**Universal Forwarder Deployment:**

## Install and Configure Splunk Universal Forwarder: Debian Linux

**Run the following commands to download and install the Universal Forwarder**

wget -O splunkforwarder-8.1.2-545206cc9f70-linux-2.6-amd64.deb 'https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86\_64&platform=linux&version=8.1.2&product=universalforwarder&filename=splunkforwarder-8.1.2-545206cc9f70-linux-2.6-amd64.deb&wget=true'

* dpkg -i splunk\_package\_name.deb

**Once installed, run the following commands to configure the forwarder to monitor and send logs to the receiving host**

* cd /opt/splunkforwarder/bin
* ./splunk start --accept-license
  + This prompts you to create a Splunk user, this is only for the forwarder, not splunk host.
* ./splunk add forward-server <host name or ip address>:<listening port>
* ./splunk add monitor /etc/passwd
* ./splunk restart

## Install and Configure Splunk Universal Forwarder: Red Hat Linux

**Run the following commands to download and install the Universal Forwarder**

wget -O splunkforwarder-8.1.1-08187535c166-linux-2.6-x86\_64.rpm '<https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&platform=linux&version=8.1.1&product=universalforwarder&filename=splunkforwarder-8.1.1-08187535c166-linux-2.6-x86_64.rpm&wget=true>'

* rpm -i splunkforwarder-<…>-linux-2.6-x86\_64.rpm

**Once installed, run the following commands to configure the forwarder to monitor and send logs to the receiving host**

* cd /opt/splunkforwarder/bin
* ./splunk start --accept-license
  + This prompts you to create a Splunk user, this is only for the forwarder, not splunk host.
* ./splunk add forward-server <host name or ip address>:<listening port>
* ./splunk add monitor /etc/passwd
* ./splunk restart

## Install and Configure Splunk Universal Forwarder: Windows

**Prepare the System**

1. Create a security group for the user that you want to run the universal forwarder as.
2. Add the user you want the universal forwarder to run as to this group.
3. (Optional) Set up the universal forwarder user as a managed service account.
4. Use the Group Policy Management Console to create and configure Group Policy or Local Security Policy objects for user rights assignments.
5. Use the Group Policy Management Console to assign appropriate security rights to the universal forwarder user.
6. If you use Active Directory, deploy the Group Policy objects with the updated settings.

**Run the following commands to download and install the Universal Forwarder**

wget -O splunkforwarder-8.1.1-08187535c166-x64-release.msi '<https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&platform=windows&version=8.1.1&product=universalforwarder&filename=splunkforwarder-8.1.1-08187535c166-x64-release.msi&wget=true>'

* msiexec.exe /i splunkuniversalforwarder\_x86.msi RECEIVING\_INDEXER="indexer1:9997" WINEVENTLOG\_SEC\_ENABLE=1 WINEVENTLOG\_SYS\_ENABLE=1 AGREETOLICENSE=Yes /quiet
  + Installs the universal forwarder, enable indexing of the Windows security and system event logs, and run the installer in silent mode

## Install and Configure Syslog-NG on Linux

* <https://www.syslog-ng.com/community/b/blog/posts/introducing-the-syslog-ng-stable-rpm-repositories>

yum install epel-release

wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm

rpm -Uvh epel-release-latest-7.noarch.rpm

cd /etc/yum.repos.d/

wget <https://copr.fedorainfracloud.org/coprs/czanik/syslog-ng-stable/repo/epel-7/czanik-syslog-ng-stable-epel-7.repo>

yum install syslog-ng

systemctl enable syslog-ng

systemctl start syslog-ng