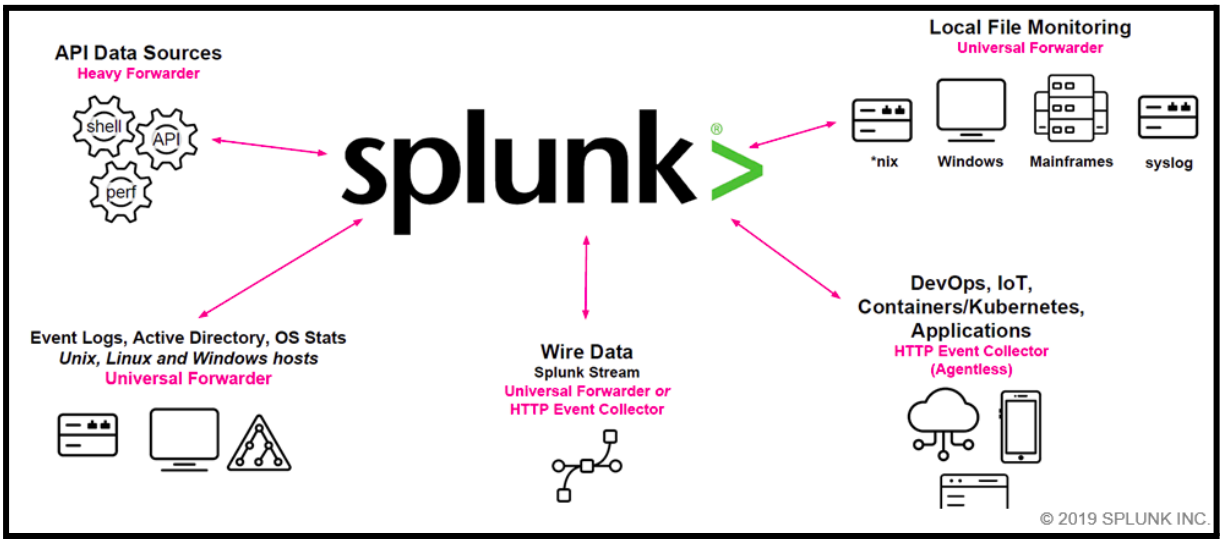
Guía de Configuración de Splunk Enterprise en Ubuntu
Introducción



Splunk Enterprise es una plataforma poderosa para analizar y visualizar datos generados por máquinas. Ofrece información en tiempo real, permitiendo tomar decisiones informadas. En esta guía, se detalla el proceso de instalación de Splunk Enterprise en Ubuntu, una de las distribuciones Linux más populares.

Paso 1: Requisitos Previos
Antes de comenzar, asegúrese de que su sistema Ubuntu cumpla con los siguientes requisitos:

1. Una versión soportada de Ubuntu (por ejemplo, Ubuntu 20.04 LTS).
2. Espacio en disco y recursos del sistema suficientes.
3. Acceso a internet para descargar el paquete de Splunk Enterprise.

Paso 2: Descargar Splunk Enterprise

1. Abra un navegador web y navegue al sitio web de Splunk: https://www.splunk.com.
2. Cree una cuenta o inicie sesión en su cuenta.
3. En la sección de Productos, haga clic en "Free Trials & Downloads".
4. Desplácese hacia abajo y, en Splunk Enterprise, haga clic en "Get My Free Trial".
5. Seleccione la versión apropiada de Splunk Enterprise para Linux (64 bits) y elija el formato de paquete Debian (.deb).
6. Cancele el proceso de descarga y haga clic en "Download via Command Line (wget)".
7. Haga clic en 'here' para copiar el comando completo.

Paso 3: Instalar Splunk Enterprise

Abra una terminal en su sistema Ubuntu.
Navegue al directorio de Descargas donde se descargará el paquete de Splunk Enterprise:
cd Downloads

Pegue y ejecute el comando obtenido del sitio de Splunk para descargar Splunk Enterprise.
Para ver el archivo descargado, escriba:
#ls

Ejecute el siguiente comando para instalar Splunk Enterprise:
#sudo apt install ./splunk<version>.deb

Nota: Reemplace <version> con el número de versión actual del paquete de Splunk Enterprise descargado.

Después de completar la instalación, inicie Splunk Enterprise ejecutando:
sudo /opt/splunk/bin/splunk start --accept-license

Escriba 'y' para aceptar la licencia.
Splunk Enterprise le pedirá que cree una contraseña de administrador. Siga las instrucciones para establecer una contraseña segura.

Paso 4: Acceder a la Interfaz Web de Splunk Enterprise
Inicie la interfaz web de Splunk ejecutando:
sudo /opt/splunk/bin/splunk start

Después de cargar, haga clic derecho en el enlace junto a "The Splunk web interface is at" y seleccione "Abrir Enlace".

Debería aparecer la página de inicio de sesión de Splunk Enterprise. Ingrese el nombre de usuario y la contraseña que configuró en el Paso 3.

Una vez dentro, puede comenzar a utilizar Splunk Enterprise para ingerir, buscar y analizar sus datos.