Study Club for Splunk @ BSides SPL 22
Hands-on with AD & LDAP

This Study Club for Splunk hands-on lab is a continuation of the three all attendee hands-on labs that we delivered in person as part of .conf22 in Las Vegas. As a participating attendee, you will be able to request an individual Global Academy for Splunk (GAS) lab to be automatically orchestrated for you to have an awesomely immersive experience and fully interact with the speakers, Aleem and Gregg.

The lab will be a walkthrough of the Splunk LDAP Authentication method to integrate with Microsoft Active Directory (AD) using LDAP.

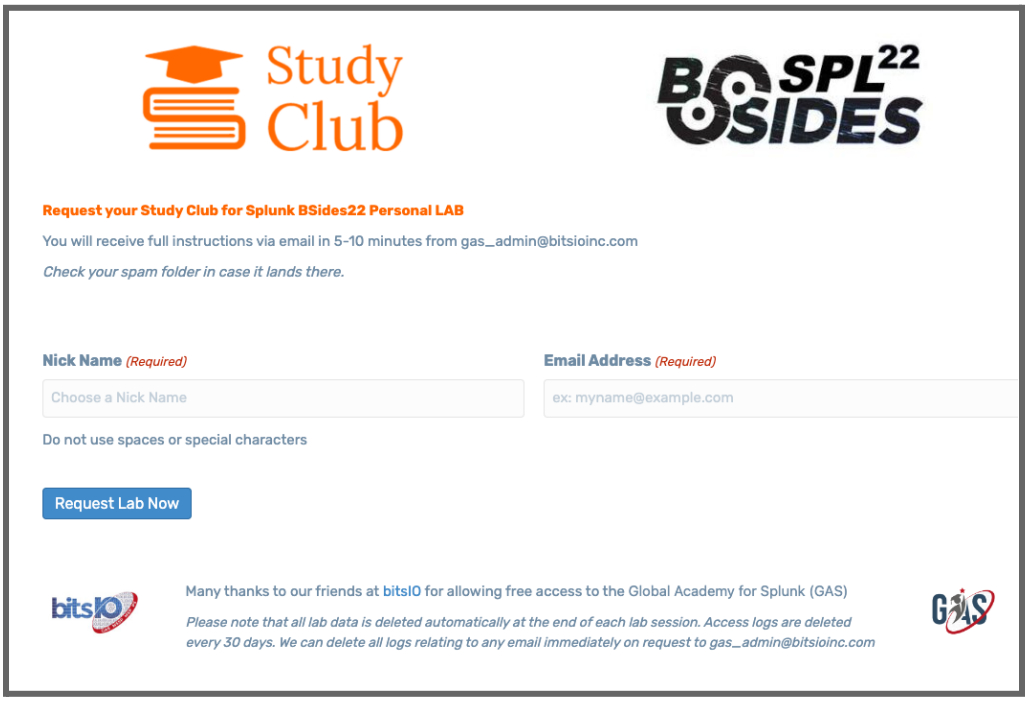
Together, we will be creating and mapping roles in Splunk to Windows AD groups. We will go through how to control access to Splunk dashboards and verify the access is working. We then will go through the backend via the command line. We will close out the session with a fireside chat where we will share observations, insights, gotchas, best practices and next steps.
We are working to allow the community to spin up the GAS lab while watching the session later via video on demand after BSides22 has concluded. This will be super cool as part of support for our beloved Splunk community and global user groups. The session video is available at http://bsides22.video.studyclub.community.

We have a dedicated Study Club for Splunk Slack channel on splunk-usergroups. It is named study-club-for-splunk. The direct link is http://splunk-slack.studyclub.community

Many thanks to bitsIO Inc for allowing us to use their GAS platform for our Splunk community.

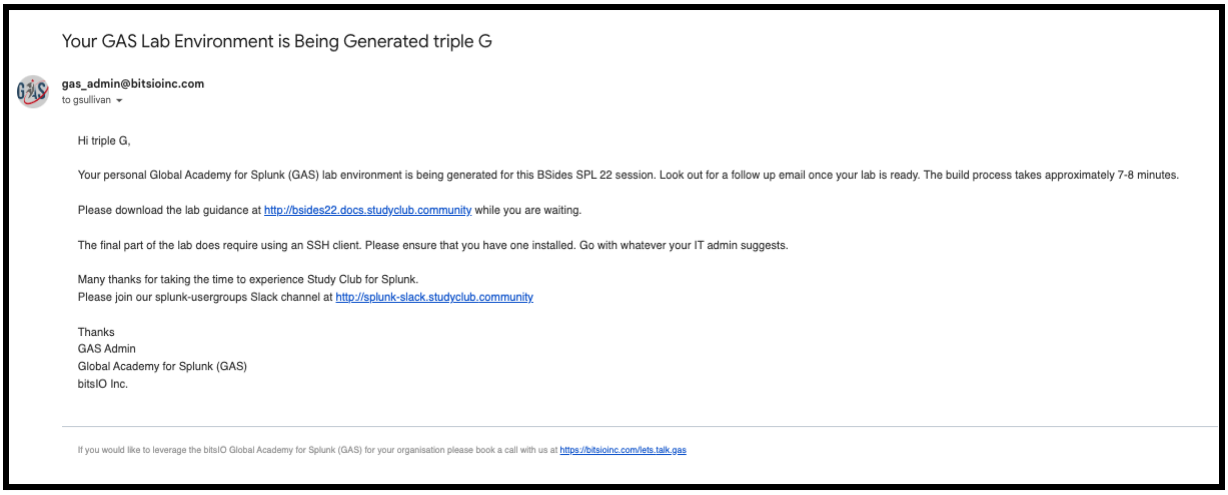
Step 1 - Request a BSides SPL 22 personal GAS lab

Go to http://bsides22.studyclub.community
Enter a nickname and an email address and click the Request Lab Now button.



You will receive a request confirmation

Within a minute or so, you will receive an initial email notification from gas_admin@bitsioinc.com. Check your spam folder and further allow emails as needed



Your GAS Lab Environment is Being Generated triple G

gas_admin@bitsioinc.com
to gsullivan

Hi triple G,

Your personal Global Academy for Splunk (GAS) lab environment is being generated for this BSides SPL 22 session. Look out for a follow up email once your lab is ready. The build process takes approximately 7-8 minutes.

Please download the lab guidance at http://bsides22.docs.studyclub.community while you are waiting.

The final part of the lab does require using an SSH client. Please ensure that you have one installed. Go with whatever your IT admin suggests.

Many thanks for taking the time to experience Study Club for Splunk.
Please join our splunk-usergroups Slack channel at http://splunk-slack.studyclub.community

Thanks
GAS Admin
Global Academy for Splunk (GAS)
bitsIO Inc.

If you would like to leverage the bitsIO Global Academy for Splunk (GAS) for your organisation please book a call with us at https://bitsioinc.com/lets.talk.gas

You will receive a further email with full lab instructions after approximately 7-8 minutes

Your Global Academy for Splunk (GAS) environment for BSIDES SPL 22 is now ready, triple G

gas_admin@bitsioinc.com
to gsullivan

Hi triple G,

Your Global Academy for Splunk (GAS) environment for BSIDES SPL 22 is now ready for your use.

URL for the publicly accessible Splunk All-In-One
https://bitsIO-GAS-9eW8Fk-bsides22-ad-ldap-node.gas.bitsioservices.com

User name: admin
Password: cxapkygnz2

The credentials for command line access via ssh
User name: triple G
Password: cxapkygnz2

The command to connect from your local machine's terminal client to the Linux Jump Box is
ssh triple G@bitsIO-GAS-9eW8Fk-bsides22-ad-ldap-jumpbox.gas.bitsioservices.com
Password: cxapkygnz2

The command to connect from the Linux Jump Box to the publicly accessible Splunk All-In-One
ssh triple G@10.4.5.200
Password: cxapkygnz2

LDAP Server
IP address is 10.4.4.123
Password: spladmin123!

Lab access will expire in approximately 120 minutes

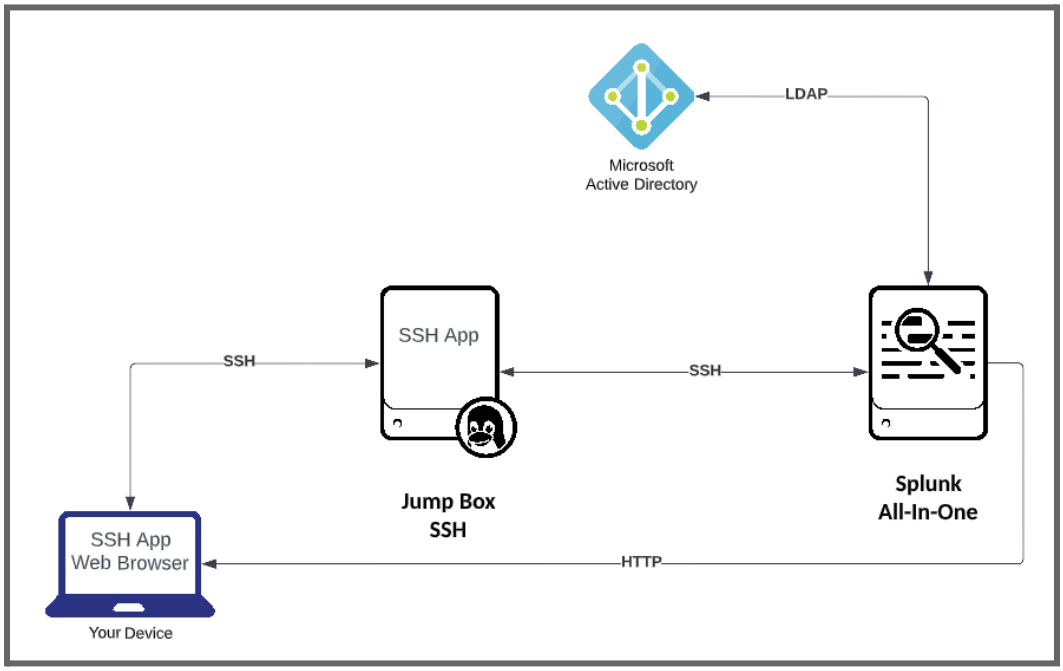
Please follow the lab guidance at http://bsides22.docs.studyclub.community

Please join our splunk-usergroups Slack channel at http://splunk-slack.studyclub.community

Thanks
GAS Admin
Global Academy for Splunk (GAS)
bitsIO Inc.

If you would like to leverage the bitsIO Global Academy for Splunk (GAS) for your organisation please book a call with us at https://bitsioinc.com/lets.talk.gas

GAS Lab Environment



Splunk All-In-One
This is a standard Splunk instance. It is referred to as an all-in-one as all default features are enabled. The URL and credentials for your instance is listed in the second email.

Jump Box
This is a Linux server that is created as security best practice. It is used for accessing the backend/command-line of the all-in-one instance. Essentially, you will access this jump box directly via its public address using an SSH client. From there you will access the all-in-one instance via its private address using the same SSH client session. We refer to this as a Jump Box. Others may refer to it as a Jump Host.

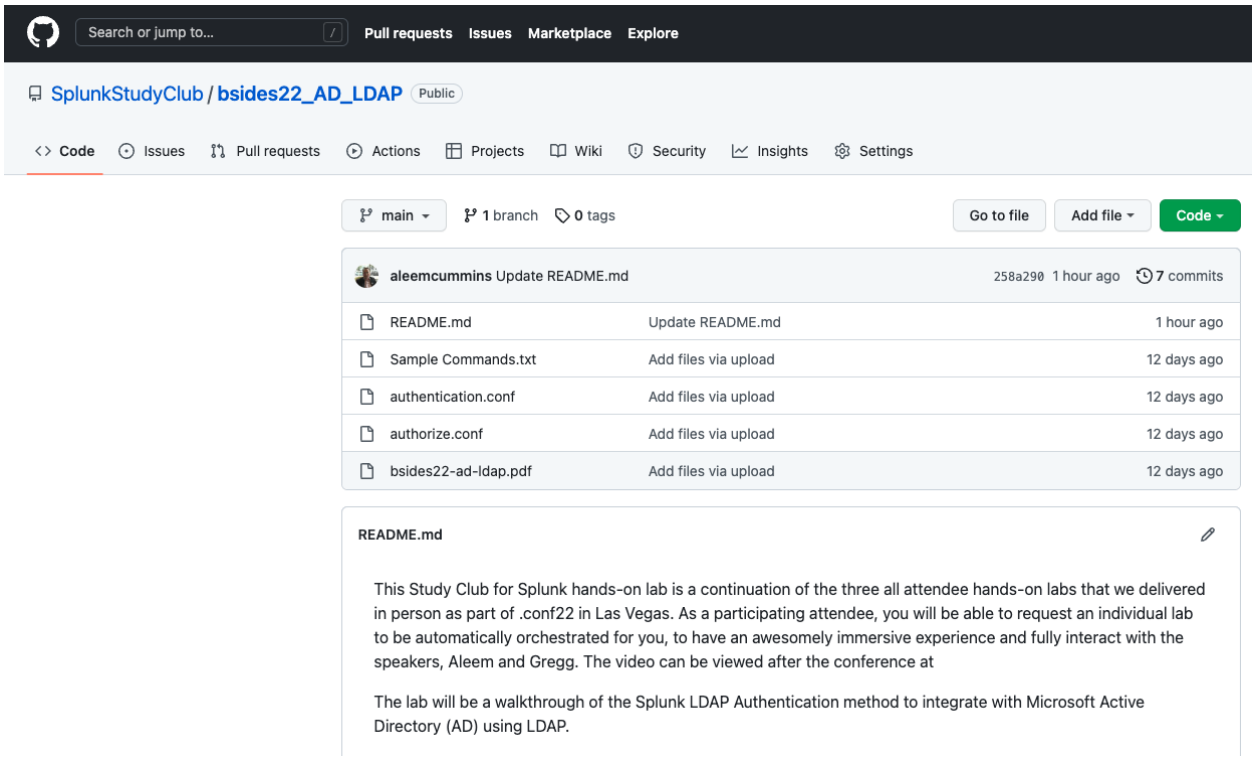
For reference, a jump server is located in what is known as a Demilitarised Zone (DMZ). This is a special network arrangement where servers within this zone are accessible from a private network and a public network. This allows us to keep servers on pirate networks more secure while still being accessible as needed. SSH uses port 22.

We have purposely kept the diagram high level and avoided overlaying the entire system architecture. For a more detailed architecture please see your session from BSides SPL 21 at http://bsides21.video.studyclub.community

Microsoft Active Directory (AD)
This is a Windows server instance running AD. We have pre-built users and groups as laid out in Appendix A. We map Splunk roles to these groups.

GitHub Repositories

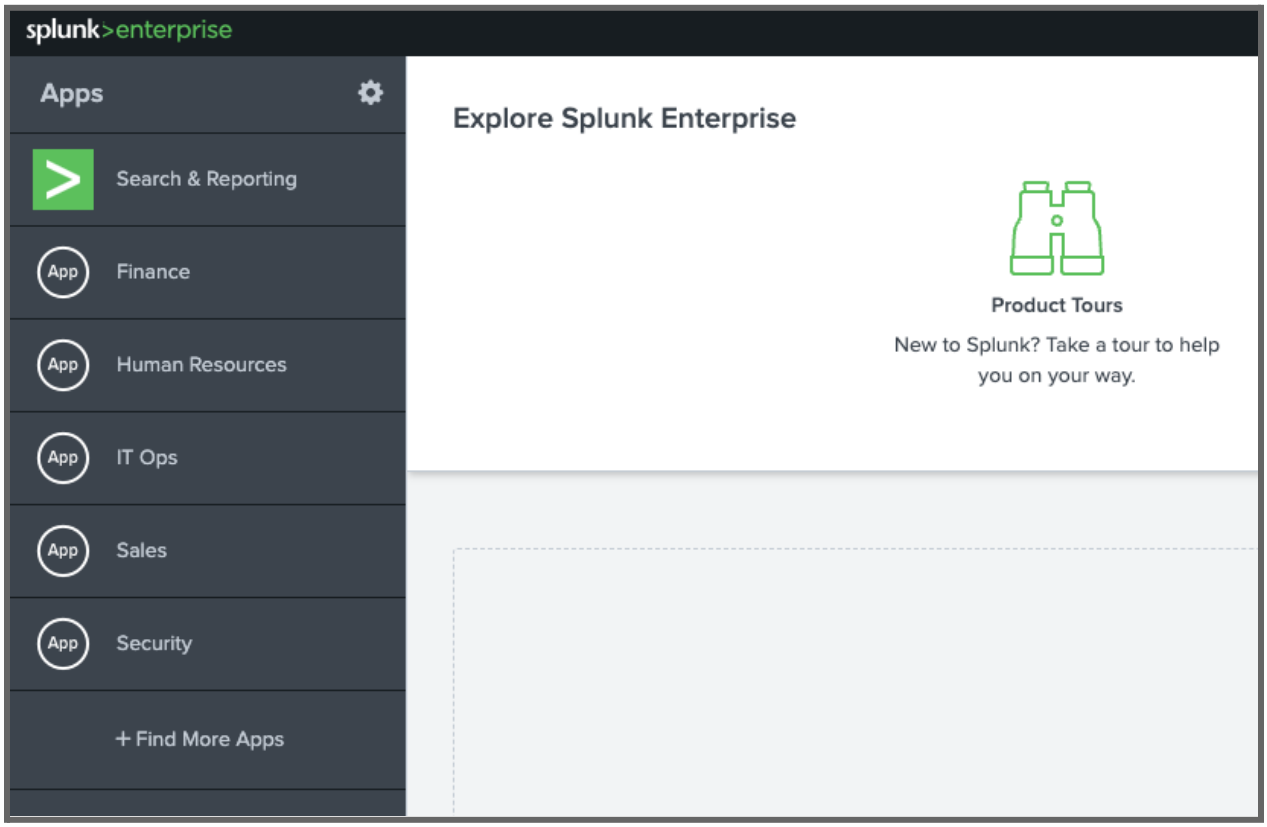
The Study Club for Splunk GitHub repositories are located at http://github.studyclub.community
All of the assets from our previous work are available there.



Step 2 - Login to Splunk

Access the Splunk instance via the link and credentials from the second email

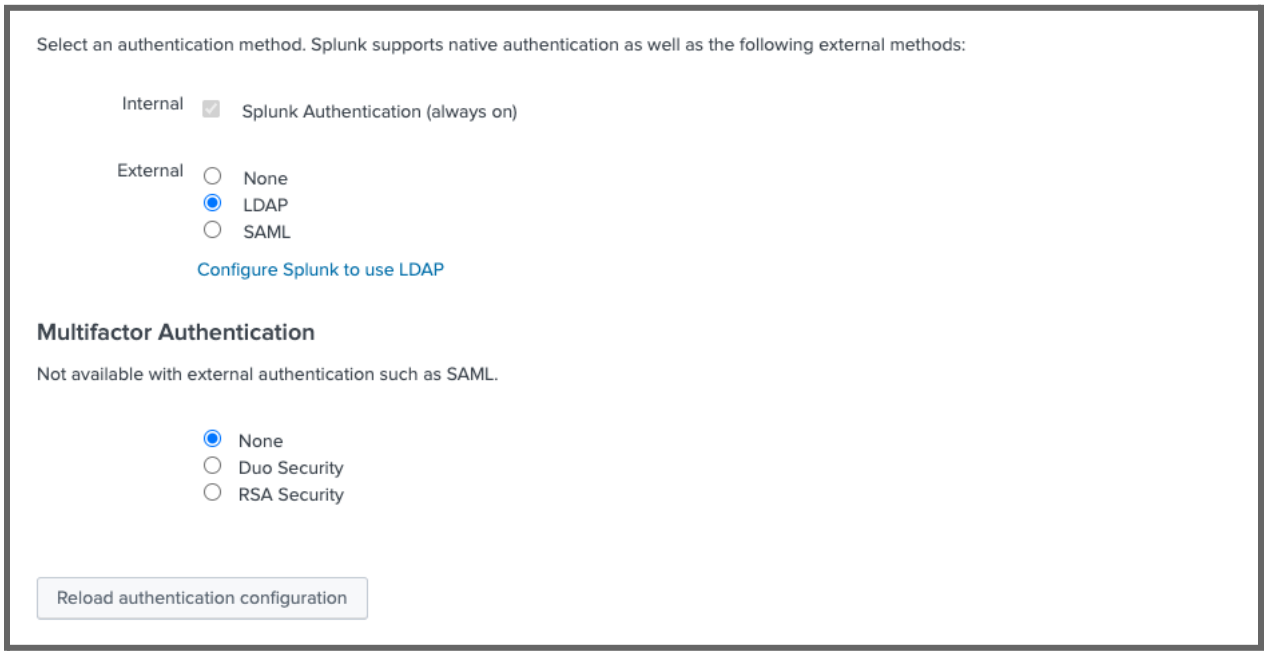
Notice that there are five custom apps visible to you as the admin user



Step 3 - Configure LDAP

For this session we will be configuring LDAP Authentication

Click **Settings** followed by **Authentication Methods**



Super Useful Resources

We wholeheartedly recommend as essential learning

- "The Practical User's Guide for Setting up LDAP in Splunk". It was created by SplunkTrust member, Tom Kopchak over at Hurricane Labs. Check it out at https://hurricanelabs.com/splunk-tutorials/the-practical-users-guide-for-setting-up-ldap-in-splunk/
- Live Demo of SAML (OKTA) and LDAP from a Dallas Fort Worth user group session. Logan Carter and Dustin Church go into truly amazing detail . Check it out at https://bit.ly/saml-ldap-okta

Click **Configure Splunk to use LDAP**

Click **New LDAP** green button 

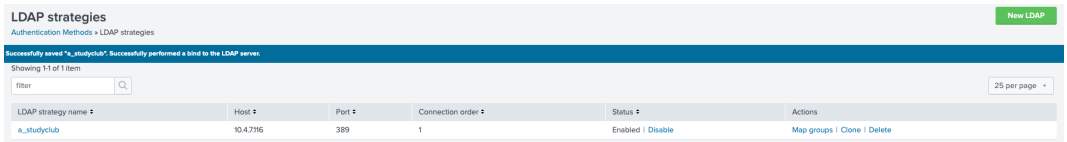
We talk through these settings in the video. **Be sure to use LDAP host IP provided with the second email**. The LDAP password is fixed for the lab.

LDAP strategy name * Enter a unique name for this strategy.	a_studyclub
LDAP connection settings	
Host * Your Splunk server must be able to resolve this host.	10.4.7.116 - example
Port The LDAP server port defaults to 389 if you are not using SSL, or 636 if SSL is enabled. ☐ SSL enabled You must also have SSL enabled on your LDAP server.	389
Bind DN This is the distinguished name used to bind to the LDAP server. This is typically the DN of an administrator with access to all LDAP users you wish to add to Splunk. However, you can leave this blank if anonymous bind is sufficient.	CN=SplunkAdmin Student,CN=Manage d Service Accounts,DC=bitsio,D C=local
Bind DN Password Enter the password for your Bind DN user.	
Confirm password	spladmin123!

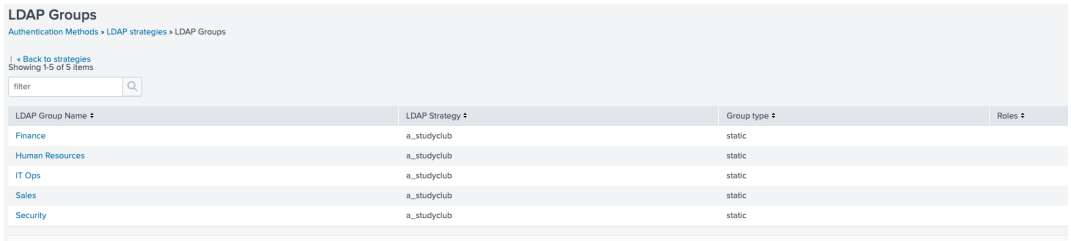
User settings	
User base DN * The location of your LDAP users, specified by the DN of your user subtree. If necessary, you can specify several DNs separated by semicolons.	CN=Users,DC=bit sio,DC=local
User base filter The LDAP search filter used to filter users. Highly recommended if you have a large amount of user entries under your user base DN. For example, '(department=IT)'	
User name attribute * The user attribute that contains the username. Note that this attribute's value should be case insensitive. Set to 'uid' for most configurations. In Active Directory (AD), this should be set to 'sAMAccountName'.	samaccountname
Real name attribute * The user attribute that contains a human readable name. This is typically 'cn' (common name) or 'displayName'.	cn
Email attribute The user attribute that contains the user's email address. This is typically 'mail'.	mail
Group mapping attribute The user attribute that group entries use to define their members. If your LDAP groups use distinguished names for membership you can leave this field blank.	dn

Group settings Group base DN * The location of your LDAP groups, specified by the DN of your group subtree. If necessary, you can specify several DNs separated by semicolons. Static group search filter The LDAP search filter used to retrieve static groups. Highly recommended if you have a large amount of group entries under your group base DN. For example, '(department=IT)' Group name attribute * The group attribute that contains the group name. A typical value for this is 'cn'. Static member attribute * The group attribute whose values are the group's members. Typical values are 'member' or 'memberUid'. Groups list user members with values of groupMappingAttribute, as specified above. ☐ Nested groups Controls whether Splunk will expand nested groups using the 'memberof' extension. Only check this if you have nested groups and the 'memberof' extension on your LDAP server. **Dynamic group settings** Dynamic member attribute The dynamic group attribute that contains the LDAP URL used to find members. This setting is required to configure dynamic groups. A typical value is 'memberURL'. Dynamic group search filter The LDAP search filter used to retrieve dynamic groups (optional). For example, '(objectclass=groupOfURLs)' ☐ Advanced settings Cancel Save	OU=Splunk,DC=bitsio,DC=local cn member

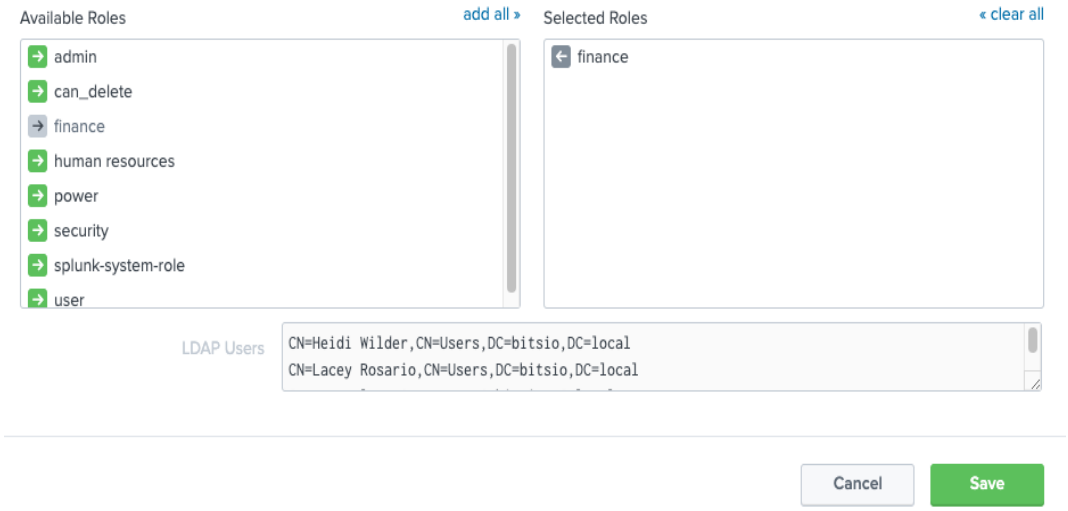
Click the green SAVE button



Step 4 - Map AD Groups to Splunk Roles



Click Finance

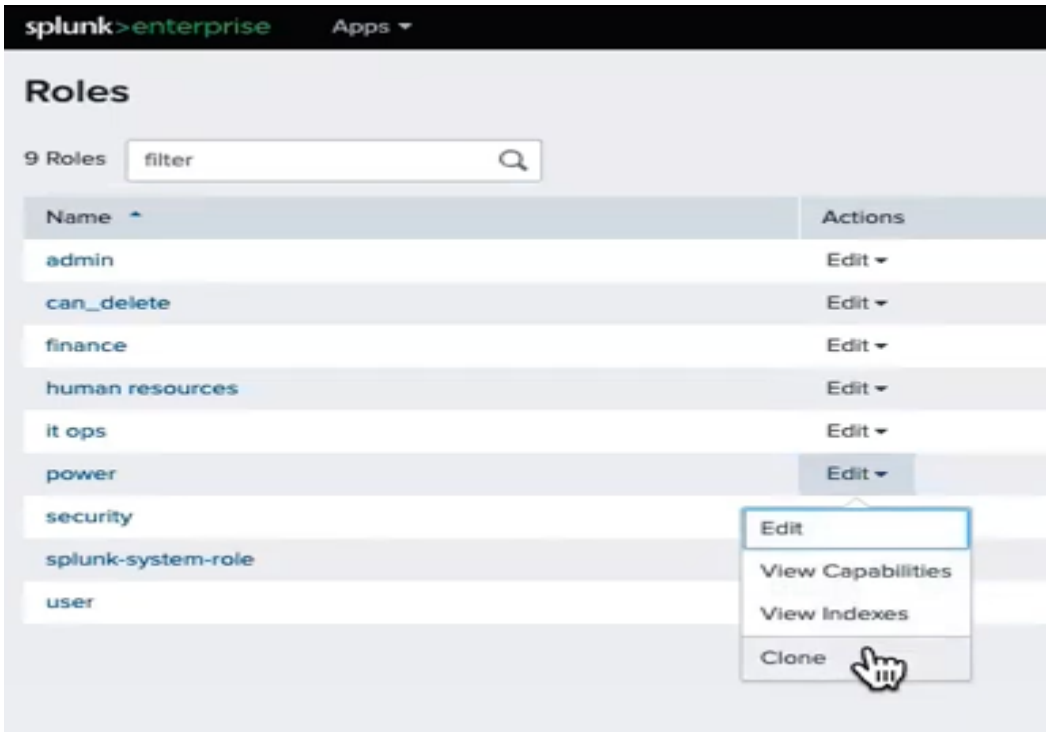


Click finance under “Available Roles”
Click green Save button

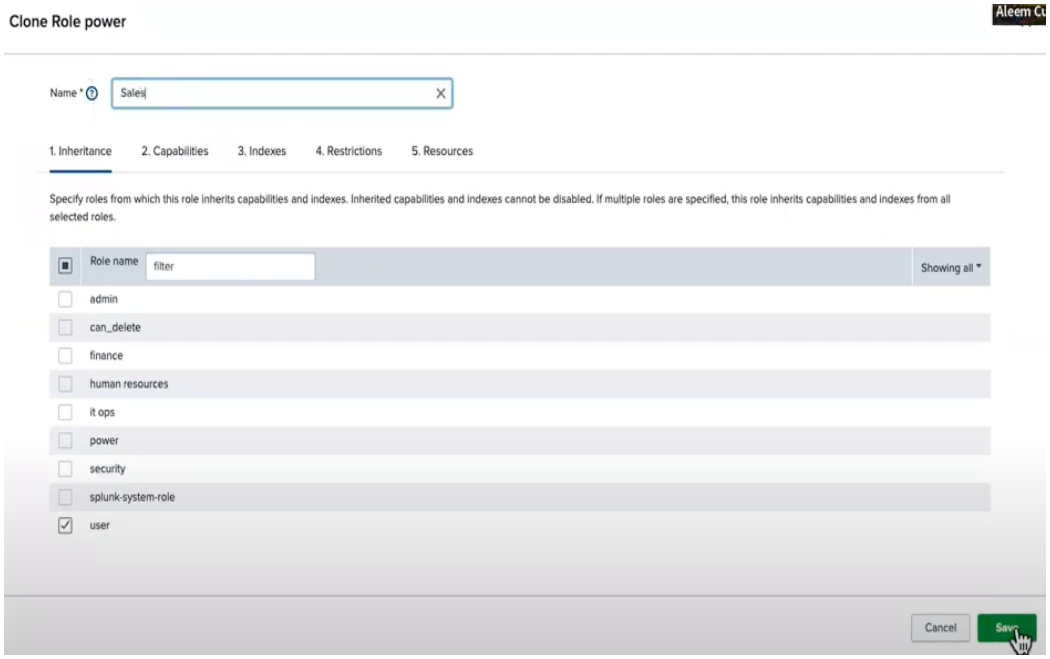
Repeat for **Security** and **Human Resources** AD Groups

Notice that there are no existing Splunk roles for **IT Ops** and **Sales**
Let's start adding those roles by clicking on **Settings** followed by **Roles**

Click the down arrow in the **Actions** column for **power** role and select **Clone**



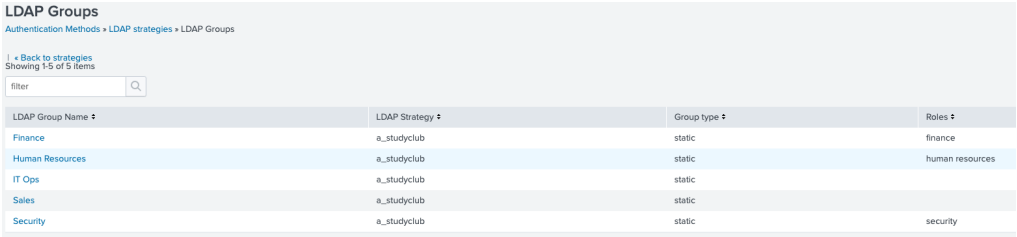
Add **Sales** as Name



Repeat to add **IT Ops** role

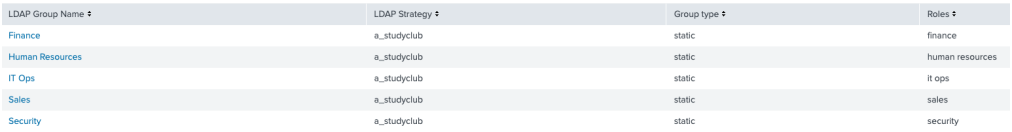
Now we need to Map AD Groups to these newly created Splunk Roles

Click **Settings** followed by **Authentication Methods**
Check the **LDAP** radio button followed by **LDAP Settings**
Click **Map groups** from the **Actions** column



Click **IT Ops** and repeat steps from earlier
Click **Sales** and repeat steps from earlier

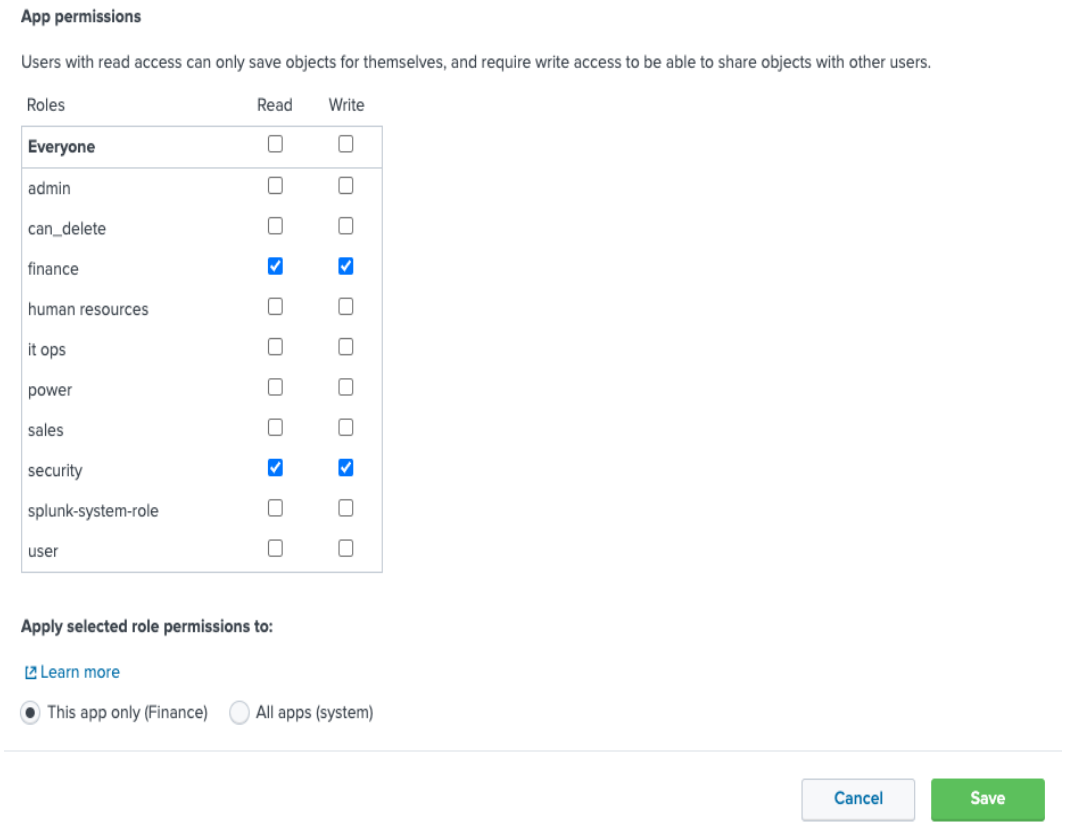
All Splunk roles are now mapped to AD Groups



Step 4 - Configure App Permissions

Lock down permissions for finance app to finance role

Security role is also added as best practice



Repeat to

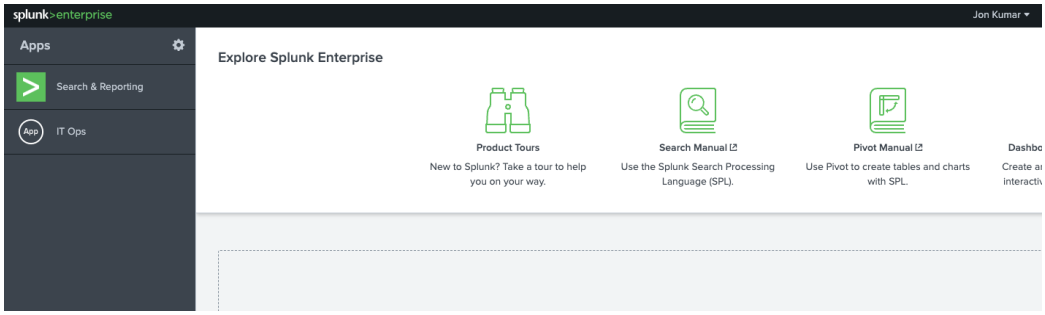
- Lock down permissions for IT Ops app to IT Ops role
- Lock down permissions for Sales app to Sales role
- Lock down permissions for Security app to Security role
- Lock down permissions for Human Resources app to Human Resources role

Step 5 - Test LDAP Authentication Configuration

Let's validate our configuration by logging in as users from multiple AD groups. The apps listed should match the permissions we applied.

Test 1

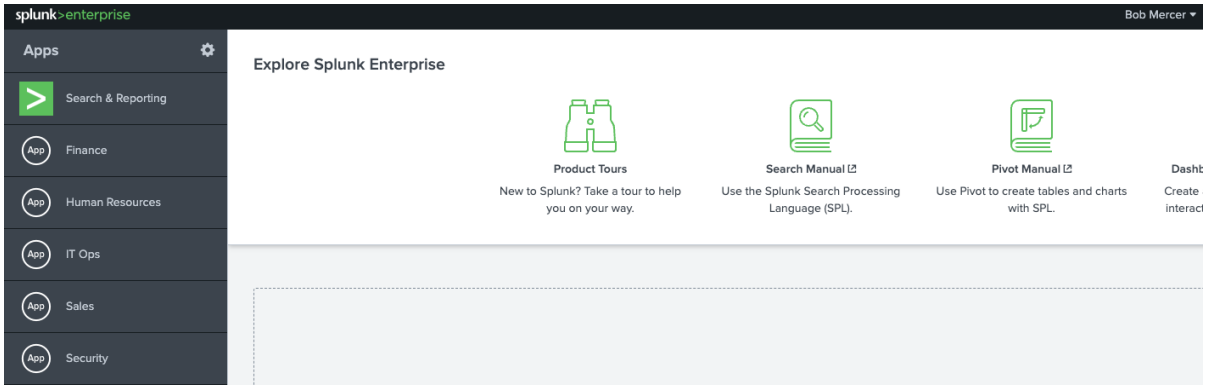
Logout as **Admin** user
Login as IT Ops user **jon.kumar** with password **spljk123!**



Jon from the IT Ops Splunk role mapped to the AD Group IT Ops can only see the IT Ops dashboard as anticipated.
Logout as **jon.kumar** user

Test 2

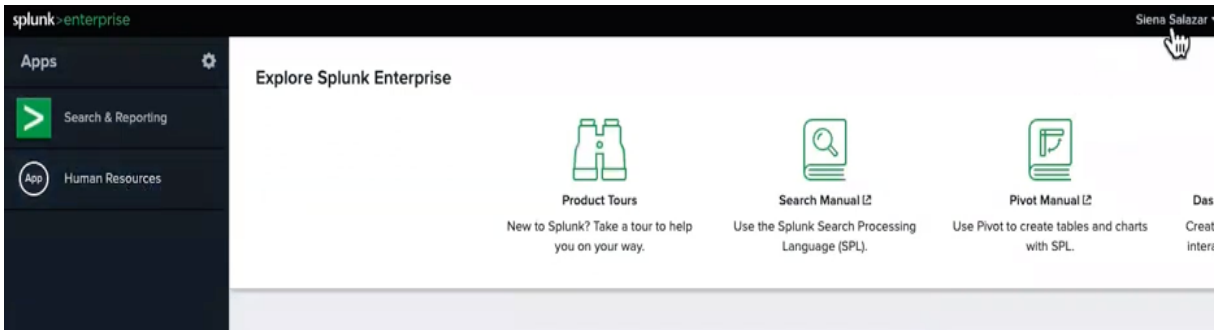
Login as Security user **bob.mercer** with password **splbm123!**



Bob from the Security Splunk role mapped to the AD Group Security can see the Security dashboard and also the dashboards from Sales, Human Resources, IT Ops and Finance as anticipated.
Logout as **bob.mercer** user

Test 3

Login as Human Resources user **siena.salazar** with password **splbm123!**



Bob from the Security Splunk role mapped to the AD Group Security can see the Security dashboard and also the dashboards from Sales, Human Resources, IT Ops and Finance as anticipated.

Logout as **siena.salazar** user

A complete list of AD Groups and Users can be seen in Appendix A. Feel free to play around with the app permissions on the UI or even in the CLI to aid your shared learning

Step 6 - View Configuration Files

SSH Client Application

To fully participate in the lab you will need an SSH client on your computer. If you do not own your computer, please speak to your IT support team. The following are common options

Name	OS	Download
PuTTY	Windows	https://www.putty.org
MobaXterm	Windows	https://mobaxterm.mobatek.net
Terminal	Mac	Built into Mac OS
iTerm2	Mac	https://iterm2.com

Tip: When pasting commands from applications such as pdf readers, non printing characters may also be inadvertently copied. If this happens, then the commands will look okay but simply not run.

```
#Required btool command
/opt/splunk/bin/splunk cmd btool authorize list --debug | grep /local

#Non printing character pollution
/opt/splunk/bin/splunk cmd btool authorize list --debug | grep /local
```

The sample commands can be safely copied from
http://bsides22.commands.studyclub.community
Or alternatively, copying to an application such as Microsoft Visual Studio Code and copying again from there will solve this.

Access Jump Box via SSH

```
aleem@MacBook-Pro-8 .ssh % ssh studyclub@bitsio-gas-kig8uk-bsides22-ad-ldap-jumpbox.gas.bitsioservices.com
The authenticity of host 'bitsio-gas-kig8uk-bsides22-ad-ldap-jumpbox.gas.bitsioservices.com (54.81.250.184)' can't be established.
ED25519 key fingerprint is SHA256:AYOCk5LcN4XwuGn73HF/oT37noz5StCwWBwOynC9i3E.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'bitsio-gas-kig8uk-bsides22-ad-ldap-jumpbox.gas.bitsioservices.com' (ED25519) to the list of known hosts.
studyclub@bitsio-gas-kig8uk-bsides22-ad-ldap-jumpbox.gas.bitsioservices.com's password:
Last login: Wed Oct  5 11:00:20 2022 from cpc138124-hatf10-2-0-cust290.9-3.cable.virginm.net

  ___ _          _        ___ _     _
 / __| |_ _  _ __| |_  _   / __| |_  _| |__
 \__ \  _| || / _` | || | | (__| | || | '_ \  Powered by GAS
 |___/\__|\_,_\__,_|\_, |  \___|_|\_,_|_.__/
                    |__/

[studyclub@bitsio-gas-kig8uk-bsides22-ad-ldap-jumpbox ~]$
```

An example of the command format is as follows

```
ssh nickname@bitsio-gas-kig8uk-bsides22-ad-ldap-jumpbox.gas.bitsioservices.com
```

The first time around you will need to add the fingerprint for the servers by typing **yes**. You will then be challenged for the **password**

The exact command and the password will be included in the second email

Access All-In-One Splunk Instance via SSH

An example of the command format is as follows

```
ssh nickname@10.4.7.14
```

The first time around you will need to add the fingerprint for the servers by typing **yes**. You will then be challenged for the **password.** Please note here that the connection is to the internal IP address.

The exact command and the password will be included in the second email

```
aleem@MacBook-Pro-8 .ssh % ssh studyclub@bitsio-gas-kig8uk-bsides22-ad-ldap-jumpbox.gas.bitsioservices.com
The authenticity of host 'bitsio-gas-kig8uk-bsides22-ad-ldap-jumpbox.gas.bitsioservices.com (54.81.250.184)' can't be established.
ED25519 key fingerprint is SHA256:AYOCk5LcN4XwuGn73HF/oT37noz5StCwWBwOynC9i3E.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'bitsio-gas-kig8uk-bsides22-ad-ldap-jumpbox.gas.bitsioservices.com' (ED25519) to the list of known hosts.
studyclub@bitsio-gas-kig8uk-bsides22-ad-ldap-jumpbox.gas.bitsioservices.com's password:
Last login: Wed Oct  5 11:00:20 2022 from cpc138124-hatf10-2-0-cust290.9-3.cable.virginm.net

  ___ _           _         ___ _      _
 / __| |_ _  _ __| |_  _   / __| |_  _| |__
 \__ \  _| || / _` | || | | (__| | || | '_ \  Powered by GAS
 |___/\__|\_,_\__,_|\_, |  \___|_|\_,_|_.__/
                    |__/

[studyclub@bitsio-gas-kig8uk-bsides22-ad-ldap-jumpbox ~]$ ssh studyclub@10.4.5.163
The authenticity of host '10.4.5.163 (10.4.5.163)' can't be established.
ECDSA key fingerprint is SHA256:SVLVW1Yq5mOZpcKDqvvUsqjXvaaVnJuBR44SqwSnfPA.
ECDSA key fingerprint is MD5:9c:f2:34:4f:85:19:3f:b5:f2:fe:0a:8f:8f:98:1c:43.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.4.5.163' (ECDSA) to the list of known hosts.
studyclub@10.4.5.163's password:
Last login: Wed Oct  5 11:00:35 2022 from ip-10-4-7-14.ec2.internal

  ___ _           _         ___ _      _
 / __| |_ _  _ __| |_  _   / __| |_  _| |__
 \__ \  _| || / _` | || | | (__| | || | '_ \  Powered by GAS
 |___/\__|\_,_\__,_|\_, |  \___|_|\_,_|_.__/
                    |__/

[studyclub@bitsio-gas-kig8uk-bsides22-ad-ldap-node ~]$
```

BTOOL

Btool is a command line utility for troubleshooting splunk configurations. If ships with Splunk. We know that Splunk configurations can exist in many places. Btool will merge all configurations that have been written to disk and display the merged configurations. We did a Study Club for Splunk session at .conf21 all about how btool is your friend. It absolutely is. Splunk docs has this covered at https://docs.splunk.com/Documentation/Splunk/latest/Troubleshooting/Usebtooltotroubleshootconfigurations

Tip: Splunk does not need to be running to use btool

Locate Roles Configuration File

authorize.conf is the configuration file for storing role configuration in Splunk. This file is relied upon by the Splunk UI when we map AD Groups to Splunk Roles. To locate this file we use the following command assuming install folder is /opt/splunk

```
/opt/splunk/bin/splunk cmd btool authorize list --debug | grep /local
```

This command will be executed under the user which you are logged in as. In the lab, Splunk is running under the account of ‘splunk’. This will mean that your command will fail on permissions

```
[studyclub@bitsio-gas-kig8uk-bsides22-ad-ldap-node ~]$ /opt/splunk/bin/splunk cmd btool authorize list --debug | grep /local
Please run 'splunk ftr' as boot-start user
```

To run the command, you will need to run as the user account ‘splunk’. This is achieved using the sudo command.

```
[studyclub@bitsio-gas-kig8uk-bsides22-ad-ldap-node ~]$ sudo su splunk
```

The output will then display the location of authorize.conf

```
/opt/splunk/etc/system/local/authorize.conf        [role_sales]
/opt/splunk/etc/system/local/authorize.conf        cumulativeRTSrchJobsQuota = 200
/opt/splunk/etc/system/local/authorize.conf        cumulativeSrchJobsQuota = 100
/opt/splunk/etc/system/local/authorize.conf        edit_log_alert_event = enabled
/opt/splunk/etc/system/local/authorize.conf        edit_sourcetypes = enabled
/opt/splunk/etc/system/local/authorize.conf        edit_statsd_transforms = enabled
/opt/splunk/etc/system/local/authorize.conf        embed_report = enabled
/opt/splunk/etc/system/local/authorize.conf        importRoles = user
/opt/splunk/etc/system/local/authorize.conf        metric_alerts = enabled
/opt/splunk/etc/system/local/authorize.conf        rtSrchJobsQuota = 20
/opt/splunk/etc/system/local/authorize.conf        rtsearch = enabled
/opt/splunk/etc/system/local/authorize.conf        run_msearch = enabled
/opt/splunk/etc/system/local/authorize.conf        schedule_search = enabled
/opt/splunk/etc/system/local/authorize.conf        search_process_config_refresh = enabled
/opt/splunk/etc/system/local/authorize.conf        srchDiskQuota = 500
/opt/splunk/etc/system/local/authorize.conf        srchIndexesAllowed = *;main
/opt/splunk/etc/system/local/authorize.conf        srchIndexesDefault = main
/opt/splunk/etc/system/local/authorize.conf        srchJobsQuota = 10
/opt/splunk/etc/system/local/authorize.conf        srchMaxTime = 8640000
```

We can then use the view command to examine the content of the file

```
[splunk@bitsio-gas-kig8uk-bsides22-ad-ldap-node studyclub]$ view /opt/splunk/etc/system/local/authorize.conf
```

```
[role_human resources]
cumulativeRTSrchJobsQuota = 200
cumulativeSrchJobsQuota = 100
edit_log_alert_event = enabled
edit_sourcetypes = enabled
edit_statsd_transforms = enabled
embed_report = enabled
importRoles = user
metric_alerts = enabled
rtSrchJobsQuota = 20
rtsearch = enabled
run_msearch = enabled
schedule_search = enabled
search_process_config_refresh = enabled
srchDiskQuota = 500
srchIndexesAllowed = *;main
srchIndexesDefault = main
srchJobsQuota = 10
srchMaxTime = 8640000

[role_security]
cumulativeRTSrchJobsQuota = 200
cumulativeSrchJobsQuota = 100
edit_log_alert_event = enabled
edit_sourcetypes = enabled
edit_statsd_transforms = enabled
embed_report = enabled
importRoles = user
metric_alerts = enabled
rtSrchJobsQuota = 20
rtsearch = enabled
run_msearch = enabled
schedule_search = enabled
search_process_config_refresh = enabled
srchDiskQuota = 500
srchIndexesAllowed = *;main
srchIndexesDefault = main
srchJobsQuota = 10
srchMaxTime = 8640000
```

An example file can been seen on our gitHub repository at
https://github.com/SplunkStudyClub/bsides22_AD_LDAP/blob/main/authorize.conf

Locate Authentication Configuration File

authentication.conf is the configuration file for storing authentication configuration in Splunk. This configuration is relied upon by Splunk when connecting to external authentication systems. To locate this file we use the following command assuming install folder is /opt/splunk

```
/opt/splunk/bin/splunk cmd btool authentication list --debug | grep /local
```

```
[splunk@bitsio-gas-kig8uk-bsides22-ad-ldap-node studyclub]$ /opt/splunk/bin/splunk cmd btool authentication list --debug | grep /local
/opt/splunk/etc/system/local/authentication.conf   [a_studyclub]
/opt/splunk/etc/system/local/authentication.conf   SSLEnabled = 0
/opt/splunk/etc/system/local/authentication.conf   anonymous_referrals = 1
/opt/splunk/etc/system/local/authentication.conf   bindDN = CN=SplunkAdmin Student,CN=Managed Service Accounts,DC=bitsio,DC=local
/opt/splunk/etc/system/local/authentication.conf   bindDNpassword = $7$Wjk5qU8wPe63iHxXHISyEDgX6SpimfJQH7Kd3WYteBn3zIA+/in+bsbAZ5A=
/opt/splunk/etc/system/local/authentication.conf   charset = utf8
/opt/splunk/etc/system/local/authentication.conf   emailAttribute = mail
/opt/splunk/etc/system/local/authentication.conf   enableRangeRetrieval = 0
/opt/splunk/etc/system/local/authentication.conf   groupBaseDN = OU=Splunk,DC=bitsio,DC=local
/opt/splunk/etc/system/local/authentication.conf   groupMappingAttribute = dn
/opt/splunk/etc/system/local/authentication.conf   groupMemberAttribute = member
/opt/splunk/etc/system/local/authentication.conf   groupNameAttribute = cn
/opt/splunk/etc/system/local/authentication.conf   host = 10.4.7.116
/opt/splunk/etc/system/local/authentication.conf   nestedGroups = 0
/opt/splunk/etc/system/local/authentication.conf   network_timeout = 20
/opt/splunk/etc/system/local/authentication.conf   pagelimit = -1
/opt/splunk/etc/system/local/authentication.conf   port = 389
/opt/splunk/etc/system/local/authentication.conf   realNameAttribute = cn
/opt/splunk/etc/system/local/authentication.conf   sizelimit = 1000
/opt/splunk/etc/system/local/authentication.conf   timelimit = 15
/opt/splunk/etc/system/local/authentication.conf   userBaseDN = CN=Users,DC=bitsio,DC=local
/opt/splunk/etc/system/local/authentication.conf   userNameAttribute = samaccountname
/opt/splunk/etc/system/local/authentication.conf   [authentication]
/opt/splunk/etc/system/local/authentication.conf   authSettings = a_studyclub
/opt/splunk/etc/system/local/authentication.conf   authType = LDAP
/opt/splunk/etc/system/local/authentication.conf   [roleMap_a_studyclub]
/opt/splunk/etc/system/local/authentication.conf   finance = Finance
/opt/splunk/etc/system/local/authentication.conf   human resources = Human Resources
/opt/splunk/etc/system/local/authentication.conf   it ops = IT Ops
/opt/splunk/etc/system/local/authentication.conf   sales = Sales
/opt/splunk/etc/system/local/authentication.conf   security = Security
```

We can then use the view command to examine the content of the file

```
[splunk@bitsio-gas-kig8uk-bsides22-ad-ldap-node studyclub]$ view /opt/splunk/etc/system/local/authentication.conf
```

```
[a_studyclub]
SSLEnabled = 0
anonymous_referrals = 1
bindDN = CN=SplunkAdmin Student,CN=Managed Service Accounts,DC=bitsio,DC=local
bindDNpassword = $7$Wjk5qU8wPe63iHxXHISyEDgX6SpimfJQH7Kd3WYteBn3zIA+/in+bsbAZ5A=
charset = utf8
emailAttribute = mail
enableRangeRetrieval = 0
groupBaseDN = OU=Splunk,DC=bitsio,DC=local
groupMappingAttribute = dn
groupMemberAttribute = member
groupNameAttribute = cn
host = 10.4.7.116
nestedGroups = 0
network_timeout = 20
pagelimit = -1
port = 389
realNameAttribute = cn
sizelimit = 1000
timelimit = 15
userBaseDN = CN=Users,DC=bitsio,DC=local
userNameAttribute = samaccountname

[authentication]
authSettings = a_studyclub
authType = LDAP

[roleMap_a_studyclub]
finance = Finance
human resources = Human Resources
it ops = IT Ops
sales = Sales
security = Security
```

An example file can been seen on our gitHub repository at authentication.conf
https://github.com/SplunkStudyClub/bsides22_AD_LDAP/blob/main/authentication.conf

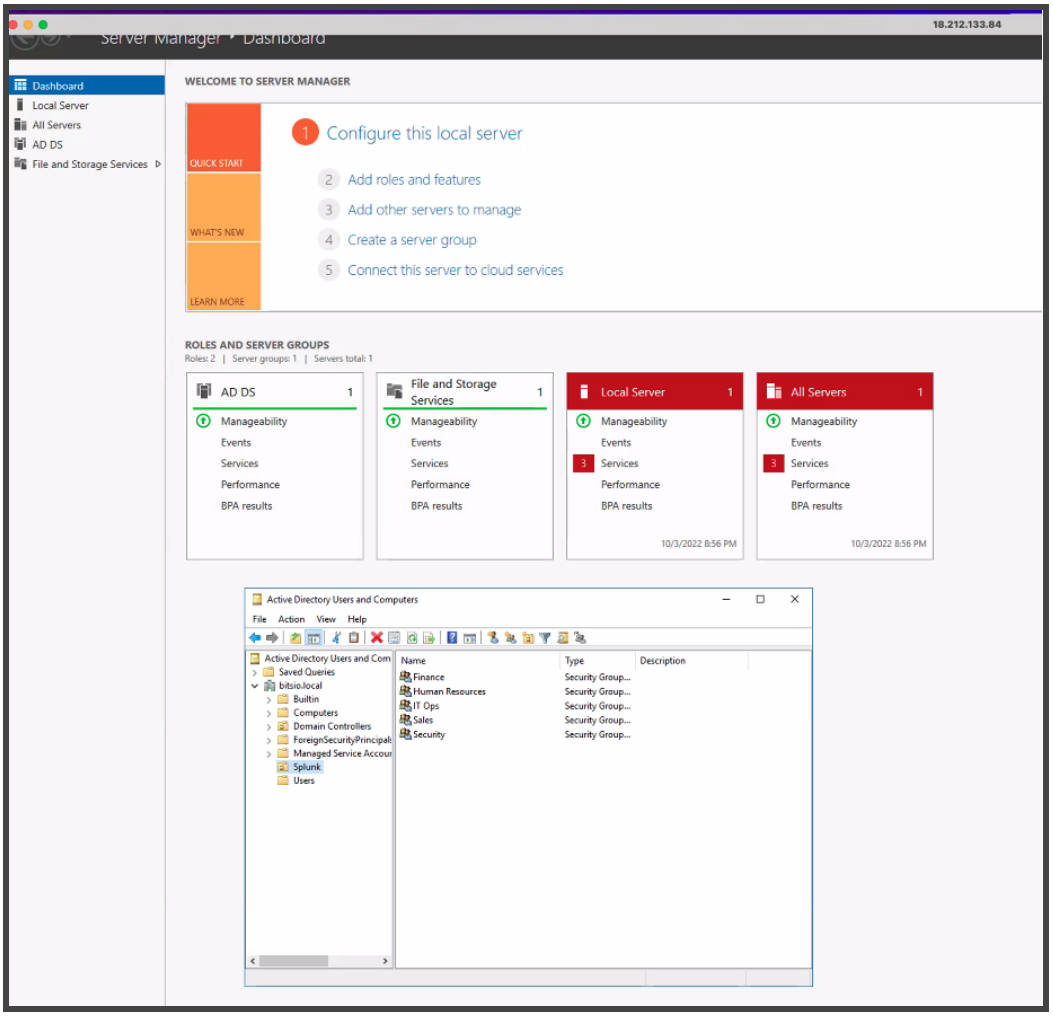
The LDAP password is hashed when configuration is saved using the UI or when Splunk is restarted is added using the command line

Appendix A - AD Groups and Users

AD Group	AD User	AD Username	AD User Password
IT Ops	Jon Kumar	jon.kumar	spljk123!
	Laurel Carson	laurel.carson	spllc123!
	Sally Pitts	sally.pitts	splsp123!
Security	Gita Singh	gita.singh	splgs123!
	Bob Mercer	bob.mercer	splbm123!
	Rita Murphy	rita.murphy	splrm123!
Finance	Heidi Wilder	heidi.wilder	splhw123!
	Lacey Rosario	lacey.rosario	spllr123!
	Rea Nelson	rea.nelson	splrn123!
Human Resources	Siena Salazar	siena.salazar	splss123!
	Jude Fountain	jude.fountain	spljf123!
	Otto Bull	otto.bull	splob123!
Sales	Tia Lister	tia.lister	spltl123!
	Emma Kenny	emma.kenny	splek123!
	Brent Ireland	brent.ireland	splbi123!

Appendix B - Microsoft Active Directory (AD)

The study club lab includes a configured Microsoft AD. It is accessible via the Splunk LDAP configuration only. For reference, this is what the user interface looks like for the lab.



Watch Logan Carter and Dustin Church go into greater detail in their session video at https://bit.ly/saml-ldap-okta