CCN
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1428

Procedimiento de empleo seguro
Switches Juniper QFX5100 y EX4600, JunOS 18.1R1

Marzo 2022

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.03.10 12:31:45 +01'00'

Pº de la Castellana 109, 28046 Madrid
Centro Criptológico Nacional, 2022
NIPO: 083-22-068-7

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

1. El presente documento pretende servir de guía para establecer una **configuración segura** de los switches Ethernet de Juniper Networks **EX4600 y QFX5100** que ejecutan el sistema operativo **Junos OS 18.1R1**.
2. Estos switches son dispositivos seguros de red, con una interfaz de gestión limitada y protegida, y un sistema operativo de propósito especial que no proporciona ninguna capacidad de propósito general, sino únicamente funciones de gestión, control y conmutación de paquetes IP.
3. EX4600 y QFX5100 son *switches* altamente flexibles y de alto rendimiento, que permiten a los operadores de los centros de datos construir redes automatizadas protegidas, escalables que se adapten a sus necesidades de implementación y que evolucionen fácilmente a medida que los requisitos cambian con el tiempo.
4. Los dispositivos son físicamente autónomos y albergan el *software*, el *firmware* y el *hardware* necesarios para realizar todas las funciones de conmutación.
5. Los dispositivos constan de dos (2) componentes arquitectónicos principales:
    - **Motor de enrutamiento (RE):** ejecuta el *firmware* de Junos OS. Proporciona servicios de conmutación de capa 2-3 y de administración de red para todas las operaciones necesarias para la configuración y operación del dispositivo y controla el flujo de información que lo atraviesa.
    - **Motor de reenvío de paquetes (PFE):** proporciona todas las operaciones necesarias para el encaminamiento de paquetes.
6. El motor de enrutamiento y el motor de reenvío de paquetes realizan sus tareas principales de forma independiente, mientras se comunican constantemente a través de un enlace interno de alta velocidad. Esta disposición proporciona un control de enrutamiento y reenvío optimizado y la capacidad de desplegar redes a escala de Internet a altas velocidades.
7. **Estos productos han sido cualificados e incluidos en el Catálogo de Producto y Servicios TIC (CPTSIC) en la familia "*Switches*".**

2. OBJETO Y ALCANCE

8. En la presente guía se recoge el procedimiento de empleo seguro para los ***switches* de las series EX4600 y QFX5100 con Junos OS 18.1R1**.

9. En la siguiente tabla se muestran en detalle los chasis de las series:

Chasis	Puertos de red
EX4600	**EX4600-40F-AFO** **EX4600-40F-AFI** **EX4600-40F-DC-AFO** **EX4600-40F-DC-AFI** Todos ellos con: – *Fixed 10GbE ports with 10G-USR optics, all ports forwarding (line rate), <10 m* – *4 fixed 40GbE ports with 40G-SR4 optics* – *1 4x40GbE QIC card with 4 40G-SR4 optics* – *1 8x10GbE QIC card with 8 10G-USR optics, all ports forwarding (line rate), <10 m*
QFX5100	**QFX5100-48S-AFO/AFI**: – *1GbE SFP: 48 (24 copper 1GbE)* – *10GbE SFP+: 48/72 (with breakout cable)* – *40GbE QSFP+: 6* **QFX5100-48T-AFO/AFI**: – *100 Mbps RJ-45: 48* – *1GbE RJ-45: 48* – *10GbE RJ-45: 48* – *10GbE SFP+: 24 (with breakout cable)* – *40GbE QSFP+: 6* **QFX5100-24Q-AFO/AFI**: – *1GbE SFP: N/A* – *10GbE SFP+: 96/104 (with breakout cable)* – *40GbE QSFP+: 24/32 (with 2 x QFX-EM-4Q)* **QFX5100-24Q-AA-AFO/AFI**: – *1GbE SFP: N/A* – *10GbE SFP+: 96/104 (with breakout cable)* – *40GbE QSFP+: 24/32 (with 2 x QFX-EM-4Q)* **QFX5100-96S-AFO/AFI**: – *1GbE SFP: 96 (48 Copper 1GbE)* – *10GbE SFP+: 104 (with breakout cable)* – *40GbE QSFP+: 8*

Tabla 1 – Chasis series QFX5100 y EX4600

3. ORGANIZACIÓN DEL DOCUMENTO

10. El presente documento se divide en las siguientes secciones, de acuerdo a distintas fases que componen el ciclo de vida del producto:

    a) **Apartado 4.** En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

    b) **Apartado 5.** En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

    c) **Apartado 6**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

    d) **Apartado 7.** En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

    e) **Apartado 8.** En este apartado se incluye una *checklist* con las tareas necesarias.

    f) **Apartado 9.** Incluye un listado de la documentación que ha sido referenciada a lo largo del documento.

    g) **Apartado 10.** Incluye el listado de las abreviaturas empleadas a lo largo del documento.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

11. Durante el proceso de entrega deberán llevarse a cabo una serie de tareas de comprobación para garantizar que el producto recibido no haya sido manipulado indebidamente:

    a) **Etiqueta de envío.** Deberá comprobarse que la etiqueta de envío identifica correctamente el nombre del cliente, su dirección y el dispositivo.

    b) **Embalaje externo.** Deberá inspeccionarse la caja de envío externa y la cinta adhesiva. Se comprobará que la cinta adhesiva no esté cortada ni se haya deteriorado en ningún punto. Así mismo, la caja no deberá presentar cortes ni daños que permitan acceder al dispositivo.

    c) **Embalaje interno.** Deberá inspeccionarse la bolsa de plástico y el sistema de sellado. La bolsa no deberá presentar cortes ni haber sido extraída. El sistema de sellado deberá estar intacto.

12. En caso de identificarse algún problema durante la inspección, el cliente deberá ponerse en contacto inmediatamente con el proveedor, al que se le indicará el número de pedido, el número de seguimiento y una descripción del problema.

13. Además, es necesario realizar una serie de comprobaciones para garantizar que la caja recibida la envió Juniper Networks y no existe una suplantación de identidad:

    a) Verificar la existencia de un pedido de compra al fabricante. Juniper Networks nunca envía dispositivos sin pedido de compra.

    b) Comprobar que se ha recibido la notificación de envío de Juniper Networks en la dirección de correo electrónico que se indicó cuando se realizó el pedido. Este mensaje deberá incluir la siguiente información:

        - Número de pedido de compra.
        - Número de pedido de Juniper Networks, utilizado para hacer un seguimiento del envío.
        - Número de seguimiento del transportista, utilizado para hacer un seguimiento del envío.
        - Lista de artículos enviados, incluidos los números de serie.
        - Dirección y contacto del proveedor y del cliente.

    c) Verificar que el envío lo inició Juniper Networks. Para ello, sería necesario:

        - Comparar el número de seguimiento de pedido del transportista que aparece en la notificación de envío de Juniper Networks, con el número de seguimiento en el paquete recibido.

- Iniciar sesión en el portal de ayuda al cliente en línea de Juniper Networks en la dirección: *https://support.juniper.net/support/* para ver el estado del pedido.

4.2 ENTORNO DE INSTALACIÓN SEGURO

14. Los dispositivos deberán instalarse dentro de un Centro de Proceso de Datos (CPD), cuyo acceso estará limitado a un conjunto de personas que posean una autorización expresa.
15. Para ello, la sala en la que se ubica el CPD estará dotada de un sistema de control de acceso que asegure que únicamente el personal autorizado puede acceder al dispositivo (incluido fuera del horario laboral).
16. Deberán seguirse las recomendaciones indicadas en este Procedimiento de Empleo Seguro y en la documentación de los dispositivos EX4600 y QFX5100. Otros servicios deberán ser realizados únicamente por el personal autorizado.
17. Antes de instalar el dispositivo, deben revisarse las condiciones para la infraestructura necesaria, indicadas en la documentación de los dispositivos EX4600 y QFX5100, y así asegurarse de que el área de despliegue cumpla con los requisitos de energía, ambientales y de espacio libre para el *switch*.
18. Antes de conectar el dispositivo a una fuente de alimentación, se debe revisar las instrucciones de instalación en la documentación de los dispositivos EX4600 y QFX5100
19. Si el bastidor o armario dispone de dispositivos estabilizadores se deben instalar en el bastidor antes de montar el *switch*.

4.3 COMPONENTES DEL DISPOSITIVO Y DEL ENTORNO DE OPERACIÓN

20. Los dispositivos **EX4500** y **QFX5100** se componen del *firmware* **Junos OS 18.1R1** ejecutándose en los chasis indicados en la Tabla 1.
21. Dentro de la frontera física de los dispositivos se incluye el hipervisor KVM, que proporciona la capa de virtualización en la que se ejecuta Junos OS VM, como se muestra en la Figura a continuación.

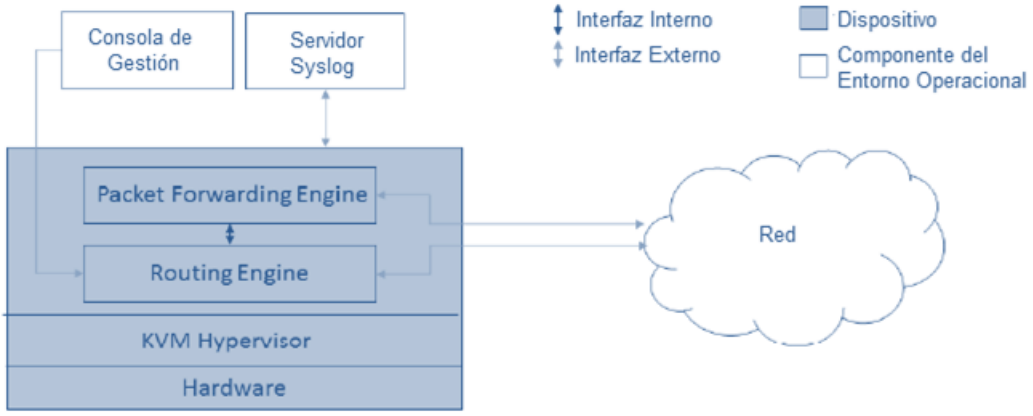

Figura 1- Arquitectura física de los dispositivos EX4600 y QFX5100

22. Los dispositivos requieren interfaces de red RJ-45, SFP/SFP + y/o QSFP+ (como se detalla en la Tabla 1) para operar y comunicarse con la red conectada.
23. El entorno operativo debe proporcionar los siguientes elementos:
    - Servidor *syslog* que admite conexiones SSHv2 para enviar registros de auditoría.
    - Cliente SSHv2 para administración remota.
    - Cliente de conexión en serie para administración local.

5. FASE DE INSTALACIÓN

24. Una vez instalado el *switch*, es necesario realizar la configuración inicial:

    a) Conectar el puerto de consola a una computadora portátil o PC utilizando un cable RJ-45 y el adaptador RJ-45 a DB-9 suministrados. El puerto de consola (CON) se encuentra en el panel de puertos del dispositivo.

    b) Iniciar sesión como *root*. Inicialmente no se requiere contraseña. Si el *software* se inicia antes de conectarse al puerto de consola, se debe presionar la tecla *Intro* para que aparezca el mensaje:

    login: root

    c) Iniciar la interfaz de línea de comandos (CLI) y entrar al modo de configuración:

    root@% cli

    root> configure

    d) Crear una contraseña para el usuario *root* (ver apartado 6.2.3.3 *ROOT*):

    [edit]

    root@# set system root-authentication plain-text-password

    New password: password

    Retype new password: password

    e) (Opcional) Configurar el nombre del *switch*. Si el nombre incluye espacios, escribirlo entre comillas.

    [edit]

    root@# set system host-name nombre_del_switch

    f) Configurar el *gateway* por defecto:

    [edit]

    root@# set routing-options static route default next-hop DirIPdelGateway

    g) Configurar la interfaz de gestión (dirección IP y la máscara de red):

    [edit]

    root@# set interfaces em0 unit 0 family inet address direcciónIP/máscara

    h) (Opcional) Configurar las rutas estáticas hacia las redes remotas con acceso a la interfaz de gestión:

    [edit]

    root@# set routing-options static route DirIP_remota/máscara next-hop DirIPpasarela retain no-readvertise

    i) Habilitar el servicio SSH para poder realizar la gestión remota del dispositivo:

[edit]
root@# set system services ssh

j) Ejecutar el comando *commit* para aplicar la configuración al *switch*:

[edit]
root@# commit

25. Una vez finalizada la configuración inicial, es necesario **comprobar que la versión de Junos instalada es la esperada** (en este caso Junos OS 18.1R1). Para ello:

a) Conectar el puerto de consola a una computadora portátil o PC utilizando un cable RJ-45 y el adaptador RJ-45 a DB-9 suministrados. El puerto de consola (CON) se encuentra en el panel de puertos del dispositivo.

b) Iniciar sesión como *root* con la contraseña configurada anteriormente. Si el *software* se inicia antes de conectarse al puerto de consola, se debe presionar la tecla *Intro* para que aparezca el mensaje:

login: root

c) Iniciar la interfaz de línea de comandos (CLI) y entrar al modo de configuración:

root@% cli

d) Ejecutar el comando para confirmar la versión de Junos OS instalada:

root@hostname> show version

e) Localizar en la salida del comando la versión instalada:

Hostname: lab

Model: QFX5100

Junos: 13.3R1.4

JUNOS Base OS boot [13.3R1.4]

JUNOS Base OS Software Suite [13.3R1.4]

JUNOS Kernel Software Suite [13.3R1.4]

JUNOS Crypto Software Suite [13.3R1.4]

[…]

26. Si la versión instalada no es la adecuada (Junos OS 18.1R1), es necesario descargar dicha versión Para ello:

a) Acceder a la web de descargas de *software* de Juniper y hacer *login* con la cuenta que tenga asociado el número de serie del equipo que se está instalando (https://support.juniper.net/support/downloads/) .

b) En la pestaña "*Downloads*" buscar el equipo para el que se quiere descargar la versión de Junos.

c) Una vez localizado el producto, localizar el paquete y la versión a descargar (Junos 18.1R1).

d) Elegir la versión correspondiente y hacer *click* en el enlace de descarga.

e) Aceptar el EULA y seleccionar la opción *proceed.*

f) Descargar la versión deseada en el equipo local y alojarla en un servidor alcanzable por el *switch* donde se va a instalar.

g) Comprobar la integridad del *software* descargado con los "*checksum*" **SHA256 o SHA512** que aparecen en la página, asociados a la descarga seleccionada.

27. Con la versión de Junos alojada en el servidor, realizar la instalación desde el *switch*:

a) Acceder al modo de configuración del equipo.

root@hostname> configure

b) Ejecutar el comando *request system software add <pathname><source> reboot* para instalar Junos 18.1R1.

root@hostname> request system software add scp://hostname/pathname/jinstall-host-qfx-5-18.1R1.n-signed.tgz reboot

Para usar autenticación, se debe usar el comando del siguiente modo:

scp://<username>:<password>@hostname/pathname/jinstall-host-qfx-5-18.1R1.n-signed.tgz

c) Una vez que el equipo se ha reiniciado, comprobar que la nueva versión se ha instalado correctamente.

root@hostname> show version

d) Localizar en la salida del comando la versión instalada:

Hostname: lab

Model: QFX5100

Junos: 18.1R1

JUNOS Base OS boot [18.1R1]

JUNOS Base OS Software Suite [18.1R1]

JUNOS Kernel Software Suite [18.1R1]

JUNOS Crypto Software Suite [18.1R1]

[…]

5.1 REGISTRO Y LICENCIAS

28. Para poder instalar la licencia esta deberá haberse adquirido previamente y se debe disponer de una conexión CLI con el dispositivo. Todas las licencias instaladas en el dispositivo se almacenarán en el directorio */config/license*.
29. Existen dos (2) formas de instalar la licencia: con sentencias del modo configuración o a través de comandos operacionales (ver apartado 6.2.1 ADMINISTRACIÓN LOCAL Y REMOTA para información sobre la interfaz de comandos).
    - La sentencia del modo configuración *system license keys key* permite añadir o borrar licencias directamente o desde un fichero de configuración.
    - El comando operacional *request system license add* instala la licencia a través de una URL o utilizando un fichero de licencias.
30. La instalación de la licencia desde el modo configuración se realiza directamente con la sentencia *system license keys key name* .
31. El parámetro *name* incluye el ID de la licencia y la clave de licencia. Tras ejecutar la sentencia, al estar en el modo de configuración, se debe ejecutar el comando *commit* para hacer efectivos los cambios:

```
user@device#configure
[edit]
user@device# set system license keys key "JUNOS_TEST_LIC_FEAT xxxxxx xxxxxx
xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx"
user@device# commit
commit complete
```

32. Se creará un fichero de configuración (por ejemplo: "*license.conf*") que contenga la sentencia *set system license keys key name* (o varias, si se quieren instalar varias licencias):

```
user@device# cat > license.conf
```

El contenido de "*license.conf*" será, por ejemplo:

```
system {
   license {
      keys {
        key "JUNOS_TEST_LIC_FEAT xxxxxx xxxxxx";
      }
   }
}
```

33. En el modo configuración, se debe cargar y ejecutar el fichero de configuración y hacer efectivos los cambios:

```
user@device# load merge license.conf
load complete
```

user@device# commit

commit complete

34. También se puede instalar la licencia desde el modo operación usando el comando operacional

    request system license add filename | url

35. Al ser un comando operacional, el cambio se aplica de forma inmediata tras ejecutar el comando. Como parámetro se le puede pasar la URL donde se encuentra la licencia, o un fichero de licencia.

36. Para mostrar las licencias se utilizará el comando operacional *show system license.*

6. FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

37. **El modo de operación seguro debe ser activado para que el dispositivo funcione de acuerdo a las garantías de seguridad requeridas.**

38. Cuando el modo de operación seguro está habilitado, el dispositivo realiza las siguientes tareas:

    - Realiza auto-chequeos de las funciones criptográficas en el arranque del dispositivo.
    - Realiza auto-chequeos continuos de la generación de números aleatorios y claves.
    - No permite el establecimiento de conexiones de gestión que no estén correctamente cifradas.
    - Obliga a que las contraseñas se almacenen protegidas con algoritmos unidireccionales sólidos (funciones hash). En el apartado 6.2.2.1 AUTENTICACIÓN CON NOMBRE DE USUARIO Y CONTRASEÑA, en la configuración de la política de contraseñas, se puede definir la función hash que será utilizada (**se recomienda el uso de SHA512**).
    - Obliga a que las contraseñas de administrador tengan 10 caracteres, como mínimo.

39. Todas las funciones y algoritmos criptográficos implementados por el dispositivo, se implementan a través de los módulos: *OpenSSL (OpenSSH), LibMD* y *Kernel*.

    - El módulo *OpenSSL* (*OpenSSH*) se utiliza para implementar los algoritmos y funciones criptográficas del protocolo SSHv2 que utiliza el dispositivo para la administración remota, y para la conexión con servidores *syslog*.
    - La generación de valores aleatorios utiliza *HMAC_DRBG* implementado en los módulos Kernel y OpenSSL.
    - Adicionalmente, las funciones SHA256 y SHA512 son implementadas en el módulo LibMD que es utilizado por el demonio Junos MGD para el *password hashing.*

40. En el modo de operación seguro se deshabilitan los algoritmos criptográficos débiles, como el estándar de cifrado DES y el algoritmo hash MD5, y únicamente se permite el uso de algoritmos y funciones criptográficas seguras. En la siguiente tabla se indican los algoritmos criptográficos que se implementan en modo de operación seguro:

Módulo criptográfico	Función	Algoritmos criptográficos
OpenSSL (OpenSSH)	*Cifrado / Descifrado*	*AES-CBC (128, 192, 256)* *AES-CTR (128, 192, 256)*
	Message Digest Generation	*SHA1, SHA2-256, SHA2-384, SHA2-512*
	Autenticación de mensajes	*HMAC-SHA1, HMAC-SHA2-256, HMAC-SHA2-512*
	Generación de claves *Generación y verificación de firma*	*ECDSA (P-256 / SHA-256)* *ECDSA (P-384 / SHA-384)* *ECDSA (P-521 / SHA-521)* *RSA (2048/3072) / SHA256*
	Random Bit Generation	*DRBG (HMAC-SHA-2-256)*
LibMD	*Message Digest Generation*	*SHA1, SHA2-256, SHA2-512*
	Message Authentication	*HMAC-SHA1, HMAC-SHA2-256*
Kernel	*Message Digest Generation*	*SHA1, SHA2-256, SHA2-384, SHA2-512*
	Message Authentication	*HMAC-SHA1, HMAC-SHA2-256*
	Random Bit Generation	*DRBG (HMAC-SHA-2-256)*

Tabla 2 – Algoritmos y funciones criptográficas en modo de operación seguro

41. En el modo de operación seguro se establece una frontera alrededor de los módulos criptográficos, de forma que ningún parámetro crítico de seguridad (CSP) puede cruzar esta frontera en texto plano, sino que deberá estar cifrado con uno de los algoritmos y funciones criptográficas aprobadas en el modo de operación seguro e indicadas en la tabla anterior. Los parámetros críticos de seguridad que maneja el dispositivo, son los siguientes:

CSP	Descripción	Funciones y algoritmos criptográficos empleados
Host Key* Privada *SSH	Claves SSH utilizadas para identificar el dispositivo como servidor SSH. Se generan en la configuración inicial del equipo.	ECDSA P-256 SSH-RSA
SSH Session Key	Claves de sesión SSH usadas para el cifrado, autenticación de mensajes y *Key Establisment*.	Claves de cifrado AES 128/256 Claves HMAC-SHA1, HMAC-SHA2-256 y HMAC-SHA2-512 Claves privadas DH Group 14 o ECDH-P256/P-384/P-512

CSP	Descripción	Funciones y algoritmos criptográficos empleados
Contraseñas de usuarios	Contraseñas en texto plano introducidas por los usuarios para su autenticación.	Las contraseñas se almacenan cifradas con un hash (SHA-256, SHA-512)
DRBG	Estado interno y "*seed key*" del DRBG	DRBG (HMAC-SHA-2-256)

Tabla 3 – Parámetros Críticos de Seguridad (CSPs)

42. Para obtener información adicional sobre el proceso de configuración del modo de operación seguro se puede consultar la guía *Junos OS Common Criteria Evaluated Configuration Guide for EX4300, EX4600, and QFX5100 Devices* [REF.3].

43. A continuación, se muestran los pasos resumidos para configurar el modo de operación seguro desde Junos OS CLI:

    a) Como usuario *root*, entrar al modo configuración y ejecutar la sentencia *set system fips level nivel_FIPS*, el dispositivo solo dispone del "*level 1*" lo cual activa todas las características indicadas:

    root@switch>configure

    Entering configuration mode

    [edit]

    root@switch# set system fips level 1

    b) Confirmar el cambio y reiniciar el dispositivo:

    root@switch# commit

    configuration check succeeds

    [edit]

    'system'

    reboot is required to transition to FIPS level 1

    commit complete

    [edit]

    root@switch# run request system reboot

    Reboot the system ? [yes,no] (no) yes

44. Cuando el dispositivo se reinicia tras la activación del modo seguro, se realizan los auto-chequeos de arranque (ver apartado 6.7 AUTO-CHEQUEOS). Una vez finalizan los auto chequeos, debe reiniciarse de nuevo el dispositivo para activar el RBG (HMAC-DRBG).

45. Para verificar que el dispositivo está en modo de operación seguro, ejecutar el comando operacional *show system*:

```
[edit]
root@switch#show system
fips {
level 1;
}
```

6.2 ADMINISTRACIÓN DEL PRODUCTO

6.2.1 ADMINISTRACIÓN LOCAL Y REMOTA

46. La interfaz de línea de comandos (CLI) de Junos OS es la interfaz de *software* que se utiliza para acceder al dispositivo y configurarlo, supervisar sus operaciones y ajustar la configuración según sea necesario. Se deberá acceder a ella a través de:

    a) **Interfaces de gestión local:** el puerto de consola RJ-45 en el panel trasero del dispositivo está configurado como equipo terminal de datos (DTE) RS-232. Se puede utilizar la interfaz de línea de comandos (CLI) en este puerto para configurar el dispositivo desde un terminal.

    b) **Protocolos de gestión remota:** el dispositivo puede gestionarse en remoto mediante cualquier interfaz Ethernet. **El protocolo SSHv2 es el único protocolo de gestión remota recomendado**. Telnet y J-Web no están disponibles en el dispositivo una vez se activa el modo de operación seguro.

47. A continuación, se explican unos conceptos necesarios para entender otros apartados de este documento. Se puede obtener más información sobre la operativa de Junos OS CLI y sus comandos, en la guía *CLI User Guide* [**REF.2**].

48. Junos OS CLI tiene dos (2) modos:

    a) **Modo Operacional**. En el modo operacional se utilizan comandos para monitorizar y solucionar problemas (*troubleshooting*) y para mostrar el estado actual del dispositivo. Comandos de ejemplo: *monitor, ping, show, test y traceroute.*

    b) **Modo Configuración**. Este modo permite configurar el dispositivo. En este modo, se ejecutarán sentencias (*configuration statements*) para configurar todas las propiedades del dispositivo, incluidos interfaces, enrutamiento, acceso de usuarios, y varias propiedades del sistema y del *hardware*.

49. Cuando se accede al modo configuración, en realidad se están haciendo los cambios sobre un archivo llamado *candidate configuration*. Este archivo permite realizar cambios de configuración sin provocar cambios en la configuración activa. El dispositivo no implementará los cambios añadidos al archivo *candidate configuration* hasta que se confirmen mediante un *commit*, lo que activa la nueva configuración en el dispositivo.

50. Cuando se configura, opera o monitoriza un dispositivo, es habitual estar cambiando de un modo a otro. Aunque existen varias formas para hacer esto, lo más sencillo

para cambiar a modo configuración desde modo operación, es ejecutar "*configure*". Y para salir del modo de configuración al de operación, teclear "*exit*".

51. Los comandos CLI están organizados en **jerarquías**:

    a) En el modo operacional, los comandos que realizan una función similar se agrupan bajo el mismo nivel de jerarquía. Por ejemplo, todos los comandos que muestran información sobre el sistema se agrupan bajo el comando *show system*, y todos los comandos que muestran información sobre la tabla de enrutamiento se agrupan bajo el comando *show route*.

    Para ejecutar un comando determinado, se debe teclear el nombre completo del comando comenzando en el nivel superior de la jerarquía. Por ejemplo, para mostrar una vista breve de las rutas, se usaría el comando *show route brief*.

    b) En el modo configuración, la jerarquía de sentencias de configuración (*configuration statements*) tiene dos (2) tipos de sentencias: sentencias contenedor (*container statements*) que contienen otras sentencias, y sentencias finales (*leaf statements*) que no contienen otras sentencias.

52. La siguiente figura muestra un ejemplo del árbol de jerarquía. La sentencia *protocols* es una sentencia "*top*" que forma parte del tronco del árbol de jerarquías. Las sentencias *ospf*, *area* e *interface* son sentencias contenedoras subordinadas (son ramas del árbol de jerarquía), y la sentencia *hello-interval* es una sentencia final (una hoja en el árbol de jerarquía).

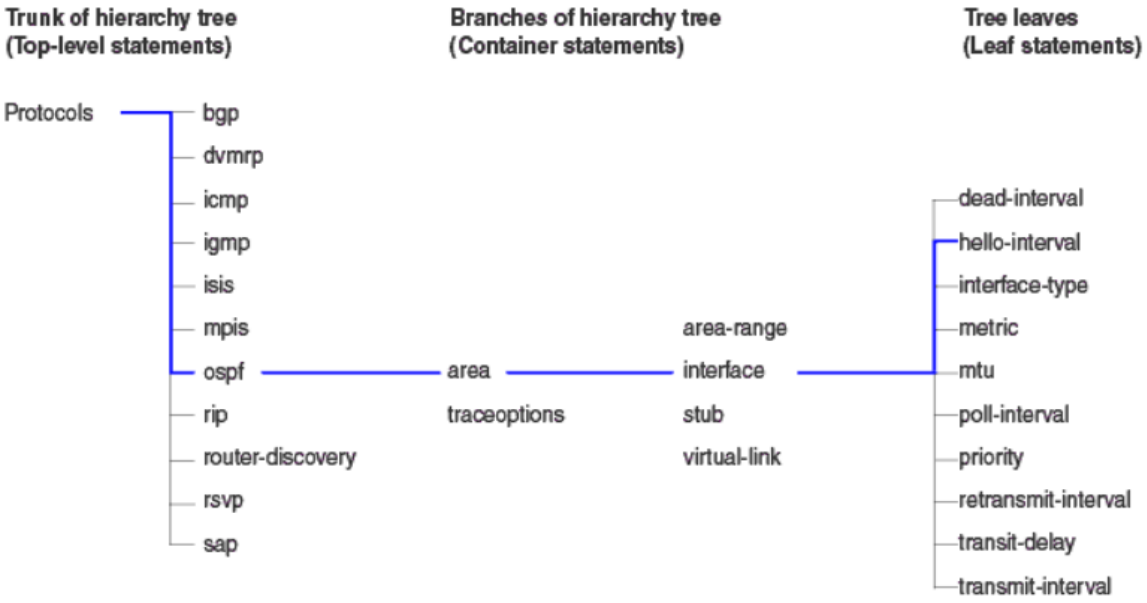

Figura 2- Ejemplo de jerarquía de sentencias de configuración

6.2.2 AUTENTICACIÓN

53. La autenticación de los usuarios puede ser de varios tipos:
    a) Autenticación con nombre de usuario y contraseña (para accesos al dispositivo a través de consola y SSH).
    b) Autenticación con nombre de usuario y clave pública (para accesos al dispositivo a través de SSH).
    c) Autenticación con RADIUS.
    d) Autenticación con TACACS+.
54. Estos dos últimos servidores de autenticación se configuran según está detallado en el apartado 6.3 AUTENTICACIÓN CON SERVIDORES EXTERNOS.
55. Se recomienda hacer uso de la autenticación local mediante nombre de usuario/contraseña o claves públicas.

6.2.2.1 AUTENTICACIÓN CON NOMBRE DE USUARIO Y CONTRASEÑA

56. Cuando se crea una cuenta de usuario, uno de los parámetros que se indican es el método de autenticación (*authentication*). En caso de utilizar contraseña, esta podrá especificarse:
    a) **En texto plano (*plain-text password*):** esta contraseña será protegida en el almacenamiento por Junos OS mediante el cifrado con funciones *hash*. El algoritmo usado por defecto en los dispositivos EX4600 y QFX5100 es SHA512 y no se recomienda modificarlo. Se recomienda hacer uso de esta modalidad, ya que permite la definición de una política de contraseñas para asegurar el uso de contraseñas seguras. En caso de especificar este método de autenticación, el dispositivo solicitará la introducción y confirmación de la contraseña:

    [edit system login user username*]*
    user@host# set authentication plain-text-password
    New password: type password here
    Retype new password: retype password here

    b) **Cifrada (*encrypted-password*):** se introduce directamente la contraseña cifrada, y es lo que directamente almacena Junos OS. El algoritmo de cifrado por defecto, es la función hash SHA 512 en los dispositivos EX4600 y QFX5100:

    [edit system login user username]
    user@host# set authentication encrypted-password "$ABC123"

57. En la autenticación por contraseña, el dispositivo fuerza un mecanismo de acceso con retardo. Para ello se deben configurar una serie de parámetros, como el número máximo de intentos fallidos de autenticación y tiempos de retardo (ver apartado 6.2.4 PARÁMETROS DE SESIÓN (*LOGIN SETTINGS*)). Si, por ejemplo, los primeros dos (2) intentos de introducir la contraseña correcta fallan, no se aplica ningún retardo.

Cuando el usuario introduce la contraseña por tercera vez, el dispositivo fuerza un retardo de 5 segundos. A cada intento fallido desde entonces, se suman 5 segundos más de retardo respecto al intento fallido anterior.

58. **Política de contraseñas**: el método de autenticación de contraseña en texto plano, permite definir una política de contraseñas a través de la sentencia de configuración *password* en el nivel de jerarquía *[edit system login]:*

```
[edit system login]
password {
   change-type (set-transitions | character-set);
   format (sha1 | sha256 | sha512);
   maximum-length length;
   maximum-lifetime days
   minimum-changes number;
   minimum-character-changes number
   minimum-length length;
   minimum-lifetime days
   minimum-lower-cases number;
   minimum-numerics number;
   minimum-reuse number
   minimum-punctuations number;
   minimum-upper-cases number;
}
```

- *change-type*: establece los requisitos para utilizar conjuntos de caracteres en la contraseña.
- *character-sets*: la contraseña puede usar sets de caracteres. Los cinco (5) sets de caracteres admitidos en Junos OS son: mayúsculas, minúsculas, números, signos de puntuación y caracteres especiales (! @ # $ % ^ & * , +< > : ;). **Se recomienda configurar el uso de, al menos, 4 conjuntos de caracteres.**
- *set-transitions*: número de transiciones entre los conjuntos de caracteres. Este parámetro se usa en combinación con *minimum-changes*. Si *change-type* es *character-sets*, entonces el número de sets de caracteres incluidos en la contraseña, se chequea contra el número especificado en *minimum-changes*. Si *change-type* es *set-transitions*, entonces el número de cambios en los sets de caracteres incluidos en la contraseña, se cheque contra el número especificado en *minimum-changes*.
- *minimum-character-changes:* mínimo número de caracteres que deben cambiar entre una contraseña y la anterior.
- *format (sha1 | sha256 | sha512):* Función hash con la que Junos OS cifrará la contraseña. En los dispositivos EX4600 y QFX5100 es **SHA512 por defecto** (las contraseñas empiezan por 6), **valor recomendado**.

- *maximum-length / mínimum-length:* longitudes máxima y mínima de la contraseña. **Se recomiendan 12 caracteres mínimo**.
- *maximum-lifetime days:* máxima duración de la contraseña en días. **Se recomienda configurar un tiempo máximo de 60 días o menos.**
- *minimum-lifetime days:* mínimo número de días que debe durar la contraseña antes de poder cambiarla. **Se recomienda configurar no menos de 7 días.**
- *minimum-lower-cases / minimum-numerics / minimum-punctuations / minimum-upper-cases*: mínimo número de caracteres de cada tipo, que debe contener la contraseña. Se recomienda que, al menos, contenga 1 carácter de cada tipo.
- *minimum-reuse:* mínimo número de contraseñas antiguas que no deben coincidir con la nueva contraseña. **Se recomienda configurar, al menos, 5.**

59. A la hora de crear las contraseñas, deberán observarse y tenerse en cuenta las recomendaciones expuestas en la guía *CCN-STIC 821, Apéndice V: Normas de Creación y Uso de Contraseñas NP40* **[REF.5]**.

6.2.2.2 AUTENTICACIÓN CON CLAVE PÚBLICA SSH

60. Con la autenticación mediante clave pública SSH, el usuario introduce el nombre de usuario y demuestra que posee la clave privada que corresponde a la clave pública que el dispositivo tiene almacenada para ese usuario.
61. Las claves SSH podrán ser ECDSA P-256 o RSA. La configuración de SSH y de las claves de autenticación, se puede consultar en el apartado 6.2.5 CONFIGURACIÓN DE SSH.

6.2.3 CONFIGURACIÓN DE USUARIOS

6.2.3.1 *LOGIN CLASSES* Y PERMISOS

62. En este apartado se indican los conceptos clave que utiliza Junos OS en relación con las cuentas de usuario y la autenticación. Se describen también los pasos básicos para la creación de usuarios y cuentas. No obstante, se puede obtener más información al respecto en *Junos OS User Access and Authentication Administration Guide* **[REF1]**.
63. Junos OS asocia los usuarios a *login classes***,** las cuales tendrán asignados ciertos privilegios de acceso. En función de ellos, se determinará qué comandos CLI se pueden ejecutar y qué configuración se puede ver y/o modificar.
64. A cada cuenta de usuario individual se le asocia una *login class*, para determinar los permisos y privilegios del usuario. Cada *login class*, además, lleva configurado un tiempo máximo de inactividad de sesión (*idle timeout*).
65. Los permisos y privilegios se asignan utilizando *Permission Bits*, que dan acceso a lectura y/o escritura de las funcionalidades del dispositivo. Los hay de dos (2) tipos:

a) Los que llevan la coletilla "-control", que proporcionan lectura y escritura de la funcionalidad.

b) Los que no llevan la coletilla "-control", que solo proporcionan capacidad de lectura sobre la funcionalidad.

Por ejemplo:

- ***access*:** permite visualizar la configuración de acceso en el modo configuración, usando el comando del modo operacional *show configuration.*
- ***access-control*:** permite visualizar y configurar la información de acceso (en el nivel de jerarquía del modo configuración *[edit access]*).

66. En la Tabla 2 (página 4) del documento *Junos OS User Access and Authentication Administration Guide* **[REF1]** se pueden consultar todos los *Permission Bits* existentes. Se destacan los siguientes:

- ***Admin:*** puede ver la información de cuentas de usuario en el modo configuración, y con el comando *show configuration*.
- ***Admin-control*:** puede ver las cuentas de usuario y configurarlas (en el nivel de jerarquía [edit system login]).
- ***All:*** todos los permisos.
- ***Clear*:** puede borrar información aprendida de la red, que se almacena en varias bases de datos de la red (utilizando los comandos *clear*).
- ***Network:*** puede acceder a la red con comandos *ping, ssh, telnet* y *traceroute*.
- ***Reset*:** puede reiniciar los procesos software utilizando el comando *restart*, y puede configurar si los procesos software están o no habilitados (en el nivel de jerarquía [*edit system processes*]).
- ***Trace*:** puede ver la configuración de los "*traces files*" en los modos de configuración y operacional.
- ***Secret:*** puede ver contraseñas y otras claves de autenticación en la configuración.
- ***Secret-control*:** puede ver contraseñas y otras claves de autenticación, y las puede modificar en el modo configuración.
- ***View*:** puede usar varios comandos para visualizar parámetros del sistema, tabla de enrutamiento, valores de protocolos y estadísticas.
- ***Security*:** puede ver la configuración de seguridad en el modo configuración y usando el comando *show configuration* del modo operacional.
- ***Security-control*:** puede ver y configurar la información de seguridad (en el nivel de jerarquía *[edit security]*).

67. Todos los usuarios que accedan al *switch*, deben encontrarse en una *login class*. Existen cuatro *login classes* predefinidas y que no pueden ser modificadas:

Login Class	*Permission bits*
Operator	*Clear, network, reset, trace, and view*
Read-only	*View*
Super-user	*All*
Unauthorized	*None*

Tabla 4 – Login classes predefinidas en Junos OS

68. Se pueden crear nuevas *login classes* personalizadas para realizar diferentes combinaciones de permisos. A continuación, se muestra un ejemplo en el que se crean tres (3) *login classes*: la primera se llama *observation*, y solo permite ver estadísticas y configuración. Tampoco permite modificar ninguna configuración. La segunda clase se llama *operation* y permite ver y modificar la configuración. La tercera se llama *engineering* y permite ilimitado acceso y control. Las tres (3) clases utilizan el mismo tiempo máximo de inactividad de sesión (*idle timeout*) de 5 minutos. Para definir una *login class*, se incluirá la sentencia de configuración *class*, en el nivel de jerarquía *[edit system login]*:

```
[edit system login]
  class observation {
                idle-timeout 5;
                permissions [ view ];
  }
  class operation {
                idle-timeout 5;
                permissions [ admin clear configure interface interface-control
                network reset routing routing-control snmp snmp-control trace-
                control firewall-control rollback ];
                }
  class engineering {
                idle-timeout 5;
                permissions all;
          }
```

6.2.3.2 CREACIÓN DE CUENTAS DE USUARIO

69. Las cuentas de usuarios se configuran para permitir a los usuarios acceder al dispositivo. Para cada cuenta se define el nombre de usuario (*login name*), la contraseña y, de forma opcional, otros parámetros y metadatos del usuario. Una vez creada la cuenta, se crea automáticamente el directorio *home* del usuario.

70. Para cada cuenta de usuario, se pueden definir los siguientes parámetros:

    - ***Username*** (requerido): nombre que identifica al usuario. Debe ser único en el dispositivo. No debe incluir espacios, dos puntos, ni comas. Tiene un tamaño máximo de 40 caracteres.
    - ***User's full name*** (opcional): nombre completo del usuario. Si incluye espacios, debe ir entre comillas. No incluir dos puntos ni comas.
    - ***User identifier*** (UID) (opcional): identificador numérico que se asocia a la cuenta de usuario. No se recomienda configurar un UID manual, ya que el software automáticamente le asignará uno. Si se configura manualmente debe ser único en el dispositivo.
    - ***User's access privilege*** (requerido): *login class* asignada al usuario.
    - ***Authentication*** (requerido): método de autenticación (*plain-text password*, *encrypted-password*, *SSH key*) y contraseña (si procede) que el usuario utilizará para el acceso.

6.2.3.3 *ROOT*

71. Cuando se instala Junos OS en el dispositivo y este está encendido, ya está listo para configurarse. Al principio, se debe iniciar sesión como usuario *root* sin contraseña.

72. Posteriormente a esta conexión inicial, el administrador **debe configurar la contraseña de *root*.** Para ello, debe seleccionar un método de autenticación de los anteriormente indicados. Esto se hace con la sentencia de configuración *root-authentication* en el nivel de jerarquía [*edit system*]:

```
[edit system]
root-authentication {
    encrypted-password "password"| plain-text-password;
    load-key-file URL filename;
    ssh-ecdsa "public-key" <from hostname>;
    ssh-rsa "public-key" <from hostname>;
}
```

73. Para habilitar el acceso de *root* a través de SSH, se debe configurar a través de la sentencia del modo configuración:

```
system services ssh root-login allow
```

74. El producto dispone de distintas acciones a nivel de *Shell* que solo se pueden llevar a cabo con el nivel de acceso *root*. **Por tanto, la cuenta *root* no debe utilizarse durante el funcionamiento normal, deberá estar restringida a la instalación inicial y a la configuración del dispositivo**.

6.2.3.4 ADMINISTRADOR DE SEGURIDAD

75. Como se ha comentado anteriormente, la cuenta *root* debe utilizarse únicamente en la instalación y configuración inicial del equipo. Para la operativa normal, se recomienda la creación de un **Administrador de Seguridad** con los permisos para poder llevar a cabo, al menos, las siguientes tareas:

    - Administración local (vía consola) y remota (vía SSHv2) del dispositivo.
    - Consultar la versión actual del firmware e iniciar actualizaciones manuales del mismo (verificando que la firma digital del paquete es correcta).
    - Configurar la auditoría: tanto el envío de registros a un servidor *syslog* externo, como los parámetros del almacenamiento local de los registros. Únicamente el administrador de seguridad podrá leer o borrar el fichero de auditoría activo o los archivados.
    - Crear, modificar o borrar cuentas de otros administradores y usuarios, incluyendo los parámetros relacionados con los intentos fallidos de autenticación (*retry-options*, ver apartado 6.2.4 PARÁMETROS DE SESIÓN (*LOGIN SETTINGS*)), el reseteo de sus contraseñas o el desbloqueo de cuentas.
    - Generar las claves de autenticación SSH.
    - Configurar parámetros de sesión, como el banner de acceso o los tiempos máximos de inactividad.
    - Importar certificados al almacén seguro del dispositivo.
    - Configurar el servidor SSH del dispositivo, incluidas las funciones criptográficas.
    - Configurar la fecha y hora del dispositivo.

76. Para crear el administrador de seguridad:

    – Crear una *login class* llamada "*security-admin*" y asignarle el *Permissions Bit "All":*

      [edit]
      user@host# set system login security-admin *permissions all*
      user@host# commit

    – Crear el administrador de seguridad utilizando la sentencia de configuración *edit system login user*, asignándole la *login class*, los datos del usuario y el método de autenticación:

      [edit]

user@host# set system login user Admin_Seguridad *class* security-admin
*authentication encrypted-password "*****"*
user@host# commit

6.2.4 PARÁMETROS DE SESIÓN (*LOGIN SETTINGS*)

77. Los parámetros de intento de sesión que deben configurarse en estos dispositivos son los siguientes:

a) **Intentos fallidos de autenticación (*retry-options*):** Los parámetros relacionados con el comportamiento del dispositivo frente a los intentos fallidos de autenticación de usuarios, se configuran con la sentencia de *retry-options* en el nivel de jerarquía *[edit system login*].

[edit]
user@host# set system login retry-options
tries-before-disconnect number;
backoff-threshold number;
backoff-factor seconds;
maximum-time seconds
minimum-time seconds;

con los siguientes campos:

- *tries-before-disconnect*: umbral de intentos fallidos de autenticación superado el cual, la conexión se cierra. Se permiten valores de 1 a 10. El valor por defecto es 10. **Se recomienda establecer un valor de tres (3) intentos fallidos.**
- *backoff-threshold*: umbral de intentos fallidos de autenticación superado el cual, se inicia un retardo antes de que el usuario pueda introducir de nuevo la contraseña. Se permiten valores de 1 a 3. El retardo se especifica en el parámetro *backoff-factor*, que permite valores de 5 a 10 segundos, siendo 5 el valor por defecto. Con cada intento, el retardo aumenta en el valor configurado. Por ejemplo, si se configura *backoff-factor* a 5 segundos, cuando se superan los intentos fallidos el retardo es de 5 segundos. Si se vuelve a introducir la contraseña incorrecta, el retardo es de 10 segundos, si la introduce de nuevo incorrecta, el retardo es de 15 segundos, etc.
- *maximum-time (seconds):* tiempo máximo que la conexión permanece abierta a la espera de que el usuario introduzca las credenciales de usuario y contraseña. El rango es de 20 a 300 segundos y por defecto está configurado a 120 segundos.
- *minimum-time (seconds):* tiempo mínimo que la conexión permanece abierta mientras el usuario intenta introducir la contraseña. El rango es de 20 a 60 segundos y por defecto está configurado a 40 segundos.

Se recomienda limitar el número de intentos fallidos de autenticación, para evitar los ataques de fuerza bruta.

Una vez el usuario ha superado el número máximo de intentos fallidos de autenticación, y comienza el retardo, el administrador puede manualmente desbloquear al usuario y sacarlo de este estado. Para ello se utiliza el comando *clear system login lockout <username>.*

El administrador puede también ver qué usuarios se encuentran bloqueados y en periodo de retardo, con el comando *show system login lockout*.

Si es el administrador el que se encuentra bloqueado, para salir de este estado deberá conectarse al puerto consola, que ignora los parámetros de bloqueo.

b) ***Login banner***: Se deben configurar *banners*, que se muestran a los usuarios autorizados cuando inician sesión. Hay dos (2) tipos:

   i. Mensaje de inicio de sesión (*login message*) que aparece antes de que el usuario inicie sesión.

   ii. Mensaje de anuncio de inicio de sesión (*login announcement*) que aparece después de que el usuario inicie sesión.

Ambos mensajes se configuran con sentencias de configuración:

```
[edit]
user@host# set system login message login-message-banner-text
    [edit]
user@host# set system login announcement system-announcement-text
```

Si el texto del mensaje contiene algún espacio, deberá encerrarse entre comillas. Se puede dar formato al mensaje con los siguientes caracteres especiales: \n Nueva línea, \t Tabulador horizontal, \' Comilla simple, \" Comilla doble, \\ *backslash*.

Dichos banners deben configurarse de forma que avisen al usuario de la sensibilidad de la información manejada en los equipos, pero no deben dar detalles que puedan facilitar un posible ataque.

c) **Restricción de acceso por fechas y horas**. Se puede restringir el acceso de un usuario a ciertos días a ciertas horas, a través de la *login class* que tenga asignada. Son las propiedades: *allowed-days, access-start, access-end.* Como ejemplo, se define la *login class operador-turnos* con restricción de acceso solo lunes, miércoles y viernes de 8.30 a 15.30h.

```
[edit system]
login {
  class operador-turnos {
    allowed-days [ monday wednesday friday];
    access-start 0830;
    access-end 1530;
          }
   }
```

Se deben crear y asignar las *login class* para que el acceso de los usuarios esté limitado a su jornada laboral. Cualquier acceso fuera de dicho horario deberá estar restringido y aprobado de forma excepcional, en caso de ser necesario.

d) **Tiempo máximo de inactividad de sesión (*idle timeout*):** Como se ha comentado en el apartado 6.2.3.1, cada *login class* lleva asociado el tiempo máximo de inactividad de sesión, a través del parámetro *idle-timeout*. Ese parámetro define el tiempo máximo en minutos, que podrá permanecer inactiva la sesión de un usuario. Inactiva quiere decir, sin recibir entrada de teclado. Transcurrido ese tiempo, la sesión se desconecta de forma automática. Se recomienda establecer un tiempo de inactividad de cinco (5) minutos antes de que la sesión cierre automáticamente.

[edit system login class class-name]
idle-timeout minutes;

Cinco (5) minutos antes de que cumpla el tiempo de inactividad, se irán mostrando mensajes al usuario en la CLI.

user@host# Session will be closed in 5 minutes if there is no activity.
Warning: session will be closed in 1 minute if there is no activity
Warning: session will be closed in 10 seconds if there is no activity
Idle timeout exceeded: closing session

El *idle-timeout* no se puede configurar para las *login class* predefinidas (*operator, read-only, super-user*).

Los usuarios pueden finalizar sus sesiones (locales y remotas). Un usuario puede cerrar una sesión existente escribiendo *logout*, y Junos OS hará que el contenido actual de la sesión sea ilegible después de que el usuario inicie la terminación de sesión. No podrá tener lugar ninguna actividad del usuario hasta que se vuelva a identificar y se autentique.

6.2.5 CONFIGURACIÓN DE SSH

78. El dispositivo utiliza el protocolo SSHv2 para la administración remota, y para la conexión con servidores remotos de auditoría (*syslog*). En ambos casos, el dispositivo actúa como servidor SSH, utilizando las funciones y algoritmos criptográficos implementados por módulo criptográfico OpenSSL (OpenSSH).

79. La siguiente tabla indica las funciones y algoritmos que pueden configurarse para SSHv2, cuando el producto opera en modo de operación seguro.

Establecimiento de claves (*Key Exchange*)	Autenticación (*Authentication*)	Cifrado (*Cipher*)	Autenticación de Mensajes (*Message Auth*)
ECDH-SHA2-NISTP256 ECDH-SHA2-NISTP384 ECDH-SHA2-NISTP521 DH GROUP 14 – SHA1	ECDSA P-256 SSH-RSA	AES CTR 128 AES CTR 256 AES CBC 128 AES CBC 256	HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-512

80. La configuración de SSH debe hacerse con el usuario *root*, en el modo configuración, y con el comando *set system services ssh*. Los pasos son los siguientes:

    – **Especificar los algoritmos para autenticación SSH**. Los algoritmos de clave pública compatible son: ECDSA y RSA.

      Se recomienda seleccionar ECDSA. En caso de seleccionar RSA, la clave SSH generada deberá ser de, al menos, 3072 bits:

      [edit]
      root@host# set system services ssh hostkey-algorithm ssh-ecdsa

    – **Especificar los métodos de Key Exchange.** Los métodos de *Key Exchange* compatibles son: *Diffie-Hellman Group 14* con SHA1, *ECDH* sobre las curvas *nistp256, nistp384, nistp512* y SHA2.

      Dado que *Diffie-Hellman Group 14* no cumple con los requisitos de fortaleza suficiente, por lo que se recomienda seleccionar ECDH:

      [edit]
      root@host# set system services ssh key-exchange ecdh-sha2-nistp256
      root@host# set system services ssh key-exchange ecdh-sha2-nistp384
      root@host# set system services ssh key-exchange ecdh-sha2-nistp521

    – **Especificar los algoritmos de autenticación de mensajes.** Los algoritmos compatibles son: HMAC-SHA1, HMAC-SHA256, HMAC-SHA512. Se recomienda seleccionar SHA256 o SHA512:

      [edit]
      root@host# set system services ssh macs hmac-sha2-256 root@host# set system services ssh macs hmac-sha2-512

    – **Especificar los algoritmos de cifrado.** Los algoritmos compatibles son AES en modos CBC y CTR y claves de 128, 256 bits.

      [edit]
      root@host# set system services ssh ciphers aes128-cbc root@host# set system services ssh ciphers aes256-cbc
      root@host# set system services ssh ciphers aes128-ctr root@host# set system services ssh ciphers aes256-ctr

81. Una vez finalizada la configuración, es posible crear una clave SSH. Para ello:

    – Acceder a la *Shell* del equipo como usuario *root*.

root@host# start shell user root
Password:
root@host%

– Regenerar las *Host Keys:*

root@host% ssh-keygen -t ecdsa -b 384 -f /etc/ssh/ssh_host_dsa_key
root@host% ssh-keygen -t rsa -b 3072 -f /etc/ssh/ssh_host_rsa_key

Estos comandos pueden solicitar una clave, pero se dejará en blanco ya que no se usa para conexiones salientes. Es posible que aparezca un mensaje indicando que la clave ya existe, en este caso hay que sobrescribirla.

6.3 AUTENTICACIÓN CON SERVIDORES EXTERNOS

82. Para usar la autenticación RADIUS en el dispositivo, es necesario configurar la información sobre uno o más servidores RADIUS en la red. El dispositivo consulta los servidores RADIUS en el orden en que están configurados. Si el servidor primario (el primero configurado) no está disponible, el dispositivo intenta contactar a cada servidor en la lista hasta que recibe una respuesta. El detalle de configuración de RADIUS se puede consultar en la *guía Junos OS User Access and Authentication Administration Guide* [REF1], en el apartado *RADIUS Authentication*

83. Para configurar un servidor RADIUS:

– Configurar la dirección IP del servidor RADIUS de autenticación.

[edit groups global access radius-server]
user@host# set server-address

– (Opcional) Configurar la IP de origen de las peticiones que se envían al servidor RADIUS.

[edit groups global access radius-server server-address]
user@host# set source-address source-address

– Configure la contraseña secreta compartida que utiliza el dispositivo de red para autenticarse con el servidor RADIUS.

[edit groups global access radius-server server-address]
user@host# set secret password

La contraseña configurada debe coincidir con la contraseña configurada en el servidor RADIUS. Si la contraseña contiene espacios, debe escribirse entre comillas.

– (Opcional) Especificar el puerto por el que se contactará con el servidor RADIUS si es diferente del puerto por defecto (1812)

[edit groups global access radius-server server-address*]*
user@host# set port port-number

- (Opcional) Configurar la cantidad de veces que el dispositivo intenta comunicarse con el servidor RADIUS y la cantidad de tiempo que el dispositivo espera para recibir una respuesta del servidor.

  [edit groups global access radius-server server-address]
  user@host# set retry number
  user@host# set timeout seconds

- Especificar el orden de la autenticación incluyendo la opción de RADIUS.

  [edit groups global system]
  user@host# set authentication-order [authentication-methods]

- Asignar una clase de inicio de sesión a los usuarios autenticados por RADIUS que no tengan una cuenta de usuario definida localmente.

  [edit groups global system login]
  user@host# set user remote class class

84. De forma predeterminada, Junos OS encamina los paquetes de autenticación, autorización y contabilidad para RADIUS a través de la instancia de enrutamiento predeterminada. También puede encaminar paquetes RADIUS a través de una interfaz de administración en una instancia VRF no predeterminada.
85. Para encaminar paquetes RADIUS a través de la instancia de administración *mgmt_junos*:
    1. Habilitar la instancia de administración *mgmt_junos*.

       [edit system]
       user@host# set management-instance

    2. Configurar la instrucción *mgmt_junos* de la instancia de enrutamiento para el servidor de autenticación RADIUS y el servidor de contabilidad RADIUS, si está configurado.

       [edit system]
       user@host# set radius-server server-address routing-instance mgmt_junos
       user@host# set accounting destination radius server server-address routing-instance mgmt_junos

86. Al igual que ocurre con la autenticación RADIUS, para usar la autenticación TACACS+ en el dispositivo, es necesario configurar la información el servidor TACACS+ en la red. El detalle de configuración de configuración de TACACS+ se puede consultar en la guía *Junos OS User Access and Authentication Administration Guide* [**REF1**], en el apartado *TACACS+ Authentication*.
87. Para configurar un servidor TACACS+:

    - Configurar el orden de autenticación eligiendo TACACS+ como primera opción.

      [edit groups global system]
      user@host# set authentication-order [authentication-methods]

- Configurar la IP y puerto del servidor TACACS+.

  [edit groups global system]
  user@host# set tacplus-server 10.1.110.150 *port* 49

- Configurar la clave compartida con el ACS (Access Control System):

  [edit groups global system]
  user@host# set tacplus-server 10.1.110.150 *secret "*secret"

- Configurar el tiempo en el que la autenticación pasará a la base de datos local si no hay respuesta del TACACS+.

  [edit groups global system]
  user@host# set tacplus-server 10.1.110.150 *timeout* 5

- Definir la Management IP de origen hacia el ACS:

  [edit groups global system]
  user@host# set tacplus-server 10.1.110.150 *source-address* 10.96.105.208

- Habilitar el *accounting* para eventos específicos:

  [edit groups global system]
  user@switch #set accounting events login
  user@switch #set accounting events change-log
  user@switch #set accounting events interactive-commands

- Configurar la IP del servidor de *accounting* ACS:

  [edit groups global system]
  user@switch #set accounting destination tacplus server 10.1.110.150 *secret "*secret"

- Configurar la IP de origen del servidor de *accounting* ACS hacia la IP de gestión del equipo

  [edit groups global system]
  user@switch #set accounting destination tacplus server 10.1.110.150 source-address 10.96.105.208

6.4 GESTIÓN DE CERTIFICADOS

88. Junos OS utiliza certificados X.509v3 para verificar los paquetes de actualización de *firmware*.

89. Estos paquetes llevan una firma digital (tipo ECDSA P-256 con SHA256) junto con el certificado ECDSA, que debe ser validado. Junos OS valida la ruta del certificado (*certificate path*) mediante la construcción de una cadena de certificados basada en el vínculo entre el emisor (*issuer*) y el sujeto (*subject*). Si algún certificado de la cadena falla en la validación, la validación falla en su totalidad. Las cadenas de certificados se validarán hasta el último certificado (*root CA*).

90. El último certificado de la cadena (*root CA*) debe coincidir con uno de los certificados guardados en el almacenamiento de confianza (*trust store*) del dispositivo o, al menos, debe haber sido emitido (*issued*) por uno de ellos. No es necesario realizar ninguna configuración en el dispositivo para esta verificación de seguridad.

6.5 SINCRONIZACIÓN

91. Los equipos deben estar correctamente sincronizados. Para definir la fecha y hora del equipo, se debe ejecutar el siguiente comando en el modo operacional. Como ya se ha comentado, al ser un comando del modo operacional, no es necesario hacer el *commit* de la configuración:

    root@switch> set date YYYYMMDDhhmm.ss

92. Los switches EX y QFX pueden actuar como cliente de algunos servicios, como el protocolo de tiempo de red (NTP). Dicho protocolo puede configurarse para obtener la hora del sistema de los servidores NTP que están conectados en la red.

93. El comando de configuración utilizado para configurar los equipos como cliente del servidor NTP externo es el siguiente:

    [edit]
    root@switch# set system ntp server <ntp_server_ip>

94. **Se debe configurar autenticación en los servidores NTP mediante SHA-256** para asegurar que el servidor es fiable.

    [edit]
    root@switch# set system ntp authentication-key 2 type sha256 value "key_value"

6.6 ACTUALIZACIONES

95. Se puede verificar la versión actual del *firmware* del dispositivo utilizando el comando CLI: *show versión local* y, si existe una nueva versión disponible, se puede iniciar la actualización manual.

96. Junos OS no proporciona actualizaciones parciales, sino versiones (*releases*) completas. No existe proceso de actualización automática, todas las actualizaciones deben llevarse a cabo de forma manual.

97. El procedimiento de actualización es el mismo que el descrito en el apartado 5 FASE DE INSTALACIÓN.

98. El paquete instalable de *firmware* para los switches EX4600 y QFX5100 está firmado digitalmente (firma ECDSA P-256 con SHA256) y proporciona una cadena de certificados ECDSA que deben finalizar con el certificado de una CA interna. Cuando se procede a la instalación del paquete, Junos OS valida automáticamente las firmas y los certificados de la cadena usados para firmar el paquete. Si se determina que la firma o alguno de los certificados no son válidos (por ejemplo, cuando un certificado haya expirado el periodo de validez, o no se pueda verificar con la *CA root* almacenada en el dispositivo), el proceso de instalación falla.

99. El proceso de verificación del certificado utiliza una lista CRL (*Certificate Revocation List*) almacenada en el almacén de confianza (*trust store*) de la caché local del dispositivo. Durante una actualización de *firmware*, se carga una CRL actualizada, ya que está embebida en el binario de *firmware*. Si el certificado a validar no está presente en la lista de certificados revocados, la validación se realiza correctamente. Si la CRL no está disponible en la caché de Junos OS, la validación del certificado falla.

100. El Kernel de Junos OS mantiene una serie de huellas digitales (*fingerprints*) de los ficheros ejecutables y otros ficheros inmutables del sistema operativo. Estas huellas se encuentran en un fichero que se llama "*manifest file*". Este fichero, a su vez, se firma y verifica con la misma clave de firma del paquete de *firmware*.

101. Cuando se emite el comando para instalar una actualización, el *manifest file* de la actualización se verifica y almacena. A partir de las huellas incluidas en el *manifest file*, los archivos ejecutables y otros archivos inmutables se verifican antes de que se ejecuten. Si la verificación no es correcta, los archivos no podrán ejecutarse.

6.7 AUTO-CHEQUEOS

102. Junos OS ejecuta una serie de auto-chequeos durante el arranque del dispositivo para verificar su correcta operación. Estos chequeos se llevan a cabo siempre, incluso si el dispositivo no tiene el modo de operación seguro habilitado. Los auto-chequeos son los siguientes:

- **Tests de arranque (*Power on tests*)**: determinan que el dispositivo de arranque (*boot-device*) responde, y realiza una verificación del tamaño de la memoria para confirmar la cantidad de memoria disponible.
- **Tests de integridad de archivos (File Integrity Tests):** verifican la integridad de todos los paquetes de *software* montados, para comprobar que los archivos del sistema no han sido alterados. Para probar la integridad del firmware, las huellas digitales (*fingerprints*) de los ejecutables y de otros archivos inmutables se validan a través de huellas digitales contenidas en el *manifest file*.
- **Tests de integridad criptográfica (*Crypto integrity tests*)**: verifican la integridad de los parámetros críticos de seguridad (CSPs), como las *SSH Host Keys.*
- **Errores de autenticación (*Authentication errors*)**: verifica que "*veriexec*", el cual es un subsistema de integridad de archivos basado en el kernel que garantiza que solo se puedan ejecutar los binarios autorizados, está habilitado y funciona correctamente utilizando */opt/sbin/kats/cannot-exec.real.*
- **Tests KAT (*Known Answer Tests*):** se realizan sobre los módulos criptográficos Kernel, LibMD y OpenSSL. Los tests KAT ejecutan cada algoritmo criptográfico con datos para los que ya se conoce la salida correcta (respuesta conocida). La salida calculada se compara con la respuesta conocida. Si no son idénticos, el test KAT falla.

103. Si los tests se completan con éxito, se actualizan los registros de auditoría con los resultados de las pruebas ejecutadas, y el dispositivo arranca correctamente.

104. Si, por el contrario, alguno de los test falla, se registra el error en los registros de auditoría y el dispositivo entra en estado de fallo y se reinicia, dejando de procesar el tráfico por los interfaces e impidiendo cualquier entrada de línea de comandos.

105. Cuando el dispositivo se reinicia, debe volver a pasar todos los auto chequeos.

6.8 ALTA DISPONIBILIDAD

106. Los switches de la serie EX y QFX de Juniper Networks admiten Virtual Chassis (VC), una tecnología flexible y escalable con la que puede conectar conmutadores individuales para formar una unidad y configurar y administrar la unidad como un solo chasis. Los puertos de chasis virtual (VCP) conectan los conmutadores miembros para formar un chasis virtual y son responsables de pasar todos los datos y controlar el tráfico entre los conmutadores miembros.

107. Es posible conectar hasta diez (10) QFX5100 o EX4600 en el mismo VC.

108. Es posible configurar el chasis virtual con:

a) **Configuración no aprovisionada:** sin aprovisionamiento, el primario asigna secuencialmente un ID de miembro a otros conmutadores miembros y determina la función de cada conmutador miembro mediante el valor de prioridad del rol principal y otros factores en el algoritmo de elección del rol principal.

b) **Configuración pre-aprovisionada:** con el aprovisionamiento previo, se puede controlar de manera determinista el ID de miembro y el rol asignado a un conmutador de miembro vinculándolo a su número de serie.

109. Para configurar el chasis virtual con una configuración no aprovisionada:

- Encender el switch designado como primario.
- Completar la configuración inicial indicada como tal en el apartado 5 FASE DE INSTALACIÓN.
- (Opcional) Configurar el conmutador principal con la interfaz Ethernet de administración virtual (VME) para la administración fuera de banda del chasis virtual:

  user@host# set interfaces vme unit 0 family inet address /ip-address/mask/

- (Opcional) Configurar la prioridad del rol principal para los switches miembros:

  [edit virtual-chassis]
  user@host# set member 0 mastership-priority 255
  user@host# set member 1 mastership-priority 255

- (Opcional) En el miembro primario, deshabilitar la funcionalidad "*Split and merge*":

[edit virtual-chassis]
user@switch# set no-split-detection

- Aplicar la configuración con *commit*.
- Encender el resto de switches miembros del VC.
- En cada switch miembro, configurar los puertos que se utilizarán para interconectar los switches miembros como VCPs:

  user@switch> request virtual-chassis vc-port set pic-slot pic-slot-number port port-number local

  La sentencia "local" solo aplica en los VC de EX4600.
- Los VCP se agrupan automáticamente en un grupo de agregación de enlaces cuando dos o más interfaces de la misma velocidad se configuran en VCP entre los mismos dos conmutadores miembros.

110. Para configurar el chasis virtual con una configuración pre-aprovisionada:

- Listar los números de serie de todos los switches que se conectarán en una configuración de chasis virtual.
- Anotar la función deseada (*routing-engine* o *line-card*) de cada switch. Si configura el miembro con una función de *routing-engine* es seleccionable para funcionar en la función principal o de respaldo. Si configura al miembro con un rol de *line-card*, no será seleccionable para funcionar en el rol principal o de respaldo.
- Enceder el switch que va a ser el switch primario.
- Completar la configuración inicial.
- (Opcional) Configurar el conmutador principal con la interfaz VME para la administración fuera de banda del chasis virtual:

  user@host# set interfaces vme unit 0 family inet address /ip-address/mask/
- Especificar el modo de configuración pre-aprovisionada:

  [edit virtual-chassis]
  user@switch# set preprovisioned
- Especificar todos los miembros que desea incluir en el VC, enumerando el número de serie de cada switch con el ID de miembro y el rol deseados:

  [edit virtual-chassis]
  user@switch# set member 0 serial-number abc123 role routing-engine
  user@switch# set member 1 serial-number def456 role routing-engine
  user@switch# set member 2 serial-number ghi789 role line-card
  user@switch# set member 3 serial-number jkl012 role line-card
- (Opcional) Deshabilitar la funcionalidad "*Split and merge*":

  [edit virtual-chassis]

user@switch# set no-split-detection

- Aplicar la configuración con un "*commit*".
- Encender el resto de switches miembros del VC.
- En cada switch miembro, configurar los puertos que se utilizarán para interconectar los switches miembros como VCPs:

  user@switch> request virtual-chassis vc-port set pic-slot pic-slot-number port port-number local

  La sentencia "local" solo aplica en los VC de EX4600.
- Los VCP se agrupan automáticamente en un grupo de agregación de enlaces cuando dos o más interfaces de la misma velocidad se configuran en VCP entre los mismos dos conmutadores miembros.

6.9 AUDITORÍA

111. Para un entorno de Junos OS seguro es necesario auditar los eventos y almacenarlos en un archivo de auditoría local. Los eventos registrados se pueden enviar de manera simultánea a un servidor de syslog externo.

112. En este apartado se indica cómo configurar, en pasos generales, la función de auditoría del dispositivo. Se recomienda consultar más información en la guía *Junos OS Network Management and Monitoring Guide (Cap 11 – System Log Messages).* **[REF.4]**.

6.9.1 REGISTRO DE EVENTOS

113. Se recomienda configurar la auditoría en el dispositivo para que registre, al menos, los siguientes eventos:

- Cambios de configuración sobre los datos secretos de claves.
- Cambios confirmados (*commits*).
- Inicio y cierre de sesiones de los usuarios.
- Arranque del sistema.
- Intentos fallidos se establecer una sesión SSH.
- Establecimiento o finalización de una sesión SSH.
- Cambios en la hora del sistema.
- Finalización de una sesión remota por parte del mecanismo de bloqueo de sesión.
- Finalización de una sesión interactiva.
- Modificación o supresión de claves criptográficas.
- Restablecimiento de contraseñas.

- Todos los cambios de configuración.

114. Como se indica en el siguiente apartado, los eventos a registrar se especificarán mediante las sentencias *Facility* y *Severity Level* del nivel de jerarquía *[edit system syslog]*.

115. La estructura de un mensaje de auditoría es la que se indica en la siguiente tabla. Para cada campo, se incluye como ejemplo su valor para el mensaje de auditoría:

Jul 24 17:43:28 switch1 mgd [4163]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set: [system radius-server 1.2.3.4 secret]

Campo	Descripción	Ejemplo
Timestamp	Fecha/Hora en la que se generó el mensaje, representada de una de las dos siguientes maneras: ▪ ***MMM-DD HH:MM:SS.MS+/-HH:MM*** corresponde al mes, día, hora, minuto, segundo y milisegundo en hora local. Las horas y los minutos que aparecen detrás del signo más (+) o del signo menos (-) representan la diferencia horaria entre la hora local y el Tiempo Universal Coordinado (UTC). ▪ ***YYYY-MM-DDTHH:MM:SS.MSZ*** corresponde al año, mes, día, hora, minuto, segundo y milisegundo en UTC.	*Jul 24 17:43:28* es la marca de tiempo expresada en la hora local de Estados Unidos.
Hostname	Nombre del *host* que creó el mensaje original.	Switch1
Process	Nombre del proceso de Junos OS que generó el mensaje.	mgd
ProcessID	ID del proceso (PID) UNIX Junos OS que generó el mensaje.	4163
TAG	Etiqueta del mensaje que identifica el mensaje unívocamente.	UI_CFG_AUDIT_SET_SECRET
username	Nombre del usuario que inició el evento.	«admin»
message-text	Descripción del evento.	set: [system radius-server 1.2.3.4 secret]

Tabla 5 – Estructura de los mensajes de auditoría

116.A continuación, se muestran algunos ejemplos de registros de auditoría:

Tipo	Mensaje de auditoría generado
Inicio y Fin de sesión SSH	Los siguientes registros, son el resultado de un intento fallido de autenticación, seguido de un intento correcto y, finalmente, la finalización de la sesión. *Dec 20 23:17:35 bilbo sshd[16645]: Failed password for op from 172.17.58.45 port 1673 ssh2* *Dec 20 23:17:53 bilbo sshd[16645]: Accepted password for op from 172.17.58.45 port 1673 ssh2* *Dec 20 23:17:53 bilbo mgd[16648]: UI_AUTH_EVENT: Authenticated user 'op' at permission level 'j-operator'* *Dec 20 23:17:53 bilbo mgd[16648]: UI_LOGIN_EVENT: User 'op' login, class 'j-operator' [16648]* *Dec 20 23:17:56 bilbo mgd[16648]: UI_CMDLINE_READ_LINE: User 'op', command 'quit '* *Dec 20 23:17:56 bilbo mgd[16648]: UI_LOGOUT_EVENT: User 'op' logout*
Reinicio del dispositivo y arranque de la función de auditoría	*Dec 20 23:17:35 bilbo syslogd: exiting on signal 14* *Dec 20 23:17:35 bilbo syslogd: restart* *Dec 20 23:17:35 bilbo syslogd /kernel: Dec 20 23:17:35 init: syslogd (PID 19128) exited with status=1* *Dec 20 23:17:42 bilbo /kernel:* *Dec 20 23:17:53 init: syslogd (PID 19200) started*

Tabla 6 – Ejemplo de mensajes de auditoría

6.9.2 ALMACENAMIENTO LOCAL

117.Los registros de auditoría se almacenan localmente en */var/log*. Para configurar el almacenamiento local de los registros de auditoría, se utiliza el usuario *root*, con modo configuración y el nivel de jerarquía *[edit system syslog].*

118.A través de sentencias de configuración en este nivel de jerarquía, se especifican varios parámetros, como el nombre del archivo que almacenará los registros de auditoría (por ejemplo, *logfile*), el tamaño máximo de este archivo (hasta 128 KB para EX4600 y hasta 1 MB para QFX5100) o el número de archivos de auditoría que se irán almacenando (10 por defecto).

119.un archivo de registro activo llamado, por ejemplo, *logfile*, alcanza el tamaño máximo configurado, la utilidad de *logging* cierra el archivo, lo comprime y lo renombra como

logfile.0.gz. La utilidad de *logging* abre y escribe en un nuevo archivo activo *logfile*. Este proceso se conoce como **rotación de archivos**. Cuando el nuevo *logfile* alcanza el tamaño máximo configurado, *logfile.0.gz* es renombrado a *logfile.1.gz*, y *logfile* se cierra, comprime y renombra como *logfile.0.gz*. Se crearán tantos *logfile.X.gz* como se haya configurado (parámetro *archive file*). Cuando se alcanza este número máximo de archivos configurado, y cuando el tamaño del archivo activo (*logfile*) alcanza el tamaño máximo configurado, se sobrescribe el archivo almacenado más antiguo, con el archivo activo actual.

120. Otra de las sentencias de configuración a tener en cuenta dentro de la jerarquía [*edit system syslog*] es *log-rotate-frequency*, que configura cada cuánto tiempo la utilidad de logging comprobará el tamaño del archivo de registros (*logfile*). El intervalo puede ser de 1 a 59 minutos, siendo 15 minutos el valor por defecto.

121. Para especificar el tipo de mensajes que se deben registrar, se utilizan los parámetros *Facility* y *Severity Level* del nivel de jerarquía [*edit system syslog*], que pueden tomar los valores indicados en las siguientes tablas:

Facility	Tipo de mensajes
kernel	Acciones realizadas o errores encontrados por el kernel de Junos OS.
user	Acciones realizadas o errores encontrados por los procesos del espacio de usuarios.
daemon	Acciones realizadas o errores encontrados por los procesos del sistema.
authorization	Intentos de autenticación y autorización.
ftp	Acciones realizadas o errores encontrados por los procesos FTP.
ntp	Acciones realizadas o errores encontrados por los procesos NTP.
security	Eventos o errores relacionados con la seguridad.
dfc	Eventos relacionados con la captura dinámica de flujo.
external	Acciones realizadas o errores encontrados por las aplicaciones locales externas.
firewall	Acciones de filtrado de paquetes realizadas por el filtro del firewall.
pfe	Acciones realizadas o errores encontrados por el motor de reenvío de paquetes (*Packet Forwarding Engine*).
conflict-log	Cuando la configuración especificada no es válida para el tipo de dispositivo.
change-log	Cambios de la configuración de Junos OS.
interactive-commands	Comandos emitidos por CLI de Junos OS o por una aplicación cliente, como un protocolo XML de Junos o un cliente XML NETCONF.
any	Todas las *facilities*.

Tabla 7 – Valores para *Facility*

Severity Level	Tipo de mensajes
none	Deshabilita el logging de todos los mensajes de la facility seleccionada.
emergency	Panic del sistema o cualquier otra condición que cause que el dispositivo deje de funcionar.
alert	Condiciones que requieren corrección inmediata, como una base de datos del sistema dañada.
critical	Condiciones críticas, como errores hardware.
error	Condiciones de error que generalmente tienen consecuencias menos graves que los errores en los niveles de emergencia, alerta y crítico.
warning	Condiciones que requieren monitorización.
notice	Condiciones que no suponen un error, pero podrían necesitar un manejo especial.
info	Eventos o condiciones de interés, que no suponen un error.
any	Incluye todos los niveles de severidad.

Tabla 8 – Valores para *Severity Level*

122.A continuación, se incluye un ejemplo de cómo configurar la auditoría:

- Especificar el número de archivos que almacenarán los eventos de auditoría:

  [edit system syslog]

  root@host#set archive files 2

- Especificar el nombre del archivo de registros de auditoría y el tipo de eventos a registrar (todos):

  [edit system syslog]

  *root@host#set **file** logfile any any*

- Especificar el tamaño del archivo de registros de auditoría:

  [edit system syslog]

  *root@host#set **file** logfile archive size 1m*

- Especificar que se registre la prioridad (*Facility* y *Severity Level*) en los mensajes.

  [edit system syslog]

  root@host#set file logfile explicit-priority

- Es recomendable registrar los mensajes del sistema de manera estructurada (formato de protocolo *syslog* especificado en la RFC 5424) en lugar de formato Junos OS. En este formato, la prioridad del mensaje se registra por defecto y el paso anterior no sería necesario.

  [edit system syslog]

  *root@host#set **file** logfile structured-data*

123. Deberá limitarse la capacidad de leer y borrar tanto el fichero activo, como los ficheros almacenados de registros de auditoría, al Administrador de Seguridad (ver apartado 6.2.3.4 ADMINISTRADOR DE SEGURIDAD). Esta capacidad corresponde al permiso "*maintenance*" de forma que la *login class* que se asigne al Administrador de Seguridad deberá disponer de este permiso (ver apartado 6.2.3.1 LOGIN CLASSES Y PERMISOS).

6.9.3 ALMACENAMIENTO REMOTO

124. Se recomienda configurar el dispositivo para el envío de los registros de auditoría a un servidor *syslog* remoto. Para ello se utilizará el protocolo NETCONF sobre SSH.

125. El servidor *syslog* remoto actuará de cliente SSH. Se debe generar una pareja de claves pública/privada SSH en el servidor *syslog*. **Se deben generar claves RSA de 3072 bits o superior, o claves ECDSA**. Por ejemplo:

$ ssh-keygen -b 3072 -t rsa -C 'syslog-monitor key pair' -f ~/.ssh/syslog-monitor

126. Se solicitará introducir una frase de contraseña. Se mostrará la ubicación del almacenamiento del par de claves (*syslog-monitor*).

127. En el dispositivo, se debe crear una *login class* llamada, por ejemplo, *monitor*, con permisos para rastrear eventos (*permission bit: trace*):

[edit]

user@host# set system login class monitor permissions trace

128. Se debe crear el usuario con el que el servidor *syslog* se conectará al dispositivo. El usuario se llamará "*syslog-mon*" y se asignará la *login class* creada (*monitor*). El tipo de autenticación será clave pública SSH y la clave será la generada en el servidor *syslog*.

[edit]

user@host# set system login user syslog-mon class monitor authentication ssh-rsa

"ssh-rsa xxxxx syslog-monitor key pair"

129. A continuación, se debe configurar el protocolo NETCONF con SSH. Para ello:

- Incluir una de las siguientes declaraciones en el nivel de jerarquía de configuración indicado:
  a. Para habilitar el acceso al subsistema NETCONF SSH usando el puerto *NETCONF-over-SSH* predeterminado (830) como lo especifica RFC 4742, incluir la declaración *netconf ssh* en el nivel de jerarquía [*edit system services*]:

     [edit system services]

     user@host# set netconf ssh

b. Para habilitar el acceso al subsistema NETCONF SSH usando un número de puerto específico, se debe configurar la declaración de puerto con el número de puerto deseado en el nivel de jerarquía [*edit system services]:*

[edit system services]

user@host# set netconf ssh port port-number

c. Para habilitar el acceso al subsistema NETCONF SSH usando el puerto SSH predeterminado (22), se debe incluir la instrucción *set ssh* en el nivel de jerarquía [*edit system services*]. Esta configuración permite el acceso SSH al dispositivo para todos los usuarios y aplicaciones. La instrucción se puede incluir en la configuración además de las instrucciones de configuración enumeradas anteriormente.

[edit system services]

user@host# set ssh

- (Opcional) Habilitar Junos OS para desconectar a los clientes NETCONF que no responden especificando el intervalo de tiempo de espera (en segundos) después del cual, si no se han recibido datos del cliente, el proceso *sshd* solicita una respuesta, así como el umbral de cliente perdido activo. respuestas que desencadenan una desconexión.

  [edit system services]

  user@host# set netconf ssh client-alive-interval 10

  user@host# set netconf ssh client-alive-count-max 10

- Se debe aplicar la configuración.

  [edit]

  user@host# commit

- Se deben seguir los pasos anteriores en cada dispositivo que ejecute Junos OS donde la aplicación cliente establezca sesiones NETCONF.

130. En el servidor *syslog* remoto, es necesario iniciar el agente SSH y añadir el par de claves generadas (syslog-monitor).

$ eval `ssh-agent`

$ ssh-add ~/.ssh/syslog-monitor

131. En el servidor *syslog* remoto, iniciar la conexión NETCONF con el dispositivo, usando el usuario *syslog-mon*:

$ ssh syslog-mon@nombre_dispositivo -s netconf > Fichero_logs.out

132. Una vez la conexión NETCONF está establecida, configurar la transmisión de mensajes de eventos. Esta RPC hará que el servicio NETCONF empiece a transmitir mensajes a través de la conexión SSH que se ha establecido.

<rpc><get-syslog-events><stream>messages</stream></get-syslog-events></rpc>

133. Una vez finalizada la configuración, se debe:

- **Monitorizar el registro de eventos** que se genera en el dispositivo, por ejemplo, para las acciones de administración, y que recibe el servidor de *syslog*. Se deben comparar para verificar que son los mismos.
- **Examinar el tráfico entre el servidor *syslog* y el dispositivo**, para comprobar que no se puede acceder a estos datos durante la transferencia y que el servidor *syslog* los recibe bien.

6.10 COPIAS DE SEGURIDAD

134. **Se debe realizar un *backup* de la configuración de los equipos**. Para realizarlo, se debe utilizar el siguiente comando:

user@switch request system software configuration-backup path

135. Este comando guardar la configuración actualmente activa y cualquier parámetro específico de la instalación. La dirección especificada puede ser una ubicación local o un servidor externo. Se recomienda almacenar las copias de seguridad en un servidor externo mediante SCP o SFTP, por ejemplo:

user@switch request system software configuration-backup scp://ftp.test.net/test

136. Se resalta que este comando no guarda los logs. Para ello, sería necesario:

- Ingresar el siguiente comando para archivar el directorio */var/log*. El siguiente comando comprimirá (tar) la carpeta */var/log* y nombrará el archivo (*logs.tar*). También enviará el archivo comprimido a la carpeta de destino */var/tmp.*

  root@host> file archive source /var/log destination /var/tmp/LOGS

  root@host> file list /var/tmp

  /var/tmp:

  .snap/

  *LOCK_FILE**

  LOGS.tar <--Archivo creado

- Exportar los logs vía SCP o SFTP.

7. FASE DE OPERACIÓN Y MANTENIMIENTO

137. El correcto funcionamiento del producto requiere de características que deben estar presentes en el entorno. Es la responsabilidad del Administrador autorizado asegurar que el **entorno operacional cumple con los siguientes requisitos**:

    a) El producto estará instalado y será mantenido en un entorno físico seguro. Esto incluye un edificio seguro con control de acceso, o un entorno móvil controlado por el administrador.

    b) El producto no contendrá ninguna aplicación de uso general como compiladores o aplicaciones de usuario.

    c) Los administradores deben asegurar con otras medidas de seguridad complementarias, el tráfico que atraviesa el producto, puesto que este no presenta ese tipo de funcionalidad.

    d) Los administradores deben estar correctamente formados en el uso y la correcta operación del producto, así como en las características del entorno seguro en que está presente. Al mismo tiempo, los administradores seguirán las guías e indicaciones presentes.

    e) Los administradores se asegurarán de que el producto cuenta con las últimas actualizaciones de *firmware* y *software* para preservar al mismo de amenazas y vulnerabilidades conocidas.

    f) Los administradores mantendrán sus credenciales de acceso al producto seguras y protegidas.

    g) Los administradores deben eliminar toda la información residual sensible que pudiera quedar resultante de operar con el producto después de terminar la vida útil de este.

7.1 MONITORIZACIÓN DE LOS REGISTROS DE AUDITORÍA

138. El Administrador de Seguridad debe realizar un correcto seguimiento y mantenimiento de los registros de auditoría, asegurando que no son borrados, modificados ni accedidos por agentes no autorizados.

139. Del mismo modo, procesará la información que contienen con el fin de agilizar el proceso de respuesta y/o mitigación de potenciales problemas de seguridad.

140. Entre los registros de mayor importancia se encuentran los relacionados con acciones administrativas, cambios de configuración, fallo de las funciones de seguridad y acceso al producto por cualquiera de sus vías.

141. Para consultar los registros de auditoría (con los permisos administrativos pertinentes) a través de CLI, ejecutar la siguiente sentencia:

    user@host> show log filename

142. La política de *backup* deberá tener en cuenta los registros de auditoría. Considerando el número máximo de registros que se almacenan y su tamaño máximo, se debe

realizar un *backup* de los mismos antes de que sean sobrescritos (por alcanzar el máximo número de ficheros, o por falta de espacio de almacenamiento) para así cumplir con los requisitos de mantenimiento de *logs* que sean de aplicación al sistema.

7.2 COPIAS DE SEGURIDAD

143. Se deben realizar copias de seguridad periódicas de forma automatizada y centralizada de la configuración actual del producto y de la información sensible que pueda contener. Esto ayuda a garantizar, en la medida de lo posible, la respuesta a incidentes de disponibilidad y pérdida de información.

7.3 COMPROBACIÓN DE LA INTEGRIDAD Y ACTUALIZACIONES

144. Se debe comprobar periódicamente la integridad del *hardware* y del *software* que compone el producto con el fin de detectar y/o mitigar posibles problemas de seguridad derivados de la presencia de malware y/o técnicas de *tampering*.

145. Los Administradores de Seguridad se encargarán de la actualización regular del *firmware*, con el fin de solventar los problemas de seguridad presentes y potenciales conocidos. De la misma manera que el propio producto, las actualizaciones serán verificadas y siempre obtenidas por vías aceptadas y reconocidas por el fabricante.

8. CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Despliegue en un entorno seguro	☐	☐	
Registro de la licencia del producto	☐	☐	
Registro de las licencias	☐	☐	
Descarga e Instalación del *firmware*	☐	☐	
CONFIGURACIÓN			
CONFIGURACIÓN DEL MODO DE OPERACIÓN SEGURO			
Activación del comando que establece el modo de operación seguro	☐	☐	
CONFIGURACIÓN DE AUTENTICACIÓN			
Establecimiento contraseñas / clave pública	☐	☐	
Establecimiento de política de contraseñas	☐	☐	
Configuración de servidores externos de autenticación	☐	☐	
CONFIGURACIÓN DE USUARIOS DE ADMINISTRACIÓN			
Creación de cuentas de usuario	☐	☐	
Creación del Administrador de Seguridad	☐	☐	
CONFIGURACIÓN DE LOS PARÁMETROS DE SESIÓN			
Configuración de tiempos de sesión e intentos de login	☐	☐	
Configuración del b*anner* de inicio de sesión	☐	☐	
Configuración de restricciones de acceso por fecha y hora	☐	☐	
CONFIGURACIÓN DE CONEXIONES SEGURAS			
Configuración segura de SSH	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
CONFIGURACIÓN DE LA SINCRONIZACIÓN HORARIA			
Configuración de fecha y hora local	☐	☐	
Configuración del servidor NTP	☐	☐	
CONFIGURACIÓN DE ACTUALIZACIONES			
Comprobación de las actualizaciones disponibles	☐	☐	
CONFIGURACIÓN DE ALTA DISPONIBILIDAD			
Configuración del chasis virtual	☐	☐	
CONFIGURACIÓN DE AUDITORÍA			
Configuración de eventos en el almacenamiento local	☐	☐	
Creación del usuario *syslog-mon*			
Configuración del protocolo NETCONF	☐	☐	
Configuración del envío de eventos al servidor remoto (*syslog*)	☐	☐	
COPIAS DE SEGURIDAD			
Realización del *backup* de la configuración de los equipos	☐	☐	
Realización del *backup* de los logs del sistema	☐	☐	

9. REFERENCIAS

REF1 *Junos® OS User Access and Authentication Administration Guide*
https://www.juniper.net/documentation/us/en/software/junos/user-access/index.html

REF2 *CLI User Guide*
https://www.juniper.net/documentation/us/en/software/junos/cli/topics/topic-map/getting-started.html

REF3 *Junos® OS Common Criteria Evaluated Configuration Guide for EX4300, EX4600, and QFX5100 Devices*
https://www.juniper.net/documentation/en_US/junos-cc18.1/information-products/pathway-pages/switches/18.1R1/18.1R1-ex4300-ex4600-qfx5100-cc-guide.html

REF4 *Junos® OS Network Management and Monitoring Guide*
https://www.juniper.net/documentation/us/en/software/junos/network-mgmt/index.html

REF5 *Guía de Seguridad de las TIC CCN-STIC 821 Apéndice V: Normas de Creación y uso de Contraseñas NP40*
https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/534-ccn-stic-821-normas-de-seguridad-en-el-ens-anexo-v/file.html

10.ABREVIATURAS

CA	*Certification Authority*
CLI	*Command-Line Interface*
CPD	Centro de Procesamiento de Datos
CRL	*Certificate Revocation List*
ENS	Esquema Nacional de Seguridad.
EULA	*End User License Agreement*
FTP	*File Transfer Protocol*
KVM	*Kernel-based Virtual Machine*
NTP	*Network Time Protocol*
OS	*Operating System*
RBG	*Random Bit Generator*
SCP	*Secure Copy*
SFTP	*Secure File Transfer Protocoll*
SSH	*Secure Shell*
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