PRATHEEK DHANANJAYA

Phone: +1(312)284-9358 | Email: pratheekdhananjaya@gmail.com | LinkedIn: https://www.linkedin.com/in/pratheek-dhananjaya/

SPLUNK Installation Document

Specifications:

Host OS: Mac OS X (Intel processor)

Host IP: 1.1.1.1 (Can be found in **system settings -> Wi-Fi -> details -> TCP/IP**)

VM: UTM

VM OS 1: Kali Linux

VM OS 2: Windows 10

- ➔ **Splunk Indexer** (Splunk Enterprise) is installed in the Host/Local system.
- ➔ **Splunk Universal Forwarder** is installed in the VM.

Splunk Indexer:

- ➔ Create a Splunk account with the necessary details and download the Splunk Enterprise version, which is free for the first 60 days. (Link)
- ➔ Install Splunk Enterprise using the .dmg file and run the application from the application folder. While installing, provide the username and password that will be used to access this application.
- ➔ Terminal commands are executed in a daemon process (which could be seen sometimes), which opens the default browser, and Splunk Enterprise is run on the localhost over port 8000.
- ➔ Provide the login details entered while installing and logging in.
- ➔ Go to **Settings -> Forwarding & Receiving -> Configure receiving (Receive data) -> New receiving port -> 9997 (Default port that Splunk uses to receive logs) -> Save.**
- ➔ On the top left, **Apps -> Search & Reporting ->** enter the query as required.

Splunk Universal Forwarder (VM OS 1):

- ➔ Download the Kali Linux .iso file. (Link)
- ➔ Open **UTM (VM) -> Create a New Virtual Machine -> Virtualize -> Linux -> Boot ISO image & browse for the downloaded .iso file -> 4 GB memory and 2 CPU cores -> 30 GB storage -> Select the shared directory path -> Check 'Open VM settings' & continue -> network tab in VM settings, select 'network mode' as Bridged (Advanced) and 'Bridged Interface' as en0 -> save & start.**
- ➔ In the VM, download Splunk Universal Forwarder using the same Splunk account through the wget link.
- ➔ Copy the link and execute the command below in the terminal.
  - ○ Paste the **wget link** and hit enter. (A directory with splunkforwarder is created, say <**abc**>)
  - ○ **tar xvzf <abc>** (extracts the compressed splunkforwarder file)
  - ○ **sudo mv splunkforwarder /opt** (moves splunkforwarder directory to /opt)
  - ○ Enter the system password
  - ○ **cd /opt/splunkforwarder**
  - ○ **./bin/splunk start –accept-license** (Accept the license and start the splunk forwarder)
  - ○ **./bin/splunk add forward-server 1.1.1.1:9997 <Host IP : Receiving Port Number>** (Add the forwarding IP details so that the indexer can catch the logs on the specific port)
  - ○ **./bin/splunk add monitor /var/log <directory that needs to be logged> -index linux_index <index name where the logs need to be indexed (optional)>**
  - ○ **./bin/splunk list forward-server** (lists the active and inactive server IPs)
  - ○ **./bin/splunk list monitor** (lists the directories that are being monitored)
  - ○ **./bin/splunk restart**
  - ○ **logger "This is TEST"**

Now go to the Host system, in the indexer, add a query as index=<index_name> (if not given while monitoring the logs, use the keyword "main"). Select the host as the hostname of the VM, and the logs of the VM can be seen in the index.
Since it is a Kali Linux system, syslog is not used.

- Traditional Linux systems (like Ubuntu, Debian) use rsyslog or syslog-ng, which writes logs to /var/log/syslog.
- Kali Linux (especially recent versions) uses systemd-journald by default instead of rsyslog.
- This means logs are stored in the systemd journal (in memory / binary format), not in plain-text files like /var/log/syslog.

Hence, "This is a TEST" log isn't seen in the logs.

To solve this, run the following commands

- **sudo apt install rsyslog -y**
- **sudo systemctl enable rsyslog**
- **sudo systemctl start rsyslog**
- **logger "This is a TEST"**
- **./bin/splunk restart**

This will help in logging the appropriate log files and provide the log "This is a TEST" in the Host machine within the Splunk Enterprise server.

Splunk Universal Forwarder (VM OS 2):

- ➔ Download Windows 10 .iso file. (Link) (To download the file, need to make changes in Chrome. **Inspect the page -> <Three dots> next to the close button on the top right in inspect element -> More Tools -> Network Conditions -> User agent -> Uncheck 'Use browser default' -> Select 'Chrome – Mac' or 'Chrome – Windows'** (as per the system's OS)**)**
- ➔ Open **UTM (VM) -> Create a New Virtual Machine -> Virtualize -> Windows -> Boot ISO image & browse for the downloaded .iso file -> 4 GB memory and 2 CPU cores -> 30 GB storage -> Select the shared directory path -> Check 'Open VM settings' & continue -> network tab in VM settings, select 'network mode' as Bridged (Advanced) and 'Bridged Interface' as en0 -> save & start.**
- ➔ Download the application, which will download a setup file.
- ➔ Run the setup file to install Splunk Universal Forwarder.
- ➔ Check the box to accept the License Agreement and select **an on-premise Splunk Enterprise instance.**
- ➔ **Select CUSTOMIZE OPTIONS.**
- ➔ Determine the path for the universal forwarder to be installed (Suggested: leave it the way it is).
- ➔ Click on Next in the SSL CERTIFICATE window since both Indexer and Forwarder lie in the local system.
- ➔ **Click on LOCAL SYSTEM.**
- ➔ Select the different types of logs that need to be indexed and click Next.
- ➔ Create credentials for the ADMIN account (Both username and password).
- ➔ Click on Next in the DEPLOYMENT SERVER window since the Indexer is on the local system and installing the universal forwarder for only the local system.

- ➔ In the Receiving Indexer window, provide the IP Address of the Host OS (where the Indexer is installed) and enter the port number as 9997 -> Install -> Finish.

The Splunk Universal Forwarder is now installed in the Windows VM on UTM. The Splunk universal forwarder would be started when installed, but to verify and restart it, the steps are as follows:

- ➔ Open PowerShell and run the commands below.
  - **cd /**
  - **cd 'Program files/SplunkUniversalForwarder/bin'** (Change the directory to the one where the forwarder was installed)
  - **./splunk status** (If it is running, 'SplunkForwarder: Running' message would appear)
  - **./splunk list forward-server** (To determine the active and inactive forward server at that instance)
  - **./splunk add forward-server 1.1.1.1:9997 <Host IP : Receiving Port Number>** (Add the forwarding IP details so that the indexer can catch the logs on the specific port)
  - **./splunk list monitor** (lists the directories that are being monitored)
  - **./splunk add monitor /var/log <directory that needs to be logged> -index linux_index <index name where the logs need to be indexed (optional)>**
  - **./splunk restart** (Restarts the forwarder)

Once these settings are configured, on the Host machine, over the Splunk Enterprise application, the logs from the Windows VM can be received and observed on Port 9997 over the 'Searching & Reporting' tab, based on the index entered in the search bar.