Inject 21

Centralized Log Reporting

Team 9

IT Manager,

We used Splunk 9.0.3 as our logging tool.

The way that we enabled logging using the centralized repository for Linux machines is as follows. Because our Linux servers are command line based, this sounds more technical than the Windows solution.

- First, we created a new user so we didn't run Splunk as root:

  useradd --system --disabed-login -m -d /opt/splunkforwarder --shell=/bin/su --group splunk

  cd /opt

  SPLUNKURL=$(whiptail --inputbox "What is the bit.ly URL? to download splunk?" --title "Splunk URL" 8 64 8 3>&1 1>&2 2>&3)

- Next, we set the home variable for Splunk to forward to:
  wget -O /opt/splunkforwarder.tgz $SPLUNKURL

  #whiptail --title "Splunk Download" --msgbox "Download Done, prepairing to extract" 8 44

  tar -xzf /opt/splunkforwarder.tgz

  #whiptail --title "Splunk Download" --msgbox "Extracting Complete" 8 44

  chown --recursive splunk:splunk /opt/splunkforwarder

- Here we set the permissions for the Splunk forwarder to make it secure:

  cd /opt/splunkforwarder/bin

  chmod 770 splunk

  ./splunk start --accept-license

  ./splunk enable boot-start -user splunk

- We add the forwarding server for the Linux server to forward its logs to Splunk

  FORWARDSERVER=$(whiptail --inputbox "What is the IP address and port number of the forwarder server?\nUse the format IP:Port. Default port is 9997" --title "Splunk Forwarder Configuratuib" 8 64 8 3>&1 1>&2 2>&3)

  ./splunk add forward-server $FORWARDSERVER

- We added /var/log for Splunk to monitor

  ./splunk add monitor /var/log

- Lastly, we restart the Splunk service to push the changes through.

  ./splunk restart

The commands we would use to enable logging to the Splunk server on a Windows machine are as follows:

- The first step was installing Splunk on the Windows server. Which can be done by downloading the latest version from the Splunk website and follow the installation instructions.

- Next, we would configure the Windows machine to send logs to Splunk: To do this, we have to install the Splunk Universal Forwarder on the Windows machine. The Universal Forwarder acts as a log collector and sends logs to the centralized Splunk repository.

- Then we would also have to install the Splunk Universal Forwarder: We were able to download the Universal Forwarder from the Splunk website and follow the installation instructions to install it on the Windows machine.

- Configure the Universal Forwarder to send logs to the centralized repository: After installing the Universal Forwarder, we need to configure it to send logs to the centralized repository which is our Splunk server. This can be done by editing the inputs.conf file in the Universal Forwarder's app directory. In this file, we need to specify the log files you want to send to Splunk and the Splunk server's IP address.

- Start the Universal Forwarder: Once we completed the configuration, we started the Universal Forwarder service. It will start collecting logs from the Windows machine and send them to the centralized repository.

- Verify logs in Splunk: Finally, we would log in to the Splunk interface and verify that the logs from the Windows machine are being received and displayed.

Unfortunately, we were unable to get our central logging application configured properly, but we will continue to work on it.

Thank you,

Team 9