



# AWS OpenSearch Security Best Practices

Status	IN PROGRESS
Owner	@ Quentin Hatcher
Contributors	 Red Cosmos  Bryan Evans
On this page	<ul style="list-style-type: none"><li>• <a href="#">AWS Recommended Security Best Practices</a></li><li>• <a href="#">AWS OpenSearch Architecture Example Diagram</a></li><li>• <a href="#">Source Links</a></li></ul>

## AWS Recommended Security Best Practices

This document contains AWS Config rules based on Amazon OpenSearch Service. Each rule offers compatibility with the majority of AWS Regions and does not require setting of any Parameters.

AWS OpenSearch provides many different configuration options. Our recommendations aim to minimize the complexity of configuring and deploying the cluster while maximizing usability and security.

No.	Security Control	Description
1.	OpenSearch access control enabled	Implemented to mitigate the risk of OpenSearch being accessed without the appropriate authorization or the risk of a data breach.
2.	OpenSearch audit logging enabled	Captured in order to record the occurrence of events, the time at which they occur, the responsible user, and the impacted resource.
3	OpenSearch encrypted at rest	Prevent a threat actor from accessing the unencrypted data by ensuring the data is encrypted when on disk.
4.	OpenSearch https required	HTTPS uses the SSL/TLS protocol to encrypt communications so that threat actors can't intercept data.
5.	OpenSearch in VPC only	VPC access is recommended, because by default it provides secure communication between the domain and other services within the VPC.
6.	OpenSearch logs to CloudWatch	Real time monitoring of the OpenSearch cluster through CloudWatch.
7.	OpenSearch Users have MFA enabled	Provides another form of authentication in addition to, username /password, and VPN

### Enable fine-grained access control

Fine-grained access control lets you control who can access certain data within an OpenSearch Service domain. Compared to generalized access control, fine-grained access control gives each cluster, index, document, and field its own specified policy for access. Access criteria can be based on a number of factors, including the role of the person who is requesting access and the action that they intend to perform on the data. For example, you might give one user access to write to an index, and another user access only to read the data on the index without making any changes.

Fine-grained access control allows data with different access requirements to exist in the same storage space without running into security or compliance issues.

### Deploy domains within a VPC

Placing your OpenSearch Service domain within a virtual private cloud (VPC) helps enable secure communication between OpenSearch Service 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 compared to domains that use public endpoints.

### Apply a restrictive access policy

Even if your domain is deployed within a VPC, it's a best practice to implement security in layers. Make sure to check the configuration of your current access policies.

Apply a restrictive resource-based access policy to your domains and follow the principle of least privilege when granting access to the configuration API and the OpenSearch API operations. As a general rule, avoid using the anonymous user principal "Principal": { "AWS": "\*" } in your access policies.

There are some situations, however, where it's acceptable to use an open access policy, such as when you enable fine-grained access control. An open access policy can enable you to access the domain in cases where request signing is difficult or impossible, such as from certain clients and tools.

### Enable encryption at rest

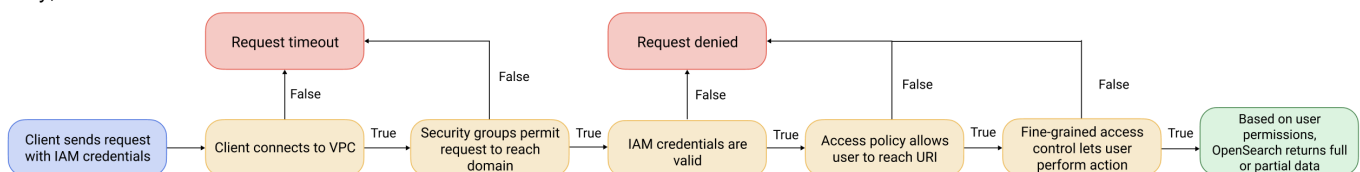
OpenSearch Service domains offer encryption of data at rest to help prevent unauthorized access to your data. Encryption at rest uses AWS Key Management Service (AWS KMS) to store and manage your encryption keys, and the Advanced Encryption Standard algorithm with 256-bit keys (AES-256) to perform the encryption.

### Enable node-to-node encryption

Node-to-node encryption provides an additional layer of security on top of the default security features within OpenSearch Service. It implements Transport Layer Security (TLS) for all communications between the nodes that are provisioned within OpenSearch. Node-to-node encryption, any data sent to your OpenSearch Service domain over HTTPS remains encrypted in transit while it's being distributed and replicated between nodes.

### AWS OpenSearch Architecture Example Diagram

The following 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.



### Source Links

- <https://github.com/awslabs/aws-config-rules/blob/master/aws-config-conformance-packs/Security-Best-Practices-for-Amazon-OpenSearch-Service.yaml>
- <https://docs.aws.amazon.com/opensearch-service/latest/developerguide/data-protection.html>
- <https://scalesec.com/aws-series/security-best-practice-for-amazon-elasticsearch-part-one/>
- <https://docs.aws.amazon.com/opensearch-service/latest/developerguide/bp.html#bp-security>
- <https://docs.aws.amazon.com/opensearch-service/latest/developerguide/fgac.html>