تكوين التشفير و MAC و خوارزميات KEX في Nexus Platforms

المحتويات

المقدمة

يصف هذه الوثيقة الخطوات أن يضيف (أو) يزيل تشفير، MACs، وخوارزميات KEX في Nexus منصة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تفهم أساسيات Linux و Bash.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات المكونات المادية والبرامج التالية:

- نظام التشغيل Nexus 3000 و 9000 NX-OS 7.0(3)I7(10)
- Nexus 3000 و 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)

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

في بعض الأحيان، يمكن أن تجد عمليات المسح الأمني طرق تشفير ضعيفة تستخدم من هذه الإزالة بطولطة المفتوحات على الملف dcos_sshd_config. إذا حدث هذا، فإن التغييرات على أجهزة Nexus قبل آمنة غير الخوارزميات.

مراجعة التشفير المتاحة وخوارزميات MAC و KEX

لتأكيد خوارزميات التشفير، MAC، و KEX التي يستخدمها النظام الأساسي وتحقق من ذلك من جهاز خارجي يمكنك استخدام هذه الخيارات:

الخيار 1. إستخدام سطر CMD من الكمبيوتر الشخصي

فتح طخ CMD على جهاز كمبيوتر شخصي يمكنه الوصول إلى جهاز Nexus واستخدام الأمر 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-sha

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 algorith

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

الخيار 2. قم بالوصول إلى ملف "dcos_sshd_config" باستخدام ميزة **BaseH-Shell**

ينطبق هذا على:

- N3K يتم تشغيله 7. X، 9. X، 10. X
- N9K زومر كافة
- N7K تشغل الإصدار 8.2 والإصدارات الأحدث

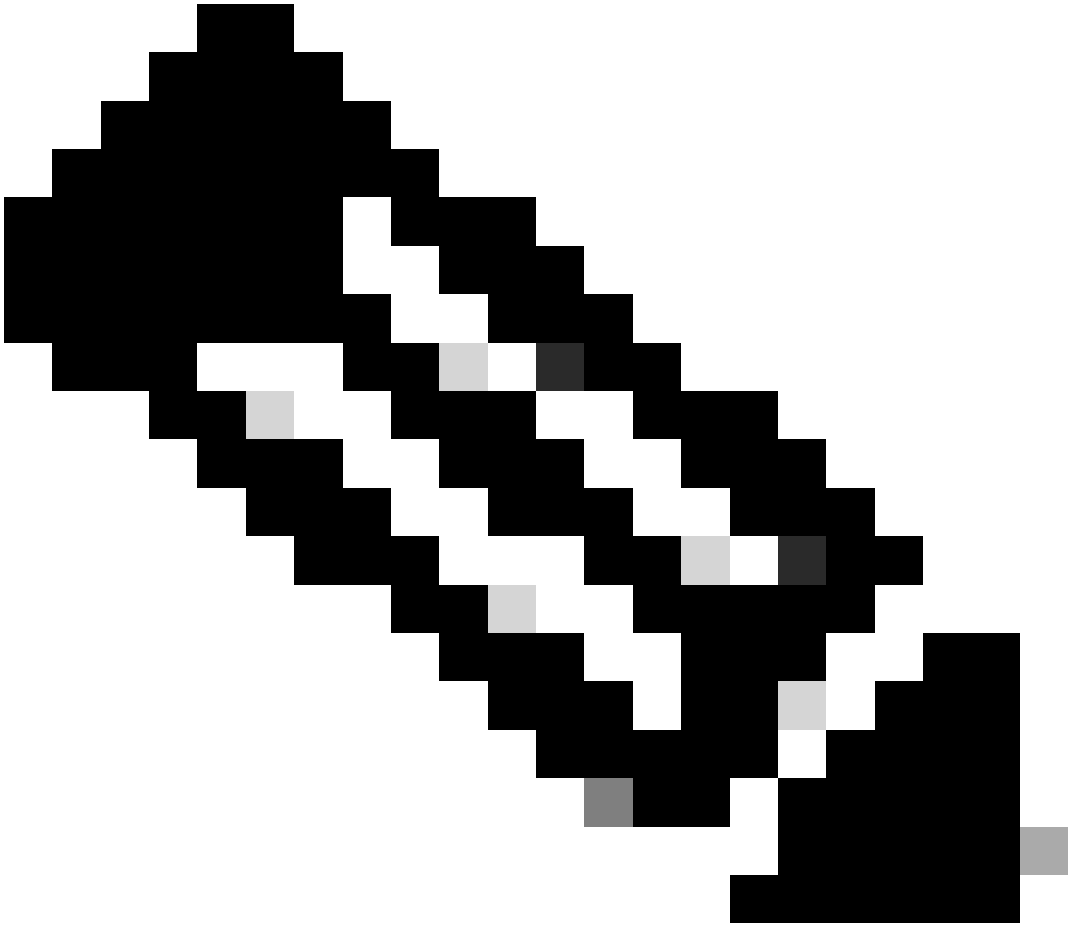
الخطوات:

- تكنت ال bash-shell سمة أو أدخلت أسلوب bash:

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

2. مراجعة المحتويات من dcos_sshd_config الملف:

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



ةظحالم: يمكنك إستخدام egrep للنظر في أسطر معينة: cat /isan/etc/dcos_sshd_config | grep MAC

الخيار 3. قم بالوصول إلى ملف "dcos_sshd_config" باستخدام **فلم DPLUG**

ينطبق هذا على:

- N3Ks يركض 6. X التي ليس لها وصول إلى القشرة القاعدية

- رومز All N5K و N6K

- N7Ks قيد التشغيل 6. X و 7. رومز X

الخطوات:

1. افتح حالة مركز المساعدة الفنية للحصول على ملف التوصيل الذي يطابق إصدار NXOS الذي يعمل على المحول.

2. قم بتحميل ملف التوصيل التوصيل إلى ذاكرة التمهيد المؤقتة (bootflash) وإنشاء نسخة منه.

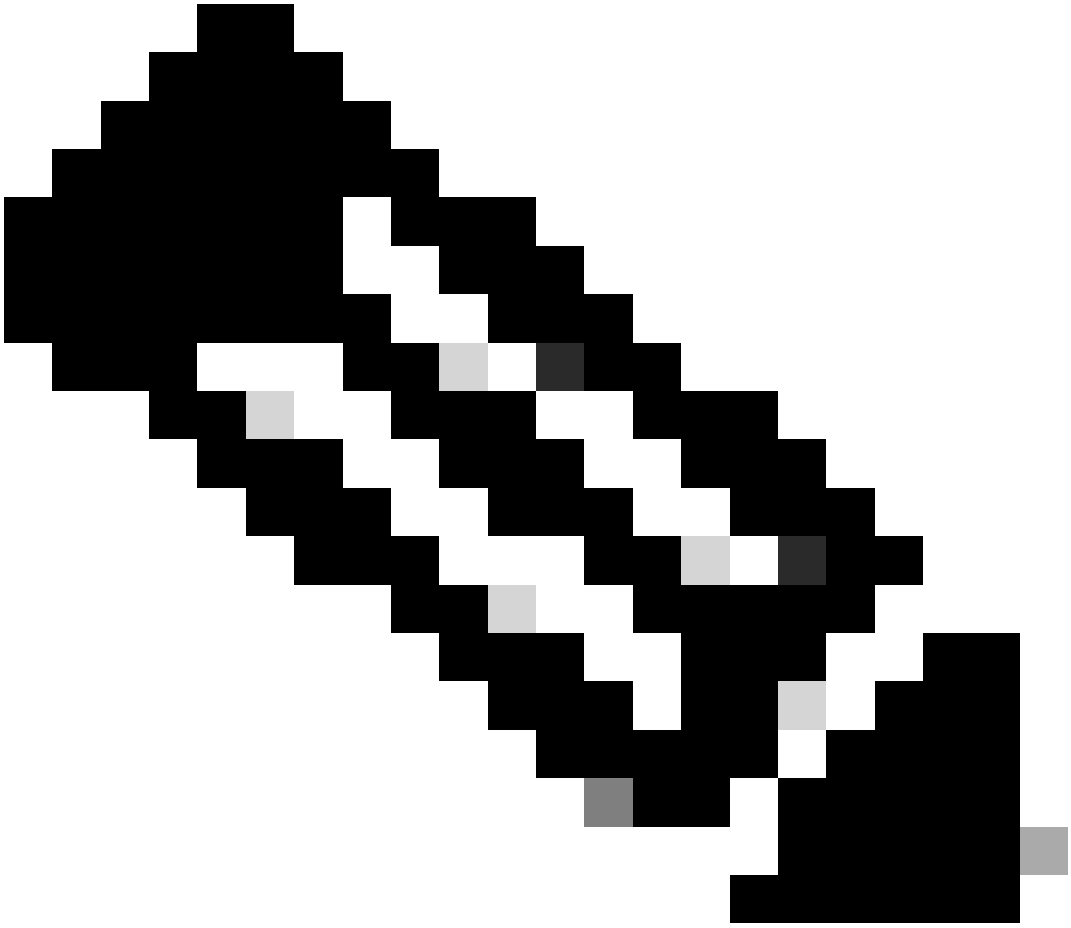
<#root>

switch# copy bootflash:

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

bootflash:

dp



ةظحلام: يتم إنشاء نسخة ("dp") من ملف DPLUG الأصلي في bootflash، بحيث تتم إزالة النسخة فقط بعد تحميل التوصيل ويبقى ملف dplug الأصلي في bootflash للتشغيل اللاحق.

3. قم بتحميل نسخة الأمر من خلال load الأمر.

<#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. مراجعة dcos_sshd_config الملف.

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

الحل

الخطوة 1. تصدير ملف "dcos_sshd_config"

1. إرسال نسخة من dcos_sshd_config الملف إلى bootflash:

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

2. تأكد من أن النسخة موجودة على bootflash:

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

3. التصدير إلى خادم:

```
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. قم بإجراء التغييرات اللازمة على الملف ثم قم باستيراده إلى bootflash.

الخطوة 2. إستيراد ملف "dcos_sshd_config"

1. قم بتحميل الملف المعدلdcos_sshd_config إلى ذاكرة Flash (الذاكرة المؤقتة) للتمهيد.

```
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#
```

الخطوة 3. استبدلت الأصل "dcos_sshd_config" مبرد مع النسخة

العملية اليدوية (غير المتواصلة عبر عمليات إعادة التمهيد) - جميع الأنظمة الأساسية

من خلال إستبدال الملف الموجودdcos_sshd_config ضمن /isan/etc/ ملفdcos_sshd_config معدل موجود في ذاكرة Bootflash (الذاكرة المؤقتة). هذه العملية غير مستمرة عبر عمليات إعادة التمهيد

- تحميل ملف معدلssh config إلى bootflash:

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

2. أثناء العمل في الوضع base أو linux(debug)#، قم باستبدال الملف الموجودdcos_sshd_config بالملف الموجود في bootflash:

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

3. تأكد من نجاح التغييرات:

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

عملية تلقائية - N7K

باستخدام برنامج IM النصي الذي يتم تشغيله عند ظهور السجل "VDC_MGR-2-VDC_ONLINE" بعد إعادة التحميل. في حالة تشغيل IM، يتم تشغيل برنامج نصي صالح ويستبدل الملف الموجود dcos_sshd_config أسفل /isan/etc/ بملفdcos_sshd_config معدل موجود في bootflash. الا يتطابق اذه إلا على إصدارات NX-OS التي تدعم "سمة bash-shell".

- تحميل ملف تكوين SSH معدل إلى bootflash:

<#root>

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

dcos_sshd_config_modified_7k

switch#

2. قم بإنشاء نص تنفيذي يطبق التغييرات على dcos_sshd_config الملف. تأكد من حفظ الملف بامتداد "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

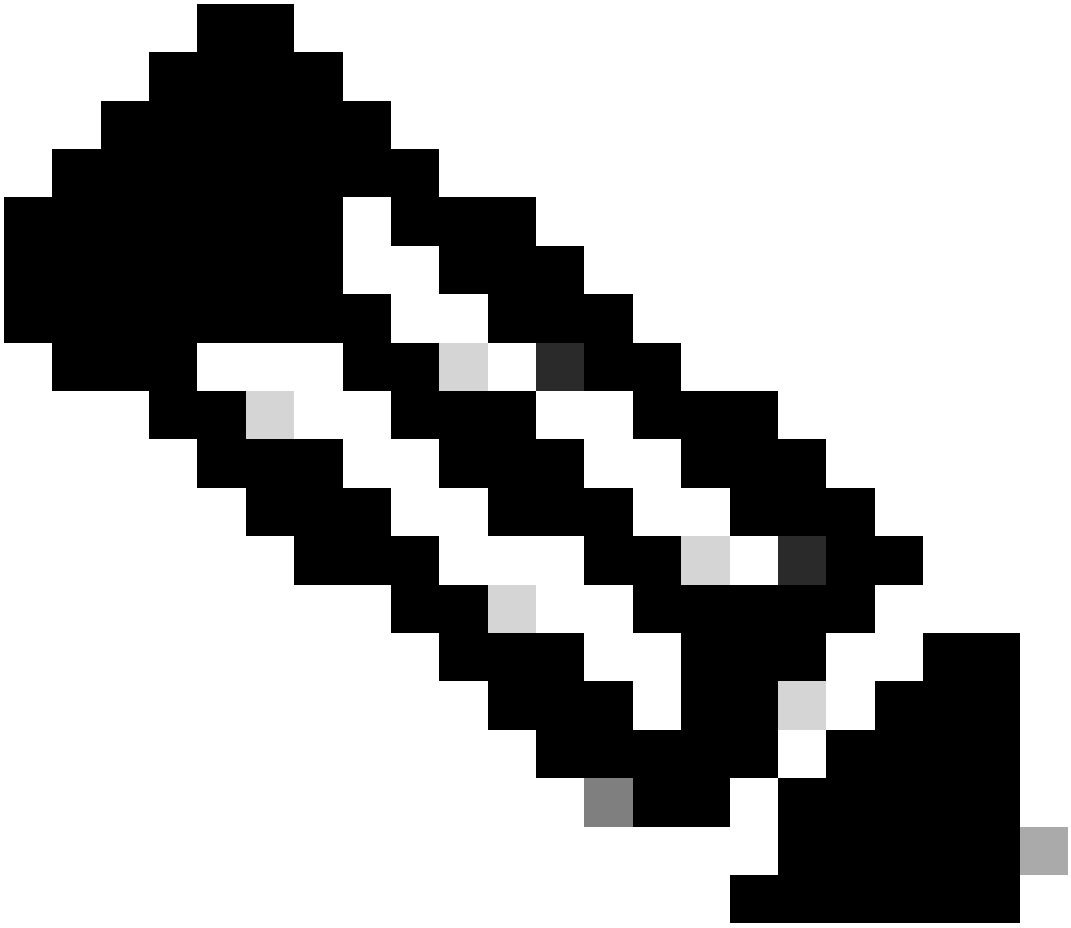
k /isan/etc/dcos_sshd_config\"")

3. تحميل البرنامج النصي Python إلى bootflash.

<#root>

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

ssh_workaround_7k.py



ملاحظة: تكون البرامج النصية ل Python متماثلة إلى حد كبير على جميع الأنظمة الأساسية، باستثناء N7K الذي يحتوي على بعض الخطوط الإضافية للتغلب على مشكلة معروفة تصحيح الأخطاء من Cisco CSCva14865.

4. تأكد من أن dcos_sshd_config اسم الملف من النص التنفيذي و bootflash (الخطوة 1.) هي نفسها:

<#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. قم بتشغيل البرنامج النصي مرة واحدة، بحيث dcos_sshd_config يتم تغيير الملف.

<#root>

switch#

source ssh_workaround_7k.py

```
switch#
```

5. قم بتكوين برنامج نصي IM، حتى يتم تشغيل البرنامج النصي PY في كل مرة يتم فيها إعادة تشغيل المحول ثم يعيد مرة أخرى.

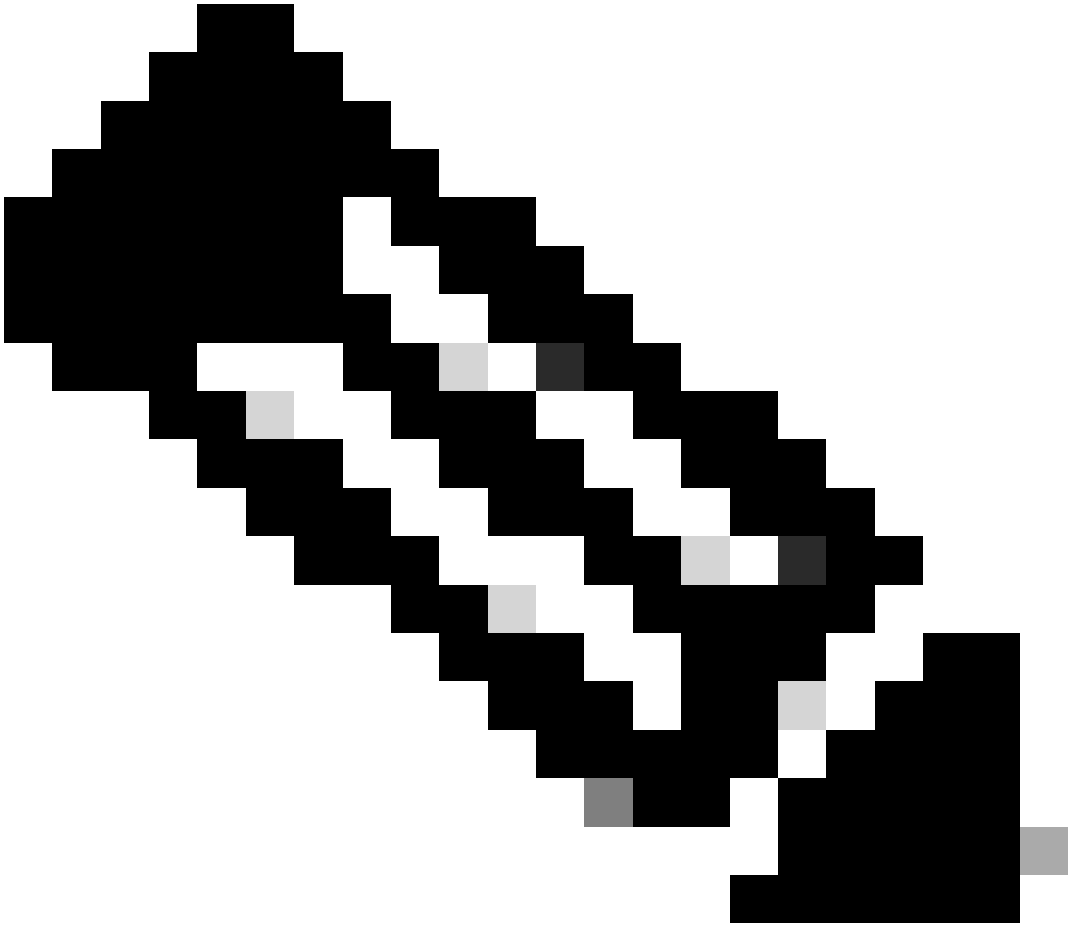
EEM N7K:

<#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"
```



ملاحظة: يمكن أن تختلف صياغة IM على إصدارات NXOS المختلفة (تتطلب بعض الإصدارات "action <id> cli" وغيرها من "action <id> cli command")، لذلك تأكد من أخذ رموز IM بشكل صحيح.

عملية تلقائية - N9K، N3K

- قم بتحميل ملف تكوين SSH معدل إلى 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. قم بإنشاء نص تنفيذي يطبق التغييرات على dcos_sshd_config الملف. تأكد من حفظ الملف باستخدام الملحق "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. تحميل البرنامج النصي python إلى bootflash.

<#root>

switch# dir | i i .py
127 Jun 18 17:21:39 2024

ssh_workaround_9k.py

switch#

4. تأكد من أن dcos_sshd_config اسم الملف من البرنامج النصي ومن bootflash (الخطوة 1.) هو نفسه:

<#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. قم بتشغيل البرنامج النصي مرة واحدة، بحيث dcos_sshd_config يتم تغيير الملف.

<#root>

switch#

python bootflash:ssh_workaround_9k.py

5. قم بتكوين برنامج نصي IM، حتى يتم تشغيل البرنامج النصي PY في كل مرة يتم فيها إعادة تشغيل المحول ثم دوعي مرة أخرى.

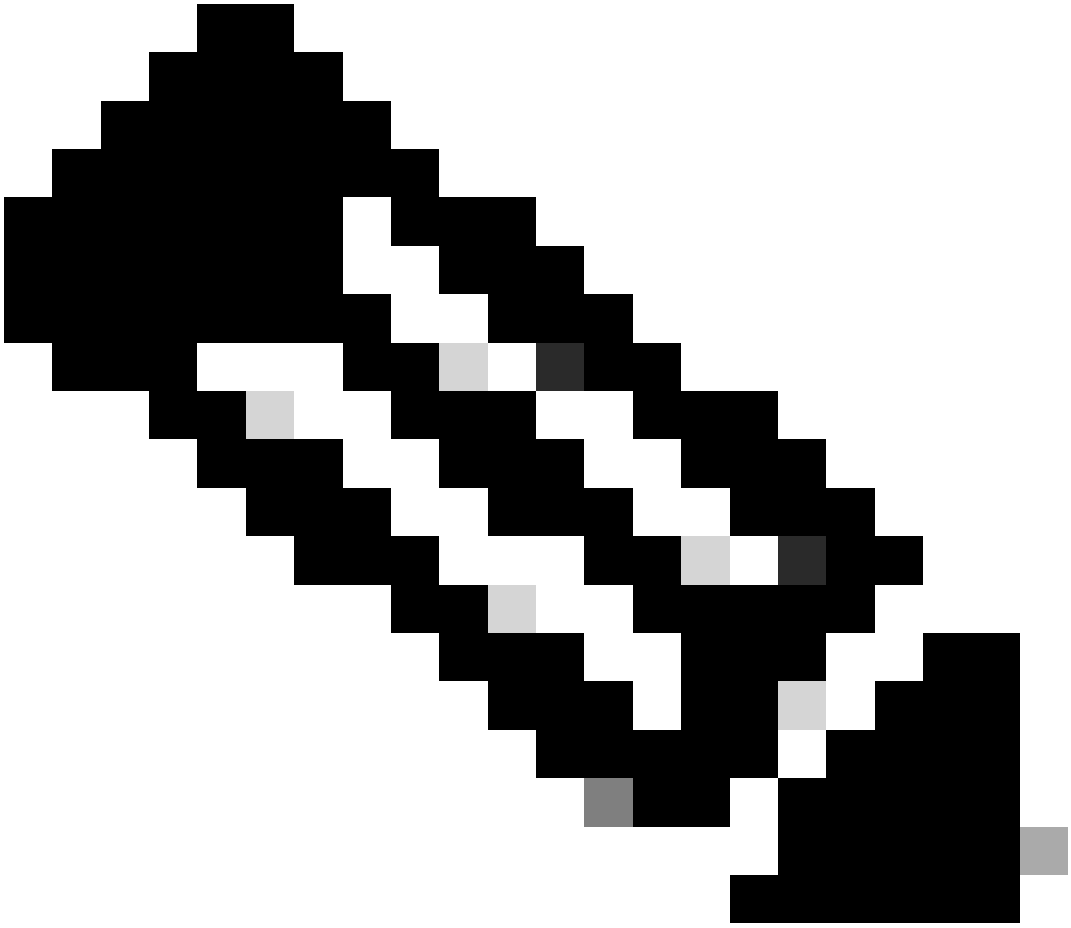
EEM N9K و N3K:

<#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
```



ملاحظة: يمكن أن تختلف صياغة IM على إصدارات NXOS المختلفة (تتطلب بعض الإصدارات "action <id> cli" وغيرها من "action <id> cli command")، لذلك تأكد من أخذ رموز IM بشكل صحيح.

عملية مؤتمتة - N5K و N6K

تم إنشاء ملف DPLUG معدل عبر معرف تصحيح الأخطاء من Cisco CSCvr23488 لإزالة خوارزميات KEX هذه:

- Diffie-hellman-group-exchange-sha256
- Diffie-hellman-group-exchange-sha1

- Diffie-hellman-group1-sha1

إن ملفات dpug المعروفة عبر cisco بـ id CSCvr23488 ليست نفسها التي تم إستخدامها للوصول إلى طبقة Linux. افتح حالة مركز المساعدة الفنية للحصول على المكون الإضافي المعدل من معرف تصحيح الأخطاء من Cisco CSCvr23488.

- دقق التقصير dcos_sshd_config عملية إعداد:

<#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

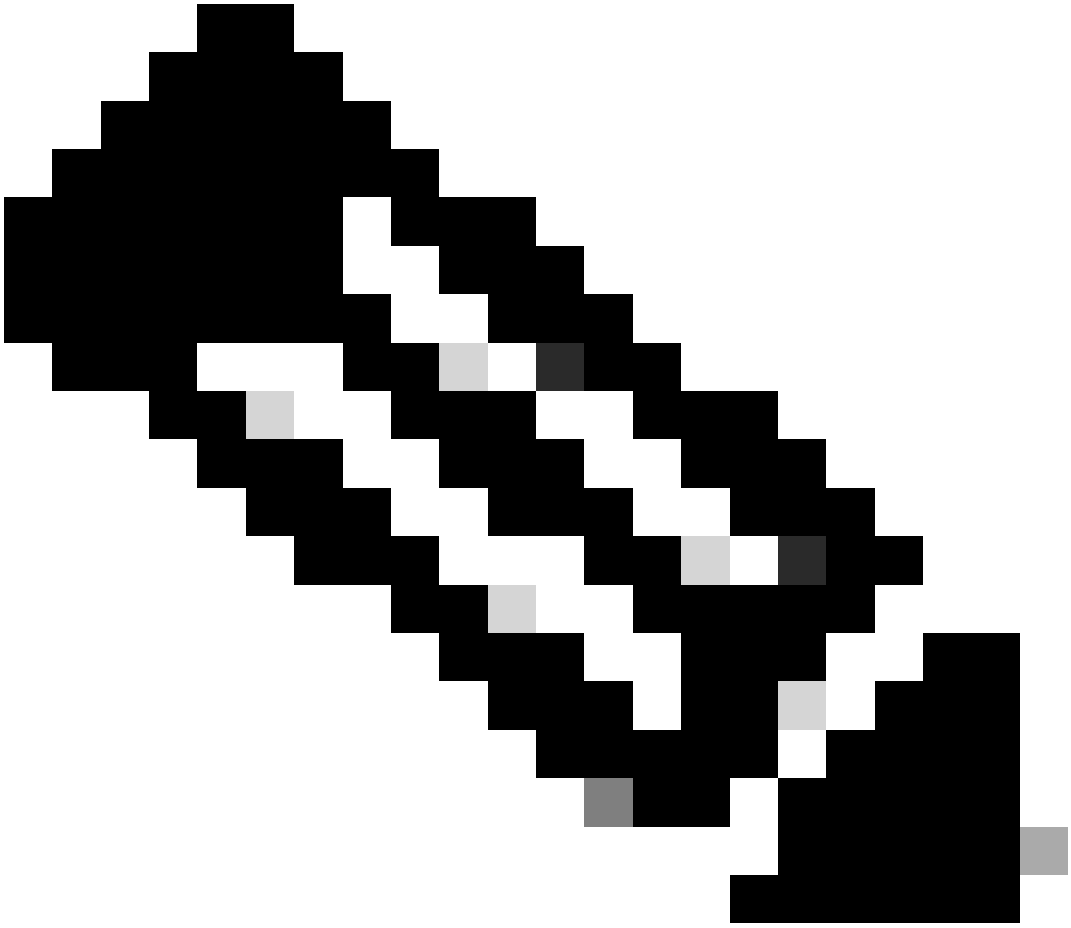
<--- mac algorithms
debug2: compression ctos: none,zlib@openssh.com
debug2:

compression stoc: none,zlib@openssh.com

<--- compression algorithms

2. قم بإنشاء نسخة من ملف DPLUG المعدل.

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



ملاحظة: يتم إنشاء نسخة ("dp") من ملف DPLUG الأصلي في bootflash بحيث تتم إزالة النسخة فقط بعد تحميل التوصيل ويبقى ملف dplug الأصلي في bootflash للتشغيل اللاحق.

---

3. تطبيق ملف التوصيل من معرف تصحيح الأخطاء من Cisco CSCvr23488 يدويا:

```
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. تحقق من الإعدادات الجديدةdcos_sshd_config:

<#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:

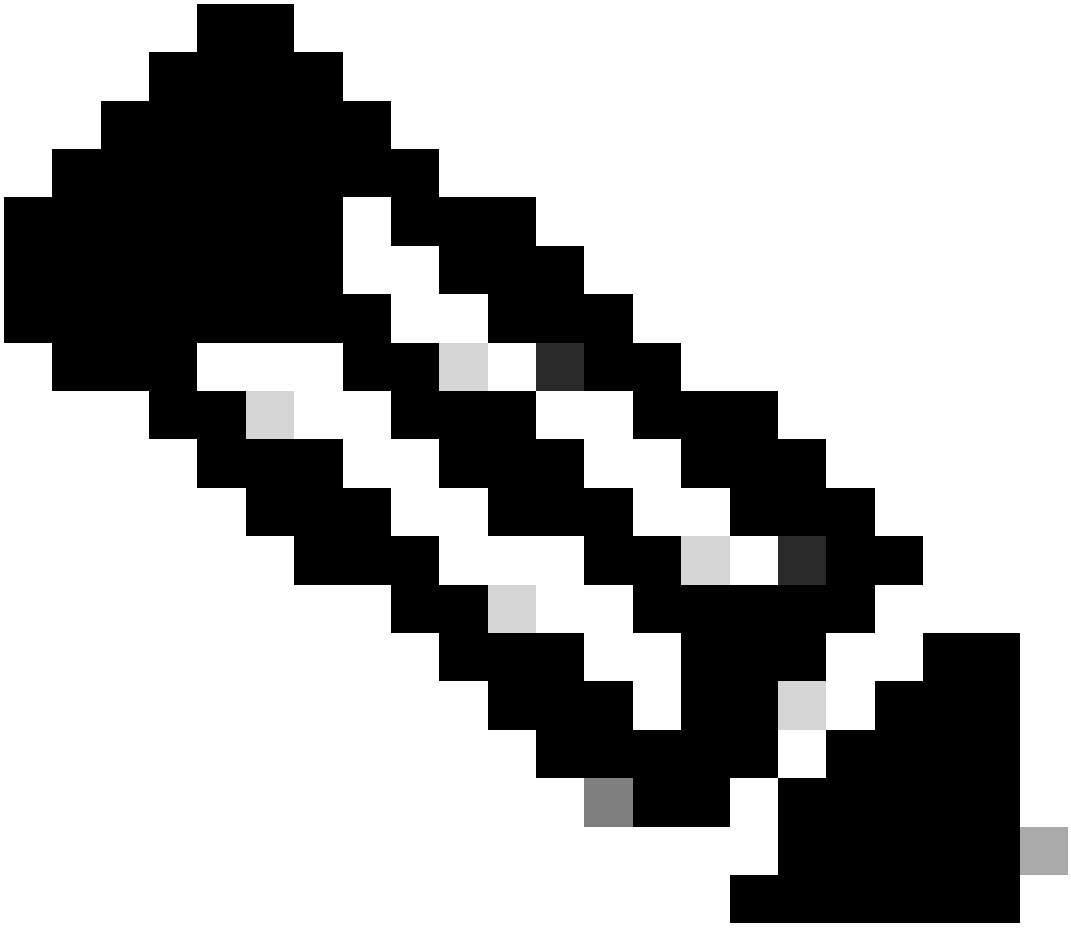
MACs stoc: hmac-sha1

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

compression stoc: none,zlib@openssh.com

5. أجعل هذا التغيير مستمر عبر عمليات إعادة التشغيل باستخدام برنامج IM:

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"



ملاحظة:

- بعد تطبيق المكون الإضافي المعدل، يجب إعادة تعيين ميزة SSH على هذا النظام الأساسي.
- تأكد من أن ملف التوصيل موجود في bootflash، وتم تكوين IM باستخدام اسم الملف المناسب. يمكن أن يختلف اسم ملف التوصيل بناء على إصدار المحول، فتأكد من تعديل النص التنفيذي حسب الحاجة.
- ينشئ الإجراء 1 نسخة من ملف DPLUG الأصلي في Bootflash إلى آخر يسمى "dp"، بحيث لا يتم حذف ملف DPLUG الأصلي بعد تحميله.

اعتبارات المنبر

N5K/N6K

- ال يمكن تغيير MAC (رمز مصادقة الرسالة) على هذه الأنظمة الأساسية بتعديل ملف dco_sshd_config. MAC الوحيد المدعوم هو HMAC-SHA1.

N7K

- لكي يتم تغيير عناوين MAC، يلزم وجود رمز 8.4. راجع معرف تصحيح الأخطاء من Cisco CSCwc26065للحصول على تفاصيل.

- "Sudo su" غير متوفرة بشكل افتراضي في 8.x. مرجع cisco بق id: CSCva14865. في حالة تنفيذه، يتم ملاحظة هذه الخطأ:

<#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$

للتغلب على هذا، اكتب ما يلي:

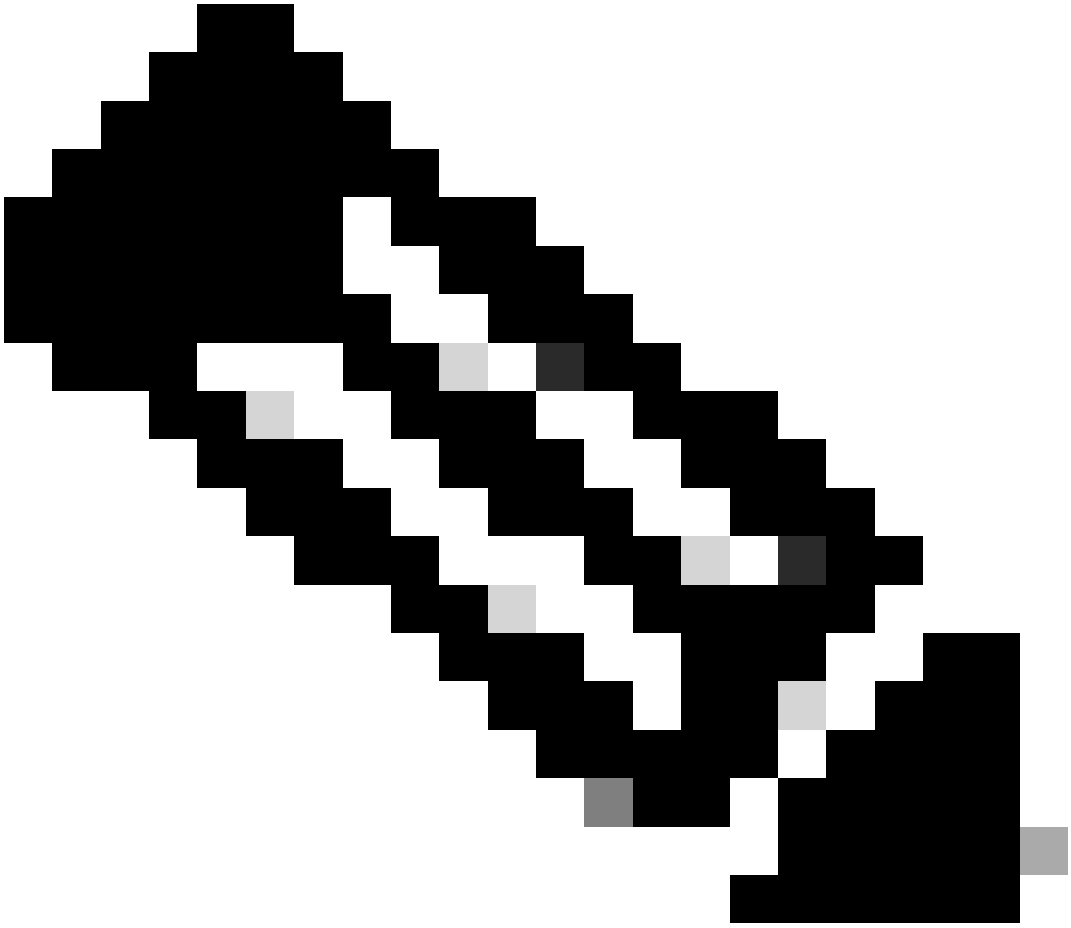
<#root>

bash-4.3$

sudo usermod -s /bin/bash root

بعد هذه الـ"سودو سو" تعمل:

bash-4.3$ sudo su
bash-4.3#



ةظحلام: ال يزجو هذا التغيير من إعادة تحميل.

- هناك ملف منفصلdcos_sshd_config لكل VDC، في حالة الحاجة إلى تعديل معلمات SSH على VDC مختلف، تأكد من تعديل الملفdcos_sshd_config المطابق.

<#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

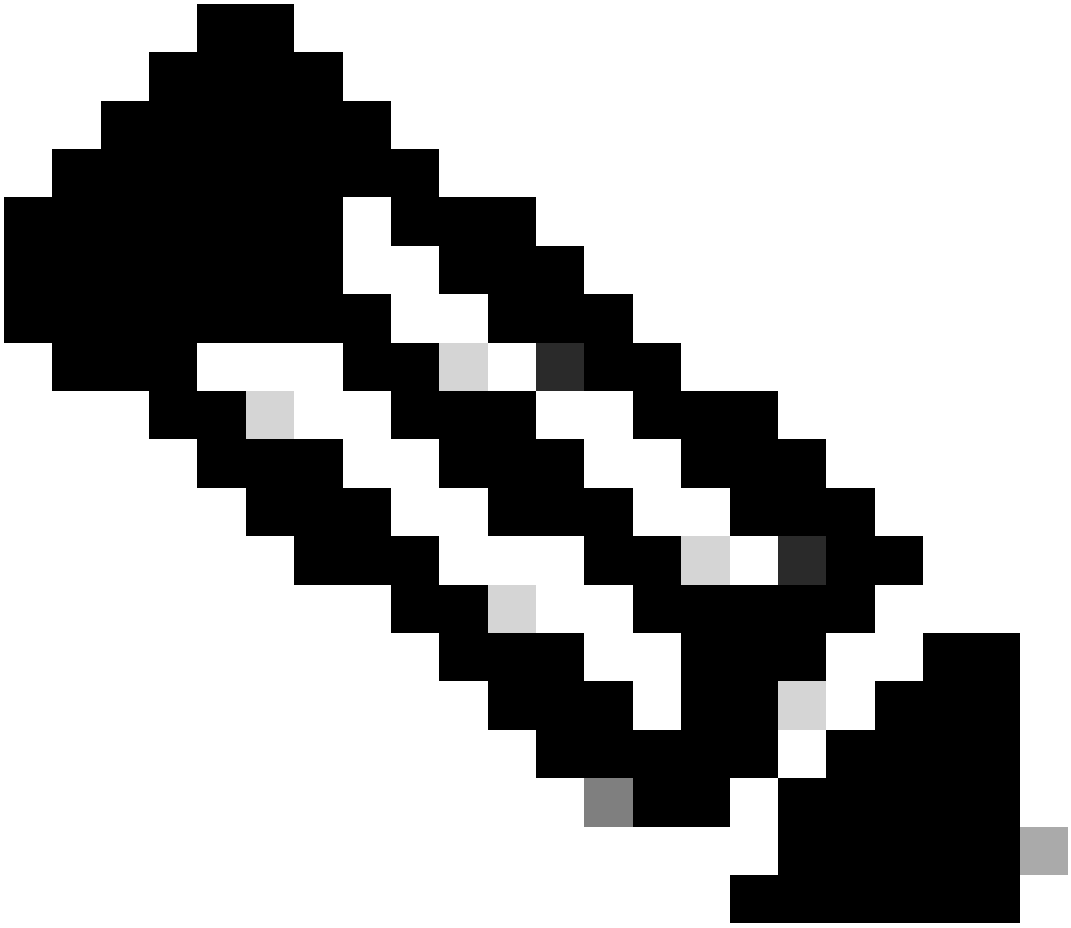
- ال يتم إجراء التغييرات علىdcos_sshd_config الملف بشكل دائم عبر عمليات إعادة التمهيد على أي نظام Nexus أساسي. إذا كانت التغييرات بحاجة إلى أن تكون مستمرة، فيمكن إستخدام IM لتعديل الملف في كل مرة يتم فيها تمهيد المحول. تحسين N9K يغير هذا بداية من 10.4. راجع معرف تصحيح الأخطاء من Cisco CSCwd82985 للحصول على تفاصيل.

N7K و N9K و N3K

هناك شفرة إضافية، MAC، وخوارزميات KexAlgorithms التي يمكن إضافتها إذا تطلب الأمر:

<#root>

switch(config)# ssh kexalgos [all | key-exchangealgorithm-name]
switch(config)# ssh macs [all | mac-name]
switch(config)# ssh ciphers [all | cipher-name]



ملاحظة: تتوفر هذه الأوامر على Nexus 7000 مع الإصدارات 8.3(1) والإصدارات الأحدث. بالنسبة للنظام الأساسي Nexus 3000/9000، يصبح الأمر متوفرا مع الإصدار 7.0(3)I7(8) والإصدارات الأحدث. (تتضمن جميع إصدارات 9.3(x) هذا الأمر أيضا. راجع دليل تكوين أمان Cisco Nexus 9000 Series NX-OS، الإصدار 9.3(x))

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).