Configurar Cifras, MACs, algoritmos Kex em plataformas Nexus

Contents

Introdução

Este documento descreve as etapas para adicionar (ou) remover Cifras, MACs e algoritmos Kex em plataformas Nexus.

Pré-requisitos

Requisitos

A Cisco recomenda que você compreenda os conceitos básicos do Linux e do Bash.

Componentes Utilizados

As informações neste documento são baseadas nas seguintes versões de 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)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Às vezes, as verificações de segurança podem encontrar métodos de criptografia fracos usados pelos dispositivos Nexus. Se isso acontecer, alterações no arquivodcos_sshd_config nos switches serão necessárias para remover esses algoritmos não seguros.

Revisar Cifras, MACs e algoritmos Kex disponíveis

Para confirmar quais Cifras, MACs e Algoritmos Kex uma plataforma usa e verificar isso de um dispositivo externo, você pode usar estas opções:

Opção 1. Usando a linha CMD do PC

Abra uma linha CMD em um PC que possa acessar o dispositivo Nexus e use o 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

Opção 2. Acesse o arquivo "dcos_sshd_config" usando o **recurso Bash-Shell**

Aplicável a:

- N3K executando 7. X, 9. X, 10. X
- Todos os códigos N9K
- N7K executando 8.2 e posterior

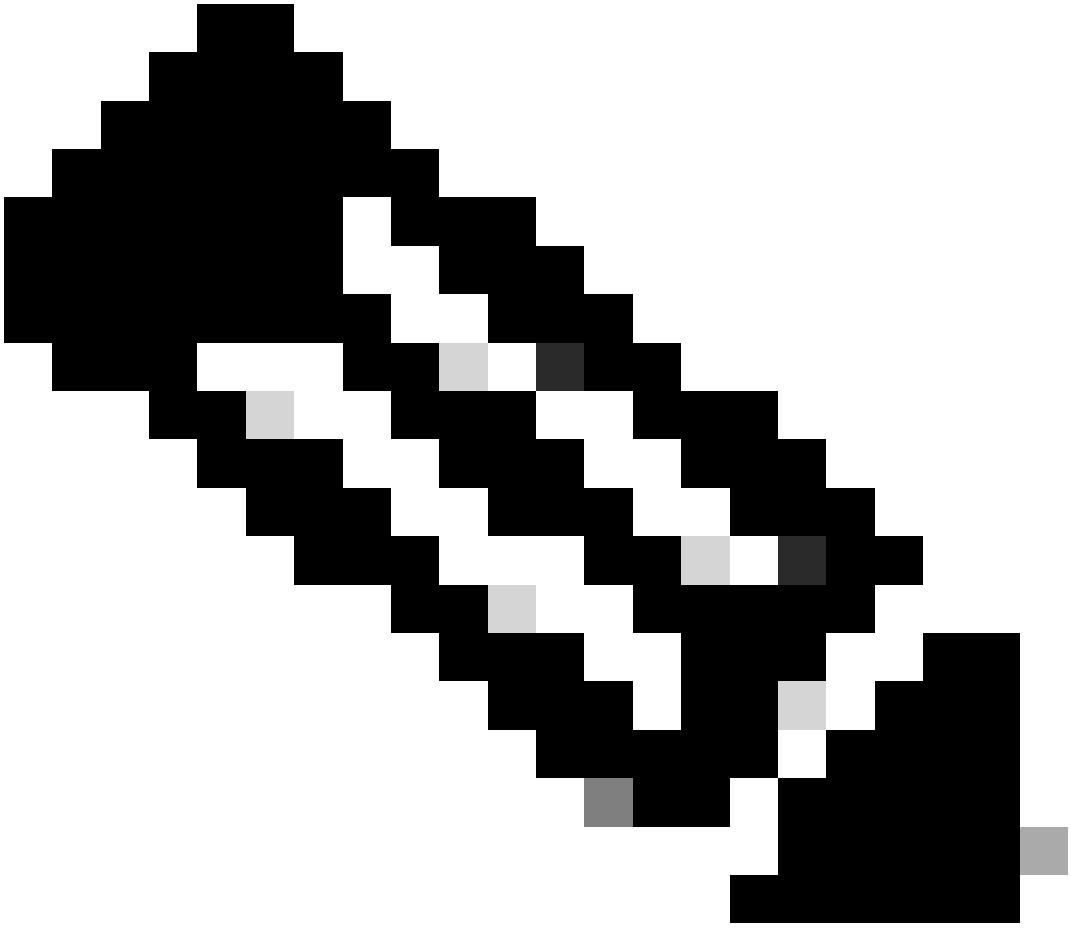
Etapas:

- Ative o recurso bash-shell e entre no modo bash:

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

2. Revise o conteúdo do arquivodcos_sshd_config:

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



Observação: você pode usar egrep para examinar linhas específicas: cat /isan/etc/dcos_sshd_config | grep MAC

Opção 3. Acesse o arquivo "dcos_sshd_config" usando um **arquivo Dplug**

Aplicável a:

- N3Ks executando 6. X que não tem acesso ao bash-shell

    - Todos os códigos N5K e N6K
- N7Ks executando 6. X e 7. Códigos X

Etapas:

1. Abra um caso TAC para obter o arquivo dplug que corresponde à versão do NXOS em execução no switch.

2. Carregue o arquivo dplug no bootflash e crie uma cópia dele.

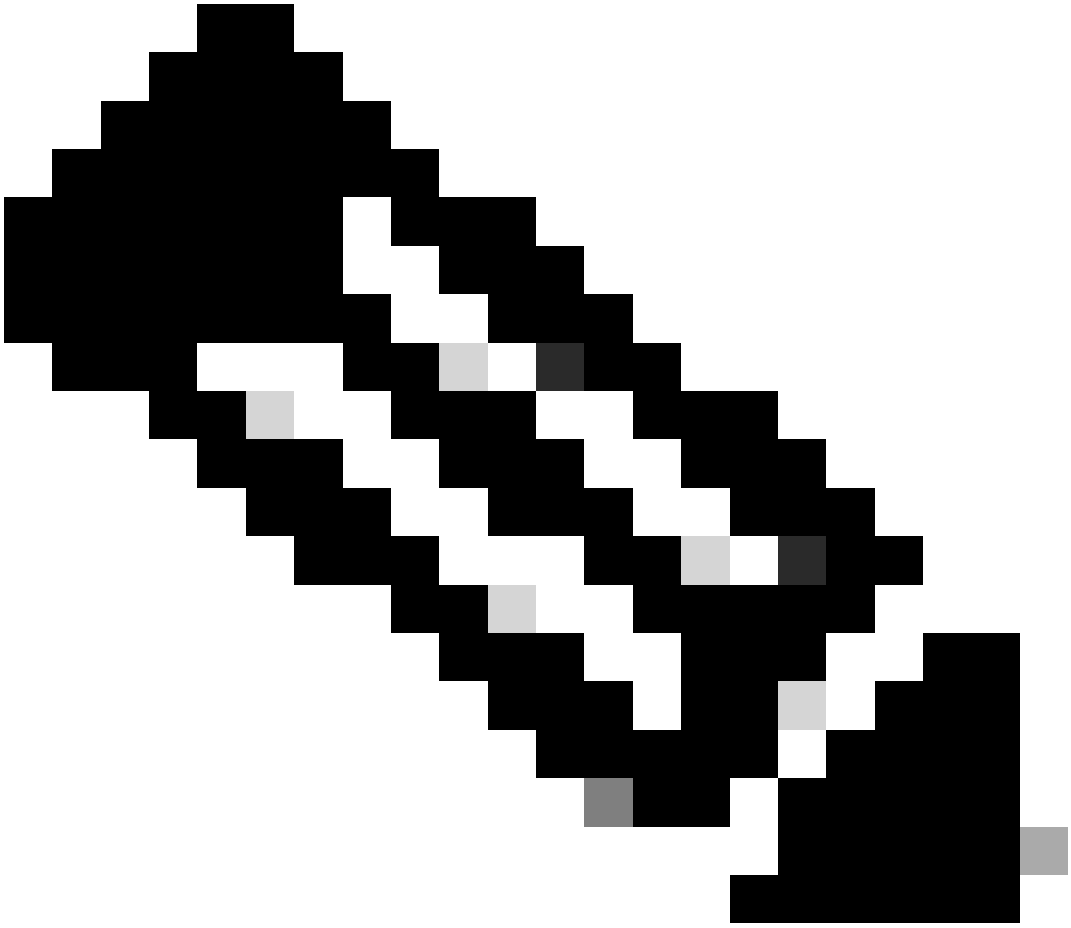
<#root>

switch# copy bootflash:

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

bootflash:

dp



Observação: uma cópia ("dp") do arquivo dplug original é criada no bootflash, de modo que somente a cópia seja removida depois que o dplug for carregado e o arquivo dplug original permaneça no bootflash para execuções subsequentes.

3. Carregue a cópia do dplug por meio do 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. Revisar dcos_sshd_config arquivo.

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

Solução

Etapa 1. Exporte o arquivo "dcos_sshd_config"

1. Envie uma cópia do arquivodcos_sshd_config para o bootflash:

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

2. Confirme se a cópia está no bootflash:

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

3. Exportar para um 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. Faça as alterações necessárias no arquivo e importe-o de volta para o bootflash.

Etapa 2. Importe o arquivo "dcos_sshd_config"

1. Carregue o arquivo modificadodcos_sshd_config na memória flash de inicialização.

```
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#
```

Etapa 3. Substitua o arquivo original "dcos_sshd_config" pela cópia

Processo manual (não persistente nas reinicializações) - Todas as plataformas

Substituindo o arquivo existentedcos_sshd_config em /isan/etc/ por um arquivo modificadodcos_sshd_config localizado no bootflash. Esse processo não é persistente nas reinicializações

- Carregar um arquivo modificadossh config no bootflash:

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

2. Enquanto estiver no modo bash ou Linux(debug)#, substitua o arquivo existentedcos_sshd_config pelo que estiver no bootflash:

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

3. Confirme se as alterações foram bem-sucedidas:

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

Processo automatizado - N7K

Usando um script EEM que é acionado quando o registro "VDC_MGR-2-VDC_ONLINE" é ativado após um recarregamento. Se o EEM for acionado, um script py será executado e substituirá o arquivo existentedcos_sshd_config em /isan/etc/ por um arquivo modificadodcos_sshd_config localizado no bootflash. Isso só se aplica às versões do NX-OS que suportam "feature bash-shell".

- Carregue um arquivo de configuração ssh modificado para o bootflash:

<#root>

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

dcos_sshd_config_modified_7k

switch#

2. Crie um script de cópia que aplique alterações ao dcos_sshd_config arquivo. Certifique-se de salvar o arquivo com a extensão "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

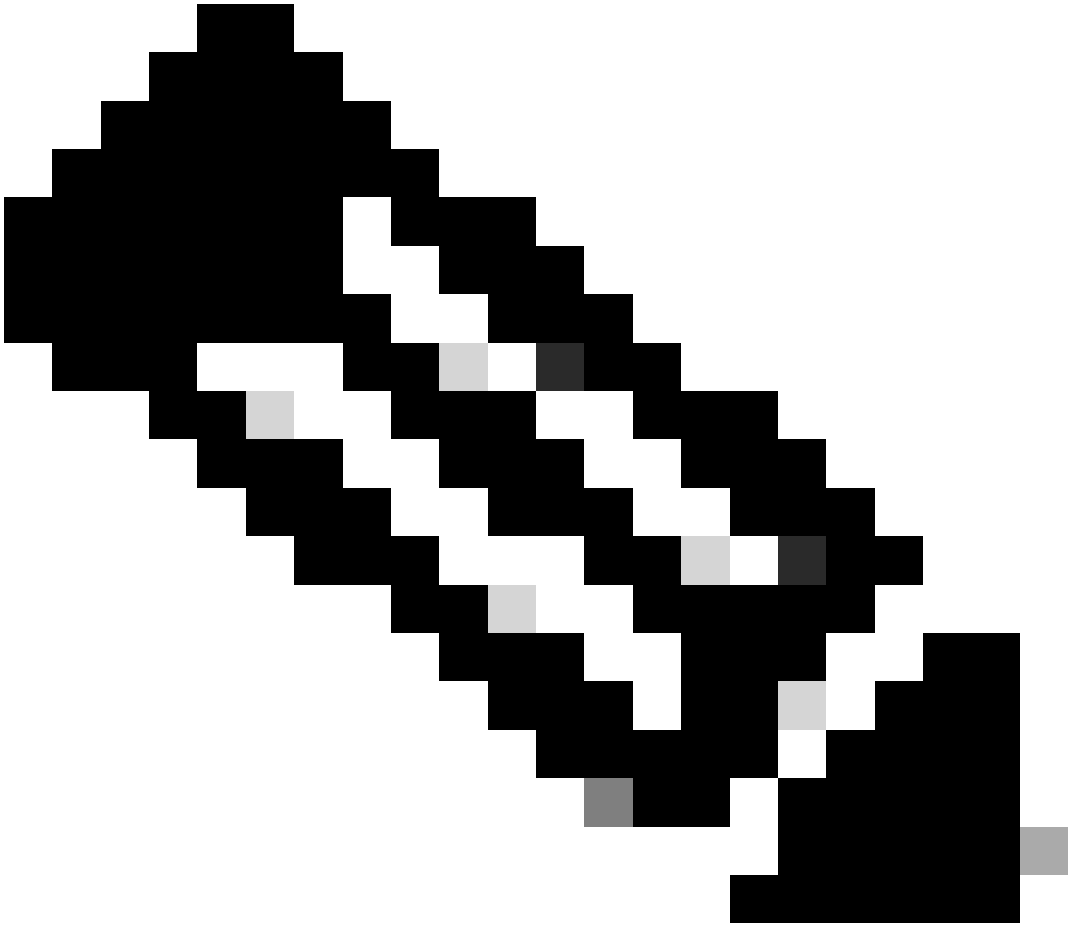
k /isan/etc/dcos_sshd_config\"")

3. Carregue o script Python no bootflash.

<#root>

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

ssh_workaround_7k.py



Observação: scripts Python são praticamente os mesmos em todas as plataformas, exceto no N7K, que contém algumas linhas adicionais para superar o bug da Cisco ID CSCva14865.

4. Certifique-se de que o nome dodcos_sshd_config arquivo do script e do bootflash (Etapa 1.) sejam os mesmos:

<#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. Execute o script uma vez, para que o arquivo sejadcos_sshd_config alterado.

<#root>

switch#

source ssh_workaround_7k.py

```
switch#
```

5. Configure um script EEM para que o script py seja executado sempre que o switch for reinicializado e voltar a funcionar.

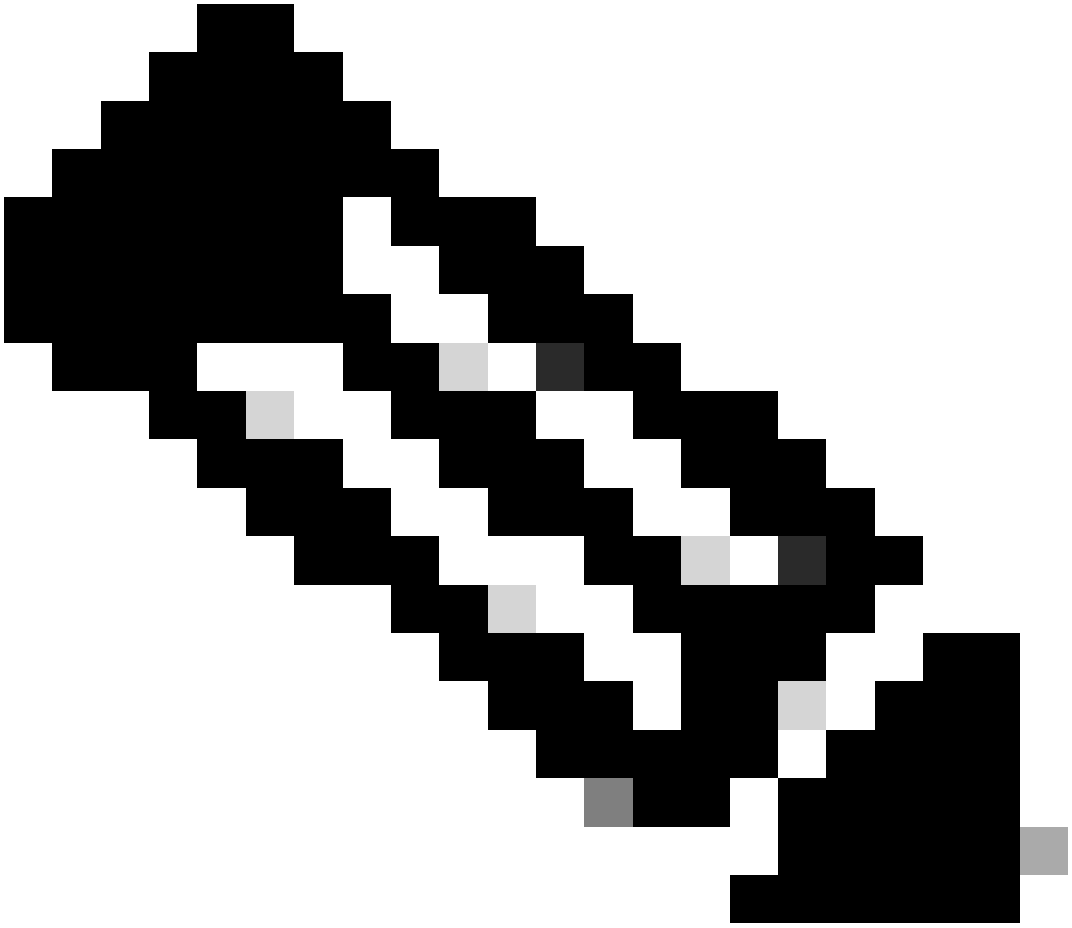
EEM N7K:

<#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"
```



Observação: a sintaxe do EEM pode variar em diferentes versões do NXOS (algumas versões exigem "CLI" e outras "comando CLI"), portanto verifique se os comandos do EEM foram usados corretamente.

Processo automatizado - N9K, N3K

- Carregue um arquivo de configuração SSH modificado para o 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. Crie um script de cópia que aplique alterações ao dcos_sshd_config arquivo. Certifique-se de salvar o arquivo com a extensão "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. Carregue o script python no bootflash.

<#root>

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

ssh_workaround_9k.py

switch#

4. Certifique-se de que o nome dodcos_sshd_config arquivo do script e do bootflash (Etapa 1.) sejam os mesmos:

<#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. Execute o script uma vez, para que o arquivo sejadcos_sshd_config alterado.

<#root>

switch#

python bootflash:ssh_workaround_9k.py

5. Configure um script EEM para que o script py seja executado sempre que o switch for reinicializado e voltar a funcionar.

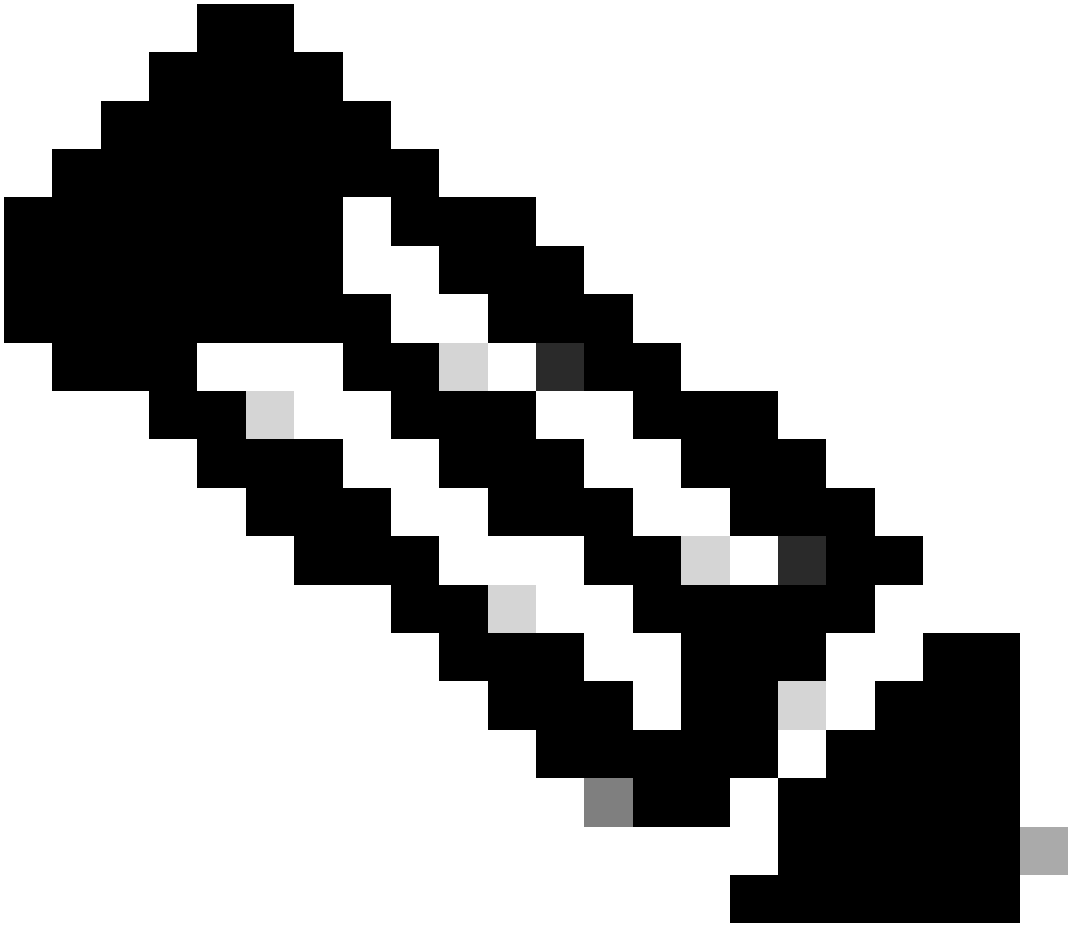
EEM N9K e N3K:

<#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



Observação: a sintaxe do EEM pode variar em diferentes versões do NXOS (algumas versões exigem "CLI" e outras "comando CLI"), portanto verifique se os comandos do EEM foram usados corretamente.

Processo automatizado - N5K, N6K

Um arquivo dplug modificado foi criado através do bug da Cisco ID CSCvr23488 para remover estes algoritmos Kex:

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

- diffie-hellman-group1-sha1

Os arquivos dpug fornecidos através do bug da Cisco ID CSCvr23488 não são os mesmos que os usados para acessar o Linux Shell. Abra um caso no TAC para obter o conector modificado a partir da ID de bug da Cisco CSCvr23488.

- Verifique as configurações padrãodcos_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

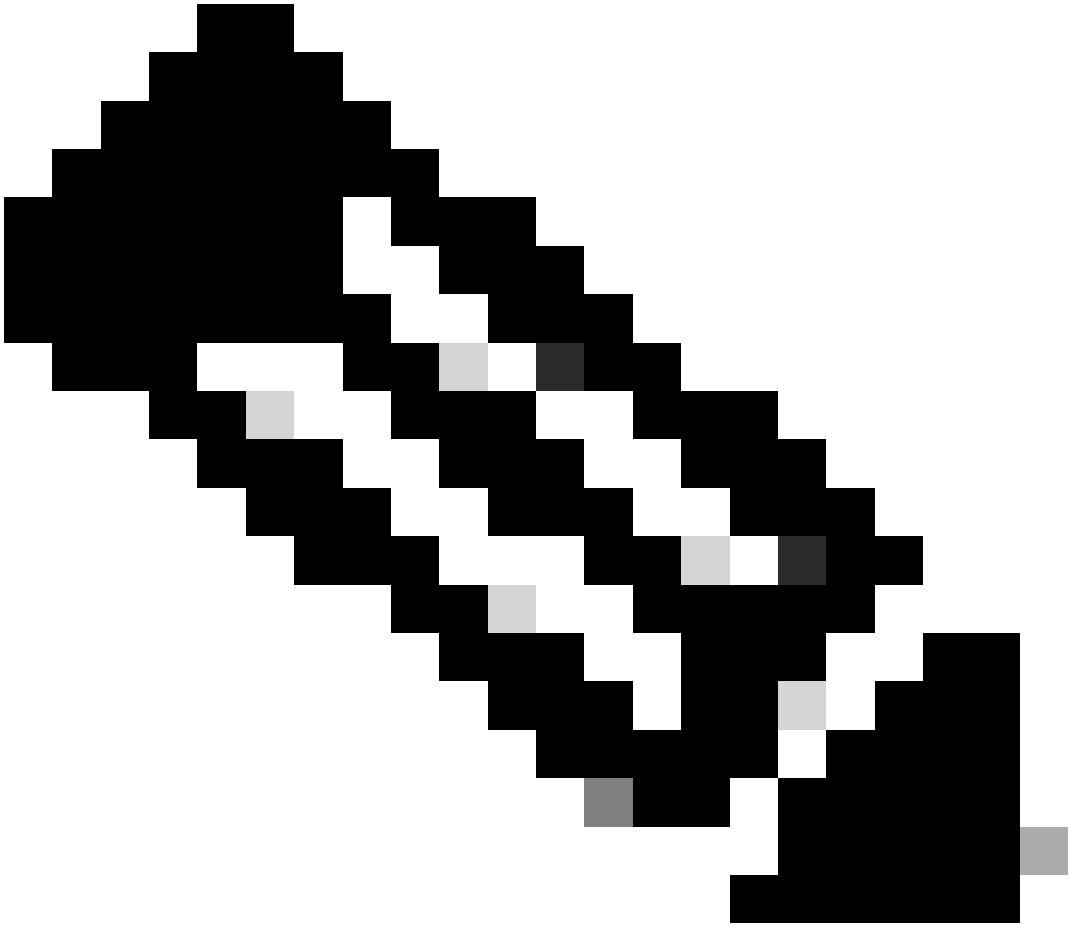
<--- mac algorithms
debug2: compression ctos: none,zlib@openssh.com
debug2:

compression stoc: none,zlib@openssh.com

<--- compression algorithms

2. Crie uma cópia do arquivo dplug modificado.

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



Observação: uma cópia ("dp") do arquivo dplug original é criada no bootflash para que somente a cópia seja removida depois que o dplug for carregado e o arquivo dplug original permaneça no bootflash para execuções subsequentes.

---

3. Aplique o arquivo dplug da ID de bug da 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. Verifique as novas dcos_sshd_config configurações:

<#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:

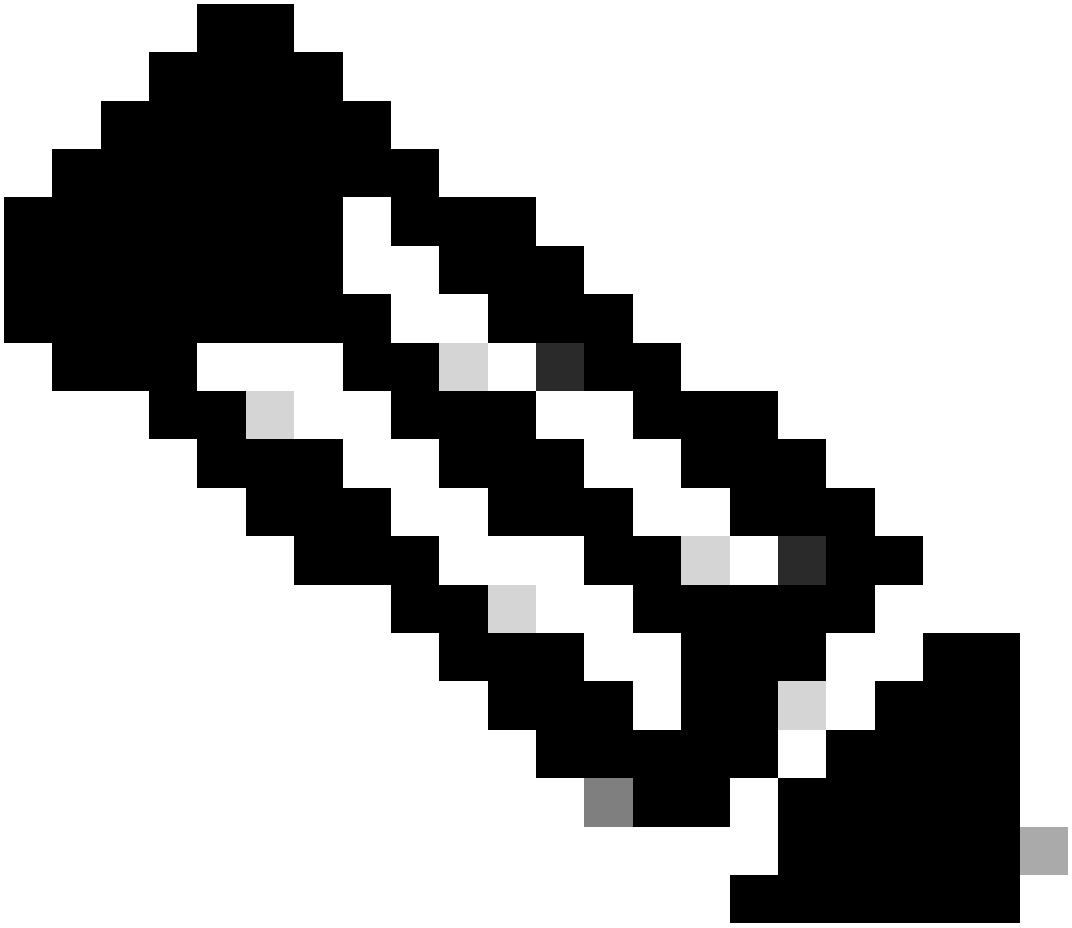
MACs stoc: hmac-sha1

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

compression stoc: none,zlib@openssh.com

5. Torne essa alteração persistente nas reinicializações com um 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"



Note:

- Depois que o dplug modificado é aplicado, o recurso SSH deve ser redefinido nesta plataforma.
- Verifique se o arquivo dplug está presente no bootflash e se o EEM está configurado com o nome de arquivo dplug apropriado. O nome do arquivo dplug pode variar dependendo da versão do switch, portanto, certifique-se de modificar o script conforme necessário.
- A ação 1 cria uma cópia do arquivo dplug original no bootflash para outro chamado "dp", de modo que o arquivo dplug original não seja excluído após ser carregado.

Considerações sobre a plataforma

N5K/N6K

- O MAC (Message Authentication Code) não pode ser alterado nessas plataformas modificando o arquivo dcos_sshd_config. O único MAC suportado é hmac-sha1.

N7K

- Para que os MACs sejam alterados, é necessário um código 8.4. Consulte o bug da Cisco ID CSCwc26065 para obter detalhes.
- "Sudo su" não está disponível por padrão no 8.X. ID do bug Cisco de referência: CSCva14865. Se executado, este erro é observado:

<#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 superar isso, digite:

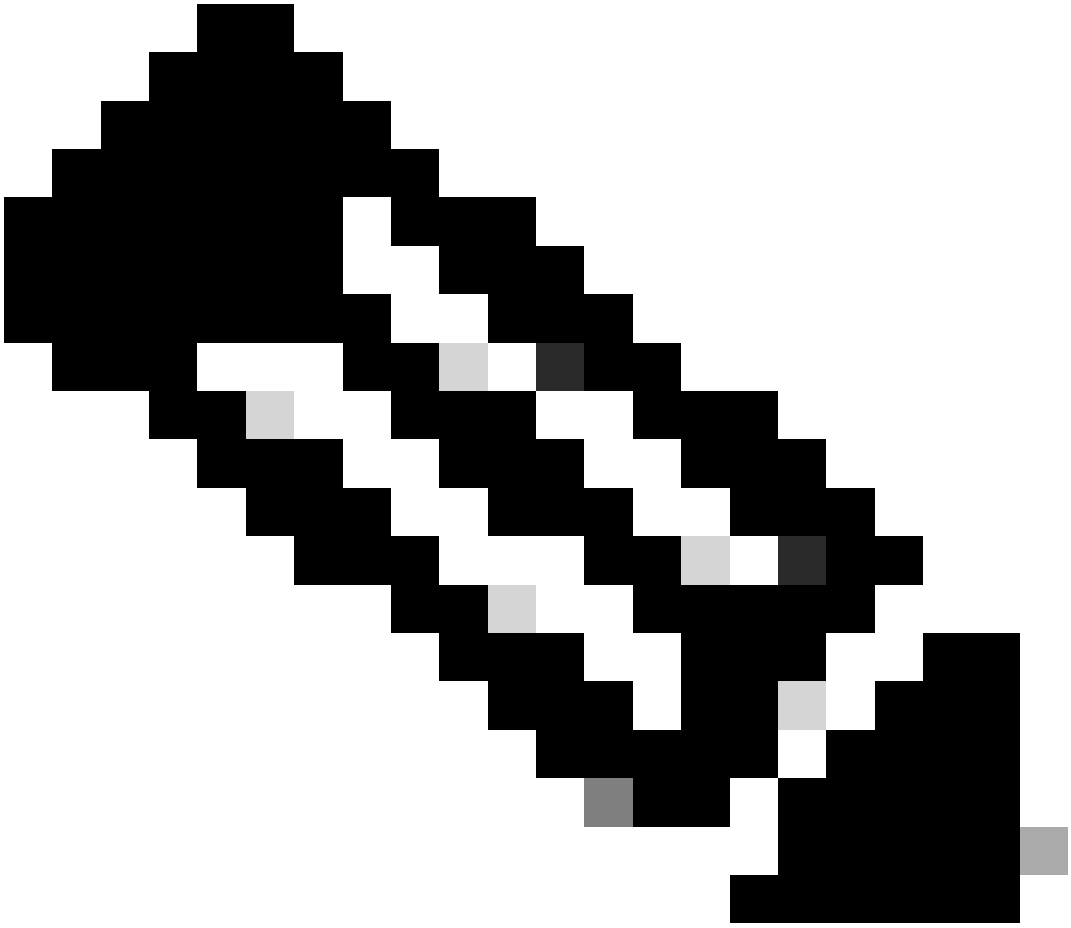
<#root>

bash-4.3$

sudo usermod -s /bin/bash root

Depois que este "sudo su" funciona:

bash-4.3$ sudo su
bash-4.3#



Observação: essa alteração não sobrevive a uma recarga.

- Há um arquivo separadodcos_sshd_config para cada VDC, caso os parâmetros SSH precisem ser modificados em um VDC diferente, certifique-se de modificar o arquivodcos_sshd_config correspondente.

<#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

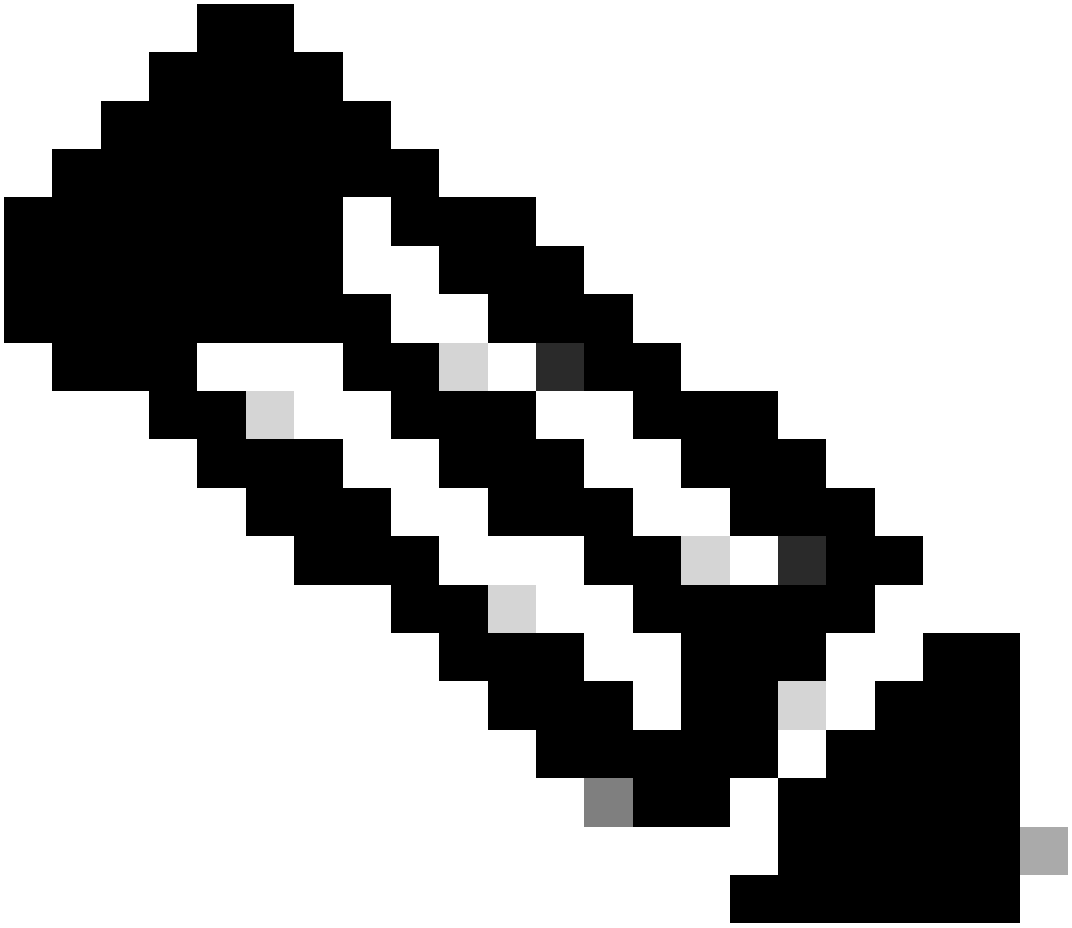
- As alterações no arquivodcos_sshd_config não são persistentes nas reinicializações em qualquer plataforma Nexus. Se as alterações precisarem ser persistentes, um EEM poderá ser usado para modificar o arquivo toda vez que o switch for inicializado. O aprimoramento no N9K altera essa versão a partir de 10.4. Consulte o bug da Cisco ID CSCwd82985 para obter detalhes.

N7K, N9K, N3K

Existem Ciphers, MACs e KexAlgorithm adicionais que podem ser adicionados se necessário:

```
<#root>

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



Observação: esses comandos estão disponíveis no Nexus 7000 com versões 8.3(1) e posteriores. Para a plataforma Nexus 3000/9000, o comando fica disponível com a versão 7.0(3)I7(8) e posterior. (Todas as versões 9.3(x) também têm esse comando. Consulte o Guia de configuração de segurança do Cisco Nexus 9000 Series NX-OS, versão 9.3(x))

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.