Splunk Forwarder (LINUX)

Thursday, March 28, 2024 8:24 AM

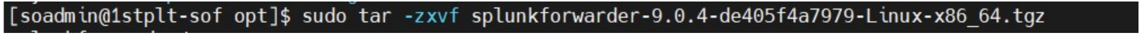
Here we install the Splunk Universal Forwarder onto a LINUX Machine

First step:

send over the installation .tgz file. This is located at " *\\share\Share\5.) Splunk\splunk-package\forwarders* "

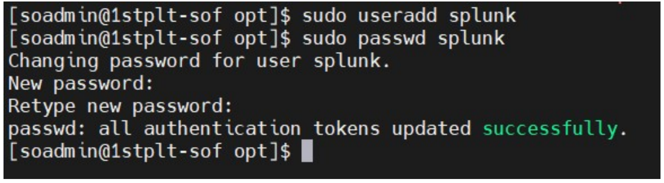
For LINUX, we're going to use the ***splunkforwarder-9.0.4-de405f4a7979-Linux-x86_64.tgz***
SCP it over to the machine you want it in.
MV it over to the /opt directory

"Once in the /opt directory, untar it"



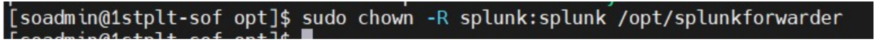
```
[soadmin@1stplt-sof opt]$ sudo tar -zxvf splunkforwarder-9.0.4-de405f4a7979-Linux-x86_64.tgz
```

Create the user "Splunk" with standard password



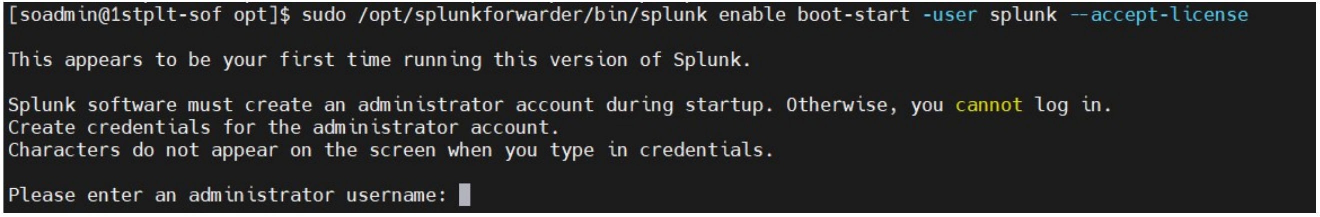
```
[soadmin@1stplt-sof opt]$ sudo useradd splunk
[soadmin@1stplt-sof opt]$ sudo passwd splunk
Changing password for user splunk.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[soadmin@1stplt-sof opt]$
```

Change the ownership of the directory to the new user



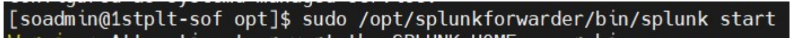
```
[soadmin@1stplt-sof opt]$ sudo chown -R splunk:splunk /opt/splunkforwarder
```

Enable splunk to be ran at boot with the new user "splunk": use dco_admin and standard passwd



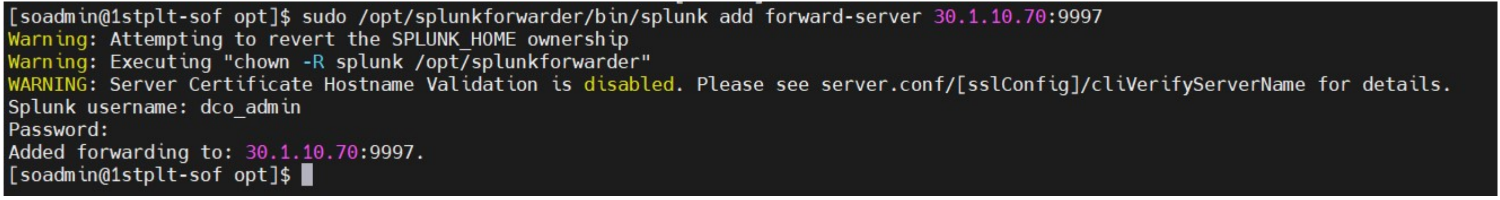
```
[soadmin@1stplt-sof opt]$ sudo /opt/splunkforwarder/bin/splunk enable boot-start -user splunk --accept-license

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username:
```

Start the Splunk Universal Forwarder



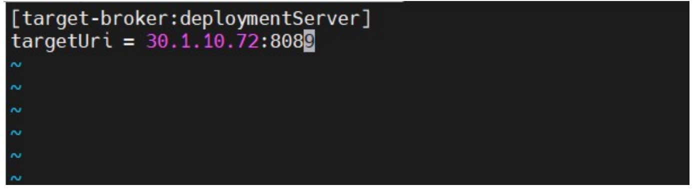
```
[soadmin@1stplt-sof opt]$ sudo /opt/splunkforwarder/bin/splunk start
```

Adding a connection to our indexer. For this example we have the (30.1.10.70) as our indexer.



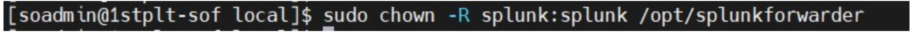
```
[soadmin@1stplt-sof opt]$ sudo /opt/splunkforwarder/bin/splunk add forward-server 30.1.10.70:9997
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunk /opt/splunkforwarder"
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Splunk username: dco_admin
Password:
Added forwarding to: 30.1.10.70:9997.
[soadmin@1stplt-sof opt]$
```

cd /opt/splunkforwarder/etc/system/local/
sudo touch deploymentclient.conf
After creating the "deployment.conf" file, write your manager ip in a distributed network, or your standalone ip.



```
[target-broker:deploymentServer]
targetUri = 30.1.10.72:8089
~
~
~
~
~
~
```

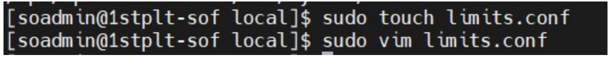
Change ownership for the whole directory to the "splunk" user.



```
[soadmin@1stplt-sof local]$ sudo chown -R splunk:splunk /opt/splunkforwarder
```

Start splunk again.
sudo /opt/splunkforwarder/bin/splunk restart
sudo /opt/splunkforwarder/bin/splunk start

Go to /opt/splunkforwarder/etc/system/local and create a limits.conf file

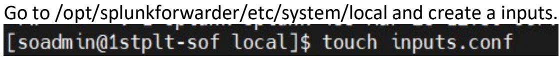


```
[soadmin@1stplt-sof local]$ sudo touch limits.conf
[soadmin@1stplt-sof local]$ sudo vim limits.conf
```

In this file, paste:

```
[thruput]
maxkBps = 0
```

Go to /opt/splunkforwarder/etc/system/local and create a inputs.conf file



```
[soadmin@1stplt-sof local]$ touch inputs.conf
```

In this file, paste all of this in:

```
[default]
host = sensor
[monitor:///nsm/zeek/logs/current/conn.log]
_TCP_ROUTING = *
index = zeek
sourcetype = zeek_conn
[monitor:///nsm/zeek/logs/current/dns.log]
_TCP_ROUTING = *
index = zeek
sourcetype = zeek_dns
[monitor:///nsm/zeek/logs/current/software.log]
_TCP_ROUTING = *
index = zeek
sourcetype = zeek_software
[monitor:///nsm/zeek/logs/current/smtp.log]
_TCP_ROUTING = *
index = zeek
sourcetype = zeek_smtp
[monitor:///nsm/zeek/logs/current/ssl.log]
_TCP_ROUTING = *
index = zeek
sourcetype = zeek_ssl
[monitor:///nsm/zeek/logs/current/ssh.log]
_TCP_ROUTING = *
index = zeek
sourcetype = zeek_ssh
[monitor:///nsm/zeek/logs/current/x509.log]
_TCP_ROUTING = *
index = zeek
sourcetype = zeek_x509
[monitor:///nsm/zeek/logs/current/ftp.log]
_TCP_ROUTING = *
index = zeek
sourcetype = zeek_ftp
[monitor:///nsm/zeek/logs/current/http.log]
_TCP_ROUTING = *
index = zeek
sourcetype = zeek_http
[monitor:///nsm/zeek/logs/current/rdp.log]
_TCP_ROUTING = *
index = zeeksud
sourcetype = zeek_rdp
[monitor:///nsm/zeek/logs/current/smb_files.log]
_TCP_ROUTING = *
index = zeek
sourcetype = zeek_smb_files
[monitor:///nsm/zeek/logs/current/smb_mapping.log]
_TCP_ROUTING = *
index = zeek
sourcetype = zeek_smb_mapping
[monitor:///nsm/zeek/logs/current/snmp.log]
_TCP_ROUTING = *
index = zeek
sourcetype = zeek_snmp
```

```
[monitor:///nsm/zeek/logs/current/sip.log]
_TCP_ROUTING = *
index = zeek
sourcetype = zeek_sip
[monitor:///nsm/zeek/logs/current/files.log]
_TCP_ROUTING = *
index = zeek
sourcetype = zeek_files

[monitor:///nsm/suricata]
_TCP_ROUTING = *
index = suricata
sourcetype = suricata_alerts
```

RESTART it again

sudo /opt/splunkforwarder/bin/splunk restart

By LCPL Norminton