

Configuración de cifrados, MAC y algoritmos Kex en plataformas Nexus

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Revisar los cifrados, MAC y algoritmos Kex disponibles](#)

[Opción 1. Utilización de la línea CMD desde el PC](#)

[Opción 2. Acceder al archivo "dcos_sshd_config" mediante Feature Bash-Shell](#)

[Opción 3. Acceda al archivo "dcos_sshd_config" mediante el archivo Dplug](#)

[Solución](#)

[Paso 1. Exportar el archivo "dcos_sshd_config"](#)

[Paso 2. Importe el archivo "dcos_sshd_config"](#)

[Paso 3. Sustituya el archivo "dcos_sshd_config" original por el archivo Copy \(Copiar\)](#)

[Proceso manual \(no persistente en los reinicios\): todas las plataformas](#)

[Proceso automatizado: N7K](#)

[Proceso automatizado: N9K, N3K](#)

[Proceso automatizado: N5K, N6K](#)

[Consideraciones de plataforma](#)

[N5K/N6K](#)

[N7K](#)

[N9K](#)

[N7K, N9K, N3K](#)

Introducción

Este documento describe los pasos para agregar (o eliminar) cifrados, MAC y algoritmos Kex en las plataformas Nexus.

Prerequisites

Requirements

Cisco recomienda que comprenda los aspectos básicos de Linux y Bash.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software y hardware.

- Nexus 3000 y 9000 NX-OS 7.0(3)I7(10)
- Nexus 3000 y 9000 NX-OS 9.3(13)
- Nexus 9000 NX-OS 10.2(7)
- Nexus 9000 NX-OS 10.3(5)
- Nexus 7000 NX-OS 8.4(8)
- Nexus 5600 NX-OS 7.3(14)N1(1)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

A veces, los análisis de seguridad pueden detectar métodos de encriptación débiles que utilizan los dispositivos Nexus. Si esto sucede, se requieren cambios en el `dcos_sshd_config` archivo de los switches para eliminar estos algoritmos inseguros.

Revisar los cifrados, MAC y algoritmos Kex disponibles

Para confirmar qué Cifras, MAC y Algoritmos Kex utiliza una plataforma y verificar esto desde un dispositivo externo, puede utilizar estas opciones:

Opción 1. Utilización de la línea CMD desde el PC

Abra una línea CMD en un PC que pueda alcanzar el dispositivo Nexus y utilice el comando `ssh -vvv <hostname>`.

<#root>

```
C:\Users\xxxxx>ssh -vvv <hostname>
```

```
----- snipped -----
```

```
debug2: peer server KEXINIT proposal
```

```
debug2:
```

```
KEX algorithms: diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha1
```

```
debug2: host key algorithms: ssh-rsa
```

```
debug2: ciphers ctos: aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,aes192-cbc,aes256-cbc
```

```
debug2:
```

```
ciphers stoc: aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,aes192-cbc,aes256-cbc <--- encryption algorithms
```

```
debug2: MACs ctos: hmac-sha1
```

```
debug2:
```

```
MACs stoc: hmac-sha1 <--- mac algorithms
```

```
debug2: compression ctos: none,zlib@openssh.com
```

```
debug2:
```

```
compression stoc: none,zlib@openssh.com <--- compression algorithms
```

Opción 2. Acceda al archivo "dcos_sshd_config" mediante **Feature Bash-Shell**

Esto se aplica a:

- N3K ejecutando 7. X, 9. X, 10. X
- Todos los códigos N9K
- N7K con 8.2 y versiones posteriores

Pasos:

- Habilite la función bash-shell y entre en el modo bash:

```
switch(config)# feature bash-shell
switch(config)#
switch(config)# run bash
bash-4.3$
```

2. Revise el contenido del dcos_sshd_config archivo:

```
bash-4.3$ cat /isan/etc/dcos_sshd_config
```



Nota: Puede utilizar egrep para ver líneas específicas: `cat /isan/etc/dcos_sshd_config | grep MAC`

Opción 3. Acceso al archivo "dcos_sshd_config" mediante un archivo **Dplug**

Esto se aplica a:

- N3K ejecutando 6. X que no tiene acceso a bash-shell

- Todos los códigos N5K y N6K
- N7Ks ejecutando 6. X y 7. Códigos X

Pasos:

1. Abra un caso TAC para obtener el archivo dplug que coincida con la versión de NXOS que se ejecuta en el switch.
2. Cargue el archivo dplug en bootflash y cree una copia del mismo.

<#root>

switch# copy bootflash:

nuova-or-dplug-mzg.7.3.8.N1.1

bootflash:

dp



Nota: Se crea una copia ("dp") del archivo dplug original en bootflash, de modo que sólo se elimine la copia después de cargar dplug y el archivo dplug original permanezca en bootflash para las siguientes ejecuciones.

3. Cargue la copia del dplug a través del load comando.

<#root>

```
n5k-1# load bootflash:dp
Loading plugin version 7.3(8)N1(1)
#####
Warning: debug-plugin is for engineering internal use only!
```

For security reason, plugin image has been deleted.

```
#####  
Successfully loaded debug-plugin!!!  
Linux(debug)#  
Linux(debug)#
```

2. Revise el dcos_sshd_config archivo.

```
Linux(debug)# cat /isan/etc/dcos_sshd_config
```

Solución

Paso 1. Exportar el archivo "dcos_sshd_config"

1. Envíe una copia del dcos_sshd_config archivo a bootflash:

```
Linux(debug)# cd /isan/etc/  
Linux(debug)# copy dcos_sshd_config /bootflash/dcos_sshd_config  
Linux(debug)# exit
```

2. Confirme que la copia está en bootflash:

```
switch(config)# dir bootflash: | i ssh  
7372 Mar 24 02:24:13 2023 dcos_sshd_config
```

3. Exportar a un servidor:

```
switch# copy bootflash: ftp:  
Enter source filename: dcos_sshd_config  
Enter vrf (If no input, current vrf 'default' is considered): management  
Enter hostname for the ftp server: <hostname>  
Enter username: <username>  
Password:  
***** Transfer of file Completed Successfully *****  
Copy complete, now saving to disk (please wait)...  
Copy complete.
```

4. Realice los cambios necesarios en el archivo y vuelva a importar a bootflash.

Paso 2. Importe el archivo "dcos_sshd_config"

1. Cargue el archivo modificado dcos_sshd_config en la memoria flash de arranque.

```
switch# copy ftp: bootflash:
Enter source filename: dcos_sshd_config_modified.txt
Enter vrf (If no input, current vrf 'default' is considered): management
Enter hostname for the ftp server: <hostname>
Enter username: <username>
Password:
***** Transfer of file Completed Successfully *****
Copy complete, now saving to disk (please wait)...
Copy complete.
switch#
```

Paso 3. Sustituya el archivo "dcos_sshd_config" original por el archivo Copy (Copiar)

Proceso manual (no persistente en los reinicios): todas las plataformas

Sustituyendo el dcos_sshd_config archivo existente en /isan/etc/ por un archivo modificado dcos_sshd_config ubicado en bootflash. Este proceso no es persistente en los reinicios

- Cargue un archivo modificado ssh config en bootflash:

```
switch# dir bootflash: | i ssh
7372 Mar 24 02:24:13 2023 dcos_sshd_config_modified
```

2. Mientras esté en el modo bash o Linux(debug)#, sobrescriba el dcos_sshd_config archivo existente con el de bootflash:

```
bash-4.3$ sudo su
bash-4.3# copy /bootflash/dcos_sshd_config_modified /isan/etc/dcos_sshd_config
```

3. Confirme que los cambios se realizaron correctamente:

```
bash-4.3$ cat /isan/etc/dcos_sshd_config
```


Proceso automatizado: N7K

Utilizando un script EEM que se activa cuando el registro "VDC_MGR-2-VDC_ONLINE" aparece después de una recarga. Si se dispara el EEM, se ejecuta un script de pago y reemplaza el dcos_sshd_config archivo existente en /isan/etc/ por un archivo modificado dcos_sshd_config ubicado en la memoria de inicialización. Esto solo se aplica a las versiones de NX-OS compatibles con "feature bash-shell".

- Cargue un archivo ssh config modificado a bootflash:

```
<#root>
```

```
switch# dir bootflash: | i ssh  
7404 Mar 03 16:10:43 2023
```

```
dcos_sshd_config_modified_7k
```

```
switch#
```

2. Cree un script de pago que aplique los cambios al dcos_sshd_config archivo. Asegúrese de guardar el archivo con la extensión "py".

```
<#root>
```

```
#!/usr/bin/env python  
import os  
os.system("sudo usermod -s /bin/bash root")  
os.system("sudo su -c \"cp  
  
/bootflash/dcos_sshd_config_modified_7  
k /isan/etc/dcos_sshd_config\"")
```

3. Cargue el script Python en bootflash.

```
<#root>
```

```
switch# dir bootflash:///scripts  
175 Mar 03 16:11:01 2023
```

```
ssh_workaround_7k.py
```

Nota: Los scripts de Python son prácticamente iguales en todas las plataformas, excepto en N7K, que contiene algunas líneas adicionales para superar el ID de bug de Cisco [CSCva14865](#).

4. Asegúrese de que el `dcos_sshd_config` nombre de archivo de la secuencia de comandos y la memoria de inicialización (Paso 1.) son iguales:

```
<#root>
```

```
switch# dir bootflash: | i ssh
```

```
7404 Mar 03 16:10:43 2023
```

```
dcos_sshd_config_modified_7k
```

```
switch#
```

```
<#root>
```

```
switch# show file bootflash:///
```

```
scripts/ssh_workaround_7k.py
```

```
#!/usr/bin/env python
import os
os.system("sudo usermod -s /bin/bash root")
os.system("sudo su -c \"cp /
bootflash/dcos_sshd_config_modified_7k
/isan/etc/dcos_sshd_config\"")
switch#
```

4. Ejecute el archivo de comandos una vez, de modo que se cambie el dcos_sshd_config archivo.

```
<#root>
```

```
switch#
```

```
source ssh_workaround_7k.py
```

```
switch#
```

5. Configure un script EEM, de modo que el script py se ejecute cada vez que el switch se reinicia y vuelve a funcionar.

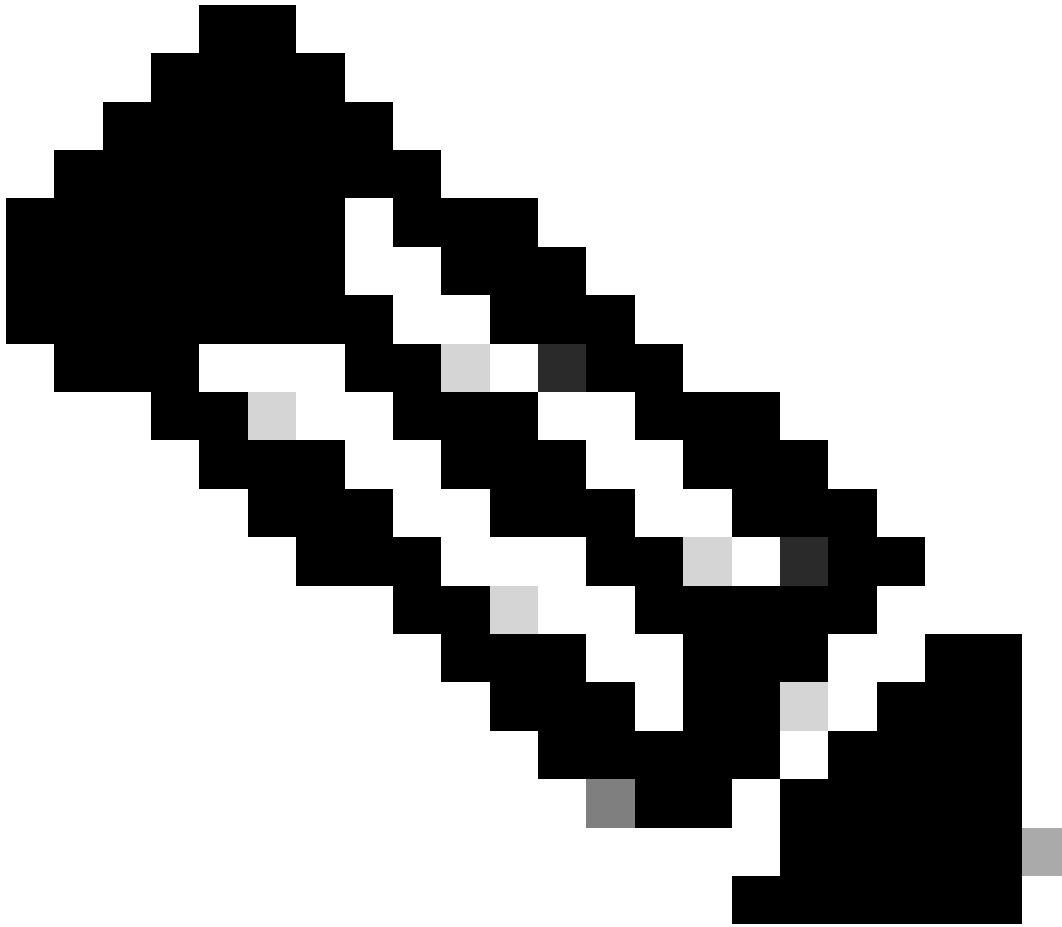
EEM N7K:

```
<#root>
```

```
event manager applet SSH_workaround
  event syslog pattern "vdc 1 has come online"
  action 1.0 cli command
```

```
"source ssh_workaround_7k.py"
```

```
  action 2 syslog priority alerts msg "SSH Workaround implemented"
```



Nota: La sintaxis de EEM puede variar en las distintas versiones de NXOS (algunas versiones requieren "CLI" y otras "CLI command"), por lo que debe asegurarse de comprobar que los comandos de EEM se ejecutan correctamente.

Proceso automatizado: N9K, N3K

- Cargue un archivo de configuración SSH modificado a bootflash.

<#root>

switch# dir | i i ssh

7732 Jun 18 16:49:47 2024 dcos_sshd_config

7714 Jun 18 16:54:20 2024

dcos_sshd_config_modified

switch#

2. Cree un script de pago que aplique los cambios al dcos_sshd_config archivo. Asegúrese de guardar el archivo con la extensión "py".

<#root>

```
#!/usr/bin/env python
```

```
import os
```

```
os.system("sudo su -c \"cp
```

```
/bootflash/dcos_sshd_config_modified
```

```
/isan/etc/dcos_sshd_config\"")
```

3. Cargue el script python en bootflash.

<#root>

```
switch# dir | i i .py
```

```
127 Jun 18 17:21:39 2024
```

ssh_workaround_9k.py

switch#

4. Asegúrese de que el dcos_sshd_config nombre de archivo de la secuencia de comandos y de bootflash (Paso 1.) es el mismo:

<#root>

```
switch# dir | i i ssh
```

```
7732 Jun 18 16:49:47 2024 dcos_sshd_config
```

```
7714 Jun 18 16:54:20 2024
```

dcos_sshd_config_modified

```
127 Jun 18 17:21:39 2024 ssh_workaround_9k.py
```

switch#

<#root>

```
switch# sh file bootflash:ssh_workaround_9k.py
```

```
#!/usr/bin/env python
import os
os.system("sudo su -c \"cp
/bootflash/dcos_sshd_config_modified
/isan/etc/dcos_sshd_config\"")
switch#
```

4. Ejecute el archivo de comandos una vez, de modo que se cambie el dcos_sshd_config archivo.

```
<#root>
```

```
switch#
```

```
python bootflash:ssh_workaround_9k.py
```

5. Configure un script EEM, de modo que el script py se ejecute cada vez que el switch se reinicia y vuelve a activarse.

EEM N9K y N3K:

```
<#root>
```

```
event manager applet SSH_workaround
 event syslog pattern "vdc 1 has come online"
 action 1.0 cli
```

```
python bootflash:ssh_workaround_9k.py
```

```
action 2 syslog priority alerts msg SSH Workaround implemented
```



Nota: La sintaxis de EEM puede variar en las distintas versiones de NXOS (algunas versiones requieren "CLI" y otras "CLI command"), por lo que debe asegurarse de comprobar que los comandos de EEM se ejecutan correctamente.

Proceso automatizado: N5K, N6K

Se creó un archivo dplug modificado mediante el ID de bug de Cisco [CSCyr23488](#) para eliminar estos algoritmos Kex:

- diffie-hellman-group-exchange-sha256
- diffie-hellman-group-exchange-sha1

- diffie-hellman-group1-sha1

Los archivos dpug provistos a través del ID de bug de Cisco [CSCvr23488](#) no son los mismos que se utilizan para acceder al Shell de Linux. Abra un caso TAC para obtener el dplug modificado del ID de bug Cisco [CSCvr23488](#).

- Compruebe la configuración predeterminada de `ssh_config`:

<#root>

```
C:\Users\user>ssh -vvv admin@<hostname>
```

```
---- snipped ----
```

```
debug2: peer server KEXINIT proposal
```

```
debug2:
```

```
KEX algorithms: ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-
```

```
<--- kex algorithms
```

```
debug2:
```

```
host key algorithms: ssh-rsa
```

```
debug2: ciphers ctos: aes128-ctr,aes192-ctr,aes256-ctr
```

```
debug2:
```

```
ciphers stoc: aes128-ctr,aes192-ctr,aes256-ctr
```

```
<--- encryption algorithms
```

```
debug2: MACs ctos: hmac-sha1
```

```
debug2:
```

```
MACs stoc: hmac-sha1
```

```
<--- mac algorithms
```

```
debug2: compression ctos: none,zlib@openssh.com
```

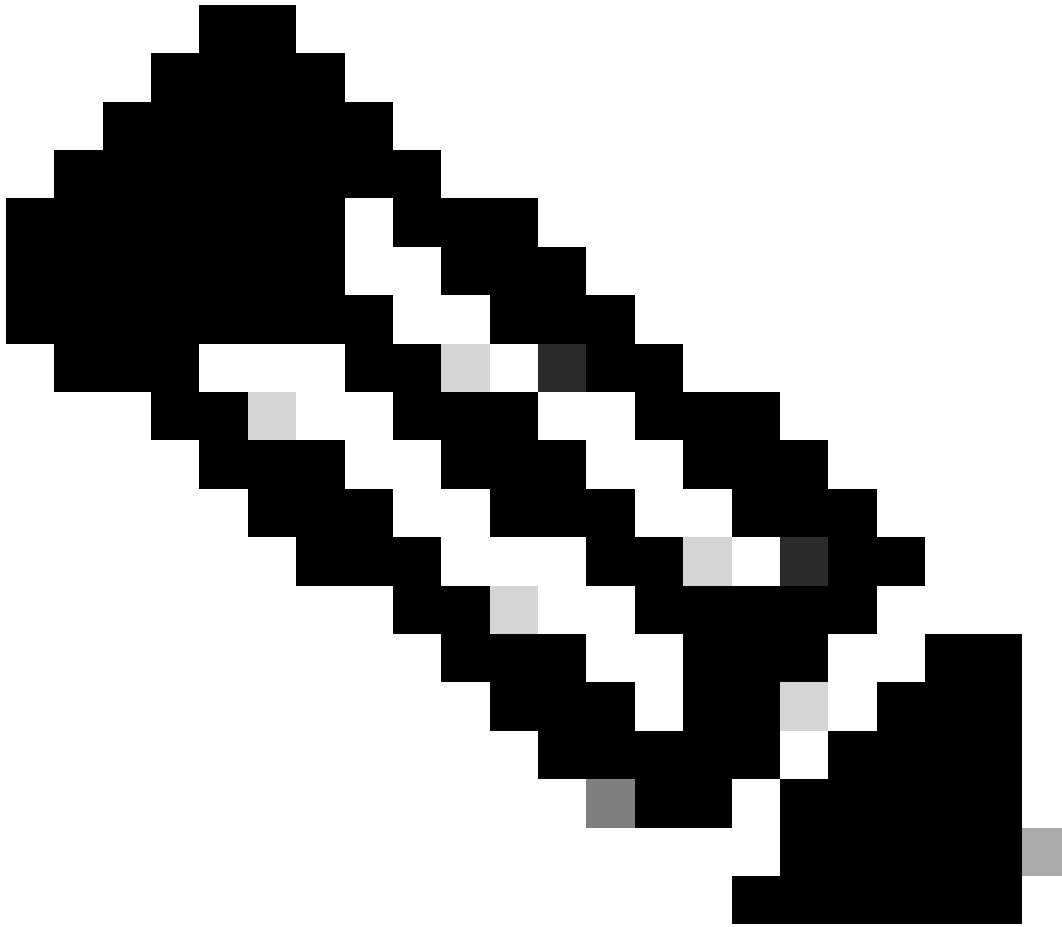
```
debug2:
```

```
compression stoc: none,zlib@openssh.com
```

```
<--- compression algorithms
```

2. Cree una copia del archivo dplug modificado.

```
switch# copy bootflash:nuova-or-dplug-mzg.7.3.14.N1.1_CSCvr23488.bin bootflash:dp
```

Nota: Se crea una copia ("dp") del archivo dplug original en bootflash para que sólo se elimine la copia después de cargar dplug y el archivo dplug original permanezca en bootflash para las ejecuciones posteriores.

3. Aplique el archivo dplug del ID de bug de Cisco [CSCvr23488](#) manualmente:

```
switch# load bootflash:dp2
Loading plugin version 7.3(14)N1(1)
#####
Warning: debug-plugin is for engineering internal use only!
For security reason, plugin image has been deleted.
#####
Successfully loaded debug-plugin!!!
```

Workaround for [CSCvr23488](#) implemented
switch#

4. Compruebe la nueva dcossd_config configuración:

<#root>

C:\Users\user>ssh -vvv admin@<hostname>

---- snipped ----

debug2: peer server KEXINIT proposal

debug2:

KEX algorithms: diffie-hellman-group14-sha1,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521

debug2: host key algorithms: ssh-rsa

debug2: ciphers ctos: aes128-ctr,aes192-ctr,aes256-ctr

debug2:

ciphers stoc: aes128-ctr,aes192-ctr,aes256-ctr

debug2: MACs ctos: hmac-sha1

debug2:

MACs stoc: hmac-sha1

debug2: compression ctos: none,zlib@openssh.com

debug2:

compression stoc: none,zlib@openssh.com

5. Haga que este cambio sea persistente en los reinicios con un script EEM:

event manager applet [CSCvr23488](#)_workaround

event syslog pattern "VDC_MGR-2-VDC_ONLINE"

action 1 cli command "copy bootflash:nuova-or-dplug-mzg.7.3.14.N1.1_CSCvr23488.bin bootflash:dp"

action 2 cli command "load bootflash:dp"

action 3 cli command "conf t ; no feature ssh ;feature ssh"

action 4 syslog priority alerts msg "CSCvr23488 Workaround implemented"



Nota:

- Después de aplicar el dplug modificado, la función SSH debe restablecerse en esta plataforma.
 - Asegúrese de que el archivo dplug esté presente en la memoria flash de inicialización y que EEM esté configurado con el nombre de archivo dplug adecuado. El nombre de archivo de dplug puede variar en función de la versión del switch, por lo que debe modificar la secuencia de comandos según sea necesario.
 - La acción 1 crea una copia del archivo dplug original en bootflash en otro archivo denominado "dp", de modo que el archivo dplug original no se elimina después de cargarse.
-

Consideraciones de plataforma

N5K/N6K

- MAC (Message Authentication Code) no se puede cambiar en estas plataformas mediante la modificación del archivo `dcos_sshd_config`. El único MAC soportado es `hmac-sha1`.

N7K

- Para cambiar los MAC, se requiere un código 8.4. Consulte ID de bug de Cisco [CSCwc26065](#) para obtener detalles.
- "Sudo su" no está disponible de forma predeterminada en 8.X. Referencia de ID de bug de Cisco: [CSCva14865](#). Si se ejecuta, se observa este error:

<#root>

```
F241.06.24-N7706-1(config)# feature bash-shell
F241.06.24-N7706-1(config)# run bash
bash-4.3$ sudo su
```

```
Cannot execute /isanboot/bin/nobash: No such file or directory <---
```

```
bash-4.3$
```

Para solucionar este problema, escriba:

<#root>

```
bash-4.3$
sudo usermod -s /bin/bash root
```

Después de esto "sudo su" funciona:

```
bash-4.3$ sudo su
bash-4.3#
```

Nota: este cambio no sobrevive a una recarga.

- Hay un archivo separado `dcos_sshd_config` para cada VDC, en caso de que los parámetros SSH deban modificarse en un VDC diferente, asegúrese de modificar el archivo correspondiente `dcos_sshd_config`.

<#root>

```
N7K# run bash
bash-4.3$ cd /isan/etc/
bash-4.3$ ls -la | grep ssh
-rw-rw-r-- 1 root root 7564 Mar 27 13:48
```

dcos_sshd_config

```
<--- VDC 1  
-rw-rw-r-- 1 root root 7555 Mar 27 13:48
```

dcos_sshd_config.2

```
<--- VDC 2  
-rw-rw-r-- 1 root root 7555 Mar 27 13:48
```

dcos_sshd_config.3

```
<--- VDC 3
```

N9K

- Los cambios en el dcos_sshd_config archivo no persisten durante los reinicios en cualquier plataforma Nexus. Si los cambios deben ser persistentes, se puede utilizar un EEM para modificar el archivo cada vez que el switch se inicia. La mejora en N9K cambia este inicio 10.4. Consulte ID de bug de Cisco [CSCwd82985](#) para obtener detalles.

N7K, N9K, N3K

Existen otros cifrados, MAC y KexAlgorithms que se pueden agregar si es necesario:

<#root>

```
switch(config)# ssh kexalgs all  
switch(config)# ssh macs all  
switch(config)# ssh ciphers all
```



Nota: estos comandos están disponibles en Nexus 7000 con las versiones 8.3(1) y posteriores. Para la plataforma Nexus 3000/9000, el comando está disponible en la versión 7.0(3)I7(8) y posteriores. (Todas las versiones 9.3(x) también tienen este comando. Consulte la [Guía de configuración de seguridad de NX-OS para Cisco Nexus serie 9000, versión 9.3\(x\)](#))

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).