Amazon Elasticsearch Service FAQs

### **General**

Q: What is Amazon Elasticsearch Service?

Amazon Elasticsearch Service is a managed service that makes it easy to deploy, operate, and scale Elasticsearch clusters in the AWS Cloud.

Q: Which Elasticsearch version does Amazon Elasticsearch Service support?

Amazon Elasticsearch Service currently supports Elasticsearch versions 6.2, 6.0, 5.5, 5.3, 5.1, 2.3, and 1.5.

#### **Get Started with AWS for Free**

[Create a Free Account](https://portal.aws.amazon.com/gp/aws/developer/registration/index.html)  
[Or Sign In to the Console](https://console.aws.amazon.com/es/home)

AWS Free Tier includes 750 hrs per month of a t2.micro.elasticsearch or t2.small.elasticsearch instance and 10GB per month of optional Amazon EBS storage (Magnetic or General Purpose)

[View AWS Free Tier Details »](https://aws.amazon.com/free/)

Q: What is an Amazon Elasticsearch domain?

Amazon Elasticsearch domains are Elasticsearch clusters created using the Amazon Elasticsearch Service console, CLI, or API. Each domain is an Elasticsearch cluster in the cloud with the compute and storage resources you specify. You can create and delete domains, define infrastructure attributes, and control access and security. You can run one or more Amazon Elasticsearch domains.

Q: What does Amazon Elasticsearch Service manage on my behalf?

Amazon Elasticsearch Service manages the work involved in setting up a domain, from provisioning infrastructure capacity in the network environment you request to installing the Elasticsearch software. Once your domain is running, Amazon Elasticsearch Service automates common administrative tasks, such as performing backups, monitoring instances and patching software. Amazon Elasticsearch Service integrates with Amazon CloudWatch to produce metrics that provide information about the state of the domains. Amazon Elasticsearch Service also offers options to modify your domain instance and storage settings to simplify the task of tailoring your domain based to your application needs.

Q: Does Amazon Elasticsearch Service support the open source Elasticsearch APIs?

Amazon Elasticsearch Service supports most of the commonly used Elasticsearch APIs, so the code, applications, and popular tools that you're already using with your current Elasticsearch environments work seamlessly. For a full list of supported Elasticsearch operations, see our [documentation](https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-gsg-supported-operations.html).

[Return to Top >>](https://aws.amazon.com/elasticsearch-service/faqs/#faqs)

### **Setup and Configuration**

Q: Can I create and modify my Amazon Elasticsearch domain through the Amazon Elasticsearch Service console?

Yes. You can create a new Amazon Elasticsearch domain with the Domain Creation Wizard in the console with just a few clicks. While creating a new domain you can specify the number of instances, instance types, and EBS volumes you want allocated to your domain. You can also modify or delete existing Amazon Elasticsearch domains using the console.

Q: Does Amazon Elasticsearch Service support Amazon VPC?

Yes, Amazon Elasticsearch Service is integrated with Amazon VPC. When choosing VPC access, IP addresses from your VPC are attached to your Amazon Elasticsearch Service domain and all network traffic stays within the AWS network and is not accessible to the Internet. Moreover, you can use security groups and IAM policies to restrict access to your Amazon Elasticsearch Service domains.

Q: Can I use CloudFormation Templates to provision Amazon ES domains?

Yes. [AWS CloudFormation](https://aws.amazon.com/cloudformation/) supports Amazon ES. For more information, see the [CloudFormation Template Reference](http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-elasticsearch-domain.html) documentation.

Q: Does Amazon Elasticsearch Service support configuring dedicated master nodes?

Yes. You can configure dedicated master nodes for your domains. When choosing a dedicated master configuration, you can specify the instance type and instance count.

Q: Can I create multiple Elasticsearch indices within a single Amazon Elasticsearch domain?

Yes. You can create multiple Elasticsearch indices within the same Amazon Elasticsearch domain. Elasticsearch automatically distributes the indices and any associated replicas between the instances allocated to the domain.

Q: How do I ingest data into my Amazon Elasticsearch Service domain?

Amazon Elasticsearch Service supports three options for data ingestion:

* For large data volumes, we recommend Amazon Kinesis Firehose, a fully managed service that automatically scales to match the throughput of your data and requires no ongoing administration. It can also transform, batch and compress the data before loading it.
* Amazon Elasticsearch Service supports integration with Logstash. You can configure your Amazon Elasticsearch Service domain as the data store for all logs arriving from your Logstash implementation.
* You can use native Elasticsearch APIs, such as the index and bulk APIs, to load data into your domain.

Q: Does Amazon Elasticsearch Service support integration with Logstash?

Yes. Amazon Elasticsearch Service supports integration with Logstash. You can set up your Amazon Elasticsearch domain as the backend store for all logs coming through your Logstash implementation. You can set up access control on your Amazon Elasticsearch domain to either use request signing to authenticate calls from your Logstash implementation, or use resource based IAM policies to include IP addresses of instances running your Logstash implementation.

Q: Does Amazon Elasticsearch Service support integration with Kibana?

Yes. Amazon Elasticsearch Service includes a built-in Kibana install that is deployed with your Amazon Elasticsearch Service domain.

Q: Can I create custom reports with the Kibana installation included with Amazon Elasticsearch Service?

Yes. Kibana supports creating and saving custom reports through the user interface. For more information on using Kibana, refer to [Kibana documentation](https://www.elastic.co/guide/en/kibana/4.0/index.html).

Q: What storage options are available with Amazon Elasticsearch Service?

You can choose between local on-instance storage or EBS volumes. During domain creation, if you select EBS storage, you can increase and decrease the size of the storage volume as necessary.

Q: What types of EBS volumes does Amazon Elasticsearch Service support?

You can choose between Magnetic, General Purpose, and Provisioned IOPS EBS volumes.

Q: Is there a limit on the amount of EBS storage that can be allocated to an Amazon Elasticsearch domain?

Yes. Amazon Elasticsearch Service supports one EBS volume (max size of 1.5 TB) per instance associated with a domain. With the default maximum of 20 data nodes allowed per Amazon Elasticsearch Service domain, you can allocate about 30 TB of EBS storage to a single domain. You can request a service limit increase up to 100 instances per domain by creating a case with the [AWS Support Center](https://console.aws.amazon.com/support/home#/). With 100 instances, you can allocate about 150 TB of EBS storage to a single domain.

[Return to Top >>](https://aws.amazon.com/elasticsearch-service/faqs/#faqs)

### **Administration**

Q: Can programs running on servers in my own data center access my Amazon Elasticsearch domains?

Yes. The programs with public Internet access can access Amazon Elasticsearch Service domains through a public endpoint. If your data center is already connected to Amazon VPC through Direct Connect or SSH tunneling, you can also use VPC access. In both cases, you can configure IAM policies and security groups to allow programs running on servers outside of AWS to access your Amazon Elasticsearch domains. [Click here](http://docs.aws.amazon.com/general/latest/gr/signature-version-4.html) for more information about signed requests.

Q: How can I migrate data from my existing Elasticsearch cluster to a new Amazon Elasticsearch domain?

To migrate data from an existing Elasticsearch cluster you should create a snapshot of an existing Elasticsearch cluster, and store the snapshot in your Amazon S3 bucket. Then you can create a new Amazon Elasticsearch domain and load data from the snapshot into the newly created Amazon Elasticsearch domain using the Elasticsearch restore API.

Q: How can I scale an Amazon Elasticsearch domain?

Amazon Elasticsearch Service allows you to control the scaling of your Amazon Elasticsearch domains using the console, API, and CLI. You can scale your Amazon Elasticsearch domain by adding, removing, or modifying instances or storage volumes depending on your application needs. Amazon Elasticsearch Service is integrated with Amazon CloudWatch to provide metrics about the state of your Amazon Elasticsearch domains to enable you to make appropriate scaling decisions for your domains.

Q: Does scaling my Amazon Elasticsearch domain require downtime?

No. Scaling your Amazon Elasticsearch domain by adding or modifying instances, and storage volumes is an online operation that does not require any downtime.

Q: What options does Amazon Elasticsearch Service provide for node failures?

Amazon Elasticsearch Service automatically detects node failures and replaces the node. The service will acquire new instances, and will then redirect Elasticsearch requests and document updates to the new instances. In the event that the node cannot be replaced, customers will be able to use any snapshots they have of their cluster to restart the domain with preloaded data.

Q: Does Amazon Elasticsearch Service support cross-zone replication?

Yes. Customers can enable Zone Awareness for their Amazon Elasticsearch domains either at domain creation time or by modifying a live domain. When Zone Awareness is enabled, Amazon Elasticsearch Service will distribute the instances supporting the domain across two different Availability Zones. Then, if replication is enabled in the Elasticsearch engine, Elasticsearch will allocate replicas of the domain across these different instances enabling cross-zone replication.

Q: Does Amazon Elasticsearch Service expose any performance metrics through Amazon CloudWatch?

Yes. Amazon Elasticsearch Service exposes several performance metrics through Amazon CloudWatch including number of nodes, cluster health, searchable documents, EBS metrics (if applicable), CPU, memory and disk utilization for data and master nodes. Please refer to the service documentation for a full listing of available CloudWatch metrics.

Q: I wish to perform security analysis or operational troubleshooting of my Amazon Elasticsearch Service deployment. Can I get a history of all the Amazon Elasticsearch Service API calls made on my account?

Yes. AWS CloudTrail is a web service that records AWS API calls for your account and delivers log files to you. The AWS API call history produced by AWS CloudTrail enables security analysis, resource change tracking, and compliance auditing. Learn more about AWS CloudTrail at the [AWS CloudTrail detail page](https://aws.amazon.com/cloudtrail/), and turn it on via [CloudTrail's AWS Management Console home page](https://console.aws.amazon.com/cloudtrail/home).

Q: What is a snapshot?

A snapshot is a copy of your Amazon Elasticsearch domain at a moment in time.

Q: Why would I need snapshots?

Creating snapshots can be useful in case of data loss caused by node failure, as well as the unlikely event of a hardware failure. You can use snapshots to recover your Amazon Elasticsearch domain with preloaded data or to create a new Amazon Elasticsearch domain with preloaded data. Another common reason to use backups is for archiving purposes. Snapshots are stored in Amazon S3.

Q: Does Amazon Elasticsearch Service provide automated snapshots?

Yes. By default, Amazon Elasticsearch Service will automatically create daily snapshots of each Amazon Elasticsearch domain. The daily snapshots are setup to occur between midnight and 1AM UTC. Customers will also be able to modify the timing of the automated snapshot to better suit their needs.

Q: Can I change the default settings for the automated daily snapshot provided by Amazon Elasticsearch Service?

Yes. You will be able to change the timing of the automated daily snapshot to suit your application schedule.

Q: How long are the automated daily snapshots stored by Amazon Elasticsearch Service?

Amazon Elasticsearch Service will retain the last 14 days worth of automated daily snapshots.

Q: Is there a charge for the automated daily snapshots?

There is no additional charge for the automated daily snapshots. The snapshots are stored for free in an Amazon Elasticsearch Service S3 bucket and will be made available for node recovery purposes.

Q: Can I create additional snapshots of my Amazon Elasticsearch domains as needed?

Yes. You can use the Elasticsearch snapshot API to create additional manual snapshots in addition to the daily-automated snapshots created by Amazon Elasticsearch Service. The manual snapshots are stored in your S3 bucket and will incur relevant Amazon S3 usage charges.

Q: Can snapshots created by the manual snapshot process be used to recover a domain in the event of a failure?

Yes. Customers can create a new Amazon Elasticsearch domain and load data from the snapshot into the newly created Amazon Elasticsearch domain using the Elasticsearch restore API.

Q: What happens to my snapshots when I delete my Amazon Elasticsearch domain?

The daily snapshots retained by Amazon Elasticsearch Service will be deleted as part of domain deletion. Before deleting a domain, you should consider creating a snapshot of the domain in your own S3 buckets using the manual snapshot process. The snapshots stored in your S3 bucket will not be affected if you delete your Amazon Elasticsearch domain.

Q: What are slow logs?

Slow logs are log files that help track the performance of various stages in an operation. Elasticsearch exposes two kinds of slow logs:

* Index Slow Logs – These logs provide insights into the indexing process and can be used to fine-tune the index setup.
* Search Slow Logs – These logs provide insights into how fast or slow queries and fetches are performing. These logs help fine tune the performance of any kind of search operation on Elasticsearch.

For complete details on Elasticsearch slow logs, please refer to [Elasticsearch documentation](https://www.elastic.co/guide/en/elasticsearch/reference/current/index-modules-slowlog.html).

Q: How can I enable slow logs on Amazon ES?

Slows logs can be enabled via the click of a button from the Console or via our CLI and APIs. For more details please refer to our [documentation](http://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-createupdatedomains.html#es-createdomain-configure-slow-logs).

Q: Can I only enable slow logs for specific indices?

Yes. You can update the settings for a specific index to enable or disable slow logs for it. For more details refer to our [documentation](http://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-createupdatedomains.html#es-createdomain-configure-slow-logs).

Q: Does turning on slow logs in Amazon ES automatically enable logging for all indexes?

No. Turning on slow logs in Amazon ES enables the option to publish the generated logs to Amazon CloudWatch Logs for indices in the given domain. However, in order to generate the logs you have to update the settings for one or more indices to start the logging process. For more details on setting the index configuration for enabling slow logs, please refer to our [documentation](http://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-createupdatedomains.html#es-createdomain-configure-slow-logs).

Q: If I turn off the Slow Logs in Amazon ES, does it mean that log files are no longer being generated?

No. The generation of log files are dependent on the index settings. To turn off generation of the log files you have to update the index configuration. For more details on setting the index configuration for enabling slow logs, see our [documentation](http://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-createupdatedomains.html#es-createdomain-configure-slow-logs).

Q: Can I adjust the granularity of logging?

Yes. Elasticsearch exposes multiple levels of logging. You need to set the appropriate level in the configuration for your index. For more details on setting the index configuration for enabling slow logs, see our [documentation](http://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-createupdatedomains.html#es-createdomain-configure-slow-logs).

Q: Does enabling Slow Logs cost me anything?

When Slow Logs are enabled, Amazon ES starts publishing the generated logs to Amazon CloudWatch Logs. Amazon ES does not charge for enabling slow logs. However, [standard CloudWatch charges](https://aws.amazon.com/cloudwatch/pricing/) apply.

Q: Is there any limit on the size of each log entry?

Yes. Each log entry made into CloudWatch will be limited to 255,000 characters. If your log entry is bigger than that, it will be truncated to 255,000 characters.

Q: What is the recommended best practice for using slow logs?

Slow logs are only needed when you want to troubleshoot your indexes or fine-tune performance. The recommended approach is to only enable logging for those indexes for which you need additional performance insights. Also, once the investigation is done, you should turn off logging so that you don’t incur any additional costs on account of it. For more details, see our [documentation](http://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-createupdatedomains.html#es-createdomain-configure-slow-logs).

Q: How can I consume logs from CloudWatch Logs?  
CloudWatch offers multiple ways to consume logs. You can [view log data](http://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/ViewingLogData.html), [export it to S3](http://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/S3Export.html), or [process it in real time](http://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/Subscriptions.html). To learn more, see the [CloudWatch Logs developer guide](http://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html).

Q: Are slow logs available for all versions of Elasticsearch supported by Amazon ES?

Yes. slow logs can be enabled for all versions of Elasticsearch supported by Amazon ES. However, there are slight differences in the way log settings can be specified for each version of Elasticsearch. Please refer to our [documentation](http://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-createupdatedomains.html#es-createdomain-configure-slow-logs) for more details.

Q: Will the cluster have any down time when logging is turned on or off?

No. There will not be any down-time. Every time the log status is updated, we will deploy a new cluster in the background and replace the existing cluster with the new one. This process will not cause any down time. However, since a new cluster is deployed the update to the log status will not be instantaneous.

[Return to Top >>](https://aws.amazon.com/elasticsearch-service/faqs/#faqs)

### **Security**

Q: How can I secure my Amazon Elasticsearch Service domain?

If you use VPC to secure your applications, data, and network traffic, you can set up VPC access for Amazon Elasticsearch Service, which allows you to control network access using your VPC security groups. You can also use IAM-based policies to provide fine-grained access control to which IAM roles can perform administrative tasks, use the Elasticsearch APIS and have access to the resources in the domain down to the index-level.

If you want to make your Amazon Elasticsearch Service domain accessible from the Internet, you can specify public access. With public access, you can control access to the endpoint by IP address and require authentication using IAM roles. IAM policies can control access to Amazon Elasticsearch domains and sub resources like indices within the domains.

With Amazon Cognito, you can also allow your end-users to log-in to Kibana through enterprise identity providers such as Microsoft Active Directory using SAML 2.0, and through social identity providers such as Google, Facebook, and Amazon.  You can also set up a secure, scalable, and simplified sign-up experience using Amazon Cognito User Pools. Once you sign-in, Amazon Cognito establishes a session using the appropriate AWS Identity and Access Management (IAM) role, which provides access to the Amazon Elasticsearch Service domain.

IAM policies can also be set up to control access to the management API for operations such as creating and scaling clusters and Elasticsearch API for operations like uploading documents and executing Elasticsearch requests.

Q: Can I encrypt my data at rest while using Amazon Elasticsearch Service?

Amazon Elasticsearch Service provides an option that allows you to encrypt your data using keys you manage through [AWS Key Management Service (KMS)](https://aws.amazon.com/kms/). If enabled, all of your data stored at rest in the underlying storage systems are encrypted, including primary and replica indices, log files, memory swap files, and automated S3 snapshots. Amazon Elasticsearch Service handles encryption and decryption seamlessly, so you don’t have to modify your application to access your data. You can choose to enable encryption when you create new domains via the AWS Management Console or API. Amazon Elasticsearch Service can create a KMS master key for you, or you can choose one of your own. Encryption at rest supports both Amazon Elastic Block Store (EBS) and instance storage.

For more information about the use of AWS KMS with Amazon Elasticsearch Service, see the [Amazon Elasticsearch Service Developer Guide](https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/encryption-at-rest.html). To learn more about AWS KMS, visit the [web page](https://aws.amazon.com/kms/).

Q: How can I set up the VPC access for Amazon Elasticsearch Service?

You configure VPC access when creating an Amazon Elasticsearch Service domain. The VPC access can be set up via a few clicks in the console or via our CLI and APIs. For more details, see the [Amazon Elasticsearch Service developer guide](https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-vpc.html).

Q: If I set up VPC access for my Amazon Elasticsearch Service domain, how can I access Kibana?

When VPC access is enabled, the endpoint for Amazon Elasticsearch Service is only accessible within the customer VPC. To use your laptop to access Kibana from outside the VPC, you need to connect the laptop to the VPC using VPN or VPC Direct Connect.

[Return to Top >>](https://aws.amazon.com/elasticsearch-service/faqs/#faqs)

### **Pricing**

Q: How will I be charged and billed for my use of Amazon Elasticsearch Service?

You pay only for what you use, and there are no minimum or setup fees. You are billed based on:

* Amazon Elasticsearch instance hours – Based on the class (e.g. Standard Small, Large, Extra Large) of the Amazon Elasticsearch instance consumed. Partial Amazon Elasticsearch instance hours consumed are billed as full hours.
* Storage (per GB per month) – EBS Storage capacity you have provisioned to your Amazon Elasticsearch instance. If you scale your provisioned storage capacity within the month, your bill will be pro-rated.
* Provisioned IOPS per month – EBS Provisioned IOPS rate, regardless of IOPS consumed (for Amazon Elasticsearch Service Provisioned IOPS (SSD) Storage only).
* Data transfer – Regular AWS data transfer charges apply.

Please refer to the Amazon Elasticsearch Service [pricing page](https://aws.amazon.com/elasticsearch-service/pricing/) for detailed pricing information.

Q: When does billing of my Amazon Elasticsearch domain begin and end?

Billing commences for an Amazon Elasticsearch instance as soon as the instance is available. Billing continues until the Amazon Elasticsearch instance terminates, which would occur upon deletion or in the event of instance failure.

Q: What defines billable instance hours for Amazon Elasticsearch Service?

Amazon Elasticsearch instance hours are billed for each hour your instance is running in an available state. If you no longer wish to be charged for your Amazon Elasticsearch instance, you must delete the domain to avoid being billed for additional instance hours. Partial Amazon Elasticsearch instance hours consumed are billed as full hours.