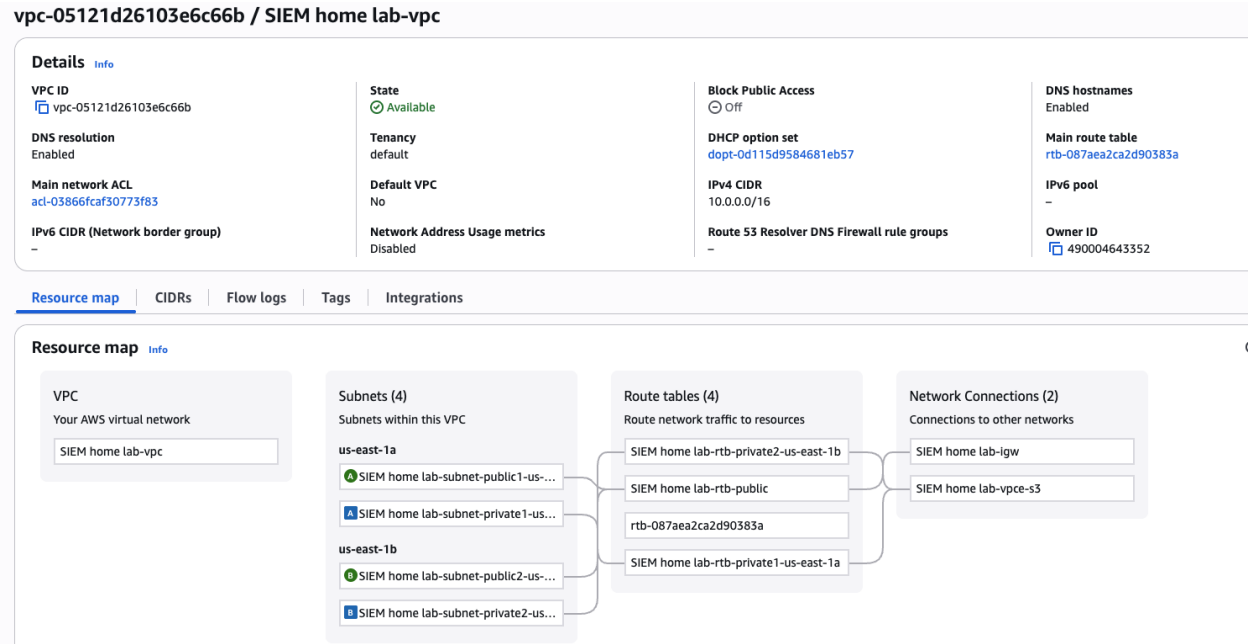
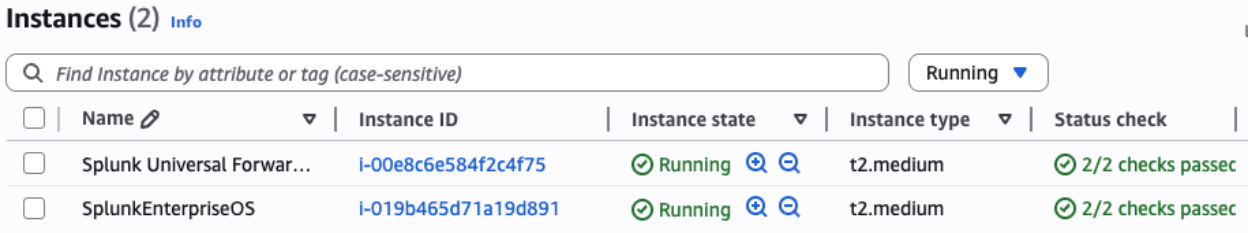
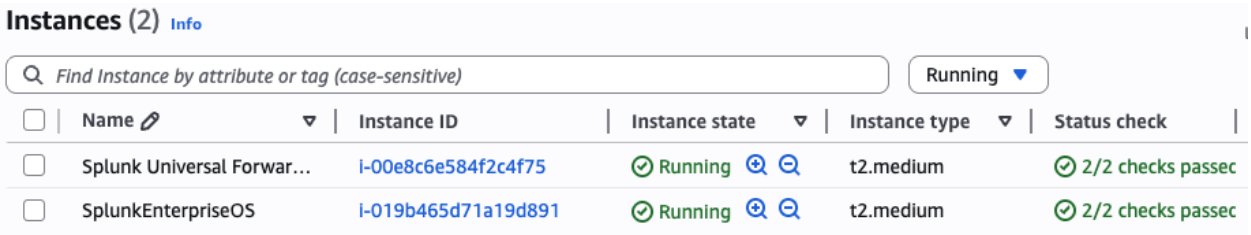
Create an AWS VPC and deploy 2 instances. These VM's will run Splunk and Splunk Forwarder:



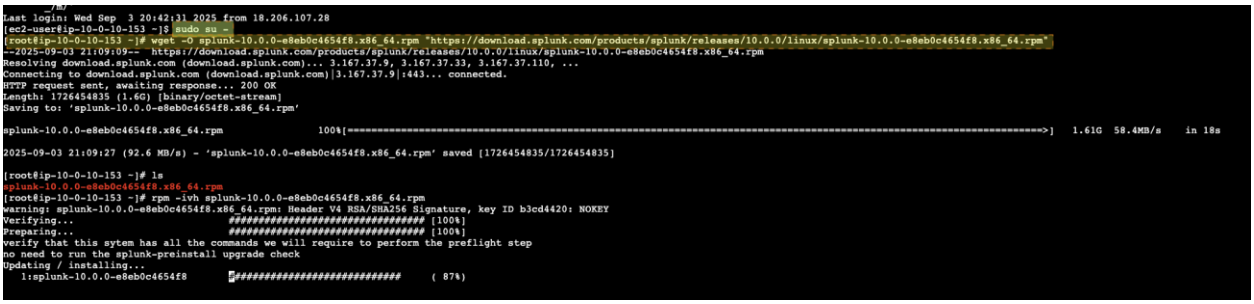


Step 1 – Connect to the Splunk EnterpriseOS VM and download the Splunk Enterprise software.

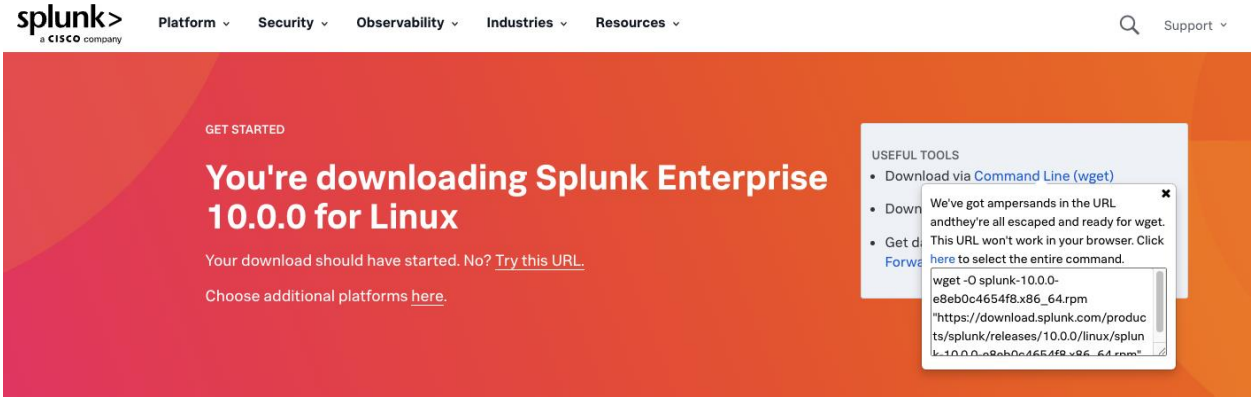


Switch to the root user once connected to the EC2 instance.

sudo su -

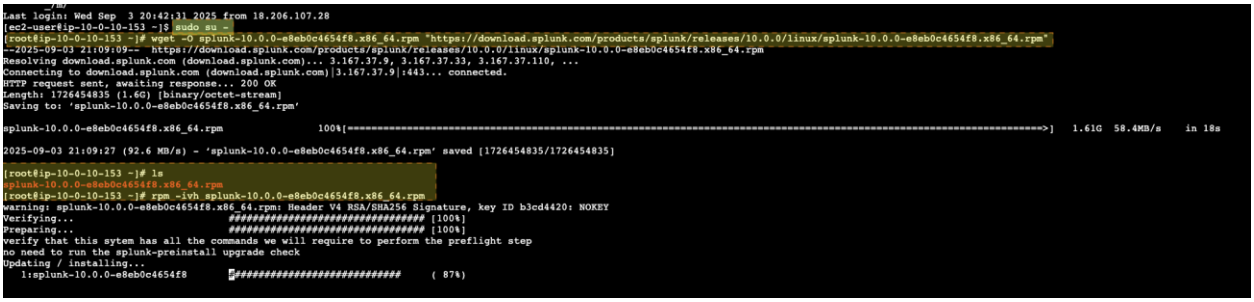


From the Splunk website download Splunk via command line widget by copying and pasting the command. The command will download the Splunk Enterprise packages



Next, we will install the Splunk software using rpm and the -ivh command.

- ls
- rpm -ivh (splunk)



Once installed, we'll need to start Splunk.

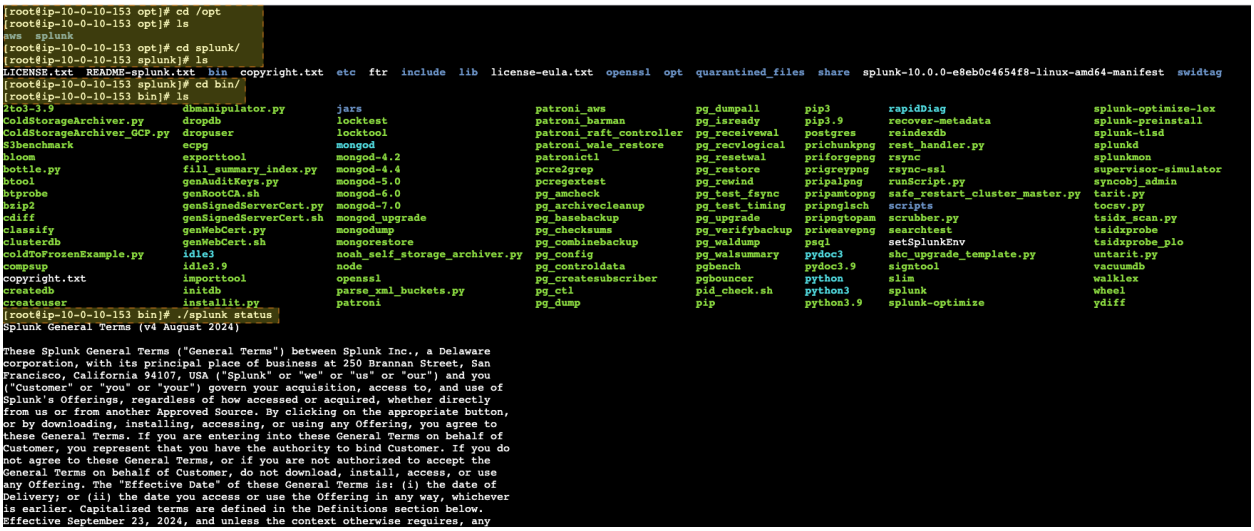
- Move to the splunk folder:
  Cd /opt/
  Ls
  Cd splunk
  ls

- Move to the bin folder and check if Splunk is active:

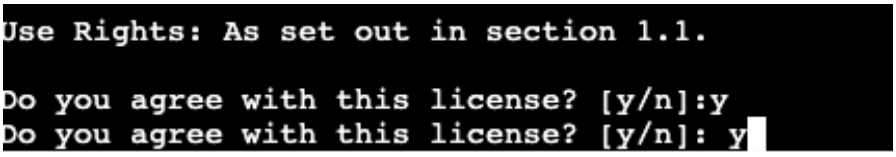
Cd bin/

ls

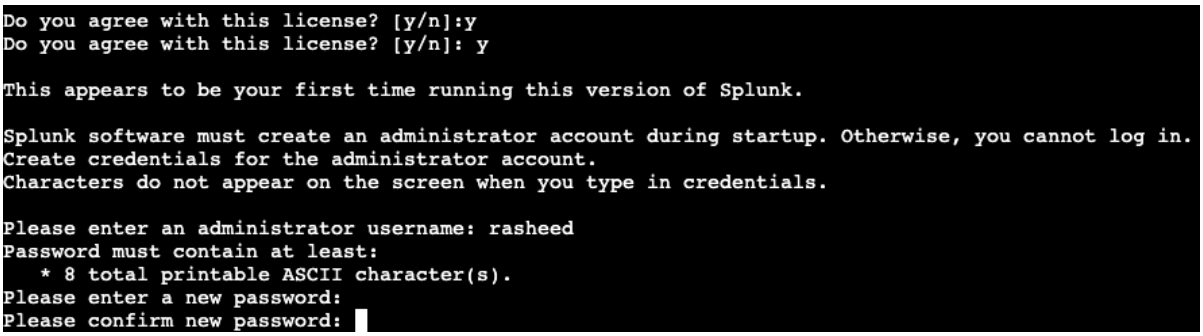
./splunk status (status command)



Next - Reply Y to the license agreement: y



Then - Create an Admin username/password:



We can see Splunk is not running. Start Splunk with command:

Start Splunk: ./splunk start

```
Moving '/opt/splunk/share/splunk/search_mrsparkle/modules.new' to '/opt/splunk/share/splunk/search_mrsparkle/modules'.
splunkd is not running.
[root@ip-10-0-10-153 bin]# ./splunk start

Splunk> All batbelt. No tights.

Checking prerequisites...
        Checking http port [8000]: open
        Checking mgmt port [8089]: open
        Checking appserver port [127.0.0.1:8065]: open
        Checking kvstore port [8191]: open
        Checking configuration... Done.
                Creating: /opt/splunk/var/lib/splunk
                Creating: /opt/splunk/var/run/splunk
                Creating: /opt/splunk/var/run/splunk/appserver/i18n
                Creating: /opt/splunk/var/run/splunk/appserver/modules/static/css
                Creating: /opt/splunk/var/run/splunk/upload
                Creating: /opt/splunk/var/run/splunk/search_telemetry
                Creating: /opt/splunk/var/run/splunk/search_log
                Creating: /opt/splunk/var/spool/splunk
                Creating: /opt/splunk/var/spool/dirmoncache
                Creating: /opt/splunk/var/lib/splunk/authDb
                Creating: /opt/splunk/var/lib/splunk/hashDb
                Creating: /opt/splunk/var/run/splunk/collect
                Creating: /opt/splunk/var/run/splunk/sessions
New certs have been generated in '/opt/splunk/etc/auth'.
New certs have been generated in '/opt/splunk/etc/auth'.
        Checking critical directories...        Done
        Checking indexes...
                Validated: _audit _configtracker _dsappevent _dsclient _dsphonehome _internal _introspection _metrics _metrics_rollup _telemetry _thefishbucket history main summary
        Done
        Checking filesystem compatibility...  Done
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunk/splunk-10.0.0-e8eb0c4654f8-linux-amd64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Using configuration from /opt/splunk/share/openssl3/openssl.cnf
....+.++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*....+...+...+.......+...+.........+..+.+...+......+...+......++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Confirm Splunk is running: ./splunk status

```
[root@ip-10-0-10-153 bin]# ./splunk status
splunkd is running (PID: 12394).
splunk helpers are running (PIDs: 12399 12565 12590 12673 12674 134978 140738 143062).
[root@ip-10-0-10-153 bin]#
```

Splunk is now Installed and running on the VM. Access Splunk using the instance public IP on port 8000.

Instance summary for i-019b465d71a19d891 (SplunkEnterpriseOS) Info

Updated 3 minutes ago

Instance ID
i-019b465d71a19d891

IPv6 address
–

Hostname type
IP name: ip-10-0-10-153.ec2.internal

Answer private resource DNS name
–

Auto-assigned IP address
44.203.82.76 [Public IP]

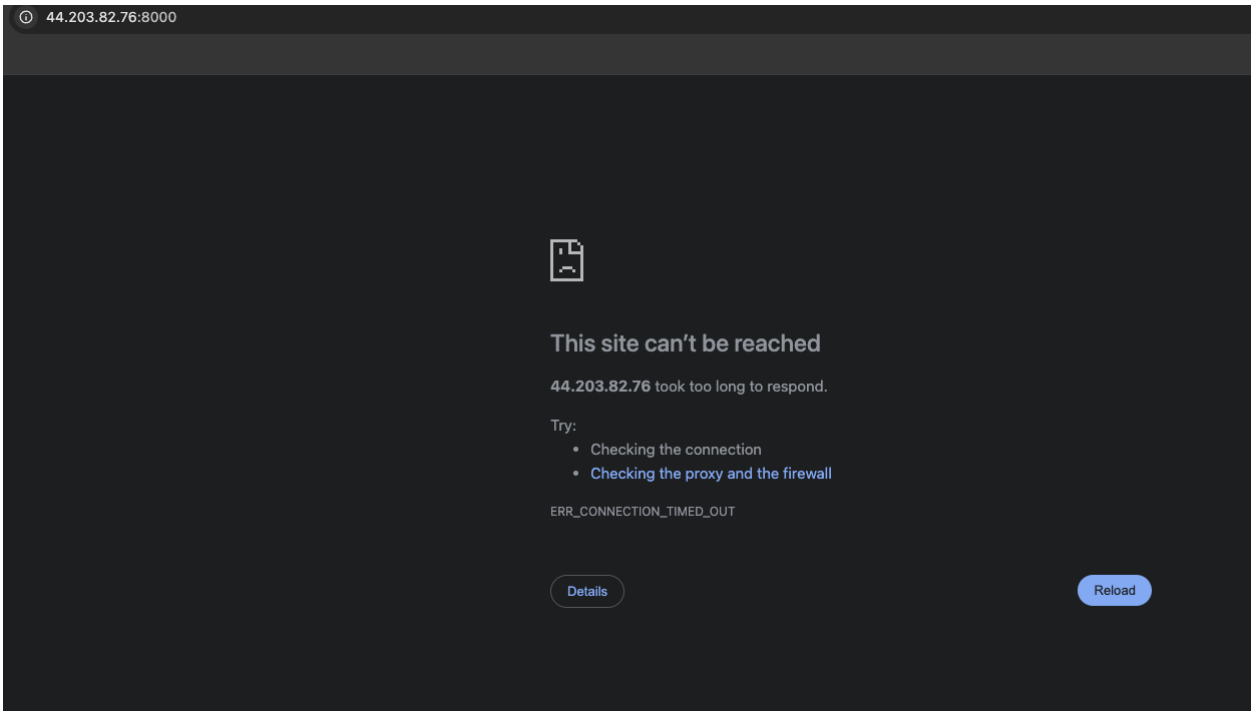
Public IPv4 address
44.203.82.76 | open address

Instance state
Running

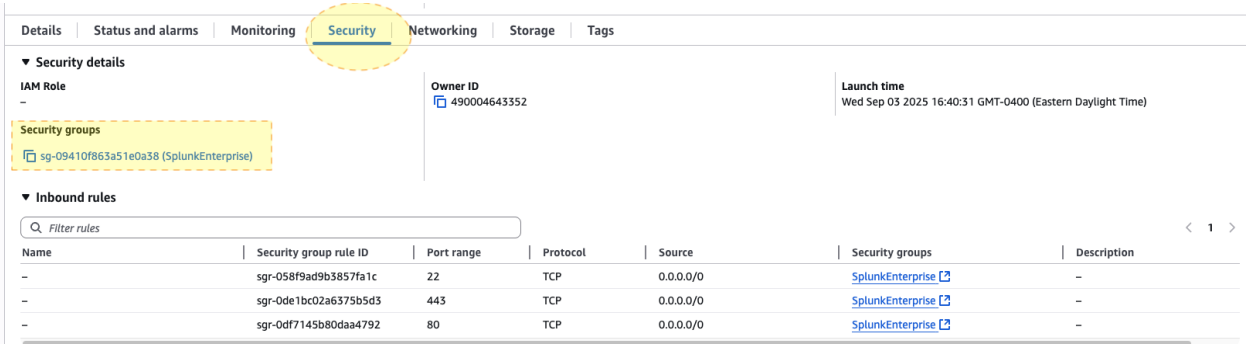
Private IP DNS name (IPv4 only)
ip-10-0-10-153.ec2.internal

Instance type
t2.medium

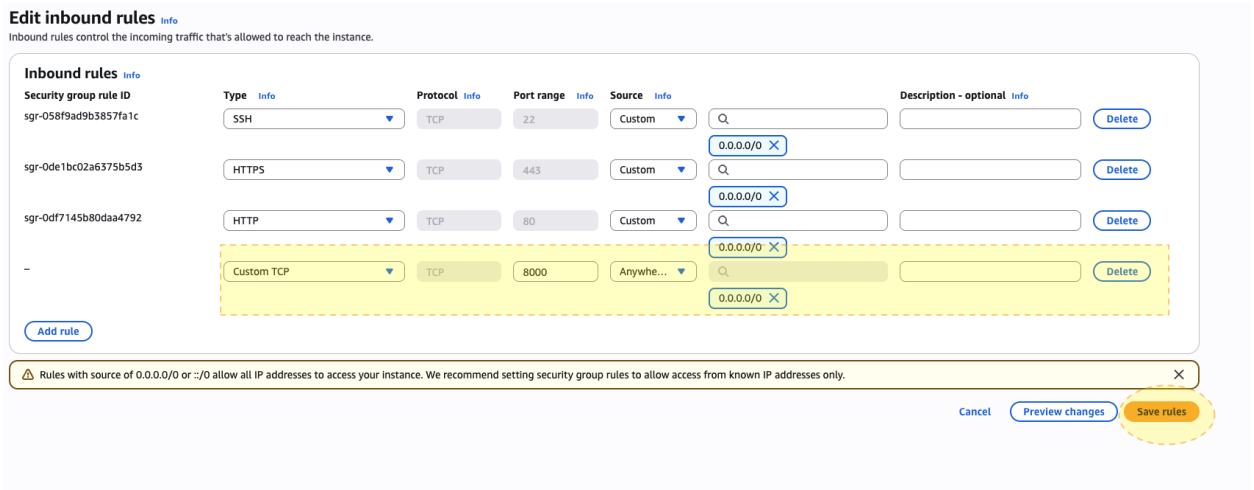
VPC ID
vpc-05121d26103e6c66b (SIEM home lab-vpc)



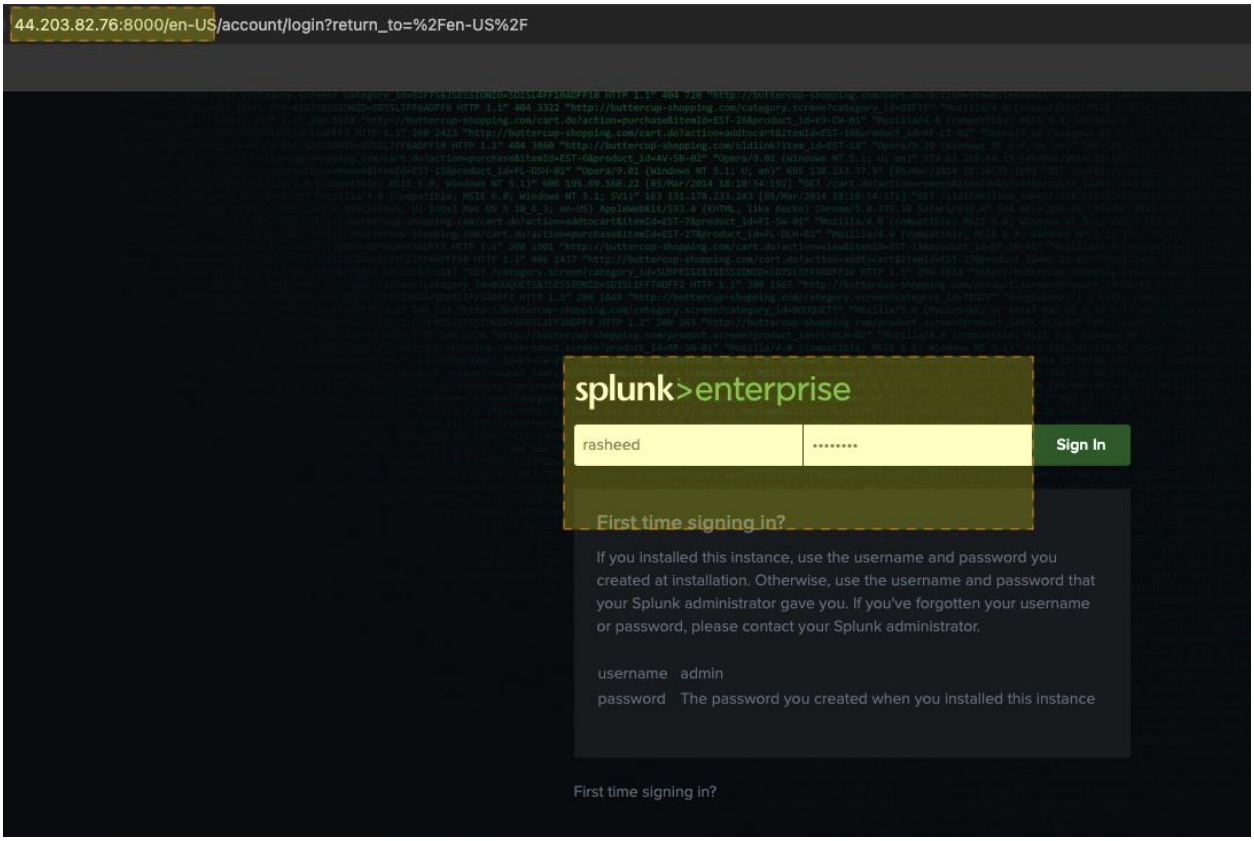
To resolve; check for appropriate traffic on the instance security group.



Edit the security group inbound rule to allow TCP traffic over port 8000 and save rule.

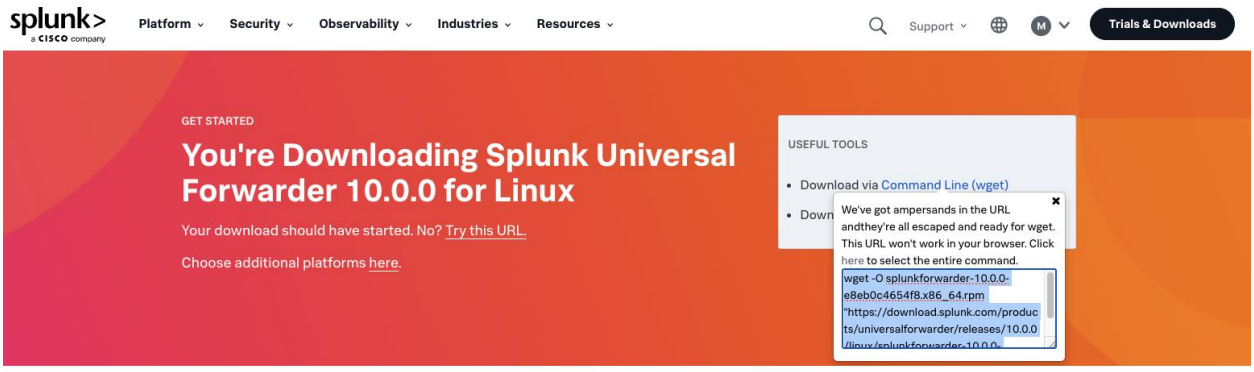


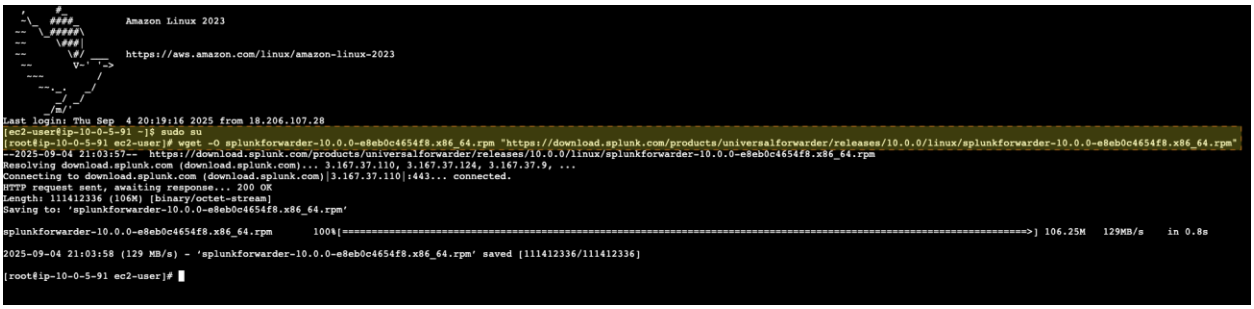
Retry logging into Splunk with the instance public IP (44.203.82.76) over port 8000. Login with created username and password:



Next - Install Splunk Universal Forwarder

- Switch over to the Splunk Universal Forwarder instance and download the Splunk Universal Forwarder file via Command Line (wget) from the Splunk website.





Once RPM file downloads, install with: sudo yum install + RPM File. Response Y when prompted.

```
[root@ip-10-0-5-91 ec2-user]# sudo yum install splunkforwarder-10.0.0-e8eb0c4654f8.x86_64.rpm
Amazon Linux 2023 Kernel Livepatch repository
Dependencies resolved.
================================================================================
 Package                    Architecture                Version
================================================================================
Installing:
 splunkforwarder            x86_64                      10.0.0-e8eb0c4654f8

Transaction Summary
================================================================================
Install  1 Package

Total size: 106 M
Installed size: 242 M
Is this ok [y/N]: y
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :
  Running scriptlet: splunkforwarder-10.0.0-e8eb0c4654f8.x86_64
verify that this sytem has all the commands we will require to perform the preflight step
no need to run the splunk-preinstall upgrade check

  Installing       : splunkforwarder-10.0.0-e8eb0c4654f8.x86_64
  Running scriptlet: splunkforwarder-10.0.0-e8eb0c4654f8.x86_64
find: '/opt/splunkforwarder/lib/python3.7/site-packages': No such file or directory
find: '/opt/splunkforwarder/lib/python3.9/site-packages': No such file or directory
complete

  Verifying        : splunkforwarder-10.0.0-e8eb0c4654f8.x86_64

Installed:
  splunkforwarder-10.0.0-e8eb0c4654f8.x86_64

Complete!
[root@ip-10-0-5-91 ec2-user]#
```

Once installed, Run the forwarder.

Switch to the Splunk forwarder bin directory then start the forwarder. commands used:

Cd /opt/splunkforwarder/bin

./splunk start

```
Installed:
  splunkforwarder-10.0.0-e8eb0c4654f8.x86_64

Complete!
[root@ip-10-0-5-91 ec2-user]# cd /opt/splunkforwarder/bin
[root@ip-10-0-5-91 bin]# ./splunk start
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Splunk General Terms (v4 August 2024)

These Splunk General Terms ("General Terms") between Splunk Inc., a Delaware
corporation, with its principal place of business at 250 Brannan Street, San
Francisco, California 94107, USA ("Splunk" or "we" or "us" or "our") and you
("Customer" or "you" or "your") govern your acquisition, access to, and use of
Splunk's Offerings, regardless of how accessed or acquired, whether directly
from us or from another Approved Source. By clicking on the appropriate button,
or by downloading, installing, accessing, or using any Offering, you agree to
these General Terms. If you are entering into these General Terms on behalf of
Customer, you represent that you have the authority to bind Customer. If you do
not agree to these General Terms, or if you are not authorized to accept the
General Terms on behalf of Customer, do not download, install, access, or use
any Offering. The "Effective Date" of these General Terms is: (i) the date of
Delivery; or (ii) the date you access or use the Offering in any way, whichever
is earlier. Capitalized terms are defined in the Definitions section below.
Effective September 23, 2024, and unless the context otherwise requires, any
reference in these General Terms to "Splunk Inc.", "Splunk", "we", "us" or "our
will be deemed to refer to "Splunk LLC".

1. Your Use Rights and Limits

1.1. Your Use Rights. We grant you a non-exclusive, worldwide, non-transferable
```

Login with credentials:

```
Please enter an administrator username: rasheed
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Creating unit file...
Important: splunk will start under systemd as user: splunkfwd
The unit file has been created.


Splunk> Finding your faults, just like mom.

Checking prerequisites...
        Checking mgmt port [8089]: open
                Creating: /opt/splunkforwarder/var/lib/splunk
                Creating: /opt/splunkforwarder/var/run/splunk
                Creating: /opt/splunkforwarder/var/run/splunk/appserver/i18n
                Creating: /opt/splunkforwarder/var/run/splunk/appserver/modules/static/css
                Creating: /opt/splunkforwarder/var/run/splunk/upload
                Creating: /opt/splunkforwarder/var/run/splunk/search_telemetry
                Creating: /opt/splunkforwarder/var/run/splunk/search_log
                Creating: /opt/splunkforwarder/var/spool/splunk
                Creating: /opt/splunkforwarder/var/spool/dirmoncache
                Creating: /opt/splunkforwarder/var/lib/splunk/authDb
                Creating: /opt/splunkforwarder/var/lib/splunk/hashDb
                Creating: /opt/splunkforwarder/var/run/splunk/collect
                Creating: /opt/splunkforwarder/var/run/splunk/sessions
New certs have been generated in '/opt/splunkforwarder/etc/auth'.
New certs have been generated in '/opt/splunkforwarder/etc/auth'.
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-10.0.0-e8eb0c4654f8-linux-amd64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done
                                                           [  OK  ]
[root@ip-10-0-5-91 bin]#
```

Splunk Univseral Forwarder is now installed and running.

Configure the forwarder to send log data to the Splunk EnterpriseOS server.

We will add the Splunk EnterpriseOS as the forwarder using the public IP address of the (44.203.82.76) over port 9997. Commands used:

./splunk add forward-server {public IP address}:9997

```
[root@ip-10-0-5-91 bin]# ./splunk add forward-server 44.203.82.76:9997
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added forwarding to: 44.203.82.76:9997.
[root@ip-10-0-5-91 bin]#
```

The Splunk Universal Forwarder server is now forwarding to the Splunk EnterpriseOS server. Next, we'll set up monitoring.

Setting Up Monitoring:

Setting a monitor to look in the var/log directory and restart. Commands used:

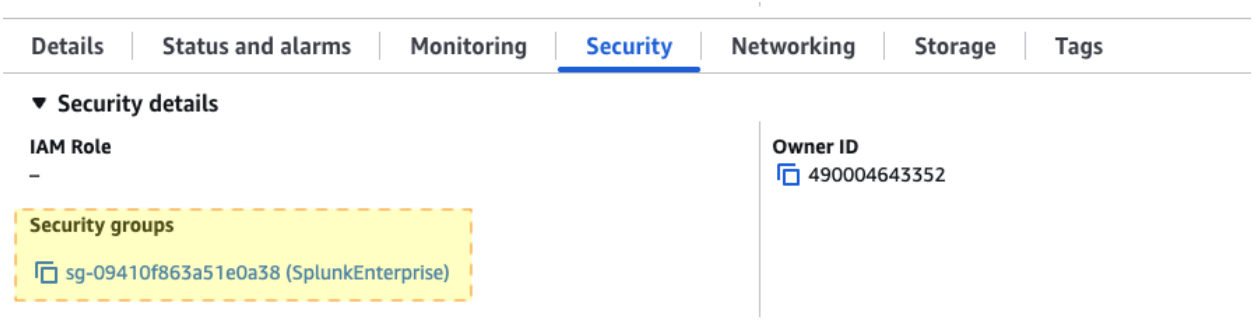
./splunk add monitor /var/log | ./splunk restart

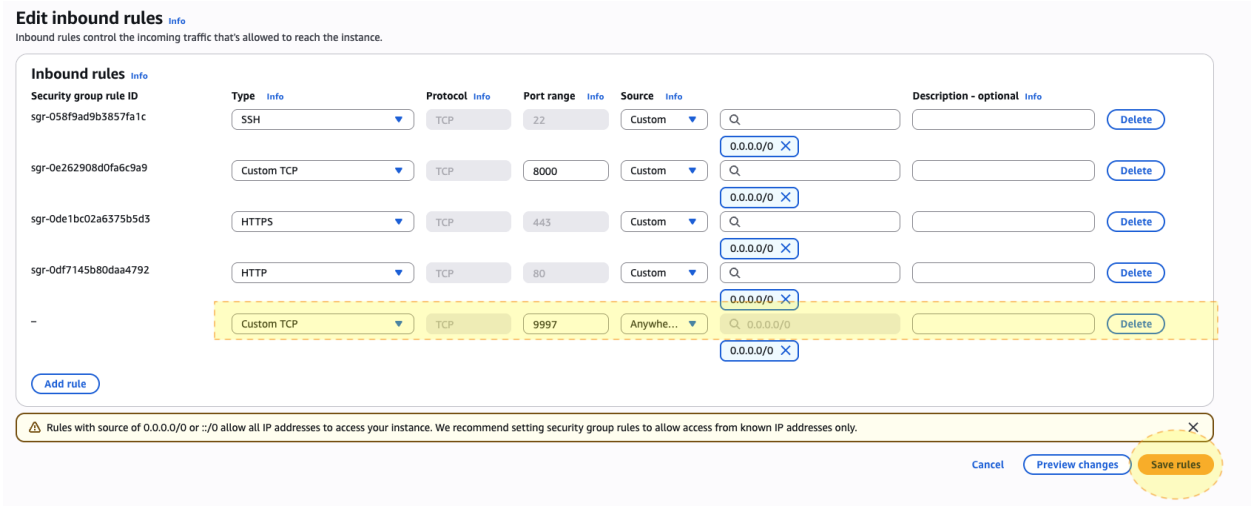
```
[root@ip-10-0-5-91 bin]# ./splunk add forward-server 44.203.82.76:9997
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added forwarding to: 44.203.82.76:9997.
[root@ip-10-0-5-91 bin]# ./splunk add monitor /var/log
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added monitor of '/var/log'.
[root@ip-10-0-5-91 bin]# ./splunk restart
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.
```

Next, go to the Splunk EneterpriseOS server and remote in. Change into the server's bin directory. Commands used:
Sudo bash | cd /opt/splunk/bin | ./splunk enable listen 9997

```
  ,     #_
  ~\_  ####_        Amazon Linux 2023
 ~~  \_#####\
 ~~     \###|
 ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
  ~~       V~' '->
   ~~~         /
     ~~._.   _/
        _/ _/
      _/m/'
Last login: Thu Sep  4 19:35:22 2025 from 18.206.107.28
[ec2-user@ip-10-0-10-153 ~]$ sudo bash
[root@ip-10-0-10-153 ec2-user]# cd /opt/splunk/bin
[root@ip-10-0-10-153 bin]# ./splunk enable listen 9997
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Splunk username: rasheed
Password:
Listening for Splunk data on TCP port 9997.
[root@ip-10-0-10-153 bin]#
```

Edit the Splunk EnterpriseOS instance security group to listen traffic over port 9997.

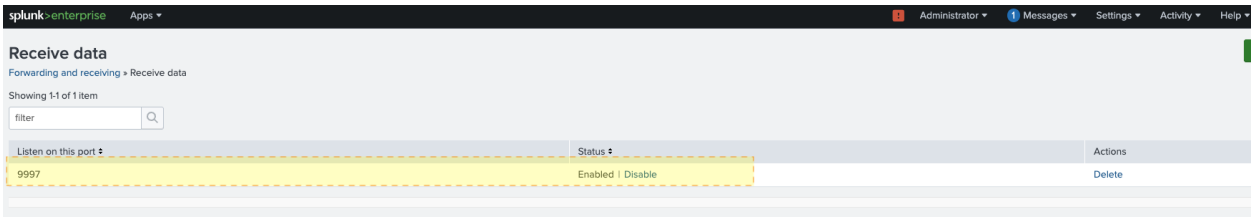




The Spunk Universal Forwarder can now forward and get into the Splunk EnterpriseOS server with data.

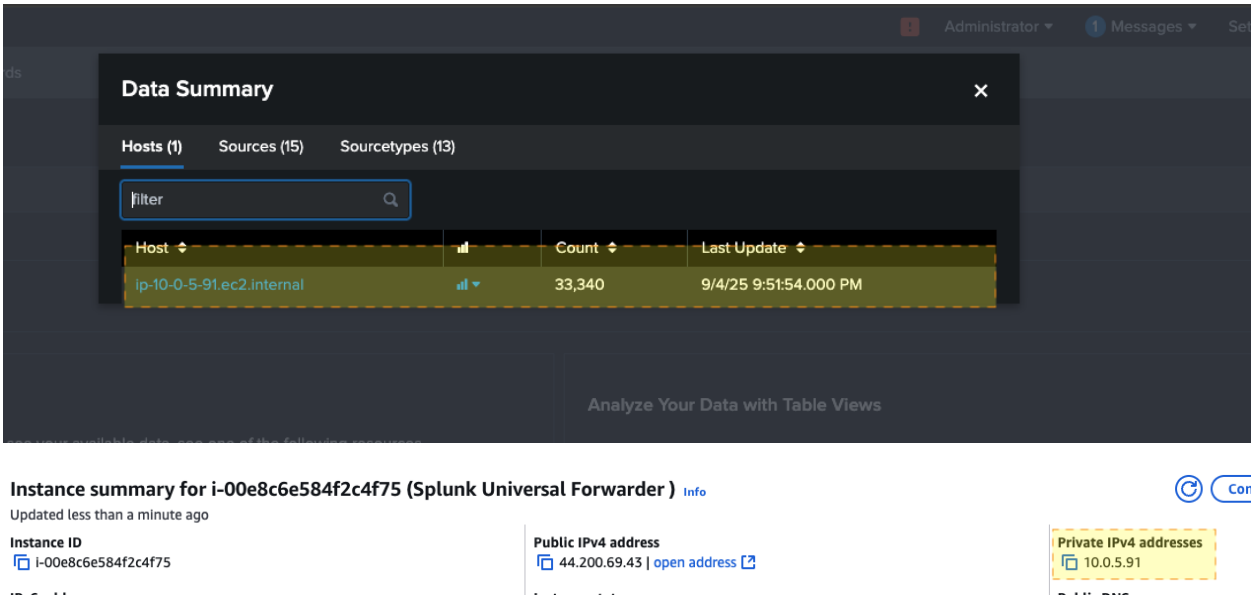
Login Splunk, click on settings -> forwarding and receiving -> configure receiving.

The listening port that was added will be displayed:

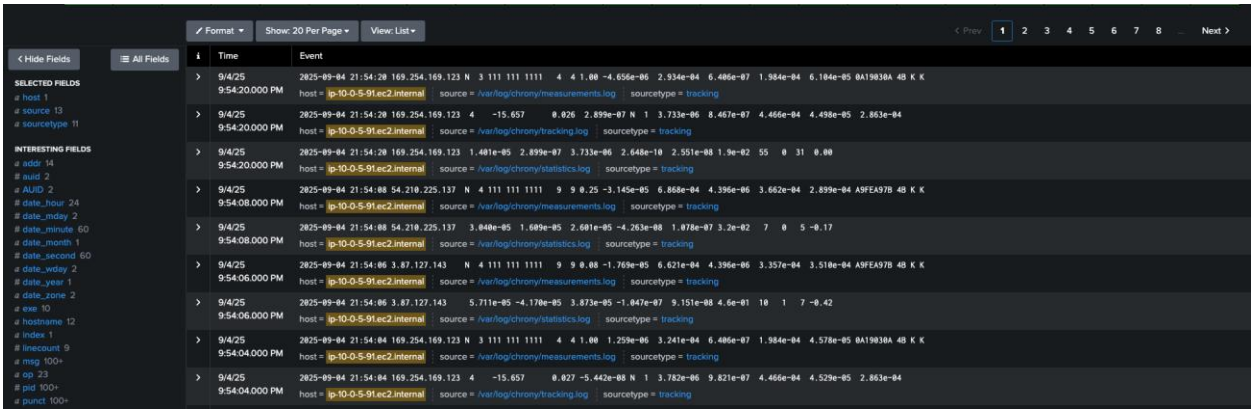


Review the data received from the Splunk Universal Forwarder.

- In the search tab, click on Data Summary to see that data is coming in from the Splunk Universal Forwarder server. Click on IP address to see various data.



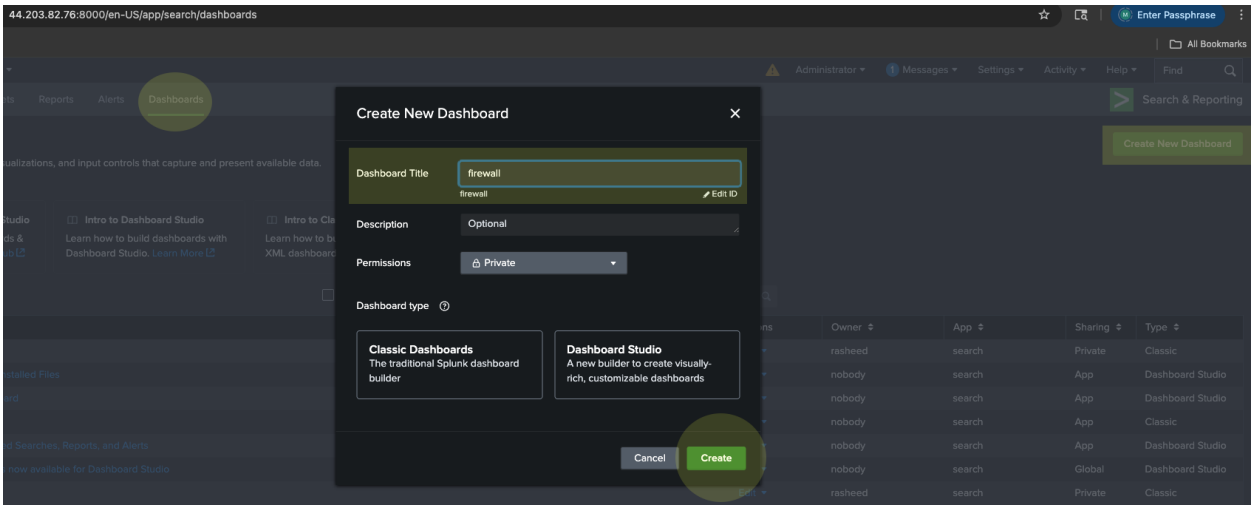
Review Log Data:



Creating dashboards in Splunk with Splunk search commands.

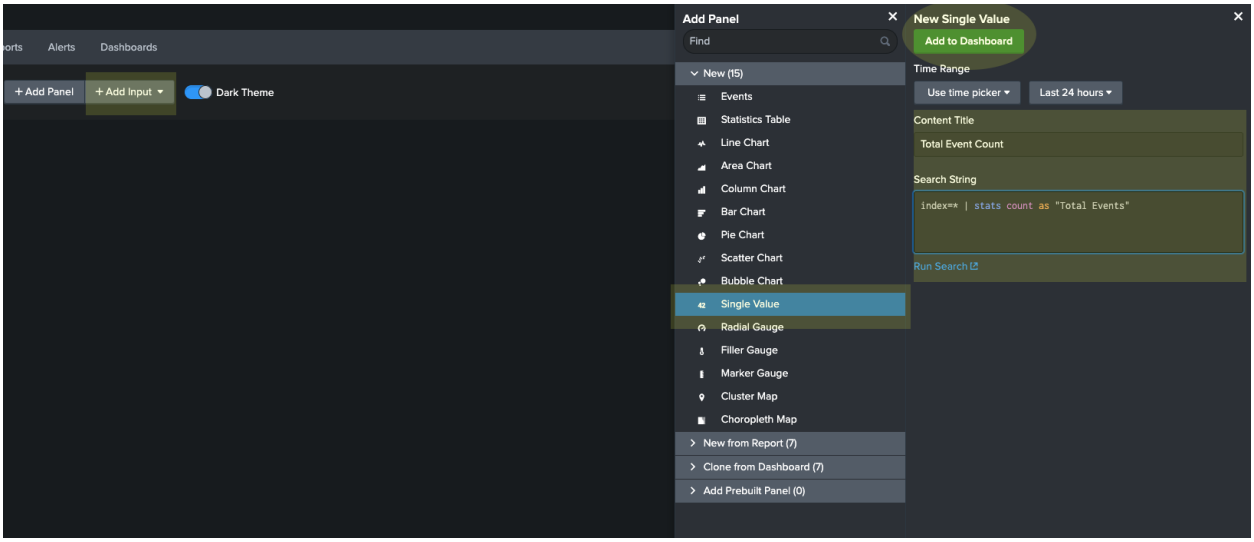
- In Splunk, click the dashboard tab, then create a new dashboard.

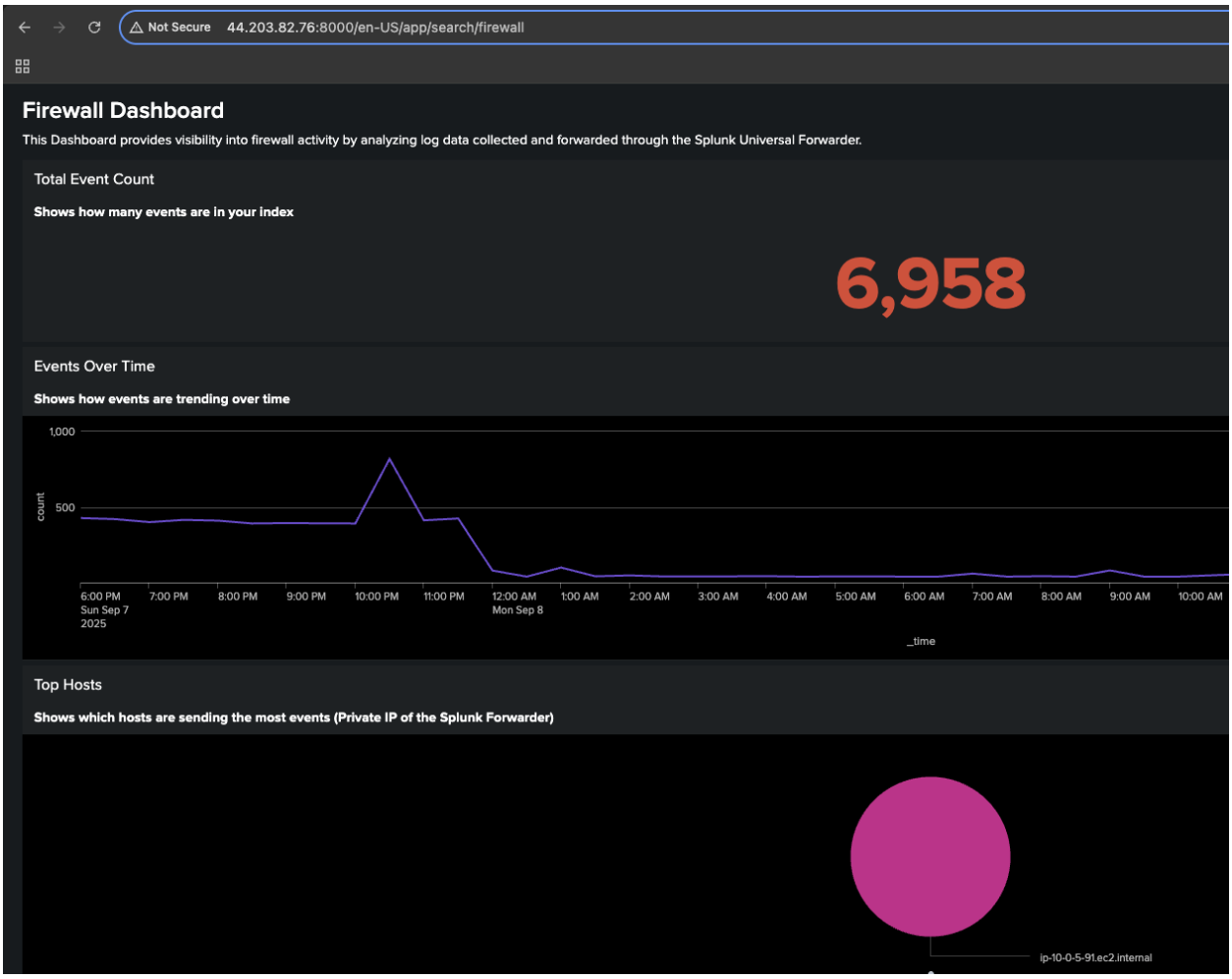
- Created dashboard called firewall:



To show how many events are in your index (DB). Select ‘single value’ for panel and use the following search string:

index=* | stats count as "Total Events"

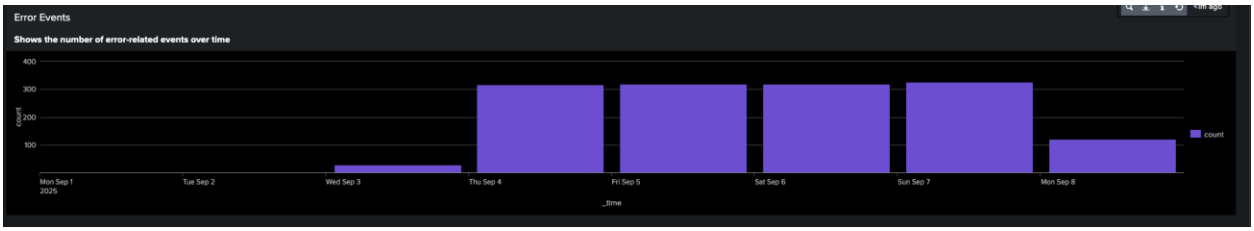




- Events Over Time Dashboard - Shows how events are trending over time.
  Panel used: Line Chart
  Search string - index=* | timechart count

- Top Hosts Dashboard – Shows which hosts are sending the most events:
  Panel used – Pie Chart
  Search string - index=* | top host

- Error Events Dashboard – Shows the number of error-related events over time.
  Panel Used: Column Chart
  Search String: index=* error OR fail | timechart count


Error Events
Shows the number of error-related events over time
400
300
200
100
count
Mon Sep 1
2025
Tue Sep 2
Wed Sep 3
Thu Sep 4
Fri Sep 5
Sat Sep 6
Sun Sep 7
Mon Sep 8
_time
count