

Procedimiento para configurar jump server

¿Cómo configurar un jump server?

A continuación, desarrollaremos el script con los pasos a seguir para la configuración de un jump server para entrar directamente a los dispositivos y extraer sus configuraciones para el módulo opConfig:

Primero, asegúrate que en el jump server, estén habilitadas las siguientes opciones en el archivo `/etc/ssh/sshd_config`

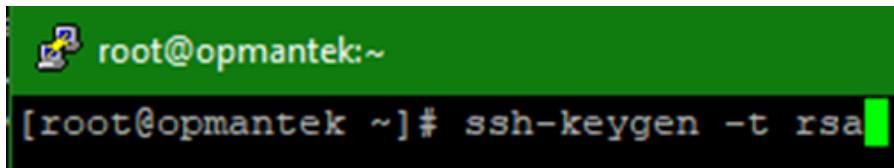
```
RSAAuthentication yes
PubkeyAuthentication yes
```

Así como el comando terminal `length 0`. Debe de mostrarte algo como esto

```
RP/0/RP0/CPU0:CUA-CORE-R01#terminal length 0

Mon Mar
12 18:08:27.389 CST
```

Entrar al servidor de NMIS con las credenciales correspondientes. Una vez dentro, generar la llave para el IdentityFile con el comando `ssh-keygen -t rsa`



```
root@opmantek:~
[root@opmantek ~]# ssh-keygen -t rsa
```

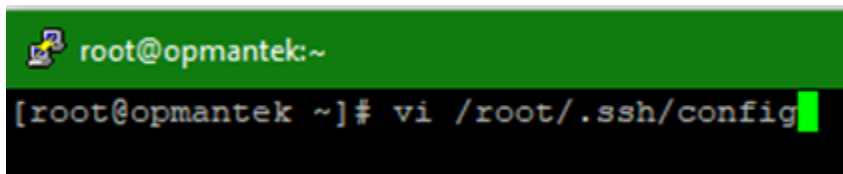
Identificar la ruta de la llave:

```
cd /root/.ssh/
```

Podemos ver el contenido con

```
cat ~/.ssh/id_rsa.pub
```

Ya una vez creada la llave, generamos el archivo config en `/root/.ssh/`



```
root@opmantek:~
[root@opmantek ~]# vi /root/.ssh/config
```

Ya que estemos en la edición de este, agregamos:

```
host <jump box IP address>
    User <jump box user name>
    Port #####
    IdentityFile /root/.ssh/key

host <node IP address>
    ProxyCommand ssh <jump box IP address> -W %h:%p
```

En el cual:

- <jump box IP address> es la dirección IP del servidor pivote
- <jump box user name> el usuario SSH para acceder al pivote
- Port ##### es el número del puerto del servidor pivote
- /root/.ssh/key ruta de la llave generada más adelante
- <node IP address> dirección IP del nodo a probar

Ejemplo:

```

root@opmantek:~
host 189.216.6.14
    User root
    Port 29292
    IdentityFile /root/.ssh/id_rsa

host 189.216.3.254
    ProxyCommand ssh 189.216.6.14 -W %h:%p

```

Ahora, copiamos la llave al servidor pivote con alguno de los siguientes comandos:

```

ssh-copy-id -i /home/user_name/.ssh/id_rsa.pub hostname
ssh-copy-id -i your_public_key user@host

```

Podemos probar si funciona, entrando vía SSH a un nodo directamente y ahí nos va a pedir las credenciales de acceso **para el nodo**, no para el jump server.

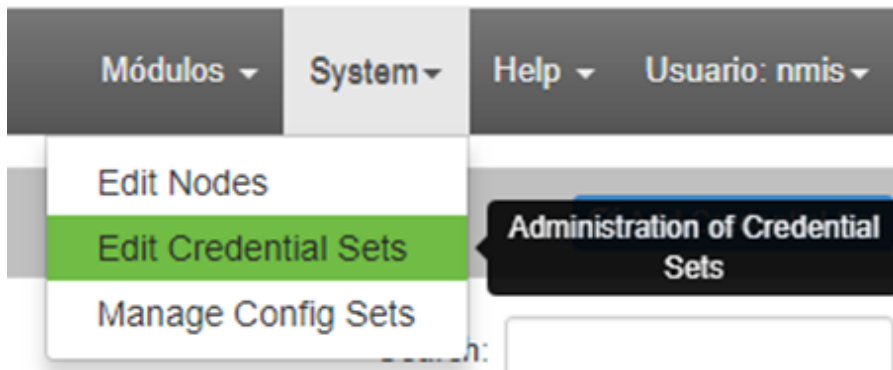
```

ssh USUARIOSSH@IPDELNODO

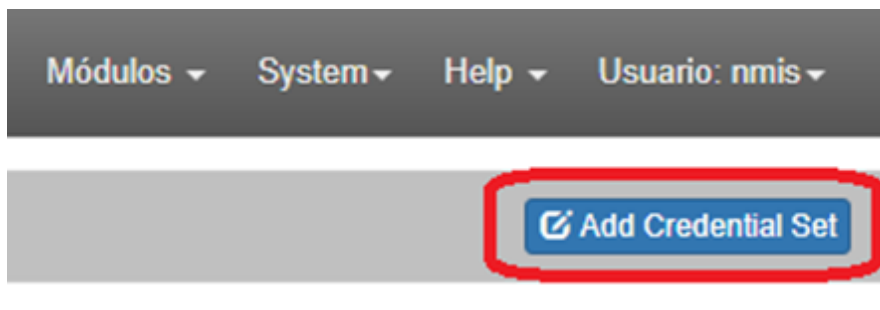
```

Ahora, en el servidor de opConfig, accedemos con las credenciales correspondientes.

Vamos a **System > Edit Credential Sets**



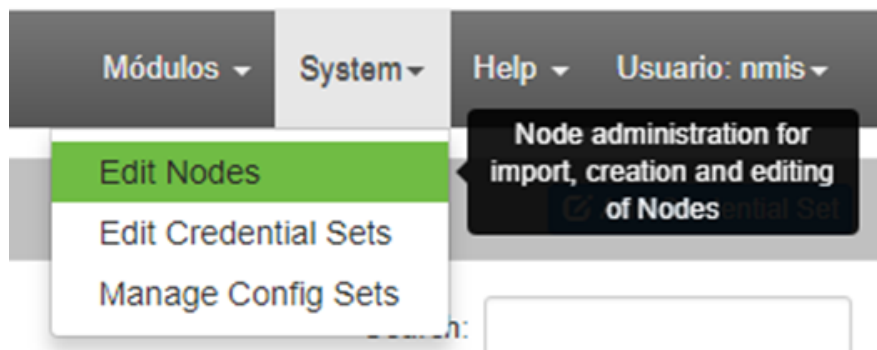
Damos clic en **Add Credential Set**



Agregamos la nueva credencial SSH para los dispositivos y damos clic en **Salvar Grupo de Credenciales**

A screenshot of a form titled 'Agregar Set de Credenciales'. The form contains several input fields: 'Nombre' (Nueva credencial), 'Descripcion' (Nueva descripción), 'User Name' (usuarioss), 'Codigo de Acceso' (Enter New Codigo de Acceso), 'Password (Superuser/Privileged/Enable)' (masked with dots), and 'SSH Key' (Enter New SSH Key). Each field has a question mark icon to its right. Below the fields, there are two buttons: 'Cancelar' and 'Salvar Grupo de Credenciales'. The text 'Current State: Not Set!' is visible below the 'Codigo de Acceso', 'Password', and 'SSH Key' fields.

Ahora vamos a **System > Edit Nodes**



Seleccionamos el nodo al que le vamos a asignar la credencial que acabamos de crear.

Nombre	Grupo	Ubicacion	Cliente	BusinessService	Nodo	Direcciones
Acapulco_BACKBONE_DD	RDS_CISCO	default	Opmantek		10.99.7.1	10.99.7.1, 10.99.18.162, 172.31.127.149, 10.99.18.193, 10.99.12.154, 10.0.0.2, 10.99.12.230, 10.99.12.234, 172.31.127.153, 10.99.12.145, 10.99.23.63

En **Conexión**, asignamos la nueva credencial SSH como se ve en la imagen. Damos clic en **Salvar Equipo**.

Nota: Es recomendable hacer un update del nodo, haciendo clic en **Actualizar Equipo desde NMIS** antes de asignar la credencial

Ahora, en consola, ejecutamos los siguientes comandos:

```
[root@opmantek ~]# /usr/local/omk/bin/opconfig-cli.exe act=discover node=NOMBREDELNODO
[root@opmantek ~]# /usr/local/omk/bin/opconfig-cli.exe act=run_command_sets node=NOMBREDELNODO
```

Con esto, quedarán configurados los nodos con las credenciales SSH correspondientes y ya podremos ver outputs en opConfig.

⚡ Command Output

```
Wed Feb 28 09:19:31.421 CST
Building configuration...
!! IOS XR Configuration 5.3.4
!! Last configuration change at Tue Feb 20 17:07:35 2018 by nperez
!
logging console debugging
logging buffered 2097152
logging buffered debugging
logging 192.168.202.58 vrf default severity info port default
logging source-interface Loopback0
service timestamps log datetime localtime msec show-timezone
service timestamps debug datetime localtime msec show-timezone
cdp
snmp-server traps selective-vrf-download role-change
end
```

<https://www.digitalocean.com/community/tutorials/how-to-configure-ssh-key-based-authentication-on-a-linux-server>