CS300 Couchbase NoSQL Server Administration

Lab 1.1 Exercise Manual

Release: 6.5.1

Revised: June 22nd, 2020

Lab #1A: Auth via LDAP

Objective: Getting Started with LDAP Authentication

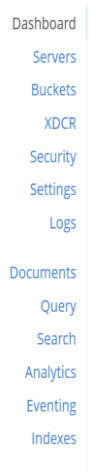
Prerequisites

Ensure that the following prerequisites are available in your environment before using PAM in Couchbase:

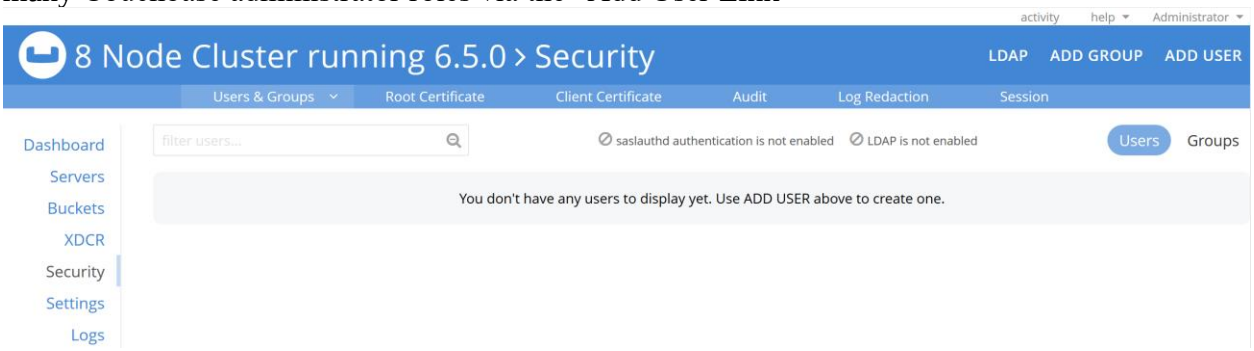
- Couchbase Server version 6.5 running on Linux environment.

Configure "Couchbase" authenticated user

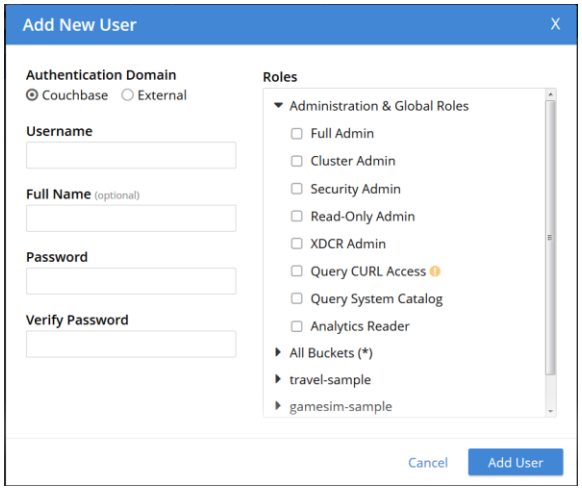
On the security link



Make sure Authentication is enabled and map the Linux login name (user name) to one or many Couchbase administrator roles via the "Add User Link"

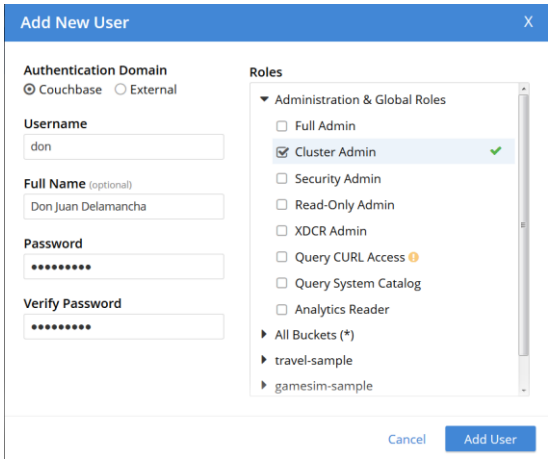


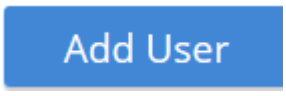
Click the ADD USER link in the uper right hand corner of the UI and this pop up will appear.

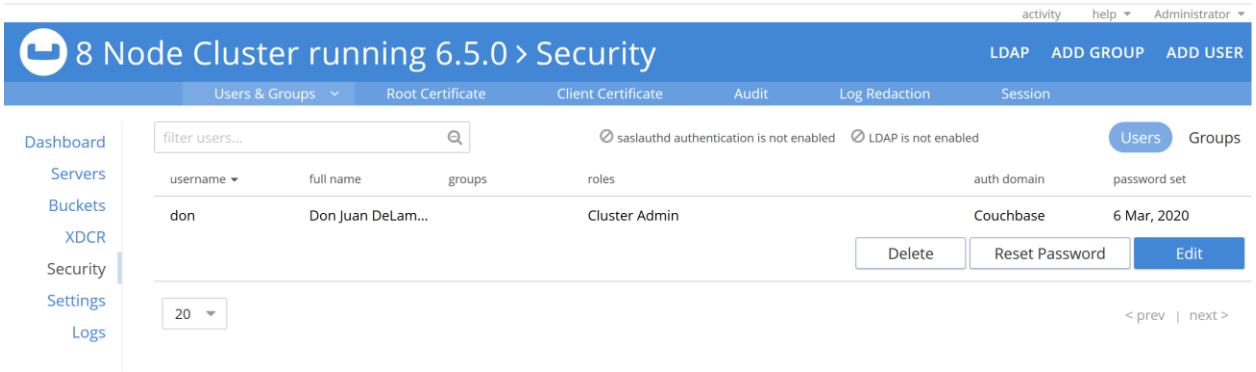


Authentication Domain Radio button select **Couchbase**

Type in Username **don**
Type in Full Name **Don Juan Delamancha**
Type in Password **couchbase**
Check box for Roles **Cluster Admin**

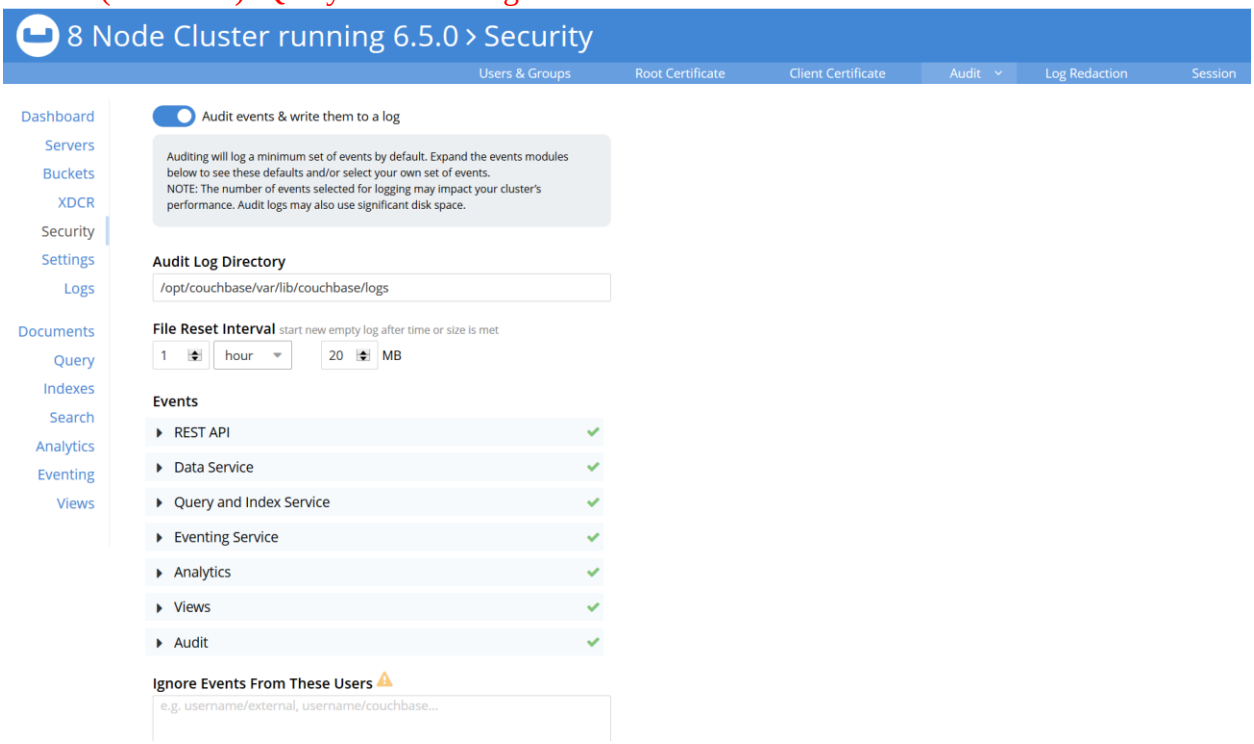


Click 



On the Security page select the "Audit" Link

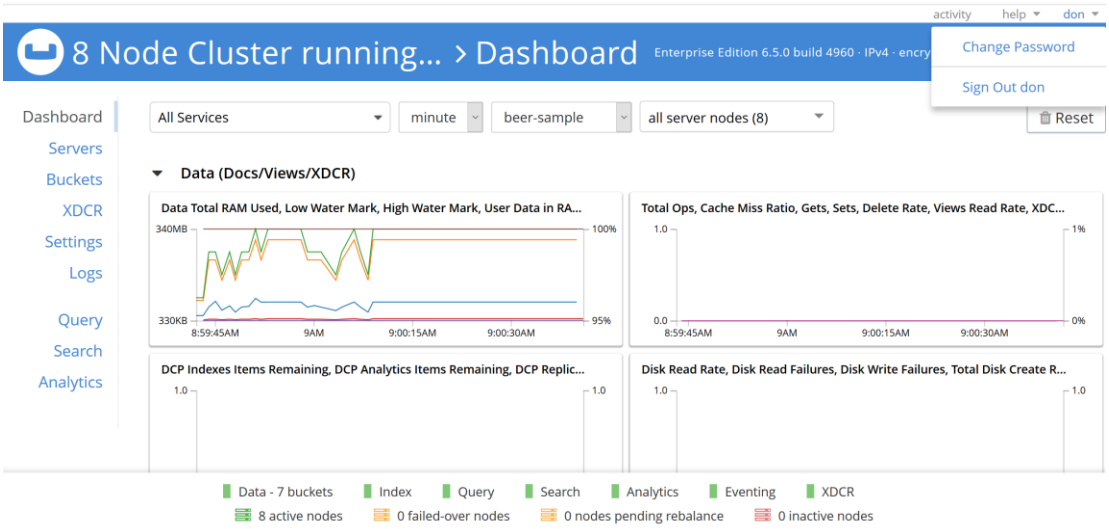
Slide button to Enable audit box,
change log rotation to 1 hour,
expand and enable all data Service Events,
turn off(de-enable) Query and Eventing and save.



Log out as Administrator.
Try connecting using the Linux user credentials,

LoginID = don Password = couchbase

Couchbase Server should permit the connection, and once authenticated, the privileges of that user in Couchbase should be as per the role mapping.



Congratulations! You've successfully logged in as a Linux user, using the privileges granted through the Cluster administrator role membership.

In the CLI become root

```
sudo -i

[root@Couchbase01 logs]# more /opt/couchbase/var/lib/couchbase/logs/audit.log

,"enabled":[20480,20482,20483,20485,20488,20489,20490,20491],"real_userid":{"
domain":"
builtin","user":"Administrator"},"sessionid":"b30c340ae95ecd91c784954bb556b4e
d","remote":{"ip":"73.241.156.190","port":54454},"times
tamp":"2018-07-31T18:24:42.599Z","id":8240,"name":"configured audit
daemon","description":"loaded configuration file for audit daemo
n"}
{"roles":["cluster_admin"],"real_userid":{"domain":"local","user":"don"},"ses
sionid":"34545aea382f2aac4f9ab50b04454fa1","remote":{"i
p":"73.241.156.190","port":54467},"timestamp":"2018-07-
31T18:26:59.511Z","id":8192,"name":"login success","description":"Successful
login to couchbase cluster"}

[root@Couchbase01 logs]#
```

This series of steps validates local "Couchbase" Authentication.

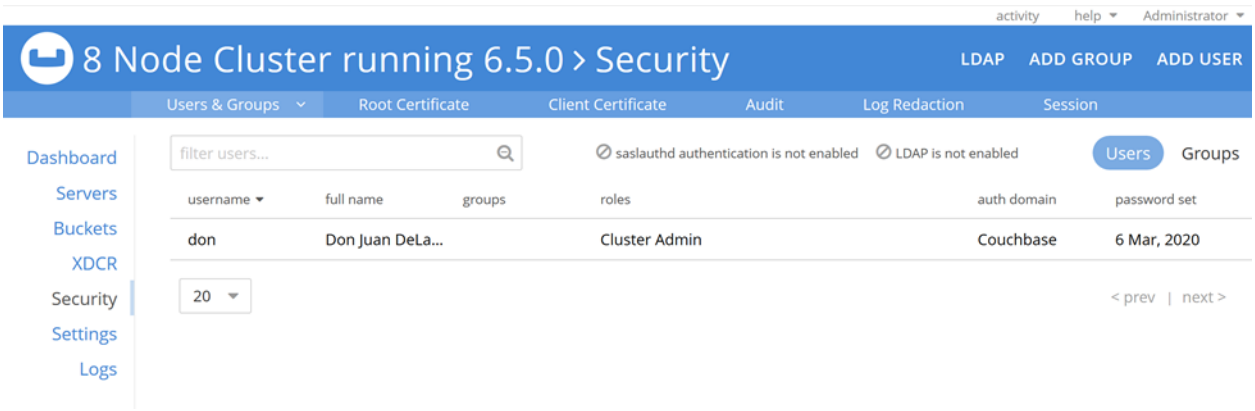
Log out of the UI and Log back in as Administrator

Next we will configure LDAP Authentication using the UI

Configuring an LDAP server is beyond the scope of this course, however there are public LDAP servers available for testing. We will use a preconfigured LDAP server located here:

https://www.forumsys.com/tutorials/integration-how-to/ldap/online-ldap-test-server/

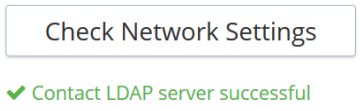
In the UI Select the LDAP Link at the righthand top of your UI

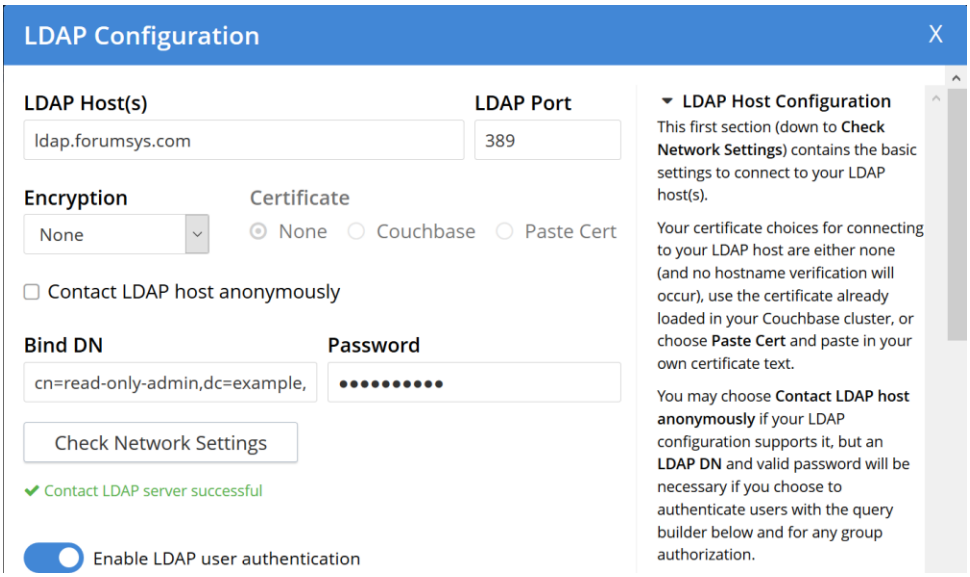


In the popup type in the following:

LDAP Host: **ldap.forumsys.com**
LDAP Port: **389**
Encryption: **None**
Deselect contact LDAP host anonymously box
Bind DN: **cn=read-only-admin,dc=example,dc=com**
Bind Password: **password**

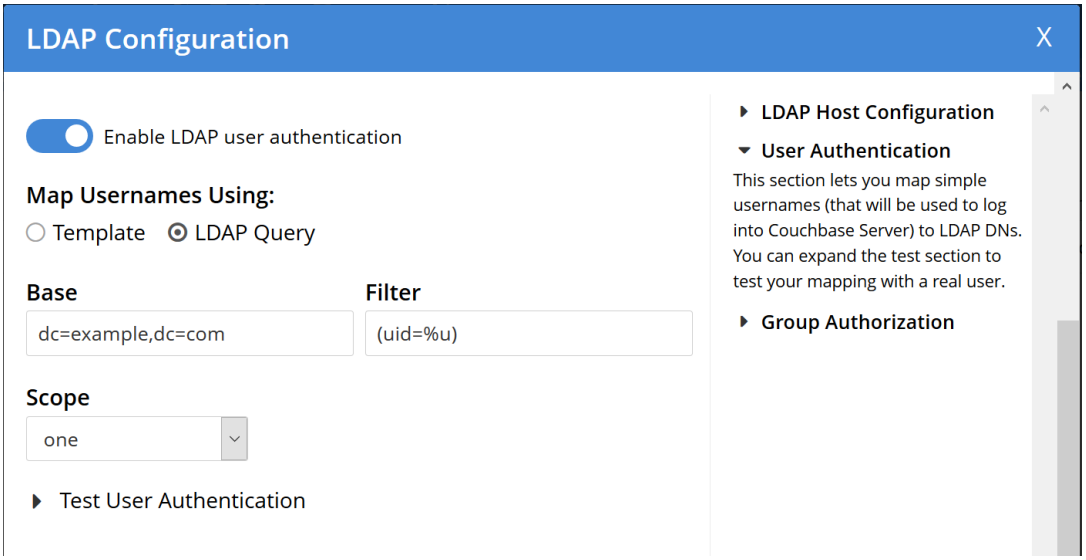
Push the check network settings button to test settings.



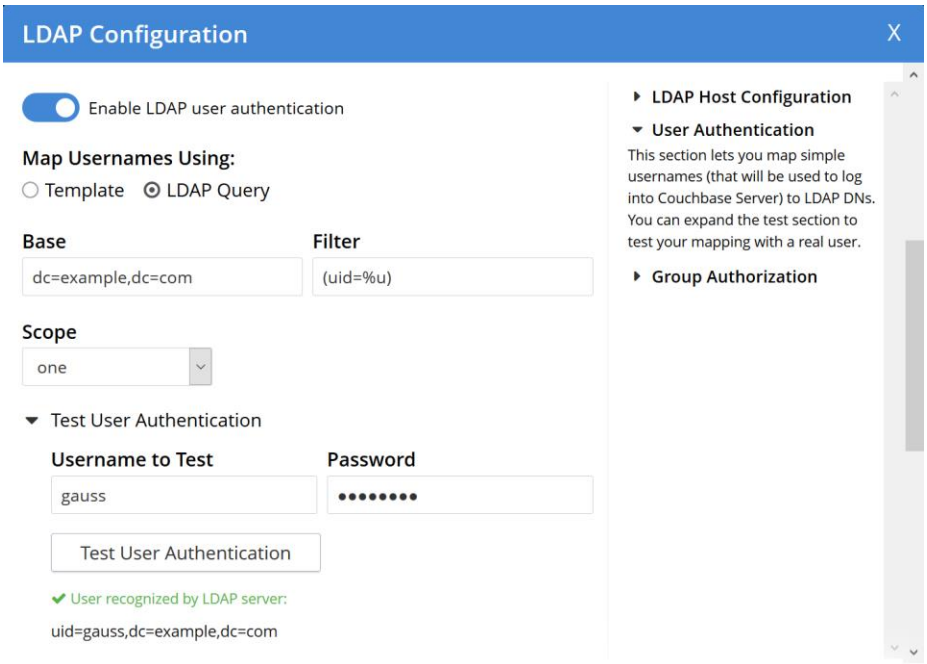


Next move down to the user authentication area.

Slide button to enable LDAP user authentication
Map usernames Using LDAP query
Base: **dc=example,dc=com**
Filter: **(uid=%u)**
Scope: **one**

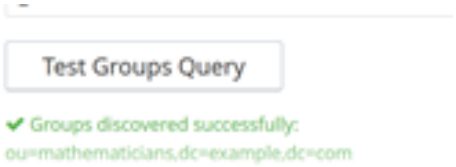


Open the Test User Authentication triangle.

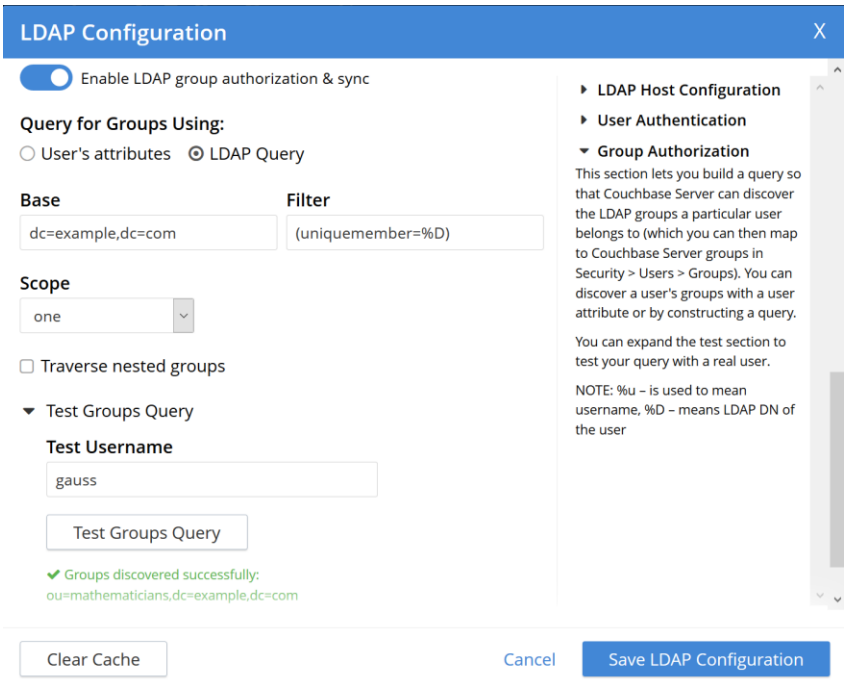


Username to Test: **gauss**

Password: **password**
Move down to the groups area in the popup.
Slide the button to enable group authorization and sync.
Query for Groups Using: **LDAP Query**
Base: **dc=example,dc=com**
Filter: **(uniquemember=%D)**
Open Test Groups Query Triangle
Test Username: gauss



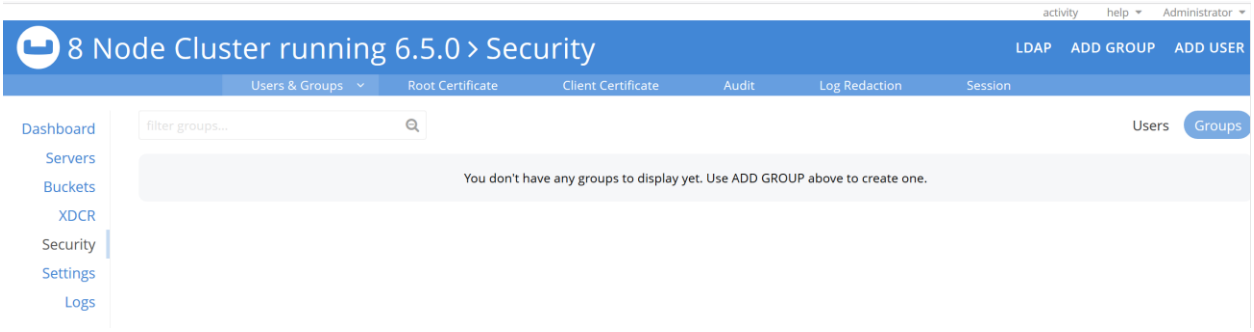
Push the to test group settings



You have now validated connection to a public LDAP server with your bindDN
And validated the user “gauss” at both individual and group level.

Lets add some group mappings to Couchbase server

On the security link> click the ADD GROUP link on the righthand side of your screen.



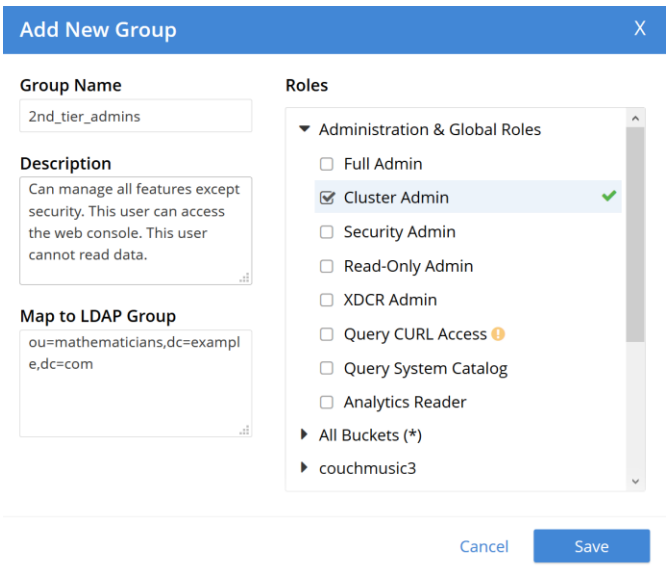
On the popup enter the following:

Group Name: 2nd_tier_admins

Description: Can manage all features except security. This user can access the web console. This user cannot read data.

Map to LDAP Group: ou=mathematicians,dc=example,dc=com

Check the Cluster Admin box



Click the save button.

Now click the ADD GROUP link and add another group.

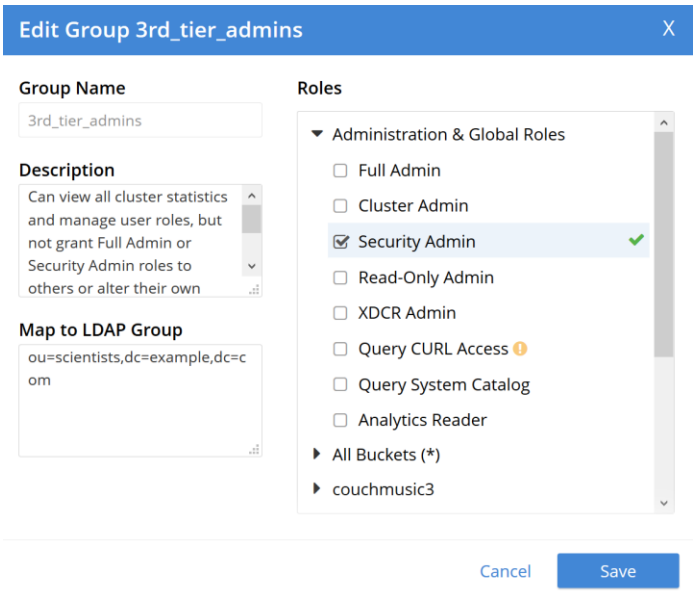
On the popup enter the following:

Group Name: 3rd_tier_admins

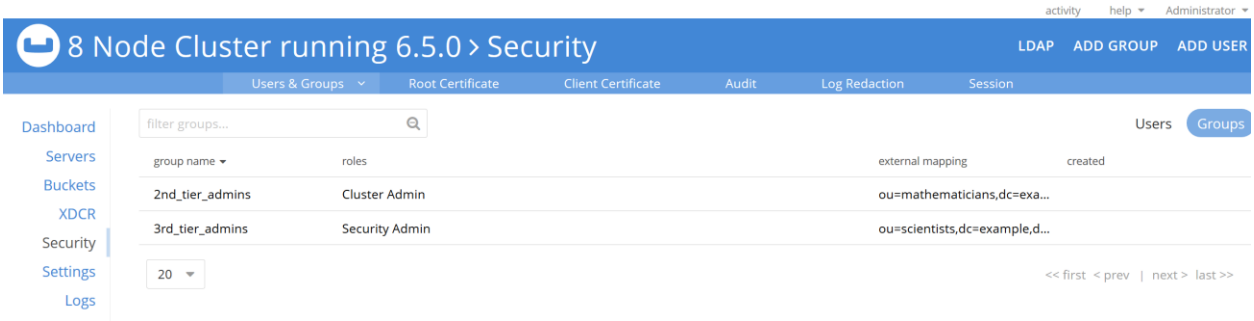
Description: Can view all cluster statistics and manage user roles, but not grant Full Admin or Security Admin roles to others or alter their own role. This user can access the web console. This user cannot read data.

Map to LDAP Group: ou=scientists,dc=example,dc=com

Check the Security Admin box

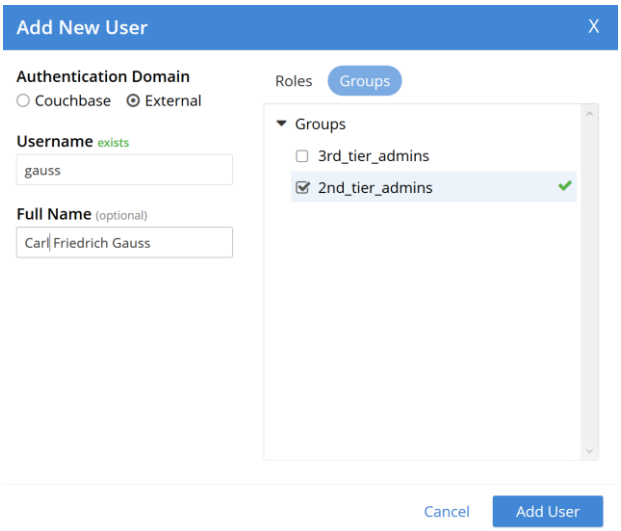


Click the save button.



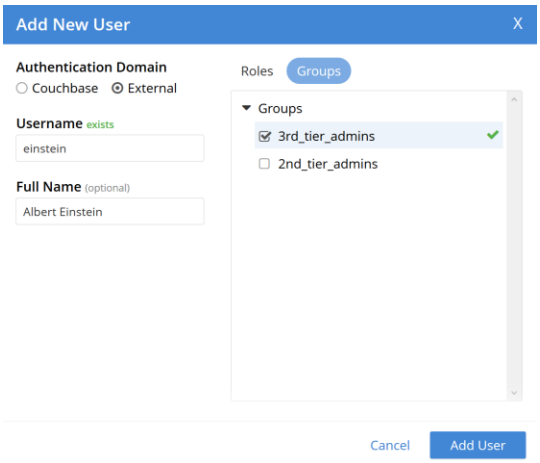
Now lets add some users and assign them these roles that have named in Couchbase and MAPPED to external groups.

Click on the USERS link, then click on the ADD USER link.
On the popup add the following:
Authentication Domain: External
Username: gauss
Full name: Carl Friedrich Gauss
On the Groups button: check 2nd_tier_admins

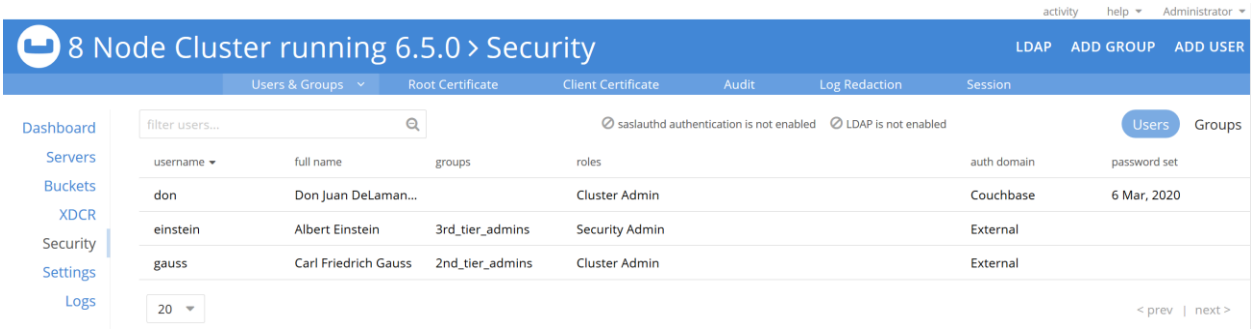


Then click the Add User button.
Click the Add User button again and add einstein.

On the popup add the following:
Authentication Domain: External
Username: einstein
Full name: Albert Einstein
On the Groups button: check 3rd_tier_admins



CLICK THE Add User button.

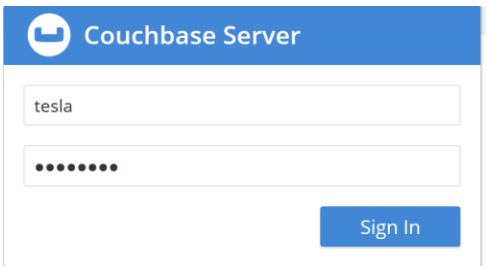


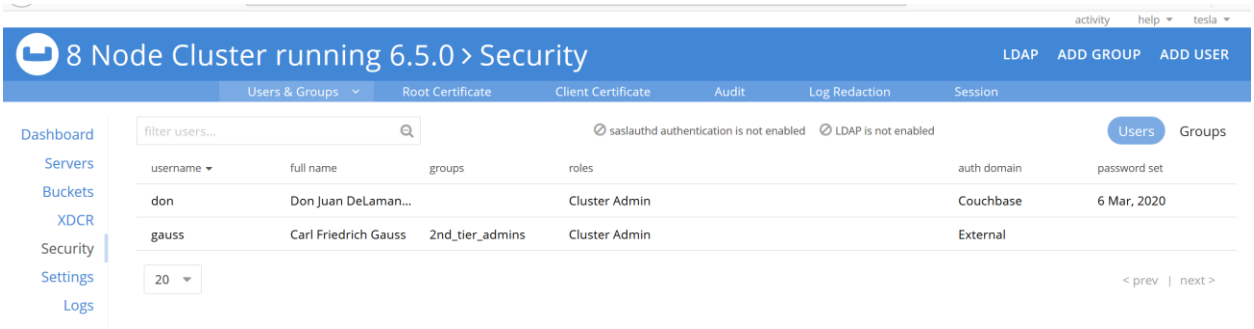
Now log out and log back in the your newly added users.
Notice what links and viewable actions are enabled as each other various users.

LoginID= gauss, password= password (view then log out)

LoginID= einstein, password= password (view then log out)

Now try a user not mapped to Couchbase(locally).
LoginID= tesla, password= password





Notice the user tesla logged in in the upper righthand corner.

So, Couchbase server will look local for loginID and then External where it will find user “tesla” with group affiliation of ou=scientist

Now log out and back in again as Administrator.

Enablement can be verified at the command line by entering the following:

```
[ec2-user@Couchbase0X ~]$ /opt/couchbase/bin/couchbase-cli setting-ldap -c
127.0.0.1:8091 -u Administrator -p couchbase --get | python3 -mjson.tool

{
    "hosts": [
        "ldap.forumsys.com"
    ],
    "port": 389,
    "encryption": "None",
    "serverCertValidation": false,
    "bindDN": "cn=read-only-admin,dc=example,dc=com",
    "authenticationEnabled": true,
    "userDNMapping": {
        "query": "dc=example,dc=com??one?(uid=%u)"
    },
    "authorizationEnabled": true,
    "nestedGroupsEnabled": false,
    "groupsQuery": "dc=example,dc=com??one?(uniquemember=%D)",
    "requestTimeout": 5000,
    "maxParallelConnections": 100,
    "maxCacheSize": 10000,
    "cacheValueLifetime": 300000,
    "nestedGroupsMaxDepth": 10,
    "bindPass": "**********",
    "failOnMaxDepth": false
}
```

End of Lab 1.1