FORWARDERS-------------------------------------------

Check for the version of splunk you’re using and get the matching forwarder version. If you can’t access splunk website to get the download, use a real machine to copy the wget link. (I know it sucks but it works)… OH and pay attention if it’s windows or Linux.

A screenshot of a computer

Description automatically generated A screenshot of a computer

Description automatically generated

THIS PART IF SPLUNK FORWARDER IS ON LINUX.

Locate Correct splunk version and download the correct package version (or copy wget into terminal)

Mkdir ~/Downloads/www # create the directory to put the forwarder

mv splunkforwarder ~/Downloads/www 🡪 cd /Downloads/www 🡪 ./bin/splunk start –accept-license 🡪 press y then change port to 9997 when asked.

install Firefox or chromium then into browser // localhost 8000

Login 🡪 settings in top tab 🡪 forwarding and receiving 🡪 configure receiving 🡪 new receiving port 🡪 port 9997 and save.

Cd /Downloads/www/splunkforwarder/bin

./splunk add forward-server (Splunk machine IP):9997 #don’t include () with your Ip. AND THE IP IS THE SPLUNK MACHINE, NOT SOMEONE ELSES IP THEY DOWNLOADED IT TOO.

next, we will tell Splunk forwarder which logs files to monitor.

./splunk add monitor /var/log -index Linux\_host

# we could specify /var/log/auth.log or /syslog

Then lets confirm it works

Cd /Downloads/www/splunkforwarder/etc/apps/search/local

ls # should see inputs.conf 🡪 cat inputs.conf

A screenshot of a computer error

AI-generated content may be incorrect.

if disabled = true or 1. do this 🡪 nano into inputs.conf and change the value to false or 0 🡪 sudo

Your outputs.conf should look like this. If not, build it yourself using text editor.

A screenshot of a computer

AI-generated content may be incorrect.

/Downloads/www/splunkforwarder/bin/splunk restart

and then sudo /opt/splunk/bin/splunk restart

Then check with Splunk Master if he/she is receiving logs.

THIS PART IF SPLUNK IS ON WINDOWS.

Open Windows Defender Firewall with Advanced Security 🡪Select "Inbound Rules" and click "New Rule..." in the Actions panel 🡪Select "Port" and click "Next" 🡪Select "TCP" and enter the specific port(s) separated by commas (8000,8089,9997,8191)🡪Select "Allow the connection" and click "Next"🡪Select which network types apply (Domain, Private, Public) and click "Next" 🡪Name the rule "Splunk Ports" with description and click "Finish"

Locate Correct splunk version and download the correct package version. (or copy wget into terminal) IF THE SPLUNK FORWARDER HAS TO BE 9.1.1, CHECK WGET LINK AND AVOID THE ONE WITH AIRGAP A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

Description automatically generated

User a secure password.

If it asks for other stuff like ssl, just skip over it or accept its default option.

A screenshot of a computer

Description automatically generated check the last box if its an AD machine.

A red and white box with black text

Description automatically generatedreplace IP with the Splunk IP and port as 8089.

Leave indexer blank

Once complete, check with Splunk Overlord if he/she is receiving logs.