

Splunk4Admins - User Management

Lab Guide

Overview

This lab guide contains the hands-on exercises for the Splunk4Admins - User Management workshop. Before proceeding with these exercises, please ensure that you have a copy of the workshop slide deck, which will help to put into context the tasks you are carrying out, as well as the cheat sheet.

Download the workshop slide deck: <https://splk.it/S4A-UM-Attendee>

Download the workshop cheat sheet: <https://splk.it/S4A-UM-Cheat-Sheet>

Prerequisites

In order to complete these exercises, you will need your own Splunk instance. Splunk's hands-on workshops are delivered via the [Splunk Show portal](#), and you will need a splunk.com account in order to access this.

If you don't already have a Splunk.com account, please create one [here](#) before proceeding with the rest of the workshop.

Troubleshooting Connectivity

If you experience connectivity issues with accessing either your workshop environment or the event page, please try the following troubleshooting steps. If you still experience issues please reach out to the team running your workshop.

- **Use Google Chrome** (if you're not already)
- If the event page (i.e. <https://show.splunk.com/event/<eventID>>) didn't load when you clicked on the link, try **refreshing the page**
- **Disconnect from VPN** (if you're using one)
- **Clear your browser cache and restart your browser** (if using Google Chrome, go to: Settings > Privacy and security > Clear browsing data)
- **Try using private browsing mode** (e.g. Incognito in Google Chrome) to rule out any cache issues
- **Try using another computer** such as your personal computer - all you need is a web browser! Cloud platforms like AWS can often be blocked on corporate laptops.

Table of Contents

Overview.....	1
Table of Contents.....	2
Exercise 1 – Configure a Role.....	3
Description.....	3
Steps.....	3
Exercise 2 – Connect Splunk to Active Directory.....	15
Description.....	15
Steps.....	15
Exercise 3 – Associate Splunk Roles to Active Directory Groups.....	20
Description.....	20
Steps.....	20
Exercise 4: Validate users/group/role membership.....	25
Description.....	25
Steps.....	25
Links.....	27

Exercise 1 – Configure a Role

Description

Create a role that has a specific set of configuration settings to meet the Use Case.

Use case: Dashboard Developer for Finance organized (Build dashboards for Finance to better understand the Finance Department)

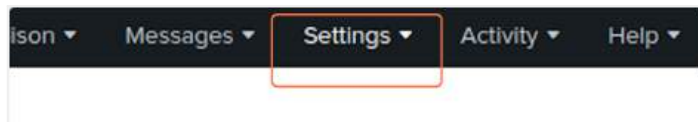
- Understand the requirements for the Use Case:

Needs to be able to:

- ✓ Build dashboards
- ✓ Run searches (including metrics)
- ✓ Schedule searches
- ✓ Install and edit apps
- ✓ Access specific indexes
- ✓ Limit the number of searches that can be executed concurrently
- ✓ No real-time searches

Steps

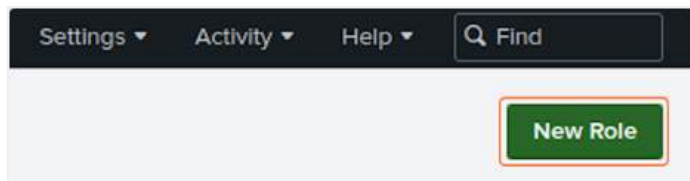
1. Click on **Settings**



2. Click on **Roles**



3. Click on the green **New Role** button



4. Type "buttercup_finance_dev_reports"

New Role

Name *

1. Inheritance 2. Capabilities 3. Indexes 4. Restrictions 5. Resource

Specify roles from which this role inherits capabilities and indexes. Inherited capabilities and indexes are enabled. If multiple roles are specified, this role inherits capabilities and indexes from all selected roles.

<input type="checkbox"/>	Role name	<input type="text" value="filter"/>
<input type="checkbox"/>	admin	
<input type="checkbox"/>	buttercup_base_power	
<input type="checkbox"/>	buttercup_base_user	
<input type="checkbox"/>	can_delete	
<input type="checkbox"/>	power	
<input type="checkbox"/>	splunk-system-role	
<input type="checkbox"/>	user	

5. "1. Inheritance" will already be selected. Click on the role from which to inherit the configuration. In this case, select the already created role called "buttercup_base_power". Also scan down the list of other roles to ensure that no other roles are selected.

1. Inheritance 2. Capabilities

Specify roles from which this role inherits capabilities and indexes. Inherited capabilities and indexes are enabled. If multiple roles are specified, this role inherits capabilities and indexes from all selected roles.

<input type="checkbox"/>	Role name	<input type="text" value="filter"/>
<input type="checkbox"/>	admin	
<input type="checkbox"/>	buttercup_base_power	
<input type="checkbox"/>	buttercup_base_user	

6. Select the next tab “**2. Capabilities**”

New Role

Name * ? buttercup_finance_dev_reports

1. Inheritance **2. Capabilities** 3. Indexes 4. Restrict

Specify roles from which this role inherits capabilities and indexes. In disabled. If multiple roles are specified, this role inherits capabilities a

<input type="checkbox"/>	Role name	filter
<input type="checkbox"/>	admin	
<input checked="" type="checkbox"/>	buttercup_base_power	
<input type="checkbox"/>	buttercup_base_user	
<input type="checkbox"/>	can_delete	
<input type="checkbox"/>	power	

7. In the **Capability Name** filter box type "schedule_search". Validate that the capability is selected.

Name * ? buttercup_finance_dev_reports

1. Inheritance **2. Capabilities** 3. Indexes 4. Restrict

Select specific capabilities for this role.

<input type="checkbox"/>	Capability Name	schedule_search	X
<input checked="" type="checkbox"/>	schedule_search		

8. In the filter field type "msearch". Validate that the capability is selected.

Name * ? buttercup_finance_dev_reports

1. Inheritance **2. Capabilities** 3. Indexes 4. Restrictions

Select specific capabilities for this role.

<input type="checkbox"/>	Capability Name	msearch	X
<input checked="" type="checkbox"/>		run_msearch	

9. In the **Capability Name** filter box type "install"

Name * ? buttercup_finance_dev_reports

1. Inheritance **2. Capabilities** 3. Indexes 4. Restrictions

Select specific capabilities for this role.

<input type="checkbox"/>	Capability Name	install	X
<input type="checkbox"/>		install_apps	

10. Click on the box to the left of the capability to enable it for the role.

Name * ? buttercup_finance_dev_reports

1. Inheritance **2. Capabilities**

Select specific capabilities for this role.

<input type="checkbox"/>	Capability Name	install	
<input type="checkbox"/>		install_apps	

11. To filter, select the **Capability Name** field and type “edit_local”

Name * ? buttercup_finance_dev_reports

1. Inheritance **2. Capabilities** 3. Indexes 4. Restrictions

Select specific capabilities for this role.

☒ Capability Name ×

☐ edit_local_apps

12. Click on the box to the left of the capability to enable it for the role

Name * ? buttercup_finance_dev_reports

1. Inheritance **2. Capabilities**

Select specific capabilities for this role.

☒ Capability Name

☐ edit_local_apps

13. Click on the next tab “**3. Indexes**”

? buttercup_finance_dev_reports

ance **2. Capabilities** **3. Indexes** 4. Restrictions

pecific capabilities for this role.

Capability Name ×

edit_local_apps

14. In the **Index Name** filter box type "fin"

The screenshot shows the '3. Indexes' tab in the Splunk configuration interface. Under the 'Wildcards' section, there is a text input field with the placeholder 'Enter a value that contains ***' and a green 'Add' button. Below this, the 'Indexes' section contains a table with the following structure:

Index Name	Included
finance_monitor	<input type="checkbox"/>
finance_security	<input type="checkbox"/>
finance_web-purchases	<input type="checkbox"/>

The 'Index Name' filter box at the top of the table contains the text 'fin'.

15. Click on 3 the three finance indexes “finance_monitor”, “finance_security”, “finance_web-purchases” to make them available for the role to search.

The screenshot shows the 'Edit Role' page for the role 'buttercup_finance_dev_reports'. The '3. Indexes' tab is selected. The 'Wildcards' section is visible. The 'Indexes' section contains a table with the following structure:

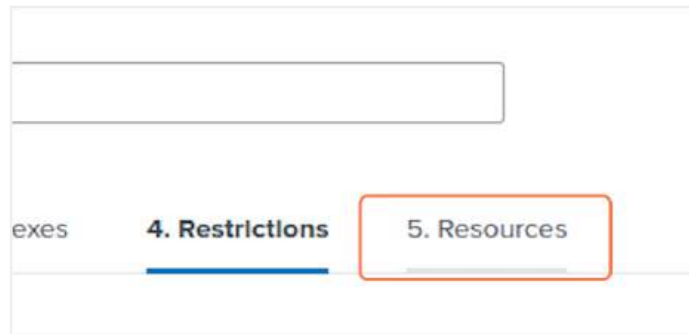
Index Name	Included
finance_monitor	<input checked="" type="checkbox"/>
finance_security	<input checked="" type="checkbox"/>
finance_web-purchases	<input checked="" type="checkbox"/>

The 'Index Name' filter box at the top of the table contains the text 'finance'.

16. Click on the next tab **“4. Restrictions”**

17. No changes are required here

18. Click on the last tab “**5. Resources**”

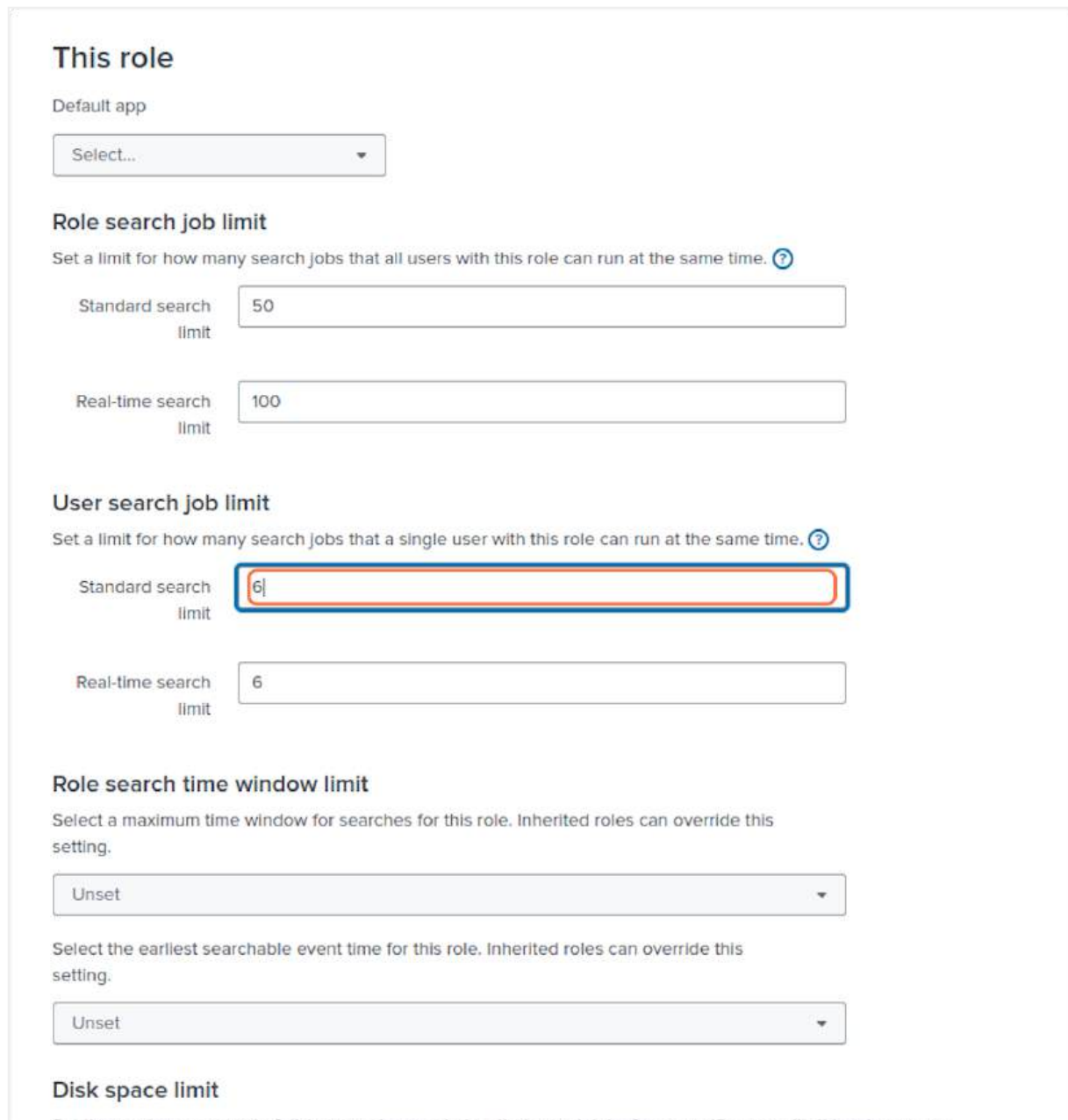


exes

4. Restrictions

5. Resources

19. Under **Standard search limit**, type "6"



This role

Default app

Select...

Role search job limit

Set a limit for how many search jobs that all users with this role can run at the same time. ?

Standard search limit 50

Real-time search limit 100

User search job limit

Set a limit for how many search jobs that a single user with this role can run at the same time. ?

Standard search limit 6

Real-time search limit 6

Role search time window limit

Select a maximum time window for searches for this role. Inherited roles can override this setting.

Unset

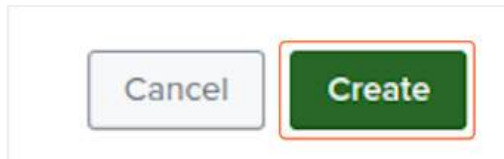
Select the earliest searchable event time for this role. Inherited roles can override this setting.

Unset

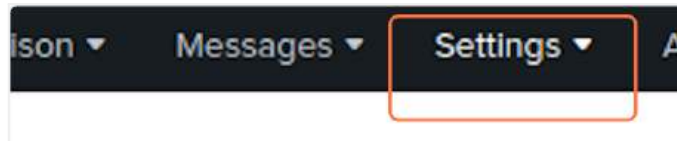
Disk space limit

Set the maximum amount of disk space, in megabytes, that search jobs for a specific user with this role can use.

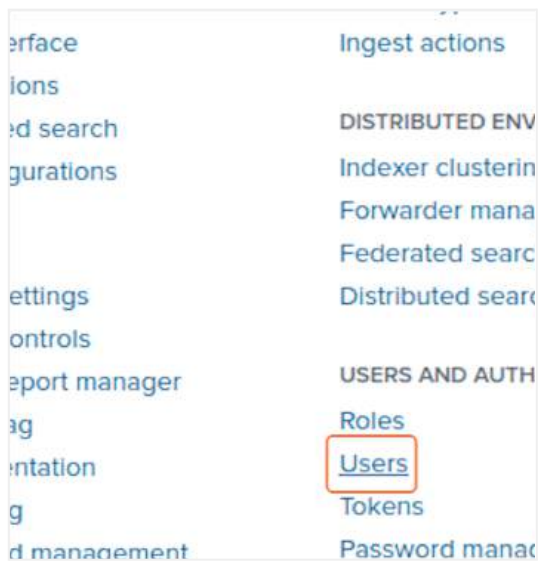
20. Click on **Create** to create the role



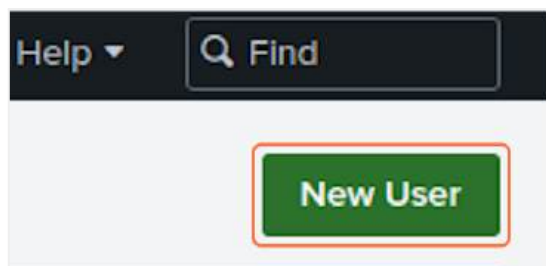
21. Create a user that is a member of the role just created, click on **Settings**



22. Click on **Users**



23. Click on **New User**



24. In the **Name** field type "test_findev"

A screenshot of the 'New User' form. The 'Name' field is highlighted with a red rectangular border and contains the text 'test_findev'. Below it are 'Full name' and 'Email address' fields, both marked as 'optional'.

25. In the **Set password** field type “changeme” (without the quotes)



A screenshot of a user creation form. The fields are: Name (test_findev), Full name (optional), Email address (optional), Set password (highlighted with a red box, containing seven dots), and Confirm password (Confirm new password). Below the fields is a note: "Password must contain at least ?".

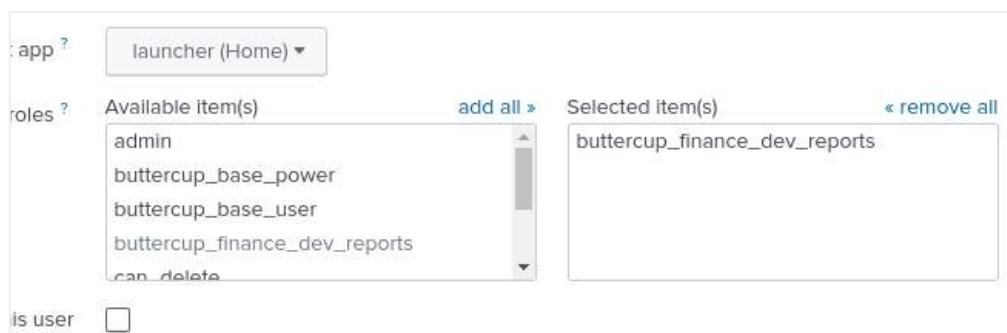
26. 6. Type in the “Confirm password” field “changeme”



A screenshot of a user creation form. The fields are: Name (test_findev), Full name (optional), Email address (optional), Set password (containing seven dots), and Confirm password (highlighted with a red box, containing seven dots). Below the fields is a note: "Password must contain at least ?".

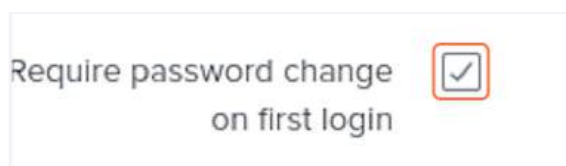
27. Under **Selected item(s)**, click on the word “user” to remove the inheritance.

Under **Available item(s)** click on “buttercup_finance_dev_reports” to add it to the inheritance for the user.



A screenshot of a role configuration interface. At the top, there's a dropdown menu for "app" set to "launcher (Home)". Below it, there's a section for "roles" with two columns: "Available item(s)" and "Selected item(s)". The "Available item(s)" column contains a list of roles: admin, buttercup_base_power, buttercup_base_user, buttercup_finance_dev_reports, and can_delete. The "Selected item(s)" column contains the role buttercup_finance_dev_reports. There are "add all" and "remove all" buttons between the columns. At the bottom, there's a checkbox labeled "is user" which is currently unchecked.

28. Click on **Require password change on first login** to deselect it, as this is only a test user.



A screenshot of a checkbox labeled "Require password change on first login". The checkbox is currently checked, and it is highlighted with a red box.

29. Click on **Save**



1. Validate the user/role are behaving as expected
2. Open an anonymous browser window
 - a. Log in with the test user just created "test_findev" and the "changeme" password

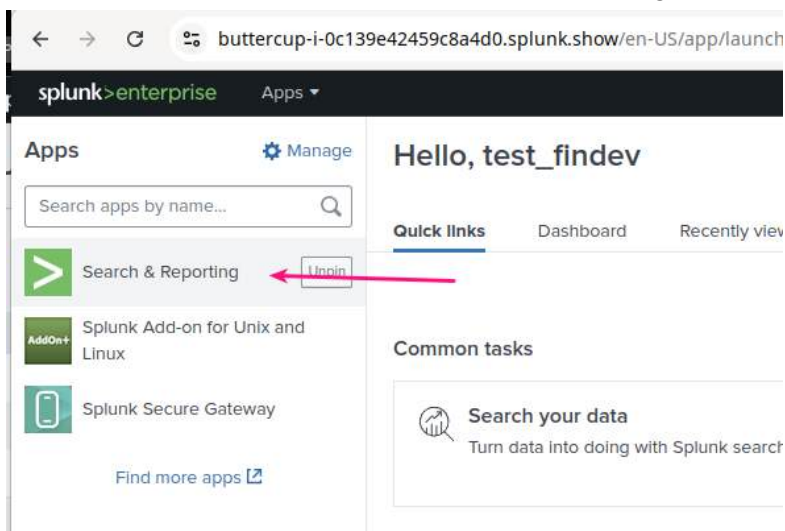
test_findev

changeme

buttercup-i-0c139e42459c8a4d0.splunk.show/en-US/account/login?return_to=%2Fen-US%2F

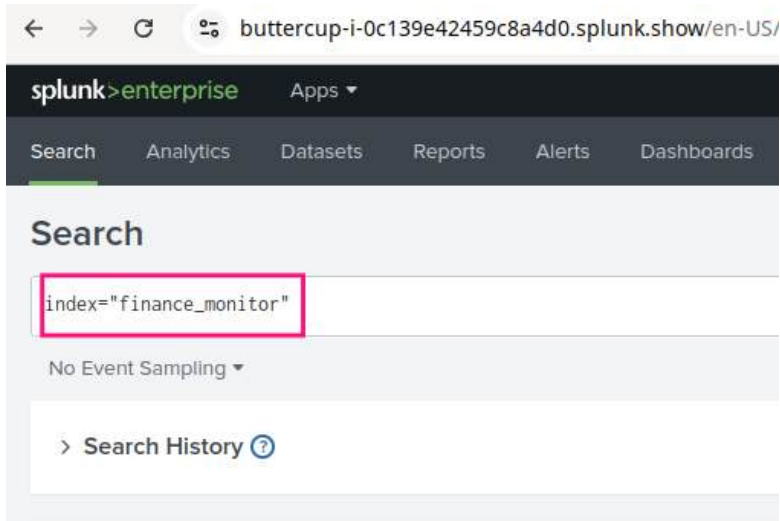


- b. Skip the tour ... twice
- c. Click on "Search & Reporting"

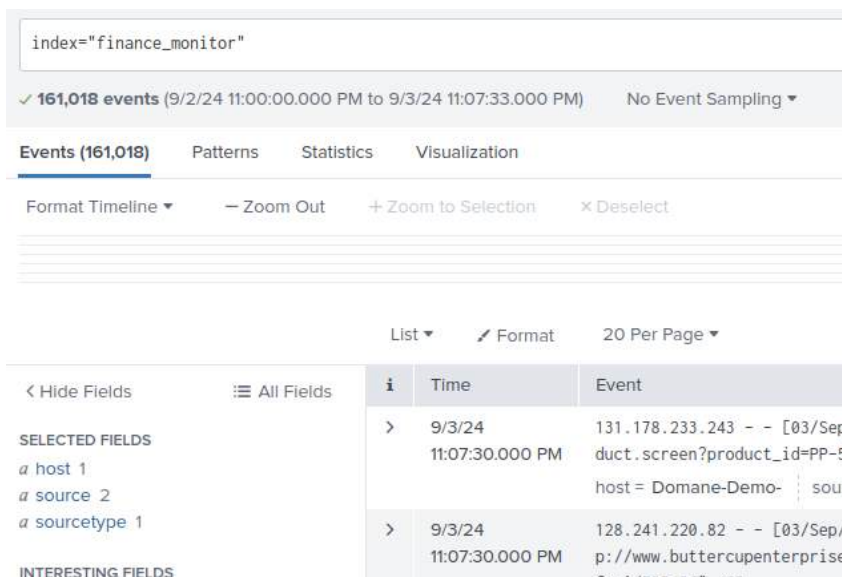


- d. In the search box, input "index=finance_monitor"

index=finance_monitor



- e. Events appearing in the window means that the relevant index is accessible by the user/role. Additional testing can be generated by validating access to the other indexes, but this spot check is likely sufficient.



Note: Use the [cheat sheet](#) to copy/paste the values, this isn't a typing exercise!

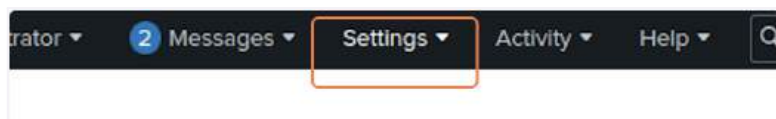
Exercise 2 – Connect Splunk to Active Directory

Description

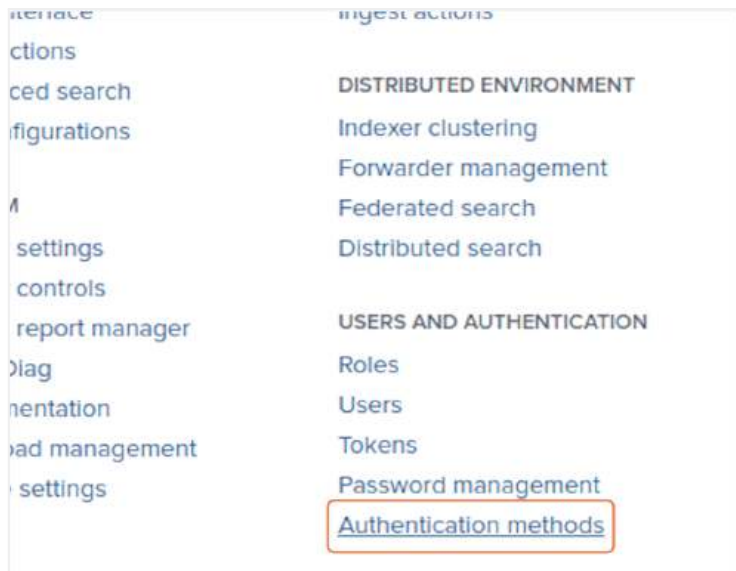
Connecting Splunk to Active Directory (or any SSO) ensures that the users have a single set of credentials provided by the Authentication team. It ensures that there are fewer failure points in accessing enterprise resources, including Splunk

Steps

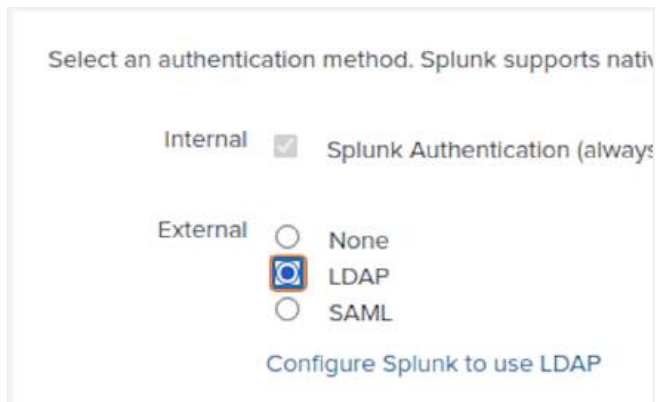
1. From the main Splunk Screen, click on **Settings**



2. Click on **Authentication methods**



3. Select **LDAP**



4. Click on **Configure Splunk to use LDAP**

Select an authentication method. Splunk supports native authentication as well as the following external methods:

Internal ☒ Splunk Authentication (always on)

External ☐ None
☒ LDAP
☐ SAML

[Configure Splunk to use LDAP](#)

5. Click on **New LDAP**

Pages ▾ Settings ▾ Activity ▾ Help ▾ Find

New LDAP

6. In the **LDAP strategy name** field type "buttercup_base"

AP strategy name *

Enter a unique name for this strategy.

in settings

7. In the **Host** field type IP/name of the AD server provided. In the SHOW interface, the AD server is presented with "RDP://AD_SERVER_IP". Do not use the "RDP://" in this field. Just the IP address (or a DNS name, either FQDN or simple name, whichever resolves correctly) is required.

Windows Active Directory Running

rdp://34.219.127.39

Instance ID	Termination Date	User ID
665a359458b10bf59c416205	1 hour 36 minutes left	-

Connection Information

Username	Administrator
Admin Password
Remote Desktop	rdp://34.219.127.39
Admin Username	admin

LDAP strategy name *

Enter a unique name for this strategy.

Connection settings

Host *

Your Splunk server must be able to resolve this host.

Port

8. In the **Port** field type "389"

Host *

Your Splunk server must be able to resolve this host.

Port

The LDAP server port defaults to 389 if you are not using SSL, or 636 if SSL is enabled.

☐ SSL enabled

9. In the **Bind DN** field type "Domain Splk 01"

☐ SSL enabled

You must also have SSL enabled on your LDAP server.

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.

10. In the **Bind DN Password** field type "SplunkRocks1!" (without the quotes)

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.

Bind DN Password

Enter the password for your Bind DN user.

11. In the **Confirm password** field type "SplunkRocks1!" again

Bind DN Password

Enter the password for your Bind DN user.

Confirm password

12. In the **User base DN** field type "CN=Users,DC=buttercup,DC=local"

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.

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)'

13. In the **User name attribute** field type "samaccountname"

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'.

Real name attribute *

The user attribute that contains a human readable name. This is typically 'cn' (common name) or 'displayName'.

14. In the **Real name attribute** field type "displayName"

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'.

Real name attribute *

The user attribute that contains a human readable name. This is typically 'cn' (common name) or 'displayName'.

15. In the **Group base DN** field type "CN=Users,DC=buttercup,DC=local"

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.

16. In the **Group name attribute** field type "cn"

Group name attribute *

The group attribute that contains the group name. A typical value for this is 'cn'.

17. In the **Static member attribute** field type "member"

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.

18. Click on **Save**



No restart is required after the “Save” is clicked to access the groups from Active Directory.

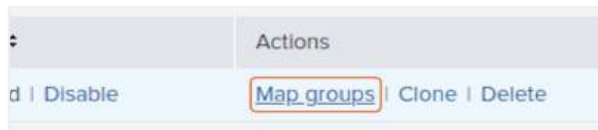
Exercise 3 – Associate Splunk Roles to Active Directory Groups

Description

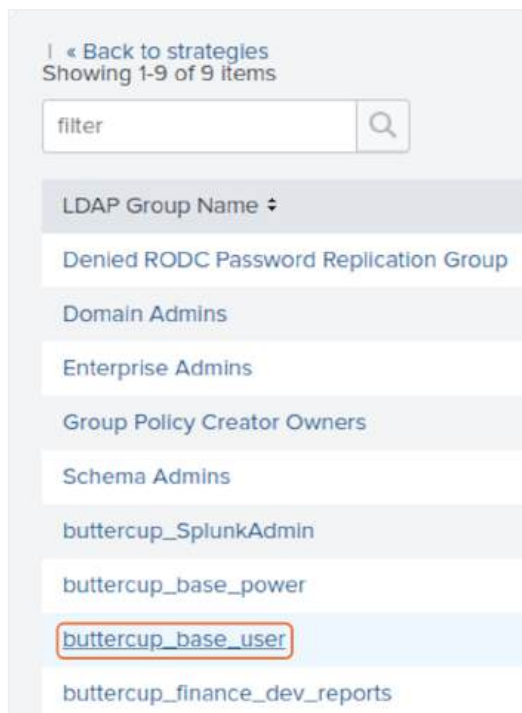
To provide access and privileges to the users coming in from AD, the roles that Splunk uses to provide that access and privilege need to be associated to groups that are fed from AD (that will include the users).

Steps

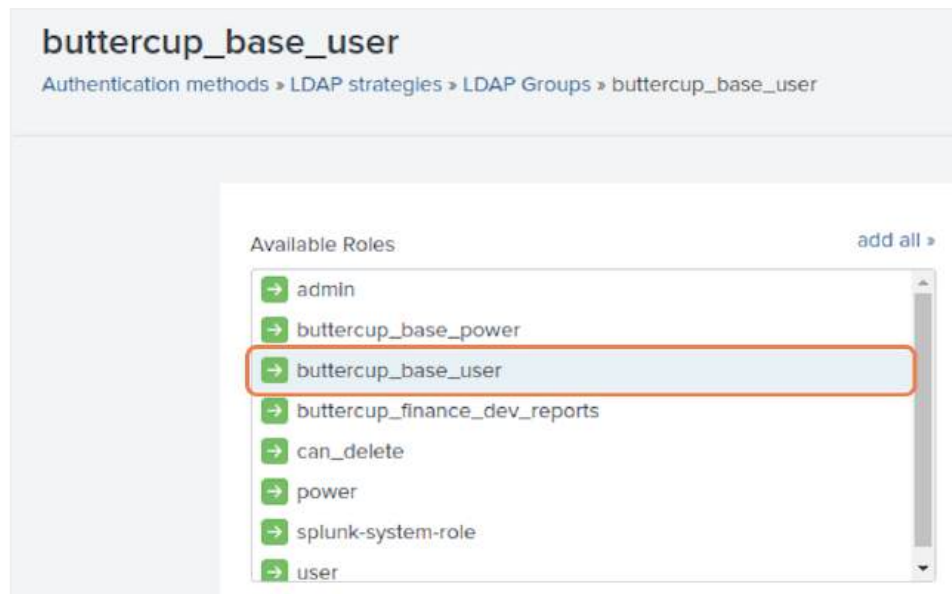
1. From the screen that appears after the “Save” button from the prior exercise, click on **Map groups** from the “buttercup_base” strategy



2. Click on the “buttercup_base_user” LDAP group name



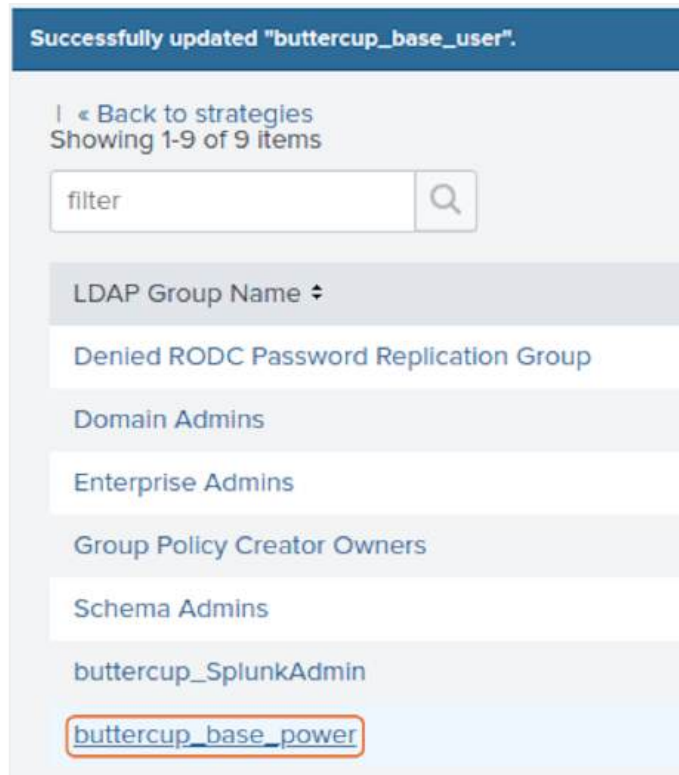
3. To associate the LDAP group “buttercup_base_user”, under **Available Roles** click on the “buttercup_base_user” role



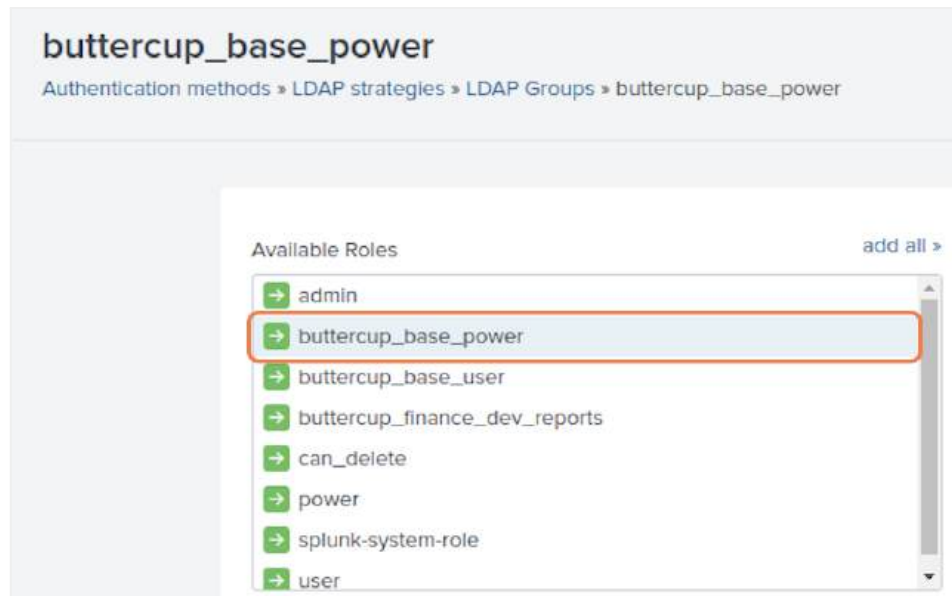
4. Click on **Save**



5. Click on the “buttercup_base_power” LDAP group name



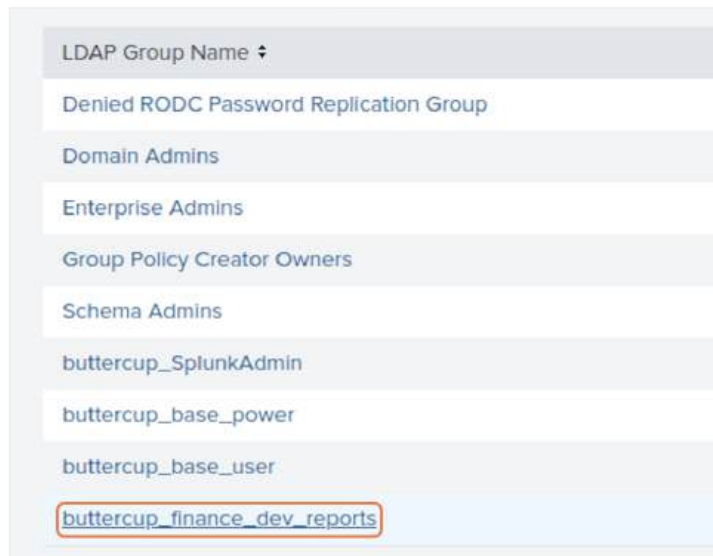
6. To associate the LDAP group “buttercup_base_power”, under **Available Roles** click on the “buttercup_base_power” role.



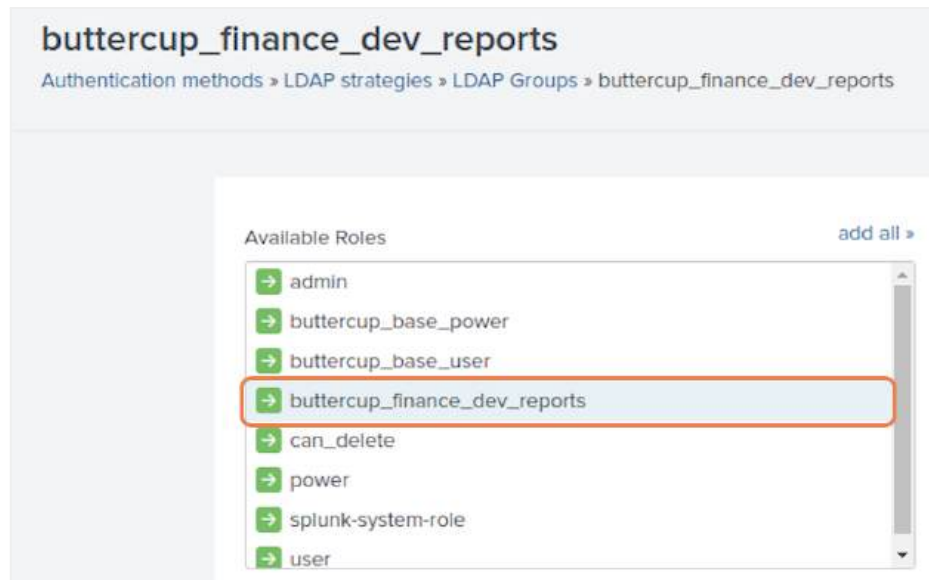
7. Click on **Save**



8. Click on “buttercup_finance_dev_reports” LDAP Group Name



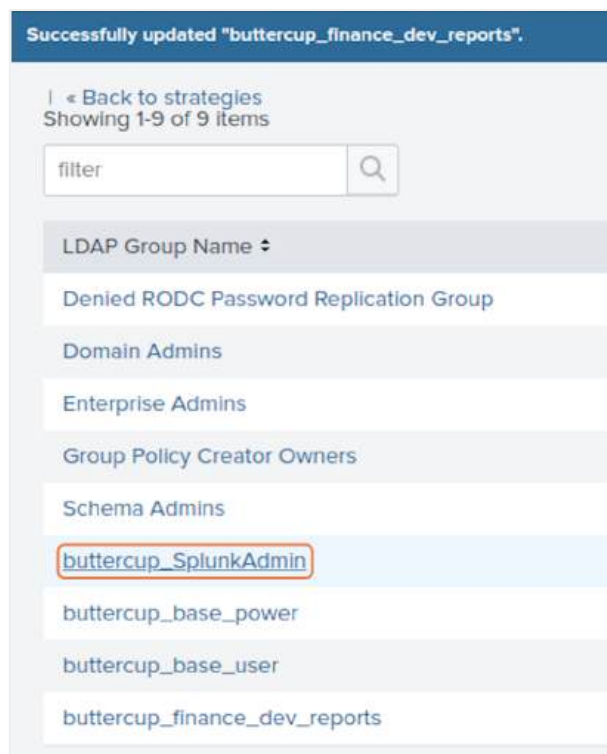
9. To associate the LDAP group “buttercup_finance_dev_reports”, under **Available Roles** click on the “buttercup_finance_dev_reports” role.



10. Click on **Save**



11. Click on “buttercup_SplunkAdmin” LDAP Group Name



12. To associate the LDAP group name “buttercup_SplunkAdmin”, under **Available Roles** click on the “admin” role.



13. Click on **Save**



Exercise 4: Validate users/group/role membership

Description

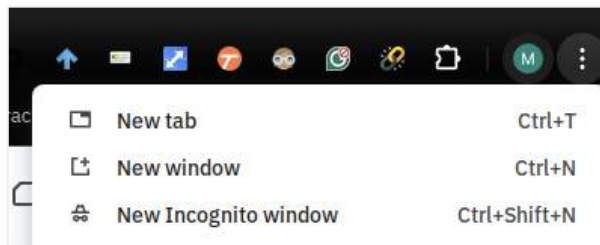
Validate the relationships among the users, the AD groups, and the Splunk roles that have been defined. There are limitations for each of the users, as they are each associated with different roles ...

AD Group	Splunk Role	Username
buttercup_user_base	buttercup_user_base	ahorse
buttercup_power_base	buttercup_power_base	bhorse
buttercup_finance_dev_reports	buttercup_finance_dev_reports	chorse
buttercup_SplunkAdmins	buttercup_SplunkAdmins	dhorse
Domain Admins	Domain Admins	d_admin01
Domain Admins	Domain Admins	d_splk01

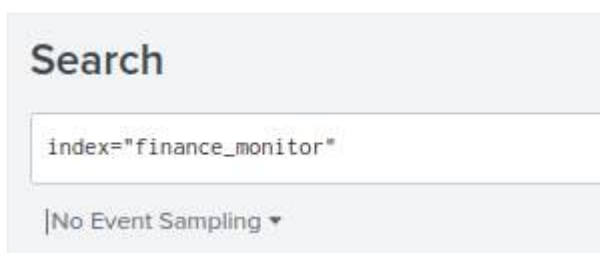
Password - SplunkRocks1!

Steps

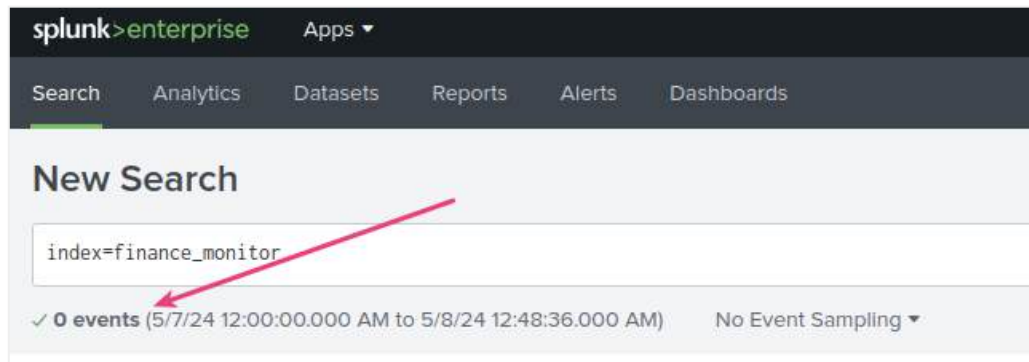
1. Use an Incognito window (or whichever anonymous login your preferred browser provides)



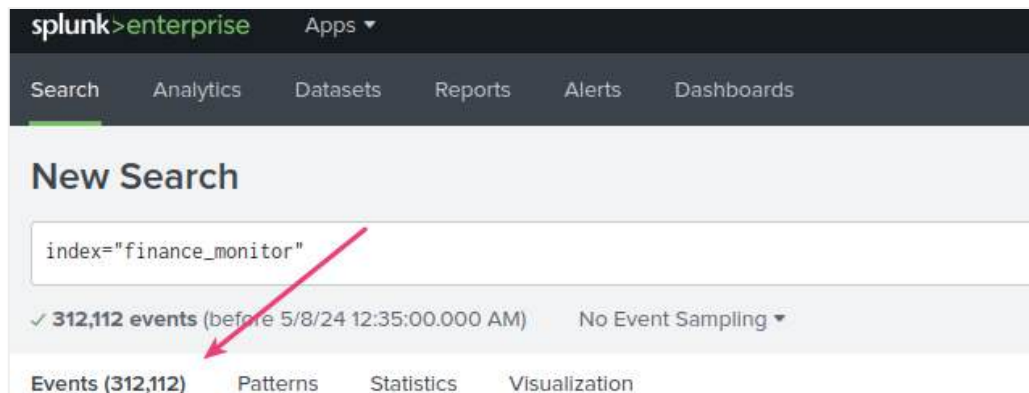
2. With a search, explore what each user can do (hint Charlie is the important one)



See



vs.



A note about connecting to the Windows AD server. If the attendee would like to make changes to the AD instance and explore how these changes affect the Splunk instance, the connection profile requires using port **11337** rather than the standard **3389**.

Links

Create New Users	Create and manage users with Splunk Web
Create New Roles	https://docs.splunk.com/Documentation/Splunk/latest/Security/Rolesandcapabilities
Setup authentication with LDAP	Set up user authentication with LDAP - Splunk Documentation
Configure AD for use with Splunk	Configuring Microsoft's Active Directory Federation Services (ADFS) Security Assertion Markup Language (SAML) Single Sign On (SSO) with Splunk Cloud
LDAP auth configuration tips	LDAP auth configuration tips Splunk
Setup SAML SSO	Configure single sign-on with SAML - Splunk Documentation
Troubleshooting SAML SSO	Troubleshoot SAML SSO - Splunk Documentation
Chrome extension: "SAML Chrome Panel"	SAML Chrome Panel
Firefox extension: SAML Message Decoder	SAML Message Decoder – Get this Extension for 🦊 Firefox (en-US)
Edge Add-on: SAML, WS-Federation and OAuth 2.0 tracer	SAML, WS-Federation and OAuth 2.0 tracer - Microsoft Edge Addons
How-to with Shared Secrets	Store Encrypted Secrets in a Splunk App
Sync passwd file with splunk.secret	Synchronizing the passwd file between Splunk serve...
Splunk.secret information	What is the splunk.secret file, and is it possible to change it?
Distributed search KO/user replication	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/HowconfrepoworksinSHC
Securing the Splunk Cloud Platform (discussion about User and Role Management inherent)	Securing the Splunk Cloud Platform
Connecting Splunk to Okta	Enabling Okta single sign-on in the Splunk platform
Configure Splunk to use a Reverse Proxy	Configure Single Sign-On with reverse proxy - Splunk Documentation
SSO using a reverse proxy	About Single Sign-On using reverse proxy - Splunk Documentation
Splunk scripted authentication	Create the authentication script - Splunk Documentation
Splunk Direct Multi-Factor Authentication	About multifactor authentication with Duo Security - Splunk Documentation
General Splunk Naming Conventions	Naming conventions - Splunk Lantern
Knowledge Object Naming Conventions	Develop naming conventions for knowledge objects - Splunk Documentation
Thoughts on Naming Conventions in Splunk	https://community.splunk.com/t5/Splunk-SOAR-f-k-a-Phantom/Recommendations-for-naming-conventions-and-organization-of/m-p/501574
SplunkBase (non-Splunk supported) - User Role Checker	User Role Checker Splunkbase
SplunkBase (non-Splunk supported) - Alert action for SAML user role map removal	Alert action for SAML user role map removal Splunkbase