Splunk Enterprise 8.0 System Administration - Class Lab Exercises

Lab typographical conventions

Replace following keys with the values indicated:

{student-ID}	Your assigned 2-digit student number
{idx-os-user}	Your assigned OS account name on your indexer
{fwd-os-user}	Your assigned OS account name on your forwarder
{password}	Your assigned Splunk Web and Linux OS account password
{host-eip}	The external IP address of your assigned Splunk Enterprise instance
{host-iip}	The internal IP address of your assigned Splunk Enterprise instance

To support the lab activities, your lab environment also includes the following shared servers:

ip-10-0-0-100	The host name of your Splunk universal forwarder. It has the private address of **10.0.0.100**.
bcgdc	The host name of a lab support server serving as the Active Directory server and a distributed search peer. It has the private address of **10.0.0.150**.

The **SPLUNK_HOME** token indicates the directory where Splunk is installed on the host:

On Linux Indexer:	**/opt/splunk**
On Windows Indexer:	**C:\Program Files\Splunk**
On Forwarders:	**/opt/home/{fwd-os-user}/splunkforwarder**

The following text editors are installed in your environment:

Linux server:	**nano** **vi**
Windows server:	**Notepad++**

If you are unfamiliar with **vi**, use **nano**. It is an easy text editor.

Some steps contain icons which denote the action to take on the appropriate OS.

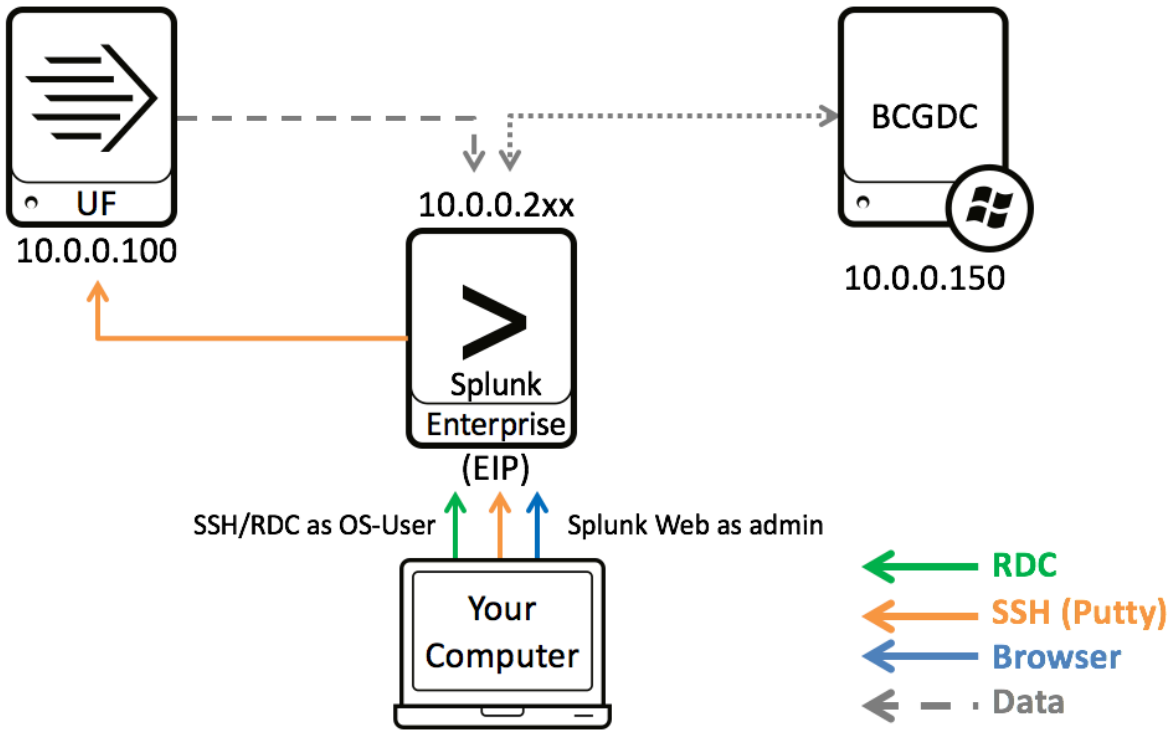
	Linux OS
	Windows OS

NOTE: When you access the Splunk user interface for the first time, Splunk asks if you want a tour of the app. Throughout the exercises, you can dismiss this prompt at any time.

Lab Environment Overview

Throughout the course, you will be working in a private network environment. This diagram provides the overview of your lab environment. Your instructor will assign you a public IP address to your Splunk Enterprise server, which is your primary access into your Splunk network. To complete your lab activities, connect to your Splunk Enterprise server with the public IP address and remote **ssh** into forwarders using the reserved private IP addresses.

Splunk Environment:



Module 1 Lab Exercise – Configure Splunk

Description

Welcome to the Splunk System Administration lab environment. In this exercise, you will perform basic configuration tasks using the Splunk Web interface and collect system information using the Splunk CLI.

Please record the following instructor-provided information:

Your student ID is a unique 2-digit identifier used throughout the lab exercises to differentiate your work from other class participants' work.

Student ID: _____
{student-ID}

The following information is required to access your Splunk Enterprise instance:

Splunk Web URL: **http://**_____**:8000**
{host-eip}

Splunk Username: **admin** Password: _____
{password}

Linux OS

To access the Linux filesystem, you will use an SSH client such as Terminal (Mac) or PuTTY (Windows).

Linux Host name: _____
{host-eip}

Linux Username: _____ Password: _____
{idx-os-user} **{password}**

Windows OS

To access the Windows filesystem, you will use a Remote Desktop client (RDC), such as Microsoft Remote Desktop.

Windows Host name: _____
{host-eip}

RDC Username: _____ Password: _____
{idx-os-user} **{password}**

Configuration Steps

Task 1: Access Splunk Web and change the basic settings.

1. Direct your web browser to your Splunk (Indexer/Search Head) instance:

   `http://{host-eip}:8000`

2. Log in as **`admin`** using your assigned password **`{password}`**.
3. Click **Got it!** in the "**Helping You Get More Value from Splunk Software**" pop-up page.
4. If an "**Important changes coming!**" pop-up page appears, click **Don't show me this again**.
5. If you are prompted to change the password, click **Skip** to continue using the provided password.
6. To identify the Splunk version and build number your server is running, click **Help** > **About**. Then click the "**x**" in the top corner to close the "**About**" page.
7. Click **Administrator** > **Account Settings** and change the **Full name** to *your name*.
8. In the **Email address** field, replace the current value with your two-digit **`{student-ID}`**.
   Hint: Leading zero required for student IDs 01-09.
9. Click **Save**.

   Notice the **User settings saved** indicator at the top. You may have to refresh your browser.
10. Navigate to **Settings > Server settings > General settings**.

    The directory where Splunk is installed is referred to as **`SPLUNK_HOME`**. Make note of the path specified in the **Installation path** field:

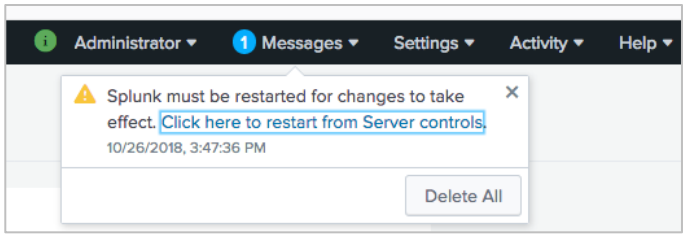
    _____

11. Rename the Splunk server name and default host name:

Splunk server name:	**`splunk{student-ID}`**	(Your assigned 2-digit ID)
Default host name:	**`splunk{student-ID}`**	(Your assigned 2-digit ID)

12. Click **Save**.

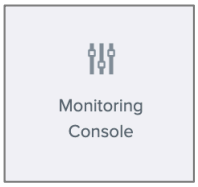
    These changes require a restart of Splunk.
13. Click **Messages > Click here to restart from Server controls > Restart Splunk > OK**.



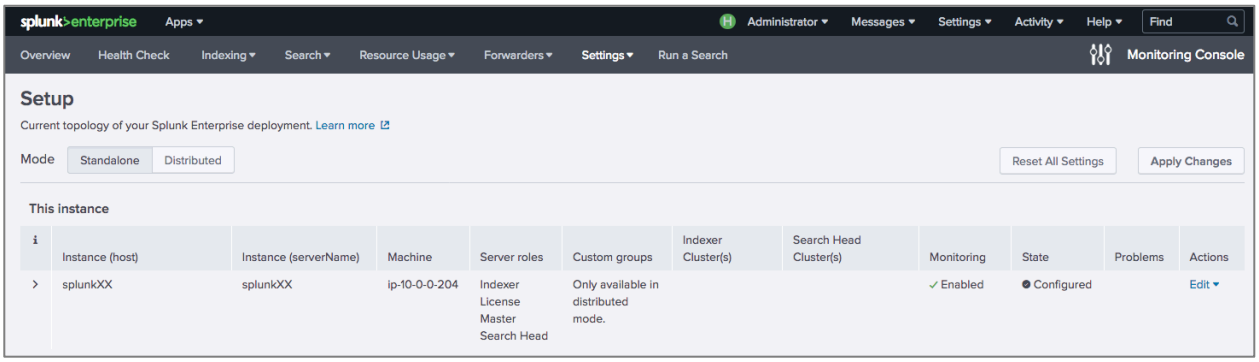
14. Click **OK** when the dialog box indicates that the restart was successful.
15. After the restart, log back into Splunk Web with your assigned password.

Check Your Work

Task 2: Enable the Monitoring Console (MC) app.



16. In Splunk Web, navigate to **Settings > Monitoring Console**. (Look for the **Monitoring Console** icon on the left side of the menu.)
17. On the Monitoring Console navigation bar (the dark grey bar found under the black Splunk Web navigation bar) click **Settings** > **General Setup**.
18. Verify the server name and make a note of the discovered server roles.

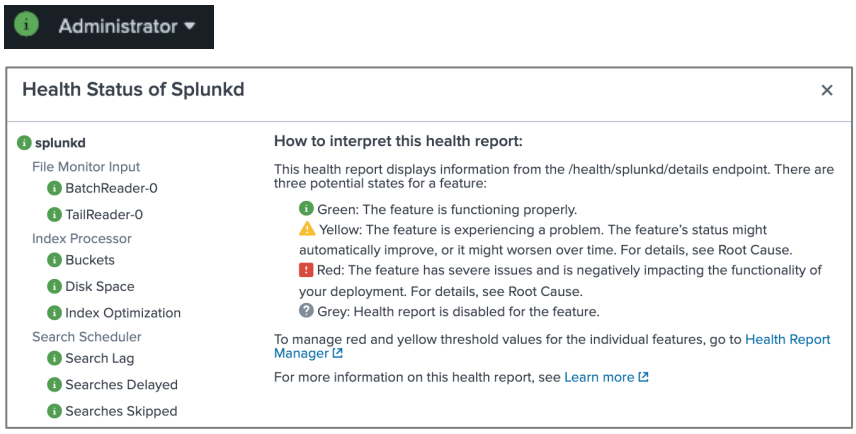


19. To complete the app setup, click **Apply Changes** > **Go to Overview**.
20. On the **Overview** page, confirm that:
    - MC is running in standalone mode.
    - No errors are displayed.
    - No extreme resource usage is detected. The **CPU Usage** or **Memory Usage** rates should not be higher than 75%.

Task 3: Start and view Health Check for your Splunk server.

21. From the Monitoring Console, click **Health Check**.

    For the lab environment, you can ignore any warnings. You just want to confirm that all components are operational.
22. Click **Start** to view the current results for the instance. Wait until the health check has completed.
23. Click the icon next to your name to check the health status of **splunkd**.



Task 4: Access the command terminal of your designated Splunk server.

24. Connect to your dedicated Splunk indexer/search head.

Use one of these two methods:

1. To start a an SSH session to your indexer from your terminal window:

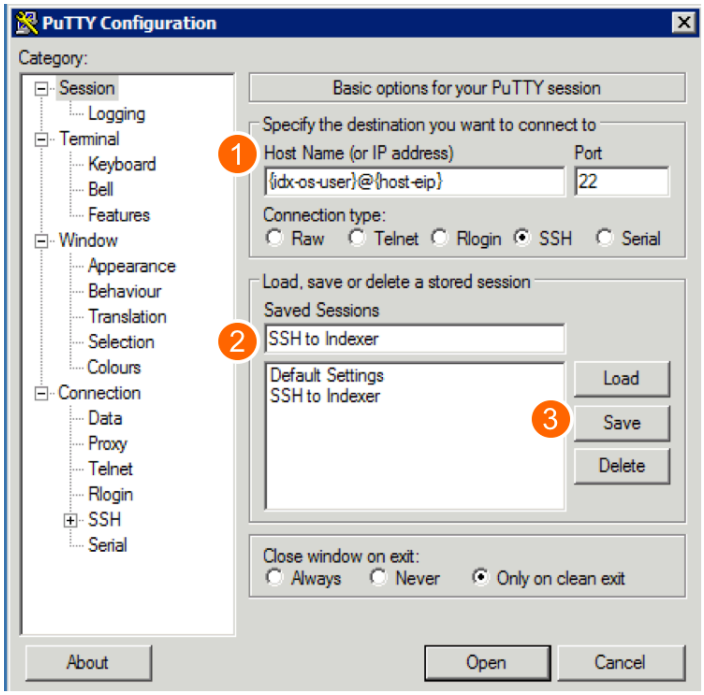
```
ssh {idx-os-user}@{host-eip}
```

2. To use PuTTy to start an SSH session to your indexer:

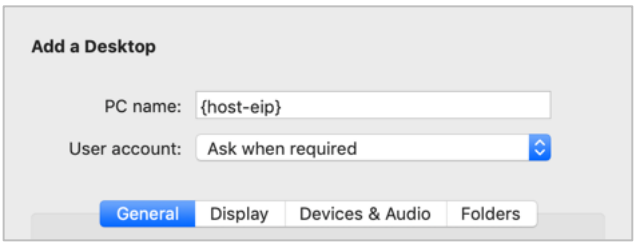
   a. ❶ Replace **`{idx-os-user}@{host-eip}`** with your designated values.

   b. ❷ Name your session and ❸ click Save (optional setting for PuTTy).

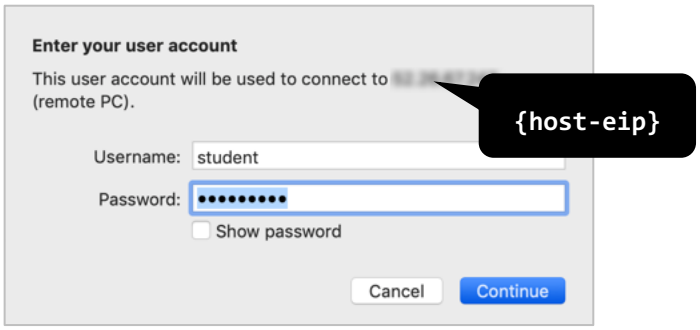
   c. Click **Open** to start an SSH session.



Use an RDC (Remote Desktop client) connection window to connect to your indexer using the designated IP address value for **`{host-eip}`**.



Open a remote desktop connection to the window and login using **`{idx-os-user}`** (normally set to **`student`**, on Windows).



In the remote Windows desktop, click **Start > Command Prompt**.

Task 5: Retrieve basic system information using CLI.

25. From your terminal window, change to your **`SPLUNK_HOME/bin`** directory:

```
cd /opt/splunk/bin
```

```
cd C:\Program Files\Splunk\bin
```

26. Run a CLI command to check the status of your Splunk services.

```
./splunk status
```

```
splunk status
```

The output shows the running status and the **`splunkd`** process IDs:

```
splunkd is running (PID: #####)
splunk helpers are running (PIDs: #####,#####,…)
```

27. Using the Splunk CLI, retrieve the following information about your Splunk server.

    If you are on the Windows server, omit the **./** from the commands. (For example, type: **splunk version**, instead of **./splunk version**)
    Use **splunk help commands** and **splunk help show** to obtain a list of Splunk CLI commands and syntax help.

> **NOTE:** You will be prompted for the Splunk administrator username and password:
> Splunk Username: **admin**
> Password: **{password}** .

Splunk version	**./splunk version**
Splunk Web port:	**./splunk show web-port** *returns* **8000**
Splunk management (splunkd) port:	**./splunk show splunkd-port** *returns* **8089**
Splunk App Server ports:	**./splunk show appserver-ports** *returns* **8065**
Splunk KV store port:	**./splunk show kvstore-port** *returns* **8191**
Splunk server name:	**./splunk show servername** *returns* **splunk{student-ID}**
Default host name:	**./splunk show default-hostname** *returns* **splunk{student-ID}**

Troubleshooting Suggestions

1. If you can't access Splunk Web, it is likely that the Splunk service is not running. In the terminal, run:

```
./splunk status
```

```
splunk status
```

2. If **splunkd** is not already running, start the **splunkd** service.

```
./splunk start
```

```
splunk start
```

Module 2 Lab Exercise – Add and Configure Splunk Licenses

Description

Update an Enterprise Trial license to an Enterprise license and modify the license pool.

Configuration Steps

Task 1: Update the initial trial license to an Enterprise license.

1. In Splunk Web, select **Settings** > **Licensing** to access the **Licensing** page.

   What license group is your server currently configured to use? Trial license group

2. Add a license by uploading a license file to Splunk Web.

   You need the **`splunk.license.big.license`** file on your local system. In this exercise, there are two ways to obtain the required license file (choose one):

   - Download it from https://splk.it/edu-lab-licenses
   - Check with your instructor if your class is using an alternate source to obtain the license.
3. From the Licensing page, click **Add license**.
4. Click **Browse** and locate the file downloaded to your local system: **`splunk.license.big.license`**
5. Click **Open** and then click **Install**.
6. Click **Restart Now > OK**.
7. After the restart, navigate back to the **Licensing** page and answer the following questions:

   What license group is your server configured to use now? Enterprise license group

   What is the maximum daily index volume licensed for your environment now? 200 MB

Task 2: Modify the license pool.

8. From the **Licensing** page, click the **Edit** link next to the **auto_generated_pool_enterprise** pool.
9. From **Allocation**, click **A specific amount** and set the allocation to **`150 MB`**.
10. From **Indexers**, click **Specific indexers**.
11. From the **Available indexers** field, select your host and move it to the **Associated indexers** field.
12. Click **Submit > OK**.
13. Confirm the settings you have configured for this pool on the **Licensing** page.

Task 3: Enable an alert to monitor the license usage.

14. Navigate to **Settings > Monitoring Console** and scroll down to the **Alerts** section of the **Overview** page and click **Enable or Disable**.
15. Click the **Enable** next to the **DMC Alert - Total License Usage Near Daily Quota** alert.
16. To confirm, click **Enable**. An alert will now fire if 90% of your pool quota is consumed.

Module 3 Lab Exercise – Install an App

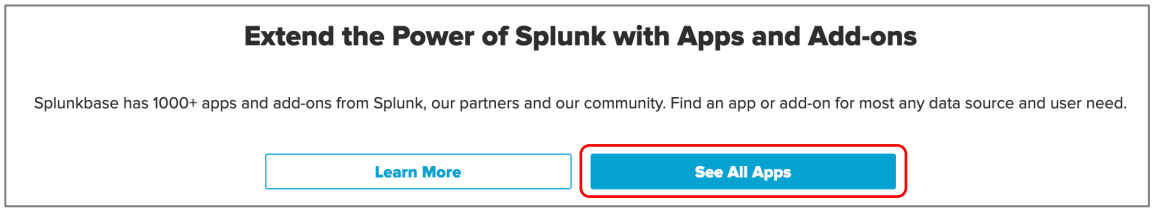
Description

Apps and add-ons are a quick way to get value from your input data. In this lab exercise, you will install a sample app that configures an input, reports, dashboards, a lookup, and an index.

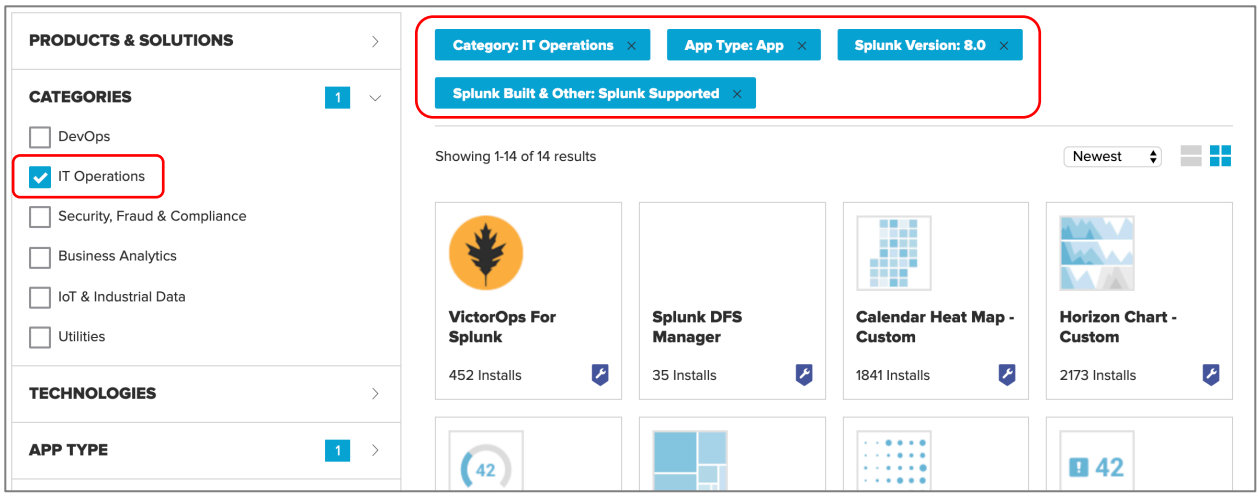
Configuration Steps

Task 1: Look for Splunk apps and download an app.

1. Visit https://splunkbase.splunk.com/. (To download any apps from splunkbase, you first need a Splunk.com account.)
2. Find and click on **See All Apps**:



3. Search for apps that meet the following criteria:
   - **Categories:** IT Operations
   - **App Type:** App (no add-ons)
   - **Splunk Version:** 8.0
   - **Splunk Built & Other:** Splunk Supported



How many apps meet the above criteria? As of this writing, 14.

4. For this exercise, download the sample app (`admin80.spl`) from https://splk.it/edu-system-80.

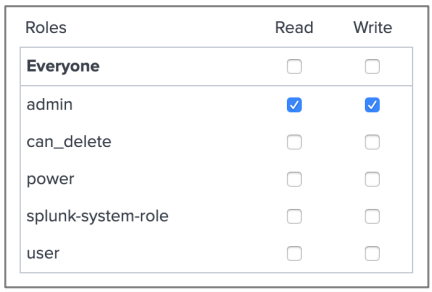
Task 2: Install the class app.

In this task, you install a custom Splunk app from a file and change the permissions of the app so that only the **admin** role has read and write access.

5. In Splunk Web, navigate to **Settings > Indexes** and note the indexes that are currently configured for this instance.
6. In Splunk Web, navigate to **Apps** > **Manage Apps** page.

   Click the ⚙ icon if you are on the **Home** page (launcher).
7. Click **Install app from file** > **Choose File** to locate the `admin80.spl` file you downloaded in step 3.
8. Click **Upload**.
9. In Splunk Web, navigate to **Settings > Indexes**. Notice that a new index called "`websales`" has been installed.
10. Navigate to the **Apps > System Admin 8.0 Class App**.

    System Admin 8.0 Class App is listed on the **Home** page as well as under the **Apps** dropdown.
11. Click **Apps > Manage Apps**.
12. For the **System Admin 8.0 Class App**, click **Permissions**.
13. Configure the permissions so only the `admin` role has Read and Write permissions.



14. Click **Save**.

Check Your Work

Task 3: Verify the app installation.

15. Log into Splunk Web as `emaxwell / open.sesam3`.
16. Confirm that the **System Admin 8.0 Class App** app is not accessible.
17. Log into Splunk Web as `admin / {password}`.
18. Click the **splunk>** logo.
19. You should see **Search & Reporting** and **System Admin 8.0 Class App** in the left navigation bar.

Module 4 Lab Exercise – Configuration Files

Description

To observe how the Splunk software handles permissions and context, you will investigate a user issue with tags. In this exercise, it appears that different users are getting different results, although they are running the same search.

You must successfully complete the Module 3 lab steps to see the expected results in this lab exercise.

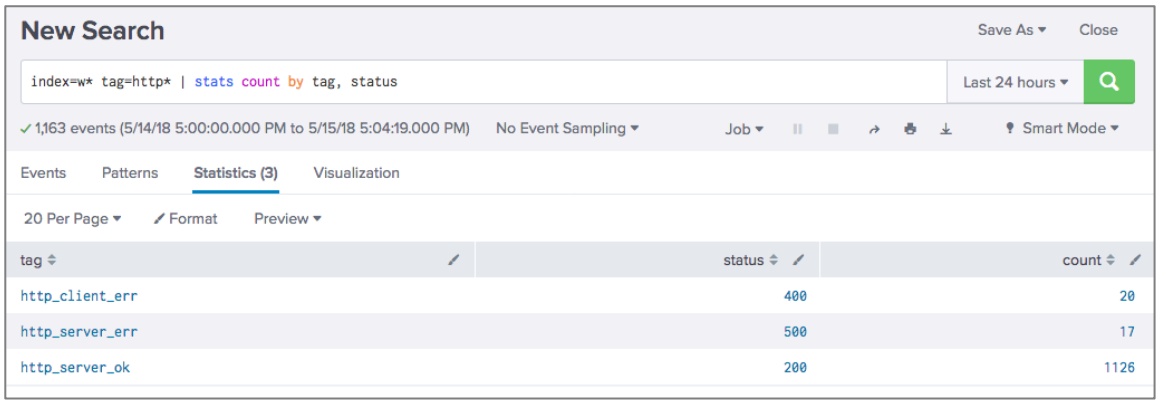
Configuration Steps

Task 1: Identify a configuration problem with tags.

1. As the user **`admin`**, navigate to **Search & Reporting** app. If a popup appears asking about a quick tour, click **Skip**. Run the following search over the **last 24 hours**:

   ```
   index=w* tag=http* | stats count by tag, status
   ```

   Notice your results. Pay attention to the different status codes displayed.

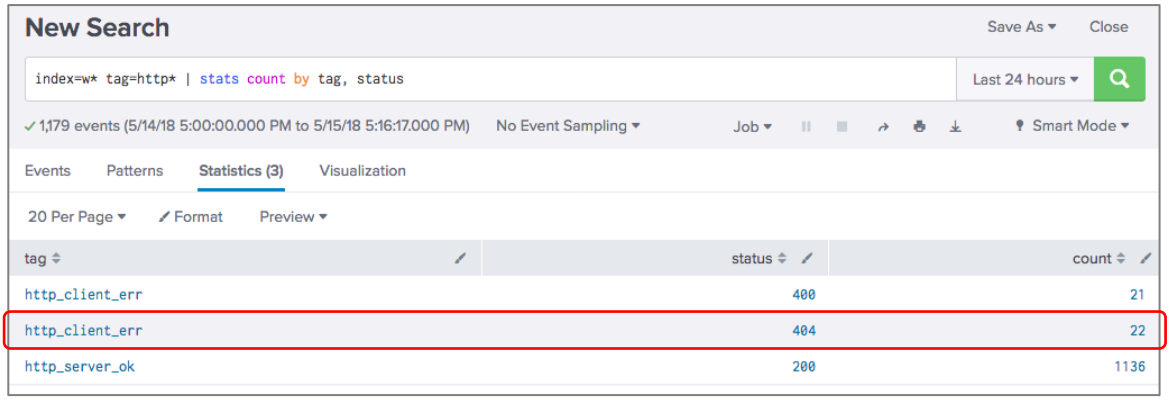
2. Log in as **`emaxwell / open.sesam3`**.

3. Navigate to **Search & Reporting** app. If a popup appears asking about a quick tour, click **Skip**. Run the same search over the **last 24 hours**:

   ```
   index=w* tag=http* | stats count by tag, status
   ```

4. Note the results that **`emaxwell`** gets from the same search.

   What are the differences between the two results? (Pay attention to the **`status`** codes)

Task 2: Use the CLI commands to investigate and troubleshoot.

In this task, use **btool** to investigate the differences between the search results. Use **splunk help btool** to display the syntax help about the command.

5. From your terminal window, navigate to the **`SPLUNK_HOME/bin`** directory:

```
cd /opt/splunk/bin
```

```
cd \Program Files\Splunk\bin
```

6. To display the tag stanzas, run the **`splunk btool`** command:

```
./splunk btool tags list --debug
```

```
splunk btool tags list --debug
```

The **`btool`** option **`--debug`** displays the file path along with the stanza settings:

```
/opt/splunk/etc/apps/search/local/tags.conf [status=200]
/opt/splunk/etc/apps/search/local/tags.conf http_server_ok = enabled
/opt/splunk/etc/apps/search/local/tags.conf [status=400]
/opt/splunk/etc/apps/search/local/tags.conf http_client_err = enabled
```

How many stanza entries for tags did **`btool`** find? 2

So, where are the tags **`http_server_err status=500`** and **`http_client_err status=404`**?

You should have seen these tags when you ran the search as **`admin`** and as **`emaxwell`**. Since they don't appear in any of the tags at the global or app levels, perhaps it is a private user tag.

The **`btool`** option, **`--debug --user={USER} --app={APP}`**, expands the listing of the private stanza settings.

7. To locate the private stanza for **emaxwell**, run:

```
./splunk btool tags list --debug --user=emaxwell --app=search
```

```
splunk btool tags list --debug --user=emaxwell --app=search
```

The command returns $**SPLUNK_HOME/etc/users/emaxwell/search/local/tags.conf** showing the tag **http_client_err status=404** as well as the relevant global and app level entries:

```
/opt/splunk/etc/apps/search/local/tags.conf           [status=200]
/opt/splunk/etc/apps/search/local/tags.conf           http_server_ok = enabled
/opt/splunk/etc/apps/search/local/tags.conf           [status=400]
/opt/splunk/etc/apps/search/local/tags.conf           http_client_err = enabled
/opt/splunk/etc/users/emaxwell/search/local/tags.conf [status=404]
/opt/splunk/etc/users/emaxwell/search/local/tags.conf http_client_err = enabled
```

8. To locate the private stanza for **admin**, run:

```
./splunk btool tags list --debug --user=admin --app=search
```

```
splunk btool tags list --debug --user=admin --app=search
```

The command returns **$SPLUNK_HOME/etc/users/admin/search/local/tags.conf** showing the tag **http_server_err status=500** as well as the relevant global and app level entries.

In conclusion, the reason that a user is seeing different results is because of his/her private tags. If this tag is important, as the administrator you may want to ask the owner to share his/her private tags.

OPTIONAL Task: Use OS tools to list Splunk configuration file contents.

Use **grep** with **xargs** on Linux or **findstr** on Windows to filter text lines matching a regular expression. Piping the Splunk CLI output to an OS search utility is very useful, especially when you want to look for matches in the btool output.

1. To confirm that your tag stanzas from the configuration steps exist, run the following command from the **SPLUNK_HOME** directory:

```
cd /opt/splunk/etc
find . -name tags.conf | xargs grep "http_"
```

You can run this if you only want to locate the files:

```
find /opt/splunk -name tags.conf
```

```
cd C:\Program Files\Splunk\etc
findstr /s /i "http_" tags.conf
```

You should see three **tags.conf** files and four distinct tag values.

Module 5 Lab Exercise – Add and Test Indexes

Description

In this exercise, you create a new index and send data. You will use these indexes in subsequent lab exercises.

Configuration Steps

Task 1: Examine the existing index configuration parameters.

1. Log into Splunk Web as **`admin`**.
2. Click **Settings > Indexes > main** to examine how the **main** index is configured.

   Note the **Max Size of Hot/Warm/Cold Bucket** setting: auto_high_volume

Task 2: Create an index for securityops.

In this task, you create a new dedicated index for the security operations data.

3. From **Settings > Indexes**, click **New Index**.
4. In the **Index Data Type** field, verify the default **Events** index is selected.
5. Populate the form as follows:
   - Index Name: **`securityops`**
   - Index Data Type: **`Events`** (Default setting)
   - Max Size of Hot/Warm/Cold Bucket: **`auto_high_volume`**
   - App: **`Search & Reporting`**

     This saves the configurations within the Search app-context.
6. Leave the rest of the fields empty to accept the defaults and click **Save**.
7. View the resulting configurations.

   Linux users can use the **cat** command to view the configuration.

```
cat /opt/splunk/etc/apps/search/local/indexes.conf
```

```
[securityops]
coldPath = $SPLUNK_DB/securityops/colddb
enableDataIntegrityControl = 0
enableTsidxReduction = 0
homePath = $SPLUNK_DB/securityops/db
maxDataSize = auto_high_volume
maxTotalDataSizeMB = 512000
thawedPath = $SPLUNK_DB/securityops/thaweddb
```

Windows users can use Notepad to view configurations are stored in `C:\Program Files\Splunk\etc\apps\search\local\indexes.conf` to view the file contents:

```
[securityops]
coldPath = $SPLUNK_DB\securityops\colddb
enableDataIntegrityControl = 0
enableTsidxReduction = 0
homePath = $SPLUNK_DB\securityops\db
maxDataSize = auto_high_volume
maxTotalDataSizeMB = 512000
thawedPath = $SPLUNK_DB\securityops\thaweddb
```

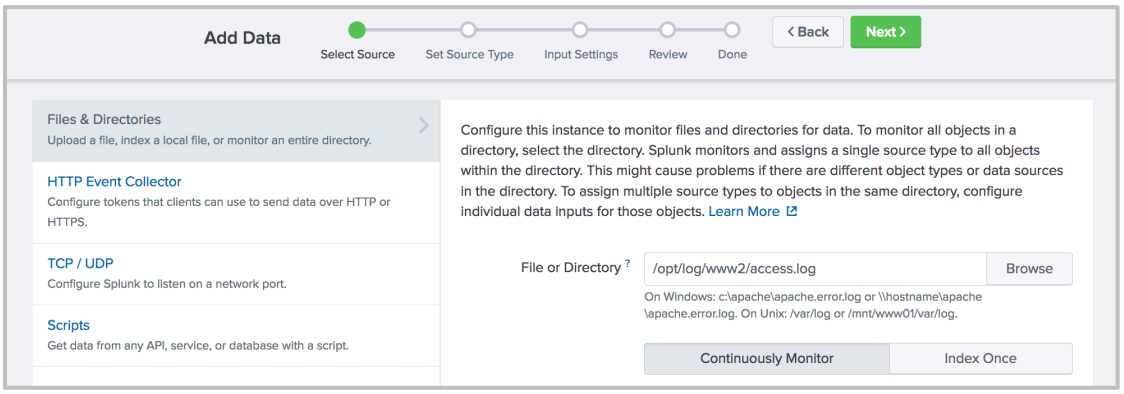
Task 3: Add a file monitor input to send events to the `securityops` index.

In this task, you create a simple local data input to test that your index was created properly. Follow the steps carefully.

8. To start indexing events into the `securityops` index, click **Settings** > **Add Data**.
9. Click **Skip** to dismiss the **Welcome** (quick tour) pop-up window.
10. Click **Monitor** to start the local input wizard.
11. On the **Select Source** step, click **Files & Directories**.
12. Click **Browse** and navigate to select the following input source:

    `/opt/log/www2/access.log`

    `C:\opt\log\www2\access.log`



13. Click **Next** to display the **Set Source Type** step.

    In this instance, Splunk automaticaly recognizes the data format and assigns a pretrained source type. Source types are explained in the Splunk Enterprise Data Administration course.

14. Click **Next** to display the **Input Settings** step.

15. On the **Input Settings** step, select the `securityops` index:

App Context	`Search & Reporting`
Host	`Constant value` (defaults to your host name `splunk##`)
Index	`securityops`

16. Click **Review**.

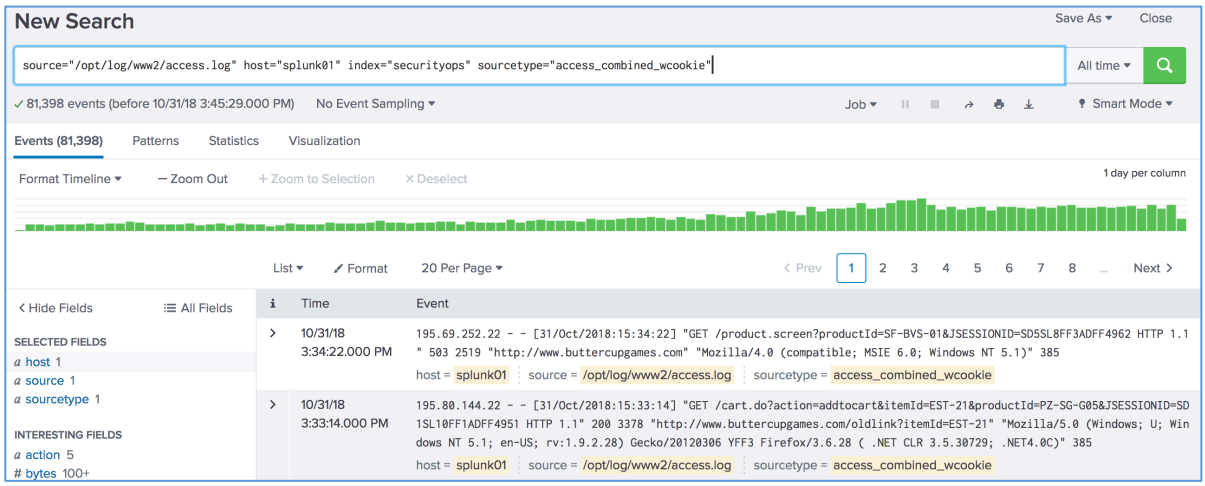
    The summary of the input should look like this:

Input Type	**File Monitor**
Source Path	**/opt/log/www2/access.log** (Linux server) **C:\opt\log\www2\access.log** (Windows server)
Continuously Monitor	**Yes**
Sourcetype	**access_combined_wcookie**
App Context	**search**
Host	**splunk##**
Index	`securityops`

17. Click **Submit**.
18. To verify your input, click **Start Searching**.

    It might take a few moments for results to display. Repeat the **Search** (click the magnifying glass icon) until results appear.

    If you don't see any results after several minutes, check with your instructor.



Module 6 Lab Exercise – Splunk Index Management

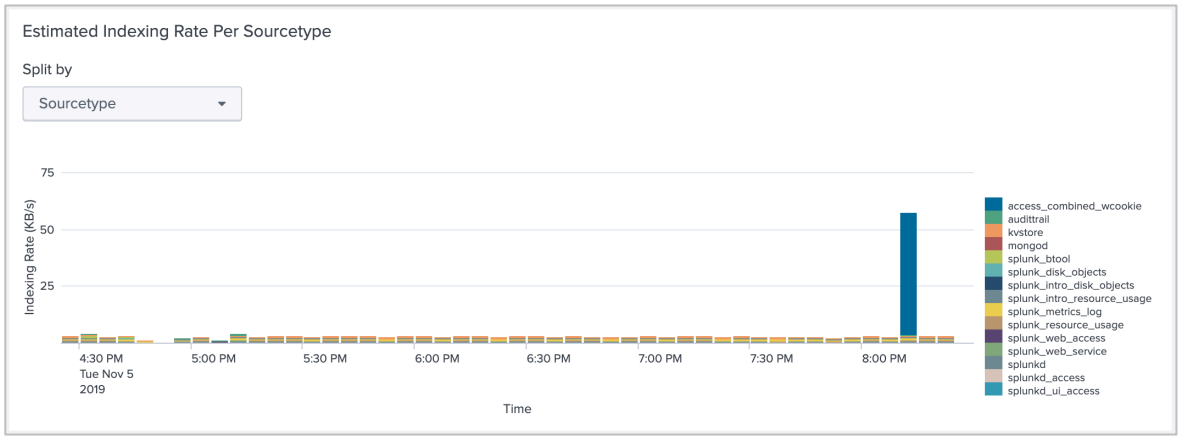
Description

During this exercise, you will perform two tasks with the **`securityops`** index you created in the previous lab exercise. First, you will use the MC to view the indexing activity. Secondly, you will create a retention policy to apply to the index.

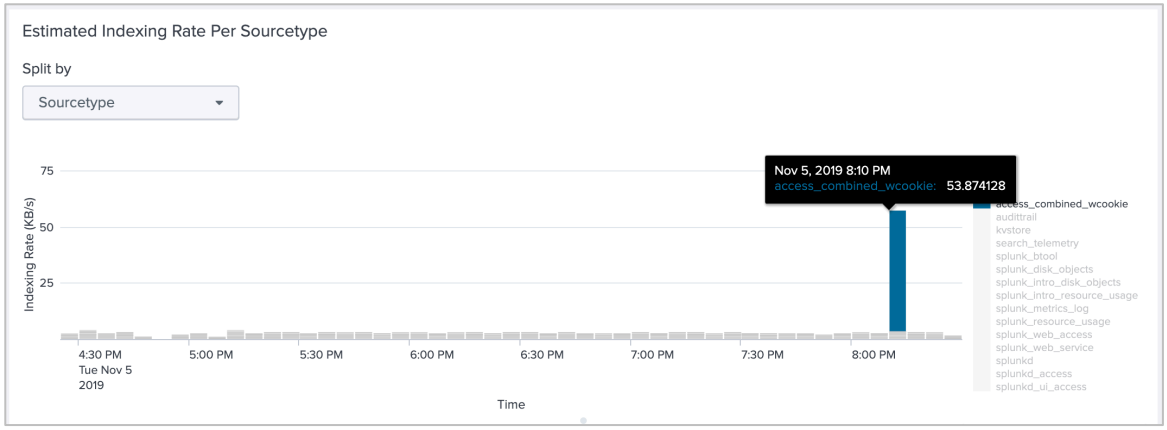
Configuration Steps

Task 1: Use the MC to check the indexing activities.

1. Navigate to **Settings > Monitoring Console**.
2. To check the indexing activity of the previous tasks, click **Indexing > Performance > Indexing Performance: Instance**.
   - Scroll down to the **Historical Charts: Estimated Indexing Rate Per Sourcetype** panel.



   - To see the specific source type rate, roll your mouse over the legend labeled **access_combined_wcookie**



3. To view the index data and path information, navigate to the top menu and select **Indexing > Indexes and Volumes > Indexes and Volumes: Instance**.

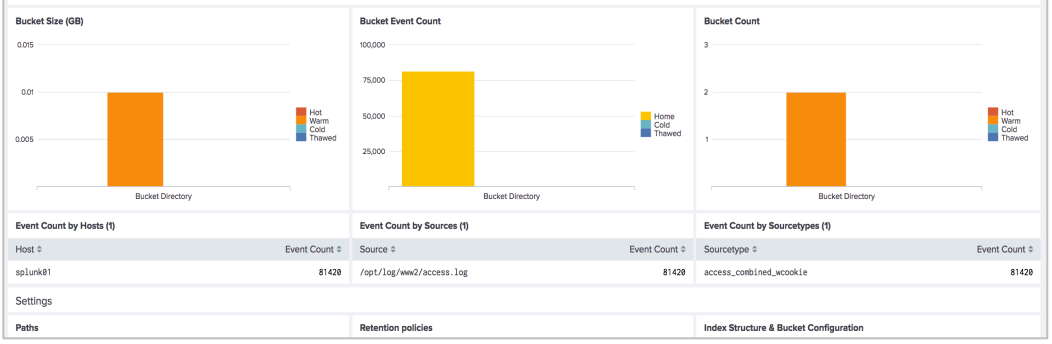
Indexes (10)

Index	Data Type	Data Age vs Frozen Age (days)	Index Usage (GB)	Home Path Usage (GB)	Cold Path Usage (GB)	Total Event Count	Total Bucket Count
_audit	event	26 / 2184	0.01 / 488.28	0.01 / unlimited	0 / unlimited	62,785	8
_internal	event	26 / 30	0.56 / 488.28	0.56 / unlimited	0 / unlimited	6,501,715	11
_introspection	event	14 / 14	0.99 / 488.28	0.99 / unlimited	0 / unlimited	887,393	4
_telemetry	event	25 / 730	0.00 / 488.28	0.00 / unlimited	0 / unlimited	98	4
airlinedata	event	14 / 2184	0.04 / 500.00	0.04 / unlimited	0 / unlimited	1,140,236	1
main	event	0 / 2184	0.00 / 488.28	0.00 / unlimited	0 / unlimited	0	0
securityops	event	116 / 2184	0.01 / 500.00	0.01 / unlimited	0 / unlimited	81,412	2
splunklogger	event	0 / 2184	0.00 / 488.28	0 / unlimited	0 / unlimited	0	0
summary	event	0 / 2184	0.00 / 488.28	0.00 / unlimited	0 / unlimited	0	0
test	event	56 / 2184	0.31 / 500.00	0.31 / unlimited	0 / unlimited	5,705,681	6

4. Click **`securityops`** to view the **Index Detail: Instance** page for the **`securityops`** index.
5. Scroll down and view the current index volume, settings, retention policies, and structure.

Index Directory	Volume Name	Volume Freezing Due to Size	Volume Usage / Capacity (GB)
home	N/A	N/A	N/A
cold	N/A	N/A	N/A

A volume is considered to be freezing or about to freeze data at 95% or more of configured disk usage capacity.



Task 2: Configure a time-based retention policy for securityops.

6. Using a text editor, append the following attributes to the **`securityops`** stanza:

(nano or vi) **`/opt/splunk/etc/apps/search/local/indexes.conf`**

```
[securityops]
coldPath = $SPLUNK_DB/securityops/colddb
enableDataIntegrityControl = 0
enalbeTsidxReduction = 0
homePath = $SPLUNK_DB/securityops/db
maxDataSize = auto_high_volume
maxTotalDataSizeMB = 512000
thawedPath = $SPLUNK_DB/securityops/thaweddb
maxHotSpanSecs = 86400              (add)   NOTE: 86400 = 1 day
frozenTimePeriodInSecs = 7776000    (add)   NOTE: 7776000 = 90 days
```

(Notepad) **C:\Program Files\Splunk\etc\apps\search\local\indexes.conf**

```
[securityops]
coldPath = $SPLUNK_DB\securityops\colddb
enableDataIntegrityControl = 0
enalbeTsidxReduction = 0
homePath = $SPLUNK_DB\securityops\db
maxDataSize = auto_high_volume
maxTotalDataSizeMB = 512000
thawedPath = $SPLUNK_DB\securityops\thaweddb
maxHotSpanSecs = 86400            (add)   NOTE: 86400 = 1 day
frozenTimePeriodInSecs = 7776000  (add)   NOTE: 7776000 = 90 days
```

These changes roll hot buckets every day and retain events in the index for 90 days.

7. Save your changes.
8. Restart Splunk using the CLI.

```
/opt/splunk/bin/splunk restart
```

```
C:\Program Files\Splunk\bin\splunk restart
```

NOTE: If you get an error during restart, it is most likely a mistake in the stanza of the **indexes.conf** file. Check your configuration and verify it is correct.

Task 3: Use the MC to check the view the retention policy settings.

9. From the MC, navigate to **Indexing > Indexes and Volumes > Index Detail: Instance**.
10. From the **Index** dropdown menu, select **securityops**.

Paths		Retention policies		Index Structure & Bucket Configuration	
Setting	Value	Setting	Value	Setting	Value
homePath	$SPLUNK_DB/security	maxTotalDataSizeMB	512000	maxDataSize	auto_high_volume
homePath_expanded	/opt/splunk/var/lib	frozenTimePeriodInSecs	7776000	maxHotBuckets	3
coldPath	$SPLUNK_DB/security	homePath.maxDataSizeMB	0	maxWarmDBCount	300
coldPath_expanded	/opt/splunk/var/lib	coldPath.maxDataSizeMB	0		
thawedPath	$SPLUNK_DB/security				
thawedPath_expanded	/opt/splunk/var/lib				

Troubleshooting Suggestion

1. Verify the indexes.conf configurations.

SPLUNK_HOME/etc/apps/search/local/indexes.conf

C:\Program Files\Splunk\etc\apps\search\local\indexes.conf

Linux server	Windows server

`[securityops]`
`coldPath = $SPLUNK_DB/securityops/colddb`
`enableDataIntegrityControl = 0`
`enableTsidxReduction = 0`
`homePath = $SPLUNK_DB/securityops/db`
`maxDataSize = auto_high_volume`
`maxTotalDataSizeMB = 512000`
`thawedPath = $SPLUNK_DB/securityops/thaweddb`
`maxHotSpanSecs = 86400`
`frozenTimePeriodInSecs = 7776000`
	`[securityops]`
	`coldPath = $SPLUNK_DB\securityops\colddb`
	`enableDataIntegrityControl = 0`
	`enableTsidxReduction = 0`
	`homePath = $SPLUNK_DB\securityops\db`
	`maxDataSize = auto_high_volume`
	`maxTotalDataSizeMB = 512000`
	`thawedPath = $SPLUNK_DB\securityops\thaweddb`
	`maxHotSpanSecs = 86400`
	`frozenTimePeriodInSecs = 7776000`

Module 7 Lab Exercise – Manage Users and Roles

Description

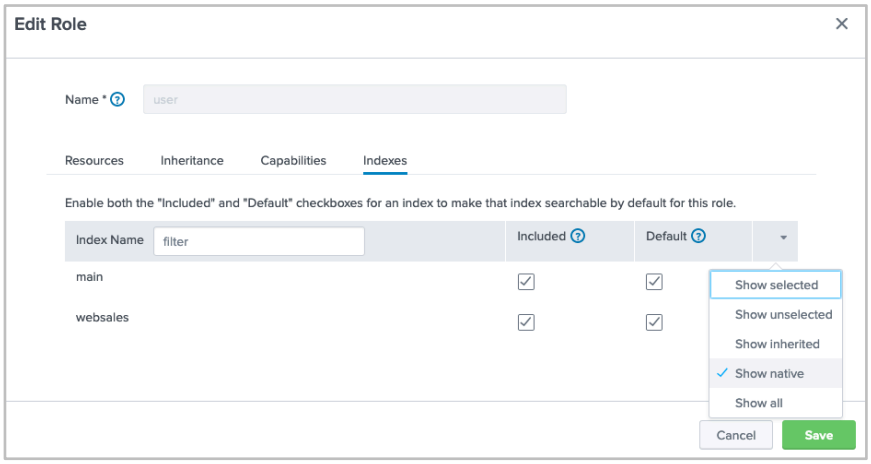
In this exercise, you will modify existing roles and add a new custom Splunk role for Data Administrators. Once the modifications are complete, verify the changes.

Configuration Steps

Task 1: Modify the User, Power and Admin role privileges.

In this task, you modify the default settings for the existing **`user`**, **`power`**, and **`admin`** roles to change the default app, indexes searched by default, and limit data access to certain indexes.

1. Navigate to **Settings > Roles** (in the **Users and Authentication** section).
2. Click the **user** role.
3. Click the **3. Indexes** tab.
4. From **Index Name** list, click the **Included** and **Default** checkbox next to **`websales`**.
5. Check the **Included** and the **Default** checkbox next to **main**.
6. Uncheck the **Included** checkbox for **All non-internal indexes**.
7. Click the filter dropdown menu on the right and select **Show native**.



8. Click **Save**.

9. Click **`power`** role.
10. From the **5. Resources** tab, select **search** in the **Default** app drop-down menu.
11. Click the **3. Indexes** tab.
12. Scroll down and notice that the **websales** and **main** indexes are inherited.

13. Click the **Included** and **Default** checkboxes next to **securityops**.
14. Leave all other parameters at their default values and click **Save**.
15. Click the **admin** role.
16. Click the **3. Indexes** tab.
17. Click the **Included** and **Default** checkboxes by **`All non-internal indexes`** and **`All internal indexes`**.

    This makes it easier for users with the admin role to see new data as it is added to the various indexes.
18. Click **Save**.

Task 2: Create a new role and assign an existing user to the new role.

19. From the **Roles** page, click **New Role**.
20. In the **New Role** dialog box, type **soc_analyst** in the **Name** field.
21. In the **1. Inheritance** tab and select the checkbox next to the **power** role.
22. Click the **3. Indexes** tab, and select the **Included** and **Default** checkboxes next to **`websales`**.
23. From the **5. Resources** tab, select **search** in the **Default app** drop-down menu.
24. Leave all other parameters at their default values and click **Create**.

NOTE: The inherited index settings will become visible only after saving the new role.

25. Navigate to **Settings > Users** (in the **Users and Authentication** section). Then click on **emaxwell**.
26. In the **Assign to roles** section, clear **power** and select **soc_analyst** and click **Save**.
27. Log out as **`admin`**.
28. Log back in as **`emaxwell`** / **`open.sesam3`**

    You should land on the **App: Search and Reporting** based on your new role properties.
29. Run the following search over the **last 24 hours**:

    ```
    host=* | stats count by index
    ```

    You configured the **`soc_analyst`** role to search the **`websales`** index by default, but why does the **`securityops`** index also appear in your search results?

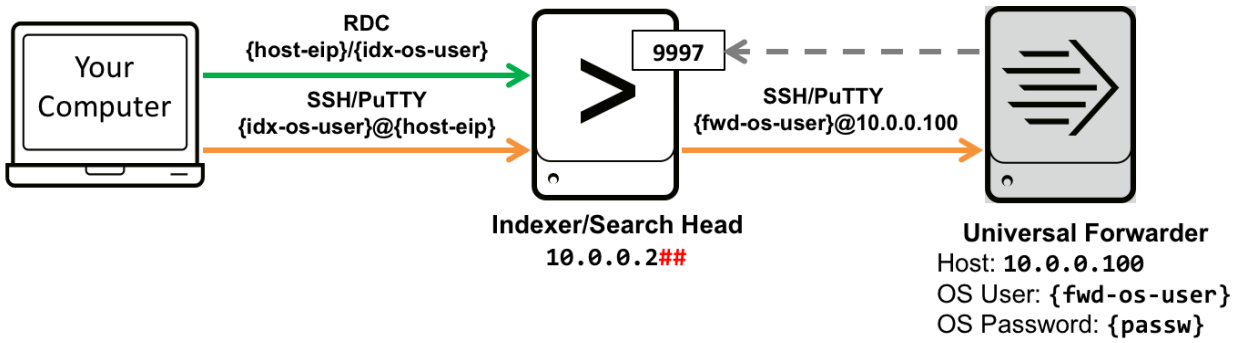
    In **Task 1**, you configured the **`power`** role to search the **`websales`** index by default (along with **`main`** and **`securityops`**). In this task, you configured the **`soc_analyst`** role to inherit the **`power`** role's attributes.
30. Log out and log back in as **`admin`**.

Module 8 Lab Exercise – Setting up Forwarders

Description

In earlier lab exercises, you set up inputs to monitor local files on the Splunk indexer. In most cases, the files that you want to monitor are not stored on a Splunk indexer. The best way to collect data from a remote system, and then send it to a Splunk indexer, is to use a forwarder.

In this exercise, you will configure your existing Splunk indexer as a receiver and set up a forwarder on a remote host. This scenario allows you to index data from a remote host to a centralized Splunk indexer.



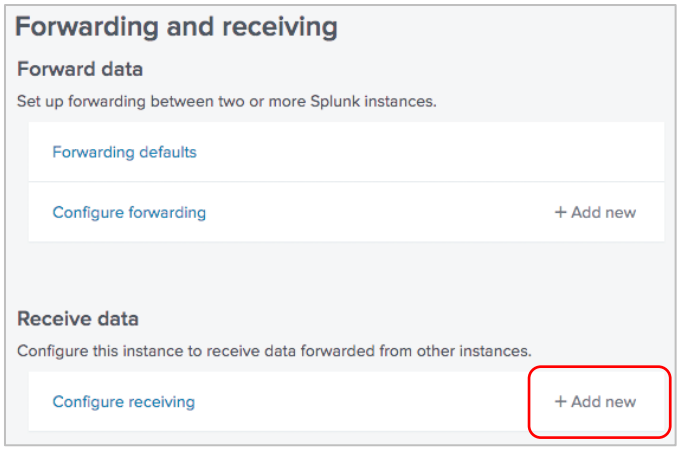
This lab exercise demonstrates a basic way to configure a forwarder.

Configuration Steps

Task 1: Set up your Splunk indexer as the receiver.

In this task, you activate a receiving port on your indexer.

1. Log in as `admin` to Splunk Web and navigate to the **Search & Reporting** app. This causes the receiving port configuration to be saved in the **search** app's local directory.
2. Navigate to **Settings** > **Forwarding and receiving > Configure receiving** and click on **+ Add new.**



3. In **Listen on this port** enter **9997** and click **Save** to configure a receiving port.

4. From your indexer's command line (**command prompt** for Windows), run **`ifconfig`** (on Linux) or **`ipconfig`** (on Windows) to identify your indexer's internal IP address.

   It should be **`10.0.0.2##`**, where **`##`** represents your assigned **`student-ID`**. If not, notify your instructor.

Task 2: Connect to your universal forwarder.

5. To connect to your forwarder (**`10.0.0.100`**), start a remote **`ssh`** session from the indexer console.

```
ssh {fwd-os-user}@10.0.0.100
```

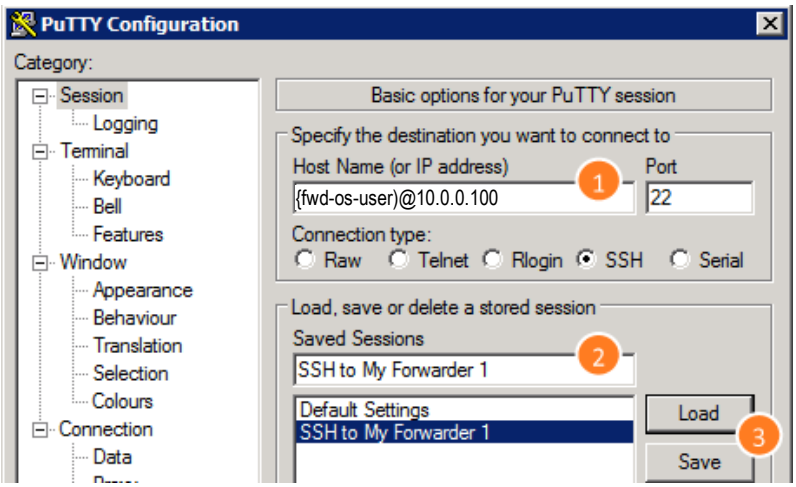
From your RDC session, locate **PuTTy** on the desktop:

Double-click the **PuTTy** application to open it, and configure an SSH session:

a. ❶ Replace **`{fwd-os-user}@10.0.0.100`** with your designated values.

b. ❷ Name your session and ❸ Save.

c. Click **Open** to start the session.



Once connected to the forwarder, the shell prompt indicates the host name:

```
fwd-os-user@ip-10-0-0-100 ~]$
```

Task 3: Start your forwarder instance.

In this task, you start your forwarder instance and use the auto-ports flag to configure the management port (splunkd).

6. Use the **start** command with the **accept-license** and **auto-ports** argument:

```
cd ~/splunkforwarder/bin
./splunk start --accept-license --auto-ports
```

NOTE: These options automatically accept Splunk EULA and configure the **splunkd-port** for you.

7. When you receive the message **"Please enter an administrator username:"**, enter **admin** and press **enter** to continue.
8. When you receive the message "**Please enter a new password:**", enter and confirm your assigned password to continue.
9. Using the **show** command, view the **splunkd-port** number (Splunk will prompt you for a Splunk username. Use **admin**, and enter the password.)

```
./splunk show splunkd-port
Splunkd port: 80##
```

Task 4: Configure your forwarder to send event data to your receiver.

In this task, you configure the forwarder to send data to the receiving port you activated on your Splunk indexer in Task 1. The **add forward-server** command creates an **outputs.conf** in the forwarder's **SPLUNK_HOME/etc/system/local** directory.

10. Configure forwarding to your indexer:

```
./splunk add forward-server 10.0.0.2##:9997        (## is your student-ID)
Added forwarding to: 10.0.0.2##:9997.
```

11. Verify forwarding is configured:

```
./splunk list forward-server
Active forwards:
        10.0.0.2##:9997
Configured but inactive forwards:
       None
```

Hint: If your server is not listed or is listed as inactive, wait about 15 seconds and run the **list** command again.

Check Your Work

Task 5: Use the Monitoring Console to validate the forwarder connection.

In this task, you enable forwarder monitoring in the Monitoring Console.

12. In Splunk Web, navigate to **Settings > Monitoring Console**.
13. On the MC menu, click **Settings > Forwarder Monitoring Setup**.
14. On the **Forwarding Monitoring Setup** page, click **Enable**, then **Save**.

    The **Build Forwarder Assets Now** dialog displays.
15. Click **Continue > Done**.
16. Click **Rebuild forwarder assets... > Start Rebuild > Done**.
17. Switch to your terminal window, and restart the universal forwarder (not the Splunk server.)

```
./splunk restart
```

NOTE: This step is only required to force log content to be sent to the indexer to speed up the process in the lab environment.

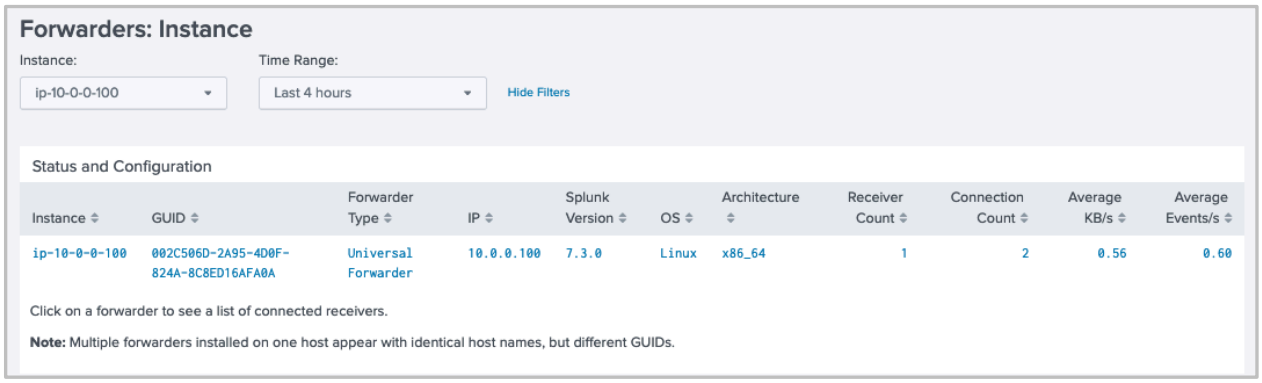
18. After the restart completes on your forwarder (**`10.0.0.100`**), list the contents of the **`outputs.conf`** file (created by the `add forward-server` command in the previous task).

```
fwd-os-user@ip-10-0-0-100 ~]$
cat ~/splunkforwarder/etc/system/local/outputs.conf
[tcpout]
defaultGroup = default-autolb-group

[tcpout:default-autolb-group]
server = 10.0.0.2##:9997

[tcpout-server://10.0.0.2##:9997]
```

19. On the MC menu, select **Forwarders** > **Forwarders: Instance** and check the status.



Instance	GUID	Forwarder Type	IP	Splunk Version	OS	Architecture	Receiver Count	Connection Count	Average KB/s	Average Events/s
ip-10-0-0-100	002C506D-2A95-4D0F-824A-8C8ED16AFA0A	Universal Forwarder	10.0.0.100	7.3.0	Linux	x86_64	1	2	0.56	0.60

It might take a few minutes for the forwarder to display. If no result is displayed after several minutes, STOP and check the troubleshooting suggestions.

Troubleshooting Suggestions

If your forwarder information is not shown, check the following to isolate the problem:

1. Is my receiver enabled and listening on the port I designated?

   Execute this CLI command on the indexer: **`./splunk display listen`**

2. Did I accidentally run the forwarder commands on the indexer?

   a. In Splunk Web, navigate to **Settings > Monitoring Console > Indexing > Indexing Performance: Instance**.

      The fill ratio of each queue in the **Splunk Enterprise Data Pipeline** should be at 0% or near zero.

   b. Run this command on the indexer:

      `./splunk btool outputs list tcpout:default-autolb-group`

      This should be empty. If it is not, locate the source of the output with **`--debug`**, delete the **`outputs.conf`** fie, and restart your indexer.

3. Is my forwarder output setup active?

   Execute this CLI command on the forwarder: **`./splunk list forward-server`**
   If it is not active, check your syntax again.
   Does the port number specified match your receiving port shown in troubleshooting step 1?

4. Are there any issues logged in **`splunkd.log`** on the forwarder:

   `egrep 'ERROR|WARN' ~/splunkforwarder/var/log/splunk/splunkd.log`

5. If you make any corrections, repeat step 10.
6. Is the indexer getting any data from the forwarder?

   Search with the time range set to **Last 15 minutes**:

   `index=_internal ERROR OR host=ip-10-0-0-100 sourcetype=splunkd`

7. If you still don't get results, ask your instructor for help.

Module 9 Lab Exercise – Distributed Search

Description

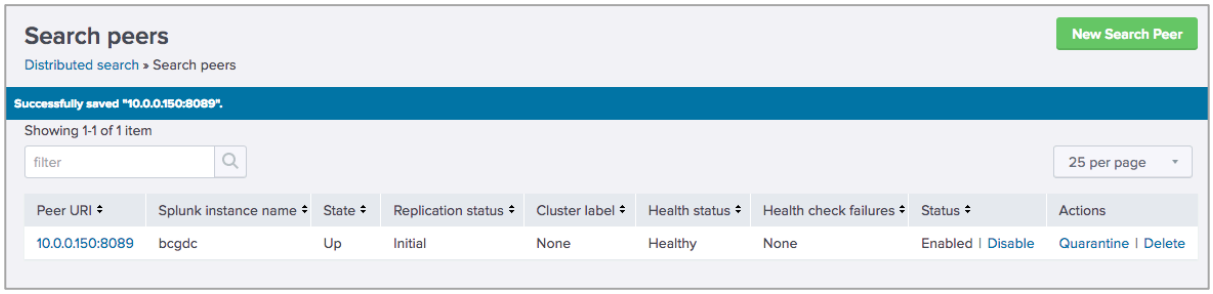
By default, the distributed search capability is enabled on all Splunk instances with the exception of universal forwarders. To be able to search events on a remote search peer (indexer), you just need to add the search peer to your search head.

In this exercise, you extend the search capabilities of your server by adding a search peer. The lab support server is already running as a Splunk indexer, so you can add it as a search peer to your existing indexer.

Configuration Steps

Task 1A: Add a search peer.

1. Click **Settings > Distributed search > Search peers > New Search Peer**.
2. Enter the following peer connection information.
   - Peer URI: `10.0.0.150:8089`
   - Remote username: `ds_user`
   - Remote password: `open.sesam3`
3. Click **Save**.



Check Your Work

Task 2A: Search for indexes and sourcetypes on the search peer.

4. Run the following search over the last 30 days:

   ```
   index=* splunk_server!=splunk* | stats count by splunk_server, index, sourcetype
   ```

   What is the Splunk server name of your search peer? **bcgdc**

   Which index(es) are available on your search peer? **main**

   What sourcetype(s) are available on your search peer? **Perfmon:bcgdc_resource**

Module 9 Lab Exercise – Create a Diag

Description

In this exercise, you create a baseline Splunk diag file and index the output to the test index. Search the diag's contents to determine the memory consumption of Splunk processes.

Steps

Task 1B: Create a Splunk diag file for the deployment server.

1. From your Splunk indexer instance, generate a baseline diag file using the **`splunk diag`** command.

```
cd /opt/splunk/bin/
./splunk diag

...
Splunk diagnosis file created: /opt/splunk/diag-ip-10-0-0-201-
2019-11-05_22-16-19.tar.gz
```

```
cd C:\Program Files\Splunk\bin
splunk diag

...
Splunk diagnosis file created:
C:\Program Files\Splunk\diag-splunk_indexer-2019-11-02_15-24-
18.tar.gz
```

Task 2B: Index the baseline diag file for your records.

2. From your Splunk instance, launch the **Add Data** wizard and click **monitor**.
3. Click **Files & Directories** and browse to the **`SPLUNK_HOME`** directory (**`/opt/splunk`** on Linux, **`C:\Program Files\Splunk`** on Windows), and select the diag file you just created, which should have the file extension **`.tar.gz`**.
4. Select the **Index Once** option and click **Next**.
5. Select **Index `main`**, and click **Review**.
6. Verify the Review page has the following settings:

Input Type	**`File Monitor`**	
Source Path	**`SPLUNK_HOME/diag*.tar.gz`**	
Continously Monitor	**`No, index once`**	
Whitelist	**`N/A`**	
Blacklist	**`N/A`**	
Sourcetype	**`Automatic`**	
App Context	**`search`**	
Host	**`splunk##`**	(where ## is your student ID)
Index	**`main`**	

7. Click **Submit**.

Check Your Work

Task 3: Search the diag contents for the system information.

8. From the DS, execute the following search over **All Time**, replacing the ## with your student ID:

   ```
   index=main source=*diag* host=splunk##  | stats count by source
   ```

   The returned search lists all the files included with the tarball diag and the associated event count.

9. From the DS, execute the following search over **All Time**, replacing the ## with your student ID:

   ```
   index=main source=*systeminfo.txt "diag launched" host=splunk##
   ```

10. In the returned event, click **Show all XXX** lines and scroll down the expanded data to see the amount of memory consumed by the Splunk processes.

    Check the values under:

    ```
    ********** Process Listing (ps) **********
    ```

    `ps aux` output lists process owner, process ID, CPU%, MEM%, total virtual memory used, non-swapped physical memory used, etc.

    Check the values under:

    ```
    ********** Process Listing (tasklist) of splunkd.exe **********
    ```

    `tasklist /V /FI IMAGENAME eq splunkd.exe` output lists name, PID, session name, session#, memory usage, status, user name, CPU time, etc.

Appendix A Lab: Configure a Volume-based Retention Policy

In this exercise, you create a new index for the IT Operations team. Then you will configure a volume-based retention policy and view the results in the MC.

Task 1: Create an index for itops.

1. Create an index for the IT operations team by navigating to **Settings > Indexes > New Index**. Use the following values:
   - Index Name: `itops`
   - Index Data Type: `Events` (Default setting)
   - Max Size of Entire Index: `100 GB`
   - App: `Search & Reporting`
   - Leave the rest of the fields empty and accept the defaults.
2. Click **Save**.

Task 2: Configure a strict volume-based retention policy for itops.

3. In your text editor, update your `indexes.conf` file as follows in the `/opt/splunk/etc/apps/search/local`:

   Insert the following two volume stanzas before the `itops` stanza:

```
...

[volume:one]
path = /opt/home/{idx-os-user}/one/
                                (substitute your {idx-os-user} name)
maxVolumeDataSizeMB = 40000

[volume:two]
path = /opt/home/{idx-os-user}/two/
                                (substitute your {idx-os-user} name)
maxVolumeDataSizeMB = 80000

[itops]
coldPath = volume:two/itops/colddb    (edit)
enableDataIntegrityControl = 0
enableTsidxReduction = 0
homePath = volume:one/itops/db        (edit)
maxTotalDataSizeMB = 102400
thawedPath = $SPLUNK_DB/itops/thaweddb
homePath.maxDataSizeMB = 30000        (add)
coldPath.maxDataSizeMB = 60000        (add)
```

Insert the following two volume stanzas before the **itops** stanza:

```
[volume:one]
path = C:/vol/one/                (NOTE: forward slashes required here)
maxVolumeDataSizeMB = 40000

[volume:two]
path = C:/vol/two/                (NOTE: forward slashes required here)
maxVolumeDataSizeMB = 80000

[itops]
coldPath = volume:two\itops\colddb   (edit)
enableDataIntegrityControl = 0
enableTsidxReduction = 0
homePath = volume:one\itops\db       (edit)
maxDataSize = auto
maxTotalDataSizeMB = 102400
thawedPath = $SPLUNK_DB\itops\thaweddb
homePath.maxDataSizeMB = 30000       (add)
coldPath.maxDataSizeMB = 60000       (add)
```

This sets the volume limit of the hot and warm buckets to be no more than 30 GB out of 40GB and the cold buckets to be no more than 60 GB out of 80 GB.

4. Save your changes and close the text editor.
5. Restart Splunk using the CLI.

```
/opt/splunk/bin/splunk restart
```

```
C:\Program Files\Splunk\bin\splunk restart
```

The local directories used to simulate a storage volume mount will automatically be created after the Splunk restart completes.

Task 5: Use the MC to view the retention settings.

6. Navigate to **Settings > Monitoring Console**.
7. To check the retention overview, navigate to **Indexing > Indexes and Volumes > Indexes and Volumes: Instance**.

Index		Data Age vs Frozen Age (days)	Index Usage (GB)	Home Path Usage (GB)	Cold Path Usage (GB)	Count	Count
_audit	event	26 / 2184	0.01 / 488.28	0.01 / unlimited	0 / unlimited	68,885	10
_internal	event	26 / 30	0.58 / 488.28	0.58 / unlimited	0 / unlimited	6,602,693	13
_introspection	event	14 / 14	1.03 / 488.28	1.03 / unlimited	0 / unlimited	912,084	6
_telemetry	event	25 / 730	0.00 / 488.28	0.00 / unlimited	0 / unlimited	99	5
airlinedata	event	14 / 2184	0.04 / 500.00	0.04 / unlimited	0 / unlimited	1,140,236	1
itops	event	56 / 2184	0.00 / 100.00	0.00 / 29.30	0 / 58.59	23,143	0
main	event	0 / 2184	0.00 / 488.28	0.00 / unlimited	0 / unlimited	0	0
securityops	event	116 / 90	0.01 / 500.00	0.01 / unlimited	0 / unlimited	81,892	4
splunklogger	event	0 / 2184	0.00 / 488.28	0 / unlimited	0 / unlimited	0	0
summary	event	0 / 2184	0.00 / 488.28	0.00 / unlimited	0 / unlimited	0	0

« prev 1 2 next »

The columns use attributes specified in indexes.conf

- **Data Age vs Frozen Age:** The first value is based on the age of the oldest event in the index. The second value is derived from the attribute frozenTimePeriodInSecs.
- **Index Usage:** The first value is the current size of the index. The second value is the index capacity, as specified in maxTotalDataSizeMB.
- **Home Path Usage:** The first value is the current size of the home path portion of the index. The second value is the home path capacity, as specified in homePath.maxDataSizeMB.
- **Cold Path Usage:** The first value is the current size of the cold path portion of the index. The second value is the cold path capacity, as specified in coldPath.maxDataSizeMB.

Volumes (2)

Volume	Volume Usage (GB)	Volume Capacity (GB)	Volume Path
one	0.00 / 39.06	39.06	/opt/home/walt/one/
two	0.00 / 78.13	78.13	/opt/home/walt/two/

8. To see the index detail of the **itops** index, click **`itops`**.
   - The **Index Detail: Instance** page opens with the **`itops`** index selected.
   - Scroll down to the **Settings** panel to confirm the retention policy changes you have made.

Settings

Paths		Retention policies		Index Structure & Bucket Configuration	
Setting	Value	Setting	Value	Setting	Value
homePath	volume:one/itops/db	maxTotalDataSizeMB	102400	maxDataSize	auto
homePath_expanded	/opt/home/panya/one	frozenTimePeriodInSecs	188697600	maxHotBuckets	3
coldPath	volume:two/itops/co	homePath.maxDataSizeMB	30000	maxWarmDBCount	300
coldPath_expanded	/opt/home/panya/two	coldPath.maxDataSizeMB	60000		
thawedPath	$SPLUNK_DB/itops/th				
thawedPath_expanded	/opt/splunk/var/lib				
summaryHomePath_expanded	/opt/home/panya/one				
tstatsHomePath	volume:_splunk_summ				
tstatsHomePath_expanded	/opt/splunk/var/lib				

Troubleshooting Suggestion

1. Verify the **`indexes.conf`** configurations.

	`/opt/splunk/etc/apps/search/local/indexes.conf`
	`C:\Program Files\Splunk\etc\apps\search\local\indexes.conf`

Linux server	Windows server

`[securityops]`
`coldPath = $SPLUNK_DB/securityops/colddb`
`enableDataIntegrityControl = 0`
`enableTsidxReduction = 0`
`homePath = $SPLUNK_DB/securityops/db`
`maxDataSize = auto_high_volume`
`maxTotalDataSizeMB = 512000`
`thawedPath = $SPLUNK_DB/securityops/thaweddb`
`maxHotSpanSecs = 86400`
`frozenTimePeriodInSecs = 7776000`
 	
`[volume:one]`
`path = /opt/home/{idx-os-user}/one/`
`maxVolumeDataSizeMB = 40000`
 	
`[volume:two]`
`path = /opt/home/{idx-os-user}/two/`
`maxVolumeDataSizeMB = 80000`
 	
`[itops]`
`coldPath = volume:two/itops/colddb`
`enableDataIntegrityControl = 0`
`enableTsidxReduction = 0`
`homePath = volume:one/itops/db`
`maxTotalDataSizeMB = 1024000`
`thawedPath = $SPLUNK_DB/itops/thaweddb`
`homePath.maxDataSizeMB = 30000`
`coldPath.maxDataSizeMB = 60000`
	`[securityops]`
	`coldPath = $SPLUNK_DB\securityops\colddb`
	`enableDataIntegrityControl = 0`
	`enableTsidxReduction = 0`
	`homePath = $SPLUNK_DB\securityops\db`
	`maxDataSize = auto_high_volume`
	`maxTotalDataSizeMB = 512000`
	`thawedPath = $SPLUNK_DB\securityops\thaweddb`
	`maxHotSpanSecs = 86400`
	`frozenTimePeriodInSecs = 7776000`
	
	`[volume:one]`
	`path = c:/vol/one/`
	`maxVolumeDataSizeMB = 40000`
	
	`[volume:two]`
	`path = c:/vol/two/`
	`maxVolumeDataSizeMB = 80000`
	
	`[itops]`
	`coldPath = volume:two\itops\colddb`
	`enableDataIntegrityControl = 0`
	`enableTsidxReduction = 0`
	`homePath = volume:one\itops\db`
	`maxTotalDataSizeMB = 1024000`
	`thawedPath = $SPLUNK_DB\itops\thaweddb`
	`homePath.maxDataSizeMB = 30000`
	`coldPath.maxDataSizeMB = 60000`

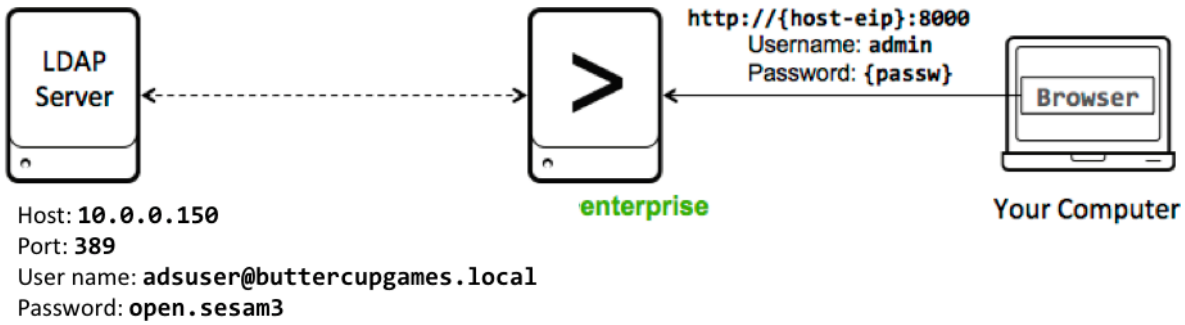
Appendix B Lab: Configure Splunk to use LDAP

Description

Your organization uses the Active Directory (AD) services to manage users and computers. AD makes use of Lightweight Directory Access Protocol (LDAP) to authenticate and authorize all users and computers in a network. In this exercise, you will configure Splunk to use AD LDAP service for access controls.

Task 1: Configure Splunk to use LDAP.

In this task, you create an LDAP strategy to use the lab environment's LDAP Server.



1. Navigate to **Settings > Users and Authentication > Authentication method**.
2. Select the **LDAP** radio button and click **Configure Splunk to use LDAP**.
3. Click **New LDAP**.
4. Populate the form as follows:
   - LDAP strategy name: `AD_splunkers`
   - Host: `10.0.0.150`
   - Port: `389`
   - Bind DN: `adsuser@buttercupgames.local`
   - Bind DN Password: `open.sesam3`
   - Confirm password: `open.sesam3`
   - User base DN: `OU=splunk,DC=buttercupgames,DC=local`
   - User base filter: *(leave blank)*
   - User name attribute: `samaccountname`
   - Real name attribute: `displayName`
   - Email attribute: *(leave blank)*
   - Group mapping attribute: `dn`
   - Group base DN: `OU=splunk,DC=buttercupgames,DC=local`
   - Static group search filter: *(leave blank)*
   - Group name attribute: `cn`
   - Static member attribute: `member`

5. Leave the rest of the fields blank or at default values. Click **Save**.

If you encounter an error, check the troubleshooting suggestions section.

Task 2: Map LDAP groups to Splunk roles.

In this task, you map Active Directory groups to Splunk roles.

6. Click **Map groups**.

LDAP strategy name	Host	Port	Connection order	Status	Actions
AD_splunkers	10.0.0.150	389	1	Enabled | Disable	Map groups | Clone | Delete

7. For each **LDAP Group Name**, assign the following Splunk **Roles** by clicking on the group name, selecting the role, and clicking **Save**:

LDAP Group Name	Splunk Roles
splunkAdmins	`admin`
splunkBizDev	`user`
splunkITOps	`power`
splunkSOC	`soc_analyst`

When you are done, it should look like this:

LDAP Group Name	LDAP Strategy	Group type	Roles
splunkAdmins	AD_splunkers	static	admin
splunkBizDev	AD_splunkers	static	user
splunkITOps	AD_splunkers	static	power
splunkSOC	AD_splunkers	static	soc_analyst

Check Your Work

Task 3: Verify the LDAP configuration.

In this task, you verify the capabilities of Active Directory users.

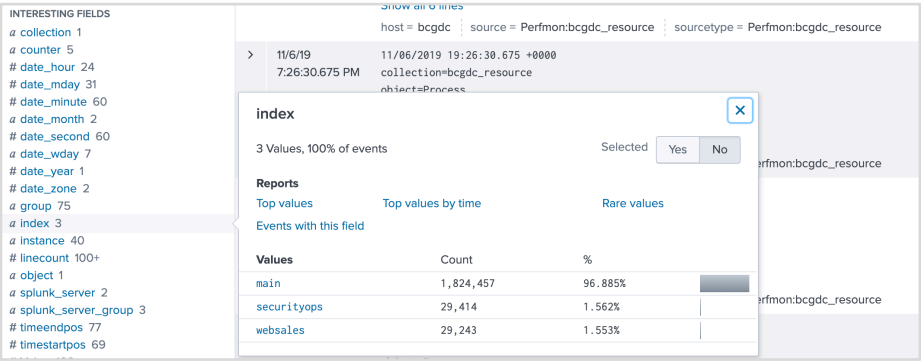
8. Navigate to **Settings > Users and Authentication > Users**.

   How many users are imported from Active Directory? 10

   Which LDAP users are mapped to the **user** role? Bao Lu (blu) and Dwight Hale (dhale)

9. Log in as `nsharpe` or `pbunch` (password: `open.sesam3`) and search `index=*` for **Last 30 days**.

   Which indexes appear in the results? main, securityops, and websales



Troubleshooting Suggestion

1. Check the output of **SPLUNK_HOME/etc/system/local/authentication.conf**. It should be:

```
[AD_splunkers]
SSLEnabled = 0
anonymous_referrals = 1
bindDN = adsuser@buttercupgames.local
bindDNpassword = <some hashed password>
charset = utf8
emailAttribute = mail
groupBaseDN = OU=splunk,DC=buttercupgames,DC=local
groupMappingAttribute = dn
groupMemberAttribute = member
groupNameAttribute = cn
host = 10.0.0.150
nestedGroups = 0
network_timeout = 20
port = 389
realNameAttribute = displayName
sizelimit = 1000
timelimit = 15
userBaseDN = OU=splunk,DC=buttercupgames,DC=local
userNameAttribute = samaccountname

[authentication]
authSettings = AD_splunkers
authType = LDAP

[roleMap_AD_splunkers]
admin = splunkAdmins
power = splunkITOps
soc_analyst = splunkSOC
user = splunkBizDev
```