CiPhers, MACs, Kex-algoritmen configureren in Nexus-platforms

Inhoud

Inleiding

In dit document worden de stappen beschreven voor het toevoegen (of verwijderen) van algoritmes, MACs en Kex-algoritmen op Nexus-platforms.

Voorwaarden

Vereisten

Cisco raadt u aan de basis van Linux en Bash te begrijpen.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende hardware- en softwareversies:

- Nexus 3000 en 9000 NX-OS 7.0(3)I7(10)
- Nexus 3000 en 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)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Soms kunnen beveiligingsscans zwakke coderingsmethoden vinden die door Nexus-apparaten worden gebruikt. Als dit gebeurt, moeten wijzigingen in hetdcos_sshd_config bestand op de switches deze onveilige algoritmen verwijderen.

Beoordeel Beschikbare algoritmen, MAC's en Kex-algoritmen

Om te bevestigen welke algoritmes, MACs, en Kex Algoritmen een platform gebruikt en dit van een extern apparaat controleren kunt u deze opties gebruiken:

Optie 1. CMD-lijn vanaf PC gebruiken

Open een CMD-lijn op een pc die het Nexus-apparaat kan bereiken en gebruik de opdracht 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

Optie 2. Toegang tot het "dcos_sshd_config" bestand met **Functie Bash-Shell**

Dit geldt voor:

- N3K hardlopen 7. X, 9. X, 10. X
- Alle N9K-codes
- N7K met 8.2 en hoger

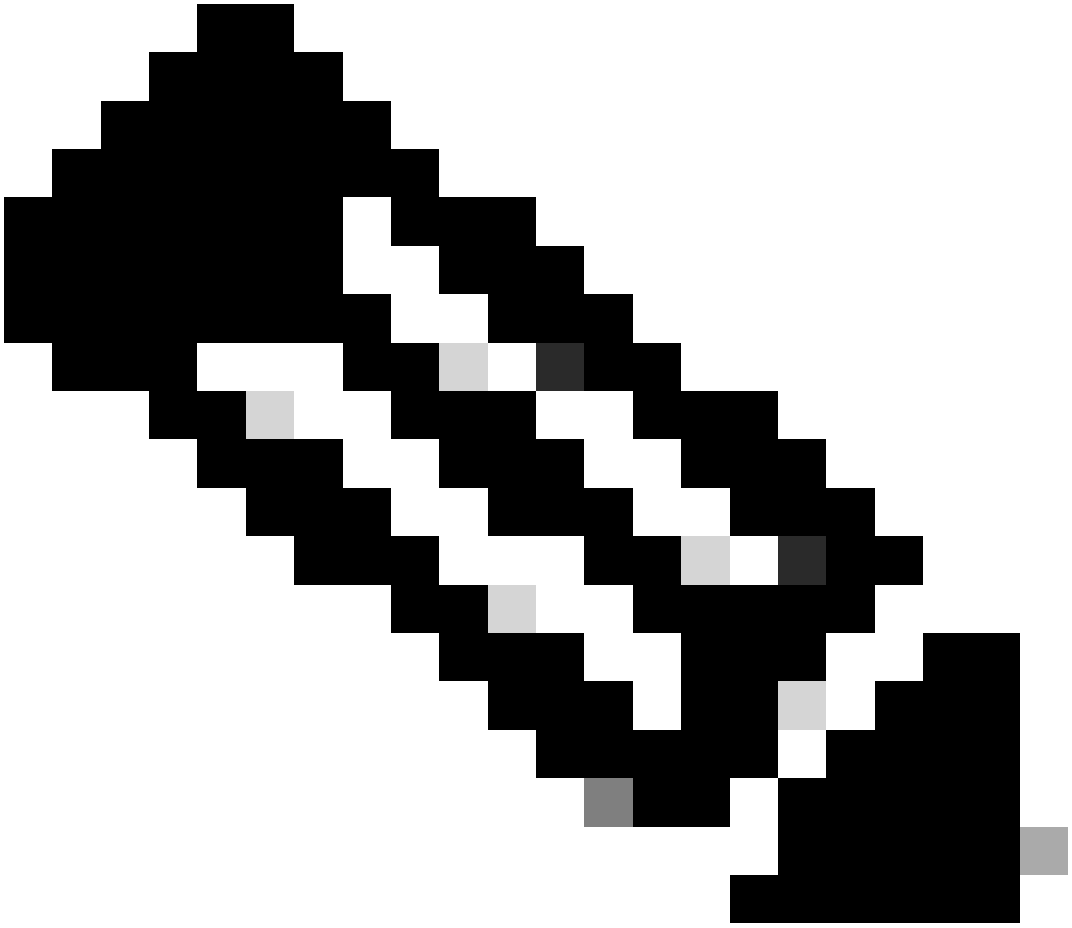
Stappen:

- Schakel de bash-shell functie in en kom in de bash modus:

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

2. Bekijk de inhoud van het dcos_sshd_config bestand:

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



Opmerking: u kunt egrep gebruiken om specifieke regels te bekijken: cat /isan/etc/dcos_sshd_config | grep MAC

Optie 3. Toegang tot het "dcos_sshd_config" bestand met behulp van een **Dplug File**

Dit geldt voor:

- N3Ks 6. X dat geen toegang heeft tot de bash-shell

    - Alle N5K- en N6K-codes
- N7Ks rijdt 6. X en 7. X-codes

Stappen:

1. Open een TAC-case om het plug-bestand te verkrijgen dat overeenkomt met de NXOS-versie die op de switch wordt uitgevoerd.

2. Upload het plug bestand naar bootflash en maak er een kopie van.

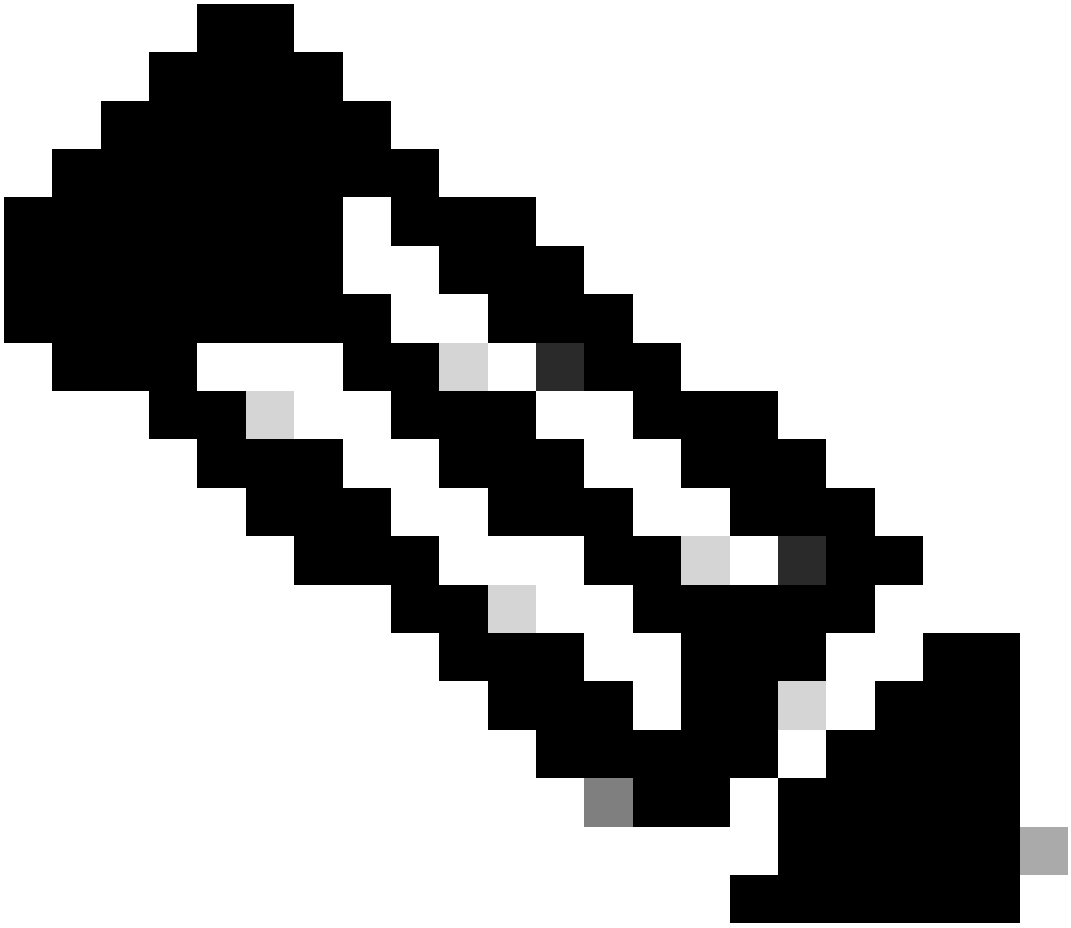
<#root>

switch# copy bootflash:

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

bootflash:

dp



Opmerking: een kopie ("dp") van het oorspronkelijke plug bestand wordt gemaakt in bootflash, zodat alleen de kopie wordt verwijderd nadat de dplug is geladen en het oorspronkelijke dplug bestand blijft in bootflash voor volgende opstellingen.

3. Laad het exemplaar van de stekker via de load opdracht.

<#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. Bestand bekijkendcos_sshd_config.

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

Oplossing

Stap 1. Exporteren van het "dcos_sshd_config" bestand

1. Verzend een kopie van het dcos_sshd_config bestand naar bootflash:

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

2. Bevestig dat het exemplaar op bootflash is:

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

3. Exporteren naar een server

```
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. Breng de gewenste wijzigingen aan in het bestand en importeer het opnieuw naar bootflash.

Stap 2. Importeer het "dcos_sshd_config" bestand

1. Upload het aangepaste dcos_sshd_config bestand om de flitser op te starten.

```
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#
```

Stap 3. Vervang het originele "dcos_sshd_config" bestand door het kopieerapparaat

Handmatig proces (niet blijvend bij opstarten) - Alle platforms

Door het bestaande dcos_sshd_config bestand onder te vervangen /isan/etc/ door een aangepast dcos_sshd_config bestand in bootflash. Dit proces is niet blijvend bij alle herstart

- Upload een aangepast ssh config bestand naar bootflash:

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

2. Terwijl in bash of Linux (debug)# modus, overschrijf het bestaande dcos_sshd_config bestand met het bestand in bootflash:

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

3. Bevestig dat de wijzigingen succesvol waren:

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

Geautomatiseerd proces - N7K

Door een EEM script te gebruiken dat wordt geactiveerd wanneer het log "VDC_MGR-2-VDC_ONLINE" na een herladen verschijnt. Als de EEM wordt geactiveerd, wordt er een ponsscript uitgevoerd en vervangt het bestaande dcos_sshd_config bestand onder /isan/etc/ door een aangepast dcos_sshd_config bestand in bootflash. Dit is alleen van toepassing op NX-OS-versies die "feature bash-shell" ondersteunen.

- Upload een aangepast ssh-configuratiebestand naar bootflash:

<#root>

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

dcos_sshd_config_modified_7k

switch#

2. Maak een script dat de wijzigingen in het dcos_sshd_config bestand toepast. Verzeker u ervan dat u het bestand met de extensie "py" opslaat.

<#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

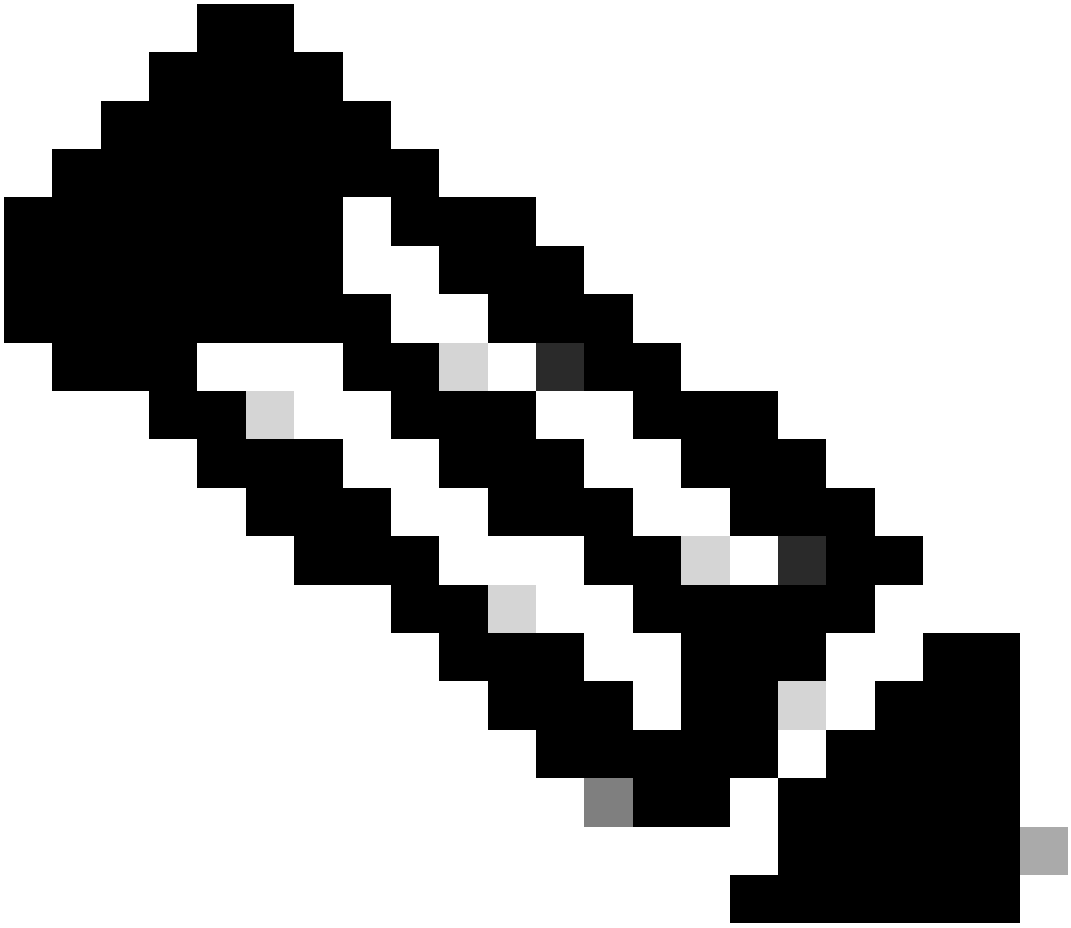
k /isan/etc/dcos_sshd_config\"")

3. Upload het Python script naar bootflash.

<#root>

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

ssh_workaround_7k.py



Opmerking: Python-scripts zijn vrijwel hetzelfde op alle platforms, behalve voor N7K, die enkele extra regels bevat om Cisco bug-id CSCva14865 te overwinnen.

4. Verzeker dat de bestandsnaam van hetdcos_sshd_config script en bootflash (Stap 1.) hetzelfde is:

```
<#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. Start het script eenmaal, zodat het dcos_sshd_config bestand wordt gewijzigd.

<#root>

switch#

source ssh_workaround_7k.py

```
switch#
```

5. Configureer een EEM-script zodat het script wordt uitgevoerd telkens wanneer de switch wordt opgestart en weer wordt opgestart.

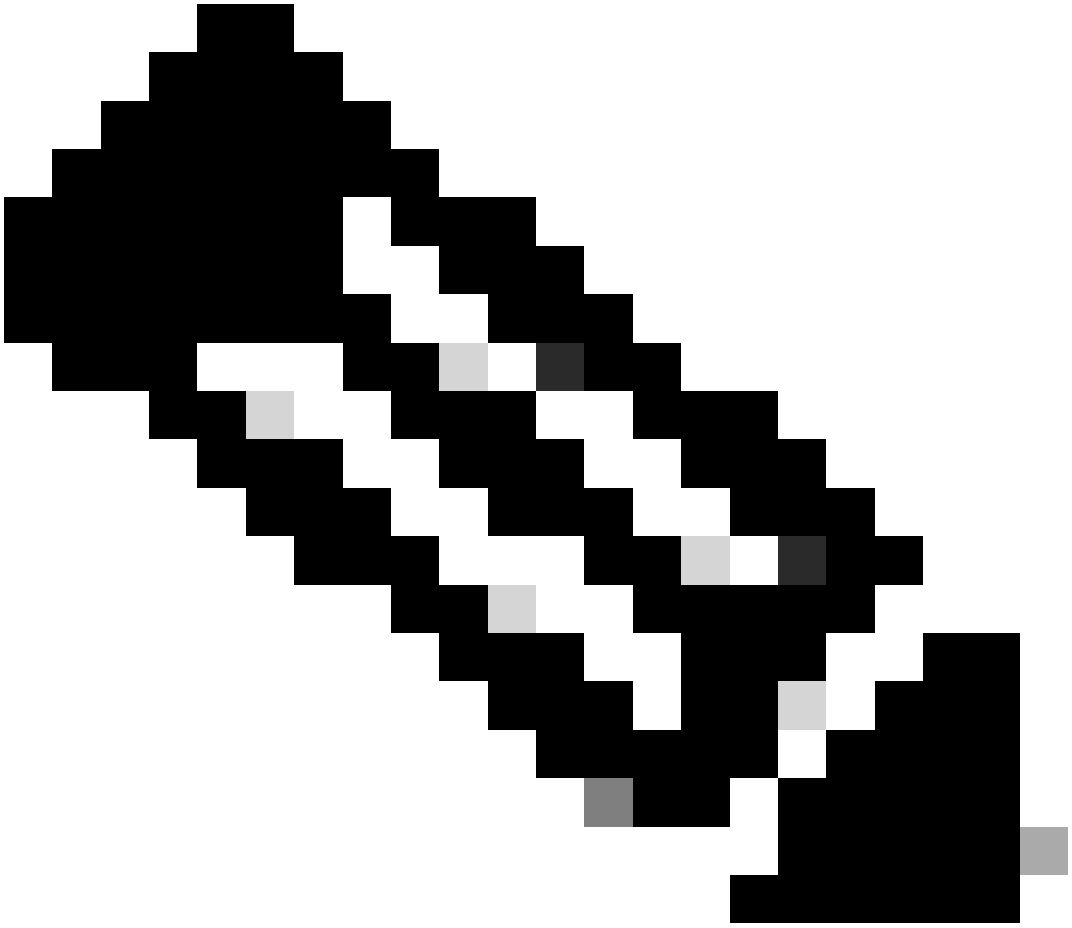
EEM N7K:

<#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"
```



Opmerking: EEM syntax kan variëren op verschillende NXOS releases (sommige versies vereisen "CLI" en anderen "CLI commando"), dus zorg ervoor dat de EEM commando's goed worden genomen.

Geautomatiseerd proces - N9K, N3K

- Upload een aangepast SSH-configuratiebestand naar 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. Maak een script dat de wijzigingen in het dcos_sshd_config bestand toepast. Verzeker u ervan dat u het bestand met de extensie "py" opslaat.

<#root>

#!/usr/bin/env python
import os
os.system("sudo su -c \"cp

/bootflash/dcos_sshd_config_modified

/isan/etc/dcos_sshd_config\"")

3. Upload het python script naar bootflash.

<#root>

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

ssh_workaround_9k.py

switch#

4. Controleer of de bestandsnaam van hetdcos_sshd_config script en van bootflash (Stap 1) hetzelfde is:

<#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. Start het script eenmaal, zodat het dcos_sshd_config bestand wordt gewijzigd.

<#root>

switch#

python bootflash:ssh_workaround_9k.py

5. Configureer een EEM script, zodat het script wordt uitgevoerd elke keer dat de switch opnieuw opgestart wordt en weer terugkomt.

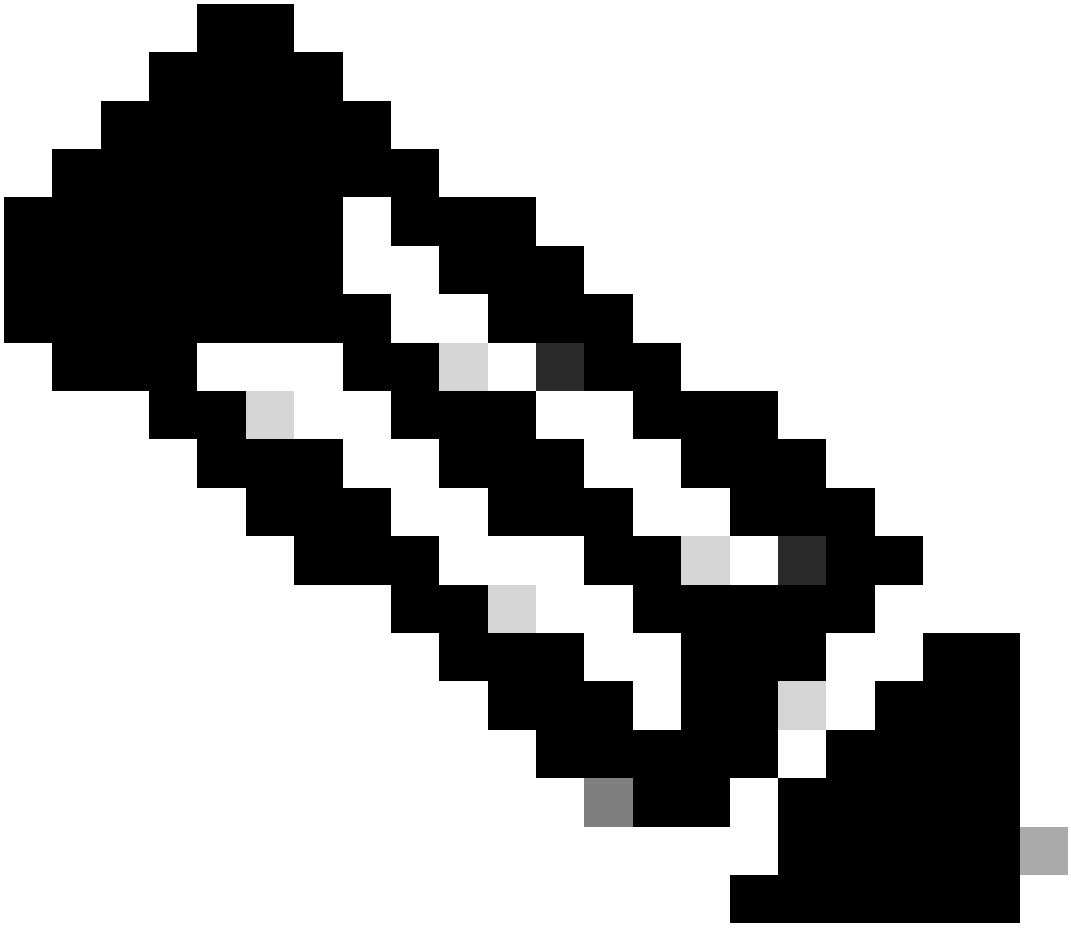
EEM N9K en N3K:

<#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



Opmerking: EEM syntax kan variëren op verschillende NXOS releases (sommige versies vereisen "CLI" en anderen "CLI commando"), dus zorg ervoor dat de EEM commando's goed worden genomen.

Geautomatiseerd proces - N5K, N6K

Er is een aangepast plug-bestand gemaakt via Cisco bug ID CSCvr23488 om deze Kex-algoritmen te verwijderen:

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

- diffie-hellman-groep1-sha1

De dpug-bestanden die via Cisco bug-id CSCvr23488 worden geleverd, zijn niet hetzelfde als de bestanden die worden gebruikt voor toegang tot de Linux Shell. Open een TAC-case om de aangepaste stekker te verkrijgen uit Cisco bug-id CSCvr23488.

- Controleer de standaardinstellingen dcos_sshd_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

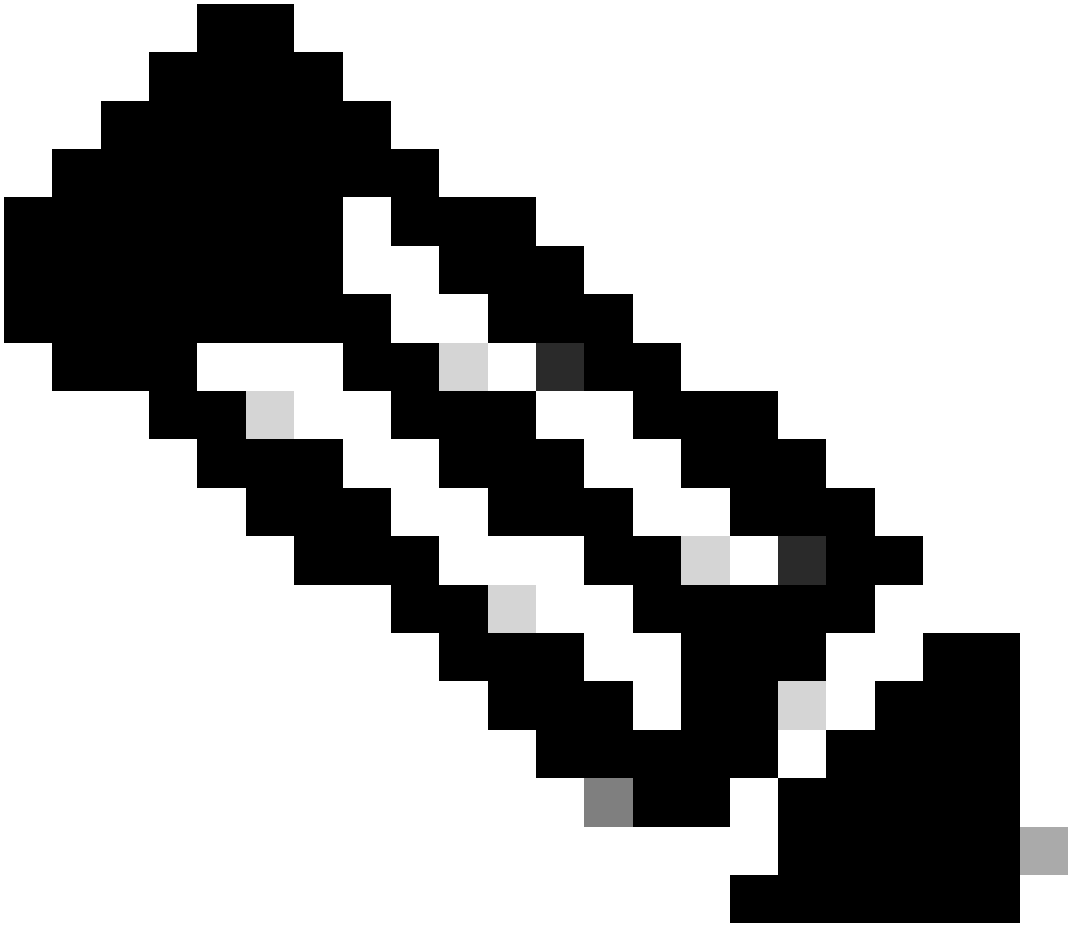
<--- mac algorithms
debug2: compression ctos: none,zlib@openssh.com
debug2:

compression stoc: none,zlib@openssh.com

<--- compression algorithms

2. Maak een kopie van het aangepaste plug-bestand.

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



Opmerking: Een kopie ("dp") van het oorspronkelijke plug bestand wordt in bootflash gemaakt, zodat alleen de kopie wordt verwijderd nadat de dplug is geladen en het oorspronkelijke dplug bestand in bootflash blijft voor volgende opstellingen.

---

3. Pas het plug-bestand van Cisco bug-id CSCvr23488 handmatig toe:

```
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. Controleer de nieuwe dcos_sshd_config instellingen:

<#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:

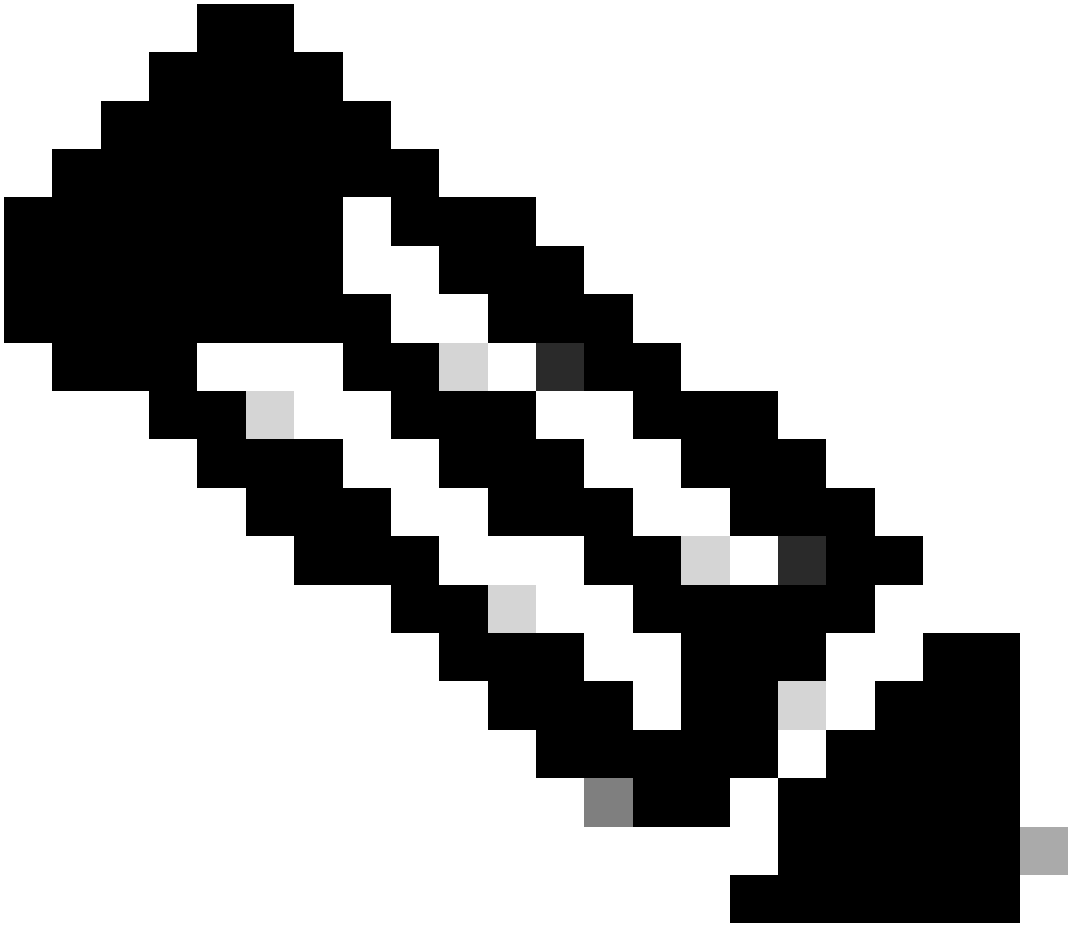
MACs stoc: hmac-sha1

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

compression stoc: none,zlib@openssh.com

5. Maak deze verandering blijvend over reboots met een EEM-script:

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"



Opmerking:

- Nadat de aangepaste stekker is toegepast, moet de SSH-functie op dit platform worden gereset.
- Zorg ervoor dat het plugbestand aanwezig is in bootflash, en het EEM is geconfigureerd met de juiste pluggable bestandsnaam. De bestandsnaam van de plug kan variëren afhankelijk van de versie van de switch, dus zorg ervoor dat u het script naar wens aanpast.
- Actie 1 maakt een kopie van het oorspronkelijke dplug-bestand in bootflash naar een andere genaamd "dp", zodat het oorspronkelijke dplug-bestand niet wordt verwijderd na te zijn geladen.

Platformoverwegingen

N5K/N6K

- MAC (Message Verification Code) kan op deze platforms niet worden gewijzigd door het dcos_sshd_config-bestand te wijzigen. De enige ondersteunde MAC is hmac-sha1.

N7K

- Voor een wijziging van de MAC is een 8.4-code vereist. Zie Cisco bug-id CSCwc26065 voor meer informatie.
- "Sudo su" is standaard niet beschikbaar op 8.X. Referentie Cisco bug-id: CSCva14865. Indien uitgevoerd, wordt deze fout opgemerkt:

```
<#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$
```

Typ om dit te overwinnen het volgende:

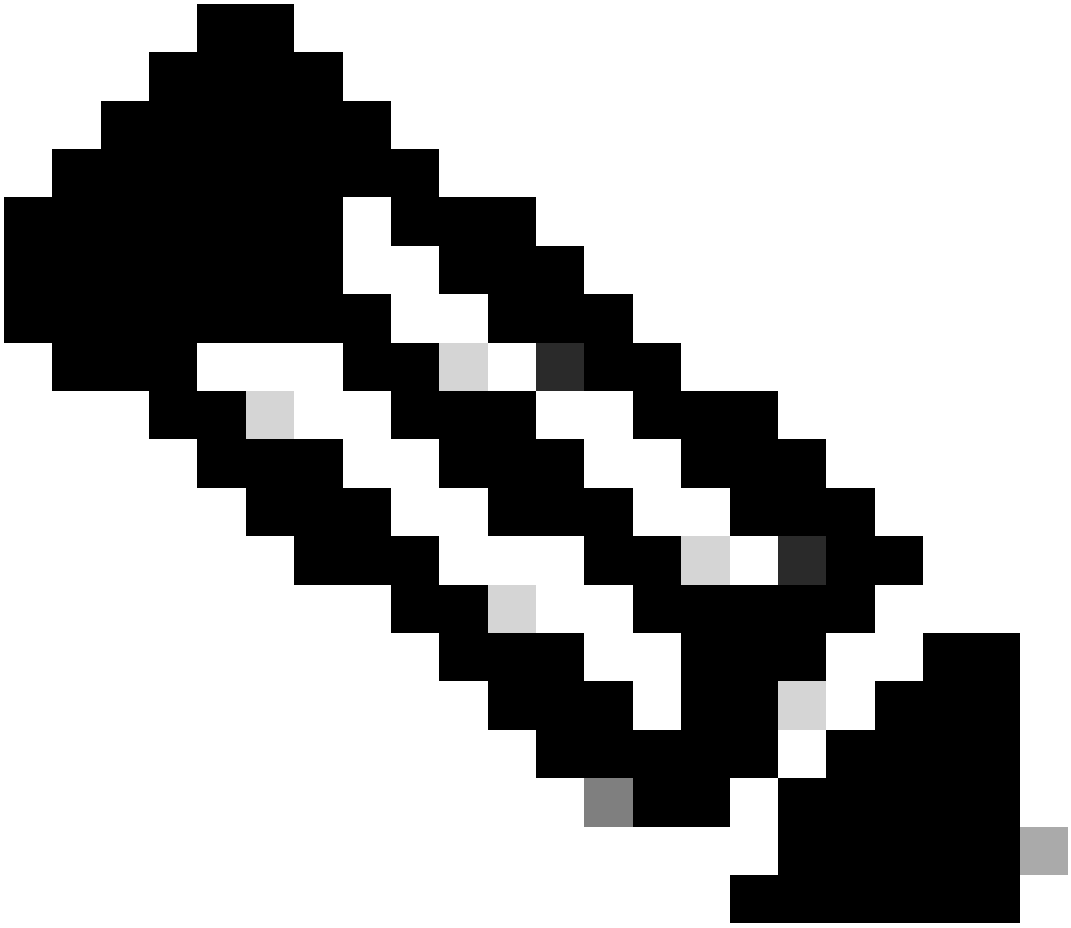
```
<#root>

bash-4.3$

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

Na dit "sudo su" werkt:

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



Opmerking: deze wijziging overleeft een herlading niet.

- Er is een afzonderlijk dcos_sshd_config bestand voor elke VDC, voor het geval dat SSH-parameters moeten worden gewijzigd op een andere VDC, zorg ervoor dat het corresponderende dcos_sshd_config bestand wordt gewijzigd.

<#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

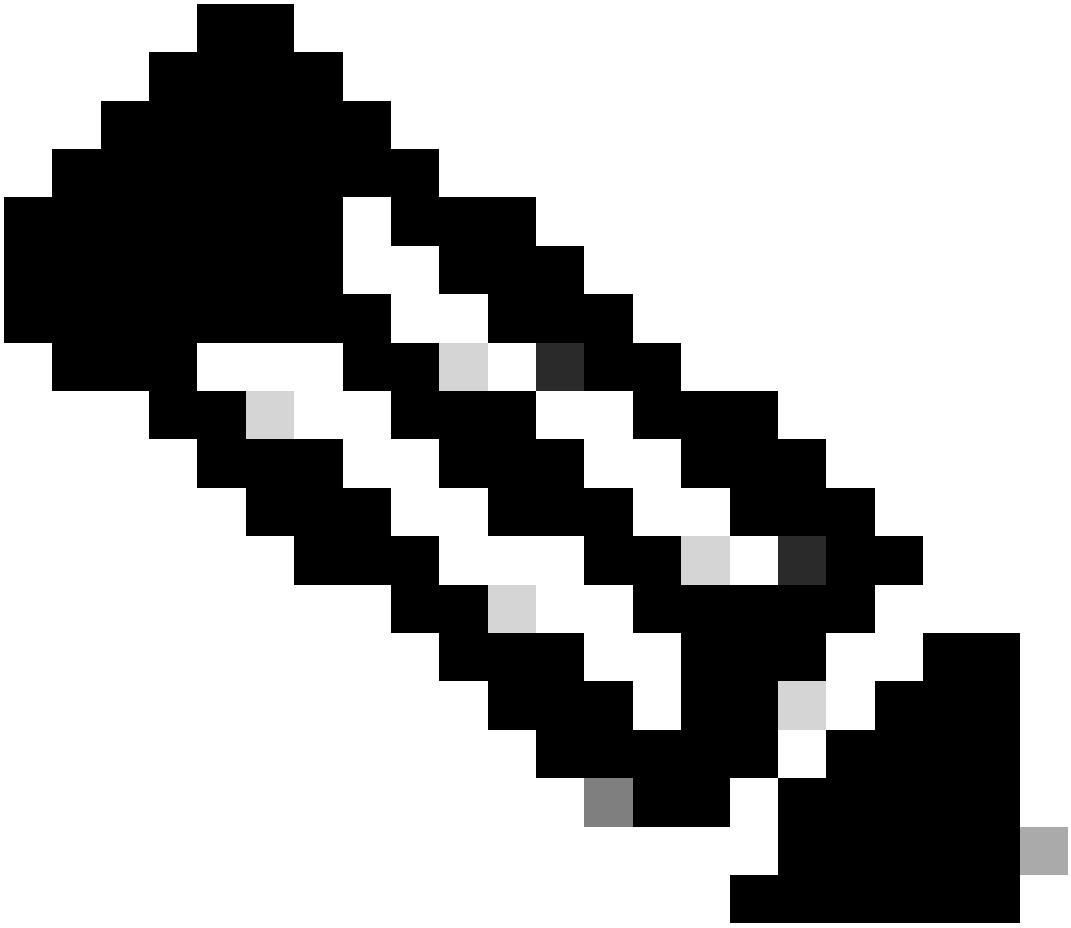
- De veranderingen in het dcos_sshd_config bestand blijven niet hardnekkig over alle reboots op elk Nexus platform. Als de veranderingen persistent moeten zijn, kan een EEM worden gebruikt om het bestand aan te passen telkens als de switch opstart. Verbetering op N9K verandert dit beginpunt 10.4. Zie Cisco bug-id CSCwd82985 voor meer informatie.

N7K, N9K, N3K

Er zijn extra algoritmen, MAC's en KexAlgorithms die indien nodig kunnen worden toegevoegd:

<#root>

switch(config)# ssh kexalgos all
switch(config)# ssh macs all
switch(config)# ssh ciphers all



Opmerking: deze opdrachten zijn beschikbaar op de Nexus 7000 met release 8.3(1) en hoger. Voor het Nexus 3000/9000-platform wordt de opdracht beschikbaar met release 7.0(3)I7(8) en hoger. (Alle 9.3(x) releases hebben ook deze opdracht. Zie Cisco Nexus 9000 Series NX-OS security configuratiegids, release 9.3(x))

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.