centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1447

Procedimiento de empleo seguro
Cisco Nexus NX-OS 9

Agosto de 2023

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
Pº de la Castellana 109, 28046 Madrid
Centro Criptológico Nacional, 2023

NIPO: 083-23-154-6
Fecha de Edición: agosto de 2023

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.09.04 13:26:55 +02'00'

ÍNDICE

1. INTRODUCCIÓN

1. El objetivo de este documento es proporcionar una guía o procedimiento de configuración y empleo seguro de la familia de conmutadores **Cisco Nexus 9000** (en adelante NX-9K Series) y Cisco Nexus 3000 (en adelante NX-3K) ejecutando la versión de sistema operativo **NX-OS Release 9.X**. Los equipos de la familia Nexus se suelen utilizar dentro de los centros de datos (CPDs) por sus especiales características:
    - Baja latencia.
    - Alta densidad de puertos de alta velocidad.
    - Operación en modo agrupado mediante funcionalidades de apilamiento virtual VPC (Virtual PortChannel).
2. La estructura del documento y sus contenidos no exigen una lectura lineal del mismo. Se recomienda al lector utilizar el índice de contenidos para localizar el capítulo que trate el aspecto concreto sobre el que se desee obtener información**.**
3. Las principales características del hardware de los conmutadores de la familia Nexus 9K/3K sobre las que el lector debe familiarizarse se resumen a continuación:
    - Procesador central que soporta todas las operaciones del sistema, tanto el plano de control (operaciones internas) como el plano de datos (transmisión de la información).
    - Memoria dinámica, empleada por el procesador central para todas las operaciones del sistema.
    - Memoria flash (EEPROM), empleada para almacenar la imagen del sistema operativo Cisco NX-OS. Los equipos de la familia Nexus sólo pueden operar con este tipo de sistema operativo.
    - Puerto USB 2.0 Tipo A para procesos de actualización y copia, con soporte de unidades flash USB con un máximo de consumo de 2.5W (0.5A).
    - Memoria no volátil de solo lectura (ROM). Se emplea para almacenar el programa Bootstrap y programas de diagnóstico de encendido.
    - Memoria no volátil de acceso aleatorio (NVRAM) que se emplea para almacenar los parámetros de configuración del conmutador, utilizados para inicializar el sistema en el arranque.
    - Puerto de gestión dedicado mediante interfaz serial RJ45 para operación por consola, ubicado en el panel posterior del conmutador.
    - Puerto de gestión Ethernet dedicado en el panel posterior del conmutador. Este puerto se encuentra en una tabla de rutas separada (instancia VRF) identificada como “Mgmt-vrf” en la configuración. De este modo, es posible disponer de una tabla de enrutamiento separada de la que utilizan los puertos de servicio, y aislar de ese modo el tráfico de gestión de tráfico de servicio.

- Interfaces de red físicas de varios tipos, ya sean basados en cobre (estándar BaseT) o fibra (estándares SFP/SFP+/QSFP+). Algunos modelos tienen un número y/o tipo de interfaces fijos; otros tienen slots para añadir interfaces de red adicionales.
- Aunque los conmutadores Nexus 9K/3K Series presenta diferentes opciones de configuración, los algoritmos criptográficos utilizados en esta guía cumplen con los requisitos estipulados en la *CCN-STIC-807 Criptología de empleo en el ENS* para la Categoría ALTA.

2. OBJETO Y ALCANCE

4. El objetivo de esta guía es establecer una referencia para la configuración segura de los conmutadores o switches de la familia la familia Nexus **9000 y 3100, 3100v, 3100z, 3200, 3400, 3500, 3600 en NXOS Release 9.X**. Incluye consejos y recomendaciones sobre la activación o desactivación de servicios y funcionalidades disponibles en el sistema operativo para mejorar la seguridad de la red.
5. Este documento, salvo menciones especiales, no aporta ajustes de configuración para la operación del producto, fuera de las directamente relacionadas con su operación en modo seguro. Aspectos como las políticas de flujo de información y el control de acceso, deben ser implementadas acorde a las políticas vigentes en la organización.
6. Las autoridades responsables de la aplicación de la política de seguridad de las TIC (STIC) determinarán el análisis y aplicación de este documento a los conmutadores Nexus 9K/3K bajo su responsabilidad.

3. ORGANIZACIÓN DEL DOCUMENTO

7. La estructura que sigue el documento es:

- **Apartado 4.** En este apartado se recogen recomendaciones a tener en cuenta durante la fase de despliegue e instalación física del producto.
- **Apartados 5**, **6**, **7**, **8**, **9**, **10**. En estos apartados se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.
- **Apartados 11**, **12**, **13**, **14**. En esto apartados se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.
- **Apartado 15**. Se presenta una *checklist* de alto nivel para desplegar los dispositivos de forma segura.
- **Apartado 16**. Incluye el listado de documentos referenciados a lo largo del documento.
- **Apartado 17.** Incluye el listado de las abreviaturas empleadas a lo largo del documento.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

8. El dispositivo Nexus 9K/3K Series debe ser examinado para comprobar que no ha sido manipulado durante su entrega siguiendo los siguientes pasos:

   - Antes de abrir el paquete donde fue entregado el Nexus 9K/3K Series, se debe comprobar que el paquete contenga la serigrafía y logo de Cisco Systems. Si no es así, se recomienda contactar con el proveedor del equipo (Cisco Systems o un distribuidor autorizado).
   - Es necesario comprobar que el paquete no ha sido abierto y después vuelto a sellar, mediante inspección de la cinta que lo cierra. Si el paquete parece haber sido abierto y después sellado de nuevo, es recomendable contactar con el proveedor del equipo (Cisco Systems o un distribuidor autorizado).
   - Se debe verificar que el paquete contiene la impresión resistente a manipulaciones de Cisco en la cara externa de la caja de cartón. Si no es así, se deberá contactar con el proveedor del equipo (Cisco Systems o un distribuidor autorizado). Esta impresión contiene el número de producto de Cisco, su número de serie e información adicional sobre el contenido de la caja.
   - Es importante chequear el número de serie del Nexus 9K/3K Series especificado en la documentación del pedido. El número de serie que figura en la etiqueta blanca de la caja se debe corresponder con el número de serie del dispositivo. Por tanto, es necesario verificar que este número concuerda con el número de serie en la factura enviada por correo. Si no es así, se debe contactar con el proveedor del equipo (Cisco Systems o un distribuidor autorizado).
   - En la recepción de la unidad, es necesario comprobar que el pedido fue enviado por el proveedor esperado (Cisco Systems o un distribuidor autorizado). Este proceso puede llevarse a cabo verificando el código de envío/paquete junto con la empresa de transporte. También es recomendable comprobar que los números de serie de los productos enviados concuerdan con los números de serie de los productos recibidos. Esta verificación debe ser llevada a cabo por algún mecanismo externo que no pertenezca al proceso de envío. Por ejemplo, teléfono, fax o un servicio online de rastreo de paquetes.
   - Una vez que el paquete ha sido abierto, es recomendable inspeccionar el dispositivo. Aquí es necesario comprobar que el número de serie mostrado en él concuerda con el número de serie que aparece en la documentación del envío y la factura. Si no es así, se debe contactar con el proveedor del equipo (Cisco Systems o un distribuidor autorizado).

9. Tras realizar los procedimientos iniciales de configuración, y antes de poner la unidad en su entorno productivo, es recomendable comprobar que el software de la unidad no ha sido comprometido. Se recomienda revisar el epígrafe 13 sobre actualización/verificación de firmware para tal efecto.

4.2 ENTORNO DE CONFIGURACÓN INICIAL SEGURO

10. El dispositivo Nexus debe instalarse en una ubicación físicamente segura donde solo se permita acceso físico al personal autorizado.

11. Los Nexus requieren los siguientes componentes para disponer de un entorno de configuración inicial seguro:

    - Puesto de gestión con cliente SSH: Este puesto hace referencia a cualquier estación de trabajo con un cliente SSH instalado que se emplea por el administrador de los Nexus 9K Series para su administración a través de los canales protegidos de SSH. Cualquier cliente SSH que soporte SSHv2 puede ser utilizado, con unas propiedades de configuración mínimas que se describen en el apartado **6.3** correspondiente al protocolo SSH. El objetivo es lograr que tanto la longitud de generación de clave como el algoritmo de generación superen el grado R (Recomendado) en la guía CCN-*STIC-807.*
    - Consola local: Esto incluye cualquier entorno de consola que esté directamente conectado a los Nexus por un puerto serie de consola. El administrador usa esta consola para la administración de los Nexus.
    - Servidor NTP: Los Nexus 9K Series soportan comunicaciones con un servidor NTP para sincronizar el tiempo, y dicho valor es uno de los requeridos por el asistente inicial de configuración, aunque pueden ser configurados/modificados posteriormente mediante línea de comandos (CLI).

4.3 ENTREGA SEGURA DEL *SOFTWARE*

12. El producto se entrega con un *software* instalado. No obstante, puede que no sea la versión del software recomendada, en cuyo caso el producto deberá actualizarse para emplear las versiones de software indicadas en el apartado **2 OBJETO Y ALCANCE**.

13. El software está disponible en el Software Center de Cisco:

    https://software.cisco.com/download/home

14. En la pantalla de descarga del software, se puede consultar el hash SHA512 del fichero a descargar. Se deberá realizar el hash del fichero descargado y verificar que coincide con el indicado en la página de descarga.

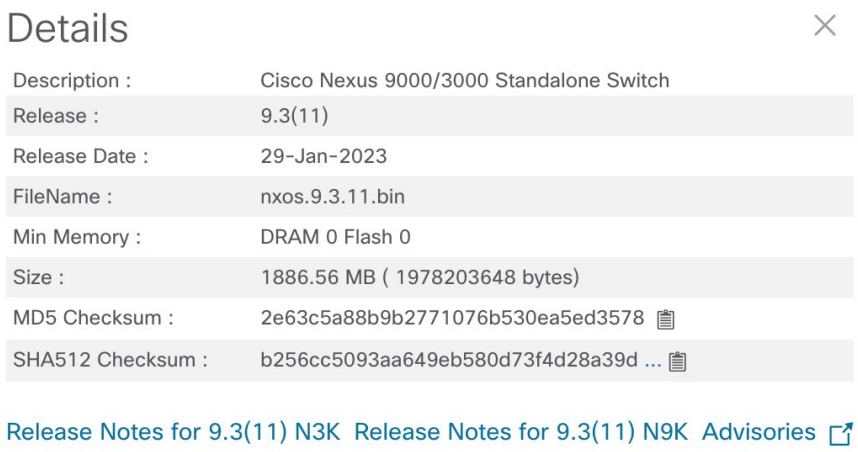

Ilustración 1: Verificación Hash descargas desde la página oficial de Cisco

NOTA: a pesar de que el SHA512 proporciona una funcionalidad criptográficamente más segura que el MD5, este último también se puede utilizar como el hash a comprobar. Como diferencia, la salida del checksum SHA512 (512 bits) está representada por 128 caracteres en formato hexadecimal, mientras que MD5 produce un valor hash de 128 bits (16 bytes), normalmente expresado como un número hexadecimal de 32 dígitos.

4.4 DATOS INICIALES DE CONFIGURACIÓN

15. El propósito del documento no es ofrecer una guía de configuración completa del equipo, si no ofrecer información sobre la operación segura del equipo en sistemas de información bajo el alcance del ENS. Pero sí que se recomienda, como preparación previa al despliegue de la unidad, tener presente una serie de valores operativos para poder luego facilitar/implementar los procedimientos de operación segura. Entre esos elementos relacionados con la seguridad del equipo, se encuentran:

    - Contraseña de administrador, y de usuarios adicionales. Estos valores pueden ser configurados en el asistente inicial de configuración, o con posterioridad accediendo al equipo mediante conexión serie/SSH. Los valores de la contraseña deberán cumplir los requisitos expresados en el apartado **5.3.1.3**.
    - Activación de protocolos de gestión remota, tales como SSH.
    - Disponibilidad de servidor de tiempos (NTP).

4.5 PRIMEROS PASOS

4.5.1 INSTALACIÓN FISICA

16. Siga la guía “Cisco Nexus 9000 Hardware Installation Guide” [1]/”Cisco Nexus 3000 Series Hardware Installation Guide” [30] para la preparación del sitio físico y la instalación del hardware.

4.5.2 CONFIGURACIÓN INICIAL CON ASISTENTE Y PUERTO DE CONSOLA

17. Los dispositivos Nexus deben ser configurados inicialmente mediante conexión directa con consola local por un puerto serie antes de ser conectado a ninguna red.
18. En una unidad Nexus sin configuración previa, es decir, sin ningún fichero de configuración en NVRAM, se inicia un asistente de configuración inicial. Una vez cargado el asistente, presenta un diálogo de configuración donde se van presentando las opciones de configuración más importantes para la operación inicial del dispositivo. Este asistente guía al administrador a través de la configuración inicial preguntándole información básica acerca del dispositivo y de la red, creando finalmente un fichero de configuración que permite a la máquina disponer de una configuración mínima funcional de arranque. Después de que el fichero está creado, un administrador privilegiado puede utilizar la CLI para añadir configuración adicional.
19. A continuación, se describe el proceso de configuración inicial usando el asistente de configuración. La sección "Using the Cisco NX-OS Setup Utility" [2] describe cómo usar el configurador para construir una configuración básica y también como modificarla.

```
Waiting for system online status before starting POAP …
Waiting for system online status before starting POAP …
Waiting for system online status before starting POAP …
Starting Auto Provisioning …
Done
Abort Auto Provisioning and continue with normal setup? (yes/no)[n]: yes
      ---- System Admin Account Setup ----
Do you want to enfoce secure password standard (yes/no) [y]: yes
  Enter the password for "admin": *****
  Confirm the password for "admin": *****
      ---- Basic System Configuration Dialog VDC: 1 ----
       This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
```

Would you like to enter the basic configuration dialog (yes/no): yes

Do you want to enforce secure password standard (yes/no) [y]: yes

Create another login account (yes/no) [n]: yes

Enter the User login Id : operator

Enter the password for "operator":

Confirm the password for "operator":

Enter the user role (network-operator|network-admin|vdc-operator|vdc-admin) [network-operator]:

Configure read-only SNMP community string (yes/no) [n]: n

Configure read-write SNMP community string (yes/no) [n]: n

Enter the switch name : NX01

Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: yes

Mgmt0 IPv4 address : 10.0.0.1

Mgmt0 IPv4 netmask : 255.255.255.0

Configure the default gateway? (yes/no) [y]: n

Configure advanced IP options? (yes/no) [n]: n

Enable the telnet service? (yes/no) [n]: n

Enable the ssh service? (yes/no) [y]: y

Type of ssh key you would like to generate (dsa/rsa) [rsa]:

Number of rsa key bits <1024-2048> [1024]: 1024

Configure the ntp server? (yes/no) [n]: n

Configure default interface layer (L3/L2) [L2]:

Configure default switchport interface state (shut/noshut) [noshut]:

Configure CoPP system profile (strict/moderate/lenient/dense) [strict]:

The following configuration will be applied:

password strength-check

username operator password <user-password> role network-operator

switchname NX01

no feature telnet

ssh key rsa 1024 force

feature ssh

system default switchport

no system default switchport shutdown

copp profile strict

interface mgmt0

```
ip address 10.0.0.1 255.255.255.0
no shutdown
Would you like to edit the configuration? (yes/no) [n]: n
Use this configuration and save it? (yes/no) [y]: y
[################] 100%
Copy complete
```

20. Una vez finalizado el proceso, se deben tener en cuenta las siguientes consideraciones:
    - La cuenta creada durante la instalación inicial es considerada como **administrador privilegiado** (*role network-admin*) y, por lo tanto, tiene concedido el acceso a todos los comandos del producto.
    - Los niveles de privilegio no son necesariamente jerárquicos puesto que son configurables. Estos niveles de privilegio describen las tareas que pueden ser realizadas por los usuarios. Para más información sobre los roles posibles de usuario, ver apartado **5.3.1.2**.
    - El número de administradores que se creen y sus consiguientes niveles de acceso deben basarse en la política de la organización. No obstante, se recomienda **atender** a los principios del mínimo privilegio.
    - El término **administrador privilegiado** se utiliza en este documento para referirse a cualquier administrador autenticado satisfactoriamente y que tiene acceso a los privilegios apropiados para realizar las tareas requeridas.
21. Consulte las referencias "NX-OS Command Reference Guide" [3] para saber más acerca de los comandos disponibles, roles asociados y niveles de privilegio.
22. Finalmente, se debe confirmar que una vez que el dispositivo ha arrancado, la versión ejecutada es la correcta. El procedimiento recomendado es actualizar el equipo a la versión recomendada según el fabricante, y usar la validación de checksum de la imagen en un equipo considerado como seguro. Para comprobar la versión que viene con el dispositivo, se puede utilizar el comando "**show version**" [6][37].

```
NX01# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2022, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source.  This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
```

limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
Software
BIOS: version 05.45
NXOS: version 9.3(9)
BIOS compile time: 07/05/2021
NXOS image file is: bootflash:///nxos.9.3.9.bin
NXOS compile time: 2/4/2022 7:00:00 [02/04/2022 08:54:27]
Hardware
cisco Nexus9000 C9348GC-FXP Chassis
Intel(R) Xeon(R) CPU D-1526 @ 1.80GHz with 24570108 kB of memory.
Processor Board ID FDO25450T4Y
Device name: NX01
bootflash: 115805708 kB
Kernel uptime is 0 day(s), 1 hour(s), 19 minute(s), 22 second(s)
Last reset at 461463 usecs after Mon Jun 6 06:07:11 2022
Reason: Module PowerCycled
System version:
Service: HW check by card-client
plugin
Core Plugin, Ethernet Plugin
Active Package(s):

23. Para asegurar que el software instalado no ha sido modificado de manera alguna es necesario comprobar que el valor hash publicado en el sitio oficial de Cisco (http://www.cisco.com/cisco/web/download/index.html) coincide con el firmware descargado.

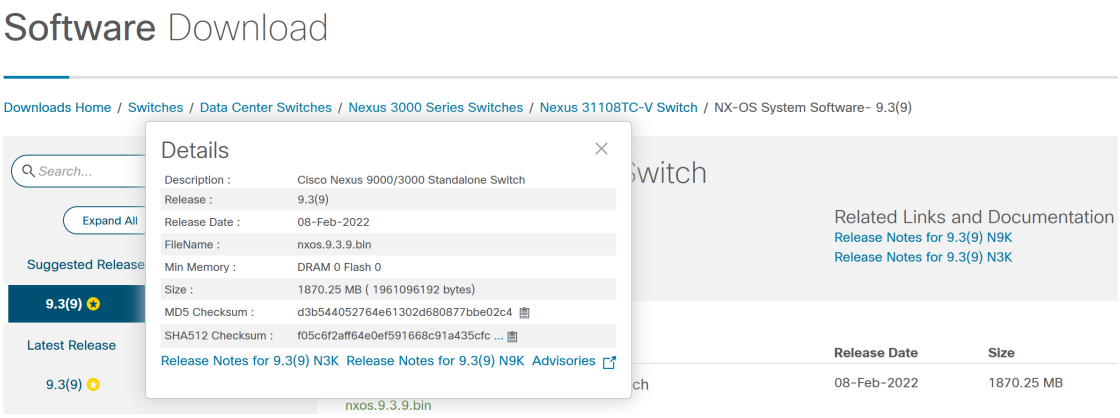

Ilustración 2. Hash SHA512 de la versión recomendada por Cisco para Nexus 9000/200 v9.3.(9)

24. Puede utilizarse alguna utilidad de comprobación de hash (como *certutil*, en equipos Windows) para obtener el hash y comprobar que coincide con el indicado en la Ilustración 2. Estos valores deberán ser comprobados visualmente, o copiados en un Bloc de Notas para su correcta comparación.

Ilustración 3. Cálculo del hash SHA512 de la versión recomendada por Cisco para Nexus 9000/200 v9.3.(9)

5. CONFIGURACIÓN BÁSICA

5.1 MODOS DE OPERACIÓN

25. Un dispositivo Nexus 9K/3K Series tiene varios modos de operación, los cuales están detallados en esta sección:

- Modo de operación Cargador de Arranque (*Boot Loader*): En el arranque, el switch descarta todo el tráfico de red hasta que su software principal y su configuración han sido cargadas.

  Este modo de operación es el encargado de proveer varios servicios destinados a corregir una carga errónea del sistema operativo principal (por estar ausente o corrupta), y progresa automáticamente hacia el modo de operación Normal, donde el software principal y su configuración entran en funcionamiento.

  Durante el arranque, un usuario podría presionar una combinación de teclas (Ctrl+C) la tecla de interrupción en una conexión de consola en los primeros 60 segundos del encendido para entrar en el modo de operación de *boot loader*. Adicionalmente, si el conmutador no encuentra una imagen del sistema operativo válida entrará en el modo *boot loader* en lugar del modo Normal protegiendo el conmutador de un arranque en un estado inseguro.

  En este modo, la BIOS realiza una serie de comprobaciones básicas (POST, memoria, y otras aplicaciones del sistema operativo). En caso de que se haya entrado en este modo, el *prompt* de la línea de comandos cambia, y los comandos disponibles son los indicados en la Ilustración 4.

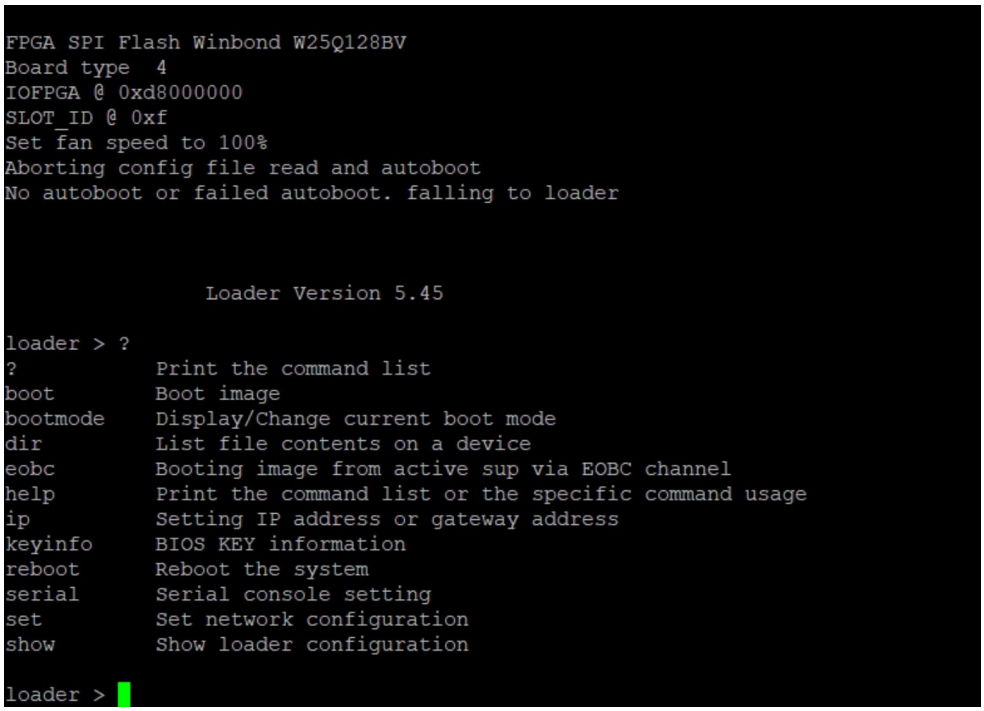

Ilustración 4. Arranque en modo Boot Loader y comandos disponibles

Tras la modificación de los parámetros de arranque (para cargar una nueva imagen en lugar de una corrupta o ausente, por ejemplo), el cargador de arranque (*boot loader*) procede a descomprimir y cargar en RAM el sistema operativo principal.

El tipo de arranque y la ubicación de la imagen pueden cambiarse mediante el comando "**boot**" dentro del modo de *Boot Loader*, por si existe algún problema con la imagen almacenada en el equipo:

#boot nxos bootflash:<image filename> loader > help boot

boot: boot image

usage: boot <image>

image : <tftp_file> | <device_file>

tftp_file : tftp://<server_ip>/<filename>

server_ip : tftp server IP address

filename : file on tftp server

device_file : [<device>:][<partition>:]<path>

device : bootflash: | usb1:| usb2:

partition : Partition number

path : File name on device

Description: Boot the specified image.

```
loader > help bootmode
bootmode: bootmode    Display/Change current boot mode
  usage: bootmode {-g | -p | -p2g | -g2p}
 no-option:   Display current bootmode
      -g:   Set next boot to GRUB
      -p:   Set next boot to PXE
    -p2g:   Set next boot to PXE followed by GRUB
    -g2p:   Set next boot to GRUB followed by PXE
Description: Display current bootmode or change bootmode to Grub
          or Pxe or Pxe2Grub or Grub2Pxe
```

Tras la elección del modo de arranque correcto, se realizan ciertas comprobaciones de seguridad de la imagen, y el sistema pasa a modo de operación normal. Para más información sobre los procesos de autovalidación criptográfica, ver "Auto-chequeos y Modo FIPS" en el apartado **14**.

```
 Power Debug Register2  : 0xf09002f
 Reset Cause Register   : 0x5
 Boot Ctrl Register     : 0xe0ff
 FPGA Update Status     : 0x20

Board Type: Pipedream

Detected CISCO MIFPGA
MIFPGA Subsystem Vendor ID 0x1172
 MIFPGA Version         : 0x10
 MIFPGA Date            : 0x20190118
 MIFPGA Update Status   : 0x20
 MIFPGA ID              : 0x11425577

Bootable Disk is detected. Device Name: INTEL SSDSCKKB240G8K
Version 2.18.1260. Copyright (C) 2021 American Megatrends, Inc.

FPGA SPI Flash Winbond W25Q128BV
Board type  4
IOFPGA @ 0xd8000000
SLOT_ID @ 0xf
Set fan speed to 100%
Standalone chassis
check_bootmode: grub: Continue grub
Trying to read config file /boot/grub/menu.lst.local from (hd0,4)
 Filesystem type is ext2fs, partition type 0x83


Security Lock
Booting bootflash:/nxos.9.3.9.bin
Trying diskboot
 Filesystem type is ext2fs, partition type 0x83
Image valid
```

Ilustración 5. Continuación del proceso de arranque, y procesos de autovalidación de imagen en la carga del NXOS

- Modo de operación Normal: La imagen de NX-OS del conmutador y su configuración han sido cargadas y el conmutador está operando tal y como se ha configurado. Todos los niveles de acceso administrativo están disponibles en este modo y todas las funciones de seguridad están operativas. Para

asegurarse de que la imagen correcta es lanzada en el arranque se emplea el comando "**boot nxos**":

```
#boot nxos bootflash:<image filename>
```

El ejemplo de modificación del parámetro de imagen de arranque sería el de la siguiente ilustración.

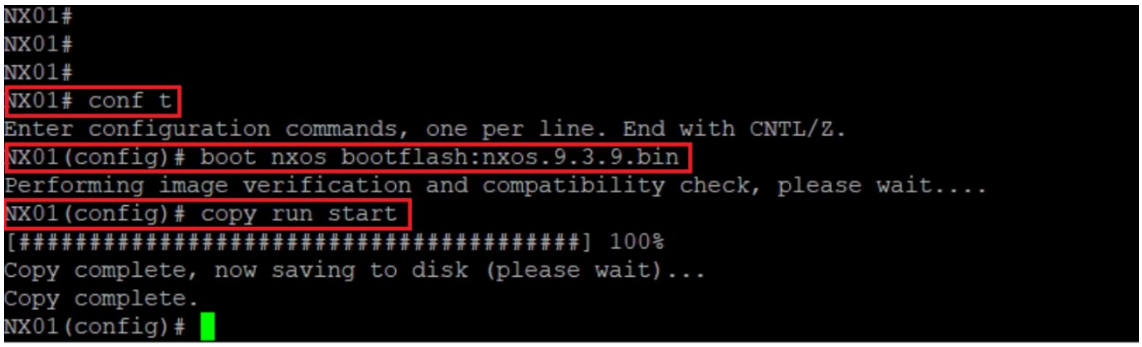

Ilustración 6. Modificación de la configuración para arranque de un firmware concreto

5.2 CONFIGURACIÓN MEDIANTE LÍNEA DE COMANDOS (CLI)

26. Los equipos Nexus son configurables mediante línea comandos (CLI, Command Line Interface), mediante protocolos SNMP, o a través de un interfaz REST-API, lo que permite que los equipos sean configurados de manera gráfica mediante herramientas propias del fabricante. Esta guía se centra en la configuración mediante el interfaz por línea de comandos, dado que no requiere de equipamiento o software externo, y permite configurar todos los aspectos de seguridad importantes del dispositivo.

27. La línea de comandos puede ser accesible por dos modos: bien en modo local, a través del puerto de consola, o bien en remoto mediante protocolos de gestión remota seguros, tales como SSHv2.

28. En el interfaz de configuración mediante comandos en un conmutador Cisco Nexus, existen diferentes contextos de gestión, donde cada contexto se identifica al gestor mediante un símbolo de sistema (*prompt*) específico, que permite en todo momento conocer en qué contexto se está actuando. La importancia de esta información radica en que ciertas acciones sólo son posibles en determinados contextos.

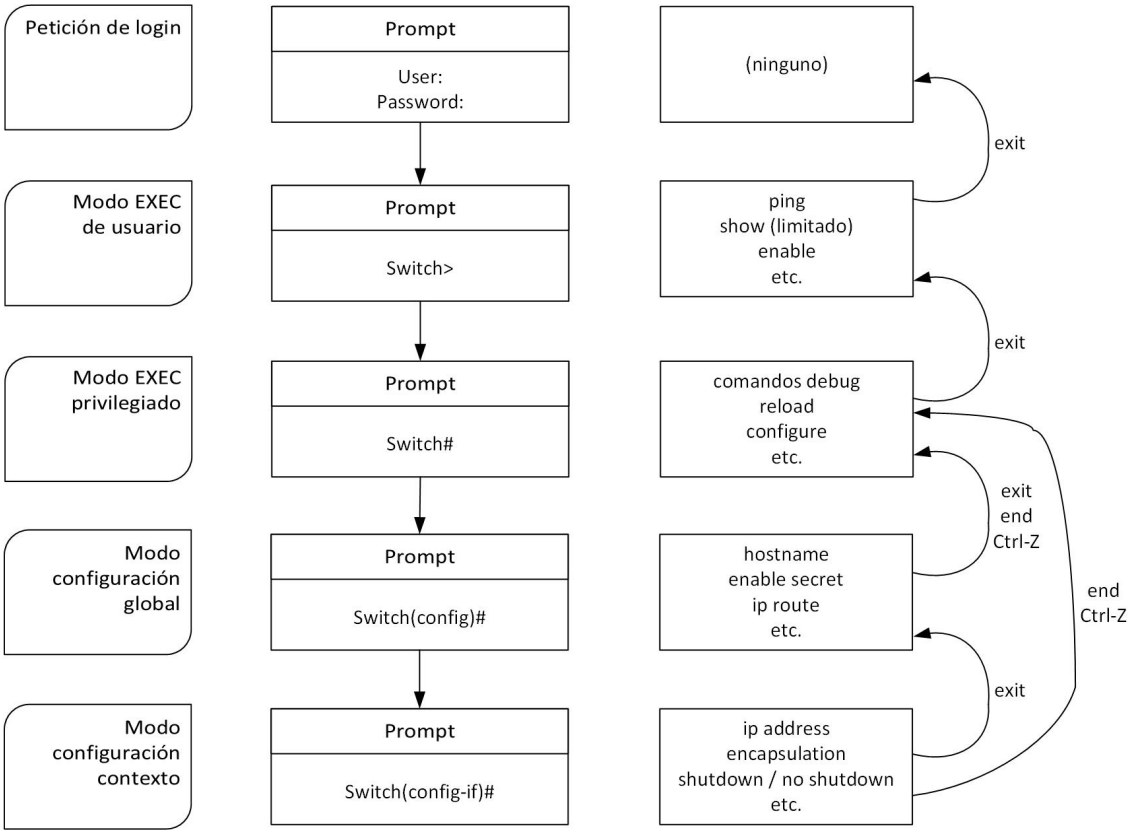

Ilustración 7. Jerarquía de utilización de los diferentes prompt de sistema y modo asociado de funcionamiento

5.3 GESTIÓN LOCAL DE USUARIOS Y SESIONES

29. En los conmutadores Nexus la autenticación de usuarios puede ser local o remota. En el primer caso, los usuarios y sus credenciales de acceso se definen localmente en cada conmutador; en el segundo, la autenticación se realiza en servidores de autenticación externos de tipo RADIUS o TACACS. Aunque, desde el punto de vista de la seguridad es mejor autenticación externa, se comenzará con la autenticación y gestión local de usuarios, porque es el punto inicial de toda configuración, y en muchas organizaciones no se dispone de dichos servidores de autenticación remotos.

30. Desde el punto de vista de la seguridad, es más conveniente la autenticación remota de los usuarios, dado que se pueden gestionar de manera centralizada, y es más fácil la protección de los usuarios al residir todos en un mismo repositorio. La configuración de la autenticación remota de usuarios se aborda en el apartado **10.1**.

31. Por defecto, y con el objeto de facilitar su puesta en marcha inicial, la configuración de fábrica de los conmutadores no incluye ninguna autenticación activa: cualquier persona con acceso físico a la consola puede acceder a la autenticación local del sistema.

5.3.1 CONFIGURACIÓN LOCAL DE USUARIOS

32. Los dispositivos Nexus requieren ser configurados para utilizar un nombre de usuario y contraseña por cada usuario del sistema, que, a su vez, tiene un tipo de rol asociado. Al contrario que en los sistemas Cisco IOS, los privilegios de los usuarios están restringidos por estos roles de usuario, no por los habituales niveles de privilegio 1-15. Las contraseñas se almacenan cifradas en el dispositivo, aunque se introduzcan en claro, y el rol del usuario es obligatorio especificarlo, con el fin de evitar posibles problemas de acceso si se omiten.
33. A continuación, se ofrece más información relacionada tanto con el almacenamiento y cifrado de las contraseñas, como con los roles de usuario.

5.3.1.1 ALMACENAMIENTO Y GESTIÓN DE CONTRASEÑAS DE USUARIOS LOCALES

34. Las contraseñas de los usuarios locales se pueden crear o bien usando texto plano, o bien usando un cifrado ya específico. En caso de usar un texto plano como contraseña, el NXOS la cifrará antes de guardarlas en el archivo de configuración del dispositivo. Concretamente, se almacenan usando un algoritmo DES, no recomendado por su vulnerabilidad. El uso de cifrado en el almacenamiento de la contraseña de usuario se indica con un "password 5" en el fichero de configuración cuando se revisa la configuración del usuario.

```
NX01(config)# username ingenia password 0 Test2022

WARNING: DES is a weak encryption algorithm and currently the default. This will be deprecated and AES128 will be made default in an upcoming release.

NX01(config)# username ingenia password 5 5$MPOOFI$C1V6xyZ2NnmIPGkY6pNxGP4NDIghb4DqjCWxr7XcP68 role network-operator
```

35. Por tanto, para almacenar las contraseñas en un formato seguro, se recomienda habilitar la función de guardado de contraseñas usando el algoritmo AES de cifrado. De ese modo, las contraseñas se almacenan cifradas mediante AES256 utilizando el siguiente comando "**feature password encryption aes".** A continuación, se deberá usar el comando "**encryption re-encrypt obfuscated**" para convertir las contraseñas al nuevo cifrado. Se puede comprobar si el sistema usa el sistema nuevo de cifrado para el almacenamiento de las contraseñas mediante el comando "**show encryption service stat**".

```
NX01(config)# feature password encryption aes

Warning: There is no master-key in the system.

Password encryption will not take place unless a master-key is configured.

Please create a master-key using command 'key config-key ...'.

NX01(config)# key config-key ascii

New Master Key:*********

Retype Master Key: *********
```

NX01(config)# encryption re-encrypt obfuscated

Encryption service is disabled. Please enable it first using 'feature password encryption aes'.

NX01(config)# show encryption service stat

Encryption service disabled

Master Encryption Key configured

Type-6 encryption is not being used

NX01(config)# feature password encryption aes

NX01(config)# show encryption service stat

Encryption service enabled

Master Encryption Key configured

Type-6 encryption is being used

NX01(config)# encryption re-encrypt obfuscated

NX01(config)#

```
username admin password 5 $5$ECJPCH$NuF8RuMrYh7WYft5WgKtGtVIKUcButAJsbBx.XW8FF6
 role network-admin
username ingenia password 5 $5$MPOOFI$ClV6xyZ2NnmIPGkY6pNxGP4NDIghb4DqjCWxr7XcP6
8  role network-operator
username ingenia passphrase  lifetime 99999 warntime 14 gracetime 3
```

Ilustración 8. Ejemplo de creación de usuario local

5.3.1.2 ROLES DE USUARIO

36. En lugar de usar un sistema de niveles de privilegio clásico de los conmutadores Cisco IOS, con niveles 1-15 de privilegio, en el sistema operativo NXOS se usa un sistema basado en roles (RBAC, Role Based Access Control), donde cada rol tiene una serie de privilegios asociados. El sistema cuenta con una serie de privilegios predefinidos, pero se pueden crear roles a medida.

37. Los dispositivos Nexus consideran los siguientes roles de usuario predefinidos:

    - Rol de desarrollador: El rol de desarrollador “dev-ops” está asociado a usuarios que deben tener acceso al entorno Bash del dispositivo, para poder así ejecutar comandos y scripts a nivel del sistema operativo Linux.

      NX01# show role name dev-ops

      Role: dev-ops

      Description: Predefined system role for devops access. This role

      cannot be modified.

      Rule Perm Type Scope Entity

```
-------------------------------------------------------------------
  6      permit  command              conf t ; username *
  5      permit  command              attach module *
  4      permit  command              slot *
  3      permit  command              bcm module *
  2      permit  command              run bash *
  1      permit  command              python *
```

- Rol de administrador/operador de red: (network-admin / network-operator) Son roles de administración y operación del dispositivo, con acceso a todos los elementos configurables del mismo (es por tanto el mayor nivel de privilegio en la unidad). Su configuración sólo está disponible desde el VDC por defecto.

```
NX01# show role name network-admin

Role: network-admin

  Description: Predefined network admin role has access to all commands  on the
switch

-------------------------------------------------------------------
  Rule    Perm    Type       Scope           Entity

-------------------------------------------------------------------
  1       permit  read-write

NX01# show role name network-operator

Role: network-operator

  Description: Predefined network operator role has access to all read  commands on
the switch

-------------------------------------------------------------------
  Rule    Perm    Type       Scope           Entity

-------------------------------------------------------------------
  1       permit  read
```

- Rol de administrador/operador de VDC: (vdc-admin / vdc-operator) Son usuarios con capacidad de realizar operaciones de lectura/escritura o únicamente lectura respectivamente, pero están limitados a una instancia VDC.

```
NX01# show role name vdc-admin

Role: vdc-admin

  Description: Predefined vdc admin role has access to all commands within a VDC
instance

-------------------------------------------------------------------
```

```
  Rule    Perm    Type       Scope           Entity
  ----------------------------------------------------------------------
  1       permit  read-write
NX01# show role name vdc-operator
Role: vdc-operator
  Description: Predefined vdc operator role has access to all read commands within
a VDC instance
  ----------------------------------------------------------------------
  Rule    Perm    Type       Scope           Entity
  ----------------------------------------------------------------------
  1       permit  read
```

- Rol no administrativo: Se otorga a los conmutadores vecinos autenticados para que puedan recibir tablas de enrutado actualizadas. No existen otras funciones y/o tipos de acceso asociados a este rol.

38. Consulte la guía "NX-OS Command Reference Guide" para encontrar los comandos disponibles, roles asociados y niveles de privilegio. [3] [4] [6][37] [10]

5.3.1.3 CONFIGURACIÓN LOCAL DE LA POLÍTICA DE CONTRASEÑAS

39. Las contraseñas de los usuarios locales deben cumplir ciertas propiedades para que sean aceptadas por el sistema, que se describen en los siguientes puntos.
40. Una contraseña puede estar compuesta por cualquier combinación de caracteres incluyendo caracteres de al menos 3 de los siguientes conjuntos: letras en mayúscula, letras en minúscula, números y los siguientes caracteres especiales: "<", ",", ">", ".", ":", ";", "/", "!", "@", "#", "$", "%", "^", "&", "*", "(", y ")" [4].
41. La mínima longitud de la contraseña puede ser establecida por un administrador con los necesarios privilegios mediante el comando "**user passphrase min-length XX max-length XX**", pudiendo establecerse en un valor mínimo recomendado de 15 caracteres. El valor mínimo para el campo "**min-length**" está entre 4 y 127 caracteres, y para el campo "**max-length**" está entre 80 y 127 caracteres [5][36] .

```
NX01(config)# userpassphrase min-length 15 max-length 80
NX01(config)# show userpassphrase length
Minimum passphrase length : 15
Maximum passphrase length : 80
```

42. Se recomienda que las contraseñas cumplan las siguientes restricciones:
    - La contraseña no puede contener más de tres caracteres consecutivos, tal como *abcd*.
    - La contraseña no puede contener más de dos caracteres respetitos, tal como *aaabbb*.

- La contraseña no puede contener palabras de diccionario ni nombres propios.
- La contraseña no puede coincidir con el nombre de usuario asociado.
- La contraseña obtenida por la capitalización (mezcla de mayúsculas y/o minúsculas de cualquier tipo) del nombre de usuario o el mismo nombre de usuario al revés no será aceptada.
- La contraseña no podrá ser “cisco”, “ocsic” o ninguna capitalización de las mismas. Tampoco es válido sustituir “1” por “|”, “i” por “!”, “o” por “0” o sustituir “s” por “$”.
- La contraseña no podrá comenzar por comillas simples (‘) o dobles (“), barra vertical (|), o cierre angular (>).

43. El dispositivo puede forzar el uso de contraseñas seguras usando el comando **“password strength-check”.** Este comando no comprueba ni modifica claves existentes que no sean seguras. Por tanto, para garantizar que las claves creadas para los usuarios locales son seguras, primero es necesario definir los valores de contraseña segura, sus longitudes, y luego usar el mencionado comando. A partir de su invocación, no se podrán crear contraseñas que no cumplan los criterios de fortaleza y longitud establecidos.

```
NX01(config)# show userpassphrase length
Minimum passphrase length : 15
Maximum passphrase length : 80
NX01(config)# password strength-check
NX01(config)# show password strength-check
Password strength check is enabled
NX01(config)# username test password 0 cccisco
Wrong Password, Reason: Length should be at least 15 characters
NX01(config)# username test password 0 cccisco0
Wrong Password, Reason: Password shouldn't contain characters, repeated three or more times consecutively.
```

5.3.2 CONFIGURACIÓN DE PARÁMETROS DE LA SESIÓN LOCAL

44. Se recomienda configurar las cuentas de usuario para que muestren un mensaje al usuario después de un número máximo de intentos fallidos de autenticación mediante SSH [6][37]. El comando para conseguir tal efecto es el siguiente:

    NX01(config)# ssh login-attempts <x>, siendo “<x>” el número de intentos requeridos antes del mensaje de aviso.

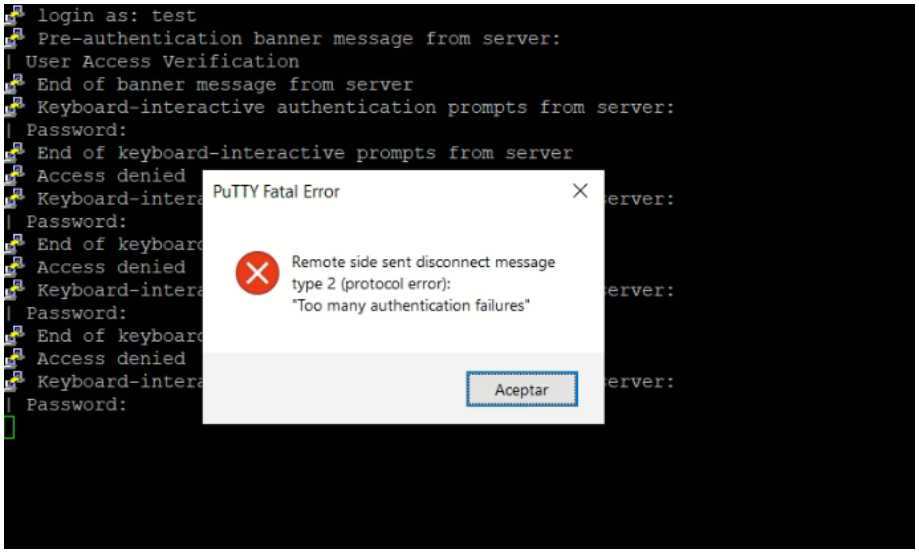

Ilustración 9. Ejemplo de creación de usuario local

45. Tras el mensaje de aviso, la sesión SSH se cierra, y es necesario abrir una nueva sesión. El usuario no es bloqueado en ningún momento, simplemente debe abrir una nueva sesión SSH para su autenticación local.

5.3.3 CONFIGURACIÓN DEL MENSAJE DE AVISO EN EL INICIO DE SESIÓN

46. Se recomienda configurar un mensaje de aviso / banner que se muestra en la interfaz de administración CLI antes de permitir cualquier acceso administrativo al dispositivo. Esta funcionalidad se provee a través del comando **"banner motd"** [7] [38].
47. Por ejemplo, para crear un banner de texto que contenga "Esto es un banner" utilice el comando:

```
Switch(config)# banner motd d Esto es un banner d
```

48. Los comandos disponibles para la configuración de banner se muestran a continuación:

```
NX01(config)# banner ?
exec  Configure banner exec message
motd  Configure banner motd message

NX01(config)# banner {exec | motd} ?
LINE  Delimiter char (first char is delimiter char) followed by message
    ending with delimiter
```

49. Toda la información relacionada con la configuración del banner puede encontrarse en “Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide: Configuring the MOTD Banner” [7] y “Cisco Nexus 3000 Series NX-OS Fundamentals Configuration Guide: Configuring the MOTD Banner” [38].

5.3.4 FINALIZACIÓN DE LA SESIÓN

50. Se recomienda configurar un tiempo máximo de inactividad de una sesión. Después de que pase el tiempo configurado, la sesión finaliza volviendo a un estado anterior al login. No se permite realizar ninguna otra actividad hasta que el administrador vuelva a autenticarse.
51. El comando “**exec-timeout”** se utiliza para configurar el tiempo de inactividad de sesión:

    (config)# line console

    (config-line)# exec-timeout <0-525600>
52. El tiempo está expresado en minutos, siendo 0 el parámetro que deshabilita el tiempo de inactividad. Utilice el prefijo **no** (**no exec-timeout**) para eliminar el tiempo previamente configurado.
53. Para que la configuración realizada tenga efecto, la sesión de consola actual debe ser cerrada. Cuando el usuario inicie sesión otra vez se le aplicará el nuevo timeout configurado.
54. Un administrador también puede cerrar la sesión manualmente mediante el comando: **logout.**

5.4 GUARDADO DE CONFIGURACIÓN EN DISCO

55. NX-OS utiliza una configuración en ejecución y una configuración inicial. Los cambios en la configuración afectan a la configuración en ejecución. Para guardar la configuración en ejecución (que se encuentra en memoria) se debe volcar a la configuración inicial. Consultar la sección “Cisco Nexus 9000 Fundamentals Configuration Guide:Using the Device File Systems, Directories, and Files” [8], i o en “Cisco Nexus 3000 Series NX-OS Fundamentals Configuration Guide:Using the Device File Systems, Directories, and Files”[53] .
56. De forma alternativa, para guardar los cambios de la configuración inicial, se puede utilizar el comando “**copy running-config startup-config**” (más detalles en Cisco Nexus 9000 Fundamentals Configuration Guide: Working with Configuration Files [9] y Cisco Nexus 3000 Fundamentals Configuration Guide: Working with Configuration Files [39]. Estos comandos deben ser usados frecuentemente cuando se realicen cambios en la configuración del dispositivo. Si el producto se reinicia

cuando se han realizado cambios sin guardar, estos se perderán y se utilizará la última configuración guardada. Para comprobar la configuración actual es posible usar el comando "**show running-config**".

6. CONFIGURACIÓN Y PROTECCIÓN DE LOS SERVICIOS DE RED OFRECIDOS POR EL EQUIPO

6.1 ENTORNO DE CONFIGURACIÓN Y OPERACIÓN REMOTA SEGURO

57. Una vez configurado de manera local, el equipo deberá contar con un entorno de operación y configuración remota seguro, donde se contemplen los siguientes aspectos, principalmente relacionados con las funciones criptográficas y protocolos de comunicación con los que va a operar el equipo:

    - Se recomienda utilizar SSHv2 en lugar de SSHv1 con la longitud mínima de clave para RSA descrita en este documento.
    - Se recomienda que la gestión remota de usuarios se realice mediante servidores de AAA centralizados, para poder gestionarlos de manera más eficiente, y para poder mejorar su seguridad al estar en un único repositorio. Por tanto, en el apartado 10.1 de la presente guía, se aborda el proceso de autenticación remota con servidores de AAA.
    - Se recomienda el uso de IPSec para dotar de cifrado y autenticación a las conexiones con dichos servidores de AAA. Dado que el equipo NXOS no soporta terminación de túneles IPSec, se recomienda realizar dicha terminación de túnel mediante equipos adicionales.
    - También se recomienda IPSec para cifrar y proteger las comunicaciones con otros servidores críticos necesarios para la operación del dispositivo, tales como el syslog o la conexión con los servidores de tiempos NTP. Para la conexión de syslog, es posible usar una capa TLS de seguridad adicional, de modo que el propio Nexus haga de iniciador de túnel TLS hacia el servidor de syslog. Para el tema del servidor de tiempos NTP es posible usar autenticación MD5 para autenticar el servidor, pero se recomienda usar la conexión a través de un enlace criptográfico seguro (mediante un tercer equipo y cifrado IPSec).

6.2 PROTOCOLO SEGURO DE CONEXIÓN DE NIVEL 2 EN NEXUS 9000 SERIES: MACSEC Y MKA

58. El producto autentica y cifra paquetes a nivel 2 entre puertos Ethernet, estableciendo un túnel seguro entre el propio conmutador y un equipo destino con funcionalidades MACsec debidamente autorizado y configurado. El protocolo MACsec Key Agreement (MKA) proporciona las claves de sesión y gestiona las claves de cifrado requeridas para proteger los datos intercambiados entre los pares, dentro de interfaces Ethernet.

59. Se recomienda el uso de MACSec principalmente en escenarios *switch-to-switch*, y usar EAPOL (802.1X) para enlaces entre equipos finales y los propios conmutadores. Los pares MACSec en la plataforma Cisco Nexus deben ser otros equipos Nexus con la misma versión de firmware si se desea usar AES_128_CMAC como suite de

cifrado. Para interoperabilidad con otras versiones diferentes (ya sean previas o posteriores) se debe usar la suite AES-_256_CMAC.

60. Los equipos Cisco Nexus sólo soportan el protocolo MKA (*MACsec Key Agreement*) para el intercambio de claves.

61. El primer paso es la definición de una política de MACSec, donde se incluya la clave preacordada (que deben compartir ambas unidades), la suite de cifrado, y la validez de dicha clave:

```
NX01(config)# key chain 1 macsec
NX01(config-macseckeychain)# key 1000
NX01(config-macseckeychain-macseckey)#key-octet-string
abcdef0123456789abcdef01
23456789abcdef0123456789abcdef0123456789 cryptographic-algorithm
AES_256_CMAC
NX01(config-macseckeychain-macseckey)# send-lifetime 00:00:00 Jun 30 2022
duration 100000
NX01(config-macseckeychain-macseckey)# sho key chain 1
Key-Chain 1 Macsec
 Key 1000 -- text 6
"JDYk8pxoWRFU0oVhaw04sMUTxSTJZ26Lmfnh7NQSXnfqtWTC9C0QNj2qXv
sHDBiEzOxy+6MDr+ASptOR2F6PsUfFpaLGtSCKyulzsPDoCce4loN/JG+YZA5g2xuLaU8
K0y0UY/fefZ
KkAA=="
   cryptographic-algorithm AES_256_CMAC
   send lifetime UTC (00:00:00 Jun 30 2022)-(duration 100000) [active]
```

62. Con esta definición, ya es posible aplicar MACsec a un puerto que permita el uso de dicho protocolo (no todos los puertos en todas las unidades Cisco Nexus lo permiten, se recomienda consultar los datasheet correspondientes para determinar los puertos y controladoras habilitados para MACsec).

```
NX01(config)# interface ethernet 1/52
NX01(config-if)# ma
mac         mac-address   macsec
NX01(config-if)# macsec keychain 1
NX01(config-if)# exit
NX01(config)#
NX01(config)#
NX01(config)# show running-config macsec
!Command: show running-config macsec
!Running configuration last done at: Thu Jun 30 12:36:22 2022
```

```
!Time: Thu Jun 30 12:36:45 2022
version 9.3(9) Bios:version 05.45
feature macsec
interface Ethernet1/52
  macsec keychain 1 policy system-default-macsec-policy
```

63. A partir de ese momento, todo el tráfico Ethernet en dicho puerto Eth1/52 estará protegido por MACsec (*unicast*, *multicast* y *broadcast*), y descartará el tráfico que no venga de un par autorizado.

```
NX01# show macsec mka session interface ethernet 1/52
Interface Name         : Ethernet1/52
    Session Status              : SECURED - Secured MKA Session with MACsec
    Local Tx-SCI                : 2c33.11b8.7d14/0001
    Local Tx-SSCI               : 1
    MKA Port Identifier         : 1
    CAK Name (CKN)              : 12
    CA Authentication Mode      : PRIMARY-PSK
    Member Identifier (MI)      : B54263EF7949A561E25CE617
    Message Number (MN)         : 523
    MKA Policy Name             : tests
    Key Server Priority         : 16
    Key Server                  : Yes
    Include ICV                 : No
    SAK Cipher Suite            : GCM-AES-XPN-256
    SAK Cipher Suite (Operational)     : GCM-AES-XPN-256
    Replay Window Size          : 148809600
    Confidentiality Offset      : CONF-OFFSET-0
    Confidentiality Offset (Operational): CONF-OFFSET-0
    Latest SAK Status           : Rx & TX
    Latest SAK AN               : 0
    Latest SAK KI               : B54263EF7949A561E25CE61700000001
    Latest SAK KN               : 1
    Last SAK key time           : 12:59:38 PST Thu Jun 30 2022
    CA Peer Count               : 1
    Eapol dest mac              : 0180.c200.0003
    Ether-type                  : 0x888e
```

```
Peer Status:
  Peer MI                 : 2C2C090E62A96F4D6E018210
  RxSCI                   : 2c33.11b8.8b88/0001
  Peer CAK                : Match
  Latest Rx MKPDU         : 13:16:54 PST Thu June 30 2022
```

64. Toda la información relacionada con la configuración de MACsec puede encontrarse en "Cisco Nexus 9000 Series NX-OS Security Configuration Guide", sección "Configuring MACsec" **[10]**.

65. En referencia a los Cisco Nexus 3000 esta feature está disponible a partir de la versión 10.X fuera de la cobertura de este documento. "Cisco Nexus 9000 Series NX-OS Security Configuration Guide", sección "Configuring MACsec" **[40]**.

6.3 PROTOCOLO SEGURO DE ADMINISTRACIÓN REMOTA SSHV2

66. El protocolo para la administración remota CLI es SSHv2, tal y como se recomienda en el apartado de SSH en la guía *CCN-STIC-807*.

67. Para asegurar que el administrador no emplee Telnet para la administración remota, el siguiente comando deshabilita el protocolo telnet en la unidad **[6] [37]**.

```
NX01# configure terminal
NX01(config)# no feature telnet
```

68. Para activar SSHv2, utilice el comando "**feature ssh**".

69. Antes de configurar la sesión SSH, se deben crear las claves para la autenticación del servidor SSH. En este tipo de dispositivos, pueden ser claves del tipo DSA, RSA o ECDSA. Por defecto, se generará una clave RSA usando 1024 bits. En el caso de RSA, se puede usar entre 768 y 2048 bits. En el caso de DSA no es posible especificar el tamaño de clave, siendo siempre de 1024 bits. La opción **"force"** se emplea para reemplazar una clave existente. La recomendación en este sentido es usar claves claves de curva elíptica EDCSA curva P-256 con una clave de 256 bits o superior, de manera que se obtenga una fortaleza mayor a 128.

```
NX01# configure terminal
NX01 (config)# ssh key {dsa [force] | rsa [bits[force]] | ecdsa [bits[force]}
```

70. Si se emplea DSA, se deben realizar adicionalmente los siguientes comandos.

```
NX01# configure terminal
NX01 (config)# ssh keytypes all
NX01 (config)# ssh kexalgos all
```

71. Se puede configurar adicionalmente la renegociación de clave de la sesión SSH con el siguiente comando que especifica tanto por tiempo, como por cantidad de datos de la sesión. Se recomienda no más de una hora y no más de un gigabyte de datos.

```
NX01#configure terminal
NX01 (config)# ssh rekey max-data {Kilo(K) | Mega(M) | Giga (G)} max-time {Seconds (S) | Minutes (M) | Hours (H)}
NX01(config)# ssh rekey ?
  max-data (no abbrev)  Data units are Kilo(K), Mega(M) and Giga(G)
NX01(config)# ssh rekey max-data ?
  WORD  Max data transmitted before key renegotiation (Max Size 7)
NX01(config)# ssh rekey max-data 1K ?
  max-time (no abbrev)  Time units are Seconds(S), Minutes(M) and Hours(H)
NX01(config)# ssh rekey max-data 1K max-time ?
  WORD  Max time lapsed before key renegotiation (Max Size 7)
NX01(config)# ssh rekey max-data 1K max-time 1M ?
<CR>
NX01(config)# ssh rekey max-data 1G max-time 60M
```

72. Por último, y para resumir los pasos y el orden de las instrucciones para habilitar las claves de autenticación de servidor y los parámetros de regeneración de claves de sesión SSH, se proponen las siguientes líneas:

```
NX01#configure terminal
NX01 (config)# no feature telnet
NX01 (config)# ssh key {dsa [force] | rsa [bits[force]] | ecdsa [bits[force]}
NX01 (config)# ssh rekey max-data {Kilo(K) | Mega(M) | Giga (G)} max-time {Seconds (S) | Minutes (M) | Hours (H)}
NX01 (config)# feature ssh
```

73. Las claves generadas se guardan en NVRAM, y es por esto que se deben guardar usando el comando "**copy running-config startup-config**". A diferencia de otros dispositivos, es posible visualizar las claves generadas usando el comando "**show ssh key**". A continuación, se muestra un ejemplo del resultado de este comando, donde se ha generado una clave RSA de 2048 bits.

```
NX01#show ssh key
**************************************
rsa Keys generated:Fri May 13 10:50:42 2022
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC1iyVXGLBAL/8Wi/NB+S+so3BynlbDzLwfS
uqj0gH9J5SDOV/i78s2Bfg/kQ6j2GkrZTpBmxxK9tWGJ0IUS8YZoTG0kdHrRfgV9xnfJ67
BPjPoebDzm3AyTvVlqUjgpCKL8f0RGuTXYJduW9uVj9Z/DhX1UvcTh3vMVQGy8HYRU
Uaig/9pIIlowlO21iiUeRUsVI2+GI8nwMHX6qo/IlaFww454wx5p9c1LQwwmhWfeTFK
/Bh7qSPGTw0y1P2Hn76A+pmGYx3jfFoD+tl8/a7GLg6L1/6rNsq9oyxGgg2z2FtDUPcTJ
zHBjw5pyYsf5VV1meOOPV7hltSUd3ZAKAJ1
```

```
bitcount:2048
fingerprint:
SHA256:oKaFgd9wZyKPaFbDMGM03aCp0PVszZg+ZHD59Ef+igI
************************************
could not retrieve dsa key information
************************************
could not retrieve ecdsa key information
************************************
```

74. Una vez determinada la identificación de clave pública del servicio, el siguiente paso es determinar los algoritmos de intercambio de claves. Para configurar los métodos tradicionales de intercambio de claves durante las conexiones, se usa por defecto el algoritmo "**Ecdh-sha2-nistp384**" (calificado como Recomendado en la guía *CCN-STIC-807)*, o bien use el comando "**ssh kexalgos all**" para habilitar todos los algoritmos disponibles en la actual versión de SSH.

```
NX01(config)# ssh kexalgos ?
  all              Enable algorithms supported in current version of SSH
ecdh-sha2-nistp384  Enable ecdh-sha2-nistp384
```

75. Los algoritmos de intercambio de claves soportados son:

- Curve25519-sha256. No recomendado según la guía *CCN-STIC-807.*
- Diffie-hellman-group-exchange-sha256. No recomendado según la guía CCN-STIC-807.
- Diffie-hellman-group1-sha1. No recomendado según la guía CCN-STIC-807.
- Diffie-hellman-group14-sha1.
- Diffiel-hellman-group1-sha1. No recomendado según la guía CCN-STIC-807.
- Ecdh-sha2-nistp256.
- Ecdh-sha2-nistp384.
- Ecdh-sha2-nistp521.

76. Se puede configurar los códigos de autenticación de mensajes (MACs) usados para detectar modificación del tráfico. Para habilitar este tipo de códigos se debe emplear el comando "**ssh macs all**". Los códigos soportados son:

- Hmac-sha1
- Hmac-sha2-256
- Hmac-sha2-512

77. Una vez obtenidas las claves mediante el correspondiente algoritmo para el intercambio de claves, los mensajes se envían cifrados mediante BPP (Binary Packet Protocol), que en el caso de los equipos Nexus puede basarse en cifrado en modo

bloque (ya sea CBC o CTR) o el uso de esquemas AEAD (modos GCM). El modo usado por defecto y que se puede configurar en cualquier momento es el "**aes256-gcm**" (calificado como Recomendado en la guía *CCN-STIC-807),* o bien usar todos los disponibles en la máquina para el actual protocolo SSHv2 mediante el comando "**ssh ciphers all**".

```
NX01(config)# ssh ciphers ?
  aes256-gcm  Enable aes256-gcm
all       Enable algorithms supported in current version of SSH
```

78. Los cifrados soportados son:
    - Aes128-cbc
    - Aes192-cbc
    - Aes256-cbc
    - Aes128-ctr
    - Aes192-ctr
    - Aes256-ctr
    - Aes256-gcm@openssh.com
    - Aes128-gcm@openssh.com
79. Se recomienda además configurar un número máximo de intentos de acceso. Por defecto, el número de intentos es tres, siendo uno el mínimo y diez el máximo. Para configurar el número de intentos, el comando a emplear es el siguiente:

```
NX01(config)# ssh login-attempts {1-10}
```

80. Del mismo modo, es recomendable configurar un tiempo máximo para la sesión de inactividad de SSH. El valor máximo es de 120 segundos y el mínimo 0 (siendo 0 el valor que deshabilita en realidad esta opción).

```
NX01 (config)# ssh idle-timeout {0-120}
```

81. Para comprobar que la conexión ssh se ha realizado correctamente, así como para desconectar las sesiones SSH que hayan podido quedar huérfanas, se debe emplear el comando "**show users**". Este comando visualiza todas las conexiones existentes, y entonces es posible eliminar aquellas conexiones mediante "**clear line {vty-line}**" [6][37].

```
NX01# show users
NAME     LINE       TIME       IDLE       PID COMMENT
admin    ttyS0      Jun  8 06:08   .       24059 *
dev-ops  pts/12     Jun 8 07:12    .       23618 *
NX01# configure terminal
NX01 (config)# clear line pts/12
```

82. Si lo que se desea es eliminar las conexiones SSH establecidas desde el dispositivo hacia otros equipos, se debe emplear el comando "**clear ssh hosts**".

83. Si se desea cambiar el puerto por defecto (22) del protocolo SSHv2 se puede realizar deshabilitando en primer lugar SSH, revisando los puertos locales disponibles y finalmente cambiando el puerto y volver a habilitar SSH. Cambiar el puerto ayuda a aumentar la privacidad e integridad de las conexiones. Se muestra un ejemplo a continuación usando el puerto 58003.

```
NX01# configure terminal
NX01 (config)# no feature ssh
NX01 (config)# show sockets local-port-range
Kstack local port range (15001 - 58000)
Netstack local port range (58001 - 60535) and nat port range (60536 - 65535)
NX01 (config)# ssh port 58003
NX01 (config)# feature ssh
```

6.4 PROTOCOLO SEGURO DE CONEXIÓN DE NIVEL 3: IPSEC

84. El producto basado en NXOS no permite el uso de la unidad como terminador de túneles IPSec, en ninguna de sus versiones (IKEv1, IKEv2) tal como se puede encontrar en "Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide", sección "Guidelines and limitations for Static NAT" [11] o "Cisco Nexus 3000 Series NX-OS Interfaces Configuration Guide" [33].

6.5 GESTIÓN DE CERTIFICADOS

85. Se recomienda configurar el dispositivo para habilitar el uso de certificados X.509v3, que pueden ser utilizados para varias tareas, como el uso de servidores de syslog remotos TLS seguros. Los certificados RSA están soportados.

86. La creación de estos certificados y su carga en el dispositivo están detalladas en [12][41]. Los aspectos más destacados de la configuración del dispositivo para el uso de estos certificados se explican en las subsecciones siguientes.

6.5.1.1 CREACIÓN DE LA SOLICITUD DE CERTIFICADO (CSR)

87. La petición de certificado para el dispositivo debe ser creada usando un par de claves RSA y un nombre de dominio.

88. Para poder generar una petición de certificado, el dispositivo debe tener establecida una relación de confianza con la CA, configurar la autenticación de dicha CA, determinar el método de inscripción (enrollment) y determinar el método para comprobar el estado de revocación de los certificados.

89. Para crear la asociación con la entidad de confianza (CA), los pasos a seguir son los siguientes:

- Con el fin de configurar el nombre de equipo utilizado durante el intercambio de claves se debe ejecutar el comando "**hostname** <nombre>" en el modo de configuración. También es recomendable definir el dominio, al tratarse de identificadores FQDN.

```
NX01(config)# hostname NX01
NX01(config)# ip domain-name testnx.com
```

- Es necesario crear la correspondiente pareja de clave pública/privada RSA, que nos va a venir identificada por un "key label", que usaremos más tarde.

```
NX01(config)# crypto key generate rsa modulus 2048
NX01(config)# end
NX01# show crypto key mypubkey rsa
key label: NX01
key size: 2048
exportable: no
key-pair already generated
```

- Para declarar la entidad de confianza (trustpoint asociado a la CA) que debe utilizar el dispositivo, se debe utilizar el siguiente comando "**crypto pki trustpoint** <nombre>" desde el modo de configuración.
- Para configurar los parámetros del método de inscripción (enrollment), el sistema operativo NX-OS únicamente permite el uso de inscripción interactiva mediante la línea de comandos (CLI), a través de copy-paste de los valores correspondientes. Esto se realiza mediante el comando "**enrollment terminal**".
- Se especifica a continuación el par clave RSA asociado a este punto de entidad de confianza mediante el comando "rsakeypair <id>".

```
NX01(config)# crypto ca trustpoint admin-ca
NX01(config-trustpoint)# enrollment terminal
NX01(config-trustpoint)# rsakeypair NX01
NX01(config-trustpoint)# exit
```

- Se puede comprobar la información de la entidad de confianza mediante "show crypto ca trustpoint".

```
NX01# show crypto ca trustpoint
trustpoint: admin-ca; key-pair: NX01
revokation methods:  crl
```

- Para especificar la CA como confiable, es necesario introducir el comando “crypto ca authenticate <id>”, y seguir los pasos del proceso interactivo a través del CLI. En dicho proceso, se introduce la cadena de certificación en formato texto (PEM).

```
NX01(config)# crypto ca authenticate admin-ca

input (cut & paste) CA certificate (chain) in PEM format;

end the input with a line containing only END OF INPUT :

-----BEGIN CERTIFICATE-----

MIICzTCCAbWgAwIBAgIJAKLMnDabXgFlMA0GCSqGSIb3DQEBBQUAMB0xCzAJBgV

BAYTAkVTMQ4wDAYDVQQKDAVCYWJlbDAeFw0yMjA2MjQxMzQ2NTBaFw0zMjA
2MjEx

MzQ2NTBaMB0xCzAJBgNVBAYTAkVTMQ4wDAYDVQQKDAVCYWJlbDCCASIwDQYJ
KoZI

hvcNAQEBBQADggEPADCCAQoCggEBALuzIY13AkgSaQtsUo2og6RBHaco4a6kDFNt

H/CatjR3DXBEtp62qMgJKEqDdOJrVU9F0ZzNuQctpZwenVmKGCqmB7gvym894fF
U

zrzaINMFJtW1w9329zhUhN1ZfrsQ8j7K9aJ0qz9FoR6xxIf6ZTzbWKbeppjcCm81

28BK7KFAYF0MnJ0SH9nBOQhaRP9RJiSUBL1I1VBtARKfytjV7gMITx5OVWTS2QtW

3jnt+3rJ5QlUrm10TVCaR9pIC5Fn3gLSOfyRASayOXVi1f4Z+hMxkkHmMsZkMBGp

0zgjlPO5a+CrXjthQhNegi0a9fy2364iLdlBEV9bAA4DrvdKi+cCAwEAAaMQMA4w

DAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEAK0qCX/kdzfcdYCZ1rE
V

6cua2he6zcYq+pE5y0Iz4w/mJ9Icvnk0fDOlITSxNEWHOqf4srXH2Rlhs/ZrIxSB

AkfizlVk4DD6RZDPPeXtBQAMUq2i4usTi6BYX4fmlJvL1vMopN1VU+9YFyLDJDbF

Qy5f6y4tIycp7XgWsn0PTlEZULYDJHv9JqvuOfr3TxJ+AutxxVNmC6mw0RUfAsyK

JrDChazq/k2GaQVKgB2NTTK7XFl8SZp0Ok4FnQvqOivwJ02tWfJfHXhfJ+DVQbW+

Zvr5yuHFDX4oiV05TXGckm/ROKxVYLLq5PsuPCXlQRQ5lYi6vZapSA1mpOkkxKjR

aA==

-----END CERTIFICATE-----

END OF INPUT

Fingerprint(s): SHA1
Fingerprint=E6:31:84:48:D8:7D:24:1D:AA:1E:68:2A:9B:B5:61:58
:34:C7:B4:88

Do you accept this certificate? [yes/no]:yes

NX01(config)# show crypto ca cer

certificates   certstore

NX01(config)# show crypto ca certificates
```

```
Trustpoint: admin-ca
CA certificate 0:
subject= /C=ES/O=Babel
issuer= /C=ES/O=Babel
serial=A2CC9C369B5E0165
notBefore=Jun 24 13:46:50 2022 GMT
notAfter=Jun 21 13:46:50 2032 GMT
SHA1
Fingerprint=E6:31:84:48:D8:7D:24:1D:AA:1E:68:2A:9B:B5:61:58:34:C7:B4:88
purposes: sslserver sslclient
```

- Para declarar el método de revocación de certificados (CRL), se pueden escoger tres métodos: CRL, NDcPP:OCSP (para syslog) o none, si no se desea usar ninguno. El método a utilizar se escoge con el comando "revocation-check <crl | oscp | none>".
- Finalmente, para crear la petición de certificado utilice el comando "**crypto ca enroll** <id>" en el modo de configuración global, donde el nombre se debe corresponder con el del punto de confianza (trustpoint) establecido en pasos anteriores. El resultado debe ser el fichero de texto de CSR que se envíe a la entidad certificadora para su firma.

```
NX01(config)# crypto ca enroll admin-ca
 Create the certificate request ..
 Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.
  Password:nexus
 The subject name in the certificate will be the name of the switch.
 Include the switch serial number in the subject name? [yes/no]:no
 Include an IP address in the subject name [yes/no]:no
 Include the Alternate Subject Name ? [yes/no]:no
 The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
MIICpTCCAY0CAQAwGjEYMBYGA1UEAwwPTlgwMS50ZXN0bnguY29tMIIBIjANBgq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAueZM/FQ9c6HYKCSRbcQ0q1IURsGxNJy
+I+4meSDTqxU+fa11i9dZfF2NHPtUtdbMHtfIIR1N/BRioF8PwADCQK5MDwDw+Yn
7xGvRZg3C3CJS8IcMw1TuVKaZb/3XAeGZDmZIZYG0lwgX8V1Ab90+vVtQLGSrbVM
```

vhyVFelu9jH/5nZhkJ5nKiWCJ1jBx5f85tDnt5aFUfO6bUCRpg3uJZbddLb3QqaU
NaZxTV5Ef25rz7FJscV1lzBAbMeOK9TxGGUGqDOO1yp8RXvj7EvuWPx33a+M+90V
eIaDFJUABtITAcoImK5UM8ie3sSk9XCNB3L/VMkEr7/0R0vrtH1NtQIDAQABoEYw
FAYJKoZIhvcNAQkHMQcMBW5leHVzMC4GCSqGSIb3DQEJDjEhMB8wHQYDVR0RAQH/
BBMwEYIPTlgwMS50ZXN0bnguY29tMA0GCSqGSIb3DQEBCwUAA4IBAQBoIESTgZ+d
ejvsVdTZM3xURfVMKkkLD0sSYQK3iz1pDxtmBprzxYhOUZd4yetRtktHZvp3etLe
775EZQWaICnzNmFvncgFZuR9HWUmMGD+7ZqKBFQ2tAaZJdK/aTfanwPy/MwUSwln
sdaQniVsXle9LIWpIu5Bnw6ql5tu7VG/4VEGdY9ChCM8h9L1WWAGUS1Thtg+CNYl
ODoYObWysYPpc8Odbv4eAVrmXMRG6QIHIzOcbPAlZ9cu+kJ03Jbr70H7oxzpQJn6
o/rh4YP4AY8TjJ2L68t6M5IcBYCwlD5y+kimBo3+SP0A9uCmizdCkxiiBYsh4aX0
dpB2nISAZXL+

-----END CERTIFICATE REQUEST-----

6.5.1.2 INSTALACIÓN DEL CERTIFICADO

90. Tras la creación de solicitud del certificado (CSR), se devolverá al administrador del sistema un certificado en formato PEM que podrá introducir en el sistema, para la identificación segura del dispositivo.

91. Los requisitos previos para poder instalar el certificado son los siguientes:

    - Disponer de una asociación con la CA válida.
    - Considerar dicha CA como confiable.

92. El certificado se instala mediante el comando "**crypto ca import <id> certificate**", y se realiza copiando el certificado en modo PEM en el proceso interactivo del CLI. A partir de ese momento, el correspondiente certificado estará disponible para su uso en las actividades que requieran dicho certificado X.509.

```
#NX01(config)# crypto ca import admin-ca certificate
input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIDLDCCAhSgAwIBAgIJALv1CHUf61TFMA0GCSqGSIb3DQEBCwUAMB0xCzAJBgNV
BAYTAkVTMQ4wDAYDVQQKDAVCYWJlbDAeFw0yMjA2MjQxNjE4MDlaFw0yNDA5MjYx
NjE4MDlaMBoxGDAWBgNVBAMMD05YMDEudGVzdG54LmNvbTCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBALnmTPxUPXOh2CgkkW3ENKtSFEbBsYTScviPuJnk
g06sVPn2tdYvXWXxdjRz7VLXWzB7XyCEdTfwUYqBfD8AAwkCuTA8A8PmJ+8Rr0WY
NwtwiUvCHDMNU7lSmmW/91wHhmQ5mSGWBtJcIF/FdQG/dPr1bUCxkq21TL4clRXp
bvYx/+Z2YZCeZyolgidYwceX/ObQ57eWhVHzum1AkaYN7iWW3XS290KmlDWmcU1e
```

RH9ua8+xSbHFdZcwQGzHjivU8RhlBqgzjtcqfEV74+xL7lj8d92vjPvdFXiGgxSV
AAbSEwHKCJiuVDPInt7EpPVwjQdy/1TJBK+/9EdL67R9TbUCAwEAAaNyMHAwNwYD
VR0jBDAwLqEhpB8wHTELMAkGA1UEBhMCRVMxDjAMBgNVBAoMBUJhYmVsggkAosyc
NpteAWUwCQYDVR0TBAIwADAOBgNVHQ8BAf8EBAMCA+gwGgYDVR0RBBMwEYIPTlgw
MS50ZXN0bnguY29tMA0GCSqGSIb3DQEBCwUAA4IBAQAnnMM0e7RaikZzJ65mD77W
tTM8f2exjWO+6QiWtgQtbop0M1todIWsE9bRybIVwQGatttFr05moTsEIZUmUBU8
aSueSEP/CuLCVocMmKwXqGvpymOGhSAaGlD+u5l6R1u7b6Bsd27tyUdT1asX8I2n
5bMIcZktlKOgbXJ41yX/+d5np2LFNnHTX4HZplzvxWFK/vHSQubqSN1K6+DEIsTO
JgaulPvA9uRQncukztmJo4CB2MG7kvIaVzIMyP9chz4F7dZPXoOc2bpYA/G8xBu7
1rVHzP334xFzsLO4bdQnClwjN2xqW67vuIOf56RgNtHBSmfX1U8QFJbjFmt2vXw/
-----END CERTIFICATE-----

```
NX01(config)# show crypto ca certificates
Trustpoint: admin-ca
certificate:
subject= /CN=NX01.testnx.com
issuer= /C=ES/O=Babel
serial=BBF508751FEB54C5
notBefore=Jun 24 16:18:09 2022 GMT
notAfter=Sep 26 16:18:09 2024 GMT
SHA1 Fingerprint=D2:F3:A1:4B:96:89:0C:3A:4E:15:66:B3:58:2E:B2:63:B0:51:55:02
purposes: sslserver sslclient
CA certificate 0:
subject= /C=ES/O=Babel
issuer= /C=ES/O=Babel
serial=A2CC9C369B5E0165
notBefore=Jun 24 13:46:50 2022 GMT
notAfter=Jun 21 13:46:50 2032 GMT
SHA1 Fingerprint=E6:31:84:48:D8:7D:24:1D:AA:1E:68:2A:9B:B5:61:58:34:C7:B4:88
purposes: sslserver sslclient
```

6.6 SINCRONIZACIÓN HORARIA (NTP)

93. Los dispositivos Nexus pueden operar en un entorno sin protocolo horario (NTP), o uno que permita el acceso a un servidor NTP para sincronización horaria. Aunque se recomienda esta segunda opción, si no estuviera disponible, la hora del equipo se puede establecer manualmente mediante el comando "**clock**", tanto para la zona

horaria como para el establecimiento manual. La administración del reloj está reservada al administrador privilegiado.

```
NX01# configure terminal
NX01(config)# clock protocol none
NX01(config)# clock timezone CEST 2 0
NX01(config)# clock set 17:16:00 22 jun 2022
Wed Jun 22 17:16:00 CEST 2022
```

94. El servidor NTP, si está configurado, es proporcionado por el entorno IT. Sin autenticación o control de acceso, NTP es inseguro y puede ser usado por un atacante para enviar paquetes NTP e intentar sobrecargar o bloquear el dispositivo.
95. Para habilitar NTP se debe emplear el comando "**feature ntp**" en modo privilegiado.
96. Se recomienda emplear, de ser posible, emplear algún tipo de autenticación contra el servidor NTP, que como mínimo debería ser usando claves simétricas o Message Digest 5 (MD5). Para crear una clave MD5 use el comando mostrado a continuación. El parámetro "id" es un identificador numérico de la clave que puede estar entre 1 y 65535, y la cadena puede ser un conjunto alfanumérico de hasta 15 caracteres. A continuación, sería necesario habilitar la autenticación de NTP mediante el comando "**ntp authenticate**".

```
configure terminal
(config)# ntp authentication-key {id} md5 {cadena}
```

97. Para configurar el servidor NTP con el que el dispositivo se va a sincronizar, use el siguiente comando. La dirección del servidor puede ser una dirección IPv4 o IPv6 además de un nombre FQDN. El parámetro "***key***" es el definido anteriormente, mientras que "***maxpoll/minpoll***" son los intervalos máximos y mínimos de consulta al servidor expresados en segundos y deben ser potencias de dos (con un máximo de exponente 16). El parámetro VRF puede ser "*default*", "*Management*" o cualquier nombre de VRF hasta 32 caracteres

```
# configure terminal
(config)# ntp server {ip-address | ipv6-address | dns-name} [key key-id] [maxpoll max-poll] [minpoll min-poll] [prefer] [use-vrf vrf-name]
```

98. Desde un punto de vista de la seguridad, si se va a usar NTP, es recomendable utilizar la autenticación NTP usando claves simétricas o Message Digest 5 (MD5) y el comando "***ntp Access-group***". Si NTP se habilita de forma global, es recomendable desactivarlo en todas las interfaces en las cuales no sea necesario.
99. Para obtener más información, consultar *"Cisco Nexus Series NX-OS System Management Configuration Guide"*, capítulo "Configuring NTP" [13] [42] .

6.7 SNMP

100. Se recomienda en los dispositivos Nexus, que el protocolo SNMP permanezca desactivado.

101. Para comprobar que la configuración inicial no contempla el uso de un servidor SNMP, examinar el fichero de configuración para asegurar que no existe una entrada de tipo "servidor-snmp". Para asegurarse de que no hay funcionando ningún agente de servidor snmp, utilice el comando "**no snmp-server protocol enable**" como se describe en [14] [43].

6.8 TELNET

102. Dado que se trata de un tipo de acceso remoto basado en un protocolo no seguro (sin mecanismo de cifrado, ni verificación de manipulación de paquetes), se recomienda en los dispositivos Nexus que el protocolo Telnet permanezca desactivado

103. El protocolo Telnet viene deshabilitado por defecto, pero en caso de que la unidad por cualquier motivo lo tuviera habilitado, y se quisiera deshabilitar, se puede realizar mediante el comando "**no feature**".

```
NX01(config)# no feature telnet
```

6.9 INTERFAZ API/REST: NX-API

104. El interfaz NX-API permite realizar tareas de configuración, mediante el uso del CLI, pero a través de ubicaciones remotas, gracias al protocolo HTTP/HTTPS. Se basa en el uso de un servidor HTTP Nginx para recibir comandos CLI como *payload* de peticiones REST API, de modo que se pueda articular un elevado grado de programabilidad y orquestación en la máquina.

105. Dado que se trata de otro tipo de acceso remoto basado en HTTP/HTTPS, con el elevado número de vulnerabilidades que se han ido descubriendo recientemente (ejecución de comandos a través de usuarios no privilegiados, o directamente no autorizados), se recomienda por seguridad no habilitar esta función, a no ser que sea estrictamente necesario para la operación de la misma.

106. El interfaz NX-API viene deshabilitado por defecto, pero en caso de que la unidad por cualquier motivo lo tuviera habilitado, y se quisiera deshabilitar, se puede realizar mediante el comando "**no feature**".

```
NX01(config)# no feature nxapi

Removal of controller configuration takes several minutes. Please wait before saving
running-config.
```

7. CONTROL DE TRÁFICO Y SEGURIDAD EN LOS PUERTOS DE RED

7.1 APAGADO DE LOS PUERTOS

107. La primera medida que debemos llevar a cabo en esta fase es el bloqueo o cierre de los puertos que no vayan a ser utilizados. Para ello, se pueden emplear las siguientes expresiones:

```
NX01# configure terminal
NX01 (config)# interface <interface-id>
NX01 (config-if)# switchport block multicast
NX01 (config-if)# switchport block unicast
NX01 (config-if)# shutdown
NX01 (config-if)# end
```

108. Con estos pasos, se asegura que los puertos que no está previsto utilizar por el momento, no pueden ser utilizados sin conocimiento y/o autorización previa.

7.2 MEDIDAS DE PROTECCIÓN DE LOS PUERTOS

109. Configurar la seguridad a nivel de puerto consiste en definir qué equipos van a poder conectarse en cada puerto, cuantas conexiones máximas se van a permitir en cada puerto y qué hacer en caso de que se alcance es el número máximo de conexiones. Para poder llevar a cabo esta configuración es necesario tener un inventario de las direcciones físicas de los equipos que se van a conectar en cada puerto.

110. Direcciones MAC Seguras de tipo **Static**: Estas direcciones son configuradas de forma manual en el equipo, almacenadas en una tabla de direcciones, y añadidas a la running-configuration cada vez que este arranca.

111. Direcciones MAC Seguras de tipo **Dynamic**: Estas direcciones son aprendidas de forma dinámica mediante la interacción entre el *conmutador* y otros equipos, almacenadas en la tabla de direcciones, pero son eliminadas cuando el equipo se reinicia.

112. Direcciones MAC Seguras de tipo **Sticky**: Estas direcciones pueden ser aprendidas de dos formas, o bien de forma dinámica, o bien porque han sido introducidas manualmente. Además, es posible elegir si se desea que sean salvadas en una tabla de direcciones permanentes, y por lo tanto el *conmutador* no tendrá que aprenderlas de nuevo al reiniciarse, o tratarlas como direcciones dinámicas y que por tanto se perderán con el siguiente reinicio.

113. Es necesario remarcar que hay un número máximo de direcciones MAC seguras que se puedan configurar, y que viene fijado por el número máximo de direcciones MAC que sistema es capaz de gestionar.

114. Durante el tiempo en que el *conmutador* se encuentra funcionando, pueden darse casos de violaciones de la seguridad. Estos casos pueden suceder, bien porque el número máximo de direcciones MAC seguras en un puerto se ha alcanzado, o bien porque una dirección aprendida en un interfaz se ha detectado en otro interfaz seguro en esa VLAN, por ello es indispensable poner los medios necesarios para impedir que se conecten máquinas en la red sin autorización. Se pueden configurar los equipos de red para que reaccionen de cuatro formas:

- *Protect*: Cuando se alcanza el máximo número de direcciones MAC seguras permitidas en el puerto, los paquetes de direcciones desconocidas se desechan hasta que no se reduzca el número de direcciones MAC en la lista por debajo del máximo o se incremente el máximo. Además, en este estado el equipo no notifica a los administradores que la violación de seguridad ha ocurrido. No es recomendable configurar este modo en un puerto trunk, ya que este modo deshabilita la opción de aprender cuando cualquier Virtual LAN(VLAN) alcanza su límite máximo incluso si ese puerto en cuestión no ha alcanzado su máximo.
- *Restrict*: Cuando se alcanza el máximo número de direcciones permitidas en el puerto, los paquetes de direcciones desconocidas se desechan hasta que no se reduzca el número de direcciones MAC en la lista por debajo del máximo o se incremente el máximo. Además, en este estado el equipo notifica a los administradores que la violación de seguridad ha ocurrido. Se envía un trap SNMP (en caso de que este servicio se encuentre habilitado), se crea un mensaje de tipo syslog y el contador de violaciones se incrementa.
- *Shutdown*: Una violación de seguridad en el puerto provoca que el interfaz adquiera el estado error-disabled y se apague, de forma inmediata el LED del puerto. También se envía un trap SNMP (en caso de que este servicio se encuentre habilitado), se crea un mensaje de syslog y el contador de violaciones se incrementa. Cuando un puerto seguro está en el estado error-disabled, se le puede reactivar mediante el comando:

```
NX01(config)#
NX01(config)# errdisable recovery cause ?
  all                Enable timer to recover from all causes
  bpduguard          Enable timer to recover from BPDU Guard error disable state
  dcbx-no-ack        Enable timer to recover from no DCBX Acks
  failed-port-state  Enable timer to recover from stp set port state failure
  link-flap          Enable timer to recover from linkstate flapping
  loopback           Enable timer to recover from loopback error disabled state detected
by UDLD
  pause-rate-limit   Enable timer to recover from pause rate limit error disabled state
  psecure-violation  Enable timer to recover from psecure violation disable state
```

security-violation Enable timer to recover from 802.1x violation disable state

storm-control Enable timer to recover from storm control error disabled state

udld Enable timer to recover from udld error disabled state

vlan-membership Enable timer to recover from vlan memberbship failure

vpc-peerlink Enable timer to recover from inconsistent vpc peer-link

También puede ser reactivado manualmente introduciendo los comandos shutdown y no shutdown en el menú de configuración del interfaz. Este último es el modo por defecto.

115. Para poder utilizar la funcionalidad de port-security es necesario habilitarla a nivel global:

```
NX01 (config)# feature port-security
```

116. Es importante saber que, una vez habilitada la funcionalidad, la configuración por defecto del conmutador (out-of-the-box configuration) vendrá con la seguridad a nivel de puertos desactivada y las direcciones sticky desactivadas. Por lo tanto y una vez definidas estas terminologías, las configuraciones se ofrecen a continuación:

```
NX01# configure terminal
NX01 (config)# interface <interface-id>
NX01 (config-if)# switchport port-security maximum <valor>
```

117. Se utiliza esta instrucción por cada dirección que se quiera añadir a las tablas estáticas. Solo se puede introducir un número de entradas igual o inferior al máximo establecido con anterioridad.

118. En caso de desear introducir direcciones de tipo sticky o activar el modo de gestión de direcciones del puerto al modelo sticky, se usarían los siguientes comandos:

```
NX01# configure terminal
NX01 (config-if)# switchport port-security
NX01 (config-if)# switchport port-security violation shutdown
NX01 (config-if)# switchport port-security maximum 1
NX01 (config-if)# switchport port-security mac-address sticky
```

119. En este ejemplo, el aprendizaje de la dirección mac del equipo que se conecte al puerto del *conmutador*, se aprenderá de forma automática. Sólo se va a permitir la conexión desde una dirección mac origen, que es la que se va a aprender en la primera conexión, y en caso de que otro equipo intente realizar una conexión a este puerto, este será desactivado por el conmutador de forma permanente, hasta que se haga un shutdown-no shutdown del mismo.

120. Se puede configurar el tiempo durante el cual va a permanecer bloqueado un puerto tras un intento de violación de acceso. Y además se puede configurar para que, tras el tiempo de bloqueo se permita el acceso al puerto, siempre que no se haya detectado ningún tipo de tráfico, tal y como muestra el ejemplo, en el que se

ha definido que, tras un bloqueo, se interrumpa la actividad durante un periodo de diez minutos en el que no se detecte tráfico en el puerto **[15] [44]**:

```
NX01 (config-if)# switchport port-security aging time 10
NX01 (config-if)# switchport port-security aging type inactivity
```

121. El comando 'aging' no se puede configurar con direcciones MAC del tipo 'sticky'

122. Una vez acabada la configuración se procede al salvado de la misma:

```
NX01# show port-security
NX01# copy running-config startup-config
```

7.3 SPANNING TREE. PROTECCIÓN FRENTE A ENVÍO DE MENSAJES DE CONTROL STP

123. STP (Spanning Tree Protocol), definido en el estándar IEEE 802.1D, es un protocolo de encaminamiento de nivel 2 que evita bucles en la red, al tiempo que ofrece redundancia en las rutas de envío de paquetes. Los bucles pueden ocurrir cuando han sido configurados caminos redundantes para incrementar la resistencia de la red ante la caída de algún enlace. En caso de establecerse un bucle es posible que las estaciones comiencen a recibir mensajes duplicados, y crear situaciones que vuelvan inestable nuestra red. Para evitar esta situación se produce un intercambio constante de información entre *conmutadores*. La información se envía en tramas Ethernet Multicast conocidas como Bridge Protocol Data Units (BPDUs).

124. Las vulnerabilidades más graves de este protocolo pueden resumirse en las siguientes líneas. Primero, el equipo con el "bridge ID" más bajo será elegido como root bridge desde el cual se puede afectar a los flujos de datos y reducir la eficiencia de la red (el "bridge ID" se compone de 2 bytes de prioridad y seis bytes de la dirección MAC del equipo). Además, en este protocolo no se ha definido ningún tipo de identificación que permita averiguar la validez de la información recibida, lo cual provoca que un sistema dentro de la red puede modificar a voluntad la topología de STP. En consecuencia, STP ha de ser usado solo entre los equipos de red gestionados por los administradores.

125. Por lo tanto y ya que por defecto está activado es recomendable seguir una de las dos siguientes acciones:

- Desactivar STP en todas las VLANs del equipo, lo cual provocaría que el equipo deje de responder a las BPDUs que reciba de los equipos conectados.
- Definir adecuadamente el contexto de los puertos, para que el protocolo STP pueda funcionar adecuadamente. Existen tres contextos de STP en los que se puede encontrar un puerto:
- Modo *Normal*: los puertos de acceso operan con las temporizaciones habituales del protocolo STP, y reaccionan a los paquetes BPDU recibidos según el estándar. Es el recomendado para interconexión con otros

conmutadores de la red, y es el modo por defecto en el que se encuentran los puertos en NXOS.

- Modo *Edge*: destinados a puestos de usuario final (Layer 2), el puerto entra inmediatamente en modo Forwarding, y no deberían procesar paquetes BPDU.
- Modo *Network*: es similar al modo Normal, pero permite la funcionalidad de *Bridge Assurance*, la cual evita ciertas condiciones de error cuando el otro conmutador conectado también permite el uso de dicha funcionalidad *Network Assurance*. Es el modo que se recomienda para la interconexión de dispositivos Nexus entre sí para formar un vPC.

126. Para desactivar STP en una VLAN es necesario introducir el siguiente comando desde el "privileged EXEC mode" [16] [45]:

```
NX01# configure terminal
NX01 (config)# no spanning-tree vlan <vlan-id>
NX01 (config)# end Switch# show spanning-tree vlan <vlan-id>
NX01# copy running-config startup-config
```

127. Configurar un puerto en modo *Edge* implica que este puerto comienza directamente en el estado de *forwarding* dentro de los posibles estados de Spanning-Tree. Por lo tanto, es necesario utilizar este comando con cuidado, ya que es esencial garantizar que no existen bucles en la VLAN. Además, en los puertos que configuremos como Port Fast podemos activar la BPDU Guard a nivel global en todos los puertos de tipo *Edge*, que nos permitirá asegurarnos de que no recibimos por esos enlaces información errónea, la cual podría alterar la estructura de red que hemos descubierto al ejecutar STP entre los conmutadores:

```
NX01# configure terminal
NX01(config)# spanning-tree port type edge bpduguard default
NX01(config)#interface <interface-id>
NX01(config-if)# spanning-tree port type edge
NX01(config-if)#end
```

128. Para configurar un puerto en modo Network, se deberán utilizar los siguientes comandos:

```
NX01# configure terminal
NX01(config)#interface <interface-id>
NX01(config-if)# spanning-tree port type network
NX01(config-if)#end
```

129. Otra opción de configuración es el uso de Root Guard. Si sabemos que el conmutador B no debe ser root, podemos activar este servicio en el puerto del conmutador A al que está conectado B, de tal forma que este puerto se bloquee si

el conmutador B intenta actuar como root. Esta opción puede ser configurada por medio del comando:

```
NX01# configure terminal
NX01 (config)# interface <interface-id>
NX01 (config-if)# spanning-tree guard root
NX01 (config-if)# end Switch# show running-config
NX01# copy running-config startup-config
```

7.4 LISTAS DE ACCESO IP (ACL)

130. Las listas de acceso son una herramienta fundamental, la cual permite seleccionar que direcciones IP se van a permitir acceder por el puerto al que esté asociada. Las ACLs se evalúan línea a línea, hasta que se encuentra una coincidencia, por lo que hay que definir primero los casos más específicos y avanzar hasta llegar a los casos más generales. Una vez se establece una ACL en un interfaz, por defecto se deniega todo el tráfico en dicho interfaz, por lo que es necesario definir correctamente los tráficos necesarios.

131. Las recomendaciones generales a la hora de hacer una ACL son las siguientes:

- Para evitar el bloqueo total del tráfico, en cada ACL hace falta por lo menos una regla tipo *permit*.
- Una ACL se aplica sólo en un sentido, por tanto, solo se aplicará a la mitad de los paquetes (entrantes o salientes) que pasen por el interfaz al que ha sido aplicada. Se debe minimizar el número de reglas.
- Para conocer las estadísticas de una ACL (número de paquetes que son admitidos o denegados), es posible usar el comando “statistics per-entry” dentro de cada ACL en particular.
- Todas las ACLs tienen implícita una regla final, que deniega todo tipo de tráfico que no cumpla con ninguna de las reglas anteriores.

7.4.1 TIPOS DE ACLS

132. Las ACLs definidas en los dispositivos Nexus son similares al tipo *extended* de las reglas en Cisco IOS, y, por tanto, pueden permitir o bloquear paquetes basándose en protocolos, dirección IP origen o destino, puertos TCP/UDP origen o destino y también tipos de mensaje ICMP/IGMP. Sólo existe un tipo de regla, que tiene estas características, no existen reglas *standard* o *extended* como en Cisco IOS.

133. Las ACLs en los dispositivos Nexus pueden definirse tanto para tráfico IPv4 como para tráfico IPv6.

7.4.2 CREACIÓN DE ACLS

134. Para definir una lista de acceso en NXOS, es necesario utilizar la siguiente estructura:

```
NX01#conf t
NX01(config)#ip[v6] access-list name
NX01(config-acl)# [sequence number] {deny | permit} <protocol> {<source-ip-prefix|source-mask>} {<destination-ip-prefix|destination-mask>}
NX01(config-acl)# [statistics per-entry]
NX01(config-acl)# end
NX01# show ip access-list name
```

- Para una ACL destinada a controlar tráfico IPv6, se debería usar el comando **#ipv6 access-list *name.***
- *Name*: Etiqueta identificadora de la ACL, pudiendo permitirse hasta 64 carateres.
- *Deny|Permit*: Define si la dirección que se introducirá a continuación en el campo source, debe ser admitida o rechazada.
- *Protocol:* Define el protocolo al que afecta la regla. Para ciertos protocolos es posible usar una convención de nombres, o bien, usar un puerto.
- *Sequence-number*: Las reglas dentro de la ACL se ejecutan en orden, por lo tanto, es muy importante definir correctamente el orden de evaluación de las reglas. Este número de secuencia puede estar entre 1 y 4294967295.
- *<source-ip-prefix|source-mask>:* Define la dirección origen a la que se está dando o denegando acceso, ya sea mediante un prefijo (que sólo compara los primeros bits contiguos), o bien en formato *netmask*, que utiliza la dirección CIDR con su correspondiente máscara de red.
- *<destination-ip-prefix|destination-mask>:* Define la dirección destino a la que se está dando o denegando acceso, ya sea mediante un prefijo (que sólo compara los primeros bits contiguos), o bien en formato *netmask*, que utiliza la dirección CIDR con su correspondiente máscara de red.
- *Statistics per-entry:* Permite definir si queremos registrar las estadísticas de paquetes (permitidos, denegados) para esa ACL en concreto.

7.4.3 APLICACIÓN DE LISTAS DE ACCESO

135. Las listas de control de acceso se pueden aplicar a los siguientes elementos dentro de un equipo Cisco Nexus:

- Interfaces de nivel 2 (switchport). Se denominan “Port ACLs”.

- Interfaces de nivel 3 (interfaces SVI en una VLAN, interfaces de nivel 3, o interfaces de gestión). Se denominan “Router ACLs”.
- VLANs. Se denominan “VLAN ACLs”.

136. En cualquiera de esas instancias, por ejemplo, la ACL de enrutado, la aplicación de dicha ACL se realiza mediante el comando:

```
NX01#conf t
NX01(config)# interface {level 2 port | level 3 port | SVI VLAN}
Switch(config)# ip access-group <access-list> {in | out}
```

137. Para obtener más información sobre ACL, consulte “Cisco Nexus Series NX-OS Security Configuration Guide”, capítulo “Configuring IP ACLs” [17] [46].

8. MEDIDAS PARA PREVENIR LA CAIDA DEL SISTEMA

138. Muchos ataques de los que sufren los equipos que ocupan posiciones estratégicas en una red tienen como objetivo el provocar que el equipo en cuestión no pueda seguir ofreciendo sus servicios hacia la red. Son los denominados ataques de denegación de servicio (DoS).

139. A continuación, se ofrecen algunas de las vulnerabilidades del sistema que pueden ser utilizadas por los atacantes.

140. El control de flujo en los puertos permite a los puertos que están recibiendo tráfico, pausar la transmisión de paquetes en su origen durante momentos de congestión. Si se activa esta posibilidad, se corre el riesgo de recibir una instrucción de pausa deteniendo la transmisión de paquetes de datos. Por lo tanto, los mensajes de pausa utilizados por este sistema de control de flujo pueden ser utilizadas en un ataque de denegación de servicio. Las direcciones de envío y retransmisión se pueden configurar por separado.

141. Algunos tipos de ataques y ciertos errores también pueden provocar sobrecarga de paquetes (packet floods) en los puertos de un *conmutador*.

142. El servicio Unidirectional Link Detection (UDLD) se utiliza para determinar si existe un link unidireccional entre dos conmutadores, y en ese caso el puerto se desconecta hasta que sea restaurado manualmente. Por lo tanto, los mensajes de UDLD pueden ser usados en ataques de denegación de servicio.

143. Algunas medidas básicas que se pueden aplicar para reducir las posibilidades de sufrir los ataques previamente descritos pueden resumirse en los siguientes párrafos.

144. Mediante el siguiente comando es posible desactivar el control de flujo en cada interfaz Ethernet para evitar que sea susceptible de un ataque:

```
NX01# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
NX01(config)# interface Eth1/1
NX01(config-if)# flowcontrol {send | receive} off
```

145. Otro servicio que se recomienda desactivar es UDLD, el cual puede ser deshabilitado globalmente o en cada interfaz donde no es necesario. En los equipos Cisco Nexus, para poder utilizar comandos relacionados con el UDLD es necesario primero habilitar la función correspondiente, mediante el comando "**feature udld**" [18] [47]. Una vez habilitado Para desactivarlo de forma global es necesario usar la siguiente instrucción:

```
NX01#feature udld
NX01(config)# udld disable
```

146. Para realizar esta desactivación en cada interfaz, se puede utilizar la siguiente instrucción dentro del menú de configuración de ese interfaz:

```
witch(config-if)# udld disable
```

8.1 LIMITACIÓN DEL TRÁFICO DE BROADCAST Y OTROS TIPOS

147. Un elemento de seguridad muy importante es el conocido como Broadcast Storm Control, el cual previene que el tráfico en una LAN se vea alterado por culpa de una "tormenta" broadcast, multicast o unicast por uno de los interfaces físicos. Una tormenta LAN tiene lugar cuando una aglomeración de paquetes inunda la red, creando un tráfico excesivo y disminuyendo la efectividad de la red. Estas inundaciones suelen ser provocadas por una implementación errónea de un protocolo, errores en una configuración de red, o algún usuario llevando a cabo un ataque de denegación de servicio.

148. Este sistema de control basa su funcionamiento en monitorizar los paquetes que pasan por un interfaz, y determina si el paquete es unicast, multicast o broadcast. Entonces el conmutador cuenta el número de paquetes de cada tipo recibidos en un intervalo de 1 segundo, y lo compara con el número límite de este tipo de mensajes establecido por el administrador. Cuando ese límite es superado, el puerto bloquea ese tipo de tráfico, y permanece bloqueado hasta que baja el índice de mensajes de ese tipo por debajo del máximo establecido.

149. Por defecto el Storm Control está desactivado, o lo que es lo mismo, el nivel de supresión está al 100%, con lo cual no se bloquea ninguna cantidad de tráfico. En cambio, un nivel de supresión del 0.0% implicaría que todo el tráfico unicast, multicast y broadcast en ese puerto sería bloqueado.

150. Para configurar este sistema de control es necesario seguir los siguientes pasos desde el nivel de privileged EXEC mode:

```
NX01# configure terminal
NX01(config)# interface <interface-id>
NX01(config-if)# storm-control {broadcast | multicast | unicast } level {level}
```

Las posibles opciones para la configuración del storm-control puden consultarse en Cisco Nexus 9000 Series NX-OS Security Configuration Guide (Configuring Traffic Storm Control) [19] y se destacan:

- *Broadcast/Unicast/Multicast*: Configurar el storm control para broadcast, unicast o multicast.
- *Level*: Permite decidir qué porcentaje de tráfico va a ser el límite establecido. Su rango varía entre 0.00 hasta 100.00 si se mide en el porcentaje de capacidad del puerto, o en pps (*pakects per second*). El tráfico será bloqueado cuando el límite se alcance

151. Se define además la acción a realizar en caso de violación de los parámetros máximos establecidos para el tráfico broadcast, unicast o multicast, que en el caso de los Cisco Nexus es enviar una alarma SNMP:

```
NX01(config-if)# storm-control action {shutdown | trap}
NX01(config-if)# end
```

Se puede verificar el estado del storm control en un determinado interfaz y sobre un determinado tráfico [20]:

```
NX01# show interface counters storm-control <interface-id> [broadcast | multicast | unicast]
```

152. Para poder desactivar este servicio es necesario introducir la siguiente instrucción dentro del menú de configuración del interfaz en que queremos desactivarlo:

```
NX01(config-if)# no storm-control {broadcast | multicast | unicast} level
```

8.2 ARP SPOOFING

153. El ataque conocido como ARP poisoning o ARP spoofing (envenenar o suplantar ARP) es el que un atacante se coloca en el medio (man in the middle) y mediante la suplantación de MAC, enviando mensajes de ARP no solicitados dando la IP del gateway con su propia MAC, con lo que los hosts/servers actualizan su tabla de ARP con este nuevo valor enviando todo el tráfico al atacante, con lo que obtiene el tráfico de otro servidor o dispositivos que luego puede filtrar o espiar o simplemente rechazar de forma transparente para el usuario o dispositivo final.

154. Los conmutadores Nexus 9K/3K pueden usar la característica llamada Dynamic ARP Inspection (DAI, Inspección de ARP dinámica) para ayudar a mitigar este tipo de ataques que consiste en definir interfaces de confianza o no confianza. DAI intercepta, manda logs y rechaza mensajes ARP en las interfaces de NO confianza que no coinciden con las uniones MAC/IP del DHCP snooping. Todo el tráfico que coincida pasa, el que no se descarta.

155. Para configurar Dynamic ARP Inspection en equipos de la gama Nexus, primero debemos habilitar la funcionalidad de DHCP que lo permite, mediante el comando "**feature dhcp**".

```
NX01(config)# feature dhcp
```

156. Para configurar Dynamic ARP Inspection debe habilitarse primero en una o más VLANs con el siguiente comando:

```
NX01(config)# ip arp inspection vlan <vlan-range>
```

157. Con esto se consigue que se intercepten, se registren en logs y descarten paquetes ARP con asociaciones inválidas de MAC-to-IP. Para ello se inspecciona en la base de datos de DHCP snooping o en las tablas de ARP introducidas estáticamente.

158. Por defecto todas las interfaces asociadas a las VLANs configuradas para inspeccionar son consideradas de no confianza, por lo que se inspeccionan. Si se desea que una interface no sea inspeccionada y por lo tanto considerada como de

confianza (enlace contra otro *conmutador*, por ejemplo) se debe configurar la interfaz de la siguiente forma:

```
NX01(config)# interface <interface-id>
NX01(config-if)# ip arp inspection trust
```

159. Para validar que un paquete de respuesta ARP viene de la dirección listada dentro de él, se puede habilitar la validación de Dynamic ARP Inspection con el siguiente comando:

```
NX01(config)# ip arp inspection validate {[src-mac] [dst-mac] [ip]}
```

160. Se debe asegurar de que se especifica al menos una opción:

- *Src-mac*: comprueba la dirección MAC origen en la cabecera Ethernet contra la dirección MAC del emisor (sender) en la respuesta ARP.
- *Dst-mac*: comprueba la dirección MAC destino en la cabecera Ethernet contra la dirección MAC del destino (target) en la respuesta ARP.
- *Ip*: comprueba la dirección Ip del emisor (sender) en todas las peticiones ARP, comprueba la dirección Ip del emisor (sender) contra la dirección destino en todas las respuestas ARP

161. Se debe tener en cuenta los siguientes puntos sobre Dynamic ARP Inspection (DAI):

- SOLO puede actuar en puertos de entrada (ingress ports)
- Soporta puertos de acceso, trunk, Etherchannels e interfaces de VLANs privadas.
- Debería configurarse en todos los puertos de acceso como no confianza (untrusted) y en los puertos que interconectan conmutadores (incluidos routers) de confianza (trusted).

162. Para obtener más información sobre ARP Spoofing, consultar “Cisco Nexus Series NX-OS Security Configuration Guide”, capítulo “Configuring ARP Dynamic Inspection” [21] [48].

8.3 DHCP SNOOPING

163. El DHCP Snooping es una característica de seguridad que provee seguridad filtrando los mensajes DHCP "no confiables" y construyendo y manteniendo una tabla de asociaciones DHCP Snooping.

164. Un mensaje "no confiable" es un mensaje que es recibido desde fuera de la red o del cortafuegos y que puede ser parte de un ataque contra la red.

165. La tabla de asociaciones DHCP Snooping contiene las direcciones MAC, direcciones IP, tiempo de préstamo, tipo de asociación, número de VLAN e interfaz que corresponde a las interfaces locales "no confiables" de un *conmutador*. No contiene sin embargo información de los hosts conectados a una interface "confiable".

166. En términos de seguridad una interfaz "no confiable" es una interfaz que está configurada para recibir mensajes desde fuera de la red local o actúa como parte externa de un cortafuegos. Una interfaz "confiable" es una interfaz configurada para recibir solamente mensajes desde dentro de la propia red.

167. El DHCP Snooping actúa como cortafuegos entre los hosts "no confiables" y los servidores DHCP.

168. También permite contar con una forma de diferenciar entre interfaces "no confiables" conectadas a usuarios finales e interfaces "confiables" conectadas a los servidores DHCP o a otro Conmutador.

169. Es posible configurar DHCP Snooping por Conmutador y por VLANs. Cuando se habilita el DHCP Snooping en un conmutador, una interfaz actúa como un bridge de capa 2 interceptando y salvaguardando los mensajes DHCP que se dirigen a una VLAN de capa 2. Cuando se habilita DHCP Snooping en una VLAN, el Conmutador actúa como un puente de capa 2 dentro del dominio de la VLAN.

170. El DHCP Snooping es necesario para prevenir los ataques de tipo "man-in-the-middle" en las redes internas.

171. Las redes modernas tienen el potencial para que un atacante intente instalar un DHCP Server falso y responder a los mensajes DHCPDISCOVER antes de que lo haga un servidor DHCP legítimo. El DHCP Snooping permite a los Conmutadores en la red "confiar" en el puerto (la interfaz) al que está conectado el servidor DHCP legítimo (podría ser un puerto troncal) y "desconfiar" de los demás puertos.

172. También se mantiene una lista de asociaciones de direcciones DHCP que se logra inspeccionando el tráfico que fluye entre los clientes y el servidor DHCP, el cual provee certeza de quienes son los verdaderos hosts. La información de asociación recolectada por el DHCP Snooping es usada por otras características de seguridad como IPSG y DAI.

173. Los clientes se conectan a puertos "no confiables" (untrusted), todos los puertos son "no confiables" por defecto cuando se habilita el DHCP Snooping. Cuando el PC del cliente envía un mensaje DHCPDISCOVER y el DHCP Snooping está habilitado, el Conmutador solamente va a enviar el mensaje de broadcast DHCP a los puertos "confiables" (trusted).

174. Cuando se configura DHCP Snooping en el Conmutador, se está configurando el Conmutador para diferenciar entre interfaces "no confiables" e interfaces "confiables". Es necesario habilitar globalmente el DHCP Snooping antes de poder usarlo en una VLAN. Es necesario habilitar el DHCP Snooping independientemente de otras características de DHCP.

175. Para habilitar DHCP Snooping puede usar esos comandos, dependiendo si queremos activarlo globalmente o en algunas VLANs en concreto:

```
NX01(config)# ip dhcp snooping
NX01(config)# ip dhcp snooping vlan number [number] | vlan {vlan range}]
```

176. Es posible también habilitar la verificación de la dirección MAC en el paquete de solicitud de DHCP, de modo que se rechace el paquete en caso de que la dirección MAC del dispositivo que genera la petición, y la MAC incluida dentro de la petición no coincidan:

```
NX01 (config-if)#  ip dhcp snooping verify mac-address
```

9. VLANS

177. Se puede definir una VLAN o Virtual Local Area Network como un dominio de difusión, o lo que es lo mismo, todos los miembros pertenecientes a una VLAN reciben los paquetes de *broadcast* de los otros miembros de su VLAN, pero no de los pertenecientes a otras VLANs.

178. Su mayor beneficio y lo que las diferencia de las LANs tradicionales es que las agrupaciones de equipos y la creación de subredes se va a implementar de forma lógica y, por lo tanto, la pertenencia a una VLAN no depende de la ubicación física del equipo. Es por esto que las labores de administración de las LANs se facilitan enormemente gracias a las VLANs, ya que para modificar la pertenencia de equipos a las distintas subredes no se va a necesitar de un desplazamiento físico de los mismos.

9.1 CREACIÓN DE VLANS COMO MEDIDA DE AISLAMIENTO

179. A nivel de seguridad, las VLANs van a permitir crear distintos dominios de difusión donde no influya la situación física del equipo, sino el grupo al que haya sido asignado. Por lo tanto, vamos a poder definir LANs que sólo contengan ciertos equipos críticos y los equipos que los gestionan sin que estos tengan que estar situados físicamente juntos, y al mismo tiempo limitan el número de equipos que tienen acceso a estos. Por lo tanto, es posible crear una capa de seguridad alrededor del entorno de gestión.

180. Además, esta capacidad de crear subredes a las cuales solo pueden acceder los equipos que nosotros designemos puede ser aplicada para proteger el propio conmutador. Las VLANs en nuestro conmutador pueden ser definidas de forma que podamos crear los distintos dominios de difusión agrupando distintos puertos del conmutador. Pero como toda implementación que llevemos a cabo en los equipos, si no se hace la manera adecuada podemos estar creando nuevas debilidades en vez de incrementando la seguridad. En el caso de las VLANs en la configuración por defecto que tienen los equipos de Cisco, siempre aparece una VLAN inicial creada como VLAN 1 y en la cual están asignados todos los puertos incluidos los puertos de gestión, por lo cual la primera acción recomendable de llevar a cabo sería la creación de una nueva VLAN que mantenga los puertos de configuración fuera de las subredes a las que accedan los usuarios no administradores. Mediante este sistema hemos se consigue incrementar la seguridad de gestión del propio conmutador.

181. Otra recomendación de seguridad es la de establecer una VLAN en la cual agrupemos todos los puertos inactivos y aislar éstos de cualquier VLAN que contenga puertos activos. Por lo tanto, es una buena política la de asignar de inicio todos los puertos a una VLAN distinta a la creada por defecto por el conmutador, para que luego se vayan sacando de ese grupo y siendo asignados a las VLAN a las que pertenecerán, de esta forma nunca se utilizará la VLAN por defecto lo que se mejora la seguridad del entorno.

182. A continuación, los pasos que hay que seguir para realizar la configuración de las VLANs siempre usando un usuario con permisos o rol de administrador:

```
NX01# configure terminal
NX01(config)# vlan <vlan-id>
```

183. Donde *vlan-id* puede ser un id no usado hasta el momento para definir una nueva VLAN o bien el id de una VLAN ya definida para poder modificarla. El identificador se compone de un número entre los valores 1 a 4094, siendo desde la 1006 a la 4094 consideradas Extended Range VLANs cuyo funcionamiento es ligeramente distinto al de las VLANs habituales. Es recomendable analizar esas diferencias antes de implementar una Extended VLAN, por ejemplo, no se guardan en la base de datos de las VLANs, y tienen un conjunto de opciones de configuración más limitado que el de las VLANs normales.

184. Un comando opcional permite darle un nombre a la VLAN que nos facilite la gestión de las mismas. De no introducirse ninguno el nombre de la VLAN pasará a ser VLAN seguido de cuatro dígitos, que se obtienen de preceder el vlan-id de los ceros necesarios para que la cifra tenga 4 dígitos, es decir, para la VLAN 2 su nombre sería VLAN0002:

```
NX01(config-vlan)# name <vlan-name>
```

185. Una vez creada la VLAN es necesario configurar los puertos que se deseen incorporar a esta VLAN:

```
NX01# configure terminal
NX01(config)# interface <interface-id>
NX01(config-if)# switchport port mode access
NX01(config-if)# switchport access vlan <vlan-id>
NX01(config-if)# end
NX01# show running-config interface <interface-id>
NX01# copy running-config startup-config
```

186. Con estos dos bloques de instrucciones ya es posible crear una VLAN y asignar los diversos puertos a las distintas VLAN que se creen en el conmutador. La utilización de macros y la posibilidad de usar rangos de interfaces, puede ser decisiva para agilizar el proceso de configuración de las VLANs.

```
NX01(config)# interface eth1/1-3
NX01(config-if-range)#
```

9.2 VLAN TRUNKS

187. Si se ha realizado la definición de las VLAN basándose en puertos, a la hora de definir una VLAN que se distribuya más allá de un solo conmutador es necesario asignar a esa VLAN un puerto en cada uno de los conmutadores que se van a unir, para que

el enlace también pertenezca a la VLAN y los mensajes de broadcast se extiendan por él.

188. Para conseguir tal funcionalidad, es necesario configurar VLAN Trunks, que permiten interconectar VLANs de distintos conmutadores sin emplear tantos puertos. Las VLAN Trunks permiten limitar el empleo de recursos usando identificadores en los paquetes que se envían. Estos identificadores sirven para determinar a qué VLAN pertenecen y gracias a ello es posible usar sólo un enlace entre conmutadores. Una vulnerabilidad clara de este sistema es que de ser usado en puertos cuyo acceso físico no esté limitado, una persona ajena al equipo de mantenimiento de la red podría conectarse a él y presentándose como otro conmutador podría configurar un enlace contra el puerto, por lo que podría recibir los mensajes de todas las VLANs. Por lo tanto, es recomendable implementarlo, pero sólo en los puertos a los cuales el acceso físico este controlado y en los puertos que se usen para interconectar con otros conmutadores.

189. Para configurar un puerto en Trunk son necesarios los siguientes comandos, que permita las VLANs especificadas:

```
NX01# configure terminal
NX01(config)# interface <interface-id>
NX01(config-if)# switchport port mode trunk
NX01(config-if)# switchport trunk vlan <vlans-id>
NX01(config-if)# end
NX01# show running-config interface interface-id
NX01# copy running-config startup-config
```

10.SERVIDOR AAA

10.1 AUTENTICACIÓN REMOTA

190. El producto puede ser configurado para utilizar autenticación local o autenticación con servidores externos de autenticación RADIUS o TATACS+. En este caso la comunicación irá protegida con SSHv2 o IPsec.

191. Se recomienda consultar "Cisco Nexus 9000 Series NX-OS Security Configuration Guide", sección "Configuring TACACS+" [22] [49] para familiarizarse con los conceptos relativos a autenticación remota. También se puede consultar comandos específicos en la sección "Configuring RADIUS" [23] [50] para la configuración de RADIUS.

10.2 SERVIDOR DE AUTENTICACIÓN

192. RADIUS se puede utilizar para la autenticación de los administradores privilegiados del dispositivo. Está desactivado por defecto, pero puede ser activado por administradores. Es importante implementar buenas prácticas para la selección y protección de la clave, asegurando que la clave no es fácilmente adivinable ni compartida con usuarios desautorizados.

193. Para más información acerca de cómo configurar RADIUS, consultar "Cisco Nexus 9000 Series NX-OS Security Configuration Guide", sección "Configuring RADIUS" de [23] [50]. Es recomendable leer las secciones referenciadas para familiarizarse con los conceptos de autenticación remota antes de proceder a la configuración.

10.3 CONFIGURAR SERVIDORES RADIUS AAA EXTERNOS

194. Para configurar un servidor RADIUS como servidor AAA externo, se deben seguir los siguientes pasos.

195. La primera parte de la configuración hace referencia a la creación de un host como servidor RADIUS remoto mediante el comando "**radius-server host**", y la configuración de un grupo de servidores de AAA como de tipo RADIUS, mediante el comando "**aaa group server radius <Id>**". Se usará el servidor de AAA tanto como servidor de autenticación (*authentication*) como servidor de registro de eventos (*accounting*).

```
NX01#configure terminal
NX01(config)# radius-server host 10.0.0.3 key 7 "qabzk01" authentication accounting
NX01(config)# aaa group server radius RadServer
NX01(config-radius)# server 10.0.0.3
NX01(config-radius)#use-vrf management
```

196. Cabe mencionar que la configuración de clave (pair secret) entre ambos dispositivos (Nexus y servidor de AAA) queda cifrada en la configuración, pero se transmite en abierto en la conexión con el servidor de AAA, por lo que es necesaria una capa adicional de seguridad para esta conexión. Tal y como se ha comentado en otros apartados, la unidad NXOS no puede actuar como terminador de túneles IPSec, por lo que se deberá usar un tercer equipo para el establecimiento del túnel. Igualmente es necesario destacar que es necesario indicar el VRF que se va a utilizar para la comunicación ("**use-vrf <VRF_ID>**"), de modo que el equipo saque los paquetes de AAA mediante el enrutamiento correcto.

197. Una vez configurado esos valores, ya es posible definir los usuarios remotos en el servidor RADIUS correspondiente. Debe prestarse especial atención al uso del atributo RADIUS "cisco av-pair" dado que en dicho atributo, devuelto por el servidor AAA, se indica el rol del usuario que se va a autenticar. Para que el usuario remoto disponga de privilegios de "network-admin" y "vdc-admin", el valor del atributo debería ser el siguiente:

```
Cisco-AVPair = "shell:roles*\"network-admin vdc-admin\""
```

198. Con el usuario y su rol definido en el servidor de AAA, es posible hacer un test de autenticación usando el comando "**test aaa server radius**".

```
NX01# test aaa server radius 10.0.0.3 vrf management testnx testnx
user has been authenticated
```

199. Desde el punto de vista del servidor RADIUS:

```
(3) Sent Access-Accept Id 24 from 10.0.0.3:1812 to 10.0.0.1:59407 length 71
(3)   Service-Type = NAS-Prompt-User
(3)   Cisco-AVPair = "shell:roles*\"network-admin vdc-admin\""
```

200. A partir de este momento, ya es posible crear como método de autenticación por defecto el nuevo grupo RADIUS creado, que será el primero que se consulte cuando se haga un proceso de autenticación contra el equipo. De manera nativa, se produce un proceso de fallback a la autenticación local en caso de que el servidor de AAA no esté disponible.

```
login as: admin
Pre-authentication banner message from server:
| User Access Verification
End of banner message from server
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
Remote AAA servers unreachable; local authentication done
```

11.FASE DE OPERACIÓN

201. Durante la fase de operación de los dispositivos Nexus 9K/3K Series, los administradores privilegiados deberán llevar a cabo las siguientes tareas de mantenimiento:

- Mantenimiento del control de acceso al dispositivo. De forma que el personal designado pueda acceder con el rol de usuario asignado.
- Comprobaciones periódicas del hardware y software para asegurar que no se ha introducido hardware o software no autorizado.
- Verificaciones periódicas del sistema operativo NX-OS y su integridad, para comprobar que está libre de software malicioso.
- Aplicación regular de los parches de seguridad, con el objetivo de mantener una configuración segura.
- Mantenimiento de los registros de auditoría. Estos registros estarán protegidos de borrados y modificaciones no autorizadas, y solamente el personal de seguridad autorizado podrá acceder a ellos.
- La información de auditoria se guardará en las condiciones y por el periodo establecido en la normativa de seguridad.
- Auditar, al menos, los eventos especificados en la normativa de referencia y aquellos otros extraídos del análisis de riesgos.

12.AUDITORÍA

202. El dispositivo es capaz de generar registros de auditoría que son almacenados internamente dentro del dispositivo cuando un evento de auditoría sucede, así como descargarlo a un servidor syslog externo de manera simultánea.

203. El administrador puede establecer el nivel de registros de auditoría almacenados en un buffer local, mostrados en la consola, enviados al servidor syslog o todo lo anterior.

204. El búfer de registro local es circular. Los mensajes más nuevos sobrescriben los mensajes más antiguos una vez que el búfer está lleno. Los administradores deben supervisar el búfer de registro empleando el comando de EXEC privilegiado show logging para visualizar los registros de auditoría. El primer mensaje mostrado es el más antiguo en el búfer.

205. Cuando esté configurada una copia de seguridad en syslog el dispositivo descargará de manera simultánea eventos desde un búfer separado al servidor externo de syslog. Este búfer se emplea para poner eventos en cola para ser enviados al servidor syslog si la conexión con el servidor se pierde. Es un búfer circular, de manera que cuando los eventos sobrepasan el espacio de almacenamiento los eventos más antiguos son sobrescritos.

12.1 REGISTROS DE EVENTOS

206. Los dispositivos Nexus 9K/3K Series pueden ser configurados para generar registros de auditoría cuando ocurra algún evento auditable. Los tipos de eventos que pueden ser auditados incluyen eventos de aplicación de políticas de flujo de información, identificación, autenticación y administrativos. Cada uno de los eventos es registrado con suficiente detalle como para identificar el usuario al cual está asociado el evento (identidad de usuario, dirección MAC, dirección IP), cuándo sucedió el evento, dónde sucedió, el resultado del evento y a qué tipo de evento pertenece.

207. Adicionalmente, el inicio y apagado genera también un evento para indicar que está operativo o que todos los procesos han sido terminados. Se puede encontrar una lista completa de todos los eventos de auditoría disponibles para los productos Nexus 9K/3K en “Cisco Nexus 9000 Series NX-OS System Management Configuration Guide”, apartado “Configuring System Message Logging” [24] [51].

208. Cada ocasión en la que un usuario con permisos de administración se registra en el sistema, se genera un evento de auditoría, que contiene: día de la semana, fecha, acción, identificación de usuario e información del terminal usado para acceder (si aplica). Los mismos datos se guardan cada vez que un usuario realiza un cambio en la configuración del sistema.

209. Cuando el registro del evento es en modo local, el dispositivo sobrescribe el último registro cuando el registro de eventos está lleno. El tamaño del registro de eventos

puede ser modificado por el administrador, con un valor por defecto (y máximo) de 4194304 bytes, y uno mínimo de 4096 bytes.

210. Solo los usuarios con permisos de administración están autorizados a acceder al registro de eventos de auditoría. No existe ningún interfaz que permita realizad modificaciones al registro de eventos de auditoría, salvo por el hecho de realizar una purga de los mismos para liberar espacio.

211. Los registros de eventos se pueden configurar de manera individual para cada uno de los destinos de los mensajes de eventos, indicando si están habilitados o no, y el nivel de severidad configurado para cada uno de ellos. Para mostrar el estado actual, se usa el comando "*show logging*", para cambiar cualquiera de los destinos, el comando *"logging <destino> <severidad>".*

```
NX01# show logging
Logging console:            enabled (Severity: critical)
Logging monitor:            enabled (Severity: notifications)
Logging linecard:           enabled (Severity: notifications)
Logging timestamp:          Seconds
Logging source-interface :     disabled
Logging rate-limit:         enabled
Logging server:             disabled
Logging origin_id :         disabled
Logging RFC :               disabled
Logging logflash:           enabled (Severity: information)(threshold percentage: 0)
Logging logfile:            disabled
….
NX01# logging <console | monitor | server> <severity>
NX01# logging onsole 3
```

212. También, y con el fin evitar la pérdida de datos de auditoria si falla el conmutador, los registros de eventos deben guardarse en la memoria flash utilizando el comando "logging logfile":

```
NX01#logging logfile <nombre_fichero> <severidad>
NX01#logging logfile test.log 6
NX01#show logging
….
Logging logfile:            enabled
      Name - test.log: Severity - information Size - 4194304
```

213. Así mismo, se pueden habilitar eventos de sistema para cada uno de los subsistemas (Facilities) del equipo, con su correspondiente nivel de severidad. Para cambiar el nivel de severidad para cada subsistema, se usa el comando "**logging level <facility> <severidad>**".

```
NX01# sho logging
……
Facility      Default Severity      Current Session Severity
--------      ----------------      ------------------------
aaa                3                3
acllog             2                2
aclmgr             3                3
aclqos             5                5
adbm               2                2
arp                3                3
auth               0                0
authpriv           3                3
bootvar            5                5
callhome           2                2
capability         2                2
cdp                2                2
cert_enroll        2                2
cfs                3                3
clis               3                3
clk_mgr            2                2
confcheck          2                2
copp               2                2
core-dmon          3                3
cron               3                3
……
NX01# logging level aaa 2
NX01# show logging
….
Facility      Default Severity      Current Session Severity
--------      ----------------      ------------------------
aaa                3                2
```

214. Las marcas de tiempo (timestamps) en el registro de eventos están habilitadas por defecto, y únicamente es posible cambiar su unidad temporal:

```
NX01(config)# logging timestamp ?
  microseconds  Timestamp in micro-seconds
  milliseconds  Timestamp in milli-seconds
  seconds       Timestamp in seconds (Default)
```

12.2 ALMACENAMIENTO LOCAL

12.2.1 BORRANDO REGISTROS DE AUDITORÍA

215. El dispositivo provee a los administradores privilegiados la funcionalidad de borrar los registros de auditoría almacenados en el dispositivo mediante el comando "**clear logging**".

216. Para obtener más información, consulte el apartado"Clear Logging" de "Cisco Nexus 9000 Series NX-OS System Management Configuration Guide" [24] [51].

12.2.2 REVISIÓN DE REGISTROS DE AUDITORÍA

217. Los dispositivos Nexus 9K/3K Series mantiene registros en múltiples localizaciones: almacenamiento local de los registros de auditoría generados, y la descarga simultanea de esos eventos en el servidor externo de syslog. Para la visión completa de los eventos auditados, en todos los dispositivos, y para visualizar y revisar los eventos auditables los administradores deben revisar el registro de auditoría de manera regular.

218. Mediante la línea de comandos (CLI) de los dispositivos de las Series Nexus 9K/3K, los administradores privilegiados pueden revisar los eventos auditados. La información provista en los registros de auditoría incluye la fecha y hora del evento, el tipo de evento, identificación del sujeto (si aplica), el detalle del evento e información adicional relacionada con el propio evento.

219. Para revisar los registros de auditoría almacenados localmente, se debe utilizar el comando "**show logging**".

220. Los mensajes de log del sistema pueden contener hasta 80 caracteres y un signo de porcentaje (%), que sigue el número de secuencia opcional o la información de fecha y hora. La parte del mensaje que precede al símbolo de porcentaje depende de los ajustes del comando de configuración global del servicio. La siguiente información es la información básica que se incluye en un registro de auditoría.

- ***Element***: Descripción.
- ***Sequence no***: Imprime mensajes de log con un número de secuencia solo si el comando de configuración global del servicio sequence-numbers está configurado.
- Formato de ***timestamp***:

- Mm/dd hh:mm:ss (short uptime) o d h (long uptime).
- Fecha y hora del mensaje o evento. Esta información aparece solo si el comando de configuración global del servicio timestamps log [datetime | log] está configurado.

- ***Facility***: Servicio al cual se refiere el mensaje (por ejemplo, SNMP, SYS, etc.).
- ***Severity***: Código de un solo dígito del 0 al 7 que indica la severidad del mensaje.
- ***MNEMONIC:*** Cadena de texto que describe el mensaje inequívocamente.
- ***Description***: Cadena de texto que contiene información detallada sobre el evento que se está reportando.
- ***Hostname-n***: Nombre de host del miembro del stack de conmutadores y el número de conmutador en la pila. Aunque el maestro de la pila también es un miembro, no adjunta su nombre de host a los mensajes del sistema.

En "Cisco Nexus 9000 Series NX-OS System Messages Reference" [25], y "Cisco Nexus 3000 Series NX-OS System Messages Reference" [52] y "Cisco NX-OS System Routing Messages Reference" [26] pueden encontrarse mensajes de registros de auditoría para eventos del sistema y de routing.

12.3 ALMACENAMIENTO REMOTO

221. El procedimiento para habilitar el almacenamiento remoto de los registros de auditoría puede consultarse en "Cisco Nexus 9000 Series NX-OS System Management Configuration Guide (Configuring System Message Logging)" [24] [51]. Se recomienda leer la sección entera para familiarizarse con los conceptos y parámetros de configuración antes de configurar el registro remoto.

222. Para evitar la pérdida de datos de auditoría, el dispositivo debe configurarse para enviar registros a un servidor syslog externo. Por ejemplo, todas las emergencias, alertas, errores y mensajes de precaución pueden enviarse a la consola para avisar al administrador de que deben tomarse las acciones pertinentes puesto que estos mensajes indican que la funcionalidad del conmutador está afectada. Todas las notificaciones y mensajes de información pueden enviarse al servidor syslog, aunque estos no afecten a la funcionalidad del conmutador.

223. La conectividad con el servidor syslog debe protegerse mediante algún tipo de método de cifrado, como podría ser TLS o un túnel IPsec. Sin dichos sistemas, no se puede garantizar que la conexión entre ambos extremos sea confidencial, así como tampoco la integridad de los datos transportados.

224. Para establecer el envío de mensajes un servidor remoto seguro syslog mediante TLS debe ejecutarse el siguiente comando:

```
NX01# logging server <hostname> secure trustpoint client-identity <trustpoint_id>
{facility | use-vrf}
```

225. Si se va a usar un sistema seguro de Syslog basado en TLS, los condicionantes son los siguientes:

- Para los propósitos de cifrado de la capa de transporte y de autenticación mutua, NXOS soporta TLSv1.2.
- Es necesario disponer de un punto de confianza (*trustpoint*) previamente configurado que sea aceptado tanto por el dispositivo NXOS como por el servidor remoto de syslog. Este punto de confianza se implementa mediante los comandos "**crypto ca trustpoint**" and "**crypto ca authenticate**", ya comentado en el apartado **6.5.1.1**.
- El parámetro <hostname> debe permitir la resolución DNS del servidor de syslog, con el fin de permitir la correcta verificación de los certificados. La verificación se realiza contra el SAN del servidor de syslog (en caso de que el servidor administre varios certificados), o contra su CN si el SAN no está presente.
- Se recomienda el uso de un servidor de syslog seguro que soporte el estándar RFC 5425 (Transport Layer Security Transport Mapping for Syslog), y los mensajes usarán el puerto TCP 6514.

226. Cuando la conexión con el servidor remoto syslog esté caída (porque el túnel IPsec esté caído, o el servidor de syslog no disponible), el dispositivo Nexus 9K/3K Series continuará registrando mensajes en el búfer local.

13. BACKUP Y ACTUALIZACIÓN

13.1 BACKUP

227. El proceso de copia de seguridad de un dispositivo Nexus 9K/3K Series consiste en la copia de los ficheros de configuración en una localización alternativa.

228. Para mostrar el contenido del fichero de configuración en ejecución del dispositivo debe ejecutarse el siguiente comando:

```
Switch# show running-config
```

229. Para mostrar el contenido del fichero de configuración de arranque del dispositivo debe ejecutarse el siguiente comando:

```
Switch# show startup-config
```

230. Por defecto, el fichero de configuración de arranque del dispositivo es almacenado en NVRAM.

231. Como precaución, y debido a que pueden surgir problemas de operación, es recomendable guardar una copia de la configuración en la propia memoria flash del dispositivo. Basta aplicar los comandos que se muestran a continuación para salvar tanto la configuración en ejecución, como la configuración de arranque.

```
Switch# copy {running-config | startup-config} bootflash:nombre-nexus-config.bak
Copy complete, now saving to disk (please wait)…
Copy complete
```

232. Además de esto, se recomienda guardar la configuración en al menos un dispositivo externo (servidor o memoria USB). En el siguiente ejemplo se muestra cómo guardar la configuración en un servidor TFTP.

```
Switch# copy {running-config | startup-config} tftp://IP_server/nombre-nexus-config.bak
Enter vrf (if no input, current vrf 'default' is considered): management
Trying to connect to tftp server….
Connection to Server Established
TFTP put operation was successful
Copy complete, now saving to disk (please wait)…
Copy complete.
```

233. La información acerca de la configuración de copia de seguridad de la configuración de los dispositivos Nexus 9K/3K Series puede consultarse en la sección "Managing Configuration Files" en "Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide " [27] [54].

13.2 ACTUALIZACIONES Y COMPROBACIONES DE *FIRMWARE*

234. El proceso de actualización de la unidad siempre comienza con la descarga de la nueva versión a implementar. Para comprobar que el *software* no ha sido manipulado en ningún momento, se recomienda el procedimiento siguiente:

- Descargar la imagen a instalar en el dispositivo directamente del sitio oficial de Cisco (http://www.cisco.com/cisco/web/download/index.html) y almacenarla en un equipo confiable. La razón para descargar la imagen en un sistema confiable tiene como objetivo garantizar que la imagen no es manipulada antes de su instalación.
- A continuación, se deberá copiar el fichero de actualización mediante las opciones disponibles:
  - FTP
  - TFTP
  - SCP
  - SFTP
- En el siguiente ejemplo, se muestra la copia de la imagen 9.3.9 mediante FTP

```
Switch# copy ftp://IP_Server_FTP/nxos.9.3.9.bin bootflash:nxos.9.3.9.bin
Enter vrf (If no input, current vrf 'default' is considered):
Enter username: ****
Password: *****
***** Transfer of file Completed Successfully *****
Copy complete, now saving to disk (please wait)...
Copy complete
```

- Seguidamente, y tras varios procesos de transferencia del fichero, se recomienda comprobar la integridad del fichero recientemente copiado para detectar si está incompleto o corrupto. Para ello, se puede consultar la suma de comprobación con algoritmos Hash SHA-256)., como se muestra a continuación según Cisco Nexus NX-OS Software Upgrade and Downgrade Guide [28] [55]:

```
Switch# show file bootflash:nxos.9.3.9.bin sha256sum
1ad837ee51090d2b94568f7c2d7aa9dabd88b139d16ddf276187059d730e5049
```

- Estos resultados deben coincidir con los mostrados en la web de descarga de Cisco.
- El software ha sido firmado digitalmente, y la verificación de la imagen se hace con el hash SHA-256 o SHA-512. Una vez la imagen se haya cargado en la memoria flash, para mostrar la información relacionada con la autenticidad del software para cada imagen específica, deberá utilizarse el comando en modo privilegiado "***show software authenticity file [image_filename]***".

Este comando permite mostrar la información relacionada con la autenticación del software, que comprende información de credenciales de la imagen, tipo de clave usado para la verificación, información de la cabecera, y otros atributos de la firma, específicamente para cada imagen. El comando extraerá la cabecera de la firma y sus campos a partir del archivo de la imagen, y volcará la información necesaria.

```
# show software authenticity file {bootflash0:filename | bootflash1:filename | bootflash:filename | nvram:filename | usbflash0:filename | usbflash1:filename}.

NX01# show software authenticity file bootflash:nxos.9.3.9.bin

/bootflash/nxos.9.3.9.bin

Image type                : Release

  Signer Information

    Common Name          : CiscoSystems

    Organization Unit    : Nexus9k

    Organization Name    : CiscoSystems

  Certificate Serial Number : 61FCEB28

  Hash Algorithm          : SHA512

  Signature Algorithm     : 2048-bit RSA

  Key Version             : A
```

- Si se confirma que la imagen no ha sufrido alteraciones durante el proceso, el siguiente paso es comprobar si existe algún tipo de incompatibilidad con el sistema. En primer lugar, se puede comprobar incompatibilidad con la configuración actual de la siguiente manera:

```
Switch# show incompatibility-all nxos bootflash:nxos.9.3.9.bin

Enter Checking incompatible configuration(s) for vdc 'NX01':

No incompatible configurations

Checking dynamic incompatibilities:

No incompatible configurations
```

- El siguiente paso es comprobar si existe algún tipo de incompatibilidad hardware, de la siguiente forma:

```
Switch# show install all impact nxos bootflash:nxos.9.3.9.bin

Installer will perform impact only check. Please wait.

Verifying image bootflash:/nxos.9.3.9.bin for boot variable "nxos".

[####################] 100% -- SUCCESS

Verifying image type.

[####################] 100% -- SUCCESS
```

```
Preparing "nxos" version info using image bootflash:/nxos.9.3.9.bin.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.3.9.bin.
[####################] 100% -- SUCCESS

Performing module support checks.
[####################] 100% -- SUCCESS

Notifying services about system upgrade.
[####################] 100% -- SUCCESS

Compatibility check is done:
Module  bootable        Impact  Install-type  Reason
------  --------  --------------  ------------  ------
1       yes     disruptive        reset  default upgrade is not hitless

Images will be upgraded according to following table:
Module     Image             Running-Version(pri:alt)        New-Version  Upg-Required
------  ----------  ----------------------------------------  --------------------  ------------
1       nxos                          9.3(8)            9.3(9)         yes
1       bios    v05.45(07/05/2021):v05.45(07/05/2021)   v05.45(07/05/2021)         no
```

- Si el resultado de incompatibilidades es positivo se deberá revisar y deshabilitar las *features* o módulos que sean incompatibles con la versión deseada a instalar. En caso de que el resultado de incompatibilidades sea negativo, se está en condiciones idóneas de realizar la instalación. Para realizarla, se debe emplear el siguiente comando:

```
Switch# install all nxos bootflash:nxos.9.3.9.bin
Installer will perform impact only check. Please wait.
Installer is forced disruptive
Verifying image bootflash:/nxos.9.3.9.bin for boot variable "nxos".
[####################] 100% -- SUCCESS
Verifying image type.
[####################] 100% -- SUCCESS
```

Preparing "nxos" version info using image bootflash:/nxos.9.3.9.bin.

[####################] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.3.9.bin.

[####################] 100% -- SUCCESS

Performing module support checks.

[####################] 100% -- SUCCESS

Notifying services about system upgrade.

[####################] 100% -- SUCCESS

Compatibility check is done:

Module bootable Impact Install-type Reason

------ -------- -------------- ------------ ------

1 yes disruptive reset default upgrade is not hitless

Images will be upgraded according to following table:

Module Image Running-Version(pri:alt) New-Version Upg-Required

------ ---------- -- -------------------- ------------

1 nxos 9.3(8) 9.3(9) yes

1 bios v05.45(07/05/2021):v05.45(07/05/2021) v05.45(07/05/2021) no

Switch will be reload for disruptive upgrade.

Do you want to continue with the installation (y/n)? [n] **y**

Install is in progress, please wait.

Performing runtime checks.

[####################] 100% -- SUCCESS

Setting boot variables.

[####################] 100% -- SUCCESS

Performing configuration copy.

[####################] 100% -- SUCCESS

Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.

Warning: please do not remove or power off the module at this time.

[####################] 100% -- SUCCESS

2022 Jun 29 12:31:03 NX01 %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE: Successfully deactivated virtual service 'guestshell+'

```
Finishing the upgrade, switch will reboot in 10 seconds.
```

- Una vez que el equipo se reinicia y arranca con la imagen recientemente instalada, se debe verificar que la versión que está ejecutando la unidad es la deseada. Para verificar la imagen en ejecución, ejecutar el comando “show version”.

```
Switch# show version
<-- Salida omitida -->
Software
  BIOS: version 05.45
 NXOS: version 9.3(9)
  BIOS compile time:  07/05/2021
  NXOS image file is: bootflash:///nxos.9.3.9.bin
  NXOS compile time:  2/4/2022 7:00:00 [02/04/2022 10:54:27]
```

235. Si se desea comprobar la información de validación de la imagen que está corriendo, el comando “show software authenticity” también permite validar información relacionada con la autenticación del software (ya visto en el anterior punto).

```
NX01# show software authenticity file running
NXOS IMAGE
-----------------------
Image type                : Release
   Signer Information
      Common Name         : CiscoSystems
      Organization Unit   : Nexus9k
      Organization Name   : CiscoSystems
   Certificate Serial Number : 61FCEB28
   Hash Algorithm          : SHA512
   Signature Algorithm     : 2048-bit RSA
   Key Version             : A
   Verifier Information
      Verifier Name       : BIOS
      Verifier Version    : 05.45
```

236. Para comprobar la clave pública empleada para la firma digital de la imagen, el comando “show software certificate” permite la impresión de la clave pública usada para la firma de la imagen en funcionamiento (indicada como “Key Version: A” en el comando anterior).

```
NX01# show software authenticity keys
Public Key #1 Information
-------------------------
Key Type            : Release  (PRIMARY KEY STORAGE)
Public Key Algorithm : RSA
Modulus (256 bytes)   :
     c6:64:53:69:18:a5:9d:1b:94:9b:fb:b3:6e:f0:c4:9f:
     ca:bc:60:2b:52:c5:f8:97:bb:dc:e0:af:82:df:a0:76:
     6a:bb:04:27:07:a8:47:81:25:34:8b:b6:3c:15:be:1d:
     a1:24:71:03:f1:26:8d:c4:14:80:eb:e0:b3:60:3d:cb:
     5c:f6:c2:18:08:8f:3a:a8:64:f2:08:8a:04:b2:e7:35:
     46:88:f1:24:ea:c0:d3:65:e6:3e:81:cd:65:62:41:dd:
     d7:e0:76:6c:a5:69:33:4d:05:af:ab:30:75:8b:09:b0:
     73:40:df:dc:22:b7:d9:e0:68:50:55:4f:91:15:7f:01:
     84:d8:d0:e7:53:1f:7e:a2:30:dd:6b:29:13:7c:ca:cb:
     ef:dc:76:ce:fa:22:87:cc:af:a1:ff:c6:f3:a9:6b:71:
     9f:d7:2e:e3:bc:85:13:24:10:d7:ae:5f:db:1b:7a:24:
     05:77:69:96:e3:38:cd:d8:1d:de:4a:b2:37:1a:30:23:
     7f:a1:51:7d:95:13:7c:cd:fb:6f:9f:1b:c2:79:8a:75:
     b2:39:79:e3:68:b0:f2:c0:13:c0:f2:b5:94:49:69:30:
     78:7d:6b:76:85:a5:94:8b:1b:94:62:a8:4e:2a:b2:7a:
     42:ae:a4:64:af:86:60:9e:b1:38:c3:72:71:6a:01:87
Exponent (4 bytes)   : 10001
Key Version          : A
Product Name         : Nexus9k
```

237. Si una actualización de software falla, Nexus 9K/3K Series muestra un evento de error cuando un administrador privilegiado trate de iniciar el sistema. Después, se inicia el terminal en modo *bootloader*:

```
FPGA SPI Flash Winbond W25Q128BV
Board type  4
IOFPGA @ 0xd8000000
SLOT_ID @ 0xf
Set fan speed to 100%
Aborting config file read and autoboot
No autoboot or failed autoboot. falling to loader



               Loader Version 5.45

loader > ?
?           Print the command list
boot        Boot image
bootmode    Display/Change current boot mode
dir         List file contents on a device
eobc        Booting image from active sup via EOBC channel
help        Print the command list or the specific command usage
ip          Setting IP address or gateway address
keyinfo     BIOS KEY information
reboot      Reboot the system
serial      Serial console setting
set         Set network configuration
show        Show loader configuration

loader >
```

Ilustración 10. Ejemplo de arranque fallido tras actualización

238. El siguiente paso sería comprobar si existe una imagen válida de arranque por parte del *bootloader*, y lanzar la carga de dicha imagen:

```
XOS

loader > dir
Setting listing for bootflash:
Number of devices detected by BIOS is 1
Number of devices detected by BIOS is 1
Number of devices detected by BIOS is 1
Going to print files for device bootflash: 1
 .rpmstore
 nxos.9.2.1.bin
 bootflash_sync_list
 .swtam
 virtual-instance
 virtual-instance.conf
 virt_strg_pool_bf_vdc_1
 scripts
 20181128_110337_poap_30876_init.log
 20181128_110337_poap_30876_1.log
 platform-sdk.cmd
Number of devices detected by BIOS is 1
Number of devices detected by BIOS is 1
Number of devices detected by BIOS is 1
Clearing listing for bootflash:

loader > boot nxos.9.2.1.bin
```

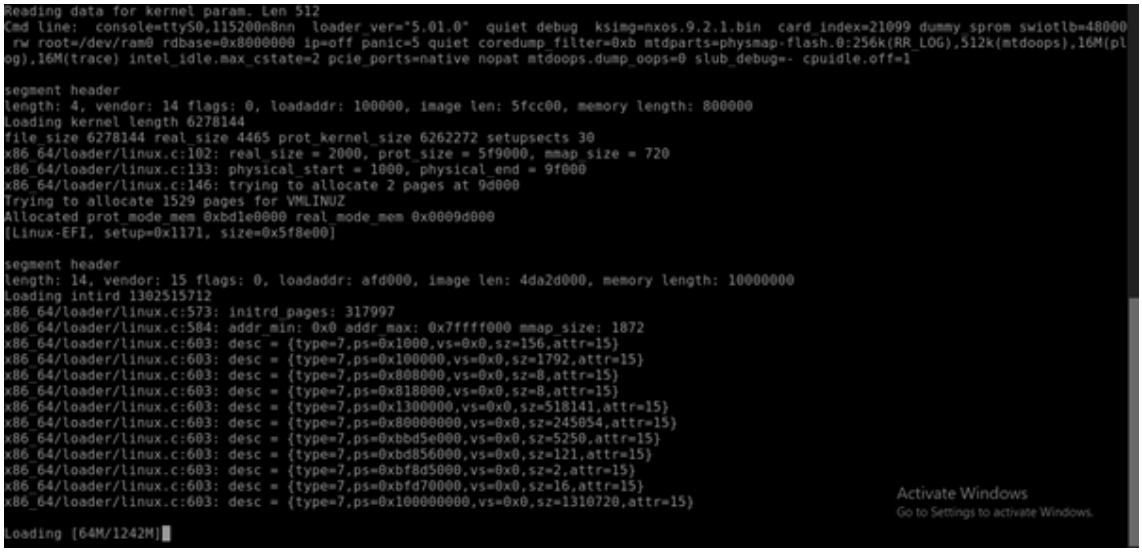

Ilustración 11. Ejemplo de carga manual de una imagen de arranque válida

239. Si la carga manual de la imagen se ha producido correctamente, se podrá hacer el correspondiente proceso de *login* en el conmutador:

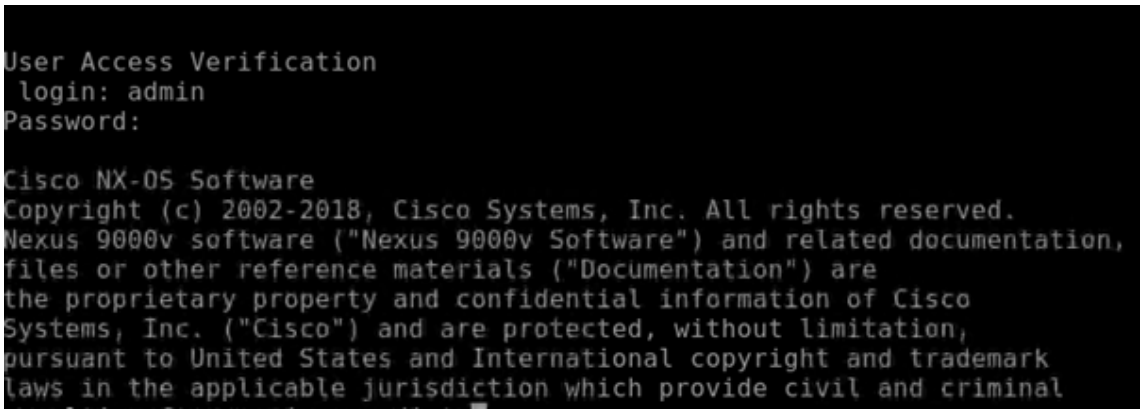

Ilustración 12. Login en el sistema tras la carga manual

240. Si se desea ampliar la información acerca del proceso de actualización del dispositivo, se debe revisar la guía "Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide" **[28]** y la guía "Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide" **[55]**

14. AUTO-CHEQUEOS Y MODO FIPS

241. Es necesario habilitar el modo FIPS para que se realicen auto chequeos criptográficos en el arranque, y habilitar la operación en modo seguro de la unidad. Para habilitar dicho modo, los requerimientos son los siguientes:

    - Deshabilitar Telnet.
    - Deshabilitar SNMPv1 y SNMPv2. Solo se permite SHA para autenticación y AES para privacidad en SNMPv3.
    - Borrar todas las claves SSH RSA1.
    - Habilitar HMAC-SHA1 MIC para su uso durante la negociación SAP en Cisco TrustSec.

242. Para habilitar el modo, se usa el comando "**fips mode enable**", y se requiere de un reinicio.

    NX01(config)# fips mode enable

    2022 Jul 1 11:14:16 NX01 %$ VDC-1 %$ %USER-2-SYSTEM_MSG: FIPS mode is Enabled for service securityd - securityd

    FIPS mode is enabled

    System reboot is required after saving the configuration for the system to be in FIPS mode

243. Cuando el sistema arranca en modo FIPS, la tarjeta supervisora realiza una serie de chequeos criptográficos en el arranque. Si cualquiera de estos test fallara, el sistema se mueve a un estado de "FIPS error". En este estado, todas las claves criptográficas se borran, y no se procesa tráfico en los puertos de comunicaciones. Si el error ocurre durante el auto-chequeo en el arranque, se indica un mensaje de error, y queda registrado en el sistema:

    Example Error Message Error Message SECURITYD-2-FIPS_SELF_TEST_FAILED: FIPS self-test failure : [chars]

    Explanation FIPS self-test failed [chars] for service [chars]

244. El auto test criptográfico en el arranque incluye los siguientes apartados:

    - **Power-on Self-Tests:**
        - *Firmware Integrity Test*

        check_bootmode: grub: Continue grub

        Trying to read config file /boot/grub/menu.lst.local from (hd0,4)

        Filesystem type is ext2fs, partition type 0x83

        Security Lock

        Booting bootflash:/nxos.9.3.9.bin

        Trying diskboot

Filesystem type is ext2fs, partition type 0x83

Image valid

Image Signature verification was Successful.

Boot Time: 7/1/2022 9:20:15

Security Lock

Installing klm_card_index

done

Linking n9k flash devices

creating flash devices BOOT_DEV= sda

NIT: version 2.88 booting

- *Known Answer Tests*: el dispositivo utiliza un algoritmo criptográfico de respuesta conocida (Known Answer Test, KAT), para cada una de las funciones criptográficas aprobadas en el estándar FIPS 140-2 (cifrado, descifrado, autenticación y generación de números aleatoria).

[Inicio de la secuencia de arranque]

…..

2022 Jul 1 11:21:30 NX01 %$ VDC-1 %$ %USER-2-SYSTEM_MSG: FIPS mode is Enabled for service securityd - securityd

2022 Jul 1 11:21:31 NX01 %$ VDC-1 %$ %SECURITYD-2-FIPS_POWERUP_SELF_TEST_STATUS: FIPS RSA power-up self-test status : PASSED

2022 Jul 1 11:21:31 NX01 %$ VDC-1 %$ %SECURITYD-2-FIPS_POWERUP_SELF_TEST_STATUS: FIPS DSA power-up self-test status : PASSED

2022 Jul 1 11:21:31 NX01 %$ VDC-1 %$ %SECURITYD-2-FIPS_POWERUP_SELF_TEST_STATUS: FIPS DES power-up self-test status : PASSED

2022 Jul 1 11:21:31 NX01 %$ VDC-1 %$ %SECURITYD-2-FIPS_POWERUP_SELF_TEST_STATUS: FIPS AES power-up self-test status : PASSED

2022 Jul 1 11:21:31 NX01 %$ VDC-1 %$ %SECURITYD-2-FIPS_POWERUP_SELF_TEST_STATUS: FIPS SHA power-up self-test status : PASSED

2022 Jul 1 11:21:31 NX01 %$ VDC-1 %$ %SECURITYD-2-FIPS_POWERUP_SELF_TEST_STATUS: FIPS HMAC SHA1 power-up self-test status : PASSED

2022 Jul 1 11:21:31 NX01 %$ VDC-1 %$ %SECURITYD-2-FIPS_POWERUP_SELF_TEST_STATUS: FIPS ECDSA power-up self-test status : PASSED

....

[Continuación de la secuencia de arranque]

- **Conditional Self-Tests** (se ejecutan periódicamente durante la ejecución normal del sistema, cada vez que una función de seguridad que lo puede utilizar es invocada):
    - Continuous Random Number Generator test for DRBG
    - Continuous Random Number Generator test for Entropy Source
    - Pairwise Consistency Test, que se ejecuta cuando un par clave pública-clave privada es generado.
    - Bypass Test, para asegurar que el texto cifrado nunca es mostrado en claro.

245. Se comprueban todos los módulos (hardware y software). Adicionalmente, durante las comprobaciones se inhibe el acceso a los algoritmos criptográficos. También, estos tests se realizan después de inicializar los módulos criptográficos, pero antes de inicializar las interfaces externas; esto previene las complicaciones de seguridad derivadas de introducir datos antes de completar los test y entrar en el modo de operación seguro. Si ocurriese un error durante estos test, el módulo criptográfico implicado forzaría a la plataforma NX-OS a reiniciarse junto con el sistema operativo y el módulo en cuestión. Esta operación garantiza que no se puedan utilizar los algoritmos criptográficos a no ser que todos los test tengan un resultado satisfactorio.

246. Información adicional acerca de la administración criptográfica de los test criptográficos se puede encontrar en “Cisco Nexus 9000 Series NX-OS Security Configuration Guide”, sección “Configuring FIPS” [29] y Cisco Nexus 3000 Series NX-OS Security Configuration Guide”, sección “Configuring FIPS [56].

15.LISTA DE COMPROBACIÓN

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Verificación de la descarga de la imagen evaluada del sistema	☐	☐	
Instalación correcta de la imagen del sistema	☐	☐	
CONFIGURACIÓN			
Modo de Operación seguro activado (FIPS-CC)	☐	☐	
Configuración remota a través de SSHv2	☐	☐	
Establecida la política de contraseñas	☐	☐	
Establecidas los criterios de bloqueo de cuentas	☐	☐	
Mensaje de aviso en el inicio de sesión	☐	☐	
Configuración de *timeouts*	☐	☐	
Configuración de la CA	☐	☐	
Establecimiento del almacenamiento local de certificados	☐	☐	
Configuración de la validación de la cadena de certificación	☐	☐	
Sincronización horaria	☐	☐	
Desactivado SNMP, Telnet	☐	☐	
Registro de auditoría activo y configurado	☐	☐	
Proceso de *Backup* definido	☐	☐	

16. REFERENCIAS

CÓDIGO	REFERENCIA
CCN-STIC-807	Guía de Seguridad de las TIC Criptología de empleo en el Esquema Nacional de Seguridad
[1]	*Cisco Nexus 9000 Hardware Installation Guide* *(all platforms)*
[2]	*Cisco Nexus 9000 Fundamentals Configuration Guide*
[3]	*Cisco Nexus 9000 Security Configuration Guide* *(Configuring User Accounts and RBAC)*
[4]	*Assurance Activity Report for Cisco Nexus 3000 and 9000 Series switches running on NX-OS 9.3*
[5]	*Cisco Nexus 9000 Security Configuration Guide* *(Configuring AAA)*
[6]	*Cisco Nexus 9000 Security Configuration Guide* *(Configuring SSH and Telnet)*
[7]	*Cisco Nexus 9000 Fundamentals Configuration Guide* *(Configuring MOTD Banner)*
[8]	*Cisco Nexus 9000 Fundamentals Configuration Guide* *(Using the Device File Systems, Directories, and Files)*
[9]	*Cisco Nexus 9000 Fundamentals Configuration Guide* *(Working with Configuration Files)*
[10]	*Cisco Nexus 9000 Security Configuration Guide* *(Configuring MACsec)*
[11]	*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide* *(Configuring Static and Dynamic NAT Translation)*
[12]	*Cisco Nexus 9000 Series NX-OS Security Configuration Guide* *(Configuring PKI)*
[13]	*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide* *(Configuring NTP)*
[14]	*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide* *(Configuring SNMP)*

CÓDIGO	REFERENCIA
[15]	*Cisco Nexus 9000 Series NX-OS Security Configuration Guide* (Configuring Port Security)
[16]	*Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide* (Configuring STP Extensions Using Cisco NX-OS)
[17]	*Cisco Nexus 9000 Series NX-OS Security Configuration Guide* (Configuring IP ACLs)
[18]	*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide* (Configuring Basic Interface Parameters)
[19]	*Cisco Nexus 9000 Series NX-OS Security Configuration Guide* (Configuring Traffic Storm Control)
[20]	*Cisco Nexus 9000 Series NX-OS Command Reference* (Show Commands)
[21]	*Cisco Nexus 9000 Series NX-OS Security Configuration Guide* (Configuring Dynamic ARP Inspection)
[22]	*Cisco Nexus 9000 Series NX-OS Security Configuration Guide* (Configuring TACACS+)
[23]	*Cisco Nexus 9000 Series NX-OS Security Configuration Guide* (Configuring RADIUS)
[24]	*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide* (Configuring System Message Logging)
[25]	*Cisco Nexus 9000 Series NX-OS System Messages Reference*
[26]	*Cisco NX-OS System Routing Messages Reference*
[27]	*Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide* (Working with configuration files)
[28]	*Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide*
[29]	*Cisco Nexus 9000 Series NX-OS Security Configuration Guide*
[30]	*Cisco Nexus 3000 Series Hardware Installation Guide*
[31]	*Cisco Nexus 3000 Series NX-OS Fundamentals Configuration Guide*
[32]	*Cisco Nexus 3600 NX-OS Security Configuration Guide*
[33]	*Cisco Nexus 3000 Series NX-OS Interfaces Configuration Guide*
[34]	*Cisco Nexus 3600 NX-OS Security Configuration Guide*

CÓDIGO	REFERENCIA
[35]	*Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide*
[36]	*Cisco Nexus 3000 Security Configuration Guide* (Configuring Authentication, Authorization and Accounting)
[37]	*Cisco Nexus 3000 Security Configuration Guide* (Configuring SSH and Telnet)
[38]	*Cisco Nexus 3000 Fundamentals Configuration Guide* (Configuring MOTD Banner)
[39]	*Cisco Nexus 3000 Fundamentals Configuration Guide* (Working with Configuration Files)
[40]	*Cisco Nexus 3000 version 10.X Security Configuration Guide* (Configuring MACsec)
[41]	*Cisco Nexus 3000 Series NX-OS Security Configuration Guide* (Configuring PKI)
[42]	*Cisco Nexus 3000 Series NX-OS System Management Configuration Guide* (Configuring NTP)
[43]	*Cisco Nexus 3000 Series NX-OS System Management Configuration Guide* (Configuring SNMP)
[44]	*Cisco Nexus 3000 Series NX-OS Security Configuration Guide* (Configuring Port Security)
[45]	*Cisco Nexus 3000 Series NX-OS Layer 2 Switching Configuration Guide* (Configuring STP Extensions Using Cisco NX-OS)
[46]	*Cisco Nexus 3000 Series NX-OS Security Configuration Guide* (Configuring IP ACLs)
[47]	*Cisco Nexus 3000 Series NX-OS Interfaces Configuration Guide* (Configuring Basic Interface Parameters)
[48]	*Cisco Nexus 3000 Series NX-OS Security Configuration Guide* (Configuring Dynamic ARP Inspection
[49]	*Cisco Nexus 3000 Series NX-OS Security Configuration Guide* (Configuring TACACS+)
[50]	*Cisco Nexus 3000 Series NX-OS Security Configuration Guide* (Configuring RADIUS)

CÓDIGO	REFERENCIA
[51]	*Cisco Nexus 3000 Series NX-OS System Management Configuration Guide* *(Configuring System Message Logging)*
[52]	*Cisco Nexus 3000 Series NX-OS System Messages Reference*
[53]	Cisco Nexus 3000 Series NX-OS Fundamentals Configuration Guide *(Using the Device File Systems, Directories, and File)*
[54]	*Cisco Nexus 3000 Fundamentals Configuration Guide* *(Working with Configuration Files)*
[55]	*Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide*
[56]	*Cisco Nexus 3000 Series NX-OS Security Configuration Guide*

17.ABREVIATURAS

AAA	*Authentication, Authorization and Accounting*
ACL	*Access Control List*
AEAD	*Authenticated Encryption with Associated Data*
AES	*Advanced Encryption Standard*
API	*Application Programming Interface*
ARP	*Address Resolution Protocol*
BIOS	*Basic Input-Output System*
BPDU	*Bridge Protocol Data Unit*
BPP	*Binary Packet Protocol*
CA	*Certification Authority*
CBC	*Cypher-Block Chaining*
CLI	*Command Line Interface*
CPD	*Centro de Procesamiento de Datos*
CRL	*Certificate Revocation List*
CSR	*Certificate Signing Request*
DAI	*Dynamic ARP Inspection*
DHCP	*Dynamic Host Configuration Protocol*
DoS	*Denegation of Service*
DSA	*Digital Signature Algorithm*
EAPOL	*Extensible Authentication Protocol Over LAN*
ECDSA	*Elliptic Curve Digital Signature Algorithm*
EEPROM	*Electrically Erasable Programmable Read-Only Memory*
ENS	*Esquema Nacional de Seguridad*
FIPS	*Federal Information Processing Standard*
FQDN	*Fully Qualified Domain Name*
FTP	*File Transfer Protocol*
HTTP / S	*Hypertext Transfer Protocol / Secure*
ICMP	*Internet Control Message Protocol*
IGMP	*Internet Group Management Protocol*
IKE	*Internet Key Exchange*
IPSec	*Internet Protocol Security*

LAN	*Local Area Network*
MAC	*Media Access Control*
MACsec	*Media Access Control Security*
MD5	*Message Digest 5*
MKA	*MACsec Key Agreement*
NTP	*Network Time Protocol*
NVRAM	*Non-Volatile Random Access Memory*
POST	*Power-On Self-Test*
RADIUS	*Remote Authentication Dial In User Service*
RAM	*Random Access Memory*
RBAC	*Role Based Access Control*
RFC	*Request for Comments*
RSA	*Rivest Shamir and Adleman*
SAP	*Algo relacionado con MKA*
SCP	*Secure Copy Protocol*
SFP	*Small Form Platform*
SFTP	*Secure File Transfer Protocol*
SNMP	*Simple Network Management Protocol*
SSH	*Secure Shell*
STP	*Spanning Tree Protocol*
TACACS	*Terminal Access Control Access Control System*
TFTP	*Trivial File Transfer Protocol*
TIC	*Tecnologías de la Información y la Comunicación*
TLS	*Transport Layer Security*
UDLD	*Unidirectional Link Detection*
USB	*Universal Serial Bus*
VDC	*Virtual Device Context*
VLAN	*Virtual Local Area Network*
VPC	*Virtual PortChannel*
VRF	*Virtual Routing and Forwarding*

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA SUBSECRETARÍA DE DEFENSA SECRETARÍA GENERAL TÉCNICA SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL