

## mod19\_ex02: Configuring Ranger

The purpose of this exercise is to make configuration changes to bring Ranger online. This will include configuring Ranger Usersync to import users from LDAP, assigning Ranger administrative internal and external administrative users, and in configuring a Ranger policy to support Ranger auditing.

### Reference Information

- TBD

1. Open a Mate terminal as the user training.



```
Mate Terminal
File Edit View Search Terminal Help
training@cmhost:~$
```

2. Configure SSSD to support Ranger Usersync.

Ranger usersync will synchronize users and groups from the ID provider, UNIX and LDAP in this case. SSSD is able to cache the list of users and groups for Usersync. The enumerate property will source all available users and groups from LDAP and cache them onto the local machine. From this cache usersync will synchronize the Ranger database.

2.1 Use the ssh command to reach the host edge.example.com.



```
Mate Terminal
File Edit View Search Terminal Help
training@cmhost:~$ ssh edge.example.com
```

```
$ ssh edge.example.com
```

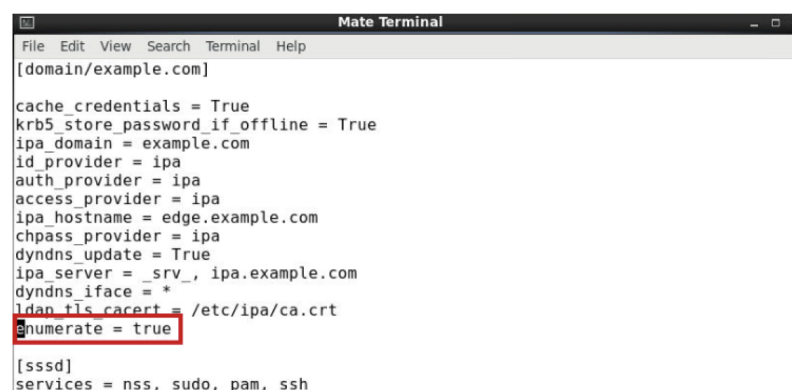
2.2 Use a text editor to open the sssd.conf file.



```
Mate Terminal
File Edit View Search Terminal Help
training@edge:~$ sudo vim /etc/sss/sss.conf
```

```
$ sudo vim /etc/sss/sss.conf
```

2.3 In the [domain/example.com] add the property enumerate = true. Save and quite the configuration file.



```
Mate Terminal
File Edit View Search Terminal Help
[domain/example.com]

cache_credentials = True
krb5_store_password_if_offline = True
ipa_domain = example.com
id_provider = ipa
auth_provider = ipa
access_provider = ipa
ipa_hostname = edge.example.com
chpass_provider = ipa
dyndns_update = True
ipa_server = _srv_, ipa.example.com
dyndns_iface = *
ldap_tls_cacert = /etc/ipa/ca.crt
enumerate = true

[sss]
services = nss, sudo, pam, ssh
```

```
enumerate = true
```

2.4 Use the `systemctl` command to restart the `sssd` daemon. SSSD will locally cache all users and groups from LDAP. Within one minute Usersync will collect and write these users and groups into the Ranger database.

```
Mate Terminal
File Edit View Search Terminal Help
training@edge:~$ sudo systemctl restart sssd
training@edge:~$
```

```
$ sudo systemctl restart sssd
```

3. Login into Cloudera Manager as the administrative user, `allan_admin`.

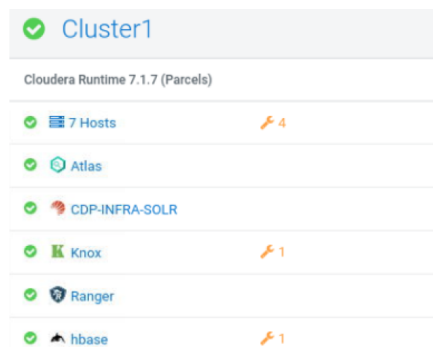
3.1 Login into Cloudera Manager as the administrative user, `allan_admin`.

---

☐ Remember me

4. Verify the Ranger authentication method.

4.1 From Cloudera Manager Home select Ranger. Select Configuration.



4.2 Search for "auth". Ranger Admin authentication is automatically configured during the install. Admin Authentication Method should be set to PAM. The Admin UNIX Auth Remote login should be checked. And the Admin UNIX Auth Service Hostname should be set to the variable `{{(RANGER_USERSYNC_HOST)}}`.

The screenshot shows the Ranger Admin configuration interface for the 'auth' search. On the left, there are filters for SCOPE and CATEGORY. The main configuration area is divided into three sections:

- Admin Authentication Method:** The property `ranger.authentication.method` is set to `ranger_authentication_method`. The default group is 'Ranger Admin Default Group'. The options are:
  - ☐ UNIX
  - ☐ LDAP
  - ☐ ACTIVE\_DIRECTORY
  - ☒ PAM
  - ☐ NONE
- Admin UNIX Auth Remote Login:** The property `ranger.unixauth.remote.login.enabled` is set to `ranger.unixauth.remote.login.enabled`. The default group is 'Ranger Admin Default Group'. The option is:
  - ☒ Ranger Admin Default Group
- Admin UNIX Auth Service Hostname:** The property `ranger.unixauth.service.hostname` is set to `ranger.unixauth.service.hostname`. The default group is 'Ranger Admin Default Group'. The value is `{{(RANGER_USERSYNC_HOST)}}`.

4.3 Search for "groupbuild". The property for Source for Syncing User and Groups is set to a Java class `UnixUserGroupBuilder`. This class is written to communicate with Linux.

The screenshot shows the Ranger Admin configuration interface for the 'groupbuild' search. On the left, there are filters for SCOPE. The main configuration area is divided into two sections:

- Source for Syncing User and Groups:** The property `ranger.usersync.source.impl.class` is set to `ranger.usersync.source.impl.class`. The default group is 'Ranger Usersync Default Group'. The options are:
  - ☒ `org.apache.ranger.unixusersync.process.UnixUserGroupBuilder`
  - ☐ `org.apache.ranger.unixusersync.process.FileSourceUserGroupBuilder`
  - ☐ `org.apache.ranger.ldapusersync.process.LdapUserGroupBuilder`

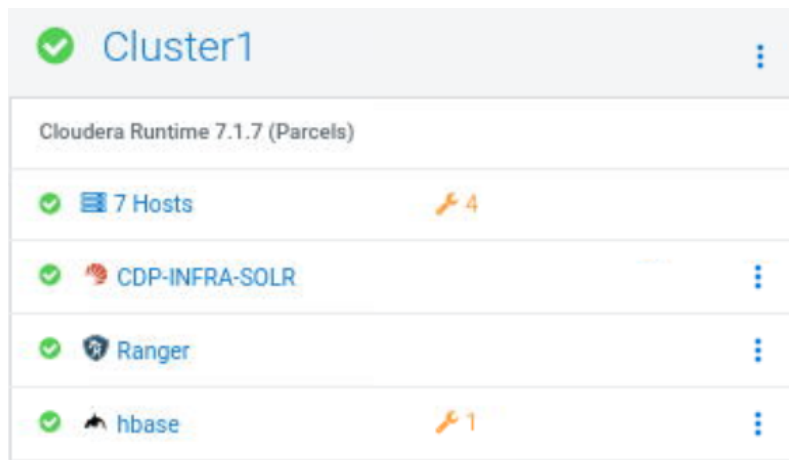
4.4 Search for "nss". The Ranger Usersync Unix Backend will use the `/etc/nsswitch.conf` file to look up users and groups. The `nsswitch` file will direct the lookup first to the local files and then to `sssd`.

The screenshot shows the Ranger Admin configuration interface for the 'nss' search. On the left, there are filters for SCOPE. The main configuration area is divided into two sections:

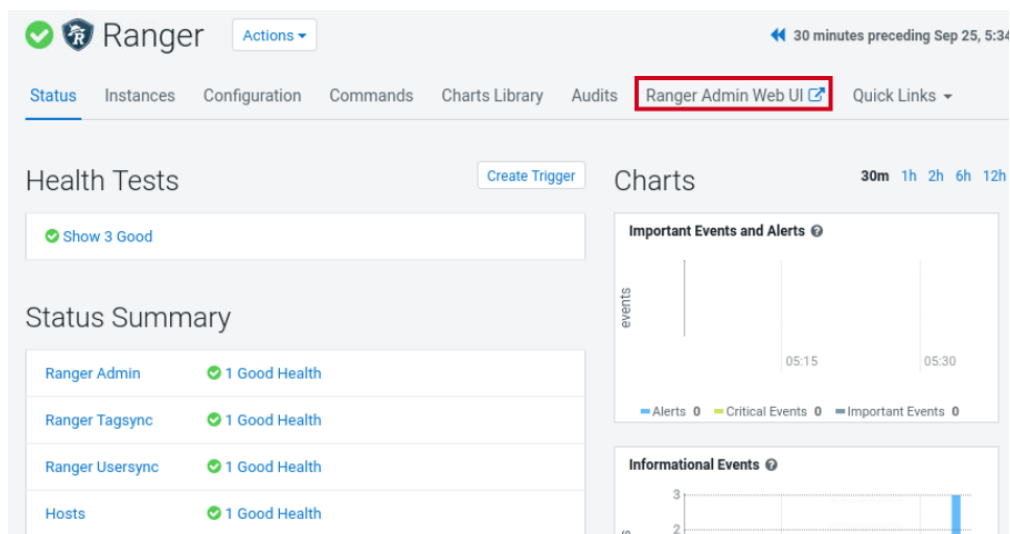
- Ranger Usersync Unix Backend:** The property `ranger.usersync.unix.backend` is set to `ranger.usersync.unix.backend`. The default group is 'Ranger Usersync Default Group'. The options are:
  - ☐ passwd
  - ☒ nss

5. Log in to Ranger as the Ranger administrative user, admin.

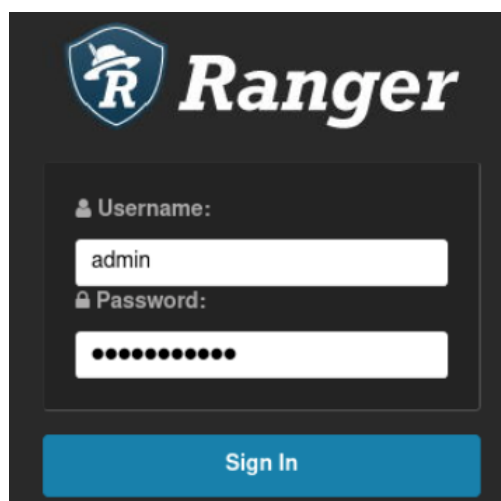
5.1 From Cloudera Manager Home select Ranger.



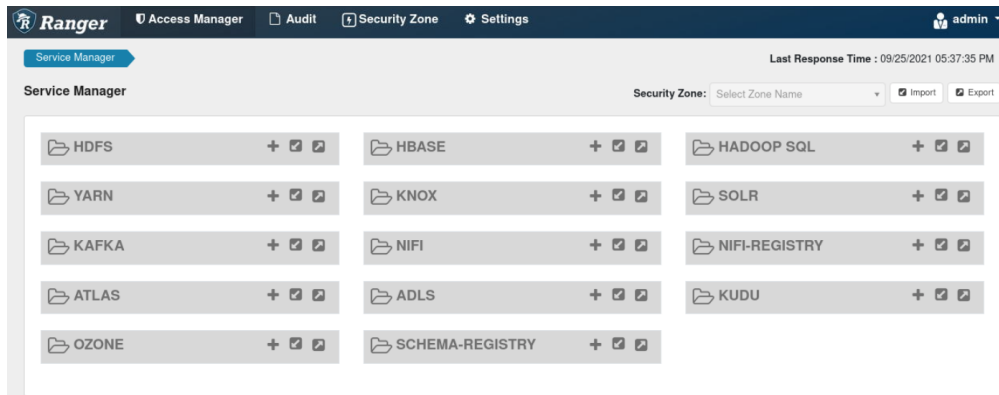
5.2 On Ranger select Ranger Admin Web UI.



5.3 On the Ranger login page log in as user admin with password <password>.



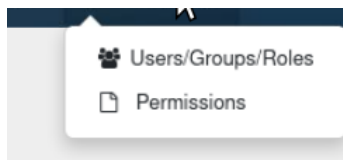
## 5.4 Land on the Service Manager page.



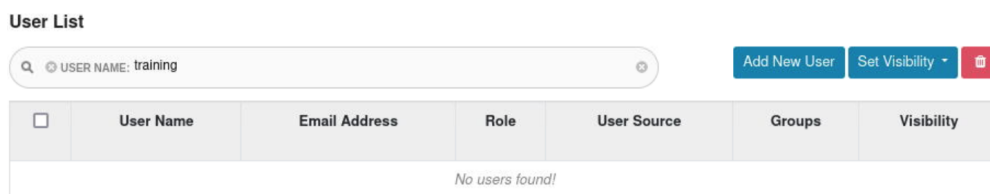
## 6. Create internal Ranger administrative user.

It is a recommend practice to have an internal administrative user in the Ranger database. You will setup user cdpadmin as an internal administrative user in the Ranger database. It a good practice to hide the user admin after you have tested the new administrative user. For class purposes you will leave the user admin in place.

### 6.1 Select Settings and select Users/Groups/Roles.



### 6.2 Select Add New User.



6.3 Add the user cdpadmin. Use password <password>. Use the provided information. Select Role to Admin. Assign group admins. Click Save.

User Name \*

First Name \*

Last Name

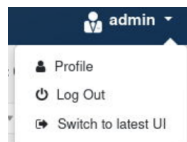
Email Address

Select Role \*

Group admins

```
User Name: cdpadmin
First Name: CDP
Last Name: Admin
Select Role: Admin
Group: admins
```

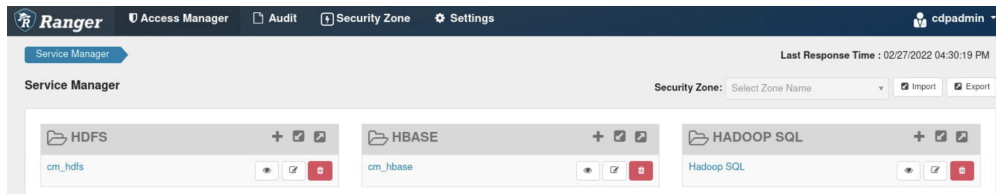
6.4 Select admin. Select Log Out.



6.5 Log in with the Ranger internal administrative user, cdpadmin, and password <password>.

A screenshot of the Ranger login interface. It features the Ranger logo at the top. Below the logo, there are two input fields: 'Username:' with the value 'cdpadmin' and 'Password:' with masked characters. A blue 'Sign In' button is located at the bottom of the form.

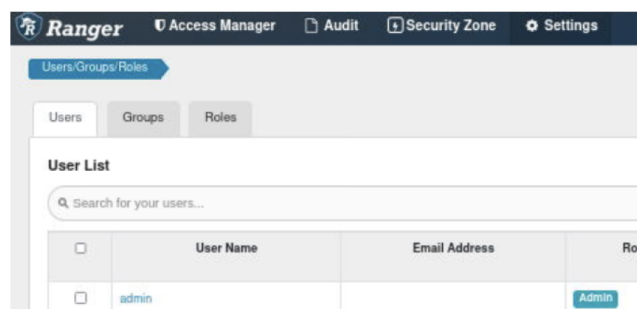
## 6.6 Confirm user cdadmin.



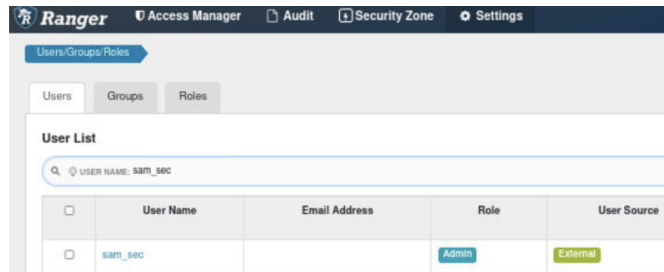
## 7. Assign external Ranger administrative users.

The current Ranger administrative user is cdadmin. Grant the LDAP users allan\_admin and sam\_sec privileges as Ranger administrators. The user sam\_sec is your security administrator. The security administrator should create and edit all Ranger policies. The user allan\_admin is also assigned, but this is for training purposes.

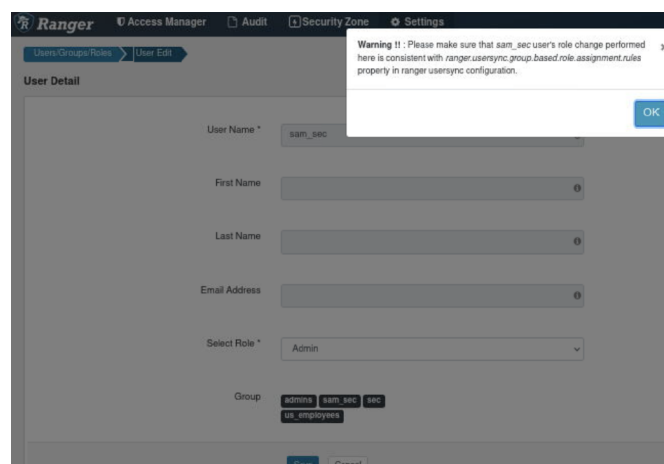
### 7.1 On Ranger select Settings. Select Users/Groups/Roles.



### 7.2 Filter for User Name:sam\_sec. Select sam\_sec.



### 7.3 Change Select Role to Admin. Click OK. Click Save.





## 7.4 Assign allan\_admin as a Ranger admin.

User Name \*

First Name

Last Name

Email Address

Select Role \*

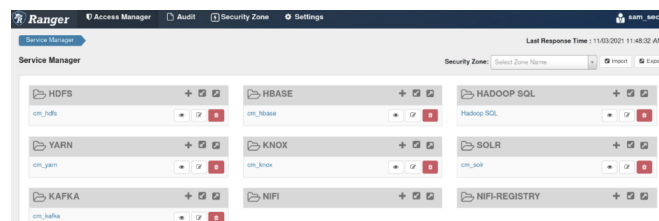
Group

☐ admins
 ☐ allan\_admin
 ☐ gov
 ☐ supergroup
 ☐ ww\_employees

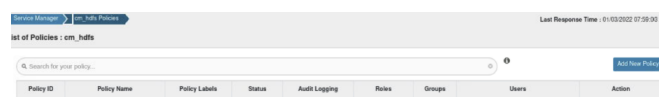
## 8. Create a Ranger policy for Ranger auditing.

Every service user needs read and write access to the Ranger audit directory. You will use this task to learn how to create Ranger policy.

### 8.1 On Ranger select Access Manager. Select HDFS cm\_hdfs.



### 8.2 On List of Policies: cm\_hdfs select Add New Policy.



### 8.3 Ranger policies have two sections. First is the Policy Details.

#### Policy Details:

- Policy type: access or deny
- Policy ID: A sequential ID number assigned to every policy
- Policy Name: free text
- Policy Label: Create labels to group policy for reporting purposes
- Resource Path: identify the object/s for the policy.
- Description: free text
- Audit Logging: yes/no
- Enabled: yes/no
- Recursive: yes/no

**IMPORTANT:** Ranger is in communications with the Ranger plugins. As you enter the resource path it will map to the object. Always select the object from the pop-up field.

### 8.4 Enter Policy Details. Use information provided.

The screenshot shows the 'Policy Details' configuration form in Ranger. The form includes the following fields and controls:

- Policy Type:** A dropdown menu set to 'Access'.
- Policy ID:** A text field containing the value '94'.
- Policy Name:** A text field containing 'access: ranger audit'. To its right are two radio buttons: 'Enabled' (selected) and 'Normal'.
- Policy Label:** A text field containing 'Policy Label'.
- Resource Path:** A text field containing '/ranger/audit'. To its right is a 'Recursive' radio button.
- Description:** A large text area for additional details.
- Audit Logging:** A checkbox labeled 'Yes' which is checked.

Policy Name: access: ranger audit  
Resource Path: /ranger/audit

### 8.5 Second section is the Allow and Deny Conditions. The Allow and Deny Conditions section grants or revokes the privileges to the Resource Path object. Roles, groups, and/or users can be assigned permissions.

8.6 Assign allow conditions to service users. Use information provided.

Allow Conditions: hide

Select Role	Select Group	Select User	Permissions	Delegate Admin
Select Roles	Select Groups	<div> <span>x atlas</span> <span>x hbase</span> <span>x hdfs</span> <span>x hive</span> </div> <div> <span>x impala</span> <span>x kafka</span> <span>x knox</span> <span>x solr</span> </div> <div> <span>x yarn</span> </div>	<div> <span>Read</span> <span>Write</span> <span>Execute</span> </div>	<input type="checkbox"/>

Select Users: atlas, hbase, hdfs, hive, impala, kafka, knox, solr, yarn.  
Permissions: Read, Write, Execute

8.7 Scroll to the bottom. Click Add to save the policy into the Ranger database. The policy will be turned into a JSON file and transmitted to the Ranger plugin within 10 to 30 seconds.

Add Cancel

8.8 Close the Firefox browser tab for Ranger.

9. Return to Cloudera Manager Home.