Splunk

Sunday, January 28, 2024 8:51 PM

Installing Splunk Enterprise

- Create a free splunk account > download splunk enterprise trial
- Sudo apt install curl
- Sudo dkpg -i [splunk file]
- Cd /opt/splunk/bin
- ./splunk start
- Accept T&C, set username & pw

Installing forwarders on machines

- https://www.splunk.com/en_us/download/universal-

forwarder.html
- https://docs.splunk.com/Documentation/Forwarder/9.0.2/Forwarder/Installanixuniversalforwarder

This is the wget command I was able to find only after making an account:

- wget -O splunkforwarder-9.2.0-1fff88043d5f-linux-2.6-amd64.deb https://download.splunk.com/products/universalforwarder/releases/9.2.0/linux/splunkforwarder-9.2.0-1fff88043d5f-linux-2.6-amd64.deb
- This might or might not be a unique link that can only be used once. Hopefully we can either use this or they already have it installed.
- Steps after getting the

.deb (or whatever) file:

- Useradd –m splunk
- Groupadd splunk

For our VM WebServer6:
Splunk:Password
Splunk administrator:
yoda:Password

Installing:
https://docs.splunk.com/Documentation/Forwarder/9.0.2/Forwarder/Installanixuniversalforwarder
Configure:
https://docs.splunk.com/Documentation/Forwarder/9.0.2/Forwarder/Enableareceiver

https://docs.splunk.com/Documentation/Forwarder/9.0.2/Forwarder/Configurethe universalforwarder

https://docs.splunk.com/Documentation/Forwarder/9.2.0/Forwarder/C

onfigurethe universalforwarder#:~:text=the%20universal%20forwarder.-,Find%20the%20configuration%20files,your%20Universal%20Forwarder%20configuration%20files.

We might need to add inputs.conf and outputs.conf

User created alert