Configure Single-Sign On (SSO)

Step 1) Retrieve IDP Information to be configured

Before you can configure SSO for the cluster, you will need to configure your IDP to enable communication with the Cluster's Cognito User Pool.

One of the parameters needed for IDP configuration is the IDP response redirect URI. You can retrieve the cluster's IDP response redirect URI using the **show-idp-info** sub-command.

```
$ ./idea-admin.sh sso show-idp-info -h
Usage: idea-admin sso show-idp-info [OPTIONS]

  print single sign-on IDP redirect uri and related information for the cluster

  When provider_type = OIDC:
  Identity Provider Redirect URI = [cognito_domain_url]/oauth2/idpresponse

  When provider_type = SAML:
  Identity Provider Redirect URI = [cognito_domain_url]/saml2/idpresponse
  Entity ID = urn:amazon:cognito:sp:[cognito_user_pool_id]

  Use this URI to configure your Identity Provider before you enable SSO for the cluster.

Options:
  --cluster-name TEXT   Cluster Name  [required]
  --aws-region TEXT     AWS Region  [required]
  --aws-profile TEXT    AWS Profile Name
  --provider-type TEXT  Identity Provider Type. Can be one of [OIDC, SAML].  [required]
  -h, --help            Show this message and exit.
```

In order to reduce the potential for misconfiguration, the parameter **--provider-type** is required when displaying the redirect information. This will display the proper redirect URI for the selected provider type.

```
$ ./idea-admin.sh sso show-idp-info --aws-region=us-east-1 --cluster-name=idea-ssoo --provider-type=OIDC
Redirect URL
https://idea-ssoo-b71b7d94-1b8b-4076-bd46-b0589311bf47.auth.us-east-1.amazoncognito.com/oauth2/idpresponse

Configure the above information in your IDP prior to running ./idea-admin.sh sso configure ...
```

Step 2) Configure your IDP (External)

This step is a manual step and needs to be performed outside any tooling supported by IDEA.

While any OIDC/SAML provider should work these are routinely tested as part of the IDEA development process:

1. Azure (AzureAD)
2. Okta
3. Ping Identity

If you have a specific provider that needs to be added for regular testing - please reach out to the IDEA team.

Your IDP must support **OIDC** or **SAML v2** protocols to enable SSO on IDEA cluster. When configuring your IDP, you will need to ensure 2 things:

1. The IDP Redirect URI configured on the IDP must match the same as returned in Step 1
2. The claims from IDP must contain an email address. Make sure to note the name of the email attribute as we will use it in Step 3. (Used as **--provider-email-attribute**)

Redirect URI Warning

Make sure to generate and configure the redirect URI for the proper protocol / provider-type !

Attempting to use a SAML provider with an OIDC URI (**/oauth**..) or vice-versa will not work and can be easy to overlook during the installation/configuration process!

Step 3) Configure SSO for your IDEA Cluster

You can configure SSO for your IDEA cluster using the **idea-admin.sh sso configure** command.

```
$ ./idea-admin.sh sso configure --help
Usage: idea-admin sso configure [OPTIONS]

  configure single sign-on for the cluster

Options:
  --cluster-name TEXT             Cluster Name  [required]
  --aws-region TEXT               AWS Region  [required]
  --aws-profile TEXT              AWS Profile Name
  --provider-name TEXT            Identity Provider Name  [required]
  --provider-type TEXT            Identity Provider Type. Can be one of [OIDC, SAML].  [required]
  --provider-email-attribute TEXT
                                  The name of the email attribute from Provider.  [required]
  --refresh-token-validity-hours INTEGER
                                  Refresh token validity in hours. Default: 12
  --oidc-client-id TEXT           OIDC Client Id.
  --oidc-client-secret TEXT       OIDC Client Secret
  --oidc-issuer TEXT              OIDC Issuer. The issuer URL you received from the OIDC provider.
  --oidc-attributes-request-method TEXT
                                  OIDC Attributes Request Method
  --oidc-authorize-scopes TEXT    OIDC Authorize Scopes
  --oidc-authorize-url TEXT       OIDC Authorize URL. The endpoint a user is redirected to at sign-in.
  --oidc-token-url TEXT           OIDC Token URL. The endpoint Amazon Cognito uses to exchange the code
received in a user's request for an ID token.
  --oidc-attributes-url TEXT      OIDC Attributes URL. Also called as UserInfo endpoint. The userInfo endpoint
is used by Cognito to retrieve information about the authenticated user.
  --oidc-jwks-uri TEXT            OIDC JWKS URI. The endpoint used to decode and verify tokens issued by the
identity provider.
  --saml-metadata-url TEXT        SAML Metadata URL
  --saml-metadata-file TEXT       SAML Metadata File
  -h, --help                      Show this message and exit.
```

To configure an OIDC based IDP, you can the the **sso configure** command as below:

TODO - Update this Example 9 Dec 2022 - Out of date !

```
./idea-admin.sh sso configure --cluster-name idea-dev1 --aws-region us-east-1 \
                                                    --provider-name AmazonFederate \
                                                    --provider-type OIDC \
                                                    --provider-email-attribute EMAIL \
                                                    --oidc-client-id idea-dev1-us-east-1 \
                                                    --oidc-client-secret YOUR_OIDC_SECRET \
                                                    --oidc-issuer https://idp-integ.federate.amazon.com \
                                                    --oidc-authorize-url https://idp-integ.federate.amazon.com
/api/oauth2/v1/authorize \
                                                    --oidc-token-url https://idp-integ.federate.amazon.com/api
/oauth2/v2/token \
                                                    --oidc-attributes-url https://idp-integ.federate.amazon.com
/api/oauth2/v1/userinfo \
                                                    --oidc-jwks-uri https://idp-integ.federate.amazon.com/api
/oauth2/v2/certs
updating config: cluster.cognito.sso_idp_provider_name = AmazonFederate
updating config: cluster.cognito.sso_idp_identifier = single-sign-on-identity-provider
* identity provider created
updating config: cluster.cognito.sso_client_id = 7lda3qh4uguvqho4o5jpioqod5
updating config: cluster.cognito.sso_client_secret = arn:aws:secretsmanager:us-east-1:640877479485:secret:idea-
dev1-sso-client-secret-yzgvaZ
* user pool client created
system administration user found: clusteradmin. skip linking with IDP.
* existing users linked with IDP
updating config: cluster.cognito.sso_enabled = True
* Single Sign-On enabled for cluster
```

Example: Configure SAML based IDP

In this example we are configuring/updating a SAMLv2 provider (Azure AD).

Note the full use of the email attribute URL as this is how it is configured in the AzureAD portal.

SAML Example

```
$ ./idea-admin.sh sso configure --aws-region us-east-1 --cluster-name idea-sso3 --provider-type SAML  --
provider-name SAML  --provider-email-attribute=http://schemas.xmlsoap.org/ws/2005/05/identity/claims
/emailaddress --saml-metadata-url=https://login.microsoftonline.com/158864e7-df42-46f1-9001-61a0295efc5e
/federationmetadata/2007-06/federationmetadata.xml?appid=0b6c222f-7bab-4c0f-8479-3f3702777303
updating config: identity-provider.cognito.sso_idp_provider_name = SAML
updating config: identity-provider.cognito.sso_idp_provider_type = SAML
updating config: identity-provider.cognito.sso_idp_identifier = single-sign-on-identity-provider
updating config: identity-provider.cognito.sso_idp_provider_email_attribute = http://schemas.xmlsoap.org/ws/2005
/05/identity/claims/emailaddress
? identity provider created
? user pool client created
system administration user found: clusteradmin. skip linking with IDP.
? existing users linked with IDP
updating config: identity-provider.cognito.sso_enabled = True
? Single Sign-On enabled for cluster
$
```

Example: Okta - SAML Provider with a downloaded Metadata file.

Download the metadata file (XML file) from the provider and make it available on the system where **idea-admin.sh** is being run.

In this example we have copied the file to **okta.xml** in the same directory. Additionally we can see the attribute name of "**emailaddress**" is being used from the Okta configuration to match the email address of our invited IDEA users.

```
$  ./idea-admin.sh sso configure --provider-type=SAML --provider-name=Okta --provider-email-
attribute=emailaddress --aws-region=us-east-1 --cluster-name idea-ssoo  --saml-metadata-file=okta.xml
updating config: identity-provider.cognito.sso_idp_provider_name = Okta
updating config: identity-provider.cognito.sso_idp_provider_type = SAML
updating config: identity-provider.cognito.sso_idp_identifier = single-sign-on-identity-provider
updating config: identity-provider.cognito.sso_idp_provider_email_attribute = emailaddress
? identity provider created
updating config: identity-provider.cognito.sso_client_id = 44r7fuc6ivu0jga052kbu6969u
updating config: identity-provider.cognito.sso_client_secret = arn:aws:secretsmanager:us-east-1:682922835204:
secret:idea-ssoo-sso-client-secret-sUXyAu
? user pool client created
system administration user found: clusteradmin. skip linking with IDP.
? existing users linked with IDP
updating config: identity-provider.cognito.sso_enabled = True
? Single Sign-On enabled for cluster
$
```

Step 4) User Login