centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1474

Procedimiento de Empleo Seguro
iMaster NCE Campus

Octubre 2025

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

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-26-129-1

Fecha de Edición: Octubre de 2025

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.05.05 10:32:32 +02'00'

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1 INTRODUCCIÓN

1. iMaster NCE Campus, es una plataforma unificada que gestiona, controla y mantiene redes SDN basadas en la nube. NCE puede utilizarse en escenarios de servicios carrier, empresariales y residenciales.
2. iMaster NCE Campus es un sistema de software para la gestión de redes en la nube y se sitúa en la capa de gestión y control de la red basada en la nube. Puede gestionar y controlar dispositivos de red ubicuos, incluidos dispositivos de transporte, IP y acceso. Proporciona interfaces abiertas para integrarse rápidamente con sistemas de aplicaciones de capa superior, como orquestadores de servicios OSS y aplicaciones de servicios. Se pueden desarrollar y personalizar varias aplicaciones para acelerar la innovación de los servicios y lograr operaciones de estilo comercio electrónico.
3. iMaster NCE Campus es un sistema basado en la nube que utiliza una arquitectura de software orientada a servicios. Se despliega en una plataforma virtualizada y puede escalarse con flexibilidad.
4. Basado en la plataforma en nube, NCE implementa tres módulos lógicos (gestión de red, control de red y análisis de red) y varias aplicaciones orientadas a escenarios como servicios y componentes. Esto permite a los clientes desplegar NCE de forma flexible y modular para satisfacer sus requisitos específicos.

2 OBJETO Y ALCANCE

5. El presente documento tiene como objetivo detallar las configuraciones de seguridad de iMaster NCE Campus con el ***firmware V300R023C00SPC010T***, de forma que la protección y funcionamiento del producto se realice de acuerdo con unas garantías mínimas de seguridad.
6. La configuración evaluada del producto y por lo tanto incluida en la presente guía de empleo seguro consiste en solo el software el cual se supone que está instalado en un servidor de hardware no especificado.
7. El producto iMaster NCE Campus ha sido cualificado en el catálogo CPSTIC para categoría ENS ALTA en la familia “Redes definidas por software (SDN)”.

3 ORGANIZACIÓN DEL DOCUMENTO

8. Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.
9. Apartado 5. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.
10. 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.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

11. Al tratarse de una combinación *hardware/software*, iMaster NCE Campus toda la información y servidores del producto necesario se entregan por correo ordinario. Se debe comprobar:

    - **Información de envío.** Se debe comprobar la documentación de envío para verificar que concuerda con la orden de compra original y que el envío ha sido realizado por Huawei.
    - **Embalaje externo.** Se debe inspeccionar el embalaje y la cinta de embalaje con la marca de Huawei. Se debe comprobar que la cinta esté intacta y que no haya sido cortada ni se haya deteriorado en ningún punto. Además, se debe inspeccionar que la caja no presente cortes ni daños que permitan acceder al dispositivo.
    - **Embalaje interno.** Se debe comprobar el embalaje interior de la misma manera que el embalaje exterior. Adicionalmente, se debe comprobar que la etiqueta presente en el embalaje exterior concuerda con el modelo de dispositivo adquirido.
    - **Sello de garantía.** Se deberá verificar que la placa de identificación del producto, alojada en el chasis, es consistente con la etiqueta del embalaje del producto.

12. En caso de que exista algún desperfecto o alguna inconsistencia será necesario contactar con el soporte de Huawei de manera inmediata para recibir instrucciones. No se recomienda realizar la instalación en este caso.

4.2 ENTORNO DE INSTALACIÓN SEGURO

13. Los componentes del producto deben instalarse en un entorno en el cual solo el personal técnico dispone de autorización para la configuración, despliegue y mantenimiento del producto.

4.3 REGISTRO Y LICENCIAS

14. Existen dos (2) tipos de licencias para los dispositivos iMaster NCE Campus*:*

    - **Licencia COMM**: la mayoría de las licencias adquiridas por contrato tienen una validez permanente, aunque puede darse el caso de que algunas tienen un período de validez hasta una fecha determinada.
    - **Licencia DEMO**: son licencias usadas para casos especiales como pruebas o evaluaciones.

15. Para registrar la licencia se necesita contar con el archivo de licencia. Para obtener dicho archivo, se debe obtener la contraseña de activación en el "*Proof of Entitlement*" que se recibe al adquirir el producto.

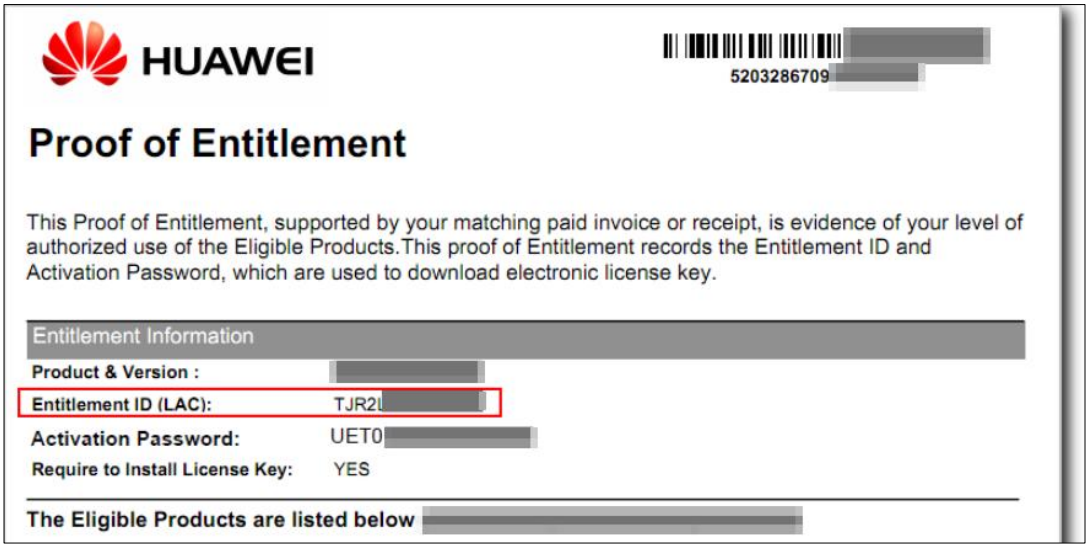

Ilustración 1: Obtención de licencias

- Hacer *login* en el dispositivo y ejecutar el comando ***display esn*** para obtener el ESN del dispositivo.
- Hacer *login* en el ESDP de Huawei en http://app.huawei.com/isdp.
- Acceder a "*License Activation*" → *"Password Activation"*.
- Introducir la contraseña de activación obtenida del "Proof of Entitlement", seleccionar "*I have read the above carefully*" ¸ *y después pulsar "Next"*.
- Introducir el ESN obtenido anteriormente y hacer clic en "*Next*".
- Confirmar la activación haciendo clic en *"Activate License"*.
- Finalmente, para descargar el archivo hacer clic en "*Download*".

16. Una vez obtenido el archivo de licencia, se debe acceder al dispositivo desde la interfaz web con la cuenta de administrador. Posteriormente se navegará a System → User Management → License. Luego se pulsará el botón de "Upload License".

17. En la ventana emergente se seleccionará el archivo de licencia obtenido anteriormente y se hará clic en el botón "OK" para cargar la licencia. Si la licencia se instala correctamente, el proceso habrá concluido.

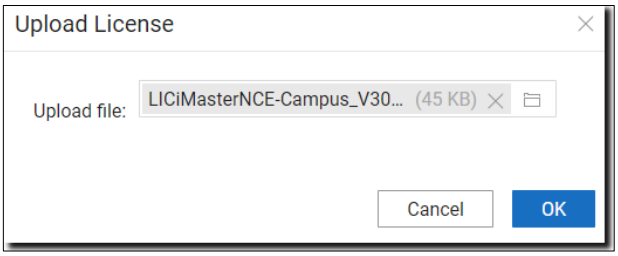

Ilustración 2: Ventana de diálogo para cargar el archivo de licencia.

18. Para más información consultar la sección "License Guide" de [GUÍA_PRODUCTO].

4.4 CONSIDERACIONES PREVIAS

19. A la hora de instalar el producto, se debe asegurar que se tiene acceso físico al dispositivo, aunque se deben situar en sitios seguros lo más restringidos posibles.

20. Se debe asegurar que se cuentan con las herramientas de conectividad necesarias, tales como conectores RJ45 o cables serie necesarios para la administración del dispositivo.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

21. El entorno de operación del producto debe estar compuesto por los siguientes elementos hardware en su entorno:
    - **Consola Local**: PC conectado al producto por puerto serie para la administración local de este.
    - **Red**: Representa la red que el dispositivo utiliza para gestionarla (puede incluir dispositivos de red como switches, routers, firewalls, etc.)
22. Si se requiere hacer uso de la funcionalidad de administración remota, el entorno además debe incluir el siguiente componente:
    - **Ordenador de Administración:** Representa el dispositivo que el usuario administrador utiliza para conectarse al dispositivo y gestionarlo.

5 FASE DE INSTALACIÓN

5.1 INSTALACIÓN DEL PRODUCTO

23. El fabricante hace entrega del hardware con el producto ya instalado. Para más información consultar la sección “Installing iMaster NCE-Campus” de [GUÍA_PRODUCTO].

5.2 VERIFICACIÓN DEL FIRMWARE

24. Se debe verificar que el firewall disponga del ***firmware V300R023C00SPC010T*** instalado. Para verificarlo, seguir los siguientes pasos:

    - Para listar el *firmware* del sistema el producto se debe acceder al dispositivo desde la interfaz web con la cuenta de administrador. Posteriormente se navegará a Maintenance > File Management > File Management. Luego se pulsará en la columna “Operation” donde se podrá ver el firmware y parches instalados.

25. En caso contrario, se deberá instalar dicho *firmware*. El detalle de actualización del *firmware* se puede consultar en el apartado 6.8 ACTUALIZACIONES.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

26. La configuración necesaria para que el producto opere de forma segura consiste en aplicar una configuración segura de varias políticas a través de la interfaz de línea de comandos. Esta interfaz es accesible a través de SSH por el puerto ETH.

27. Se debe editar el archivo de configuración de SSH localizado en */etc/ssh/sshd_config* modificándolo con los siguientes algoritmos:

```
Ciphers aes128-ctr, aes192-ctr, aes256-ctr
KexAlgorithms ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521
MACs hmac-sha2-512-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512, hmac-sha2-256
```

28. Se debe configurar las ciphers para el servicio de Syslog modificando el archivo */opt/oss/share/NCECAMPUS/NBIFrmNotifyService/conf/syslog_external/cipher.properties* modificándolo con los siguientes algoritmos:

```
ssl.enabled.protocols=TLSv1.2
ssl.cipher.suites=TLS_ECHDE_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_ECHDE_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECHDE_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECHDE_RSA_WITH_AES_128_GCM_SHA256
```

6.2 AUTENTICACIÓN

29. Los mecanismos de autenticación que utiliza el producto para autenticar a un usuario son los siguientes:

    - Credenciales locales, mediante usuario y contraseña de acceso. La gestión de usuarios locales se puede consultar en el apartado 6.3.2 CONFIGURACIÓN DE ADMINISTRADORES.
    - Autenticación mediante servidor externo RADIUS, ver apartado 6.6 SERVIDORES DE AUTENTICACIÓN.
    - Clave RSA para autenticación del servicio SSH.

30. Los mecanismos de autenticación que utiliza el producto para autenticar a otros sistemas o dispositivos son los siguientes:

    - Certificado TLS para comunicarse con el servidor syslog externo. Su configuración se indica en el apartado 6.11.3 ALMACENAMIENTO REMOTO.
    - Clave pre-compartida para las comunicaciones con un servidor NTP externo. Su configuración se indica en el apartado 6.7 SINCRONIZACIÓN .
    - Clave pre-compartida para cifrar la comunicación entre un servidor RADIUS externo y el producto. Su configuración se indica en el apartado 6.6 SERVIDORES DE AUTENTICACIÓN.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

31. La administración local del producto se realiza a través de la interfaz *serial*, para ello es necesario conectar un PC al producto con un cable de consola. Para acceder a las funciones de administración de la línea de comandos es necesario autenticarse con la contraseña del usuario *root* definida en *5 FASE DE INSTALACIÓN*. Sin embargo, no se espera que el usuario final tenga acceso a esta cuenta por lo que tendría que solicitarla al fabricante.
32. La administración remota del producto se realiza a través de SSH, para ello es necesario conectar un PC al producto con un cable de Ethernet en una interfaz física habilitada para tal propósito. Para acceder a las funciones de administración de la línea de comandos es necesario autenticarse con las credenciales de un usuario autorizado para conectarse por SSH al producto.
33. La administración remota del producto también puede realizarse por HTTPS a través de un navegador web, obteniendo una interfaz gráfica.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

34. El producto define 3 tipos de usuarios: administrador del sistema, administrador MSP y administrador tenant.
35. La siguiente tabla presenta los tipos de usuarios y roles:

Tipo de Usuario	Role	Descripción
Administrador del sistema.	Administrador del sistema.	Gestiona los servidores iMaster NCE-Campus, supervisa los clústeres, gestiona las alarmas de los clústeres y configura los servicios del sistema y otras funciones.
	Operador	Gestiona el servicio del sistema en ejecución.
	Operador abierto de Api	Realiza la autenticación cuando un sistema de terceros northbound invoca las API de northbound de iMaster NCE-Campus.
Administrador MSP	Adminstrador MSP	Opera servicios de tenant y realiza configuraciones relacionadas.
	Operador	Gestiona el servicio del sistema en ejecución

	Operador abierto de Api	Opera servicios API abiertos y realiza configuraciones relacionadas.
Administrador Tenant	Monitor	Visualiza los servicios de los tenants y las configuraciones relacionadas.
	Operador abierto de Api	Opera servicios API abiertos y realiza configuraciones relacionadas.
	Administrador tenant	Opera servicios de tenants y realiza configuraciones relacionadas.
	Operador	Gestiona el servicio del sistema en ejecución.
	Operador CLI	Emite comandos a los dispositivos a través de la plantilla CLI.

Tabla 1: Usuarios y roles.

36. Para más información consultar la sección “User Management” de [GUÍA_PRODUCTO].

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

37. En este caso no es necesario hacer ninguna configuración en específico para el producto.

6.5 GESTIÓN DE CERTIFICADOS

38. El producto usa certificados X.509 autoafirmados para comunicarse con un servidor *syslog* externo. Los certificados pueden ser generados con la herramienta openSSL y luego cargados mediante SFTP. Para más información consultar la sección “Managing Service Certificates” de [GUÍA_PRODUCTO].
39. El producto verifica la vigencia de un certificado, comprobándolo contra su propia fecha y hora. Además, se puede subir al producto un archivo CRL para comprobar si los certificados siguen siendo válidos, o configurar una dirección de un servidor OSCP para que lo compruebe contra el mismo servidor.

6.6 SERVIDORES DE AUTENTICACIÓN

40. El dispositivo permite la configuración de servidores externos de autenticación como RADIUS o LDAP entre otros.
41. Para llevar a cabo la configuración de RADIUS, se debe crear un *authorization-schema* y un *accounting-schema*. A continuación, se exponen los pasos necesarios:

```
$ system-view
$ aaa
```

```
$ authentication-scheme radius
$ authentication-mode radius
$ quit
$ accounting-scheme radius
```

42. A continuación, se debe configurar una RADIUS template para especificar los parámetros del servidor RADIUS. Para ello se deben ejecutar los siguientes comandos:

```
$ system-view
$ radius-server template <nombre>
$ radius-server authentication <direccion RADIUS> <puerto RADIUS>
$ radius-server accounting <direccion RADIUS> <puerto RADIUS>
$ radius-server shared-key cipher <contraseña>
```

43. Por último, se debe crear un perfil de autenticación y asociar los esquemas creados en los pasos previos:

```
$ system-view
$ authentication-profile name <nombre perfil>
$ authentication-scheme radius
$ accounting-scheme radius
$ radius-server <nombre template>
```

44. El detalle de configuración de RADIUS se puede consultar en el apartado Configuration Guide --> Object --> Authentication Server --> Configuring Authentication Servers Using the CLI --> Configuring a RADIUS Server, de la guía [GUÍA_PRODUCTO].

45. Para la configuración de un servidor de autenticación LDAP se deben seguir los siguientes pasos:

```
$ system-view
$ ldap-server template <nombre template>
$ ldap-server server-type { ad-ldap | ibm-tivoli | open-ldap | sun-one
}
$ ldap-server authentication <direccion LDAP>
$ ldap-server authentication base-dn <base-dn>
$ ldap-server authentication manager <usuario manager LDAP>
$ ldap-server authentication manager-password <password>
$ ldap-server ssl version tlsv1.2
$ ldap-server authorization bind-user enable
```

46. Adicionalmente, el detalle de configuración de LDAP se puede consultar en el apartado Configuration Guide --> Object --> Authentication Server --> Configuring Authentication Servers Using the CLI --> Configuring a LDAP Server Template, de la guía [GUÍA_PRODUCTO].

6.7 SINCRONIZACIÓN

47. El dispositivo permite el uso de NTP para la sincronización horaria. En lugar de establecer el tiempo manualmente, **se recomienda el uso de un servidor NTP para la sincronización horaria.** Se deben ejecutar las siguientes instrucciones para establecer un servidor externo NTP:

```
$ system-view
$ ntp-service unicast-server <IP_NTP> version <versión>
```

48. Por defecto, se utiliza la versión 3 del protocolo NTP, la cual es considerada segura. **Se debe hacer uso de la versión 3 o la 4**.

49. Es posible autenticar la conexión estableciendo una clave predefinida entre el servidor NTP y el firewall, se debe hacer uso de HMAC-SHA-256. Para ello, una vez configurada la clave en el servidor NTP, se deben ejecutar las siguientes instrucciones en el producto

```
$ system-view
$ ntp-service authentication enable
$ ntp-service authentication-keyid <ID_Clave> authentication-mode hmac-
sha256 cipher <Clave>
$ ntp-service reliable authentication-keyid <ID_clave>
```

50. Para más información seguir los pasos descritos en seguir los pasos descritos en la sección "Configuring NTP" de la [GUÍA_PRODUCTO].

6.8 ACTUALIZACIONES

51. El producto contempla dos tipos de actualizaciones:
    - Paquete de parches: Conjunto de parches que actúan sobre una versión del software del sistema. El producto comprueba la validez del conjunto de parches antes de cargarlos en el sistema. El nombre de archivo con su extensión sigue el siguiente esquema: (*iMasterNCE-Campus_{version}_EulerOS2.9Patch-x86-64.tar*).
    - Software/firmware del sistema: Se puede definir como el sistema operativo del producto. Al igual que los paquetes de parches, el producto comprueba la validez e integridad del software del sistema. El nombre de archivo con su extensión sigue el siguiente esquema: (*iMasterNCE-Campus_{version}_Base_linux-x86-64.zip*).
52. Para más información consultar la sección "Software Package Management" de [GUÍA_PRODUCTO].

6.9 AUTO-CHEQUEOS

53. Cuando el producto se enciende o se reinicia realiza los siguientes autochequeos:
    - Autochequeo de la integridad del *software* del sistema.
    - Autochequeo de los algoritmos de cifrado.
54. Además, en el caso de establecer un nuevo parche o firmware, se verifica la integridad de la actualización. La verificación es automática y transparente al usuario. Solo en caso de error al intentar instalar el software se notifica al usuario.

6.10 ALTA DISPONIBILIDAD

55. El producto tiene la posibilidad de utilizar la Alta Disponibilidad, lo que permite, que un dispositivo secundario reemplace a otro activo que está fallando o que está fuera de servicio.

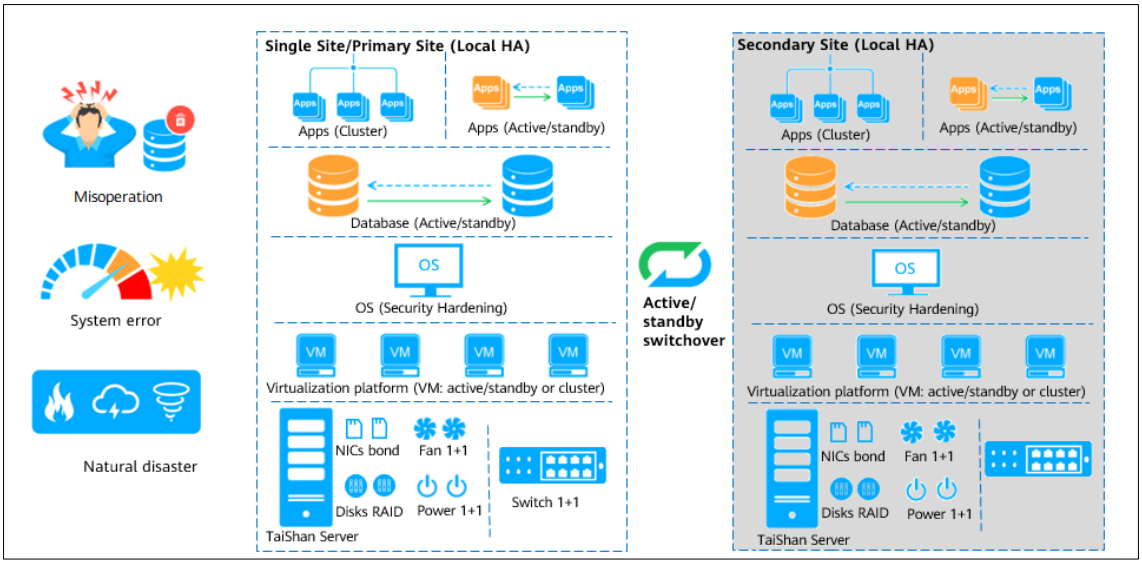

Ilustración 3: Configuración de la Alta Disponibilidad en escenario on-premise.

56. Como se puede apreciar, en un escenario on-premise, el producto proporciona soluciones integrales de protección de Alta Disponibilidad para el hardware, la capa de virtualización y la capa de aplicación de un solo sitio. Estas soluciones pueden prevenir riesgos desconocidos causados por algunos fallos de hardware o software y garantizar un funcionamiento seguro y estable de iMaster NCE-Campus.

57. El detalle de configuración para la funcionalidad de Alta Disponibilidad se puede consultar en [GUÍA_PRODUCTO].

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

58. El producto almacena los siguientes eventos de seguridad en sus registros de auditoría:

- *Login* y *logout* de los usuarios.
- Inicio de las acciones de auditoría.
- Cambio o generación de claves criptográficas.
- Cambios en la configuración del producto.
- Resetear o cambiar claves.
- Intentos de *login* fallidos.
- Configuración de un servidor NTP o eliminación del mismo.
- Terminación de una sesión local o remota por el usuario o por inactividad.
- Intentos de iniciar una actualización.
- Fallos en establecer una sesión SSH.

59. El producto guarda la siguiente información de los eventos:

Campo	Descripción
Fecha y hora	Fecha y hora en la que se produce el evento.
Tipo de evento	Clase de evento que se produce (ej.: *login*, reseteo de clave…).

Sujeto que produce el evento	Usuario e IP (si corresponde).
Resultado	Resultado del evento, si aplica.

Tabla 2: Información que se guarda de los registros de auditoría.

60. Es posible configurar el mínimo nivel de gravedad de los logs, de manera que solo se registrarían aquellos, que superen el valor mínimo establecido. Hay ocho (0-7) niveles de gravedad:

Nivel	Descripción
0 (Emergencia)	Estado de emergencia.
1 (Alerta)	Errores que necesitan acciones inmediatas.
2 (Crítico)	Estado crítico.
3 (Error)	Errores que necesitan ser atendidos pero que no son críticos.
4 (Advertencia)	Estado de advertencia, lo que significa que es probable que se produzcan errores.
5 (Aviso)	Información que requiere la atención.
6 (Información)	Información genérica.
7 (Depuración)	Información de depuración.

Tabla 3: Niveles de gravedad de los logs.

61. Se puede consultar esta configuración que más detalle en "Log Management" de [GUÍA_PRODUCTO].

6.11.2 ALMACENAMIENTO LOCAL

62. El producto almacena localmente los registros de auditoría en el directorio */opt/oss/share/manager/MCCommonService/dump/timestamp.* Los logs dumpeados son guardados en formato .zip. (Si el plano de gestión se despliega en modo de servidor único y el nodo de gestión y el nodo de producto son el mismo nodo, cambiar en la ruta MCCommonService por UniEPLiteService).
63. En caso de que se alcance el espacio de almacenamiento máximo, se borrarán archivos con formato ZIP antiguos. Es por esto que se recomienda realizar la configuración de un servidor de auditoría externo, tal como se indica en el siguiente epígrafe.
64. Para más información consultar la sección "Viewing Logs" de [GUÍA_PRODUCTO].

6.11.3 ALMACENAMIENTO REMOTO

65. El producto se puede configurar para enviar sus registros de auditoría a un servidor *syslog* externo. Es recomendable configurar la comunicación con dicho servidor bajo TLS 1.2, cifrando toda comunicación.
66. Para configurar el servidor syslog externo, desde la interfaz web navegar a System > System Management > Third-party Service desde el menú principal y luego hacer clic en

"Syslog Configuration". Posteriormente hacer clic en el botón "Add" y rellenar la información necesario del servidor syslog remoto.

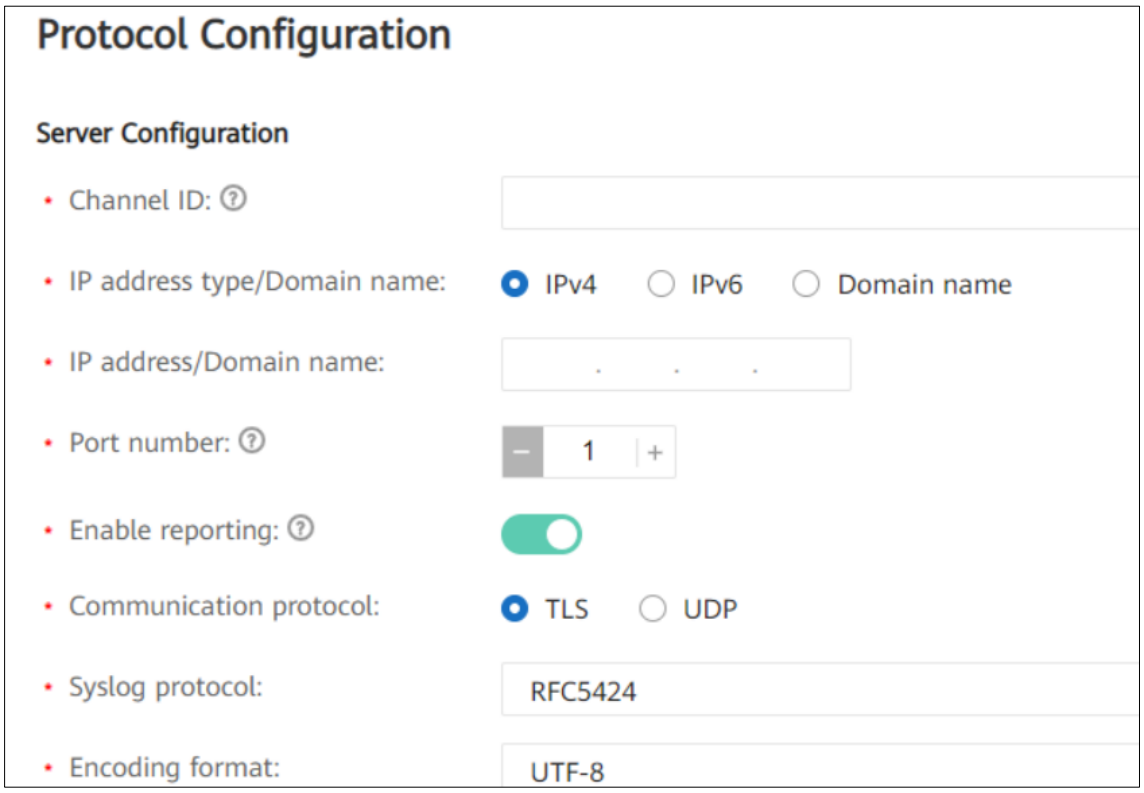

Ilustración 4: Configuración del servidor syslog remoto.

67. Para más información consultar la sección "Configuring Syslog" de [GUÍA_PRODUCTO].

6.12 BACKUP

68. Por defecto, iMaster NCE-Campus está preconfigurado con dos tareas de copia de seguridad programadas:
    - Copia de seguridad programada de los datos del producto -iMaster NCE-Campus: Los datos de producto de NCE-Campus se respaldarán automáticamente cada 24 horas.
    - Copia de seguridad programada del plano de gestión: Esta tarea se crea automáticamente durante el despliegue del plano de gestión. Los datos de NCE-OMP se copian una sola vez.
69. También es posible crear de manera manual una tarea de copia de seguridad programada una sola vez o una tarea de copia de seguridad programada periódica según sea necesario.
70. Las copias de seguridad pueden ser extraídas de dos formas, bien sea manualmente o estableciendo un servidor tercero para backups. Para más información consultar la sección "Configuring Backup Parameters" de [GUÍA_PRODUCTO].

7 REFERENCIAS

[GUÍA_PRODUCTO] iMasterNCE Campus V300R020C10 Product Documentation (2024-04-30)

8 ABREVIATURAS

AES	Advanced Encryption Standard
DEMO	Demonstration
ESDP	Electronic Software Delivery Platform
ENS	Esquema Nacional de Seguridad
ESN	Equipment Serial Number
ETH	Ethernet
Gbit	Gigabit
GE	Gigabit Ethernet
HMAC	Hash-based Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
COMM	Communication
ID	Identification
ICMP	Internet Control Message Protocl
IDC	Internet Data Center
IP	Internet Protocol
MAC	Media Access Control
Mbit	Megabit
NMS	Network Management System
NTP	Network Time Protocol
PC	Personal Computer
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RSA	Rivest, Shamir, & Adleman (public key encryption technology)
SHA	Secure Hash Algorithm
SDN	Software Defined Networking
SSH	Secure Shell
SSL	Secure Sockets Layer
SNMP	Simple Network Management Protocol
SYN	Synchronization
TLS	Transport Layer Security

PUBLICACIONES DE DEFENSA

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