

Splunk Enterprise System Administration – 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 (If you are unfamiliar with vi , use nano . It is an easy text editor.)
Windows server:	Notepad++

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



Linux OS



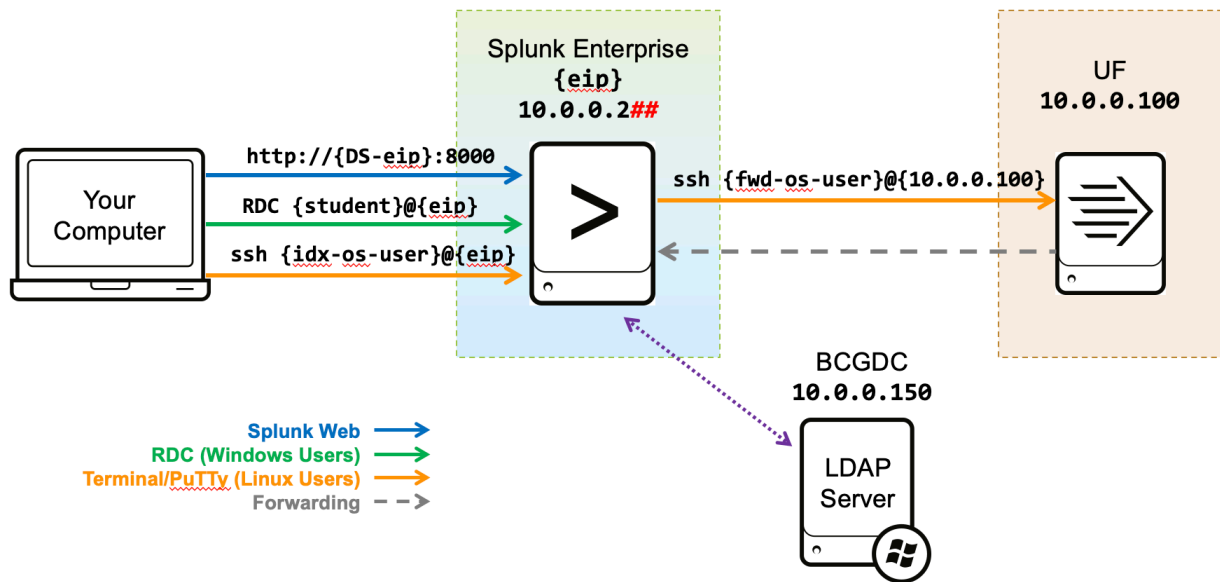
Windows OS

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 a Splunk Server

Description

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

Please ensure you are able to identify all of the following values that have been provided to you.

Your student ID is a unique 2-digit identifier used throughout the lab exercises to differentiate your work from other class participants' work. When asked in the labs, substitute the “##” references with your student ID

Student ID:

{student-ID}

Splunk Server Credentials

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

Splunk Web URL:

https://_____:8000
 {host-eip}

Splunk Username

admin

Password:

{password}

Linux OS Credentials

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

Linux Host name:

{host-eip}

Linux Username:

{idx-os-user}

Password:

{password}

Windows OS Credentials

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

Windows Host name:

{host-eip}

RDC Username:

{idx-os-user}

Password:

{password}

Steps

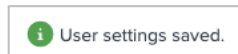
Task 1: Access Splunk Web and change the basic settings.

1. Direct your web browser to your Splunk (Indexer/Search Head) instance:
https://{host-eip}:8000
2. Log in as **admin** using your assigned password **{password}**.
3. Dismiss any unnecessary informational messages.
 - Click **Got it!** in the “**Helping You Get More Value from Splunk Software**” pop-up page.
 - If an “Important changes coming!” pop-up page appears, click **Don’t show me this again**.
 - If you are prompted to change the password, click **Skip** to continue using the provided password.
4. 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.
5. Click **Administrator > Account Settings** and change the **Full name** to *your name*.
6. In the **Email address** field, replace the current value with your two-digit **{student-ID}**.

Hint: Leading zero required for student IDs 01-09.

7. Click **Save**.

Notice the **User settings saved** indicator at the top. (You may have to refresh your browser.)



8. Navigate to **Settings > Server settings > General settings**.

Make note of the path specified in the **Installation path** field: _____

This directory where Splunk is installed is referred to as **SPLUNK_HOME**.

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

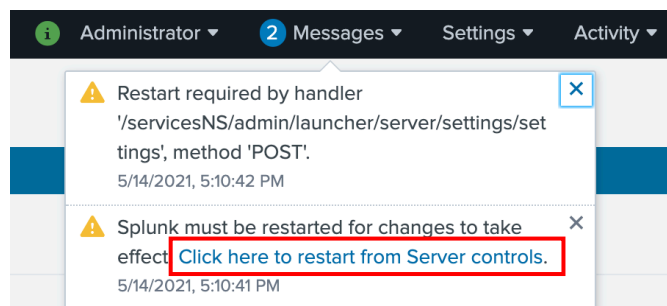
Splunk server name: **splunk##** where **##** is your **{student-ID}**

Default host name: **splunk##** where **##** is your **{student-ID}**

10. Click **Save**.

These changes require a restart of Splunk.

11. Click **Messages > Click here to restart from Server controls > Restart Splunk > OK**.



12. Click **OK** when the dialog box indicates that the restart was successful.

13. After the restart, log back into Splunk Web with user **admin** and your assigned password.

After you log back in if you see the **Server controls** page, do *not* click the **Restart Splunk** button again.

Task 2: Access the command terminal of your designated Splunk server.

14. Connect to the command line of your dedicated Splunk indexer/search head.



If your Indexer is Linux, use one of these two methods:

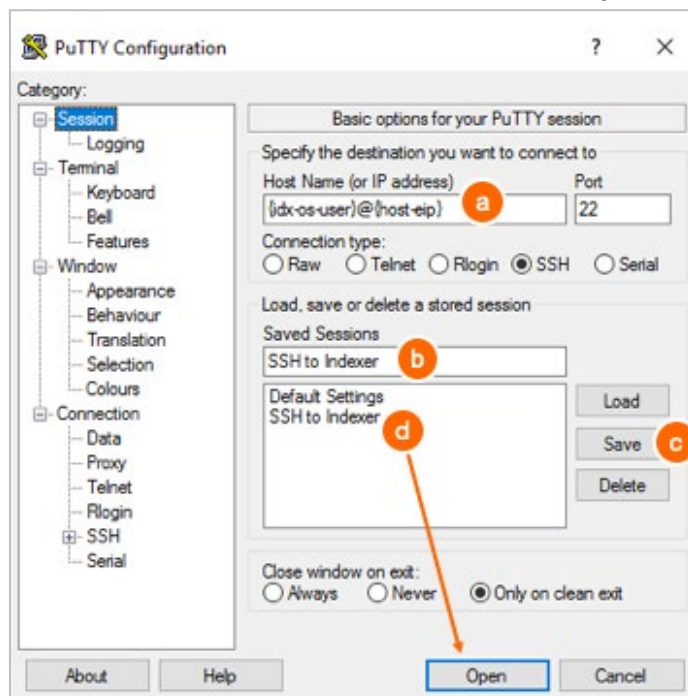
1. If your home computer is running *nix (or macOS), start an SSH session to your indexer by opening a terminal window and executing:

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

2. OR, if your home computer is Windows, use an SSH client, such as PuTTY. (PuTTY is a free and reliable SSH client found at <https://www.putty.org/>)

To use PuTTY to start an SSH session to your indexer:

- a. Replace **{idx-os-user}@{host-eip}** with your designated values.
- b. Name your session, for example **"SSH to Indexer"**
- c. Save the session for later re-use.
- d. Click on the session **"SSH to Indexer"** and click **Open** to start the session.





If your indexer is Windows, 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**.

15. When prompted for the authenticity of the host and the key fingerprint, type "yes" to continue.

Task 3: Retrieve basic system information using CLI.

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



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



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

17. Run a 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: #####,#####,...)
```



```
Splunkd: Running (pid #####)
```

18. 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
Splunk management (splunkd) port:	./splunk show splunkd-port
Splunk App Server ports:	./splunk show appserver-ports
Splunk KV store port:	./splunk show kvstore-port
Splunk server name:	./splunk show servername
Default host name:	./splunk show default-hostname

```
./splunk version
Splunk 8.2.0 (build #####)

./splunk show web-port
Your session is invalid. Please login.
Splunk username: admin
Password: ***** (using the admin password {password})
Web port: 8000

./splunk show splunkd-port
Splunkd port: 8089

./splunk show appserver-ports
Application server ports on loopback interface: 8065

./splunk show kvstore-port
KV Store port: 8191

./splunk show servername
Server name: splunk## (where ## is your {student-ID})

./splunk show default-hostname
Default hostname for data inputs: splunk##. (where ## is your {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 – Splunk Server Monitoring


Description

In this lab you will enable the Monitoring Console, run Splunk diag, update an Enterprise Trial license to an Enterprise license and modify the license pool, and enable a Monitoring Console alert.

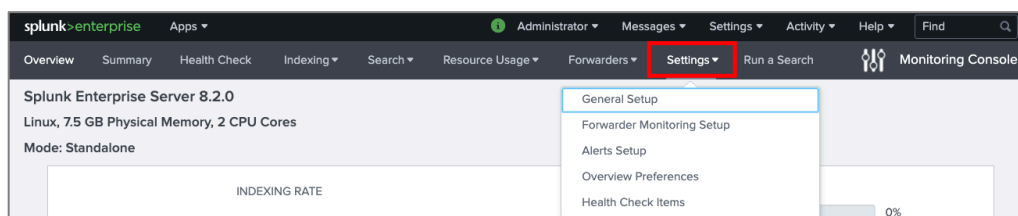
Check Your Work

Task 1: Enable the Monitoring Console (MC) app.

1. In Splunk Web, navigate to **Settings > Monitoring Console**.

Look for the **Monitoring Console** icon on the left side of the **Settings** menu. 

2. On the Monitoring Console navigation bar (the dark grey bar found under the black Splunk Web navigation bar) click **Settings > General Setup**.



3. Verify the server name and make a note of the discovered server roles.

Setup

Current topology of Splunk Enterprise deployment. [Learn more](#)

Mode

Standalone

Distributed

Reset All Settings

Apply Changes

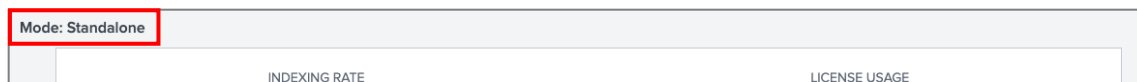
This instance

i	Instance (host)	Instance (serverName)	Machine	Server roles	Custom groups	Indexer Cluster(s)	Search Head Cluster(s)	Monitoring	State	Problems	Actions
>	splunk02	splunk02	ip-10-0-0-202	Indexer License Master KV Store Search Head	Only available in distributed mode.			✓ Enabled	● Configured		Edit

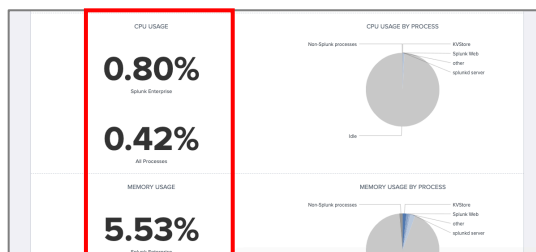
4. To complete the app setup, click **Apply Changes > Go to Overview**.

5. On the **Overview** page, review the following:

- Monitoring Console is running in standalone mode.



- No errors are displayed.
- No excessive resource usage is detected. The CPU Usage and Memory Usage rates should be low (less than 20%).



Task 2: Start and view Health Check for your Splunk server.

- From the Monitoring Console, click **Health Check**.
- Click **Start** to view the current results for the instance. Wait until the health check has completed.

For the lab environment ignore any warnings, and just confirm that other components are operational.

Check ↕	Category ↕	Tags ↕	Results ↕
System hardware provisioning assessment	System and Environment	best_practices, capacity, scalability	⚠ One or more hosts has returned CPU or mem
Assessment of server ulimits	System and Environment	best_practices, operating_system	⚠ One or more Splunk instances are running on
Event-processing issues	Data Collection	event_breaking, indexing, timestamp_extraction	✅ This health check item was successful.
Expiring or expired licenses	Data Indexing	licensing	✅ This health check item was successful.
Indexing status	Data Indexing	buckets, indexing	✅ This health check item was successful.
License warnings and violations	Data Indexing	indexing, licensing	✅ This health check item was successful.
Saturation of event-processing queues	Data Indexing	indexing, queues	✅ This health check item was successful.
Search scheduler skip ratio	Data Search	scheduler, searches_skipped	✅ This health check item was successful.
Excessive physical memory usage	Splunk Miscellaneous	resource_usage	✅ This health check item was successful.
Integrity check of installed files	Splunk Miscellaneous	configuration, installation	✅ This health check item was successful.
KV Store status	Splunk Miscellaneous	kv_store	✅ This health check item was successful.
Orphaned scheduled searches	Splunk Miscellaneous	configuration, search, searches_skipped	✅ This health check item was successful.
Near-critical disk usage	System and Environment	capacity, disk_space, searches_skipped, storage	✅ This health check item was successful.
Linux kernel transparent huge pages	System and Environment	best_practices, operating_system	✅ This health check item was successful.
Missing forwarders	Data Indexing	batchreader, forwarding, tailreader	⚪ This health check item is not applicable.

- Click the green information (i) icon next to your name to check the health status of **splunkd**.



Health Status of Splunkd

splunkd

- File Monitor Input
 - BatchReader-0
 - Ingestion Latency
 - TailReader-0
- Index Processor
 - Buckets
 - Disk Space
 - Index Optimization
- Resource Usage
 - IOWait
- Search Scheduler
 - Search Lag
 - Searches Delayed
 - Searches Skipped
- Workload Management

How to interpret this health report:

This health report displays information from the `/health/splunkd/details` endpoint. There are three potential states for a feature:

- i Green: The feature is functioning properly.
- ⚠ Yellow: The feature is experiencing a problem. The feature's status might automatically improve, or it might worsen over time. For details, see Root Cause.
- ! Red: The feature has severe issues and is negatively impacting the functionality of your deployment. For details, see Root Cause.
- ? Grey: Health report is disabled for the feature.

To manage red and yellow threshold values for the individual features, go to [Health Report Manager](#).

For more information on this health report, see [Learn more](#).

You should see that the health reports show green. The title on a standalone deployment is “Health Status of Splunkd”. (On a distributed deployment the title is “Health Status of Splunk Deployment” and some reports and indicators will be sourced from remote systems.)

Task 3: Update the initial trial license to an Enterprise license.

9. In Splunk Web, select **Settings > Licensing** to access the **Licensing** page.
What license group is your server currently configured to use? **Trial license group**
10. Get a temporary Splunk license to use for testing in this lab.
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.
11. From the **Licensing** page, click **Add license**.
12. Click **Choose File** and locate the file downloaded to your local system: **splunk.license.big.license**
13. Click **Open** and then click **Install**.
14. Click **Restart Now > OK**.
15. After the restart, log back into Splunk Web with user **admin** and your assigned password, 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 4: Modify the license pool.

16. From the **Licensing** page, click the **Edit** link next to the **auto_generated_pool_enterprise** pool.
17. From **Allocation**, click **A specific amount** and set the allocation to **150 MB**.
18. From **Indexers**, click **Specific indexers**.
19. From the **Available indexers** field, select your host and move it to the **Associated indexers** field.
20. Click **Submit > OK**.
21. Confirm the settings you have configured for this pool on the **Licensing** page.

Task 5: Enable an alert to monitor the license usage.

22. Navigate to **Settings > Monitoring Console** and scroll down to the **Alerts** section of the **Overview** page and click **Enable or Disable**.
23. Click the **Enable** next to the **DMC Alert - Total License Usage Near Daily Quota** alert.
24. To confirm, click **Enable**.
An alert will be provided if 90% of your pool quota is consumed.
25. Click the **Edit** button next to the **DMC Alert - Total License Usage Near Daily Quota** alert.



26. Change the **License Quota Usage** to 60 and click **Save**.
Notice the alert text was updated to show "60%".



NOTE: You will see this alert triggered later in this course.

Task 6: Create a Splunk diag file for a Splunk server using the command line.

27. From your Splunk server, generate a baseline diag file using the **splunk diag** command in a console window.



```
cd /opt/splunk/bin/  
./splunk diag  
  
...  
Splunk diagnosis file created: /opt/splunk/diag-ip-10-0-0-202-  
2021-05-17_16-39-36.tar.gz
```



```
cd C:\Program Files\Splunk\bin  
splunk diag  
  
...  
Splunk diagnosis file created:  
C:\Program Files\Splunk\diag-splunk_indexer-2021-05-17_15-24-  
18.tar.gz
```

NOTE: We ingest this file into Splunk for analysis later in this course.

Module 3 Lab Exercise – Install an App

Description

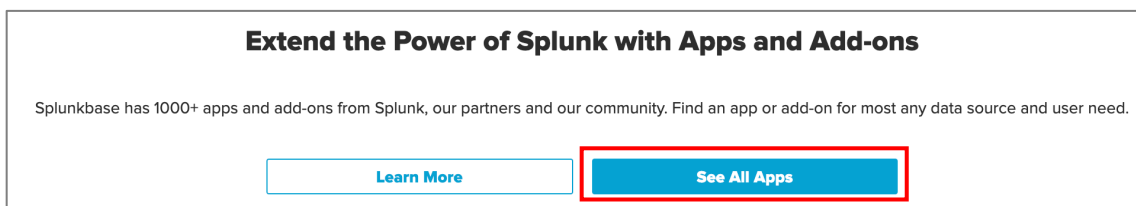
Apps and add-ons are a quick way to get value from your input data. In this lab exercise, you will install a sample app that configures an input, reports, dashboards, a lookup, and an index.

Steps

Task 1: Explore Splunk apps on Splunkbase.

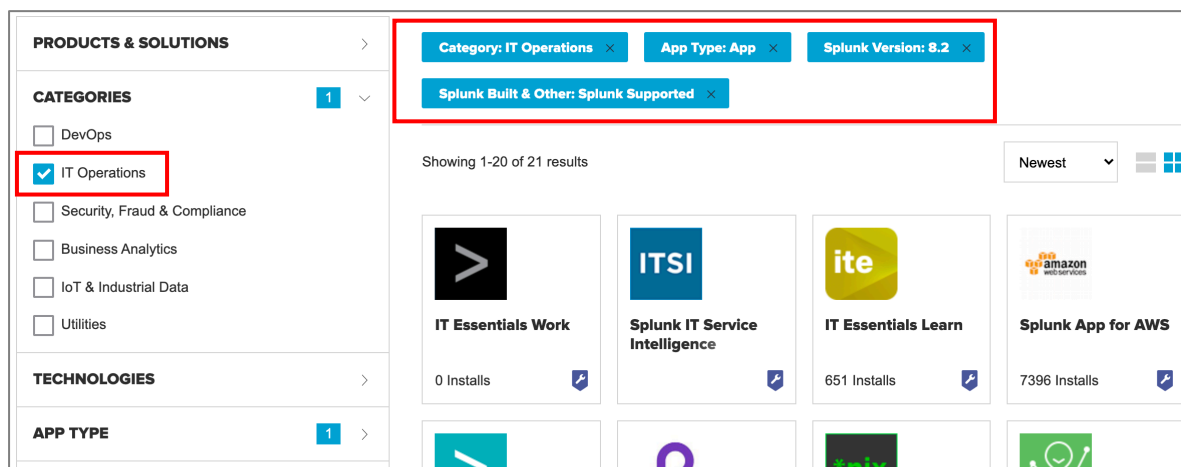
In this task, you explore the Splunkbase website and view some of the Splunk apps currently available on that site.

1. Visit <https://splunkbase.splunk.com/>. (Note that to download any apps from Splunkbase, you first need a Splunk.com account. You do not need to create a Splunk.com account for this exercise.)
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:** 8.2
- **Splunk Built & Other:** Splunk Supported



How many apps meet the above criteria?

As of this writing, 21.

4. Optionally explore other areas and applications on the Splunkbase site, at your leisure.

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. For this exercise, download the sample app (**admin82.sp1**) from <https://splk.it/edu-sysadmin-81>.
6. In Splunk Web, navigate to **Settings > Indexes** and note the indexes that are currently configured for this instance.

You should see a number of internal indexes starting with an underscore (_), such as **_internal** and **_thefishbucket**. There are also some default indexes, such as **main**.

7. In Splunk Web, navigate to **Apps > Manage Apps** page.
Alternatively, click the gear icon (⚙) if you are on the **Home** page (launcher).
8. Click **Install app from file > Choose File** to locate the **admin82.sp1** file you downloaded in step 5.
9. Click **Upload**.

Notice on the **Apps** page that **System Admin 8.2 Class App** now appears in the list.

10. In Splunk Web, navigate to **Settings > Indexes**.
Notice that a new index called **"websales"** has been installed.

11. Navigate to the **Apps > System Admin 8.2 Class App**.
System Admin 8.2 Class App is listed on the **Home** page as well as under the **Apps** dropdown.

12. Click **Apps > Manage Apps**.
13. For the **System Admin 8.2 Class App**, click **Permissions**.
14. Configure the permissions so only the **admin** role has **Read** and **Write** permissions.

Roles	Read	Write
Everyone	<input type="checkbox"/>	<input type="checkbox"/>
admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
can_delete	<input type="checkbox"/>	<input type="checkbox"/>
power	<input type="checkbox"/>	<input type="checkbox"/>
splunk-system-role	<input type="checkbox"/>	<input type="checkbox"/>
user	<input type="checkbox"/>	<input type="checkbox"/>

NOTE: To be able to click on the checkboxes for **admin**, you will first need to uncheck **Read** and **Write** permissions for **Everyone**.

15. Click **Save**.

Check Your Work

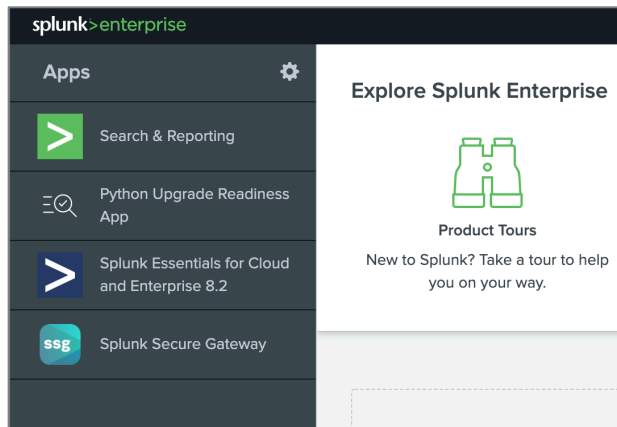
Task 3: Verify the app installation.

16. Log out of Splunk Web as **admin** by clicking on your username and selecting **Logout**.

17. Log into Splunk Web as **emaxwe11 / open.sesam3**.

18. Confirm that the **System Admin 8.2 Class App** app is not accessible.

You should see only the default apps, such as **Search & Reporting**, in the left navigation bar.

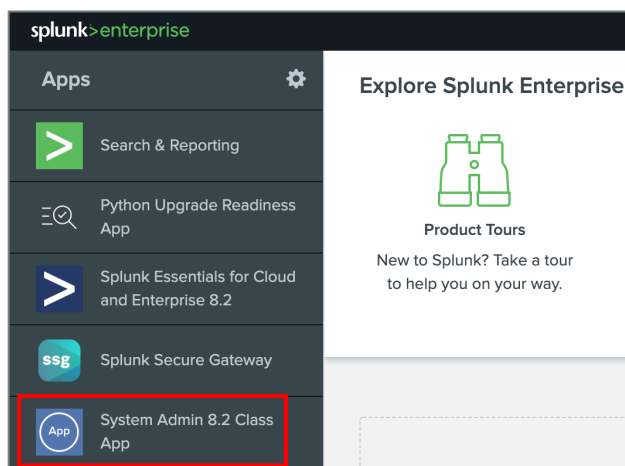


19. Log out of Splunk Web as **emaxwell** by clicking on username **emaxwell > Logout**.

20. Log into Splunk Web as **admin / {password}**.

21. Click the **splunk>enterprise** logo in the top left.

You should see additionally see the **System Admin 8.2 Class App** in the left navigation bar.



Module 4 Lab Exercise – Examine User 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.

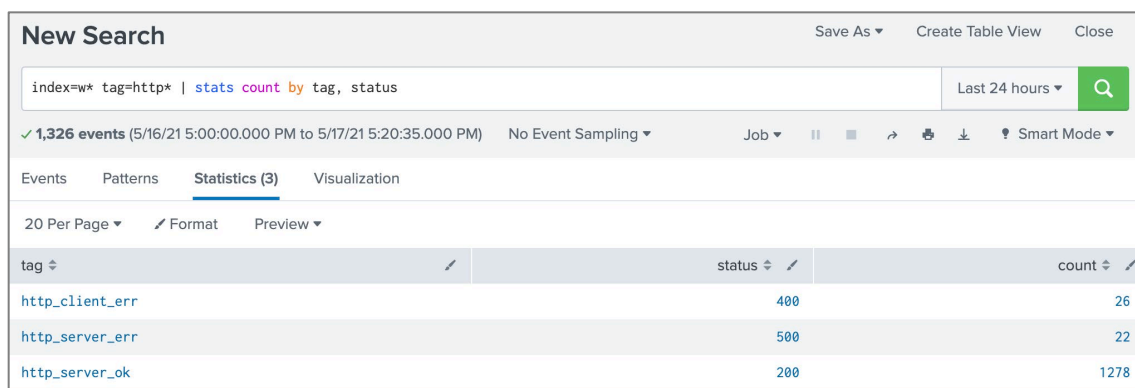
NOTE: You must successfully complete the Module 3 lab steps to see the expected results in this lab exercise.

Steps

Task 1: Identify a configuration problem with tags.

- 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.

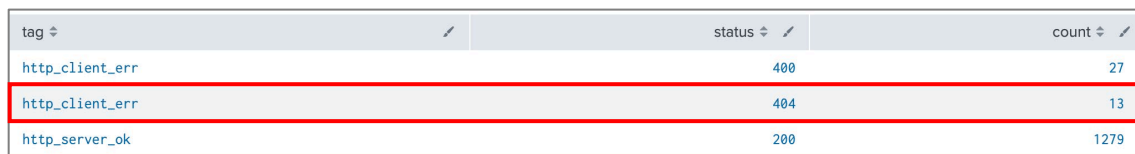


The screenshot shows the 'New Search' interface in Splunk. The search query is 'index=w* tag=http* | stats count by tag, status' and the time range is 'Last 24 hours'. The results show 1,326 events. The table displays the following data:

tag	status	count
http_client_err	400	26
http_server_err	500	22
http_server_ok	200	1278

- Log in as **emaxwell / open.sesam3**.
- 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
- Note the results that **emaxwell** gets from the same search.

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



The screenshot shows the search results for user emaxwell. The table displays the following data:

tag	status	count
http_client_err	400	27
http_client_err	404	13
http_server_ok	200	1279

Investigate the Problem

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

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

- From your terminal window, navigate to the **SPLUNK_HOME/bin** directory:



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



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

- To display the tag stanzas, run the **splunk bttool** command:



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



```
splunk bttool tags list --debug
```

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

9. 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
```

10. 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.

```
/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/admin/search/local/tags.conf [status=500]
/opt/splunk/etc/users/admin/search/local/tags.conf http_server_err = enabled
```

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

Task 3: (OPTIONAL) 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 **bttool** output.

11. 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.

For example, on Linux:

```
./apps/search/local/tags.conf:http_server_ok = enabled
./apps/search/local/tags.conf:http_client_err = enabled
./users/emaxwell/search/local/tags.conf:http_client_err = enabled
./users/admin/search/local/tags.conf:http_server_err = enabled
```

For example, on Windows:

```
apps\search\local\tags.conf:http_server_ok = enabled
apps\search\local\tags.conf:http_client_err = enabled
users\admin\search\local\tags.conf:http_server_err = enabled
users\emaxwell\search\local\tags.conf:http_client_err = enabled
```

Viewing the contents of files will show the associated **[status=###]** stanzas. The contents of **emaxwell's tags.conf** file shows:

```
[status=404]
http_client_err = enabled
```

The contents of **admin's tags.conf** file shows:

```
[status=500]
http_server_err = enabled
```

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.

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 Entire Index** setting: **500000 MB**
 - Note the **Max Size of Hot/Warm/Cold Bucket** setting: **auto_high_volume**
3. Click **Cancel**.

Task 2: Create an index for securityops.

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

4. From **Settings > Indexes**, click **New Index**.
5. In the **Index Data Type** field, verify the default **Events** index is selected.
6. 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.

7. Leave the rest of the fields empty to accept the defaults and click **Save**.
8. View the resulting configurations.



Linux users can view the configuration using the **cat** command:

```
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 view the configuration using Notepad by opening the file `C:\Program Files\Splunk\etc\apps\search\local\indexes.conf`, or run:

```
type "C:\Program Files\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
```

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.

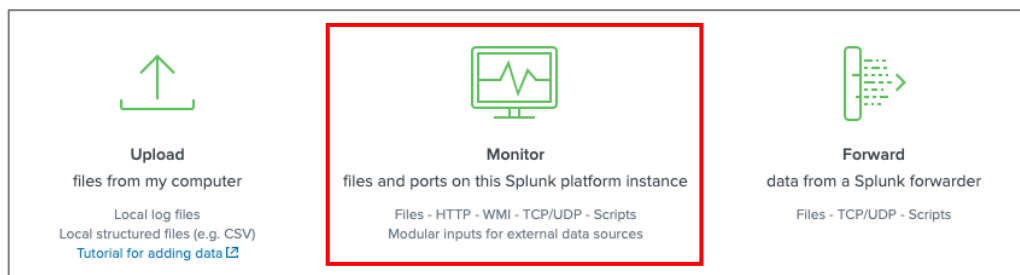
- To start indexing events into the **securityops** index, click **Settings > Add Data**.

Look for the **Add Data** icon on the left side of the **Settings** menu.



- Click **Skip** to dismiss the **Welcome** (quick tour) pop-up window.

- Click **Monitor** to start the local input wizard.



- On the **Select Source** step, click **Files & Directories**.

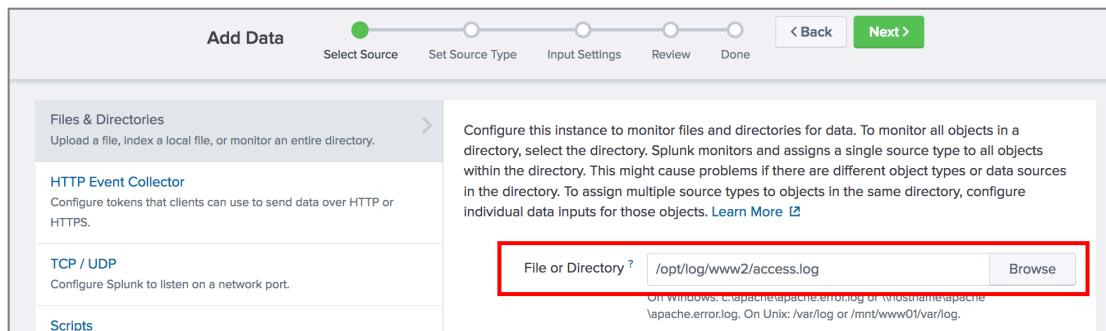
- Next to **File or Directory**, click **Browse** and navigate to select the following input source:



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



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



14. At the top of the page, click **Next** to display the **Set Source Type** step.



15. Verify the source type and proper event creation.

In this instance, Splunk automatically recognizes the data format and assigns a pretrained source type. In this case, **Source type: access_combined_wcookie**.

Also notice under the **Time** column that the events contain the correct timestamps from the **Event** information.

	Time	Event
1	2/13/21 4:44:39.000 PM	147.213.138.201 - - [13/Feb/2021:16:44:39] "GET /oldlink?itemId=EST-27&JSESSIONID=SD8SL5FF4ADFF4965 HTTP 1.1" 200 2468 "http://www.buttercupgames.com" "Opera/9.01 (Windows NT 5.1; U; en)" 303
2	2/13/21 4:44:44.000 PM	147.213.138.201 - - [13/Feb/2021:16:44:44] "GET /category.screen?categoryId=STRATEGY&JSESSIONID=SD8SL5FF4ADFF4965 HTTP 1.1" 200 2804 "http://www.buttercupgames.com/category.screen?categoryId=STRATEGY" "Opera/9.01 (Windows NT 5.1; U; en)" 300

Source types are explained in the *Splunk Enterprise Data Administration* course.

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

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

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

18. Click **Review**. The summary of the input should look like this:

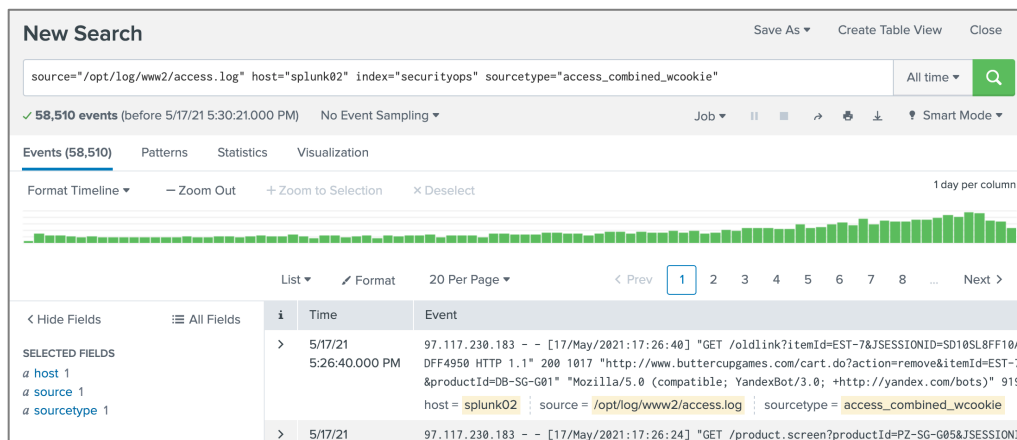
Input Type	File Monitor
Source Path	/opt/log/www2/access.log (Linux server) C:\opt\log\www2\access.log (Windows server)
Continuously Monitor	Yes
Sourcetype	access_combined_wcookie
App Context	search
Host	splunk##
Index	securityops

19. Click **Submit**.

20. 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.



Task 4: Index the baseline diag file for your records.

21. From your Splunk instance, click on **Settings > Add Data** to launch the **Add Data** wizard.

22. Click **Monitor**.

23. 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 created in Lab 2, Task 7, and click **Select**.

The filename should start with **diag**, and have the file extension of **.tar.gz**.

24. Select the **Index Once** option and click **Next** at the top of the page.

The Splunk diag output is ingested once, and we no longer require Splunk to monitor the file. These input settings are discussed in more detail in the *Splunk Enterprise Data Administration* course.

25. Select **App Context** as **Search & Reporting (search)** and **Index** as **main**, and click **Review**.

26. Verify the Review page has the following settings:

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

27. Click **Submit**.

Task 5: Search the diag contents for the system information.

28. From the Splunk server under **Apps > Search & Reporting**, 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 within the Splunk diag file and the associated event count.

source	count
/opt/splunk/diag-ip-10-0-0-202-2021-05-17-16-39-36.tar.gz:/diag-ip-10-0-0-202-2021-05-17-16-39-36/etc/apps/alert_logevent/README/alert_actions.conf.spec	1
/opt/splunk/diag-ip-10-0-0-202-2021-05-17-16-39-36.tar.gz:/diag-ip-10-0-0-202-2021-05-17-16-39-36/etc/apps/alert_logevent/README/savedsearches.conf.spec	1
/opt/splunk/diag-ip-10-0-0-202-2021-05-17-16-39-36.tar.gz:/diag-ip-10-0-0-202-2021-05-17-16-39-36/etc/apps/alert_logevent/bin/logevent.py	1
/opt/splunk/diag-ip-10-0-0-202-2021-05-17-16-39-36.tar.gz:/diag-ip-10-0-0-202-2021-05-17-16-39-36/etc/apps/alert_logevent/default/alert_actions.conf	11
/opt/splunk/diag-ip-10-0-0-202-2021-05-17-16-39-36.tar.gz:/diag-ip-10-0-0-202-2021-05-17-16-39-36/etc/apps/alert_logevent/default/app.conf	14

29. Execute the following search over **All Time**, replacing the **##** with your student ID:

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

The results currently show only the first few lines of the event, followed by **"Show all ### lines"**.

i	Time	Event
>	5/17/21 4:39:40.000 PM	<pre>diag launched by: user2 SPLUNK_HOME: /opt/splunk SPLUNK_ETC: not redirected ***** Splunk Version ***** Splunk 8.2.0 (build e053ef3c985f) Show all 257 lines host = splunk02 source = /opt/splunk/diag-ip-10-0-0-202-2021-05-17-16-39-36.tar.gz:/diag-ip-10-0-0-202-... sourcetype = systeminfo</pre>

30. In the returned event, click **Show all ### 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 *****

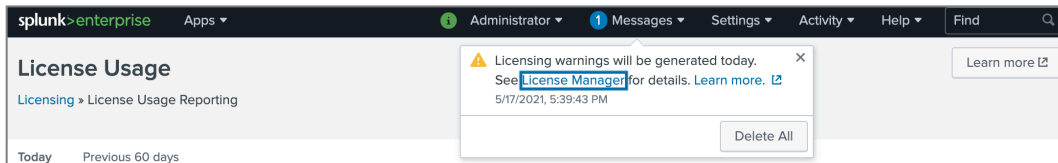
tasklist /V /FI IMAGENAME eq splunkd.exe output lists name, PID, session name, session#, memory usage, status, user name, CPU time, etc.

NOTE: On Windows you may not see **"Show all ### lines"**. If this is the case, you can still view the additional events by searching for **index=main source=*systeminfo.txt**.

Task 6: View license alerts.

Earlier in the Splunk Server Monitoring lab you set up an alert for licensing. In this task we examine what happens after ingesting the large diag file into Splunk has triggered our license alert.

31. Click **Messages** to view the license warning.



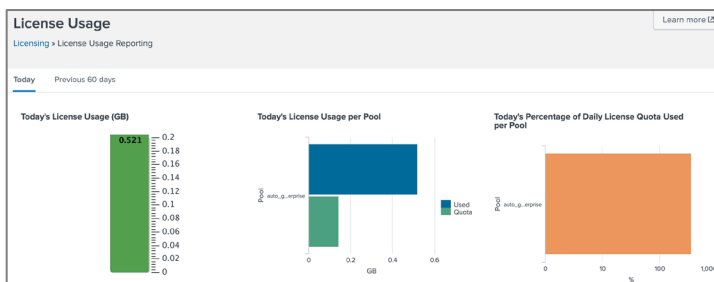
NOTE: It may take some time for the alert to appear. If you see “No triggered alerts found”, instead of waiting, feel free to come back to this step after a later lab.

32. Click **Settings > Licensing** and view the information under **Pools**.

Pools	Indexers	Volume used today
auto_generated_pool_enterprise		199 MB / 150 MB
	splunk02	199 MB (132.352%)

33. On the **Licensing** page, click on the **Usage report** button.

Notice the license usage reports.



34. In Splunk Web, click on **Activity > Triggered Alerts**. Ensure that the **App** drop-down field has **Monitoring Console** selected and **Owner** drop-down field is set to **All**.

NOTE: It may take up to 30 minutes for the alert to appear. If you see “No triggered alerts found”, instead of waiting, feel free to come back to this step after a later lab.

The **DMC Alert – Total License Usage Near Daily Quota** has been triggered.

App

Monitoring Console (splunk_mon...)

Owner

Administrator (admin)

Severity

All

Alert

All

Filter

«Prev

Next»

Showing 1-1 of 1 result

	Time	Fired alerts	App	Type	Severity	Mode	Actions
<input type="checkbox"/>	2020-10-12 18:33:00 UTC	DMC Alert - Total License Usage Near Daily Quota	splunk_monitoring_console	Scheduled	<div>Medium</div>	Digest	View results Edit search Delete

35. Click on **View results**.

Under the **New Search**, view the results that show which instance triggered the alert.

Instance	License quota used (%)	License quota used (GB)	Total license quota (GB)
splunk02	99.5	0.194	0.195

Module 6 Lab Exercise – Splunk Index Management

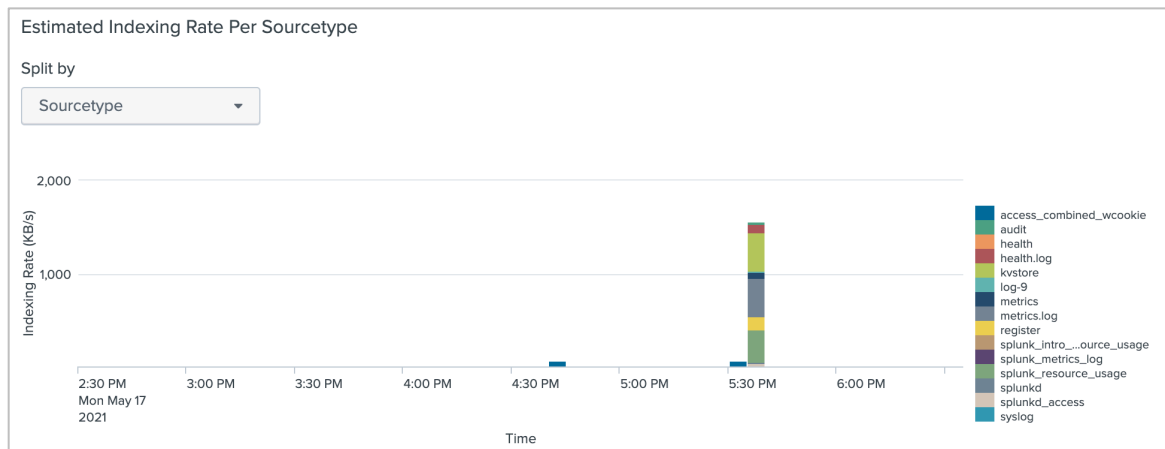
Description

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.

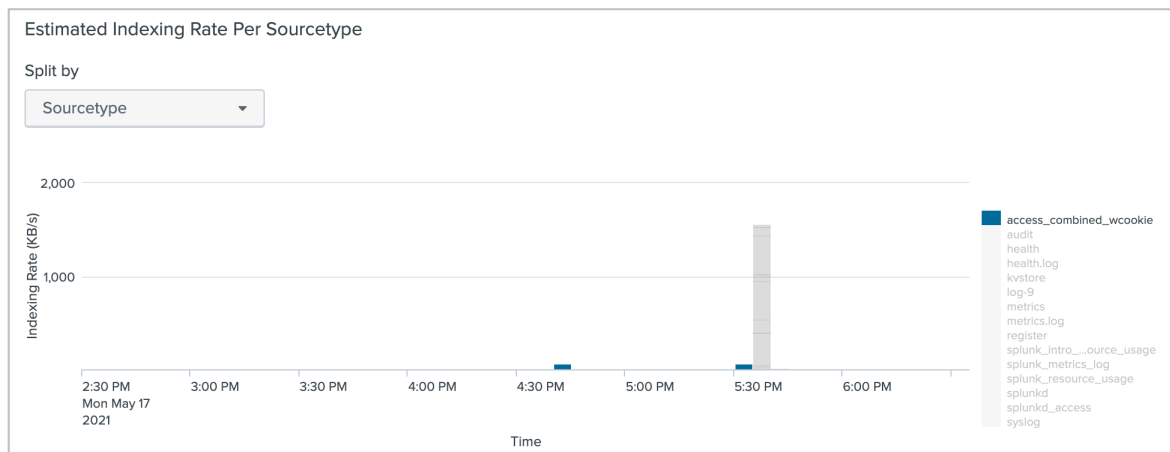
Steps

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**



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

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	3 / 2184	0.00 / 488.28	0.00 / unlimited	0 / unlimited	29,132	3
_internal	event	3 / 30	0.09 / 488.28	0.09 / unlimited	0 / unlimited	1,554,989	3
_introspection	event	3 / 14	0.19 / 488.28	0.19 / unlimited	0 / unlimited	246,164	3
_telemetry	event	3 / 730	0.00 / 488.28	0.00 / unlimited	0 / unlimited	22	2
main	event	1830 / 2184	0.24 / 488.28	0.24 / unlimited	0 / unlimited	1,838,393	8
securityops	event	93 / 2184	0.01 / 500.00	0.01 / unlimited	0 / unlimited	58,547	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
websales	event	93 / 2184	0.01 / 50.00	0.01 / unlimited	0 / unlimited	58,566	2

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

Bucket Size (GB)

Bucket Event Count

Bucket Count

Host ↕	Event Count ↕
splunk02	58560

Source ↕	Event Count ↕
/opt/log/www2/access.log	58560

Sourcetype ↕	Event Count ↕
access_combined_wcookie	58560

Setting ↕	Value ↕	Setting ↕	Value ↕	Setting ↕	Value ↕
homePath	\$SPLUNK_DB/securityops/db	maxTotalDataSizeMB	512000	maxDataSize	auto_high_volume
homePath_expanded	/opt/splunk/var/lib/splunk/securit	frozenTimePeriodInSecs	188697600	maxHotBuckets	auto
coldPath	\$SPLUNK_DB/securityops/colddb	homePath.maxDataSizeMB	0	maxWarmDBCount	300
coldPath_expanded	/opt/splunk/var/lib/splunk/securit	coldPath.maxDataSizeMB	0		
thawedPath	\$SPLUNK_DB/securityops/thaweddb				

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

- 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
enableTsidxReduction = 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
enableTsidxReduction = 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.

- Save your changes.
- Restart Splunk using the CLI.



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



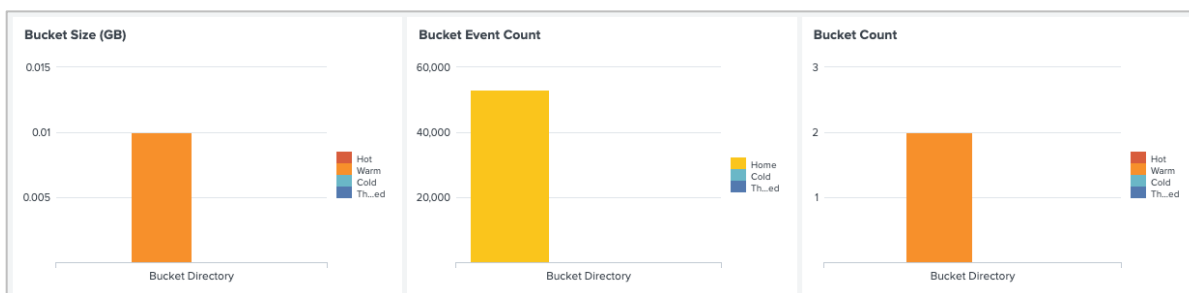
```
"C:\Program Files\Splunk\bin\splunk" restart
```

NOTE: If you get an error during restart, it is most likely a mistake in the stanza of the **indexes.conf** file. Check the changes you performed in step 6, and verify the configuration file is correct.

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

10. Log into Splunk Web as **admin**, after the Splunk restart.
11. From the MC, navigate to **Indexing > Indexes and Volumes > Index Detail: Instance**.
12. From the **Index** dropdown menu, select **securityops**.

You may observe that buckets that were previously Hot are now Warm after the Splunk restart:



Also observe that the **frozenTimePeriodInSecs** setting has changed to the newly configured value.

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

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
<pre>[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</pre>	<pre>[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</pre>

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.

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.

Notice the **Included** checkbox is checked for *** (All non-internal indexes)**.

Also notice the **Included** checkbox is not checked for **_* (All internal indexes)**.

Index Name	filter	Included ?	Default ?
* (All non-internal indexes)		<input checked="" type="checkbox"/>	<input type="checkbox"/>
_* (All internal indexes)		<input type="checkbox"/>	<input type="checkbox"/>

4. Verify the **Default** checkbox next to **main** is checked.

The **Included** checkbox is already checked due to the setting for *** (All non-internal indexes)**.

5. In the **Index Name** list, click the **Default** checkbox next to **websales**.

The **Included** checkbox is already checked due to the setting for *** (All non-internal indexes)**.

6. Click the filter dropdown menu on the right and select **Show native**.

Index Name	filter	Included ?	Default ?	Showing native ▾
* (All non-internal indexes)		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
main		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
websales		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

☒ Show selected
☐ Show unselected
☒ Show native
☐ Show inherited
☐ Show wildcards
☐ Show all

7. Click **Save**.
8. Click **power** role.
9. From the **5. Resources** tab, select **search** in the **Default app** drop-down menu.
10. Click the **3. Indexes** tab.

11. Scroll down and notice that the **websales** and **main** indexes are inherited.

Leaving the mouse cursor over the checkbox shows “This index is inherited”.

main	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
securityops	<input checked="" type="checkbox"/>	<input type="checkbox"/>
summary	<input checked="" type="checkbox"/>	This Index is inherited
websales	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

12. In the **Index Name** list, click the **Default** checkbox next to **securityops**.

The **Included** checkbox is already checked due to the setting for ***(All non-internal indexes)**.

13. Leave all other parameters at their default values and click **Save**.

14. Click the **admin** role.

15. Click the **3. Indexes** tab.

16. Click the **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 various indexes.

17. Click **Save**.

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

18. From the **Roles** page, click **New Role**.

19. In the **New Role** dialog box, type **soc_analyst** in the **Name** field.

20. In the **1. Inheritance** tab and select the checkbox next to the **power** role.

21. Click the **3. Indexes** tab and verify the **Included** and **Default** checkboxes next to **main**, **securityops**, and **websales**.

Permissions from these indexes are inherited from the **power** role and are greyed out.

22. From the **5. Resources** tab, select **search** in the **Default app** drop-down menu.

23. Leave all other parameters at their default values and click **Create**.

24. Navigate to **Settings > Users** (in the **Users and Authentication** section). Then click on **emaxwell**.

25. In the **Assign to roles** section, clear **power** and select **soc_analyst** and click **Save**.

26. Log out as **admin**.

27. Log back in as **emaxwell / open.sesam3**

If you get a message for a quick tour, click **Skip**.

You should land on the **App: Search and Reporting** based on your new role properties.

28. Run the following search over the **last 24 hours**:

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

Notice that the results include events from all indexes that are inherited as part of the role, such as **securityops** and **websales**.

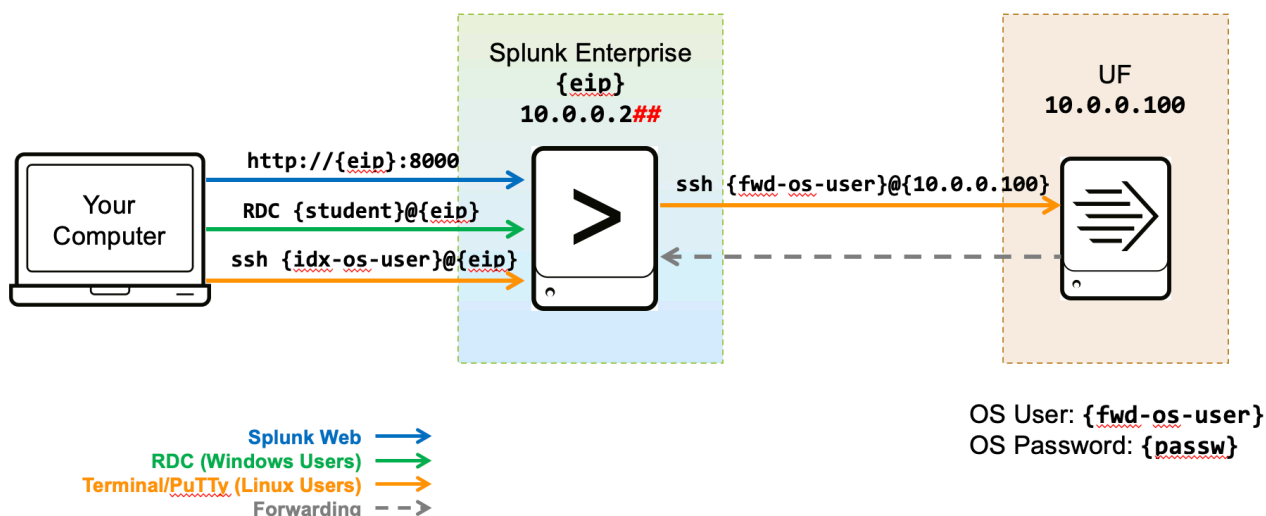
29. Log out and log back in as **admin**.

Module 8 Lab Exercise – Basic Forwarder Configuration

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.



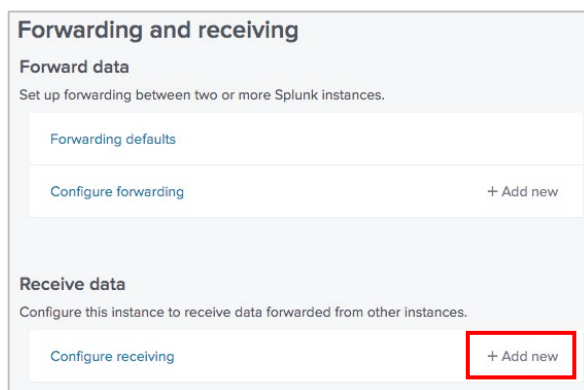
This lab exercise demonstrates a basic way to configure a forwarder.

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.

- From your indexer's command line identify your indexer's internal IP address.



```
ifconfig
```

```
eth0      Link encap:Ethernet  HWaddr XX:XX:XX:XX:XX:XX
          inet addr:10.0.0.2##  Bcast:10.0.0.255  Mask:255.255.255.0
...

```



```
ipconfig
```

```
Ethernet adapter Ethernet #:
Connection-specific DNS Suffix  . : xx-xxxx-x.compute.internal
Link-local IPv6 Address . . . . . : XXXX::XXXX:XXXX:XXXX:XXXX%X
IPv4 Address. . . . . : 10.0.0.2##
...

```

It should be **10.0.0.2##**, where **##** represents your **student-ID**. If this not the case, notify your instructor.

Task 2: Connect to your universal forwarder.

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



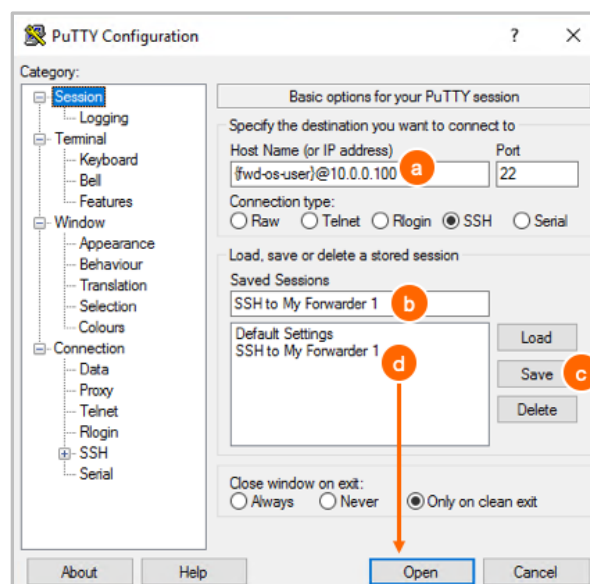
```
ssh {fwd-os-user}@10.0.0.100
```



From your RDC session, locate **PutTy** on the desktop. 

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

- Replace **{fwd-os-user}** with your designated value.
- Name your session, for example **"SSH to My Forwarder 1"**
- Save the session for later re-use.
- Click on the session **"SSH to My Forwarder 1"** and click **Open** to start the session



- When prompted for the authenticity of the host and the key fingerprint, type "yes" to continue, and use your assigned password **{password}** to log in.

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).

7. 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.

8. When you receive the message “Please enter an administrator username:”, enter **admin** and press **enter** to continue.
9. When you receive the message “Please enter a new password:”, enter and confirm your assigned password to continue.
10. After installation, using the **splunk show splunkd-port** 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 **splunk add forward-server** command creates an **outputs.conf** in the forwarder's **SPLUNK_HOME/etc/system/local** directory.

11. 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.
```

12. Verify forwarding is configured:

NOTE: The indexer may alternate between **Active** and **Configured but inactive forwards**. You may need to run the command multiple times to view these states.

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

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

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.

13. In Splunk Web, navigate to **Settings > Monitoring Console**.
14. On the MC menu, click **Settings > Forwarder Monitoring Setup**.
15. On the **Forwarding Monitoring Setup** page, click **Enable**, then **Save**.
The **Build Forwarder Assets Now** dialog displays.
16. Click **Continue > Done**.
17. Click **Rebuild forwarder assets... > Start Rebuild > Done**.
18. Switch to your terminal window and restart the universal forwarder (not the Splunk server.)



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

19. 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]
```

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

Forwarders: Instance

Instance: Time Range: [Hide Filters](#)

Instance	GUID	Forwarder Type	IP	Splunk Version	OS	Architecture	Receiver Count	Connection Count	Average KB/s	Average Events/s
ip-10-0-0-100	5E3CDBE5-3D3E-4A9D-99CD-81AB12F74E3A	Universal Forwarder	10.0.0.100	8.1.0	Linux	x86_64	1	2	0.98	1.30

Click on a forwarder to see a list of connected receivers.

Note: Multiple forwarders installed on one host appear with identical host names, but different GUIDs.

NOTE: 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** file, 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.

In this exercise, you also 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.

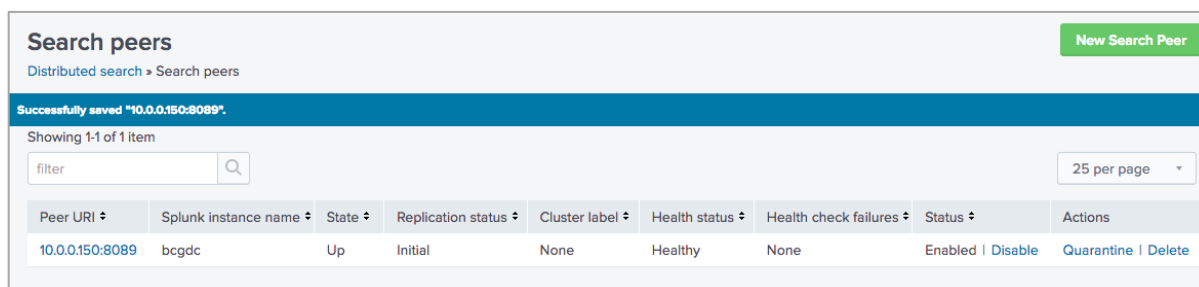
Steps for Distributed Search

Task 1: Add a search peer.

1. Click **Settings > Distributed search > Search peers > + Add New**.
2. Enter the following peer connection information.

Peer URI:	10.0.0.150:8089
Remote username:	ds_user
Remote password:	open.sesam3
Confirm password:	open.sesam3

3. Click **Save**.



Peer URI	Splunk instance name	State	Replication status	Cluster label	Health status	Health check failures	Status	Actions
10.0.0.150:8089	bcgdc	Up	Initial	None	Healthy	None	Enabled Disable	Quarantine Delete

Check Your Work for Distributed Search

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

4. Navigate to **Apps > Search & Reporting**, and 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

Appendix A Lab: Configure Splunk to use LDAP

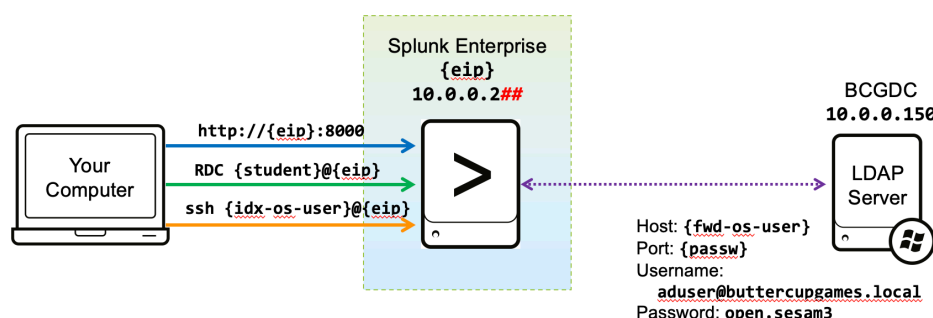
Description

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.

Steps

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 > Authentication method** (under **Users and Authentication**).
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
LDAP connection settings	
Host:	10.0.0.150
Port:	389
SSL enabled (checkbox):	(leave unchecked)
Bind DN:	adsuser@buttercupgames.local
Bind DN Password:	open.sesam3
Confirm password:	open.sesam3
User settings	
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 settings	
Group base DN:	OU=splunk,DC=buttercupgames,DC=local
Static group search filter:	(leave blank)
Group name attribute:	cn
Static member attribute:	member

- 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.

- 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

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

<u>LDAP Group Name</u>	<u>Splunk Roles</u>
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** (under **Users and Authentication**).

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 **nsharp** or **pbunch** (password: **open.sesam3**) and search **index=*** for **Last 24 hours**.

Which indexes appear in the results? **main, securityops, and websales** (Note that the search is for the last 24 hours, so results may depend on when you completed prior labs.)

The screenshot shows the Splunk Web interface. On the left, the 'INTERESTING FIELDS' list includes 'index' with a count of 38, which is highlighted with a red box. The main search results pane shows a table with the following data:

Index	Count	%
main	1,170,250	99.792%
websales	1,292	0.11%
securityops	1,144	0.098%

The 'index' field in the table is also highlighted with a red box. The 'Reports' section on the right shows 'Top values by time' and 'Rare values'.

10. Log out of Splunk Web.

Troubleshooting Suggestion

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

```
[AD_splunkers]
SSLEnabled = 0
anonymous_referrals = 1
bindDN = adsuser@buttercupgames.local
bindDNpassword = <some hashed password>
charset = utf8
emailAttribute = mail
enableRangeRetrieval = 0
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
```

Appendix B Lab: Configure a Volume-based Retention Policy

Description

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.

Steps

Task 1: Create an index for itops.

1. Log in as **admin** to Splunk Web.
2. 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.

3. Click **Save**.

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

4. In your text editor, update your **indexes.conf** file in the **search** app local directory:



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

Insert the following two volume stanzas before the **itops** stanza, and edit and add the additional stanzas below as instructed:

```
...
[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)
```



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

Insert the following two volume stanzas before the **itops** stanza, and edit and add the additional stanzas below as instructed:

```
...
[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
maxDataSize = auto
maxTotalDataSizeMB = 102400
thawedPath = $SPLUNK_DB\itops\thaweddb
homePath.maxDataSizeMB = 30000
coldPath.maxDataSizeMB = 60000
```

(NOTE: forward slashes required here)

(edit)

(edit)

(add)

(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.

5. Save your changes and close the text editor.
6. 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 3: Use the MC to view the retention settings.

- Navigate to **Settings > Monitoring Console**.
- To check the retention overview, navigate to **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	1 / 2184	0.00 / 488.28	0.00 / unlimited	0 / unlimited	27,060	4
._internal	event	1 / 30	0.04 / 488.28	0.04 / unlimited	0 / unlimited	559,423	4
._introspection	event	1 / 14	0.08 / 488.28	0.08 / unlimited	0 / unlimited	74,818	4
._telemetry	event	1 / 730	0.00 / 488.28	0.00 / unlimited	0 / unlimited	8	3
itops	event	0 / 2184	0.00 / 100.00	0.00 / 29.30	0 / 58.59	0	0
main	event	1631 / 2184	0.16 / 488.28	0.16 / unlimited	0 / unlimited	1,739,898	10
securityops	event	91 / 90	0.01 / 500.00	0.01 / unlimited	0 / unlimited	53,412	3
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
websales	event	91 / 2184	0.01 / 50.00	0.01 / unlimited	0 / unlimited	52,378	3

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/user2/one/
two	0.00 / 78.13	78.13	/opt/home/user2/two/

- To see the index detail of the **itops** index, navigate to **Indexing > Indexes and Volumes > Indexes Detail: Instance**., and in the **Index** drop-down, select **itops**.
- Scroll down to the **Settings** panel to confirm the retention policy changes you have made.

Settings				
Paths		Retention policies		Index Structure &
Setting ↕	Value ↕	Setting ↕	Value ↕	Setting ↕
homePath	volume:one/itops/db	maxTotalDataSizeMB	102400	maxDataSize
homePath_expanded	/opt/home/user2/one/itops/db	frozenTimePeriodInSecs	188697600	maxHotBuckets
coldPath	volume:two/itops/colddb	homePath.maxDataSizeMB	30000	maxWarmDBCount
coldPath_expanded	/opt/home/user2/two/itops/colddb	coldPath.maxDataSizeMB	60000	
thawedPath	\$SPLUNK_DB/itops/thaweddb			
thawedPath_expanded	/opt/splunk/var/lib/splunk/itops/			
summaryHomePath_expanded	/opt/home/user2/one/itops/summary			
tstatsHomePath	volume:_splunk_summaries/\$_index_			
tstatsHomePath_expanded	/opt/splunk/var/lib/splunk/itops/			

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
<pre>[securityops] coldPath = \$SPLUNK_DB/securityops/coldddb 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/coldddb enableDataIntegrityControl = 0 enableTsidxReduction = 0 homePath = volume:one/itops/db maxTotalDataSizeMB = 1024000 thawedPath = \$SPLUNK_DB/itops/thaweddb homePath.maxDataSizeMB = 30000 coldPath.maxDataSizeMB = 60000</pre>	<pre>[securityops] coldPath = \$SPLUNK_DB\securityops\coldddb 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\coldddb enableDataIntegrityControl = 0 enableTsidxReduction = 0 homePath = volume:one\itops\db maxTotalDataSizeMB = 1024000 thawedPath = \$SPLUNK_DB\itops\thaweddb homePath.maxDataSizeMB = 30000 coldPath.maxDataSizeMB = 60000</pre>