

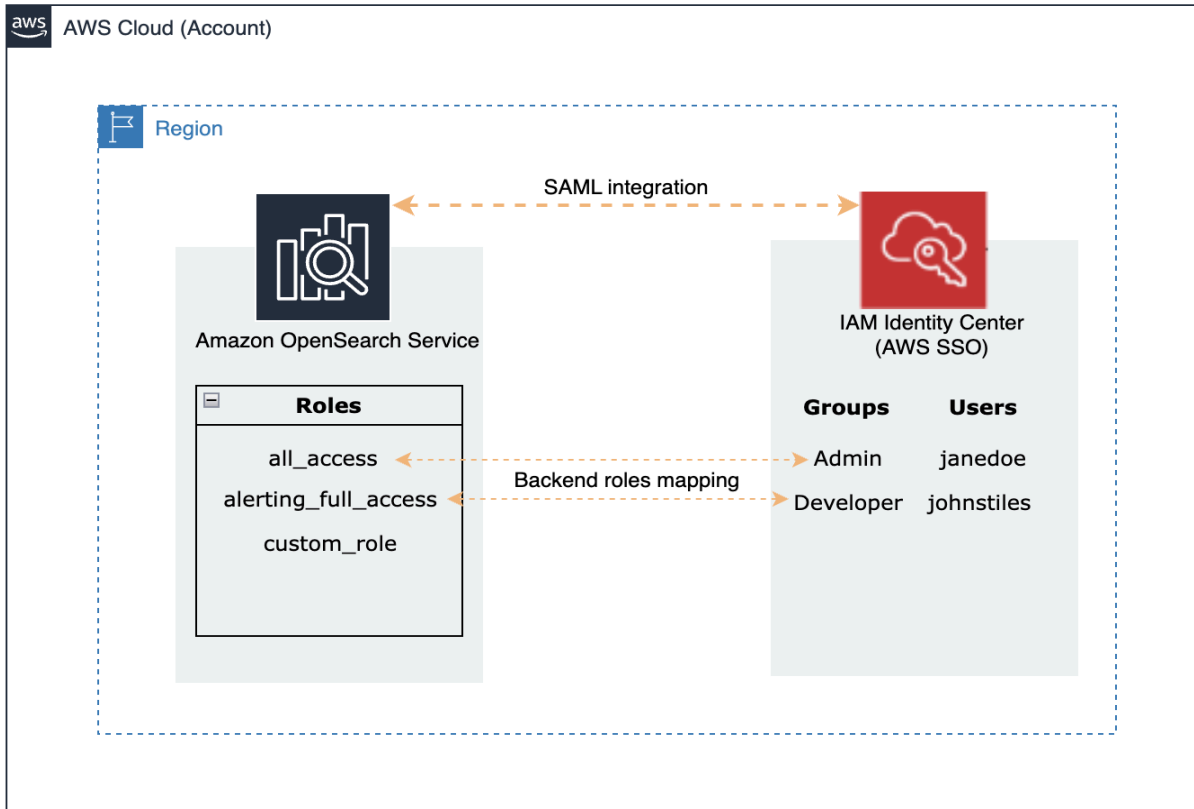
AWS OpenSearch Integration with IAM Identity Center

The Problem: This Document addresses the challenge of managing user access to an OpenSearch cluster where all users have master credentials. This can lead to security vulnerabilities and make it difficult to control who has access to sensitive data.

The Solution: The article proposes using AWS IAM Identity Center (successor to AWS Single Sign-On) to implement Role based control in OSS. IAM Identity Center acts as a central point for managing user identities and assigning roles.

Below, we demonstrate a step-by-step procedure on how we have implemented IAM Identity Center to OpenSearch Service via native SAML integration, and configure role-based access control in OpenSearch Dashboards by using group attributes in IAM Identity Center.

This solution uses IAM Identity Center to manage user access to an OpenSearch Service cluster. It maps users and groups in IAM Identity Center to specific roles in OpenSearch Service. For example, the "Admin" group is mapped to the "all_access" role, while the "Developer" group is mapped to the "alerting_full_access" role. This allows for fine-grained control over user permissions, ensuring that users only have access to the resources they need. The solution is illustrated with a diagram showing the mapping of users, groups, and roles.



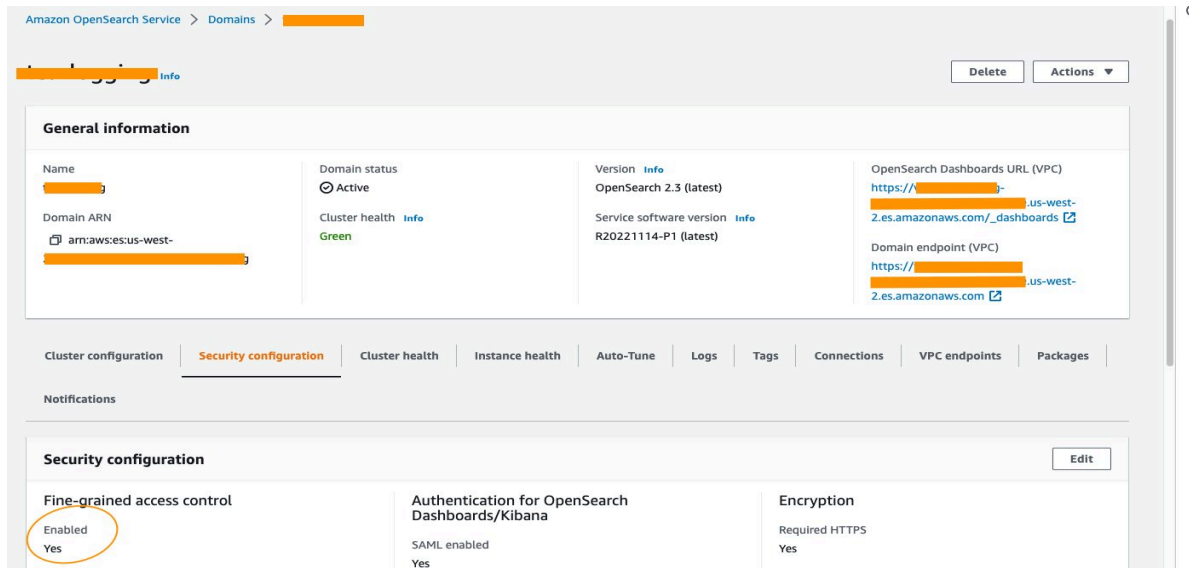
Prerequisites:

1. We have opensearch cluster in Log Archive account
2. We have enabled the [Organization instance](#) for IAM Identity Center in Root Account with the help of which we create SSO users.

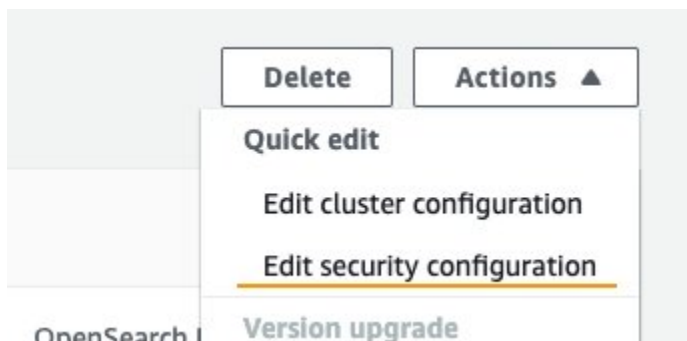
Steps to Configure IAM Identity Center with AWS OSS.

1. Enable SAML in Amazon OpenSearch Service and copy SAML parameters.

- confirm that Fine-grained access control is enabled



- On the Actions menu, choose Edit security configuration.



- Select Enable SAML authentication.
- You can also configure SAML during domain creation if you are creating a new OpenSearch domain. For more information, refer to [SAML authentication for OpenSearch Dashboards](#).
- Copy the values for Service provider entity ID and IdP-Initiated SSO URL.

SAML authentication for OpenSearch Dashboards/Kibana
SAML authentication lets you use your existing identity provider for single sign-on for OpenSearch Dashboards/Kibana. [Learn more](#)

☒ Enable SAML authentication

Enabling or disabling SAML makes OpenSearch Dashboards/Kibana unavailable for up to 30 seconds.

Configure identity provider (IdP)
Use the following information to create a new application with SAML support in your IdP. To configure authentication through your IdP's application directory, use the IdP-initiated SSO URL. To configure authentication through the OpenSearch Dashboards/Kibana URL, use the SP-initiated SSO URL. [Learn more](#)

Service provider entity ID

IdP-initiated SSO URL

SP-initiated SSO URL

Import IdP metadata
After you configure your IdP, provide its metadata file here. [Learn more](#)

2. Create a SAML application in IAM Identity Center



- On the IAM Identity Center console, choose Applications in the navigation pane.
- Choose Add application.
- Select Add customer SAML 2.0 application, then choose Next.
- Enter your application name for Display name.
- Under IAM Identity Center metadata, choose Download to download the SAML metadata file.

Configure application

Display name
Custom SAML 2.0 application

Description
The description you type here does not appear in the AWS access portal. However, it will be visible in the IAM Identity Center console and when using IAM Identity Center APIs.
Custom SAML 2.0 application

IAM Identity Center metadata
Your cloud application may require the following certificate and metadata details to recognize IAM Identity Center as the identity provider.

IAM Identity Center SAML metadata file
 Download
 <https://portal.sso.us-west-2.amazonaws.com/saml/metadata/>

- Under Application metadata, select Manually type your metadata values.
- For Application ACS URL, enter the IdP-initiated URL you copied earlier.
- For Application SAML audience, enter the service provider entity ID you copied earlier.

Application metadata
IAM Identity Center requires specific metadata about your cloud application before it can trust this application. You can type this metadata manually or upload a metadata exchange file.

☒ Manually type your metadata values ☐ Upload application SAML metadata file

Application ACS URL
https://portal.sso.us-west-2.amazonaws.com/_dashboards/_opendistro/_security/saml/acs/ldpinitiated


Application SAML audience
<https://portal.sso.us-west-2.amazonaws.com>

- After Submitting , On the Actions menu, choose Edit attribute mappings.

IAM Identity Center > Applications > Opensearch-tea-logging

Opensearch-tea-logging

Details

	Display name Opensearch-tea-logging	Description Custom SAML 2.0 application	<div> <div>Actions ▴</div> <div> Edit configuration Edit attribute mappings </div> </div>
---	--	--	---

- Create attributes and map the following values:
- Subject map to `${user:email}`, the format is emailAddress.
- Role map to `${user:groups}`, the format is unspecified.

The screenshot shows the 'Attribute mapping' configuration page in the IAM Identity Center console. It features three columns: 'User attribute in the application', 'Maps to this string value or user attribute in IAM Identity Center', and 'Format'. The first row shows 'Subject' mapped to `${user:email}` with the format 'emailAddress'. The second row shows 'Role' mapped to `${user:groups}` with the format 'unspecified'. There is a 'Remove' button next to the second row and an 'Add new attribute mapping' button at the bottom. At the bottom right, there are 'Cancel' and 'Save changes' buttons.

User attribute in the application	Maps to this string value or user attribute in IAM Identity Center	Format
Subject	<code>\${user:email}</code>	emailAddress
Role	<code>\${user:groups}</code>	unspecified

Buttons: Add new attribute mapping, Remove, Cancel, Save changes

- On the IAM Identity Center console, choose Groups in the navigation pane.
- Create two groups: Developer and Admin. And assign the two groups to the SAML application we just created.

The screenshot shows the 'Groups' page in the IAM Identity Center console. The left navigation pane includes 'Dashboard', 'Users', 'Groups' (selected), and 'Settings'. The main content area shows 'Groups (2)' with a search bar and a table of groups. The table has columns for 'Group name', 'Description', and 'Created by'. Two groups are listed: 'Developer' and 'Admin'. There are 'Delete group' and 'Create group' buttons at the top right.

Group name	Description	Created by
Developer	-	Manual
Admin	Administrator	Manual

The screenshot shows the 'Assign users to' page for the 'Opensearch-tea-logging' application. It includes a warning message about multi-account access. Below the warning, there is a search bar and a table of groups. The table has columns for 'Group name' and 'Description'. Two groups are listed: 'Developer' and 'Admin'. There are 'Users (3)' and 'Groups (2)' tabs at the top.

Assign users to

ⓘ Users you assign here must also have equivalent accounts in the Custom SAML 2.0 application before they can have multi-account access to the application from the AWS access portal. You can create these accounts manually or enable just-in-time (JIT) provisioning in the application to create these accounts automatically.

You can search for the users and groups to grant multi-account access. You can select more than one user or group. [Learn more](#)

Group name	Description
Developer	-
Admin	Administrator

- Create two Users and assign it to a group Admin and Developer Permissions.
- Open the Admin group and copy the group ID.

Admin Delete group

General Information Edit description

Group name Admin	Created time December 11, 2022	Last updated December 11, 2022
Group ID [Group ID]	Created by Manual	Updated by Manual
Description Administrator		

3. Finish SAML configuration and map the SAML primary backend role

- On the OpenSearch Service console, choose Domains in the navigation pane.
- Open your domain and choose Edit security configuration.
- Under SAML authentication for OpenSearch Dashboards/Kibana, for Import IdP metadata, choose Import from XML file.
- Upload the IdP metadata downloaded from the IAM Identity Center metadata file.

Configure identity provider (IdP)

Use the following information to create a new application with SAML support in your IdP. To configure authentication through your IdP's application directory, use the IdP-initiated SSO URL. To configure authentication through the OpenSearch Dashboards/Kibana URL, use the SP-initiated SSO URL. [Learn more](#)

Service provider entity ID

[https://\[redacted\]us-west-2.es.amazonaws.com](#)

IdP-initiated SSO URL

[https://\[redacted\]us-west-2.es.amazonaws.com/_dashboards/_opendistro/_security/saml/acs/idpinitiated](#)

SP-initiated SSO URL

[https://\[redacted\]us-west-2.es.amazonaws.com/_dashboards/_opendistro/_security/saml/acs](#)

Import IdP metadata

After you configure your IdP, provide its metadata file here. [Learn more](#)

Metadata from IdP
Add or edit metadata

[Import from XML file](#)

```
1 <?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:md"
2 <md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:md"
3 <md:KeyDescriptor use="signing">
4 <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
5 <ds:X509Data>
```

- Under SAML master backend role, enter the group ID of the Admin group you copied earlier.
- For Roles key, enter Role for the SAML assertion.
- This is because we defined and mapped Role to `${user:groups}` as a SAML attribute in IAM Identity Center.

SAML master backend role - optional

Any users with this backend role (usually called "groups" or "roles" in your IdP) receives full permission in OpenSearch Dashboards/Kibana. To use a SAML master backend role, configure the Roles key below.

88812390[redacted]

SAML master backend role must be no more than 256 characters.

Additional settings

Subject key - optional

If the IdP does not use the NameID element of the SAML assertion for username, specify the correct attribute here.

Roles key - optional

Specify the attribute of SAML assertion that contains backend role (usually called "groups or roles" in your IdP).

Role

Session time to live

By default, OpenSearch Dashboards/Kibana sessions last for 1440 minutes (24 hours).

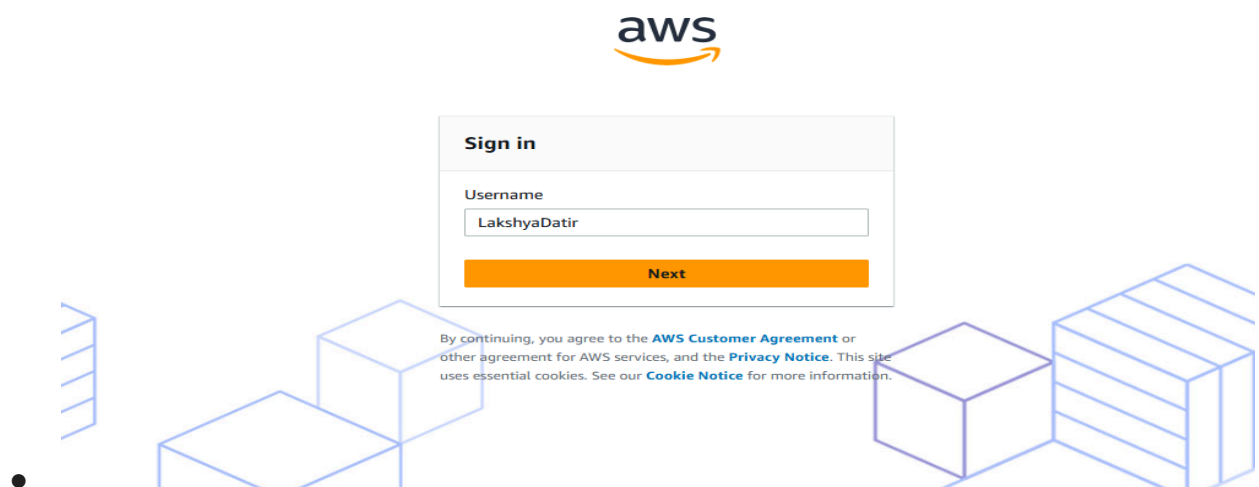
60 minutes

Specify an integer between 1 and 1,440 (24 hours).

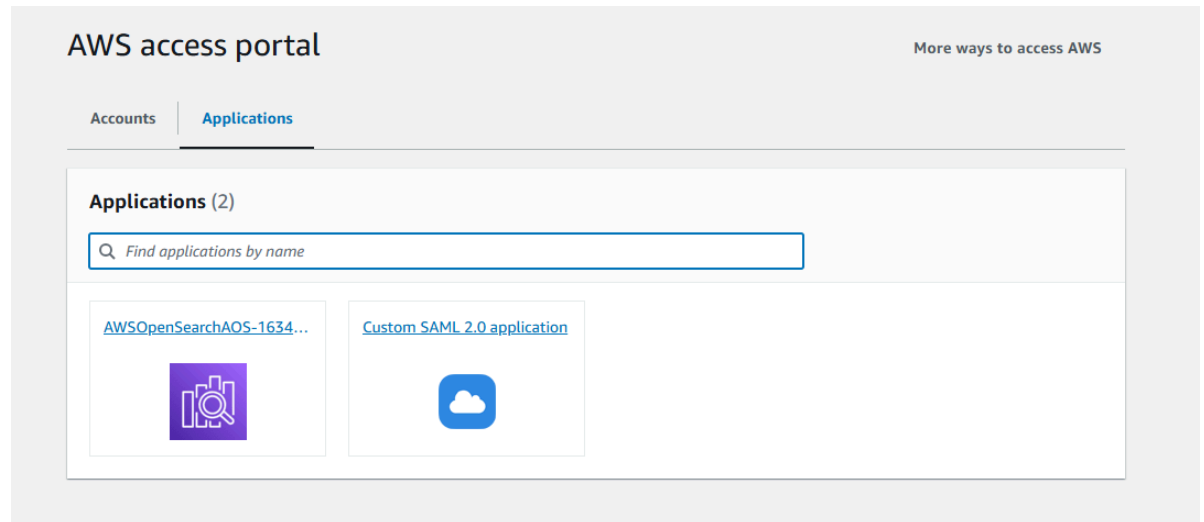
4. Configure backend role mapping for the Developer group

You have completely integrated IAM Identity Center with OpenSearch Service and mapped the Admin group as the primary role (all_access) in OpenSearch Service. Now you will log in to OpenSearch Dashboards as Admin and configure mapping for the Developer group.

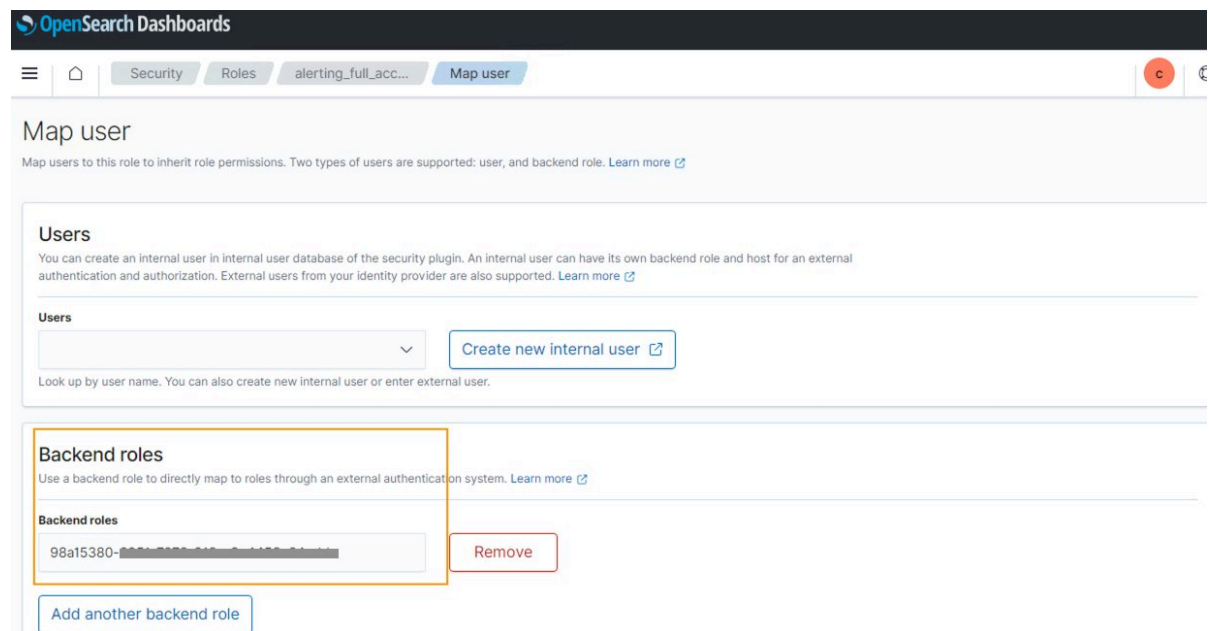
- OpenSearch Dashboards URL – On the OpenSearch Service console, navigate to your domain and choose the Dashboards URL under General Information. (For example, https://opensearch-domain-name-random-keys.us-west-2.es.amazonaws.com/_dashboards)
- AWS access portal URL – On the IAM Identity Center console, choose Dashboard in the navigation pane and choose the access portal URL under Settings summary. (For example, <https://d-1234567abc.awsapps.com/start>)
- Log in as the user in the Admin group.



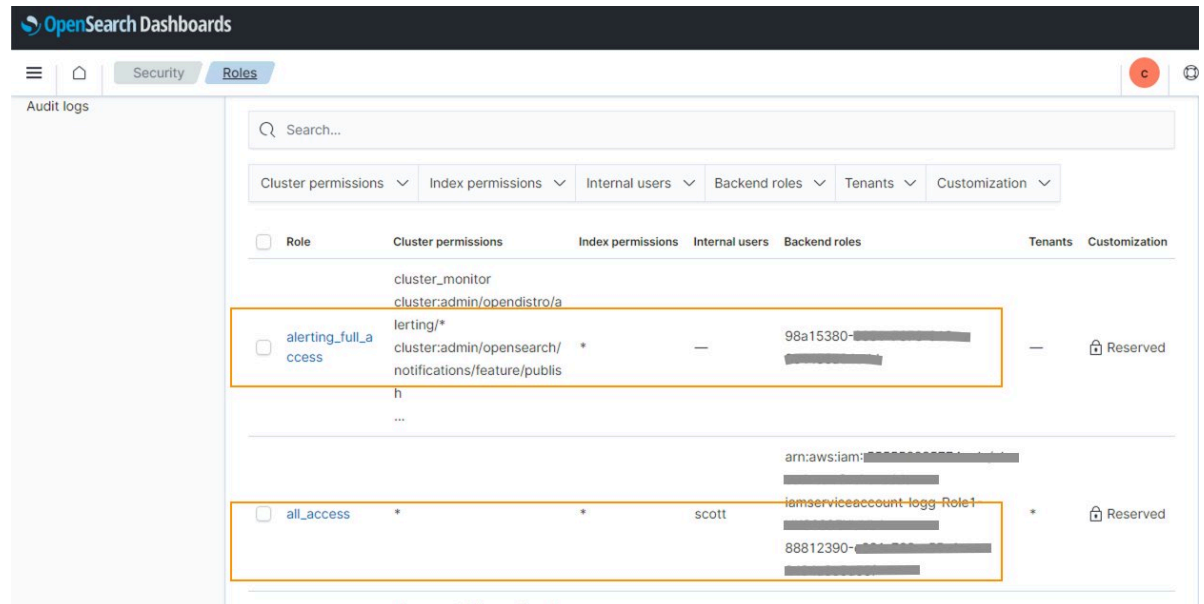
- Under the Application we can see our custom application that we have just created.



-
- Choose the menu icon, then choose Security, Roles.
- Choose the alerting_full_access role and on the Mapped users tab, choose Manage mapping.
- For Backend roles, enter the group ID of Developer.
- Choose Map to apply the change.



-
- Now you have successfully mapped the Developer group to the alerting_full_access role in OpenSearch Service.



5. Verify Permission

- Log out of the Admin account in OpenSearch Service as log in as a Developer user.
- Choose the OpenSearch Service application tile to be redirected to OpenSearch Dashboards.

Conclusion

In the Doc, we walked through a solution of how to map roles in Amazon OpenSearch Service to groups in IAM Identity Center by using SAML attributes to achieve role-based access control for accessing OpenSearch Dashboards. We connected IAM Identity Center users to OpenSearch Dashboards, and also mapped predefined OpenSearch Service security roles to IAM Identity Center groups based on group attributes. This makes it easier to manage permissions without updating the mapping when new users belonging to the same workgroup want to log in to OpenSearch Dashboards.

