Secure OpenSearch Access with IAM Identity Center (SSO)

A step-by-step overview of integrating Amazon OpenSearch Service with AWS IAM Identity Center using SAML for secure, role-based access control.

The Problem

OpenSearch clusters often rely on shared master credentials, creating security risks and making it difficult to enforce least privilege access.

The Solution

Integrating IAM Identity Center with OpenSearch through SAML enables centralized user management, group-to-role mapping, and fine-grained access control.

Architecture Overview

IAM Identity Center users → Groups → SAML Assertion → OpenSearch Roles (Admin → all_access, Developer → alerting_full_access).

Step 1: Enable SAML in OpenSearch

- Enable Fine-Grained Access Control
- Enable SAML Authentication
- Copy Service Provider Entity ID & IdP-Initiated SSO URL

Step 2: Configure IAM Identity Center

- Create a custom SAML application
- Map attributes: Subject → email, Role → groups
- Create Admin & Developer groups
- Assign users to groups

Step 3: Upload Metadata to OpenSearch

- Import IdP metadata
- Set Admin group ID as SAML master backend role
- Set 'Role' as the assertion key

Step 4: Map Developer Role

- Login as Admin in Dashboards
- Map Developer group ID → alerting_full_access role
- Save backend role mapping

Final Outcome

✓ Secure SSO login into OpenSearch Dashboards

✓ Automatic role mapping via IAM groups

✓ No manual updates when new users join

✓ Cleaner, scalable access management

Conclusion

This integration enhances security and automation by replacing shared credentials with centralized SSO + role-based access control across the AWS environment.