

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

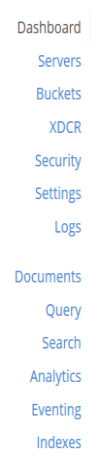
Prerequisites

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

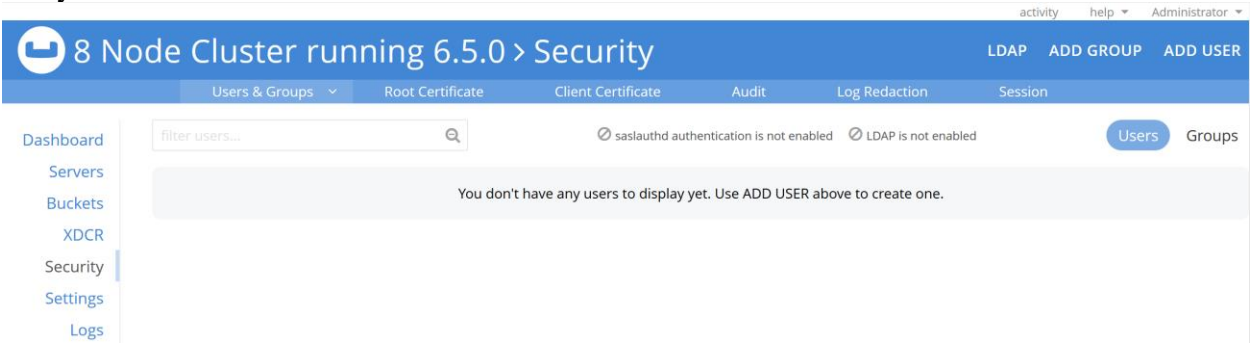
- [Couchbase Server version 6.5](#) running on Linux environment.

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





activity

help

Administrator

8 Node Cluster running 6.5.0 > Security

LDAPADD GROUPADD USER

Users & Groups

Root Certificate

Client Certificate

Audit

Log Redaction

Session

Dashboard

Servers

Buckets

XDCR

Security

Settings

Logs

filter users...

saslauthd authentication is not enabled

LDAP is not enabled

Users

Groups

username	full name	groups	roles	auth domain	password set
don	Don Juan DeLam...		Cluster Admin	Couchbase	6 Mar, 2020

20

< prev | next >

Delete

Reset Password

Edit

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.

8 Node Cluster running 6.5.0 > Security

Users & GroupsRoot CertificateClient CertificateAuditLog RedactionSession

Dashboard

Servers

Buckets

XDCR

Security

Settings

Logs

Documents

Query

Indexes

Search

Analytics

Eventing

Views

Audit events & write them to a log

Auditing will log a minimum set of events by default. Expand the events modules below to see these defaults and/or select your own set of events.
NOTE: The number of events selected for logging may impact your cluster's performance. Audit logs may also use significant disk space.

Audit Log Directory

/opt/couchbase/var/lib/couchbase/logs

File Reset Interval

start new empty log after time or size is met

1 hour20 MB

Events

REST API

Data Service

Query and Index Service

Eventing Service

Analytics

Views

Audit

Ignore Events From These Users

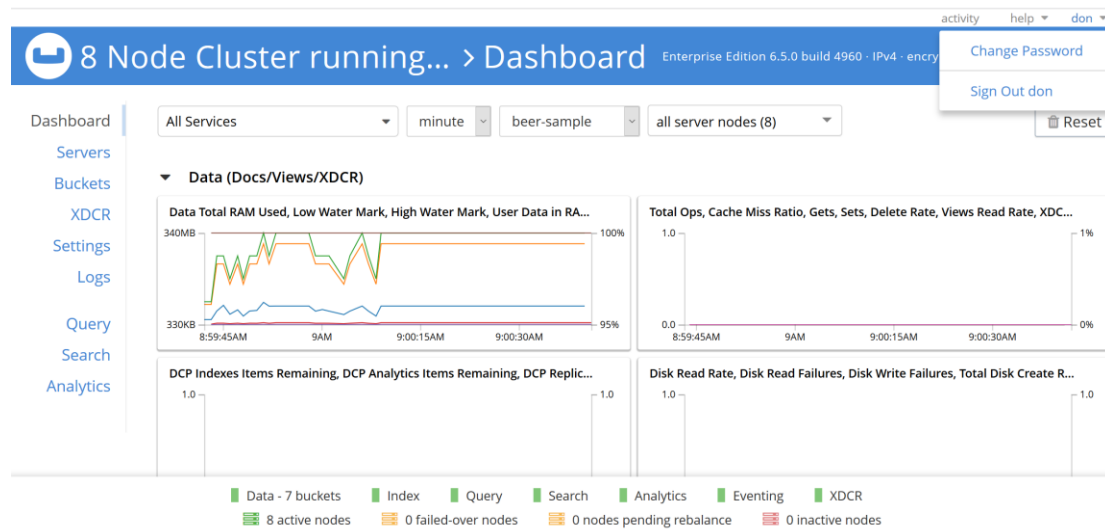
e.g. username/external, username/couchbase...

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/>



Online LDAP Test Server

By Mamoon Yunus | Date posted: February 22, 2014



Here are the credentials for an Online LDAP Test Server that you can use for testing your applications that require LDAP-based authentication. Our goal is to eliminate the need for you to download, install and configure an LDAP sever for testing. If all you need is to test connectivity and authentication against a few identities, you have come to the right place. If you find this useful or would like us to enhance/modify this test LDAP server, please leave a comment.

LDAP Server Information (read-only access):

Server: *ldap.forumsys.com*
Port: *389*

Bind DN: *cn=read-only-admin,dc=example,dc=com*
Bind Password: *password*

All user passwords are *password*.

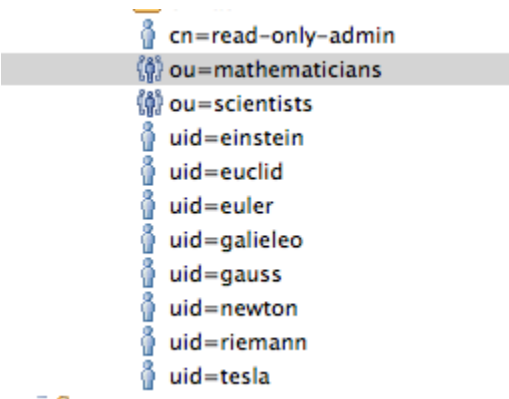
You may also bind to individual Users (uid) or the two Groups (ou) that include:

ou=mathematicians,dc=example,dc=com

- *riemann*
- *gauss*
- *euler*
- *euclid*

ou=scientists,dc=example,dc=com

- *einstein*
- *newton*
- *galileo*
- *tesla*





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

The screenshot shows the Couchbase Security interface. At the top, there's a blue header bar with the Couchbase logo and the title "8 Node Cluster running 6.5.0 > Security". On the right side of the header, there are links for "activity", "help", and "Administrator". Below the header, there's a navigation bar with tabs: "Users & Groups" (selected), "Root Certificate", "Client Certificate", "Audit", "Log Redaction", and "Session". To the left of the main content area is a sidebar menu with options: "Dashboard", "Servers", "Buckets", "XDCR", "Security" (highlighted), "Settings", and "Logs". The main content area has a search box labeled "filter users..." and two status indicators: "sasauthd authentication is not enabled" and "LDAP is not enabled". There are also buttons for "Users" and "Groups". Below this is a table listing users:

username	full name	groups	roles	auth domain	password set
don	Don Juan DeLa...		Cluster Admin	Couchbase	6 Mar, 2020

At the bottom of the main content area, there's a pagination control showing "20" and navigation links "< prev | next >".

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.

Check Network Settings

✔ Contact LDAP server successful

LDAP Configuration

LDAP Host(s)

ldap.forumsys.com

LDAP Port

389

Encryption

None

Certificate

☒ None

☐ Couchbase

☐ Paste Cert

☐ Contact LDAP host anonymously

Bind DN

cn=read-only-admin,dc=example,

Password

••••••••

Check Network Settings

☒ Contact LDAP server successful

☒ Enable LDAP user authentication

LDAP Host Configuration

This first section (down to **Check Network Settings**) contains the basic settings to connect to your LDAP host(s).

Your certificate choices for connecting to your LDAP host are either none (and no hostname verification will occur), use the certificate already loaded in your Couchbase cluster, or choose **Paste Cert** and paste in your own certificate text.

You may choose **Contact LDAP host anonymously** if your LDAP configuration supports it, but an **LDAP DN** and valid password will be necessary if you choose to authenticate users with the query builder below and for any group authorization.



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**

LDAP Configuration

Enable LDAP user authentication

Map Usernames Using:

Template

LDAP Query

Base

dc=example,dc=com

Filter

(uid=%u)

Scope

one

Test User Authentication

LDAP Host Configuration

User Authentication

This section lets you map simple usernames (that will be used to log into Couchbase Server) to LDAP DNs. You can expand the test section to test your mapping with a real user.

Group Authorization

Open the Test User Authentication triangle.

LDAP Configuration

Enable LDAP user authentication

Map Usernames Using:

Template

LDAP Query

Base

dc=example,dc=com

Filter

(uid=%u)

Scope

one

Test User Authentication

Username to Test

gauss

Password

.....

Test User Authentication

User recognized by LDAP server:

uid=gauss,dc=example,dc=com

LDAP Host Configuration

User Authentication

This section lets you map simple usernames (that will be used to log into Couchbase Server) to LDAP DNs. You can expand the test section to test your mapping with a real user.

Group Authorization

Username to Test: **gauss**

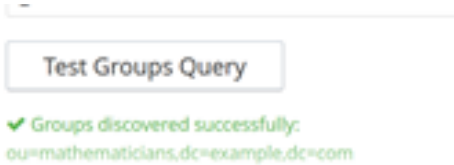
Couchbase course materials are exclusively for use by a single participant in a hands-on training course delivered by Couchbase, Inc. or a Couchbase Authorised Training Partner, as listed at www.couchbase.com. Use or distribution other than to a participant in such training event is prohibited. If you believe these course materials have been reproduced or distributed in print or electronic without permission of Couchbase, Inc. please email: training@couchbase.com

Copyright © 2020 Couchbase, Inc. All rights reserved

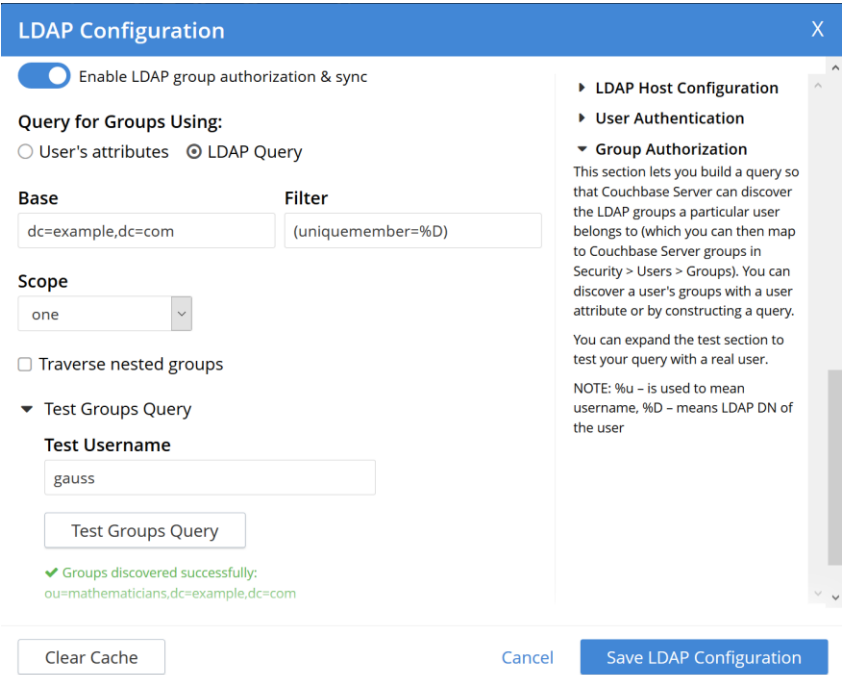
CS300 Couchbase Server Administration



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

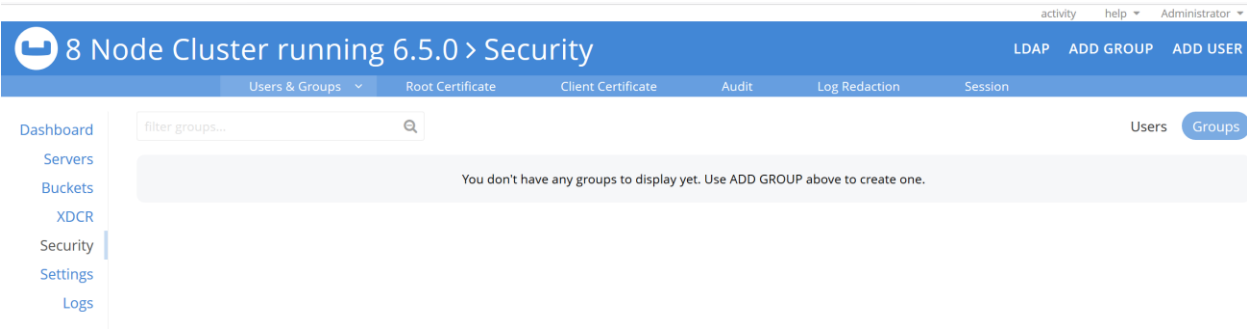


You have now validated connection to a public LDAP server with your bindDN
And validated the user “gauss” at both individual and group level.



Lets add some group mappings to Couchbase server

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



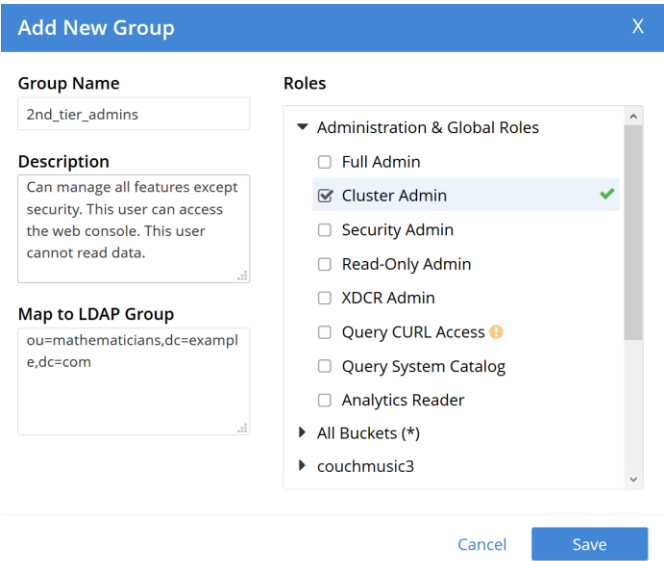
On the popup enter the following:

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

Edit Group 3rd_tier_admins

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

Map to LDAP Group

ou=scientists,dc=example,dc=com

Roles

Administration & Global Roles

☐ Full Admin

☐ Cluster Admin

☒ Security Admin

☐ Read-Only Admin

☐ XDCR Admin

☐ Query CURL Access

☐ Query System Catalog

☐ Analytics Reader

All Buckets (*)

couchmusic3

Cancel

Save

Click the save button.

8 Node Cluster running 6.5.0 > Security

LDAP

ADD GROUP

ADD USER

Users & Groups

Root Certificate

Client Certificate

Audit

Log Redaction

Session

filter groups...

Users

Groups

group name	roles	external mapping	created
2nd_tier_admins	Cluster Admin	ou=mathematicians,dc=exa...	
3rd_tier_admins	Security Admin	ou=scientists,dc=example,d...	

20

<< first < prev | next > last >>

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

Add New User

Authentication Domain

☐ Couchbase ☒ External

Username exists

gauss

Full Name (optional)

Carl Friedrich Gauss

Roles

Groups

Groups

☐ 3rd_tier_admins

☒ 2nd_tier_admins

Cancel

Add User

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

Add New User

Authentication Domain

☐ Couchbase ☒ External

Username exists

einstein

Full Name (optional)

Albert Einstein

Roles

Groups

Groups

☒ 3rd_tier_admins

☐ 2nd_tier_admins

Cancel

Add User

CLICK THE Add User button.



activityhelpAdministrator

8 Node Cluster running 6.5.0 > SecurityLDAPADD GROUPADD USER

Users & GroupsRoot CertificateClient CertificateAuditLog RedactionSession

DashboardServersBucketsXDCRSecuritySettingsLogs

filter users...

saslauthd authentication is not enabledLDAP is not enabled

UsersGroups

username	full name	groups	roles	auth domain	password set
don	Don Juan DeLaman...		Cluster Admin	Couchbase	6 Mar, 2020
einstein	Albert Einstein	3rd_tier_admins	Security Admin	External	
gauss	Carl Friedrich Gauss	2nd_tier_admins	Cluster Admin	External	

20< prev | next >

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

Couchbase Server

tesla

.....

Sign In

activityhelptesla

8 Node Cluster running 6.5.0 > SecurityLDAPADD GROUPADD USER

Users & GroupsRoot CertificateClient CertificateAuditLog RedactionSession

DashboardServersBucketsXDCRSecuritySettingsLogs

filter users...

saslauthd authentication is not enabledLDAP is not enabled

UsersGroups

username	full name	groups	roles	auth domain	password set
don	Don Juan DeLaman...		Cluster Admin	Couchbase	6 Mar, 2020
gauss	Carl Friedrich Gauss	2nd_tier_admins	Cluster Admin	External	

20< prev | next >

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