

## Project Description

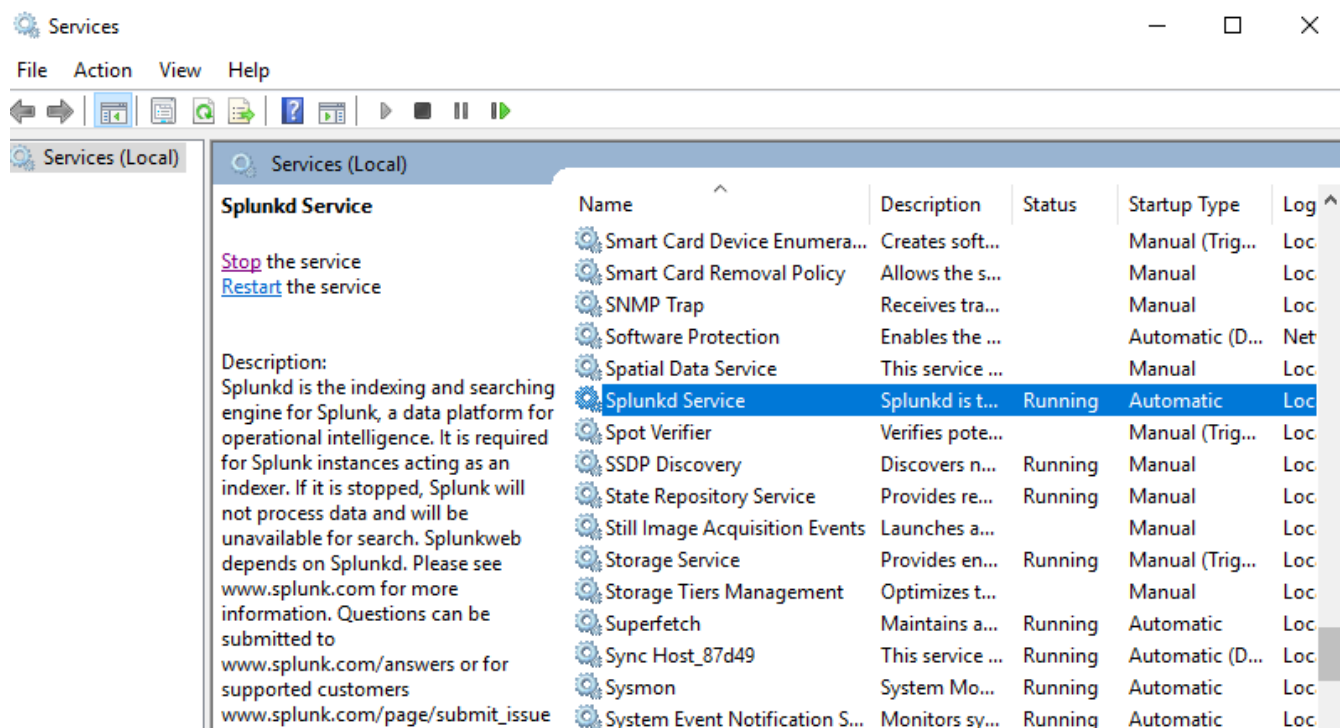
In this lab, I take on the role of a security professional performing threat monitoring with the SIEM (Security Information Event Monitoring) tool Splunk enterprise.

## Contents

Project Description  
Installing Splunk  
Loading Logs  
Forwarding Logs  
Extracting Fields  
Performing a Search  
Excluding Search Terms  
Creating an Alert  
Bug Fixes  
Summary  
References

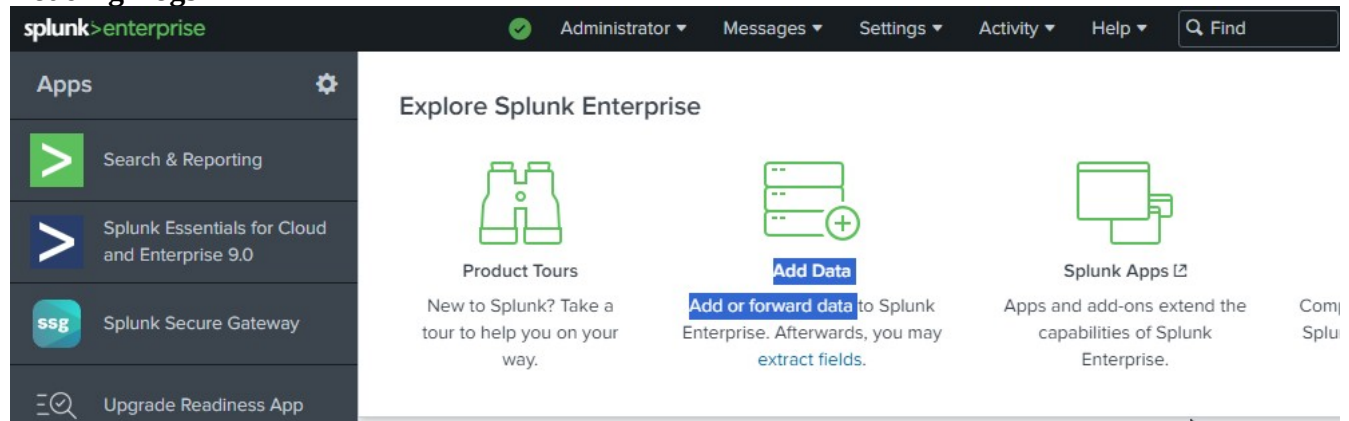
## Installing Splunk

In this lab Splunk enterprise [1] has been installed on a Windows 10 virtual machine.



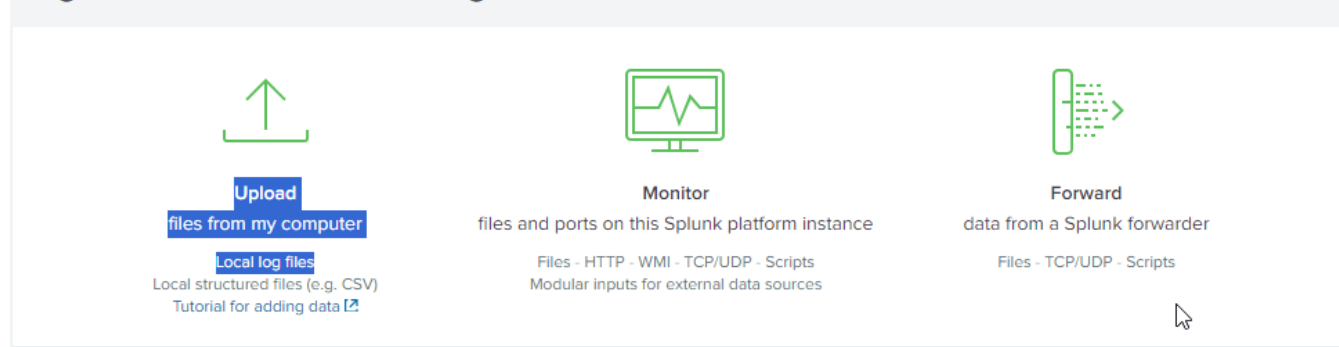
The Splunkd service is automatically started by the installer, it is the index and search engine for Splunk.

## Loading Logs



I select “Add data” from the main Splunk menu.

## Or get data in with the following methods



I select “Upload” to upload data to Splunk.

## Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. [Learn More](#)

Preview is not supported for this archive file, but it can still be indexed.

Selected File: **serverlogs.zip**

Select File

I select the zipped log files [2] to upload them to Splunk and follow through the wizard by selecting “Next”.

I import a second log file and name this log file with the index “splunk\_logs2” to distinguish its entries from the first log file’s.

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

- ☒ Constant value  
☐ Regular expression on path  
☐ Segment in path

Host field value DESKTOP-UAB80KH

## Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Index Default Create a new index

## New Index

### General Settings

Index Name splunk\_logs2

Set index name (e.g., INDEX\_NAME). Search using index=INDEX\_NAME.

Index Data Type Events Metrics

The type of data to store (event-based or metrics).

Home Path optional

Hot/warm db path. Leave blank for default (\$SPLUNK\_DB/INDEX\_NAME/db).

Cold Path optional

Cold db path. Leave blank for default (\$SPLUNK\_DB/INDEX\_NAME/colddb).

Thawed Path optional

Thawed/resurrected db path. Leave blank for default (\$SPLUNK\_DB/INDEX\_NAME/thaweddb).

Save

Cancel

## New Search

Save As Create Table View Close

index="splunk\_logs2" result.c\_ip="\*"

All time



22,614 events (before 06/12/2023 20:29:20.000) No Event Sampling

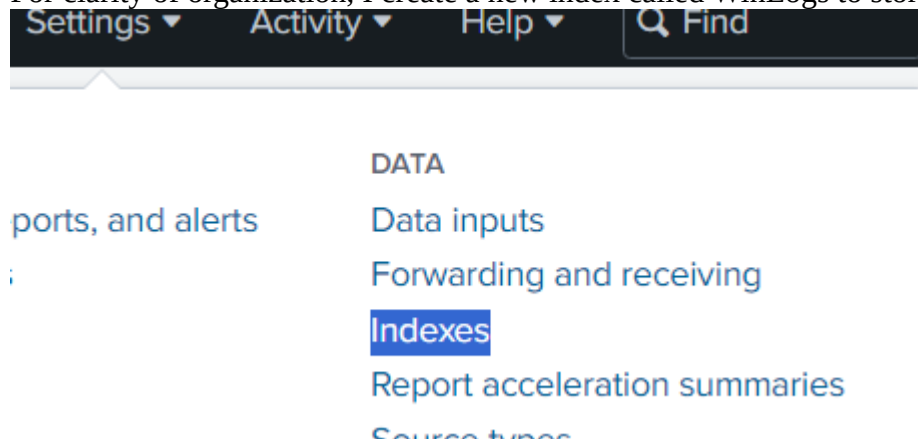
Job Smart Mode

I enter the search term index to identify logs belonging to the second log file.

## Forwarding Logs

### Creating a New Index Label for clarity

For clarity of organization, I create a new index called WinLogs to store locally forwarded logs.



I select Settings → Indexes to access the index page.



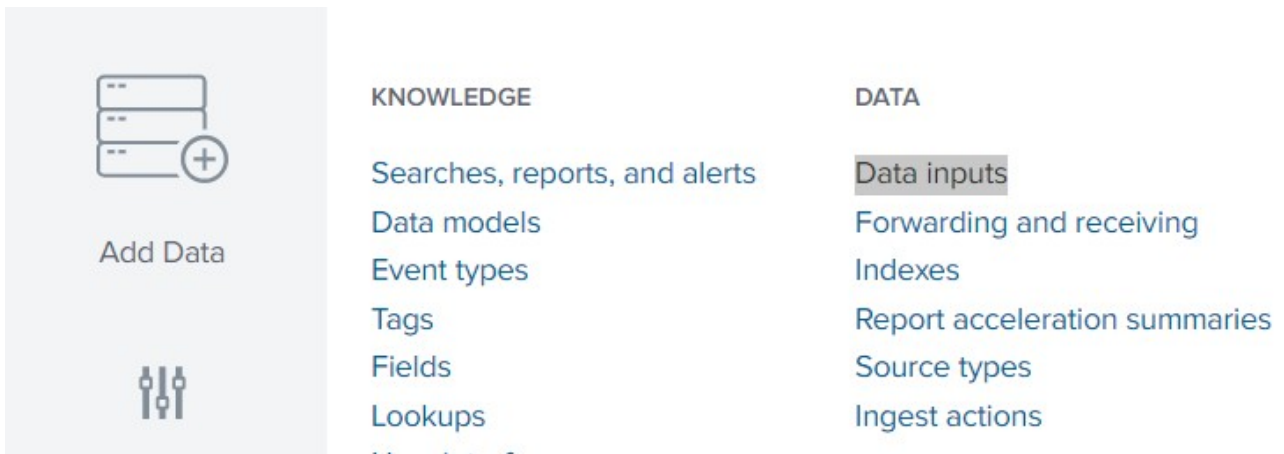
I select the “New Index” button.

A screenshot of the 'New Index' configuration window in Splunk. The window has a title bar with 'New Index' and a close button. Below the title bar is a 'General Settings' section. It contains four fields: 'Index Name' with the value 'WinLogs' and a description 'Set index name (e.g., INDEX\_NAME). Search using index=INDEX\_NAME.'; 'Index Data Type' with a toggle between 'Events' (selected) and 'Metrics'; 'Home Path' with the value 'optional' and a description 'Hot/warm db path. Leave blank for default (\$SPLUNK\_DB/INDEX\_NAME/db).'; and 'Cold Path' with the value 'optional'. At the bottom right of the form are 'Save' and 'Cancel' buttons.

I enter the name of the new index “WinLogs” and click “Save”.

### Forwarding a local data input

I then proceed to add a locally forwarded data input.



I select Settings → Data inputs.

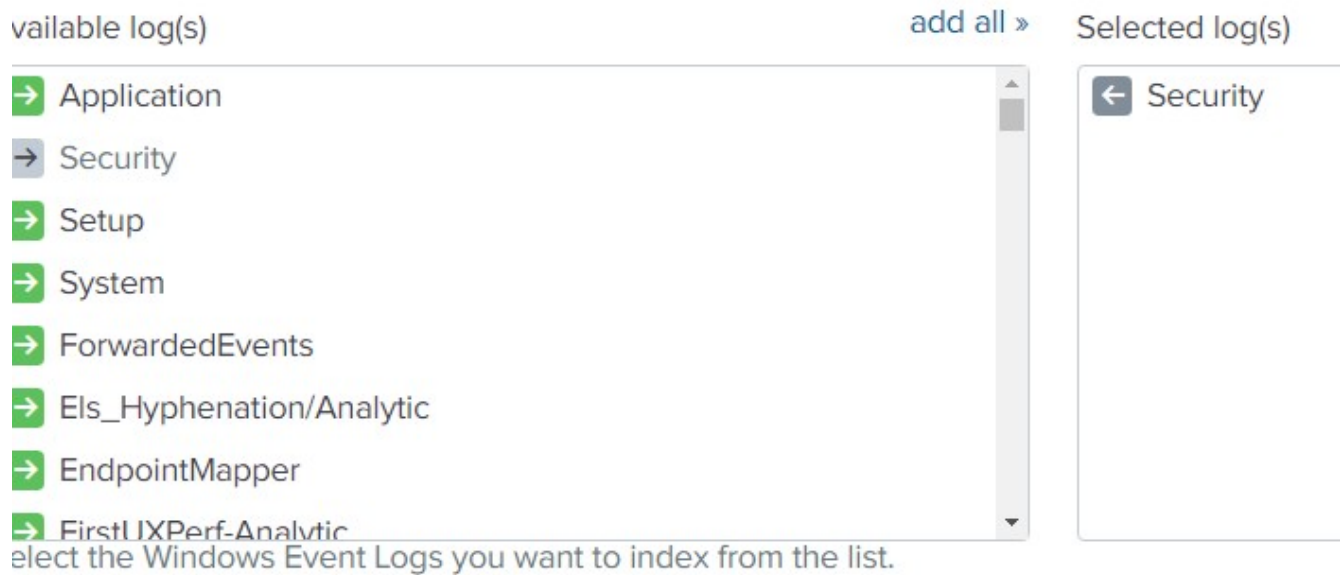
## Data inputs

Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving instances, go to [Forwarding and receiving](#).

### Local inputs

Type	Inputs
<a href="#">Local event log collection</a> Collect event logs from this machine.	-

I choose “Local event log collection” as the input source.



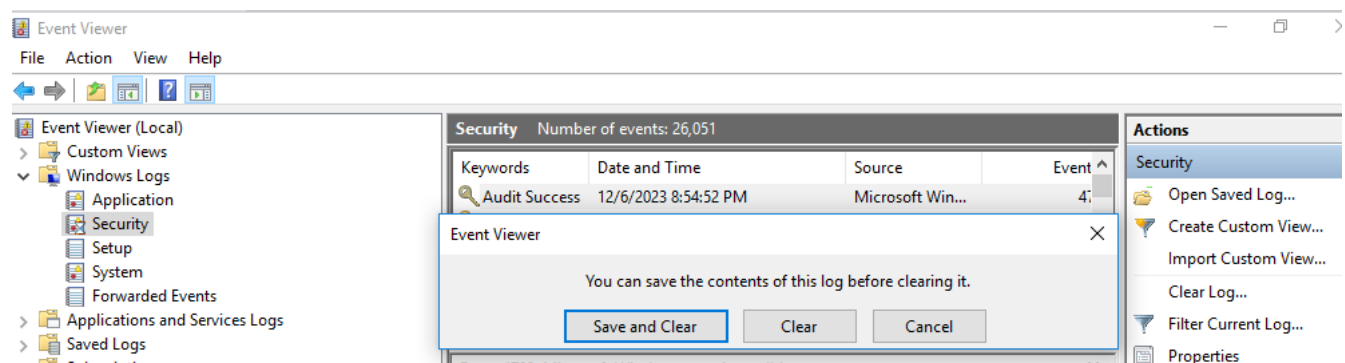
## index

set the destination index for this source.



I choose “Security” to select the security event log, and choose to forward it to the “winlogs” index.

## Searching for locally forwarded security logs



I clear the event log and search for event 1102 in Splunk.

# New Search

Save As ▾Create Ta

index="winlogs" 1102

✓ 1 event (before 06/12/2023 21:01:43.000)No Event Sampling ▾Job ▾||▣↻🖨️⬇️💡 Smart Mod

Events (1)PatternsStatisticsVisualization

Format Timeline ▾- Zoom Out+ Zoom to Selectionx Deselect

List ▾✍️ Format20 Per Page ▾

< Hide Fields

☰ All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

a Account\_Name 1

a ComputerName 1

i	Time	Event
>	06/12/2023 20:57:41.000	12/06/2023 08:57:41 PM LogName=Security EventCode=1102 EventType=4 ComputerName=DESKTOP-UAB80KH.mydomain.local <a href="#">Show all 17 lines</a> host = DESKTOP-UAB80KH   source = <a href="#">WinEventLog:Security</a> sourcetype = WinEventLog:Security

## Logging local Sysmon events

spunk>enterprise

Messages ▾Settings ▾Activity ▾Help ▾

# localhost

Data inputs » Event log collections » localhost

Available log(s)

add all >

Selected log(s)

→ Microsoft-Windows-Superfetch/Main

→ Microsoft-Windows-Superfetch/PfApLog

→ Microsoft-Windows-Superfetch/StoreLog

→ Microsoft-Windows-Sysmon/Operational

→ Microsoft-Windows-Sysprep/Analytic

→ Microsoft-Windows-System-Profile-HardwareId/Diagnostic

→ Microsoft-Windows-SystemSettingsHandlers/Debug

← Microsoft-Windows-Sysmon/Operational

← Security

Select the Windows Event Logs you want to index from the list.

I select “Microsoft-Windows-Sysmon/Operational” under Local event log collection.

```
C:\Windows\system32>net user newuser /delete
The command completed successfully.

C:\Windows\system32>net user newuser 1234567aA /add
The command completed successfully.
```

<https://cyberiumarena.com/lab/>

nx220/splunkforwarder.zip

I create a new user called “newuser” from the command line.

**New Search** Save As ▼ Create T

index="winlogs" newuser

✓ 28 events (before 06/12/2023 21:22:32.000) No Event Sampling ▼ Job ▼ || ■ ➔ 🖨️ ⬇️ ⚠️ Smart Mo

Events (28) Patterns Statistics Visualization

Format Timeline ▼ — Zoom Out + Zoom to Selection × Deselect

List ▼ ✎ Format 20 Per Page ▼ < Prev

< Hide Fields	≡ All Fields	i	Time	Event
+ Extract New Fields		>	06/12/2023 21:20:50.000	... 24 lines omitted ... OriginalFileName: net1.exe CommandLine: C:\Windows\system32\net1 user newuser CurrentDirectory: C:\Windows\system32\ ... 9 lines omitted ... ParentCommandLine: net user newuser 1234567aA /add ParentUser: DESKTOP-UAB80KH\Caleb <a href="#">Show all 38 lines</a>

I search the “winlogs” index for the term “newuser” and find the command executed. Note that the index “winlogs” must be specified in order for this result to appear.

### Forwarding events from another Windows virtual machine

I download [5] and install Splunk forwarder on another Windows virtual machine.



UniversalForwarder Setup

# splunk>universal forwarder

If you intend to use a Splunk deployment server to configure this UniversalForwarder, please specify the host or IP, and port (default port is 8089). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

## Deployment Server

Hostname or IP

:

*Enter the hostname or IP of your deployment server, e.g. ds.splunk.com* *default is 8089*

I setup Splunk forwarder to forward logs to the machine on which Splunk is installed.

UniversalForwarder Setup

# splunk>universal forwarder

If you intend to use a Splunk receiving indexer to configure this UniversalForwarder, please specify the host or IP, and port (default port is 9997). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

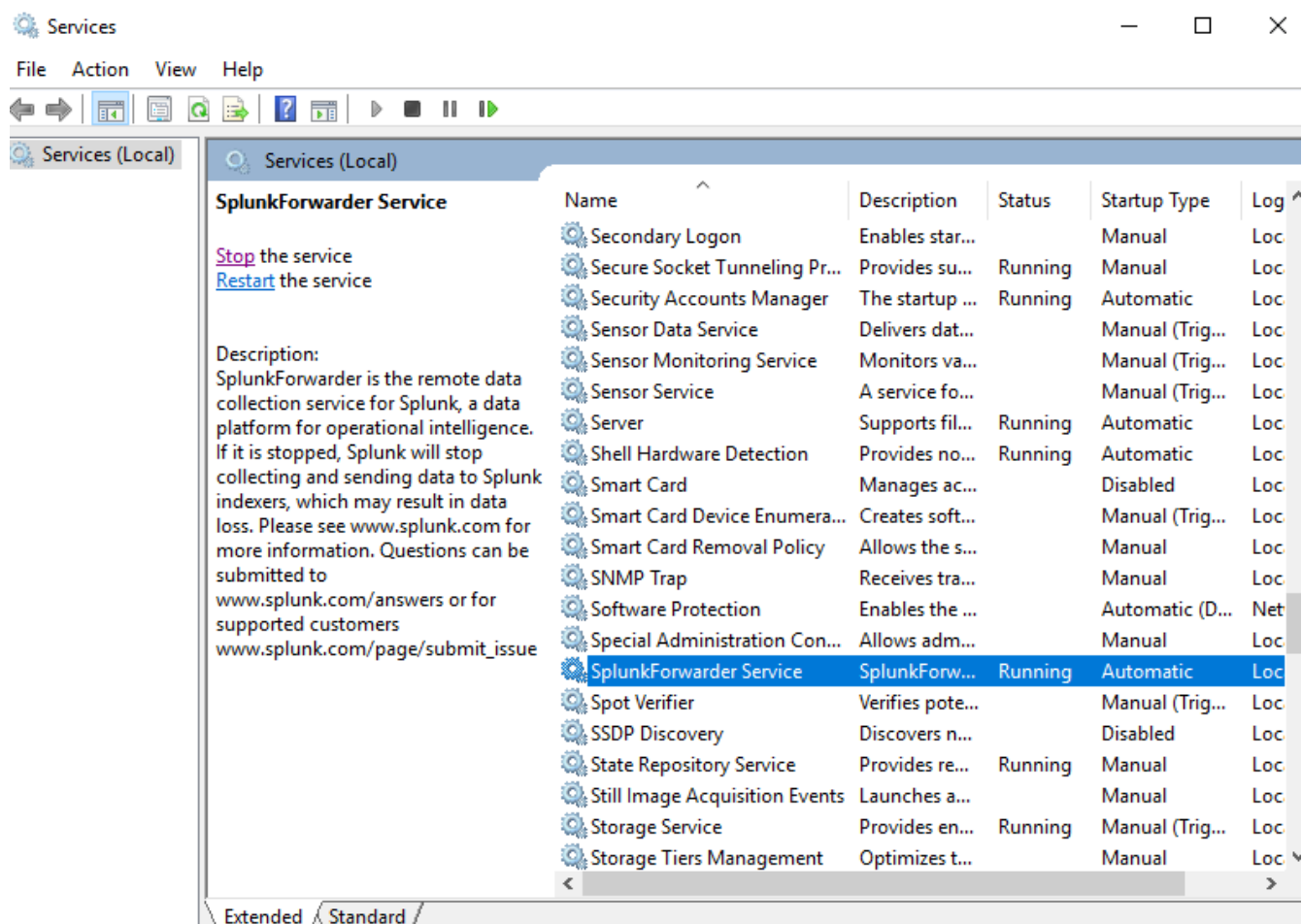
## Receiving Indexer

Hostname or IP

:

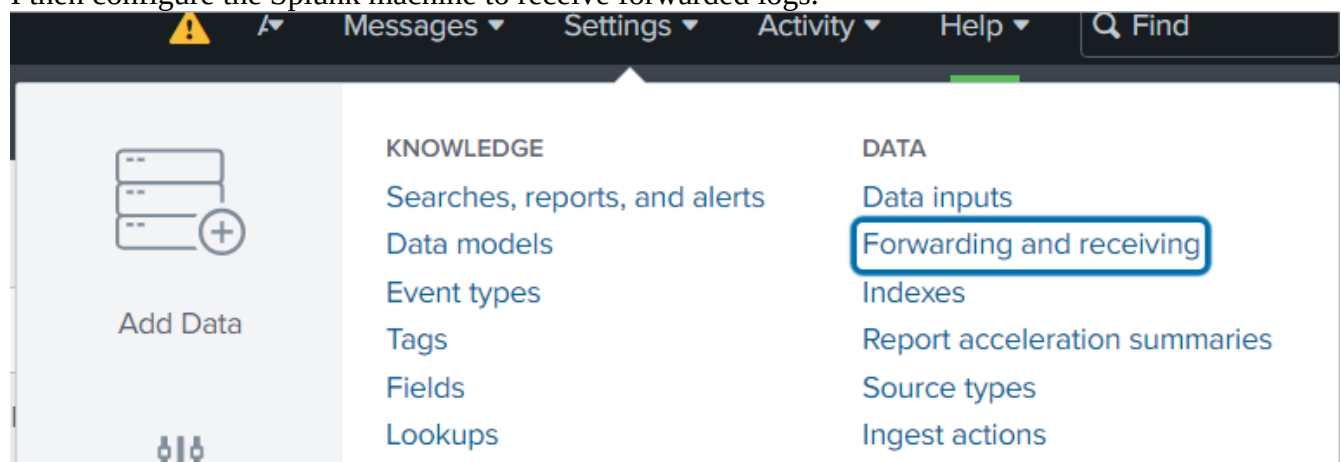
*Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com* *default is 9997*

I specify the receiving indexer to be the machine on which Splunk is installed.

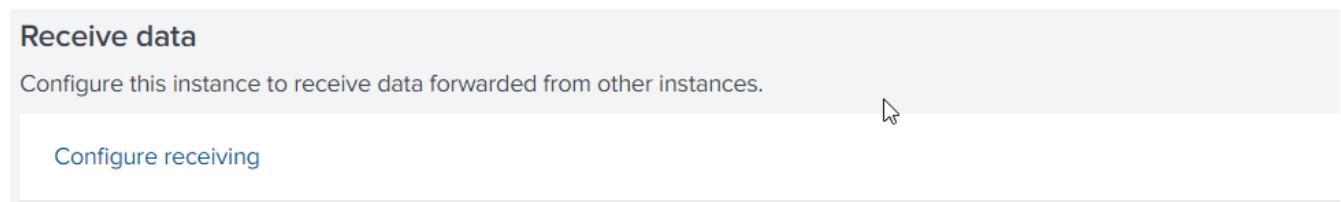


A new service SplunkForwarder Service is created.

I then configure the Splunk machine to receive forwarded logs.



I select "Settings" → "Forwarding and receiving".



I select “Configure receiving”.

### Configure receiving

Set up this Splunk instance to receive data from forwarder(s).

Listen on this port \*

9997

For example, 9997 will receive data on TCP port 9997.

I select “New receiving port” and enter “9997”.

## Extracting Fields

The screenshot shows the Splunk Enterprise interface. At the top, the navigation bar includes 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', and 'Help'. Below this, the 'Search & Reporting' section is active. The main area is titled 'New Search' and shows a search query 'root' with 'All time' selected. Below the search bar, it indicates '2,631 events (before 06/12/2023 19:28:02.000)' and 'No Event Sampling'. The 'Events (2,631)' tab is selected, showing a timeline view. A context menu is open over the first event, with 'Extract Fields' highlighted. The 'Event Actions' dropdown is also visible, showing a table of fields to be extracted.

Type	Field	Value	Actions
Selected	host	DESKTOP	
	source	serverlogs.zip:\secure_mail.log	

I perform a search for a keyword such as “\*” or “root” in this case. I then view one of the logs and select Event Actions → Extract fields. This allows me to rename fields in the log to facilitate searches.

## Select Method

Indicate the method you want to use to extract your field(s). [Learn more](#)

[I prefer to write the regular expression myself >](#)

Source type

secure\_mail

```
Thu Sep 08 2022 00:15:06 mailsv1 sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2
```

(.\*?)

### Regular Expression

Splunk Enterprise will extract fields using a Regular Expression.

x|y|z

### Delimiters

Splunk Enterprise will extract fields using a delimiter (such as commas, spaces, or characters). Use this method for delimited data like comma separated values (CSV files).

I choose delimiters when asked to select a method to extract fields.

The screenshot shows the Splunk Enterprise web interface. At the top, the navigation bar includes 'splunk>enterprise', 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a search bar. Below this, the 'Extract Fields' progress bar shows 'Select Method' as the first step and 'Rename Fields' as the current step. The 'Rename Fields' section has a 'Delimitter' dropdown set to 'Space'. Below the dropdown is a table of fields with their values. A 'Rename Field' dialog box is open over 'field6', showing its current value 'Thu' and a 'Rename Field' button. The 'Preview (16 fields)' section shows a list of fields with their corresponding colors. At the bottom, there is a status bar indicating '1,000 events (07/09/2023 00:00:00.000 to 06/12/2023 19:33:29.000)' and a pagination bar with 'Prev', '1', '2', '3', '4', '5', '6', '7', '8', '...', and 'Next' buttons.

**Extract Fields**

Select Method   Rename Fields   Save   < Back   Next >

### Rename Fields

Select a delimiter. In the table that appears, rename fields by clicking on field names or values. [Learn more](#)

Delimiter

Space   Comma   Tab   Pipe   Other

field1	field2	field3	field4	field5	field6	field7	field8	field9	field10	field11	field12
Thu	Sep	08	2022		Failed	password	for	root	from		

Field Name: field6

Rename Field

### Preview (16 fields)

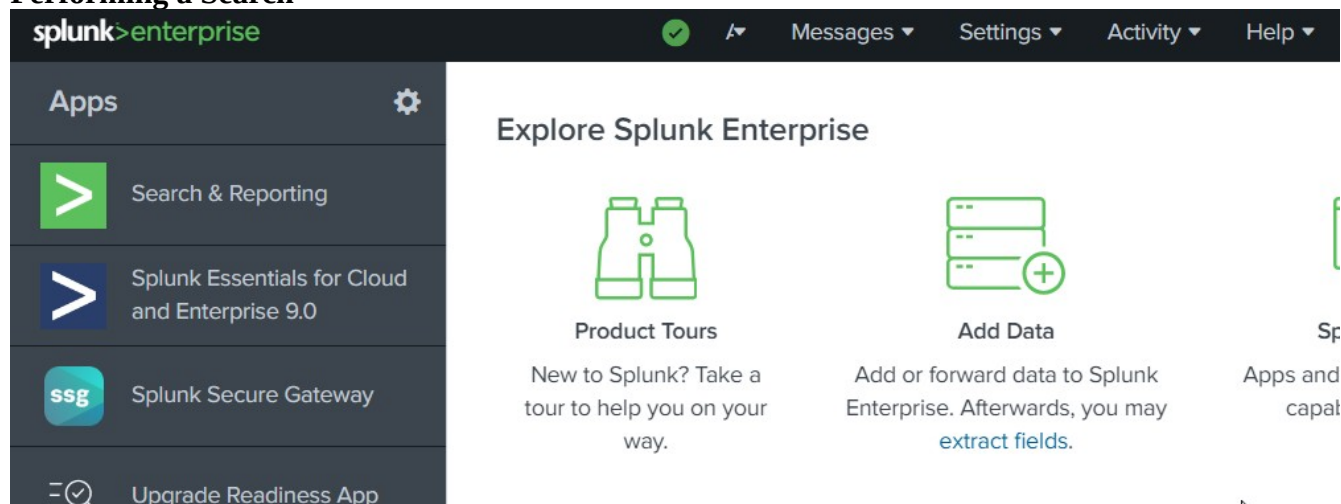
Events   field1   field2   field3   field4   field5   field6   field7   field8   field9   field10   field11

✓ 1,000 events (07/09/2023 00:00:00.000 to 06/12/2023 19:33:29.000)

< Prev   1   2   3   4   5   6   7   8   ...   Next >

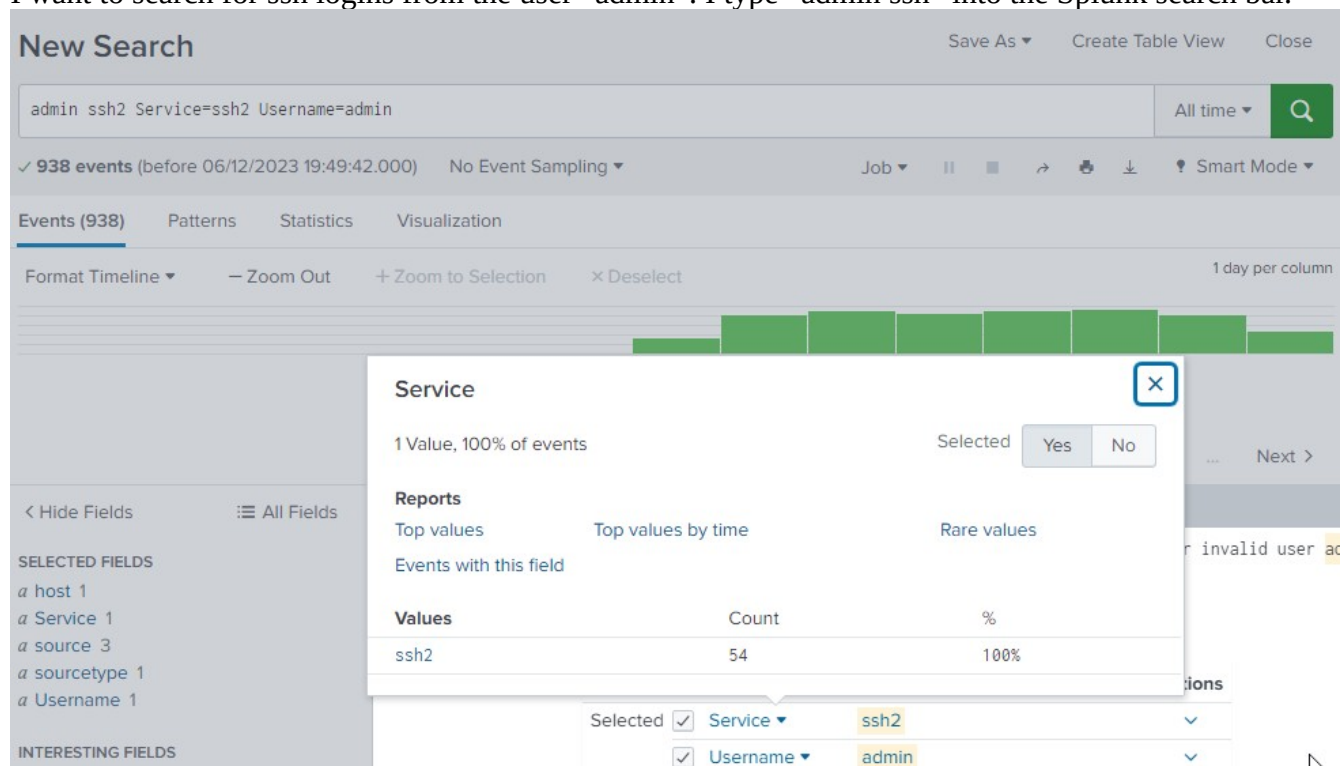
I choose space as the delimiter and proceed to rename useful fields.

## Performing a Search



I select “Search & Reporting” from the main Splunk page to access search.

I want to search for ssh logs from the user “admin”. I type “admin ssh” into the Splunk search bar.



I open one of the logs and select fields of interest. I click a field and choose an element of interest, such as the service ssh2 in this case. This updates the search bar in Splunk to include the phrase “Service=ssh2”.

### Identifying field elements with the most number of logs

I want to identify the IP address with the most failed attempts for invalid usernames attempting to login via ssh.

New Search

Save As Create Table View Close

invalid failed Service=ssh2

All time

Q

I first perform a search for invalid failed Service=ssh2.

INTERESTING FIELDS

# Date 8

# date\_hour 1

# date\_mday 8

# date\_minute 1

a date\_month 1

# date\_second 5

a date\_wday 7

# date\_year 1

a date\_zone 1

a Day 7

a device\_ID 100+

a field10 1

a field11 1

a field12 1

a field14 1

a field16 1

a field8 1

a field9 1

a hostname 4

a index 1

a IP\_Address 100+

i

Time

Event

< Prev

1

2

3

4

5

6

7

8

source = serverlogs.zip.:secure\_mail.log ; sourcetype = secure\_mail

> 08/09/2022 Thu Sep 08 2022 00:15:06 mailsv1 sshd[3760]: Failed password for ngodb from 194.8.74.23 port 2472 ssh2

IP\_Address

>100 Values, 100% of events

Selected

Yes

No

Reports

Top values

Top values by time

Rare values

Events with this field

Top 10 Values

Count

%

87.194.216.51

691

2.878%

211.166.11.101

549

2.286%

128.241.220.82

459

1.912%

194.215.205.19

375

1.562%

109.169.32.135

373

1.553%

216.221.226.11

321

1.337%

I then select IP\_Address from the list of interesting fields. Splunk automatically identifies the top 10 IP addresses.

Counting the number of unique field elements

splunk>enterprise

Apps

Administrator

Messages

Settings

Activity

Help

Q Find

Search

Analytics

Datasets

Reports

Alerts

Dashboards

Search & Reporting

New Search

Save As Create Table View Close

invalid failed Service=ssh2 | stats count by IP\_Address

All time

Q

✓ 24,011 events (before 06/12/2023 20:00:44.000)

No Event Sampling

Job

||

Smart Mode

Events

Patterns

Statistics (182)

Visualization

20 Per Page

Format

Preview

< Prev

1

2

3

4

5

6

7

8

...

Next >

IP\_Address

count

107.3.146.207

198

108.65.113.83

174

I want to know the number of unique IP addresses that have attempted to login via ssh but failed to do so due to having invalid usernames. I enter “invalid failed Service=ssh2 | stats count by IP\_Address” into the search bar and run a Splunk search. The results show that there are 182 unique IP addresses, and 24011 events.



invalid failed Service=ssh2 | stats distinct\_count(IP\_Address)

✓ 24,011 events (before 06/12/2023 20:04:55.000) No Event Sampling

Events Patterns **Statistics (1)** Visualization

20 Per Page ▼ Format Preview ▼

distinct\_count(IP\_Address) ↕

182

Another way to count the number of unique IP addresses is to conduct a search for “invalid failed Service=ssh2 | stats distinct\_count(IP\_Address)”. The result returned is also 182.

### Adding conditions to the count returned

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search Save As Create Table View Close

invalid failed Service=ssh2 | stats count by IP\_Address | where count>100 All time Q

✓ 24,011 events (before 06/12/2023 20:08:14.000) No Event Sampling Job || ↻ ⌵ ⌴ Smart Mode ▼

Events Patterns **Statistics (135)** Visualization

20 Per Page ▼ Format Preview ▼ < Prev 1 2 3 4 5 6 7 Next >

IP_Address ↕	count ↕
107.3.146.207	198
108.65.113.83	174

I add the phrase “| where count > 100” to select only the IP addresses that have at least 100 invalid username failed attempts.

### **Excluding Search Terms**

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

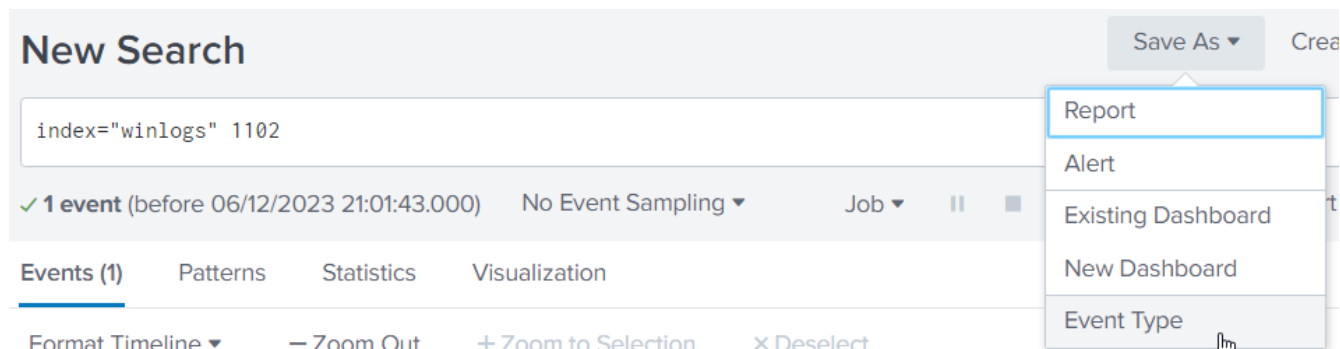
New Search Save As Create Table View Close

NOT User="root" NOT service="ssh2" All time Q

21,056 of 21,056 events matched No Event Sampling 98.8% of the time range scanned. Job || ↻ ⌵ ⌴ Smart Mode ▼

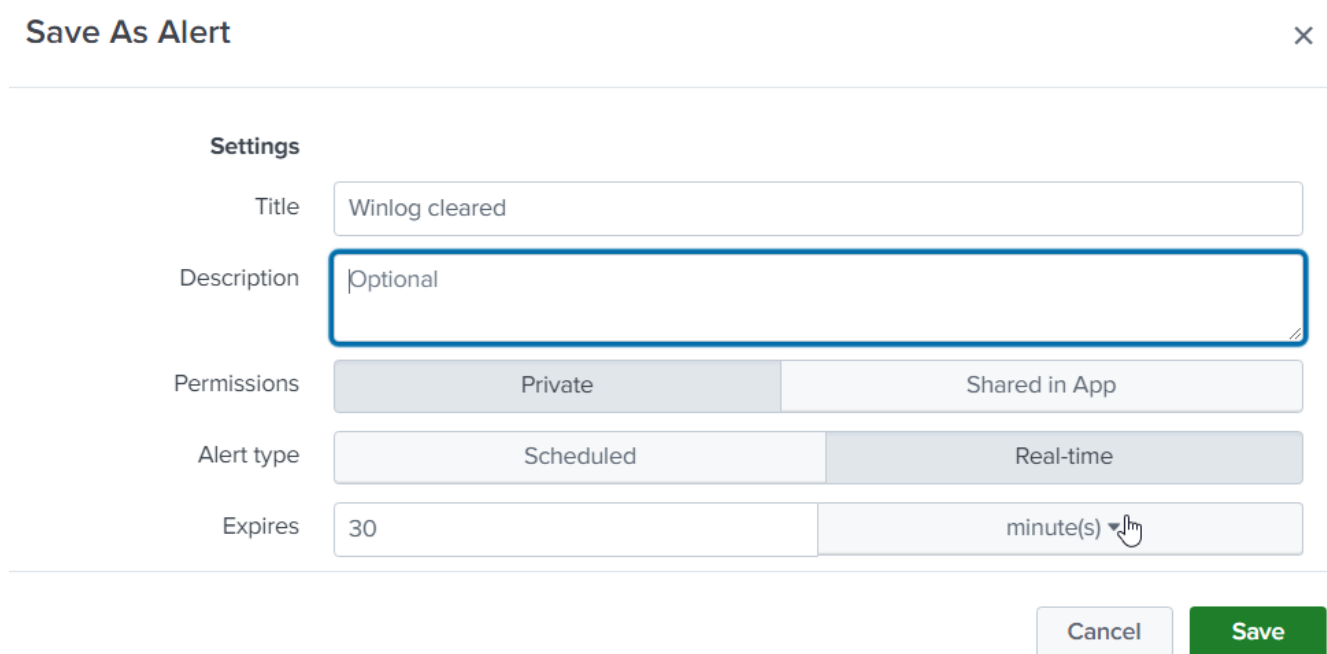
I use the NOT keyword to exclude terms from search results.

## Creating an Alert



The screenshot shows the 'New Search' interface. At the top, there's a search bar containing 'index="winlogs" 1102'. Below the search bar, it indicates '1 event (before 06/12/2023 21:01:43.000)' and 'No Event Sampling'. A 'Save As' dropdown menu is open, showing options: 'Report', 'Alert', 'Existing Dashboard', 'New Dashboard', and 'Event Type'. The 'Alert' option is highlighted. Below the search bar, there are tabs for 'Events (1)', 'Patterns', 'Statistics', and 'Visualization'. At the bottom, there are controls for 'Format Timeline', 'Zoom Out', 'Zoom to Selection', and 'Deselect'.

I enter a search term, here: index="winlogs" 1102, and select "Save As" and "Alert" to create an alert.



The screenshot shows the 'Save As Alert' dialog box. It has a title bar with a close button. The dialog is divided into sections. The 'Settings' section includes a 'Title' field with the value 'Winlog cleared', a 'Description' field with the value 'Optional', a 'Permissions' section with 'Private' selected, an 'Alert type' section with 'Real-time' selected, and an 'Expires' section with '30' selected and 'minute(s)' as the unit. At the bottom right, there are 'Cancel' and 'Save' buttons.

I set the alert type to monitor in real-time. For testing purposes I specify that the alert monitoring should expire in 30 minutes.

## Save As Alert



Trigger alert when Per-Result ▼

Throttle ? ☐

### Trigger Actions

+ Add Actions ▼

When triggered

▼ Add to Triggered Alerts Remove

Severity High ▼

Cancel

Save

I specify the trigger action to add an alert to triggered alerts under the severity level “High”.

The screenshot shows the Splunk Enterprise interface. At the top, the navigation bar includes 'splunk>enterprise', a status indicator, and menu items: 'Messages', 'Settings', 'Activity', and 'Help'. Below the navigation bar, there are filters for 'App' (Search & Reporting (search)), 'Owner' (Administrator (admin)), 'Severity' (All), and 'Alert' (All). A dropdown menu is open under 'Activity', showing 'Jobs' and 'Triggered Alerts'. Below the filters, there are navigation links '«Prev' and 'Next»'. The main content area displays a table of triggered alerts.

	Time ↕	Fired alerts ↕	App	Type ↕	Severity ↕	Mode ↕	Actions
<input type="checkbox"/>	2023-12-06 21:10:32 Malay Peninsula Standard Time	Winlog cleared	search	Real-time	High	Per Result	<a href="#">View results</a>   <a href="#">Delete</a>

I clear the security event log again and view the triggered alert by selecting “Activity” → “Triggered Alerts”.

## Bug fixes

### Faulty field name searches

I noticed that the number of search results returned is sometimes 0 when specifying the field name, whereas the same search without the fieldname's name specified returns results.

**New Search** Save As Create Table View Close

accepted hostname=www3 Service=ssh2 All time Q

✓ 0 events (before 06/12/2023 20:17:28.000) No Event Sampling Job || [ ] ↗ [ ] [ ] [ ] Smart Mode

**New Search** Save As Create Table View Close

accepted hostname=www3 ssh2 All time Q

✓ 387 events (before 06/12/2023 20:18:54.000) No Event Sampling Job || [ ] ↗ [ ] [ ] [ ] Smart Mode

Events (387) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection x Deselect 1 day per column

List Format 20 Per Page < Prev 1 2 3 4 5 6 7 8 ... Next >

< Hide Fields All Fields

SELECTED FIELDS

- a field16 1
- a host 1
- a hostname 1
- a source 1
- a sourcetype 1

i	Time	Event
✓	08/09/2022 00:15:03.000	Thu Sep 08 2022 00:15:03 www3 sshd[57740]: Accepted password for djohnson from 0.3.10.46 port 9507 ssh2

Event Actions

Type	Field	Value	Actions
Selected	field16	ssh2	⌵

After some debugging, I realized this was due to a differently formatted log entry that had the element “ssh2” named under a different field.

### Need to specify index when searching for Windows Logs

New Search

Save As ▼ Create T

✓ 28 events (before 06/12/2023 21:22:32.000)

No Event Sampling ▼

Job ▼

||

■

↗

🖨

↓

💡 Smart Mo

Events (28)

Patterns

Statistics

Visualization

Format Timeline ▼

— Zoom Out

+ Zoom to Selection

× Deselect

List ▼

✍ Format

20 Per Page ▼

< Prev

< Hide Fields

⋮ All Fields

+ Extract New Fields

i	Time	Event
>	06/12/2023 21:20:50.000	... 24 lines omitted ... OriginalFileName: net1.exe CommandLine: C:\Windows\system32\net1 user newuser CurrentDirectory: C:\Windows\system32\ ... 9 lines omitted ... ParentCommandLine: net user newuser 1234567aA /add ParentUser: DESKTOP-UAB80KH\Caleb <a href="#">Show all 38 lines</a>

The search term “newuser” returns a search result when the index “winlogs” is specified.

New Search

Save As ▼ Create T

✓ 0 events (before 06/12/2023 21:25:29.000)

No Event Sampling ▼

Job ▼

||

■

↗

🖨

↓

💡 Smart Moc

I noticed that the same “newuser” search term returns no results when the index “winlogs” is not specified.

### Unable to forward logs to Splunk machine

```
Pinging 172.16.50.20 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.50.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

I noticed that the Splunk machine was unreachable via ping from the other Windows virtual machine, despite putting both machines on LAN via vmware settings and running pfsense in the background (as the default gateway 172.16.50.1). I also noticed that both machines could ping 8.8.8.8.

```
C:\Users\Caleb>ping 172.16.50.254

Pinging 172.16.50.254 with 32 bytes of data:
Reply from 172.16.50.254: bytes=32 time<1ms TTL=128
Reply from 172.16.50.254: bytes=32 time=1ms TTL=128
Reply from 172.16.50.254: bytes=32 time=3ms TTL=128
Reply from 172.16.50.254: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.50.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\Users\Caleb>ipconfig

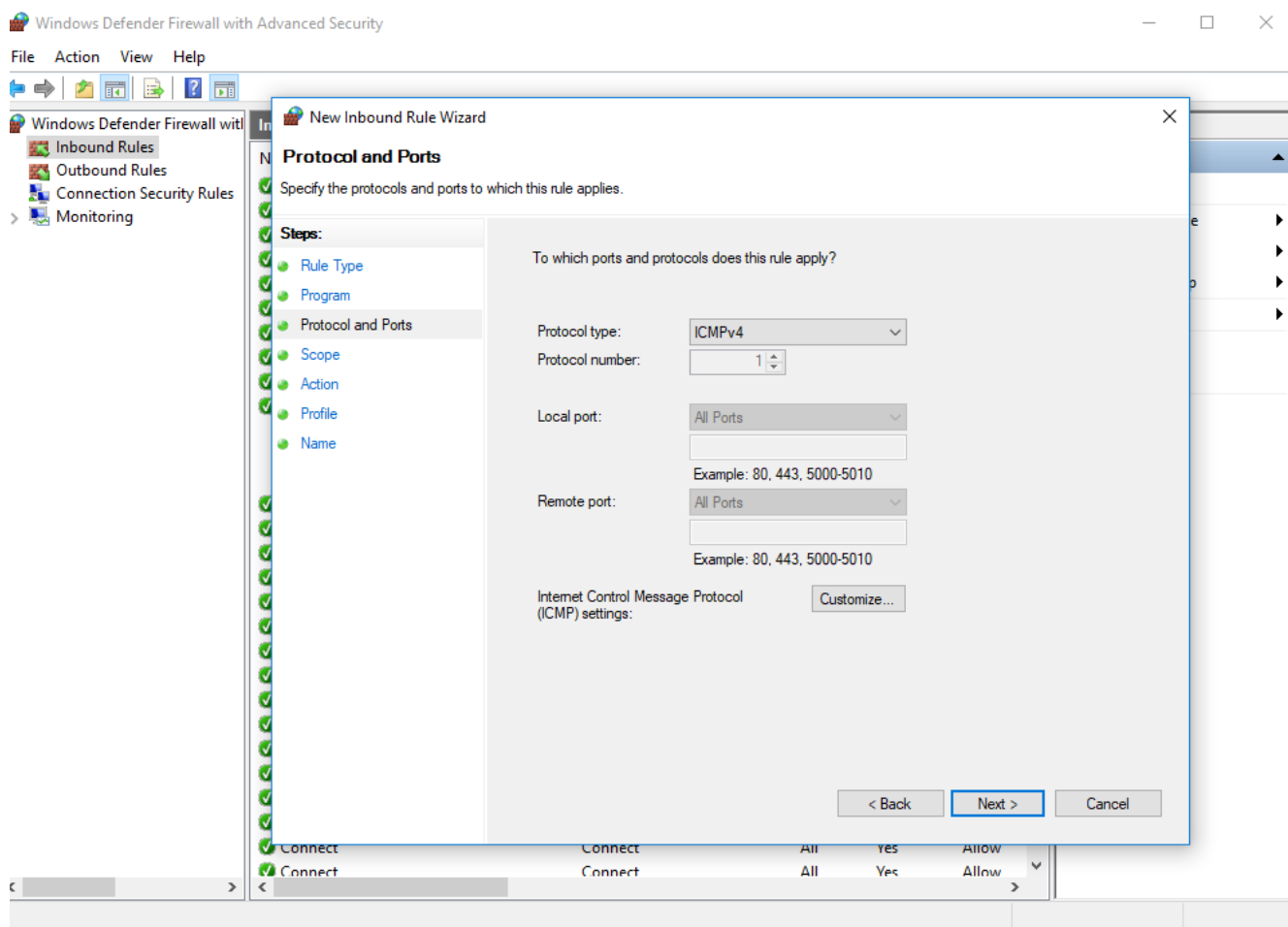
Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::a5:7d00:95ec:5c9a%7
    IPv4 Address. . . . . : 172.16.50.20
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.50.1
```

I noticed that the other Windows machine was reachable via ping from the Splunk machine.

[Troubleshooting: Enabling ICMP packets inbound via Windows Firewall](#)



I allowed inbound ICMP packets on the Windows 10 machine on which Splunk was installed.

I am now able to ping the Windows 10 machine. I create a second firewall rule to allow inbound traffic on TCP port 9997, to accept forwarded Splunk logs.

```
C:\Windows\system32>netstat -nabo | findstr 9997
TCP    0.0.0.0:9997          0.0.0.0:0           LISTENING      2308
TCP    172.16.50.20:9997    172.16.50.254:50449 ESTABLISHED    2308
```

I check that a connection has been established using netstat -nabo. The b flag lists the application, the o flag lists the owning application. The system is now functioning properly.

## Summary

In this lab I learned how to install a SIEM, load log data, label log fields and perform search queries using Splunk enterprise. These queries include identifying the top occurring elements in a field, counting the number of unique elements in a field, and searching only for elements that occur at least a certain number of times. I also learned about the keywords AND, OR and NOT (which can be used to exclude search terms from a query).

## References

### Setup

1. <https://tinyurl.com/cfcsplunk>
2. <https://tinyurl.com/cfcsplunkeglogs>
5. <https://tinyurl.com/cfcsplunkforwarder>

### Splunk

3. RichG (2022) *How to exclude a particular string from set of server logs* <https://stackoverflow.com/questions/73932074/how-to-exclude-a-particular-string-from-set-of-server-logs>.

### Searching Logs

4. Esa Jokinen (2020) *Where can I view successful logon attempts for SSHD?* <https://serverfault.com/questions/1047754/where-can-i-view-successful-logon-attempts-for-sshd>

In the lab I had to identify the number of accepted logins via ssh. I used the keyword accepted [4] to perform this search.