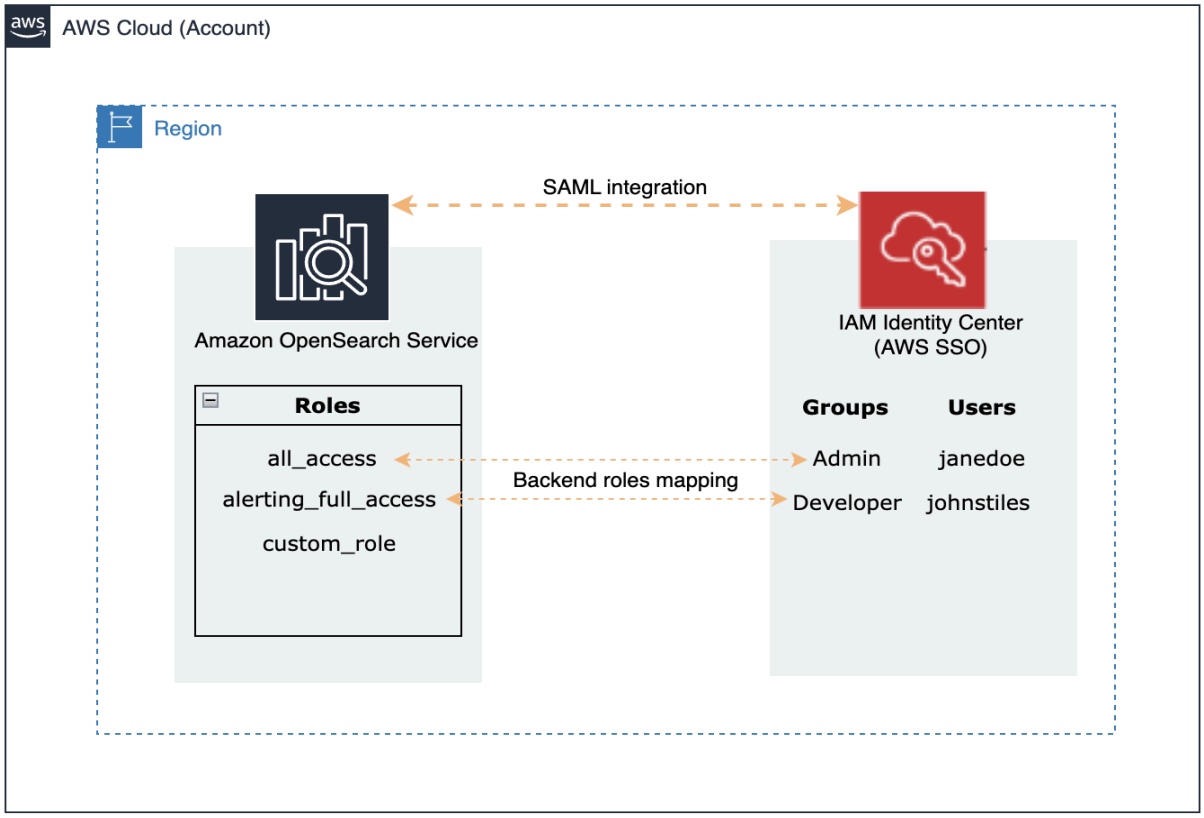
AWS OpenSearch Integration with IAM Identity Center

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.

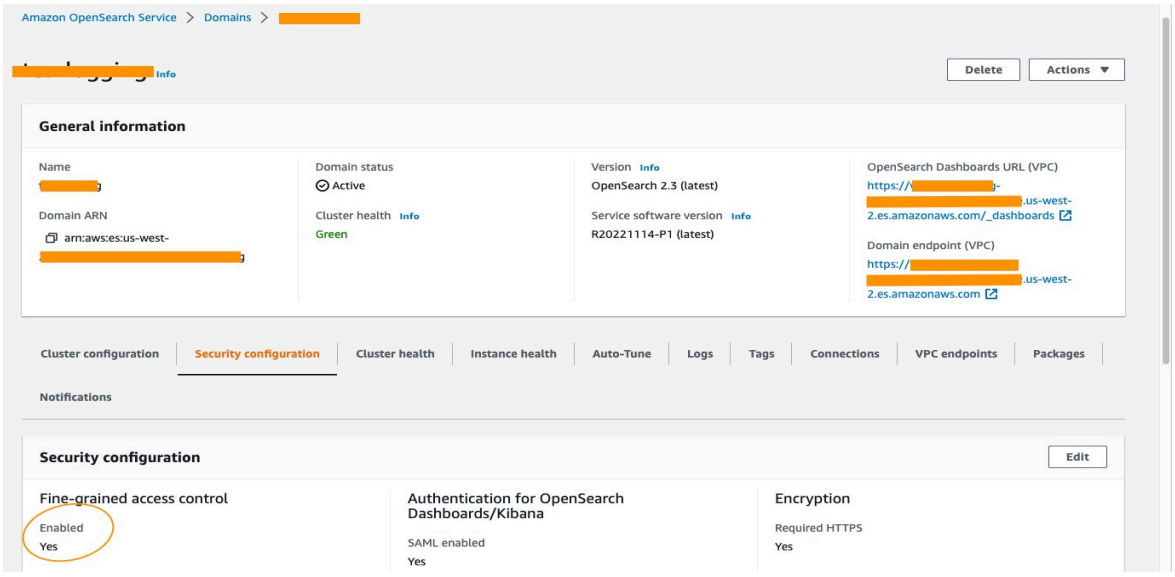


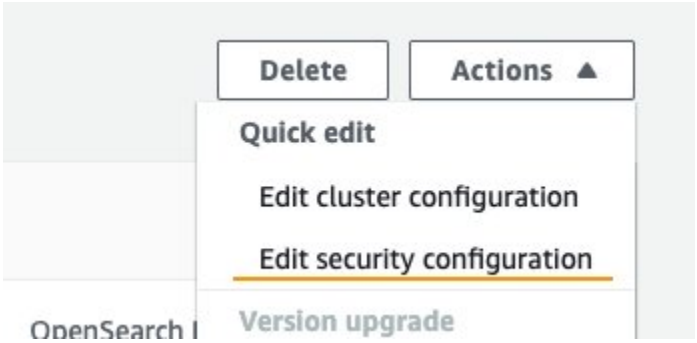
Prerequisites:

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.

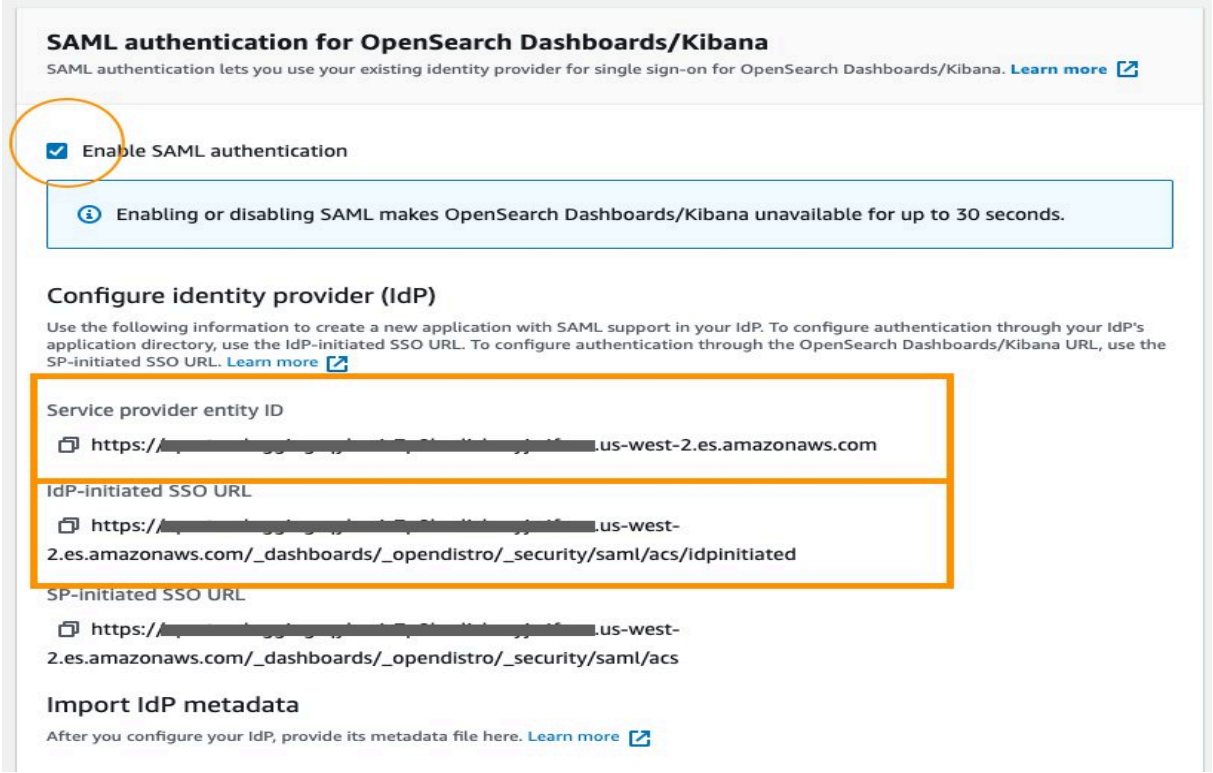
Steps to Configure IAM Identity Center with AWS OSS.

1. **Enable SAML in Amazon OpenSearch Service and copy SAML parameters.**
    - confirm that Fine-grained access control is enabled

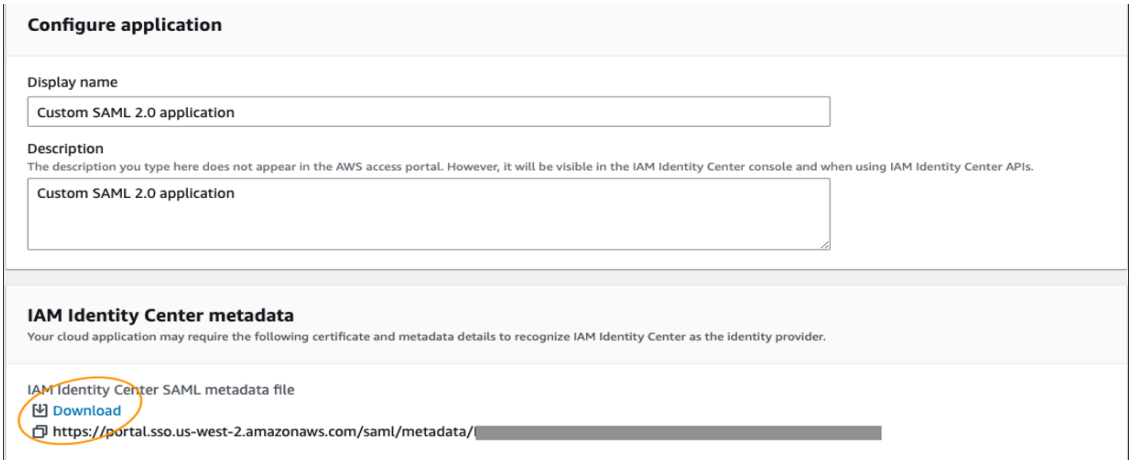
- 

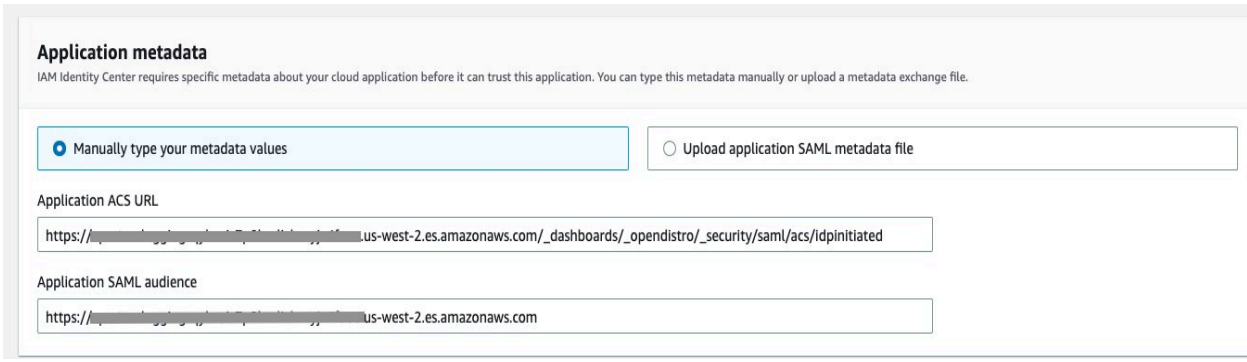
- On the Actions menu, choose Edit security configuration.
- 

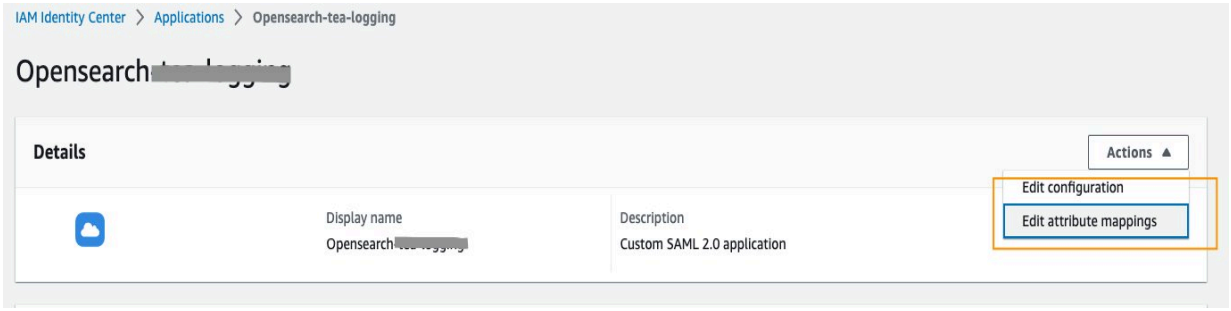
- Select Enable SAML authentication.
- You can also configure SAML during domain creation if you are creating a new OpenSearch domain. For more information, refer to SAML authentication for OpenSearch Dashboards.
- Copy the values for Service provider entity ID and IdP-Initiated SSO URL.

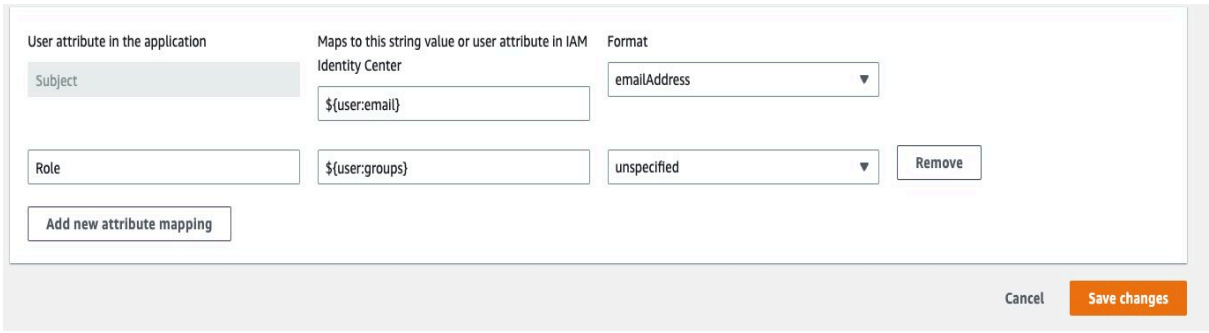
- 

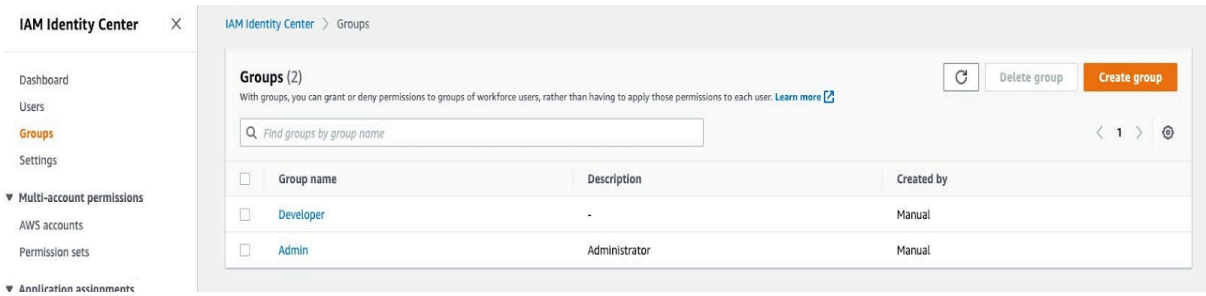
2. **Create a SAML application in IAM Identity Center**
    - On the IAM Identity Center console, choose Applications in the navigation pane.
    - Choose Add application.
    - Select Add customer SAML 2.0 application, then choose Next.
    - Enter your application name for Display name.
    - Under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

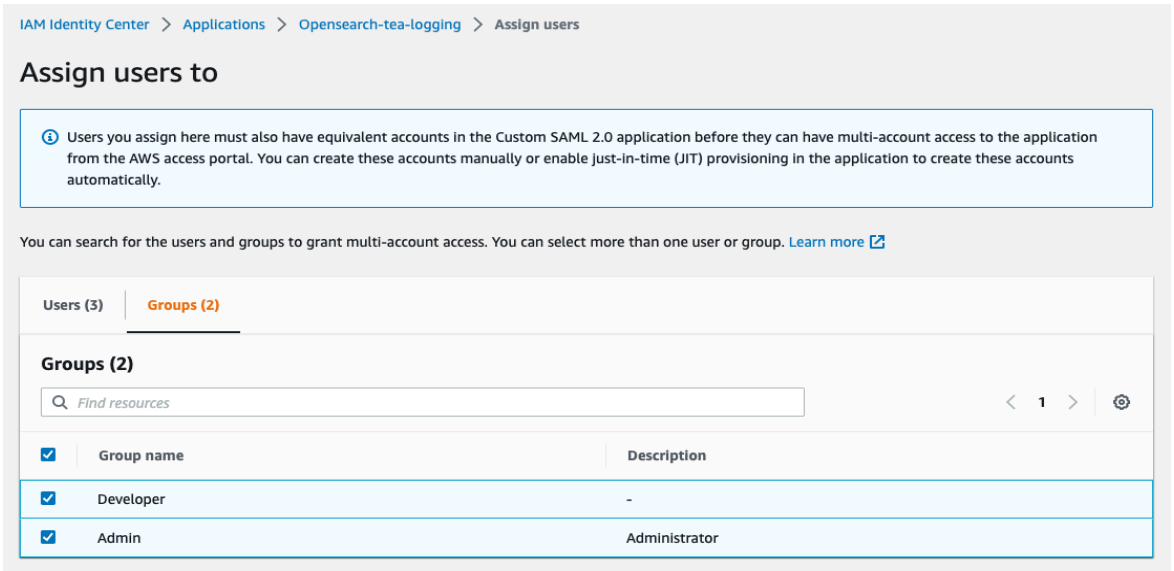
- 

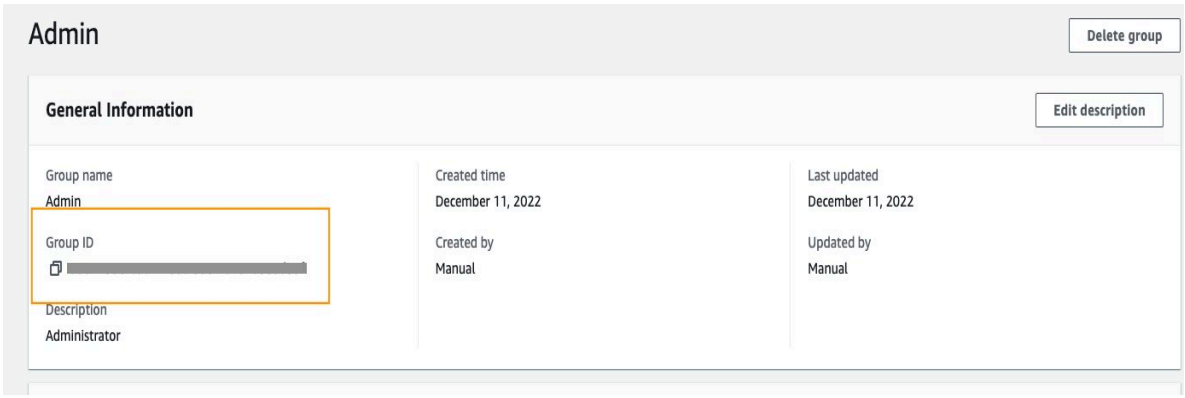
- Under Application metadata, select Manually type your metadata values.
- For Application ACS URL, enter the IdP-initiated URL you copied earlier.
- For Application SAML audience, enter the service provider entity ID you copied earlier.
- 

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

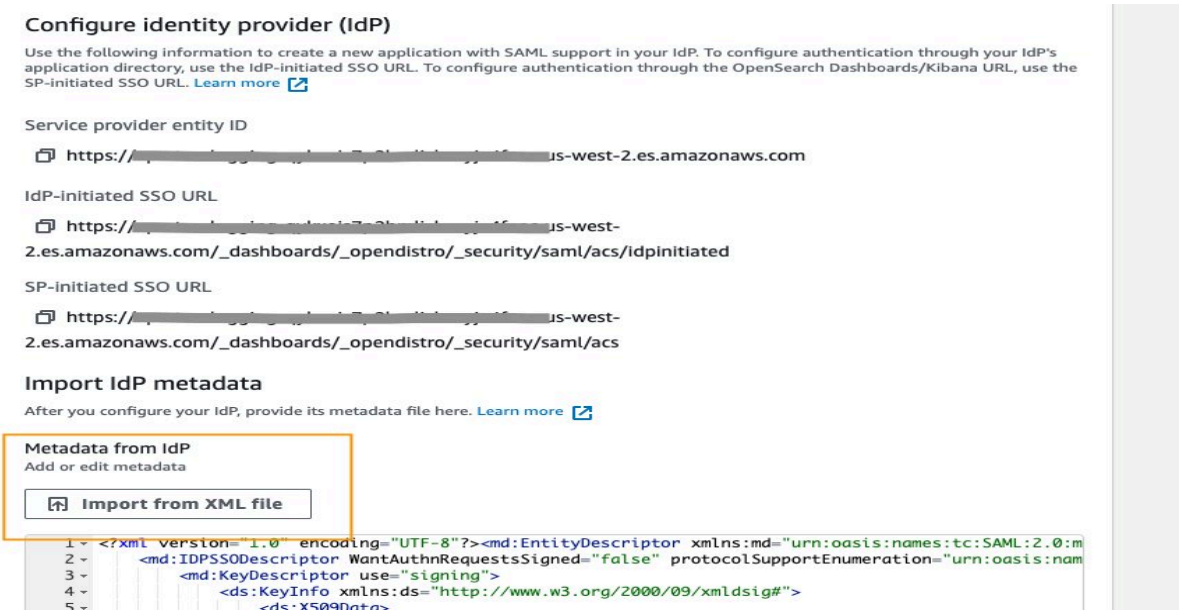
- Create attributes and map the following values:
- Subject map to ${user:email}, the format is emailAddress.
- Role map to ${user:groups}, the format is unspecified.
- 

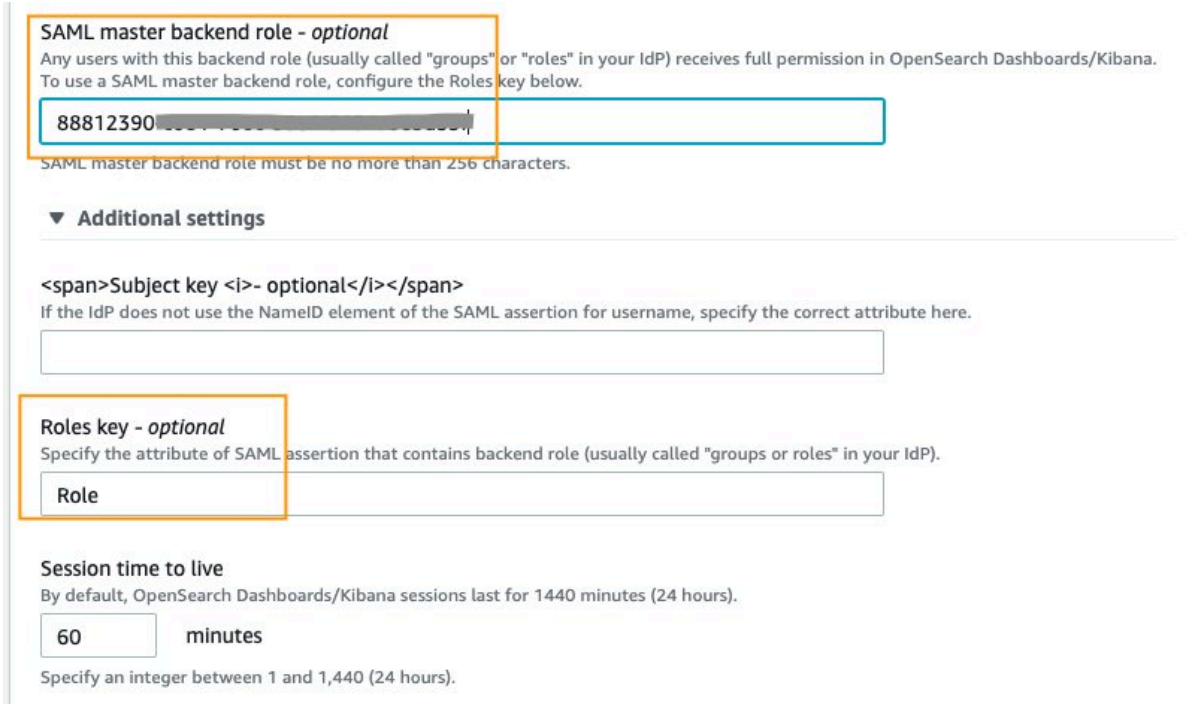
- On the IAM Identity Center console, choose Groups in the navigation pane.
- Create two groups: Developer and Admin. And assign the two groups to the SAML application we just created.
- 

- 

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

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.

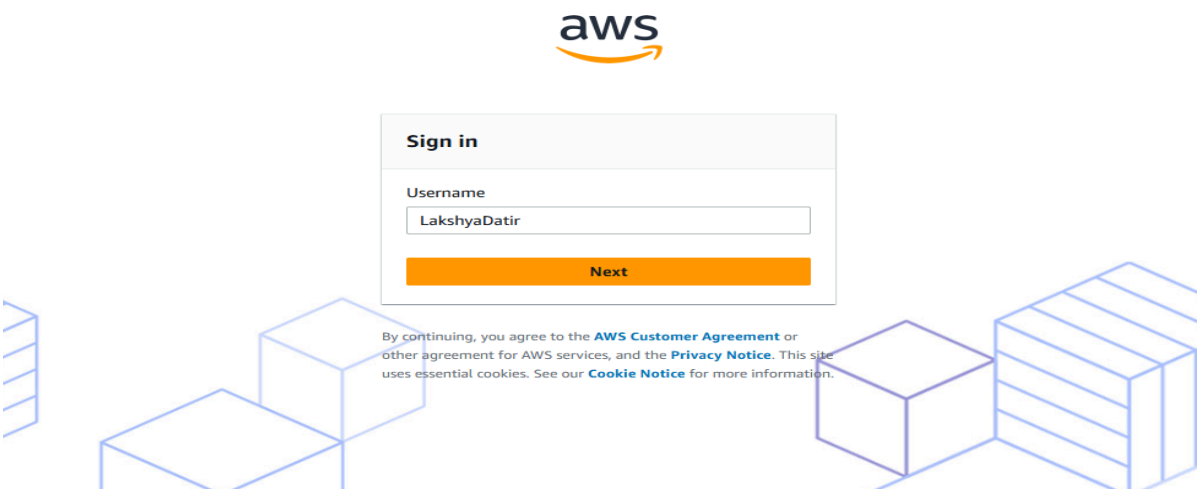
- 

- 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.
- 

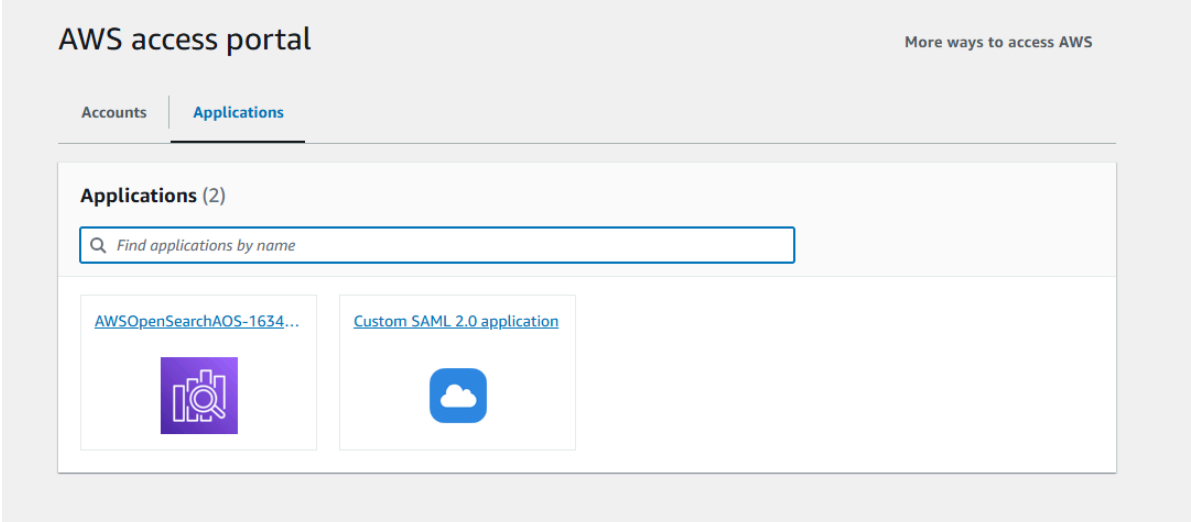
4. Configure backend role mapping for the Developer group

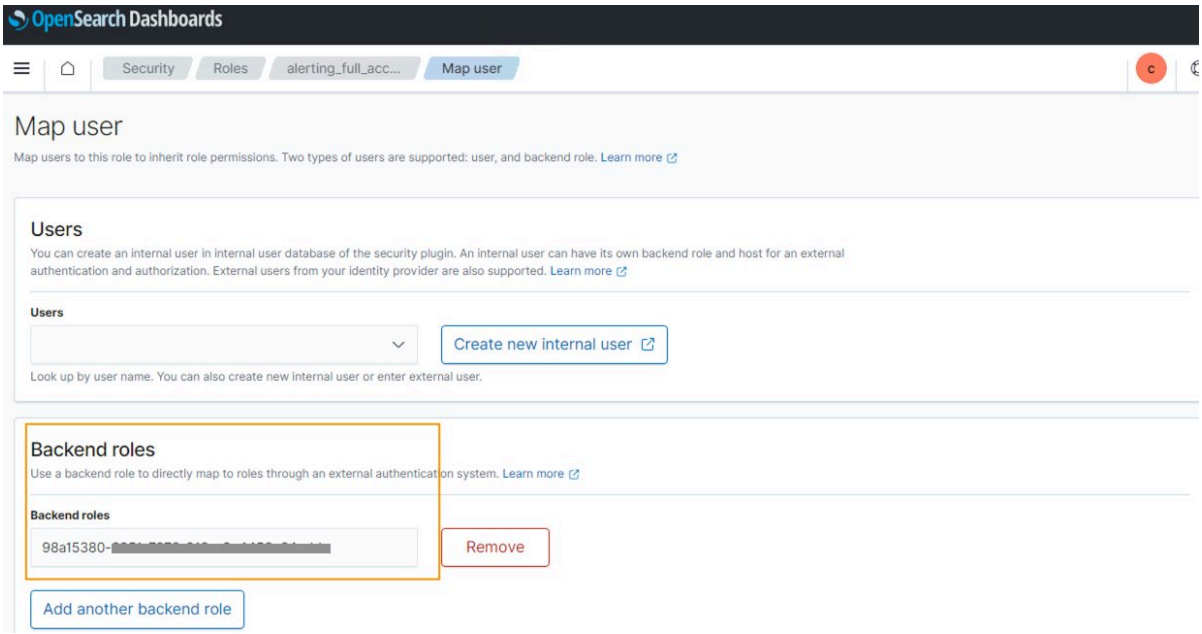
You have completely integrated IAM Identity Center with OpenSearch Service and mapped the Admin group as the primary role (all_access) in OpenSearch Service. Now you will log in to OpenSearch Dashboards as Admin and configure mapping for the Developer group.

- 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.

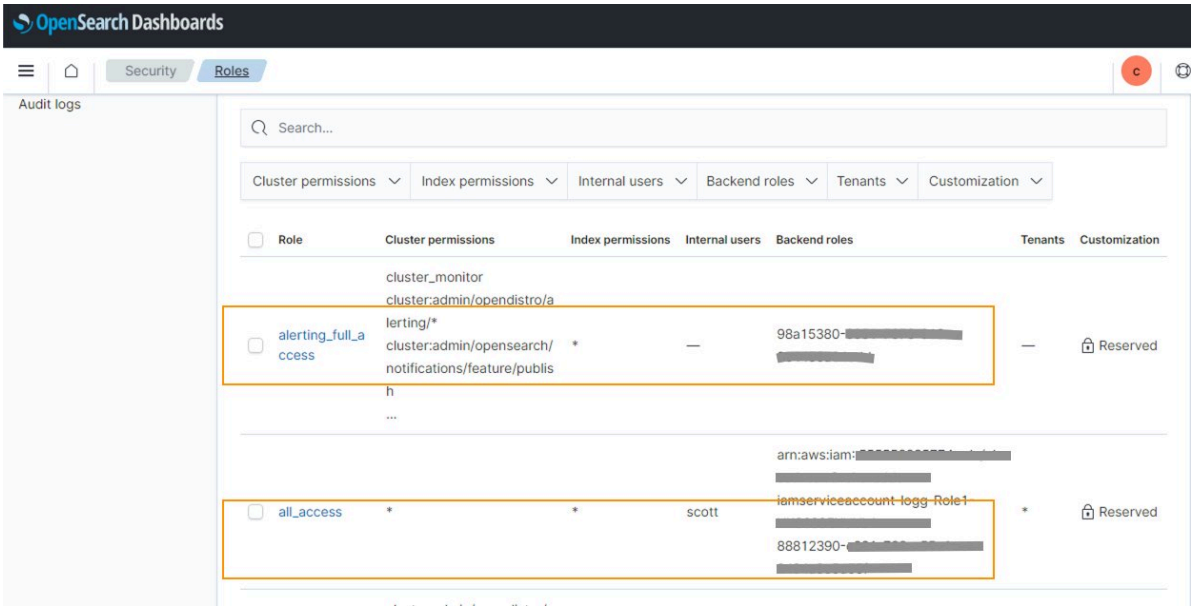


- Under the Application we can see our custom application that we have just created.

- 

- 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.