

## Splunk Enterprise 7.0 System Administration - Class Lab Exercises

### Lab typographical conventions

Replace following keys with the values indicated:

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

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

<b>ip-10-0-0-100</b>	The host name of your Splunk universal forwarder. It has the private address of <b>10.0.0.100</b> .
<b>bcgdc</b>	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 <b>10.0.0.150</b> .

The **SPLUNK\_HOME** token indicates the directory where Splunk is installed on the host:

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

The following text editors are installed in your environment:

Linux server:	<b>nano</b> <b>vi</b>
Windows server:	<b>Notepad++</b>

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



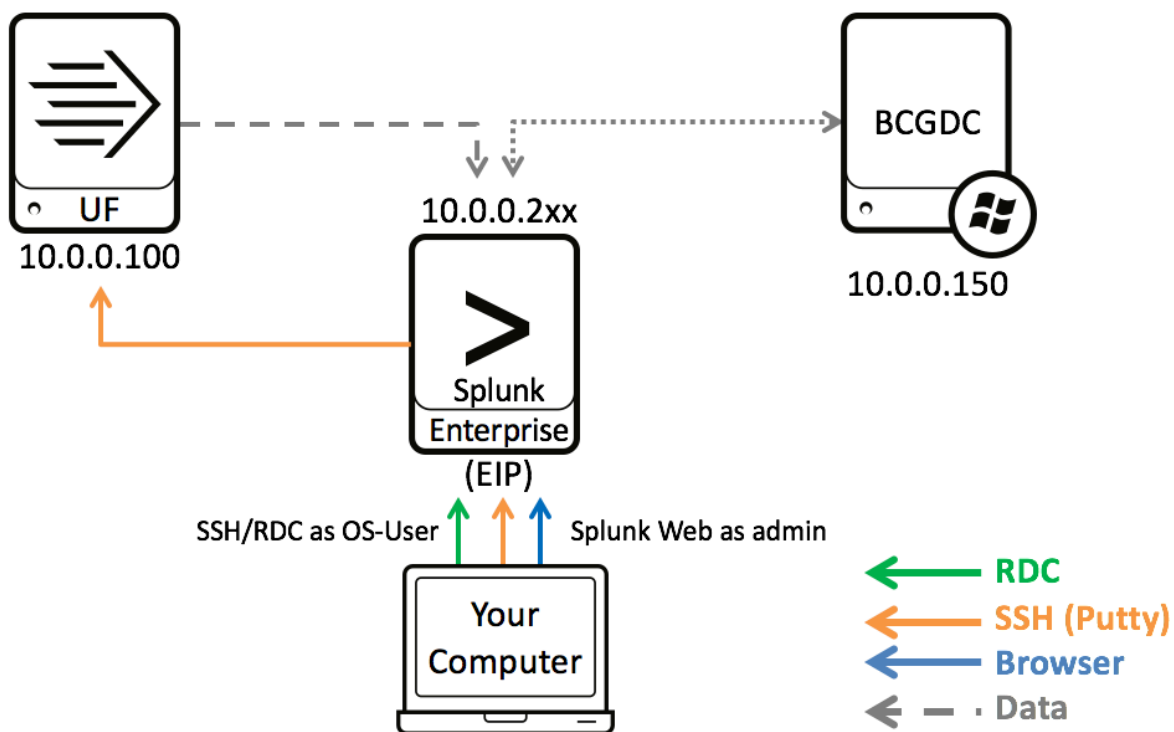
Windows OS

**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: 06  
**{student-ID}**

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

Splunk Web URL: **http://** 13.56.164.225 **:8000**  
**{host-eip}**

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

### Linux OS

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

Linux Host name: 10.0.0.206  
**{host-eip}**

Linux Username: sys06 Password: splunkIT  
**{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: Not Applicable  
**{host-eip}**

RDC Username: Not Applicable Password: **sp1unk3du**  
**{idx-os-user}**

## 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`

**NOTE:** The default password changeme has been changed. Please refer to the handouts, or ask the instructor for the assigned password.

2. Log in as **admin** using your assigned password `{password}`.
3. When prompted to change the password, click **Skip** to continue using the provided password.
4. Click **Skip** in the “**Help us improve Splunk Software**” pop-up page.
5. To identify the Splunk version and build number your server is running, click **Help > About**.
6. Click **Administrator > Account Settings** and change the **Full name** to *your name*.
7. In the **Email address** field, replace the current value with your two-digit `{student-ID}`.  
**Hint:** Leading zero required for student IDs 01-09.
8. Click **Save**.
9. 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:

- 
10. Rename the Splunk server name and default host name:

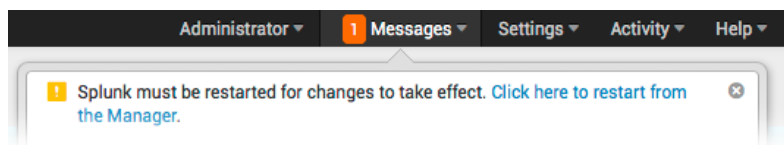
Splunk server name: `splunk{student-ID}` (Your assigned 2-digit ID)

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

11. Click **Save**.

These changes require a restart of Splunk.

12. Click **Messages > Click here to restart from the Manager > Restart Splunk > OK**.



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

## Check Your Work

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

15. On the Monitoring Console navigation bar, click **Settings > Monitoring Console**.
16. To enable the app, click **Settings > General Setup** on the MC menu.
17. Verify the server name and make a note of the discovered server roles.

**Setup**  
Current topology of your 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
>	splunkXX	splunkXX	ip-10-0-0-211	Indexer License Master Search Head	Only available in distributed mode.			✓ Enabled

18. To complete the app setup, click **Apply Changes > Go to Overview**.
19. 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.

20. 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.
21. Click **Start** to view the current results for the instance.

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

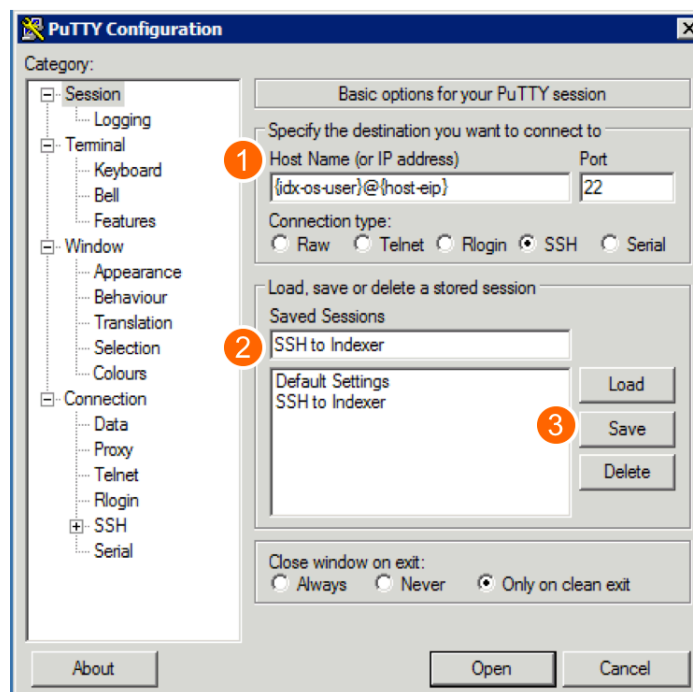
22. Connect to your dedicated Splunk indexer/search head.



Use Terminal or PuTTY to start an SSH session to your indexer.

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

- 1 Replace `{idx-os-user}@{host-eip}` with your designated values.
- 2 Name your session and 3 click Save (optional setting for PuTTY).
- c. Click **Open** to start an SSH session.



For Windows servers, connect using a Remote Desktop client (RDC).

- a. Start your **RDC** and enter `{host-eip}`.
- b. User name is `{idx-os-user}` and password is `splunk3du`.
- c. In the remote Windows desktop, click **Start > Command Prompt**.

## Task 5: Retrieve basic system information using CLI.

23. Change to your `SPLUNK_HOME/bin` directory:



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



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

24. 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 (PIDs: #####)
splunk helpers are running (PIDs: #####,#####,...)
```

25. 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	<b>./splunk version</b>	7.0.4
Splunk Web port:	<b>./splunk show web-port</b> returns <b>8000</b>	
Splunk management (splunkd) port:	<b>./splunk show splunkd-port</b> returns <b>8089</b>	
Splunk App Server ports:	<b>./splunk show appserver-ports</b> returns <b>8065</b>	
Splunk KV store port:	<b>./splunk show kvstore-port</b> returns <b>8191</b>	
Splunk server name:	<b>./splunk show servername</b> returns <b>splunk{student-ID}</b>	
Default host name:	<b>./splunk show default-hostname</b> returns <b>splunk{student-ID}</b>	

## 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://splunk.box.com/admin-big-lic> (password: **open.sesam3**)
  - Check with your instructor if your class is using an alternate source to obtain the license.
3. From the Licensing page, click **Add license > Choose File...**
4. Locate the file downloaded to your local system: **splunk.license.big.license**
5. Click **Install**.
6. Click **Restart now > OK**.
7. After the restart, review the information on 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. Click **A specific amount** and set the allocation to **150 MB**.
10. Click **Specific indexers**.
11. From the **Available indexers** field, select your host and move it to the **Associated indexers for this pool** 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. Click **Enable or Disable**.
15. Click the **Enable** action on the alert **DMC Alert - Total License Usage Near Daily Quota**.
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. Click **See All Apps** and search for apps that meet the following criteria:
  - Category: IT Operations
  - App only (no add-ons)
  - Compatible with 7.0 or later
  - Supported by Splunk

How many apps meet the above criteria?


As of this writing, 14.

3. For this exercise, download the sample app from <https://splunk.box.com/v/admin70-class-app>.  
Password: `open.sesam3`

---

#### 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.

4. In Splunk Web, navigate to **Settings > Indexes** and note the indexes that are currently configured for this instance.
5. In Splunk Web, navigate to **Apps > Manage Apps** page.  
Click the  icon if you are on the **Home** page (launcher).
6. Click **Install app from file > Browse** to locate the **admin70.spl** file you downloaded in step 3.
7. Click **Upload**.
8. In Splunk Web, navigate to **Settings > Indexes**. Notice that a new index called “**websales**” has been installed.
9. Navigate to the **Apps > System Admin 7.0 Class App**.  
**System Admin 7.0 Class App** is listed on the **Home** page as well as under the **Apps** dropdown.
10. Click **Apps > Manage Apps**.
11. For the **System Admin 7.0 Class App**, click **Permissions**.
12. Configure the permissions so only the **admin** role has Read and Write permissions.
13. Click **Save**.

## Check Your Work

### Task 3: Verify the app installation.

---

14. Log into Splunk Web as `emaxwell` / `open.sesam3`.
15. Confirm that the **System Admin 7.0 Class App** app is not accessible.
16. Log into Splunk Web as `admin` / `{password}`.
17. Click the **splunk>** logo.
18. You should see **Search & Reporting** and **System Admin 7.0 Class App** on 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 and 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.

tag	status	count
http_client_err	400	18
http_server_err	500	19
http_server_ok	200	1142

2. Log in as **emaxwell** / **open.sesam3**.
3. Navigate to **Search & Reporting** app and 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)

tag	status	count
http_client_err	400	972
http_client_err	404	905
http_server_ok	200	45849

## Investigate the Problem

### 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.

- 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 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.

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 **emaxwell1**. 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.

- 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.

- 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, you as the administrator 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.

- 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 /m "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 two new indexes and send data to a new index. 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**
  - Max Size of Hot/Warm/Cold Bucket: **auto\_high\_volume**
  - App: **Search & Reporting**  
This saves the configurations within the Search app-context.
  - Leave the rest of the fields empty to accept the defaults.
6. Click **Save**.

---

#### Task 3: Create another index for itops.

---

7. Create an index for the IT operations team using the following values:
  - Index Name: **itops**
  - Max Size of Entire Index: **100 GB**
  - App: **Search & Reporting**
  - Leave the rest of the fields empty and accept the defaults.
8. Click **Save**.

9. View the resulting configurations.



The resulting configurations are stored in `SPLUNK_HOME/etc/apps/search/local/indexes.conf`. Use the `cat` command to list 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

[itops]
coldPath = $SPLUNK_DB/itops/colddb
enableDataIntegrityControl = 0
enableTsidxReduction = 0
homePath = $SPLUNK_DB/itops/db
maxTotalDataSizeMB = 102400
thawedPath = $SPLUNK_DB/itops/thaweddb
```



The resulting configurations are stored in `SPLUNK_HOME/etc/apps/search/local/indexes.conf`. Use Notepad 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

[itops]
coldPath = $SPLUNK_DB\itops\colddb
enableDataIntegrityControl = 0
enableTsidxReduction = 0
homePath = $SPLUNK_DB\itops\db
maxTotalDataSizeMB = 102400
thawedPath = $SPLUNK_DB\itops\thaweddb.
```

## Check Your Work

### Task 4: 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.

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



15. Click **Next** to display the **Set Source Type** step.
16. Click **Next** to display the **Save Source Type** dialog and populate as follows:
 

Name:	<b>secure</b>
Category:	<b>Custom</b>
App:	<b>Search &amp; Reporting</b>
17. Click **Save**.
18. On the **Input Settings** step, select the **securityops** index:
 

App Context	<b>Search &amp; Reporting</b>
Host	<b>Constant value</b> (defaults to your host name <b>splunk##</b> )
Index	<b>securityops</b>



19. Click **Review**.

The summary of the input should look like this:

Input Type	<b>File Monitor</b>
Source Path	<b>/opt/log/www1/secure.log</b> (Linux server) <b>C:\opt\log\www1\secure.log</b> (Windows server)
Continuously Monitor	<b>Yes</b>
Sourcetype	<b>secure</b>
App Context	<b>search</b>
Host	<b>splunk##</b>
Index	<b>securityops</b>

20. Click **Submit**.

21. 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 – Configure Retention Policies

### Description

In this exercise, you will manually edit the `indexes.conf` file to configure more strict retention policies for the two indexes you created in the previous exercise.

### Configuration Steps

#### Task 1: Configure a strict time-based retention policy for securityops.

In the previous exercise, you created your indexes in the `search` app. The `indexes.conf` file should be located in `SPLUNK_HOME/etc/apps/search/local`.

1. To set a time-based retention policy for the `securityops` index, open the `indexes.conf` file with a text editor and append the following attributes to the `securityops` stanza:



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

```
[securityops]
coldPath = $SPLUNK_DB/securityops/coldddb
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\coldddb
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.

2. Save your changes, but do not close your text editor.

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

In this task, you enforce a specific volume-based retention policy for the **itops** index.

3. In your text editor, update your **indexes.conf** file as follows:



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 = 1024000
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 = 1024000
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 to 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.

**NOTE:** If you see any errors upon the restart, it is likely there is a mistake in the `indexes.conf` file and it must be corrected before proceeding to the next task. Ask your instructor for help.

## Check Your Work

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

1. To start indexing events into the `itops` index, click **Settings > Add Data**.
2. Click **monitor** to start the local input wizard.
3. On the **Select Source** step, click **Files & Directories**.
4. Click **Browse** and navigate to select the following input source:



```
/opt/log/mailsv1/maillog
```



```
C:\opt\log\mailsv1\maillog
```

5. Click **Next** twice to advance to the **Input Settings** step.
6. Configure the **Input Settings** page as follows:

App Context	<b>Search &amp; Reporting</b>
Host	<b>Constant value</b> (defaults to your host name <code>splunk##</code> )
Index	<b>itops</b>

## 7. Click **Review**.

The summary of the input should look like this:

Input Type	<b>File Monitor</b>
Source Path	<b>/opt/log/mailsv1/maillog (Linux)</b> <b>C:\opt\log\mailsv1\maillog (Windows)</b>
Continuously Monitor	<b>Yes</b>
Sourcetype	<b>sendmail_syslog</b>
App Context	<b>search</b>
Host	<b>splunk##</b>
Index	<b>itops</b>

## 8. Click **Submit**.

### Task 4: Use the MC to check the indexing activities and the retention settings.

## 9. Navigate to **Settings > Monitoring Console**.

## 10. To check the indexing activity of the previous tasks, click **Indexing > 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 **sendmail\_syslog**, **secure**, and **access\_combined\_wcookie**

## 11. To check the retention overview, navigate to **Indexing > Indexes and Volumes > Indexes and Volumes: Instance**.

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	0 / 2184	0.00 / 488.28	0.00 / unlimited	0 / unlimited	11,235	4
._internal	event	0 / 30	0.00 / 488.28	0.00 / unlimited	0 / unlimited	35,519	4
._introspection	event	0 / 14	0.01 / 488.28	0.01 / unlimited	0 / unlimited	8,770	4
._telemetry	event	0 / 730	0.00 / 488.28	0.00 / unlimited	0 / unlimited	0	0
itops	event	30 / 2184	0.00 / 100.00	0.00 / 29.30	0 / 58.59	1,953	0
main	event	0 / 2184	0.00 / 488.28	0.00 / unlimited	0 / unlimited	0	0
securityt	event	30 / 90	0.00 / 500.00	0.00 / unlimited	0 / unlimited	3,843	1
splunklog	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	90 / 2184	0.01 / 50.00	0.01 / unlimited	0 / unlimited	52,501	2

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.

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/

## 12. 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.
- Due to `$SPLUNK_HOME/etc/system/local/props.conf` (and `transforms.conf`) you will see the regex that extracts the host value from the path and the hostname is **mailsv1** and not **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  [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 = 102400 thawedPath = \$SPLUNK_DB/itops/thaweddb homePath.maxDataSizeMB = 30000 coldPath.maxDataSizeMB = 60000</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  [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</pre>

## Module 7 Lab Exercise – Modify and Create 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 > Access controls > Roles**.
2. Click **user**.
3. Scroll down to the **Indexes searched by default** section at the bottom of the page.
4. From the **Available indexes** list, click **websales** to add it to the **Selected indexes** list.
5. In the **Indexes** section, click **clear all** next to the **Selected search indexes** list to remove the **All non-internal indexes** selection.
6. From the **Available search indexes** list, click **main** and **websales** to add them to the **Selected search indexes** list. Leave all other parameters at their default values.
7. Click **Save**.
8. Modify the existing **power** role as follows:
  - Default app: **search**
  - Indexes searched by default: **itops** and **main**
  - Searchable Indexes: **itops**, **main**, and **websales** (clear **All non-internal indexes**)
  - Leave all other parameters at their default values.
9. Click **Save**.
10. Modify the existing **admin** role as follows:
  - Indexes searched by default: **All non-internal indexes** (clear **main**)

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

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

---

12. Create and configure a new role called **soc\_analyst** based on the **power** role with the following parameters:

- Role name: **soc\_analyst**
- Default app: **search**
- Role inheritance: **power**
- Indexes searched by default: **websales** (clear **main**)
- Leave all other parameters at their default values.

13. Click **Save**.

14. Navigate to **Access controls > Users > emaxwell**.

15. In the **Assign to roles** section, clear **power** and select **soc\_analyst**.

16. Click **Save**.

17. Log out as admin.

18. Log back in as emaxwell / open.sesam3.

19. 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 **itops** index also appear in your search results?

In **Task 1**, you configured the **power** role to search the **itops** index by default (along with **main** and **websales**). In this task, you configured the **soc\_analyst** role to inherit the **power** role's attributes.

20. Log out and log back in as admin.



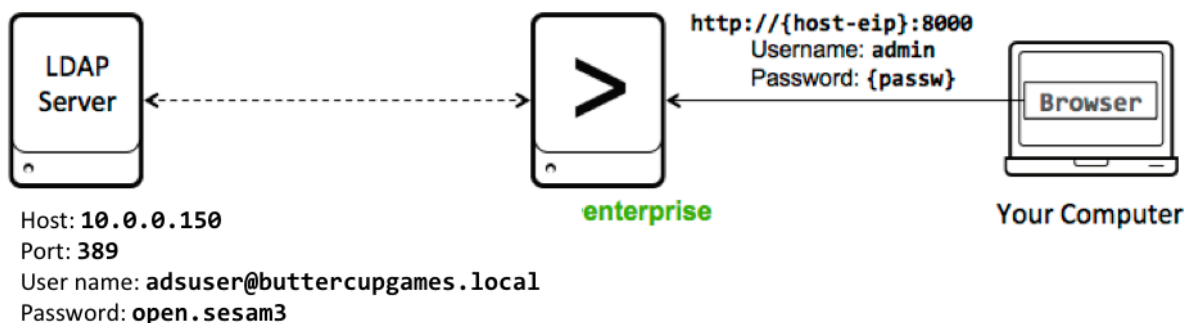
## Module 8 Lab Exercise – Configure Splunk to use LDAP

### 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 > Access controls > Authentication method**.
2. Select the **LDAP** radio button and click **Configure Splunk to use LDAP**.
3. Click **New**.
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 name attribute: **samaccountname**
  - Real name attribute: **displayname**
  - Group mapping attribute: **dn**
  - Group base DN: **OU=splunk,DC=buttercupgames,DC=local**
  - Group name attribute: **cn**
  - Static member attribute: **member**
5. 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**.
7. For each LDAP Group Name, assign the following Splunk roles:

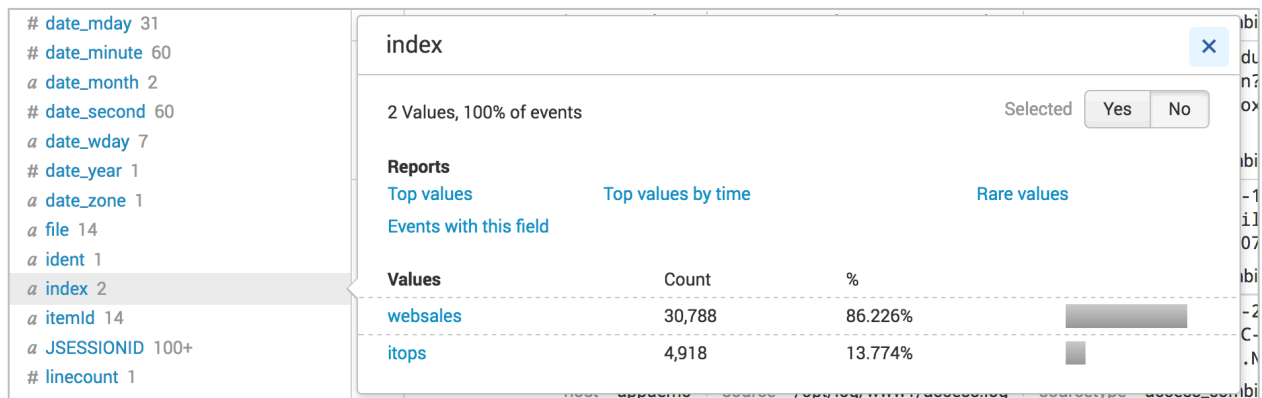
<u>LDAP Group Name</u>	<u>Splunk Roles</u>
splunkAdmins	<b>admin</b>
splunkBizDev	<b>user</b>
splunkITops	<b>power</b>
splunkSOC	<b>soc_analyst</b>

## Check Your Work

## Task 3: Verify the LDAP configuration.

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

8. Navigate to **Settings > Access controls > Users**.  
 How many users are imported from Active Directory? **10**  
 Which LDAP users are mapped to the **user** role? **Bao Lu & Dwight Hale**
9. Log in as **nsharpe** or **pbunch** (password: **open.sesam3**) and search **index=\*** for **Last 30 days**.  
 Which indexes appear in the results? **websales and itops**



## 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

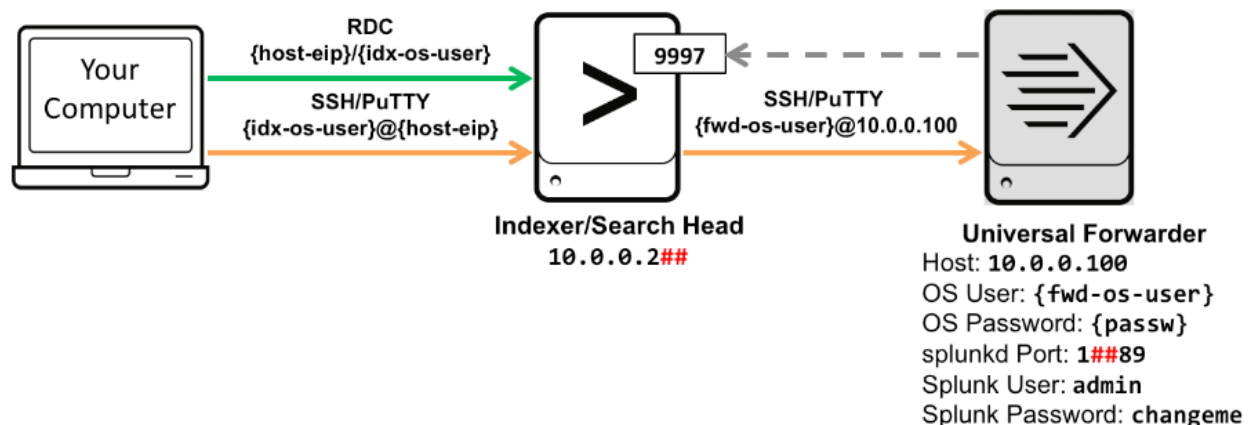
[roleMap_AD_splunkers]
admin = splunkAdmins
power = splunkITOps
soc_analyst = splunkSOC
user = splunkBizDev
```

## Module 9 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.



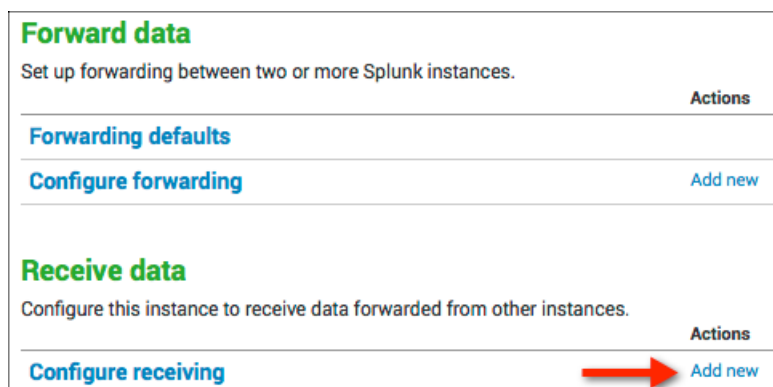
This lab exercise demonstrates a basic way to configure a forwarder.

### 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** and configure a receiving port to listen on port **9997**.



- 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.

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

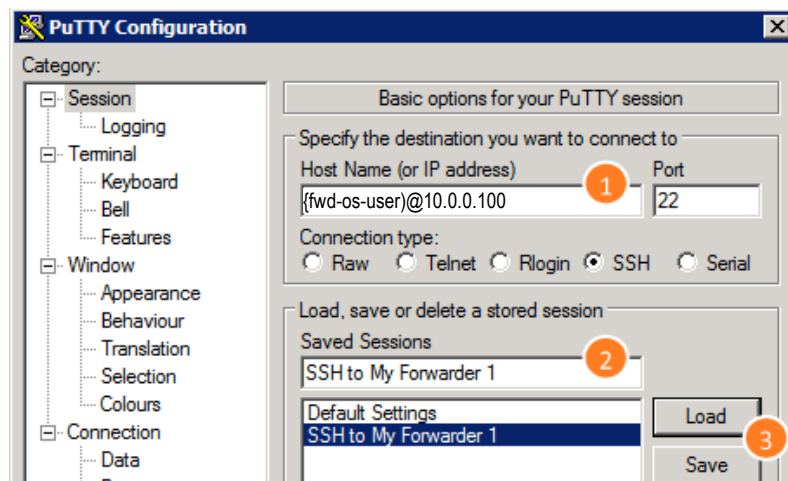


```
ssh {fwd-os-user}@10.0.0.100
```



From your RDC session, launch **PuTTY** and configure a **ssh** session:

- Replace **{fwd-os-user}@10.0.0.100** with your designated values.
- Name your session and **Save**.
- 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 configure its management port (**splunkd**) to use your assigned **splunkd** port number.

- Use the **start** command with the **accept-license** argument:

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

- When you see the message, **"ERROR: The mgmt port [8089] is already bound,"** and you are asked to change the port, answer **"y"** to change the port number.

**IMPORTANT:** You must use your assigned forwarder port number because you are sharing the system with other users in this lab environment. This defines the management port number (splunkd) for your forwarder instance.

7. Enter your designated forwarder management port number (for example, 1##89 where ## is your **student-ID**).
8. Use the show command to confirm your **splunkd-port** number:

```
./splunk show splunkd-port
Splunk username: admin
Password: changeme
Splunkd port: 1##89      (## is your student-ID)
```

If the port number is incorrect, then use the set command to change it:

```
./splunk set splunkd-port 1##89      (## is your student-ID)
```

#### 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.

9. 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.
```

10. 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.

11. In Splunk Web, navigate to **Settings > Monitoring Console**.
12. On the MC menu, click **Settings > Forwarder Monitoring Setup**.
13. On the Forwarding Monitoring Setup page, click **Enable**, then **Save**.  
The Build Forwarder Assets Now dialog displays.
14. Click **Continue > Done**.

15. Click **Rebuild forwarder assets... > Start Rebuild > Done**.
16. Switch to your terminal window, and restart the forwarder.



```
./splunk restart
```



```
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.

17. 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]
```

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

Forwarders: Instance

Instance: 

ip-10-0-0-100

Time Range: 

Last 4 hours

[Hide Filters](#)

Status and Configuration

Instance ^	GUID ^	Forwarder Type ^	IP ^	Splunk Version ^	OS ^	Architecture ^	Receiver Count ^	Connection Count ^	Average KB/s ^	Average Events/s ^
ip-10-0-0-100	551AF2FE-A705-47C2-8E3F-D41D469F385D	Universal Forwarder	10.0.0.100	7.0.0	Linux	x86_64	1	1	1.07	1.39

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 the step 10.
6. Is 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 10 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 1: Add a search peer.

1. Click **Settings > Distributed search > Search peers > New**.
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**.

Search peers

Distributed search » Search peers

New

Showing 1-1 of 1 item

Results per page25

Peer URI	Splunk instance name	State	Replication status	Cluster label	Health status	Health check failures	Status	Actions
<a href="#">10.0.0.150:8089</a>	bcgdc	Up	Successful	None	Healthy	None	Enabled   <a href="#">Disable</a>	<a href="#">Quarantine</a>   <a href="#">Delete</a>

### Check Your Work

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

4. Run the following search over the last 15 minutes:  
`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**