

SIEM

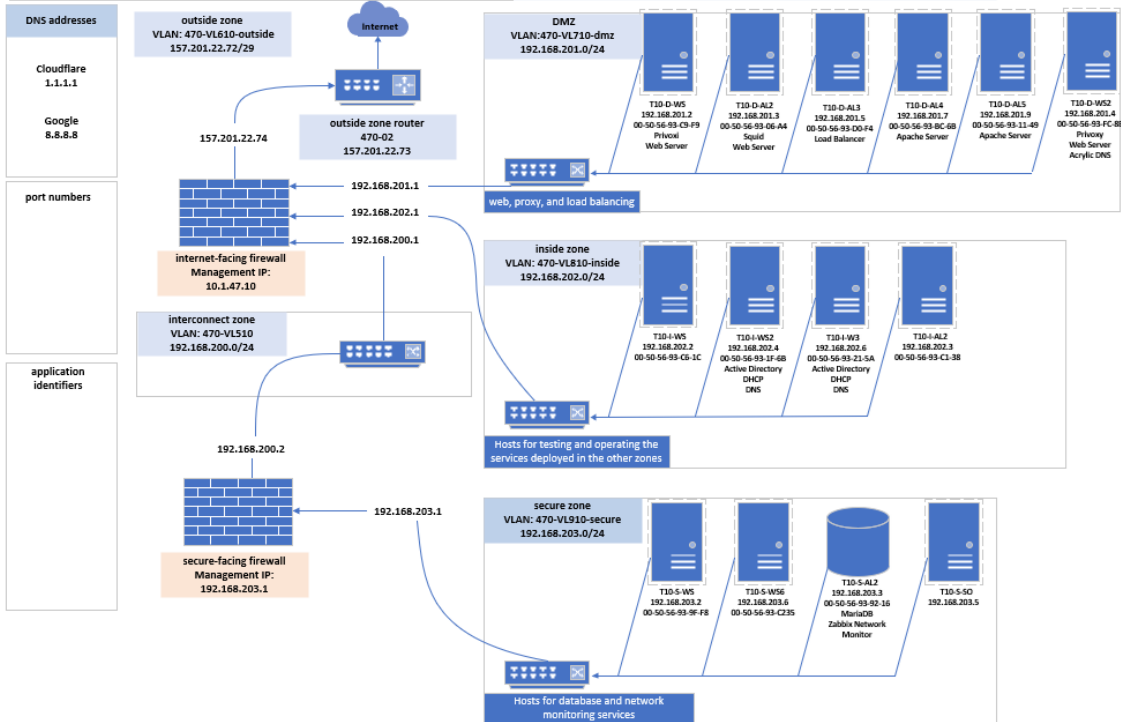
By Christopher Ditto, Carlos Gerez, Mark Riley Slik

cit470

Task: Diagram

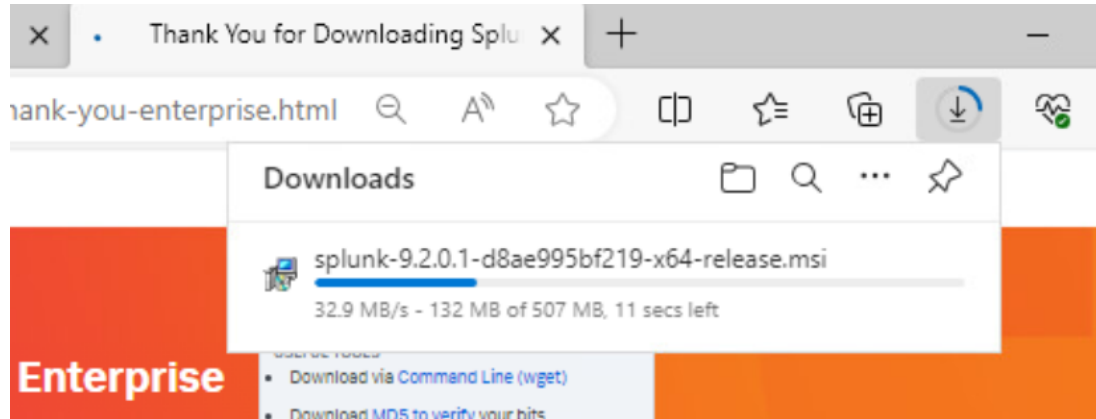
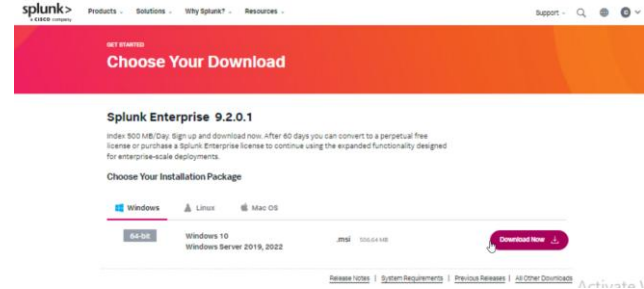
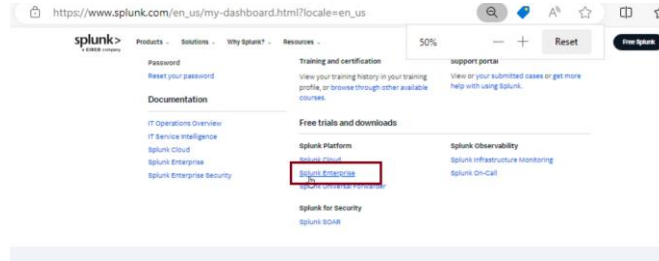
Team 10 Layer 3: outside zones' public IPv4 address assignments

| public space (IPv4 subnet ID) | router | firewall (dynamic NAT) | static NAT | (broadcast) |
|----------------------------------|---------------|--|---------------------------------|---------------|
| 157.201.22.72/29 | 157.201.22.73 | 157.201.22.74 470t10ra.cit.byui.edu | 157.201.22.75- 157.201.22.78 | 157.201.22.79 |



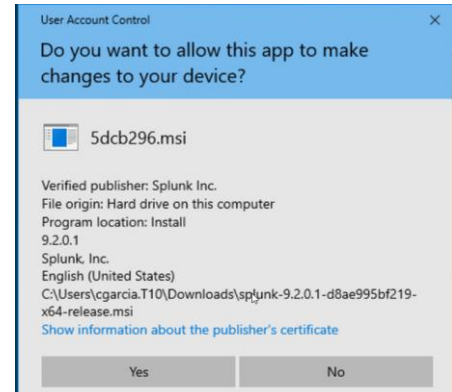
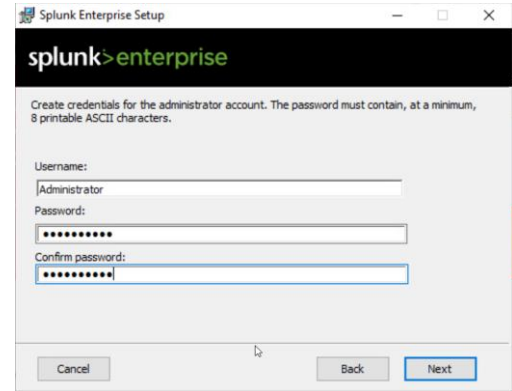
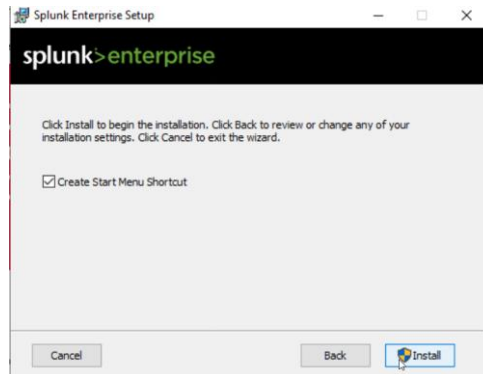
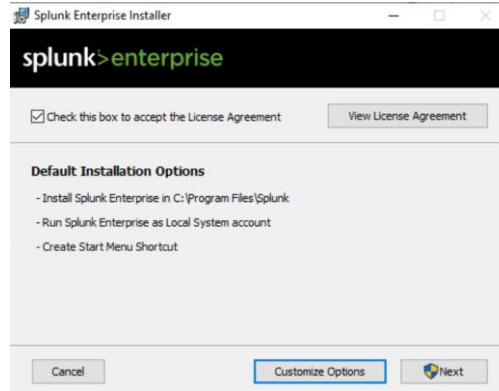
Download Splunk free trial

We need to create an account to use the splunk enterprise software.

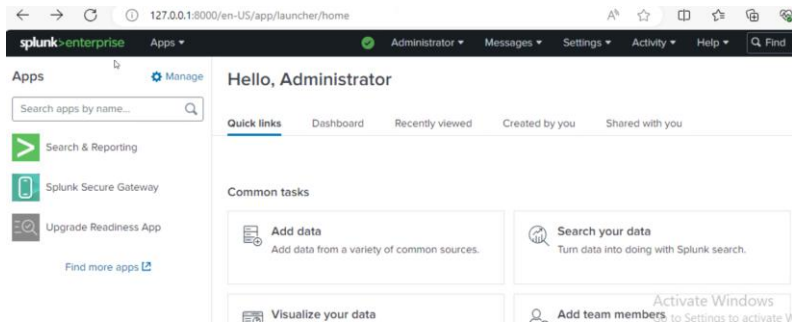
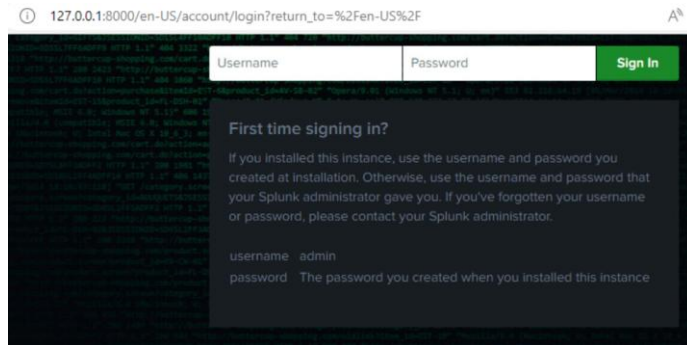
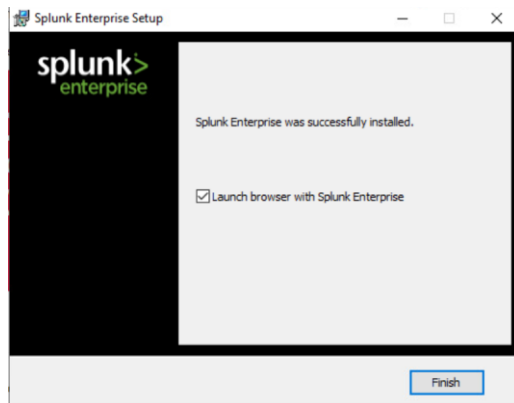


Run the install of splunk and make a user

Follow the guide to install the host, use a username and password. Default installations options will work well.

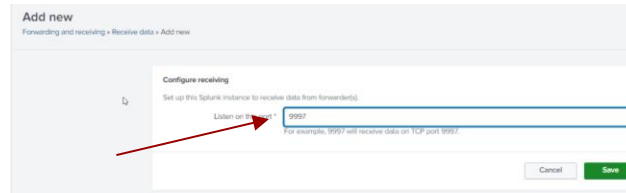
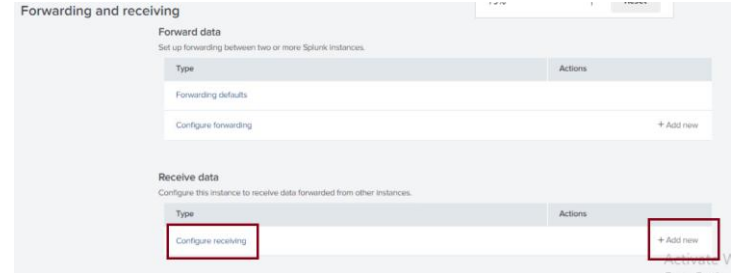
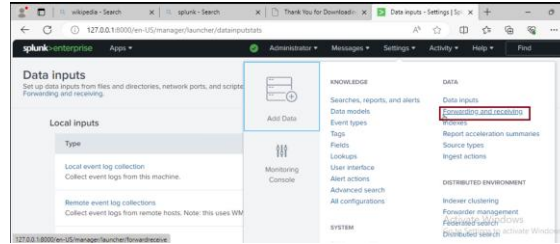


Log in with the username and password you made before.



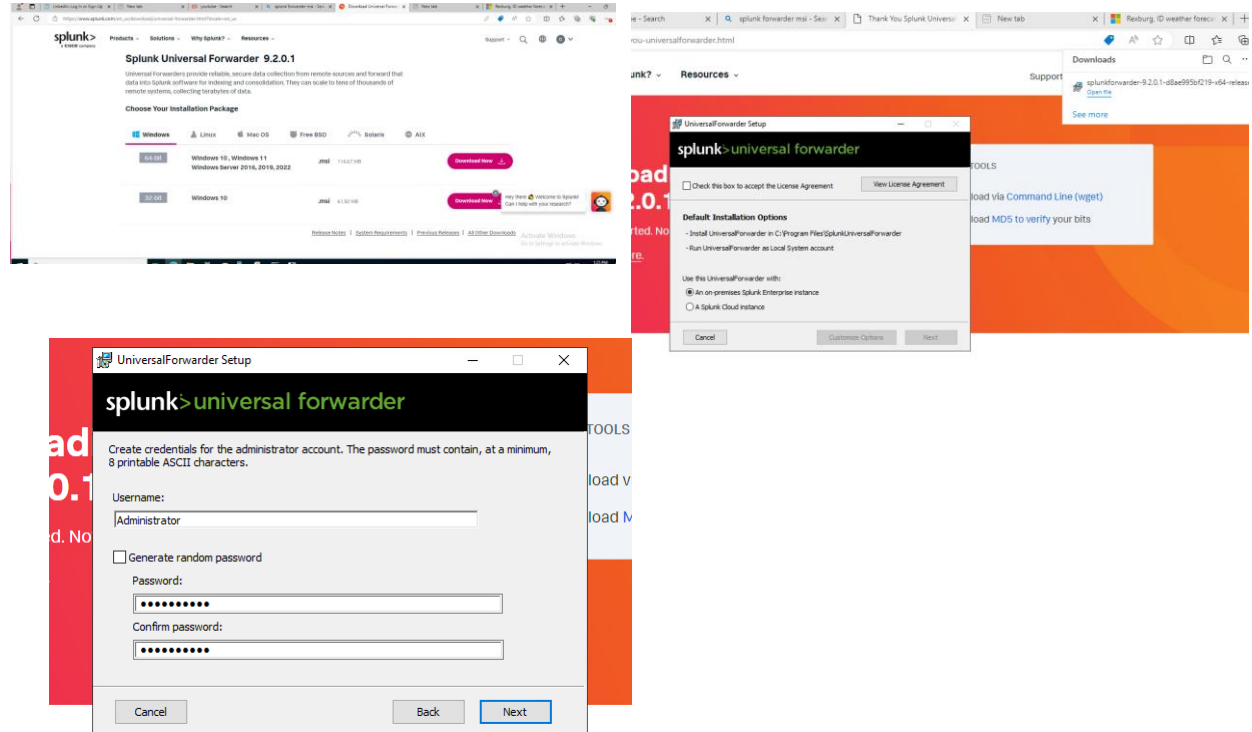
Configure the host to listen from port 9997.

On settings select Forwarding and receiving and add new port default 9997. This setting allows to receive logs from forwarders.



Universal Forwarder configuration on Windows endpoint.

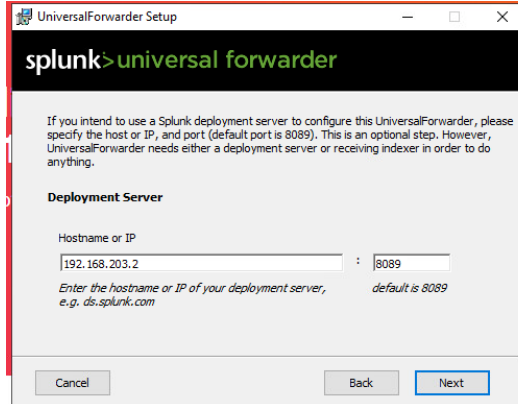
1. Download forwarder
2. Follow the guide and fill the prompts.
3. On Username use the same as in the creation of the host, and the same password.



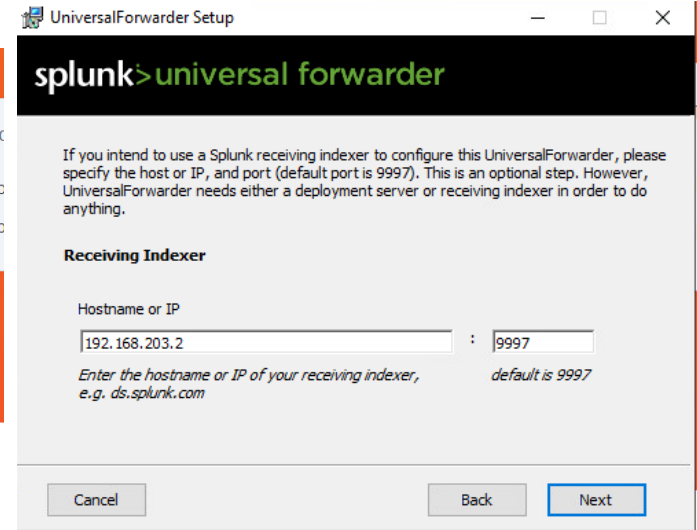
Universal Forwarder configuration on Windows endpoint

On Deployment server hostname use the ip address of the host already created and use the default port 8089.

On Receiving Indexer use the same address as before and the default port 9997.



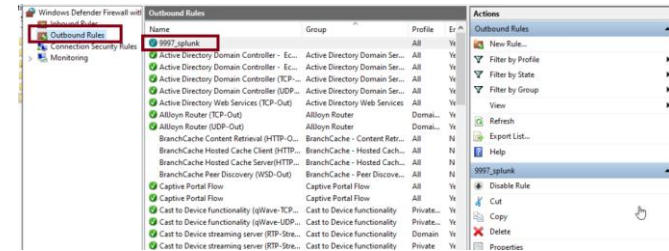
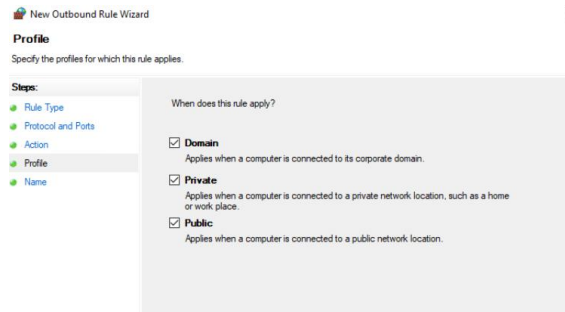
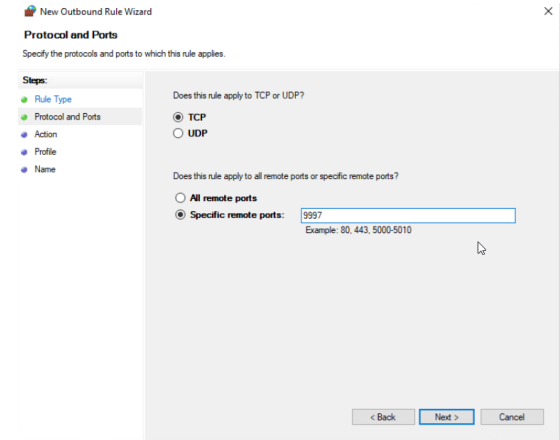
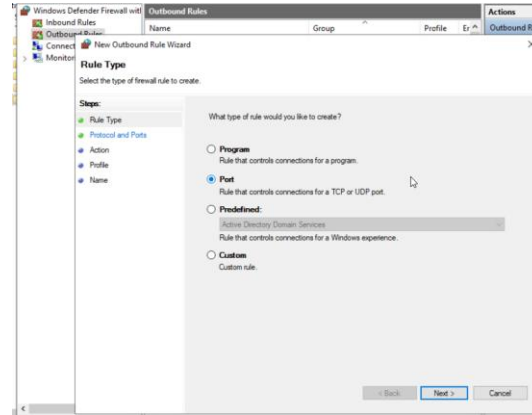
The screenshot shows the 'UniversalForwarder Setup' window. The title bar says 'UniversalForwarder Setup'. The main header is 'splunk>universal forwarder'. Below this, there is a paragraph of text: 'If you intend to use a Splunk deployment server to configure this UniversalForwarder, please specify the 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.' Below the text is the 'Deployment Server' section. It has a label 'Hostname or IP' and a text input field containing '192.168.203.2'. To the right of the input field is a label ':' and a port input field containing '8089'. Below the input fields is a note: 'Enter the hostname or IP of your deployment server, e.g. ds.splunk.com' and 'default is 8089'. At the bottom of the window are three buttons: 'Cancel', 'Back', and 'Next'.



The screenshot shows the 'UniversalForwarder Setup' window. The title bar says 'UniversalForwarder Setup'. The main header is 'splunk>universal forwarder'. Below this, there is a paragraph of text: '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.' Below the text is the 'Receiving Indexer' section. It has a label 'Hostname or IP' and a text input field containing '192.168.203.2'. To the right of the input field is a label ':' and a port input field containing '9997'. Below the input fields is a note: 'Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com' and 'default is 9997'. At the bottom of the window are three buttons: 'Cancel', 'Back', and 'Next'.

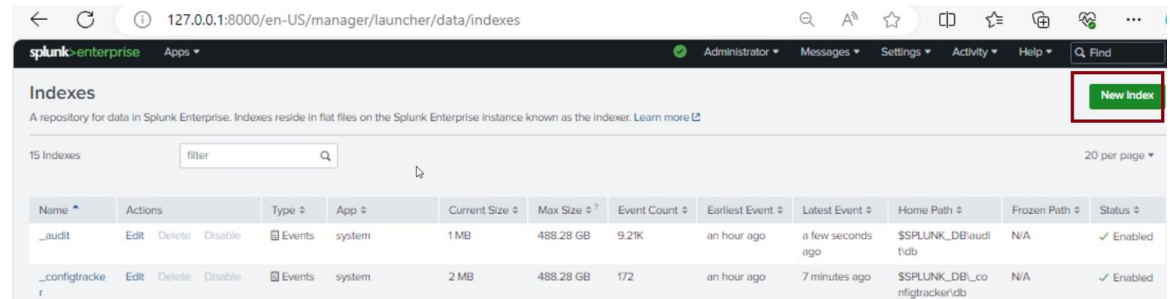
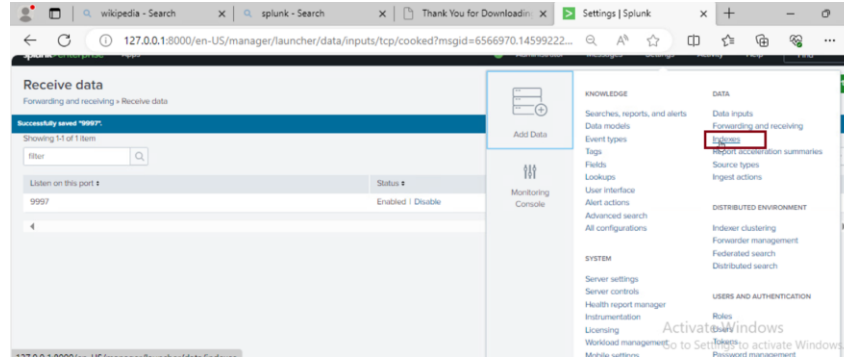
Universal Forwarder configuration Firewall rule on Windows

Add an outbound new rule to allow TCP on port 9997.



On the host machine create a new index to receive the logs.

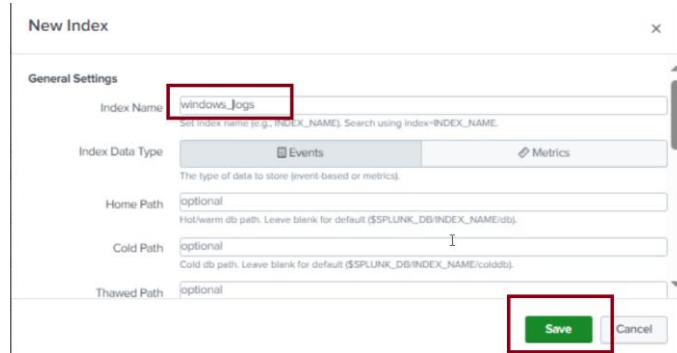
After open the web interface with the address 127.0.0.1:8000 and authenticate, under Settings go to Index and create a new index. The index serve as a repository for the logs.



Check that the host receive logs from the forwarder

We give in this example the name windows_logs name and save.

We can start to check that we receive logs from the user by open in settings, Add Data.



New Index

General Settings

Index Name: windows_logs

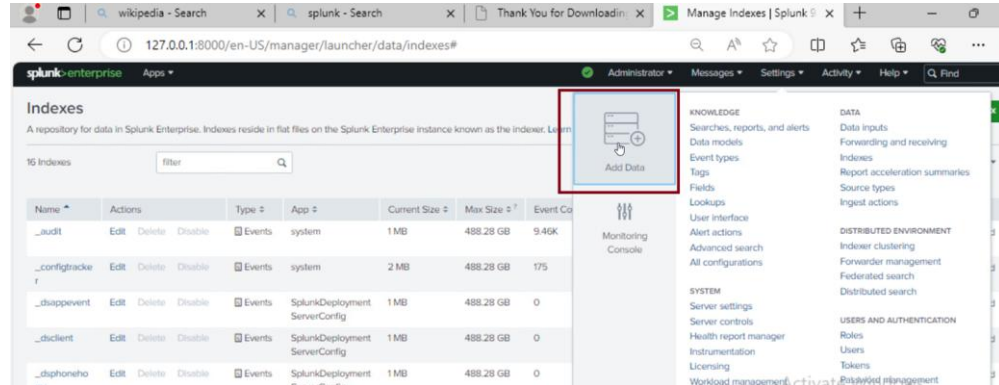
Index Data Type: Events

Home Path: optional

Cold Path: optional

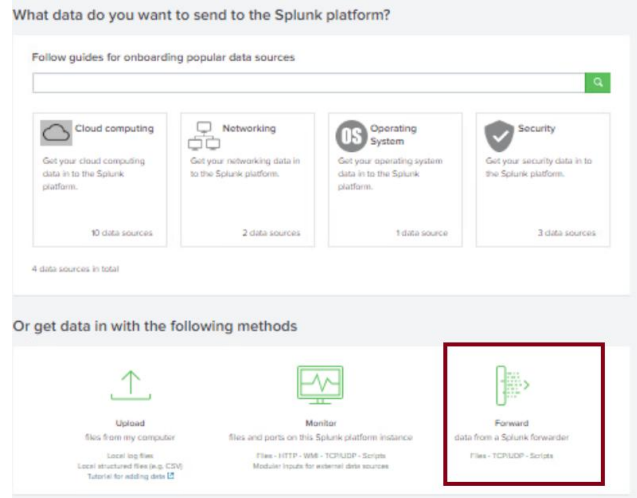
Thawed Path: optional

Save Cancel



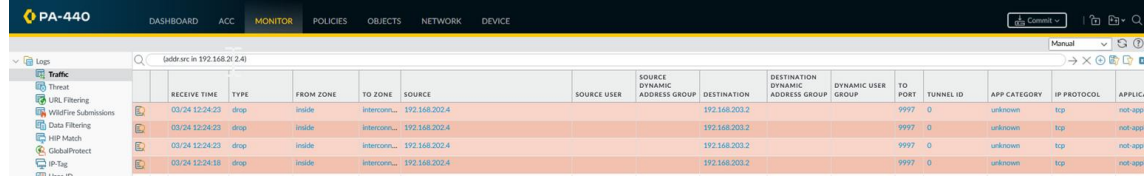
Check that the host receive logs from the forwarder

After we select forward as a receiving method, we should see that the windows machine is sending his first data to us. However we don't see it yet.



First rules to allow traffic over the firewalls

In the first screenshot we see that the Palo Alto firewall is blocking the packages. Then we made a firewall rule to allow the transfer of those package on Palo Alto and also add a new rule to allow incoming packages on the Fortigate firewall on the secure zone.



The screenshot shows the Palo Alto PA-440 firewall logs. The interface includes a top navigation bar with tabs: DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. The 'MONITOR' tab is active, and the 'Logs' section is selected. A search bar at the top right contains the text '(addr in 192.168.20.24)'. The logs table displays the following data:

| RECEIVE TIME | TYPE | FROM ZONE | TO ZONE | SOURCE | SOURCE USER | SOURCE DYNAMIC ADDRESS GROUP | DESTINATION | DESTINATION DYNAMIC ADDRESS GROUP | DYNAMIC USER GROUP | TO PORT | TUNNEL ID | APP CATEGORY | IP PROTOCOL | APPLIC |
|----------------|------|-----------|--------------|---------------|-------------|------------------------------|---------------|-----------------------------------|--------------------|---------|-----------|--------------|-------------|---------|
| 03/24 12:24:23 | drop | inside | Interconn... | 192.168.202.4 | | | 192.168.203.2 | | | 9997 | 0 | unknown | tcp | not-app |
| 03/24 12:24:23 | drop | inside | Interconn... | 192.168.202.4 | | | 192.168.203.2 | | | 9997 | 0 | unknown | tcp | not-app |
| 03/24 12:24:23 | drop | inside | Interconn... | 192.168.202.4 | | | 192.168.203.2 | | | 9997 | 0 | unknown | tcp | not-app |
| 03/24 12:24:18 | drop | inside | Interconn... | 192.168.202.4 | | | 192.168.203.2 | | | 9997 | 0 | unknown | tcp | not-app |

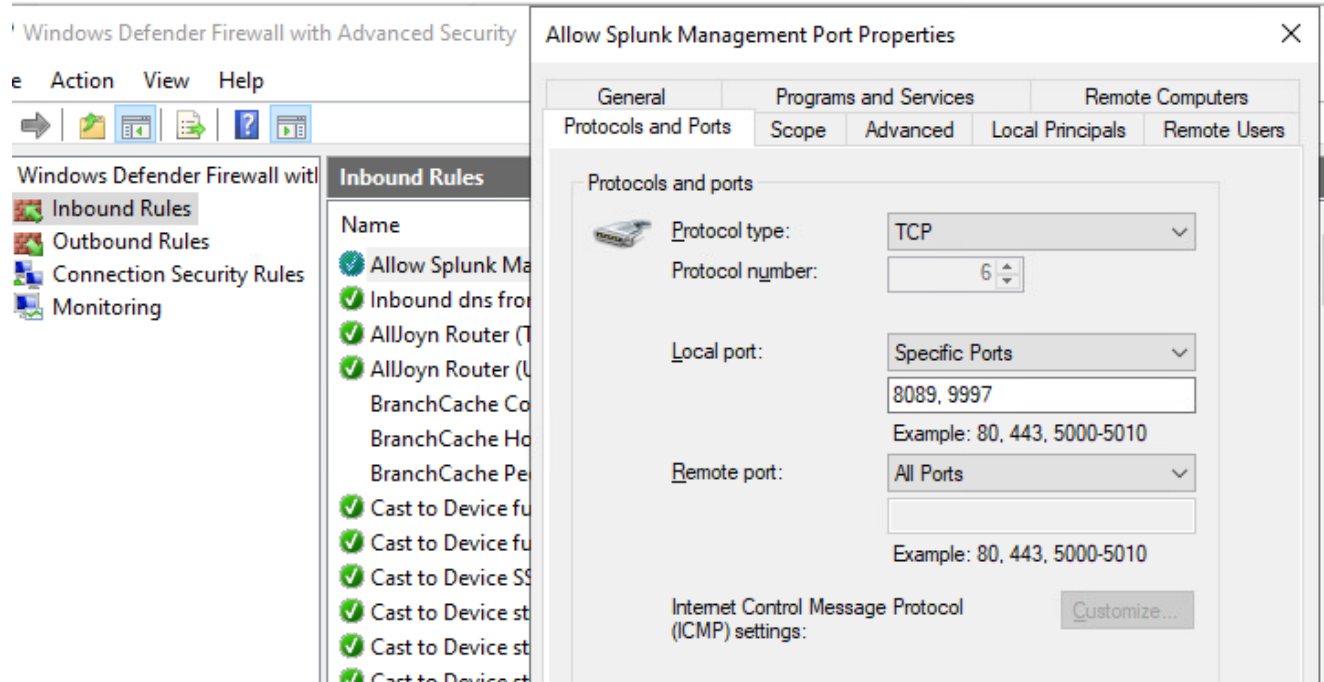
| | | | | | | | | | | | | |
|----|-------------|------|-----------|---|-----|-----|-----|--|---|-----|--|---|
| 16 | splunk_9997 | none | universal |  dms  inside | any | any | any |  interconnect |  192.168.203.2 | any |  splunk |  application-default |
|----|-------------|------|-----------|---|-----|-----|-----|--|---|-----|--|---|

| | | | | | | | | | | | | | |
|----------------|-----|-----|--------------|---------------|---------------|--|--|--|-----|---|-----|-----|--------------|
| 03/24 13:33:28 | any | any | interconnect | 192.168.203.2 | 192.168.203.2 | | | | any | 0 | any | any | interconnect |
|----------------|-----|-----|--------------|---------------|---------------|--|--|--|-----|---|-----|-----|--------------|

| | | | | | | | | | |
|--------------------|---------|--------|--------|--------|----------------|--------|----------|---------------|-----|
| income_splunk_9997 | Address | all | splunk | always | splunk_monitor | ACCEPT | Disabled | no-inspection | UTM |
| | Type | Subnet | | | | | | | |

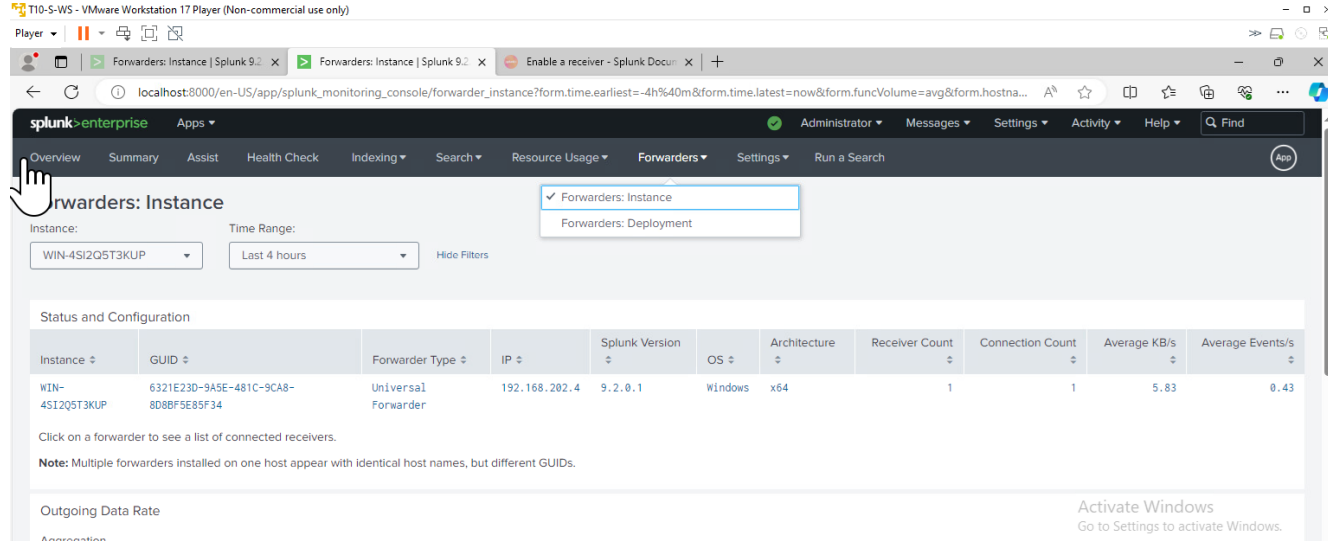
Firewall rules for inbound and outbound on the host.

We also need to add new inbound and outbound rules for the host to allow ports 8089 and 9997 communications.



Receiving data from the forwarder.

On settings and forwarders instances appears the windows endpoint that we configure to send data.



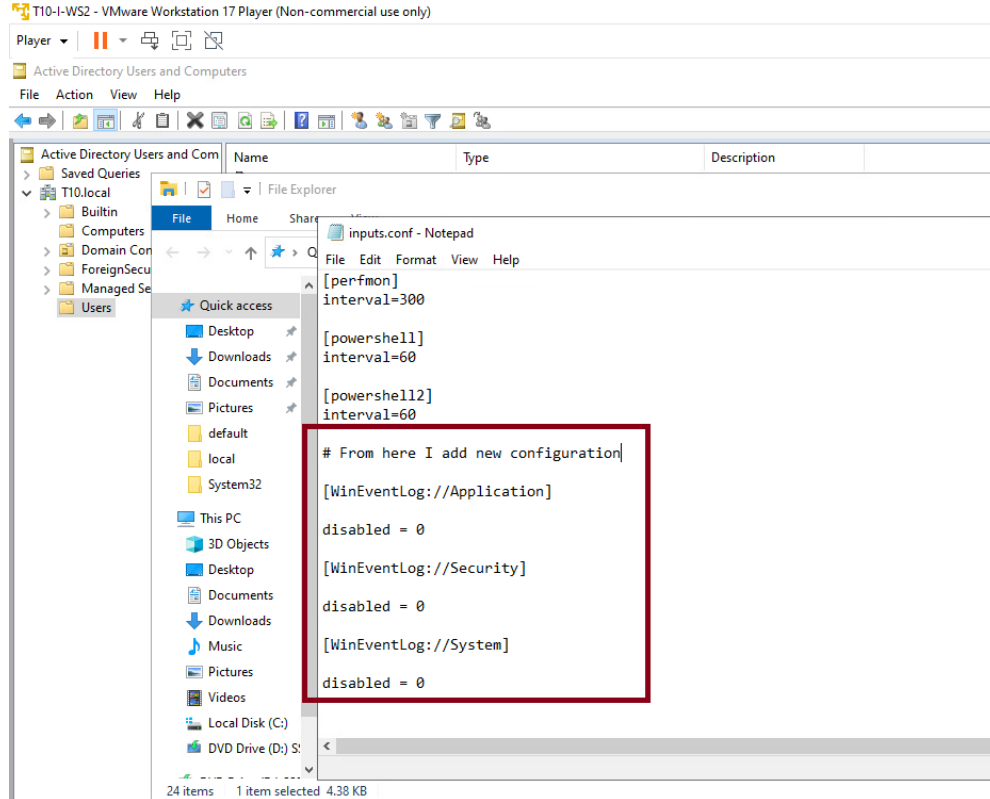
The screenshot shows the Splunk Enterprise web interface. The 'Forwarders: Instance' page is active, displaying a table of forwarder status and configuration. A hand cursor is pointing at the 'Forwarders: Instance' link in the left sidebar. The table lists one forwarder instance with the following details:

| Instance | GUID | Forwarder Type | IP | Splunk Version | OS | Architecture | Receiver Count | Connection Count | Average KB/s | Average Events/s |
|-----------------|--------------------------------------|---------------------|---------------|----------------|---------|--------------|----------------|------------------|--------------|------------------|
| WIN-4SI2Q5T3KUP | 6321E23D-9A5E-481C-9CA8-8D8BF5E85F34 | Universal Forwarder | 192.168.202.4 | 9.2.0.1 | Windows | x64 | 1 | 1 | 5.83 | 0.43 |

Below the table, there is a note: "Note: Multiple forwarders installed on one host appear with identical host names, but different GUIDs." At the bottom, there is a section for "Outgoing Data Rate" and a link to "Activate Windows".

Configuration on inputs.conf on forwarder to send Event Logs

We add the event logs to be sent to the host. Has to restart the service after saving changes.



Add data to the index we created before on the host.

On settings select Add Data , and select the available forwarder endpoint. Has to give a class name to get data from the forwarder.

The screenshot shows the 'Add Data' configuration page in Splunk Enterprise. The page title is 'Add Data - Select Forwarders'. The breadcrumb navigation shows 'Add Data' with a progress bar indicating the current step is 'Select Forwarders'. The page content includes instructions on creating or selecting a server class for data inputs. It features two tabs: 'New' and 'Existing'. Under the 'New' tab, there are two lists: 'Available host(s)' and 'Selected host(s)'. The 'Available host(s)' list contains 'WIN-4SI2Q5T3KUP' and 'WINDOWS'. The 'Selected host(s)' list also contains 'WIN-4SI2Q5T3KUP' and 'WINDOWS'. At the bottom, there is a text input field for 'New Server Class Name' with the value 'Windows Log'. The page footer shows the user is logged in as 'Administrator'.

localhost:8000/en-US/manager/search/adddatamethods/selectforwarders

splunk>enterprise Apps

Administrator Messages Settings

Add Data

Select Forwarders Select Source Input Settings Review Done

< Back Next >

Select Forwarders

Create or select a server class for data inputs. Use this page only in a single-instance Splunk environment.

To enable forwarding of data from deployment clients to this instance, set the output configurations on your forwarders. [Learn More](#)

Select Server Class

New Existing

Available host(s) add all >

WIN-4SI2Q5T3KUP
WINDOWS

Selected host(s) < remove all

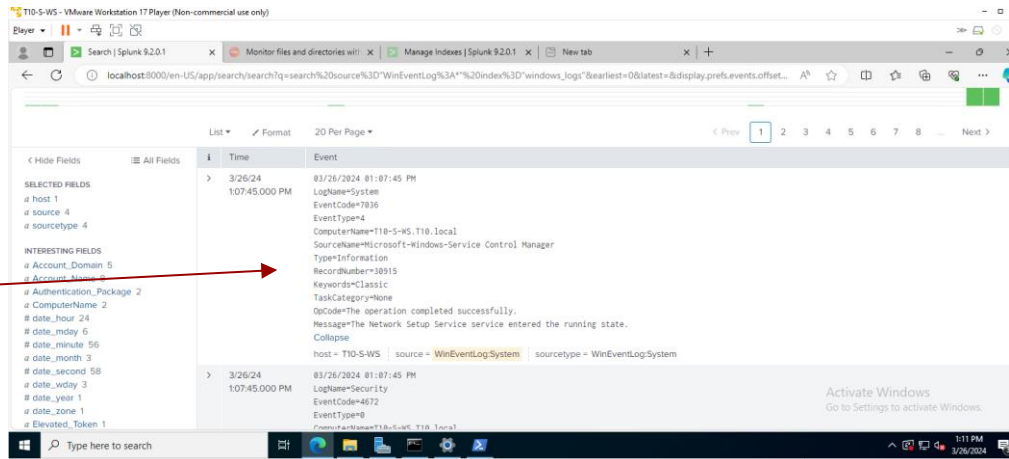
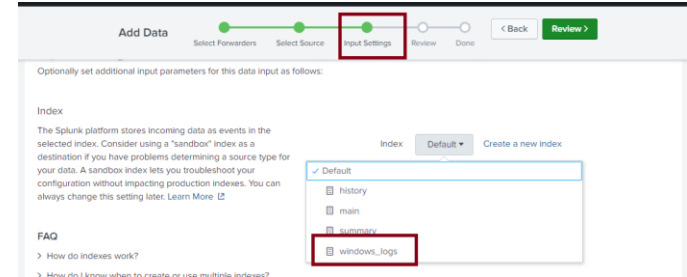
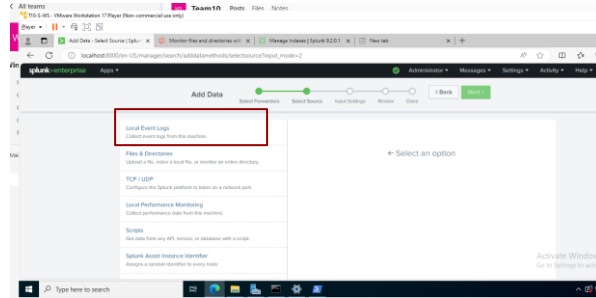
WIN-4SI2Q5T3KUP
WINDOWS

New Server Class Name Windows Log

Add data to the index we created before on the host.

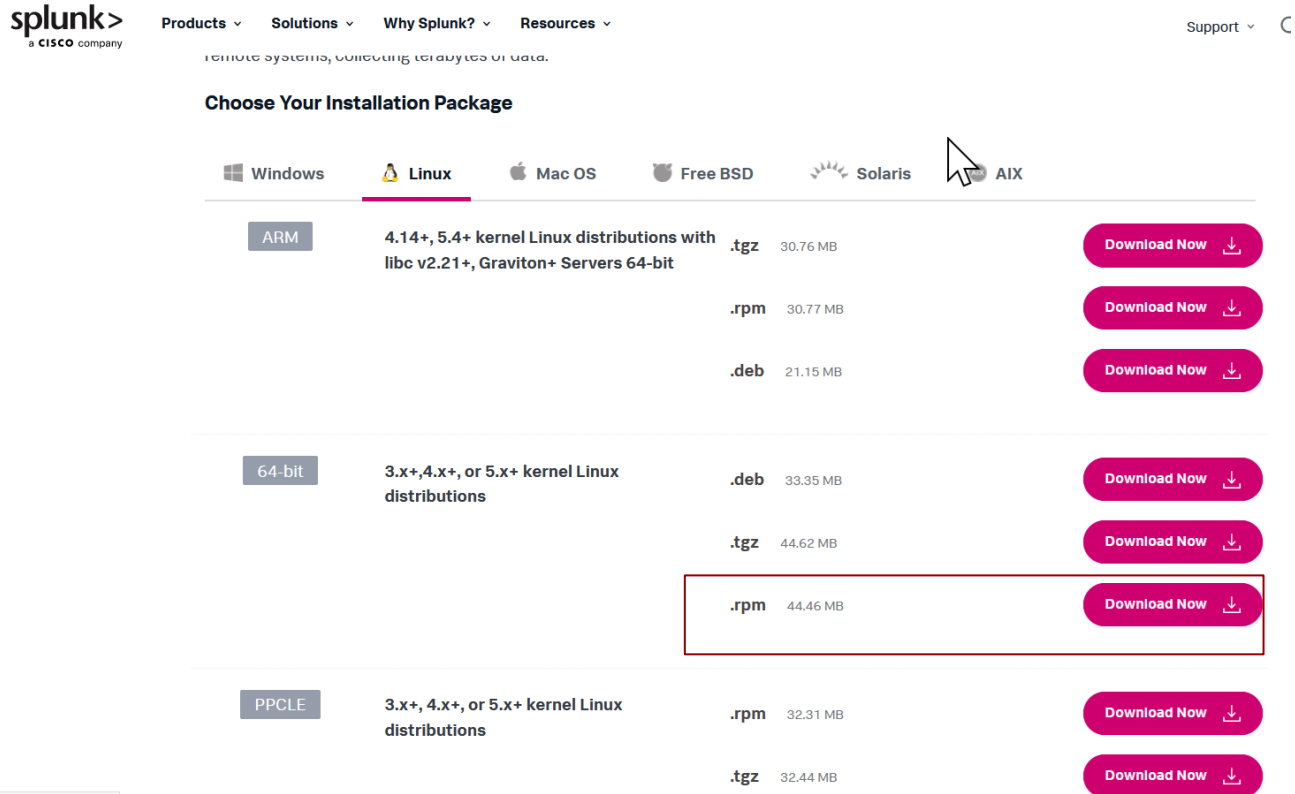
First select local events logs , and on the next step select the index we created before.

After finishing select collect data and the collected data start to appear from the windows endpoint.



Alma Linux Universal Forwarder configuration.

Go to splunk web site, authenticate and select to download the right version for your Linux system
We have Alma Linux, then we download 64 bit .rpm.



The screenshot shows the Splunk website's download page for Linux Universal Forwarder. The 'Linux' tab is selected under 'Choose Your Installation Package'. The page lists three categories: ARM, 64-bit, and PPCLE. The 64-bit category is expanded, showing three options: .tgz (30.76 MB), .rpm (30.77 MB), and .deb (21.15 MB). The .rpm option is highlighted with a red box. The .rpm option for the 64-bit category is highlighted with a red box.

| Architecture | Description | Format | Size | Action |
|--------------|---|--------|----------|------------------------------|
| ARM | 4.14+, 5.4+ kernel Linux distributions with libc v2.21+, Graviton+ Servers 64-bit | .tgz | 30.76 MB | Download Now |
| | | .rpm | 30.77 MB | Download Now |
| | | .deb | 21.15 MB | Download Now |
| 64-bit | 3.x+, 4.x+, or 5.x+ kernel Linux distributions | .deb | 33.35 MB | Download Now |
| | | .tgz | 44.62 MB | Download Now |
| | | .rpm | 44.46 MB | Download Now |
| PPCLE | 3.x+, 4.x+, or 5.x+ kernel Linux distributions | .rpm | 32.31 MB | Download Now |
| | | .tgz | 32.44 MB | Download Now |

Alma Linux Universal Forwarder configuration.

Copy the script for the command line to download the file.

Use the script to download the file.

Review that the file was download with

||



```
cdm@T10-D-AL2:~$ wget -O splunkforwarder-9.2.1-78803f08aabb.x86_64.rpm https://download.splunk.com/products/universalforwarder/releases/9.2.1/linux/splunkforwarder-9.2.1-78803f08aabb.x86_64.rpm
--2024-03-27 16:13:48-- https://download.splunk.com/products/universalforwarder/releases/9.2.1/linux/splunkforwarder-9.2.1-78803f08aabb.x86_64.rpm
Connecting to download.splunk.com (download.splunk.com)... 44.40M 42.0MB/s in 1.0s
HTTP request sent, awaiting response... 200 OK
Length: 46614849 (44M) [binary/octet-stream]
Saving to: 'splunkforwarder-9.2.1-78803f08aabb.x86_64.rpm'

splunkforwarder-9.2 100%[=====] 44.40M 42.0MB/s in 1.0s
2024-03-27 16:13:48 (42.6 MB/s) - 'splunkforwarder-9.2.1-78803f08aabb.x86_64.rpm' saved [46614849/46614849]
```

```
cgerez@T10-D-AL3:~$ ll
total 45524
drwxr-xr-x. 2 cgerez cgerez 6 Jan 18 15:29 Desktop
drwxr-xr-x. 2 cgerez cgerez 6 Jan 18 15:29 Documents
drwxr-xr-x. 2 cgerez cgerez 59 Mar 28 02:58 Downloads
drwxr-xr-x. 2 cgerez cgerez 6 Jan 18 15:29 Music
drwxr-xr-x. 2 cgerez cgerez 53 Jan 18 15:34 Pictures
drwxr-xr-x. 2 cgerez cgerez 6 Jan 18 15:29 Public
-rw-rw-r--. 1 cgerez cgerez 46614849 Mar 26 17:10 splunkforwarder-9.2.1-78803f08aabb.x86_64.rpm
drwxr-xr-x. 2 cgerez cgerez 6 Jan 18 15:29 Templates
drwxr-xr-x. 2 cgerez cgerez 6 Jan 18 15:29 Videos
cgerez@T10-D-AL3:~$
```

Alma Linux Universal Forwarder configuration.

Install the forwarder. Use:

`sudo rpm -i` and copy and paste the name of the file in red. Here you must change the user to continue, use:

`su - splunkfwd`

This user is created upon installation.

Then will be necessary to navigate to the right directory to perform enable start and configurations.

`cd /opt/splunkforwarder/bin`

```
cgerez@T10-D-AL3:~$ ll
total 45524
drwxr-xr-x. 2 cgerez cgerez    6 Jan 18 15:29 Desktop
drwxr-xr-x. 2 cgerez cgerez    6 Jan 18 15:29 Documents
drwxr-xr-x. 2 cgerez cgerez   59 Mar 28 02:58 Downloads
drwxr-xr-x. 2 cgerez cgerez    6 Jan 18 15:29 Music
drwxr-xr-x. 2 cgerez cgerez   53 Jan 18 15:34 Pictures
drwxr-xr-x. 2 cgerez cgerez    6 Jan 18 15:29 Public
-rw-r--r--. 1 cgerez cgerez 46614849 Mar 26 17:10 splunkforwarder-9.2.1-78803f08aabb.x86_64.rpm
drwxr-xr-x. 2 cgerez cgerez    6 Jan 18 15:29 Templates
drwxr-xr-x. 2 cgerez cgerez    6 Jan 18 15:29 Videos
cgerez@T10-D-AL3 ~]$ rpm -isplunkforwarder-9.2.1-78803f08aabb.x86_64.rpm
rpm: -isplunkforwarder-9.2.1-78803f08aabb.x86_64.rpm: unknown option
cgerez@T10-D-AL3 ~]$ rpm -i splunkforwarder-9.2.1-78803f08aabb.x86_64.rpm
warning: splunkforwarder-9.2.1-78803f08aabb.x86_64.rpm: Header V4 RSA/SHA256 Sig
nature, key ID b3cd4420: NOKEY
error: can't create transaction lock on /var/lib/rpm/.rpm.lock (Permission denied)
cgerez@T10-D-AL3 ~]$ sudo rpm -i splunkforwarder-9.2.1-78803f08aabb.x86_64.rpm
warning: splunkforwarder-9.2.1-78803f08aabb.x86_64.rpm: Header V4 RSA/SHA256 Sig
nature, key ID b3cd4420: NOKEY
complete
cgerez@T10-D-AL3 ~]$
```

```
splunkfwd@T10-D-AL3:/opt/splunkforwarder/bin$ ll
-r--r--r--. 1 splunkfwd splunkfwd  57 Mar 28 18:38 copyright.txt
drwxr-xr-x. 14 splunkfwd splunkfwd 4096 Mar 28 03:10 etc
-rw-r--r--. 1 splunkfwd splunkfwd  364 Mar 28 03:10 ftr
drwxr-xr-x. 2 splunkfwd splunkfwd   27 Mar 28 03:10 include
drwxr-xr-x. 6 splunkfwd splunkfwd  4996 Mar 28 03:10 lib
-r--r--r--. 1 splunkfwd splunkfwd 85405 Mar 28 18:38 license-eula.txt
drwxr-xr-x. 3 splunkfwd splunkfwd   58 Mar 28 03:10 openssl
-r--r--r--. 1 splunkfwd splunkfwd  519 Mar 28 18:42 README-splunk.txt
drwxr-xr-x. 4 splunkfwd splunkfwd   63 Mar 28 03:10 share
-r--r--r--. 1 splunkfwd splunkfwd 63230 Mar 28 19:04 splunkforwarder-9.2.1-78803f08aabb-linux-2.6-x86_64-manifest
drwxr-xr-x. 2 splunkfwd splunkfwd   55 Mar 28 03:10 swidtag
-rw-r--r--. 1 splunkfwd splunkfwd    0 Mar 28 19:03 uf
[splunkfwd@T10-D-AL3 splunkforwarder]$ cd cmake
[splunkfwd@T10-D-AL3 cmake]$ ls
pcr2-config.cmake  pcr2-config-version.cmake
[splunkfwd@T10-D-AL3 cmake]$ cd ..
[splunkfwd@T10-D-AL3 splunkforwarder]$ ls bin
lib3.7      idle3      pipalpng   slim
tool        idle3.7    pipamtpng splunk
xprobe      openssl    prpnglsch splunkd
zip2        pcr2-config prpngtopam splunkmon
classify    pid check.sh priweavepng splunk-tlsd
copyright.txt  pip3       pydoc3     supervisor-simulator
```

Alma Linux Universal Forwarder configuration.

To run the next commands use sudo and refers the splunk file with ./ as:

`sudo ./splunk add forward-server 192.168.203.2:9997`

And

`sudo ./splunk set deploy-poll 192.168.203.2:8089`

```
Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done

[splunkfwd@T10-D-AL3 bin]$ sudo ./splunk add forward-server 192.168.203.2
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Splunk username: Administrator
Password:
192.168.203.2 specified in incorrect format. Please specify in <host>:<port> for m
[splunkfwd@T10-D-AL3 bin]$ sudo ./splunk add forward-server 192.168.203.2:9997
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added forwarding to: 192.168.203.2:9997.
[splunkfwd@T10-D-AL3 bin]$ sudo ./splunk set deploy-poll 192.168.203.2:8089
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Configuration updated.
[splunkfwd@T10-D-AL3 bin]$
```

Alma Linux Universal Forwarder configuration.

Finally restart the service to make the new configuration available with:

`sudo ./splunk restart`

```
[splunkfwd@T10-D-AL3 bin]$ sudo ./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.
[ OK ]
Stopping splunk helpers...
[ OK ]
Done.
splunkd.pid doesn't exist...
Splunk> Australian for grep.
Checking prerequisites...
  Checking mgmt port [8089]: open
  Checking conf files for problems...
  Done
  Checking default conf files for edits...
  Validating installed files against hashes from '/opt/splunkforwarder'
  All installed files intact.
  Done
All preliminary checks passed.
Starting splunk server daemon (splunkd)...
Done
[ OK ]
[splunkfwd@T10-D-AL3 bin]$
```

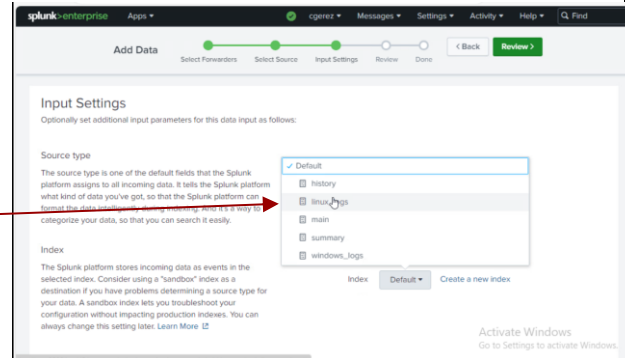
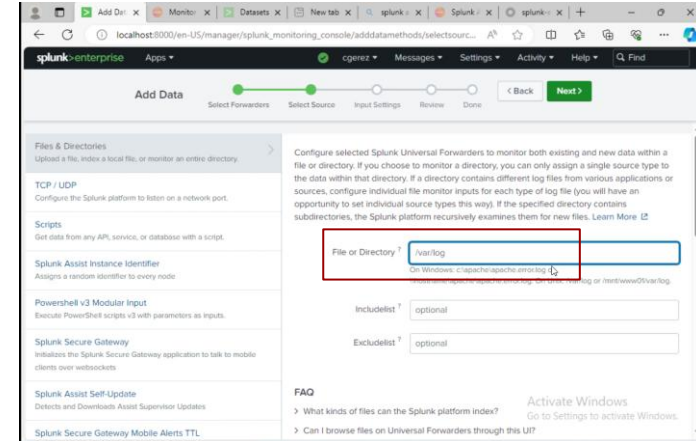
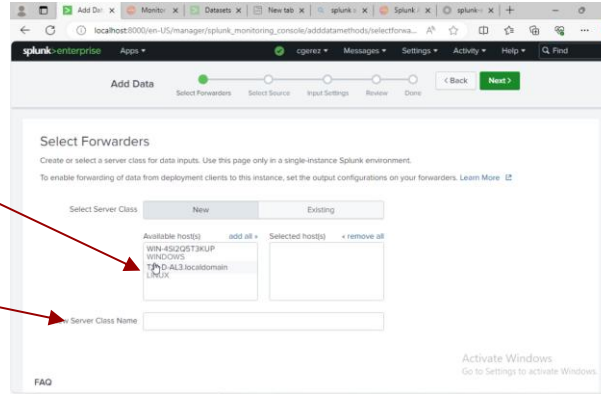
Received data from the new Linux forwarder.

On Add Data under settings on the host, select the new linux machine and add a class name.

Select files and directories to collect logs and set the path to:

`/var/log/*`

Use a previous created index for linux.



Alma Linux Universal Forwarder configuration.

Review and submit
the search and start
searching data in
the next screen.

The screenshot shows the 'Review' step of the 'Add Data' wizard. At the top, a progress bar indicates the steps: Select Forwarders, Select Source, Input Settings, Review, and Done. The 'Review' step is currently active. Below the progress bar, the 'Review' section contains the following configuration details:

- Server Class Name: Linux Alma
- List of Forwarders: LINUX | T10-D-AL3.localdomain
- Input Type: File Monitor
- Source Path: /var/log
- Includelist: N/A
- Excludelist: N/A
- Source Type: Automatic
- Index: linux_logs

At the bottom right of the 'Review' section, there are '< Back' and 'Submit >' buttons. A red arrow points from the text 'Review and submit' to the 'Submit >' button.

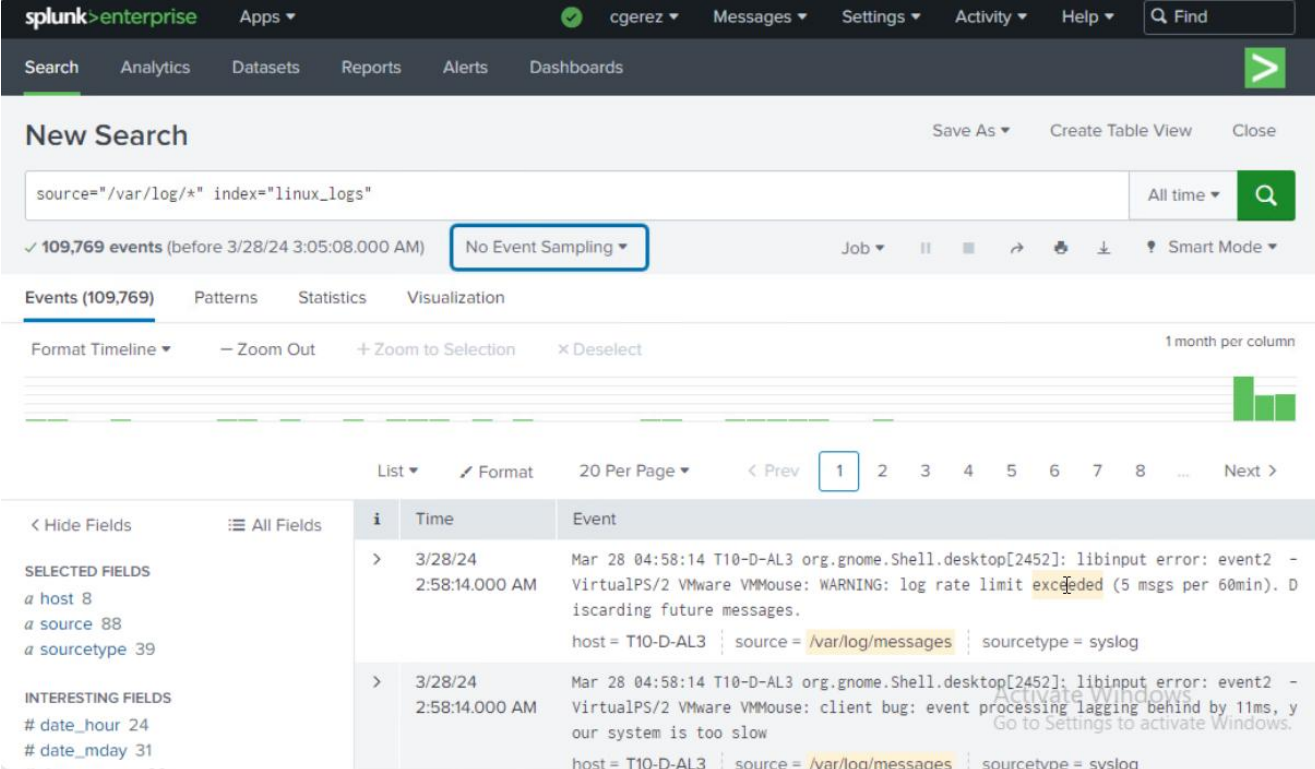
The screenshot shows the 'Add Data' success screen in the Splunk web interface. The progress bar at the top now shows 'Done' as the final step. The main content area displays a green checkmark and the message: 'File input has been created successfully. Configure your inputs by going to Settings > Data Inputs'. Below this message, there is a 'Start Searching' button and several other options:

- Start Searching**: Search your data now or see [examples and tutorials](#).
- Extract Fields**: Create search-time field extractions. [Learn more about fields](#).
- Add More Data**: Add more data inputs now or see [examples and tutorials](#).
- Download Apps**: Apps help you do more with your data. [Learn more](#).
- Build Dashboards**: Visualize your searches. [Learn more](#).

A red arrow points from the text 'the search and start searching data in the next screen.' to the 'Start Searching' button.

Alma Linux Universal Forwarder configuration.

Receiving log data
from the linux
machine.



New Search Save As Create Table View Close

source="/var/log/*" index="linux_logs" All time Q

✓ 109,769 events (before 3/28/24 3:05:08.000 AM) No Event Sampling Job || ■ ↶ ↷ ⬇ 💡 Smart Mode

Events (109,769) Patterns Statistics Visualization

Format Timeline — Zoom Out + Zoom to Selection x Deselect 1 month per column

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

| | i | Time | Event |
|---|---|---------------------------|---|
| > | | 3/28/24 2:58:14.000 AM | Mar 28 04:58:14 T10-D-AL3 org.gnome.Shell.desktop[2452]: libinput error: event2 - VirtualPS/2 VMware VMMouse: WARNING: log rate limit exceeded (5 msgs per 60min). Discarding future messages. host = T10-D-AL3 source = /var/log/messages sourcetype = syslog |
| > | | 3/28/24 2:58:14.000 AM | Mar 28 04:58:14 T10-D-AL3 org.gnome.Shell.desktop[2452]: libinput error: event2 - VirtualPS/2 VMware VMMouse: client bug: event processing lagging behind by 11ms, your system is too slow host = T10-D-AL3 source = /var/log/messages sourcetype = syslog |

SELECTED FIELDS
a host 8
a source 88
a sourcetype 39

INTERESTING FIELDS
date_hour 24
date_mday 31

Add users and passwords for the team on the host splunk enterprise.

Under settings
locate the tab users
to create users for
the team.

