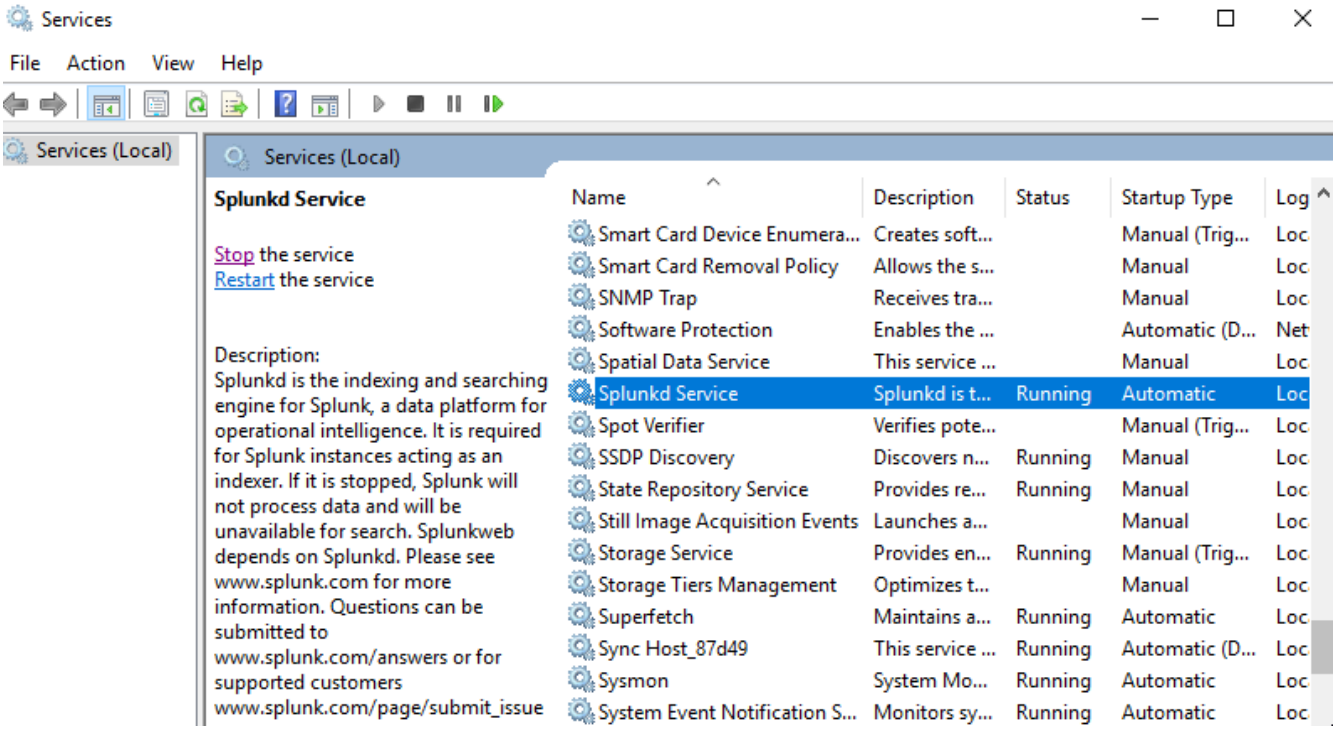
Project Description

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

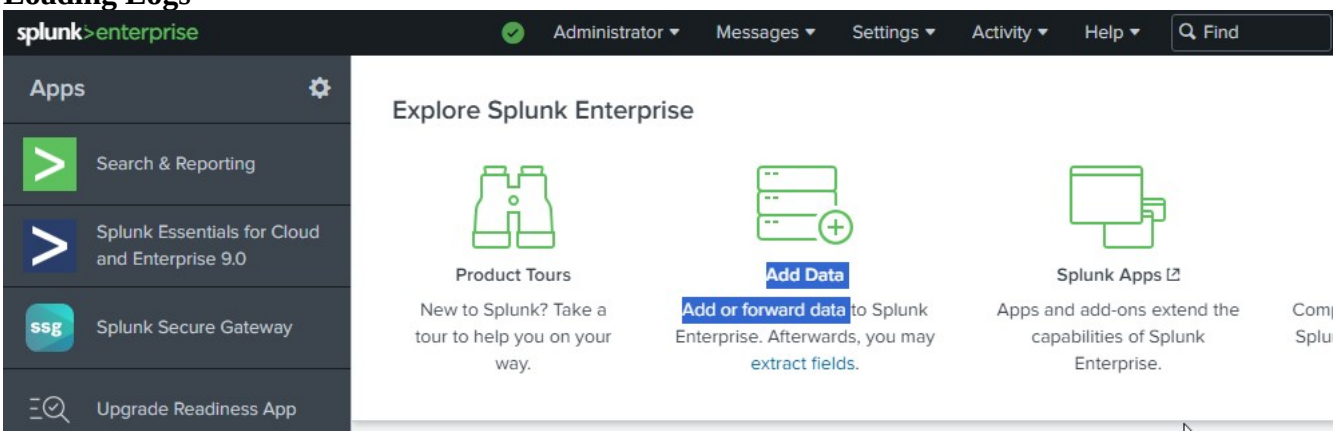
Installing Splunk

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

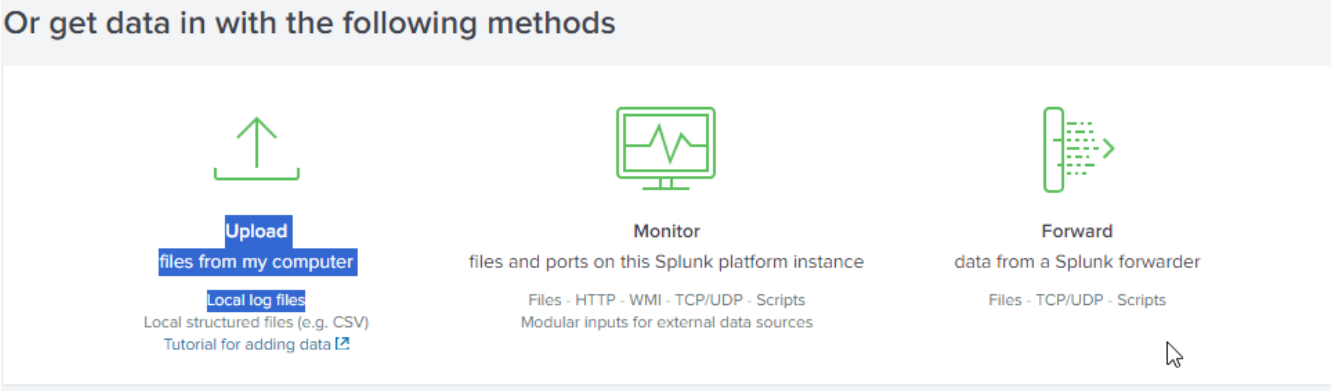


The Splunkd service is automatically started by the installer, it is the index and search engine for Splunk.

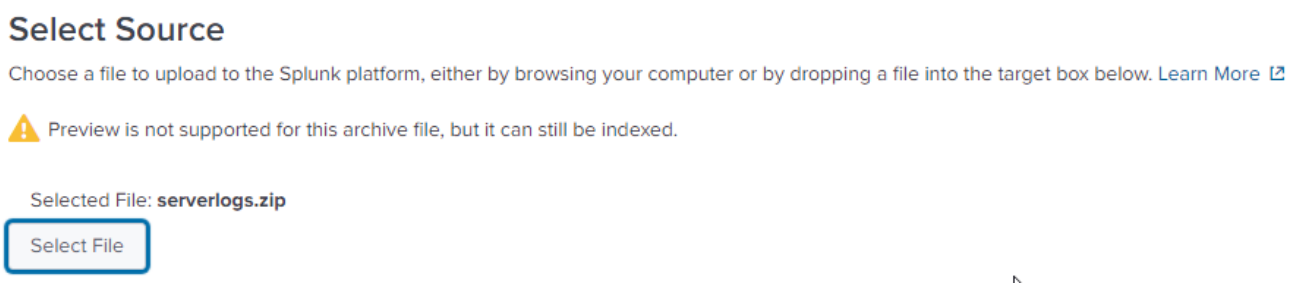
Loading Logs



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



I select “Upload” to upload data to Splunk.



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.

splunk>enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Add Data

Select Source — Input Settings — Review — Done

< Back Review >

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 ▾

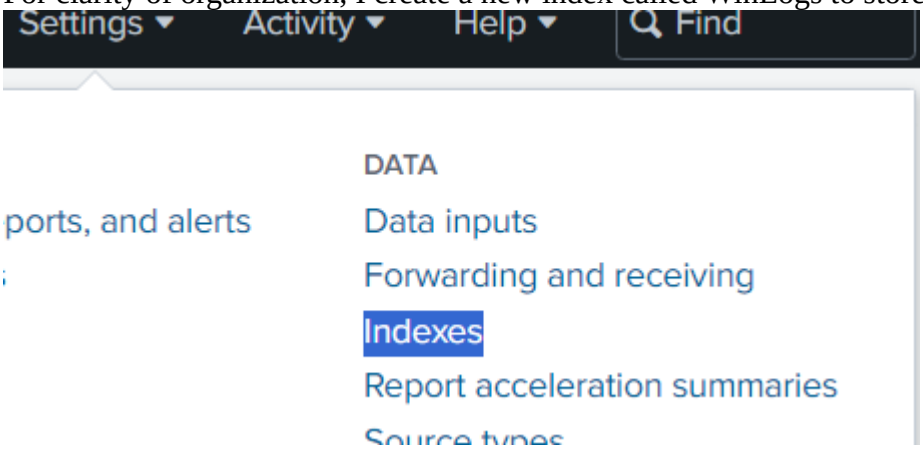
✓ **22,614 events** (before 06/12/2023 20:29:20.000) No Event Sampling ▾ Job ▾ Smart Mode ▾

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

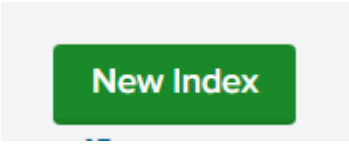
Forwarding Logs

Creating a New Index Label for clarity

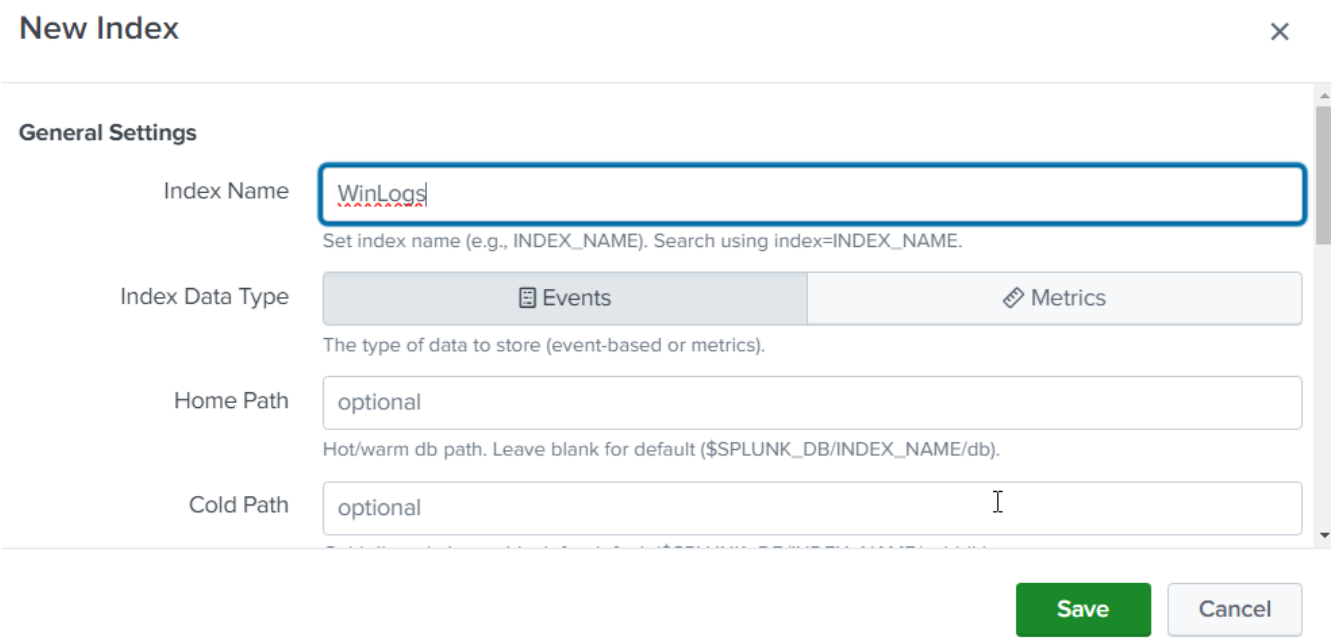
For clarity of organization, I create a new index called WinLogs to store locally forwarded logs.



I select Settings → Indexes to access the index page.



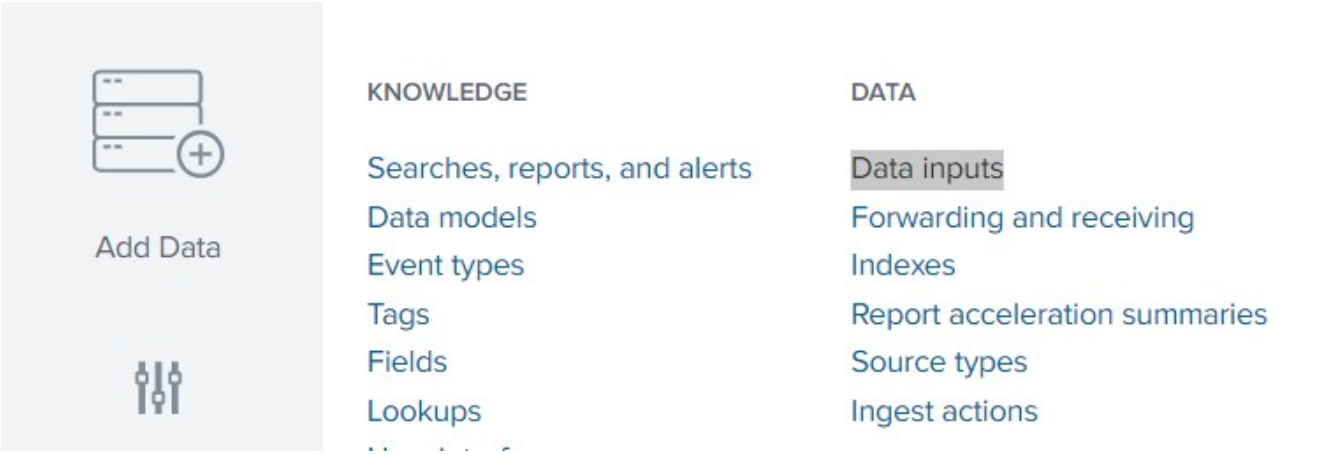
I select the "New Index" button.



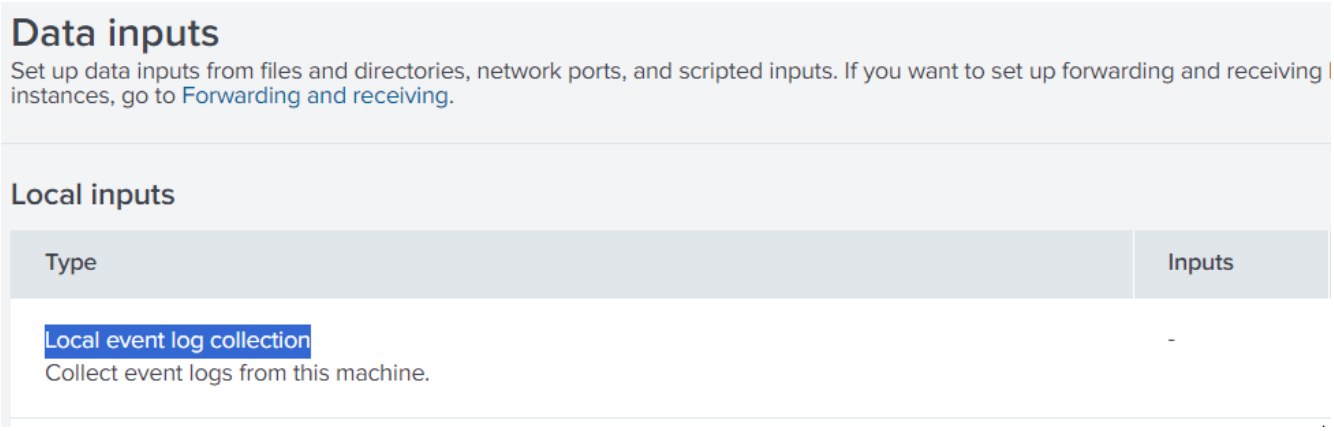
I enter the name of the new index "WinLogs" and click "Save".

Forwarding a local data input

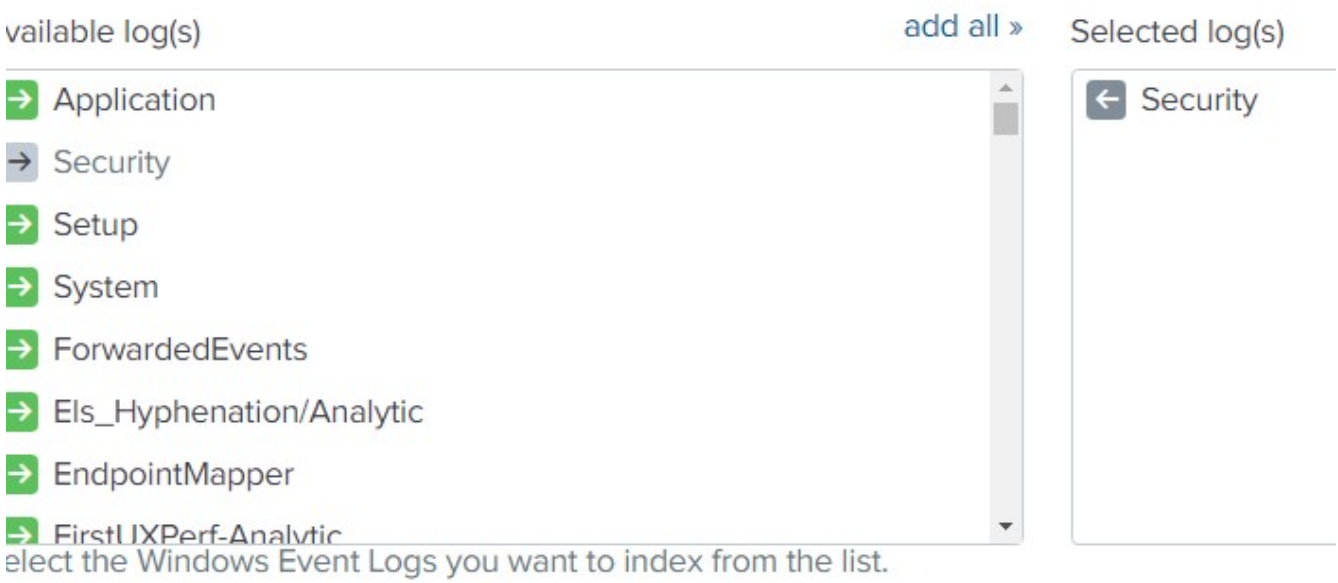
I then proceed to add a locally forwarded data input.



I select Settings → Data inputs.

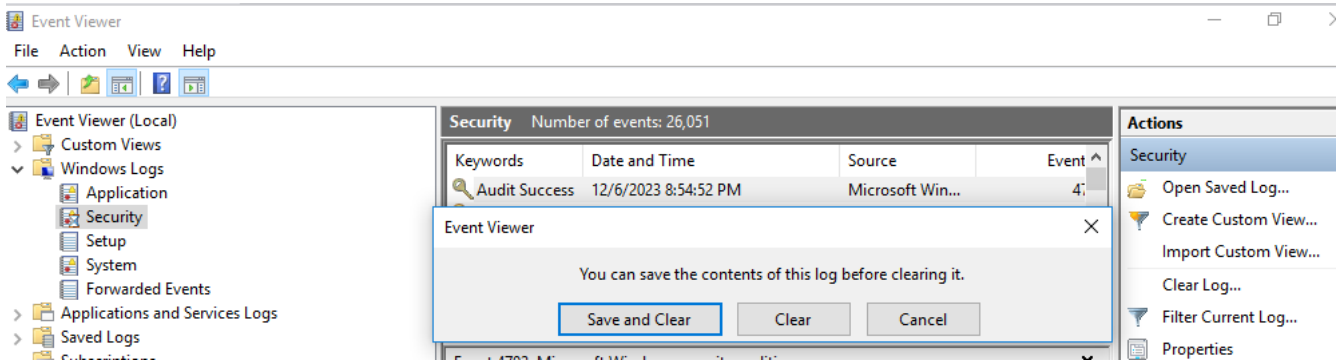


I choose “Local event log collection” as the input source.

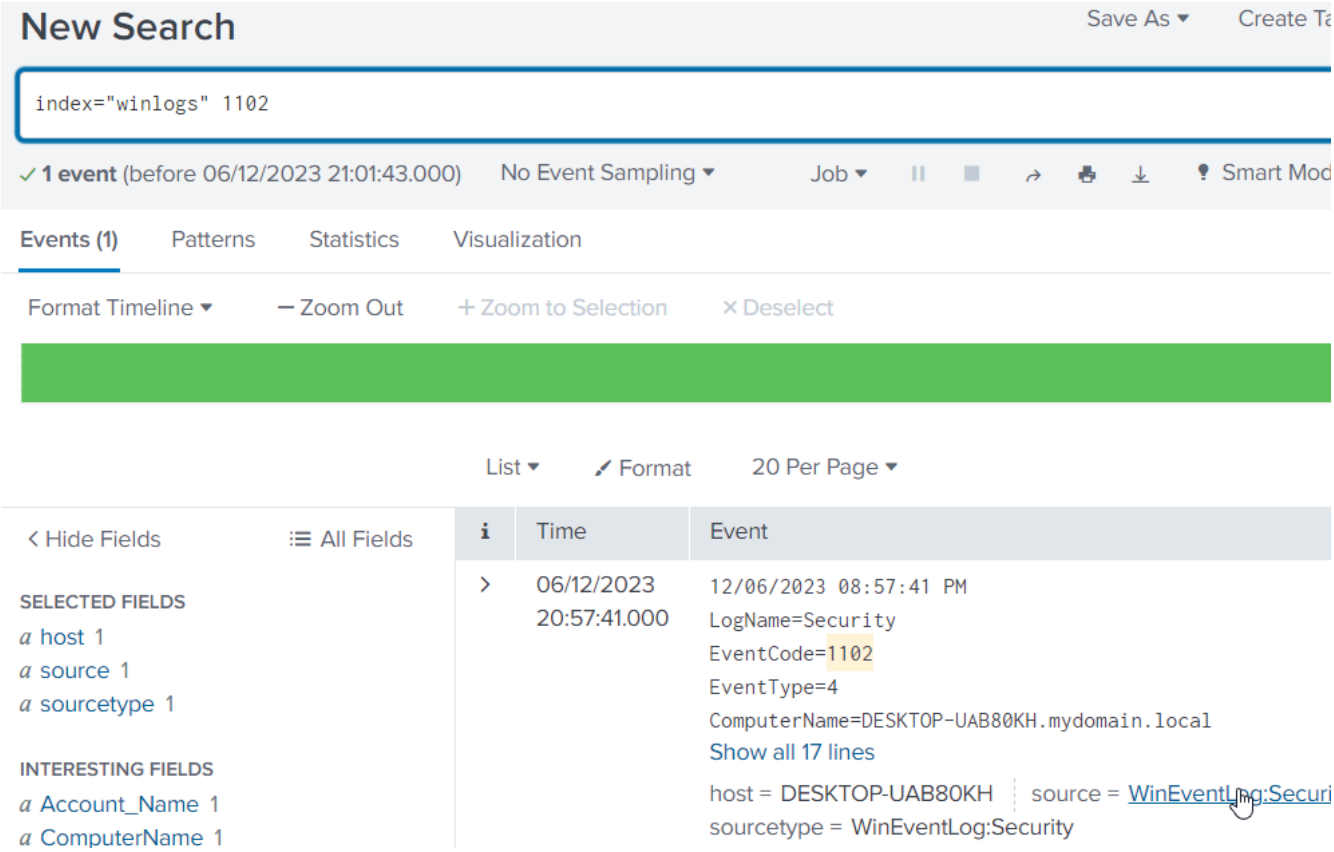


I choose “Security” to select the security event log, and choose to forward it to the “winlogs” index.

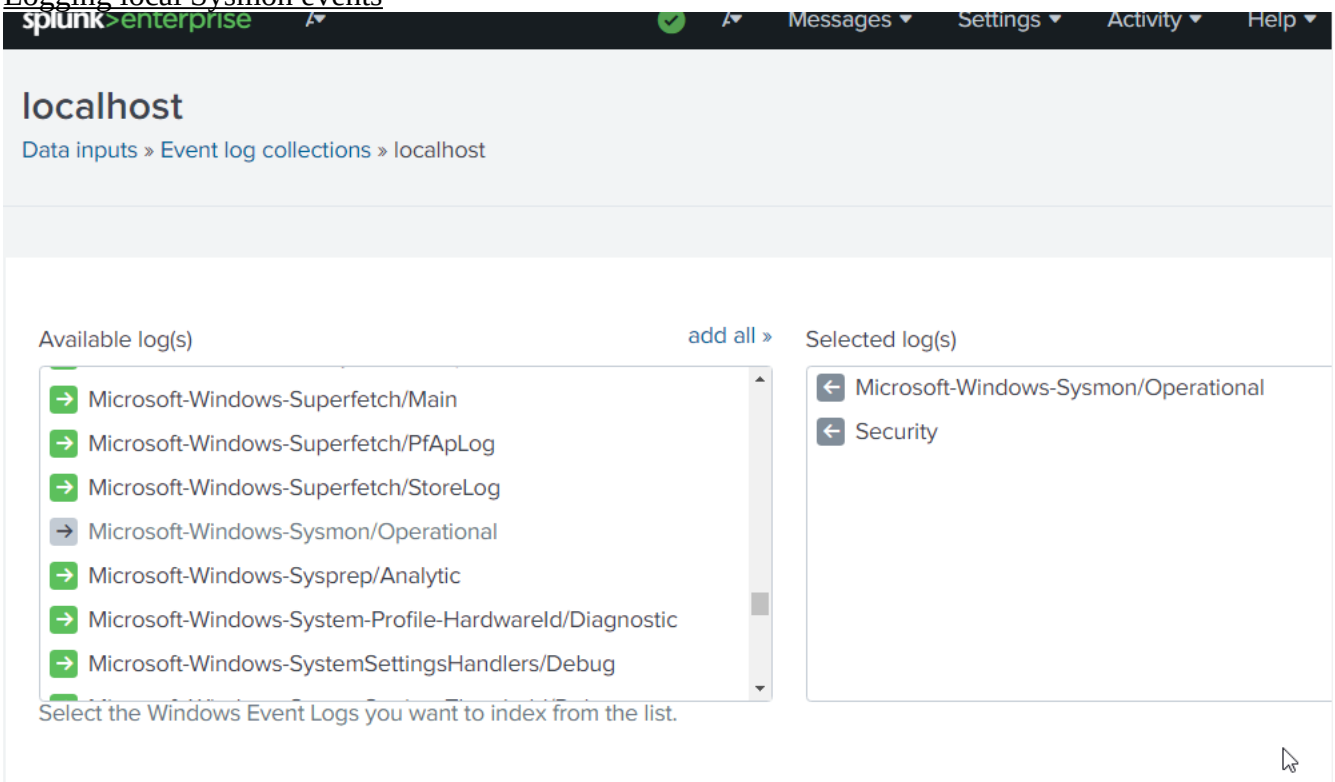
<u>Searching for locally forwarded security logs</u>



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



Logging local Sysmon events

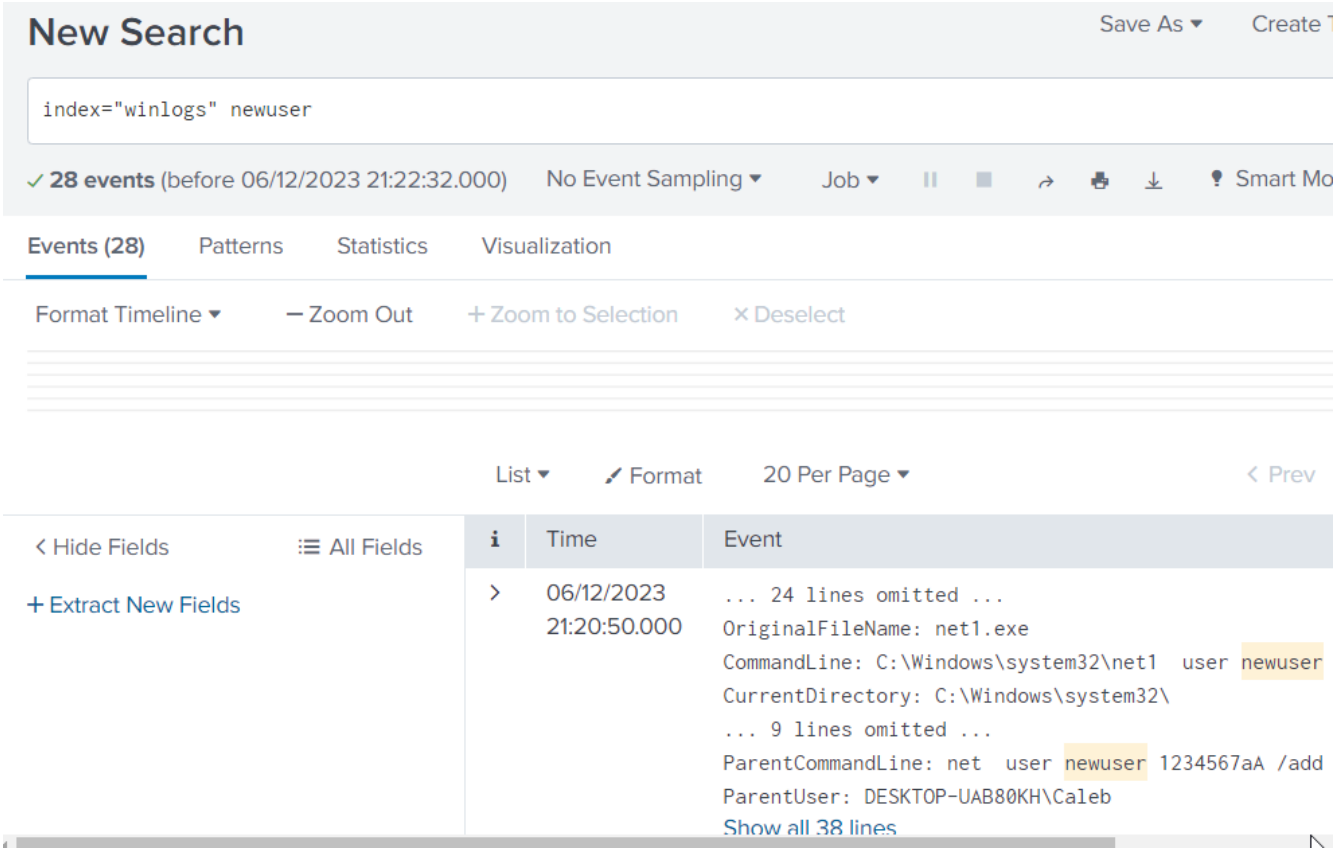


I select “Microsoft-Windows-Sysmon/Operational” under Local event log collection.

```
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

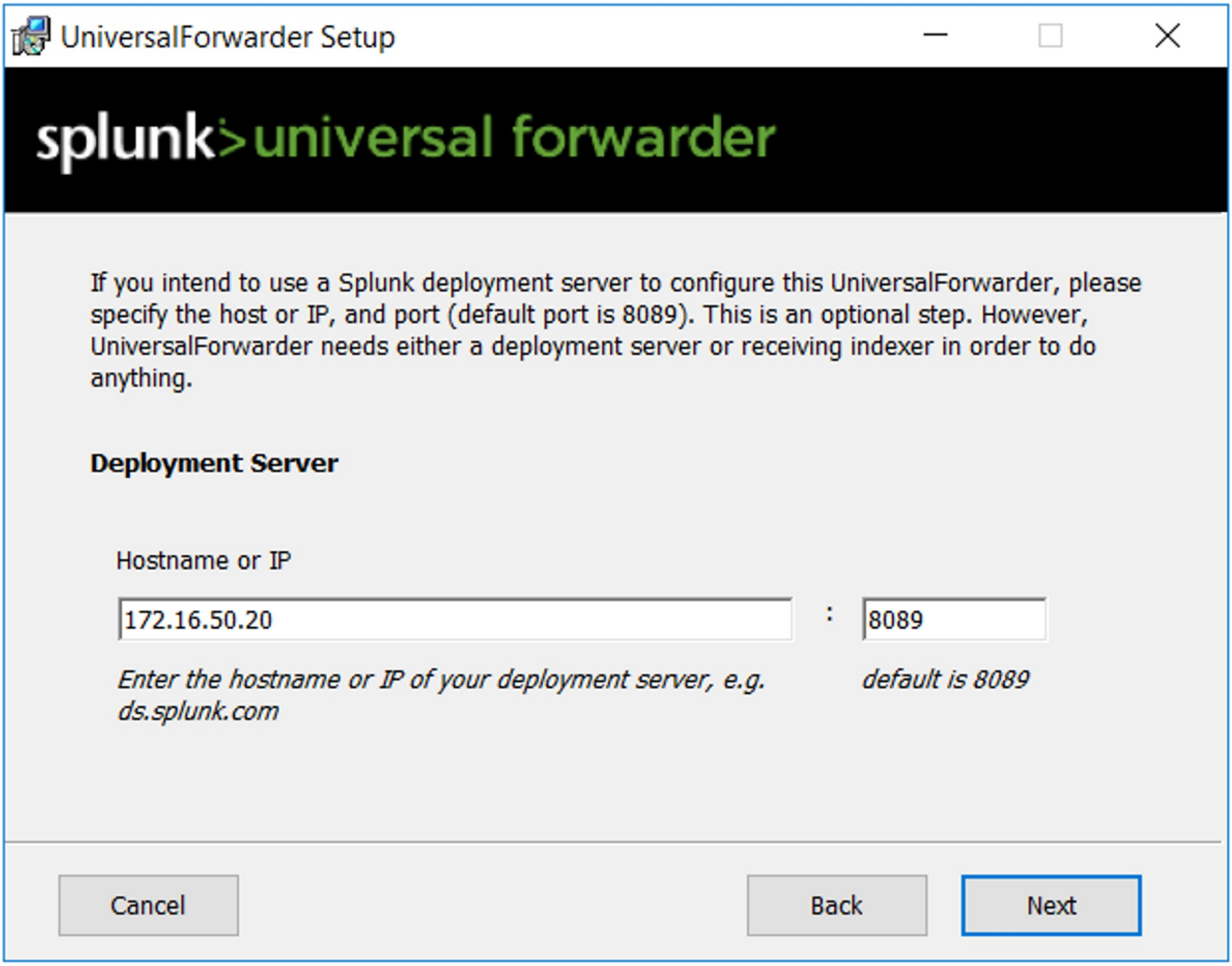
I create a new user called “newuser” from the command line.



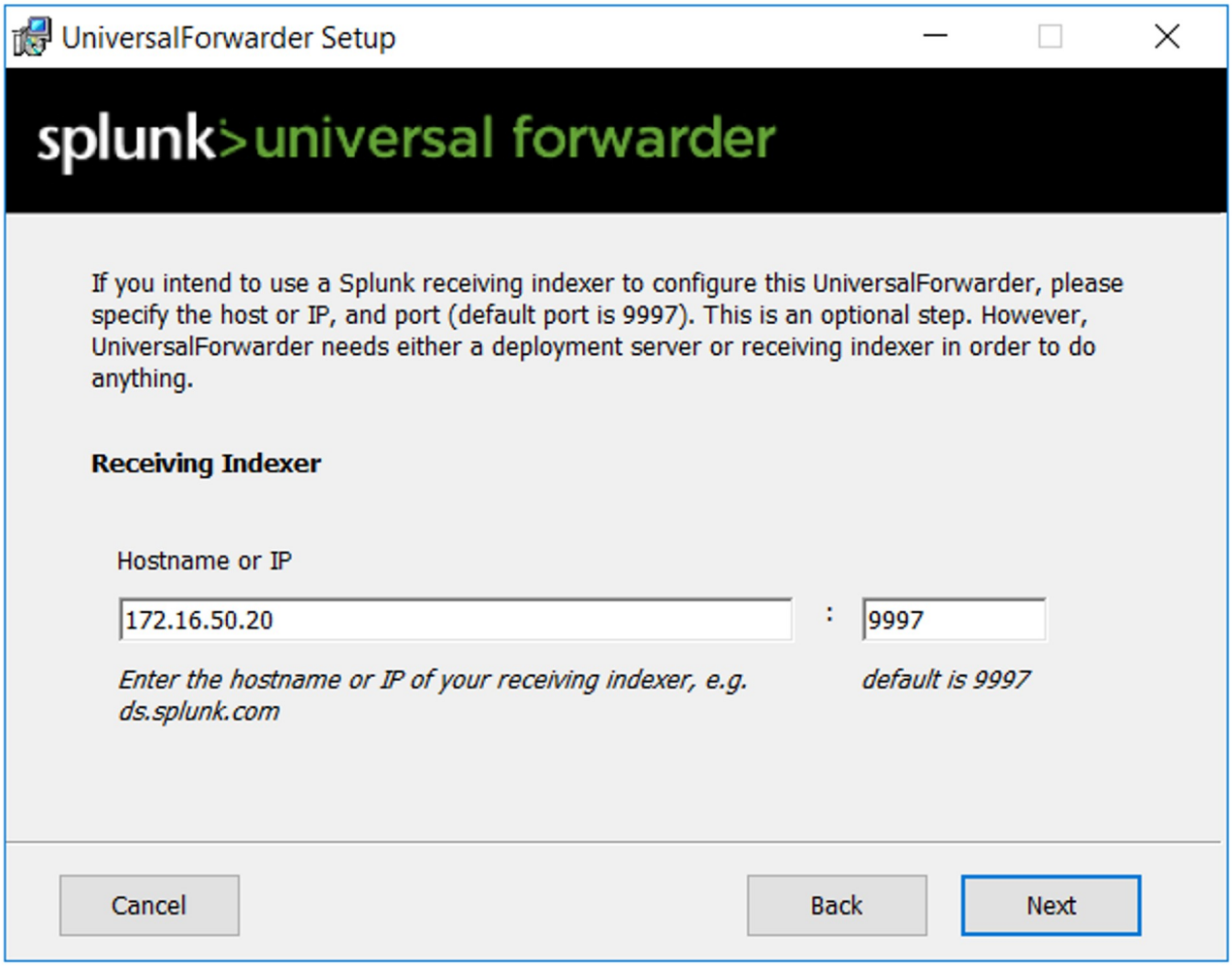
I search the “winlogs” index for the term “newuser” and find the command executed. Note that the index “winlogs” must be specified in order for this result to appear.

<u>Forwarding events from another Windows virtual machine</u>

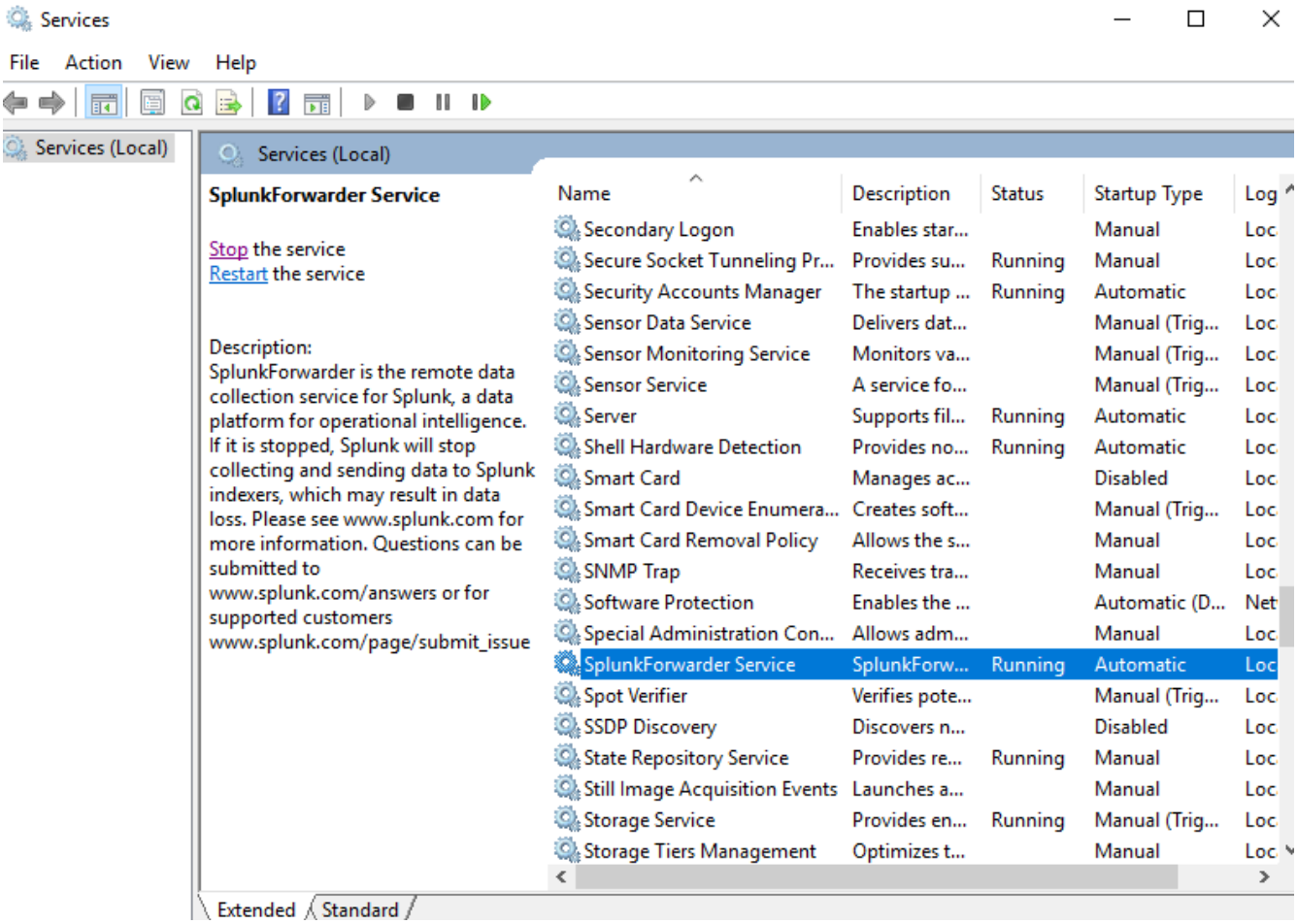
I download [5] and install Splunk forwarder on another Windows virtual machine.



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

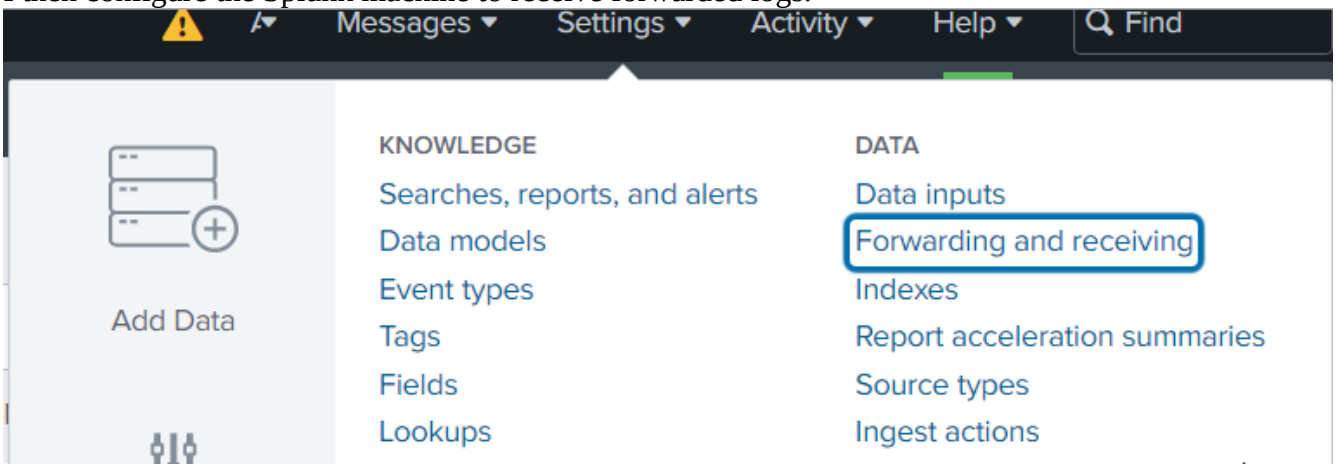


I specify the receiving indexer to be the machine on which Splunk is installed.

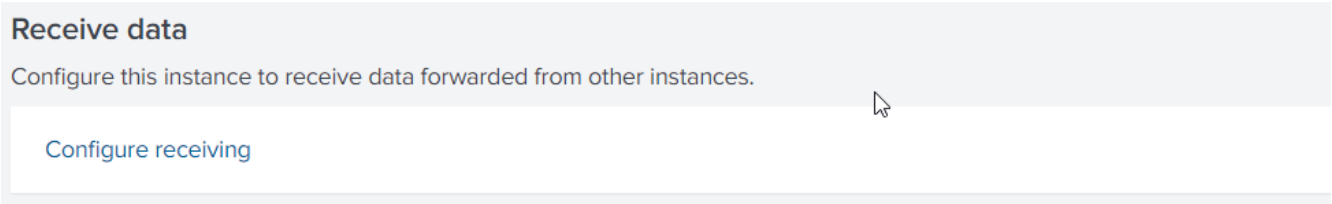


A new service SplunkForwarder Service is created.

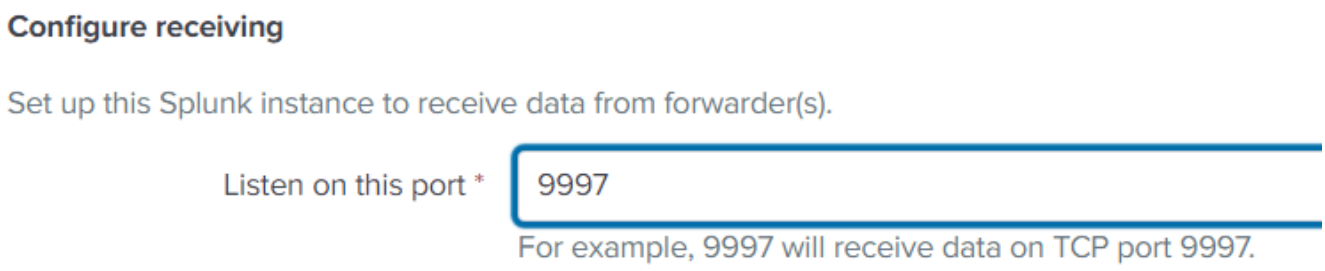
I then configure the Splunk machine to receive forwarded logs.



I select “Settings” → “Forwarding and receiving”.

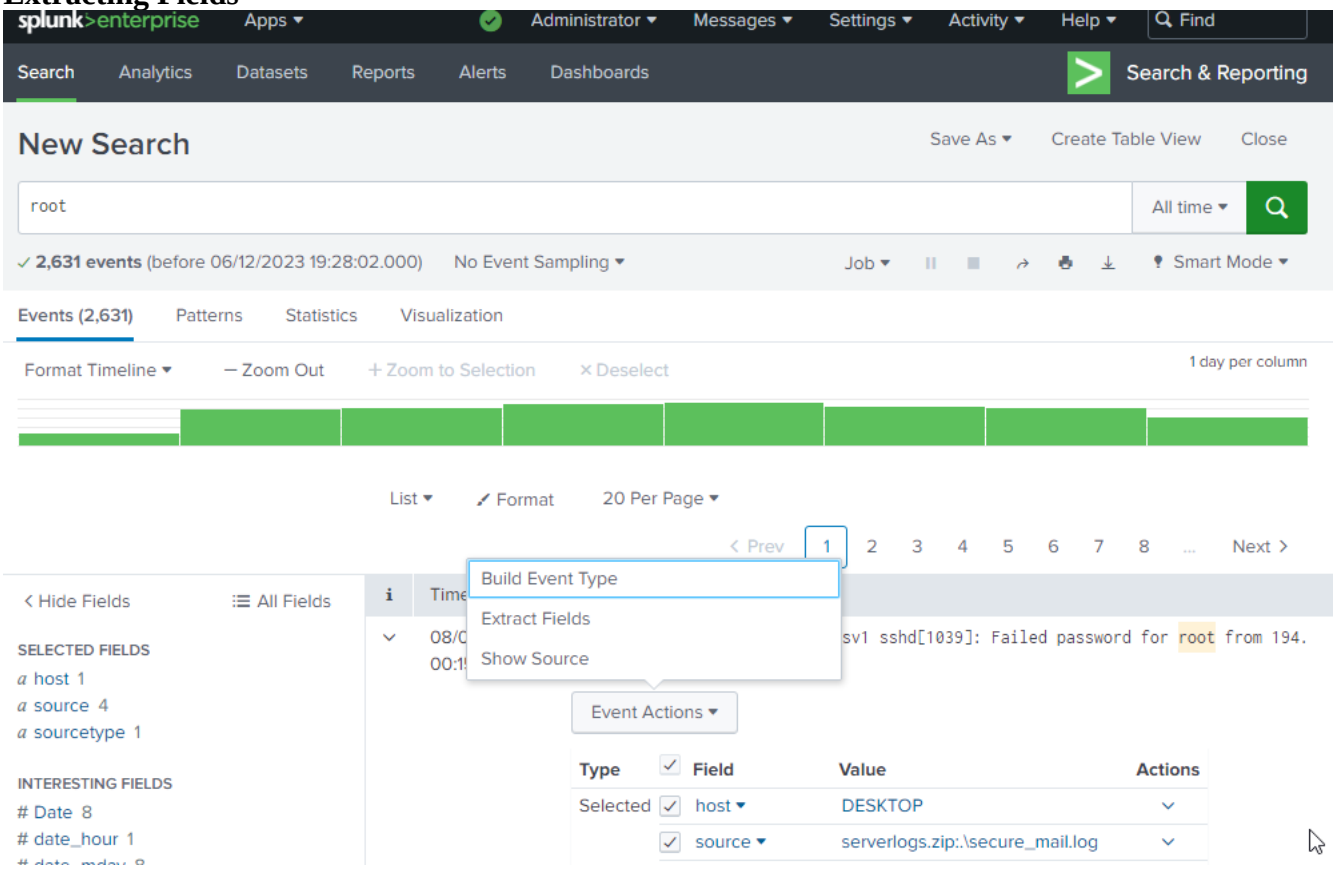


I select “Configure receiving”.

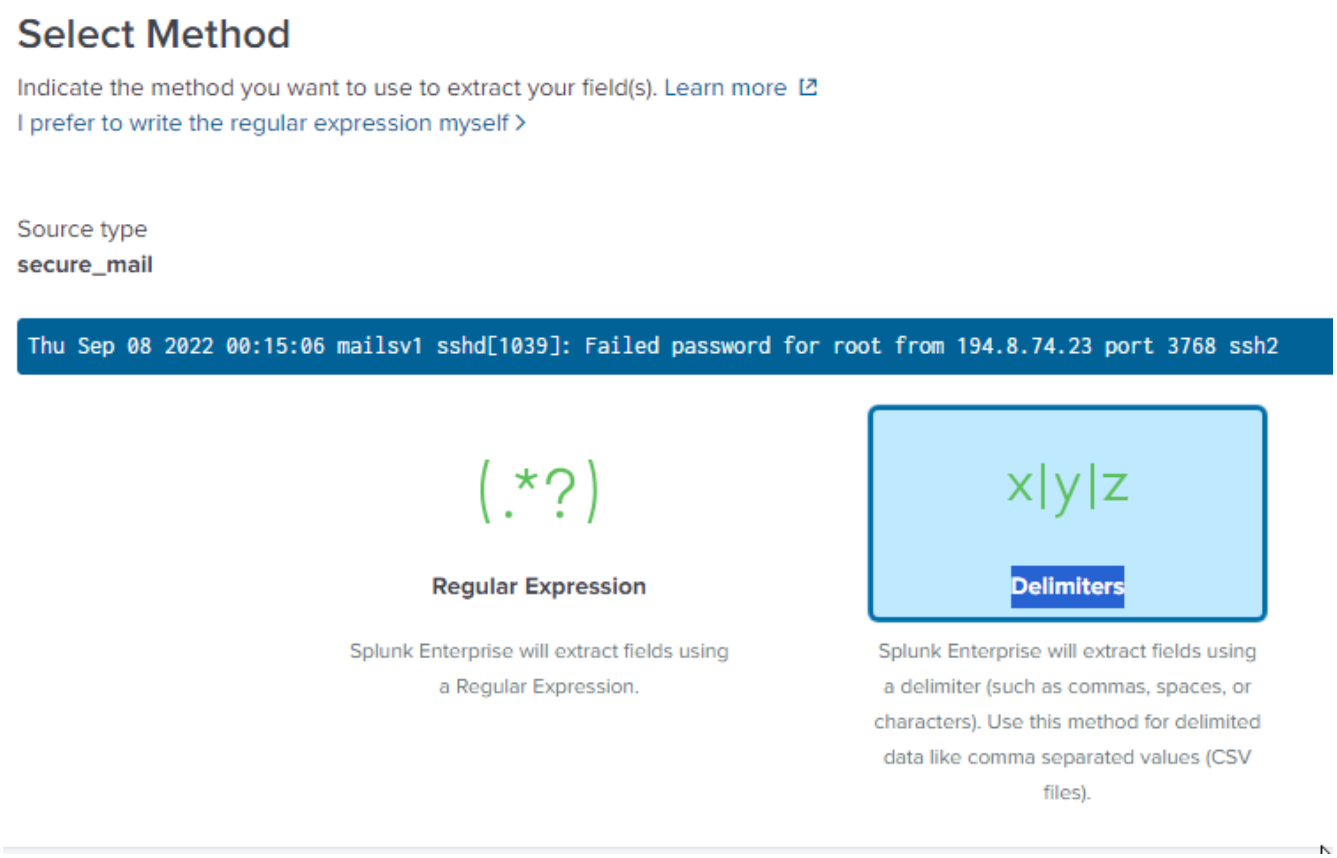


I select “New receiving port” and enter “9997”.

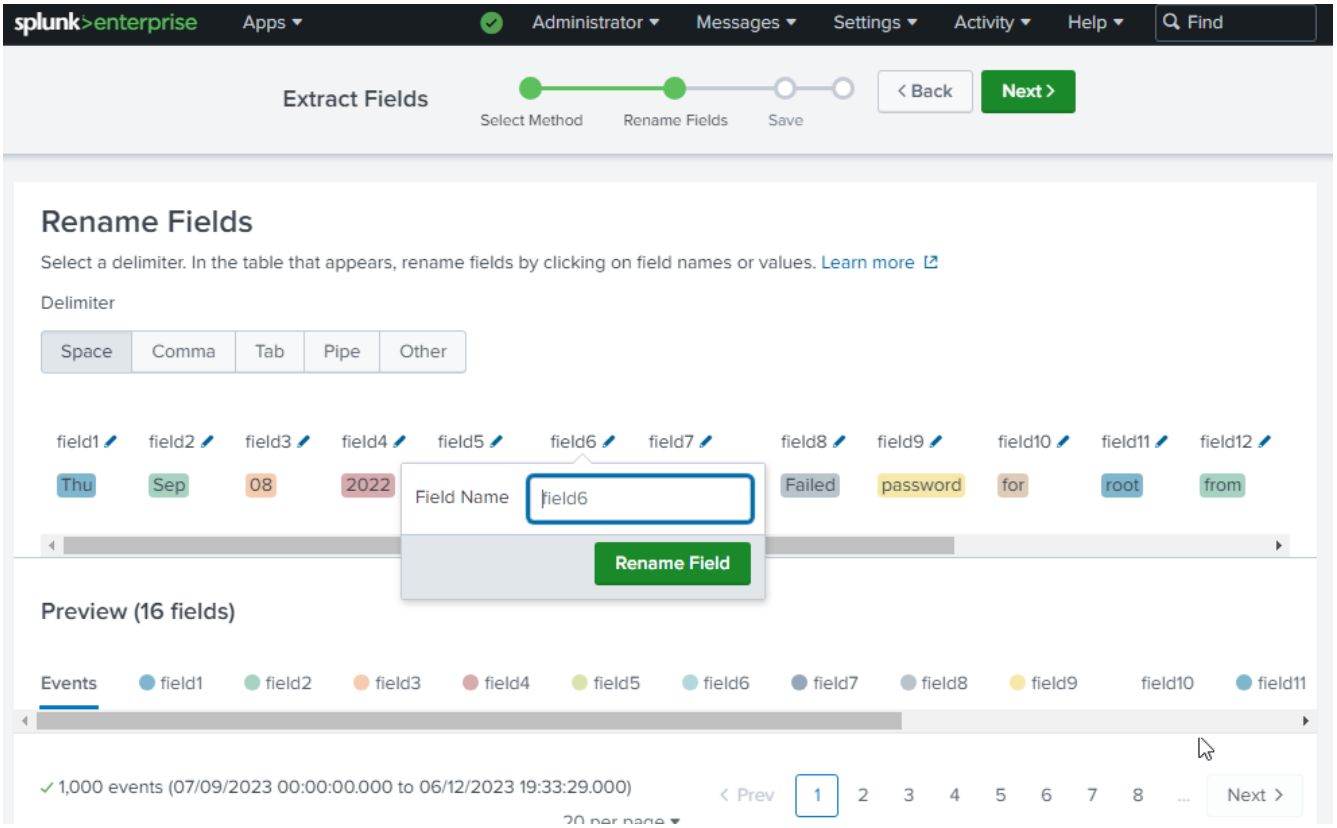
Extracting Fields



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.

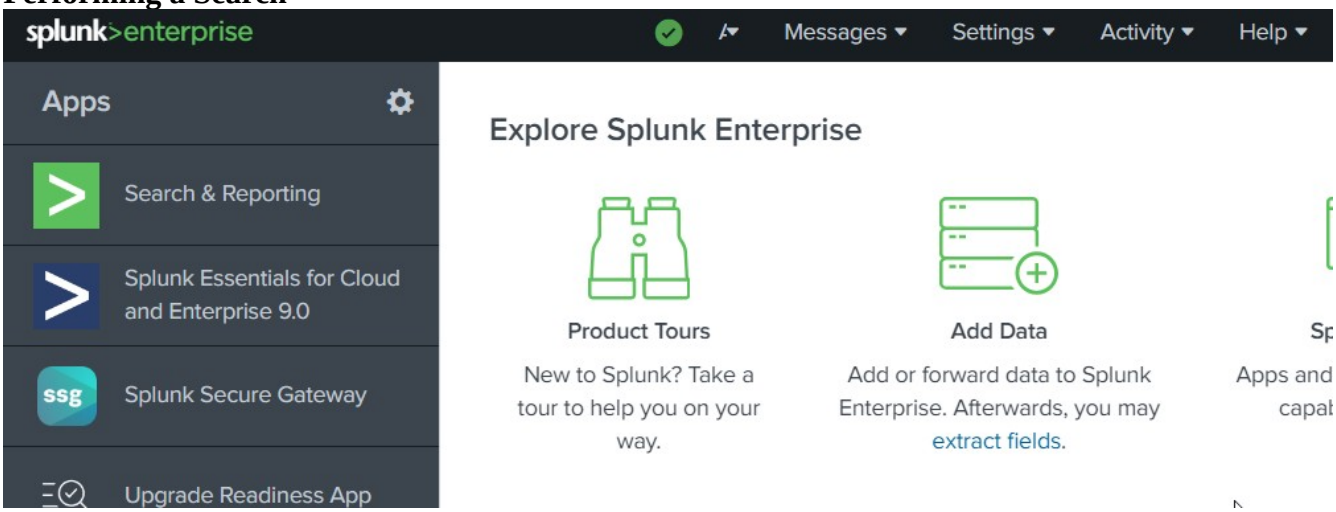


I choose delimiters when asked to select a method to extract fields.



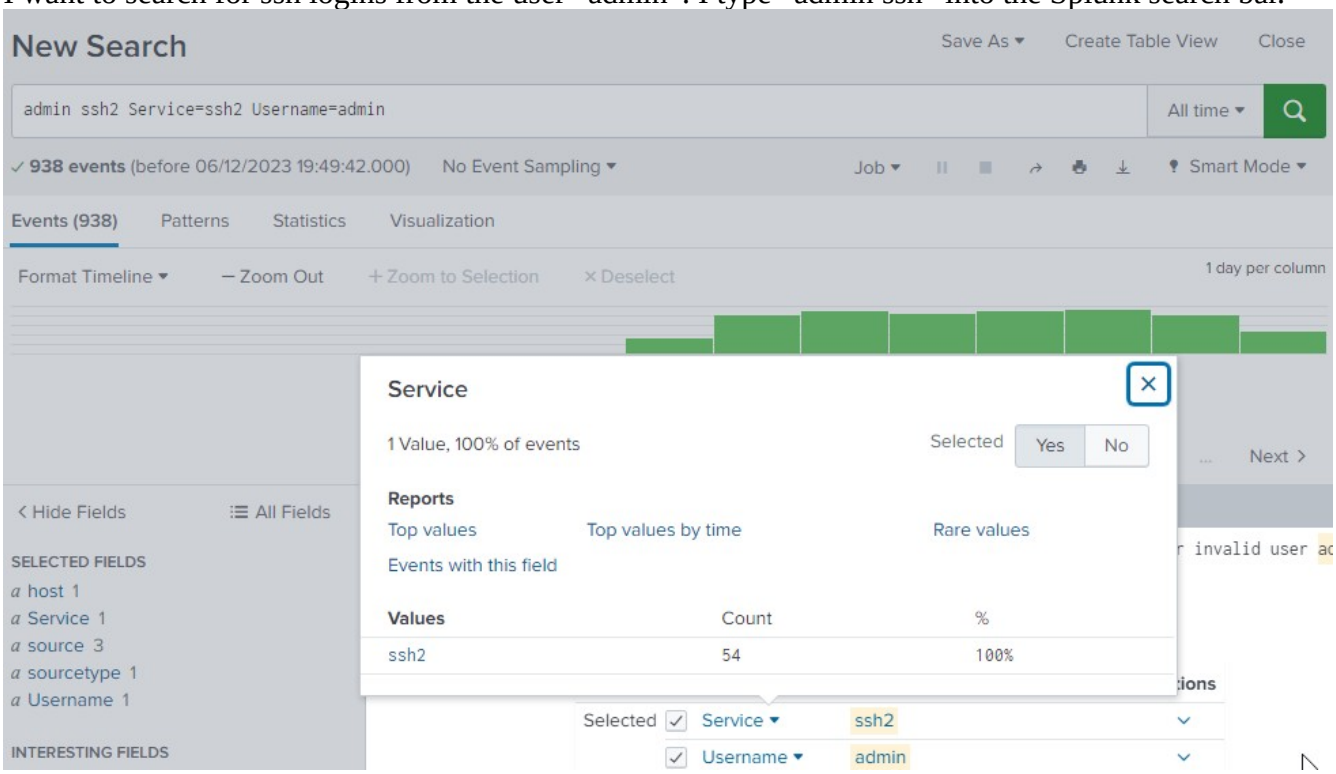
I choose space as the delimiter and proceed to rename useful fields.

Performing a Search



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

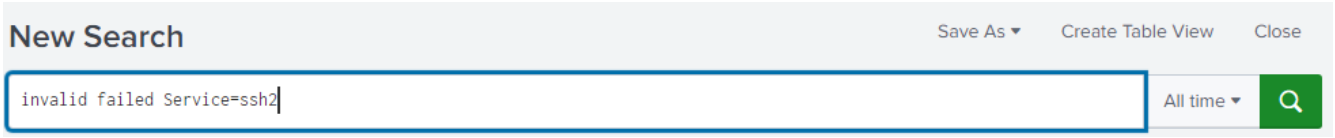
I want to search for ssh logins from the user “admin”. I type “admin ssh” into the Splunk search bar.



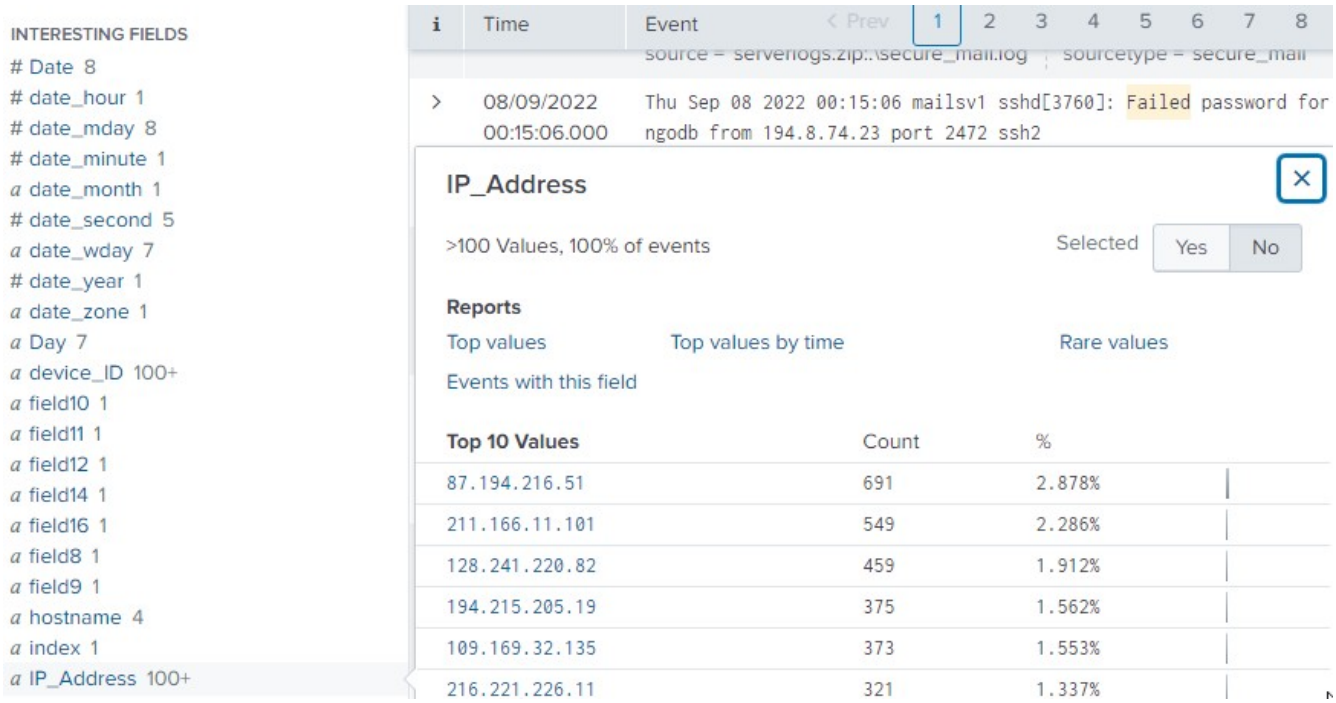
I open one of the logs and select fields of interest. I click a field and choose an element of interest, such as the service ssh2 in this case. This updates the search bar in Splunk to include the phrase “Service=ssh2”.

<u>Identifying field elements with the most number of logs</u>

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

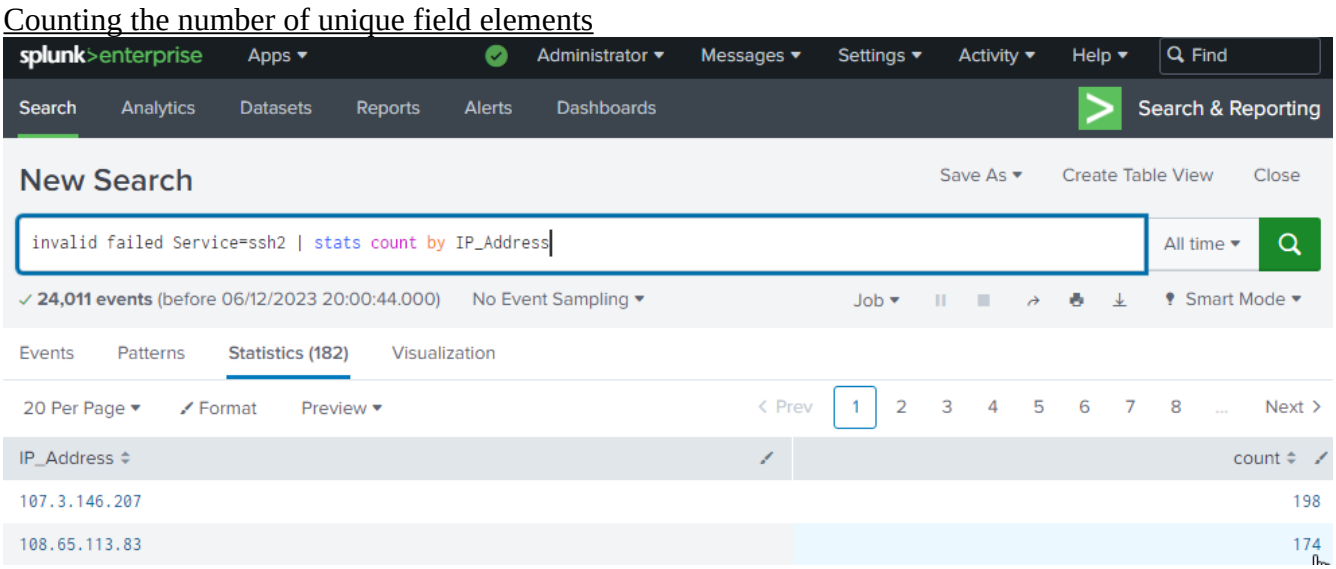


I first perform a search for invalid failed Service=ssh2.

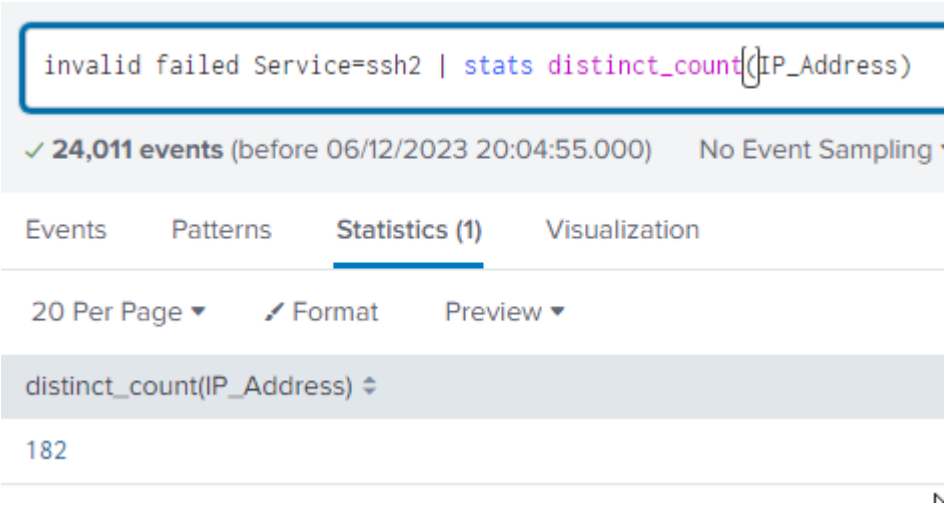


I then select IP_Address from the list of interesting fields. Splunk automatically identifies the top 10 IP addresses.

<u>Counting the number of unique field elements</u>

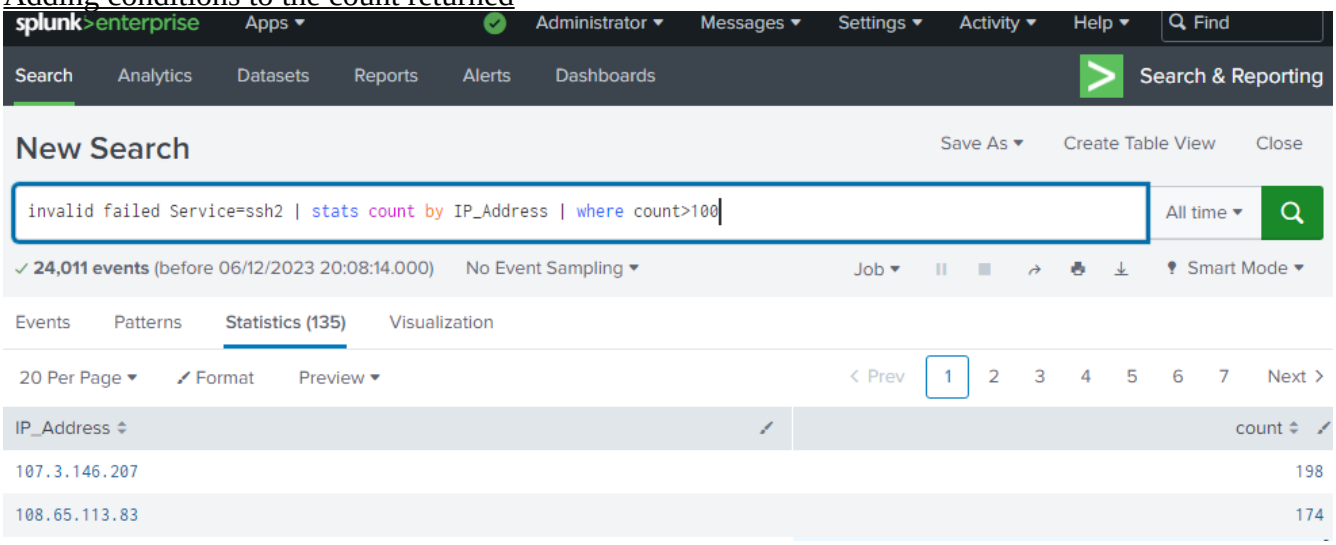


I want to know the number of unique IP addresses that have attempted to login via ssh but failed to do so due to having invalid usernames. I enter “invalid failed Service=ssh2 | stats count by IP_Address” into the search bar and run a Splunk search. The results show that there are 182 unique IP addresses,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



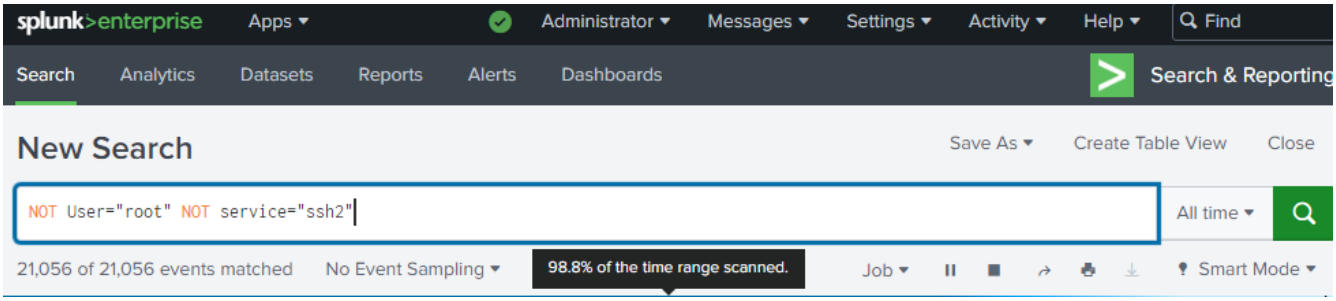
Another way to count the number of unique IP addresses is to conduct a search for “invalid failed Service=ssh2 | stats distinct_count(IP_Address)”. The result returned is also 182.

Adding conditions to the count returned



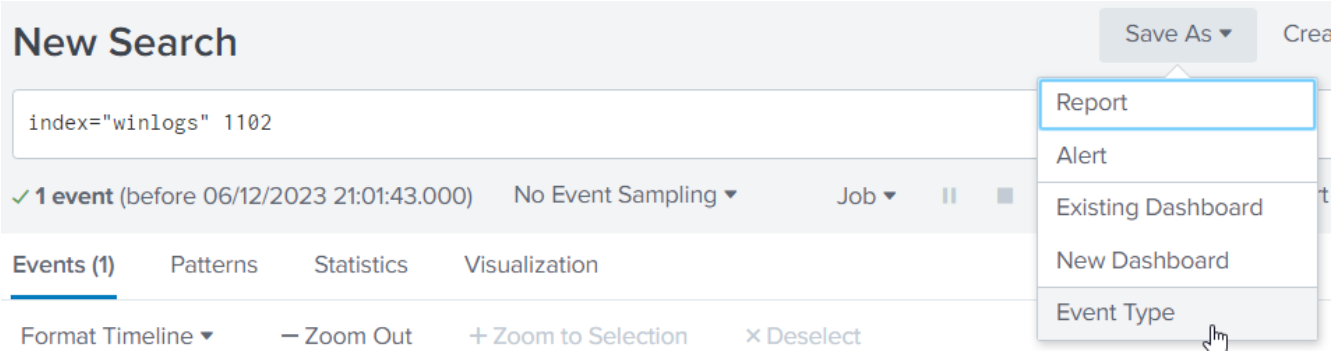
I add the phrase “| where count > 100” to select only the IP addresses that have at least 100 invalid username failed attempts.

Excluding Search Terms

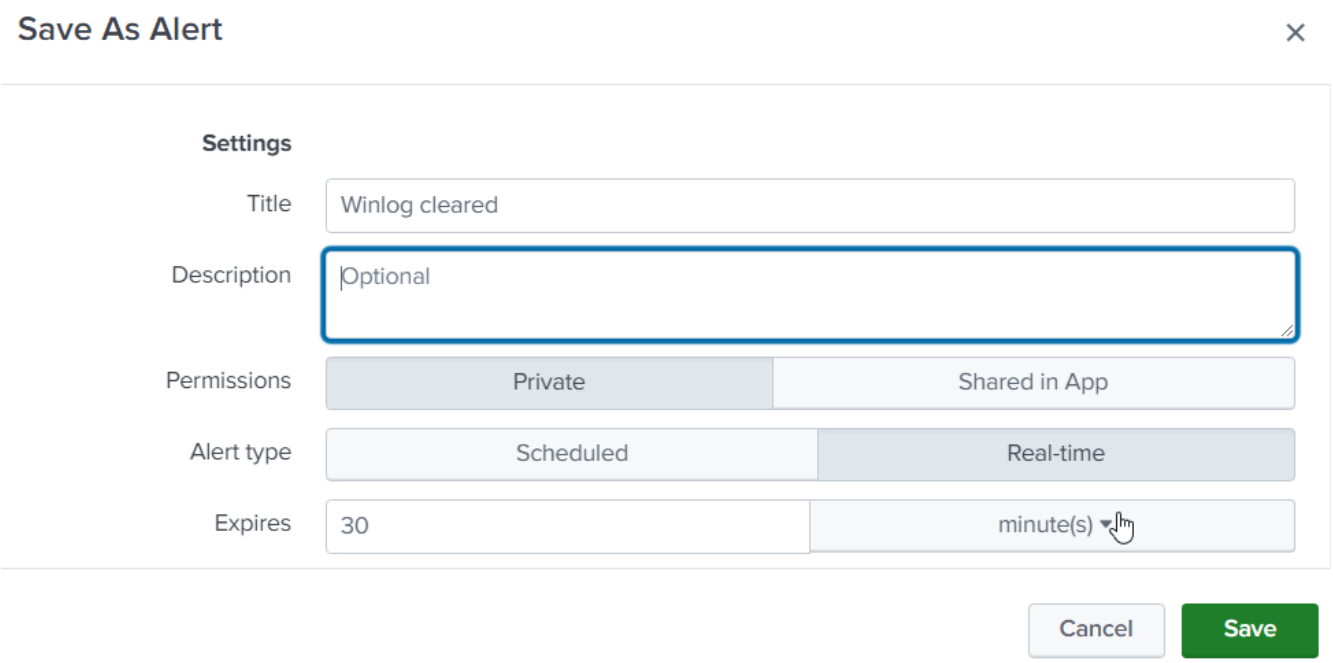


I use the NOT keyword to exclude terms from search results.

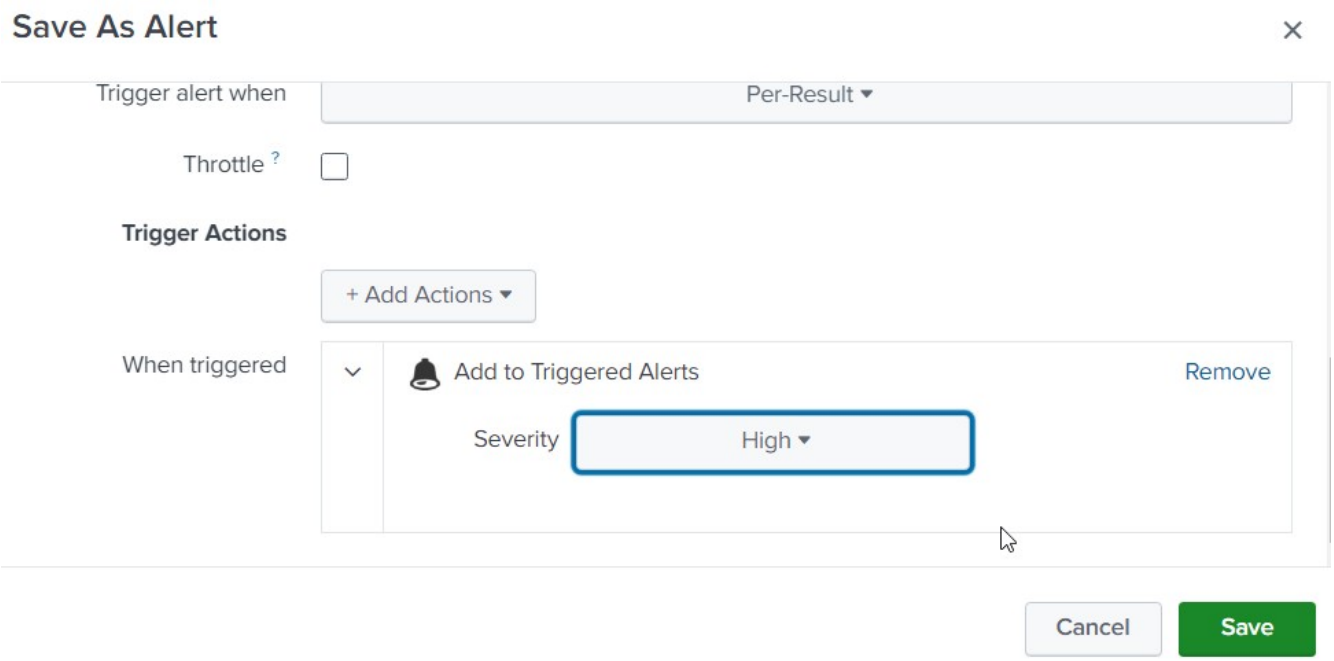
Creating an Alert



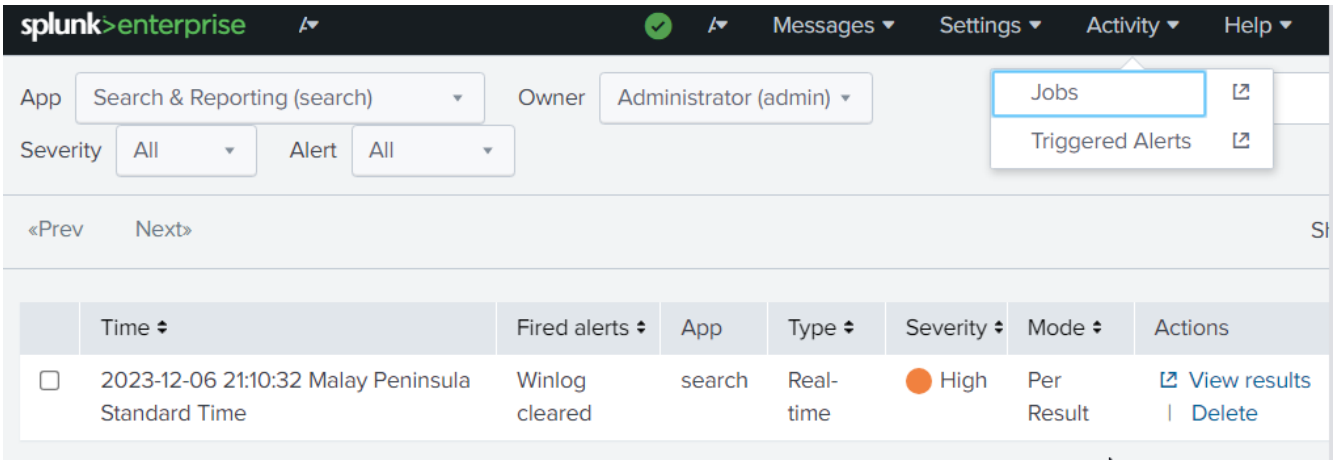
I enter a search term, here: index=”winlogs” 1102, and select “Save As” and “Alert” to create an alert.



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



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

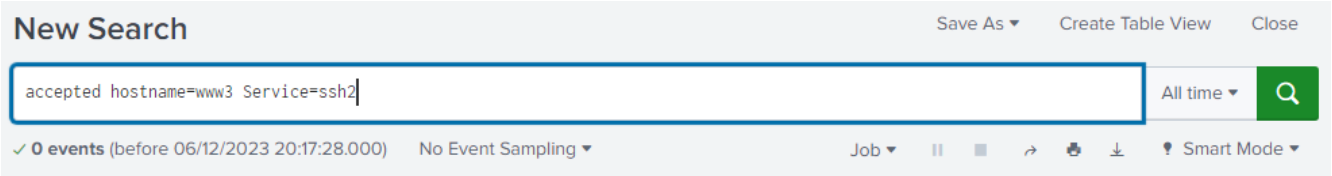


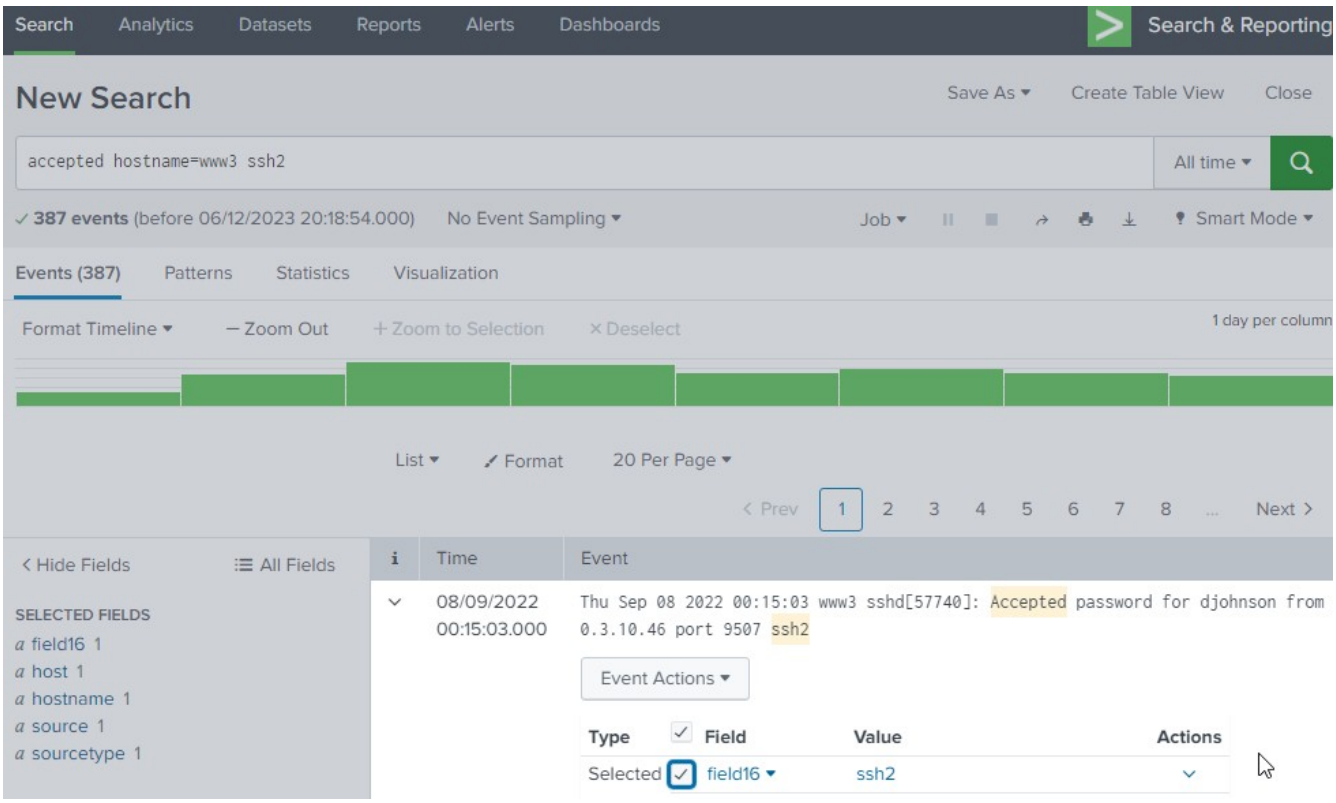
I clear the security event log again and view the triggered alert by selecting “Activity” → “Triggered Alerts”.

Bug fixes

Faulty field name searches

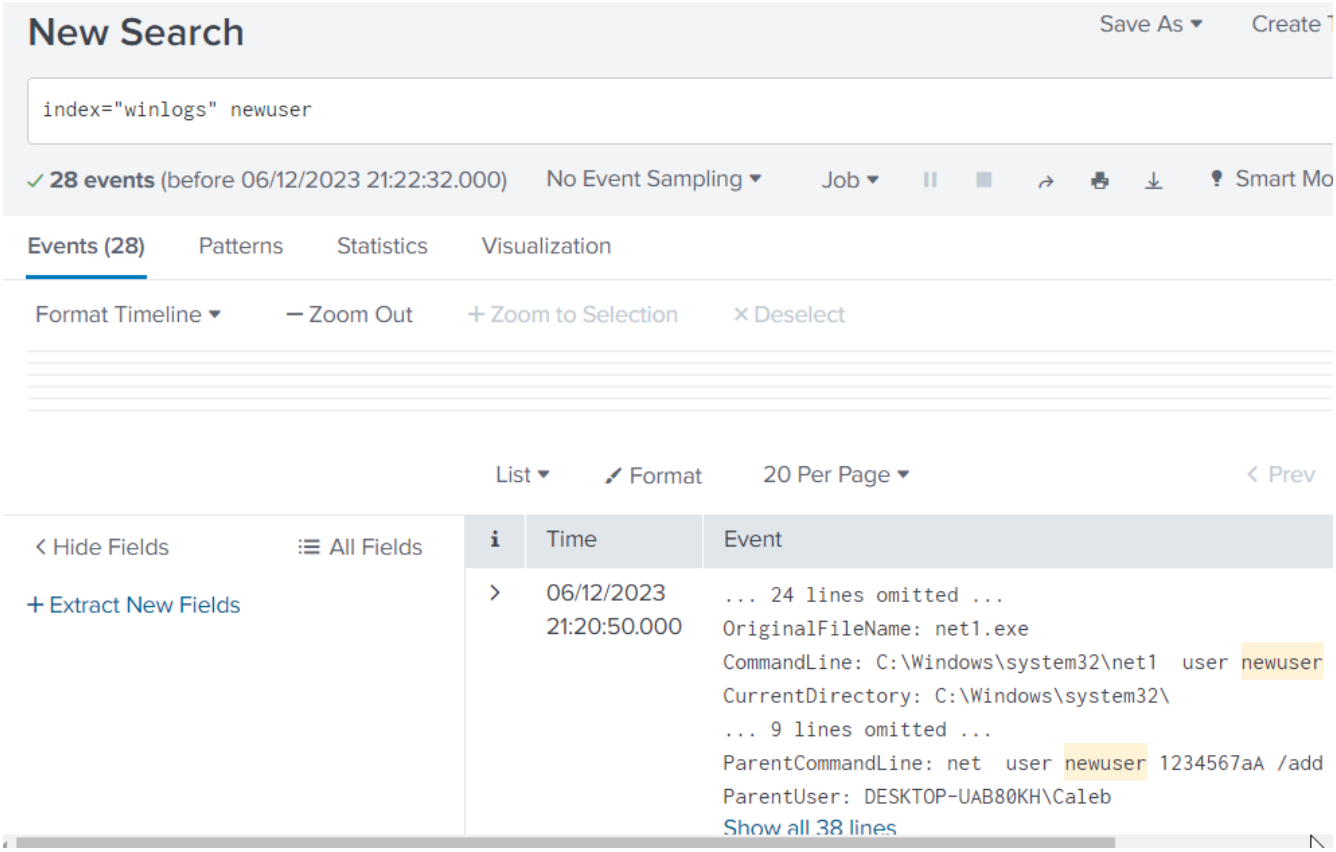
I noticed that the number of search results returned is sometimes 0 when specifying the field name, whereas the same search without the fieldname's name specified returns results.



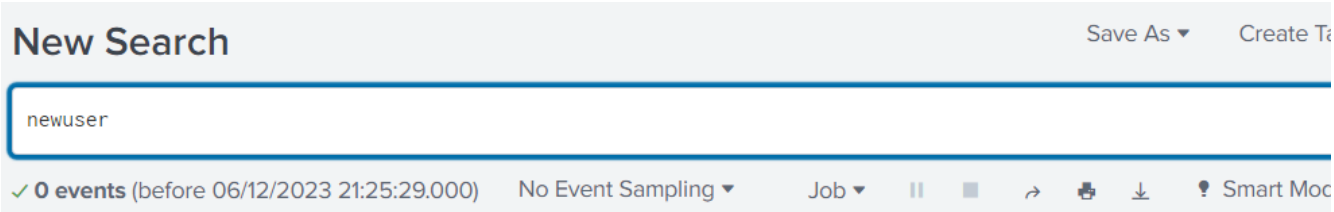


After some debugging, I realized this was due to a differently formatted log entry that had the element "ssh2" named under a different field.

Need to specify index when searching for Windows Logs



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



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

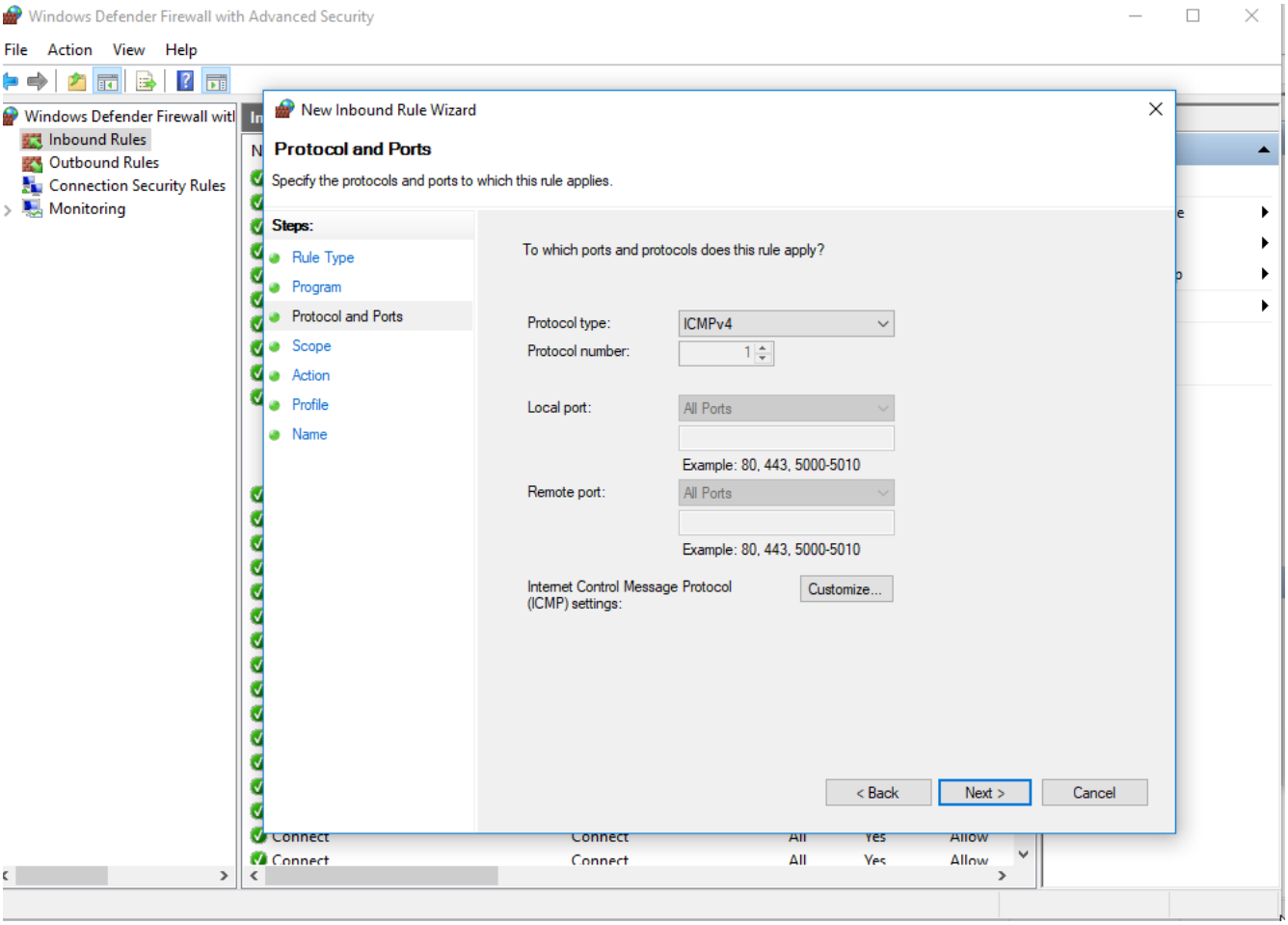
```
Pinging 172.16.50.20 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

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.