Configurazione di cifrari, MAC, algoritmi Kex nelle piattaforme Nexus

Sommario

Introduzione

Questo documento descrive la procedura per aggiungere (o rimuovere) Cifre, MAC e Algoritmi Kex nelle piattaforme Nexus.

Prerequisiti

Requisiti

Cisco consiglia di comprendere le nozioni di base di Linux e Bash.

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni hardware e software:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

A volte, le scansioni di sicurezza possono trovare metodi di crittografia deboli utilizzati dai dispositivi Nexus. In questo caso, per rimuovere gli algoritmi non sicuri, è necessario modificare dcos_sshd_config il file sugli switch.

Esame di cifrari, MAC e algoritmi Kex disponibili

Per verificare quali cifrari, MAC e algoritmi Kex vengono utilizzati da una piattaforma e controllare da un dispositivo esterno, è possibile utilizzare le seguenti opzioni:

Opzione 1. Utilizzo della linea CMD del PC

Aprire una riga CMD su un PC in grado di raggiungere il dispositivo Nexus e utilizzare il 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-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

Opzione 2. Accedete al file "dcos_sshd_config" utilizzando la **feature Bash-Shell**

Ciò si applica a:

- N3K in esecuzione 7. X, 9. X, 10. X
- Tutti i codici N9K
- N7K con versione 8.2 e successive

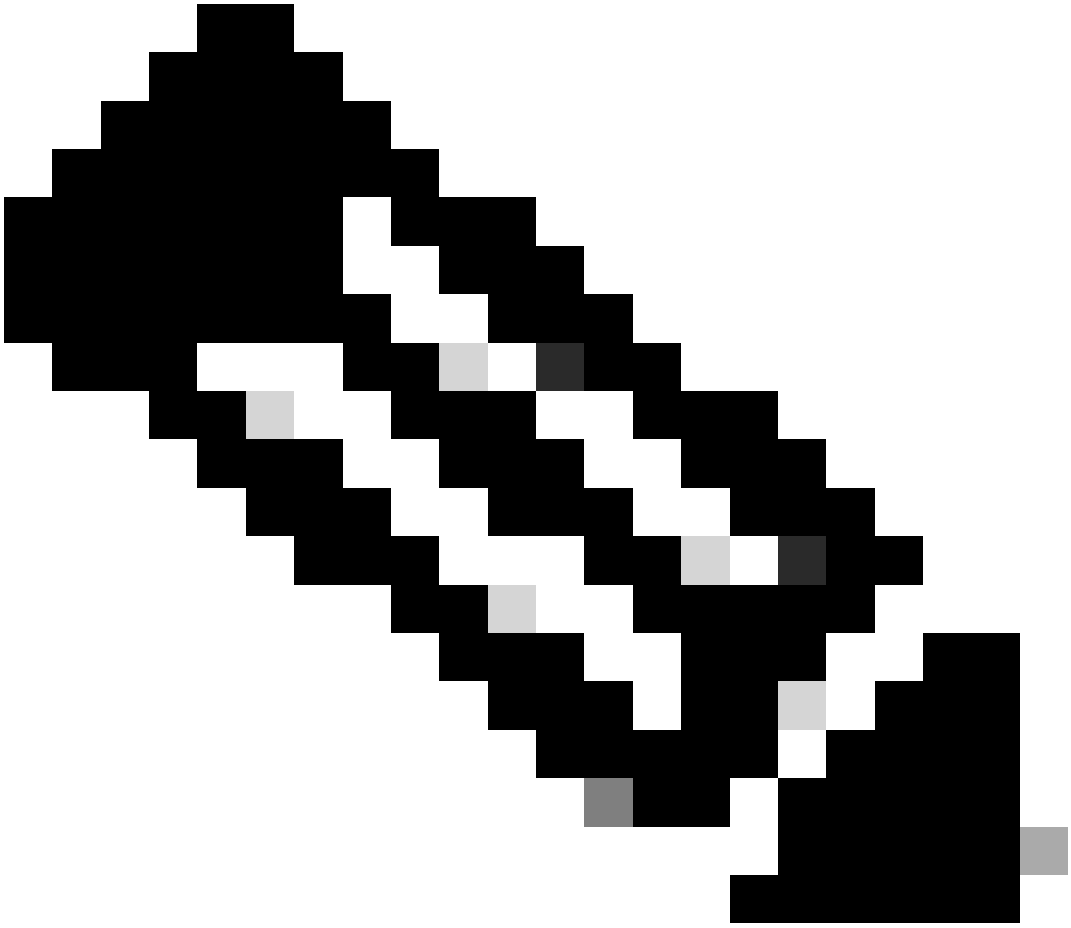
Passaggi:

- Attivate la feature bash-shell e attivate la modalità bash:

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

2. Esaminare il contenuto del dcos_sshd_config file:

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



Nota: è possibile utilizzare egrep per esaminare linee specifiche: cat /isan/etc/dcos_sshd_config | grep MAC

Opzione 3. Accedere al file "dcos_sshd_config" utilizzando un **file Dplug**

Ciò si applica a:

- N3K in esecuzione 6. X che non ha accesso alla shell

    - Tutti i codici N5K e N6K
- N7K in esecuzione 6. X e 7. Codici X

Passaggi:

1. Aprire una richiesta TAC per ottenere il file dplug corrispondente alla versione NXOS in esecuzione sullo switch.

2. Caricare il file dplug in bootflash e crearne una copia.

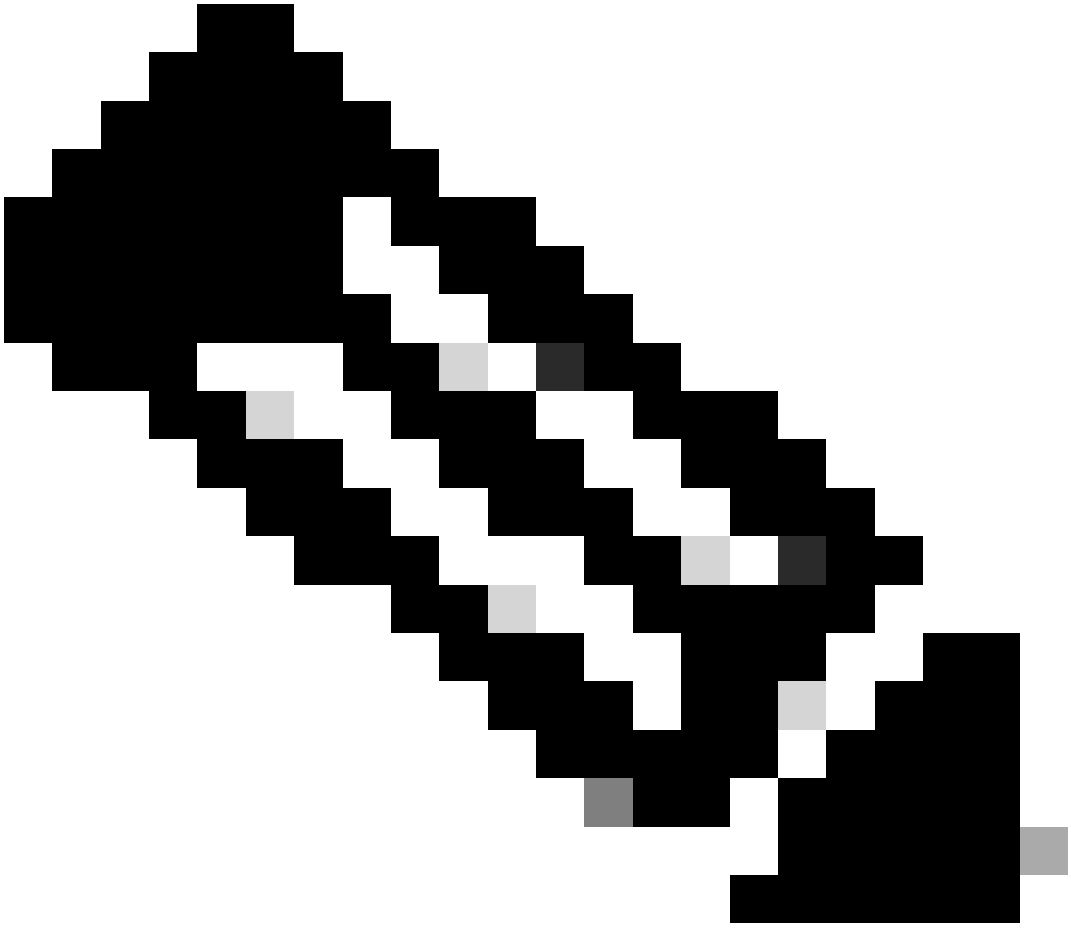
<#root>

switch# copy bootflash:

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

bootflash:

dp



Nota: una copia ("dp") del file dplug originale viene creata in bootflash, in modo che solo la copia venga rimossa dopo il caricamento del dplug e il file dplug originale rimanga in bootflash per le esecuzioni successive.

3. Caricare la copia del dplug con il 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. Esaminare il dcos_sshd_config file.

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

Soluzione

Passaggio 1. Esportare il file "dcos_sshd_config"

1. Inviare una copia del dcos_sshd_config file a bootflash:

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

2. Verificare che la copia sia in bootflash:

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

3. Esporta in un 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. Apportare le modifiche necessarie al file e reimportarlo in bootflash.

Passaggio 2. Importare il file "dcos_sshd_config"

1. Caricare il file modificatodcos_sshd_config in flash di avvio.

```
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#
```

Passaggio 3. Sostituire il file "dcos_sshd_config" originale con il comando Copia

Processo manuale (non persistente nei riavvii) - Tutte le piattaforme

Sostituendo il file esistentedcos_sshd_config in /isan/etc/ con un file modificatodcos_sshd_config situato in bootflash. Questo processo non è persistente dopo il riavvio

- Caricare un file modificatossh config in bootflash:

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

2. In modalità bash o Linux(debug)#, sovrascrivere il file esistentedcos_sshd_config con quello in bootflash:

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

3. Confermare l'esito delle modifiche:

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

Processo automatico - N7K

Utilizzando uno script EEM che viene attivato quando il log "VDC_MGR-2-VDC_ONLINE" viene attivato dopo un ricaricamento. Se EEM viene attivato, viene eseguito uno script ping e il file esistentedcos_sshd_config in viene sostituito/isan/etc/ con un file modificatodcos_sshd_config in bootflash. Questo vale solo per le versioni NX-OS che supportano "feature bash-shell".

- Caricare un file di configurazione ssh modificato in bootflash:

<#root>

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

dcos_sshd_config_modified_7k

switch#

2. Creare uno script ping che applichi le modifiche al dcos_sshd_config file. Assicurarsi di salvare il file con l'estensione "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

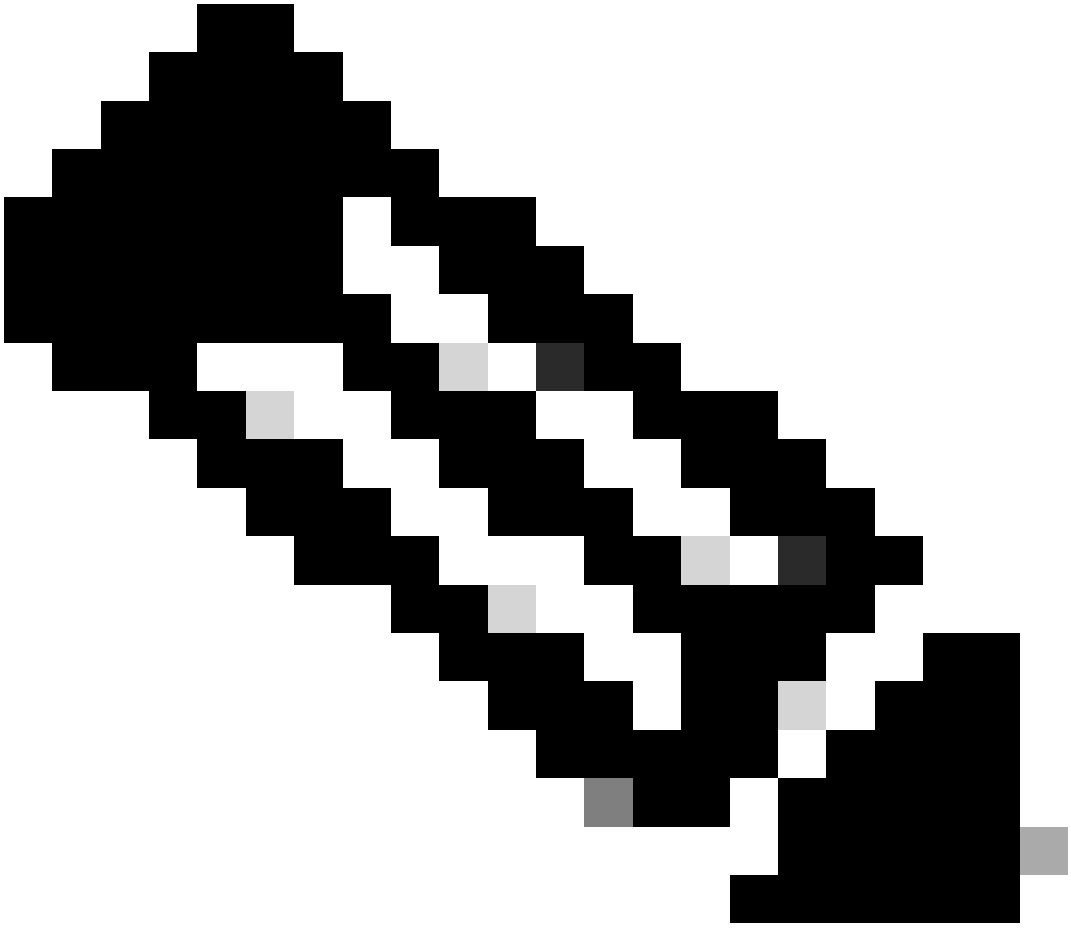
k /isan/etc/dcos_sshd_config\"")

3. Caricare lo script Python su bootflash.

<#root>

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

ssh_workaround_7k.py



Nota: gli script Python sono più o meno gli stessi su tutte le piattaforme, ad eccezione del N7K che contiene alcune righe aggiuntive per superare l'ID bug Cisco CSCva14865.

4. Assicurarsi che il nome deldcos_sshd_config file dello script e del bootflash (Passaggio 1.) siano gli stessi:

```
<#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. Eseguire lo script una volta, in modo che il file vengadcos_sshd_config modificato.

<#root>

switch#

source ssh_workaround_7k.py

```
switch#
```

5. Configurare uno script EEM in modo che lo script ping venga eseguito ogni volta che lo switch viene riavviato e riavviato.

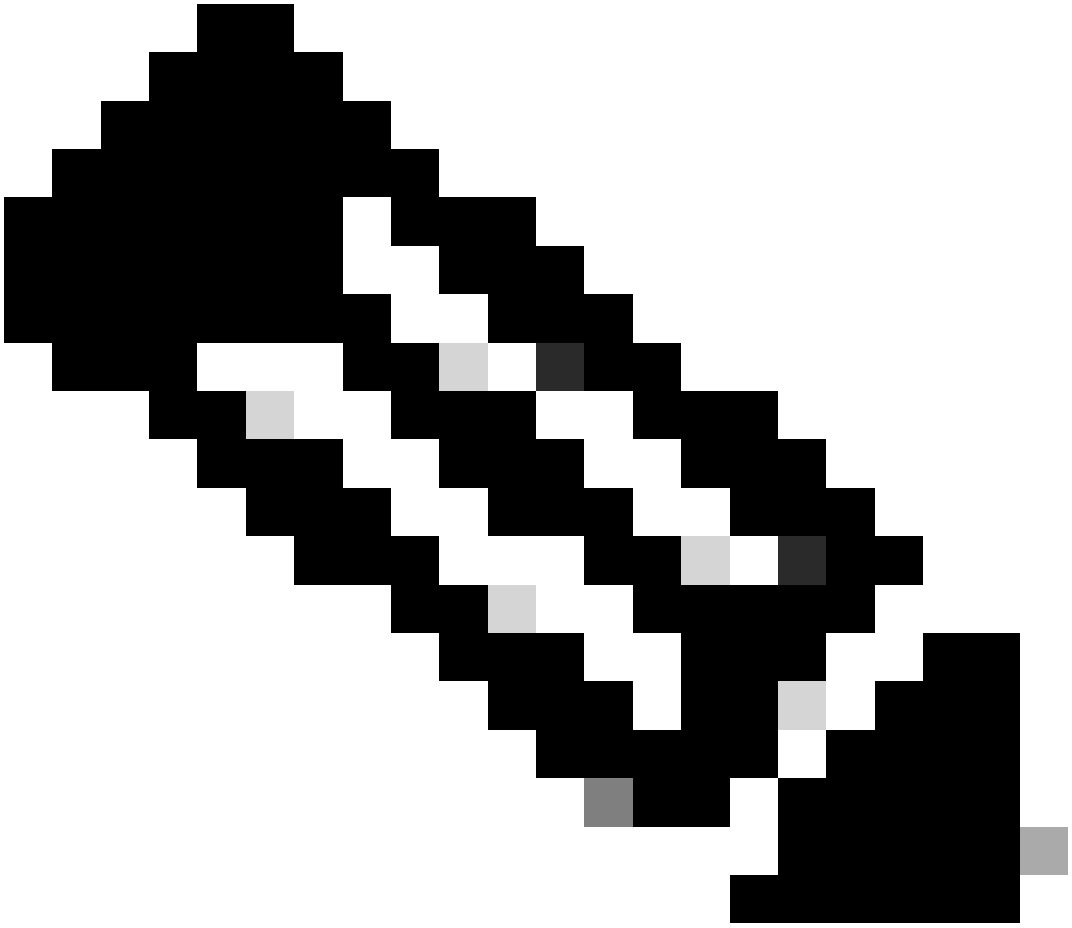
EEM N7K:

<#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 sintassi EEM può variare a seconda delle versioni di NXOS (alcune versioni richiedono "CLI" e altre "comandi CLI"), quindi accertarsi di controllare che i comandi EEM siano utilizzati correttamente.

Processo automatico - N9K, N3K

- Caricare un file di configurazione SSH modificato in 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. Creare uno script ping che applichi le modifiche al dcos_sshd_config file. Assicurarsi di salvare il file con l'estensione "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. Caricare lo script python su bootflash.

<#root>

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

ssh_workaround_9k.py

switch#

4. Assicurarsi che il nome deldcos_sshd_config file dello script e del bootflash (Passaggio 1.) siano gli stessi:

<#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. Eseguire lo script una volta, in modo che il file vengadcos_sshd_config modificato.

<#root>

switch#

python bootflash:ssh_workaround_9k.py

5. Configurare uno script EEM in modo che lo script ping venga eseguito ogni volta che lo switch viene riavviato e riavviato.

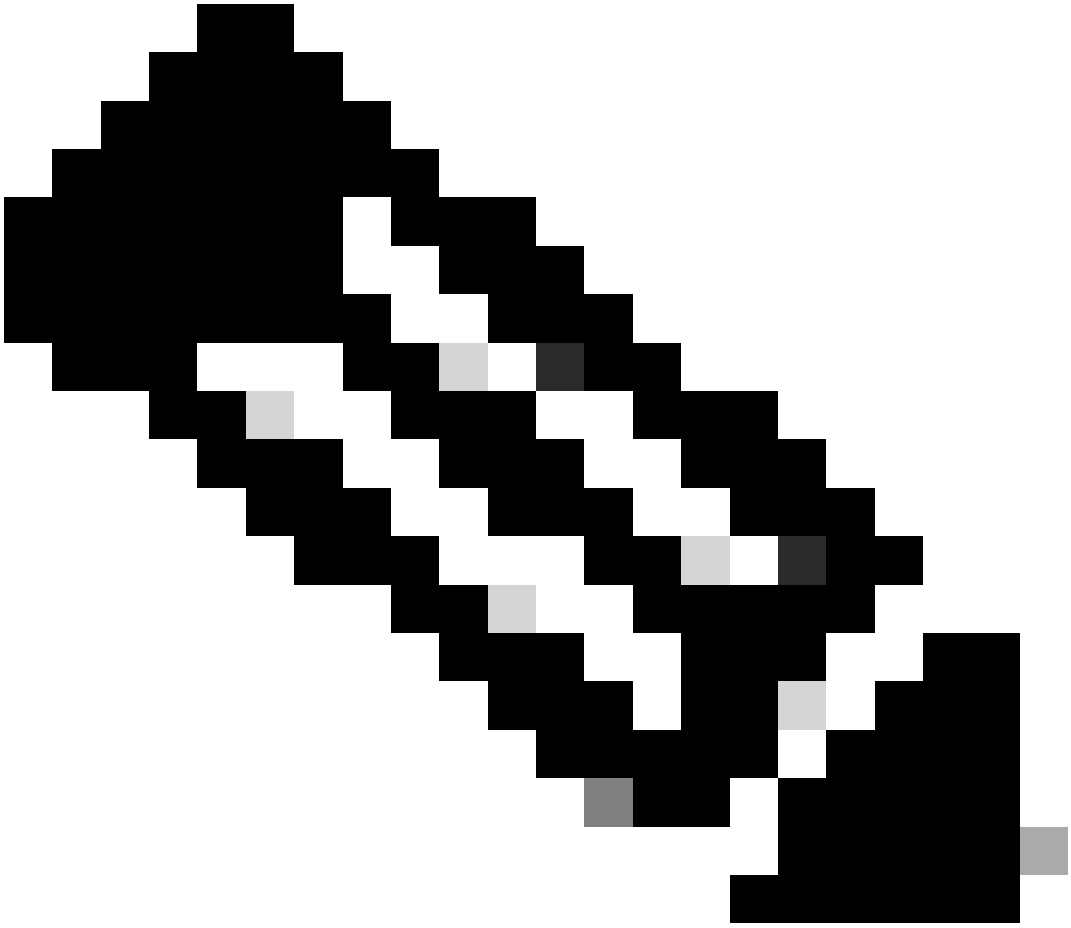
EEM N9K e N3K:

<#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 sintassi EEM può variare a seconda delle versioni di NXOS (alcune versioni richiedono "CLI" e altre "comandi CLI"), quindi accertarsi di controllare che i comandi EEM siano utilizzati correttamente.

Processo automatico - N5K, N6K

Un file dplug modificato è stato creato con l'ID bug Cisco CSCvr23488 per rimuovere i seguenti algoritmi Kex:

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

- diffie-hellman-group1-sha1

i file debug forniti tramite l'ID bug Cisco CSCvr23488 non sono gli stessi utilizzati per accedere alla shell Linux. Aprire una richiesta TAC per ottenere il dplug modificato dall'ID bug Cisco CSCvr23488.

- Verificare le impostazioni predefinitedcos_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

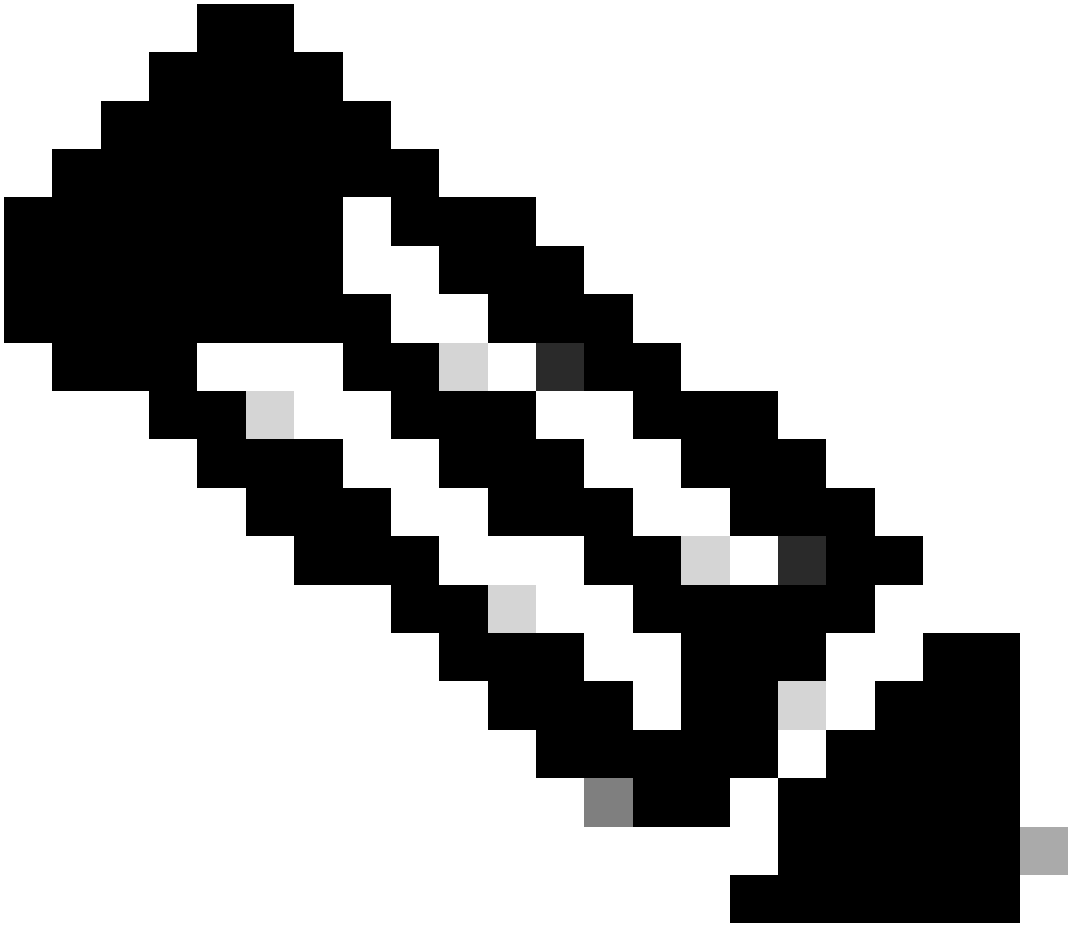
<--- mac algorithms
debug2: compression ctos: none,zlib@openssh.com
debug2:

compression stoc: none,zlib@openssh.com

<--- compression algorithms

2. Creare una copia del file dplug modificato.

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



Nota: una copia ("dp") del file dplug originale viene creata in bootflash in modo che solo la copia venga rimossa dopo il caricamento del dplug e il file dplug originale rimanga in bootflash per le esecuzioni successive.

---

3. Applicare manualmente il file dplug dall'ID bug Cisco CSCvr23488:

```
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. Verificare le nuove dcos_sshd_config impostazioni:

<#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:

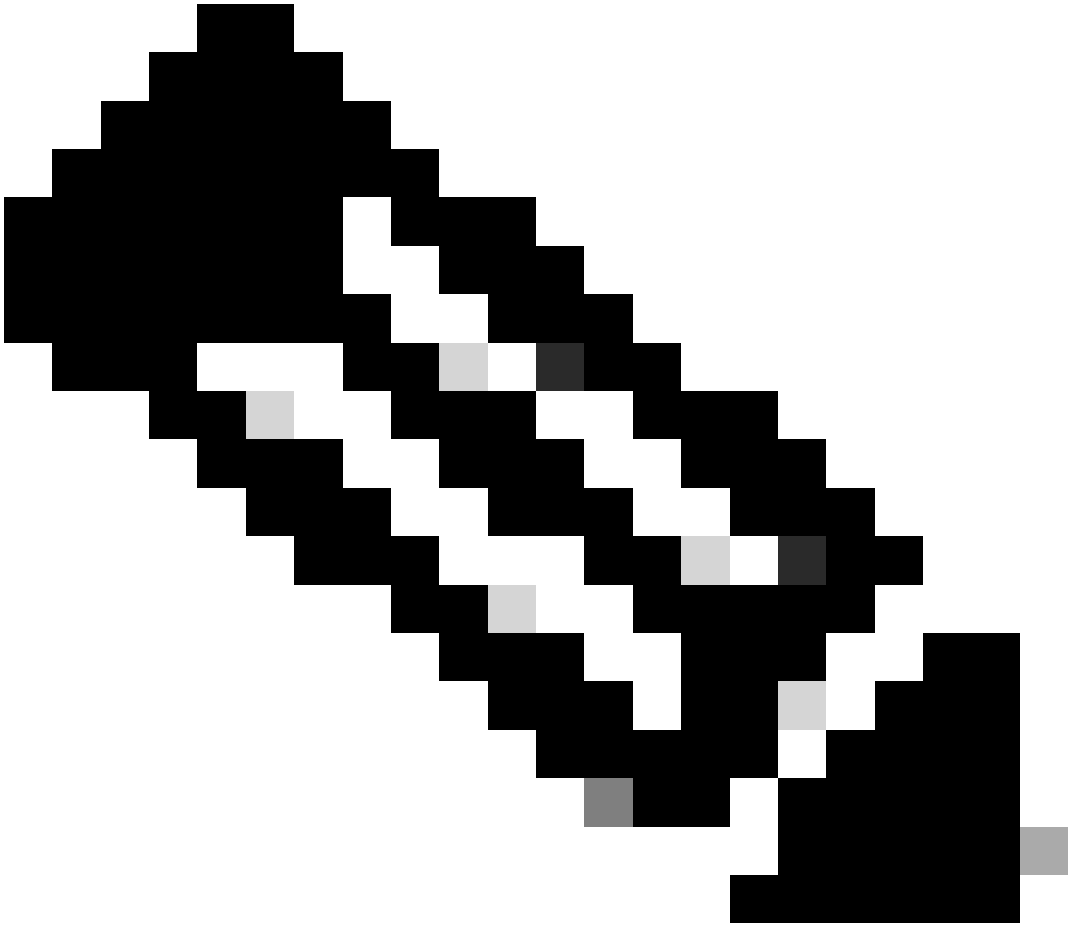
MACs stoc: hmac-sha1

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

compression stoc: none,zlib@openssh.com

5. Rendere persistente la modifica dopo il riavvio con uno 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:

- Dopo aver applicato il dplug modificato, la funzionalità SSH deve essere reimpostata su questa piattaforma.
- Verificare che il file dplug sia presente in bootflash e che EEM sia configurato con il nome file dplug corretto. Il nome del file dplug può variare a seconda della versione dello switch, quindi accertarsi di modificare lo script in base alle esigenze.
- L'azione 1 crea una copia del file dplug originale in bootflash in un altro file denominato "dp", in modo che il file dplug originale non venga eliminato dopo il caricamento.

Considerazioni sulla piattaforma

N5K/N6K

- Non è possibile modificare l'indirizzo MAC (Message Authentication Code) su queste piattaforme modificando il file dcos_sshd_config. L'unico MAC supportato è hmac-sha1.

N7K

- Per modificare gli indirizzi MAC, è necessario un codice 8.4. Per ulteriori informazioni, vedere l'ID bug Cisco CSCwc26065.
- "Sudo su" non è disponibile per default su 8.X. Fare riferimento all'ID bug Cisco: CSCva14865. Se eseguito, viene osservato questo errore:

```
<#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$
```

Per risolvere il problema, digitare:

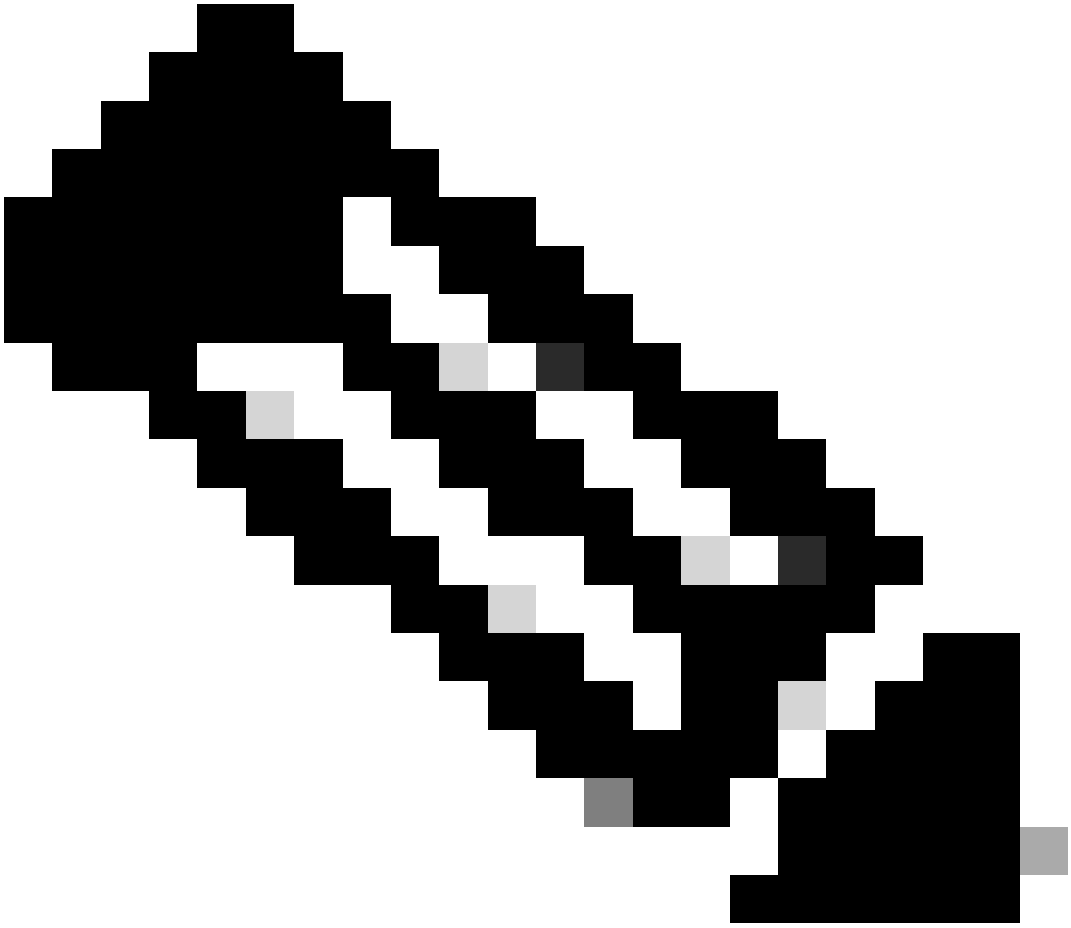
```
<#root>

bash-4.3$

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

Dopo questo "sudo su" funziona:

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



Nota: questa modifica non viene mantenuta dopo un ricaricamento.

- Esiste un file separatodcos_sshd_config per ogni VDC; nel caso in cui i parametri SSH debbano essere modificati su un VDC diverso, accertarsi di modificare il file corrispondentedcos_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

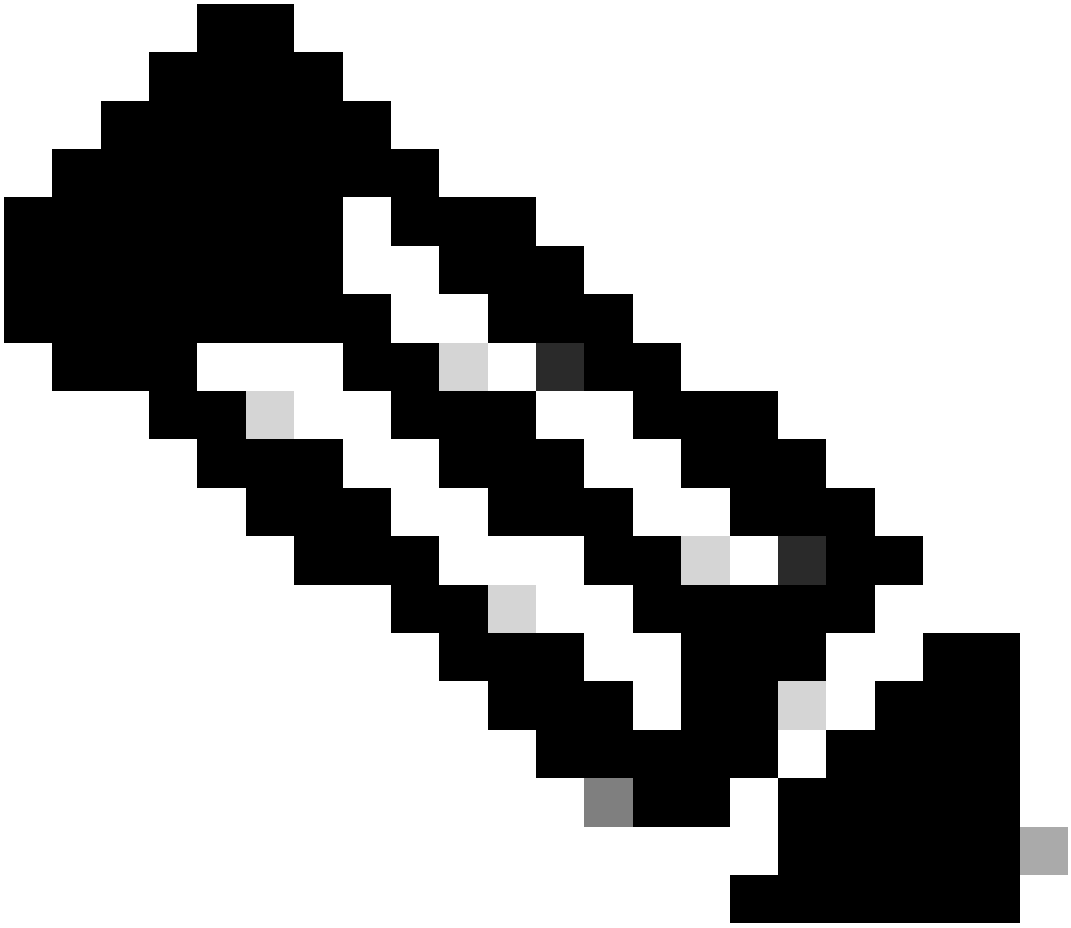
- Le modifiche sul dcos_sshd_config file non sono persistenti dopo il riavvio su nessuna piattaforma Nexus. Se le modifiche devono essere persistenti, è possibile utilizzare EEM per modificare il file a ogni avvio dello switch. Il miglioramento apportato a N9K modifica questo valore a partire da 10.4. Per ulteriori informazioni, vedere l'ID bug Cisco CSCwd82985.

N7K, N9K, N3K

Se necessario, è possibile aggiungere ulteriori elementi Ciphers, MAC e KexAlgorithms:

```
<#root>

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



Nota: questi comandi sono disponibili su Nexus 7000 con le versioni 8.3(1) e successive. Per la piattaforma Nexus 3000/9000, il comando è disponibile a partire dalla versione 7.0(3)I7(8). (Tutte le versioni 9.3(x) dispongono anche di questo comando. Vedere la guida alla configurazione della sicurezza di Cisco Nexus serie 9000 NX-OS, versione 9.3(x))

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).