Anexo 2

Despliegue de Netskope CE en Red Hat 9

Jordi Guillem Ferrer Bozzano
Máster Universitario en Ciberseguridad y Privacidad
Seguridad empresarial

Iñaki Moreno Fernández
Víctor García Font

10 de enero de 2023

Despliegue de Netskope CE en Red Hat 9

1. **INSTALACIÓN DE NETSKOPE CLOUD EXCHANGE** 3
2. **AÑADIR EL TENANT DE NETSKOPE** 7
3. **CONFIGURACIÓN DE LOG SHIPPER** 8
4. **REFERENCIAS** 11

ÍNDICE DE ILUSTRACIONES

ILUSTRACIÓN 1: SELECCIÓN DE VERSIÓN EN LA INSTALACIÓN NETSKOPE CE 4
ILUSTRACIÓN 2: ESPECIFICAR NOMBRE TENANT EN LA INSTALACIÓN DE NETSKOPE CE 4
ILUSTRACIÓN 3: ESPECIFICAR PROTOCOLO Y PUERTO PARA EL NETSKOPE CE UI 4
ILUSTRACIÓN 4: INTRODUCIR CREDENCIALES TOKEN Y MONGODB PARA NETSKOPE CE 5
ILUSTRACIÓN 5: EJECUTAR INSTALACIÓN DE NETSKOPE CE 5
ILUSTRACIÓN 6: VENTANA INICIAL DE NETSKOPE CE UI 6
ILUSTRACIÓN 7: AÑADIR TENANT EN NETSKOPE CE UI 7
ILUSTRACIÓN 8: VISTA DE TENANT EN NETSKOPE CE UI 7
ILUSTRACIÓN 9: ACTIVACIÓN DE MÓDULO LOG SHIPPER EN NETSKOPE CE UI 8
ILUSTRACIÓN 10: SELECCIÓN DE PLUGINS PARA LOG SHIPPER 8
ILUSTRACIÓN 11: CONFIGURACIÓN DE PLUGIN DE NETSKOPE PARA LOG SHIPPER 9
ILUSTRACIÓN 12:CONFIGURACIÓN DE PLUGIN DE IBM QRADAR PARA LOG SHIPPER 9
ILUSTRACIÓN 13: CREACIÓN DE MAPPING DE LOG SHIPPER 10

1. Instalación de Netskope Cloud Exchange

La instalación de Netskope Cloud Exchange se realiza desde un sistema operativo Red Hat 9 actualizado con los últimos paquetes del repositorio oficial de Red Hat. Los pasos para poder instalar Netskope CE son los siguientes:

1.1. Instalar los requisitos correspondientes a Red Hat 9:

#> yum -y install podman podman-compose podman-plugins python3

1.2. Asegurarse que el idioma del sistema esté en inglés.

#> echo $LANG

En el caso que no esté en inglés ejecutar el siguiente comando:

#> localectl set-locale LANG=*en_US*

1.3. Clonar el proyecto GIT:

#> mkdir /opt/netskope

#> git clone https://github.com/netskopeoss/ta_cloud_exchange

1.4. Ejecutar el comando de configuración de Netskope CE:

#> cd /opt/netskope/ta_cloud_exchange

#> python3 ./setup

1.5. Seleccionar la versión CE v4-latest:

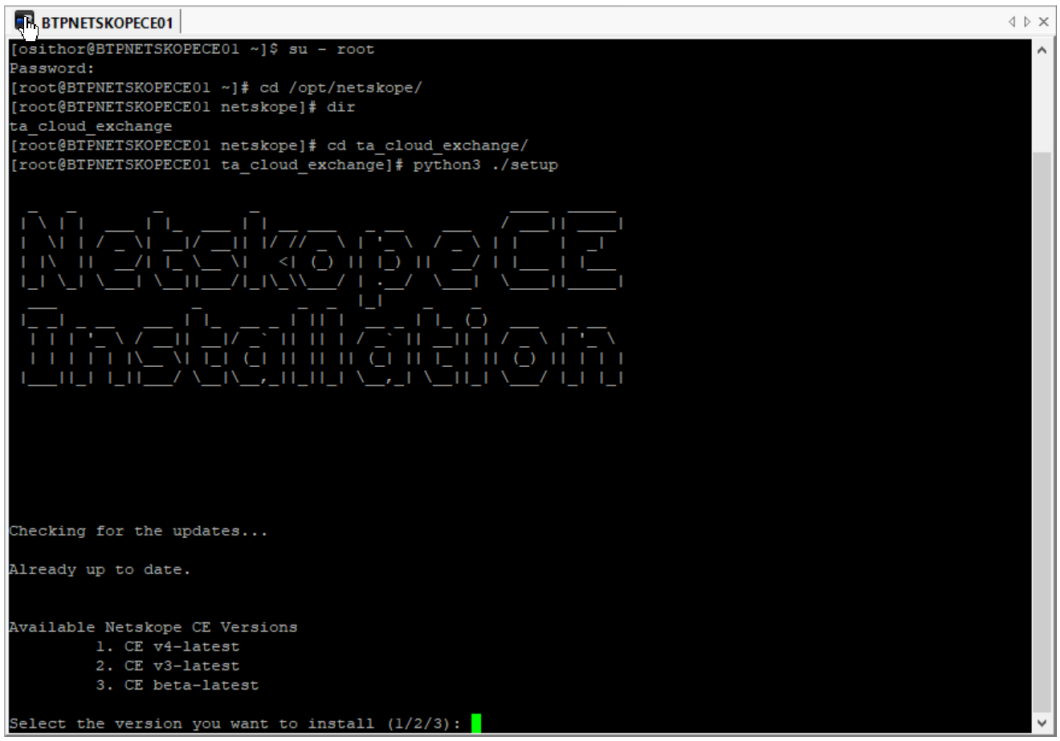

Ilustración 1: Selección de versión en la Instalación Netskope CE

1.6. Especificar el nombre del tenant de Netskope zanomme.eu

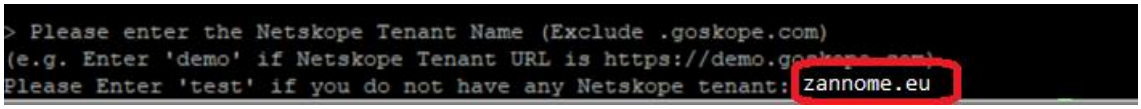

Ilustración 2: Especificar nombre tenant en la instalación de Netskope CE

1.7. Elegir el protocolo cifrado HTTPS y el puerto 443 para el acceso a la consola de Netskope CE:

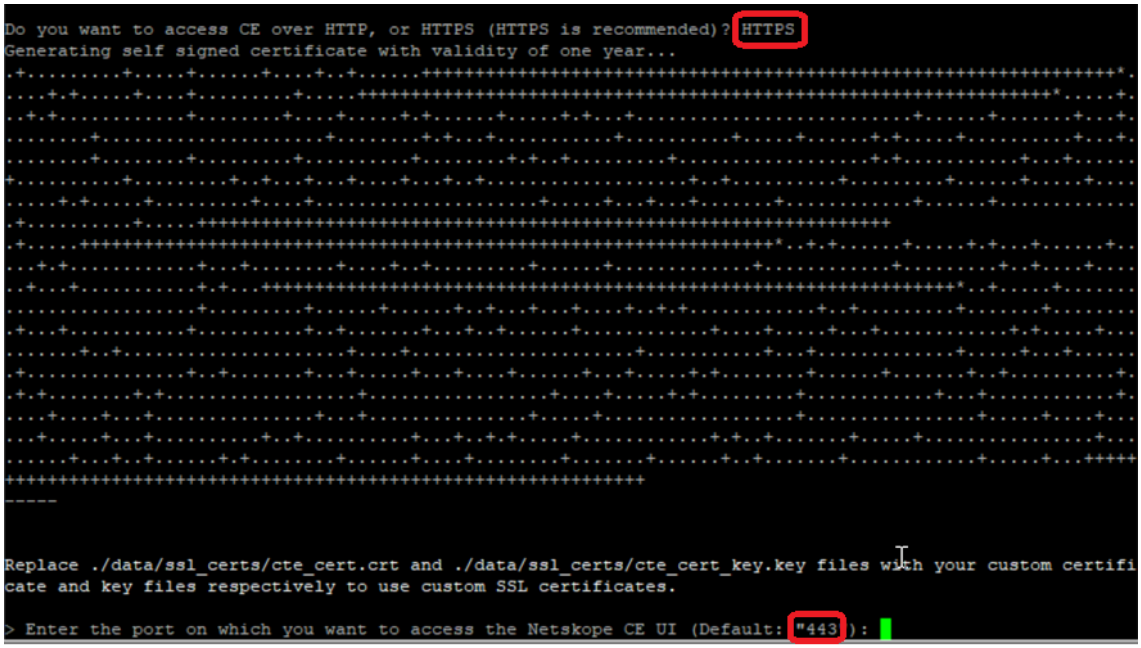

Ilustración 3: Especificar protocolo y puerto para el Netskope CE UI

1.8. Especificar la contraseña para el **JSON Web Secret** (JWT Secret) y el **Maintenance password** que se usará para Rabbit y MongoDB:

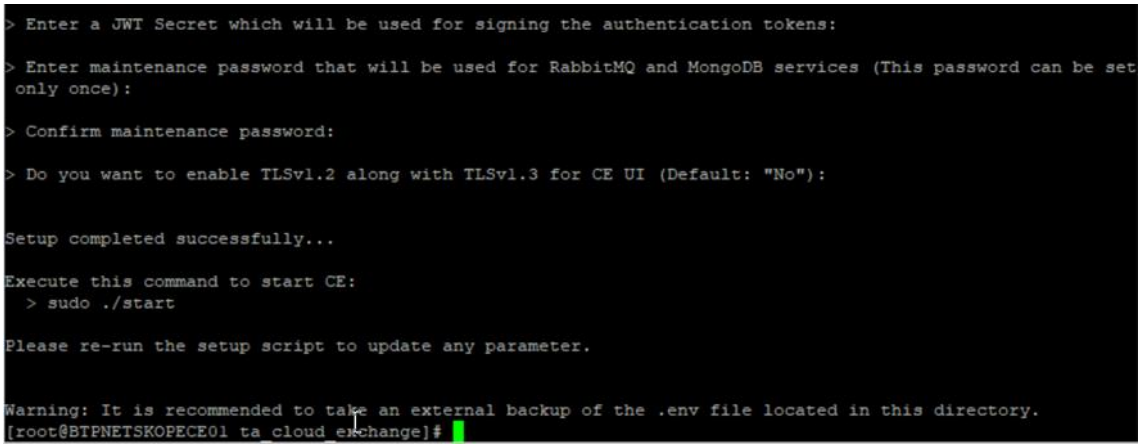

Ilustración 4: Introducir credenciales token y MongoDB para Netskope CE

1.9. Ejecutar comando de instalación con ./start, la salida es la siguiente:

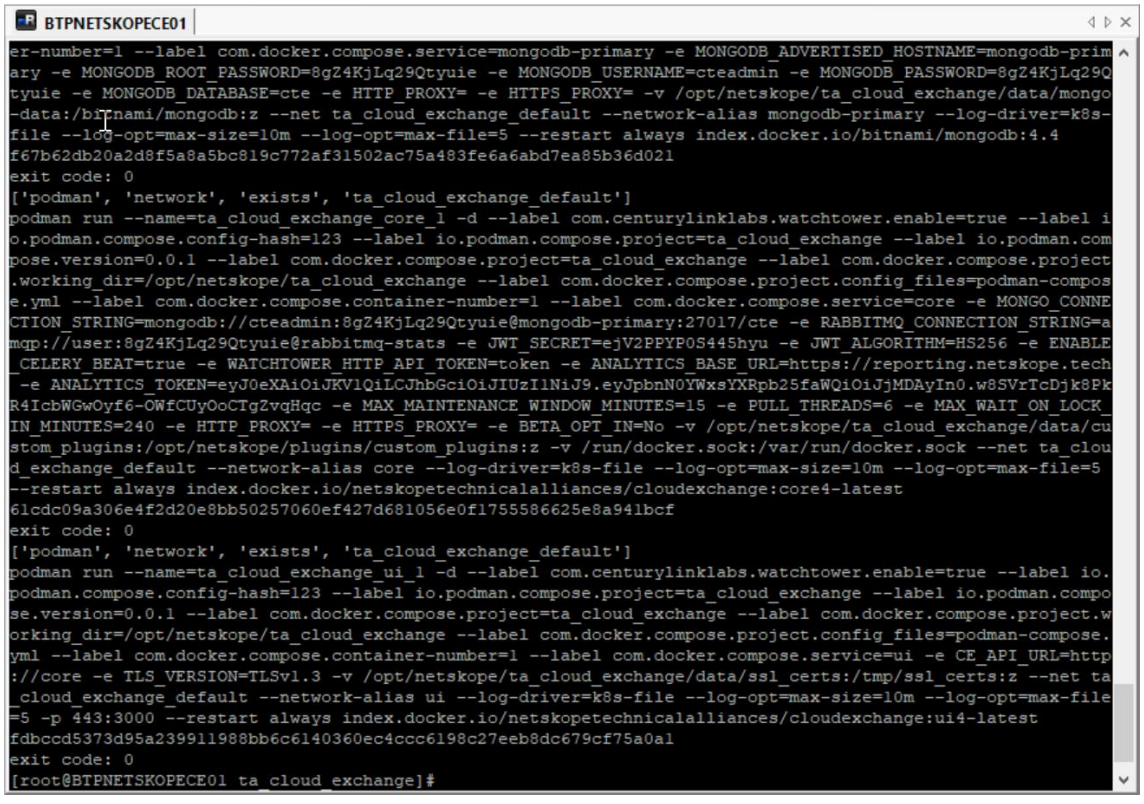

Ilustración 5: Ejecutar instalación de Netskope CE

Todos los *exit codes* deberán estar en 0 para saber si la instalación ha sido satisfactoria.

1.10. Comprobar el acceso a Netskope CE UI mediante la URL correspondiente https://btpnetskopece01.tous.net

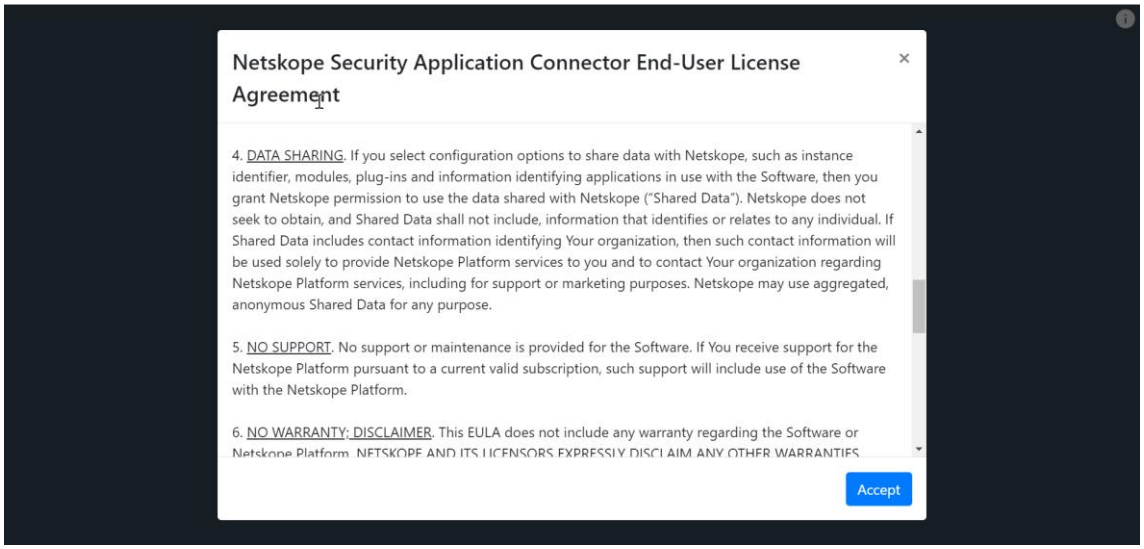

Ilustración 6: Ventana inicial de Netskope CE UI

2. Añadir el tenant de Netskope

2.1. Es necesario asociar el Netskope Cloud Exchange con el tenant de Netskope, para ello hay que obtener los API v1 y v2 del tenant e introducirlos dentro de los campos de creación en **Settings** > **Netskope tenants** > **Add Tenant** (En la imagen no se muestra la información de API Token)

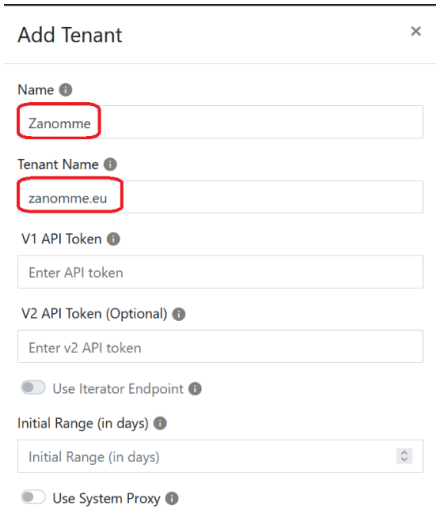

Ilustración 7: Añadir tenant en Netskope CE UI

2.2. Comprobar la creación del *tenant* como se muestra en la imagen siguiente:

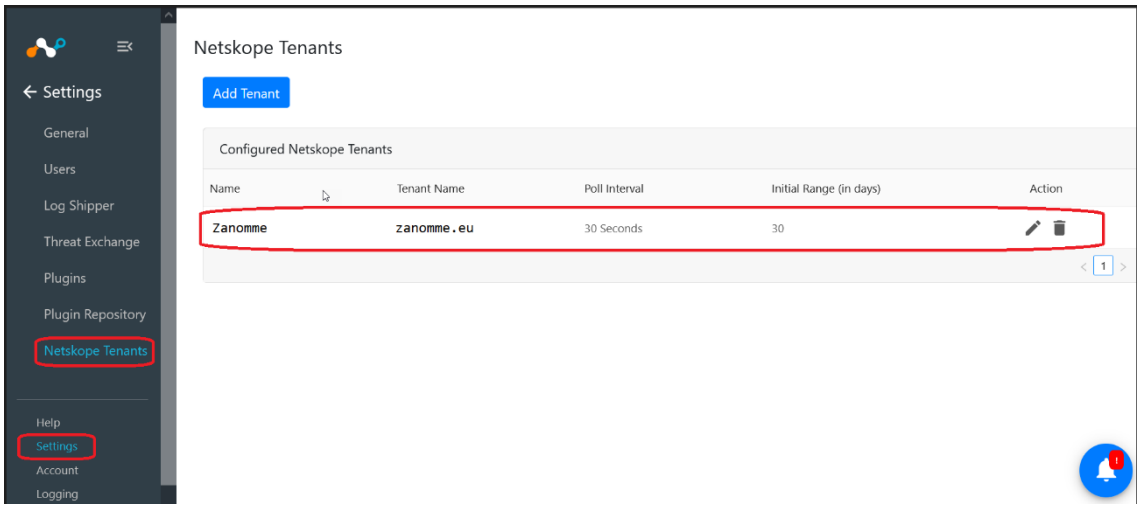

Ilustración 8: Vista de tenant en Netskope CE UI

3. Configuración de Log Shipper

3.1. Activar el módulo de Log Shipper en **Settings** > **General** > **Log Shipper:**

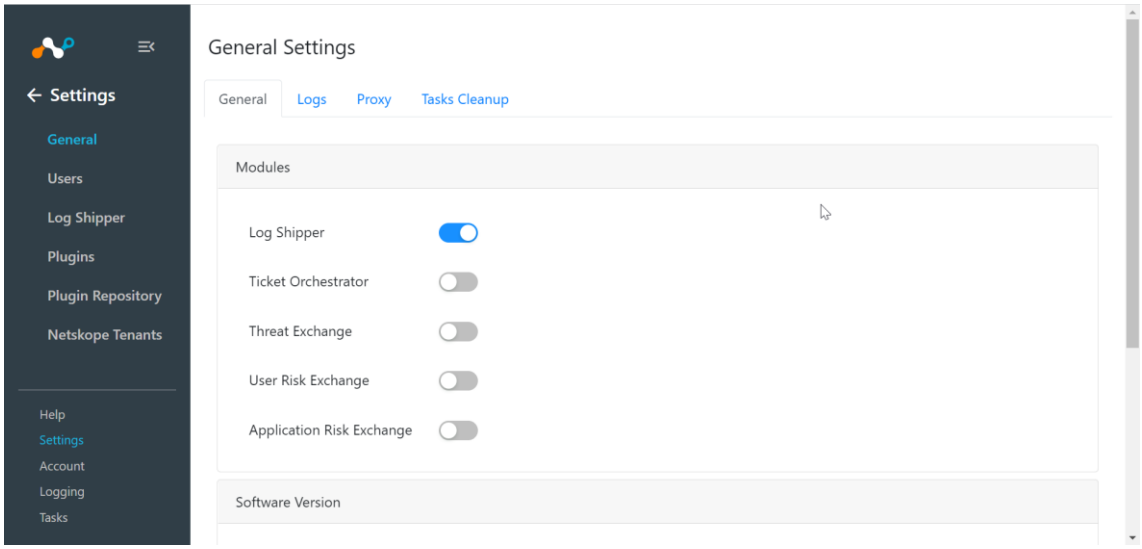

Ilustración 9: Activación de módulo Log Shipper en Netskope CE UI

3.2. Seleccionar los plugins necesarios desde **Settings** > **Plugins** en este caso se selecciona el correspondiente de **Netskope** y el de **IBM Security QRadar:**

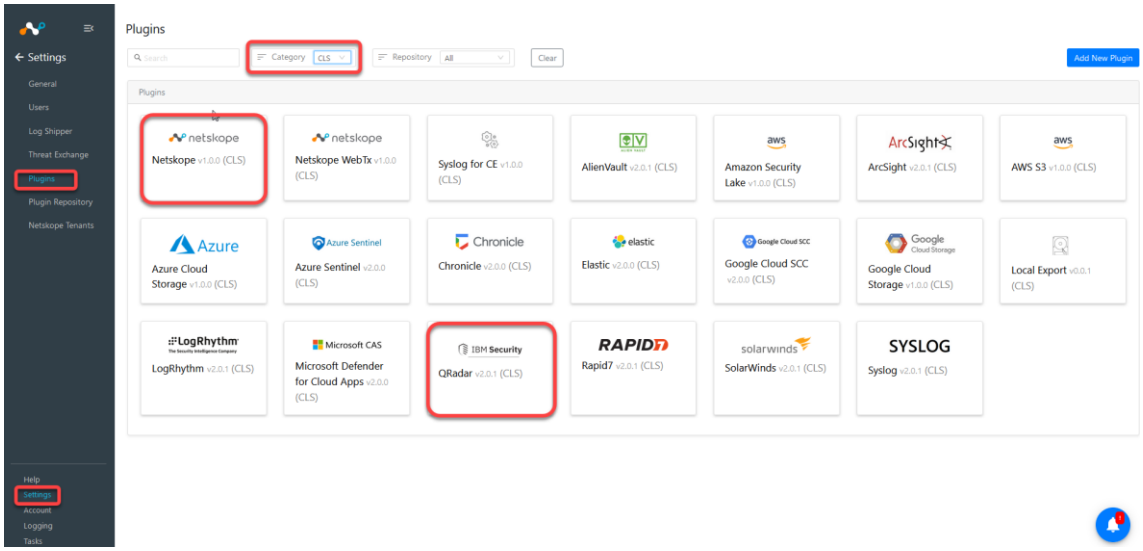

Ilustración 10: Selección de plugins para Log Shipper

3.3. Configurar el correspondiente a Netskope:

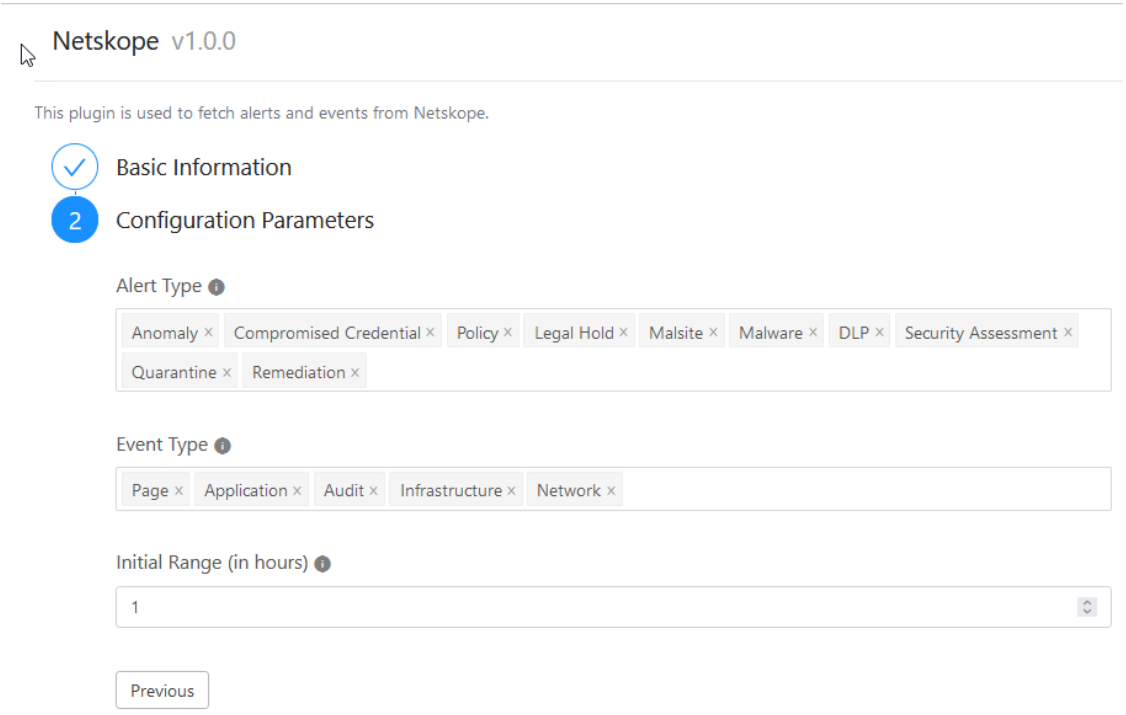

Ilustración 11: Configuración de plugin de Netskope para Log Shipper

3.4. Configurar el plugin de IBM Security QRadar, en el caso del laboratorio realizado en este proyecto se especifica la IP del colector interno el cual acepta conexiones Syslog en la red interna, este colector interno enviará los eventos al Cloud de IBM Qradar:

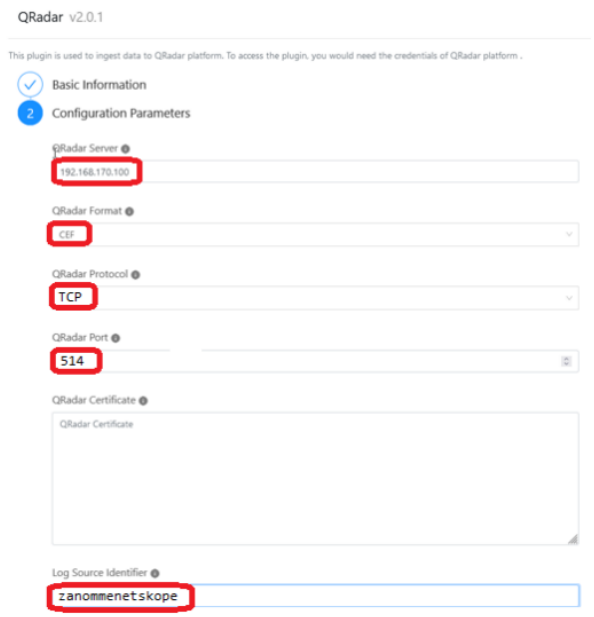

Ilustración 12:Configuración de plugin de IBM Qradar para Log Shipper

3.5. Desde **Log Shipper** > **SIEM Mappings** crear el *mapping* correspondiente al origen **zanomme** (Netskope Plugin) y como destino al **SIEMSOC**.

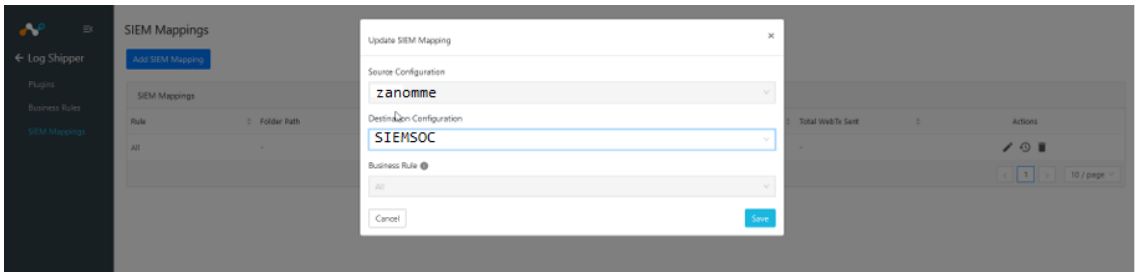

Ilustración 13: Creación de mapping de Log Shipper

3.6. Una vez guardado el *mapping* los eventos del tenant de Netskope se deberían de empezar a recibir en el colector interno de IBM QRadar para poder enviarlo definitivamente al Cloud SIEM de QRadar.

4. Referencias

Netskope Cloud Exchange. (s. f.). https://docs.netskope.com/en/netskope-cloud-exchange.html