtual machine (JVM) heap size for the machine.

Full documentation for Data Prepper is available in the Open Distro for Elasticsearch documentation. For convenience, we also provide an AWS CloudFormation template that installs Data Prepper on an Amazon EC2 instance.

## Exploring trace data

The **Dashboard** view groups traces together by HTTP method and path so that you can see the average latency, error rate, and trends associated with a particular operation. For a more focused view, try filtering by trace group name.
To drill down on the traces that make up a trace group, choose the number of traces in the right-hand column. Then choose an individual trace for a detailed summary.

The **Services** view lists all services in the application, plus an interactive map that shows how the various services connect to each other. In contrast to the dashboard (which helps identify problems by operation), the service map helps you identify problems by service. Try sorting by error rate or latency to get a sense of potential problem areas of your application.
Best practices for Amazon Elasticsearch Service

This chapter addresses some best practices for operating Amazon Elasticsearch Service (Amazon ES) domains and provides general guidelines that apply to many use cases. Production domains should adhere to the following standards:

- Apply a restrictive resource-based access policy (p. 77) to the domain (or enable fine-grained access control), and follow the principle of least privilege when granting access to the configuration API and the Elasticsearch APIs.
- Configure at least one replica, the Elasticsearch default, for each index.
- Use three dedicated master nodes (p. 268).
- Deploy the domain across three Availability Zones (p. 19). This configuration lets Amazon ES distribute replica shards to different Availability Zones than their corresponding primary shards.
- Upgrade to the latest Elasticsearch versions (p. 61) as they become available on Amazon Elasticsearch Service.
- Update to the latest service software (p. 16) as it becomes available.
- Size the domain appropriately for your workload. For storage volume, shard size, and data node recommendations, see the section called “Sizing domains” (p. 263) and the section called “Petabyte scale” (p. 267). For dedicated master node recommendations, see the section called “Dedicated master nodes” (p. 268).
- Have no more than 1,000 shards on any data node. This limit is the default in Elasticsearch 7.x and later. For a more nuanced guideline, see the section called “Choosing the number of shards” (p. 265).
- Use the latest-generation instances available on the service. For example, use I3 instances rather than I2 instances.
- Don’t use T2 or t3.small instances for production domains; they can become unstable under sustained heavy load. t3.medium instances are an option for small production workloads (both as data nodes and dedicated master nodes).
- If appropriate for your network configuration, create the domain within a VPC (p. 22).
- If your domain stores sensitive data, enable encryption of data at rest (p. 74) and node-to-node encryption (p. 76).

For more information, see the remaining topics in this chapter.

Topics
- Sizing Amazon Elasticsearch Service domains (p. 263)
- Petabyte scale for Amazon Elasticsearch Service (p. 267)
- Dedicated master nodes in Amazon Elasticsearch Service (p. 268)
- Recommended CloudWatch alarms for Amazon Elasticsearch Service (p. 270)

Sizing Amazon Elasticsearch Service domains

No surefire method of sizing Amazon Elasticsearch Service (Amazon ES) domains exists, but by starting with an understanding of your storage needs, the service, and Elasticsearch itself, you can make an
educated initial estimate on your hardware needs. This estimate can serve as a useful starting point for
the most critical aspect of sizing domains: testing them with representative workloads and monitoring
their performance.

Topics
• Calculating storage requirements (p. 264)
• Choosing the number of shards (p. 265)
• Choosing instance types and testing (p. 266)

Calculating storage requirements

Most Elasticsearch workloads fall into one of two broad categories:

• Long-lived index: You write code that processes data into one or more Elasticsearch indices and then
updates those indices periodically as the source data changes. Some common examples are website,
document, and e-commerce search.

• Rolling indices: Data continuously flows into a set of temporary indices, with an indexing period
and retention window, such as a set of daily indices that is retained for two weeks. Some common
examples are log analytics, time-series processing, and clickstream analytics.

For long-lived index workloads, you can examine the source data on disk and easily determine how much
storage space it consumes. If the data comes from multiple sources, just add those sources together.

For rolling indices, you can multiply the amount of data generated during a representative time period
by the retention period. For example, if you generate 200 MiB of log data per hour, that's 4.7 GiB per day,
which is 66 GiB of data at any given time if you have a two-week retention period.

The size of your source data, however, is just one aspect of your storage requirements. You also have to
consider the following:

1. Number of replicas: Each replica is a full copy of an index and needs the same amount of disk space.
   By default, each Elasticsearch index has one replica. We recommend at least one to prevent data
   loss. Replicas also improve search performance, so you might want more if you have a read-heavy
   workload.

2. Elasticsearch indexing overhead: The on-disk size of an index varies, but is often 10% larger than the
   source data. After indexing your data, you can use the _cat/indices?v API and pri.store.size
   value to calculate the exact overhead. _cat/allocation?v also provides a useful summary.

3. Operating system reserved space: By default, Linux reserves 5% of the file system for the root user
   for critical processes, system recovery, and to safeguard against disk fragmentation problems.

4. Amazon ES overhead: Amazon ES reserves 20% of the storage space of each instance (up to 20 GiB)
   for segment merges, logs, and other internal operations.

   Because of this 20 GiB maximum, the total amount of reserved space can vary dramatically
   depending on the number of instances in your domain. For example, a domain might have three
   m6g.xlarge.elasticsearch instances, each with 500 GiB of storage space, for a total of
   1.46 TiB. In this case, the total reserved space is only 60 GiB. Another domain might have 10
   m3.medium.elasticsearch instances, each with 100 GiB of storage space, for a total of 0.98 TiB.
   Here, the total reserved space is 200 GiB, even though the first domain is 50% larger.

   In the following formula, we apply a "worst-case" estimate for overhead that includes additional free
   space to help minimize the impact of node failures and Availability Zone outages.

In summary, if you have 66 GiB of data at any given time and want one replica, your minimum storage
requirement is closer to $66 \times 2 \times 1.1 / 0.95 / 0.8 = 191$ GiB. You can generalize this calculation as follows:
Choosing the number of shards

After you understand your storage requirements, you can investigate your indexing strategy. By default in Amazon ES, each index is divided into five primary shards and one replica (total of 10 shards). Because you can't easily change the number of primary shards for an existing index, you should decide about shard count before indexing your first document.

The overarching goal of choosing a number of shards is to distribute an index evenly across all data nodes in the cluster. However, these shards shouldn't be too large or too numerous. A good rule of thumb is to try to keep shard size between 10–50 GiB. Large shards can make it difficult for Elasticsearch to recover from failure, but because each shard uses some amount of CPU and memory, having too many small shards can cause performance issues and out of memory errors. In other words, shards should be small enough that the underlying Amazon ES instance can handle them, but not so small that they place needless strain on the hardware.

For example, suppose you have 66 GiB of data. You don't expect that number to increase over time, and you want to keep your shards around 30 GiB each. Your number of shards therefore should be approximately 66 * 1.1 / 30 = 3. You can generalize this calculation as follows:

\[(\text{Source Data} + \text{Room to Grow}) \times (1 + \text{Indexing Overhead}) / \text{Desired Shard Size} = \text{Approximate Number of Primary Shards}\]

This equation helps compensate for data growth over time. If you expect those same 66 GiB of data to quadruple over the next year, the approximate number of shards is \((66 + 198) \times 1.1 / 30 \approx 10\). Remember, though, you don't have those extra 198 GiB of data yet. Check to make sure that this preparation for the future doesn't create unnecessarily tiny shards that consume huge amounts of CPU and memory in the present. In this case, \(66 \times 1.1 / 10\) shards = 7.26 GiB per shard, which will consume extra resources and is below the recommended size range. You might consider the more middle-of-the-road approach of six shards, which leaves you with 12 GiB shards today and 48 GiB shards in the future. Then again, you might prefer to start with three shards and reindex your data when the shards exceed 50 GiB.

A far less common issue involves limiting the number of shards per node. If you size your shards appropriately, you typically run out of disk space long before encountering this limit. For example, an \texttt{m6g.large.elasticsearch} instance has a maximum disk size of 512 GiB. If you stay below 80% disk usage and size your shards at 20 GiB, it can accommodate approximately 20 shards. Elasticsearch 7.x and later have a limit of 1,000 shards per node, adjustable using the \texttt{cluster.max.shards.per.node} setting.

Sizing shards appropriately almost always keeps you below this limit, but you can also consider the number of shards for each GiB of Java heap. On a given node, have no more than 20 shards per GiB of Java heap. For example, an \texttt{m5.large.elasticsearch} instance has a 4 GiB heap, so each node should...
have no more than 80 shards. At that shard count, each shard is roughly 5 GiB in size, which is well below our recommendation.

Choosing instance types and testing

After you calculate your storage requirements and choose the number of shards that you need, you can start to make hardware decisions. Hardware requirements vary dramatically by workload, but we can still offer some basic recommendations.

In general, the storage limits (p. 295) for each instance type map to the amount of CPU and memory that you might need for light workloads. For example, an m6g.large.elasticsearch instance has a maximum EBS volume size of 512 GiB, 2 vCPU cores, and 8 GiB of memory. If your cluster has many shards, performs taxing aggregations, updates documents frequently, or processes a large number of queries, those resources might be insufficient for your needs. If you believe your cluster falls into one of these categories, try starting with a configuration closer to 2 vCPU cores and 8 GiB of memory for every 100 GiB of your storage requirement.

Tip
For a summary of the hardware resources that are allocated to each instance type, see Amazon Elasticsearch Service Pricing.

Still, even those resources might be insufficient. Some Elasticsearch users report that they need many times those resources to fulfill their requirements. Finding the right hardware for your workload means making an educated initial estimate, testing with representative workloads, adjusting, and testing again:

Step 1: Make an initial estimate

To start, we recommend a minimum of three nodes to avoid potential Elasticsearch issues, such as split brain (when a lapse in communication leads to a cluster having two master nodes). If you have three dedicated master nodes (p. 268), we still recommend a minimum of two data nodes for replication.

Step 2: Calculate storage requirements per node

If you have a 184 GiB storage requirement and the recommended minimum number of three nodes, use the equation $184 \div 3 = 61$ GiB to find the amount of storage that each node needs. In this example, you might select three m6g.large.elasticsearch instances, each using a 90 GiB EBS storage volume so that you have a safety net and some room for growth over time. This configuration provides 6 vCPU cores and 24 GiB of memory, so it's suited to lighter workloads.

For a more substantial example, consider a 14 TiB (14,336 GiB) storage requirement and a heavy workload. In this case, you might choose to begin testing with $2 \times 144 = 288$ vCPU cores and $8 \times 144 = 1152$ GiB of memory. These numbers work out to approximately 18 i3.4xlarge.elasticsearch instances. If you don't need the fast, local storage, you could also test 18 r6g.4xlarge.elasticsearch instances, each using a 1 TiB EBS storage volume.

If your cluster includes hundreds of terabytes of data, see the section called “Petabyte scale” (p. 267).

Step 3: Perform representative testing

After configuring the cluster, you can add your indices (p. 158) using the number of shards you calculated earlier, perform some representative client testing using a realistic dataset, and monitor CloudWatch metrics (p. 28) to see how the cluster handles the workload.

Step 4: Succeed or iterate

If performance satisfies your needs, tests succeed, and CloudWatch metrics are normal, the cluster is ready to use. Remember to set CloudWatch alarms (p. 270) to detect unhealthy resource usage.
If performance isn't acceptable, tests fail, or CPUUtilization or JVMMemoryPressure are high, you might need to choose a different instance type (or add instances) and continue testing. As you add instances, Elasticsearch automatically rebalances the distribution of shards throughout the cluster.

Because it is easier to measure the excess capacity in an overpowered cluster than the deficit in an underpowered one, we recommend starting with a larger cluster than you think you need. Next, test and scale down to an efficient cluster that has the extra resources to ensure stable operations during periods of increased activity.

Production clusters or clusters with complex states benefit from dedicated master nodes (p. 268), which improve performance and cluster reliability.

Petabyte scale for Amazon Elasticsearch Service

Amazon Elasticsearch Service (Amazon ES) domains offer attached storage of up to 3 PB. You can configure a domain with 200 i3.16xlarge.elasticsearch instance types, each with 15 TB of storage. Because of the sheer difference in scale, recommendations for domains of this size differ from our general recommendations (p. 263). This section discusses considerations for creating domains, costs, storage, and shard size.

While this section frequently references the i3.16xlarge.elasticsearch instance types, you can use several other instance types to reach 1 PB of total domain storage.

Creating domains

Domains of this size exceed the default limit of 40 instances per domain. To request a service limit increase of up to 200 instances per domain, open a case at the AWS Support Center.

Pricing

Before creating a domain of this size, check the Amazon Elasticsearch Service Pricing page to ensure that the associated costs match your expectations. Examine the section called “UltraWarm storage” (p. 222) to see if a hot-warm architecture fits your use case.

Storage

The i3 instance types are designed to provide fast, local non-volatile memory express (NVMe) storage. Because this local storage tends to offer performance benefits when compared to Amazon Elastic Block Store, EBS volumes are not an option when you select these instance types in Amazon ES. If you prefer EBS storage, use another instance type, such as r5.12xlarge.elasticsearch.

Shard size and count

A common Elasticsearch guideline is not to exceed 50 GB per shard. Given the number of shards necessary to accommodate large domains and the resources available to i3.16xlarge.elasticsearch instances, we recommend a shard size of 100 GB.

For example, if you have 450 TB of source data and want one replica, your minimum storage requirement is closer to 450 TB * 2 * 1.1 / 0.95 = 1.04 PB. For an explanation of this calculation, see the section called “Calculating storage requirements” (p. 264). Although 1.04 PB / 15 TB = 70 instances, you might select 90 or more i3.16xlarge.elasticsearch instances to give yourself a storage safety net, deal with node failures, and account for some variance in the amount of data over time. Each instance adds another 20 GiB to your minimum storage requirement, but for disks of this size, those 20 GiB are almost negligible.

Controlling the number of shards is tricky. Elasticsearch users often rotate indices on a daily basis and retain data for a week or two. In this situation, you might find it useful to distinguish between "active" and "inactive" shards. Active shards are, well, actively being written to or read from. Inactive shards might service some read requests, but are largely idle. In general, you should keep the
number of active shards below a few thousand. As the number of active shards approaches 10,000, considerable performance and stability risks emerge.

To calculate the number of primary shards, use this formula: 450,000 GB * 1.1 / 100 GB per shard = 4,950 shards. Doubling that number to account for replicas is 9,900 shards, which represents a major concern if all shards are active. But if you rotate indices and only 1/7th or 1/14th of the shards are active on any given day (1,414 or 707 shards, respectively), the cluster might work well. As always, the most important step of sizing and configuring your domain is to perform representative client testing using a realistic dataset.

Dedicated master nodes in Amazon Elasticsearch Service

Amazon Elasticsearch Service (Amazon ES) uses dedicated master nodes to increase cluster stability. A dedicated master node performs cluster management tasks, but does not hold data or respond to data upload requests. This offloading of cluster management tasks increases the stability of your domain. Just like all other node types, you pay an hourly rate for each dedicated master node.

We recommend that you add three dedicated master nodes to each production Amazon ES domain. Never choose an even number of dedicated master nodes.

1. One dedicated master node means that you have no backup in the event of a failure.
2. Two dedicated master nodes means that your cluster does not have the necessary quorum of nodes to elect a new master node in the event of a failure.
   
   A quorum is the number of dedicated master nodes / 2 + 1 (rounded down to the nearest whole number), which Amazon ES sets to discovery.zen.minimum_master_nodes when you create your domain.
   
   In this case, 2 / 2 + 1 = 2. Because one dedicated master node has failed and only one backup exists, the cluster doesn't have a quorum and can't elect a new master.
3. Three dedicated master nodes, the recommended number, provides two backup nodes in the event of a master node failure and the necessary quorum (2) to elect a new master.
4. Four dedicated master nodes are no better than three and can cause issues if you use multiple Availability Zones (p. 19).
   
   • If one master node fails, you have the quorum (3) to elect a new master. If two nodes fail, you lose that quorum, just as you do with three dedicated master nodes.
   
   • In a three Availability Zone configuration, two AZs have one dedicated master node, and one AZ has two. If that AZ experiences a disruption, the remaining two AZs don't have the necessary quorum (3) to elect a new master.
5. Having five dedicated master nodes works as well as three and allows you to lose two nodes while maintaining a quorum. But because only one dedicated master node is active at any given time, this configuration means paying for four idle nodes. Many users find this level of failover protection excessive.

If a cluster has an even number of master-eligible nodes, Elasticsearch versions 7.x and later ignore one node so that the voting configuration is always an odd number. In this case, four dedicated master nodes are essentially equivalent to three (and two to one).

**Note**

If your cluster doesn't have the necessary quorum to elect a new master node, write and read requests to the cluster both fail. This behavior differs from the Elasticsearch default.

Dedicated master nodes perform the following cluster management tasks:
• Track all nodes in the cluster
• Track the number of indices in the cluster
• Track the number of shards belonging to each index
• Maintain routing information for nodes in the cluster
• Update the cluster state after state changes, such as creating an index and adding or removing nodes in the cluster
• Replicate changes to the cluster state across all nodes in the cluster
• Monitor the health of all cluster nodes by sending heartbeat signals, periodic signals that monitor the availability of the data nodes in the cluster

The following illustration shows an Amazon ES domain with ten instances. Seven of the instances are data nodes and three are dedicated master nodes. Only one of the dedicated master nodes is active; the two gray dedicated master nodes wait as backup in case the active dedicated master node fails. All data upload requests are served by the seven data nodes, and all cluster management tasks are offloaded to the active dedicated master node.

Although dedicated master nodes don't process search and query requests, their size is highly correlated with the number of instances, indices, and shards that they can manage. For production clusters, we recommend the following instance types for dedicated master nodes. These recommendations are based on typical workloads and can vary based on your needs. Clusters with many shards or field mappings can benefit from larger instance types. Monitor the dedicated master node metrics (p. 270) to see if you need to use a larger instance type.
### Recommended CloudWatch alarms for Amazon Elasticsearch Service

CloudWatch alarms perform an action when a CloudWatch metric exceeds a specified value for some amount of time. For example, you might want AWS to email you if your cluster health status is red for longer than one minute. This section includes some recommended alarms for Amazon Elasticsearch Service (Amazon ES) and how to respond to them.

For more information about setting alarms, see Creating Amazon CloudWatch Alarms in the Amazon CloudWatch User Guide.

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Issue</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ClusterStatus.red</code> maximum is &gt;= 1 for 1 minute, 1 consecutive time</td>
<td>At least one primary shard and its replicas are not allocated to a node. See the section called “Red cluster status” (p. 329).</td>
</tr>
<tr>
<td><code>ClusterStatus.yellow</code> maximum is &gt;= 1 for 1 minute, 1 consecutive time</td>
<td>At least one replica shard is not allocated to a node. See the section called “Yellow cluster status” (p. 331).</td>
</tr>
<tr>
<td><code>FreeStorageSpace</code> minimum is &lt;= 20480 for 1 minute, 1 consecutive time</td>
<td>A node in your cluster is down to 20 GiB of free storage space. See the section called “Lack of available storage space” (p. 331). This value is in MiB, so rather than 20480, we recommend setting it to 25% of the storage space for each node.</td>
</tr>
<tr>
<td><code>ClusterIndexWritesBlocked</code> is &gt;= 1 for 5 minutes, 1 consecutive time</td>
<td>Your cluster is blocking write requests. See the section called “ClusterBlockException” (p. 331).</td>
</tr>
<tr>
<td>Alarm</td>
<td>Issue</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Nodes minimum is ( &lt; x ) for 1 day, 1 consecutive time</td>
<td>( x ) is the number of nodes in your cluster. This alarm indicates that at least one node in your cluster has been unreachable for one day. See the section called “Failed cluster nodes” (p. 332).</td>
</tr>
</tbody>
</table>
| AutomatedSnapshotFailure maximum is \( \geq 1 \) for 1 minute, 1 consecutive time | An automated snapshot failed. This failure is often the result of a red cluster health status. See the section called “Red cluster status” (p. 329). For a summary of all automated snapshots and some information about failures, try one of the following requests:  

GET `domain_endpoint/_snapshot/cs-automated/_all`  
GET `domain_endpoint/_snapshot/cs-automated-enc/_all` |
| CPUUtilization or WarmCPUUtilization maximum is \( \geq 80\% \) for 15 minutes, 3 consecutive times | 100% CPU utilization isn't uncommon, but *sustained* high usage is problematic. Consider using larger instance types or adding instances. |
| JVMMemoryPressure or WarmJVMMemoryPressure maximum is \( \geq 80\% \) for 5 minutes, 3 consecutive times | The cluster could encounter out of memory errors if usage increases. Consider scaling vertically. Amazon ES uses half of an instance's RAM for the Java heap, up to a heap size of 32 GiB. You can scale instances vertically up to 64 GiB of RAM, at which point you can scale horizontally by adding instances. |
| MasterCPUUtilization maximum is \( \geq 50\% \) for 15 minutes, 3 consecutive times | Consider using larger instance types for your dedicated master nodes (p. 268). Because of their role in cluster stability and blue/green deployments (p. 14), dedicated master nodes should have lower CPU usage than data nodes. |
| MasterJVMMemoryPressure maximum is \( \geq 80\% \) for 15 minutes, 1 consecutive time | Consider using larger instance types for your dedicated master nodes (p. 268). Because of their role in cluster stability and blue/green deployments (p. 14), dedicated master nodes should have lower CPU usage than data nodes. |
| KMSKeyError is \( \geq 1 \) for 1 minute, 1 consecutive time | The KMS encryption key that is used to encrypt data at rest in your domain is disabled. Re-enable it to restore normal operations. For more information, see the section called “Encryption at rest” (p. 74). |
| KMSKeyInaccessible is \( \geq 1 \) for 1 minute, 1 consecutive time | The KMS encryption key that is used to encrypt data at rest in your domain has been deleted or has revoked its grants to Amazon ES. You can't recover domains that are in this state, but if you have a manual snapshot, you can use it to migrate to a new domain. To learn more, see the section called “Encryption at rest” (p. 74). |

**Note**  
If you just want to view metrics, see Monitoring CloudWatch Metrics (p. 28).
General reference for Amazon Elasticsearch Service

Amazon Elasticsearch Service (Amazon ES) supports a variety of instances, operations, plugins, and other resources.

Topics

- Supported instance types in Amazon Elasticsearch Service (p. 272)
- Features by Elasticsearch version (p. 273)
- Plugins by Elasticsearch version (p. 275)
- Supported Elasticsearch operations (p. 277)
- Amazon Elasticsearch Service limits (p. 295)
- Reserved Instances in Amazon Elasticsearch Service (p. 302)
- Other supported resources in Amazon Elasticsearch Service (p. 305)

Supported instance types in Amazon Elasticsearch Service

Amazon Elasticsearch Service (Amazon ES) supports the following instance types. Not all Regions support all instance types. For availability details, see Amazon Elasticsearch Service Pricing.

For information about which instance type is appropriate for your use case, see the section called "Sizing domains" (p. 263), the section called "EBS volume size limits" (p. 296), and the section called "Network limits" (p. 299).

<table>
<thead>
<tr>
<th>Instance Type</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>C4</td>
<td></td>
</tr>
<tr>
<td>C5</td>
<td>The C5 instance types require Elasticsearch version 5.1 or later.</td>
</tr>
<tr>
<td>C6G</td>
<td>The C6G instance types require Elasticsearch version 7.9 or later.</td>
</tr>
<tr>
<td>I2</td>
<td></td>
</tr>
<tr>
<td>I3</td>
<td>The I3 instance types require Elasticsearch version 5.1 or later and do not support EBS storage volumes.</td>
</tr>
<tr>
<td>M3</td>
<td>The M3 instance types do not support encryption of data at rest, fine-grained access control, or cross-cluster search.</td>
</tr>
<tr>
<td></td>
<td>The M3 instance types have additional restrictions by Elasticsearch version. To learn more, see the section called &quot;Invalid M3 instance type&quot; (p. 335).</td>
</tr>
<tr>
<td>M4</td>
<td></td>
</tr>
<tr>
<td>M5</td>
<td>The M5 instance types require Elasticsearch version 5.1 or later.</td>
</tr>
<tr>
<td>M6G</td>
<td>The M6G instance types require Elasticsearch version 7.9 or later.</td>
</tr>
<tr>
<td>Instance Type</td>
<td>Restrictions</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td>R3</td>
<td>The R3 instance types do not support encryption of data at rest or fine-grained access control.</td>
</tr>
<tr>
<td>R4</td>
<td>-</td>
</tr>
<tr>
<td>R5</td>
<td>The R5 instance types require Elasticsearch version 5.1 or later.</td>
</tr>
<tr>
<td>R6G</td>
<td>The R6G instance types require Elasticsearch version 7.9 or later.</td>
</tr>
<tr>
<td>R6GD</td>
<td>The R6GD instance types require Elasticsearch version 7.9 or later and do not support EBS storage volumes.</td>
</tr>
</tbody>
</table>
| T2            | - You can use the T2 instance types only if the instance count for your domain is 10 or fewer.  
- The t2.micro.elasticsearch instance type supports only Elasticsearch 1.5 and 2.3.  
- The T2 instance types do not support encryption of data at rest, fine-grained access control, UltraWarm storage, cold storage, cross-cluster search, or Auto-Tune. |
| T3            | - The T3 instance types require Elasticsearch version 5.6 or later.  
- You can use the t3.small and t3.medium instance types only if the instance count for your domain is 10 or fewer.  
- The T3 instance types do not support UltraWarm storage, cold storage, or Auto-Tune. |

**Tip**
We often recommend different instance types for dedicated master nodes (p. 268) and data nodes.

---

## Features by Elasticsearch version

Many Amazon ES features have a minimum Elasticsearch version requirement. If you meet the minimum Elasticsearch version for a feature, but the feature isn't available on your domain, update your domain's service software (p. 16).

<table>
<thead>
<tr>
<th>Feature</th>
<th>Minimum Required Elasticsearch Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC support</td>
<td>Included on all domains</td>
</tr>
<tr>
<td>Require HTTPS for all traffic to the domain</td>
<td></td>
</tr>
<tr>
<td>Multi-AZ support</td>
<td></td>
</tr>
<tr>
<td>Dedicated master nodes</td>
<td></td>
</tr>
<tr>
<td>Custom packages</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Minimum Required Elasticsearch Version</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>Custom endpoints</td>
<td></td>
</tr>
<tr>
<td>Error and slow logs publishing</td>
<td>5.1</td>
</tr>
<tr>
<td>Curator CLI support</td>
<td></td>
</tr>
<tr>
<td>Encryption of data at rest</td>
<td></td>
</tr>
<tr>
<td>Cognito authentication for Kibana</td>
<td></td>
</tr>
<tr>
<td>In-place Elasticsearch upgrades</td>
<td></td>
</tr>
<tr>
<td>Hourly automated snapshots</td>
<td>5.3</td>
</tr>
<tr>
<td>Node-to-node encryption</td>
<td>6.0</td>
</tr>
<tr>
<td>Java high-level REST client support</td>
<td></td>
</tr>
<tr>
<td>HTTP request and response compression</td>
<td></td>
</tr>
<tr>
<td>Alerting</td>
<td>6.2</td>
</tr>
<tr>
<td>SQL</td>
<td>6.5</td>
</tr>
<tr>
<td>Cross-cluster search</td>
<td>6.7</td>
</tr>
<tr>
<td>Fine-grained access control</td>
<td></td>
</tr>
<tr>
<td>SAML authentication for Kibana</td>
<td></td>
</tr>
<tr>
<td>Auto-Tune</td>
<td></td>
</tr>
<tr>
<td>Remote reindex</td>
<td></td>
</tr>
<tr>
<td>UltraWarm</td>
<td>6.8</td>
</tr>
<tr>
<td>Index State Management</td>
<td>6.8</td>
</tr>
</tbody>
</table>
### Plugins by Elasticsearch version

Amazon Elasticsearch Service (Amazon ES) domains come prepackaged with plugins from the Elasticsearch community. The service automatically deploys and manages plugins for you, but it deploys different plugins depending on the version of Elasticsearch you choose for your domain.

The following table lists plugins by version. It only includes plugins that you might interact with—it’s not comprehensive. Amazon ES uses additional plugins to enable core service functionality, such as the S3 Repository plugin for snapshots and the Open Distro for Elasticsearch Performance Analyzer plugin for optimization and monitoring. For a complete list of all plugins running on your domain, make the following request:

---

<table>
<thead>
<tr>
<th>Feature</th>
<th>Minimum Required Elasticsearch Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>k-NN by Euclidean distance</td>
<td>7.1</td>
</tr>
<tr>
<td>Anomaly Detection</td>
<td>7.4</td>
</tr>
<tr>
<td>k-NN by cosine similarity</td>
<td>7.7</td>
</tr>
<tr>
<td>Learning to Rank</td>
<td></td>
</tr>
<tr>
<td>Piped processing language</td>
<td>7.9</td>
</tr>
<tr>
<td>Kibana reports</td>
<td></td>
</tr>
<tr>
<td>Kibana Trace Analytics</td>
<td></td>
</tr>
<tr>
<td>ARM-based Graviton instances</td>
<td></td>
</tr>
<tr>
<td>Cold storage</td>
<td></td>
</tr>
<tr>
<td>Hamming distance, L1 Norm distance, and Painless scripting for k-NN</td>
<td>7.10</td>
</tr>
<tr>
<td>Asynchronous search</td>
<td></td>
</tr>
</tbody>
</table>

For information about plugins, which enable some of these features and additional functionality, see the section called “Plugins by Elasticsearch version” (p. 275). For information about the Elasticsearch API for each version, see the section called “Supported Elasticsearch operations” (p. 277).
### Plugins by Elasticsearch version

```
GET _cat/plugins?v
```

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Minimum Required Elasticsearch Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICU Analysis</td>
<td>Included on all domains</td>
</tr>
<tr>
<td>Japanese (kuromoji) Analysis</td>
<td></td>
</tr>
<tr>
<td>Phonetic Analysis</td>
<td>2.3</td>
</tr>
<tr>
<td>Seunjeon Korean Analysis</td>
<td>5.1</td>
</tr>
<tr>
<td>Smart Chinese Analysis</td>
<td></td>
</tr>
<tr>
<td>Stempel Polish Analysis</td>
<td></td>
</tr>
<tr>
<td>Ingest Attachment Processor</td>
<td></td>
</tr>
<tr>
<td>Ingest User Agent Processor</td>
<td></td>
</tr>
<tr>
<td>Mapper Murmur3</td>
<td></td>
</tr>
<tr>
<td>Mapper Size</td>
<td>5.3</td>
</tr>
<tr>
<td>Ukrainian Analysis</td>
<td></td>
</tr>
<tr>
<td>Open Distro for Elasticsearch slering (p. 253)</td>
<td>6.2</td>
</tr>
<tr>
<td>Open Distro for Elasticsearch SQL (p. 183)</td>
<td>6.5</td>
</tr>
<tr>
<td>Open Distro for Elasticsearch security (p. 90)</td>
<td>6.7</td>
</tr>
<tr>
<td>Open Distro for Elasticsearch Index State Management (p. 238)</td>
<td>6.8</td>
</tr>
<tr>
<td>Open Distro for Elasticsearch k-NN (p. 186)</td>
<td>7.1</td>
</tr>
</tbody>
</table>
Supported Elasticsearch operations

Amazon ES supports many versions of Elasticsearch. The following topics show the operations that Amazon ES supports for each version.

Topics

- Notable API differences (p. 278)
- Version 7.10 (p. 279)
- Version 7.9 (p. 280)
- Version 7.8 (p. 281)
- Version 7.7 (p. 282)
- Version 7.4 (p. 283)
- Version 7.1 (p. 284)
- Version 6.8 (p. 285)
- Version 6.7 (p. 286)
- Version 6.5 (p. 287)
- Version 6.4 (p. 287)
- Version 6.3 (p. 288)
- Version 6.2 (p. 289)
- Version 6.0 (p. 290)
- Version 5.6 (p. 291)
- Version 5.5 (p. 291)
- Version 5.3 (p. 292)
- Version 5.1 (p. 293)
- Version 2.3 (p. 294)
Notable API differences

Index templates

Elasticsearch switched from _template to _index_template in version 7.8. At present, Amazon ES supports only the older _template path.

Settings and statistics

Amazon ES only accepts PUT requests to the _cluster/settings API that use the "flat" settings form. It rejects requests that use the expanded settings form.

```java
// Accepted
PUT _cluster/settings
{
   "persistent": {
      "action.auto_create_index": false
   }
}

// Rejected
PUT _cluster/settings
{
   "persistent": {
      "action": {
         "auto_create_index": false
      }
   }
}
```

The high-level Java REST client uses the expanded form, so if you need to send settings requests, use the low-level client.

Prior to Elasticsearch 5.3, the _cluster/settings API on Amazon ES domains supported only the HTTP PUT method, not the GET method. Later versions support the GET method, as shown in the following example:

```bash
GET https://domain.region.es.amazonaws.com/_cluster/settings?pretty
```

Here is a return example:

```json
{
   "persistent": {
      "cluster": {
         "routing": {
            "allocation": {
               "cluster_concurrent_rebalance": "2",
               "node_concurrent_recoveries": "2",
               "disk": {
                  "watermark": {
                     "low": "1.35gb",
                     "flood_stage": "0.45gb",
                     "high": "0.9gb"
                  }
               }
            }
         }
      }
   }
}```
If you compare responses from an open source Elasticsearch cluster and Amazon ES for certain settings and statistics APIs, you might notice missing fields. Amazon ES redacts certain information that exposes service internals, such as the file system data path from _nodes/stats or the operating system name and version from _nodes.

**Shrink**

The _shrink API can cause upgrades, configuration changes, and domain deletions to fail. We don't recommend using it on domains that run Elasticsearch versions 5.3 or 5.1. These versions have a bug that can cause snapshot restoration of shrunken indices to fail.

If you use the _shrink API on other Elasticsearch versions, make the following request before starting the shrink operation:

```plaintext
PUT https://domain.region.es.amazonaws.com/source-index/_settings
{
  "settings": {
    "index.routing.allocation.require._name": "name-of-the-node-to-shrink-to",
    "index.blocks.read_only": true
  }
}
```

Then make the following requests after completing the shrink operation:

```plaintext
PUT https://domain.region.es.amazonaws.com/source-index/_settings
{
  "settings": {
    "index.routing.allocation.require._name": null,
    "index.blocks.read_only": false
  }
}

PUT https://domain.region.es.amazonaws.com/shrunken-index/_settings
{
  "settings": {
    "index.routing.allocation.require._name": null,
    "index.blocks.read_only": false
  }
}
```

**Version 7.10**

For Elasticsearch 7.10, Amazon ES supports the following operations.

- All operations in the index path (such as `/index-name/`
- `/delete_by_query`
- `/_refresh`
For Elasticsearch 7.9, Amazon ES supports the following operations.

<table>
<thead>
<tr>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>• All operations in the index path (such as /index-name/_forcemerge,</td>
</tr>
<tr>
<td>/index-name/update/id, and /index-name/_close)</td>
</tr>
<tr>
<td>• /_delete_by_query¹</td>
</tr>
<tr>
<td>• /_explain</td>
</tr>
<tr>
<td>• /_field_caps</td>
</tr>
<tr>
<td>• /_field_stats</td>
</tr>
<tr>
<td>• /_flush</td>
</tr>
<tr>
<td>• /_ingest/pipeline</td>
</tr>
<tr>
<td>• /_ltr</td>
</tr>
<tr>
<td>• /_mapping</td>
</tr>
<tr>
<td>• /_mget</td>
</tr>
<tr>
<td>• /_msearch</td>
</tr>
<tr>
<td>• /_mtermvectors</td>
</tr>
<tr>
<td>• /_nodes</td>
</tr>
<tr>
<td>• /_opendistro/_alerting</td>
</tr>
<tr>
<td>• /_opendistro/_anomaly_detection</td>
</tr>
<tr>
<td>• /_opendistro/_ism</td>
</tr>
<tr>
<td>• /_opendistro/_ppl</td>
</tr>
<tr>
<td>• /_opendistro/Security</td>
</tr>
<tr>
<td>• /_opendistro/_sql</td>
</tr>
<tr>
<td>• /_percolate</td>
</tr>
<tr>
<td>• /_plugin/kibana</td>
</tr>
<tr>
<td>• /_rank_eval</td>
</tr>
<tr>
<td>• /_reindex¹</td>
</tr>
<tr>
<td>• /_refresh</td>
</tr>
<tr>
<td>• /_render</td>
</tr>
<tr>
<td>• /_resolve/index</td>
</tr>
<tr>
<td>• /_rollover</td>
</tr>
<tr>
<td>• /_scripts³</td>
</tr>
<tr>
<td>• /_search²</td>
</tr>
<tr>
<td>• /_search_profile</td>
</tr>
<tr>
<td>• /_shard_stores</td>
</tr>
<tr>
<td>• /_shrink⁵</td>
</tr>
<tr>
<td>• /_snapshot</td>
</tr>
<tr>
<td>• /_split</td>
</tr>
<tr>
<td>• /_stats</td>
</tr>
<tr>
<td>• /_status</td>
</tr>
<tr>
<td>• /_tasks</td>
</tr>
<tr>
<td>• /_template</td>
</tr>
<tr>
<td>• /_update_by_query¹</td>
</tr>
<tr>
<td>• /_validate</td>
</tr>
</tbody>
</table>

1. Cluster configuration changes might interrupt these operations before completion. We recommend that you use the /_tasks operation along with these operations to verify that the requests completed successfully.

2. DELETE requests to /_search/scroll with a message body must specify "Content-Length" in the HTTP header. Most clients add this header by default. To avoid a problem with = characters in scroll_id values, use the request body, not the query string, to pass scroll_id values to Amazon ES.

3. For considerations about using scripts, see the section called “Other supported resources” (p. 305).

4. Refers to the PUT method. For information about the GET method, see the section called “Notable API differences” (p. 278).

5. See the section called “Shrink” (p. 279).

Version 7.9

For Elasticsearch 7.9, Amazon ES supports the following operations.
For Elasticsearch 7.8, Amazon ES supports the following operations.

- All operations in the index path (such as /index-name/_forcemerge, /index-name/update/id, and /index-name/_close)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat(except /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings for several properties:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count

Amazon Elasticsearch Service Developer Guide

Version 7.8

1. Cluster configuration changes might interrupt these operations before completion. We recommend that you use the /_tasks operation along with these operations to verify that the requests completed successfully.

2. DELETE requests to /_search/scroll with a message body must specify "Content-Length" in the HTTP header. Most clients add this header by default. To avoid a problem with = characters in scroll_id values, use the request body, not the query string, to pass scroll_id values to Amazon ES.

3. For considerations about using scripts, see the section called “Other supported resources” (p. 305).

4. Refers to the PUT method. For information about the GET method, see the section called “Notable API differences” (p. 278).

5. See the section called “Shrink” (p. 279).
### Version 7.7

For Elasticsearch 7.7, Amazon ES supports the following operations:

<table>
<thead>
<tr>
<th>Operations</th>
<th>Operations</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>• /_bulk</td>
<td>• /_ingest/pipeline</td>
<td>• /_shrink(^5)</td>
</tr>
<tr>
<td>• /_cat (except /_cat/nodeattrs)</td>
<td>• /_ltr</td>
<td>• /_snapshot</td>
</tr>
<tr>
<td>• /_cluster/allocation/explain</td>
<td>• /_mapping</td>
<td>• /_split</td>
</tr>
<tr>
<td>• /_cluster/health</td>
<td>• /_mget</td>
<td>• /_stats</td>
</tr>
<tr>
<td>• /_cluster/pending_tasks</td>
<td>• /_msearch</td>
<td>• /_status</td>
</tr>
<tr>
<td>• /_cluster/settings for several properties(^4):</td>
<td>• /_mtermvectors</td>
<td>• /_tasks</td>
</tr>
<tr>
<td>• action.auto_create_index</td>
<td>• /_nodes</td>
<td>• /_template</td>
</tr>
<tr>
<td>• action.search.shard_count.limit</td>
<td>• /_opendistro/alerting</td>
<td>• /_update_by_query(^1)</td>
</tr>
<tr>
<td>• indices.breaker.fielddata.limit</td>
<td>• /_opendistro/ism</td>
<td>• /_validate</td>
</tr>
<tr>
<td>• indices.breaker.request.limit/indices.breaker.total.limit</td>
<td>• /_opendistro/security</td>
<td></td>
</tr>
<tr>
<td>• cluster.max_shards_per_node</td>
<td>• /_opendistro/_sql</td>
<td></td>
</tr>
<tr>
<td>• /_alias</td>
<td>• /_percolate</td>
<td></td>
</tr>
<tr>
<td>• /_aliases</td>
<td>• /_plugin/kibana</td>
<td></td>
</tr>
<tr>
<td>• /all</td>
<td>• /_rank_eval</td>
<td></td>
</tr>
<tr>
<td>• /_analyze</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• /_bulk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• /_cat (except /_cat/nodeattrs)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• /_cluster/allocation/explain</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Cluster configuration changes might interrupt these operations before completion. We recommend that you use the /_tasks operation along with these operations to verify that the requests completed successfully.

2. DELETE requests to /_search/scroll with a message body must specify "Content-Length" in the HTTP header. Most clients add this header by default. To avoid a problem with = characters in scroll_id values, use the request body, not the query string, to pass scroll_id values to Amazon ES.

3. For considerations about using scripts, see the section called “Other supported resources” (p. 305).

4. Refers to the PUT method. For information about the GET method, see the section called “Notable API differences” (p. 278).

5. See the section called “Shrink” (p. 279).
### Version 7.4

For Elasticsearch 7.4, Amazon ES supports the following operations.

<table>
<thead>
<tr>
<th>/_cluster/health</th>
<th>/msearch</th>
<th>/status</th>
</tr>
</thead>
<tbody>
<tr>
<td>/_cluster/pending_tasks</td>
<td>/_mtermvectors</td>
<td>/_tasks</td>
</tr>
<tr>
<td>/_cluster/settings for several properties 4:</td>
<td>/_nodes</td>
<td>/_template</td>
</tr>
</tbody>
</table>
| action.auto_create_index | /openjestro/
| action.search.shard_count.limit | _alerting |
| indices.breaker.fielddata.limit | /openjestro/
| indices.breaker.request.limit | _anomaly_detection |
| indices.breaker.total.limit 5 | /openjestro/
| cluster.max_shards_per_node | _ism |
| /_msearch | /_refresh |
| /_mtermvectors | /_reindex 1 |
| /_nodes | /_render  |
| /_openjestro/
| _alerting | /_rollover |
| /_opendistro/
| _alerting | /_scripts 3 |
| /_opendistro/
| _anomaly_detection | /_search 2 |
| /_opendistro/
| _ism | /_search_profile |
| /_opendistro/
| _security | /_shard_stores |
| /_opendistro/
| _sql | /_shrink 5 |
| /_percolate | /_snapshot |
| /_plugin/kibana | /_split |
| /_rank_eval | /_stats |

1. Cluster configuration changes might interrupt these operations before completion. We recommend that you use the /_tasks operation along with these operations to verify that the requests completed successfully.

2. DELETE requests to /_search/scroll with a message body must specify "Content-Length" in the HTTP header. Most clients add this header by default. To avoid a problem with = characters in scroll_id values, use the request body, not the query string, to pass scroll_id values to Amazon ES.

3. For considerations about using scripts, see the section called “Other supported resources” (p. 305).

4. Refers to the PUT method. For information about the GET method, see the section called “Notable API differences” (p. 278).

5. See the section called “Shrink” (p. 279).
1. Cluster configuration changes might interrupt these operations before completion. We recommend that you use the `_tasks` operation along with these operations to verify that the requests completed successfully.

2. DELETE requests to `/search/scroll` with a message body must specify "Content-Length" in the HTTP header. Most clients add this header by default. To avoid a problem with `=` characters in `scroll_id` values, use the request body, not the query string, to pass `scroll_id` values to Amazon ES.

3. For considerations about using scripts, see the section called “Other supported resources” (p. 305).

4. Refers to the `PUT` method. For information about the `GET` method, see the section called “Notable API differences” (p. 278).

5. See the section called “Shrink” (p. 279).

### Version 7.1

For Elasticsearch 7.1, Amazon ES supports the following operations.
• indices.breaker.total.limit
• cluster.max_shards_per_node
• _plugin/kibana
• _rank_eval

1. Cluster configuration changes might interrupt these operations before completion. We recommend that you use the /_tasks operation along with these operations to verify that the requests completed successfully.

2. DELETE requests to /_search/scroll with a message body must specify "Content-Length" in the HTTP header. Most clients add this header by default. To avoid a problem with = characters in scroll_id values, use the request body, not the query string, to pass scroll_id values to Amazon ES.

3. For considerations about using scripts, see the section called “Other supported resources” (p. 305).

4. Refers to the PUT method. For information about the GET method, see the section called “Notable API differences” (p. 278).

5. See the section called “Shrink” (p. 279).

### Version 6.8

For Elasticsearch 6.8, Amazon ES supports the following operations.

- All operations in the index path (such as /index-name/_forcemerge and /index-name/update/id) except /index-name/_close
- /_alias
- /_aliases
- /_analyze
- /_bulk
- /_cat (except /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings for several properties:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.blocks.read_only
  - cluster.max_shards_per_node
- /_refresh
- /_reindex
- /_render
- /_rollover
- /_scripts
- /_search
- /_search profile
- /_shard_stores
- /_shrink
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query
- /_validate

1. Cluster configuration changes might interrupt these operations before completion. We recommend that you use the /_tasks operation along with these operations to verify that the requests completed successfully.
For Elasticsearch 6.7, Amazon ES supports the following operations.

- All operations in the index path (such as /index-name/_forcemerge and /index-name/update/id) except /index-name/_close
- /_alias
- /_aliases
- /_analyze
- /_bulk
- /_cat (except /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings for several properties:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.1ft
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_delete_by_query
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_opendistro/alerting
- /_opendistro/_sql
- /_percolate
- /_refresh
- /_reindex
- /_render
- /_rollover
- /_scripts
- /_search
- /_search profile
- /_shard_stores
- /_shrink
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query
- /_validate

1. Cluster configuration changes might interrupt these operations before completion. We recommend that you use the /_tasks operation along with these operations to verify that the requests completed successfully.

2. DELETE requests to /_search/scroll with a message body must specify "Content-Length" in the HTTP header. Most clients add this header by default. To avoid a problem with = characters in scroll_id values, use the request body, not the query string, to pass scroll_id values to Amazon ES.

3. For considerations about using scripts, see the section called “Other supported resources” (p. 305).

4. Refers to the PUT method. For information about the GET method, see the section called “Notable API differences” (p. 278).

5. See the section called “Shrink” (p. 279).
Version 6.5

For Elasticsearch 6.5, Amazon ES supports the following operations.

- All operations in the index path (such as `/index-name/_forcemerge` and `/index-name/update/id`) except `/index-name/_close`
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat (except /_cat/nodeattrs)`
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` for several properties:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`

1. Cluster configuration changes might interrupt these operations before completion. We recommend that you use the `/_tasks` operation along with these operations to verify that the requests completed successfully.

2. DELETE requests to `/_search/scroll` with a message body must specify "Content-Length" in the HTTP header. Most clients add this header by default. To avoid a problem with = characters in `scroll_id` values, use the request body, not the query string, to pass `scroll_id` values to Amazon ES.

3. For considerations about using scripts, see the section called “Other supported resources” (p. 305).

4. Refers to the PUT method. For information about the GET method, see the section called “Notable API differences” (p. 278).

5. See the section called “Shrink” (p. 279).

Version 6.4

For Elasticsearch 6.4, Amazon ES supports the following operations.

- All operations in the index path (such as `/index-name/_forcemerge` and `/index-name/update/id`) except `/index-name/_close`

- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query`
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_opendistro/_sql`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_refresh`
- `/_reindex`
- `/_render`
- `/_rollover`
- `/_scripts`
- `/_search`
- `/_search profile`
- `/_shard_stores`
- `/_shrink`
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query`
- `/_validate`
Cluster configuration changes might interrupt these operations before completion. We recommend that you use the /_tasks operation along with these operations to verify that the requests completed successfully.

2. DELETE requests to /_search/scroll with a message body must specify "Content-Length" in the HTTP header. Most clients add this header by default. To avoid a problem with = characters in scroll_id values, use the request body, not the query string, to pass scroll_id values to Amazon ES.

3. For considerations about using scripts, see the section called “Other supported resources” (p. 305).

4. Refers to the PUT method. For information about the GET method, see the section called “Notable API differences” (p. 278).

5. See the section called “Shrink” (p. 279).

Version 6.3

For Elasticsearch 6.3, Amazon ES supports the following operations.

- All operations in the index path (such as /index-name/_forcemerge and /index-name/update/id) except /index-name/_close
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (except /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/state
- /_cluster/stats
- /_count
- /_delete_by_query
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_merge
- /_mtermvectors
- /_nodes
- /_opendistro/_alerting
- /_percolate
- /_rekister/_plugin/kibana
- /_refresh
- /_reindex
- /_render
- /_rollover
- /_scripts
- /_search
- /_search_profile
- /_shard_stores
- /_shrink
- /_snapshot
- /_split
- /_stats
- /_tasks
- /_template
- /_update_by_query
- /_validate
• /_cluster/health
• /_cluster/pending_tasks
• /_cluster/settings for several properties:
  • action.auto_create_index
  • action.search.shard_count.limit
  • indices.breaker.fielddata.limit
  • indices.breaker.request.limit
  • indices.breaker.total.limit
• /_mtermvectors
• /_nodes
• /_opendistro/alerting
• /_percolate
• /_plugin/kibana
• /_rank_eval
• /_refresh
• /_reindex
• /_render
• /_rollover
• /_scripts
• /_search
• /_search_profile
• /_shardStores
• /_shrink
• /_snapshot
• /_split
• /_stats
• /_tasks
• /_template
• /_update_by_query
• /_validate

1. Cluster configuration changes might interrupt these operations before completion. We recommend that you use the /_tasks operation along with these operations to verify that the requests completed successfully.

2. DELETE requests to /_search/scroll with a message body must specify "Content-Length" in the HTTP header. Most clients add this header by default. To avoid a problem with = characters in scroll_id values, use the request body, not the query string, to pass scroll_id values to Amazon ES.

3. For considerations about using scripts, see the section called “Other supported resources” (p. 305).

4. Refers to the PUT method. For information about the GET method, see the section called “Notable API differences” (p. 278).

5. See the section called “Shrink” (p. 279).

**Version 6.2**

For Elasticsearch 6.2, Amazon ES supports the following operations.

• All operations in the index path (such as /index-name/_forcemerge and /index-name/update/id) except /index-name/_close
• /_alias
• /_aliases
• /_all
• /_analyze
• /_bulk
• /_cat (except /_cat/nodeattrs)
• /_cluster/allocation/explain
• /_cluster/health
• /_cluster/pending_tasks
• /_cluster/settings for several properties:
  • action.auto_create_index
  • action.search.shard_count.limit
  • indices.breaker.fielddata.limit
  • indices.breaker.request.limit
• /_status
• /_tasks
• /_template
• /_update_by_query
• /_validate
1. Cluster configuration changes might interrupt these operations before completion. We recommend that you use the `_tasks` operation along with these operations to verify that the requests completed successfully.

2. DELETE requests to `/search/scroll` with a message body must specify "Content-Length" in the HTTP header. Most clients add this header by default. To avoid a problem with = characters in `scroll_id` values, use the request body, not the query string, to pass `scroll_id` values to Amazon ES.

3. For considerations about using scripts, see the section called “Other supported resources” (p. 305).

4. Refers to the PUT method. For information about the GET method, see the section called “Notable API differences” (p. 278).

5. See the section called “Shrink” (p. 279).

## Version 6.0

For Elasticsearch 6.0, Amazon ES supports the following operations.

<table>
<thead>
<tr>
<th>Operations</th>
<th>Operations</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>• All operations in the index path (such as <code>/index-name/_forcemerge</code> and <code>/index-name/update/id</code>) except <code>/index-name/_close</code></td>
<td>• <code>_cluster/state</code></td>
<td>• <code>/_render</code></td>
</tr>
<tr>
<td>• <code>_alias</code></td>
<td>• <code>_cluster/stats</code></td>
<td>• <code>/_rollover</code></td>
</tr>
<tr>
<td>• <code>_aliases</code></td>
<td>• <code>_count</code></td>
<td>• <code>/_scripts</code></td>
</tr>
<tr>
<td>• <code>_analyze</code></td>
<td>• <code>_delete_by_query</code></td>
<td>• <code>/_search</code></td>
</tr>
<tr>
<td>• <code>_bulk</code></td>
<td>• <code>_explain</code></td>
<td>• <code>/_search_profile</code></td>
</tr>
<tr>
<td>• <code>_cat</code> (except <code>/_cat/nodeattrs</code>)</td>
<td>• <code>_field_caps</code></td>
<td>• <code>/_shard_stores</code></td>
</tr>
<tr>
<td>• <code>_cluster/allocation/</code></td>
<td>• <code>_field_stats</code></td>
<td>• <code>/_shrink</code></td>
</tr>
<tr>
<td>• <code>explain</code></td>
<td>• <code>_flush</code></td>
<td>• <code>/_snapshot</code></td>
</tr>
<tr>
<td>• <code>_cluster/health</code></td>
<td>• <code>_ingest/pipeline</code></td>
<td>• <code>/_stats</code></td>
</tr>
<tr>
<td>• <code>_cluster/pending_tasks</code></td>
<td>• <code>_mapping</code></td>
<td>• <code>/_status</code></td>
</tr>
<tr>
<td>• <code>_cluster/settings for several properties</code>4:</td>
<td>• <code>_mget</code></td>
<td>• <code>/_tasks</code></td>
</tr>
<tr>
<td>• action.auto_create_index</td>
<td>• <code>_msearch</code></td>
<td>• <code>/_template</code></td>
</tr>
<tr>
<td>• action.search.shard_count.limit.reindex`1</td>
<td>• <code>_mtermvectors</code></td>
<td>• <code>/_update_by_query</code></td>
</tr>
<tr>
<td>• indices.breaker.fielddata.limit</td>
<td>• <code>_nodes</code></td>
<td>• <code>/_validate</code></td>
</tr>
<tr>
<td>• indices.breaker.request.limit</td>
<td>• <code>_percolate</code></td>
<td></td>
</tr>
<tr>
<td>• indices.breaker.total.limit</td>
<td>• <code>_plugin/kibana</code></td>
<td></td>
</tr>
<tr>
<td>• /_refresh</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• /_render</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• /_rollover</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• /_scripts3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• /_search2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• /_search profile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• /_shard_stores</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• /_shrink5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• /_snapshot</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• /_stats</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• /_tasks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• /_template</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• /_update_by_query1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• /_validate</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Version 5.6

For Elasticsearch 5.6, Amazon ES supports the following operations.

- All operations in the index path (such as /index-name/_forcemerge and /index-name/update/id) except /index-name/_close
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (except /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings for several properties:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
- /_cluster/state
- /_cluster/stats
- /_count
- /_delete_by_query
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_percolate
- /_plugin/kibana
- /_refresh
- /_reindex
- /_render
- /_rollover
- /_scripts
- /_search
- /_search_profile
- /_shard_stores
- /_shrink
- /_snapshot
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query
- /_validate
- /_render

1. Cluster configuration changes might interrupt these operations before completion. We recommend that you use the /_tasks operation along with these operations to verify that the requests completed successfully.
2. DELETE requests to /_search/scroll with a message body must specify "Content-Length" in the HTTP header. Most clients add this header by default. To avoid a problem with '=' characters in scroll_id values, use the request body, not the query string, to pass scroll_id values to Amazon ES.
3. For considerations about using scripts, see the section called “Other supported resources” (p. 305).
4. Refers to the PUT method. For information about the GET method, see the section called “Notable API differences” (p. 278).
5. See the section called “Shrink" (p. 279).

Version 5.5

For Elasticsearch 5.5, Amazon ES supports the following operations.
1. Cluster configuration changes might interrupt these operations before completion. We recommend that you use the `/_tasks` operation along with these operations to verify that the requests completed successfully.

2. DELETE requests to `/_search/scroll` with a message body must specify "Content-Length" in the HTTP header. Most clients add this header by default. To avoid a problem with `=` characters in `scroll_id` values, use the request body, not the query string, to pass `scroll_id` values to Amazon ES.

3. For considerations about using scripts, see the section called "Other supported resources" (p. 305).

4. Refers to the PUT method. For information about the GET method, see the section called "Notable API differences" (p. 278).

5. See the section called "Shrink" (p. 279).

## Version 5.3

For Elasticsearch 5.3, Amazon ES supports the following operations.
For Elasticsearch 5.1, Amazon ES supports the following operations.

<table>
<thead>
<tr>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>• /_all</td>
</tr>
<tr>
<td>• /analyze</td>
</tr>
<tr>
<td>• /bulk</td>
</tr>
<tr>
<td>• /_cat (except /_cat/nodeattrs)</td>
</tr>
<tr>
<td>• /_cluster/allocation/explain</td>
</tr>
<tr>
<td>• /_cluster/health</td>
</tr>
<tr>
<td>• /_cluster/pending_tasks</td>
</tr>
<tr>
<td>• /_cluster/settings for several properties (PUT only):</td>
</tr>
<tr>
<td>• action.auto_create_index</td>
</tr>
<tr>
<td>• action.search.shard_count.limit</td>
</tr>
<tr>
<td>• indices.breaker.fielddata.limit</td>
</tr>
<tr>
<td>• indices.breaker.request.limit</td>
</tr>
<tr>
<td>• indices.breaker.total.limit</td>
</tr>
<tr>
<td>• /_flush</td>
</tr>
<tr>
<td>• /_ingest/pipeline</td>
</tr>
<tr>
<td>• /_mapping</td>
</tr>
<tr>
<td>• /_mget</td>
</tr>
<tr>
<td>• /_msearch</td>
</tr>
<tr>
<td>• /_mtermvectors</td>
</tr>
<tr>
<td>• /_nodes</td>
</tr>
<tr>
<td>• /_percolate</td>
</tr>
<tr>
<td>• /_plugin/kibana</td>
</tr>
<tr>
<td>• /_refresh</td>
</tr>
<tr>
<td>• /_reindex</td>
</tr>
<tr>
<td>• /_cluster/state</td>
</tr>
<tr>
<td>• /_cluster/stats</td>
</tr>
<tr>
<td>• /_count</td>
</tr>
<tr>
<td>• /_delete_by_query</td>
</tr>
<tr>
<td>• /_explain</td>
</tr>
<tr>
<td>• /_field_caps</td>
</tr>
<tr>
<td>• /_field_stats</td>
</tr>
<tr>
<td>• /_flush</td>
</tr>
<tr>
<td>• /_ingest/pipeline</td>
</tr>
<tr>
<td>• /_mapping</td>
</tr>
<tr>
<td>• /_mget</td>
</tr>
<tr>
<td>• /_msearch</td>
</tr>
<tr>
<td>• /_mtermvectors</td>
</tr>
<tr>
<td>• /_nodes</td>
</tr>
<tr>
<td>• /_percolate</td>
</tr>
<tr>
<td>• /_render</td>
</tr>
<tr>
<td>• /_rollover</td>
</tr>
<tr>
<td>• /_search</td>
</tr>
<tr>
<td>• /_search profile</td>
</tr>
<tr>
<td>• /_shard_stores</td>
</tr>
<tr>
<td>• /_shrink</td>
</tr>
<tr>
<td>• /_snapshot</td>
</tr>
<tr>
<td>• /_stats</td>
</tr>
<tr>
<td>• /_tasks</td>
</tr>
<tr>
<td>• /_template</td>
</tr>
<tr>
<td>• /_update_by_query</td>
</tr>
<tr>
<td>• /_validate</td>
</tr>
</tbody>
</table>

1. Cluster configuration changes might interrupt these operations before completion. We recommend that you use the /_tasks operation along with these operations to verify that the requests completed successfully.

2. DELETE requests to /_search/scroll with a message body must specify "Content-Length" in the HTTP header. Most clients add this header by default. To avoid a problem with = characters in scroll_id values, use the request body, not the query string, to pass scroll_id values to Amazon ES.

3. Refers to the PUT method. For information about the GET method, see the section called “Notable API differences” (p. 278).

4. See the section called “Shrink” (p. 279).
1. Cluster configuration changes might interrupt these operations before completion. We recommend that you use the \_/tasks operation along with these operations to verify that the requests completed successfully.

2. DELETE requests to \_/search/scroll with a message body must specify "Content-Length" in the HTTP header. Most clients add this header by default. To avoid a problem with = characters in scroll_id values, use the request body, not the query string, to pass scroll_id values to Amazon ES.

3. See the section called “Shrink” (p. 279).

**Version 2.3**

For Elasticsearch 2.3, Amazon ES supports the following operations.

- All operations in the index path (such as \/_index-name/_forcemerge and \/_index-name/_recovery) except \/_index-name/_close
- \_/alias
- \_/aliases
- \_/all
- \_/analyze
- \_/bulk
- \_/cache/clear (index only)
- \_/cat (except \_/cat/nodeattrs)
- \_/cluster/health
- \_/cluster/settings for several properties (PUT only):
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - threadpool.get.queue_size
  - threadpool.bulk.queue_size
  - threadpool.index.queue_size
  - threadpool.percolate.queue_size
  - threadpool.search.queue_size
  - threadpool.suggest.queue_size

**Version 1.5**

For Elasticsearch 1.5, Amazon ES supports the following operations.
• All operations in the index path, such as `/index-name/_optimize` and `/index-name/_warmer`, except `/index-name/_close`
  • `/_alias`
  • `/_aliases`
  • `/_all`
  • `/_analyze`
  • `/_bulk`
  • `/_cat`
  • `/_cluster/health`
  • `/_cluster/settings` for several properties (PUT only):
    • `indices.breaker.fielddata.limit`
    • `indices.breaker.request.limit`
    • `indices.breaker.total.limit`
    • `threadpool.get.queue_size`
    • `threadpool.bulk.queue_size`
    • `threadpool.index.queue_size`
    • `threadpool.percolate.queue_size`
    • `threadpool.search.queue_size`
    • `threadpool.suggest.queue_size`
• `/_cluster/stats`
  • `/_count`
  • `/_flush`
  • `/_mapping`
  • `/_mget`
  • `/_msearch`
  • `/_nodes`
  • `/_percolate`
  • `/_plugin/kibana`
  • `/_plugin/kibana3`
  • `/_plugin/migration`
  • `/_refresh`
  • `/_search`
  • `/_snapshot`
  • `/_stats`
  • `/_status`
  • `/_template`

---

## Amazon Elasticsearch Service limits

The following tables show limits for Amazon Elasticsearch Service (Amazon ES) resources, including the number of nodes per cluster, the minimum and maximum sizes for EBS volumes, and network limits.

### Cluster and instance limits

The following table shows Amazon ES limits for clusters and instances.

<table>
<thead>
<tr>
<th>Clusters and Instances</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of data nodes per cluster</td>
<td>40 (except for the T2 and T3 instance types, which have a maximum of 10)</td>
</tr>
</tbody>
</table>
  To request an increase up to 200 data nodes (for Elasticsearch 2.3 or later), create a case with the [AWS Support Center](https://aws.amazon.com/support/). For more information about requesting an increase, see [AWS Service Limits](https://aws.amazon.com/service-quotas/). |
| Maximum number of warm (p. 222) nodes per cluster | 150 |
| Maximum total number of data and warm nodes per cluster | 200 |
  You might have to request a data node limit increase to reach this total. For example, your domain might have 80 data nodes and 120 warm nodes. |
Clusters and Instances | Limit
--- | ---
Maximum number of dedicated master nodes per cluster | 5
You can use the T2 and T3 instance types for dedicated master nodes only if the number of data nodes is 10 or fewer. We don't recommend T2 or t3.small instance types for production domains.
Maximum total storage per cluster | 3 PiB
This maximum is the sum of all data nodes and warm nodes. For example, your domain might have 45 r6gd.16xlarge.elasticsearch instances and 140 ultrawarm1.large.elasticsearch instances for a total of 2.88 PiB of storage.
Smallest supported instance type per Elasticsearch version | t2.micro.elasticsearch (versions 1.5 and 2.3) and t2.small.elasticsearch (version 5.x and 6.x).
Maximum number of domains per account (per Region) | 100
Maximum number of custom packages per account (per Region) | 25
Maximum number of custom packages per domain | 20

For a list of the instance types that Amazon ES supports, see Supported Instance Types (p. 272).

UltraWarm storage limits

The following table lists the UltraWarm instance types and the maximum amount of storage that each type can use. For more information about UltraWarm, see the section called “UltraWarm storage” (p. 222).

<table>
<thead>
<tr>
<th>Instance Type</th>
<th>Maximum Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>ultrawarm1.medium.elasticsearch</td>
<td>1.5 TiB</td>
</tr>
<tr>
<td>ultrawarm1.large.elasticsearch</td>
<td>20 TiB</td>
</tr>
</tbody>
</table>

EBS volume size limits

The following table shows the minimum and maximum sizes for EBS volumes for each instance type that Amazon ES supports. For information about which instance types include instance storage and additional hardware details, see Amazon Elasticsearch Service Pricing.

- If you choose magnetic storage under **EBS volume type** when creating your domain, the maximum volume size is 100 GiB for all instance types except t2.micro, t2.small, t2.medium, and all Graviton instances (M6G, C6G, R6G, and R6GD), which don't support magnetic storage. For the maximum sizes listed in the following table, choose one of the SSD options.
- 512 GiB is the maximum volume size for Elasticsearch version 1.5.
• Some older-generation instance types include instance storage, but also support EBS storage. If you choose EBS storage for one of these instance types, the storage volumes are not additive. You can use either an EBS volume or the instance storage, not both.

<table>
<thead>
<tr>
<th>Instance Type</th>
<th>Minimum EBS Size</th>
<th>Maximum EBS Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>t2.micro.elasticsearch</td>
<td>10 GiB</td>
<td>35 GiB</td>
</tr>
<tr>
<td>t2.small.elasticsearch</td>
<td>10 GiB</td>
<td>35 GiB</td>
</tr>
<tr>
<td>t2.medium.elasticsearch</td>
<td>10 GiB</td>
<td>35 GiB</td>
</tr>
<tr>
<td>t3.small.elasticsearch</td>
<td>10 GiB</td>
<td>100 GiB</td>
</tr>
<tr>
<td>t3.medium.elasticsearch</td>
<td>10 GiB</td>
<td>200 GiB</td>
</tr>
<tr>
<td>m3.medium.elasticsearch</td>
<td>10 GiB</td>
<td>100 GiB</td>
</tr>
<tr>
<td>m3.large.elasticsearch</td>
<td>10 GiB</td>
<td>512 GiB</td>
</tr>
<tr>
<td>m3.xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>512 GiB</td>
</tr>
<tr>
<td>m3.2xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>512 GiB</td>
</tr>
<tr>
<td>m4.large.elasticsearch</td>
<td>10 GiB</td>
<td>512 GiB</td>
</tr>
<tr>
<td>m4.xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>1 TiB</td>
</tr>
<tr>
<td>m4.2xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>1.5 TiB</td>
</tr>
<tr>
<td>m4.4xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>1.5 TiB</td>
</tr>
<tr>
<td>m4.10xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>1.5 TiB</td>
</tr>
<tr>
<td>m5.large.elasticsearch</td>
<td>10 GiB</td>
<td>512 GiB</td>
</tr>
<tr>
<td>m5.xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>1 TiB</td>
</tr>
<tr>
<td>m5.2xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>1.5 TiB</td>
</tr>
<tr>
<td>m5.4xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>3 TiB</td>
</tr>
<tr>
<td>m5.12xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>9 TiB</td>
</tr>
<tr>
<td>m6g.large.elasticsearch</td>
<td>10 GiB</td>
<td>512 GiB</td>
</tr>
<tr>
<td>m6g.xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>1 TiB</td>
</tr>
<tr>
<td>m6g.2xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>1.5 TiB</td>
</tr>
<tr>
<td>m6g.4xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>3 TiB</td>
</tr>
<tr>
<td>m6g.8xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>6 TiB</td>
</tr>
<tr>
<td>m6g.12xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>9 TiB</td>
</tr>
<tr>
<td>c4.large.elasticsearch</td>
<td>10 GiB</td>
<td>100 GiB</td>
</tr>
<tr>
<td>c4.xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>512 GiB</td>
</tr>
<tr>
<td>c4.2xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>1 TiB</td>
</tr>
<tr>
<td>Instance Type</td>
<td>Minimum EBS Size</td>
<td>Maximum EBS Size</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>c4.4xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>1.5 TiB</td>
</tr>
<tr>
<td>c4.8xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>1.5 TiB</td>
</tr>
<tr>
<td>c5.large.elasticsearch</td>
<td>10 GiB</td>
<td>256 GiB</td>
</tr>
<tr>
<td>c5.xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>512 GiB</td>
</tr>
<tr>
<td>c5.2xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>1 TiB</td>
</tr>
<tr>
<td>c5.4xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>1.5 TiB</td>
</tr>
<tr>
<td>c5.9xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>3.5 TiB</td>
</tr>
<tr>
<td>c5.18xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>7 TiB</td>
</tr>
<tr>
<td>c6g.large.elasticsearch</td>
<td>10 GiB</td>
<td>256 GiB</td>
</tr>
<tr>
<td>c6g.xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>512 GiB</td>
</tr>
<tr>
<td>c6g.2xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>1 TiB</td>
</tr>
<tr>
<td>c6g.4xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>1.5 TiB</td>
</tr>
<tr>
<td>c6g.8xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>3 TiB</td>
</tr>
<tr>
<td>c6g.12xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>4.5 TiB</td>
</tr>
<tr>
<td>r3.large.elasticsearch</td>
<td>10 GiB</td>
<td>512 GiB</td>
</tr>
<tr>
<td>r3.xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>512 GiB</td>
</tr>
<tr>
<td>r3.2xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>512 GiB</td>
</tr>
<tr>
<td>r3.4xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>512 GiB</td>
</tr>
<tr>
<td>r3.8xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>512 GiB</td>
</tr>
<tr>
<td>r4.large.elasticsearch</td>
<td>10 GiB</td>
<td>1 TiB</td>
</tr>
<tr>
<td>r4.xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>1.5 TiB</td>
</tr>
<tr>
<td>r4.2xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>1.5 TiB</td>
</tr>
<tr>
<td>r4.4xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>1.5 TiB</td>
</tr>
<tr>
<td>r4.8xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>1.5 TiB</td>
</tr>
<tr>
<td>r4.16xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>1.5 TiB</td>
</tr>
<tr>
<td>r5.large.elasticsearch</td>
<td>10 GiB</td>
<td>1 TiB</td>
</tr>
<tr>
<td>r5.xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>1.5 TiB</td>
</tr>
<tr>
<td>r5.2xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>3 TiB</td>
</tr>
<tr>
<td>r5.4xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>6 TiB</td>
</tr>
<tr>
<td>r5.12xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>12 TiB</td>
</tr>
<tr>
<td>r6g.large.elasticsearch</td>
<td>10 GiB</td>
<td>1 TiB</td>
</tr>
</tbody>
</table>
### Network limits

The following table shows the maximum size of HTTP request payloads.

<table>
<thead>
<tr>
<th>Instance Type</th>
<th>Minimum EBS Size</th>
<th>Maximum EBS Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>r6g.xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>1.5 TiB</td>
</tr>
<tr>
<td>r6g.2xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>3 TiB</td>
</tr>
<tr>
<td>r6g.4xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>6 TiB</td>
</tr>
<tr>
<td>r6g.8xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>8 TiB</td>
</tr>
<tr>
<td>r6g.12xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>12 TiB</td>
</tr>
<tr>
<td>r6gd.large.elasticsearch</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>r6gd.xlarge.elasticsearch</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>r6gd.2xlarge.elasticsearch</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>r6gd.4xlarge.elasticsearch</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>r6gd.8xlarge.elasticsearch</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>r6gd.12xlarge.elasticsearch</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>r6gd.16xlarge.elasticsearch</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>i2.xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>512 GiB</td>
</tr>
<tr>
<td>i2.2xlarge.elasticsearch</td>
<td>10 GiB</td>
<td>512 GiB</td>
</tr>
<tr>
<td>i3.large.elasticsearch</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>i3.xlarge.elasticsearch</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>i3.2xlarge.elasticsearch</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>i3.4xlarge.elasticsearch</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>i3.8xlarge.elasticsearch</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>i3.16xlarge.elasticsearch</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Instance Type</td>
<td>Maximum Size of HTTP Request Payloads</td>
<td></td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------------</td>
<td></td>
</tr>
<tr>
<td>m3.large.elasticsearch</td>
<td>10 MiB</td>
<td></td>
</tr>
<tr>
<td>m3.xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>m3.2xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>m4.large.elasticsearch</td>
<td>10 MiB</td>
<td></td>
</tr>
<tr>
<td>m4.xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>m4.2xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>m4.4xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>m4.10xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>m5.large.elasticsearch</td>
<td>10 MiB</td>
<td></td>
</tr>
<tr>
<td>m5.xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>m5.2xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>m5.4xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>m5.12xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>m6g.large.elasticsearch</td>
<td>10 MiB</td>
<td></td>
</tr>
<tr>
<td>m6g.xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>m6g.2xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>m6g.4xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>m6g.8xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>m6g.12xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>c4.large.elasticsearch</td>
<td>10 MiB</td>
<td></td>
</tr>
<tr>
<td>c4.xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>c4.2xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>c4.4xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>c4.8xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>c5.large.elasticsearch</td>
<td>10 MiB</td>
<td></td>
</tr>
<tr>
<td>c5.xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>c5.2xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>c5.4xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>c5.9xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>c5.18xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>c6g.large.elasticsearch</td>
<td>10 MiB</td>
<td></td>
</tr>
<tr>
<td>Instance Type</td>
<td>Maximum Size of HTTP Request Payloads</td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------</td>
<td></td>
</tr>
<tr>
<td>c6g.xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>c6g.2xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>c6g.4xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>c6g.8xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>c6g.12xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>r3.large.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>r3.xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>r3.2xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>r3.4xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>r3.8xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>r4.large.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>r4.xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>r4.2xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>r4.4xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>r4.8xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>r4.16xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>r5.large.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>r5.xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>r5.2xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>r5.4xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>r5.12xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>r6g.large.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>r6g.xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>r6g.2xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>r6g.4xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>r6g.8xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>r6g.12xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>r6gd.large.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>r6gd.xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>r6gd.2xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
<tr>
<td>r6gd.4xlarge.elasticsearch</td>
<td>100 MiB</td>
<td></td>
</tr>
</tbody>
</table>
Java process limit

Amazon ES limits Java processes to a heap size of 32 GiB. Advanced users can specify the percentage of the heap used for field data. For more information, see the section called “Advanced options” (p. 13) and the section called “JVM OutOfMemoryError” (p. 332).

Domain policy limit

Amazon ES limits access policies on domains (p. 77) to 100 KiB.

Reserved Instances in Amazon Elasticsearch Service

Reserved Instances (RIs) in Amazon Elasticsearch Service (Amazon ES) offer significant discounts compared to standard On-Demand Instances. The instances themselves are identical; RIs are just a billing discount applied to On-Demand Instances in your account. For long-lived applications with predictable usage, RIs can provide considerable savings over time.

Amazon ES RIs require one- or three-year terms and have three payment options that affect the discount rate:

- **No Upfront** – You pay nothing upfront. You pay a discounted hourly rate for every hour within the term.
- **Partial Upfront** – You pay a portion of the cost upfront, and you pay a discounted hourly rate for every hour within the term.
- **All Upfront** – You pay the entirety of the cost upfront. You don't pay an hourly rate for the term.

Generally speaking, a larger upfront payment means a larger discount. You can't cancel Reserved Instances—when you reserve them, you commit to paying for the entire term—and upfront payments are nonrefundable.
RIs are not flexible; they only apply to the exact instance type that you reserve. For example, a reservation for eight c5.2xlarge.elasticsearch instances does not apply to sixteen c5.xlarge.elasticsearch instances or four c5.4xlarge.elasticsearch instances. For full details, see Amazon Elasticsearch Service Pricing and FAQ.

Topics
- Purchasing Reserved Instances (console) (p. 303)
- Purchasing Reserved Instances (AWS CLI) (p. 303)
- Purchasing Reserved Instances (AWS SDKs) (p. 305)
- Examining costs (p. 305)

Purchasing Reserved Instances (console)
The console lets you view your existing Reserved Instances and purchase new ones.

To purchase a reservation
1. Go to https://aws.amazon.com, and then choose Sign In to the Console.
2. Under Analytics, choose Elasticsearch Service.
3. Choose Reserved Instances.
   On this page, you can view your existing reservations. If you have many reservations, you can filter them to more easily identify and view a particular reservation.
   Tip
   If you don’t see the Reserved Instances link, create a domain (p. 9) in the region.
4. Choose Purchase Reserved Instance.
5. For Reservation Name, type a unique, descriptive name.
6. Choose an instance type, size, and number of instances. For guidance, see the section called “Sizing domains” (p. 263).
7. Choose a term length and payment option.
8. Review the payment details carefully.
9. Choose Submit.
10. Review the purchase summary carefully. Purchases of Reserved Instances are non-refundable.
11. Choose Purchase.

Purchasing Reserved Instances (AWS CLI)
The AWS CLI has commands for viewing offerings, purchasing a reservation, and viewing your reservations. The following command and sample response show the offerings for a given AWS Region:

```
aws es describe-reserved-elasticsearch-instance-offerings --region us-east-1
{
    "ReservedElasticsearchInstanceOfferings": [
        {
            "FixedPrice": "x",
            "ReservedElasticsearchInstanceOfferingId": "1a2a3a4a5-1a2a-3a4a-5a6a-1a2a3a4a5a6a",
            "RecurringCharges": [
                {
                    "RecurringChargeAmount": "y",
                    "RecurringChargeFrequency": "Hourly"
                }
            ]
        }
    ]
}
```
For an explanation of each return value, see the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FixedPrice</td>
<td>The upfront cost of the reservation.</td>
</tr>
<tr>
<td>ReservedElasticsearchInstanceOfferingId</td>
<td>The offering ID. Make note of this value if you want to reserve the offering.</td>
</tr>
<tr>
<td>RecurringCharges</td>
<td>The hourly rate for the reservation.</td>
</tr>
<tr>
<td>UsagePrice</td>
<td>A legacy field. For Amazon ES, this value is always 0.</td>
</tr>
<tr>
<td>PaymentOption</td>
<td>No Upfront, Partial Upfront, or All Upfront.</td>
</tr>
<tr>
<td>Duration</td>
<td>Length of the term in seconds:</td>
</tr>
<tr>
<td></td>
<td>• 31536000 seconds is one year.</td>
</tr>
<tr>
<td></td>
<td>• 94608000 seconds is three years.</td>
</tr>
<tr>
<td>ElasticsearchInstanceType</td>
<td>The instance type for the reservation. For information about the hardware resources that are allocated to each instance type, see Amazon Elasticsearch Service Pricing.</td>
</tr>
<tr>
<td>CurrencyCode</td>
<td>The currency for FixedPrice and RecurringChargeAmount.</td>
</tr>
</tbody>
</table>

This next example purchases a reservation:

```bash
aws es purchase-reserved-elasticsearch-instance-offering --reserved-elasticsearch-instance-offering-id 1a2a3a4a5-1a2a-3a4a-5a6a-1a2a3a4a5a6a --reservation-name my-reservation --instance-count 3 --region us-east-1
{
  "ReservationName": "my-reservation",
  "ReservedElasticsearchInstanceId": "9a8a7a6a-5a4a-3a2a-1a0a-9a8a7a6a5a4a"
}
```

Finally, you can list your reservations for a given region using the following example:

```bash
aws es describe-reserved-elasticsearch-instances --region us-east-1
{
  "ReservedElasticsearchInstances": [
  {
    "FixedPrice": 0.0,
    "ReservedElasticsearchInstanceOfferingId": "1a2a3a4a5-1a2a-3a4a-5a6a-1a2a3a4a5a6a",
    "ReservationName": "my-reservation",
    "PaymentOption": "PARTIAL_UPFRONT",
    "UsagePrice": 0.0,
  }
  ]
}
"ReservedElasticsearchInstanceId": "9a8a7a6a-5a4a-3a2a-1a0a-9a8a7a6a5a4a",
"RecurringCharges": [
  {
    "RecurringChargeAmount": y,
    "RecurringChargeFrequency": "Hourly"
  }
],
"State": "payment-pending",
"StartTime": 1522872571.229,
"ElasticsearchInstanceCount": 3,
"Duration": 31536000,
"ElasticsearchInstanceType": "m4.2xlarge.elasticsearch",
"CurrencyCode": "USD"
]
}

**Note**
StartTime is Unix epoch time, which is the number of seconds that have passed since midnight UTC of 1 January 1970. For example, 1522872571 epoch time is 20:09:31 UTC of 4 April 2018. You can use online converters.

To learn more about the commands used in the preceding examples, see the AWS CLI Command Reference.

**Purchasing Reserved Instances (AWS SDKs)**

The AWS SDKs (except the Android and iOS SDKs) support all the operations that are defined in the Amazon ES Configuration API Reference (p. 339), including the following:

- DescribeReservedElasticsearchInstanceOfferings
- PurchaseReservedElasticsearchInstanceOffering
- DescribeReservedElasticsearchInstances

For more information about installing and using the AWS SDKs, see AWS Software Development Kits.

**Examining costs**

Cost Explorer is a free tool that you can use to view your spending data for the past 13 months. Analyzing this data helps you identify trends and understand if RIs fit your use case. If you already have RIs, you can group by Purchase Option and show amortized costs to compare that spending to your spending for On-Demand instances. You can also set usage budgets to make sure you are taking full advantage of your reservations. For more information, see Analyzing Your Costs with Cost Explorer in the AWS Billing and Cost Management User Guide.

**Other supported resources in Amazon Elasticsearch Service**

This topic describes additional resources that Amazon Elasticsearch Service (Amazon ES) supports.

**bootstrap.memory_lock**

Amazon ES enables bootstrap.memory_lock in elasticsearch.yml, which locks JVM memory and prevents the operating system from swapping it to disk. This applies to all supported instance types except for the following:
Other supported resources

- t2.micro.elasticsearch
- t2.small.elasticsearch
- t2.medium.elasticsearch
- t3.small.elasticsearch
- t3.medium.elasticsearch

Scripting module

Amazon ES supports scripting for Elasticsearch 5.x and later domains. It does not support scripting for 1.5 or 2.3.

Supported scripting options include the following:

- Painless
- Lucene Expressions
- Mustache

For Elasticsearch 5.5 and later domains, Amazon ES supports stored scripts using the `_scripts` endpoint. Elasticsearch 5.3 and 5.1 domains support inline scripts only.

TCP transport

Amazon ES supports HTTP on port 80 and HTTPS over port 443, but does not support TCP transport.
Amazon Elasticsearch Service
Tutorials

This chapter includes several start-to-finish tutorials for working with Amazon Elasticsearch Service (Amazon ES), including how to migrate to the service, build a simple search application, and create a Kibana dashboard.

Topics

• Migrating to Amazon Elasticsearch Service (p. 307)
• Creating a search application with Amazon Elasticsearch Service (p. 312)
• Visualizing customer support calls with Amazon Elasticsearch Service and Kibana (p. 318)

Migrating to Amazon Elasticsearch Service

Index snapshots are a popular way to migrate from a self-managed Elasticsearch cluster to Amazon Elasticsearch Service (Amazon ES). Broadly, the process consists of the following steps:

1. Take a snapshot of the existing cluster, and upload the snapshot to an Amazon S3 bucket.
2. Create an Amazon ES domain.
3. Give Amazon ES permissions to access the bucket, and give your user account permissions to work with snapshots.
4. Restore the snapshot on the Amazon ES domain.

This walkthrough provides more detailed steps and alternate options, where applicable.

Take and upload the snapshot

Although you can use the repository-s3 plugin to take snapshots directly to S3, you have to install the plugin on every node, tweak elasticsearch.yml, restart each node, add your AWS credentials, and finally take the snapshot. The plugin is a great option for ongoing use or for migrating larger clusters.

For smaller clusters, a one-time approach is to take a shared file system snapshot and then use the AWS CLI to upload it to S3. If you already have a snapshot, skip to step 4.

To take a snapshot and upload it to Amazon S3

1. Add the path.repo setting to elasticsearch.yml on all nodes, and then restart each node.

   ```
   path.repo: ["/my/shared/directory/snapshots"]
   ```

2. Register the snapshot repository:

   ```
   PUT _snapshot/migration-repository
   ```
"type": "fs",
"settings": {
  "location": "/my/shared/directory/snapshots"
}
}

3. Take the snapshot:

```plaintext
PUT _snapshot/migration-repository/migration-snapshot
{
  "indices": "migration-index1,migration-index2,other-indices-*",
  "include_global_state": false
}
```

4. Install the AWS CLI, and run `aws configure` to add your credentials.

5. Navigate to the snapshot directory. Then run the following commands to create a new S3 bucket and upload the contents of the snapshot directory to that bucket:

```plaintext
aws s3 mb s3://migration-bucket --region us-west-2
aws s3 sync . s3://migration-bucket --sse AES256
```

Depending on the size of the snapshot and the speed of your internet connection, this operation can take a while.

Create a domain

Although the console is the easiest way to create a domain, in this case, you already have the terminal open and the AWS CLI installed. Modify the following command to create a domain that fits your needs:

```plaintext
aws es create-elasticsearch-domain \
  --domain-name migration-domain \
  --elasticsearch-version 7.9 \
  --elasticsearch-cluster-config InstanceType=c5.large.elasticsearch,InstanceCount=2 \
  --ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=100 \
  --encryption-at-rest-options Enabled=true \
  --domain-endpoint-options EnforceHTTPS=true,TLSSecurityPolicy=Policy-Min-TLS-1-2-2019-07 \
  --advanced-security-options Enabled=true,InternalUserDatabaseEnabled=true,MasterUserOptions='{{MasterUserName=master-user,MasterUserPassword=master-user-password}}' \
  --access-policies '{"Version":"2012-10-17","Statement":[{"Effect":"Allow","Principal":{"AWS":[]}},"Action":[]}]}' \
  --region us-west-2
```

As is, the command creates an internet-accessible domain with two data nodes, each with 100 GiB of storage. It also enables fine-grained access control (p. 90) with HTTP basic authentication and all encryption settings. Use the Amazon ES console if you need a more advanced security configuration, such as a VPC.

Before issuing the command, change the domain name, master user credentials, and account number. Specify the same region that you used for the S3 bucket and an Elasticsearch version that is compatible with your snapshot.

**Important**

Snapshots are only forward-compatible, and only by one major version. For example, you can’t restore a snapshot from a 2.x cluster on a 1.x cluster or a 6.x cluster, only a 2.x or 5.x cluster.
Minor version matters, too. You can't restore a snapshot from a self-managed 5.3.3 cluster on a 5.3.2 Amazon ES domain. We recommend choosing the most-recent version of Elasticsearch that your snapshot supports.

Provide permissions to the S3 bucket

In the AWS Identity and Access Management (IAM) console, create a role with the following permissions and trust relationship. Name the role `AmazonESSnapshotRole` so that it's easy to find.

**Permissions**

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "s3:ListBucket"
    ],
    "Effect": "Allow",
    "Resource": [
      "arn:aws:s3:::migration-bucket"
    ],
  },
  { "Action": [
    "s3:GetObject",
    "s3:PutObject",
    "s3:DeleteObject"
  ],
  "Effect": "Allow",
  "Resource": [
    "arn:aws:s3:::migration-bucket/**
  ]
  ]
}
```

**Trust Relationship**

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "Service": "es.amazonaws.com"
    },
    "Action": "sts:AssumeRole"
  }]
}
```

Then give your personal IAM user or role—whatever you used to configure the AWS CLI earlier—permissions to assume `AmazonESSnapshotRole`. Create the following policy and attach it to your identity:

**Permissions**

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": 
```
Then log in to Kibana using the master user credentials you specified when you created the Amazon ES domain. You can find the Kibana URL in the Amazon ES console. It takes the form of https://domain-endpoint/_plugin/kibana/.

From the Kibana main menu, choose Security, Roles, and manage_snapshots. Choose Mapped users, Manage mapping. Then specify the ARN for your personal IAM user or role in the appropriate field. User ARNs go in the Users section. Role ARNs go in the Backend roles section. This step uses fine-grained access control (p. 98) to give your identity permissions to work with snapshots.

Map user

Map users to this role to inherit role permissions. Two types of users are supported: user, and backend role. Learn more

Users

You can create an internal user in internal user database of the security plugin. An internal user can have its own backend role are also supported. Learn more

Users

Create new internal user

Look up by user name. You can also create new internal user or enter external user.

Backend roles

Use a backend role to directly map to roles through an external authentication system. Learn more

Backend roles

Remove

Add another backend role

Restore the snapshot

At this point, you have two ways to access your Amazon ES domain: HTTP basic authentication with your master user credentials or AWS authentication using your IAM credentials. Because snapshots use Amazon S3, which has no concept of the master user, you must use your IAM credentials to register the snapshot repository with your Amazon ES domain.

Most programming languages have libraries to assist with signing requests (p. 143), but the simpler approach is to use a tool like Postman and put your IAM credentials into the Authorization section.
To restore the snapshot

1. Regardless of how you choose to sign your requests, the first step is to register the repository:

   ```
   PUT _snapshot/migration-repository
   {
     "type": "s3",
     "settings": {
       "bucket": "migration-bucket",
       "region": "us-west-2",
       "role_arn": "arn:aws:iam::123456789012:role/AmazonESSnapshotRole"
     }
   }
   ```

2. Then list the snapshots in the repository, and find the one you want to restore. At this point, you can continue using Postman or switch to a tool like `curl`.

   **Shorthand**

   ```
   GET _snapshot/migration-repository/_all
   ```

   ```
   curl
   ```

   ```
   curl -XGET -u 'master-user:master-user-password' https://domain-endpoint/_snapshot/migration-repository/_all
   ```

3. Restore the snapshot.

   **Shorthand**

   ```
   POST _snapshot/migration-repository/migration-snapshot/_restore
   {
     "indices": "migration-index1,migration-index2,other-indices-**",
     "include_global_state": false
   }
   ```

   ```
   curl
   ```

   ```
   curl -XPOST -u 'master-user:master-user-password' https://domain-endpoint/_snapshot/migration-repository/migration-snapshot/_restore \
   -H 'Content-Type: application/json' \
   -d '{"indices":"migration-index1,migration-index2,other-indices-**","include_global_state":false}'
   ```
4. Finally, verify that your indices restored as expected.

**Shorthand**

```
GET _cat/indices?v
```

```
curl
```

```
curl -XGET -u 'master-user:master-user-password' https://domain-endpoint/_cat/indices?v
```

At this point, the migration is complete. You might configure your clients to use the new Amazon ES endpoint, resize the domain (p. 263) to suit your workload, check the shard count for your indices, switch to an IAM master user (p. 95), or start building Kibana dashboards.

**Creating a search application with Amazon Elasticsearch Service**

A common way to create a search application with Amazon Elasticsearch Service (Amazon ES) is to use web forms to send user queries to a server. Then you can authorize the server to call the Elasticsearch APIs directly and have the server send requests to Amazon ES.

If you want to write client-side code that doesn't rely on a server, however, you should compensate for the security and performance risks. Allowing unsigned, public access to the Elasticsearch APIs is inadvisable. Users might access unsecured endpoints or impact cluster performance through overly broad queries (or too many queries).

This chapter presents a solution: use Amazon API Gateway to restrict users to a subset of the Elasticsearch APIs and AWS Lambda to sign requests from API Gateway to Amazon ES.

**Note**

Standard API Gateway and Lambda pricing applies, but within the limited usage of this tutorial, costs should be negligible.

**Step 1: Index sample data**

A prerequisite for these steps is an Amazon ES domain. Download `sample-movies.zip`, unzip it, and use the `_bulk` API to add the 5,000 documents to the `movies` index:

```json
POST https://search-my-domain.us-west-1.es.amazonaws.com/_bulk
{
  "index": (
    "_index": "movies", 
    "_type": "movie",
    "_id": "tt1979320"
  )
  "fields": {
    "directors": ["Ron Howard"],
    "release_date": "2013-09-02T00:00:00Z",
    "rating": 8.3,
    "genres": ["Action", "Biography", "Drama", "Sport"],
    "image_url": "http://ia.media-imdb.com/images/M/MV5BMTQyMDE0MTY0OV5BMl5BanBnXkFtZTcwMjI2OTI0OQ@@._V1_SX400_.jpg",
    "plot": "A recreation of the merciless 1970s rivalry between Formula One rivals James Hunt and Niki Lauda.",
    "title": "Rush",
    "year": 2013,
    "actors": ["Daniel Brühl", "Chris Hemsworth", "Olivia Wilde"],
    "running_time_secs": 7380,
    "id": "tt1979320",
    "type": "add"
  }

  { "index": { 
    "_index": "movies", 
    "_type": "movie",
    "_id": "tt1951264"
  } 
  "fields": { 
    "directors": ["Francis Lawrence"],
    "release_date": "2013-11-11T00:00:00Z",
    "genres": ["Action", "Adventure", "Sci-Fi", "Thriller"],
    "image_url": "http://ia.media-imdb.com/images/M/MV5BMTAyMjQ3OTAxMzIwOTUxMjIzNV5BMl5BanBnXkFtZTcwMjI2OTI0OQ@@._V1_SX400_.jpg",
    "plot": "Katniss Everdeen and Peeta Mellark become targets of the Capitol after their victory in the 74th Hunger Games sparks a rebellion in the Districts of Panem.",
    "title": "The Hunger Games: "
  }
}
```
Step 2: Create the API in API Gateway

Using API Gateway lets you create a more limited API and simplifies the process of interacting with the Elasticsearch _search API. API Gateway lets you enable security features like Amazon Cognito authentication and request throttling. Perform the following steps to create and deploy an API:

Create and configure the API

To create your API using the API Gateway console

1. Within API Gateway, choose Create API.
2. Locate REST API (not private) and choose Build.
3. Configure the following fields:
   - API name: search-es-api
   - Description: Public API for searching an Amazon Elasticsearch Service domain
   - Endpoint Type: Regional
4. Choose Create API.
5. Choose Actions > Create Method.
6. Choose GET in the dropdown and click the checkmark to confirm.
7. Configure the following settings, then click Save:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration type</td>
<td>Lambda function</td>
</tr>
<tr>
<td>Use Lambda proxy integration</td>
<td>Yes</td>
</tr>
<tr>
<td>Lambda region</td>
<td>us-west-1</td>
</tr>
<tr>
<td>Lambda function</td>
<td>search-es-lambda (you'll configure this later in Lambda)</td>
</tr>
<tr>
<td>Use default timeout</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Configure the method request

Choose Method Request and configure the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization</td>
<td>NONE</td>
</tr>
<tr>
<td>Request Validator</td>
<td>Validate query string parameters and headers</td>
</tr>
<tr>
<td>API Key Required</td>
<td>false</td>
</tr>
</tbody>
</table>
Step 3: Create and deploy the Lambda function

After you create your API in API Gateway, create the Lambda function that it passes requests to.

Create the Lambda function

In this solution, API Gateway passes requests to the following Python 3.8 Lambda function, which queries Amazon ES and returns results. Name the function search-es-lambda.

```python
import boto3
import json
import requests
from requests_aws4auth import AWS4Auth
```

Because this sample function uses external libraries, you need to create a deployment package and upload it to Lambda for the code to work. For more information about creating Lambda functions and deployment packages, see Creating a Deployment Package (Python) in the AWS Lambda Developer Guide and the section called “Create the Lambda deployment package” (p. 161) in this guide.
region = '' # For example, us-west-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
    session_token=credentials.token)

host = '' # The ES domain endpoint with https:// and a trailing slash
index = 'movies'
url = host + '/' + index + '/_search'

# Lambda execution starts here
def lambda_handler(event, context):

    # Put the user query into the query DSL for more accurate search results.
    # Note that certain fields are boosted (^).
    query = {
        "size": 25,
        "query": {
            "multi_match": {
                "query": event['queryStringParameters']['q'],
                "fields": ["fields.title^4", "fields.plot^2", "fields.actors",
                    "fields.directors"]
            }
        }
    }

    # ES 6.x requires an explicit Content-Type header
    headers = { "Content-Type": "application/json" }

    # Make the signed HTTP request
    r = requests.get(url, auth=awsauth, headers=headers, data=json.dumps(query))

    # Create the response and add some extra content to support CORS
    response = {
        "statusCode": 200,
        "headers": {
            "Access-Control-Allow-Origin": '*'
        },
        "isBase64Encoded": False
    }

    # Add the search results to the response
    response['body'] = r.text
    return response

Modify the handler

The handler is the method in your function code that processes events. You need to change the handler name according to the name of the file in your deployment package where the Lambda function is located. For example, if your file is named es-function.py, rename the handler to es-function.lambda_handler. For more information, see Lambda function handler in Python.

Configure a trigger

Choose Add trigger and create the HTTP endpoint that invokes your function. The trigger must have the following configuration:

<table>
<thead>
<tr>
<th>Trigger</th>
<th>API</th>
<th>Deployment Stage</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>API Gateway</td>
<td>search-es-api</td>
<td>search-es-api-test</td>
<td>Open</td>
</tr>
</tbody>
</table>
Step 4: Modify the domain access policy

Your Amazon ES domain must allow the Lambda function to make GET requests to the movies index. The following policy provides search-es-lambda-role (created through Lambda) access to the movies index:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:role/service-role/search-es-lambda-role-1abcdefg"
            },
            "Action": "es:ESHttpGet",
        }
    ]
}
```

**Note**

To get the exact name of the role that Lambda automatically creates, go to the AWS Identity and Access Management (IAM) console, choose **Roles**, and search for "lambda".

For more information about access policies, see the section called “Configuring access policies” (p. 13).

Step 5: Test the web application

To test the web application

1. Download `sample-site.zip`, unzip it, and open `scripts/search.js` in your favorite text editor.
2. Update the `apigatewayendpoint` variable to point to your API Gateway endpoint. The endpoint takes the form of `https://some-id.execute-api.us-west-1.amazonaws.com/search-es-api-test`.
3. Open `index.html` and try running searches for `thor`, `house`, and a few other terms.
Movie Search

thor

Found 7 results.

Thor

2011 — The powerful but arrogant god Thor is56 amongst humans in Midgard (Earth), where he tests their finest defenders.

Thor: The Dark World

2013 — Faced with an enemy that even Thor cannot withstand, Thor must embark on his most perilous and personal journey yet, one that will reunite him with Jane Foster and put everything to save us all.

Vikingdom

2013 — A forgotten king, Eirick, is tasked with defeating Thor, the God of Thunder.
Next steps

This chapter is just a starting point to demonstrate a concept. You might consider the following modifications:

- Add your own data to the Amazon ES domain.
- Add methods to your API.
- In the Lambda function, modify the search query or boost different fields.
- Style the results differently or modify search.js to display different fields to the user.

Visualizing customer support calls with Amazon Elasticsearch Service and Kibana

This chapter is a full walkthrough of the following situation: a business receives some number of customer support calls and wants to analyze them. What is the subject of each call? How many were positive? How many were negative? How can managers search or review the the transcripts of these calls?

A manual workflow might involve employees listening to recordings, noting the subject of each call, and deciding whether or not the customer interaction was positive.

Such a process would be extremely labor-intensive. Assuming an average time of 10 minutes per call, each employee could listen to only 48 calls per day. Barring human bias, the data they generate would be highly accurate, but the amount of data would be minimal: just the subject of the call and a boolean for whether or not the customer was satisfied. Anything more involved, such as a full transcript, would take a huge amount of time.

Using Amazon S3, Amazon Transcribe, Amazon Comprehend, and Amazon Elasticsearch Service (Amazon ES), you can automate a similar process with very little code and end up with much more data. For example, you can get a full transcript of the call, keywords from the transcript, and an overall "sentiment" of the call (positive, negative, neutral, or mixed). Then you can use Elasticsearch and Kibana to search and visualize the data.

While you can use this walkthrough as-is, the intent is to spark ideas about how to enrich your JSON documents before you index them in Amazon ES.

Estimated Costs

In general, performing the steps in this walkthrough should cost less than $2. The walkthrough uses the following resources:

- S3 bucket with less than 100 MB transferred and stored
  
  To learn more, see Amazon S3 Pricing.
- Amazon ES domain with one t2.medium instance and 10 GiB of EBS storage for several hours
  
  To learn more, see Amazon Elasticsearch Service Pricing.
- Several calls to Amazon Transcribe
  
  To learn more, see Amazon Transcribe Pricing.
- Several natural language processing calls to Amazon Comprehend

API Version 2015-01-01
318
To learn more, see Amazon Comprehend Pricing.

Topics
- Step 1: Configure prerequisites (p. 319)
- Step 2: Copy sample code (p. 319)
- (Optional) Step 3: Index sample data (p. 322)
- Step 4: Analyze and visualize your data (p. 323)
- Step 5: Clean up resources and next steps (p. 327)

Step 1: Configure prerequisites

Before proceeding, you must have the following resources.

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon S3 Bucket</td>
<td>For more information, see Creating a Bucket in the Amazon Simple Storage Service Getting Started Guide.</td>
</tr>
<tr>
<td>Amazon ES Domain</td>
<td>The destination for data. For more information, see Creating Amazon ES domains (p. 9).</td>
</tr>
</tbody>
</table>

If you don't already have these resources, you can create them using the following AWS CLI commands:

```
aws s3 mb s3://my-transcribe-test --region us-west-2
```

**Note**
These commands use the us-west-2 region, but you can use any region that Amazon Comprehend supports. To learn more, see the AWS General Reference.

Step 2: Copy sample code

1. Copy and paste the following Python 3 sample code into a new file named call-center.py:

```python
import boto3
import datetime
import json
import requests
from requests_aws4auth import AWS4Auth
import time
import urllib.request

# Variables to update
audio_file_name = '' # For example, 000001.mp3
bucket_name = '' # For example, my-transcribe-test
```
domain = '' # For example, https://search-my-transcribe-test-12345.us-west-2.es.amazonaws.com
index = 'support-calls'
type = '_doc'
es_region = 'us-west-2'

# Upload audio file to S3.
s3_client = boto3.client('s3')

audio_file = open(audio_file_name, 'rb')
print('Uploading ' + audio_file_name + '...')
response = s3_client.put_object(
    Body=audio_file,
    Bucket=bucket_name,
    Key=audio_file_name
)

## Build the URL to the audio file on S3.
## Only for the us-east-1 region.
mp3_uri = 'https://' + bucket_name + '.s3.amazonaws.com/' + audio_file_name

# Get the necessary details and build the URL to the audio file on S3.
# For all other regions.
response = s3_client.get_bucket_location(
    Bucket=bucket_name
)
bucket_region = response['LocationConstraint']
mp3_uri = 'https://' + bucket_name + '.s3-' + bucket_region + '.amazonaws.com/' + audio_file_name

# Start transcription job.
transcribe_client = boto3.client('transcribe')

print('Starting transcription job...')
response = transcribe_client.start_transcription_job(
    TranscriptionJobName=audio_file_name,
    LanguageCode='en-US',
    MediaFormat='mp3',
    Media={
        'MediaFileUri': mp3_uri
    },
    Settings={
        'ShowSpeakerLabels': True,
        'MaxSpeakerLabels': 2 # assumes two people on a phone call
    }
)

# Wait for the transcription job to finish.
print('Waiting for job to complete...')
while True:
    response = transcribe_client.get_transcription_job(TranscriptionJobName=audio_file_name)
    if response['TranscriptionJob']['TranscriptionJobStatus'] in ['COMPLETED', 'FAILED']:
        break
    else:
        print('Still waiting...')
        time.sleep(10)

transcript_uri = response['TranscriptionJob']['Transcript']['TranscriptFileUri']

# Open the JSON file, read it, and get the transcript.
response = urllib.request.urlopen(transcript_uri)
raw_json = response.read()
loaded_json = json.loads(raw_json)
transcript = loaded_json['results'][0]['transcript']

# Send transcript to Comprehend for key phrases and sentiment.
comprehend_client = boto3.client('comprehend')

# If necessary, trim the transcript.
# If the transcript is more than 5 KB, the Comprehend calls fail.
if len(transcript) > 5000:
    trimmed_transcript = transcript[:5000]
else:
    trimmed_transcript = transcript

print('Detecting key phrases...')
response = comprehend_client.detect_key_phrases(
    Text=trimmed_transcript,
    LanguageCode='en'
)

keywords = []
for keyword in response['KeyPhrases']:
    keywords.append(keyword['Text'])

print('Detecting sentiment...')
response = comprehend_client.detect_sentiment(
    Text=trimmed_transcript,
    LanguageCode='en'
)

sentiment = response['Sentiment']

# Build the Amazon Elasticsearch Service URL.
id = audio_file_name.strip('.mp3')
url = domain + '/' + index + '/' + type + '/' + id

# Create the JSON document.
json_document = {'transcript': transcript, 'keywords': keywords, 'sentiment': sentiment, 'timestamp': datetime.datetime.now().isoformat()}

# Provide all details necessary to sign the indexing request.
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, es_region, 'es', session_token=credentials.token)

# Add explicit header for Elasticsearch 6.x.
headers = {'Content-Type': 'application/json'}

# Index the document.
print('Indexing document...')
response = requests.put(url, auth=awsauth, json=json_document, headers=headers)

print(response)
print(response.json())

2. Update the initial six variables.
3. Install the required packages using the following commands:
   pip install boto3
   pip install requests
   pip install requests_aws4auth

4. Place your MP3 in the same directory as call-center.py and run the script. A sample output follows:
   # python call-center.py
call-center.py performs a number of operations:

1. The script uploads an audio file (in this case, an MP3, but Amazon Transcribe supports several formats) to your S3 bucket.
2. It sends the audio file’s URL to Amazon Transcribe and waits for the transcription job to finish.

   The time to finish the transcription job depends on the length of the audio file. Assume minutes, not seconds.

   **Tip**
   
   To improve the quality of the transcription, you can configure a custom vocabulary for Amazon Transcribe.

3. After the transcription job finishes, the script extracts the transcript, trims it to 5,000 characters, and sends it to Amazon Comprehend for keyword and sentiment analysis.
4. Finally, the script adds the full transcript, keywords, sentiment, and current timestamp to a JSON document and indexes it in Amazon ES.

   **Tip**
   
   LibriVox has public domain audiobooks that you can use for testing.

---

(Optional) Step 3: Index sample data

If you don’t have a bunch of call recordings handy—and who does?—you can index (p. 158) the sample documents in sample-calls.zip, which are comparable to what call-center.py produces.

1. Create a file named bulk-helper.py:

   ```python
   import boto3
   from elasticsearch import Elasticsearch, RequestsHttpConnection
   import json
   from requests_aws4auth import AWS4Auth

   host = '' # For example, my-test-domain.us-west-2.es.amazonaws.com
   region = '' # For example, us-west-2
   service = 'es'

   bulk_file = open('sample-calls.bulk', 'r').read()

   credentials = boto3.Session().get_credentials()
   awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service, session_token=credentials.token)
   ```
Step 4: Analyze and visualize your data

Now that you have some data in Amazon ES, you can visualize it using Kibana.


2. Before you can use Kibana, you need an index pattern. Kibana uses index patterns to narrow your analysis to one or more indices. To match the support-calls index that call-center.py created, define an index pattern of support*, and then choose Next step.

3. For Time Filter field name, choose timestamp.

4. Now you can start creating visualizations. Choose Visualize, and then add a new visualization.

5. Choose the pie chart and the support* index pattern.
6. The default visualization is basic, so choose **Split Slices** to create a more interesting visualization.

For **Aggregation**, choose **Terms**. For **Field**, choose **sentiment.keyword**. Then choose **Apply changes** and **Save**.

7. Return to the **Visualize** page, and add another visualization. This time, choose the horizontal bar chart.

8. Choose **Split Series**.

    For **Aggregation**, choose **Terms**. For **Field**, choose **keywords.keyword** and change **Size** to 20. Then choose **Apply Changes** and **Save**.
9. Return to the Visualize page and add one final visualization, a vertical bar chart.

10. Choose Split Series. For Aggregation, choose Date Histogram. For Field, choose timestamp and change Interval to Daily.

11. Choose Metrics & Axes and change Mode to normal.

12. Choose Apply Changes and Save.
13. Now that you have three visualizations, you can add them to a Kibana dashboard. Choose **Dashboard**, create a dashboard, and add your visualizations.
Step 5: Clean up resources and next steps

To avoid unnecessary charges, delete the S3 bucket and Amazon ES domain. To learn more, see Delete a Bucket in the Amazon Simple Storage Service Developer Guide and Delete an Amazon ES domain (p. 8) in this guide.

Transcripts require much less disk space than MP3 files. You might be able to shorten your MP3 retention window—for example, from three months of call recordings to one month—retain years of transcripts, and still save on storage costs.

You could also automate the transcription process using AWS Step Functions and Lambda, add additional metadata before indexing, or craft more complex visualizations to fit your exact use case.
Troubleshooting Amazon Elasticsearch Service

This topic describes how to identify and solve common Amazon Elasticsearch Service (Amazon ES) issues. Consult the information in this section before contacting AWS Support.

Can't access Kibana

The Kibana endpoint doesn't support signed requests. If the access control policy for your domain only grants access to certain IAM users or roles and you haven't configured Amazon Cognito authentication (p. 128), you might receive the following error when you attempt to access Kibana:

"User: anonymous is not authorized to perform: es:ESHttpGet"

If your Amazon ES domain uses VPC access, you might not receive this error, but the request might time out. To learn more about correcting this issue and the various configuration options available to you, see the section called “Controlling access to Kibana” (p. 216), the section called “About access policies on VPC domains” (p. 25), and the section called “Identity and Access Management” (p. 77).

Can't access VPC domain

See the section called “About access policies on VPC domains” (p. 25) and the section called “Testing VPC domains” (p. 26).

Cluster in read-only state

Compared to earlier versions, Elasticsearch 7.x uses a different system for cluster coordination. In this new system, when the cluster loses quorum, the cluster is unavailable until you take action. Loss of quorum can take two forms:

- If your cluster uses dedicated master nodes, quorum loss occurs when half or more are unavailable.
- If your cluster does not use dedicated master nodes, quorum loss occurs when half or more of your data nodes are unavailable.

If quorum loss occurs and your cluster has more than one node, Amazon ES restores quorum and places the cluster into a read-only state. You have two options:

- Remove the read-only state and use the cluster as-is.
- Restore the cluster or individual indices from a snapshot (p. 59).

If you prefer to use the cluster as-is, verify that cluster health is green using the following request:
If cluster health is red, we recommend restoring the cluster from a snapshot. You can also see the section called "Red cluster status" (p. 329) for troubleshooting steps. If cluster health is green, check that all expected indices are present using the following request:

```
GET _cat/indices?v
```

Then run some searches to verify that the expected data is present. If it is, you can remove the read-only state using the following request:

```
PUT _cluster/settings
{
  "persistent": {
    "cluster.blocks.read_only": false
  }
}
```

If quorum loss occurs and your cluster has only one node, Amazon ES replaces the node and does not place the cluster into a read-only state. Otherwise, your options are the same: use the cluster as-is or restore from a snapshot.

In both situations, Amazon ES sends two events to your Personal Health Dashboard. The first informs you of the loss of quorum. The second occurs after Amazon ES successfully restores quorum. For more information about using the Personal Health Dashboard, see the AWS Health User Guide.

## Red cluster status

A red cluster status means that at least one primary shard and its replicas are not allocated to a node. Amazon ES keeps trying to take automated snapshots of all indices regardless of their status, but the snapshots fail while the red cluster status persists.

The most common causes of a red cluster status are failed cluster nodes (p. 332) and the Elasticsearch process crashing due to a continuous heavy processing load.

**Note**

Amazon ES stores automated snapshots for 14 days regardless of the cluster status. Therefore, if the red cluster status persists for more than two weeks, the last healthy automated snapshot will be deleted and you could permanently lose your cluster's data. If your Amazon ES domain enters a red cluster status, AWS Support might contact you to ask whether you want to address the problem yourself or you want the support team to assist. You can set a CloudWatch alarm (p. 270) to notify you when a red cluster status occurs.

Ultimately, red shards cause red clusters, and red indices cause red shards. To identify the indices causing the red cluster status, Elasticsearch has some helpful APIs.

- **GET /_cluster/allocation/explain** chooses the first unassigned shard that it finds and explains why it cannot be allocated to a node:

```json
{
  "index": "test4",
  "shard": 0,
  "primary": true,
  "current_state": "unassigned",
  "can_allocate": "no",
}
```
Recovering from a continuous heavy processing load

To determine if a red cluster status is due to a continuous heavy processing load on a data node, monitor the following cluster metrics.

<table>
<thead>
<tr>
<th>Relevant Metric</th>
<th>Description</th>
<th>Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>JVMMemoryPressure</td>
<td>Specifies the percentage of the Java heap used for all data nodes in a cluster. View the Maximum statistic for this metric, and look for smaller and smaller drops in memory pressure as the Java garbage collector fails to reclaim sufficient memory. This pattern likely is due to complex queries or large data fields. The Concurrent Mark Sweep (CMS) garbage collector triggers when 75% of the “old generation” object space is full. This collector runs alongside other threads to keep pauses to a minimum. If CMS is unable to reclaim enough memory during these normal collections, Elasticsearch triggers a different garbage collection algorithm that halts all threads. Nodes are unresponsive during these stop-the-</td>
<td>Set memory circuit breakers for the JVM. For more information, see the section called “JVM OutOfMemoryError” (p. 332). If the problem persists, delete unnecessary indices, reduce the number or complexity of requests to the domain, add instances, or use larger instance types.</td>
</tr>
</tbody>
</table>
Yellow cluster status

A yellow cluster status means that the primary shards for all indices are allocated to nodes in a cluster, but the replica shards for at least one index are not. Single-node clusters always initialize with a yellow cluster status because there is no other node to which Amazon ES can assign a replica. To achieve green cluster status, increase your node count. For more information, see the section called “Sizing domains” (p. 263).

Multi-node clusters might briefly have a yellow cluster status after creating a new index or after a node failure. This status self-resolves as Elasticsearch replicates data across the cluster. Lack of disk space (p. 331) can also cause yellow cluster status; the cluster can only distribute replica shards if nodes have the disk space to accommodate them.

ClusterBlockException

You might receive a ClusterBlockException error for the following reasons.

Lack of available storage space

If no nodes have enough storage space to accommodate shard relocation, basic write operations like adding documents and creating indices can begin to fail. the section called “Calculating storage requirements” (p. 264) provides a summary of how Amazon ES uses disk space.
To avoid issues, monitor the `FreeStorageSpace` metric in the Amazon ES console and create CloudWatch alarms (p. 270) to trigger when `FreeStorageSpace` drops below a certain threshold. GET `/_cat/allocation?v` also provides a useful summary of shard allocation and disk usage. To resolve issues associated with a lack of storage space, scale your Amazon ES domain to use larger instance types, more instances, or more EBS-based storage.

**Blocked disks due to low memory**

When the `JVMMemoryPressure` metric exceeds 92% for 30 minutes, Amazon ES triggers a protection mechanism and blocks all write operations to prevent the cluster from reaching red status. When the protection is on, write operations fail with a `ClusterBlockException` error, new indices can’t be created, and the `IndexCreateBlockException` error is thrown.

When the `JVMMemoryPressure` metric returns to 88% or lower for five minutes, the protection is disabled, and write operations to the cluster are unblocked.

**JVM OutOfMemoryError**

A JVM `OutOfMemoryError` typically means that one of the following JVM circuit breakers was reached.

<table>
<thead>
<tr>
<th>Circuit Breaker</th>
<th>Description</th>
<th>Cluster Setting Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Breaker</td>
<td>Total percentage of JVM heap memory allowed for all circuit breakers. The default value is 95%.</td>
<td><code>indices.breaker.total.limit</code></td>
</tr>
<tr>
<td>Field Data Breaker</td>
<td>Percentage of JVM heap memory allowed to load a single data field into memory. The default value is 40%. If you upload data with large fields, you might need to raise this limit.</td>
<td><code>indices.breaker.fielddata.limit</code></td>
</tr>
<tr>
<td>Request Breaker</td>
<td>Percentage of JVM heap memory allowed for data structures used to respond to a service request. The default value is 60%. If your service requests involve calculating aggregations, you might need to raise this limit.</td>
<td><code>indices.breaker.request.limit</code></td>
</tr>
</tbody>
</table>

**Failed cluster nodes**

Amazon EC2 instances might experience unexpected terminations and restarts. Typically, Amazon ES restarts the nodes for you. However, it’s possible for one or more nodes in an Elasticsearch cluster to remain in a failed condition.

To check for this condition, open your domain dashboard on the Amazon ES console. Choose the Cluster health tab, and then choose the Nodes metric. See if the reported number of nodes is fewer than the
number that you configured for your cluster. If the metric shows that one or more nodes is down for
more than one day, contact AWS Support.

You can also set a CloudWatch alarm (p. 270) to notify you when this issue occurs.

Note
The Nodes metric is not accurate during changes to your cluster configuration and during
routine maintenance for the service. This behavior is expected. The metric will report the
correct number of cluster nodes soon. To learn more, see the section called “Configuration
changes” (p. 14).

To protect your clusters from unexpected node terminations and restarts, create at least one replica for
each index in your Amazon ES domain.

Exceeded maximum shard limit

The 7.x versions of Elasticsearch have a default setting of no more than 1,000 shards per node.
Elasticsearch throws an error if a request, such as creating a new index, would cause you to exceed this
limit. If you encounter this error, you have several options:

• Add more data nodes to the cluster.
• Increase the _cluster/settings/cluster.max_shards_per_node setting.
• Use the _shrink API (p. 279) to reduce the number of shards on the node.

Can't enable audit logs

You might encounter the following error when you try to enable audit log publishing using the Amazon
ES console:

The Resource Access Policy specified for the CloudWatch Logs log group does not grant sufficient
permissions for Amazon Elasticsearch Service to create a log stream. Please check the Resource Access
Policy.

If you encounter this error, verify that the resource element of your policy includes the correct log
group ARN. If it does, take the following steps:

1. Wait several minutes.
2. Refresh the page in your web browser.
3. Choose Use existing log group.
4. Under Existing log group, choose the log group that you created before receiving the error message.
5. Choose Select an existing policy.
6. Under Existing policy, choose the policy that you created before receiving the error message.
7. Choose Enable.

If the error persists after repeating steps 1–7 several times, contact AWS Support.

Can't close index

Amazon ES supports the _close API only for Elasticsearch versions 7.4 or later. If you're using an older
version and are restoring an index from a snapshot, you can delete the existing index (before or after
reindexing it). The other option is to use the `rename_pattern` and `rename_replacement` fields to rename the index as you restore it:

```
POST /_snapshot/my-repository/my-snapshot/_restore
{
  "indices": "my-index-1,myindex-2",
  "include_global_state": true,
  "rename_pattern": "my-index-(\d)",
  "rename_replacement": "restored-my-index-$1"
}
```

If you plan to reindex, shrink, or split an index, you likely want to stop writing to it before performing the operation.

### Mapper parsing exception while indexing

Elasticsearch 7.10 deprecated several parameters (`ignore_malformed`, `coerce`, and others) for use within dynamic templates. If you add a document to an index with a dynamic template that contains a deprecated parameter, Elasticsearch throws an exception:

```
"error" : {
    "root_cause" : [
      {
        "type" : "mapper_parsing_exception",
        "reason" : "unknown parameter [ignore_malformed] on mapper [mykeyword] of type [text]"
      }
    ]
}
```

If you encounter this error, remove the deprecated parameter from your template and retry the request.

### Client license checks

The default distributions of Logstash and Beats include a proprietary license check and fail to connect to the open source version of Elasticsearch. Make sure you use the Apache 2.0 (OSS) distributions of these clients with Amazon ES.

### Request throttling

If you receive persistent 403 Request throttled due to too many requests or 429 Too Many Requests errors, consider scaling vertically. Amazon Elasticsearch Service throttles requests if the payload would cause memory usage to exceed the maximum size of the Java heap.

### Can't SSH into node

You can't use SSH to access any of the nodes in your Elasticsearch cluster, and you can't directly modify `elasticsearch.yml`. Instead, use the console, AWS CLI, or SDKs to configure your domain. You can specify a few cluster-level settings using the Elasticsearch REST APIs, as well. To learn
more, see Configuration API reference (p. 339) and the section called “Supported Elasticsearch operations” (p. 277).

If you need more insight into the performance of the cluster, you can publish error logs and slow logs to CloudWatch (p. 47).

"Not Valid for the Object's Storage Class" snapshot error

Amazon ES snapshots do not support the S3 Glacier storage class. You might encounter this error when you attempt to list snapshots if your S3 bucket includes a lifecycle rule that transitions objects to the S3 Glacier storage class.

If you need to restore a snapshot from the bucket, restore the objects from S3 Glacier, copy the objects to a new bucket, and register the new bucket (p. 55) as a snapshot repository.

Invalid host header

Amazon ES requires that clients specify Host in the request headers. A valid Host value is the domain endpoint without https://, such as:

```
Host: search-my-sample-domain-ih2hn2ew2scurji.us-west-2.es.amazonaws.com
```

If you receive an Invalid Host Header error when making a request, check that your client or proxy includes the Amazon ES domain endpoint (and not, for example, its IP address) in the Host header.

Invalid M3 instance type

Amazon ES does not support adding or modifying M3 instances to existing domains running Elasticsearch versions 6.7 or later. You can continue to use M3 instances with Elasticsearch 6.5 and earlier.

We recommend choosing a newer instance type. For domains running Elasticsearch 6.7 and later, the following restriction apply:

- If your existing domain does not use M3 instances, you can no longer change to them.
- If you change an existing domain from an M3 instance type to another instance type, you can't switch back.

Hot queries stop working after enabling UltraWarm

When you enable UltraWarm on a domain, if there are no preexisting overrides to the search.max_buckets setting, Amazon ES automatically sets the value to 10000 to prevent memory-heavy queries from saturating warm nodes. If your hot queries are using more than 10,000 buckets, they might stop working when you enable UltraWarm.
Because you can't modify this setting due to the managed nature of Amazon Elasticsearch Service, you need to open a support case to increase the limit. Limit increases don't require a premium support subscription.

Can't downgrade after upgrade

In-place upgrades (p. 61) are irreversible, but if you contact AWS Support, they can help you restore the automatic, pre-upgrade snapshot on a new domain. For example, if you upgrade a domain from Elasticsearch 5.6 to 6.4, AWS Support can help you restore the pre-upgrade snapshot on a new Elasticsearch 5.6 domain. If you took a manual snapshot of the original domain, you can perform that step yourself (p. 51).

Need summary of domains for all regions

The following script uses the Amazon EC2 describe-regions AWS CLI command to create a list of all regions in which Amazon ES could be available. Then it calls list-domain-names for each region:

```bash
for region in `aws ec2 describe-regions --output text | cut -f4`
do
echo "\nListing domains in region '$region':"
   aws es list-domain-names --region $region --query 'DomainNames'
done
```

You receive the following output for each region:

```
Listing domains in region:'us-west-2'...
[
  
  "DomainName": "sample-domain"
]
```

Regions in which Amazon ES is not available return "Could not connect to the endpoint URL."

Browser error when using Kibana

Your browser wraps service error messages in HTTP response objects when you use Kibana to view data in your Amazon ES domain. You can use developer tools commonly available in web browsers, such as Developer Mode in Chrome, to view the underlying service errors and assist your debugging efforts.

To view service errors in Chrome

1. From the menu, choose View, Developer, Developer Tools.
2. Choose the Network tab.
3. In the Status column, choose any HTTP session with a status of 500.

To view service errors in Firefox

1. From the menu, choose Tools, Web Developer, Network.
2. Choose any HTTP session with a status of 500.
Unauthorized operation after selecting VPC access

When you create a new domain using the Amazon ES console, you have the option to select VPC or public access. If you select **VPC access**, Amazon ES queries for VPC information and fails if you don't have the proper permissions:

```
You are not authorized to perform this operation. (Service: AmazonEC2; Status Code: 403; Error Code: UnauthorizedOperation)
```

To enable this query, you must have access to the `ec2:DescribeVpcs`, `ec2:DescribeSubnets`, and `ec2:DescribeSecurityGroups` operations. This requirement is only for the console. If you use the AWS CLI to create and configure a domain with a VPC endpoint, you don't need access to those operations.

Stuck at loading after creating VPC domain

After creating a new domain that uses VPC access, the domain's **Configuration state** might never progress beyond **Loading**. If this issue occurs, you likely have AWS Security Token Service (AWS STS) **disabled** for your region.

To add VPC endpoints to your VPC, Amazon ES needs to assume the `AWSServiceRoleForAmazonElasticsearchService` role. Thus, AWS STS must be enabled to create new domains that use VPC access in a given region. To learn more about enabling and disabling AWS STS, see the **IAM User Guide**.

Can't connect from Alpine Linux

Alpine Linux limits DNS response size to 512 bytes. If you try to connect to your Amazon ES domain from Alpine Linux, DNS resolution can fail if the domain is in a VPC and has more than 20 nodes. If your domain is in a VPC, we recommend using other Linux distributions, such as Debian, Ubuntu, CentOS, Red Hat Enterprise Linux, or Amazon Linux 2, to connect to it.

Certificate error when using SDK

Because AWS SDKs use the CA certificates from your computer, changes to the certificates on the AWS servers can cause connection failures when you attempt to use an SDK. Error messages vary, but typically contain the following text:

```
Failed to query Elasticsearch
...SSL3_GET_SERVER_CERTIFICATE:certificate verify failed
```

You can prevent these failures by keeping your computer's CA certificates and operating system up-to-date. If you encounter this issue in a corporate environment and do not manage your own computer, you might need to ask an administrator to assist with the update process.

The following list shows minimum operating system and Java versions:
• Microsoft Windows versions that have updates from January 2005 or later installed contain at least one of the required CAs in their trust list.
• Mac OS X 10.4 with Java for Mac OS X 10.4 Release 5 (February 2007), Mac OS X 10.5 (October 2007), and later versions contain at least one of the required CAs in their trust list.
• Red Hat Enterprise Linux 5 (March 2007), 6, and 7 and CentOS 5, 6, and 7 all contain at least one of the required CAs in their default trusted CA list.
• Java 1.4.2_12 (May 2006), 5 Update 2 (March 2005), and all later versions, including Java 6 (December 2006), 7, and 8, contain at least one of the required CAs in their default trusted CA list.

The three certificate authorities are:

• Amazon Root CA 1
• Starfield Services Root Certificate Authority - G2
• Starfield Class 2 Certification Authority

Root certificates from the first two authorities are available from Amazon Trust Services, but keeping your computer up-to-date is the more straightforward solution. To learn more about ACM-provided certificates, see AWS Certificate Manager FAQs.

Note
Currently, Amazon ES domains in the us-east-1 region use certificates from a different authority. We plan to update the region to use these new certificate authorities in the near future.
Configuration API reference for Amazon Elasticsearch Service

This reference describes the actions, data types, and errors in the Amazon Elasticsearch Service (Amazon ES) configuration API. The configuration API is a REST API that you can use to create and configure Amazon ES domains over HTTP. You also can use the AWS CLI and the console to configure Amazon ES domains. For more information, see Creating and Configuring Amazon ES Domains (p. 9).

- Actions (p. 339)
- Data Types (p. 377)
- Errors (p. 393)

Actions

The following table provides a quick reference to the HTTP method required for each operation for the REST interface to the Amazon Elasticsearch Service configuration API. The description of each operation also includes the required HTTP method.

**Note**
All configuration service requests must be signed. For more information, see Signing Amazon Elasticsearch Service Requests (p. 82) in this guide and Signature Version 4 Signing Process in the AWS General Reference.

<table>
<thead>
<tr>
<th>Action</th>
<th>HTTP Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>AcceptInboundCrossClusterSearchConnection (p. 341)</td>
<td>PUT</td>
</tr>
<tr>
<td>AddTags (p. 341)</td>
<td>POST</td>
</tr>
<tr>
<td>the section called “AssociatePackage” (p. 342)</td>
<td>POST</td>
</tr>
<tr>
<td>CreateElasticsearchDomain (p. 342)</td>
<td>POST</td>
</tr>
<tr>
<td>CreateOutboundCrossClusterSearchConnection (p. 346)</td>
<td>POST</td>
</tr>
<tr>
<td>the section called “CreatePackage” (p. 347)</td>
<td>POST</td>
</tr>
<tr>
<td>DeleteElasticsearchDomain (p. 348)</td>
<td>DELETE</td>
</tr>
<tr>
<td>DeleteElasticsearchServiceRole (p. 348)</td>
<td>DELETE</td>
</tr>
<tr>
<td>DeleteInboundCrossClusterSearchConnection (p. 349)</td>
<td>DELETE</td>
</tr>
<tr>
<td>DeleteOutboundCrossClusterSearchConnection (p. 350)</td>
<td>DELETE</td>
</tr>
<tr>
<td>the section called “DeletePackage” (p. 350)</td>
<td>DELETE</td>
</tr>
<tr>
<td>the section called “DescribeDomainAutoTunes” (p. 350)</td>
<td>GET</td>
</tr>
<tr>
<td>DescribeElasticsearchDomain (p. 351)</td>
<td>GET</td>
</tr>
<tr>
<td>DescribeElasticsearchDomainConfig (p. 352)</td>
<td>GET</td>
</tr>
<tr>
<td>Action</td>
<td>HTTP Method</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>DescribeElasticsearchDomains (p. 353)</td>
<td>POST</td>
</tr>
<tr>
<td>DescribeElasticsearchInstanceTypeLimits (p. 353)</td>
<td>GET</td>
</tr>
<tr>
<td>DescribeInboundCrossClusterSearchConnections (p. 354)</td>
<td>POST</td>
</tr>
<tr>
<td>DescribeOutboundCrossClusterSearchConnections (p. 355)</td>
<td>POST</td>
</tr>
<tr>
<td>the section called “DescribePackages“ (p. 356)</td>
<td>POST</td>
</tr>
<tr>
<td>DescribeReservedElasticsearchInstanceOfferings (p. 357)</td>
<td>GET</td>
</tr>
<tr>
<td>DescribeReservedElasticsearchInstances (p. 358)</td>
<td>GET</td>
</tr>
<tr>
<td>the section called “DissociatePackage“ (p. 359)</td>
<td>POST</td>
</tr>
<tr>
<td>GetCompatibleElasticsearchVersions (p. 360)</td>
<td>GET</td>
</tr>
<tr>
<td>the section called “GetPackageVersionHistory“ (p. 361)</td>
<td>GET</td>
</tr>
<tr>
<td>GetUpgradeHistory (p. 362)</td>
<td>GET</td>
</tr>
<tr>
<td>GetUpgradeStatus (p. 363)</td>
<td>GET</td>
</tr>
<tr>
<td>ListDomainNames (p. 363)</td>
<td>GET</td>
</tr>
<tr>
<td>the section called “ListDomainsForPackage“ (p. 364)</td>
<td>GET</td>
</tr>
<tr>
<td>ListElasticsearchInstanceTypeDetails (p. 365)</td>
<td>GET</td>
</tr>
<tr>
<td>ListElasticsearchInstanceTypes (p. 366)</td>
<td>GET</td>
</tr>
<tr>
<td>ListElasticsearchVersions (p. 367)</td>
<td>GET</td>
</tr>
<tr>
<td>the section called “ListPackagesForDomain“ (p. 368)</td>
<td>GET</td>
</tr>
<tr>
<td>ListTags (p. 368)</td>
<td>GET</td>
</tr>
<tr>
<td>PurchaseReservedElasticsearchInstanceOffering (p. 369)</td>
<td>POST</td>
</tr>
<tr>
<td>RejectInboundCrossClusterSearchConnection (p. 370)</td>
<td>PUT</td>
</tr>
<tr>
<td>RemoveTags (p. 370)</td>
<td>POST</td>
</tr>
<tr>
<td>StartElasticsearchServiceSoftwareUpdate (p. 371)</td>
<td>POST</td>
</tr>
<tr>
<td>StopElasticsearchServiceSoftwareUpdate (p. 371)</td>
<td>POST</td>
</tr>
<tr>
<td>UpdateElasticsearchDomainConfig (p. 372)</td>
<td>POST</td>
</tr>
<tr>
<td>the section called “UpdatePackage“ (p. 375)</td>
<td>POST</td>
</tr>
<tr>
<td>UpgradeElasticsearchDomain (p. 376)</td>
<td>POST</td>
</tr>
</tbody>
</table>
AcceptInboundCrossClusterSearchConnection

Allows the destination domain owner to accept an inbound cross-cluster search connection request.

Syntax

```
PUT https://es.us-east-1.amazonaws.com/2015-01-01/es/ccs/inboundConnection/{ConnectionId}/accept
```

Request parameters

This operation does not use HTTP request parameters.

Request body

This operation does not use the HTTP request body.

Response elements

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CrossClusterSearchConnection</td>
<td>Object</td>
<td>Inbound connection details.</td>
</tr>
</tbody>
</table>

AddTags

Attaches resource tags to an Amazon ES domain. For more information, see Tagging Amazon ES Domains (p. 70).

Syntax

```
POST https://es.us-east-1.amazonaws.com/2015-01-01/tags
{
  "ARN": "domain-arn",
  "TagList": [{
    "Key": "tag-key",
    "Value": "tag-value"
  }]
}
```

Request parameters

This operation does not use request parameters.

Request body

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TagList</td>
<td>the section called &quot;TagList&quot; (p. 392)</td>
<td>Yes</td>
<td>List of resource tags.</td>
</tr>
</tbody>
</table>
AssociatePackage

Associates a package with an Amazon ES domain.

Syntax

```
POST https://es.us-east-1.amazonaws.com/2015-01-01/packages/associate/package-id/domain-name
```

Request parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PackageID</td>
<td>String</td>
<td>Yes</td>
<td>Internal ID of the package that you want to associate with a domain. Use the section called “DescribePackages” (p. 356) to find this value.</td>
</tr>
<tr>
<td>DomainName</td>
<td>the section called “DomainName” (p. 381)</td>
<td>Yes</td>
<td>Name of the domain that you want to associate the package with.</td>
</tr>
</tbody>
</table>

Request body

This operation does not use the HTTP request body.

Response elements

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainPackageDetails</td>
<td>the section called “DomainPackageDetails” (p. 381)</td>
</tr>
</tbody>
</table>

CreateElasticsearchDomain

Creates an Amazon ES domain. For more information, see the section called “Creating Amazon ES domains” (p. 9).
Note
If you attempt to create an Amazon ES domain and a domain with the same name already exists, the API does not report an error. Instead, it returns details for the existing domain.

Syntax

```json
POST https://es.us-east-1.amazonaws.com/2015-01-01/es/domain
{
  "ElasticsearchClusterConfig": {
    "ZoneAwarenessConfig": {
      "AvailabilityZoneCount": 3,
    },
    "ZoneAwarenessEnabled": true|false,
    "InstanceCount": 3,
    "DedicatedMasterEnabled": true|false,
    "DedicatedMasterType": "c5.large.elasticsearch",
    "DedicatedMasterCount": 3,
    "InstanceType": "r5.large.elasticsearch",
    "WarmCount": 3,
    "WarmEnabled": true|false,
    "WarmType": "ultrawarm1.large.elasticsearch",
    "ColdStorageOptions": {
      "Enabled": true|false
    },
    "EBSOptions": {
      "EBSEnabled": true|false,
      "VolumeType": "io1|gp2|standard",
      "Iops": 1000,
      "VolumeSize": 35
    },
    "EncryptionAtRestOptions": {
      "Enabled": true|false,
      "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:alias/my-key"
    },
    "SnapshotOptions": {
      "AutomatedSnapshotStartHour": 3
    },
    "VPCOptions": {
      "VPCId": "vpc-12345678",
      "SubnetIds": ["subnet-abcdefg1", "subnet-abcdefg2", "subnet-abcdefg3"],
      "SecurityGroupIds": ["sg-12345678"
    },
    "AdvancedOptions": {
      "rest.action.multi.allow_explicit_index": true|false,
      "indices.fielddata.cache.size": 40,
      "indices.query.bool.max_clause_count": 1024
    },
    "CognitoOptions": {
      "Enabled": true|false,
      "UserPoolId": "us-east-1_121234567",
      "IdentityPoolId": "us-east-1:12345678-1234-1234-1234-123456789012",
      "RoleArn": "arn:aws:iam::123456789012:role/service-role/CognitoAccessForAmazonES"
    },
    "NodeToNodeEncryptionOptions": {
      "Enabled": true|false
    },
    "DomainEndpointOptions": {
      "EnforceHTTPS": true|false,
      "CustomEndpointEnabled": true|false,
      "CustomEndpoint": "www.my-custom-endpoint.com",
      "CustomEndpointCertificateArn": "arn:aws:iam::123456789012:certificate/my-certificate"
    },
    "LogPublishingOptions": {
  
```
},
"AdvancedSecurityOptions": {  "Enabled": true|false,  "InternalUserDatabaseEnabled": true|false,  "MasterUserOptions": {  "MasterUserARN": "arn:aws:iam::123456789012:role/my-master-user-role"  "MasterUserName": "my-master-username",  "MasterUserPassword": "my-master-password"  } },

**Request parameters**

This operation does not use HTTP request parameters.

**Request body**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainName</td>
<td>the section called &quot;DomainName&quot; (p. 381)</td>
<td>Yes</td>
<td>Name of the Amazon ES domain to create.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Data Type</td>
<td>Required?</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------</td>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ElasticsearchVersion</td>
<td>String</td>
<td>No</td>
<td>Version of Elasticsearch. If not specified, 1.5 is used as the default. For the full list of supported versions, see the section called “Supported Elasticsearch versions” (p. 2).</td>
</tr>
<tr>
<td>ElasticsearchClusterConfig</td>
<td>the section called “ElasticsearchClusterConfig” (p. 382)</td>
<td>No</td>
<td>Container for the cluster configuration of an Amazon ES domain.</td>
</tr>
<tr>
<td>EBSOptions</td>
<td>the section called “EBSOptions” (p. 382)</td>
<td>No</td>
<td>Container for the parameters required to enable EBS-based storage for an Amazon ES domain.</td>
</tr>
<tr>
<td>VPCOptions</td>
<td>the section called “VPCOptions” (p. 393)</td>
<td>No</td>
<td>Container for the values required to configure VPC access domains. If you don't specify these values, Amazon ES creates the domain with a public endpoint. To learn more, see Launching your Amazon Elasticsearch Service domains using a VPC (p. 22).</td>
</tr>
<tr>
<td>CognitoOptions</td>
<td>the section called “CognitoOptions” (p. 379)</td>
<td>No</td>
<td>Key-value pairs to configure Amazon ES to use Amazon Cognito authentication for Kibana.</td>
</tr>
<tr>
<td>AccessPolicies</td>
<td>String</td>
<td>No</td>
<td>IAM policy document specifying the access policies for the new Amazon ES domain. For more information, see the section called “Identity and Access Management” (p. 77).</td>
</tr>
<tr>
<td>SnapshotOptions</td>
<td>the section called “SnapshotOptions” (p. 391)</td>
<td>No</td>
<td>DEPRECATED. For domains running Elasticsearch 5.3 and later, Amazon ES takes hourly automated snapshots, making this setting irrelevant. For domains running earlier versions of Elasticsearch, Amazon ES takes daily automated snapshots. This value acts as a container for the hour of the day at which you want the service to take the snapshot.</td>
</tr>
<tr>
<td>AdvancedOptions</td>
<td>the section called “AdvancedOptions” (p. 377)</td>
<td>No</td>
<td>Key-value pairs to specify advanced configuration options. For more information, see Configuring Advanced Options (p. 13).</td>
</tr>
</tbody>
</table>
### CreateOutboundCrossClusterSearchConnection

Creates a new cross-cluster search connection from a source domain to a destination domain.

**Syntax**

```json
POST https://es.us-east-1.amazonaws.com/2015-01-01/es/ccs/outboundConnection
{
    "ConnectionAlias": "StringValue",
    "SourceDomainInfo": {
        "DomainName": "Domain-name",
        "Region": "us-east-1"
    },
    "DestinationDomainInfo": {
        "OwnerId": "Account-id",
        "DomainName": "Domain-name",
        "Region": "us-east-1"
    }
}
```

**Request parameters**

This operation does not use HTTP request parameters.
CreatePackage

Add a package for use with Amazon ES domains.

Syntax

POST https://es.us-east-1.amazonaws.com/2015-01-01/packages
{
  "PackageName": "my-package-name",
  "PackageType": "TXT-DICTIONARY",
  "PackageDescription": "My synonym file.",
  "PackageSource": {
    "S3BucketName": "my-s3-bucket",
    "S3Key": "synonyms.txt"
  }
}

Request parameters

This operation does not use request parameters.

Request body

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SourceDomainInfo</td>
<td>Object</td>
<td>Yes</td>
<td>Name and region of the source domain.</td>
</tr>
<tr>
<td>DestinationDomainInfo</td>
<td>Object</td>
<td>Yes</td>
<td>Name and region of the destination domain.</td>
</tr>
<tr>
<td>ConnectionAlias</td>
<td>String</td>
<td>Yes</td>
<td>Name of the connection.</td>
</tr>
<tr>
<td>ConnectionStatus</td>
<td>String</td>
<td></td>
<td>The status of the connection.</td>
</tr>
<tr>
<td>CrossClusterSearchConnectionId</td>
<td>String</td>
<td></td>
<td>The ID for the outbound connection.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PackageName</td>
<td>String</td>
<td>Yes</td>
<td>Unique name for the package.</td>
</tr>
</tbody>
</table>
DeleteElasticsearchDomain

Deletes an Amazon ES domain and all of its data. A domain cannot be recovered after it is deleted.

Syntax

```
DELETE https://es.us-east-1.amazonaws.com/2015-01-01/es/domain/domain-name
```

Request parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainName</td>
<td>the section called &quot;DomainName&quot; (p. 381)</td>
<td>Yes</td>
<td>Name of the Amazon ES domain that you want to delete.</td>
</tr>
</tbody>
</table>

Request body

This operation does not use the HTTP request body.

Response elements

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainStatus</td>
<td>the section called “ElasticsearchDomainStatus” (p. 384)</td>
</tr>
</tbody>
</table>

DeleteElasticsearchServiceRole

Deletes the service-linked role between Amazon ES and Amazon EC2. This role gives Amazon ES permissions to place VPC endpoints into your VPC. A service-linked role must be in place for domains with VPC endpoints to be created or function properly.
DeleteInboundCrossClusterSearchConnection

Allows the destination domain owner to delete an existing inbound cross-cluster search connection.

Syntax

```
DELETE https://es.us-east-1.amazonaws.com/2015-01-01/es/ccs/inboundConnection/{ConnectionId}
```

Request parameters

This operation does not use HTTP request parameters.

Request body

This operation does not use the HTTP request body.

Response elements

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CrossClusterSearchConnection</td>
<td><code>Object</code></td>
<td>Inbound connection details.</td>
</tr>
</tbody>
</table>

DeleteOutboundCrossClusterSearchConnection

Allows the source domain owner to delete an existing outbound cross-cluster search connection.

Syntax

```
DELETE https://es.us-east-1.amazonaws.com/2015-01-01/es/ccs/outboundConnection/{ConnectionId}
```
Request parameters

This operation does not use HTTP request parameters.

Request body

This operation does not use the HTTP request body.

Response elements

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CrossClusterSearchConnection</td>
<td>Object</td>
<td>Outbound connection details.</td>
</tr>
</tbody>
</table>

DeletePackage

Deletes a package from Amazon ES. The package must not be associated with any Amazon ES domain.

Syntax

DELETE https://es.us-east-1.amazonaws.com/2015-01-01/packages/package-id

Request parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PackageID</td>
<td>String</td>
<td>Yes</td>
<td>Internal ID of the package that you want to delete. Use the section called &quot;DescribePackages&quot; (p. 356) to find this value.</td>
</tr>
</tbody>
</table>

Request body

This operation does not use the HTTP request body.

Response elements

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>PackageDetails</td>
<td>the section called &quot;PackageDetails&quot; (p. 389)</td>
</tr>
</tbody>
</table>

DescribeDomainAutoTunes

Returns the list of optimizations that Auto-Tune has made to the domain.
DescribeElasticsearchDomain

Syntax

GET https://es.us-east-1.amazonaws.com/2015-01-01/es/domain/domain-name/autoTunes

Request parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainName</td>
<td>the section called “DomainName” (p. 381)</td>
<td>Yes</td>
<td>Name of the Amazon ES domain that you want Auto-Tune details about.</td>
</tr>
</tbody>
</table>

Request body

This operation does not use the HTTP request body.

Response elements

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoTunes</td>
<td>List</td>
<td>List of optimizations.</td>
</tr>
<tr>
<td>NextToken</td>
<td>String</td>
<td>Used for pagination. Only necessary if a previous API call produced a result containing NextToken. Accepts a next-token input to return results for the next page, and provides a next-token output in the response, which clients can use to retrieve more results.</td>
</tr>
</tbody>
</table>

DescribeElasticsearchDomain

Describes the domain configuration for the specified Amazon ES domain, including the domain ID, domain service endpoint, and domain ARN.

Syntax

GET https://es.us-east-1.amazonaws.com/2015-01-01/es/domain/domain-name

Request parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainName</td>
<td>the section called “DomainName” (p. 381)</td>
<td>Yes</td>
<td>Name of the Amazon ES domain that you want Auto-Tune details about.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Data Type</td>
<td>Required?</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------</td>
<td>-----------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>domain that you want to describe.</td>
</tr>
</tbody>
</table>

### Request body

This operation does not use the HTTP request body.

### Response elements

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainStatus</td>
<td>the section called “ElasticsearchDomainStatus” (p. 384)</td>
<td></td>
</tr>
</tbody>
</table>

### DescribeElasticsearchDomainConfig

Displays the configuration of an Amazon ES domain.

### Syntax

GET https://es.us-east-1.amazonaws.com/2015-01-01/es/domain/domain-name/config

### Request parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainName</td>
<td>the section called “DomainName” (p. 381)</td>
<td>Yes</td>
<td>Name of the Amazon ES domain configuration that you want to describe.</td>
</tr>
</tbody>
</table>

### Request body

This operation does not use the HTTP request body.

### Response elements

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainConfig</td>
<td>the section called “ElasticsearchDomainConfig” (p. 383)</td>
<td></td>
</tr>
</tbody>
</table>
DescribeElasticsearchDomains

Describes the domain configuration for up to five specified Amazon ES domains. Information includes the domain ID, domain service endpoint, and domain ARN.

Syntax

```
POST https://es.us-east-1.amazonaws.com/2015-01-01/es/domain-info
{
   "DomainNames": [ 
      "domain-name1",
      "domain-name2",
   ]
}
```

Request parameters

This operation does not use HTTP request parameters.

Request body

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainNames</td>
<td>the section called &quot;DomainNameList&quot; (p. 381)</td>
<td>Yes</td>
<td>Array of Amazon ES domain names.</td>
</tr>
</tbody>
</table>

Response elements

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainStatusList</td>
<td>the section called &quot;ElasticsearchDomainStatusList&quot; (p. 386)</td>
</tr>
</tbody>
</table>

DescribeElasticsearchInstanceTypeLimits

Describes the instance count, storage, and master node limits for a given Elasticsearch version and instance type.

Syntax

```
GET https://es.us-east-1.amazonaws.com/2015-01-01/es/instanceTypeLimits/elasticsearch-version/instance-type?domainName=domain-name
```

Request parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ElasticsearchVersion</td>
<td>String</td>
<td>Yes</td>
<td>Elasticsearch version. For a list of supported versions, see</td>
</tr>
</tbody>
</table>


DescribeInboundCrossClusterSearchConnections

This operation lists all the inbound cross-cluster search connections for a destination domain.

**Syntax**

```json
{
    "Filters": [
    {
        "Name": filter-name (str),
        "Values": [val1, val2, ..] (list of strings)
    },
    ...
    "MaxResults": int (Optional, default value = 100),
    "NextToken": "next-token-string (optional)"
}
```

**Response elements**

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LimitsByRole</td>
<td>Map</td>
<td>Map that contains all applicable instance type limits. &quot;data&quot; refers to data nodes. &quot;master&quot; refers to dedicated master nodes.</td>
</tr>
</tbody>
</table>

**Request parameters**

This operation does not use HTTP request parameters.
Request body

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filters</td>
<td>Object</td>
<td>Yes</td>
<td>List of filter names and values that you can use for the &quot;Describe&quot; requests. The following fields are supported: cross-cluster-search-connection-id, source-domain-info.domain-name, source-domain-info.owner-id, source-domain-info.region, and destination-domain-info.domain-name.</td>
</tr>
<tr>
<td>MaxResults</td>
<td>Integer</td>
<td>No</td>
<td>Limits the number of results. The default is 100.</td>
</tr>
<tr>
<td>NextToken</td>
<td>String</td>
<td>No</td>
<td>Used for pagination. Only necessary if a previous API call produced a result containing NextToken. Accepts a next-token input to return results for the next page, and provides a next-token output in the response, which clients can use to retrieve more results.</td>
</tr>
</tbody>
</table>

Response elements

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CrossClusterSearchConnections</td>
<td>Object</td>
<td>List of inbound connections.</td>
</tr>
<tr>
<td>NextToken</td>
<td>String</td>
<td>Used for pagination. Only necessary if a previous API call produced a result containing NextToken. Accepts a next-token input to return results for the next page, and provides a next-token output in the response, which clients can use to retrieve more results.</td>
</tr>
</tbody>
</table>

DescribeOutboundCrossClusterSearchConnections

Lists all outbound cross-cluster search connections for a source domain.

Syntax

```json
POST https://es.us-east-1.amazonaws.com/2015-01-01/es/ccs/outboundConnection/search
{
  "Filters": [
    {
      "Name": filter-name (str),
      "Values" : [val1, val2, ..] (list of strings)
    },
    ...
  
```
"MaxResults": int (Optional, default value = 100),
"NextToken": "next-token-string (optional)"
}

Request parameters

This operation does not use HTTP Request parameters.

Request body

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filters</td>
<td>Object</td>
<td>Yes</td>
<td>List of filter names and values that you can use for the &quot;Describe&quot; requests. The following fields are supported: cross-cluster-search-connection-id, source-domain-info.domain-name, source-domain-info.owner-id, source-domain-info.region, and destination-domain-info.domain-name</td>
</tr>
<tr>
<td>MaxResults</td>
<td>Integer</td>
<td>No</td>
<td>Limits the number of results. The default is 100.</td>
</tr>
<tr>
<td>NextToken</td>
<td>String</td>
<td>No</td>
<td>Used for pagination. Only necessary if a previous API call produced a result containing NextToken. Accepts a next-token input to return results for the next page, and provides a next-token output in the response, which clients can use to retrieve more results.</td>
</tr>
</tbody>
</table>

Response elements

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CrossClusterSearchConnections</td>
<td>Object</td>
<td>List of outbound connections.</td>
</tr>
<tr>
<td>NextToken</td>
<td>String</td>
<td>Used for pagination. Only necessary if a previous API call produced a result containing NextToken. Accepts a next-token input to return results for the next page, and provides a next-token output in the response, which clients can use to retrieve more results.</td>
</tr>
</tbody>
</table>

**DescribePackages**

Describes all packages available to Amazon ES. Includes options for filtering, limiting the number of results, and pagination.
Syntax

POST https://es.us-east-1.amazonaws.com/2015-01-01/packages/describe
{
    "Filters": [{
        "Name": "PackageStatus",
        "Value": [
            "DELETING", "AVAILABLE"
        ]
    }],
    "MaxResults": 5,
    "NextToken": "next-token",
}

Request parameters

This operation does not use request parameters.

Request body

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filters</td>
<td>the section called &quot;Filters&quot; (p. 387)</td>
<td>No</td>
<td>Only returns packages that match the provided values.</td>
</tr>
<tr>
<td>MaxResults</td>
<td>Integer</td>
<td>No</td>
<td>Limits results to a maximum number of packages.</td>
</tr>
<tr>
<td>NextToken</td>
<td>String</td>
<td>No</td>
<td>Used for pagination. Only necessary if a previous API call includes a non-null NextToken value. If provided, returns results for the next page.</td>
</tr>
</tbody>
</table>

Response elements

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PackageDetailsList</td>
<td>List</td>
<td>List of the section called &quot;PackageDetails&quot; (p. 389) objects.</td>
</tr>
</tbody>
</table>

DescribeReservedElasticsearchInstanceOfferings

Describes the available Reserved Instance offerings for a given Region.

Syntax

GET https://es.us-east-1.amazonaws.com/2015-01-01/es/reservedInstanceOfferings?
offeringId=offering-id&maxResults=max-results&nextToken=next-token
Request parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OfferId</td>
<td>String</td>
<td>No</td>
<td>The offering ID.</td>
</tr>
<tr>
<td>MaxResults</td>
<td>Integer</td>
<td>No</td>
<td>Limits the number of results. Must be between 30 and 100.</td>
</tr>
<tr>
<td>NextToken</td>
<td>String</td>
<td>No</td>
<td>Used for pagination. Only necessary if a previous API call produced a result that contains NextToken. Accepts a next-token input to return results for the next page, and provides a next-token output in the response, which clients can use to retrieve more results.</td>
</tr>
</tbody>
</table>

Request body

This operation does not use the HTTP request body.

Response elements

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReservedElasticsearchInstance</td>
<td></td>
<td>Container for all information about a Reserved Instance offering. For more information, see the section called “Purchasing Reserved Instances (AWS CLI)” (p. 303).</td>
</tr>
</tbody>
</table>

DescribeReservedElasticsearchInstances

Describes the instance that you have reserved in a given Region.

Syntax

GET https://es.us-east-1.amazonaws.com/2015-01-01/es/reservedInstances?reservationId=reservation-id&maxResults=max-results&nextToken=next-token

Request parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReservationId</td>
<td>String</td>
<td>No</td>
<td>The reservation ID, assigned after you purchase a reservation.</td>
</tr>
</tbody>
</table>
DissociatePackage

Removes the package from the specified Amazon ES domain. The package must not be in use with any ES index for dissociate to succeed. The package will still be available in the Amazon ES service for associating later.

Syntax

POST https://es.us-east-1.amazonaws.com/2015-01-01/packages/dissociate/package-id/domain-name

Request parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PackageID</td>
<td>String</td>
<td>Yes</td>
<td>Internal ID of the package that you want to dissociate from the domain. Use the section called “ListPackagesForDomain” (p. 368) to find this value.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Data Type</td>
<td>Required?</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------</td>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DomainName</td>
<td>the section called “DomainName” (p. 381)</td>
<td>Yes</td>
<td>Name of the domain that you want to dissociate the package from.</td>
</tr>
</tbody>
</table>

Request body

This operation does not use the HTTP request body.

Response elements

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainPackageDetails</td>
<td>the section called “DomainPackageDetails” (p. 381)</td>
</tr>
</tbody>
</table>

GetCompatibleElasticsearchVersions

Returns a map of Elasticsearch versions and the versions you can upgrade them to.

Syntax

GET https://es.us-east-1.amazonaws.com/2015-01-01/es/compatibleVersions?domainName=domain-name

Request parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainName</td>
<td>the section called “DomainName” (p. 381)</td>
<td>No</td>
<td>The name of an existing domain.</td>
</tr>
</tbody>
</table>

Request body

This operation does not use the HTTP request body.

Response elements

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CompatibleElasticsearchVersions</td>
<td>Map</td>
<td>A map of Elasticsearch versions and the versions that you can upgrade them to:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;CompatibleElasticsearchVersions&quot;: [</td>
</tr>
<tr>
<td></td>
<td></td>
<td>]</td>
</tr>
</tbody>
</table>

API Version 2015-01-01 360
GetPackageVersionHistory

Returns a map of Elasticsearch versions and the versions you can upgrade them to.

Syntax

GET https://es.us-east-1.amazonaws.com/2015-01-01/packages/package-id/history?maxResults=max-results&nextToken=next-token

Request parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PackageID</td>
<td>String</td>
<td>Yes</td>
<td>The name of an existing domain.</td>
</tr>
<tr>
<td>MaxResults</td>
<td>Integer</td>
<td>No</td>
<td>Limits the number of results. Must be between 30 and 100.</td>
</tr>
<tr>
<td>NextToken</td>
<td>String</td>
<td>No</td>
<td>Used for pagination. Only necessary if a previous API call produced a result containing NextToken. Accepts a next-token input to return results for the next page, and provides a next-token output in the response, which clients can use to retrieve more results.</td>
</tr>
</tbody>
</table>

Request body

This operation does not use the HTTP request body.

Response elements

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PackageVersionHistoryList</td>
<td>Map</td>
<td>A list of commit messages, updates times, and versions for the given package:</td>
</tr>
</tbody>
</table>

"PackageVersionHistoryList": [ 

GetUpgradeHistory

Returns a list of the domain's 10 most-recent upgrade operations.

Syntax

```
GET https://es.us-east-1.amazonaws.com/2015-01-01/es/upgradeDomain/domain-name/history?
maxResults=max-results&amp;nextToken=next-token
```

Request parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaxResults</td>
<td>Integer</td>
<td>No</td>
<td>Limits the number of results. Must be between 30 and 100.</td>
</tr>
<tr>
<td>DomainName</td>
<td>the section called &quot;DomainName&quot; (p. 381)</td>
<td>Yes</td>
<td>The name of an existing domain.</td>
</tr>
<tr>
<td>NextToken</td>
<td>String</td>
<td>No</td>
<td>Used for pagination. Only necessary if a previous API call produced a result containing NextToken. Accepts a next-token input to return results for the next page, and provides a next-token output in the response, which clients can use to retrieve more results.</td>
</tr>
</tbody>
</table>

Request body

This operation does not use the HTTP request body.

Response elements

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UpgradeHistoryList</td>
<td>UpgradeHistoryList</td>
<td>Container for result logs of the past 10 upgrade operations.</td>
</tr>
</tbody>
</table>
GetUpgradeStatus

Returns the most-recent status of a domain's Elasticsearch version upgrade.

Syntax

```
GET https://es.us-east-1.amazonaws.com/2015-01-01/es/upgradeDomain/domain-name/status
```

Request parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainName</td>
<td>the section called &quot;DomainName&quot; (p. 381)</td>
<td>Yes</td>
<td>The name of an existing domain.</td>
</tr>
</tbody>
</table>

Request body

This operation does not use the HTTP request body.

Response elements

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UpgradeStepItem</td>
<td>UpgradeStepItem</td>
<td>Container for the most-recent status of a domain's version upgrade.</td>
</tr>
</tbody>
</table>

ListDomainNames

Displays the names of all Amazon ES domains owned by the current user in the active Region.

Syntax

```
GET https://es.us-east-1.amazonaws.com/2015-01-01/domain
```

Request parameters

This operation does not use request parameters.

Request body

This operation does not use the HTTP request body.
ListDomainsForPackage

Lists all Amazon ES domains that a package is associated with.

**Syntax**

```
GET https://es.us-east-1.amazonaws.com/2015-01-01/packages/package-id/domains?
maxResults=max-results&amp;nextToken=next-token
```

**Request parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PackageID</td>
<td>String</td>
<td>Yes</td>
<td>The package for which to list domains.</td>
</tr>
<tr>
<td>MaxResults</td>
<td>Integer</td>
<td>No</td>
<td>Limits the number of results.</td>
</tr>
<tr>
<td>NextToken</td>
<td>String</td>
<td>No</td>
<td>Used for pagination. Only necessary if a previous API call produced a result that contains NextToken. Accepts a next-token input to return results for the next page, and provides a next-token output in the response, which clients can use to retrieve more results.</td>
</tr>
</tbody>
</table>

**Response elements**

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainNameList</td>
<td>DomainNameList (p. 381)</td>
<td>The names of all Amazon ES domains owned by the current user.</td>
</tr>
<tr>
<td>DomainPackageDetailsList</td>
<td>List</td>
<td>List of the section called &quot;DomainPackageDetails&quot; (p. 381) objects.</td>
</tr>
<tr>
<td>NextToken</td>
<td>String</td>
<td>Used for pagination. Only necessary if a previous API call produced a result containing NextToken. Accepts a next-</td>
</tr>
</tbody>
</table>
### ListElasticsearchInstanceTypeDetails

Lists all Elasticsearch instance types that are supported for a given Elasticsearch version and the features that these instance types support.

#### Syntax

```
GET https://es.us-east-1.amazonaws.com/2015-01-01/es/instanceTypeDetails/elasticsearch-version?domainName=domain-name&maxResults=max-results&nextToken=next-token
```

#### Request parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ElasticsearchVersion</td>
<td>String</td>
<td>Yes</td>
<td>The Elasticsearch version.</td>
</tr>
<tr>
<td>DomainName</td>
<td>String</td>
<td>No</td>
<td>The Amazon ES domain name.</td>
</tr>
<tr>
<td>MaxResults</td>
<td>Integer</td>
<td>No</td>
<td>Limits the number of results. Must be between 30 and 100.</td>
</tr>
<tr>
<td>NextToken</td>
<td>String</td>
<td>No</td>
<td>Used for pagination. Only necessary if a previous API call produced a result containing NextToken. Accepts a next-token input to return results for the next page, and provides a next-token output in the response, which clients can use to retrieve more results.</td>
</tr>
</tbody>
</table>

#### Request body

This operation does not use the HTTP request body.

#### Response elements

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ElasticsearchInstanceTypes</td>
<td>List</td>
<td>List of supported instance types for the given Elasticsearch version and the features that these instance types support.</td>
</tr>
<tr>
<td>NextToken</td>
<td>String</td>
<td>Used for pagination. Only necessary if a previous API call produced a result</td>
</tr>
</tbody>
</table>
ListElasticsearchInstanceTypes (Deprecated)

Lists all Elasticsearch instance types that are supported for a given Elasticsearch version. This action is deprecated. Use ListElasticsearchInstanceTypeDetails (p. 365) instead.

Syntax

GET https://es.us-east-1.amazonaws.com/2015-01-01/es/instanceTypes/elasticsearch-version?domainName=domain-name&maxResults=max-results&nextToken=next-token

Request parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ElasticsearchVersion</td>
<td>String</td>
<td>Yes</td>
<td>The Elasticsearch version.</td>
</tr>
<tr>
<td>DomainName</td>
<td>String</td>
<td>No</td>
<td>The Amazon ES domain name.</td>
</tr>
<tr>
<td>MaxResults</td>
<td>Integer</td>
<td>No</td>
<td>Limits the number of results. Must be between 30 and 100.</td>
</tr>
<tr>
<td>NextToken</td>
<td>String</td>
<td>No</td>
<td>Used for pagination. Only necessary if a previous API call produced a result containing NextToken. Accepts a next-token input to return results for the next page, and provides a next-token output in the response, which clients can use to retrieve more results.</td>
</tr>
</tbody>
</table>

Request body

This operation does not use the HTTP request body.

Response elements

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ElasticsearchInstanceTypes</td>
<td>List</td>
<td>List of supported instance types for the given Elasticsearch version.</td>
</tr>
<tr>
<td>NextToken</td>
<td>String</td>
<td>Used for pagination. Only necessary if a previous API call produced a result containing NextToken. Accepts a next-token input to return results for the next page, and provides a next-token output in the response, which clients can use to retrieve more results.</td>
</tr>
</tbody>
</table>
ListElasticsearchVersions

Lists all supported Elasticsearch versions on Amazon ES.

Syntax

GET https://es.us-east-1.amazonaws.com/2015-01-01/es/versions?maxResults=max-results&nextToken=next-token

Request parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaxResults</td>
<td>Integer</td>
<td>No</td>
<td>Limits the number of results. Must be between 30 and 100.</td>
</tr>
<tr>
<td>NextToken</td>
<td>String</td>
<td>No</td>
<td>Used for pagination. Only necessary if a previous API call produced a result containing NextToken. Accepts a next-token input to return results for the next page, and provides a next-token output in the response, which clients can use to retrieve more results.</td>
</tr>
</tbody>
</table>

Request body

This operation does not use the HTTP request body.

Response elements

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ElasticsearchVersions</td>
<td>List</td>
<td>Lists all supported Elasticsearch versions.</td>
</tr>
<tr>
<td>NextToken</td>
<td>String</td>
<td>Used for pagination. Only necessary if a previous API call produced a result containing NextToken. Accepts a next-token input to return results for the next page, and provides a next-token output in the response, which clients can use to retrieve more results.</td>
</tr>
</tbody>
</table>
ListPackagesForDomain

Lists all packages associated with the Amazon ES domain.

Syntax

```
GET https://es.us-east-1.amazonaws.com/2015-01-01/domain/domain-name/packages?
maxResults=max-results&amp;nextToken=next-token
```

Request parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainName</td>
<td>String</td>
<td>Yes</td>
<td>The name of the domain for which you want to list associated packages.</td>
</tr>
<tr>
<td>MaxResults</td>
<td>Integer</td>
<td>No</td>
<td>Limits the number of results.</td>
</tr>
<tr>
<td>NextToken</td>
<td>String</td>
<td>No</td>
<td>Used for pagination. Only necessary if a previous API call produced a result containing NextToken. Accepts a next-token input to return results for the next page, and provides a next-token output in the response, which clients can use to retrieve more results.</td>
</tr>
</tbody>
</table>

Request body

This operation does not use the HTTP request body.

Response elements

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainPackageDetailsList</td>
<td>list</td>
<td>List of the section called &quot;DomainPackageDetails&quot; (p. 381) objects.</td>
</tr>
<tr>
<td>NextToken</td>
<td>String</td>
<td>Used for pagination. Only necessary if a previous API call produced a result containing NextToken. Accepts a next-token input to return results for the next page, and provides a next-token output in the response, which clients can use to retrieve more results.</td>
</tr>
</tbody>
</table>

ListTags

Displays all resource tags for an Amazon ES domain.
Syntax

**PurchaseReservedElasticsearchInstanceOffering**

Purchases a Reserved Instance.

**Syntax**


```json
{
   "ReservationName" : "my-reservation",
   "ReservedElasticsearchInstanceOfferingId" : "1a2a3a4a5-1a2a-3a4a-5a6a-1a2a3a4a5a6a",
   "InstanceCount" : 3
}
```

**Request parameters**

This operation does not use HTTP request parameters.

**Request body**

This operation does not use the HTTP request body.

**Response elements**

**Name** | **Data Type** | **Required?** | **Description**
--- | --- | --- | ---
ReservationName | String | Yes | A descriptive name for your reservation.
ReservedElasticsearchInstanceOfferingId | String | Yes | The offering ID.
InstanceCount | Integer | Yes | The number of instances that you want to reserve.
Response elements

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReservationName</td>
<td>String</td>
<td>The name of your reservation.</td>
</tr>
<tr>
<td>ReservedElasticInstanceId</td>
<td>String</td>
<td>The reservation ID.</td>
</tr>
</tbody>
</table>

RejectInboundCrossClusterSearchConnection

Allows the destination domain owner to reject an inbound cross-cluster search connection request.

Syntax

```
PUT https://es.us-east-1.amazonaws.com/2015-01-01/es/ccs/inboundConnection/{ConnectionId}/reject
```

Request parameters

This operation does not use HTTP request parameters.

Request body

This operation does not use the HTTP request body.

Response elements

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CrossClusterSearchConnection</td>
<td>Object</td>
<td>Inbound connection details.</td>
</tr>
</tbody>
</table>

RemoveTags

Removes the specified resource tags from an Amazon ES domain.

Syntax

```
POST https://es.us-east-1.amazonaws.com/2015-01-01/tags-removal
{
  "TagKeys": [
    "tag-key1",
    "tag-key2"
  ]
}
```

Request parameters

This operation does not use HTTP request parameters.
Request body

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARN</td>
<td>ARN (p. 378)</td>
<td>Yes</td>
<td>Amazon Resource Name (ARN) of an Amazon ES domain. For more information, see Identifiers for IAM Entities in Using AWS Identity and Access Management.</td>
</tr>
<tr>
<td>TagKeys</td>
<td>TagKey (p. 392)</td>
<td>Yes</td>
<td>List of tag keys for resource tags that you want to remove from an Amazon ES domain.</td>
</tr>
</tbody>
</table>

Response elements
The RemoveTags operation does not return a response element.

StartElasticsearchServiceSoftwareUpdate
Schedules a service software update for an Amazon ES domain.

Syntax
```
POST https://es.us-east-1.amazonaws.com/2015-01-01/es/serviceSoftwareUpdate/start
{
  "DomainName": "domain-name"
}
```

Request parameters
This operation does not use HTTP request parameters.

Request body

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainName</td>
<td>DomainName (p. 381)</td>
<td>Yes</td>
<td>Name of the Amazon ES domain that you want to update to the latest service software.</td>
</tr>
</tbody>
</table>

Response elements

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServiceSoftwareOptions</td>
<td></td>
<td>Container for the state of your domain relative to the latest service software.</td>
</tr>
</tbody>
</table>

StopElasticsearchServiceSoftwareUpdate
Stops a scheduled service software update for an Amazon ES domain. Only works if the domain's UpdateStatus is PENDING_UPDATE.
Syntax

{
  "DomainName": "domain-name"
}

Request parameters

This operation does not use HTTP request parameters.

Request body

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainName</td>
<td>DomainName(p.381)</td>
<td>Yes</td>
<td>Name of the Amazon ES domain that you want to update to the latest service software.</td>
</tr>
</tbody>
</table>

Response elements

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServiceSoftwareOptions</td>
<td>ServiceSoftwareOptions</td>
<td>Container for the state of your domain relative to the latest service software.</td>
</tr>
</tbody>
</table>

UpdateElasticsearchDomainConfig

Modifies the configuration of an Amazon ES domain, such as the instance type and the number of instances. You need to specify only the values that you want to update.

Syntax

{
  "ElasticsearchClusterConfig": {
    "ZoneAwarenessConfig": {
      "AvailabilityZoneCount": 3
    },
    "ZoneAwarenessEnabled": true|false,
    "InstanceCount": 3,
    "DedicatedMasterEnabled": true|false,
    "DedicatedMasterType": "c5.large.elasticsearch",
    "DedicatedMasterCount": 3,
    "InstanceType": "r5.large.elasticsearch",
    "WarmCount": 6,
    "WarmType": "ultrawarm1.medium.elasticsearch",
    "ColdStorageOptions": {
      "Enabled": true|false
    },
    "EBSOptions": {
      "EBSEnabled": true|false,
      "VolumeType": "io1|gp2|standard",
      "Iops": 1000
    }
  },
"VolumeSize": 35,
"SnapshotOptions": {
    "AutomatedSnapshotStartHour": 3
},
"EncryptionAtRestOptions": {
    "Enabled": true|false,
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:alias/my-key"
},
"NodeToNodeEncryptionOptions": {
    "Enabled": true|false
},
"VPCOptions": {
    "SubnetIds": ["subnet-abcdefg1", "subnet-abcdefg2", "subnet-abcdefg3"],
    "SecurityGroupIds": ["sg-12345678"]
},
"AdvancedOptions": {
    "rest.action.multi.allow_explicit_index": true|false,
    "indices.fielddata.cache.size": "40",
    "indices.query.bool.max_clause_count": "1024"
},
"CognitoOptions": {
    "Enabled": true|false,
    "UserPoolId": "us-east-1_121234567",
    "IdentityPoolId": "us-east-1:12345678-1234-1234-1234-123456789012",
    "RoleArn": "arn:aws:iam::123456789012:role/service-role/CognitoAccessForAmazonES"
},
"DomainEndpointOptions": {
    "EnforceHTTPS": true|false,
    "CustomEndpointEnabled": true|false,
    "CustomEndpoint": "www.my-custom-endpoint.com",
    "CustomEndpointCertificateArn": "arn:aws:iam::123456789012:certificate/my-certificate"
},
"LogPublishingOptions": {
    "SEARCH_SLOW_LOGS": {
        "Enabled": true|false
    },
    "INDEX_SLOW_LOGS": {
        "Enabled": true|false
    },
    "ES_APPLICATION_LOGS": {
        "Enabled": true|false
    }
},
"AdvancedSecurityOptions": {
    "Enabled": true|false,
    "InternalUserDatabaseEnabled": true|false,
    "MasterUserOptions": {
        "MasterUserARN": "arn:aws:iam::123456789012:role/my-master-user-role",
        "MasterUserName": "my-master-username",
        "MasterUserPassword": "my-master-password"
    },
    "SAMLOptions": {
        "Enabled": true,
        "Idp": {
            "EntityId": "entity-id",
            "MetadataContent": "metadata-content-with-quotes-escaped"
        },
        "RolesKey": "optional-roles-key"}
Request parameters

This operation does not use HTTP request parameters.

Request body

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainName</td>
<td>DomainName (p. 381)</td>
<td>Yes</td>
<td>Name of the Amazon ES domain for which you want to update the configuration.</td>
</tr>
<tr>
<td>ElasticsearchClusterConfig</td>
<td>ElasticsearchClusterConfig (p. 382)</td>
<td>No</td>
<td>Changes that you want to make to the cluster configuration, such as the instance type and number of EC2 instances.</td>
</tr>
<tr>
<td>EBSOptions</td>
<td>EBSOptions (p. 382)</td>
<td>No</td>
<td>Type and size of EBS volumes attached to data nodes.</td>
</tr>
<tr>
<td>VPCOptions</td>
<td>VPCOptions (p. 393)</td>
<td>No</td>
<td>Container for the values required to configure Amazon ES to work with a VPC. To learn more, see Launching your Amazon Elasticsearch Service domains using a VPC (p. 22).</td>
</tr>
<tr>
<td>SnapshotOptions</td>
<td>SnapshotOptions (p. 391)</td>
<td>No</td>
<td>DEPRECATED. Hour during which the service takes an automated daily snapshot of the indices in the Amazon ES domain.</td>
</tr>
<tr>
<td>AdvancedOptions</td>
<td>AdvancedOptions (p. 377)</td>
<td>No</td>
<td>Key-value pairs to specify advanced configuration options. For more information, see Configuring Advanced Options (p. 13).</td>
</tr>
<tr>
<td>AccessPolicies</td>
<td>String</td>
<td>No</td>
<td>Specifies the access policies for the Amazon ES domain. For more</td>
</tr>
</tbody>
</table>
UpdatePackage

Update a package for use with Amazon ES domains.

**Syntax**

```json
POST https://es.us-east-1.amazonaws.com/2015-01-01/packages/update
{
  "PackageID": "F11111111",
  "PackageDescription": "My synonym file.",
  "CommitMessage": "Added some synonyms.",
  "PackageSource": {
    "S3BucketName": "my-s3-bucket",
    "S3Key": "synonyms.txt"
  }
}
```

**Request parameters**

This operation does not use request parameters.
UpgradeElasticsearchDomain

Upgrades an Amazon ES domain to a new version of Elasticsearch. Alternately, checks upgrade eligibility.

Syntax

POST https://es.us-east-1.amazonaws.com/2015-01-01/es/upgradeDomain
{
  "DomainName": "domain-name",
  "TargetVersion": "7.8",
  "PerformCheckOnly": true|false
}

Request parameters

This operation does not use HTTP request parameters.

Request body

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainName</td>
<td>String</td>
<td>Yes</td>
<td>Name of the Amazon ES domain that you want to upgrade.</td>
</tr>
<tr>
<td>TargetVersion</td>
<td>String</td>
<td>Yes</td>
<td>Elasticsearch version to which you want to upgrade. See the section called &quot;GetCompatibleElasticsearchVersions&quot; (p. 360).</td>
</tr>
<tr>
<td>PerformCheckOnly</td>
<td>Boolean</td>
<td>No</td>
<td>Defaults to false. If true, Amazon ES checks the eligibility of the</td>
</tr>
</tbody>
</table>
### Data Types

This section describes the data types used by the configuration API.

#### AdvancedOptions

Key-value pairs to specify advanced Elasticsearch configuration options.

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rest.action.multi.allow_explicit_index</td>
<td>Key-value pair:</td>
<td>Note the use of a string rather than a boolean. Specifies whether explicit references to indices are allowed inside the body of HTTP requests. If you want to configure access policies for domain sub-resources, such as specific indices and domain APIs, you must disable this property. For more information about access policies for sub-resources, see Configuring Access Policies (p. 13).</td>
</tr>
<tr>
<td>indices.fielddata.cache.size</td>
<td>Key-value pair:</td>
<td>Note the use of a string rather than an integer. Specifies the percentage of Java heap space that is allocated to field data. By default, this setting is unbounded.</td>
</tr>
<tr>
<td>indices.query.bool.max_clause_count</td>
<td>Key-value pair:</td>
<td>Note the use of a string rather than an integer. Specifies the maximum</td>
</tr>
</tbody>
</table>
## AdvancedSecurityOptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Boolean</td>
<td>True to enable fine-grained access control (p. 90).</td>
</tr>
<tr>
<td>InternalUserDatabaseEnabled</td>
<td>Boolean</td>
<td>True to enable the internal user database.</td>
</tr>
<tr>
<td>MasterUserOptions</td>
<td>the section called “MasterUserOptions” (p. 388)</td>
<td>Container for information about the master user.</td>
</tr>
<tr>
<td>SAMLOptions</td>
<td>SAMLOptions</td>
<td>Container for information about the SAML configuration for Kibana.</td>
</tr>
</tbody>
</table>

## ARN

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARN</td>
<td>String</td>
<td>Amazon Resource Name (ARN) of an Amazon ES domain. For more information, see IAM ARNs in the AWS Identity and Access Management documentation.</td>
</tr>
</tbody>
</table>

## AutoTuneOptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DesiredState</td>
<td>String</td>
<td>Either ENABLED or DISABLED.</td>
</tr>
<tr>
<td>MaintenanceSchedule</td>
<td>List</td>
<td>A list of maintenance schedules during which Auto-Tune can deploy changes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;StartAt&quot;: 1234567890,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;Duration&quot;: {</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;Value&quot;: 2,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;Unit&quot;: &quot;HOURS&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>}</td>
</tr>
</tbody>
</table>

API Version 2015-01-01
CognitoOptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Boolean</td>
<td>Whether to enable or disable Amazon Cognito authentication for Kibana. See the section called &quot;Amazon Cognito authentication for Kibana&quot; (p. 128).</td>
</tr>
<tr>
<td>UserPoolId</td>
<td>String</td>
<td>The Amazon Cognito user pool ID that you want Amazon ES to use for Kibana authentication.</td>
</tr>
<tr>
<td>IdentityPoolId</td>
<td>String</td>
<td>The Amazon Cognito identity pool ID that you want Amazon ES to use for Kibana authentication.</td>
</tr>
<tr>
<td>RoleArn</td>
<td>String</td>
<td>The AmazonESCognitoAccess role that allows Amazon ES to configure your user pool and identity pool.</td>
</tr>
</tbody>
</table>

ColdStorageOptions

Container for the parameters required to enable cold storage for an Amazon ES domain.

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Boolean</td>
<td>Whether to enable or disable cold storage on the domain. See the section called “Cold storage” (p. 231).</td>
</tr>
</tbody>
</table>
CreateElasticsearchDomainRequest

Container for the parameters required by the CreateElasticsearchDomain service operation.

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainName</td>
<td>DomainName (p. 381)</td>
<td>Name of the Amazon ES domain to create.</td>
</tr>
<tr>
<td>ElasticsearchClusterConfig</td>
<td></td>
<td>Container for the cluster configuration of an Amazon ES domain.</td>
</tr>
<tr>
<td>EBSOptions</td>
<td>EBSOptions (p. 382)</td>
<td>Container for the parameters required to enable EBS-based storage for an Amazon ES domain.</td>
</tr>
<tr>
<td>AccessPolicies</td>
<td>String</td>
<td>IAM policy document that specifies the access policies for the new Amazon ES domain. For more information, see Configuring Access Policies (p. 13).</td>
</tr>
<tr>
<td>DomainEndpointOptions</td>
<td>DomainEndpointOptions (p. 380)</td>
<td>Additional options for the domain endpoint, such as whether to require HTTPS for all traffic.</td>
</tr>
<tr>
<td>SnapshotOptions</td>
<td>SnapshotOptions (p. 391)</td>
<td>DEPRECATED. Container for parameters required to configure automated snapshots of domain indices.</td>
</tr>
<tr>
<td>VPCOptions</td>
<td>VPCOptions (p. 393)</td>
<td>Container for the values required to configure Amazon ES to work with a VPC.</td>
</tr>
<tr>
<td>LogPublishingOptions</td>
<td>LogPublishingOptions (p. 387)</td>
<td>Key-value string pairs to configure slow log publishing.</td>
</tr>
<tr>
<td>AdvancedOptions</td>
<td>the section called “AdvancedOptions” (p. 377)</td>
<td>Key-value pairs to specify advanced configuration options.</td>
</tr>
<tr>
<td>CognitoOptions</td>
<td>CognitoOptions (p. 379)</td>
<td>Key-value pairs to configure Amazon ES to use Amazon Cognito authentication for Kibana.</td>
</tr>
<tr>
<td>NodeToNodeEncryptionOptions</td>
<td>NodeToNodeEncryptionOptions</td>
<td>Specify whether to enable node-to-node encryption.</td>
</tr>
</tbody>
</table>

## DomainEndpointOptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EnforceHTTPS</td>
<td>Boolean</td>
<td>true to require that all traffic to the domain arrive over HTTPS.</td>
</tr>
<tr>
<td>TLSSecurityPolicy</td>
<td>String</td>
<td>The minimum TLS version required for traffic to the domain. Valid values are TLS 1.0 (default) or 1.2:</td>
</tr>
</tbody>
</table>

API Version 2015-01-01 380
<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainID</td>
<td>String</td>
<td>Unique identifier for an Amazon ES domain.</td>
</tr>
<tr>
<td>DomainName</td>
<td>String</td>
<td>Name of an Amazon ES domain.</td>
</tr>
<tr>
<td>DomainNameList</td>
<td>String Array</td>
<td>Array of Amazon ES domains in the following format:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[&quot;&lt;Domain_Name&gt;&quot;,&quot;&lt;Domain_Name&gt;&quot;...</td>
</tr>
<tr>
<td>DomainPackageDetails</td>
<td>String</td>
<td>Information on a package that is associated with a domain.</td>
</tr>
</tbody>
</table>

**Field**

- **DomainName**
  - Name of an Amazon ES domain.

**DomainPackageDetails**

- **DomainName**
  - Name of the domain you've associated a package with.
<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainPackageStatus</td>
<td>String</td>
<td>State of the association. Values are ASSOCIATING, ASSOCIATION_FAILED, ACTIVE, DISSOCIATING, and DISSOCIATION_FAILED.</td>
</tr>
<tr>
<td>ErrorDetails</td>
<td>String</td>
<td>Additional information if the package is in an error state. Null otherwise.</td>
</tr>
<tr>
<td>LastUpdated</td>
<td>Timestamp</td>
<td>Timestamp of the most-recent update to the association status.</td>
</tr>
<tr>
<td>PackageID</td>
<td>String</td>
<td>Internal ID of the package.</td>
</tr>
<tr>
<td>PackageName</td>
<td>String</td>
<td>User-specified name of the package.</td>
</tr>
<tr>
<td>PackageType</td>
<td>String</td>
<td>Currently supports only TXT-DICTIONARY.</td>
</tr>
<tr>
<td>ReferencePath</td>
<td>String</td>
<td>Denotes the location of the package on the Amazon ES cluster nodes. It's the same as synonym_path for dictionary files.</td>
</tr>
</tbody>
</table>

**EBSOptions**

Container for the parameters required to enable EBS-based storage for an Amazon ES domain.

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EBSEnabled</td>
<td>Boolean</td>
<td>Indicates whether EBS volumes are attached to data nodes in an Amazon ES domain.</td>
</tr>
<tr>
<td>VolumeType</td>
<td>String</td>
<td>Specifies the type of EBS volumes attached to data nodes.</td>
</tr>
<tr>
<td>VolumeSize</td>
<td>String</td>
<td>Specifies the size (in GiB) of EBS volumes attached to data nodes.</td>
</tr>
<tr>
<td>Iops</td>
<td>String</td>
<td>Specifies the baseline input/output (I/O) performance of EBS volumes attached to data nodes. Applicable only for the Provisioned IOPS EBS volume type.</td>
</tr>
</tbody>
</table>

**ElasticsearchClusterConfig**

Container for the cluster configuration of an Amazon ES domain.

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstanceType</td>
<td>String</td>
<td>Instance type of data nodes in the cluster.</td>
</tr>
<tr>
<td>InstanceCount</td>
<td>Integer</td>
<td>Number of instances in the cluster.</td>
</tr>
<tr>
<td>DedicatedMasterEnabled</td>
<td>Boolean</td>
<td>Indicates whether dedicated master nodes are enabled for the cluster. True if the cluster will use a dedicated master node. False if the cluster will</td>
</tr>
<tr>
<td>Field</td>
<td>Data Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ElasticsearchVersion</td>
<td>String</td>
<td>Elasticsearch version.</td>
</tr>
<tr>
<td>ElasticsearchClusterConfig</td>
<td>ElasticsearchClusterConfig</td>
<td>Container for the cluster configuration of an Amazon ES domain.</td>
</tr>
<tr>
<td>EBSOptions</td>
<td>EBSOptions (p. 382)</td>
<td>Container for EBS options configured for an Amazon ES domain.</td>
</tr>
<tr>
<td>AccessPolicies</td>
<td>String</td>
<td>Specifies the access policies for the Amazon ES domain. For more information, see Configuring Access Policies (p. 13).</td>
</tr>
<tr>
<td>SnapshotOptions</td>
<td>SnapshotOptions (p. 391)</td>
<td>DEPRECATED. Hour during which the service takes an automated daily snapshot of the indices in the Amazon ES domain.</td>
</tr>
</tbody>
</table>
### ElasticsearchDomainStatus

Container for the contents of a DomainStatus data structure.

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainID</td>
<td>DomainID (p. 381)</td>
<td>Unique identifier for an Amazon ES domain.</td>
</tr>
<tr>
<td>DomainName</td>
<td>DomainName (p. 381)</td>
<td>Name of an Amazon ES domain. Domain names are unique across all domains owned by the same account within an AWS Region. 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).</td>
</tr>
<tr>
<td>ARN</td>
<td>ARN (p. 378)</td>
<td>Amazon Resource Name (ARN) of an Amazon ES domain. For more information, see Identifiers for IAM Entities in Using AWS Identity and Access Management.</td>
</tr>
<tr>
<td>Created</td>
<td>Boolean</td>
<td>Status of the creation of an Amazon ES domain. True if creation of the domain is</td>
</tr>
<tr>
<td>Field</td>
<td>Data Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ElasticsearchVersion</td>
<td>String</td>
<td>Elasticsearch version.</td>
</tr>
<tr>
<td>ElasticsearchClusterConfig</td>
<td>ElasticsearchClusterConfig(p. 382)</td>
<td>Container for the cluster configuration of an Amazon ES domain.</td>
</tr>
<tr>
<td>EBSOptions</td>
<td>EBSOptions(p. 382)</td>
<td>Container for the parameters required to enable EBS-based storage for an Amazon ES domain.</td>
</tr>
<tr>
<td>AccessPolicies</td>
<td>String</td>
<td>IAM policy document specifying the access policies for the new Amazon ES domain. For more information, see Configuring Access Policies (p. 13).</td>
</tr>
<tr>
<td>SnapshotOptions</td>
<td>SnapshotOptions(p. 391)</td>
<td>DEPRECATED. Container for parameters required to configure the time of daily automated snapshots of Amazon ES domain indices.</td>
</tr>
<tr>
<td>VPCOptions</td>
<td>VPCDerivedInfo(p. 393)</td>
<td>Information that Amazon ES derives based on VPCOptions (p. 393) for the domain.</td>
</tr>
</tbody>
</table>
### ElasticsearchDomainStatusList

List that contains the status of each specified Amazon ES domain.

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainStatusList</td>
<td>ElasticsearchDomainStatus (p. 384)</td>
<td>List that contains the status of each specified Amazon ES domain.</td>
</tr>
</tbody>
</table>

### EncryptionAtRestOptions

Specifies whether the domain should encrypt data at rest, and if so, the AWS Key Management Service (KMS) key to use. Can be used only to create a new domain, not update an existing one. To learn more, see the section called “Enabling encryption of data at rest” (p. 75).

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Boolean</td>
<td>Specify true to enable encryption at rest.</td>
</tr>
<tr>
<td>KmsKeyId</td>
<td>String</td>
<td>The KMS key ID. Takes the form 1a2a3a4-1a2a-3a4a-5a6a-1a2a3a4a5a6a.</td>
</tr>
</tbody>
</table>
EndpointsMap

The key-value pair that contains the VPC endpoint. Only exists if the Amazon ES domain resides in a VPC.

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoints</td>
<td>Key-value string pair: &quot;vpc&quot;: &quot;&lt;VPC_ENDPOINT&gt;&quot;</td>
<td>The VPC endpoint for the domain.</td>
</tr>
</tbody>
</table>

Filters

Filters the packages included in a the section called “DescribePackages” (p. 356) response.

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String</td>
<td>Any field from the section called “PackageDetails” (p. 389).</td>
</tr>
<tr>
<td>Value</td>
<td>List</td>
<td>A list of values for the specified field.</td>
</tr>
</tbody>
</table>

LogPublishingOptions

Specifies whether the Amazon ES domain publishes the Elasticsearch application and slow logs to Amazon CloudWatch. You still have to enable the collection of slow logs using the Elasticsearch REST API. To learn more, see the section called “Setting Elasticsearch logging thresholds for slow logs” (p. 51).

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INDEX_SLOW_LOGS</td>
<td>Key-value</td>
<td>Two key-value pairs that define the CloudWatch log group and whether the Elasticsearch index slow log should be published there:</td>
</tr>
<tr>
<td>SEARCH_SLOW_LOGS</td>
<td>Key-value</td>
<td>Two key-value pairs that define the CloudWatch log group and whether the Elasticsearch search slow log should be published there:</td>
</tr>
<tr>
<td>ES_APPLICATION_LOGS</td>
<td>Key-value</td>
<td>Two key-value pairs that define the CloudWatch log group and whether the Elasticsearch application logs should be published there:</td>
</tr>
</tbody>
</table>

API Version 2015-01-01
The Elasticsearch error logs should be published there:

```
"Enabled": true
```

## MasterUserOptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MasterUserARN</td>
<td>String</td>
<td>ARN for the master user. Only specify if <code>InternalUserDatabaseEnabled</code> is false in the section called &quot;AdvancedSecurityOptions&quot; (p. 378).</td>
</tr>
<tr>
<td>MasterUserName</td>
<td>String</td>
<td>Username for the master user. Only specify if <code>InternalUserDatabaseEnabled</code> is true in the section called &quot;AdvancedSecurityOptions&quot; (p. 378).</td>
</tr>
<tr>
<td>MasterUserPassword</td>
<td>String</td>
<td>Password for the master user. Only specify if <code>InternalUserDatabaseEnabled</code> is true in the section called &quot;AdvancedSecurityOptions&quot; (p. 378).</td>
</tr>
</tbody>
</table>

## NodeToNodeEncryptionOptions

Enables or disables node-to-node encryption.

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Boolean</td>
<td>Enable with true.</td>
</tr>
</tbody>
</table>

## OptionState

State of an update to advanced options for an Amazon ES domain.

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OptionStatus</td>
<td>String</td>
<td>One of three valid values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• RequiresIndexDocuments</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Processing</td>
</tr>
</tbody>
</table>
### OptionStatus

Status of an update to configuration options for an Amazon ES domain.

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreationDate</td>
<td>Timestamp</td>
<td>Date and time when the Amazon ES domain was created.</td>
</tr>
<tr>
<td>UpdateDate</td>
<td>Timestamp</td>
<td>Date and time when the Amazon ES domain was updated.</td>
</tr>
<tr>
<td>UpdateVersion</td>
<td>Integer</td>
<td>Whole number that specifies the latest version for the entity.</td>
</tr>
<tr>
<td>State</td>
<td>OptionState (p. 388)</td>
<td>State of an update to configuration options for an Amazon ES domain.</td>
</tr>
<tr>
<td>PendingDeletion</td>
<td>Boolean</td>
<td>Indicates whether the service is processing a request to permanently delete the Amazon ES domain and all of its resources.</td>
</tr>
</tbody>
</table>

### PackageDetails

Basic information about a package.

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreatedAt</td>
<td>Timestamp</td>
<td>The time the package was created.</td>
</tr>
<tr>
<td>ErrorDetails</td>
<td>String</td>
<td>Additional information if the package is in an error state. Null otherwise.</td>
</tr>
<tr>
<td>PackageDescription</td>
<td>String</td>
<td>User-specified description of the package.</td>
</tr>
<tr>
<td>PackageID</td>
<td>String</td>
<td>Internal ID of the package.</td>
</tr>
<tr>
<td>PackageName</td>
<td>String</td>
<td>User-specified name of the package.</td>
</tr>
<tr>
<td>PackageStatus</td>
<td>String</td>
<td>Values are COPYING, COPY_FAILED, AVAILABLE, DELETING, or DELETE_FAILED.</td>
</tr>
<tr>
<td>PackageType</td>
<td>String</td>
<td>Currently supports only TXT-DICTIONARY.</td>
</tr>
</tbody>
</table>

### PackageSource

Bucket and key for the package you want to add to Amazon ES.
### SAMLOptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S3BucketName</td>
<td>String</td>
<td>Name of the bucket containing the package.</td>
</tr>
<tr>
<td>S3Key</td>
<td>String</td>
<td>Key (file name) of the package.</td>
</tr>
</tbody>
</table>

### ServiceSoftwareOptions

Container for the state of your domain relative to the latest service software.

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UpdateAvailable</td>
<td>Boolean</td>
<td>Whether a service software update is available for your domain.</td>
</tr>
<tr>
<td>Cancellable</td>
<td>Boolean</td>
<td>If you have requested a domain update, whether or not you can cancel the update.</td>
</tr>
<tr>
<td>AutomatedUpdateDate</td>
<td>Timestamp</td>
<td>The Epoch time that the deployment window closes for required updates.</td>
</tr>
<tr>
<td>Field</td>
<td>Data Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>After this time, Amazon ES schedules the software upgrade automatically.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UpdateStatus</td>
<td>String</td>
<td>The status of the update. Values are ELIGIBLE, PENDING_UPDATE, IN_PROGRESS, COMPLETED, and NOT_ELIGIBLE.</td>
</tr>
<tr>
<td>Description</td>
<td>String</td>
<td>More detailed description of the status.</td>
</tr>
<tr>
<td>CurrentVersion</td>
<td>String</td>
<td>Your current service software version.</td>
</tr>
<tr>
<td>NewVersion</td>
<td>String</td>
<td>The latest service software version.</td>
</tr>
<tr>
<td>OptionalDeployment</td>
<td>Boolean</td>
<td>Whether the service software update is optional.</td>
</tr>
</tbody>
</table>

**ServiceURL**

Domain-specific endpoint used to submit index, search, and data upload requests to an Amazon ES domain.

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServiceURL</td>
<td>String</td>
<td>Domain-specific endpoint used to submit index, search, and data upload requests to an Amazon ES domain.</td>
</tr>
</tbody>
</table>

**SnapshotOptions**

DEPRECATED. See the section called “Creating index snapshots” (p. 51). Container for parameters required to configure the time of daily automated snapshots of the indices in an Amazon ES domain.

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutomatedSnapshotStartHour</td>
<td>Integer</td>
<td>DEPRECATED. Hour during which the service takes an automated daily snapshot of the indices in the Amazon ES domain.</td>
</tr>
</tbody>
</table>

**Tag**

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>TagKey (p. 392)</td>
<td>Required name of the tag. Tag keys must be unique for the Amazon ES domain to which they are attached. For more information, see Tagging Amazon Elasticsearch Service Domains (p. 70).</td>
</tr>
<tr>
<td>Value</td>
<td>TagValue (p. 392)</td>
<td>Optional string value of the tag. Tag values can be null and do not have to be unique in a tag</td>
</tr>
</tbody>
</table>
### TagKey

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>String</td>
<td>Name of the tag. String can have up to 128 characters.</td>
</tr>
</tbody>
</table>

### TagList

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag</td>
<td>Tag (p. 391)</td>
<td>Resource tag attached to an Amazon ES domain.</td>
</tr>
</tbody>
</table>

### TagValue

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>String</td>
<td>Holds the value for a <code>TagKey</code>. String can have up to 256 characters.</td>
</tr>
</tbody>
</table>

### VPCDerivedInfo

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPCId</td>
<td>String</td>
<td>The ID for your VPC. Amazon VPC generates this value when you create a VPC.</td>
</tr>
<tr>
<td>SubnetIds</td>
<td>StringList</td>
<td>A list of subnet IDs associated with the VPC endpoints for the domain. For more information, see <a href="https://docs.aws.amazon.com/vpc/latest/userguide/">VPCs and Subnets</a> in the Amazon VPC User Guide.</td>
</tr>
<tr>
<td>Availability Zones</td>
<td>StringList</td>
<td>The list of Availability Zones associated with the VPC subnets. For more information, see <a href="https://docs.aws.amazon.com/vpc/latest/userguide/">VPC and Subnet Basics</a> in the Amazon VPC User Guide.</td>
</tr>
<tr>
<td>SecurityGroupIds</td>
<td>StringList</td>
<td>The list of security group IDs associated with the VPC endpoints for the domain. For more information, see <a href="https://docs.aws.amazon.com/vpc/latest/userguide/">Security Groups for your VPC</a> in the Amazon VPC User Guide.</td>
</tr>
</tbody>
</table>
VPCOptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SubnetIds</td>
<td>StringList</td>
<td>A list of subnet IDs associated with the VPC endpoints for the domain. If your domain uses multiple Availability Zones, you need to provide two subnet IDs, one per zone. Otherwise, provide only one. To learn more, see <a href="https://docs.aws.amazon.com/vpc/latest/userguide/vpc-subnets.html">VPCs and Subnets</a> in the <em>Amazon VPC User Guide</em>.</td>
</tr>
<tr>
<td>SecurityGroupIds</td>
<td>StringList</td>
<td>The list of security group IDs associated with the VPC endpoints for the domain. If you do not provide a security group ID, Amazon ES uses the default security group for the VPC. To learn more, see <a href="https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-security-groups.html">Security Groups for your VPC</a> in the <em>Amazon VPC User Guide</em>.</td>
</tr>
<tr>
<td>VPCId</td>
<td>String</td>
<td>ID for the VPC.</td>
</tr>
</tbody>
</table>

ZoneAwarenessConfig

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AvailabilityZoneCount</td>
<td>Integer</td>
<td>If you enabled multiple Availability Zones, this field is the number of zones that you want the domain to use. Valid values are 2 and 3.</td>
</tr>
</tbody>
</table>

Errors

Amazon ES throws the following errors:

<table>
<thead>
<tr>
<th>Exception</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BaseException</td>
<td>Thrown for all service errors. Contains the HTTP status code of the error.</td>
</tr>
<tr>
<td>ValidationException</td>
<td>Thrown when the HTTP request contains invalid input or is missing required input. Returns HTTP status code 400.</td>
</tr>
<tr>
<td>DisabledOperationException</td>
<td>Thrown when the client attempts to perform an unsupported operation. Returns HTTP status code 409.</td>
</tr>
<tr>
<td>InternalException</td>
<td>Thrown when an error internal to the service occurs while processing a request. Returns HTTP status code 500.</td>
</tr>
<tr>
<td>InvalidTypeException</td>
<td>Thrown when trying to create or access an Amazon ES domain sub-resource that is either invalid or not supported. Returns HTTP status code 409.</td>
</tr>
</tbody>
</table>
### Exceptions and Descriptions

<table>
<thead>
<tr>
<th>Exception</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LimitExceededException</td>
<td>Thrown when trying to create more than the allowed number and type of Amazon ES domain resources and sub-resources. Returns HTTP status code 409.</td>
</tr>
<tr>
<td>ResourceNotFoundException</td>
<td>Thrown when accessing or deleting a resource that does not exist. Returns HTTP status code 400.</td>
</tr>
<tr>
<td>ResourceAlreadyExistsException</td>
<td>Thrown when a client attempts to create a resource that already exists in an Amazon ES domain. Returns HTTP status code 409.</td>
</tr>
</tbody>
</table>
## Document history for Amazon Elasticsearch Service

This topic describes important changes to Amazon Elasticsearch Service.

**Relevant Dates to this History:**

- **Current product version**—2015-01-01
- **Latest product release**—May 13, 2021
- **Latest documentation update**—May 20, 2021

## Release notes

The following table describes important changes to Amazon ES. For notifications about updates, you can subscribe to the RSS feed.

**Important**  
Service software updates add support for new features, security patches, bug fixes, and other improvements. To use new features, you might need to update the service software on your domain. For more information, see the section called “Service software updates” (p. 16).

<table>
<thead>
<tr>
<th>update-history-change</th>
<th>update-history-description</th>
<th>update-history-date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cold storage (p. 395)</td>
<td>Amazon Elasticsearch Service adds cold storage, a new storage tier for infrequently accessed or historical data. Cold indices only occupy S3 storage and have no compute attached to them. Cold storage requires a domain running Elasticsearch 7.9 or later and service software R20210426 or later. For more information, see Cold storage for Amazon Elasticsearch Service.</td>
<td>May 13, 2021</td>
</tr>
<tr>
<td>ARM-based Graviton instances (p. 395)</td>
<td>Amazon Elasticsearch Service now supports ARM-based Graviton instance types (M6G, C6G, R6G, and R6GD). Graviton instance types are available on new and existing domains running Elasticsearch 7.9 or later and service software R20210331 or later. For details, see Supported instance types in Amazon Elasticsearch Service.</td>
<td>May 4, 2021</td>
</tr>
<tr>
<td>ISM templates (p. 395)</td>
<td>Amazon Elasticsearch Service adds support for ISM templates, which let you automatically</td>
<td>April 27, 2021</td>
</tr>
</tbody>
</table>
attach an ISM policy to an index if the index matches a pattern defined in the policy. ISM templates require service software R20210426 or later. This update also deprecates the `policy_id` setting, meaning you can no longer use index templates to apply ISM policies to newly created indices. The update introduces a breaking change for existing CloudFormation templates using this setting. To learn more, see [ISM templates](#).

<table>
<thead>
<tr>
<th>Elasticsearch 7.10 support (p. 395)</th>
<th>Amazon Elasticsearch Service now supports Elasticsearch version 7.10. To learn more, see <a href="#">Supported Elasticsearch versions</a> and <a href="#">Upgrading Elasticsearch</a>.</th>
<th>April 21, 2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asynchronous search (p. 395)</td>
<td>Amazon Elasticsearch Service now supports asynchronous search, which lets you run search requests in the background. Asynchronous search requires a domain running Elasticsearch 7.9 or later and service software R20210331 or later. To learn more, see <a href="#">Asynchronous search for Amazon Elasticsearch Service</a>.</td>
<td>April 21, 2021</td>
</tr>
<tr>
<td>Tag-based access control (p. 395)</td>
<td>You can now use AWS tags to control access to the Amazon ES configuration API. For more information, see <a href="#">Identity and Access Management in Amazon Elasticsearch Service</a>.</td>
<td>March 2, 2021</td>
</tr>
<tr>
<td>Auto-Tune (p. 395)</td>
<td>Amazon Elasticsearch Service adds Auto-Tune, which uses performance and usage metrics from your cluster to suggest changes to the JVM settings on your nodes. Auto-Tune requires a domain running Elasticsearch 6.7 or later and service software R20201117 or later. For more information, see <a href="#">Auto-Tune for Amazon Elasticsearch Service</a>.</td>
<td>February 24, 2021</td>
</tr>
<tr>
<td>Release note</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>Trace Analytics (p. 395)</td>
<td>The default installation of Kibana for Amazon Elasticsearch Service now includes the Trace Analytics plugin, which lets you monitor trace data from your distributed applications. The plugin requires a domain running Elasticsearch 7.9 or later and service software R20210201 or later. To learn more, see <a href="#">Trace Analytics for Amazon Elasticsearch Service</a>.</td>
<td>February 17, 2021</td>
</tr>
<tr>
<td>Kibana reports (p. 395)</td>
<td>The default installation of Kibana for Amazon Elasticsearch Service now supports on-demand reports for the Discover, Visualize, and Dashboard pages. This feature requires Elasticsearch 7.9 or later and service software R20210201 or later.</td>
<td>February 17, 2021</td>
</tr>
<tr>
<td>Kibana 5.6.16 support (p. 395)</td>
<td>Amazon Elasticsearch Service domains running Elasticsearch 5.6 now support the latest patch release for Kibana 5.6, which adds bug fixes and improves security. Amazon ES will automatically upgrade domains to this patch release.</td>
<td>February 17, 2021</td>
</tr>
<tr>
<td>Encryption for existing domains (p. 395)</td>
<td>Amazon Elasticsearch Service now supports enabling encryption of data at rest and node-to-node encryption on existing domains running Elasticsearch 6.7 or later. After you enable these settings, you can't disable them.</td>
<td>January 27, 2021</td>
</tr>
<tr>
<td>Remote reindex (p. 395)</td>
<td>Amazon Elasticsearch Service now supports remote reindex, which lets you migrate indices from remote domains. This feature requires service software R20201117 or later. To learn more, see <a href="#">Migrating Amazon Elasticsearch Service indices using remote reindex</a>.</td>
<td>November 24, 2020</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Release Date</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Piped Processing Language (p. 395)</td>
<td>Amazon Elasticsearch Service now supports Piped Processing Language (PPL), a query language that lets you use pipe (</td>
<td>) syntax to query data stored in Elasticsearch. This feature requires service software R20201117 or later. To learn more, see Querying Amazon Elasticsearch Service data using Piped Processing Language.</td>
</tr>
<tr>
<td>Kibana notebooks (p. 395)</td>
<td>Amazon Elasticsearch Service adds support for Kibana notebooks, which lets you combine live visualizations and narrative text in a single interface. This feature requires service software R20201117 or later. To learn more, see Kibana notebooks (experimental).</td>
<td>November 24, 2020</td>
</tr>
<tr>
<td>Gantt charts (p. 395)</td>
<td>The default installation of Kibana for Amazon Elasticsearch Service now supports a new visualization type, Gantt charts. This feature requires service software R20201117 or later.</td>
<td>November 24, 2020</td>
</tr>
<tr>
<td>Elasticsearch 7.9 support (p. 395)</td>
<td>Amazon Elasticsearch Service now supports Elasticsearch version 7.9. To learn more, see Supported Elasticsearch versions and Upgrading Elasticsearch. This release also includes an all-new Kibana user interface for fine-grained access control.</td>
<td>November 24, 2020</td>
</tr>
<tr>
<td>Anomaly detection updates (p. 395)</td>
<td>Anomaly detection for Amazon Elasticsearch Service adds support for high cardinality, which lets you categorize anomalies with a dimension like IP address, product ID, country code, and so on. This feature requires service software R20201117 or later. To learn more, see Anomaly detection for Amazon Elasticsearch Service.</td>
<td>November 24, 2020</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Dynamic dictionary updates</td>
<td>Amazon Elasticsearch Service now lets you update your search analyzers without reindexing. You can update the dictionary files on some or all of your domains, and Amazon ES tracks package versions over time so that you have a history of what changed and when. This feature requires service software R20201019 or later. To learn more, see Custom packages for Amazon Elasticsearch Service.</td>
<td>November 17, 2020</td>
</tr>
<tr>
<td>Custom endpoints</td>
<td>Amazon Elasticsearch Service now supports custom endpoints, which let you give your Amazon ES domain a new URL. If you ever swap domains, you can maintain the same URL. This feature requires service software R20201019 or later. To learn more, see Creating a custom endpoint for Amazon Elasticsearch Service.</td>
<td>November 5, 2020</td>
</tr>
<tr>
<td>New language plugins</td>
<td>Amazon Elasticsearch Service now supports IK (Chinese) Analysis, Vietnamese Analysis, and Thai Analysis plugins on domains running Elasticsearch 7.7 or later with service software R20201019 or later.</td>
<td>October 28, 2020</td>
</tr>
<tr>
<td>Elasticsearch 7.8 support</td>
<td>Amazon Elasticsearch Service now supports Elasticsearch version 7.8. To learn more, see Supported Elasticsearch versions and Upgrading Elasticsearch.</td>
<td>October 28, 2020</td>
</tr>
<tr>
<td>SAML authentication for Kibana</td>
<td>Amazon Elasticsearch Service now supports SAML authentication for Kibana, which lets you use third-party identity providers to log in to Kibana, manage fine-grained access control, search your data, and build visualizations. This feature requires service software R20201019 or later. For more information, see SAML authentication for Kibana.</td>
<td>October 27, 2020</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td><strong>T3 instances (p. 395)</strong></td>
<td>Amazon Elasticsearch Service now supports the <code>t3.small</code> and <code>t3.medium</code> instance types. For best practices around using these instance types, see <a href="#">Best practices for Amazon Elasticsearch Service</a>.</td>
<td>September 23, 2020</td>
</tr>
<tr>
<td><strong>Audit logs (p. 395)</strong></td>
<td>Amazon Elasticsearch Service now supports audit logs for your data, which lets you track failed login attempts, user access to indices, documents, and fields, and much more. This feature requires service software R20200910 or later. For more information, see <a href="#">Managing audit logs in Amazon Elasticsearch Service</a>.</td>
<td>September 16, 2020</td>
</tr>
<tr>
<td><strong>UltraWarm updates (p. 395)</strong></td>
<td>UltraWarm for Amazon Elasticsearch Service adds new metrics, new settings, a larger migration queue, and a cancellation API. These updates require service software R20200910 or later. For more information, see <a href="#">UltraWarm for Amazon Elasticsearch Service</a>.</td>
<td>September 14, 2020</td>
</tr>
<tr>
<td><strong>Learning to Rank (p. 395)</strong></td>
<td>Amazon Elasticsearch Service now supports the open source Learning to Rank plugin, which lets you use machine learning technologies to improve search relevance. This feature requires service software R20200721 or later. For more information, see <a href="#">Learning to Rank for Amazon Elasticsearch Service</a>.</td>
<td>July 27, 2020</td>
</tr>
<tr>
<td><strong>k-NN cosine similarity (p. 395)</strong></td>
<td>k-NN now lets you search for &quot;nearest neighbors&quot; by cosine similarity in addition to Euclidean distance. This feature requires service software R20200721 or later. For more information, see <a href="#">k-Nearest Neighbor (k-NN) search in Amazon Elasticsearch Service</a>.</td>
<td>July 23, 2020</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>gzip compression (p. 395)</td>
<td>Amazon Elasticsearch Service now supports gzip compression for most HTTP requests and responses, which can reduce latency and conserve bandwidth. This feature requires service software R20200721 or later. For more information, see Compressing HTTP requests in Amazon Elasticsearch Service.</td>
<td>July 23, 2020</td>
</tr>
<tr>
<td>Elasticsearch 7.7 support (p. 395)</td>
<td>Amazon Elasticsearch Service now supports Elasticsearch version 7.7. To learn more, see Supported Elasticsearch Versions and Upgrading Elasticsearch.</td>
<td>July 23, 2020</td>
</tr>
<tr>
<td>Kibana map service (p. 395)</td>
<td>The default installation of Kibana for Amazon Elasticsearch Service now includes a map service, except for domains in the India and China regions. For more information, see Configuring Kibana to use a WMS map server.</td>
<td>June 18, 2020</td>
</tr>
<tr>
<td>SQL improvements (p. 395)</td>
<td>SQL support for Amazon Elasticsearch Service now supports many new operations, a dedicated Kibana user interface for data exploration, and an interactive CLI. For more information, see Querying your Amazon Elasticsearch Service data with SQL.</td>
<td>June 3, 2020</td>
</tr>
<tr>
<td>Cross-cluster search (p. 395)</td>
<td>Amazon Elasticsearch Service lets you perform queries and aggregations across multiple connected domains. For more information, see Cross-cluster search for Amazon Elasticsearch Service.</td>
<td>June 3, 2020</td>
</tr>
<tr>
<td>Anomaly detection (p. 395)</td>
<td>Amazon Elasticsearch Service lets you automatically detect anomalies in near-real time. For more information, see Anomaly detection in Amazon Elasticsearch Service.</td>
<td>June 3, 2020</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>UltraWarm</strong> (p. 395)</td>
<td>UltraWarm storage for Amazon Elasticsearch Service has left public preview and is now generally available. The feature now supports a wider range of Elasticsearch versions and AWS Regions. For more information, see <a href="https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/ulawarm.html">UltraWarm for Amazon Elasticsearch Service</a>.</td>
<td>May 5, 2020</td>
</tr>
<tr>
<td><strong>Custom dictionaries</strong> (p. 395)</td>
<td>Amazon Elasticsearch Service lets you upload custom dictionary files for use with your cluster. These files improve your search results by telling Elasticsearch to ignore certain high-frequency words or to treat terms as equivalent. For more information, see <a href="https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/custom-dictionaries.html">Custom packages for Amazon Elasticsearch Service</a>.</td>
<td>April 21, 2020</td>
</tr>
<tr>
<td><strong>Elasticsearch 7.4 Support</strong> (p. 395)</td>
<td>Amazon Elasticsearch Service now supports Elasticsearch version 7.4. To learn more, see <a href="https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/supported-versions.html">Supported Elasticsearch versions</a> and <a href="https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/upgrade-cluster.html">Upgrading Elasticsearch</a>.</td>
<td>March 12, 2020</td>
</tr>
<tr>
<td><strong>k-NN</strong> (p. 395)</td>
<td>Amazon Elasticsearch Service adds support for k-nearest neighbor (KNN) search. This feature requires service software R20200302 or later. For more information, see <a href="https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/knn-search.html">k-Nearest Neighbor (k-NN) search in Amazon Elasticsearch Service</a>.</td>
<td>March 3, 2020</td>
</tr>
<tr>
<td><strong>Index State Management</strong> (p. 395)</td>
<td>Amazon Elasticsearch Service adds Index State Management (ISM), which lets you automate routine tasks, such as deleting indices when they reach a certain age. This feature requires service software R20200302 or later. For more information, see <a href="https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/ism.html">Index State Management in Amazon Elasticsearch Service</a>.</td>
<td>March 3, 2020</td>
</tr>
<tr>
<td><strong>Elasticsearch 5.6.16 support</strong> (p. 395)</td>
<td>Amazon Elasticsearch Service now supports the latest patch release for version 5.6, which adds bug fixes and improves security. Amazon ES will automatically upgrade existing 5.6 domains to this release. Note that this Elasticsearch release incorrectly reports its version as 5.6.17.</td>
<td>March 2, 2020</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Fine-grained access control (p. 395)</td>
<td>Amazon Elasticsearch Service now supports <strong>fine-grained access control</strong>, which offers security at the index, document, and field level, Kibana multi-tenancy, and optional HTTP basic authentication for your cluster.</td>
<td>February 11, 2020</td>
</tr>
<tr>
<td>UltraWarm storage (preview) (p. 395)</td>
<td>Amazon Elasticsearch Service adds UltraWarm, a new warm storage tier that uses Amazon S3 and a sophisticated caching solution to improve performance. For indices that you are not actively writing to and query less frequently, UltraWarm storage offers significantly lower costs per GiB. For more information, see <a href="https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/ulawarm.html">UltraWarm for Amazon Elasticsearch Service</a>.</td>
<td>December 3, 2019</td>
</tr>
<tr>
<td>Encryption features for China Regions (p. 395)</td>
<td>Encryption of data at rest and node-to-node encryption are now available in the <code>cn-north-1</code> (Beijing) and <code>cn-northwest-1</code> (Ningxia) Regions.</td>
<td>November 20, 2019</td>
</tr>
<tr>
<td>Require HTTPS (p. 395)</td>
<td>You can now require that all traffic to your Amazon ES domains arrive over HTTPS. When configuring your domain, check the <strong>Require HTTPS</strong> box. This feature requires service software R20190808 or later.</td>
<td>October 3, 2019</td>
</tr>
<tr>
<td>Elasticsearch 7.1 and 6.8 support (p. 395)</td>
<td>Amazon Elasticsearch Service now supports Elasticsearch version 7.1 and 6.8. To learn more, see <a href="https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/supported-versions.html">Supported Elasticsearch versions and Upgrading Elasticsearch</a>.</td>
<td>August 13, 2019</td>
</tr>
<tr>
<td>Hourly snapshots (p. 395)</td>
<td>Rather than daily snapshots, Amazon Elasticsearch Service now takes hourly snapshots of domains running Elasticsearch 5.3 and later so that you have more frequent backups from which to restore your data. To learn more, see <a href="https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/index-snapshots.html">Creating index snapshots in Amazon Elasticsearch Service</a>.</td>
<td>July 8, 2019</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Elasticsearch 6.7 support (p. 395)</td>
<td>Amazon Elasticsearch Service now supports Elasticsearch version 6.7. To learn more, see Supported Elasticsearch versions.</td>
<td>May 29, 2019</td>
</tr>
<tr>
<td>SQL support (p. 395)</td>
<td>Amazon Elasticsearch Service now lets you query your data using SQL. For more information, see Querying your Amazon Elasticsearch Service data with SQL. This feature requires service software R20190418 or later.</td>
<td>May 15, 2019</td>
</tr>
<tr>
<td>5-series instance types (p. 395)</td>
<td>Amazon Elasticsearch Service now supports MS, CS, and RS instance types. Compared to previous-generation instance types, these new types offer better performance at lower prices. For more information, see Supported Instance Types and Limits.</td>
<td>April 24, 2019</td>
</tr>
<tr>
<td>Elasticsearch 6.5 support (p. 395)</td>
<td>Amazon Elasticsearch Service now supports Elasticsearch version 6.5. To learn more, see Supported Elasticsearch versions.</td>
<td>April 8, 2019</td>
</tr>
<tr>
<td>Alerting (p. 395)</td>
<td>The alerting feature notifies you when data from one or more Elasticsearch indices meets certain conditions. To learn more, see Configuring alerts in Amazon Elasticsearch Service. This feature requires service software R20190221 or later.</td>
<td>March 25, 2019</td>
</tr>
<tr>
<td>Three Availability Zone support (p. 395)</td>
<td>Amazon Elasticsearch Service now supports three Availability Zones in many regions. This release also includes a streamlined console experience. To learn more, see Configuring a multi-AZ domain in Amazon Elasticsearch Service. This feature requires service software R20181023 or later.</td>
<td>February 7, 2019</td>
</tr>
<tr>
<td>Elasticsearch 6.4 support (p. 395)</td>
<td>Amazon Elasticsearch Service now supports Elasticsearch version 6.4. To learn more, see Supported Elasticsearch versions.</td>
<td>January 23, 2019</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>200-node clusters</td>
<td>Amazon ES now lets you create clusters with up to 200 data nodes for a total of 3 PB of storage. To learn more, see <a href="https://aws.amazon.com/es/about-es/petabyte-scale/">Petabyte scale for Amazon Elasticsearch Service</a>.</td>
<td>January 22, 2019</td>
</tr>
<tr>
<td>Service software updates</td>
<td>Amazon ES now lets you manually update the service software for your domain in order to benefit from new features more quickly or update at a low traffic time. To learn more, see <a href="https://aws.amazon.com/es/about-es/service-updates/">Service software updates in Amazon Elasticsearch Service</a>.</td>
<td>November 20, 2018</td>
</tr>
<tr>
<td>New CloudWatch metrics</td>
<td>Amazon ES now offers node-level metrics and new <code>Cluster health</code> and <code>Instance health</code> tabs in the Amazon ES console. To learn more, see <a href="https://aws.amazon.com/es/about-es/cloudwatch-metrics/">Monitoring Amazon Elasticsearch Service cluster metrics with Amazon CloudWatch</a>.</td>
<td>November 20, 2018</td>
</tr>
<tr>
<td>China (Beijing) support</td>
<td>Amazon Elasticsearch Service is now available in the cn-north-1 region, where it supports the M4, C4, and R4 instance types.</td>
<td>October 17, 2018</td>
</tr>
<tr>
<td>Node-to-node encryption</td>
<td>Amazon Elasticsearch Service now supports node-to-node encryption, which keeps your data encrypted as Elasticsearch distributes it throughout your cluster. To learn more, see <a href="https://aws.amazon.com/es/about-es/node-to-node-encryption/">Node-to-node encryption for Amazon Elasticsearch Service</a>.</td>
<td>September 18, 2018</td>
</tr>
<tr>
<td>In-place version upgrades</td>
<td>Amazon Elasticsearch Service now supports in-place version upgrades for Elasticsearch. To learn more, see <a href="https://aws.amazon.com/es/about-es/upgrading-es/">Upgrading Elasticsearch</a>.</td>
<td>August 14, 2018</td>
</tr>
<tr>
<td>Elasticsearch 6.3 and 5.6 support</td>
<td>Amazon Elasticsearch Service now supports Elasticsearch version 6.3 and 5.6. To learn more, see <a href="https://aws.amazon.com/es/about-es/supported-versions/">Supported Elasticsearch versions</a>.</td>
<td>August 14, 2018</td>
</tr>
<tr>
<td>Error logs</td>
<td>Amazon ES now lets you publish Elasticsearch error logs to Amazon CloudWatch. To learn more, see <a href="https://aws.amazon.com/es/about-es/configuring-logs/">Configuring logs in Amazon Elasticsearch Service</a>.</td>
<td>July 31, 2018</td>
</tr>
</tbody>
</table>
## Earlier updates

The following table describes important changes Amazon ES before May 2018.

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Cognito Authentication for Kibana</td>
<td>Amazon ES now offers login page protection for Kibana. To learn more, see the section called “Amazon Cognito authentication for Kibana” (p. 128).</td>
<td>April 2, 2018</td>
</tr>
<tr>
<td>Elasticsearch 6.2 Support</td>
<td>Amazon Elasticsearch Service now supports Elasticsearch version 6.2.</td>
<td>March 14, 2018</td>
</tr>
<tr>
<td>Korean Analysis Plugin</td>
<td>Amazon ES now supports a memory-optimized version of the Seunjeon Korean analysis plugin.</td>
<td>March 13, 2018</td>
</tr>
<tr>
<td>Instant Access Control Updates</td>
<td>Changes to the access control policies on Amazon ES domains now take effect instantly.</td>
<td>March 7, 2018</td>
</tr>
<tr>
<td>Petabyte Scale</td>
<td>Amazon ES now supports i3 instance types and total domain storage of up to 1.5 PB. To learn more, see the section called “Petabyte scale” (p. 267).</td>
<td>19 December 2017</td>
</tr>
<tr>
<td>Encryption of Data at Rest</td>
<td>Amazon ES now supports encryption of data at rest. To learn more, see the section called “Encryption at rest” (p. 74).</td>
<td>December 7, 2017</td>
</tr>
<tr>
<td>Elasticsearch 6.0 Support</td>
<td>Amazon ES now supports Elasticsearch version 6.0. For migration considerations and instructions, see the section called “Upgrading Elasticsearch” (p. 61).</td>
<td>December 6, 2017</td>
</tr>
<tr>
<td>VPC Support</td>
<td>Amazon ES now lets you launch domains within an Amazon Virtual Private Cloud. VPC support provides an additional layer of security and simplifies communications between Amazon ES and other services within a VPC. To learn more, see the section called “VPC support” (p. 22).</td>
<td>October 17, 2017</td>
</tr>
<tr>
<td>Slow Logs Publishing</td>
<td>Amazon ES now supports the publishing of slow logs to CloudWatch Logs. To learn more, see the section called “Logs” (p. 47).</td>
<td>October 16, 2017</td>
</tr>
<tr>
<td>Elasticsearch 5.5 Support</td>
<td>Amazon ES now supports Elasticsearch version 5.5. For new feature summaries, see the Amazon announcement of availability.</td>
<td>September 7, 2017</td>
</tr>
</tbody>
</table>

You can now restore automated snapshots without contacting AWS Support and store scripts using the Elasticsearch _scripts API.
<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elasticsearch 5.3 Support</td>
<td>Amazon ES added support for Elasticsearch version 5.3.</td>
<td>June 1, 2017</td>
</tr>
<tr>
<td>More Instances and EBS Capacity per Cluster</td>
<td>Amazon ES now supports up to 100 nodes and 150 TB EBS capacity per cluster.</td>
<td>April 5, 2017</td>
</tr>
<tr>
<td>Canada (Central) and EU (London) Support</td>
<td>Amazon ES added support for the following regions: Canada (Central), ca-central-1, and EU (London), eu-west-2.</td>
<td>March 20, 2017</td>
</tr>
<tr>
<td>More Instances and Larger EBS Volumes</td>
<td>Amazon ES added support for more instances and larger EBS volumes.</td>
<td>February 21, 2017</td>
</tr>
<tr>
<td>Elasticsearch 5.1 Support</td>
<td>Amazon ES added support for Elasticsearch version 5.1.</td>
<td>January 30, 2017</td>
</tr>
<tr>
<td>Support for the Phonetic Analysis Plugin</td>
<td>Amazon ES now provides built-in integration with the Phonetic Analysis plugin, which allows you to run &quot;sounds-like&quot; queries on your data.</td>
<td>December 22, 2016</td>
</tr>
<tr>
<td>US East (Ohio) Support</td>
<td>Amazon ES added support for the following region: US East (Ohio), us-east-2.</td>
<td>October 17, 2016</td>
</tr>
<tr>
<td>Elasticsearch 2.3 Support</td>
<td>Amazon ES added support for Elasticsearch version 2.3.</td>
<td>July 27, 2016</td>
</tr>
<tr>
<td>Asia Pacific (Mumbai) Support</td>
<td>Amazon ES added support for the following region: Asia Pacific (Mumbai), ap-south-1.</td>
<td>June 27, 2016</td>
</tr>
<tr>
<td>More Instances per Cluster</td>
<td>Amazon ES increased the maximum number of instances (instance count) per cluster from 10 to 20.</td>
<td>May 18, 2016</td>
</tr>
<tr>
<td>Asia Pacific (Seoul) Support</td>
<td>Amazon ES added support for the following region: Asia Pacific (Seoul), ap-northeast-2.</td>
<td>January 28, 2016</td>
</tr>
<tr>
<td>Amazon ES</td>
<td>Initial release.</td>
<td>October 1, 2015</td>
</tr>
</tbody>
</table>
AWS glossary

For the latest AWS terminology, see the AWS glossary in the AWS General Reference.