Cloudera on Premises Data Services 1.5.5

Cloudera Data Services on premises User Management

Date published: 2023-12-16
Date modified: 2026-08-26



https://docs.cloudera.com/

Legal Notice

© Cloudera Inc. 2026. All rights reserved.

The documentation is and contains Cloudera proprietary information protected by copyright and other intellectual property rights. No license under copyright or any other intellectual property right is granted herein.

Unless otherwise noted, scripts and sample code are licensed under the Apache License, Version 2.0.

Copyright information for Cloudera software may be found within the documentation accompanying each component in a particular release.

Cloudera software includes software from various open source or other third party projects, and may be released under the Apache Software License 2.0 (“ASLv2”), the Affero General Public License version 3 (AGPLv3), or other license terms. Other software included may be released under the terms of alternative open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

Please visit the Cloudera software product page for more information on Cloudera software. For more information on Cloudera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cloudera reserves the right to change any products at any time, and without notice. Cloudera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cloudera.

Cloudera, Cloudera Altus, HUE, Impala, Cloudera Impala, and other Cloudera marks are registered or unregistered trademarks in the United States and other countries. All other trademarks are the property of their respective owners.

Disclaimer: EXCEPT AS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT WITH CLOUDERA, CLOUDERA DOES NOT MAKE NOR GIVE ANY REPRESENTATION, WARRANTY, NOR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH CLOUDERA TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. CLOUDERA DOES NOT WARRANT THAT CLOUDERA PRODUCTS NOR SOFTWARE WILL OPERATE UNINTERRUPTED NOR THAT IT WILL BE FREE FROM DEFECTS NOR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION NOR UNAVAILABILITY, NOR THAT IT WILL MEET ALL OF CUSTOMER’S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDERA EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, NON-INFRINGEMENT, TITLE, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY REPRESENTATION, WARRANTY, OR COVENANT BASED ON COURSE OF DEALING OR USAGE IN TRADE.

Contents

Managing user access and authorization..... 5

Access paths to Cloudera and its components.....6

Onboarding users.....7
Configuring identity providers with LDAP..... 7
Configuring LDAP authentication for Cloudera on premises..... 7
Updating an identity provider..... 10
Changing your Local Administrator password..... 10
Importing or uploading users..... 11
Synchronizing group membership.....11
Configuring identity providers with SAML.....12
Generating the identity provider metadata.....14
Setting up the identity provider in Cloudera..... 15
Configuring your enterprise IdP to work with Cloudera as a service provider..... 19
Updating an identity provider..... 20
Migrating users from another preferred identity provider..... 21

Understanding Cloudera on premises user accounts.....22
Cloudera account administrator.....22
Cloudera user..... 22
Cloudera machine user..... 23

Working with machine users.....23
Creating a machine user.....23
Generating an API access key..... 24
Deleting a machine user.....25

Understanding roles.....25
Assigning account-level roles to users.....27
Assigning resources to users..... 28

Enabling admin and user access to environments..... 29

Understanding Cloudera groups.....29
Creating a group..... 29
Adding or removing a user from a group.....30
Assigning account roles to a group.....31
Assigning resource roles to a group..... 32
Assigning a group membership administrator..... 33
Removing a group membership administrator.....34
Updating a group..... 34

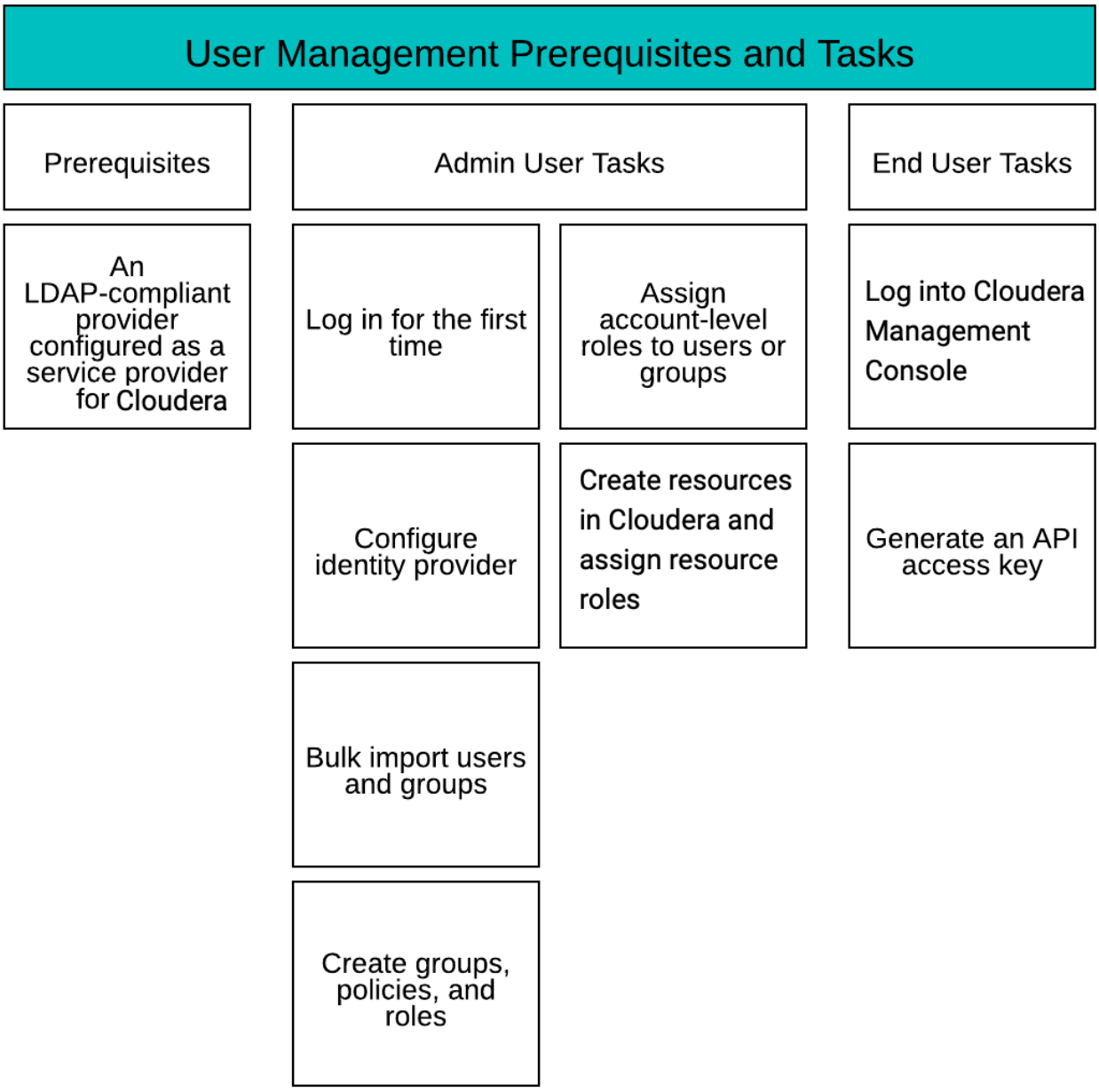
Removing account roles from a group....35
Deleting a group....35
Reserved group names....36

Managing user access and authorization

To provide access to resources such as environments and clusters, you must add users and assign roles and resources to them.

Using the Cloudera Management Console on premises, you can perform the following tasks:

- Onboarding users
  - Configuring identity providers
  - Importing or uploading users
- Managing users
  - Adding users
  - Creating machine users
  - Deleting machine users
  - Assigning roles to users
  - Assigning environments to users
  - Generating access keys to users
  - Removing roles assigned to users
  - Unassigning roles to users
  - Unassigning resources to users
- Managing groups
  - Adding groups
  - Assigning roles to groups
  - Adding users to groups
  - Assigning a group membership administrator
  - Unassigning roles to groups
  - Unassigning resources to groups



Access paths to Cloudera and its components

To access the various Cloudera components, you must understand the access paths unique to the entry points that are specific to users and situations.

The typical access entry methods and their details are as follows:

- LDAP access through Cloudera Management Console - After configuration of LDAP authentication, users can make use of their credentials to access Cloudera services such as Cloudera AI Workbench and Virtual Data Warehouses. Cloudera on premises supports both Microsoft Active Directory LDAP and Open LDAP for user authentication.
- SSO access through Cloudera Management Console - After the initial identity provider configuration, users logged into the Cloudera Management Console can automatically access services such as Cloudera AI Workbench through internal SSO.

- Machine user access - To get programmatic access to Cloudera and its services, you can create and use a machine user. The process to set up the machine user for access is as follows:
  - Create a machine user in the User Management section of Cloudera Management Console.
  - Get access keys in the Cloudera Management Console for this machine user.

Onboarding users

To enable users to work on the various Cloudera components and services, you can onboard them by using LDAP and optionally SAML.

Configuring identity providers with LDAP

You can onboard users by setting up identity federation with Cloudera.

If your organization uses an enterprise Identity Provider (IdP) that is compliant with Lightweight Directory Access Protocol (LDAP), you can set up identity federation with Cloudera. Identity federation allows users within your organization to log in to Cloudera through the authentication system in your organization without registering with Cloudera or creating a Cloudera account.

Configuring LDAP authentication for Cloudera on premises

You can configure LDAP user authentication for Cloudera on premises from the Administration page of the Cloudera Management Console.

Before you begin

If you intend to use Hue as your SQL editor in Cloudera Data Warehouse, you must use LDAP over SSL.

Procedure

1. Sign in to the Cloudera console.
2. Click Cloudera Management Console.
3. On the Cloudera Management Console home page, select Administration>Authentication.
4. Configure the following settings for LDAP authentication:

Property	Description	Sample values
LDAP URL	The LDAP server URL. The URL must be prefixed with ldap:// or ldaps://. The URL can optionally specify a custom port, for example: ldaps://ldap_server.example.com:1636. **Note:** Cloudera recommends that you use Active Directory (AD) Global Catalog ports 3268 and 3269 if you are using LDAP referrals. **Note:** If you do not use Global Catalog port, environment activation fails with "Unable to create cluster initial state: Active Directory servers should be used through the Global Catalog ports 3268/3269" error.	ldap://<ldap-host>:389 or ldaps://<ldap-host>:636 For Active Directory use: `ldap://<AD Server>:3268 or ldaps://<AD Server>:3269`

Property	Description	Sample values

CA Certificate for Secure LDAP	The X.509 PEM certificate to be used to access secure LDAP (URLs starting with ldaps://). Ensure that at least one valid certificate is provided. A typical CA certificate is structured as follows:
	`-----BEGIN CERTIFICATE-----`
	`...`
	`-----END CERTIFICATE-----`
		If you add or update CA certificates and you have deployed the Cloudera Data Warehouse service in your ECS cluster, you must refresh the affected Database Catalogs and Virtual Warehouses from the Cloudera Data Warehouse. Go to the Cloudera Data Warehouse UI, click on the more vertical menu on the Database Catalog or Virtual Warehouse and click Refresh.

LDAP Bind DN	The Distinguished Name of the user to bind to LDAP for user authentication search/bind and group lookup for role authorization.	Distinguished Name (DN) example: CN=cdh admin,OU=svcaccount,DC=example,DC=com FreeIPA example: uid=username,cn=users,cn=accounts,dc=example,dc=com
LDAP Bind Password	The bind user password.	
LDAP User Search Base	The distinguished name indicating the path within the directory information tree from which to begin user searches.	AD example: cn=users,dc=example,dc=com LDAP example: ou=people,dc=example,dc=com FreeIPA example: cn=accounts,dc=example,dc=com
LDAP User Search Filter	The search filter to use for finding users.	AD example: If you want to filter users belonging to specific group say MLgroup, then set the filter as: "" (&(sAMAccountName={0})(memberof=CN=MLgroup,OU=Users,OU=XX,OU=XXX,DC= """" LDAP example: (uid={0}) Note that a custom attribute can also be used if the directory is configured differently for user names. The {0} expands the currently authenticating user's name entered in the login form for the query. FreeIPA example: (&(uid={0})(objectClass=person))
LDAP Group Search Base	The distinguished name indicating the path within the directory information tree to begin group searches from.	cn=accounts,dc=example,dc=com

Property	Description	Sample values

LDAP Group Search Filter	The search filter to use for finding groups for authorization of authenticated users for their roles. You must configure this value such that only the groups associated with the user logging in are fetched from the IdP.
	There are two placeholders that can be used to match the groups of a user, {0} and {1}. {0} expands into the user DN and {1} expands into the username.
		For Active Directory and openLDAP compatible directories this will usually be (member={0}), where {0} will be replaced by DN string for a successfully authenticated user through the search/bind process. This requires configuration of the LDAP Bind User Distinguished Name field.
		AD example:
		`(member={0})`
		LDAP/FreeIPA example:
		`(&(member={0})(objectClass=posixgroup)(!(cn=admins)))`

Email Mapping Attribute	The LDAP attribute to be used for mapping the email in Identity Management. If no value is provided, mail is used as the default email mapping attribute. Email is a mandatory value in Cloudera. If no value is found for the email attribute, a value of {userame}@cdp.example is assumed for the user.	
Username Mapping Attribute	The LDAP attribute to be used for mapping the userId in Identity Management. **Important:** This property must be provided.	The Username Mapping Attribute must be configured as sAMAccountName. An incorrect value (for example, (sAMAccountName={0})) may result in duplicate users being created in UMS, which could cause user access and authorization issues.

Note: For information on setting search filters for nested groups, see *Nested LDAP Group Resolution*.

5. If required, select Show Other Options and configure the following additional settings:

Property	Description	Sample values
LDAP User Bind Property	The property of the LDAP user object to use when binding to verify the password.	This value should always be set to dn.
Groupname Mapping Attribute	The LDAP attribute to be used for mapping the groupId in Identity Management.	
Group DN Property	The property of user object to use in {{dn}} interpolation of groupSearchFilter.	This value should always be set to dn.
First Name Mapping Attribute	The LDAP attribute to be used for mapping the first name attribute in Identity Management.	
Last Name Mapping Attribute	The LDAP attribute to be used for mapping the last name attribute in Identity Management.	

Note: If the username and email attributes on the LDAP server contain spaces, Cloudera Management Console includes the spaces when copying the corresponding attribute information.

6. Click Test Connection to verify whether the LDAP information you have provided is valid.

   Cloudera Management Console attempts a connection with the LDAP source based on the information provided, and returns a confirmation message if the connection is successful.

7. Click Save. The LDAP users are listed on the User Management page.



Important: In Cloudera Data Services on premises 1.5.5 SP3 and higher releases, if you update LDAP configurations after creating Cloudera Data Engineering Service or Virtual Cluster, you must update and synchronize these changes in the Cloudera Data Engineering Service. For more information, see Updating and synchronizing stale configurations.

Updating an identity provider

You can update the access keys and roles associated with a CDP identity provider. To update an identity provider in CDP, you must be a CDP account administrator or have the PowerUser role.

Procedure

1. Sign in to the Cloudera console.
2. Click Cloudera Management Console.
3. In the side navigation panel, click User Management.
4. Click the user name you want to update.
5. Click the Roles tab.

   Alternatively, you can click the Actions button and select Update Roles.
6. Choose the checkbox next to the roles you want to add for the user or unclick the checkbox next to roles you want to remove for the user.
7. Click Update.
8. If you choose to use a Bind DN, enter the appropriate information in the LDAP Bind DN and LDAP Bind Password fields.
9. If you want to specify LDAP attribute for mapping the email in Identity Management, enter it in the Email Mapping Attribute field.

   If you do not enter an email, the default is mail.
10. If you are using a non-standard attribute, click Show Other Options.
    a) Enter DN in the LDAP User Bind Property field.
    b) Enter the LDAP attribute for mapping the group ID in Identify Management in the Groupname Mapping Attribute field.
    c) Enter the property of the user object in the Group DN Property field.
    d) Enter the first and last name of the attribute in the First Name Mapping Attribute and Last Name Mapping Attribute fields.

       These attributes are optional.
11. Click Save.
12. Verify the updates and click OK.

    Cloudera updates the information for the Cloudera identity provider.

Changing your Local Administrator password

Cloudera Management Console uses a default password for your Local Administrator account. After you access Cloudera Management Console for the first time you should change your Local Administrator password for security reasons.

About this task

Procedure

1. Sign in to the CDP console with the Local Administrator account..
2. Click Cloudera Management Console.
3. On the Cloudera Management Console home page, select Administration>Authentication.

4. Click Change Password then enter and confirm your new password.
5. Click Change to save your changes.

Importing or uploading users

You can bulk import users to Cloudera on premises and assign them access rights and roles. Importing users in bulk allows admins to prepare the system for the desired level of access before users log in to Cloudera on premises.

Procedure

1. Sign in to the Cloudera console.
2. Click Cloudera Management Console.
3. Click User Management in the left navigation panel.

   The Users page displays the list of all Cloudera users.
4. Click Actions.
5. From the dropdown list that appears, click Upload Users.

   The Upload Users page appears.
6. Select an identity provider from the dropdown list.
7. Select an option for adding user details:
   - File Upload - If you want to upload a CSV or a JSON file with the details of the users that you like to add.
   - Direct Input - Enter the user details in the format specified. Make sure you add the header row as specified in the sample.
8. Click Next.
9. In the Preview Users screen that appears, verify if all the details are uploaded or added accurately.
10. Click Upload.

Synchronizing group membership

Cloudera can synchronize the user's group membership provided by your enterprise Identity Provider (IdP) with the user's group membership in Cloudera.

When a user initially logs in to Cloudera through the identity management system in your organization, Cloudera creates a Cloudera user account for the user. However, without being assigned Cloudera roles, the user cannot perform tasks in Cloudera. Cloudera recommends that you create ph conkeyref="product-names/cloudera"/> groups with assigned roles and add users to the groups so that the users can take on the roles assigned to the groups.

When you create an identity provider, you can select the Sync Groups on Login option to enable Cloudera to synchronize the user group membership. By default, the Sync Groups on Login option is disabled. Clear the option selection if you do not want Cloudera to synchronize the user group membership.

Group names must be alphanumeric, may include '-' and '_', and be fewer than 32 characters long. Additionally, names can only start with an alphabet or an underscore.

Sync Groups on Login enabled

When the Sync Groups on Login option is enabled, Cloudera synchronizes a user's group in the following manner:

- The group membership that your enterprise IdP specifies for a user overrides the group membership set up in Cloudera. Each time a user logs in, Cloudera updates the user's group membership based on the groups that your enterprise IdP specifies for the user.
- If the group exists in Cloudera, Cloudera adds the user to the group. The user takes on all the roles associated with the group.
- If the group does not exist in Cloudera, Cloudera creates the group and adds the user to the group. However, no roles are assigned to the new group, so a member of the new group does not take on roles from the group.

- If the user is a member of a group in Cloudera that is not included in the list provided by your enterprise IdP, Cloudera removes the user from the group.
- If the list of groups from your enterprise IdP is empty, Cloudera removes the user from all groups in Cloudera. After login, the user will not be a member of any Cloudera group and will not have roles from any group.

To ensure that users can perform tasks in Cloudera, It is recommended that you set up the groups in Cloudera with appropriate roles before you assign them to users.

Important: Cloudera on premises currently *does not support* synchronization of user groups for Cloudera Data Warehouse workloads.

Sync Groups on Login disabled

When the Sync Groups on Login option is disabled, Cloudera does not synchronize the user's group membership in Cloudera with the user's group membership provided by the IdP. After login, a user's group membership in Cloudera is determined by the Cloudera groups assigned to the user in Cloudera. The groups assigned to the user in your enterprise IdP are ignored.

Sync Membership option for a newly created group

Additionally, once you have synced your IdP and you create a new group in Cloudera, you have an option called Sync Membership that determines whether group membership is synced to IdP when a user logs in. By default, Sync Membership is enabled when Sync Groups on Login is enabled.

The following table describes how the global Sync Groups on Login and the per-group Sync Membership options can be used:

	IdP Sync Groups on Login on	IdP Sync Groups on Login off
Group Sync Membership on	Group membership for the specific group is reflected in IdP.	Group membership for the specific group is not reflected in IdP.
Group Sync Membership off	Group membership for the specific group is not reflected in IdP.	Group membership for the specific group is not reflected in IdP.

In other words, if Sync Groups on Login is off at the IdP level, then no groups are getting synced regardless of what the setting for Sync Membership is. But if Sync Groups on Login is turned on at the IDP level, then you have the option to override it for certain groups that you explicitly leave off.

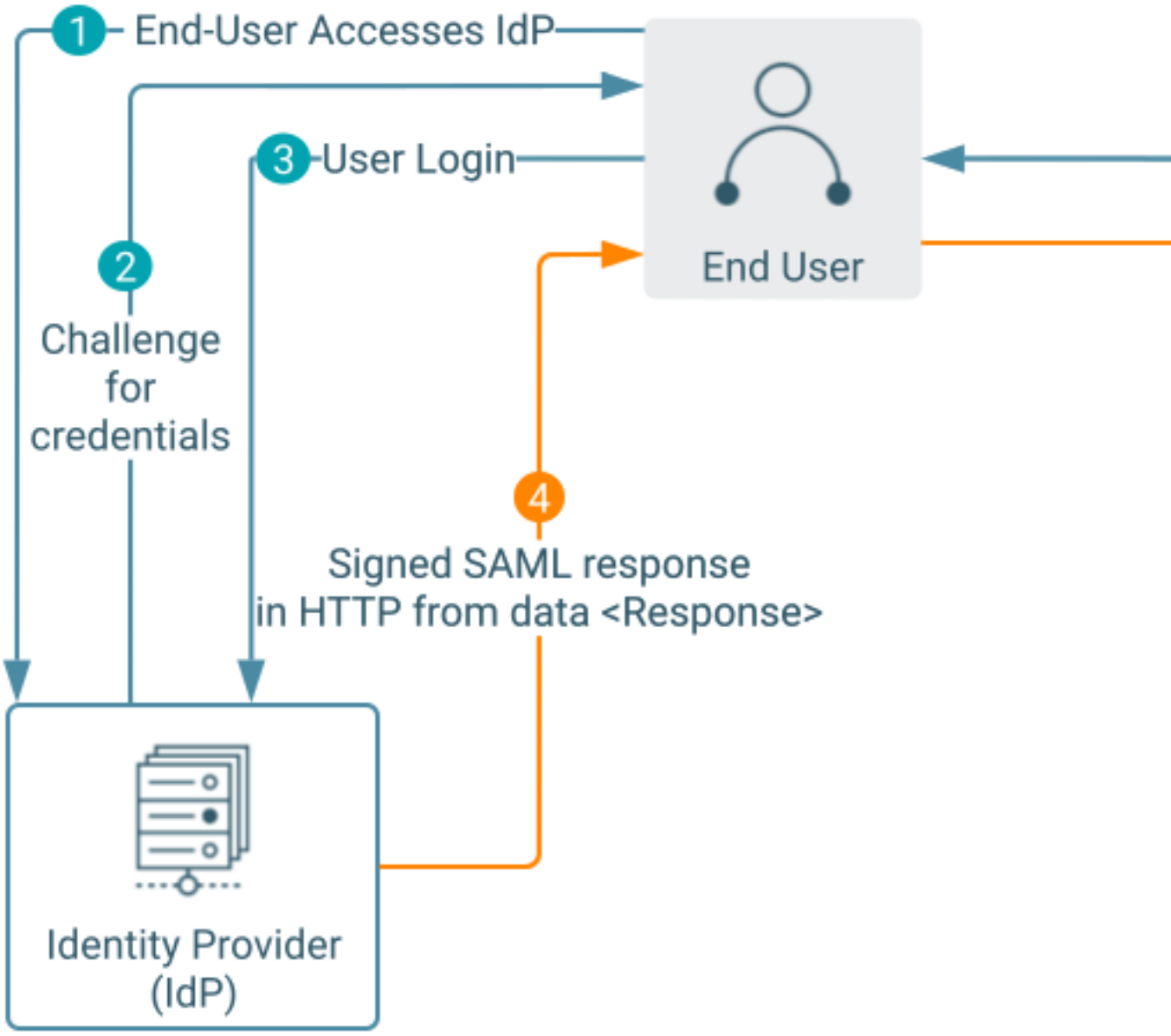
Configuring identity providers with SAML

An account administrator or PowerUser must onboard users by setting up identity federation with Cloudera.

If your organization uses an enterprise identity provider (IdP) that is compliant with Security Assertion Markup Language (SAML), you must set up identity federation with Cloudera. Identity federation allows users within your organization to log in to Cloudera through the authentication system in your organization without registering with Cloudera or creating a Cloudera account.

The following diagram illustrates how identity federation works with Cloudera:

SAML IdP SSO flow



Note:

As shown in the diagram, there is no network communication required between Cloudera and customer IdP, so there is no need to create firewall rules.

Cloudera supports the following:

- Cloudera supports the SAML 2.0 standard. You can set up any identity provider for Cloudera that uses SAML 2.0.

Setting up an identity provider for Cloudera involves the following steps:

1. The IdP administrator in your organization generates the SAML metadata that describes your enterprise IdP.
2. The Cloudera administrator sets up the identity provider in Cloudera data platform.
3. The IdP administrator configures the enterprise IdP in your organization to work with Cloudera as a service provider.

Important: SAML login may fail when using an Incognito or Private browser window if cookies lack the required properties: Secure: true, HttpOnly: true, and SameSite: None.

During the SAML authentication process, an incorrectly parameterized cookie caused the browser to remove it during redirection to the IdP. As a result, the Cloudera Control Plane could not complete the login upon return.

The cookie configuration has been corrected, and SAML login now works as expected in Incognito/Private browser sessions.

Note: An endless redirect loop between the Cloudera Control Plane and the IdP during SAML login can occur if the email attribute is not mapped, or is mapped incorrectly, in the IdP configuration.

The Cloudera Control Plane requires the email attribute to be present for successful authentication. If it is missing, the login fails and enters a redirect loop.

The behavior is fixed and a user-friendly error message is displayed instead of the redirect loop.

Generating the identity provider metadata

Use your enterprise IdP user interface to generate the identity provider SAML metadata file.

Cloudera has the following requirements for the identity provider SAML metadata file:

- The file must be a valid XML file.
- The metadata must include at least one IDPSSOdescriptor element.
- The metadata must contain information about at least one valid x.509 certificate that can be used to verify signed assertions.

The following XML file example displays the elements to include in the identity provider SAML metadata file:

```
<?xml version="1.0" encoding="UTF-8"?>
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="
http://www.w3.org/2000/09/xmldsig#" xmlns:saml="urn:oasis:names:tc:SAML:2.0:
assertion" ID="I160d976643886752" entityID="https://portal.domain.gov/cloude
raDataServices">
   <ds:Signature>
      <ds:SignedInfo>
         <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xm
l-exc-c14n#" />
         <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rs
a-sha1" />
         <ds:Reference URI="#I160d976643886752">
            <ds:Transforms>
               <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#en
veloped-signature" />
               <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" />
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig
#sha1" />
            <ds:DigestValue>SomeDigestValue</ds:DigestValue>
         </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>SomeSignatureValue</ds:SignatureValue>
      <ds:KeyInfo>
         <ds:X509Data>
            <ds:X509Certificate>MyIDPCustomCertificate</ds:X509Certificate>
         </ds:X509Data>
      </ds:KeyInfo>
   </ds:Signature>
   <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0
:protocol">
      <KeyDescriptor>
```

```
         <ds:KeyInfo>
            <ds:X509Data>
               <ds:X509Certificate>MyIDPCustomCertificate</ds:X509Certific
ate>
            </ds:X509Data>
         </ds:KeyInfo>
      </KeyDescriptor>
      <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:H
TTP-POST" Location="https://portal.domain.gov/saml/idp/profile/post/sls" Res
ponseLocation="https://portal.domain.gov/saml/idp/profile/post/slr" />
      <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:
HTTP-Redirect" Location="https://portal.domain.gov/saml/idp/profile/redirect
/sls" ResponseLocation="https://portal.domain.gov/saml/idp/profile/redirect/
slr" />
      <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</Na
meIDFormat>
      <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTT
P-POST" Location="https://portal.domain.gov/saml/idp/profile/redirectorpost/
sso" />
      <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTT
P-Redirect" Location="https://portal.domain.gov/saml/idp/profile/redirectorp
ost/sso" />
      <saml:Attribute Name="urn:oid:0.9.2342.19200300.100.1.3" NameFormat="u
rn:oasis:names:tc:SAML:2.0:attrname-format:unspecified" />
      <saml:Attribute Name="urn:oid:1.3.6.1.4.1.5923.1.5.1.1" NameFormat=
"urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified" />
      <saml:Attribute Name="urn:oid:2.5.4.42" NameFormat="urn:oasis:names:t
c:SAML:2.0:attrname-format:unspecified" />
      <saml:Attribute Name="urn:oid:2.5.4.4" NameFormat="urn:oasis:names:
tc:SAML:2.0:attrname-format:unspecified" />
   </IDPSSODescriptor>
</EntityDescriptor>
```

Setting up the identity provider in Cloudera

In Cloudera, you must create an identity provider to capture the SAML metadata and connection information for your enterprise IdP. To create an identity provider in Cloudera, you must be a Cloudera account administrator or have the PowerUser role.

About this task

Note:

There are certain group names that are reserved and therefore cannot be synchronized to Cloudera. See, Reserved group names.

Required role: Account administrator or PowerUser

Note: If Cloudera Data Engineering is installed and you plan to enable SAML authentication, ensure the service is upgraded using LDAP first. Once the upgrade is successfully completed, you can proceed to enable SAML.

Procedure

1. Sign in to the Cloudera console.
2. From the Cloudera home page, click Cloudera Management Console.
3. In the Cloudera Management Console home page, navigate to Administration and select the Authentication tab.
4. Configure the following settings for SAML:
   - Cloudera on premises requires the SAML assertions to be signed by the Identity Provider.
   - In IDP Metadata, select File Upload to upload a file that contains the identity provider SAML metadata or select Direct Input to paste the identity provider SAML metadata directly.

- To synchronize the groups, select the Sync Groups on Login option.

5. Follow below steps for Signing of SAML assertion configurations.



Note: AuthnRequest will only be signed if the signing key is set and Identity provider's metadata XML has WantAuthnRequestsSigned=true.

Setting configurations for signing and verificaton of SAML AuthnRequests are:

a. Private key for signing SAML AuthnRequest:

This is a private key that Cloudera on premises uses to sign AuthnRequest. It is optional. If you set the signing key then you must set the corresponding "current" certificate for signature verification. The Private key must be in PEM format. You can set the key by directly pasting PEM through Direct Input or by uploading PEM file through File Upload.

b. Current certificate for signature verification:

The certificate used by identity provider to verify the authenticity of the signed AuthnRequests generated by Cloudera on premises. It must be set when the Private key for signing is set, otherwise optional. It must be in PEM format. You can set the certificate by directly pasting PEM through Direct Input or by uploading PEM file through File Upload. This certificate is made available through Cloudera SAML Service Provider Metadata. You must upload the latest Service Provider metadata to your Identity Provider, so that Identity Provider can use this certificate to verify signed AuthnRequests generated by Cloudera on premises.

c. Next certificate for signature verification:

It is used during the key/certificate rotation. It is optional. It must be in PEM format. You can set the certificate by directly pasting PEM through Direct Input or by uploading PEM file through File Upload.

Once these configurations are saved, the "current" and "next" signature verification certificates can be accessed through the Cloudera SAML Service Provider Metadata XML, which will be available after saving the Authentication settings.

These signing configurations can also be configured through the CDP CLI command:

```
cdp iam set-saml-authn-request-signing-key --saml-provider
--authn-request-signing-key <pem-value>
--current-authn-request-verification-certificate <pem-value>
--next-authn-request-verification-certificate <pem-value>
```

Follow the steps to Remove or Reset signing configurations.

Follow the steps to rotate the SAML Authentication Request signing key rotation on page 18.

6. Encryption and decryption of SAML assertion configurations are:

a. Current Private key for decrypting SAML assertions: This is a private key that Cloudera on premises uses to decrypt encrypted SAML assertions and response. It is optional. If you set a decryption key then you must set the corresponding encryption certificate as well. The key must be in PEM format. You can set the decryption key by directly pasting PEM through Direct Input or by uploading PEM file through File Upload.

b. Next private key for decrypting SAML assertions:

It is used during the key/certificate rotation. It is optional. It must be in PEM format. You can set the key by directly pasting PEM through Direct Input or by uploading PEM file through File Upload.

c. Certificate for encrypting SAML responses:

The certificate used by identity provider to encrypt the SAML assertion sent to Cloudera on premises. It must be set when the "current" decryption key is set, otherwise optional. It must be in PEM format. You can set the certificate by directly pasting PEM through Direct Input or by uploading PEM file through File Upload. This certificate is made available through Cloudera SAML Service Provider Metadata after these configurations are saved.

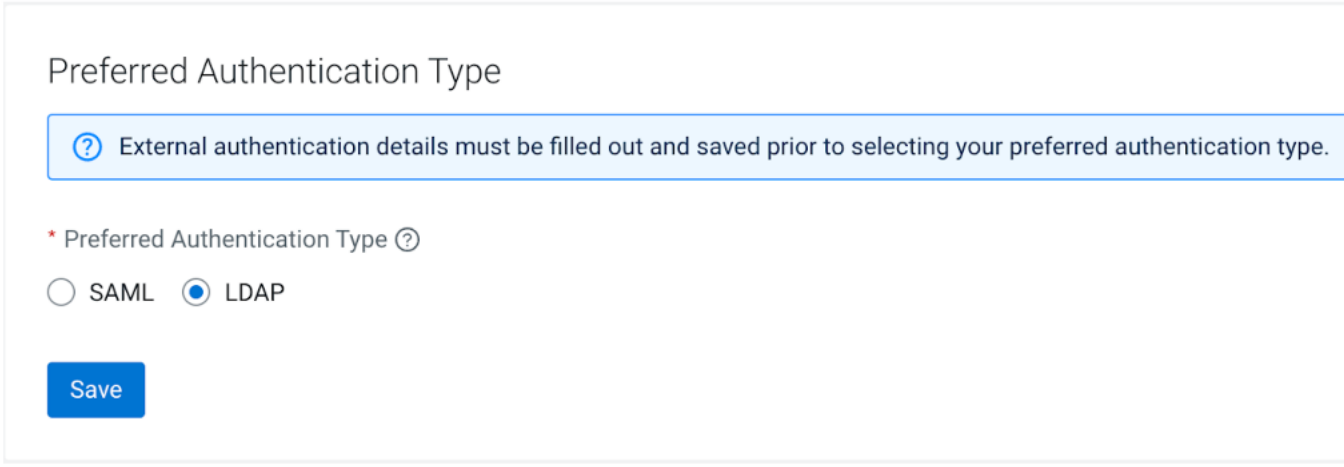
Encryption and decryption configurations can also be set through CDP CLI command:

```
cdp iam set-saml-response-decryption-key --saml-provider
--saml-response-encryption-certificate <pem-value>
--current-saml-response-decryption-key <pem-value>
--next-saml-response-decryption-key <pem-value>
```

d. Follow the steps to Remove or Reset encrypting and decrypting configurations.

Follow the steps to understand the Decryption Key and Encryption Certificate rotation on page 18.

7. If your LDAP is not configured, please ensure you fill in your LDAP configurations as they are required by Cloudera Data Services on premises for workload authorization.
8. Click Update Authentication Settings. If the signing and encryption/decryption configurations are set, the input fields will show a Sensitive value set message.
9. To set up SAML as the preferred identity provider, go to the Preferred Authentication Type section, select SAML and click Save. If you are switching your preferred authentication type from LDAP to SAML OR SAML to LDAP, ensure you migrate your users. For more information see, Migrating users from another preferred identity provider on page 21



Note: If SAML configuration is incorrect, customers can still log in as a local admin using the following URL format: https://[***MANAGEMENT CONSOLE URL***]/authenticate/login/local (Example: https://console-cdp.apps.domain.com/authenticate/login/local). This allows them to modify SAML settings as needed.

Results

Once you update your authentication settings, the Authentication Page will have your new identity provider (IdP) information. It will reflect your previously saved configurations and also provide the Cloudera SAML Service Provider Metadata with the updated signing and encryption-decryption configurations. This will be used to configure your IdP.

Note: Cloudera Data Services on premises only supports a single IDP Provider, the IDP Provider name cannot be configured, and is defaulted to cm-saml.

These are the properties for your SAML identity provider:

Property	Description
SAML Identity Provider Metadata	The identity provider SAML metadata for your enterprise IdP that you provided when you created the Cloudera identity provider.

Property	Description
Sync Groups on Login	Indicates whether Cloudera synchronizes a user's group membership in Cloudera with the user's group membership in your enterprise IdP when a user logs in. For more information about user group synchronization, see Group Membership Synchronization.
Generate workload username by email	You can optionally check this if you want the workload username to be generated based on the email instead of the default.
Cloudera SAML Service Provider Metadata	The Cloudera SAML service provider metadata to configure your enterprise IdP.

Removing or resetting the signing or encryption/decryption configurations

If you enter a value for the signing or encryption/decryption configurations and later realize it is incorrect, you can click the Reset button next to the specific configuration to revert the field to its previous value, ensuring no changes are submitted.

About this task

To delete an existing value, you may either enter an empty string or click the Remove button. Clicking Remove disables the field, and upon submission, the corresponding configuration will be deleted. If the user decides not to remove the value before submitting, clicking Reset will restore the field to its previous value, preventing any updates for that field.

SAML Authentication Request signing key rotation

Here are the steps you should follow to avoid any down time during the key and certificate rotation:

About this task

Follow the steps below to avoid any down time during the key and certificate rotation:

Procedure

1. Generate a new Private Key for signing and a corresponding verification certificate.
2. Upload this new verification certificate as the Next certificate for signature verification in the Cloudera Management Console.
3. Click Update Authentication Settings.
4. Get the latest SAML Service Provider Metadata from the Cloudera Management Console. The latest service provider metadata must now have the both “current” and “next” certificates as the "signing" cert.
5. Upload this service provider metadata to your actual Identity Provider, so that Identity Provider now has both the old and new verification certificates. Including both certificates in the SP metadata allows a smooth key rotation without downtime, ensuring that authentication requests signed with either the current or new key can be validated during the transition period.
6. In Cloudera Management Console:
   a. Upload the new Private key as the Private key for signing SAML AuthnRequest field.
   b. Upload the new verification certificate as the Current certificate for signature verification
   c. Remove the Next certificate for signature verification certificate by clicking the Remove button or by entering an empty string.
7. Click Update Authentication Settings.
8. Get the latest SAML Service Provider Metadata from Cloudera Management Console. This metadata should now have only one “signing” certificate with the latest value.
9. Upload this updated service provider metadata to your Identity Provider to complete the key rotation process.

Decryption Key and Encryption Certificate rotation

Here are the steps you should follow to avoid any down time during the key and certificate rotation:

Procedure

1. Generate a new Private Key for decrypting SAML assertion and a corresponding certificate for encrypting assertion.
2. Upload this new private key as the Next private key for decrypting SAML assertions field in the Cloudera Management Console.
3. Upload the certificate as the Certificate for Encrypting SAML Responses field in the Cloudera Management Console.
4. Click Update Authentication Settings.
5. Get the latest SAML Service Provider Metadata from the Cloudera Management Console. This should now have the new “encryption” certificate.
6. Upload this service provider metadata to your actual Identity Provider, so that Identity Provider now starts encrypting SAML assertions with the new certificate.
7. Once the IdP begins using the new encryption certificate:
   a. Upload the new Private key in the Cloudera Management Console as the Current Private Key for Decrypting SAML Assertions.
   b. Remove the Next Private Key for Decrypting SAML Assertions by clicking the Remove button next to it or by entering an empty string.
   c. Click Update Authentication Settings to finalize the key rotation.

Configuring your enterprise IdP to work with Cloudera as a service provider

Cloudera provides a service provider SAML metadata file that describes the information that Cloudera requires to enable users to log in to Cloudera through your enterprise IdP.

You can get the Cloudera SAML metadata XML from the Administration page of your Cloudera Management Console under the Authentication tab. Look for Cloudera SAML Service Provider Metadata that contains the XML metadata.

The Cloudera SAML metadata file includes the following information:

Information	Attribute	Description
Name ID formats that Cloudera supports	NameIDFormat	The metadata includes multiple name ID formats. Use one of the formats in the list for the user ID. Cloudera supports any type of name ID format other than transient. Cloudera requires that you use name ID formats that are globally unique within your identity provider. The name ID format should also be stable over time. Cloudera does not recommend using email addresses because, although they can be unique, they are typically not stable over time. The value of NameID is case-sensitive.  **Note:** Do not use email addresses as NameID.
Cloudera SSO URL	Location	It should be the same as the "Location" value of the "<AssertionConsumerService>" in the Cloudera SAML Service Provider metadata. It has a fixed format. For Example:https://console-company.apps.domain.com/consoleauth/saml?samlProviderId=68e940b4-23b2-469b-a3f5-00a292d89f43 This attribute is required.

Information	Attribute	Description
Endpoint for binding	Binding	Use the following URN as the endpoint that your enterprise IdP must bind to: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST This attribute is required.
User email address	RequestedAttribute: mail	Set the email address attribute to the following URN: urn:oid:0.9.2342.19200300.100.1.3 This attribute is required.
(Optional) List of groups that the user is a member of	RequestedAttribute: groups	Set the group list attribute to the following URN: urn:oid:1.3.6.1.4.1.5923.1.5.1.1 This attribute is optional.
(Optional) User first name	RequestedAttribute: firstName	Set the user first name attribute to the following URN: urn:oid:2.5.4.42 This attribute is optional.
(Optional) User last name	RequestedAttribute: lastName	Set the user last name attribute to the following URN: urn:oid:2.5.4.4 This attribute is optional.

If your enterprise IdP allows it, you can upload the Cloudera SAML metadata file to your enterprise IdP. Otherwise, use your enterprise IdP user interface to set up Cloudera as a service provider.

Updating an identity provider

This topic provides details on updating an IdP.

About this task

You might want to update the Cloudera identity provider to change the group synchronization option or if you want to update the list of x.509 certificates in the provider metadata.

Required role: Account administrator or PowerUser

Procedure

1. Sign in to the Cloudera console.
2. From the Cloudera home page, click Cloudera Management Console.
3. On the Cloudera Management Console, select Administration -> Authentication tab.
4. Find the section containing the SAML identity provider settings.
5. On the Identity Provider window:
   - You can change the Sync Groups on Login option.
   - You can edit the SAML Identity Provider Metadata.
   - You can check the Generate workload username by email option to have the workload username is generated based on the email instead of the default.
6. Verify the updates and click Update Authentication Settings.

Migrating users from another preferred identity provider

For additional security, Cloudera on premises treats users with the same username from different identity providers as different users, even if they are actually the same users from the same backend user storage. This is to prevent unintended access to users from different identity providers that happen to share the same username. Therefore, for Cloudera on premises installations that have been using LDAP as the default authentication method, if you want to change your preferred identity provider type to SAML, and the LDAP and SAML identity providers have the same underlying database of users, ensure that you also migrate the affected users.

About this task

Required role: Account administrator or PowerUser

Note: If you do not migrate your users from the LDAP identity provider to the SAML identity provider, a new user will be created in the Cloudera Management Console (on premises) upon login.

In previous versions (1.5.4), this new user was created with an incremental numeric suffix appended to their workload username (for example, cdpuser_0). In the current behavior (Pre and Post 1.5.4), the new user is created with the same workload username as the original user. This results in duplicate users with identical workload usernames, which can lead to inconsistent states. Therefore, migrating your users from LDAP to SAML is required to avoid duplication and maintain data consistency.

Issues caused by not migrating users:

- The new user will not inherit role or group permissions from the previous LDAP user.
- When running data services workloads with this user, Ranger policy-based authorization will fail because your LDAP/AD server is not aware of the new suffix.

Before you begin

Ensure you have:

- cdp-cli client version 0.9.128 or later
- Admin user access key and private key
- The old and new identity providers share the same underlying database of users
- The same users are configured with identical userId attributes across both identity providers.
- If those conditions are not met, then unauthorized access may be granted if a new user shares the same username as an existing user post migration.

Procedure

1. Configure SAML Identity Provider. Follow the instructions in Configuring your enterprise IdP to work with Cloudera as a service provider on page 19 with SAML as your preferred authentication type.
2. Delete duplicate users. If users have already logged in through SAML and were previously logged in through LDAP, delete the duplicate SAML users:
   a. Log in to the CDP Private Cloud Management Console as a local admin using the following URL format: https://[***MANAGEMENT CONSOLE URL***]/authenticate/login/local (Example: https://console-cdp.apps.domain.com/authenticate/login/local).
   b. Navigate to User Management > Users .
   c. Locate users with a _+numeric suffix, click the three-dot menu on the right, and delete these users.

   Note: Failing to delete these users will cause the migration to fail.
3. Migrate users using cdp-cli.
   a. Download and configure the cdp-cli client (version 0.9.128 or later, include the doc for users to set up cdp-cli: Setting up CDP-CLI). For information on the cdp-cli official doc, see CDP-CLI User Guide.

b. Run the following command to migrate users from the LDAP identity provider to the SAML identity provider:

```
cdpcli --endpoint-url <Management_Console_URL> iam migrate-users-to-iden
tity-provider --original-provider-name cm-ldap --new-provider-name cm-sa
ml
```

Note: The output will display the number of users migrated.

Note: You do not need to change original-provider-name (cm-ldap) and the new-provider-name (cm-saml) as they are pre-configured. For customers switching from SAML to LDAP, swap the original-provider-name and new-provider-name values in the command.

Understanding Cloudera on premises user accounts

User accounts identify the users who can access services, applications, and components in the Cloudera.

Roles assigned to a user account determine the actions that the user can perform in Cloudera.

There are three types of user accounts in Cloudera on premises:

- Cloudera Account administrator
- Cloudera user
- Cloudera machine user

Cloudera account administrator

Cloudera designates a default user account as a Cloudera account administrator during the initial setup.

A Cloudera account administrator has administrator privileges in Cloudera. The Cloudera account administrator user account cannot be managed within Cloudera. The default username and password for Cloudera account administrator is admin/admin. You should consider changing the default password for security purposes.

As an account administrator, you have all the privileges in Cloudera and can perform any task. You can set up users and assign roles, services, and environments to users in Cloudera according to the tasks that they need to perform. You can set up another user as a Cloudera administrator by assigning the PowerUser role to the user. However, you cannot set up another user as a Cloudera account administrator.

Cloudera user

To perform tasks using Cloudera and its services, you must be a Cloudera user with the required roles and resources assigned.

Cloudera allows users within your organization to log in to Cloudera through the authentication system in your organization without registering with Cloudera or creating a Cloudera account. During the initial process of configuring the environment, the account administrator must set up identity federation and thus automatically add users.

When a Cloudera user who is not an account administrator logs in to Cloudera for the first time, the user has limited privileges. A Cloudera administrator must assign the appropriate roles to the user after the initial user login.

The Cloudera account administrator can revoke permissions for a Cloudera user account. When you revoke permissions for a user, ensure that you remove all the roles that grant the permissions that you want to revoke.

To revoke all permissions granted to a user, complete the following steps:

- Remove all roles assigned to the user.

- Delete any access key created for the user.

A user who has a valid account in Cloudera but is not assigned any role can perform a limited number of tasks. A user who logs in to the Cloudera console without an assigned role or environment can perform only the following task:

- View the Cloudera documentation.

Cloudera machine user

A machine user account provides programmatic access to Cloudera. Create a machine user account if you have an application that needs to access the Cloudera services with Cloudera Management Console APIs.

You can define the machine user account in your application to create and manage clusters and run jobs in Cloudera using the CLI or API commands.

You can create and manage a machine user account within Cloudera. You must assign an API access key to a machine user account to enable it to access the Cloudera service. You must assign roles to a machine user account to authorize it to perform tasks in Cloudera.

A machine user account does not have an associated Cloudera user account. You cannot use a machine user to log in to the Cloudera console.

Machine users created in the control plane are not automatically created in the customer LDAP. Therefore you cannot use machine users to access data in the base cluster.

Use the following guidelines when you manage user accounts in Cloudera:

- When you create a machine user account, you assign roles and environments to the machine user account in the same way that you assign roles and environments to other user accounts.
- When you revoke permissions for a machine user, ensure that you remove all the roles that grant the permissions that you want to revoke. To revoke all permissions granted to a machine user account, complete the following steps:
  - Remove all roles assigned to the machine user.
  - Delete any access key created for the machine user.
- You can delete a machine user account in Cloudera. You can delete the machine user account on the Cloudera console.

Working with machine users

For programmatic access to Cloudera on premises, you must create a machine user. After creating the user, you must also generate an API access key.

Creating a machine user

You must create a machine user for programmatic access to Cloudera on premises.

Steps

Cloudera Management Console UI

1. Sign in to the Cloudera console.
2. Click Cloudera Management Console.
3. Select User Management > Users.
4. From the Actions menu, select Create Machine User.
5. Provide a name and click Create.

CLI

1. Use the following command to create the machine user:

```
cdp iam create-machine-user  \
--machine-user-name MACHINE_USER_NAME
```

2. Generate an API access key for your machine user by using the following command:

```
cdp iam create-machine-user-access-key \
    --machine-user-name MACHINE_USER_NAME
```

What to do next: You must generate an access key for the machine user.

Generating an API access key

A Cloudera user account (a user or a machine user) must have API access credentials to access Cloudera services.

About this task

When you use this method to generate an access key and then manually configure the access key in the ~/.cdp/credentials, the access credentials are permanent until they are removed from the ~/.cdp/credentials file. If you prefer that the API access key is shorter-lived, refer to the topic Logging into the CDP CLI/SDK, which describes a method of logging into the CLI/SDK through any SAML-compliant identity provider.

Required roles: Users who have the IAMUser role can generate an access key from their own account page. As a Cloudera administrator or PowerUser, you can generate an access key for a user account that does not have the IAMU ser role.

To generate an API access key using the CLI, refer to the following commands on the IAM documentation page:

- create-user-access-key: for generating access key for users
- create-machine-user-access-key: for generating access key for machine users

To generate an API access key using the Cloudera Management Console:

Procedure

1. Sign in to the CDP console.
2. Click on your user name in the bottom left corner and then select Profile.
3. On the user profile page that appears, click Generate Access Key.
4. On the **Generate Access Key** pop-up window, click Generate Access Key.

   Cloudera creates the key and displays the information on the screen.
5. Copy the access key and private key to a text file and send it to the Cloudera user who requires it.

   The private key is a very long string of characters. Make sure that you copy the full string. You can optionally download the credentials file containing the access key information by clicking Download Credentials File.

   Note: The CDP console displays the API access key immediately after you create it. You must copy or download the access key ID and private key information when it is displayed. Do not exit the console without copying the private key. After you exit the console, there is no other way to view or copy the private key.
6. Click Close to exit the access key window.

Results

Once you have generated the access key, you can configure CDP CLI, SDK, or other utilities that require it.

Deleting a machine user

Deleting a machine user also removes the resources associated with the user.

Steps

Cloudera Management Console

1. Sign in to the Cloudera console.
2. From the Cloudera home page, click Cloudera Management Console.
3. Click User Management.

   The Users page displays the list of all the available Cloudera users.
4. Search for the machine user that you want to delete and click the vertical ellipsis (three dots) against that user.
5. Click Delete Machine User and then OK on the confirmation screen.

CLI

Use the following command to delete the machine user:

```
cdp iam delete-machine-user \
--machine-user-name <value>
```



Note: For a detailed description of the command properties, use cdp --help:

```
cdp iam delete-machine-user --help
```

Understanding roles

To access resources and perform tasks in Cloudera, each user requires permissions. As a Cloudera administrator, you can assign a role to a user to give the user permission to perform the tasks.

A policy defines the permissions associated with a role. It consists of policy statements that grant permissions to resources. The policies attached to a role determine the operations that the role allows the user to perform. When users attempt to perform operations that are not permitted in their assigned role, they get a permission denied error message.

Cloudera provides the following types of roles:

- Account-level roles: These are global roles not associated with any specific resource. Cloudera has certain predefined account-level roles that you can assign to users.
- Resource roles: These are resource-specific roles that provide permissions to perform tasks on a specific resource, such as a Cloudera Data Warehouse virtual warehouse.

The scope of predefined roles and resource roles can vary. For example, a role might grant view access only to Cloudera AI clusters but not Cloudera Data Warehouse clusters. You might need to assign multiple roles to ensure that a user can perform all the required tasks in Cloudera.

Account-level roles

An account-level role grants permissions to perform tasks in Cloudera that are not associated with a specific resource. You explicitly assign a role to a user account.

The predefined account-level roles available in Cloudera that you can assign to Cloudera users, machine users, and groups are as follows:

Table 1: Cloudera roles

Cloudera role	Description
PowerUser	Grants permission to perform all tasks on all resources.  **Note:** Only a Cloudera account administrator or a user with the PowerUser role can create environments or assign roles to a user. Only a Cloudera account administrator or a user with the PowerUser or EnvironmentAdmin resource role can download and update the Kubernetes configuration file, and view the compute cluster information.
IamUser	Grants permission to create access keys for the user, view assigned roles, and view all users in the account.
IamViewer	Grants permission to view assigned roles and view all users in the account.
DiagnosticsCollector	Grants Cloudera user the permission to create, collect, and manage bundles, including adding redaction rules.



Note:

Only a Cloudera account administrator or a user with the PowerUser role can create environments, create and manage data lakes, and assign roles to a user.

Resource roles

A resource role grants permission to access and perform tasks using specific resources.

When you assign a resource role, you must specify the resource on which to grant the resource role permissions. For example, you can assign a user a resource role that grants permission on a virtual warehouse. The user assigned the resource role can access and perform tasks on only the resources associated with the virtual warehouse.

The resource role determines the tasks that the user can perform using the resources associated with the role. For example, the MLUser resource role assigned to a user allows the user to view the Cloudera AI Workbench provisioned within an environment.

You cannot modify the pre-defined resource roles or the policies associated with the pre-defined resource roles.

The pre-defined resource roles available in Cloudera that you can assign to Cloudera users, machine users, and groups are as follows:

- ### Table 2: Resource roles

Resource role	Description
DWAdmin	Grants a Cloudera user/group the ability to activate/terminate or launch/stop/update services in Virtual Warehouses.
DWUser	Grants a Cloudera user/group the ability to view and use Cloudera Data Warehouse clusters within a given Cloudera environment.
MLAdmin	Grants a Cloudera user/group the ability to create and delete Cloudera Machine Learning workspaces within a given Cloudera environment. MLAdmins also have Administrator level access to all the workspaces provisioned within this environment. They can run workloads, monitor, and manage all user activity on these workspaces.
MLUser	Grants a Cloudera user/group the ability to view Cloudera Machine Learning workspaces provisioned within a given Cloudera environment. MLUsers will also be able to run workloads on all the workspaces provisioned within this environment.

Resource role	Description
DEAdmin	Grants a Cloudera user/group the permissions to create, delete, and administer Data Engineering services for a given Cloudera environment.
DEUser	Grants a Cloudera user/group the permissions to list and use Data Engineering services for a given Cloudera environment.

Assigning account-level roles to users

Assign account-level roles to a Cloudera user to manage the tasks that the user can perform in Cloudera. You can assign multiple roles to users or machine users to provide them with the permissions they need to perform their required tasks.

Steps

Cloudera Management Console

1. Sign in to the Cloudera console.
2. Click Cloudera Management Console.
3. Click User Management.

   The Users page displays the list of all Cloudera users.
4. Click the name of the user to whom you want to assign a role.

   The user details page displays information about the user.
5. Click the Roles tab.
6. Click Update Roles.
7. On the Update Roles window, select the roles you want to assign to the user.

   To remove a role from the user account, clear the selected role.
8. Click Update.

   The roles that you select displays in the list of roles assigned to the user.

   To remove a role from a user account, click check box next to the assigned role that you want to remove. Click Update to confirm that you want to revoke the role permissions.

CLI

You can use the following command to assign a role to a user or a machine user:

```
cdp iam assign-user-role \
--user-name <value> \
--role <value>
```

To remove a role from a user or a machine user:

```
cdp iam unassign-user-role \
--user-name <value> \
--role <value>
```

To get a list of the roles assigned to a group:

```
cdp iam list-user-assigned-roles \
--user-name <value>
```

```
cdp iam list-machine-user-assigned-roles \
--machine-user-name <value>
```

Assigning resources to users

Assign a user or a machine user a resource role on the scope of a Cloudera environment to grant the user access to the resources they need to perform their required tasks.

Steps

Cloudera Management Console

1. Sign in to the Cloudera console.
2. Click Cloudera Management Console.
3. Click Environments.
4. In the list of environments that appear, select your environment by clicking on it.

   The Environment Clusters page appears.
5. Click Actions.
6. Click Manage Access in the dropdown list.
7. In the Access tab, enter the name of the user in the Select group or user text box.

   The Update Resource Roles window appears.
8. Select the required resource role.
9. Click Update Roles.

CLI

You can use the following command to assign a resource role to a user or a machine user:

```
cdp iam assign-user-resource-role \
--user-name <value> \
--resource-role-crn <value> \
--resource-crn <value>
```

```
cdp iam assign-machine-user-resource-role \
--machine-user-name <value> \
--resource-role-crn <value> \
--resource-crn <value>
```



Note: The resource-role-crn parameter requires the CRN of the resource role you want to assign to the user. The resource-crn parameter requires the CRN of the resource on which you want to grant the resource role permissions.

To remove a resource role from a user or a machine user:

```
cdp iam unassign-user-resource-role \
--user-name <value> \
--resource-role-crn <value> \
--resource-crn <value>
```

```
cdp iam unassign-machine-user-resource-role \
--machine-user-name <value> \
--resource-role-crn <value> \
--resource-crn <value>
```

To get a list of the resource roles assigned to a user or a machine user:

```
cdp iam list-user-assigned-resource-role \
--user-name <value>
```

```
cdp iam list-machine-user-assigned-resource-role \
```

```
--machine-user-name <value>
```

Enabling admin and user access to environments

A user with PowerUser role enables admin and user access to environments in a Cloudera on premises deployment.

1. A Cloudera user with PowerUser role creates an environment.
2. The PowerUser assigns the EnvironmentAdmin role to the intended user. For instructions, refer to Assigning account-level roles to users on page 27.
3. Additional admin resource roles enumerated in Understanding roles on page 25 should be assigned if admin access to specific Cloudera services is needed. For example, for admin access to the Data Warehouse service, assign DWAdmin role. For instructions, refer to Assigning resources to users on page 28.
4. The PowerUser assigns the EnvironmentUser to the intended users. For instructions, refer to Assigning account-level roles to users on page 27.
5. Additional user resource roles enumerated in Understanding roles on page 25 should be assigned if admin access to specific Cloudera services is needed. For example, for user access to the Cloudera Data Warehouse service, assign DWUser role. For instructions, refer to Assigning resources to users on page 28.

Understanding Cloudera groups

A Cloudera group is a collection of user accounts that have the same roles and resource roles. A group can include Cloudera user accounts and machine user accounts. A group cannot include other groups. All users in a group inherit the roles and resource roles assigned to the group.

As a Cloudera administrator, you can create a group and manage the group membership. You can also manage the roles and resources assigned to the group. If you are not a Cloudera administrator, you can add users to and remove users from a group if you have the PowerUser role.

When you create a group, you do not automatically become a member of the group. To become a member of the group, you must add your user account to the group.

You can use groups to manage user access more efficiently. If multiple users require the same roles, you can create a group, add the user accounts to the group, and assign the required roles to the group. All user accounts in the group are assigned the roles assigned to the group.



Note: You cannot delete a group that already has members, roles, or resource roles assigned. You must first remove all the assignments for the group and only then delete it.

Creating a group

You can create Cloudera groups based on the tasks performed by Cloudera users in your organization.

Before you begin: To create a Cloudera group and to manage the users, roles, and resources in the group, you must have the PowerUser role.

Steps

Cloudera Management Console

1. Sign in to the Cloudera console.
2. From the Cloudera home page, click Cloudera Management Console.
3. In the User Management section of the side navigation panel, click Groups.The Groups page displays the list of all Cloudera groups.
4. Click Create Group.

5. On the Create Group window, enter the name of the group to create.

   Note: You must consider the following when naming a group:

   - The group name must be unique and not contain any of the reserved group names.
   - The group name can be up to 64 characters and can include only alphanumeric characters, hyphens (-), and underscores (_). The first character in the name must be an alphabetic character or underscore.
   - The group name is not case sensitive. For example, the group name AAa is equivalent to the group name aaa.
   - Depending on your IdP setup in Cloudera, you may be able to manipulate the Sync Membership option. To learn more about this option, refer to Synchronizing group membership.

6. Click Create. Cloudera creates the group and adds it to the list of groups on the particular page.

CLI

You can use the following command to create a group:

```
cdp iam create-group \
--group-name <value>
```

Adding or removing a user from a group

You can add a Cloudera user or a machine user account to a group. You cannot add a group to another group. You can remove a Cloudera user or a machine user account from a group.

All members of the group inherit the roles and resources assigned to the group.

Note: To add a user or remove a user from a group, you must have the PowerUser or the IamGroupAdmin resource role.

Steps

Cloudera Management Console

1. Sign in to the Cloudera console.
2. From the Cloudera home page, click Cloudera Management Console.
3. In the User Management section of the side navigation panel, click Groups.
4. Click the name of the group to which you want to add a user.

   The details page displays information about the group.
5. Click the Members tab.
6. Add or remove users according to your requirements.

   Adding a user to a group:

   - If the group does not have members, click Add Member. Select the name of the user that you want to add to the group.
   - If the group already has a list of members, click in the Add Member dropdown box. Select the name of the user that you want to add to the group.

   Removing a user from a group:

   - **a.** Click Remove from Group next to the user that you want to remove.
     b. Click OK to confirm that you want to remove the user from the group.

CLI

You can use the following command to add a user to a group:

```
cdp iam add-user-to-group \
--group-name <value> \
```

```
--user-id <value>
```

Note: The user-id parameter requires the CRN of the Cloudera user or machine user.

To remove a user from a group:

```
cdp iam remove-user-from-group \
--group-name <value> \
--user-id <value>
```

To add a machine user to a group:

```
cdp iam add-machine-user-to-group \
--group-name <value> \
--user-id <value>
```

To remove a machine user from a group:

```
cdp iam list-groups-for-machine-user \
--machine-user-name <value>
```

To get a list of the users in a group:

```
cdp iam remove-machine-user-from-group \
--group-name <value> \
--machine-user-name <value>
```

```
cdp iam list-group-members \
--group-name <value>
```

To get the list of groups that a user or machine user is a member of:

```
cdp iam list-groups-for-user \
--user-id <value>
```

```
cdp iam list-groups-for-machine-user \
--machine-user-name <value>
```

Assigning account roles to a group

When you assign a role to a group, the role is also assigned to all user and machine user accounts in the group.

Steps

Cloudera Management Console

1. Sign in to the Cloudera console.
2. From the Cloudera home page, click Cloudera Management Console.
3. In the User Management section of the side navigation panel, click Groups.

   The Groups page displays the list of the available Cloudera groups.
4. Click the name of the group to which you want to assign a role.

   The details page displays information about the group.
5. Click the Roles tab.
6. Click Update Roles.
7. On the Update Roles window, select the roles you want to assign to the group.

8. To view the permissions that the role grants to the group, click Policies. To remove a role from the group, clear the selected role.
9. Click Update.

   The roles that you select displays in the list of group roles.

   To remove a role from a group, click Unassign Role next to the role that you want to remove. Click OK to confirm that you want to remove the role permissions from the group.

CLI

You can use the following command to assign a role to a group:

```
cdp iam assign-group-role \
--group-name <value> \
--role <value>
```

To get a list of the roles assigned to a group:

```
cdp iam list-group-assigned-roles \
--group-name <value>
```

Assigning resource roles to a group

When you assign a resource role to a group, the resource role is also assigned to all user and machine user accounts in the group.

Steps

Cloudera Management Console

1. Sign in to the Cloudera console.
2. From the Cloudera home page, click Cloudera Management Console.
3. Click Environments.
4. In the list of environments, select your environment by clicking on it.

   The details page for the selected environment appears.
5. Click Actions.
6. Click Manage Access in the dropdown list.
7. In the Access tab, enter the name of the group in the Select group or user text box.

   The Update Resource Roles window appears.
8. Select the required resource role such as EnvironmentAdmin or EnvironmentUser.
9. Click Update Roles.

CLI

You can use the following command to assign a resource role to a group:

```
cdp iam assign-group-resource-role \
--group-name <value> \
--resource-role-crn <value> \
--resource-crn <value>
```

To remove a resource role from a group:

```
cdp iam unassign-group-resource-role \
--group-name <value> \
--resource-role-crn <value> \
--resource-crn <value>
```

- The resource-role-crn parameter requires the CRN of the resource role you want to assign to the group.
- The resource-crn parameter requires the CRN of the resource on which you want to grant the resource role permissions.

To get a list of the resource roles assigned to a group:

```
cdp iam list-group-assigned-resource-role \
--group-name <value>
```

Assigning a group membership administrator

As a Cloudera administrator, you can create a Cloudera group and manage the users, roles, and resources assigned to the group. You can also assign other users and groups the IamGroupAdmin role to allow them to manage the users in the group.

Assigning a group membership

Note: The IamGroupAdmin role grants a user or group the permission to add users to or remove users from a group. The role does not grant permission to manage roles and resources for the group.

Cloudera Management Console

1. Sign in to the Cloudera console.
2. From the Cloudera home page, click Cloudera Management Console.
3. In the User Management section of the side navigation panel, click Groups.

   The Groups page displays the list of the available Cloudera groups.
4. Click the name of the group to which you want to assign a group membership administrator.

   The details page displays information about the particular group.
5. Click the Admins tab.
6. Click in the Select group or user dropdown box.

   Cloudera displays the list of groups and users to which you can give group membership administrator permissions.
7. Select the name of a group or user.

   The name of the group or user you select displays in the list of group membership administrators.

CLI

You can assign the IamGroupAdmin resource role to users and groups to allow them to manage the users in a specified group.

You can use the following command to assign the IamGroupAdmin role to a user:

```
cdp iam assign-user-resource-role \
--user <value> \
--resource-role-crn <value> \
--resource-crn <value>
```

- The user parameter requires the CRN of the user to whom you want to assign the IamGroupAdmin resource role.
- The resource-role-crn parameter requires the CRN of the IamGroupAdmin role.
- The resource-crn parameter requires the CRN of the group on which the user will have administrator permission.

To assign the IamGroupAdmin role to a group:

```
cdp iam assign-group-resource-role \
--group-name <value>e \
--resource-role-crn <value> \
--resource-crn <value>
```

- The group-name parameter requires the name of the group to which you want to assign the resource role.
- The resource-role-crn parameter requires the CRN of the IamGroupAdmin role.
- The resource-crn parameter requires the CRN of the group on which the group specified in the group-name parameter will have administrator permission.

  For example, to assign the IamGroupAdmin to GroupABC so that GroupABC can manage the users in GroupXYZ, run a command similar to the following command:

```
cdp iam assign-group-resource-role \
--group-name groupABC \
--resource-role-crn crn:cdp:iam:us-west-1:cdp:resourceRole:IamGroupAdmin \
--resource-crn crn:cdp:iam:us-west-1:4e9d74e5-1cad-47d8-b645-7ccf9edbb73
d:group:GroupXYZ/54218ac1-187b-40f7-aadb-5ghm96c35xy4
```

- To assign the users in a group to be the administrators of their own group, set the values of the group-name parameter and the resource-crn parameter to refer to the same group.

Removing a group membership administrator

If required, you can remove a particular user or group as the administrator of a group.

About this task

To remove a group membership administrator, you must have the PowerUser role.

Procedure

1. Sign in to the Cloudera console.
2. From the CDP home page, click Cloudera Management Console.
3. In the User Management section of the side navigation panel, click Groups.

   The Groups page displays the list of the available Cloudera groups.
4. Click the name of the group for which you want to remove a group membership administrator.

   The details page displays information about the particular group.
5. Click the Admins tab.
6. Click Remove Admin next to the user or group that you want to remove as the group administrator.
7. Click OK to confirm that you want to remove the selected user or group as the administrator.

Updating a group

Depending on your IdP setup in Cloudera, you can enable or disable the Sync Membership option for a group.

Before you begin: To manage Cloudera groups, you must have the PowerUser role.

Updating a group

Cloudera Management Console

1. Sign in to the Cloudera console.
2. From the Cloudera home page, click Cloudera Management Console.
3. In the User Management section of the side navigation panel, click Groups.

   The Groups page displays the list of the available Cloudera groups.
4. From the context menu to the right of the desired group, click Update Group.
5. Select or deselect the Sync Membership checkbox.
6. Click Update.

CLI

Depending on your requirement can use either of the following parameters with the cdp iam update-group command to update a group:

```
cdp iam update-group \
--group-name<value> \
--sync-membership-on-user-login
```

OR

```
cdp iam update-group \
--group-name <value> \
--no-sync-membership-on-user-login
```

Removing account roles from a group

When you unassign a role from a group, the role is also unassigned from all user and machine user accounts in the group.

Steps

Cloudera Management Console

1. Sign in to the Cloudera console.
2. From the Cloudera home page, click Cloudera Management Console.
3. In the User Management section of the side navigation panel, click Groups.

   The Groups page displays the list of all Cloudera groups.
4. Click the name of the group from which you want to remove the account role.

   The details page displays information about the group.
5. Click the Roles tab.
6. From the context menu to the right of a role, click Unassign role.
7. Click OK to confirm that you want to remove the role permissions from the group.

CLI

To remove a role from a group:

```
cdp iam unassign-group-role \
--group-name <value> \
--role <value>
```

The role parameter requires the CRN of the Cloudera role.

To get a list of the roles assigned to a group:

```
cdp iam list-group-assigned-roles \
--group-name <value>
```

Deleting a group

You can delete a Cloudera group if you have the PowerUser role.

Steps

Cloudera Management Console

1. Sign in to the Cloudera console.

2. From the Cloudera home page, click Cloudera Management Console.
3. In the User Management section of the side navigation panel, click Groups.
4. From the context menu to the right of the desired group, click Delete Group.
5. Click OK to confirm removal.

   Cloudera removes the group and from the list on the Groups page.

CLI

Use the following command to delete a Cloudera group:

```
cdp iam delete-group \
--group-name <value>
```

Reserved group names

There are certain group names that are reserved and therefore cannot be used in Cloudera. This applies to groups synchronized from your identity provider as well as groups created directly from Cloudera.

If you attempt to synchronize or register a group with a reserved name, you will get an error including the following message:

```
Invalid group name
Name cannot be a reserved group name
```

To avoid problems, review the following list and avoid synchronising or creating groups with the following names.

The following group names are reserved:

- accumulo
- admins
- atlas
- cruisecontrol
- dpprofiler
- druid
- editors
- flink
- flume
- h2o
- hbase
- hdfs
- hive
- httpfs
- hue
- impala
- ipausers
- kafka
- keytrustee
- kms
- knox
- kudu
- livy
- mapred
- nifi
- nifiregistry

- oozie
- phoenix
- ranger
- rangerraz
- schemaregistry
- sentry
- solr
- spark
- sqoop
- sqoop2
- streamsmsgmgr
- streamsrepmgr
- tez
- trust admins
- yarn
- yarn-ats
- zeppelin
- zookeeper