Cloudera Runtime 7.3.2

Securing Hue

Date published: 2020-07-28
Date modified: 2026-03-31

https://docs.cloudera.com/

Legal Notice

Contents

User management in Cloudera Data Explorer (Hue)

Data Explorer is a gateway to Cloudera cluster services and both have completely separate permissions. Being a Data Explorer superuser does not grant access to HDFS, Hive, and so on.

Users who log on to the Data Explorer UI must have permission to use Data Explorer and to each Cloudera service accessible within Data Explorer.

A common configuration is for “Hue users” to be authenticated with an LDAP server and “Cloudera users” with Kerberos. These users can differ. For example, Cloudera services do not authenticate each user who logs on to Data Explorer. Rather, they authenticate “Hue” and trust that Data Explorer has authenticated “its” users.

Once Data Explorer is authenticated by a service such as Hive, Data Explorer impersonates the user requesting use of that service. For example, to create a Hive table. The service uses Apache Ranger to ensure the group to which that user belongs is authorized for that action.

Data Explorer user permissions are at the application level only. For example, a Data Explorer superuser can filter Data Explorer user access to a Cloudera service but cannot authorize the use of its features. Again, Ranger does that.

Understanding Cloudera Data Explorer (Hue) users and groups

There are two types of users in Data Explorer - superusers and general users referred to as users, each with specific privileges. These users can be a part of certain groups. Groups enable you to control which Data Explorer applications and features your users can view and access when they log into Data Explorer.

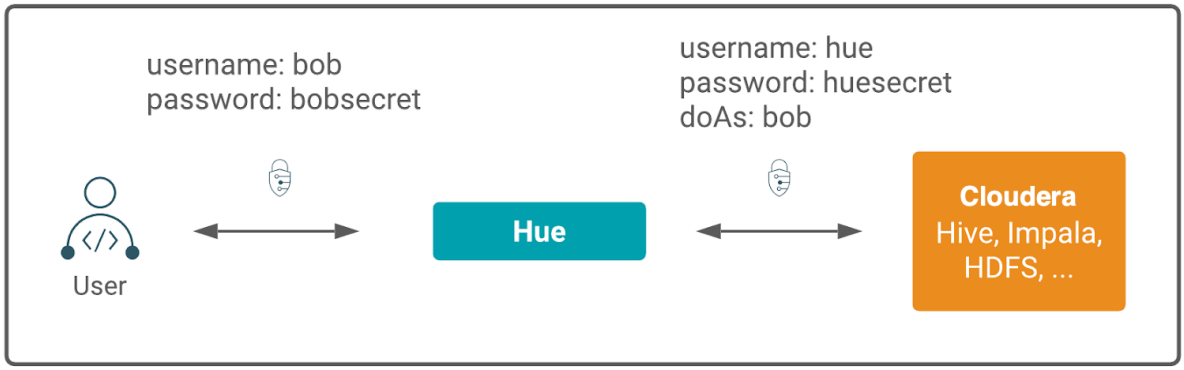
On a non-secure Cloudera cluster, the first user logging into Data Explorer after the initial installation becomes the first superuser. Superusers have the permissions to perform the following administrative functions:

- Add and delete users
- Add and delete groups
- Assign permissions to groups
- Change a user into a superuser
- Import users and groups from an LDAP server

If a user is part of the superuser LDAP group in Data Explorer, then that user is also a part of the group of superusers in Data Explorer.

Users can only change their name, e-mail address, and password. They can log in to Data Explorer and run Data Explorer applications, subject to the permissions provided by the Data Explorer groups to which they belong. This is different from how Cloudera perceives the Data Explorer application when you submit a Hive or an Impala query from the Data Explorer user interface (UI). Data Explorer is a server between the users and the Cloudera services. Data Explorer is considered as a single ‘hue’ user by the other services in the Cloudera cluster.

For example, when a user ‘bob’ submits a query from Data Explorer, Data Explorer also sends the username of this user to the corresponding service in Cloudera. The HIVE_ON_TEZ service in Cloudera considers ‘bob’ as the owner of the query and not ‘hue’. This is illustrated in the following graphic:



Data Explorer is a gateway to Cloudera cluster services and both have separate permissions. A Data Explorer superuser is not granted access to HDFS, Hive, and other Cloudera cluster services. Apache Ranger governs access to the Cloudera cluster services.

Note: Groups in Data Explorer are different from groups in Ranger.

Data Explorer user permissions are at the application level only. For example, a Data Explorer superuser can filter Data Explorer user access to a Cloudera service but cannot authorize the use of its features. Users who log on to the Data Explorer UI must have permission to use Data Explorer and to each Cloudera service accessible within Data Explorer.

Finding the list of Cloudera Data Explorer (Hue) superusers

You can fetch the list of superusers by using the Data Explorer shell with Python code or by running a SQL query on the auth_user table.

Using the Data Explorer shell and Python code to find Data Explorer superusers

1. Connecting to Data Explorer shell by running the following command:

```
/opt/cloudera/parcels/CDH/lib/hue/build/env/bin/hue shell --cm-managed
```

2. Enter the Python code as follows:

```
from django.contrib.auth.models import User
print "%s" % User.objects.filter(is_superuser = True)
```

Sample output:

```
<QuerySet [<User: admin>]>
```

Running a SQL query on the auth_user table to find Data Explorer superusers

1. Connect to Data Explorer database shell by running the following command:

```
/opt/cloudera/parcels/CDH/lib/hue/build/env/bin/hue dbshell --cm-managed
```

2. Run the following SQL query:

```
select username, is_superuser from auth_user where is_superuser=1;
```

The superuser status is stored as a boolean value, though its representation varies by database: 1 for true and 0 for false, or t for true and f for false.

Sample output:

```
----------------------+
username is_superuser
----------------------+

admin 1
----------------------+
1 row in set (0.00 sec)
```

Creating a Cloudera Data Explorer (Hue) user

You can create new Data Explorer users and superusers from the Data Explorer web UI and assign them to groups so that they can view and access Data Explorer as per the permissions granted to them.

About this task

Note: You can create a username for Data Explorer 150 characters long.

Before you begin

Per user home directories are created on HDFS when you create a new user in Data Explorer, which the user can use to store and retrieve files using the Data Explorer File Browser. To prevent unauthorized access by other Data Explorer users, add the following lines in Cloudera Manager Clusters Hue Configuration Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini :

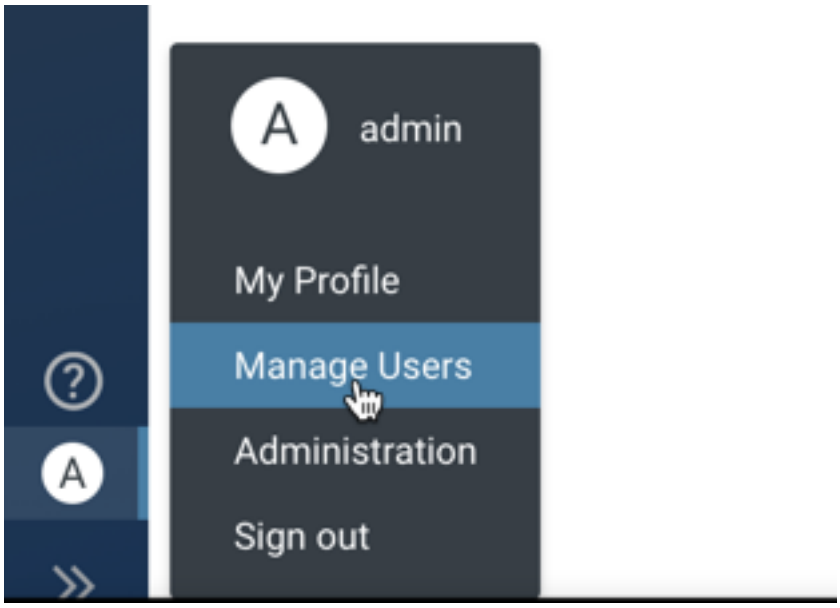
```
[useradmin]
home_dir_permissions=0700
use_home_dir_permissions=true
```

Set use_home_dir_permissions to false to use the HDFS umask.

Procedure

1. Sign in to the Hue UI as a superuser.

2. From the left assist panel, point your cursor to the user profile icon and click Manage Users.



The **User Admin** page is displayed.

3. On the **User Admin** page, click Add User.

The **Create user** page is displayed.

4. Enter the username and password for the user that you are adding on the Credentials tab.

To create a separate Hue home directory for the user, select the Create home directory option.

Click Next.

5. On the Profile and Group tab, create a profile for the user by entering the details such as name and email address.

At this point, if you have already created a group(s) that you want to assign to the user, then select it from the list displayed in the Groups field.

A user can be a part of more than one group.

Click Next.

6. (Optional) On the Advanced tab, select the Superuser status option to make this user a superuser and click Add user.

The new user is displayed on the **Users** page.

Related Information

Configuring file and directory permissions for Cloudera Data Explorer (Hue)

Controlling user access to Cloudera Data Explorer (Hue)

Administrators can control users who can access Data Explorer by creating different LDAP login groups, adding users needing access to these login groups, and then specifying the login groups in the Advanced Configuration Snippet in Cloudera Manager.

Before you begin

Ensure that you have added users needing access to Data Explorer to a login group.

Procedure

1. Log in to Cloudera Manager as an Administrator.

2. Go to Clusters Hue service Configuration and enter the following lines in the Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini field:

```
[desktop]
[[ldap]]
login_groups=[***LDAP-GRP1***], [***LDAP-GRP2***], [***LDAP-GRP3***]
```

Where, *[***LDAP-GRP1***], [***LDAP-GRP2***], [***LDAP-GRP3***]* are the login groups containing users needing access to Hue.

3. Click Save Changes.
4. Restart the Hue service.

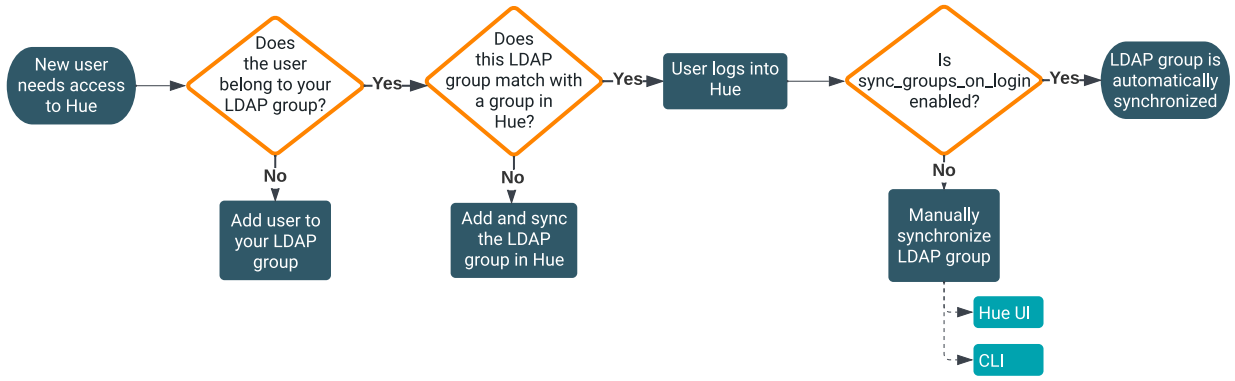
Options for importing and syncing LDAP users and groups in Cloudera Data Explorer (Hue)

Configuring Data Explorer for Lightweight Directory Access Protocol (LDAP) enables you to import users and groups from a directory service, synchronize group membership manually or automatically at login, and authenticate users with LDAP.

There are four options to import and sync LDAP users and groups in Data Explorer:

LDAP sync option	Description
Add/Sync LDAP user	Import and synchronize one user at a time
Sync LDAP users/groups	Synchronize user memberships in all groups
Add/Sync LDAP group	Import and synchronize all users in one group
sync_groups_on_login	Automatically synchronize group membership at login

The following flowchart shows the process and the options to import and synchronize new users or groups in Data Explorer:



Importing a group from LDAP creates a group in Data Explorer. When you synchronize a group, Data Explorer checks the user's group membership in LDAP and synchronizes it to the corresponding group in Data Explorer. To synchronize an LDAP group with Data Explorer, the group must be imported in the Data Explorer database.

For example, if a user belongs to 10 LDAP groups, but only 5 groups are present in Data Explorer, then only these 5 groups are synced when new users are added to these groups. This mechanism helps to avoid including irrelevant group data in the Data Explorer database.

If you have multiple LDAP groups that are synchronized with Data Explorer, then you can automate the synchronization process by turning on the sync_groups_on_login option in the Hue Advanced Configuration Snippet. However, this process can be burdensome if you have a large number of users logging in and authenticating simultaneously or new users getting added to the LDAP group, as multiple synchronization requests are triggered

which could cause collisions on database writes. An alternative approach is to synchronize users using the command line option, which you can script and automate as a cron job. To manually synchronize LDAP groups having the newly added users that need to be added to Data Explorer, run the following command separately for each LDAP group:

```
$HUE_HOME/build/env/bin/hue import_ldap_group --import-members [***LDAP-GROU
P-NAME***] --cm-managed
```

Importing and synchronizing users and groups with an LDAP server in Cloudera Data Explorer (Hue)

You can import and synchronize one user at a time, synchronize all user memberships in all groups, import and synchronize all users in one group, or enable synchronization of group memberships automatically when users in those groups log in to Data Explorer.

Before you begin

To synchronize your Data Explorer users and groups with your LDAP server:

- Data Explorer must be configured to authenticate with LDAP.
- The logged in user must have Data Explorer superuser permissions.

Note: If the backend is Isilon, then pre-create the users home folder /user/[***USERNAME***] and assign the necessary permissions to the folder owner/group. Failing to do this,causes the LDAP sync to fail because Data Explorer assigns the home folder's group permissions to be the username, but Isilon does not have a group with the username existing (unless it was pre-created.)

About this task

Important: Data Explorer does not support importing all groups at once.

Procedure

1. Log in to Hue as a superuser.
2. Go to User Admin Users .

   The **User Admin** page is displayed.
3. To import and synchronize one LDAP user in Hue:
   a) Click Add/Sync LDAP user.
   b) Add a username, check Create home directory, and click Add/Sync user.
4. To synchronize group memberships for LDAP users who have already been imported to Hue:
   a) Click Sync LDAP users/groups.
   b) Select the Create home directories option and click Sync.

   Note: This synchronizes group memberships with the LDAP server.
5. To import and synchronize one LDAP group containing its users:
   a) Click Add/Sync LDAP group.
   b) Check Create home directories, and click Sync.
6. To configure Hue to automatically synchronize LDAP groups and their users when they log in to Hue:
   a) Log in to Cloudera Manager as an Administrator.
   b) Go to Clusters Hue service Configuration and enter the following lines in the Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini field:

   ```
   [desktop]
   ```

```
[[ldap]]
  sync_groups_on_login=true
```

c) Click Save Changes.

d) Restart the Hue service.

Note: LDAP sync_groups_on_login only works with search bind authentication. This process can be burdensome if you have a large number of users logging in and authenticating simultaneously or new users getting added to the LDAP group, as multiple synchronization requests are triggered which could cause collisions on database writes.

7. To synchronize LDAP groups having the newly added users that need to be added to Hue, run the following command separately for each LDAP group:

```
$HUE_HOME/build/env/bin/hue import_ldap_group --import-members [***LDAP-
GROUP-NAME***] --cm-managed
```

You can script and automate this process using a cron job.

Locking an account after invalid login attempts

As a security measure, you can configure Data Explorer to lock an account after a set number of unsuccessful or invalid login attempts by specifying the number of attempts in the login_failure_limit parameter and setting the login_lock_out_at_failure parameter to true in the Hue Advanced Configuration Snippet in Cloudera Manager.

Procedure

1. Log in to Cloudera Manager as an Administrator.
2. Go to Clusters Hue Configuration and add the following lines in the Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini field:

```
[desktop]
[[auth]]
login_failure_limit=[***NUMBER-OF-ATTEMPTS-BEFORE-ACCOUNT-LOCKOUT***]
login_lock_out_at_failure=true
```

Replace [***NUMBER-OF-ATTEMPTS-BEFORE-ACCOUNT-LOCKOUT***] with the number of unsuccesful login attempts after which you want to lock an account. For example, if you set login_failure_limit to 3, then the user will be locked out on the third invalid attempt.

3. Click Save Changes.
4. Restart the Hue service to apply stale configurations.

   You can use the Rolling Restart option to minimize downtime.

Results

A user's account will be locked out after crossing the set number of invalid login attempts and the following message is displayed "Account locked: too many login attempts. Contact an admin to unlock your account."

Unlocking locked out user accounts in Cloudera Data Explorer (Hue)

If Data Explorer is configured to lock out a user account after a set number of invalid login attempts, then the users get an "Account locked: too many login attempts. Contact an admin to unlock your account." error message. As an Admin, you can unlock user accounts from the Data Explorer web interface.

Procedure

1. Log in to the Hue web interface as an Administrator or a Hue superuser.

2. Expand your user name on the left assist panel and click Administer Users.
   The **User Admin** page is displayed.
3. Click on the username that you want to unlock.
4. Go to the **Step 3. Advanced** tab and select the Unlock Account option.
5. Click Update User.

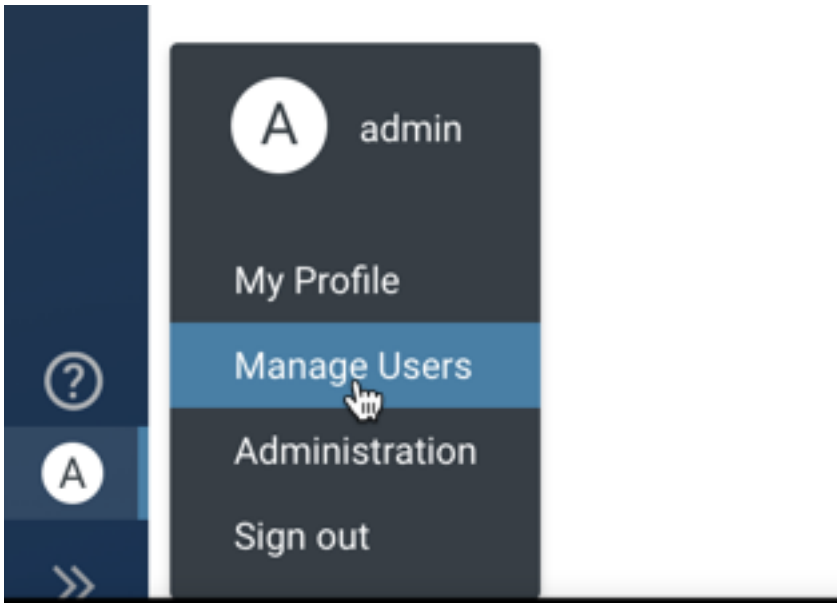
Results
The user should be able to log in to Hue.

Creating a group in Cloudera Data Explorer (Hue)

By creating groups, you can club certain permissions that you want to assign to specific users in your organization.

Procedure

1. Sign in to the Hue UI as a superuser.
2. From the left assist panel, point your cursor to the user profile icon and click Manage Users.



   The **User Admin** page is displayed.
3. Go to the Groups tab.
   The **Groups** page displays the list of existing groups, if any.
4. Click Add group.
5. On the **Create group** page, specify a name for your group.
6. (Optional) You can select the users that you want to add to this group.
7. Select the permissions that you want to associate with the group and click Add group.
   The newly added group is displayed on the **Groups** page along with the list of members and permissions associated with it.

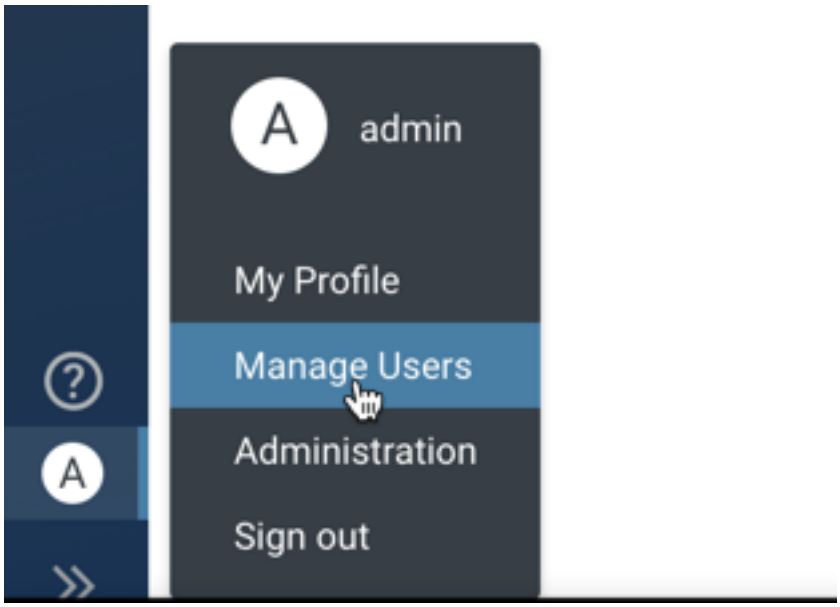
Managing Cloudera Data Explorer (Hue) permissions

Permissions for Data Explorer applications are granted to groups, with users gaining permissions based on their group membership. Group permissions define the Data Explorer applications visible to group members when they log in to

Data Explorer and the application features available to them. There is a fixed set of Data Explorer permissions. You cannot add or modify permissions. However, you can apply permission to group(s).

Procedure

1. Sign in to the Hue UI as a superuser.
2. From the left assist panel, point your cursor to the user profile icon and click Manage Users.



The **User Admin** page is displayed.

3. From the **User Admin** page, go to the Permissions tab.

The **Permissions** page displays the list of all the available permissions.

4. Click a permission that you want to assign to a group(s).

The **Edit [permission name]** page is displayed.

5. Select the group(s) on which you want to apply the permission and click Update permission.

The “Permission information updated successfully” message is displayed.

Resetting Cloudera Data Explorer (Hue) user password

The first user logging into Data Explorer after its initial installation becomes the first superuser. Even if a user does not log into the Data Explorer UI, the first security scan may log in creating an initial user and therefore resulting in an unknown username and password. You can change the password for a user if you know the username or you can create a new superuser user and then use it to log in to Data Explorer and change the password for a user.

Procedure

1. Sign in to the Hue server as the root user and go to the Hue home directory.
2. If you know the user ID of the currently logged in user, then reset the password by running the following command:

```
build/env/bin/hue changepassword [***USER-ID***] --cm-managed
```

Replace the *USER-ID* with the actual ID of the user.

3. If you do not know the user ID of the user whose password you want to change, then create a new Hue admin user by running the following command:

```
build/env/bin/hue createsuperuser --cm-managed
```

After creating a new admin user, log in to Hue and reset the password for a given user ID.

Assigning superuser status to an LDAP user

The Data Explorer User Admin application provides two levels of privileges: users and superusers. The superusers have administrative privileges.

About this task

Users can change their name, email address, and password. They can log in to Data Explorer and run Data Explorer applications according to their group permissions.

Superusers can perform administrative functions such as:

- Add and delete users and groups
- Import and sync users and groups from an LDAP server
- Assign group permissions
- Promote users to superusers and vice versa.

Data Explorer superusers have no special privileges to the underlying Cloudera cluster services. Ranger is used to add those privileges.

Important: On a non-secure cluster, the first user to log in to Data Explorer without LDAP authentication becomes the first superuser.

Procedure

In a secure cluster with LDAP deployed, there are three ways to assign superuser status to a user:

- With desktop.auth.backend.AllowAllBackend set for the Authentication Backend property in Cloudera Manager temporarily enabled, assign superuser status and synchronize one user to the LDAP server.
- With desktop.auth.backend.LdapBackend set for the Authentication Backend property in Cloudera Manager, run a Hue shell command to apply superuser status.
- Enable multiple backends so that the first user to log on still works when integrated with LDAP.

Configuring file and directory permissions for Cloudera Data Explorer (Hue)

Per user home directories are created on HDFS when you create a new user in Data Explorer, which the user can use to store and retrieve files using the Data Explorer File Browser. You must either configure Data Explorer to use the same permissions of the HDFS umask or use different permissions when a user creates files and directories from the Data Explorer File Browser. It is recommended to define the home directory permissions before creating users in Data Explorer.

About this task

When you set up Cloudera, you may have set a umask for all files and directories that would be created on HDFS using the “fs.permissions.umask-mode” parameter. The default HDFS umask is 0022. At this point, you can allow Data Explorer to use the permisions as defined by HDFS umask or you can configure Data Explorer to use a different

set of permissions. This is controlled by the following two parameters in Data Explorer: “home_dir_permissions” and “use_home_dir_permissions”. The “use_home_dir_permissions” parameter is set to true by default.

To allow Data Explorer to create files and directories with permissions different than the HDFS umask, set the following in the Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini field in Cloudera Manager:

```
[useradmin]
home_dir_permissions=[***HUE-FILE-DIR-PERMISSIONS***]
use_home_dir_permissions=true
```

For example:

```
[useradmin]
home_dir_permissions=0700
use_home_dir_permissions=true
```

To allow Data Explorer to use the same file and directory permissions as the HDFS umask, set the following in the Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini field in Cloudera Manager:

```
[useradmin]
use_home_dir_permissions=false
```

If you have not defined the home directory permissions in Data Explorer by setting the value of the home_dir_per missions property in the Hue Advanced Configuration before creating users in Data Explorer, then you can change the permissions for those users later to prevent unauthorized access.

Procedure

1. SSH in to the Hue server host as an Administrator.
2. Run the following command to change the permission for a user:

```
hdfs dfs -chmod 700 /user/[***USERNAME***]
```

User authentication in Cloudera Data Explorer (Hue)

Cloudera services do not authenticate each user that logs in to Data Explorer. The Cloudera services authenticate Data Explorer and trust that Data Explorer has authenticated its users. In a most typical configuration, Data Explorer users can be authenticated with an LDAP server and the Cloudera users can be authenticated with Kerberos. You can also use SAML for Single Sign-on (SSO) authentication.

After Hue is authenticated by a service such as Hive, Data Explorer impersonates the user requesting the use of that service, for example, to create a Hive table. In this case, the Hive service uses Apache Ranger to ensure that the group to which the user belonged is authorized for that action (to create a Hive table).

Note: By default, the Data Explorer session uses a secure cookie protocol.

Authenticating Cloudera Data Explorer (Hue) users with Kerberos

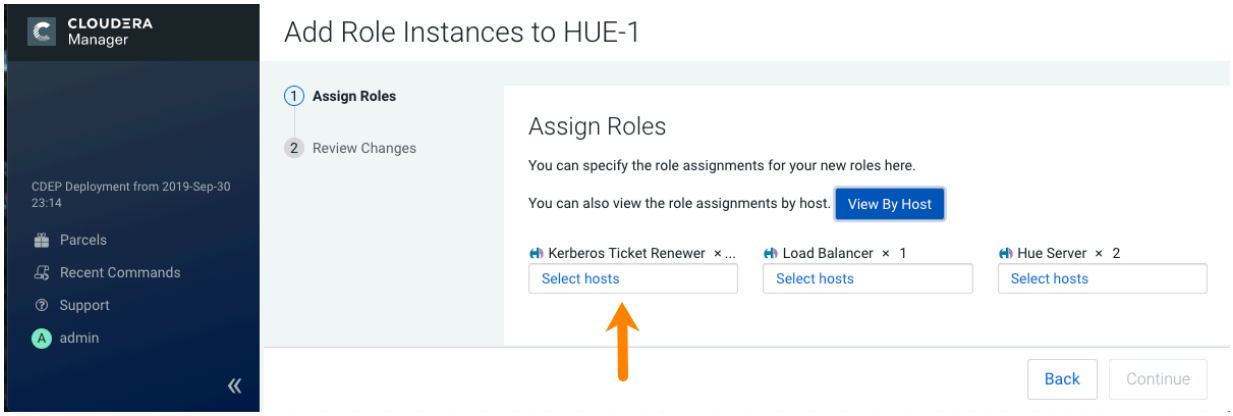
For Data Explorer to work properly with a Cloudera cluster that uses Kerberos for authentication, the Kerberos Ticket Renewer role must be added to the Data Explorer service.

About this task

Use the Cloudera Manager Admin Console to add the Kerberos Ticket Renewer role to each host with a Data Explorer Server role instance. The Data Explorer Kerberos Ticket Renewer renews only those tickets created for the Data Explorer service principal: hue/*HOSTNAME@REALM-NAME*. The Data Explorer principal impersonates other users for applications within Data Explorer such as the Job Browser, File Browser, and so on. Other services, such as HDFS and MapReduce, do not use the Data Explorer Kerberos Ticket Renewer. Instead these other services handle ticket renewal as needed by using their own mechanisms.

Procedure

1. On the Cloudera Manager home page, select the Hue service.
2. On the Hue service page, click the Instances tab.
3. On the Instances page, click Add Role Instances on the right side of the page. This launches the Add Role Instances wizard.
4. To add a Kerberos Ticket Renewer role instance to the same host that has the Hue server on your Cloudera cluster, click Select hosts under Kerberos Ticket Renewer:



   To check which host has the Hue Server role instance, click View By Host, which launches a table that lists all the hosts in your Cloudera cluster and shows all the roles each host already has.
5. In the host selection dialog box, after selecting the host where you want to add the Kerberos Ticket Renewer role instance, click OK, and Cloudera Manager adds the role instance.
6. After processing the request to add the role instance, Cloudera Manager returns you to the Instances page and prompts you to restart the service. Click the Restart the service (or the instance)... link so the configuration change can take effect.
7. After the services have restarted, click Finish to return to the Instances page.

   Repeat these steps for each Hue Server role on your cluster.

What to do next

Troubleshooting the Kerberos Ticket Renewer:

If the Hue Kerberos Ticket Renewer does not start, check the configuration of your Kerberos Key Distribution Center (KDC). Look at the ticket renewal property, maxrenewlife, to ensure that the principals, hue/<*HOST_NAME*> and krbtgt, are renewable. If these principals are not renewable, run the following commands on the KDC to enable them:

```
kadmin.local: modprinc -maxrenewlife 90day krbtgt/<YOUR_REALM.COM>
kadmin.local: modprinc -maxrenewlife 90day +allow_renewable hue/
<HOST_NAME>@<YOUR_REALM>
```

Authenticating Cloudera Data Explorer (Hue) users with LDAP

Configuring Data Explorer for Lightweight Directory Access Protocol (LDAP) enables you to import users and groups from a directory service, synchronize group membership manually or automatically at login, and authenticate with an LDAP server.

Data Explorer supports Microsoft Active Directory (AD) and open standard LDAP such as OpenLDAP and Forgerock OpenDJ Directory Services.

Integrating Hue with LDAP

When Data Explorer is integrated with LDAP, users can use their existing credentials to authenticate and inherit their existing groups transparently. There is no need to save or duplicate any employee password in Data Explorer.

When authenticating using LDAP, Hue validates login credentials against an LDAP directory service if Data Explorer is configured with the LDAP authentication backend (desktop.auth.backend.LdapBackend) in Cloudera Manager.

The LDAP authentication backend automatically creates users that do not exist in Data Explorer by default. Data Explorer needs to import users to properly perform the authentication. Passwords are never imported when importing users. You can disable automatic import of users by setting the create_users_on_login property in the Cloudera Manager Clusters Hue service Configuration Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini field to false.

```
[desktop]
[[ldap]]
create_users_on_login=false
```

The purpose of disabling the automatic import is to allow only a predefined list of manually imported users to login.

Preserving the case of the usernames

If you are using mixed case, upper case, or Camel case for usernames in your LDAP directory, then you must add the following configurations in Hue's Advanced Configuration Snippet (Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini), so that the user names are not over written in lower case in the Hue's database. Set the values of these properties to true or false depending on your requirement:

```
[desktop]
[[auth]]
ignore_username_case=true
force_username_uppercase=true/false
force_username_lowercase=true/false
[[ldap]]
ignore_username_case=true
force_username_uppercase=true/false
force_username_lowercase=true/false
```

Binding Hue with LDAP

There are two ways to bind Hue with an LDAP directory service:

Search Bind

The search bind mechanism for authenticating will perform an ldapsearch against the directory service and bind using the found distinguished name (DN) and password provided. This is the default method of authentication used by Hue with LDAP.

You can restrict the search process by configuring the following two properties under the Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini [desktop] > [[ldap]] > [[[users]]] section.

Property	Description
user_filter	General LDAP filter to restrict the search. Default: "objectclass=*"
user_name_attr	The attribute that will be considered the username to be searched against. Typical attributes to search for include: uid, sAMAccountName. Default: sAMAccountName

With the above configuration, the LDAP search filter takes the following form:

```
(&(objectClass=*)(sAMAccountName=[***USERNAME-ENTERED-BY-USER***]))
```

Note: Setting search_bind_authentication=true tells Hue to perform an LDAP search using the bind credentials specified for the bind_dn and bind_password configuration properties. Hue will start searching the subtree starting from the base DN specified for the base_dn property. It will then search the base DN for an entry whose attribute, specified in user_name_attr, has the same value as the short name provided on login. The search filter, defined in user_filter will also be used to limit the search.

Direct Bind

The direct bind mechanism for authenticating binds to the LDAP server using the username and password provided at login.

Hue authenticates (without searching) in one of two ways:

- NT Domain (nt_domain): (Only for use with Microsoft Active Directory) Hue binds to the AD with username@domain using the User Principal Names (UPN) to bind to the LDAP service. This AD-specific property allows Hue to authenticate with AD without having to follow LDAP references to other partitions. This typically maps to the email address of the user or the user's ID in conjunction with the domain. Default: mycompany.com.
- Username Pattern (ldap_username_pattern): Bind to open standard LDAP with full path of directory information tree (DIT). It provides a template for the DN that is ultimately sent to the directory service when authenticating. The [***USERNAME***] parameter is replaced with the username provided at login.

  Default:

  ```
  "uid=[***USERNAME***],ou=People,dc=mycompany,dc=com"
  ```

  Note: Setting search_bind_authentication=false tells Hue to perform a direct bind to LDAP using the credentials provided (not bind_dn and bind_password specified in the Advanced Configuration Snippet). There are two ways direct bind works depending on whether the nt_domain property is specified in the Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini :

  - nt_domain is specified: This is used to connect to an Active Directory service. In this case, the UPN is used to perform a direct bind. Hue forms the UPN by concatenating the short name provided at login with the nt_domain. For example, [***SHORT-NAME***]@[***NT-DOMAIN***]. The ldap_username_pattern property is ignored.
  - nt_domain is not specified: This is used to connect to all other directory services (can handle AD, but nt_domain is the preferred way for AD). In this case, ldap_username_pattern is used and takes the following form:

    ```
    cn=[***USERNAME-PROVIDED-AT-LOGIN***],dc=example,dc=com
    ```

Note: Username pattern does not work with AD because AD inserts spaces into the UID which Hue cannot process.

Encryption

To prevent credentials from transmitting in the clear, encrypt with LDAP over SSL, using the LDAPS protocol on the LDAPS port, which uses port 636 by default. An alternative, is to encrypt with the StartTLS operation using the standard LDAP protocol, which uses port 389 by default. Cloudera recommends LDAPS. You must have a CA Certificate in either case.

Table 1: Hue Supported LDAP authentication and encryption methods

LDAP Auth Action	Encrypted (LDAPS)	Encrypted (LDAP+TLS)	Not Encrypted (LDAP)
Search Bind	AD, LDAP	AD, LDAP	AD, LDAP
Direct Bind - NT Domain	AD	AD	AD
Direct Bind - User Pattern	LDAP	LDAP	LDAP

Prerequisites

To authenticate Hue users with LDAP, you must have:

- LDAP server
- Bind account (or support for anonymous binds)
- Cloudera Manager access with Full Administrator permissions
- [optional] LDAP server with LDAPS or StartTLS encryption.

Important: To authenticate securely, configure your LDAP server with either LDAP over SSL (LDAPS) or StartTLS encryption. Both methods require a Certificate Authority (CA) chain in a .pem file.

Configuring authentication with LDAP and Search Bind

Search Bind authentication executes ldapsearch against one or more directory services and binds with the distinguished name (DN) and password. Data Explorer searches the subtree from the base distinguished name. If the LDAP Username Attribute is set, Data Explorer looks for an entry whose attribute has the same value as the short name given at login.

About this task

Important: Search Binding works with all directory service types. It is also the only method that allows synchronizing groups at login (set with sync_groups_on_login in a safety-valve).

Watch the video at https://www.youtube.com/embed/pCgUxQ8CU4o

Procedure

1. Log on to Cloudera Manager and click Hue.
2. Click the Configuration tab and filter by scope=Service-wide and category=Security.
3. Set the following required properties:

Authentication Backend	desktop.auth.backend.LdapBackend
LDAP URL	• ldaps://<ldap_server>:636 if using Secure LDAP • ldap://<ldap_server>:389 if not using encryption Note: If ldaps:// is specified in the LDAP URL, then do not set LDAP TLS.

Enable LDAP TLS	• TRUE if not using Secure LDAP (LDAPS) but want to establish a secure connection using TLS • FALSE if using LDAPS or not encrypting
LDAP Server CA Certificate	/path_to_certificate/cert.pem
LDAP Search Base	DC=mycompany,DC=com
LDAP Bind User Distinguished Name	username@domain
LDAP Bind Password	bind_user_password
Use Search Bind Authentication	TRUE
Create LDAP users on login	TRUE

Note: To encrypt with TLS, set LDAP URL to ldap://<ldap_server>:389 and check Enable LDAP TLS. For a proof of concept without encryption, use ldap://<ldap_server>:389, remove the value for LDAP Server CA Certificate, and uncheck Enable LDAP TLS.

4. You can optionally improve search performance with attributes and filters:

LDAP User Filter	objectclass=user (default = *)
LDAP Username Attribute	sAMAccountName (AD default), uid (LDAP default)
LDAP Group Filter	objectclass=group (default = *)
LDAP Group Name Attribute	cn (default)
LDAP Group Membership Attribute	member (default)

Note: With the user settings in the table above, the LDAP search filter has the form: (&(objectClass=user)(sAMAccountName=<user entered username>)).

5. Add any valid user and/or valid group to quickly test your LDAP configuration:

LDAP Username for Test LDAP Configuration	Any valid user
LDAP Group Name for Test LDAP Configuration	Any valid group

6. Click Save Changes.
7. Test your LDAP configuration, and when successful click Restart Hue.

Note: The syntax of Bind Distinguished Name differs per bind method:

- Search Bind: username@domain
- Direct Bind with NT Domain: username
- Direct Bind with Username Pattern: DN string (full DIT path)

Do not use if anonymous binding is supported.

You can test ldapsearch at the command line as follows:

```
LDAPTLS_CACERT=/<path_to_cert>/<ca_certificate> ldapsearch -H ldaps://<l
dap_server>:636 \
-D "<bind_dn>" -w <bind_password> -b <base_dn> "samaccountname=<user>"
```

Note: To run ldapsearch with a CA certificate, you may need to install ldap_utils on Debian/Ubuntu and openldap-clients on RHEL/CentOS.

Configuring authentication with LDAP and Direct Bind

To authenticate with Direct Binding, Data Explorer needs either the User Principal Name (UPN) for Active Directory, or the full path to the LDAP user in the Directory Information Tree (DIT) for open standard LDAP.

About this task

Important: Direct binding only works with one domain. For multiple directories, use search bind.

Watch the video at https://www.youtube.com/embed/w9PQKytKr1A

To directly bind to an Active Directory/LDAP server with NT domain:

Procedure

1. Log in to Cloudera Manager and click Hue.
2. Click the Configuration tab and filter by scope=Service-wide and category=Security.
3. Set the following LDAP properties:

Authentication Backend	desktop.auth.backend.LdapBackend
LDAP URL	• ldaps://<ldap_server>:636 if using Secure LDAP • ldap://<ldap_server>:389 if not using encryption Note: If ldaps:// is specified in the LDAP URL, then do not set LDAP TLS.
Enable LDAP TLS	• TRUE if not using Secure LDAP (LDAPS) but want to establish a secure connection using TLS • FALSE if using LDAPS or not encrypting
LDAP Server CA Certificate	/path_to_certificate/cert.pem
LDAP Search Base	DC=mycompany,DC=com
LDAP Bind User Distinguished Name	<username> Only the username is required for Direct Bind. There is no need to specify the domain.
LDAP Bind Password	bind_user_password
Active Directory Domain	<your NT domain>
Use Search Bind Authentication	FALSE
Create LDAP users on login	TRUE

4. Click Save Changes
5. Test your LDAP configuration, and when successful, click Restart Hue.

   To directly bind to an open standard LDAP server with a username pattern:

   a. Remove the value for the Active Directory Domain.
   b. Set both LDAP Username Pattern and LDAP Bind User Distinguished Name to a DN string that represents the full path of the directory information tree, from UID to top level domain.

   Note: When using Direct Bind, set the LDAP Search Base property. This is not for authentication because you can log in to Hue without it, but to synchronize Hue with the LDAP server.

Configuring Cloudera Data Explorer (Hue) for authentication against multiple LDAP/ Active Directory servers

Some organizations have more than one LDAP or Active Directory (AD), and users in one LDAP/AD may not be present in the other. Data Explorer supports the ability to authenticate users against multiple LDAP/AD servers.

Before you begin

Before attempting LDAP authentication against multiple servers, ensure you have configured LDAP synchronization for each server, as described in the previous sections. As long as users and groups are synchronised across LDAP and Data Explorer, authentication should work.

Procedure

1. Log in to Cloudera Manager as an Administrator.
2. Go to Clusters Hue service Configuration Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini , and add the following lines for each LDAP server:

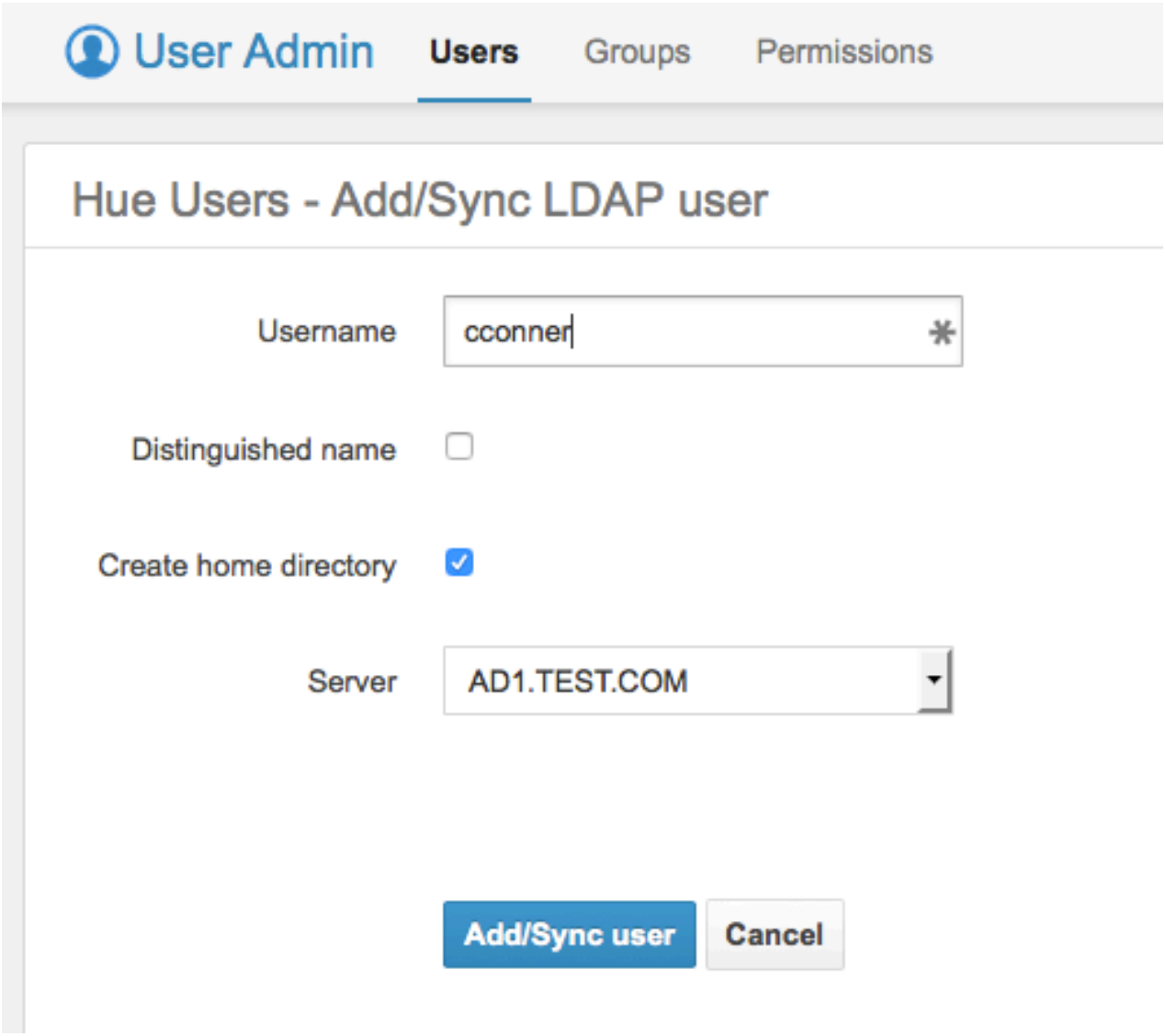
```
[desktop]
[[ldap]]
[[[ldap_servers]]]

[[[[AD1.TEST.COM]]]]
ldap_url=ldap://w2k8-ad1
search_bind_authentication=true
create_users_on_login=true
base_dn="cn=users,dc=ad1,dc=test,dc=com"
bind_dn="cn=Administrator,cn=users,dc=ad1,dc=test,dc=com"
bind_password="[***PASSWORD***]"
[[[[AD2.TEST.COM]]]]
ldap_url=ldap://w2k8-ad2
search_bind_authentication=true
create_users_on_login=true
base_dn="cn=users,dc=ad2,dc=test,dc=com"
bind_dn="cn=Administrator,cn
bind_password="[***PASSWORD***]"
```

   The above code snippet is for a demo LDAP server called "AD1.TEST.COM" and "AD2.TEST.COM".
3. Click Save Changes.
4. Restart the Hue service.

Results

When you log into Hue or while synchronizing LDAP users from the Hue web interface, you need to select the LDAP/AD server from the dropdown list.



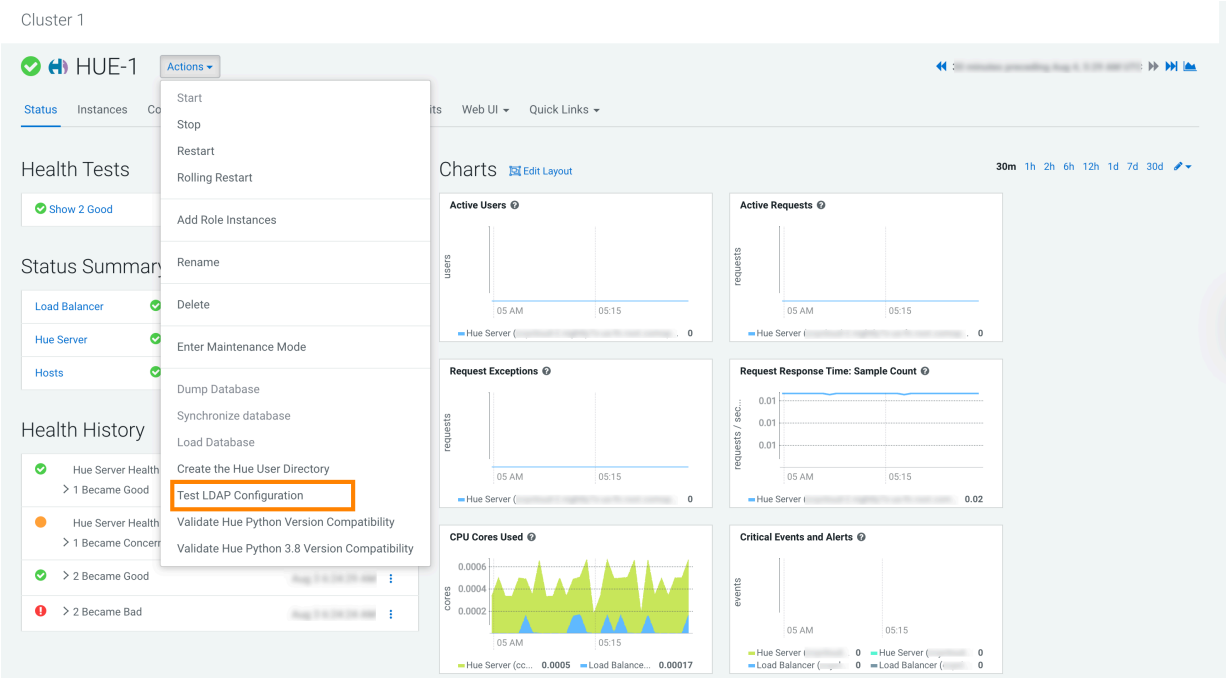
Testing the LDAP configuration

You can test your Data Explorer LDAP configuration without restarting the Data Explorer service. Add the values and save your changes.

Procedure

1. Configure Hue to authenticate with LDAP by using search bind or direct bind.
2. Add a user and group name for Test LDAP Configuration.
3. Click Save Changes.
4. Select ActionsTest LDAP Configuration.

5. Click Test LDAP Configuration:

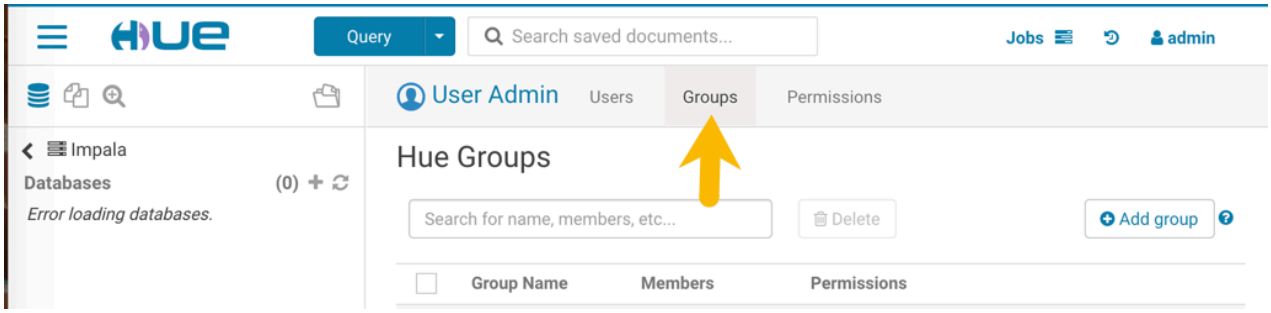


6. Click Restart Hue. When the test succeeds, log in to the Hue Web UI.

Configuring group permissions

You can configure permissions for members of groups on the Groups tab of the Data Explorer User Admin application.

About this task



Note: A best practice is to remove all permissions from the default group and assign permissions as appropriate to your own groups.

Procedure

1. Log on to the Hue UI as a superuser.
2. Go to User AdminGroups.
3. Click the name of the group you want to alter.
4. Deselect any users that you do not want to change (all users in the group are selected by default).
5. Select or deselect the permissions you want to apply or remove.
6. Click Update Group.

Enabling LDAP authentication with HiveServer2 and Impala

LDAP authentication with HiveServer2 and Impala can be enabled by setting the auth_username and auth_password properties under the [beeswax] section for Hive and the [impala] section for Impala in a Cloudera Manager safety valve configuration property.

Important: Set these properties in the Cloudera Manager Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini property.

auth_username	LDAP username of the Hue user to be authenticated to the server.
auth_password	LDAP password of the Hue user to be authenticated to the server.

For example:

```
[beeswax]
   auth_username=<HIVESERVER2_LDAP_USER_NAME>
   auth_password=<HIVESERVER2_LDAP_PASSWORD>
[impala]
   auth_username=<IMPALA_LDAP_USER_NAME>
   auth_password=<IMPALA_LDAP_PASSWORD>
```

These login details are only used by Impala and Hive to authenticate to the LDAP server. The Impala and Hive services trust Data Explorer to have already validated the user being impersonated instead of passing on the credentials.

LDAP properties

These are the properties you can use to configure LDAP for Data Explorer in Cloudera Manager or in the hue.ini file for unmanaged clusters.

Property Name	Description and Syntax
General Hue LDAP Properties	
Authentication Backend backend	Authentication Mode. Select desktop.auth.backend.LdapBackend. Multiple backends are allowed. Create a list and add it to the Hue safety-valve.
LDAP URL ldap_url	URL for the LDAP server. Syntax: ldaps://<ldap_server>:<636> or ldap://<ldap_server>:<389> Important: To prevent usernames and passwords from transmitting in the clear, use ldaps:// or ldap:// + "Enable LDAP TLS".
Create LDAP users on login create_users_on_login	Flag to create new LDAP users at Hue login. If true, any user who logs into Hue is automatically created. If false, only users that exist in useradmin can log in.
Direct Bind Properties	
Active Directory Domain nt_domain	For direct binding with Microsoft Active Directory only. Typically maps to the user email address or ID in conjunction with the domain. Allows Hue to authenticate without having to follow LDAP references to other partitions. Hue binds with User-Principal-Name (UPN) if provided. Example: ad.<mycompany>.com Important: Do not use nt_domain with LDAP Username Pattern or Search Bind.
LDAP Username Pattern ldap_username_pattern	For direct binding with LDAP (non-Active Directory) only (because AD uses UPNs which have a space in them). Username Pattern finds the user attempting to login into LDAP by adding the username to a predefined DN string. Use <username> to reference the user logging in. An example is "uid=<username>,ou=people,dc=mycompany,dc=com".
Search Bind Properties	

Property Name	Description and Syntax
Use Search Bind Authentication search_bind_authentication	Flag to enable/disable Search Bind.
LDAP Search Base base_dn	Distinguished name to use as a search base for finding users and groups. Syntax: dc=ad, dc=sec, dc=mycompany,dc=com
Encryption Properties	
LDAP Server CA Certificate ldap_cert	Full path to .pem file with Certificate Authority (CA) chain used to sign the LDAP server certificate. If left blank, all certificates are trusted and otherwise encrypted usernames and passwords are vulnerable to attack.
Enable LDAP TLS use_start_tls	Flag to enable/disable encryption with the StartTLS operation.
Import / Sync Properties	
LDAP Bind User Distinguished Name bind_dn	Bind user. Only use if LDAP/AD does not support anonymous binds. (Typically, LDAP supports anonymous binds and AD does not.) Bind User differs per auth type: • Search Bind: username@domain • Direct Bind with NT Domain: username • Direct Bind with Username Pattern: DN string (and same as LDAP Username Pattern)
LDAP Bind Password bind_password	Bind user password.
Filter Properties	
LDAP User Filter user_filter	General LDAP text search filter to restrict search of valid users. Only used by Search Bind authentication and LDAP Sync. The default is objectclass=* but can differ. For example, some LDAP environments support Posix objects for *nix authentication and the user filter might need to be objectclass=posixAccount.
LDAP Username Attribute user_name_attr	Username to search against (the attribute in LDAP that contains the username). Typical attributes include sAMAccountName (default for AD/LDAP) and uid (LDAP default). Maintain case sensitivity when setting attributes for AD/LDAP.
LDAP Group Filter group_filter	General LDAP text search filter to restrict search of valid groups. Only used by LDAP Sync (not authentication). If left blank, no filtering is used and all groups in LDAP are synced. The default is objectclass=* but can differ. For example, some LDAP environments support Posix objects for *nix authentication and the user filter might need to be objectclass=posixGroup.
LDAP Group Name Attribute group_name_attr	Group name to search against (the attribute in LDAP that contains the groupname). If left blank, the default is "cn" (common name), that typically works with AD/LDAP. Maintain case sensitivity when setting attributes for AD/LDAP.
LDAP Group Membership Attribute group_member_attr	Attribute in the group that contains DNs of all the members.(Optional) - If left blank, the default is "memberOf" or "member", that typically works with Active Directory/LDAP.
Test Properties	
LDAP Username for Test LDAP Configuration test_ldap_user	Any user (ideally with low privileges) used to verify the LDAP configuration.

Property Name	Description and Syntax
LDAP Group Name for Test LDAP Configuration test_ldap_group	Any group (and not necessarily one that includes the test user) used to verify the LDAP configuration.

Configuring LDAP on unmanaged clusters

If your clusters are not managed with Cloudera Manager, you must manually set the LDAP configuration properties in the hue.ini file.

Refer to the following examples of LDAP configurations in the hue.ini file:

Example of a Search Bind configuration encrypted with LDAPS:

```
[[custom]]
[[auth]]
backend=desktop.auth.backend.LdapBackend

[[ldap]]
ldap_url=ldaps://<hostname>.ad.sec.<domain_name>.com:636
search_bind_authentication=true
ldap_cert=/<path_to_cacert>/<cert_filename>.pem
use_start_tls=false
create_users_on_login=true
base_dn="DC=ad,DC=sec,DC=<domain_name>,DC=com"
bind_dn="<username>@ad.sec.<domain_name>.com"
bind_password_script=<path_to_password_script>/<script.sh>
test_ldap_user="testuser1"
test_ldap_group="testgroup1"

[[[users]]]
user_filter="objectclass=user"
user_name_attr="sAMAccountName"

[[[groups]]]
group_filter="objectclass=group"
group_name_attr="cn"
group_member_attr="member"
```

Example of a Direct Bind configuration for Active Directory encrypted with LDAPS:

```
[[ldap]]
ldap_url=ldaps://<hostname>.ad.sec.<domain_name>.com:636
search_bind_authentication=false
nt_domain=ad.sec.<domain_name>.com
ldap_cert=/<path_to_cacert>/<cert_filename>.pem
use_start_tls=false
create_users_on_login=true
base_dn="DC=ad,DC=sec,DC=<domain_name>,DC=com"
bind_dn="<username>"
bind_password_script=<path_to_password_script>/<script.sh>
...
```

Example of a Direct Bind configuration for Active Directory encrypted with StartTLS:

```
[[ldap]]
ldap_url=ldap://<hostname>.ad.sec.<domain_name>.com:389
search_bind_authentication=false
nt_domain=ad.sec.<domain_name>.com
ldap_cert=/opt/cloudera/security/cacerts/<cert_filename>.pem
use_start_tls=true
create_users_on_login=true
base_dn="DC=ad,DC=sec,DC=<domain_name>,DC=com"
```

```
bind_dn="<username>"
bind_password_script=<path_to_password_script>/<script.sh>
...
```

Authenticating Cloudera Data Explorer (Hue) users with SAML

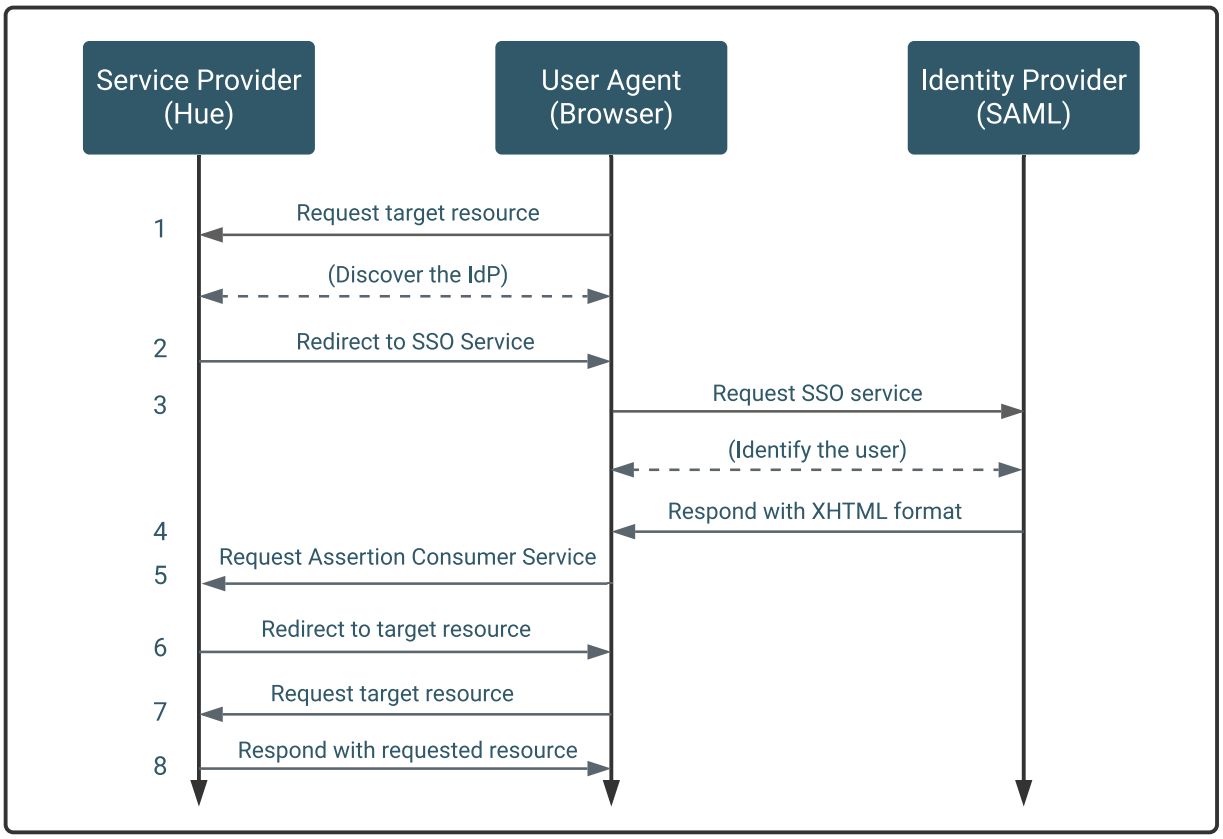
Data Explorer supports SAML (Security Assertion Markup Language) for Single Sign-on (SSO) authentication.

The SAML 2.0 Web Browser SSO profile has three components:

- User Agent - Browser that represents you, the user, seeking resources.
- Service Provider (SP) - Service (Hue) that sends authentication requests to SAML.
- Identity Provider (IdP) - SAML service that authenticates users.

When a user requests access to an application, the Service Provider (Hue) sends an authentication request from the User Agent (browser) to the identity provider. The identity provider authenticates the user, sends a response, and redirects the browser back to Data Explorer as shown in the following diagram:

Figure 1: SAML SSO protocol flow in a web browser



The Service Provider (Hue) and the identity provider use a metadata file to confirm each other's identity. Data Explorer stores metadata from the SAML server, and the identity provider stores metadata from the Data Explorer server.

Configuring SAML authentication on managed clusters

To configure Data Explorer for SAML authentication on managed clusters, you must add the SAML authentication properties to the Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini in Cloudera Manager.

Before you begin

These instructions assume that you have an Identity Provider set up and running. You can use any identity provider of your choice. For example, Okta, Ping Identity, and OpenAM.

Procedure

1. Log on to Cloudera Manager and go to Hue Configuration .
2. In the search text box, enter hue_safety_valve.ini to locate the Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini.
3. Enter the SAML parameters into the Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini text box. For example:

```
## Example Settings using Open AM:
[desktop]
redirect_whitelist="^\/.*$,^https:\/\/idp.example.com:8080\/.*$"
[[auth]]
backend=libsaml.backend.SAML2Backend
[libsaml]
want_response_signed=True
want_assertions_signed=True
xmlsec_binary=/usr/bin/xmlsec1
metadata_file=/opt/cloudera/security/saml/idp-metadata.xml
key_file=/opt/cloudera/security/saml/host.key
cert_file=/opt/cloudera/security/saml/host.pem
key_file_password=Config(
  key="key_file_password",
  help=_t("key_file_password password of the private key"),
  default=None) ## If using encrypted private key
username_source=nameid
name_id_format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
entity_id=[***HOST-BASE-NAME***]
logout_enabled=false
```

   If you are using an encrypted private key file, then you must specify the password in the key_file_password property. Or you can use an unencrypted private key file.

   To create an unencrypted private key file from an encrypted key:

   a. SSH into a terminal as a root user.
   b. Change to the directory where you have stored the ssl certificate key.
   c. Run the following command:

```
openssl rsa -in ssl_certificate.key -out ssl_certificate-nocrypt.key
```

   d. When prompted, enter the password that you use to access the ssl_certificate.key file.

      The output file (ssl_certificate-nocrypt.key) is an unencrypted PEM-formatted key.

   Note: For SLES distributions, the xmlsec binary may be located in /usr/local/bin/. If so:

   - Set xmlsec_binary=/usr/local/bin/xmlsec1 in the Hue Service Advanced Configuration Snippet.
   - Set LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/local/lib/ in the Hue Service Environment Advanced Configuration Snippet.

4. Go to Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini) and comment or remove any Knox-SSO configurations, if present.

   Caution: Knox-SSO and SAML are incompatible and mutually exclusive. Hue authetication may fail with a redirection loop if you have the Knox-SSO and SAML configurations present in the Hue Advanced Configuration Snippet at the same time, as it confuses the authentication redirect to the IdP and back to Hue.

5. Click Save Changes, then select, ActionsRestart Hue.

Manually configuring SAML authentication

To manually configure Data Explorer for SAML authentication on unmanaged clusters, you must add GCC Python libraries and install xmlsec1 tools on all the hosts in your cluster.

Before you begin

These instructions assume that you have an Identity Provider set up and running. You can use any identity provider of your choice. For example, Okta, Ping Identity, and OpenAM.

Important: You may need to disable cipher algorithms before manually configuring Data Explorer for SAML authentication.

Procedure

1. Install the following libraries on all hosts in your cluster:

```
## RHEL/CentOS
yum install git gcc python-devel swig openssl
```

```
## Ubuntu/Debian
apt-get install git gcc python-dev swig openssl
```

```
## SLES
zypper install git gcc python-devel swig openssl make libxslt-devel libl
tdl-devel
```

2. Install xmlsec1 and xmlsec1-openssl on all hosts in the cluster:

Important: Ensure that the xmlsec1 package is executable by the user, hue.

```
## RHEL/CentOS
yum install xmlsec1 xmlsec1-openssl
```

Note: If xmlsec libraries are not available, use the appropriate epel repository:

```
## For RHEL/CentOS 7
wget http://dl.fedoraproject.org/pub/epel/7/x86_64/e/epel-relea
se-7-6.noarch.rpm
rpm -ivh epel-release-7-6.noarch.rpm
```

```
## Ubuntu/Debian
apt-get install xmlsec1 libxmlsec1-openssl
```

```
## SLES (get latest version)
wget http://www.aleksey.com/xmlsec/download/xmlsec1-1.2.24.tar.gz
tar -xvzf xmlsec1-1.2.24.tar.gz
cd xmlsec1-1.2.24
./configure && make
make install
```

3. Copy metadata from your identity provider's SAML server and save it as an XML file on every host with a Hue server. For example, if your identity provider is Shibboleth, visit https://<idp_host>:8443/idp/shibboleth, copy the

metadata content, and paste it into an XML file. Read the documentation of your identity provider for details on how to copy the XML of the SAML server metadata.

Note: You may have to edit the copied metadata; for example, the identity provider's port number (8443) might be missing from its URL.

```
mkdir -pm 755 /opt/cloudera/security/saml/
cd /opt/cloudera/security/saml/
```

```
vim idp-<your idp provider>-metadata.xml
# Paste IdP SAML here and save
```

4. Add the files that the key_file and cert_file SAML properties point to for encrypted assertions and make sure you add this properties to the hue.ini configuration file.
   - The key_file parameter points to the location of the private key that is used to encrypt metadata. Its file format must be <file_name>.PEM.
   - The cert_file parameter points to the location of the X.509 certificate that is sent with encrypted metadata. Its file format must be <file_name>.PEM.

   Warning:

   Add the key and cert files even if you are not encrypting assertions. Hue checks for the existence and validity of these files even if they are not needed. They cannot be empty files. This is a known issue. If necessary, create a valid self-signed certificate:

   ```
   openssl req -x509 -newkey rsa:2048 -sha256 -days 3560 -nodes -keyout
    host.key -out host.pem -subj '/CN=Hue SAML'
   ```

Integrating your identity provider's SAML server with Cloudera Data Explorer (Hue)

After Data Explorer is configured for SAML authentication and restarted, copy the metadata that is generated by the Data Explorer server and send it to your identity provider so they can configure the SAML server.

Before you begin

Ensure that you have configured Data Explorer for SAML authentication and restarted it before you integrate your identity provider's SAML server with Data Explorer.

Procedure

1. Ensure Hue is configured, restarted, and running.
2. Go to http://<hue_fqdn>:8889/saml2/metadata.
3. Copy the metadata and send it to your identity provider.
4. Ensure that your identity provider configures the SAML server with the Hue metadata. It is the same process you used to configure the Hue server with SAML metadata.

SAML properties

You can set SAML properties in the hue.ini file for unmanaged clusters. A subset of them can be set in the Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini for managed clusters.

Table 2: Table of SAML parameters

SAML parameter	Description
authn_requests_signed	Boolean, that when True, signs Hue-initiated authentication requests with X.509 certificate.
backend	Hard-coded value set to SAML backend library packaged with Hue (libsaml.backend.SAML2Backend).

SAML parameter	Description
base_url	URL that SAML Identity Provider uses for responses. Typically used in Load balanced Hue environments.
cert_file	Path to X.509 certificate sent with encrypted metadata. File format must be .PEM.
create_users_on_login	Boolean, that when True, creates users from OpenId, upon successful login.
entity_id	Service provider ID. Can also accept pattern where '<base_url>' is replaced with server URL base.
key_file	Path to private key used to encrypt metadata. File format must be .PEM.
key_file_password	Password used to decrypt the X.509 certificate in memory.
logout_enabled	Boolean, that when True, enables single logout.
logout_requests_signed	Boolean, that when True, signs Hue-initiated logout requests with an X.509 certificate.
metadata_file	Path to readable metadata XML file copied from Identity Provider.
name_id_format	Format of NameID that Hue requests from SAML server.
optional_attributes	Comma-separated list of optional attributes that Hue requests from Identity Provider.
required_attributes	Comma-separated list of required attributes that Hue requests from Identity Provider. For example, uid and email.
redirect_whitelist	Fully qualified domain name of SAML server: "^\/.*$,^https:\/\/<SAML_server_FQDN>\/.*$".
user_attribute_mapping	Map of Identity Provider attributes to Hue django user attributes. For example, {'uid':'username', 'email':'email'}.
username_source	Declares source of username as nameid or attributes.
want_response_signed	A boolean parameter, when set to True, requires SAML response wrapper returned by an IdP to be digitally signed by the IdP. The default value is False.
want_assertions_signed	A boolean parameter, when set to True, requires SAML assertions returned by an IdP to be digitally signed by the IdP. The default value is False.
xmlsec_binary	Path to xmlsec_binary that signs, verifies, encrypts/decrypts SAML requests and assertions. Must be executable by user, hue.

SAML properties that can be set for managed clusters

- redirect_whitelist [desktop]

  Set to the fully qualified domain name of the SAML server so that Hue can redirect to the SAML server for authentication.

  ```
  [desktop]
  redirect_whitelist=^\/.$,^https:\/\/<SAML_server_fully_qualified_domain_name>\/.$
  ```

  Note: Hue uses redirect_whitelist to protect itself from redirecting to unapproved URLs.

- backend [desktop]>[[auth]]

  Point to the SAML backend that is packaged with Hue:

  ```
  backend=libsaml.backend.SAML2Backend
  ```

- xmlsec_binary [libsaml]

  Point to the xmlsec1 library path:

  ```
  xmlsec_binary=/usr/bin/xmlsec1
  ```

  Note: To find the path, run: which xmlsec1

- metadata_file [libsaml]

  Point to the path of the XML file you created from the identity provider's metadata:

  ```
  metadata_file=/path/to/<your_idp_metadata_file>.xml
  ```

- key_file and cert_file [libsaml]

  To encrypt communication between Hue and the Identity Provider (IdP), you need a private key and certificate. The private key signs requests sent to the IdP, and decrypts messages from the IdP. The certificate is used to encrypt messages to Hue from the IdP, and must be provided to the IdP. Typically, the cert_file is shared by providing Hue's Service Provider metadata XML to the IdP admins, but you may also share a copy of the cert_file itself.

  The SAML certificate and private key must be the same on all Hue Server hosts, and can be self-signed, obtained from a commercial CA vendor, or from your internal PKI administrators. Both key_file and cert_file must be in PEM format.

  Users with password-protected certificates can set the property, key_file_password in the hue.ini file. Hue uses the password to decrypt the SAML certificate in memory and passes it to xmlsec1 through a named pipe. The decrypted certificate never touches the disk. This only works for POSIX-compatible platforms.

Troubleshooting SAML authentication

Before troubleshooting your SAML authentication configuration in Data Explorer, enable DEBUG for the Hue Django logs that are located in /var/log/hue. In the Data Explorer Web UI, go to the Home page, select Server Logs, and check Force Debug Level. For managed clusters, you can use Cloudera Manager to enable DEBUG by navigating to the Hue service, selecting the Configuration tab, check Enable Django Debug mode, click Save Changes, and then Restart.

SAML SSL error

OpenSSL might fail with this message:

```
SSLError: [Errno bad handshake] [('SSL routines', 'SSL3_CHECK_CERT_AND_ALGOR
ITHM', 'dh key too small')]
```

To resolve, append the following code to the file, /usr/java/<your_jdk_version>-cloudera/jre/lib/securi
ty/java.security:

```
jdk.tls.disabledAlgorithms=MD5, RC4, DH
```

SAML decrypt error

The following error is an indication that you are using a slightly different SAML protocol from what Hue expects:

```
Error: ('failed to decrypt', -1)
```

To resolve:

1. Download and rename the fix-xmlsec1.txt Python script.

```
https://docs.cloudera.com/application-resources/latest/shared/fix-xmlsec1.txt
```

2. Change permissions as appropriate, for example:

```
chmod 755 fix-xmlsec1.py
```

3. In hue.ini, set xmlsec_binary=<path_to_script>/fix-xmlsec1.py.
4. Run fix-xmlsec1.py.

This script repairs the known issue whereby xmlsec1 is not compiled with RetrievalMethod and cannot find the location of the encrypted key. SAML2 responses would sometimes place EncryptedKey outside of the EncryptedData tree. This script moves EncryptedKey under EncryptedData.

Authenticating Cloudera Data Explorer (Hue) users with Knox SSO

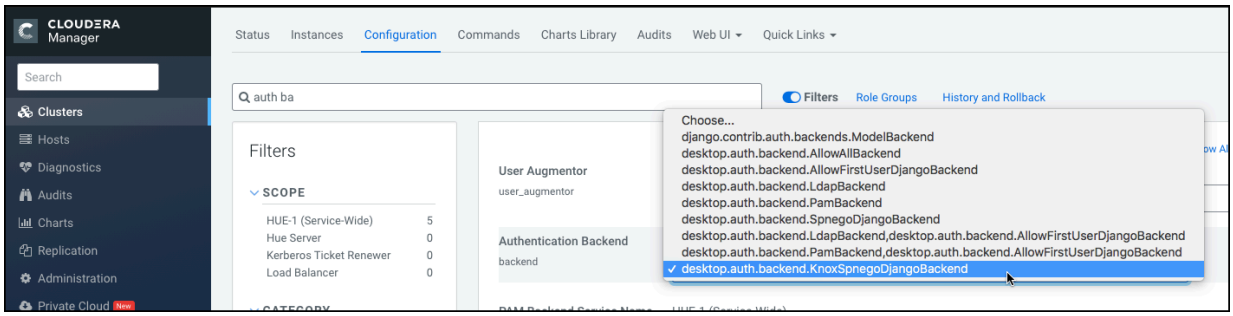
You can use the Apache Knox Gateway to interact with Data Explorer REST APIs and the Data Explorer user interface, along with other Cloudera components and services. To set up Knox Single Sign-on (SSO) to authenticate users, you must configure the KnoxSpnegoDjangoBackend property using Cloudera Manager.

Before you begin

To authenticate users using Knox SSO, you must have Knox installed on your Cloudera cluster, also known as a secure cluster.

Procedure

1. Sign in to Cloudera Manager as an Administrator.
2. Go to Clusters Hue service Configurations and search for the Authentication Backend field.
3. Select desktop.auth.backend.KnoxSpnegoDjangoBackend from the dropdown.



4. Go to Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini) and comment or remove any SAML-specific configurations, if present.

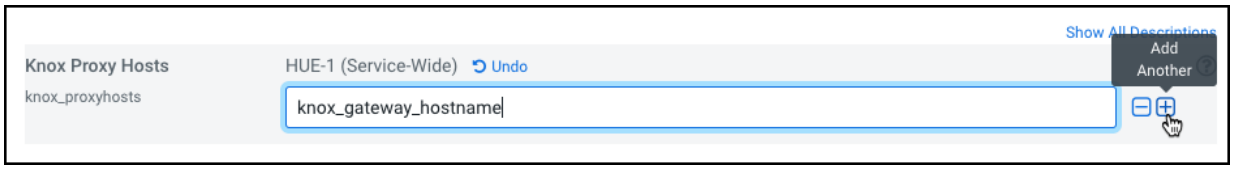
Caution: Knox-SSO and SAML are incompatible and mutually exclusive. Hue authetication may fail with a redirection loop if you have the Knox-SSO and SAML configurations present in the Hue Advanced Configuration Snippet at the same time, as it confuses the authentication redirect to the IdP and back to Hue.

5. Click Save Changes.
6. Go to Clusters $Knox service Instances and note down the hostnames of the Knox Gateways.

   You must provide these details in the next step.

   If you have set up Knox in High-Availablity (HA) mode, then you can see more than one Knox Gateways listed on the Instances tab.
7. Go back to Clusters Hue service Configurations and search for the Knox Proxy Hosts field.

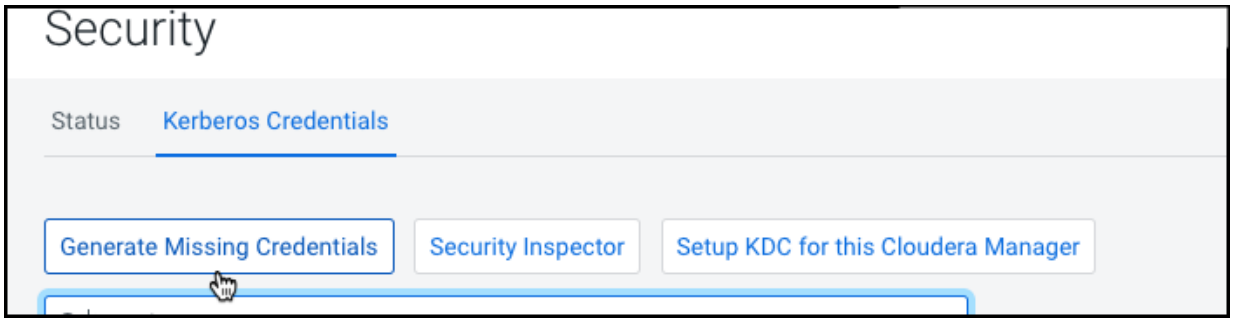
8. Enter the hostname of the Knox Gateway that you noted earlier.
   If you have set up Knox HA, then click + to add another hostname.



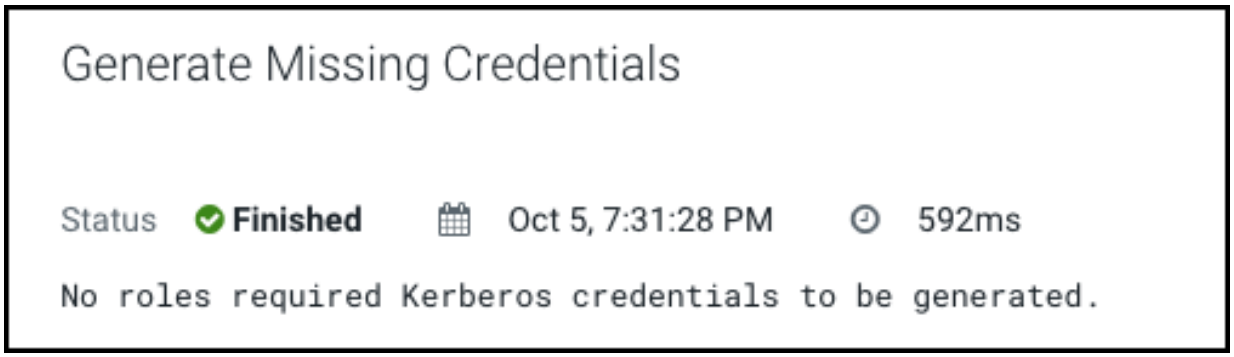
9. When integrating Hue with Knox, it is essential to deploy a Hue Load Balancer. After deployment, specify the Load Balancer hostname in the Knox Proxy Hosts field by clicking the + icon.
10. Click Save Changes.
    You would see the following warning:

```
Role is missing Kerberos keytab. Go to the Kerberos Credentials page and
 click the Generate Missing Credentials button.
```

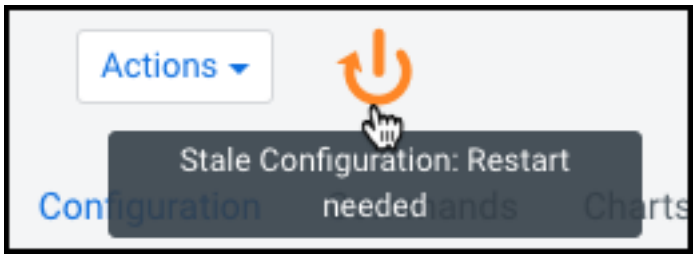
11. Click Administration on the Cloudera Manager left navigation panel and select Security.
12. Go to the Kerberos Credentials tab and click Generate Missing Credentials.



A pop-up showing the status is displayed.



13. Go to Clusters Hue service and click Restart next to Actions.



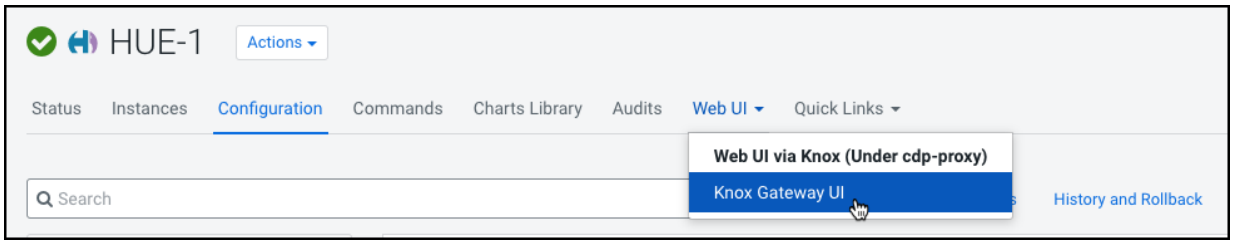
14. On the **Stale Configurations** page, click Restart Stale Services.
    The **Restart Stale Services** wizard is displayed.

15. On the Review Changes page, select Redeploy client configuration, and click Restart Now.

    The **Command Details** page shows the live status as the service restarts.

    When all the steps are complete, click Finish.

16. From the Hue service page, click Web UI Knox Gateway UI .

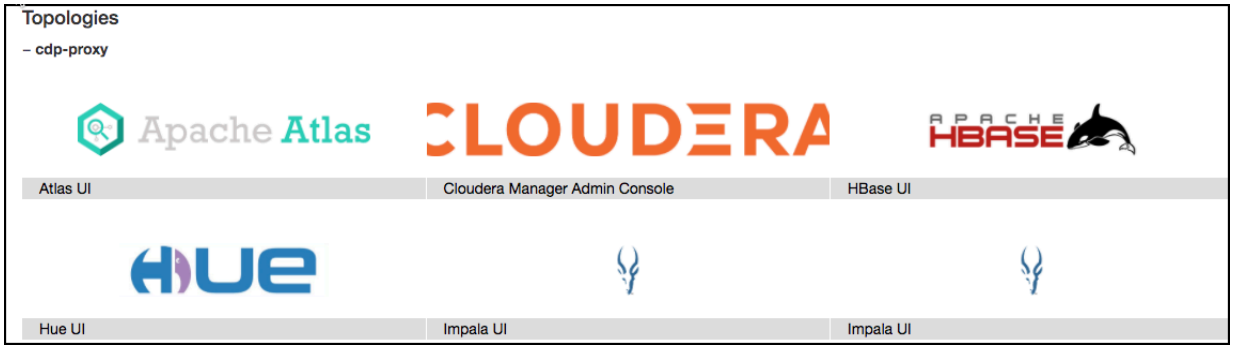


    The Knox Gateway UI is displayed.

17. On the **General Proxy Information** page, expand the CDP Proxy topology by clicking + cdp-proxy under Topologies.

    The list of services that are configured with the cdp-proxy topology is displayed.

18. Click on the Hue logo.



    You should be able to log in to the Hue web UI.

    You can also log into Hue using the following URL:

```
https://[***HOSTNAME***]:[***PORT***]/gateway/cdp-proxy/hue/
```

19. Go to Clusters Knox Configuration and add the following entries in the Knox Simplified Topology Management - cdp-proxy field:

```
HUE:httpclient.socketTimeout=[***TIMEOUT-IN-MINUTES***]
```

```
HUE:httpclient.connectionTimeout=[***TIMEOUT-IN-MINUTES***]
```

    Replace *[***TIMEOUT-IN-MINUTES***]* with the actual timeout value depending on the load on your load on the cluster or environment. For example, to set a timeout of 20 minutes, specify 20m. The default timeout value is 5m.

    Note: This step is required to prevent query timeouts, and if you are seeing errors such as “Results have expired, rerun the query if needed” in the Hue logs.

20. Restart the Knox service.

Authenticating Cloudera Data Explorer (Hue) users with PAM

You can use Pluggable Authentication Modules (PAM) for authentication in Data Explorer.

Procedure

1. Log in to Cloudera Manager as an Administrator.
2. Go to Clusters Hue Configuration and select desktop.auth.backend.PamBackend from the Authentication Backend drop-down menu.

   The default value of the PAM Backend Service Name property is “login”.

   Note: On RHEL 9, you must change the value of PAM Backend Service Name to sshd.
3. Click Save Changes.
4. Restart the Hue service.

Applications and permissions reference

Data Explorer is a web-based UI for several cluster services that you can access by using Data Explorer applications and their associated permissions.

Data Explorer applications

These Cloudera services are available in Data Explorer. Currently, Spark is only available in the upstream version of Data Explorer.

Data Explorer Application	Application Dependencies
HBase	HBase Browser
HDFS	Core, File Browser
Hive	Metastore Tables, Hive Editor
Impala	Metastore Tables, Impala Editor
MapRed / YARN	Job Browser, Job Designer, Oozie, Hive Editor, Pig, Sqoop
Oozie	Job Designer, Oozie Editor/Dashboard
Solr (Search)	Hadoop Security
Spark	Spark

Data Explorer application permissions

Data Explorer application permissions are composed of name.permission:action.

For example, filebrowser.access:Launch this application(3)

In this example:

- filebrowser = Data Explorer application name
- access = Execute permissions
- Launch this application = Action that is enabled
- (3) = Process ID of the filebrowser application in the Data Explorer database

Data Explorer Application	Permission	Read/Write/Execute	Action Description
about	access	execute	Launch this application
beeswax	access	execute	Launch this application
dashboard	access	execute	Launch this application
filebrowser	access	execute	Launch this application

Data Explorer Application	Permission	Read/Write/Execute	Action Description
filebrowser	s3_access	execute	Access to S3 from filebrowser and filepicker
filebrowser	adls_access	execute	Access to ADLS from filebrowser and filepicker
filebrowser	abfs_access	execute	Access to ABFS from filebrowser and filepicker
filebrowser	gs_access	execute	Access to GS from filebrowser and filepicker
help	access	execute	Launch this application
hive	access	execute	Launch this application
impala	access	execute	Launch this application
indexer	access	execute	Launch this application
jobbrowser	access	execute	Launch this application
jobsub	access	execute	Launch this application
kafka	access	execute	Launch this application
metadata	access	execute	Launch this application
metadata	write	write	Allow edition of metadata like tags
metastore	access	execute	Launch this application
metastore	write	write	Allow DDL operations. Need the app access too
notebook	access	execute	Launch this application
oozie	access	execute	Launch this application
oozie	dashboard_jobs_access	execute	Oozie Dashboard read-only user for all jobs
oozie	disable_editor_access	execute	Disable Oozie Editor access
proxy	access	execute	Launch this application
rdbms	access	execute	Launch this application
search	access	execute	Launch this application
useradmin	access_view:useradmin:edit_user	read/write/execute	Access to profile page on User Admin
useradmin	access_view:useradmin:view_user	read/write/execute	Access to any profile page on User Admin
useradmin	access	execute	Launch this application

Securing Cloudera Data Explorer (Hue) passwords with scripts

You can secure passwords in Data Explorer by using one consolidated script, or multiple individual scripts. Data Explorer runs each password script at startup and extracts passwords from stdout.

About this task

Store scripts in a directory that only Data Explorer can read, write, and execute. You can choose password script names but you cannot change hue.ini property names to which you assign those scripts. Add the suffix _script to any password property and set it equal to the script name.

Procedure

1. At the command line, create one or more password scripts. For example, create a consolidated script named my_passwords_script.sh:

```
#!/bin/bash
SERVICE=$1
if [[ ${SERVICE} == "ldap_password" ]]
then
 echo "<YOUR_LDAP_PASSWORD>"
fi

if [[ ${SERVICE} == "ssl_password" ]]
then
 echo "<YOUR_SSL_PASSWORD>"
fi

if [[ ${SERVICE} == "bind_password" ]]
then
 echo "<YOUR_BIND_PASSWORD>"
fi

if [[ ${SERVICE} == "db_password" ]]
then
 echo "<YOUR_DATABASE_PASSWORD>"
fi
```

2. Log on to Cloudera Manager and go to Hue Configuration .
3. Search on Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini.
4. Add script properties. In the following example, the required _script is added to the password property:

```
[desktop]
ldap_username=hueservice
ldap_password_script="/var/lib/hue/password_script.sh ldap_password"
ssl_password_script="/var/lib/hue/password_script.sh ssl_password"

[[ldap]]
bind_password_script="/var/lib/hue/password_script.sh bind_password"
[[database]]
db_password_script="/var/lib/hue/password_script.sh db_password"
```

5. Click Save Changes and Restart Hue.

Directory permissions when using PAM authentication backend

If you are using Pluggable Authentication Modules (PAM) for authenticating Data Explorer users, then ensure that the Data Explorer users have access to the /etc/shadow directory. Use an approach suitable to your organization's security policies.

Making Data Explorer application user a member of the shadow group

This approach involves creating a “shadow” group and adding Data Explorer to this group. Then you must grant the “shadow” group, read permission to the /etc/shadow directory.

Using Access Contol Lists (Recommended)

You can use Linux's ACLs to permit Data Explorer user a read permission to the /etc/shadow directory by using the `setfacl` command. Cloudera recommends this approach.

Configuring TLS/SSL for Cloudera Data Explorer (Hue)

You can independently enable TLS/SSL for Data Explorer.

Cloudera recommends that your cluster and the Data Explorer service use Kerberos for authentication. If you enable TLS/SSL for a cluster that has not been configured to use Kerberos, a warning is displayed. You should integrate the cluster with your Kerberos deployment before proceeding.

Creating a truststore file in PEM format

You must create the Data Explorer Truststore by consolidating certificates of all SSL-enabled servers (or a single CA Certificate chain) that Data Explorer communicates with into one file. This generally includes certificates of all the Oozie, HDFS, MapReduce, and YARN daemons, and any other SSL-enabled services.

About this task

Server certificates are stored in Java KeyStore (JKS) format. The Data Explorer Truststore must be in the Privacy Enhanced Mail (PEM) format whereas other services use the JKS format by default. To create the Data Explorer truststore, extract each certificate from Hadoop's Java Keystore with the Java keytool, convert the certificate to PEM format with the OpenSSL.org openssl tool, and then add it to the Data Explorer truststore:

Procedure

1. Extract the certificate from the keystore of each TLS/SSL-enabled server with which Data Explorer communicates. For example, if you have hadoop-server.keystore that contains a server certificate, foo-1.example.com with a password of example123, you would use the following keytool command:

   ```
   keytool -exportcert -keystore hadoop-server.keystore -alias foo-1.example.com -storepass example123 -file foo-1.cert
   ```

2. Convert each certificate into a PEM file. Here is what the openssl tool command looks like for the foo-1.cert file that was extracted in Step 1:

   ```
   openssl x509 -inform der -in foo-1.cert > foo-1.pem
   ```

3. Concatenate all the PEM certificates you extracted and converted from the server truststore into one PEM file:

   ```
   cat foo-1.pem foo-2.pem foo-N.pem ... > hue_truststore.pem
   ```

   Concatenate the certificate files in the following order: SSL certificate followed by intermediate certificate, followed by the root CA certificate.

   Important: Ensure the final PEM truststore is deployed in a location that is accessible by the Data Explorer service.

4. Log in to Cloudera Manager as an Administrator.

5. Go to Clusters Hue Configuration and add the following line in the Hue Service Environment Advanced Configuration Snippet (Safety Valve) field:

```
REQUESTS_CA_BUNDLE=[***PATH-TO-HUETRUST.PEM-FIL E***]
```

6. Click Save Changes.
7. Restart the Data Explorer service.

Configuring Cloudera Data Explorer (Hue) as a TLS/SSL client

Data Explorer acts as a TLS/SSL client when communicating with other services, such as core Hadoop, HBase, Oozie, and cloud providers like Amazon S3 or Azure.

To act as a TLS/SSL client, Data Explorer must authenticate HDFS, MapReduce, YARN daemons, the HBase Thrift server, and so on. To do this, Data Explorer needs to have the certificate chains of these components' hosts in the Data Explorer trust store.

The Data Explorer truststore is a single PEM (Privacy Enhanced Mail) file that contains the certificate authority (CA) root certificate and all intermediate certificates to authenticate the certificate installed on each TLS/SSL-enabled server. These servers host the services with which Data Explorer communicates.

Note: A certificate is specific to a host. It is signed by a CA and tells the requesting client, which is Data Explorer in this case, that the host is the same one as is represented by the host public key. Data Explorer uses a chain of signing authority in its truststore to validate the CA that signed the host certificate.

Enabling Cloudera Data Explorer (Hue) as a TLS/SSL client

After you create a Data Explorer truststore file in PEM format, you can configure Data Explorer as a TLS/SSL client by using Cloudera Manager.

Procedure

1. Log in to Cloudera Manager as an Administrator.
2. Go to Clusters Hue service Configuration Hue TLS/SSL Server CA Certificate (PEM Format) ssl_cacerts and add the path to the *HUE_TRUSTSTORE*.pem file on the host that is running the Data Explorer web server.
3. Click Save Changes.
4. Restart the Data Explorer service.

Configuring Cloudera Data Explorer (Hue) as a TLS/SSL server

Data Explorer and other Python-based services expect certificates and keys to be stored in PEM (Privacy Enhanced Mail) format.

Before you enable TLS/SSL for the Data Explorer server, you must generate a private key and certificate by using the openssl command-line tool and reuse a host's existing Java keystore by converting it to the PEM format.

Enabling Cloudera Data Explorer (Hue) as a TLS/SSL server using Cloudera Manager

You can use Cloudera Manager to enable TLS/SSL for the Data Explorer server.

Procedure

1. Log in to Cloudera Manager as an Administrator.

2. Go to Clusters Hue service Configuration and filter by SCOPE Hue Server and CATEGORY Security .
3. Edit the following Data Explorer TLS/SSL properties according to your cluster configuration:
   - Enable TLS/SSL for Hue: Select the check box to encrypt communication between clients and Data Explorer with TLS/SSL.
   - Hue TLS/SSL Server Certificate File (PEM Format) ssl_certificate: Specifies the path to the TLS/SSL certificate on the host that is running the Data Explorer web server.

     Ensure that you include the complete chain in the ssl_certificate PEM file.

     The order of the certificates should be as follows from the top to bottom: server, intermediate, root.

     If there are multiple intermediate CA certificates, then you must add them in the correct order. For example:

     ```
     Subject: CN=Hue Server Certificate
     Issuer: CN=Intermediate 2

       Subject: CN=Intermediate 2
       Issuer: CN=Intermediate 1

         Subject: CN=Intermediate 1
         Issuer: CN=RootCA

           Subject: CN=RootCA
           Issuer: CN=RootCA
     ```
   - Hue TLS/SSL Server Private Key File (PEM Format) ssl_private_key: Specifies the path to the TLS/SSL private key on the host running the Data Explorer web server.
   - Hue TLS/SSL Private Key Password ssl_password: Specifies the password for the private key in the Data Explorer TLS/SSL Server Certificate and Private Key file.
   - Hue TLS/SSL Server CA Certificate (PEM Format) ssl_cacerts: Specifies the path to the TLS/SSL certificate authority root certificate on the host that is running the Data Explorer web server.
4. Add the path to the certificate chain PEM file in [desktop] section of the Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini field:

   ```
   [desktop]
   ssl_certificate_chain=/[***PATH***]/[***TO***]/[***FULL-CHAIN***].pem
   ```
5. Click Save Changes.
6. Select Actions Restart to restart the Data Explorer service.

What to do next

Change the permissions for Data Explorer to read the certificates after you have enabled TLS/SSL as follows:

```
chmod 644 [***PATH-WHERE-SSL-FILES-FOR-HUE-ARE-LOCATED***]
```

Enabling TLS/SSL for Cloudera Data Explorer (Hue) Load Balancer

To configure the Data Explorer Load Balancer to use HTTPS or operate as a TLS/SSL server, you need a self-signed SSL certificate and a private key file. If the private key file is password protected, then you must configure the Data Explorer Load Balancer to use the corresponding key password.

Procedure

1. Log in to Cloudera Manager as an Administrator.
2. Go to Clusters Hue service Configuration Scope Load Balancer .

3. Enter the location of the file that contains the server certificate key for TLS/SSL on the host running Data Explorer Load Balancer in the Hue Load Balancer TLS/SSL Server Certificate File (PEM Format) field.

   The certificate file must be in the Privacy-Enhanced Mail (PEM) format.
4. Enter the location of the TLS/SSL file that contains the private key used for TLS/SSL on the host running Data Explorer Load Balancer, in the Hue Load Balancer TLS/SSL Server Private Key File (PEM Format) field.

   The certificate file must be in PEM format.
5. (Optional) If the private key file is password protected perform the following steps:
   a) Create a password file in your chosen security directory and insert the private key password as shown in the following example:

   ```
   echo "abc123" > /etc/security/password.txt
   ```

   Where abc123 is the private key password and password.txt is the password file.
   b) Set the file ownership and permissions as shown in the following example:

   ```
   chown hue:hue password.txt
   chmod 700 password.txt
   ```

   c) Enter the path to the file containing the passphrase used to encrypt the private key of the Data Explorer Load Balancer server in the Hue Load Balancer TLS/SSL Server SSLPassPhraseDialog field.
6. Click Save Changes.
7. Restart the Data Explorer service.

Enabling TLS/SSL communication with HiveServer2

For Data Explorer to communicate with HiveServer2 using TLS/SSL, Data Explorer needs the Hive certificate and certificate chain.

To enable TLS/SSL communication with HiveServer2, add the following properties in the [beeswax] section under [[ssl]] in the Cloudera Manager Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini configuration property:

Property	Description

`[beeswax]`
`[[ssl]]`
`enabled`
	Valid values: true | false
	Enables or disables TLS/SSL communication for this server.
	Default setting: false
	Example: enabled=true

`[beeswax]`
`[[ssl]]`
`cacerts`
	Valid values: directory path
	Specifies the path to the Certificate Authority certificates.
	Default setting: /etc/hue/cacerts.pem
	Example: cacerts=/opt/cloudera/security/CAcerts/cacerts

`[beeswax]`
`[[ssl]]`
`validate`
	Valid values: true | false
	Specifies whether Data Explorer validates certificates received from the server.
	Default setting: true
	Example: validate=true

Enabling TLS/SSL communication with Impala

For Data Explorer to communicate with Impala using TLS/SSL, Data Explorer needs the Impala certificate and certificate chain.

To enable TLS/SSL communication with Impala, add the following properties in the [impala] section under [[ssl]] in the Cloudera Manager Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini configuration property:

Property	Description

`[impala]`
`[[ssl]]`
`enabled`
	Valid values: true | false
	Enables or disables TLS/SSL communication for this server.
	Default setting: false
	Example: enabled=true

`[impala]`
`[[ssl]]`
`cacerts`
	Valid values: directory path
	Specifies the path to the Certificate Authority certificates.
	Default setting: /etc/hue/cacerts.pem
	Example: cacerts=/opt/cloudera/security/CAcerts/cacerts

`[impala]`
`[[ssl]]`
`validate`
	Valid values: true | false
	Specifies whether Data Explorer validates certificates received from the server.
	Default setting: true
	Example: validate=true

Securing database connections with TLS/SSL

Data Explorer uses different clients to communicate with each database internally. Client-specific options, such as secure connectivity can be configured using Cloudera Manager.

Procedure

1. Log in to Cloudera Manager as an administrator.
2. Go to Clusters Hue service Configuration and add the following section in the Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini field:

```
[desktop]
  [[database]]
    …
    options={"ssl":{"ca":"/tmp/ca-cert.pem"}}
```

   This identifies the Certificate Authority (CA) certificate for the backend database. You can also identify public and private keys as follows:

```
options='{"ssl": {"ca": "/tmp/newcerts2/ca.pem", "key": "/tmp/newcerts2/
client-key.pem", "cert": “/tmp/newcerts2/client-cert.pem"}}'
```

3. Click Save Changes.
4. Restart the Data Explorer service.

Disabling CA Certificate validation from Cloudera Data Explorer (Hue)

By default, Data Explorer validates CA Certificates for Oozie, HTTPFS, Resource Manager, and Job History Server when SSL is enabled for any of these services. If you have not enabled TLS/SSL on your cluster, then you can disable Data Explorer from validating the CA Certificates for other services on your Cloudera cluster.

Procedure

1. Log in to Cloudera Manager as an Administrator.

2. Go to Clusters Hue Configuration and add the following lines in the Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini field:

```
[hadoop]
[[hdfs_clusters]]
[[[default]]]
ssl_cert_ca_verify = False #HTTPFS service
[[yarn_clusters]]
[[[default]]]
ssl_cert_ca_verify = False #Resource Manager/Job History Server
[[[ha]]]
ssl_cert_ca_verify = False #Resource Manager HA
[liboozie]
ssl_cert_ca_verify = False
```

3. Click Save Changes.
4. Restart the hue service.

Securing sessions

Securing the Data Explorer sessions ensures that authenticated user access remains protected throughout the lifetime of the web sessions. Additionally, when a Data Explorer session expires, the screen blurs and the user automatically logs out the web interface.

Session timeout

User sessions are controlled with the ttl (time-to-live) property, which is set in the Cloudera Manager Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini property as follows:

```
[desktop]
     [[session]]
     ttl=[***NUMBER-OF-SECONDS***]
```

The default setting for ttl is 1,209,600 seconds, which equals two weeks. The ttl property determines the length of time that the cookie with the user's session ID lives before expiring. After the ttl setting is reached, the user's session expires whether it is active or not.

Idle session timeout

Idle sessions are controlled with the idle_session_timeout property, which is set in the Cloudera Manager Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini property as follows:

```
[desktop]
     [[auth]]
     idle_session_timeout=[***NUMBER-OF-SECONDS***]
```

Sessions expire that are idle for the number of seconds set for this property. For example, if you set idle_session_tim eout=900, sessions expire after being idle for 15 minutes. You can disable the property by setting it to a negative value, like idle-session_timeout=-1.

Secure session login

Session login properties are set under the [desktop] [[auth]] section in the Cloudera Manager Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini property as follows:

```
[desktop]
     [[auth]]
```

```
[***SET-SESSION-LOGIN-PARAMETERS-HERE***]
```

Note: These configuration settings are based on django-axes 1.5.0.

Use the following properties to configure session login behavior:

change_default_password	**Valid values**Valid values: true | false
	If this property is set to true, users must change their passwords on first login attempt.
	Example:
	`[desktop]`
	`[[auth]]`
	`change_default_password=true`
	To use this property, you must enable the AllowFirstUserDjangoBackend in Data Explorer. For example:
	`[desktop]`
	`[[auth]]`
	`backend=desktop.auth.backend.AllowFirstUserDjangoBackend`

expires_after	Use this property to configure the number of seconds after logout that user accounts are disabled. For example, user accounts are disabled 900 seconds or 15 minutes after logout with the following configuration:
	`[desktop]`
	`[[auth]]`
	`expires_after=900`
	If you set this property to a negative value, user sessions never expire. For example, expires_after=-1.

expire_superusers	Use to expire superuser accounts after the specified number of seconds after logout. For example, expire_superusers=900 causes superuser accounts to expire 15 minutes after logging out.
login_cooloff_time	Sets the number of seconds after which failed logins are forgotten. For example, if you set login_cooloff_time=900, a failed login attempt is forgotten after 15 minutes.
login_failure_limit	Sets the number of login attempts allowed before a failed login record is created. For example, if you set login_failure_limit=3, a failed login record is created after 3 login attempts.
login_lock_out_at_failure	**Valid values**: true | false If set to true: • The IP address that is attempting to log in is locked out after exceeding the limit set for login_failure_limit. • If login_lock_out_by_combination_user_and_ip is also set to true, both the IP address and the user are locked out after exceeding the limit set for login_failure_limit. • If login_lock_out_use_user_agent is also set to true, both the IP address and the agent application (such as a browser) are locked out after exceeding the limit set for login_failure_limit.
login_lock_out_by_combination_user_and_ip	**Valid values**: true | false If set to true, both the IP address and the user are locked out after exceeding the limit set for login_failure_limit.
login_lock_out_use_user_agent	**Valid values**: true | false If set to true, the agent application (such as a browser) is locked out after exceeding the limit set for login_failure_limit.

Secure session cookies

Session cookie properties are set under the [desktop] [[session]] section in the Cloudera Manager Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini property as follows:

```
[desktop]
     [[session]]
     [***SET-SESSION-COOKIE-PROPERTIES-HERE***]
```

Use the following properties to configure session cookie behavior:

secure	**Valid values**: true | false
	If this property is set to true, the user session ID is secured.
	Important: To use this property, HTTPS must be enabled.
	Example:
	`[desktop]`
	`[[session]]`
	`secure=true`
	By default this property is set to false.

http_only	**Valid values**: true | false
	If this property is set to true, the cookie with the user session ID uses the HTTP only flag.
	Example:
	`[desktop]`
	`[[session]]`
	`http_only=true`
	Important: If the HttpOnly flag is included in the HTTP response header, the cookie cannot be accessed through a client side script.
	By default this property is set to true.

expire_at_browser_close	**Valid values**: true | false
	If this property is set to true, only session-length cookies are used. Users are automatically logged out when the browser window is closed.
	Example:
	`[desktop]`
	`[[session]]`
	`expire_at_browser_close=true`
	By default this property is set to false.

Session security and validation

Session security is set to moderate by default. You can configure the security validation strictness based on your environment requirements. Use the following properties in the [desktop][[session]] section to define session security behavior:

same_site	**Valid values**: Strict | Lax | None **Default value**: Lax Specifies the SameSite attribute for session cookies to prevent Cross-Site Request Forgery (CSRF). • Lax: Provides CSRF protection while allowing SAML and OIDC authentication flows. • Strict: Provides maximum security by ensuring cookies are only sent in a first-party context. This setting can prevent SAML or OIDC authentication from functioning correctly. • None: Disables SameSite protection. If you use this setting, you must also set the secure property to true.

session_validation_mode	**Valid values**: strict | moderate | moderate_vpn | permissive | off
	Default value: moderate
	Specify the strictness of session validation to prevent session hijacking.
	• strict : Set to require an exact IP address and User-Agent match. This provides the highest level of security.
	• moderate Set to require a subnet and User-Agent family match with a grace period.
	• moderate_vpn: Set to use a wider subnet match. This is intended for environments where users access the system through a Virtual Private Network (VPN).
	• permissive: Set to validate the User-Agent only and enable audit logging.
	• off: Set to disable session validation.
	Example for disabling security validation
	`[desktop]`
	`[[session]]`
	`session_validation_mode=off`

Session_ip_validation	**Valid values**: true | false **Default value**: true Enables IP address validation for sessions. • true : Set this property, Hue validates that the incoming request IP address matches the session's original IP address. • false: Set to disable the IP validation
Session_ip_subnet_bits	**Valid values**: 8 | 16 | 24 | 32 **Default value**: 24 Defines the number of bits used for IP subnet mask validation. • 32: Set to require an exact IP address match for the session. • 24 : Set to validate the session against a /24 subnet. This ensures the user remains on the same network. • 16 : Set to validate the session against a /16 subnet. This allows for a wider range of IP addresses, such as in environments with a Virtual Private Network (VPN). • 8 : Set to validate the session against an /8 subnet
session_user_agent_validation	**Valid values**: true | false **Default value**: true Enables User-Agent validation for sessions to protect against session hijacking from different browsers or devices. • true : Set to validate the User-Agent string of the client. Ensures that the browser or device identity remains consistent throughout the session. • false: Set to disable the user agent validation.
session_user_agent_match	**Valid values**: exact | family **Default value**: family Sets the strictness of the User-Agent matching process. • exact: Set to require an exact match of the User-Agent string. This ensures that the session is restricted to the specific browser version and operating system used at login. • family: Set to match only the browser family, such as Chrome or Firefox. This allows for minor browser updates or sub-version changes without invalidating the session

session_allow_ip_changes	**Valid values**: -1 to Number **Default value**: 1 Defines the maximum number of IP address changes allowed within the grace period before the system requires re-authentication. • -1: Set to allow an unlimited number of IP address changes. • 0: Set to prevent any IP address changes. This requires you to re-authenticate if your IP address changes. • 1: Set to allow one IP address change. This is the default setting and is intended to support users on a Virtual Private Network (VPN).
session_ip_change_grace_period	**Valid values**: seconds **Default value**: 300 Defines the grace period, in seconds, for IP address changes. This period allows for network transitions, such as connecting to or disconnecting from a Virtual Private Network (VPN), without requiring you to log in again immediately. For example, the default setting is 300 seconds. After this period expires, any detected IP address change requires you to re-authenticate.
session_rotation_on_ip_change	**Valid values**: true | false **Default value**: true Determines whether to generate a new session ID when an IP address change is detected. • true: Set to rotate the session ID when an IP address change occurs. This is the preferred setting for higher security. • false: Set to disable the session IP address rotation.
session_security_audit_log	**Valid values**: true | false **Default value**: true Enables detailed audit logging for session security events. • true: Set to record detailed audit logs for events such as IP address changes and validation failures. Data Explorer writes these logs to the Data Explorer security log. • false: Set to disable detailed audit logging for session security events.

Specifying HTTP request methods

You can specify the HTTP request methods that the Data Explorer server responds to.

Use the http_allowed_methods property under the [desktop] section in the Cloudera Manager Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini property.

By default, the http_allowed_methods property is set to options, get, head, post, put, delete, connect.

Restricting supported ciphers for Cloudera Data Explorer (Hue)

You can configure the list of ciphers that Data Explorer supports with HTTPS.

Use the ssl_cipher_list property under the [desktop] section in the Cloudera Manager Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini property:

```
[desktop]
ssl_cipher_list=[***LIST-OF-ACCEPTED-CIPHERS***]
```

By default, the ssl_cipher_list property is set to !aNULL:!eNULL:!LOW:!EXPORT:!SSLv2. Specify ciphers using the cipher list format described at OpenSSL Cryptograpy and SSL/TLS Toolkit Manpages by selecting the SSL version, and then going to Commands ciphers .

Specifying domains or pages to which Cloudera Data Explorer (Hue) can redirect users

You can restrict the domains or pages to which Data Explorer can redirect users.

Use the redirect_whitelist property under the [desktop] section in the Cloudera Manager Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini property:

```
[desktop]
redirect_whitelist=[***REDIRECT-URL***]
```

Specify the redirect_whitelist value with a comma-separated list of regular expressions that match the redirect URL. For example, to restrict redirects to your local domain and fully-qualified domain name (FQDN), use the following value:

```
redirect_whitelist=^\/.*$,^http:\/\/www.mydomain.com\/.*$
```

Securing Cloudera Data Explorer (Hue) from CWE-16

Data Explorer may have allowed external domains such as doubleclick.net, .googletagmanager.com, or *.google-analytics.com to run JavaScript scripts, for certain URLs in the Content Security Policy (CSP) headers. This may lead to Common Weakness Enumeration (CWE-16). To secure Hue from CWE-16 class of weaknesses, you can add the X-Content-Type-Options response HTTP header and prevent attacks based on MIME-type confusions in Hue's Advanced Configuration Snippet using Cloudera Manager.

Procedure

1. Log in to Cloudera Manageras an Administrator.
2. Go to Clusters Hue Configuration and add the following lines in the Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.in field:

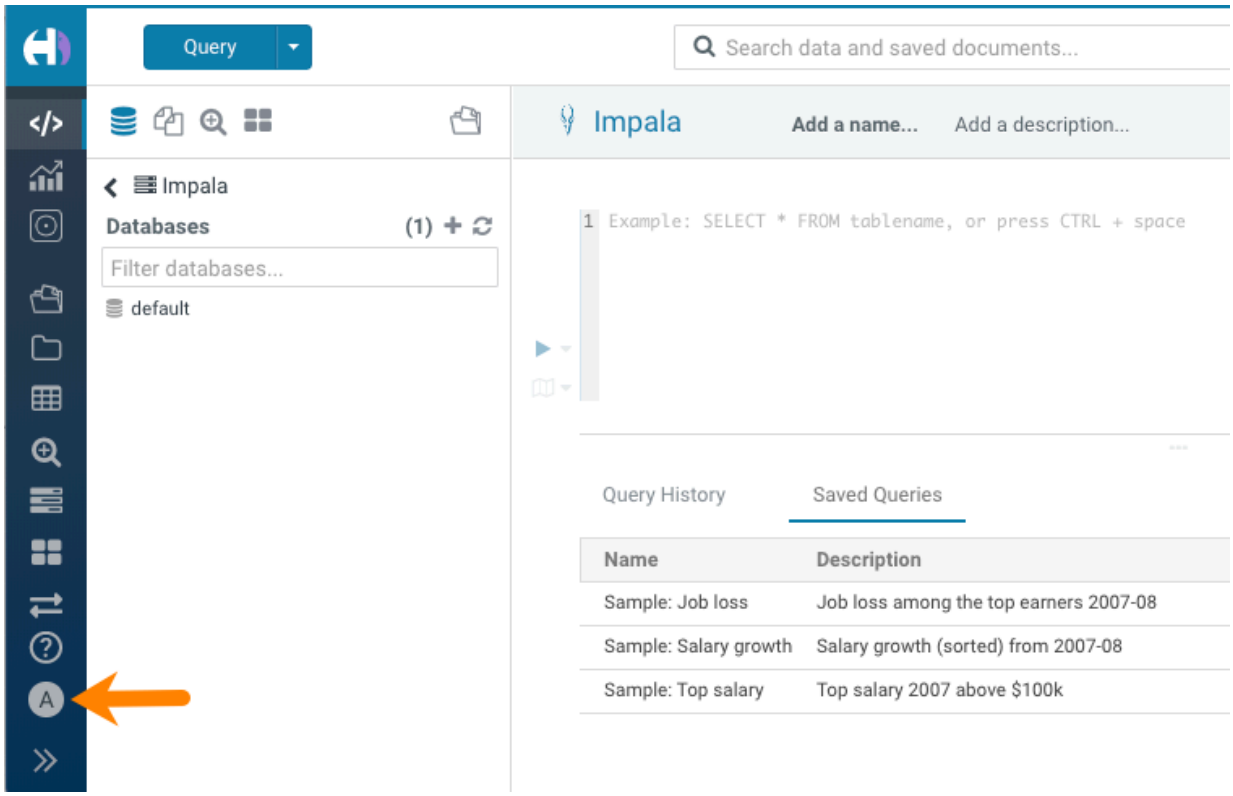
   ```
   [desktop]
   # X-Content-Type-Options: nosniff This is an HTTP response header
   # feature that helps prevent attacks based on MIME-type confusion.

   secure_content_security_policy="script-src 'self' 'unsafe-inline' 'unsafe-
   eval' *.googletagmanager.com *.doubleclick.net data:;img-src 'self' *.doub
   leclick.net http://*.tile.osm.org *.tile.osm.org *.gstatic.com data:;sty
   le-src 'self' 'unsafe-inline' fonts.googleapis.com;connect-src 'self' *.
   google-analytics.com;frame-src *;child-src 'self' data: *.vimeo.com;obje
   ct-src 'none'"
   ```
3. Click Save Changes.
4. Restart the Hue service.

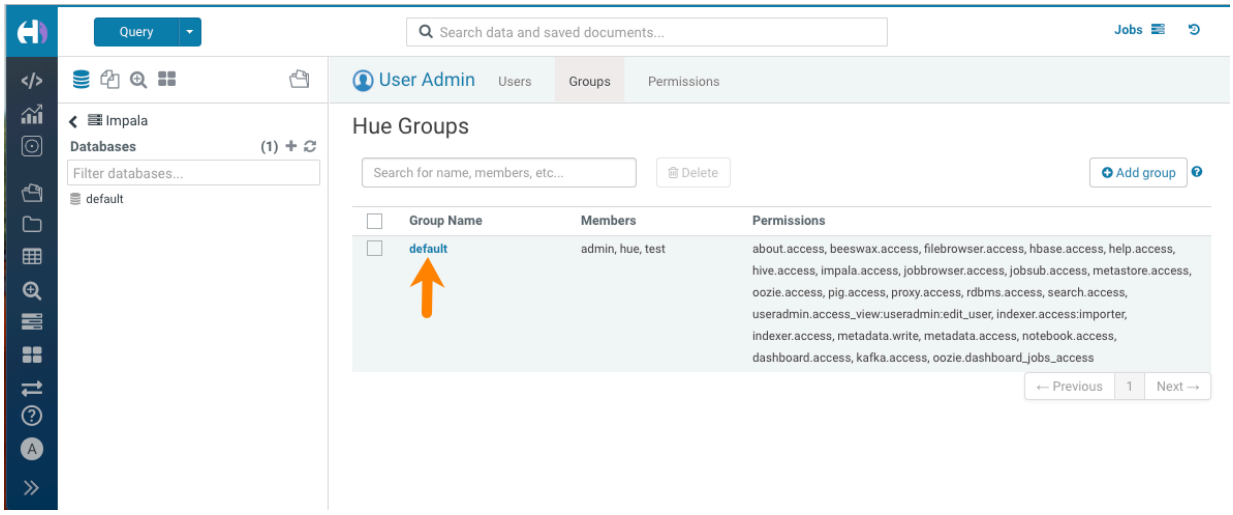
Setting Oozie permissions

You can control access to the Oozie dashboard and editor by using controls in the Data Explorer Web UI.

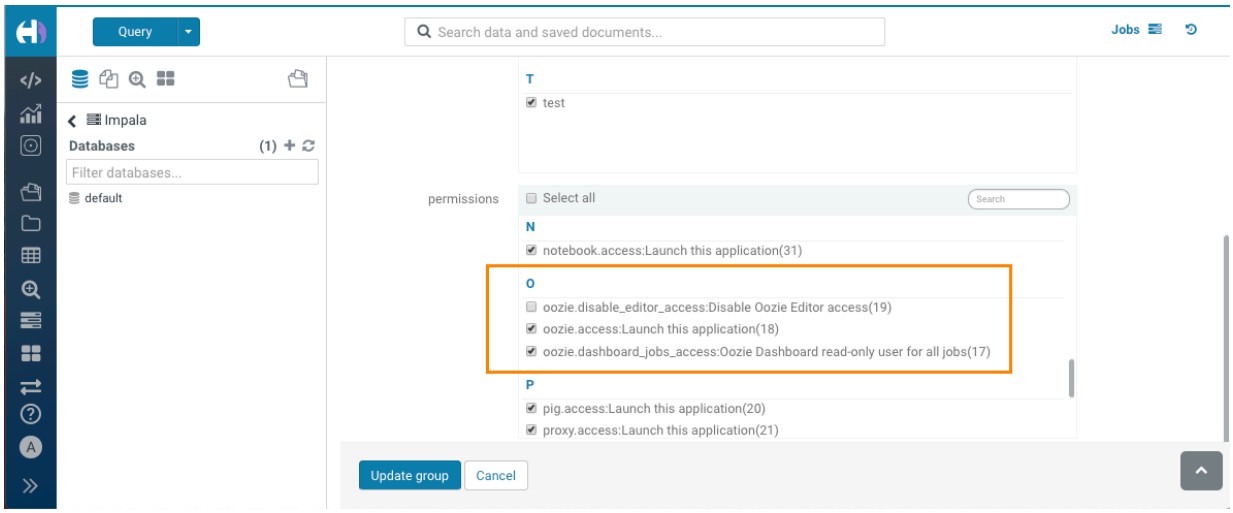
1. On the Cloudera Manager home page, click the Hue service.
2. On the Hue service page, select Web UIHue Load Balanced - recommended .
3. Log in to the Hue Web UI.
4. In the Hue Web UI, click the admin menu icon in the lower part of the left menu and select Manage Users:



5. On the User Admin page, click the Groups tab.
6. On the Hue Groups page, in the Group Name column, click the default group.



7. On the Hue Groups - Edit group page, scroll down to locate the list of permissions and then scroll further to locate the Oozie permissions:



Groups property in UI	Description
oozie.disable_editor_access	Disables access to the Oozie editor for the selected groups Default setting: Unchecked, which disables this permission.
oozie.access	Enables access to the Oozie editor in Hue. Default setting: Checked, which enables access to the Oozie editor.
oozie.dashboard_jobs_access	Enables read-only access for all jobs in the Oozie dashboard. Default setting: Check, which enables this permission.

8. Check or uncheck the permissions as needed and then click Update group to save the permission change.

Configuring secure access between Solr and Cloudera Data Explorer (Hue)

If you are using Solr (search) to build dynamic search dashboards and explore data from the Data Explorer web UI, and have secured your Cloudera cluster using Kerberos, then you must enable secure access between the Solr service and Data Explorer by turning on the security_enabled parameter in the hue_safety_valve.ini file.

About this task

The security_enabled parameter is set to false, by default. To enable secure access between Solr and Data Explorer:

Procedure

1. Sign in to Cloudera Manager as an Administrator.
2. Go to Clusters Hue service Configuration and search for the Hue Service Advanced Configuration Snippet (Safety Valve) for hue_safety_valve.ini field.
3. Go to the [search] section and set the value of the security_enabled parameter to true, as shown in the following sample:

```
[search]
# Requires FQDN in solr_url if enabled
security_enabled=true
# URL of the Solr Server
```

```
solr_url=http://[***FQDN-SOLR-HOST***]:8983/solr
```

Note: If you set security_enabled=true, then you must provide the fully-qualified domain name of the Solr host in the Solr URL.

4. Click Save Changes.
5. Restart the Hue service.