Nexus 플랫폼에서 암호화, MAC, Kex 알고리즘 구성

목차

소개

이 문서에서는 Nexus 플랫폼에서 암호, MAC 및 Kex 알고리즘을 추가(또는 제거)하는 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

Linux 및 Bash의 기본 사항을 이해하는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

보안 스캔을 통해 Nexus 디바이스에서 사용하는 취약한 암호화 방법을 찾을 수 있는 경우가 있습니다. 이 경우 스위치의 파일을 dcos_sshd_config 변경하여 안전하지 않은 이러한 알고리즘을 제거해야 합니다.

사용 가능한 암호, MAC 및 Kex 알고리즘 검토

플랫폼에서 사용하는 암호, MAC 및 Kex 알고리즘을 확인하고 외부 디바이스에서 이를 확인하려면 다음 옵션을 사용할 수 있습니다.

옵션 1. PC에서 CMD 회선 사용

Nexus 디바이스에 연결할 수 있는 PC에서 CMD 줄을 열고 명령을 사용합니다 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

옵션 2. 기능 Bash-Shell을 사용하여 "dcos_sshd_config" 파일 **액세스**

이는 다음 경우에 적용됩니다.

- N3K 실행 7. X, 9. X, 10 X
- 모든 N9K 코드
- N7K(8.2 이상 실행)

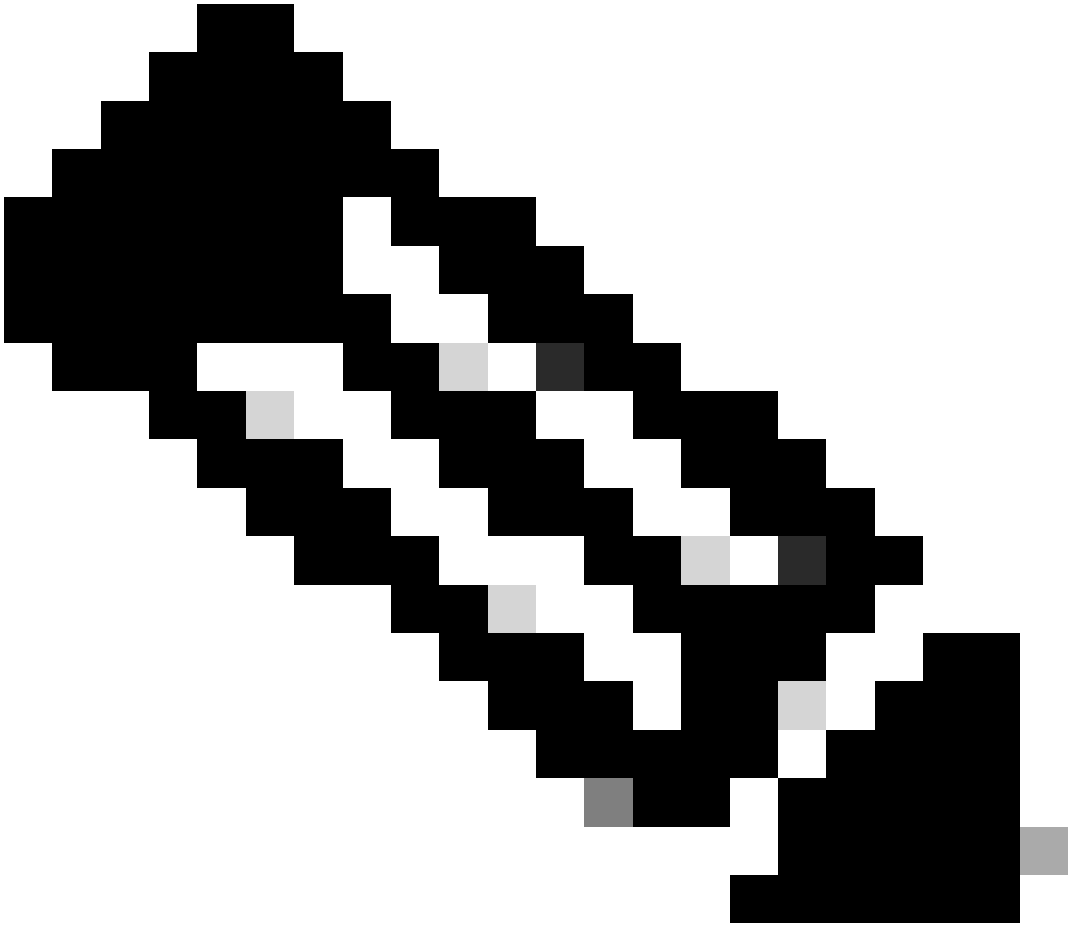
단계:

- bash-shell 기능을 활성화하고 bash 모드로 들어갑니다.

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

2. 파일에서 내용을 dcos_sshd_config 검토합니다.

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



참고: egrep를 사용하여 특정 행을 살펴볼 수 있습니다. cat /isan/etc/dcos_sshd_config | grep MAC

옵션 3. Dplug 파일을 사용하여 "dcos_sshd_config" **파일 액세스**

이는 다음 경우에 적용됩니다.

- N3K 실행 6. bash-shell에 액세스할 수 없는 X

    - 모든 N5K 및 N6K 코드
- N7K 실행 6. X와 7. X 코드

단계:

1. TAC 케이스를 열어 스위치에서 실행 중인 NXOS 버전과 일치하는 dplug 파일을 가져옵니다.

2. dplug 파일을 bootflash에 업로드하고 복사본을 만듭니다.

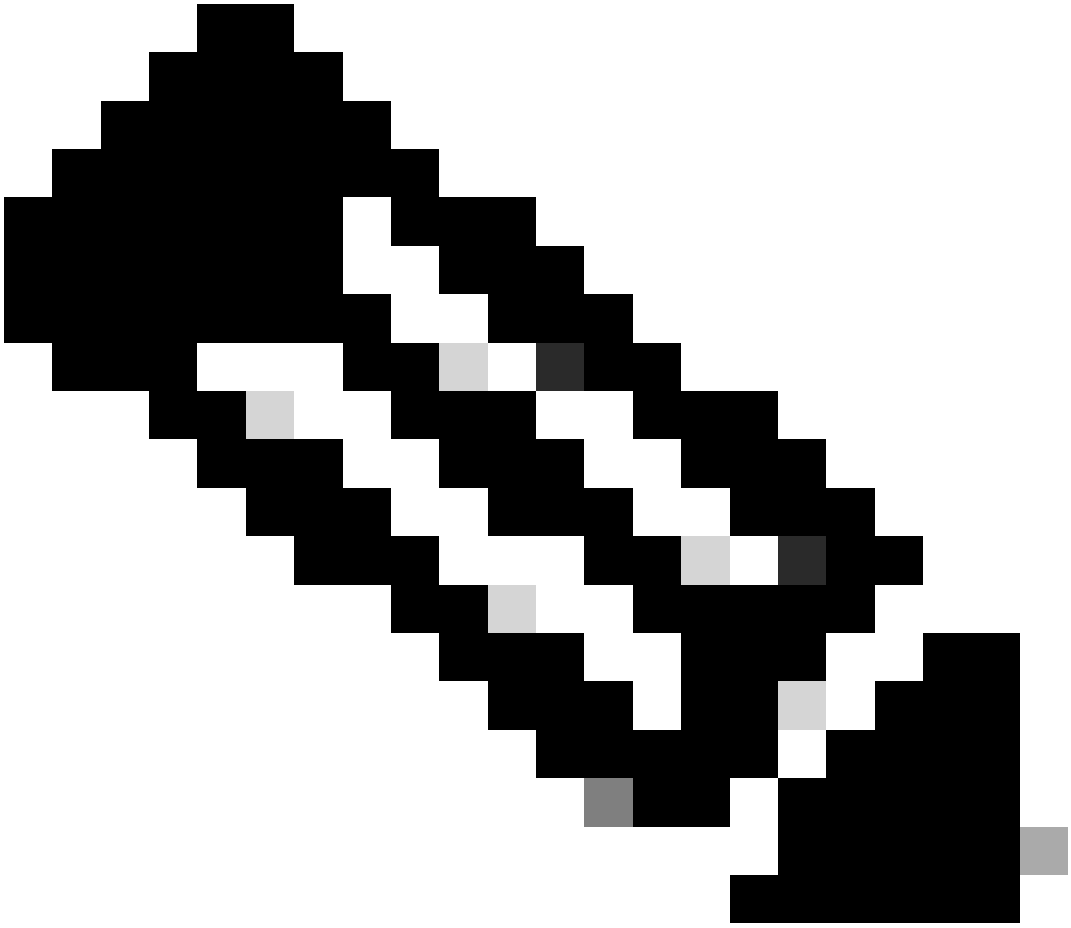
<#root>

switch# copy bootflash:

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

bootflash:

dp



참고: 원래 dplug 파일의 복사본("dp")이 bootflash에서 만들어지므로, dplug가 로드된 후에만 복사본이 제거되고 이후 실행을 위해 원래 dplug 파일이 bootflash에 남아 있습니다.

3. 명령을 통해 dplug 사본을 load 로드합니다.

<#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. dcos_sshd_config 파일 검토

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

솔루션

1단계. "dcos_sshd_config" 파일 내보내기

1. bootflash로 dcos_sshd_config 파일 복사본 보내기:

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

2. 복사본이 bootflash에 있는지 확인합니다.

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

3. 서버로 내보내기:

```
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. 파일을 필요한 대로 변경하고 bootflash로 다시 가져옵니다.

2단계. "dcos_sshd_config" 파일 가져오기

1. 수정된 파일을 dcos_sshd_config 업로드하여 플래시를 부팅합니다.

```
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#
```

3단계. 원본 "dcos_sshd_config" 파일을 복사본으로 바꿉니다.

수동 프로세스(재부팅 시 지속되지 않음) - 모든 플랫폼

의 기존 dcos_sshd_config 파일을 bootflash에/isan/etc/ 있는 수정된 dcos_sshd_config 파일로 교체합니다. 이 프로세스는 재부팅할 때마다 지속되지 않습니다

- 수정된 파일을 ssh config bootflash에 업로드:

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

2. bash 또는 Linux(debug)# 모드에서 기존dcos_sshd_config 파일을 bootflash의 파일로 덮어씁니다.

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

3. 변경이 성공했는지 확인합니다.

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

자동화된 프로세스 - N7K

다시 로드 후 "VDC_MGR-2-VDC_ONLINE" 로그가 나타날 때 트리거되는 EEM 스크립트를 사용하는 방법 EEM이 트리거될 경우, py 스크립트가 실행되며 기존 dcos_sshd_config 파일을 bootflash에 있는 수정된/isan/etc/ dcos_sshd_config 파일로 교체합니다. 이는 "feature bash-shell"을 지원하는 NX-OS 버전에만 적용됩니다.

- 수정된 ssh 구성 파일을 bootflash에 업로드합니다.

<#root>

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

dcos_sshd_config_modified_7k

switch#

2. 파일에 변경 사항을 적용하는 PY 스크립트를 dcos_sshd_config 생성합니다. 확장자가 "py"인 파일을 저장하십시오.

<#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

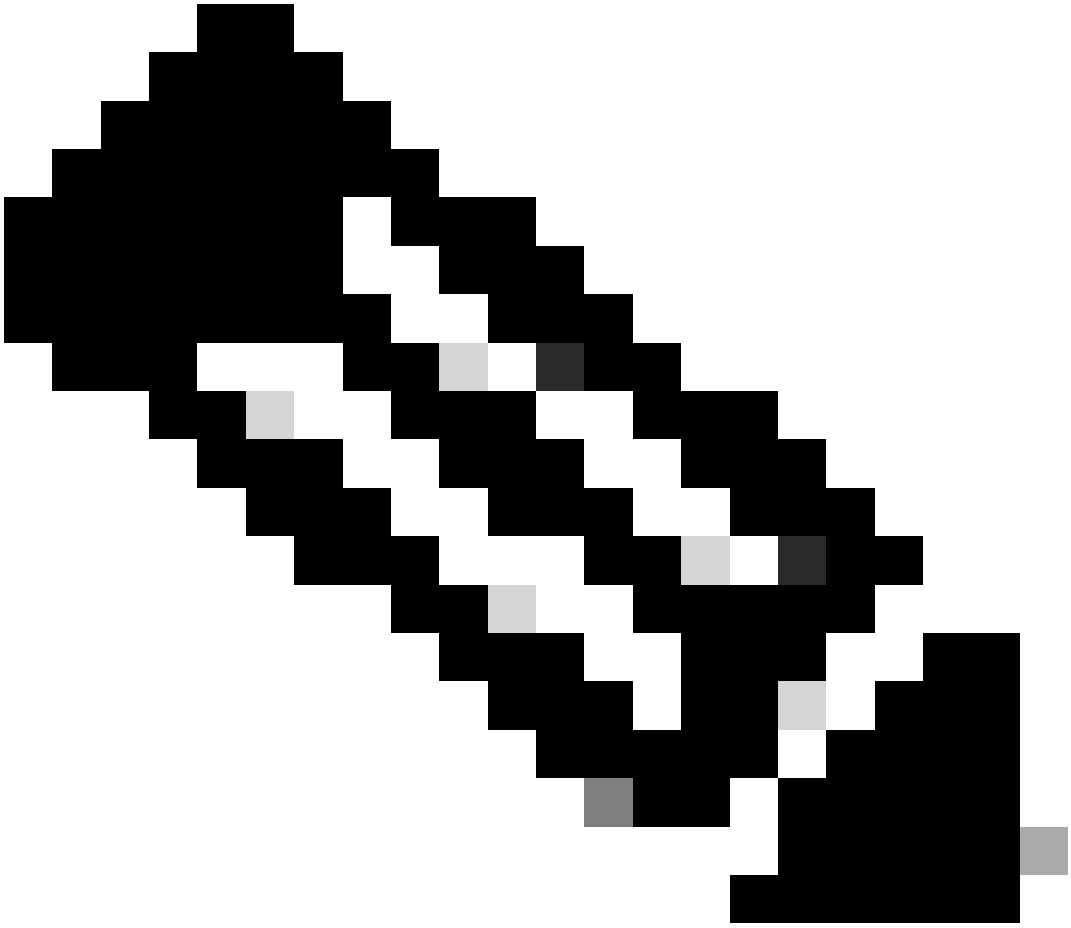
k /isan/etc/dcos_sshd_config\"")

3. Python 스크립트를 bootflash에 업로드합니다.

<#root>

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

ssh_workaround_7k.py



참고: Python 스크립트는 Cisco 버그 ID CSCva14865를 극복하기 위한 몇 가지 추가 라인이 포함된 N7K를 제외하고 모든 플랫폼에서 거의 동일합니다.

---

4. 스크립트dcos_sshd_config 및 bootflash의 파일 이름이 동일한지 확인합니다(1단계).

<#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. 파일을 변경할 수 있도록 스크립트를 한 번dcos_sshd_config 실행합니다.

<#root>

switch#

source ssh_workaround_7k.py

```
switch#
```

5. EEM 스크립트를 구성하여 스위치를 재부팅하고 다시 시작할 때마다 EEM 스크립트를 실행합니다.

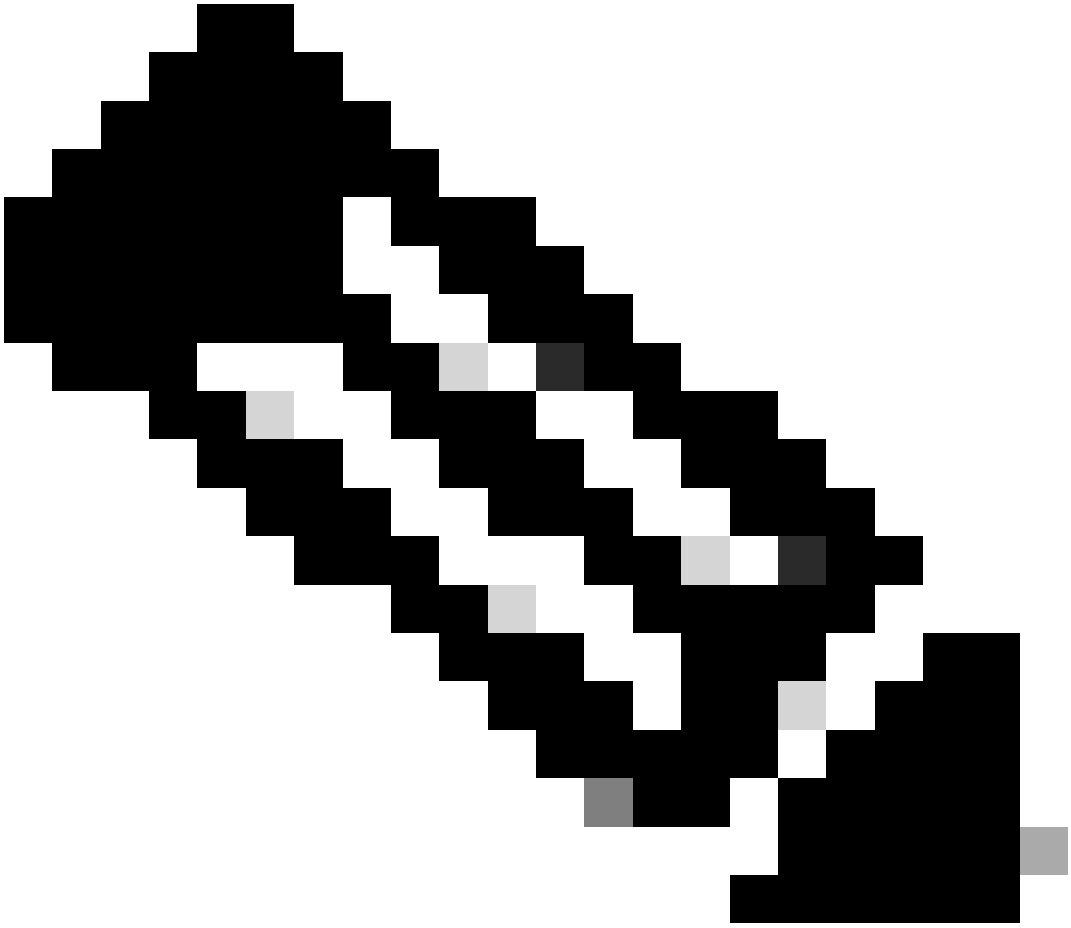
EEM N7K:

<#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"
```



참고: EEM 구문은 여러 NXOS 릴리스에 따라 달라질 수 있습니다(일부 버전에는 "CLI" 및 다른 버전에는 "CLI 명령"이 필요함). 따라서 EEM 명령이 제대로 실행되었는지 확인합니다.

자동화된 프로세스 - N9K, N3K

- 수정된 SSH 컨피그레이션 파일을 bootflash에 업로드합니다.

<#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. 파일에 변경 사항을 적용하는 PY 스크립트를 dcos_sshd_config 생성합니다. 파일을 "py" 확장자로 저장하십시오.

<#root>

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

/bootflash/dcos_sshd_config_modified

 /isan/etc/dcos_sshd_config\"")

3. python 스크립트를 bootflash에 업로드합니다.

<#root>

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

ssh_workaround_9k.py

switch#

4. 스크립트의dcos_sshd_config 파일 이름과 bootflash의 파일 이름이 동일한지 확인합니다(1단계).

<#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. 파일을 변경할 수 있도록 스크립트를 한 번dcos_sshd_config 실행합니다.

<#root>

switch#

python bootflash:ssh_workaround_9k.py

5. EEM 스크립트를 구성하여 스위치를 재부팅하고 다시 시작할 때마다 이 스크립트를 실행합니다.

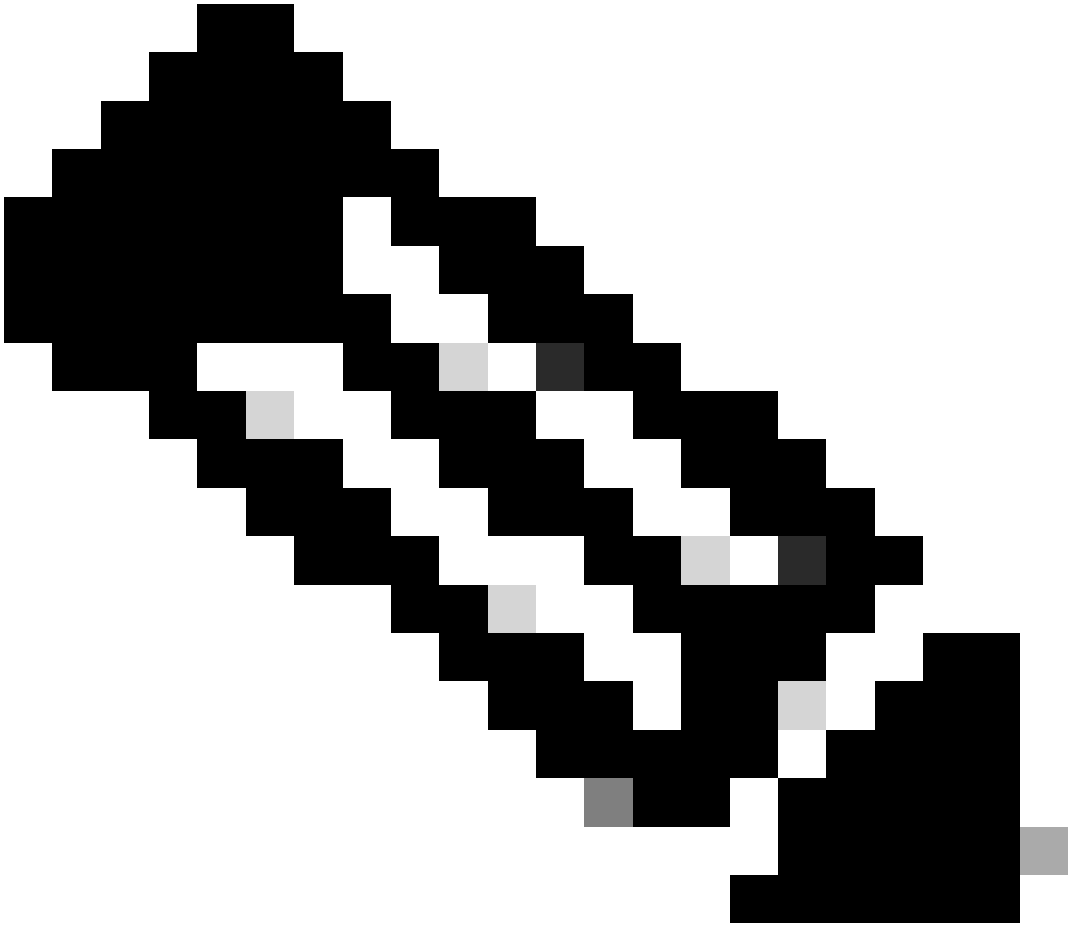
EEM N9K 및 N3K:

<#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



참고: EEM 구문은 여러 NXOS 릴리스에 따라 달라질 수 있습니다(일부 버전에는 "CLI" 및 다른 버전에는 "CLI 명령"이 필요함). 따라서 EEM 명령이 제대로 실행되었는지 확인합니다.

자동화된 프로세스 - N5K, N6K

Cisco 버그 ID CSCvr23488을 통해 수정된 dplug 파일을 생성하여 다음 Kex 알고리즘을 제거했습니다.

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

- diffie-hellman-group1-sha1

Cisco 버그 ID CSCvr23488을 통해 제공되는 dpug 파일은 Linux 셸에 액세스하는 데 사용되는 것과 동일하지 않습니다. TAC 케이스를 열어 Cisco 버그 ID CSCvr23488에서 수정된 플러그를 가져옵니다.

- 기본 설정을 dcos_sshd_config 확인합니다.

<#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

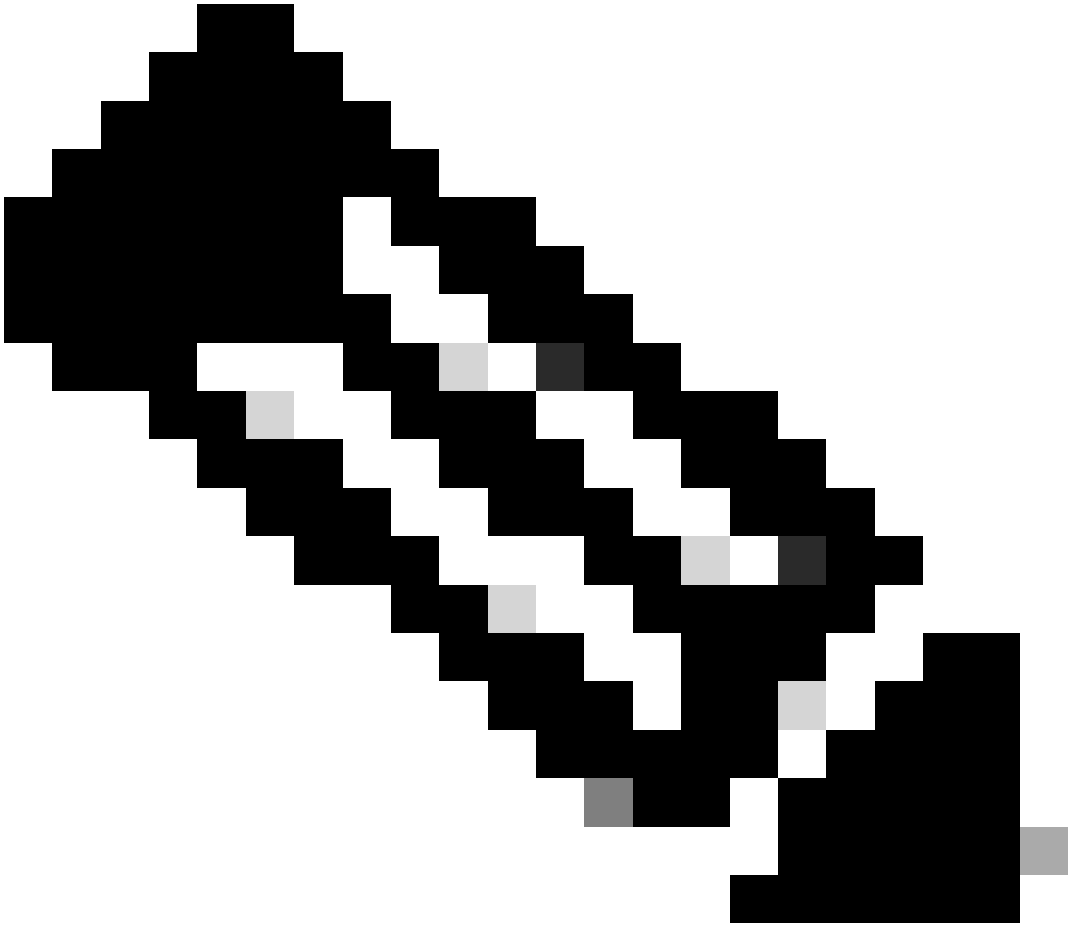
<--- mac algorithms
debug2: compression ctos: none,zlib@openssh.com
debug2:

compression stoc: none,zlib@openssh.com

<--- compression algorithms

2. 수정된 dplug 파일의 복사본을 생성합니다.

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



참고: 원래 dplug 파일의 복사본("dp")이 bootflash에서 만들어지므로 dplug가 로드된 후에만 복사본이 제거되고 이후 실행을 위해 원래 dplug 파일이 bootflash에 남아 있습니다.

---

3. Cisco 버그 ID CSCvr23488에서 dplug 파일을 수동으로 적용합니다.

```
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. 새 설정을 dcos_sshd_config 확인합니다.

<#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:

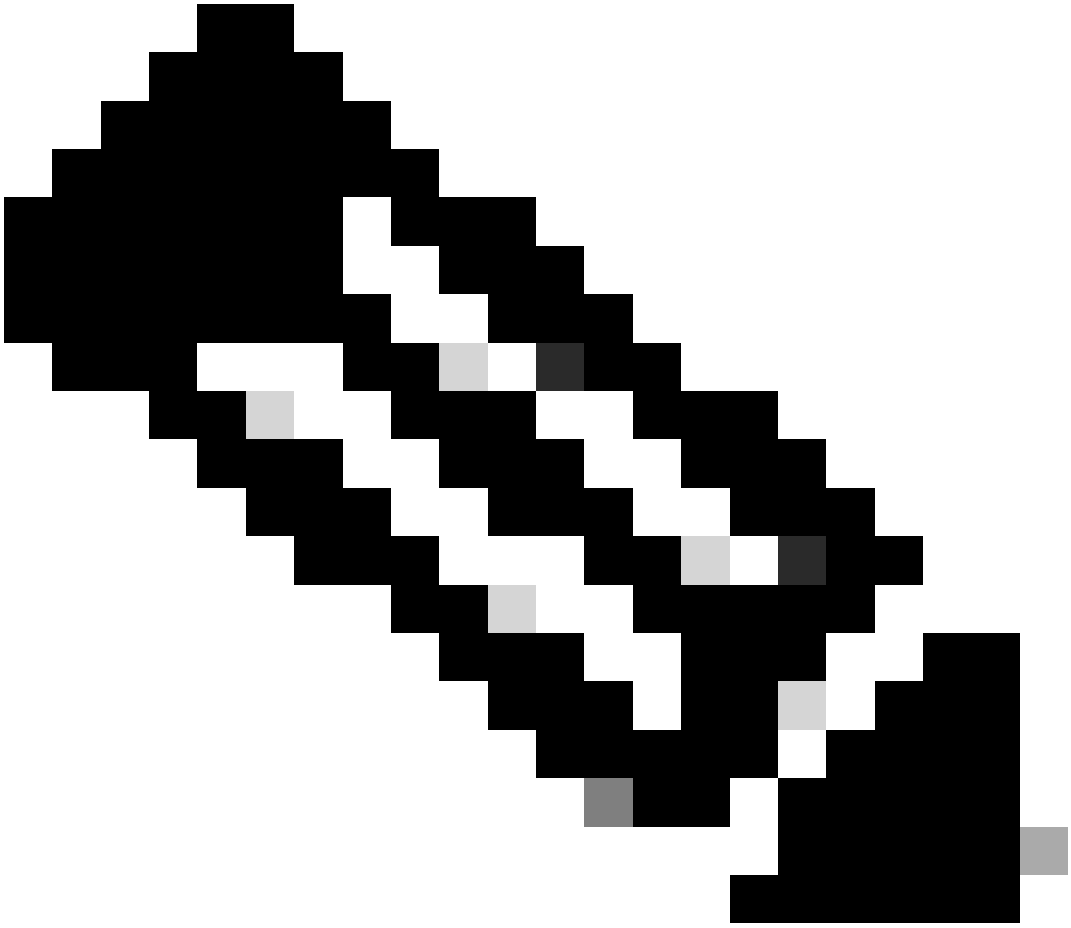
MACs stoc: hmac-sha1

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

compression stoc: none,zlib@openssh.com

5. EEM 스크립트를 사용하여 재부팅 시에도 이 변경을 지속되게 합니다.

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"



참고:

- 수정된 dplug를 적용한 후 이 플랫폼에서 SSH 기능을 재설정해야 합니다.
- Bootflash에 dplug 파일이 있고 EEM이 올바른 dplug 파일 이름으로 구성되어 있는지 확인합니다. dplug 파일 이름은 스위치 버전에 따라 달라질 수 있으므로 필요에 따라 스크립트를 수정해야 합니다.
- 작업 1은 bootflash에서 원본 dplug 파일의 복사본을 "dp"라는 다른 파일에 만들어 로드한 후 원본 dplug 파일이 삭제되지 않도록 합니다.

플랫폼 고려 사항

N5K/N6K

- dcos_sshd_config 파일을 수정하여 이러한 플랫폼에서 MAC(메시지 인증 코드)를 변경할 수 없습니다. 지원되는 유일한 MAC는 hmac-sha1입니다.

N7K

- MAC을 변경하려면 8.4 코드가 필요합니다. 자세한 내용은 Cisco 버그 ID CSCwc26065를 참조하십시오.
- 8.X에서는 기본적으로 "Sudo su"를 사용할 수 없습니다. 참조 Cisco 버그 ID: CSCva14865. 이 오류가 실행되면 다음과 같은 오류가 발생합니다.

<#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$

이를 해결하려면 다음과같이 입력합니다.

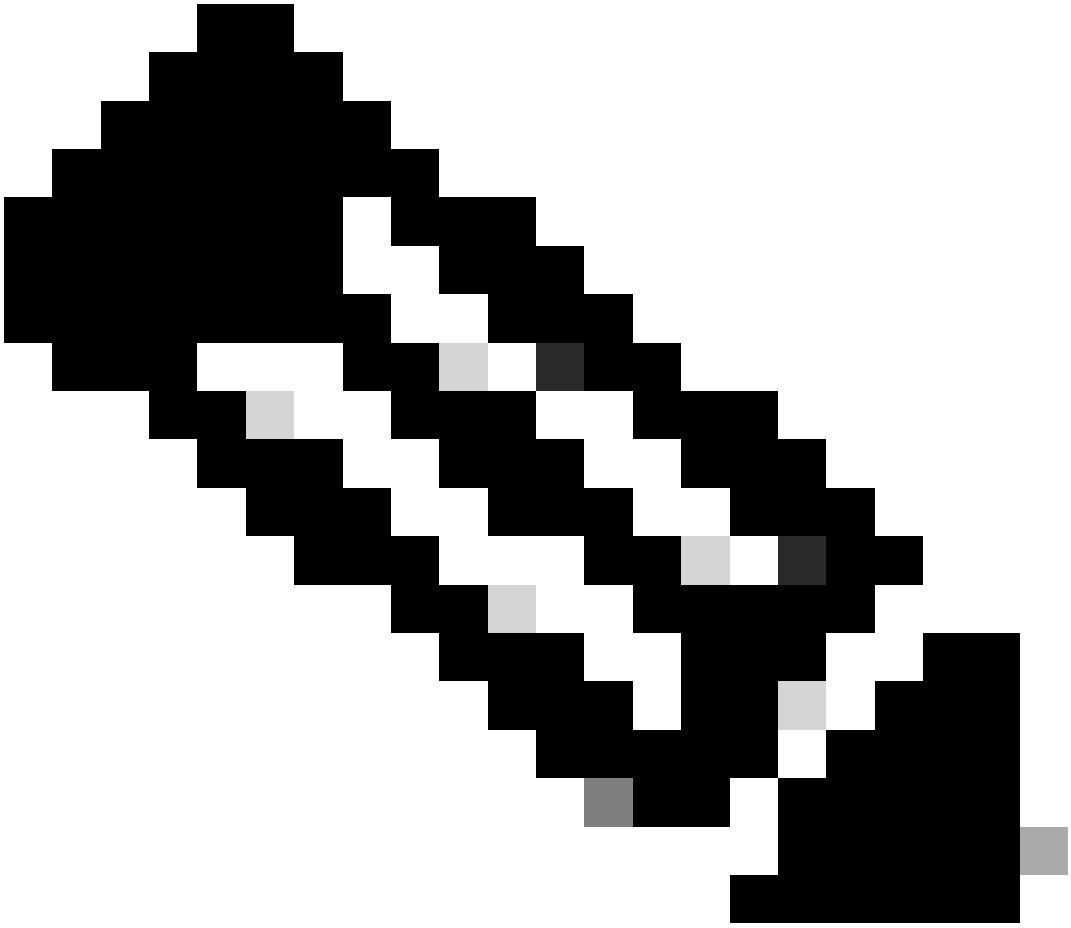
<#root>

bash-4.3$

sudo usermod -s /bin/bash root

이 "수도수"는 다음 작업을 수행 합니다.

bash-4.3$ sudo su
bash-4.3#



참고: 이 변경 사항은 다시 로드되지 않습니다.

- 각 VDC에는 별도의 dcos_sshd_config파일이 있습니다. 다른 VDC에서 SSH 매개변수를 수정해야 하는 경우 해당 파일을 수정해야 dcos_sshd_config 합니다.

<#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

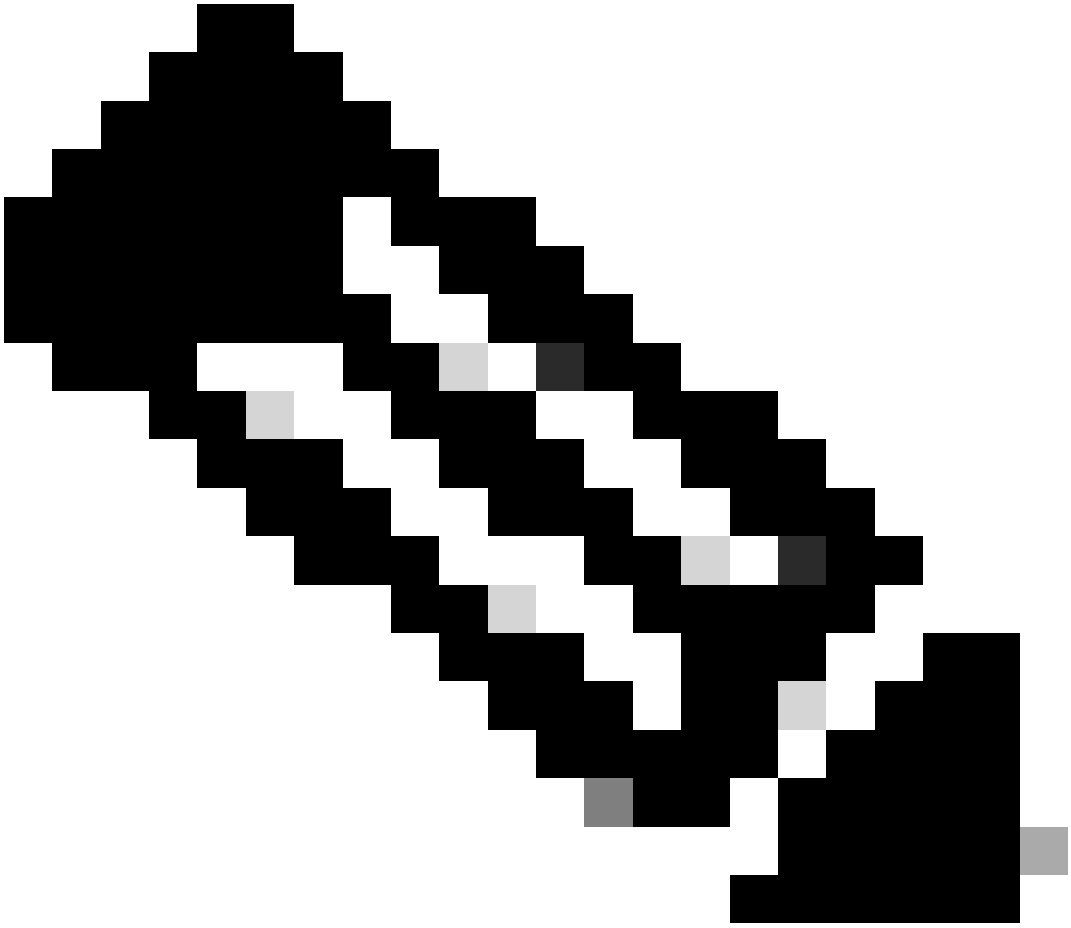
- Nexus 플랫폼의dcos_sshd_config 재부팅 시에도 파일의 변경 사항이 지속되지 않습니다. 변경 사항을 유지해야 하는 경우 EEM을 사용하여 스위치가 부팅될 때마다 파일을 수정할 수 있습니다. N9K의 향상은 이 시작 10.4를 변경합니다. 자세한 내용은 Cisco 버그 ID CSCwd82985를 참조하십시오.

N7K, N9K, N3K

필요한 경우 추가할 수 있는 추가 암호, MAC 및 KexAlgorithms가 있습니다.

<#root>

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



참고: 이 명령은 Nexus 7000 릴리스 8.3(1) 이상에서 사용할 수 있습니다. Nexus 3000/9000 플랫폼의 경우 이 명령을 릴리스 7.0(3)I7(8) 이상에서 사용할 수 있습니다. (모든 9.3(x) 릴리스에도 이 명령이 있습니다. Cisco Nexus 9000 Series NX-OS 보안 컨피그레이션 가이드, 릴리스 9.3(x)를 참조하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.