centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1615

Procedimiento de Empleo Seguro
SUSE 15 SP4

Abril de 2024

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: 083-24-161-6.
Fecha de Edición: abril de 2024.

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
2024.04.29 10:23:25 +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. La distribución **SUSE LINUX Enterprise Server (SLES) 15 SP4** está diseñada para proporcionar un sistema operativo de propósito general seguro y fiable. La seguridad de las aplicaciones que se ejecuten sobre el sistema operativo están fuera del alcance de este documento.

2. Este documento es una guía de seguridad que explica cómo preparar la configuración evaluada y proporciona información a los administradores y usuarios para garantizar el funcionamiento seguro del sistema. Se pretende que sea suficiente para abordar los problemas más importantes a nivel general e incluye referencias a otra documentación en caso de que se necesiten más detalles.

3. El documento se dirige principalmente a los administradores, pero la sección 7.3 PAUTAS DE SEGURIDAD PARA LOS USUARIOS está dirigida tanto a los usuarios del sistema como a los administradores.

1.1 CÓMO UTILIZAR ESTE DOCUMENTO

4. Las palabras clave "DEBE" (MUST o SHALL), "NO DEBE" (MUST NOT o SHALL NOT), "NECESARIO" (REQUIRED), "DEBERÍA" (SHOULD), "NO DEBERÍA" (SHOULD NOT), "RECOMIENDA" (RECOMMENDED), "RECOMENDADO" (RECOMMENDED), "PUEDE" (MAY) y "OPCIONAL" (OPTIONAL) de este documento deben interpretarse como se describe en la referencia RFC 2119 http://www.ietf.org/rfc/rfc2119.txt.

5. Tenga en cuenta que los términos "DEBERÍA" y "NO DEBERÍA" definidos en RFC 2119 como "SHOULD" y "SHOULD NOT" se evitan en este documento en la medida de lo posible. Los requisitos pueden ser absolutos (y se marcan con DEBE y términos equivalentes) o totalmente opcionales (en el sentido de que no afectan a las funciones de seguridad requeridas) y se marcan con RECOMENDADO, PUEDE u OPCIONAL.

6. Si sigue los requisitos de este documento al preparar y utilizar el sistema, la configuración coincidirá con la configuración evaluada. Algunas opciones de configuración se marcan como OPCIONALES y PUEDE modificarlas según sea necesario, pero NO DEBE realizar otros cambios, ya que harán que el sistema no coincida con la configuración evaluada.

7. En los casos en que los requisitos y recomendaciones de este documento entren en conflicto con los de otras fuentes (como la documentación en línea), la información de esta Guía de configuración tiene mayor prioridad. DEBE seguir los pasos descritos aquí para llegar a la configuración evaluada, incluso si otra documentación describe métodos diferentes.

8. En esta guía se usan las convenciones habituales cuando se hace referencia a las páginas *man* que se incluyen en la distribución del *software*. Por ejemplo, la notación *ls*(1) significa que al ejecutar el comando "*man -S 1 ls*" se mostrará la página *man* del comando *ls* de la sección uno de la documentación instalada. En la mayoría de los casos, el indicador *-S* y el número de sección pueden omitirse en el comando. Solo se necesitan si existen páginas con el mismo nombre en distintas secciones.

2 OBJETO Y ALCANCE

9. El objeto de la presente guía es proporcionar unos procedimientos de instalación, configuración, operación y mantenimiento para que el sistema operativo SUSE 15 SP4 funcione en cumplimiento con los niveles de seguridad exigidos por el Centro Criptológico Nacional en el Esquema Nacional de Seguridad.

10. El sistema operativo SUSE 15 SP4 ha sido cualificado e incluido en el catálogo CPSTIC en la familia “Sistemas Operativos”.

3 ORGANIZACIÓN DEL DOCUMENTO

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.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

11. **DEBE descargar las imágenes ISO estándares del sitio Web de SUSE** en un equipo independiente conectado a Internet y grabarlas en un dispositivo USB, o bien hacer que el contenido esté disponible como se describe en la guía de distribución de SLES 15 SP4 que encontrará en https://documentation.suse.com/en-us/sles/15-SP4/. Puede descargar las siguientes imágenes específicas de cada plataforma de https://www.suse.com/download/sles/.

12. Si la imagen que desea descargar no aparece en la página, inicie sesión en su cuenta primero.

SUSE Linux Enterprise Server 15 SP4 para IBM Z System

- Nombre de archivo: SLE-15-SP4-Full-s390x-QU3-Media1.iso
- Suma de comprobación SHA256: 60a4e8306cbdbe693353fb85836c04e0267ca64cd1adbb40f405f2708027cfe4

SUSE Linux Enterprise Server 15 SP4 para IBM POWER

- Nombre de archivo: SLE-15-SP4-Full-ppc64le-QU3-Media1.iso
- Suma de comprobación SHA256: afd6a7843da52ffa8c44e0f0c1567a141a331fbe4ee3f2bd16eaac43cbaa65bb

SUSE Linux Enterprise Server 15 SP4 para Intel 64/AMD64

- Nombre de archivo: SLE-15-SP4-Full-x86_64-QU3-Media1.iso
- Suma de comprobación SHA256: 447baa21dd85e5433a1a2b2f46fe91491e8792f559397aca86fdf7a114c23c06

SUSE Linux Enterprise Server 15 SP4 para ARM64

- Nombre de archivo: SLE-15-SP4-Full-aarch64-QU3-Media1.iso
- Suma de comprobación SHA256: 664f17cf0d853ffdaca8781670249cd39213e9cfcc64e1de4318b6a5e9bb0eff

13. **DEBE usar SUSE Linux Enterprise Server 15 SP4. Asegúrese de usar la versión adecuada para su plataforma**; consulte la sección 4.2.1 "REQUISITOS DE *HARDWARE*" de esta guía para obtener la lista de hardware compatible y la versión correspondiente necesaria.

14. DEBE verificar que las sumas de comprobación SHA256 de los archivos de imagen ISO de SLES 15 SP4 sean correctas. Se RECOMIENDA comprobar las sumas de comprobación, incluida la firma que se muestra en el sitio Web de SUSE, realizando los pasos descritos en la página Web de seguridad de http://www.suse.com/security/download-verification.html.

4.2 ENTORNO DE INSTALACIÓN SEGURO

4.2.1 REQUISITOS DE *HARDWARE*

15. La plataforma sobre la que corra el sistema operativo DEBE ser una de las siguientes:

ARQUITECTURA	MODELO	PROCESADOR
Intel x86 de 64 bits	Delta D20x-M1-PC-32-8-96GB-1TB-2x1G	Cascade Lake
AMD x86_64	Servidor AMD EPYC DP R181-Z90	EPYC de primera generación
IBM	IBM Z System z15	z15
IBM POWER	IBM Power10 9080-HEX	Power 10
ARM	Gigabyte R181-T90	ARMv8.2-A

Tabla 1: hardware soportados

16. La ejecución del *software* certificado en otro *hardware* similar puede dar como resultado un nivel de seguridad equivalente, pero la certificación no se aplica si el *hardware* es diferente del utilizado para los procesos de prueba durante la evaluación.

17. Tenga en cuenta que el funcionamiento correcto de todas las partes del *software* solo se garantiza si se utilizan los sistemas de *hardware* mencionados anteriormente, ya que varios mecanismos de *hardware* que pueden no estar presentes en otros sistemas son vitales para la seguridad del sistema.

18. PUEDE conectar los siguientes periféricos sin invalidar los resultados de la evaluación. NO DEBE instalar ni conectar ningún otro hardware al sistema.

    - Cualquier dispositivo de almacenamiento y de copia de seguridad compatible con el sistema operativo (esto incluye discos duros, unidades de CD-ROM y unidades de cinta).
    - Todos los adaptadores de red Ethernet compatibles con el sistema operativo. Los módems, RDSI y otros adaptadores WAN no forman parte del entorno evaluado.
    - Cualquier impresora compatible con el sistema operativo.
    - Consolas del operador compuestas por un teclado, un monitor de vídeo y, opcionalmente, un ratón. Además, PUEDE conectar directamente terminales en serie compatibles (consulte la sección 6.11 "USO DE TERMINALES EN SERIE" de esta guía), pero no módems, tarjetas RDSI ni otros terminales de acceso remoto.

    NO DEBEN instalarse tarjetas IBM Crypto Express. Esta restricción se debe a la limitación de los recursos y de ninguna manera es una indicación de que el hardware o los controladores de software asociados se hayan implementado incorrectamente.

4.2.2 REQUISITOS DE *SOFTWARE*

19. El *software* DEBE coincidir con la configuración evaluada. En el caso de un sistema operativo, también se requiere que el kernel instalado, el sistema y el software de aplicación sean los mismos. La documentación (incluida esta guía) especificará las variaciones permitidas, como la modificación de determinados archivos y ajustes de configuración, así como las instalaciones de *software* que no tengan la capacidad de afectar a la seguridad del sistema (normalmente, aquellos que no requieren privilegios de usuario *root*).

4.2.3 REQUISITOS DEL ENTORNO DEL SISTEMA

20. El producto está pensado para ser instalado en equipos conectados en una red no hostil, con una comunidad de usuarios bien gestionada y no hostil. No cubre las necesidades de un servidor conectado directamente a Internet, ni el caso en el que se vayan a proporcionar servicios a usuarios potencialmente hostiles.

21. Se presupone que el valor de los activos almacenados es moderadamente susceptible de recibir intentos de penetración o ataques de enmascaramiento intensos. También se presupone que los controles físicos existentes alertarían a las autoridades del sistema de la presencia física de atacantes dentro del espacio controlado.

22. **DEBE configurar el servidor (o los servidores) en un entorno físicamente seguro, donde estén protegidos contra el robo y la manipulación por parte de personas no autorizadas.**

23. DEBE asegurarse de que todas las conexiones a los dispositivos periféricos y todas las conexiones de red estén protegidas contra manipulaciones, interferencias y otras modificaciones. El uso de los protocolos seguros de TLSv1.2 y versiones superiores, SSHv2 o IPSECv3 (IKEv2) se considera protección suficiente para las conexiones de red. **Todas las demás conexiones deben permanecer completamente dentro del entorno del servidor físicamente seguro.**

4.2.4 REQUISITOS DE CONECTIVIDAD

24. Se presupone que todos los componentes de la red, como los *routers*, los conmutadores y los concentradores que se utilizan para la comunicación, transmiten los datos del usuario de forma fiable y sin modificaciones. Se permite la traducción de elementos de protocolos (como NAT), siempre que esas modificaciones no den lugar a una situación en la que la información se dirija a otra persona que no sea el sistema destinatario previsto. El cableado de red y periférico debe estar aprobado para la transmisión de los datos más confidenciales del sistema.

25. Cualquier otro sistema con el que se comunique el producto DEBE configurarse y gestionarse con el mismo control de gestión y DEBE funcionar con las mismas restricciones de la directiva de seguridad.

26. Tenga en cuenta que la información que se transfiere a otro sistema deja de estar bajo control del sistema remitente y que es el sistema receptor el que deberá proteger esta información contra el acceso no autorizado. Si una organización desea implementar una directiva de seguridad uniforme que cubra varios sistemas de una red, los procedimientos de la organización DEBEN garantizar que todos esos sistemas sean fiables y estén configurados con ajustes de seguridad compatibles que apliquen una directiva de seguridad en toda la organización. La forma de hacerlo queda fuera del alcance de esta Guía de configuración. Si configura un enlace de comunicación con un sistema que esté fuera de su control, tenga en cuenta que no podrá aplicar ninguna directiva de seguridad a la información que pase a dicho sistema a través del enlace de comunicación o de otras formas (por ejemplo, con medios de almacenamiento extraíbles).

4.3 REGISTRO Y LICNECIAS

27. Para obtener asistencia técnica y actualizaciones del producto, deberá registrar y activar SUSE Linux Enterprise Server en el SUSE Customer Center. Se recomienda registrarse durante la instalación, ya que así podrá instalar el sistema con las últimas actualizaciones y parches disponibles. No obstante, si no está conectado o desea omitir el paso de registro, puede registrarse en cualquier momento posterior desde el sistema instalado.

28. Los módulos y extensiones añaden funciones a su sistema y le permiten personalizarlo según sus necesidades. Estos componentes también deben registrarse y pueden gestionarse con YaST o con herramientas de línea de comandos.

29. Para más detalles consulte:

    https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-register-sle.html

    https://documentation.suse.com/sles/15-SP4/html/SLES-all/article-modules.html

4.4 CONSIDERACIONES PREVIAS

4.4.1 REQUISITOS PREVIOS PARA LA INSTALACIÓN

30. Se RECOMIENDA que desconecte todas las conexiones de red hasta que finalice la configuración del sistema posterior a la instalación. PUEDE utilizar una red si es necesario para la instalación (por ejemplo, si utiliza un servidor de archivos NFS en lugar de un CD-ROM). Si utiliza una red, DEBE asegurarse de que sea segura; por ejemplo, conectando directamente el nuevo sistema a un servidor NFS independiente sin otras conexiones de red.

31. Necesitará los siguientes componentes para instalar un sistema en la configuración evaluada como se explica en las siguientes secciones:

    - El sistema de destino que se instalará. Consulte la sección 4.2.1 REQUISITOS DE *HARDWARE* de esta guía para obtener la lista de *hardware* compatible. El sistema de destino REQUIERE al menos un disco duro local que se borrará y volverá a particionar para que lo utilice la configuración evaluada.

    - La distribución de **SUSE LINUX Enterprise Server 15 SP4** aplicable al sistema de *hardware* seleccionado debe estar disponible. Si utiliza *hardware* basado en Intel, tenga en cuenta que DEBE utilizar la versión de 64 bits marcada como *x86_64*. No se deben usar imágenes remezcladas, sino que se DEBE usar la imagen estándar de SLES.

    - Utilice una dirección IP estática si pretende conectar el sistema de destino a una red. **No se debe utilizar DHCP**. Además, deberá configurar manualmente la máscara de red, la puerta de enlace y la lista de servidores DNS. Si necesita utilizar una dirección IP estática durante la instalación, se debe utilizar la opción de arranque

      netsetup=1

      ya que, de lo contrario, el instalador utilizará por defecto DHCP.

    - Utilice un método para hacer que el contenido de las imágenes ISO que contengan SLES esté disponible para el sistema de destino, incluida la posibilidad de arrancar la

imagen de arranque proporcionada con el remezcla de las imágenes ISO de SLES. Estos métodos pueden ser, por ejemplo, el almacenamiento de las imágenes ISO en un DVD-R y el arranque desde él, el uso de TFTP y NFS, el uso de una distribución de imágenes basada en HTTP, etc. Los posibles métodos de instalación se explican en la guía de distribución de SLES 15 SP4 que encontrará en https://documentation.suse.com/en-us/sles/15-SP4/.

32. Después de obtener las imágenes ISO, DEBE verificar la integridad de los archivos descargados con las claves proporcionadas en el sitio Web de seguridad de SUSE: https://www.suse.com/support/security/keys/.

4.4.2 REQUISITOS PARA LOS USUSARIOS DEL SISTEMA

33. El objetivo de seguridad responde a las necesidades de seguridad de los usuarios que cooperan en un entorno benigno, que utilizarán el sistema de forma responsable para llevar a cabo sus tareas.

34. Tenga en cuenta que la disponibilidad del sistema no se aborda en esta evaluación y que un usuario malintencionado podría inhabilitar un servidor mediante el agotamiento de los recursos o con métodos similares.

35. Los requisitos específicos para los usuarios son estos:

    - Las cuentas de usuario DEBEN asignarse solo a aquellos usuarios que necesiten acceder a los datos protegidos por el sistema. Estos usuarios DEBEN ser lo suficientemente de confianza como para no abusar de esos privilegios. Por ejemplo, el sistema no puede evitar que un usuario autorizado redistribuya intencionadamente los datos a terceros no autorizados.
    - Se confía en que los usuarios realicen algunas tareas o grupos de tareas dentro de un entorno de TI seguro mediante el control total de sus datos.

36. Todos los usuarios del sistema DEBEN tener la capacidad suficiente para comprender las implicaciones de seguridad de sus acciones, y DEBEN comprender y seguir los requisitos indicados en la sección 7.3 “PAUTAS DE SEGURIDAD PARA LOS USUARIOS” de esta guía. Se DEBE proporcionar la formación adecuada para garantizarlo.

37. Es parte de su responsabilidad como administrador del sistema verificar que se cumplen estos requisitos, así como estar disponible para los usuarios si necesitan su ayuda para mantener la seguridad de sus datos.

4.4.3 REQUISITOS PARA LOS ADMINISTRADORES

38. DEBE haber una o más personas competentes asignadas para gestionar el sistema y la seguridad de la información que contiene. Estas personas serán las únicas responsables de las siguientes funciones: (a) crear y mantener roles, (b) establecer y mantener las relaciones entre los roles, (c) asignar y revocar roles a los usuarios. Además, estas personas (como propietarios de todos los datos de la empresa), junto con los propietarios de objetos, tendrán la capacidad de asignar y revocar derechos de acceso a los objetos a los roles.

39. El personal administrativo del sistema NO DEBE ser descuidado, negligente ni hostil, y DEBE seguir y acatar las instrucciones proporcionadas en la documentación del administrador.

40. Toda persona que tenga la capacidad de realizar acciones administrativas porque pueda pasar a ser usuario *root* tiene control total sobre el sistema y podría, por accidente o de forma deliberada, socavar la seguridad del sistema y ponerlo en un estado inseguro. Esta Guía de configuración proporciona directrices básicas sobre cómo configurar y utilizar el sistema de forma segura, pero no pretende ser la única información necesaria para que un administrador del sistema aprenda a utilizar Linux de forma segura.

41. En esta Guía de configuración, se presupone que los administradores que utilizan la guía tienen un buen conocimiento y comprensión de los principios de seguridad operativos en general, y de los comandos administrativos de Linux y las opciones de configuración en particular. No obstante, se recomienda encarecidamente a las organizaciones que deseen utilizar el sistema en la configuración evaluada que formen a sus administradores sobre los principios de seguridad del sistema operativo y las funciones, las propiedades y la configuración de seguridad de SLES.

42. Todas las organizaciones necesitan confiar en que los administradores de sus sistemas no van a socavar deliberadamente la seguridad del sistema. Aunque la configuración evaluada incluye funciones de auditoría que se pueden utilizar para hacer que los usuarios sean responsables de sus acciones, un administrador puede detener el subsistema de auditoría y volver a configurarlo para que sus acciones dejen de auditarse. Disponer de administradores bien formados y de confianza es un elemento clave para el funcionamiento seguro del sistema. Esta Guía de configuración proporciona información adicional para que los administradores del sistema instalen, configuren y utilicen el sistema de acuerdo con los requisitos definidos en el objetivo de seguridad para la evaluación de Criterios Comunes.

43. Las presuposiciones indicadas anteriormente implican que los permisos de DAC de los directorios del sistema, los archivos binarios del sistema y sus archivos de configuración no se modificarán. Entre otras cosas, esto garantiza que solo los administradores puedan añadir nuevo *software* de confianza a la instalación.

44. Para garantizar la integridad del sistema, **DEBE programar revisiones periódicas del funcionamiento y la integridad del sistema**. Por ejemplo, se puede invocar una verificación de integridad mediante la herramienta *rpm*. Otra posibilidad de validar la integridad del sistema es el uso de aide.

5 FASE DE INSTALACIÓN

45. La evaluación cubre una instalación nueva de SLES 15 SP4 en una de las plataformas de *hardware* compatibles, como se define en la sección 4.2.1 de esta guía.

46. La configuración evaluada DEBE ser el único sistema operativo instalado en el servidor.

5.1 PROCESO DE INSTALACIÓN AUTOMATIZADO

47. En esta sección se describen detalladamente los pasos que se deben realizar al instalar el sistema operativo SLES en el servidor de destino.

48. El proceso de instalación es totalmente automático, excepto las opciones de configuración que debe proporcionar el administrador, como indicar la configuración de red o los nombres de usuario y las contraseñas para los usuarios administrativos.

49. Todos los ajustes indicados aquí son NECESARIOS a menos que se indique específicamente lo contrario.

5.1.1 PROCESO DE INSTALACIÓN

50. La preparación del arranque inicial y el modo en que se accede al indicador de arranque dependen del *hardware* y la configuración elegidos. Consulte la documentación de SLES específica de la arquitectura para configurar el entorno de arranque.

51. Las siguientes ilustraciones sirven solo como ayuda para explicar el proceso. La información real que aparezca puede ser ligeramente diferente.

52. En la siguiente ilustración se muestra un ejemplo de cómo arrancar directamente desde una unidad de memoria USB de SLES. Si se utiliza un mecanismo de arranque distinto, esta ilustración puede no ser aplicable.

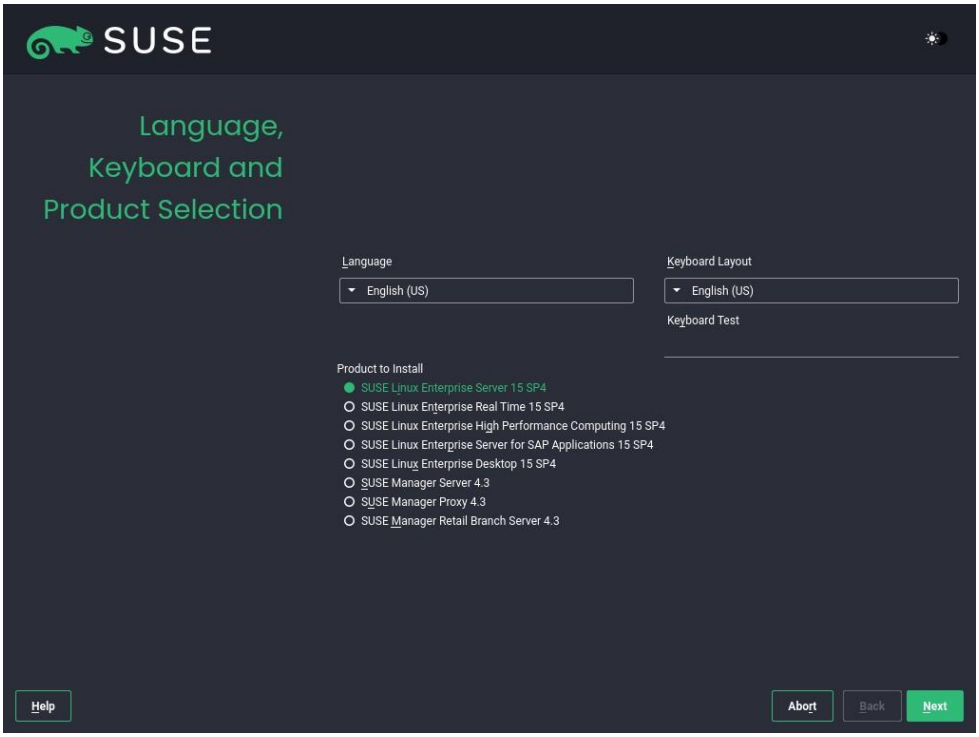

Ilustración 1: Arranque desde USB de SLES

53. Cuando el instalador le pregunte el idioma de instalación, DEBE seleccionar "*English*" (Inglés), ya que es el único idioma admitido para la configuración evaluada. También puede seleccionar la distribución del teclado que mejor le convenga. DEBE leer atentamente el acuerdo de licencia y marcar la casilla de verificación si está de acuerdo.

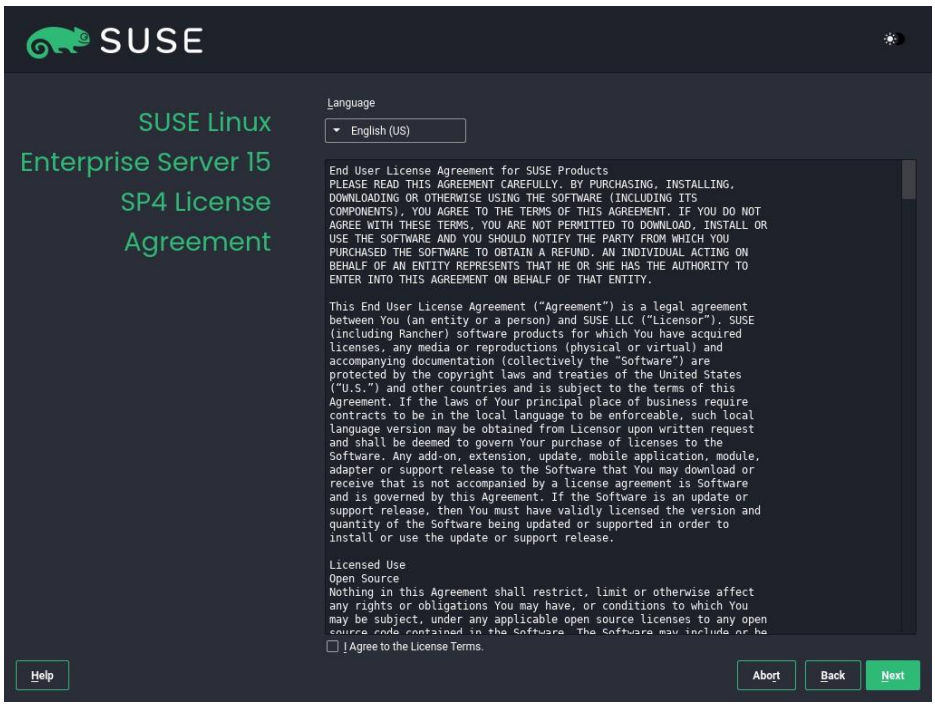

Ilustración 2: Acuerdo de licencia

54. Después de aceptar el acuerdo de licencia, se RECOMIENDA que registre el producto en *scc.suse.com* o en un servidor RMT local.

55. Si omite el registro en este punto, DEBERÍA registrar el producto después de finalizar la configuración del sistema posterior a la instalación.

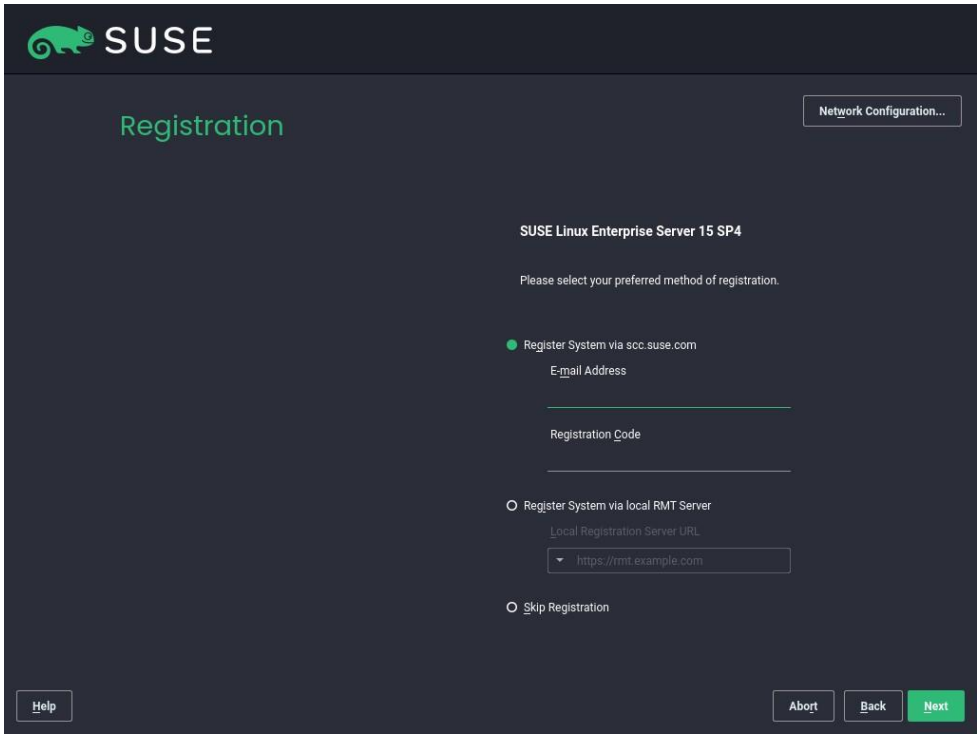

Ilustración 3: Registro del producto

56. En la selección de extensiones y módulos, los dos módulos

    - Basesystem Module (Módulo de sistema base)
    - Server Application Module (Módulo de aplicación de servidor)

57. DEBEN estar seleccionados. Se PUEDEN seleccionar paquetes adicionales; sin embargo, se aplican las mismas restricciones que se indican en 6.3 "GESTIÓN DE CUENTAS DE USUARIO".

5.1.2 CREACIÓN DE USUARIOS

58. Utilice el comando useradd(8) para crear nuevas cuentas de usuario y, a continuación, el comando passwd(1) para asignar una contraseña inicial al usuario. Como alternativa, si el usuario está presente cuando se crea la cuenta, permítale elegir su propia contraseña. Consulte las páginas man de useradd(8) y passwd(1) para obtener más información.

59. Si asigna una contraseña inicial para un nuevo usuario, DEBE transferírsela de forma segura al usuario, asegurándose de que ningún tercero obtenga la información. Por ejemplo, puede decirle personalmente la contraseña a un usuario que conozca. Si no es posible, PUEDE enviarle la contraseña por escrito en una carta cerrada. Esto puede también hacerse cuando se define una contraseña nueva para un usuario en caso de que este haya olvidado la suya o la contraseña haya caducado. DEBE informar al usuario de

que DEBE cambiar esta contraseña inicial cuando inicie por primera vez la sesión en el sistema y seleccionar su propia contraseña de acuerdo con las reglas definidas en la sección 7.3.3 "POLÍTICA DE CONTRASEÑAS" de esta guía.

60. NO DEBE utilizar la opción -p para useradd(8), ya que si especifica una contraseña de ese modo, se omitirá el mecanismo de comprobación de la calidad de la contraseña.

61. El usuario DEBE cambiar la contraseña temporal definida por el administrador lo antes posible. Utilice el comando chage(8) con la opción -d para definir la fecha del último cambio de contraseña con un valor que servirá para recordarle al usuario que debe cambiar la contraseña. El valor RECOMENDADO se basa en los ajustes de /etc/login.defs y equivale a la fecha de hoy más el valor de PASS_WARN_AGE menos el de PASS_MAX_DAYS.

62. Ejemplo:

    useradd -m -c
    "John Doe" jdoe
    passwd jdoe
    chage -d $(date +%F -d "hace 53 días") jdoe

63. La opción -m para useradd(8) crea un directorio principal para el usuario basado en una copia del contenido del directorio /etc/skel/. PUEDE modificar algunos ajustes de configuración por defecto para los usuarios, como el de umask(2) o la zona horaria, editando los archivos de configuración global correspondientes:

    /etc/profile
    /etc/bash.bashrc
    /etc/csh.cshrc

5.1.3 CAMBIO DE CONTRASEÑAS DE USUARIO

64. Si es necesario, PUEDE restablecer la contraseña del usuario a un valor conocido utilizando passwd USUARIO e introduciendo la nueva contraseña. No es posible recuperar la contraseña utilizada anteriormente, ya que la función hash que se emplea no es reversible.

5.1.4 AUTENTICACIÓN BASADA EN CLAVE SSH

65. El TOE permite configurar la autenticación basada en clave para SSH. La autenticación basada en clave se configura usuario por usuario, gestionando el archivo .ssh/authorized_keys en el directorio personal de un usuario. Para obtener información sobre cómo utilizar ese archivo, consulte sshd(8).

66. Para generar claves que se puedan usar en la autenticación basada en clave, se proporciona la herramienta ssh-keygen(8), cuyo uso se RECOMIENDA encarecidamente, ya que solo esta utilidad proporcionada con el TOE ha estado sujeta a la evaluación de seguridad. Dado que el daemon de SSH solo acepta la versión 2 del protocolo SSH, con este daemon únicamente se admiten las claves del protocolo 2. Por lo tanto, solo DEBE utilizar la opción -t rsa o -t ecdsa cuando genere una clave con ssh keygen.

67. La utilidad *ssh-keygen* permite especificar el tamaño de clave para RSA, con un valor por defecto de 2048 bits. Si selecciona un tamaño de clave diferente, **DEBE utilizar tamaños de clave de más de 2048 bits**. Se permiten todos los tamaños de clave admitidos para ECDSA.

68. La parte de la clave privada DEBE almacenarse en *~/.ssh/* y debe quedar fuera del alcance de otros usuarios. Este archivo debe tratarse de forma similar a una contraseña. Se RECOMIENDA encarecidamente que se proteja esta clave con una contraseña codificada mediante *ssh-keygen*.

69. La siguiente línea de comandos es un ejemplo que genera una clave ECDSA:

    sh-keygen -t ecdsa -C "clave de John Doe"

70. El comando solicita una contraseña codificada donde DEBERÍA proporcionarse una contraseña codificada segura.

71. El bloqueo de la cuenta no impide que los usuarios puedan entrar en el sistema con la autenticación basada en clave SSH.

5.1.5 CAMBIO DE LAS PROPIEDADES DEL USUARIO

72. PUEDE utilizar el comando *usermod(8)* para cambiar las propiedades del usuario. Las propiedades a modificar se pueden ver en el propio manual del comando.

5.1.6 BLOQUEO Y DESBLOQUEO DE CUENTAS DE USUARIO

73. Se PUEDE bloquear (inhabilitar) a los usuarios mediante *passwd -l USUARIO* y volver a habilitarlos mediante *passwd -u USUARIO*. Tenga en cuenta que este bloqueo solo impide los intentos de autenticación basados en contraseña. La autenticación basada en clave SSH no se ve afectada por el uso de *passwd -l*. Para evitar inicios de sesión basados en clave SSH, se DEBE eliminar el archivo *.ssh/authorized_keys* ubicado en el directorio personal del usuario.

74. El módulo PAM *pam_tally2.so* aplica un bloqueo automático después de que se supere un número de intentos de autenticación fallidos. Utilice el programa *pam_tally2* para ver y restablecer el contador si es necesario, como se indica en la página man de *pam_tally2(8)*.

75. Tenga en cuenta que el orden es muy importante a la hora de añadir configuraciones a los archivos de configuración pam */etc/pam.d/login* y */etc/pam.d/common-auth*. Como la importancia del orden no se describe en profundidad en *pam_tally2(8)*, se proporciona un ejemplo a continuación en el que se denegará el acceso después de 4 intentos:

76. Archivo /etc/pam.d/login:

```
#%PAM-1.0
auth       required        pam_env.so
auth       required        pam_tally2.so   onerr=fail deny=4
auth       requisite       pam_nologin.so
auth       include         common-auth
account    include         common-account
password   include         common-password
session    required        pam_loginuid.so
```

```
session    optional        pam_keyinit.so  force revoke
session    include         common-session
#session   optional        pam_lastlog.so  nowtmp showfailed
session    optional        pam_mail.so standard
```

77. Archivo /etc/pam.d/common-auth:

```
auth     required        pam_env.so
auth     optional        pam_gnome_keyring.so
auth     required        pam_unix.so     try_first_pass
auth     required        pam_tally2.so   onerr=fail deny=4
```

78. Es importante que *pam_tally2.so* se indique como segunda entrada después de *pam_env.so* en */etc/pam.d/login*. Y también, *pam_tally2.so* debe indicarse en */etc/pam.d/common-auth* después de *pam_env.so*.

79. El mecanismo *pam_tally2* no impide los ataques de adivinación de contraseñas, solo impide el uso de la cuenta después de que se haya detectado un ataque de este tipo. Por lo tanto, DEBE asignar una nueva contraseña al usuario antes de reactivar una cuenta. Por ejemplo:

```
# muestra el valor
actual del contador
pam_tally2 --user jdoe
# establece una nueva contraseña y restablece el contador
pam_tally2 --user jdoe --reset
```

80. La utilidad *chage*(1) PUEDE utilizarse para ver y modificar la caducidad de las cuentas de usuario. Los usuarios sin privilegios pueden ver, pero no modificar, sus propios ajustes de caducidad.

5.1.7 ELIMINACIÓN DE USUARIOS

81. La utilidad userdel(8) elimina la cuenta de usuario del sistema, pero no elimina los archivos que están fuera del directorio personal (ni el archivo de cola de correo). Tampoco elimina los procesos que pertenecen a este usuario. Utilice kill (o rearranque el sistema) y find para hacerlo manualmente si es necesario, por ejemplo:

```
# ¿Qué usuario se debe suprimir?
U=jdoe

# Bloquea la cuenta de usuario, pero no la elimina todavía
passwd -l $U

# Elimina todos los procesos de usuario, repetir si es necesario (o rearrancar)
kill -9 `ps -la --User $ U --user $ U |awk '{print $ 4}'`

# Elimina de forma recurrente todos los archivos y directorios que
# pertenecen al usuario (usar con cuidado, porque puede eliminar los
# archivos que pertenecen a otros si están almacenados en un directorio.
```

```
# propiedad de este usuario)
# Utilice el tipo de sistema de archivos aplicable a su sistema.
find / -depth \( ! -fstype ext3 -prune -false \) \
-o -user $U -exec rm -rf {} \;

# Elimina las tareas de cron y at
crontab -u $U -r
find /var/spool/atjobs -user $U -exec rm {} \;

# Ahora suprime la cuenta
userdel $U
```

82. Lo mismo ocurre cuando se elimina un grupo. El administrador DEBE asegurarse de que los archivos asociados con el grupo se reasignan a otros grupos o se suprimen. El administrador también DEBE gestionar los procesos que se están ejecutando actualmente con el grupo suprimido.

83. Además, el administrador debe tener en cuenta que el ID de usuario puede estar en uso en las ACL en las que se debe comprobar la validez de estas ACL.

84. Si necesita crear grupos adicionales o modificar grupos existentes, utilice los comandos *groupadd*(8), *groupmod*(8) y *groupdel*(8).

85. En la configuración evaluada NO se admiten contraseñas de grupo. Se han inhabilitado eliminando el bit de SUID del programa *newgrp*(8). NO DEBE volver a habilitar esta función y NO DEBE utilizar *passwd*(1) con el indicador -g ni con el comando *gpasswd*(1) para definir contraseñas de grupo.

5.1.8 DEFINICIÓN DE CUENTAS ADMINISTRATIVAS

86. Los usuarios administrativos DEBEN ser miembros del grupo trusted. Especifique la opción *-G trusted* para el comando *useradd(8)* al crear usuarios administrativos.

87. También PUEDE utilizar el comando *usermod*(8) para cambiar la pertenencia a grupos. Por ejemplo, si desea añadir el usuario "*jdoe*" al grupo *trusted*, puede utilizar lo siguiente:

```
# Muestra los grupos de los que es miembro el usuario:
groups jdoe

# Añade el grupo adicional
usermod -G $(groups jdoe | sed 's/.*: //; s/ /,/g'),trusted jdoe
```

5.2 CONFIGURACIÓN DE LA DIRECTIVA DE CONTRASEÑAS

88. Para configurar la longitud mínima de la contraseña, el número mínimo de caracteres especiales y numéricos, así como el número mínimo de caracteres en mayúsculas y minúsculas en las contraseñas, se puede añadir o actualizar la línea siguiente en */etc/pam.d/common-password* mediante *pam_cracklib(8)*:

```
password requisite pam_cracklib.so minlen=X dcredit=X ocredit=X ucredit=X
lcredit=X
```

- *minlen* es el tamaño mínimo aceptable de la nueva contraseña
- *dcredit* con N < 0 es el número mínimo de dígitos que deben tener las contraseñas nuevas
- *ocredit* con N < 0 es el número mínimo de otros caracteres que deben tener las contraseñas nuevas
- *ucredit* con N < 0 es el número mínimo de letras mayúsculas que deben tener las contraseñas nuevas
- *lcredit* con N < 0 es el número mínimo de letras minúsculas que deben tener las contraseñas nuevas

5.3 GESTION DE OBJETOS DE DATOS

5.3.1 REVOCACIÓN DEL ACCESO

89. Como ocurre con la mayoría de los sistemas operativos, los derechos de acceso solo se comprueban una vez: cuando el proceso accede por primera vez al objeto. Si la comprobación de permisos inicial se ha realizado correctamente, las operaciones de lectura y escritura se permiten de forma indefinida sin más comprobaciones, incluso si los derechos de acceso al objeto se cambian o se revocan.
90. Si esta revocación diferida no es aceptable en su caso y necesita asegurarse de que ningún proceso de usuario acceda a un objeto después de haber cambiado los derechos de acceso a ese objeto, DEBE rearrancar el sistema. Esto garantiza que ningún proceso tenga descriptores abiertos que permitan un acceso continuo.

5.3.2 MEMORIA COMPARTIDA SYSV Y OBJETOS IPC

91. El sistema admite el uso de memoria compartida compatible con *SYSV*, objetos *IPC* y colas de mensajes. Si los programas no pueden liberar los recursos que han utilizado (por ejemplo, debido a un fallo), el administrador PUEDE utilizar la utilidad *ipcs(8)* para mostrar información sobre esos recursos, e *ipcrm(8)* para forzar la supresión de objetos innecesarios. Estos recursos también se liberan cuando se rearranca el sistema.
92. Para obtener información adicional, consulte la página *man* de *ipc*(2).

5.3.3 COLAS DE MENSAJES POSIX

93. Las colas de mensajes *POSIX* se admiten como alternativa a las colas de mensajes *SYSV*. Los usuarios y administradores PUEDEN utilizar las llamadas al sistema y las funciones de biblioteca correspondientes descritas en la página *man* de *mq_overview(7)*, como *mq_open(2)* y *mq_unlink(2)*.
94. El sistema de archivos de cola de mensajes (tipo *mqueue*) PUEDE estar montado en caso de que se solicite el acceso basado en el sistema de archivos a las colas de mensajes POSIX.

5.3.4 CONFIGURACIÓN DE DERECHOS DE ACCESO A OBJETOS

95. Los administradores PUEDEN utilizar las herramientas *chown(1)*, *chgrp(1)* y *chmod(1)* para configurar los derechos de acceso de DAC. NO DEBE otorgar acceso adicional a los objetos que forman parte de la configuración evaluada.

96. Consulte las páginas *man* correspondientes para obtener más información acerca de estas herramientas.

97. En el paso siguiente DEBE seleccionar "*Common Criteria evaluated configuration*" (Configuración evaluada de Criterios Comunes) para instalar SUSE Linux Enterprise Server en la configuración evaluada.

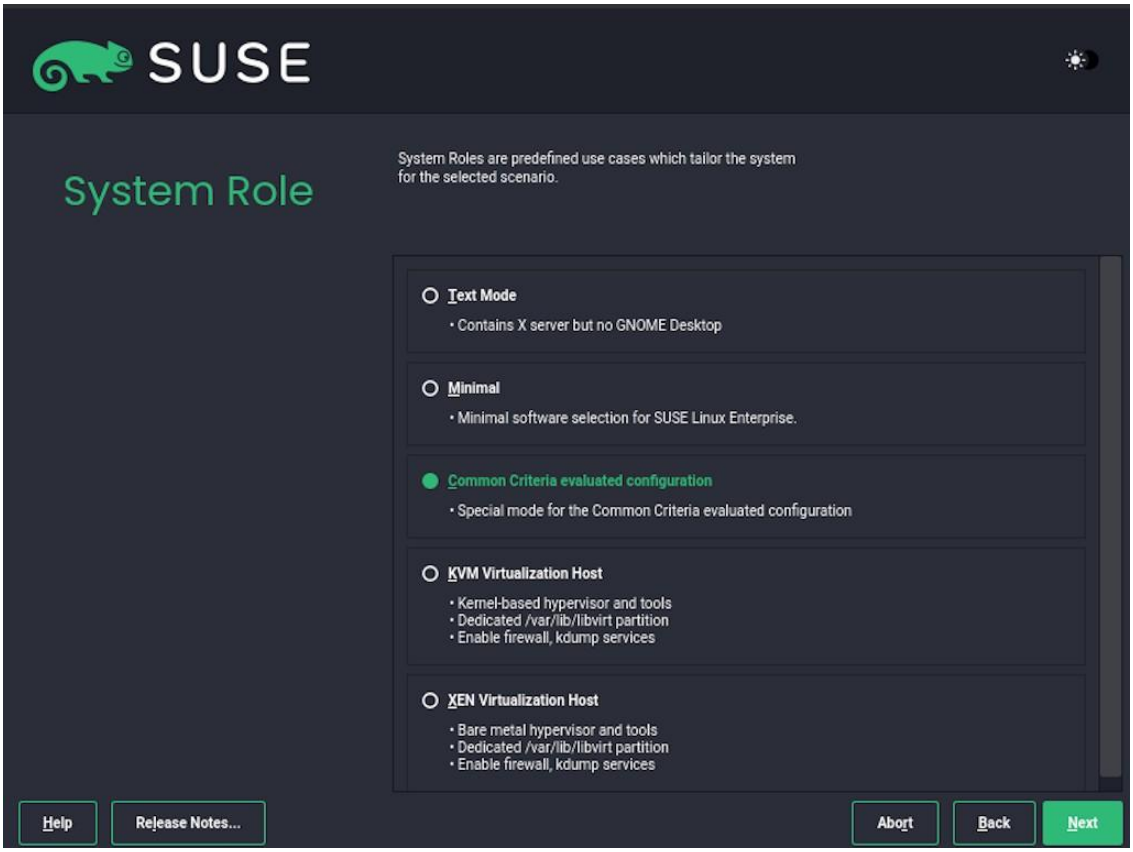

Ilustración 4: Selección de modo de configuración

98. Esta configuración contiene algunas restricciones a las opciones disponibles.

99. El siguiente paso es la partición. PUEDE modificar los siguientes ajustes en este punto:

    - El diseño de las particiones puede adaptarse a las necesidades de la organización. En particular, PUEDE cambiar las particiones; sin embargo, NO DEBE cambiar la configuración de la partición para */boot* si se arranca la configuración de cifrado de disco completo. Además, PUEDE cambiar los sistemas de archivos utilizados a EXT3, EXT4, BTRFS o XFS. NO DEBE utilizar ningún otro sistema de archivos. VFAT PUEDE seleccionarse automáticamente para */boot* o */boot/efi*, donde NO DEBE cambiar esa selección. Si cambia los ajustes, DEBE asegurarse de que se formatean las particiones; el valor por defecto garantiza que las particiones se formatean.

- El esquema de particionamiento sugerido no configura particiones para */tmp* ni */var/tmp*. La configuración automatizada monta particiones *tmpfs* en estos directorios para evitar que se almacenen archivos temporales en el disco. PUEDE crear una partición para cualquier directorio. La instalación automatizada omitirá la configuración de la partición *tmpfs* si los directorios ya son puntos de montaje. Se RECOMIENDA que especifique las opciones de montaje de *nosuid* y *nodev* para las particiones montadas en */tmp* o */var/tmp*.
- PUEDE modificar la configuración de particiones durante el tiempo de ejecución, siempre que solo se utilicen los tipos de sistemas de archivos permitidos indicados en el párrafo anterior.
- Si tiene previsto utilizar el sistema para alojar máquinas virtuales y los dispositivos de disco que proporcionan espacio en disco a las máquinas virtuales deben contar con archivos normales, se RECOMIENDA que determine la ubicación de estos archivos en este momento. Estos archivos son potencialmente muy grandes. La ubicación por defecto elegida por *libvirtd* es */var/lib/libvirt/images/*. PUEDE modificar el diseño de particiones para otorgar espacio a los archivos utilizados como *backends* de dispositivos de disco para las máquinas virtuales.
- PUEDE modificar las opciones del cargador de arranque; por ejemplo, PUEDE establecer una contraseña. Sin embargo, NO DEBE modificar el tipo de cargador de arranque, la ubicación del cargador de arranque ni la opción "*Linux - CC evaluated configuration*" seleccionada del cargador de arranque, que debe ser la opción por defecto.
- Ahora se le pedirá la zona horaria aplicable al sistema. PUEDE seleccionar la zona horaria que quiera. Además, PUEDE configurar un servidor NTP en este punto seleccionando "*Change*" (Cambiar) en el recuadro "*Date and Time*" (Fecha y hora).

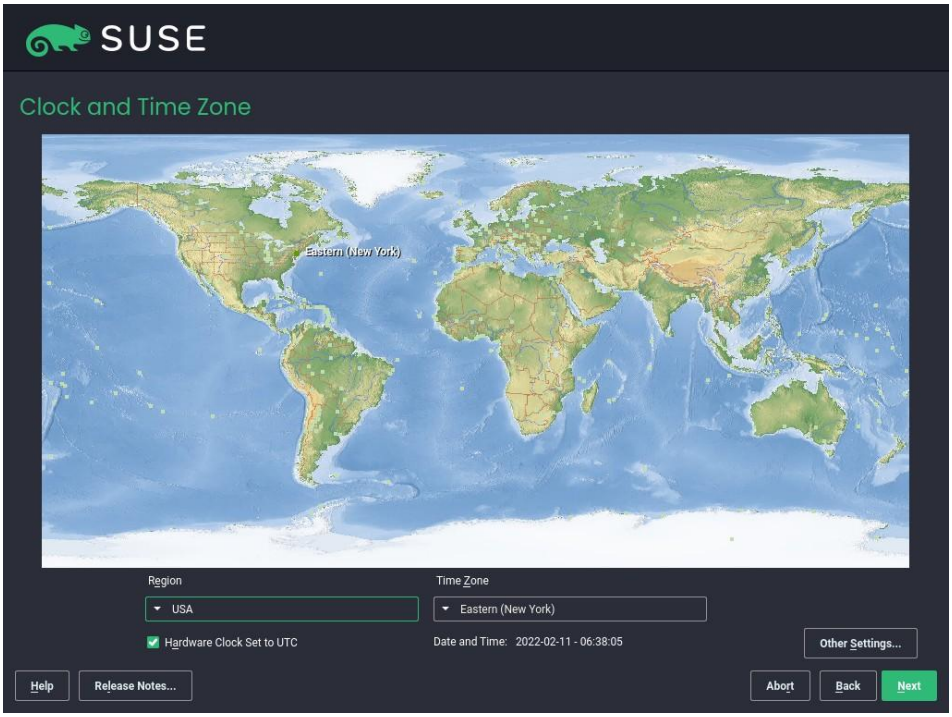

Ilustración 5: Selección de zona horaria

- Posteriormente, se puede crear un nuevo usuario local, como se muestra en la siguiente ilustración.

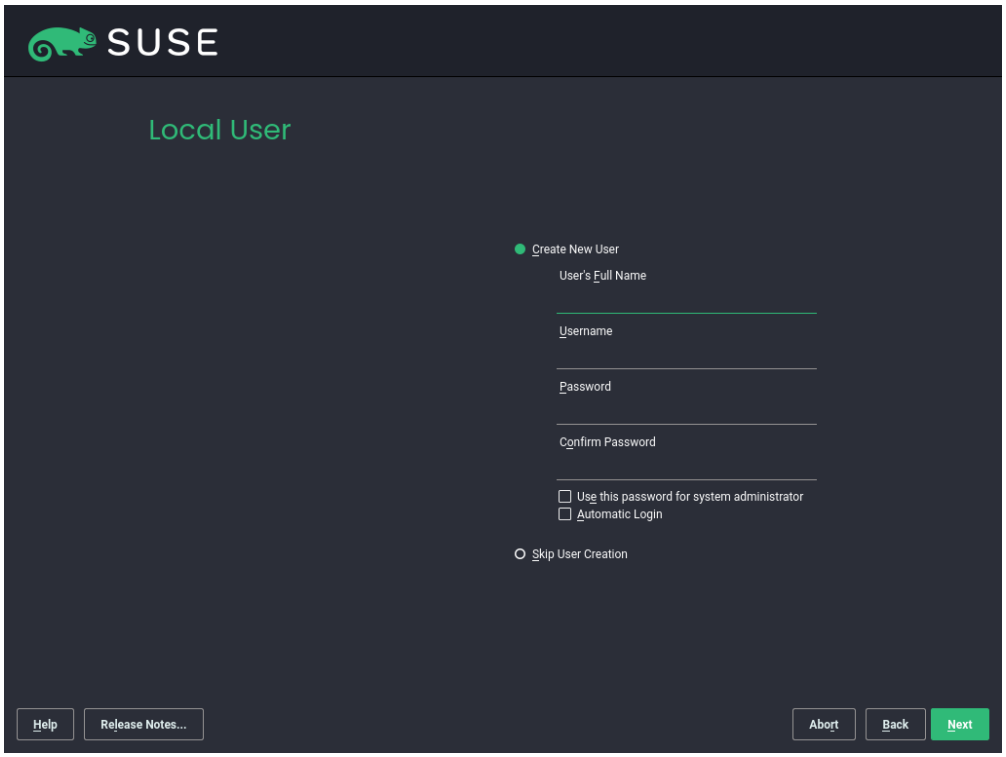

Ilustración 6: Creación de usuario local

- Después de configurar todas las opciones, se invoca el proceso de instalación haciendo clic en "*Install*" (Instalar). Las particiones se generan y se formatean y los paquetes se instalan.
- Una vez finalizado el proceso de instalación, el sistema se rearranca y entra en la fase posterior a la instalación. El sistema se configura automáticamente. No es necesaria la intervención del administrador.
- DEBE asegurarse de que se muestre una configuración correcta como resultado. Si falla algún paso de la configuración, NO DEBE continuar, ya que el sistema se encuentra en un estado desconocido en este momento.
- Después de finalizar la instalación, el usuario creado durante el proceso de instalación ya debe formar parte del grupo *trusted* para permitir el acceso a la identidad y los privilegios de usuario *root*. Si el usuario no forma parte del grupo *trusted*, se puede utilizar el siguiente comando para añadir a este usuario a dicho grupo, donde <USUARIO> hace referencia al nombre del usuario añadido anteriormente:

  usermod -G trusted -a <USUARIO>

INSTALACIÓN EN IBM Z SYSTEM

100. A la hora de realizar la instalación en *IBM Z System*, hay que tener en cuenta ciertos elementos, por ejemplo, cómo acceder al sistema de instalación. Normalmente, los

equipos IBM Z System son sistemas autónomos en los que se accede a la consola z/VM de forma remota. Para instalar la imagen descargada anteriormente, se requiere una conexión VPN al entorno HMC z15. Además, para el servidor FTP, donde se monta la imagen ISO s390x, es necesario definir un nombre de usuario y una contraseña.

101. El primer paso para instalar SUSE Linux Enterprise 15 SP4 es la recuperación desde un medio remoto, como se muestra en la siguiente ilustración.

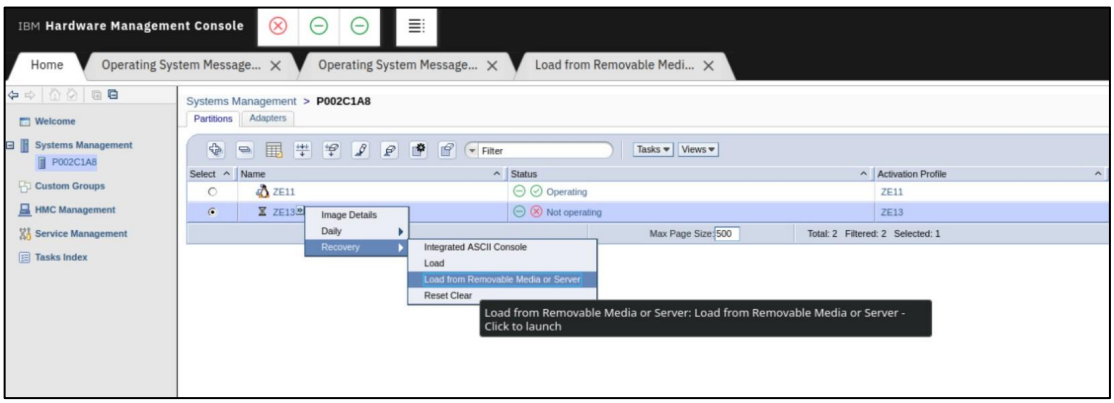

Ilustración 7: Recuperación desde un medio remoto

102. Ahora introduzca las credenciales de FTP, incluido el nombre de *host* y la vía del archivo. En el siguiente paso, seleccione *[...]/suse.ins (no [...]/susehmc.ins)* y continúe. Después de proporcionar la contraseña del usuario, la imagen se cargará y el proceso continuará correctamente.

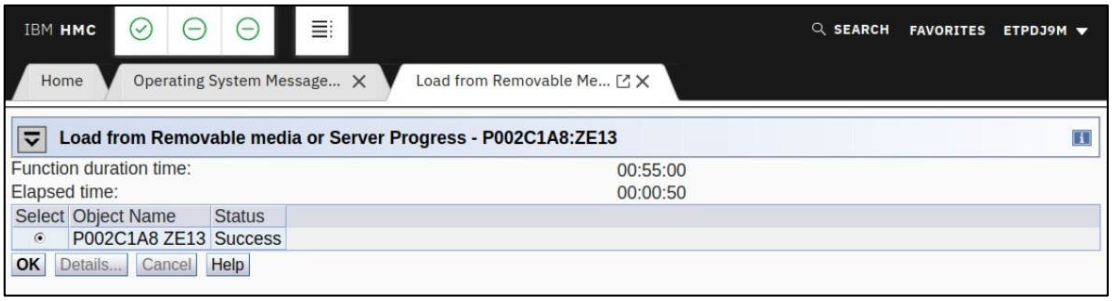

Ilustración 8: Carga de la imagen

103. El siguiente paso es acceder a la salida del sistema operativo de HMC. Inicie la instalación (1), elija como red de origen y como protocolo FTP (1). Elija la primera tarjeta de red dentro de la máquina virtual de System Z, que siempre debe ser 0.0.1.b00, y utilice los valores por defecto. No utilice compatibilidad con OSI Layer 2 (2).

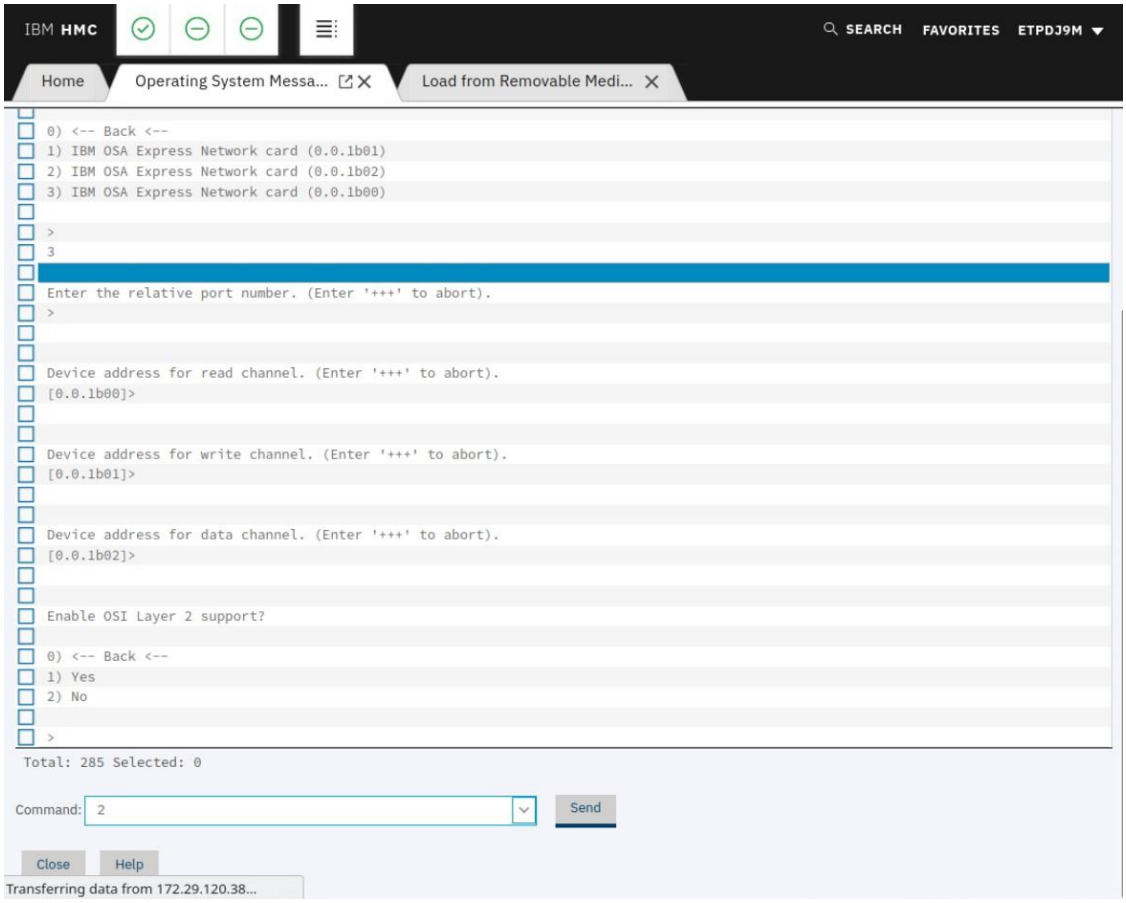

Ilustración 9: Selección de la tarjeta de red

104. Ahora debe configurarse la conexión de la interfaz de red con el servidor FTP. Por lo tanto, deben definirse la dirección IP, la puerta de enlace y el servidor DNS. El dominio de búsqueda está vacío.

105. A continuación, introduzca la dirección IP del servidor FTP y el directorio de medios. Seleccione que se necesita una contraseña para acceder al servidor FTP (1) e introduzca el nombre de usuario y la contraseña.

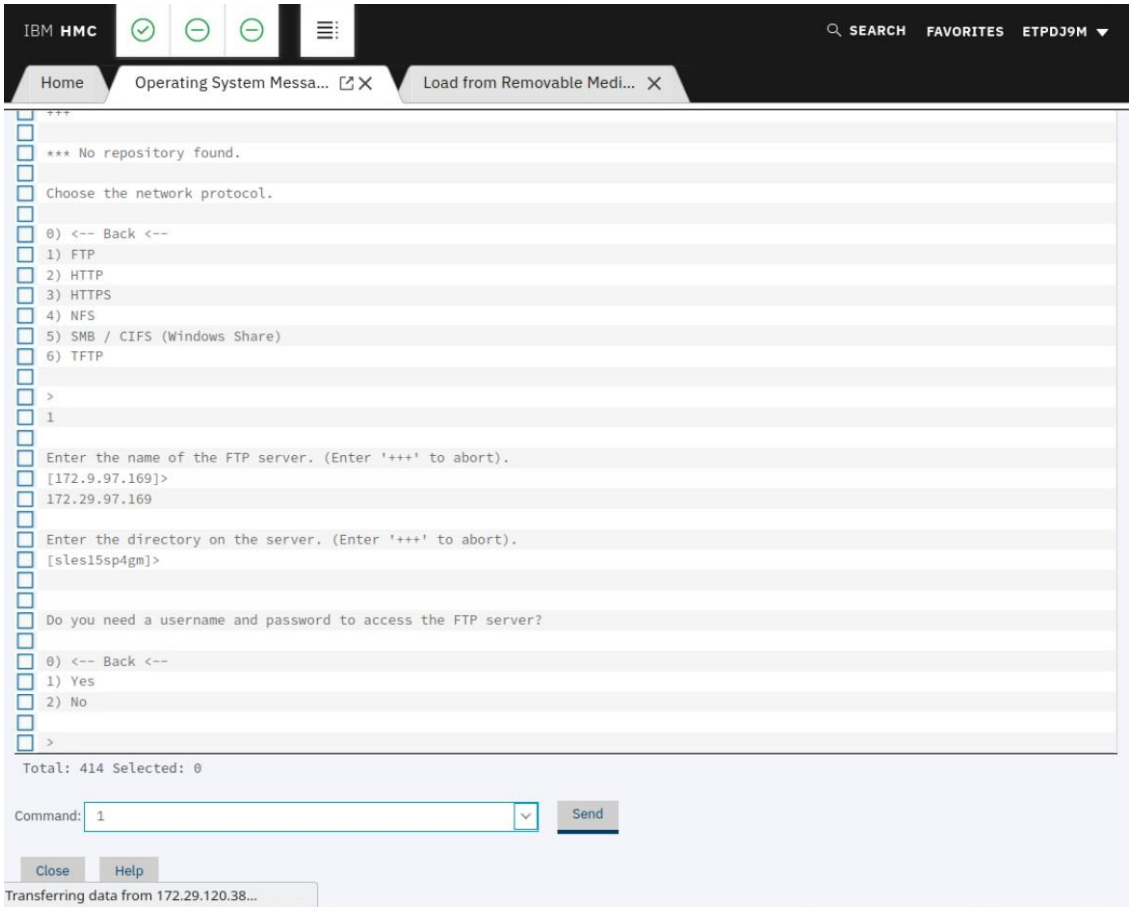

Ilustración 10: Acceso al FTP

106. Seleccione que no se necesita proxy (2). El sistema de instalación ya está cargado. Seleccione la instalación SSH (3) y defina una contraseña, ya que solo se admite SSH. Al seleccionar la opción para acceder al sistema a través de SSH, se generan las claves SSH y se inicia el servidor SSH. Este es el método de acceso sugerido cuando se inicia la interfaz gráfica YaST en caso de que el equipo cliente del administrador aloje un sistema de ventanas X11 y el administrador habilite el reenvío X11 con el cliente SSH. Conéctese por VPN a través de SSH al sistema de instalación.

107. Después de arrancar y seleccionar el método de acceso para la instalación, la imagen de arranque espera a que el administrador entre e inicie "*yast.ssh*" en la línea de comandos. YaST invocará automáticamente el proceso de instalación automática.

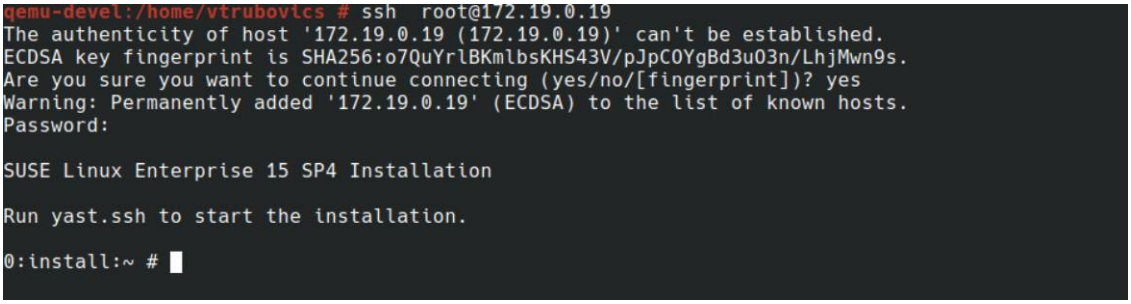

Ilustración 11: Consola previa a la ejecución de YaST

108. Después de seleccionar SUSE Linux Enterprise Server 15 SP4 y aceptar el acuerdo de licencia, seleccione "*Configure ZFCP Disks*" (Configurar discos ZFCP) y siga los pasos descritos en 5.1.1. Después, podrá conectarse al sistema a través de SSH.

INSTALACIÓN EN IBM POWER

109. A la hora de realizar la instalación en *IBM POWER System*, hay que tener en cuenta ciertos elementos, por ejemplo, cómo acceder al sistema de instalación. Normalmente, los equipos IBM POWER System son sistemas autónomos en los que se accede de forma remota a la consola. Para instalar la imagen descargada anteriormente, se requiere una conexión VPN al entorno HMC.

110. El primer paso después de cargar la imagen ISO de SUSE Linux Enterprise 15 SP4 en un IBM POWER LPAR existente es conectarse a la consola Web del sistema IBM POWER y desplazarse a Resources (Recursos) > All Systems (Todos los sistemas) > <system name> (nombre del sistema) > Virtual Storage (Almacenamiento virtual) y seleccionar "*Manage Virtual Storage*" (Gestionar almacenamiento virtual). Donde <system name> (nombre del sistema) es el nombre del sistema gestionado.

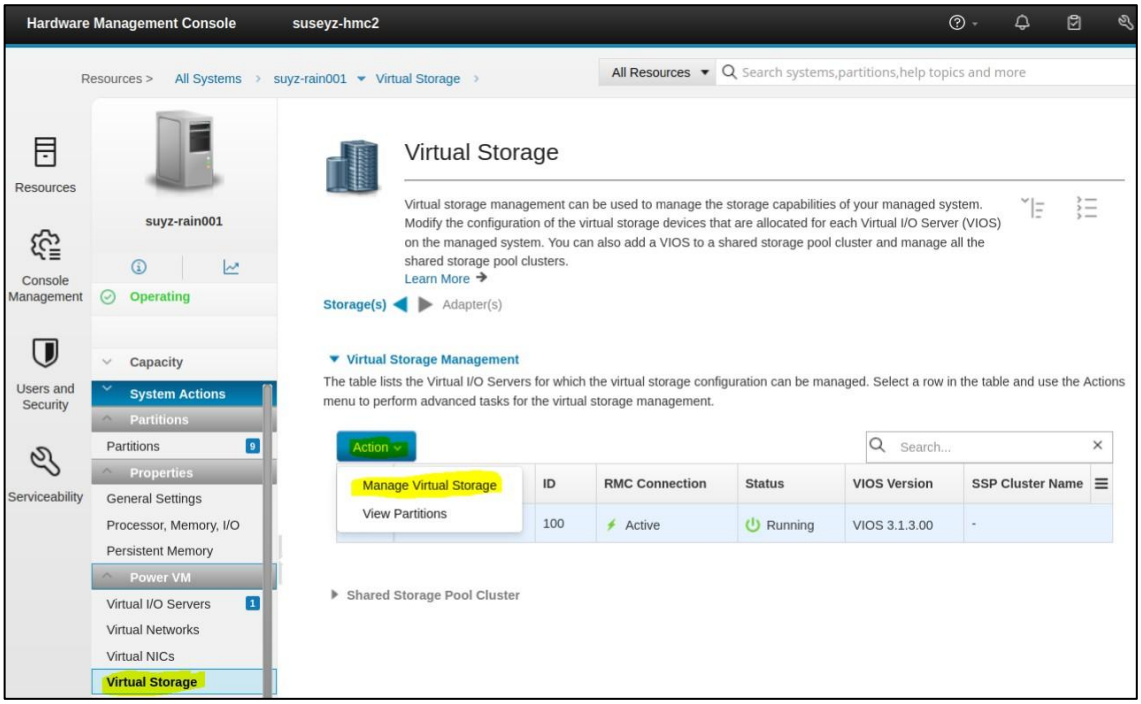

Ilustración 12: Almacenamiento virtual

111. Abra la pestaña "Optical Device" (Dispositivo óptico) y seleccione la acción "Add Media" (Añadir medio). Introduzca el nombre del medio y el nombre del archivo del medio óptico y continúe con OK (Aceptar). Ahora, cree una partición como se muestra a continuación.

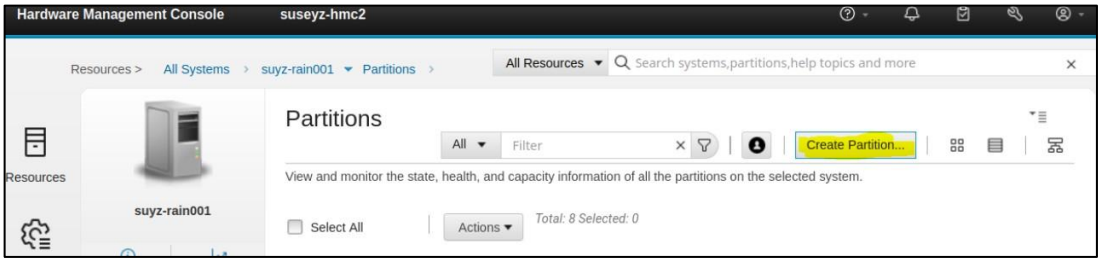

Ilustración 13: Selección de la partición

112. Siga las instrucciones seleccionando un nombre de partición, el tipo de partición "AIX/Linux", el modo del procesador, la configuración de la memoria y finalice el proceso de creación de la partición aprobando con OK (Aceptar).

113. Para continuar con el paso siguiente, seleccione la partición recién creada dentro de la pestaña "Partitions" (Particiones) y seleccione la acción "View Partitions Properties" (Ver propiedades de las particiones).

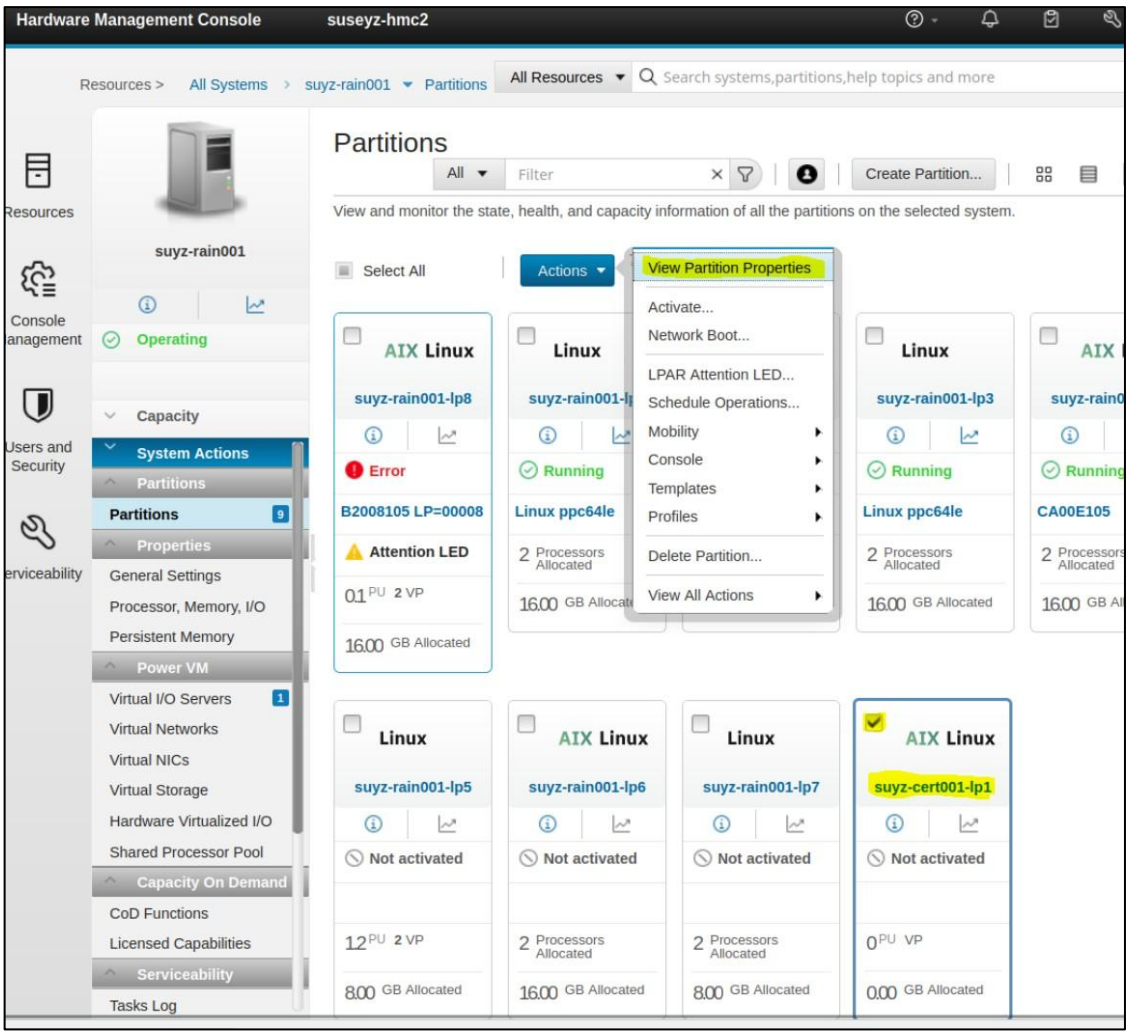

Ilustración 14: Propiedades de la partición

114. Ahora, seleccione "Virtual Storage" (Almacenamiento virtual) en el menú de la izquierda y añada un volumen lógico. Proporcione un nombre de dispositivo y el tamaño de almacenamiento que se va a asignar.

115. Después de asignar el almacenamiento, es necesario añadir una red virtual. Para ello, seleccione en el menú de la izquierda "Virtual Networks" (Redes virtuales), seguido de "Attach Virtual Network" (Adjuntar red virtual) como se muestra a continuación y adjunte una red virtual de la lista.

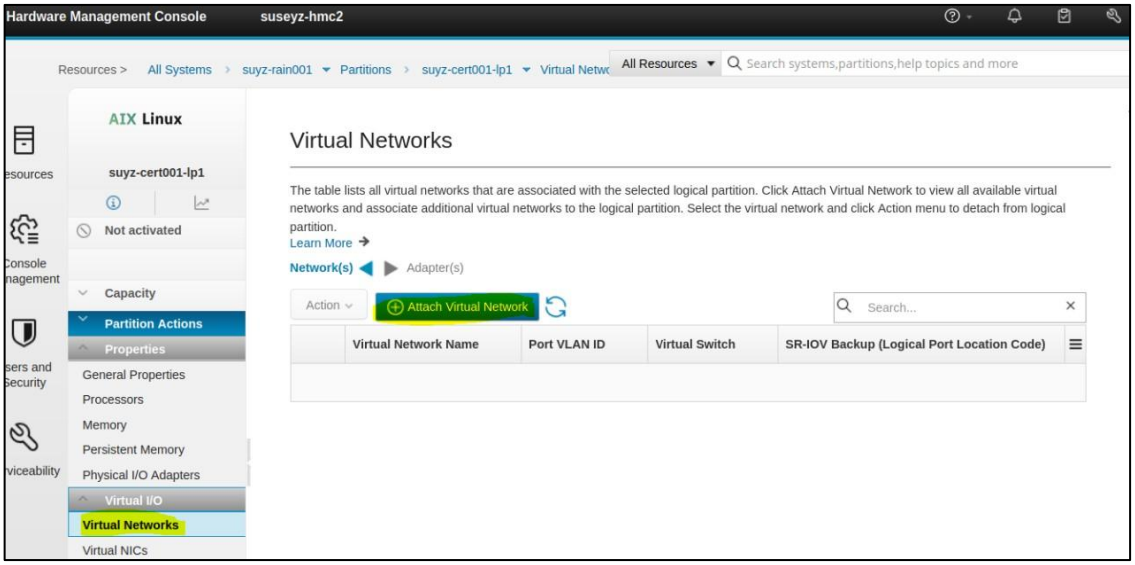

Ilustración 15: Selección de red virutal

116. Para la NIC (controlador de interfaz de red) virtual, haga lo mismo que para la red virtual. Para ello, seleccione en el menú de la izquierda "Virtual NICs" (NIC virtuales), seguido de "Add Virtual NIC" (Añadir NIC virtual), seleccione el código de ubicación del puerto físico y marque la casilla de verificación como se muestra a continuación.

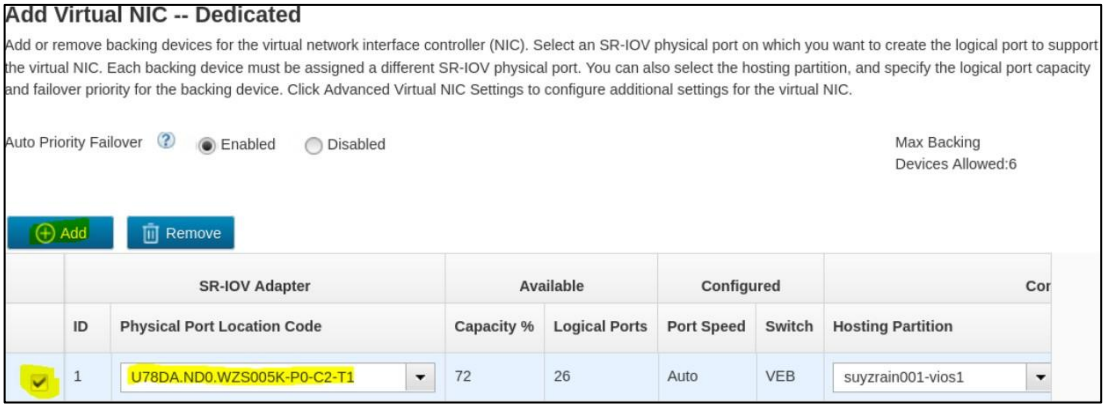

Ilustración 16: Selección de ubicación del puerto físico

117. Termine de configurar la NIC virtual aprobando con OK (Aceptar). El siguiente paso es montar la imagen ISO en el dispositivo óptico virtual. Para ello, seleccione "Virtual Storage" (Almacenamiento virtual) en el menú de la izquierda y la pestaña "Virtual Optical Device" (Dispositivo óptico virtual). Ahora, añada un dispositivo óptico virtual proporcionando el nombre del dispositivo y seleccionando el servidor de E/S virtual. Continúe con OK (Aceptar), seleccione Action (Acción) > Load (Cargar) en la pestaña "Virtual Optical Device" (Dispositivo óptico virtual) y elija la imagen ISO de SUSE Linux Enterprise 15 SP4.

118. Para activar la partición, seleccione "Partitions" (Particiones) en el menú de la izquierda y la partición recién creada y modificada, seguido de Actions (Acciones) > Activate (Activar), como se muestra a continuación.

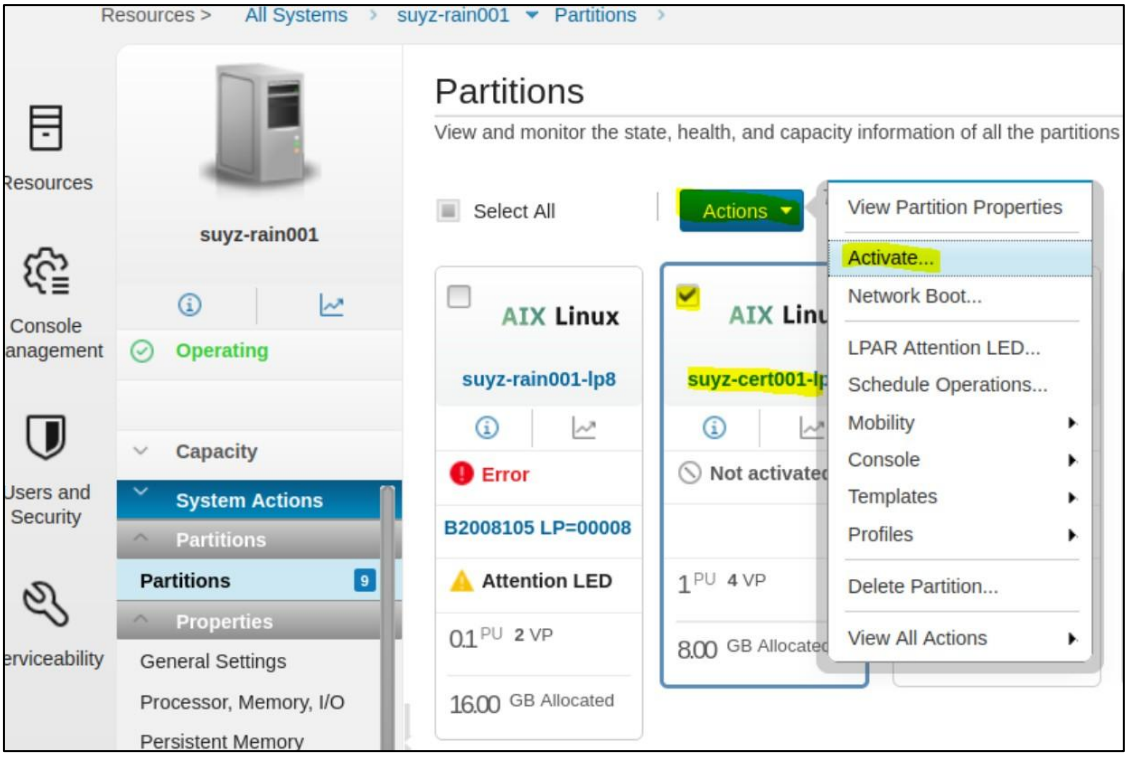

Ilustración 17: Activación de la partición

119. Seleccione "Activate" (Activar) como "Operation Type" (Tipo de operación), "System Management Services" (Servicios de gestión del sistema) para "Boot Mode" (Modo de arranque) y continúe con el botón Finish (Finalizar).

120. Ahora, inicie sesión en HMC con ssh e inicie un terminal virtual con *vtmenu*. Elija la partición creada y siga los pasos siguientes:

    1. Seleccione las opciones de arranque (5)
    2. Configure el orden de los dispositivos de arranque (2)
    3. Seleccione el primer dispositivo de arranque (1)
    4. Muestre todos los dispositivos (6)
    5. Vaya al CD-ROM SCSI (3)
    6. Defina la secuencia de arranque: configúrelo como primer dispositivo de arranque (2)

121. Después de volver al menú principal escribiendo "M" y de salir de los servicios de gestión del sistema con "X", siga los pasos descritos en 5.1.1. Después, podrá conectarse al sistema a través de SSH.

122. En los pasos de configuración posteriores NO DEBE utilizar la herramienta YaST.

5.3.5 CONFIGURACIÓN ADICIONAL

123. Después de finalizar el proceso de instalación como se describe en el capítulo anterior, DEBE seguir las configuraciones basadas en la plataforma indicada en este capítulo, y PUEDE instalar los siguientes paquetes mediante el comando *zypper* si desea habilitar la auditoría remota, las actualizaciones automáticas y las manuales con el Centro de servicios al cliente de SUSE (SCC) y las configuraciones del cortafuegos:

    zypper install audit-audispd-plugins yast2-online-update yast2-online-update-configuration firewalld

124. Además, se DEBEN instalar los siguientes paquetes de actualización, que están disponibles a través del mecanismo de actualización después de que el sistema se registre con los canales de actualización descritos en la sección 6.17 "CONFIGURACIÓN DE LAS ACTUALIZACIONES":

Kernel de Linux

125. SE RECOMIENDA instalar el paquete kernel-default versión 5.14.21-150400.24.69.1, añadiendo la opción de montaje noexec para evitar la ejecución accidental de archivos o guiones en sistemas de archivos montados adicionales.

126. Estos ajustes no protegen por completo contra código y datos dañinos, por lo que DEBE verificar que los datos proceden de una fuente de confianza y no ponen en peligro la seguridad del servidor. En concreto, tenga en cuenta los siguientes problemas:

    - Incluso los programas y guiones sin privilegios pueden contener código malicioso que utilice los derechos del usuario que realiza la llamada de formas no deseadas, por ejemplo, corrompiendo los datos del usuario, introduciendo troyanos en el sistema, atacando a otros equipos de la red, revelando documentos confidenciales o enviando correo electrónico comercial no solicitado ("spam").
    - Los datos del sistema de archivos adicional DEBEN tener los derechos de acceso adecuados para evitar la divulgación o también para extraer todos los paquetes dependientes.

OpenSSH

127. Instale los paquetes de OpenSSH versión 8.4p1-150300.3.22.1 actualizados ejecutando los siguientes comandos:

    openssh-8.4p1-150300.3.22.1

    openssh-clients-8.4p1-150300.3.22.1

    openssh-common-8.4p1-150300.3.22.1

    openssh-fips-8.4p1-150300.3.22.1

    openssh-server-8.4p1-150300.3.22.1

128. Además, para el cargador de arranque, DEBE definirse lo siguiente en la línea de comandos del kernel:

    "random.trust_cpu=0"

129. La ubicación exacta de este parámetro se encuentra en el archivo "/boot/ grub2/ grub.cfg" que se compila a partir del archivo "/etc/default/ grub" y se encuentra en el directorio "/etc/grub.d" al ejecutar el comando "grub2-mkconfig -o /boot/grub2/grub.cfg". Por lo tanto, nunca debe editar el archivo manualmente. En su lugar, edite los archivos fuente relacionados o utilice el módulo gestor de arranque de YaST para modificar la configuración como se describe en la Sección 18.3.3.2 "Kernel Parameters tab" según la referencia que se muestra a continuación.

    https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-grub2.html

5.3.6 CONFIGURACIÓN X86

130. La siguiente versión del paquete kernel-default DEBE estar instalada en sistemas x86 junto con la siguiente actualización del paquete de microcódigo:
    - kernel-default-5.14.21-150400.24.81.1
    - ucode-intel-20230808-150200.27.1
131. En las CPU x86, el conjunto de instrucciones AES-NI está disponible para acelerar la operación de AES. Si en su lugar se va a utilizar la compatibilidad solo con software, se DEBE aplicar la siguiente configuración.
132. Tenga en cuenta que en la configuración evaluada, AES- NI DEBE estar desactivado. Por lo tanto, para que el resultado de la evaluación sea conforme, DEBE aplicar las siguientes configuraciones.
133. Después del primer arranque, DEBE inhabilitar los módulos AES-NI y Bluetooth del kernel de Linux para evitar que se utilicen. Para ello, cree los siguientes archivos con el siguiente contenido:

ARCHIVO	CONTENIDO
/lib/modprobe.d/aesni_intel.conf	install aesni_intel /bin/true
/lib/modprobe.d/bluetooth.conf	install bluetooth /bin/true

Tabla 2: Configuración x86

5.3.7 CONFIGURACIÓN DEL SISTEMA ARM64

134. En las CPU ARM, el conjunto de instrucciones CE está disponible para acelerar las operaciones de AES y SHA. Si en su lugar se va a utilizar la compatibilidad solo con *software*, se DEBE aplicar la siguiente configuración.
135. Tenga en cuenta que **en la configuración evaluada, CE DEBE estar desactivado**. Por lo tanto, para que el resultado de la evaluación sea conforme, DEBE aplicar las siguientes configuraciones.

136. Después del primer arranque, DEBE **inhabilitar los módulos del kernel de CE Linux para evitar que se utilicen**. Para ello, cree el siguiente archivo con el siguiente contenido:

ARCHIVO	CONTENIDO
/lib/modprobe.d/aes_ce.conf	install aes_ce_cipher /bin/true install aes_ce_blk /bin/true install sha2_ce /bin/true install ghash_ce /bin/true install crct10dif_ce /bin/true

Tabla 3: Configuración del sistema ARM64

5.3.8 CONFIGURACIÓN DEL SISTEMA IBM Z

137. Después del primer arranque, DEBE inhabilitar varios módulos del kernel de Linux para evitar que se utilicen. Para ello, cree los siguientes archivos con el siguiente contenido:

ARCHIVO	CONTENIDO
/lib/modprobe.d/aes_s390.conf	install aes_s390 /bin/true
/lib/modprobe.d/des_s390.conf	install des_s390 /bin/true
/lib/modprobe.d/ghash_s390.conf	install ghash_s390 /bin/true
/lib/modprobe.d/sha1_s390.conf	install sha1_s390 /bin/true
/lib/modprobe.d/sha256_s390.conf	install sha256_s390 /bin/true
/lib/modprobe.d/sha512_s390.conf	install sha512_s390 /bin/true

Tabla 4: Configuración del sistema IBM Z

138. Después de actualizar la configuración, DEBE reiniciar el sistema.

5.3.9 CONFIGURACIÓN DEL SISTEMA IBM POWER

139. Para los sistemas IBM POWER, el procesador proporciona instrucciones para implementar la compatibilidad con AES y SHA2 denominado VMX. Esta compatibilidad NO DEBE utilizarse. En su lugar, deben usarse los algoritmos de solo software. Por lo tanto, se DEBEN aplicar las siguientes configuraciones.

140. Después del primer arranque, DEBE inhabilitar varios módulos del kernel de Linux para evitar que se utilicen. Para ello, cree los siguientes archivos con el siguiente contenido:

ARCHIVO	CONTENIDO
/lib/modprobe.d/aes-ppc-spe.conf	install aes-ppc-spe /bin/true
/lib/modprobe.d/sha1-ppc-spe.conf	install sha1-ppc-spe /bin/true

141. Después de actualizar la configuración, DEBE reiniciar el sistema.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

142. Para garantizar que los sistemas permanezcan en un estado seguro, se DEBE tener especial cuidado durante el funcionamiento del sistema.

6.1.1 INICIO, APAGADO Y RECUPERACIÓN TRAS FALLOS DEL SISTEMA

143. Utilice los programas *shutdown*(8), *halt*(8) o *reboot*(8) según sea necesario para apagar o reiniciar el sistema.

144. Cuando se enciende (o cuando se carga el programa inicial de la partición lógica en un sistema host), el sistema arranca en el sistema operativo SLES. Si es necesario (por ejemplo, después de un fallo), se realizará automáticamente una comprobación del sistema de archivos. En raras ocasiones, puede ser necesaria una intervención manual. Consulte la documentación de *fsck*(8) y *debugfs*(8) para obtener más información.

145. En caso de que se necesite un proceso de arranque no estándar (por ejemplo, desde un disquete o un CD-ROM para sustituir un disco duro defectuoso), se puede utilizar la interacción con el cargador de arranque o con el sistema de gestión del host para modificar el procedimiento de arranque para la recuperación. Por ejemplo, el argumento de la línea de comandos del kernel para arrancar en el modo de emergencia puede ser útil:

    systemd.unit=emergency.target

146. Además, el destino rescue proporciona un entorno útil:

    systemd.unit=rescue.target

147. Consulte la documentación pertinente del cargador de arranque, así como la guía del administrador de SLES, para obtener más información.

6.1.2 INSTALACIÓN DE SOFTWARE ADICIONAL

148. PUEDEN instalarse paquetes de software adicionales según sea necesario, siempre que no entren en conflicto con los requisitos de seguridad.

149. El *software* adicional que se pueda añadir no está diseñado para utilizarse con privilegios de superusuario. El administrador DEBE utilizar para las tareas de administración solo los programas que forman parte de la configuración original, excepto si el administrador se ha asegurado por su parte de que el uso del *software* adicional no supone un riesgo para la seguridad.

150. Los administradores PUEDEN añadir guiones para automatizar tareas siempre y cuando solo dependan de programas que formen parte de la configuración evaluada y se ejecuten en esos programas.

151. Los requisitos de seguridad para el *software* adicional son estos:

- **NO DEBE instalar ni cargar módulos del kernel distintos de los proporcionados como parte de la configuración evaluada.** NO DEBE cargar el módulo del kernel *tux*

(el servidor Web del kernel no es compatible). NO DEBE añadir compatibilidad para formatos binarios que no sean ELF ni para emulación de formato binario foráneo que eluda la auditoría de llamadas al sistema. NO DEBE activar *knfsd* ni exportar sistemas de archivos NFS.

- NO DEBE añadir al sistema nodos especiales del dispositivo.
- NO DEBE añadir al sistema programas de *root* de SUID, programas de *root* de SGID ni programas con capacidades de sistema de archivos. PUEDE añadir programas que utilicen los bits SUID o SGID para ejecutarse con identidades que no sean de usuario *root* si los valores numéricos de SUID y SGID no son inferiores a 500, tal como se define con los valores *UID_MIN* y *GID_MIN* en el archivo de configuración */etc/login.defs*. Esta restricción es necesaria para evitar conflictos con los ID de usuario y grupo del sistema, como el grupo "*disk*".
- **NO DEBE modificar el contenido, los permisos ni la propiedad de ninguno de los objetos del sistema de archivos existentes** (incluidos los directorios y los nodos de dispositivo) que formen parte de la configuración evaluada. PUEDE añadir archivos y directorios a directorios existentes siempre que esto no infrinja ningún otro requisito.
- **NO DEBE añadir al sistema programas lanzados automáticamente con privilegios de usuario *root***. Excepción: se permiten los procesos que cambian de forma *inmediata* y *permanente* a una identidad sin privilegios durante el lanzamiento; por ejemplo, usar "su *USERID -c LAUNCH_COMMAND*" en el archivo de inicio, o alternativamente usar las llamadas al sistema *setgroups*(2), *setgid*(2) y *setuid*(2) en un binario. Las llamadas *setuid*(2), etc. no son suficientes: **si el administrador no puede identificar cuándo y cómo se eliminan los privilegios, la aplicación NO DEBE instalarse**.

152. Los mecanismos de lanzamiento automático son:

- Destinos y unidades como parte del mecanismo *systemd*.
- Tareas programadas mediante cron (incluidas las entradas de los archivos */etc/cron**)
- Aplicaciones iniciadas utilizando el DBUS del sistema, que se configura mediante */etc/dbus-1/system.d/*.
- Aplicaciones especificadas en */etc/sudoers* o con reglas ubicadas en un archivo en el directorio */etc/sudoers.d*. Tenga en cuenta que ese archivo puede contener la palabra clave *ALL* como espacio reservado para un comando. En ese caso, el usuario autorizado a ejecutar todos los comandos con esa regla utilizando el ID de usuario *root* DEBE asegurarse de que las aplicaciones adicionales no se ejecutan mediante *sudo*. Este requisito solo se puede cumplir con procedimientos operativos.
- Aplicaciones generadas a través de *udev*, donde las reglas se añaden a */lib/udev/rules.d.*

153. Ejemplos de programas que normalmente no entran en conflicto con estos requisitos y que PUEDEN instalarse son los compiladores, los intérpretes, los servicios de red que se ejecutan con derechos de usuario no *root* y programas similares. Los requisitos indicados anteriormente DEBEN verificarse en cada caso específico.

6.2 ADMINISTRACIÓN DEL PRODUCTO

154. Las tareas de administración del sistema requieren privilegios de superusuario. La entrada directa a la red como usuario *root* está inhabilitada. Para obtener derechos de superusuario, primero DEBE autenticarse utilizando un ID de usuario sin privilegios y, a continuación, utilizar el comando *su* o *sudo* para cambiar de identidad. NO DEBE utilizar los derechos de usuario *root* para nada que no sean las tareas administrativas que requieran estos privilegios; todas las demás tareas DEBEN realizarse utilizando su ID de usuario normal (no *root*).

155. Los ID de usuario que pertenecen a usuarios administrativos se asignan al grupo *trusted*. SLES utiliza un grupo denominado *trusted* para proporcionar acceso de administrador a los usuarios, a diferencia de otras distribuciones de Linux que pueden utilizar un grupo denominado *wheel*. Ese grupo NO DEBE utilizarse para ningún otro ID de usuario. Solo los usuarios que pertenecen al grupo *trusted* pueden invocar el comando *su* para evitar ataques de contraseña contra la cuenta del usuario *root*.

6.2.1 USO DE *SU*

156. El comando *su* permite un cambio permanente del ID de usuario para la sesión actual. DEBE utilizar exactamente la siguiente línea de comando de *su*(1) para obtener acceso de superusuario:

    /usr/bin/su -

157. Esto garantiza que se ejecuta el binario correcto, independientemente de los ajustes de PATH o los alias de *shell*, y que la *shell* raíz comienza con un entorno limpio no contaminado con los ajustes del usuario inicial. Esto es necesario porque la configuración de *shell .profile* y otros archivos similares se pueden escribir desde un ID sin privilegios, lo que permitiría a un atacante elevar fácilmente sus privilegios a los de usuario *root* si pudiera subvertir estos ajustes.

158. Los administradores NO DEBEN añadir ningún directorio a la vía PATH del usuario *root* en la que cualquier otro usuario que no sea *root* pueda escribir. Y del mismo modo, NO DEBEN utilizar ni ejecutar ningún guion, binario ni archivo de configuración en los que cualquier otro usuario que no sea *root* pueda escribir, ni tampoco en ningún directorio que los contenga.

6.2.2 USO DE *SUDO*

159. El comando *sudo* permite invocar un comando con un ID de usuario configurado, incluido el ID de usuario *root*. El cambio al ID de usuario de destino solo se conserva durante el tiempo de ejecución del comando especificado.

160. La configuración por defecto de *sudo* no permite que ningún usuario sin privilegios invoque comandos con privilegios. Dependiendo de sus requisitos, los siguientes ejemplos pueden utilizarse como guía para configurar *sudo*. Puede obtener más información en la página *man* de *sudoers*(5).

161. La siguiente configuración permite a todos los usuarios asociados al grupo *trusted* utilizar todos los comandos con privilegios:

%trusted ALL=(ALL) ALL

162. El uso de comandos con la identidad de usuario *root*, otras identidades del sistema o grupos de sistemas DEBE estar restringido a los usuarios del grupo *trusted*.

6.3 GESTIÓN DE CUENTAS DE USUARIO

6.3.1 CREACIÓN DE USUARIOS

163. Utilice el comando *useradd*(8) para crear nuevas cuentas de usuario y, a continuación, el comando *passwd*(1) para asignar una contraseña inicial al usuario. Como alternativa, si el usuario está presente cuando se crea la cuenta, permítale elegir su propia contraseña. Consulte las páginas *man* de *useradd*(8) y *passwd*(1) para obtener más información.

164. Si asigna una contraseña inicial para un nuevo usuario, DEBE transferírsela de forma segura al usuario, asegurándose de que ningún tercero obtenga la información. Por ejemplo, puede decirle personalmente la contraseña a un usuario que conozca. Si no es posible, PUEDE enviarle la contraseña por escrito en una carta cerrada. Esto puede también hacerse cuando se define una contraseña nueva para un usuario en caso de que este haya olvidado la suya o la contraseña haya caducado. DEBE informar al usuario de que DEBE cambiar esta contraseña inicial cuando inicie por primera vez la sesión en el sistema y seleccionar su propia contraseña de acuerdo con las reglas definidas en la sección 7.3.3 "POLÍTICA DE CONTRASEÑAS" de esta guía.

165. NO DEBE utilizar la opción -p para *useradd*(8), ya que si especifica una contraseña de ese modo, se omitirá el mecanismo de comprobación de la calidad de la contraseña.

166. El usuario DEBE cambiar la contraseña temporal definida por el administrador lo antes posible. Utilice el comando *chage*(8) con la opción -d para definir la fecha del último cambio de contraseña con un valor que servirá para recordarle al usuario que debe cambiar la contraseña. El valor RECOMENDADO se basa en los ajustes de */etc/login.defs* y equivale a la fecha de hoy más el valor de *PASS_WARN_AGE* menos el de *PASS_MAX_DAYS*.

167. Ejemplo:

```
useradd -m -c
"John Doe" jdoe
passwd jdoe
chage -d $(date +%F -d "hace 53 días") jdoe
```

168. La opción -m para *useradd*(8) crea un directorio principal para el usuario basado en una copia del contenido del directorio */etc/skel/*. PUEDE modificar algunos ajustes de configuración por defecto para los usuarios, como el de *umask*(2) o la zona horaria, editando los archivos de configuración global correspondientes:

/etc/profile
/etc/bash.bashrc
/etc/csh.cshrc

6.3.2 CAMBIO DE CONTRASEÑAS DE USUARIO

169. Si es necesario, PUEDE restablecer la contraseña del usuario a un valor conocido utilizando *passwd USUARIO* e introduciendo la nueva contraseña. No es posible recuperar la contraseña utilizada anteriormente, ya que la función hash que se emplea no es reversible.

6.3.3 AUTENTICACIÓN BASADA EN CLAVE SSH

170. El TOE permite configurar la autenticación basada en clave para SSH. La autenticación basada en clave se configura usuario por usuario, gestionando el archivo *.ssh/authorized_keys* en el directorio personal de un usuario. Para obtener información sobre cómo utilizar ese archivo, consulte *sshd*(8).

171. Para generar claves que se puedan usar en la autenticación basada en clave, se proporciona la herramienta *ssh-keygen*(8), cuyo uso se RECOMIENDA encarecidamente, ya que solo esta utilidad proporcionada con el TOE ha estado sujeta a la evaluación de seguridad. Dado que el *daemon* de SSH solo acepta la versión 2 del protocolo SSH, con este daemon únicamente se admiten las claves del protocolo 2. Por lo tanto, solo DEBE utilizar la opción *-t rsa* o *-t ecdsa* cuando genere una clave con *ssh-keygen*.

172. La utilidad *ssh-keygen* permite especificar el tamaño de clave para RSA, con un valor por defecto de 2048 bits. Si selecciona un tamaño de clave diferente, **DEBE utilizar tamaños de clave de más de 2048 bits**. Se permiten todos los tamaños de clave admitidos para ECDSA.

173. La parte de la clave privada DEBE almacenarse en *~/.ssh/* y debe quedar fuera del alcance de otros usuarios. Este archivo debe tratarse de forma similar a una contraseña. Se RECOMIENDA encarecidamente que se proteja esta clave con una contraseña codificada mediante *ssh-keygen*.

174. La siguiente línea de comandos es un ejemplo que genera una clave ECDSA:

    sh-keygen -t ecdsa -C "clave de John Doe"

175. El comando solicita una contraseña codificada donde DEBERÍA proporcionarse una contraseña codificada segura.

176. El bloqueo de la cuenta no impide que los usuarios puedan entrar en el sistema con la autenticación basada en clave SSH.

6.3.4 CAMBIO DE LAS PROPIEDADES DEL USUARIO

177. PUEDE utilizar el comando *usermod*(8) para cambiar las propiedades del usuario. Las propiedades a modificar se pueden ver en el propio manual del comando.

6.3.5 BLOQUEO Y DESBLOQUEO DE CUENTAS DE USUARIO

178. Se PUEDE bloquear (inhabilitar) a los usuarios mediante *passwd -l USUARIO* y volver a habilitarlos mediante *passwd -u USUARIO*. Tenga en cuenta que este bloqueo solo impide los intentos de autenticación basados en contraseña. La autenticación basada en clave SSH no se ve afectada por el uso de *passwd -l*. Para evitar inicios de sesión basados en clave SSH, se DEBE eliminar el archivo *.ssh/authorized_keys* ubicado en el directorio personal del usuario.

179. El módulo PAM *pam_tally2.so* aplica un bloqueo automático después de que se supere un número de intentos de autenticación fallidos. Utilice el programa *pam_tally2* para ver y restablecer el contador si es necesario, como se indica en la página man de *pam_tally2*(8).

180. Tenga en cuenta que el orden es muy importante a la hora de añadir configuraciones a los archivos de configuración pam */etc/pam.d/login* y */etc/pam.d/common-auth*. Como la importancia del orden no se describe en profundidad en *pam_tally2*(8), se proporciona un ejemplo a continuación en el que se denegará el acceso después de 4 intentos:

181. Archivo /etc/pam.d/login:

```
#%PAM-1.0
auth       required        pam_env.so
auth       required        pam_tally2.so   onerr=fail deny=4
auth       requisite       pam_nologin.so
auth       include         common-auth
account    include         common-account
password   include         common-password
session    required        pam_loginuid.so
session    optional        pam_keyinit.so  force revoke
session    include         common-session
#session   optional        pam_lastlog.so  nowtmp showfailed
session    optional        pam_mail.so standard
```

182. Archivo /etc/pam.d/common-auth:

```
auth     required        pam_env.so
auth     optional        pam_gnome_keyring.so
auth     required        pam_unix.so     try_first_pass
auth     required        pam_tally2.so   onerr=fail deny=4
```

183. Es importante que *pam_tally2.so* se indique como segunda entrada después de *pam_env.so* en */etc/pam.d/login*. Y también, *pam_tally2.so* debe indicarse en */etc/pam.d/common-auth* después de *pam_env.so*.

184. El mecanismo *pam_tally2* no impide los ataques de adivinación de contraseñas, solo impide el uso de la cuenta después de que se haya detectado un ataque de este tipo. Por lo tanto, DEBE asignar una nueva contraseña al usuario antes de reactivar una cuenta. Por ejemplo:

```
# muestra el valor
actual del contador
pam_tally2 --user jdoe
# establece una nueva contraseña y restablece el contador
pam_tally2 --user jdoe --reset
```

185. La utilidad *chage*(1) PUEDE utilizarse para ver y modificar la caducidad de las cuentas de usuario. Los usuarios sin privilegios pueden ver, pero no modificar, sus propios ajustes de caducidad.

6.3.6 ELIMINACIÓN DE USUARIOS

186. La utilidad *userdel*(8) elimina la cuenta de usuario del sistema, pero no elimina los archivos que están fuera del directorio personal (ni el archivo de cola de correo). Tampoco elimina los procesos que pertenecen a este usuario. Utilice kill (o rearranque el sistema) y find para hacerlo manualmente si es necesario, por ejemplo:

```
# ¿Qué usuario se debe suprimir?
U=jdoe

# Bloquea la cuenta de usuario, pero no la elimina todavía
passwd -l $U

# Elimina todos los procesos de usuario, repetir si es necesario (o rearrancar)
kill -9 `ps -la --User $ U --user $ U |awk '{print $ 4}'`

# Elimina de forma recurrente todos los archivos y directorios que
# pertenecen al usuario (usar con cuidado, porque puede eliminar los
# archivos que pertenecen a otros si están almacenados en un directorio.
# propiedad de este usuario)
# Utilice el tipo de sistema de archivos aplicable a su sistema.
find / -depth \( ! -fstype ext3 -prune -false \) \
-o -user $U -exec rm -rf {} \;

# Elimina las tareas de cron y at
crontab -u $U -r
find /var/spool/atjobs -user $U -exec rm {} \;

# Ahora suprime la cuenta
userdel $U
```

187. Lo mismo ocurre cuando se elimina un grupo. El administrador DEBE asegurarse de que los archivos asociados con el grupo se reasignan a otros grupos o se suprimen. El administrador también DEBE gestionar los procesos que se están ejecutando actualmente con el grupo suprimido.

188. Además, el administrador debe tener en cuenta que el ID de usuario puede estar en uso en las ACL en las que se debe comprobar la validez de estas ACL.

189. Si necesita crear grupos adicionales o modificar grupos existentes, utilice los comandos *groupadd*(8), *groupmod*(8) y *groupdel*(8).

190. En la configuración evaluada NO se admiten contraseñas de grupo. Se han inhabilitado eliminando el bit de SUID del programa *newgrp*(8). NO DEBE volver a habilitar esta función y NO DEBE utilizar *passwd*(1) con el indicador -g ni con el comando *gpasswd*(1) para definir contraseñas de grupo.

6.3.7 DEFINICIÓN DE CUENTAS ADMINISTRATIVAS

191. Los usuarios administrativos DEBEN ser miembros del grupo *trusted*. Especifique la opción *-G trusted* para el comando *useradd*(8) al crear usuarios administrativos.

192. También PUEDE utilizar el comando *usermod*(8) para cambiar la pertenencia a grupos. Por ejemplo, si desea añadir el usuario "*jdoe*" al grupo *trusted*, puede utilizar lo siguiente:

```
# Muestra los grupos de los que es miembro el usuario:
groups jdoe

# Añade el grupo adicional
usermod -G $(groups jdoe | sed 's/.*: //; s/ /,/g'),trusted jdoe
```

6.4 CONFIGURACIÓN DE LA DIRECTIVA DE CONTRASEÑAS

193. Para configurar la longitud mínima de la contraseña, el número mínimo de caracteres especiales y numéricos, así como el número mínimo de caracteres en mayúsculas y minúsculas en las contraseñas, se puede añadir o actualizar la línea siguiente en */etc/pam.d/common-password* mediante *pam_cracklib*(8):

```
password requisite pam_cracklib.so minlen=X dcredit=X ocredit=X ucredit=X lcredit=X
```

- *minlen* es el tamaño mínimo aceptable de la nueva contraseña
- *dcredit* con N < 0 es el número mínimo de dígitos que deben tener las contraseñas nuevas
- *ocredit* con N < 0 es el número mínimo de otros caracteres que deben tener las contraseñas nuevas
- *ucredit* con N < 0 es el número mínimo de letras mayúsculas que deben tener las contraseñas nuevas
- *lcredit* con N < 0 es el número mínimo de letras minúsculas que deben tener las contraseñas nuevas

6.5 GESTIÓN DE OBJETOS DE DATOS

6.5.1 REVOCACIÓN DEL ACCESO

194. Como ocurre con la mayoría de los sistemas operativos, los derechos de acceso solo se comprueban una vez: cuando el proceso accede por primera vez al objeto. Si la

comprobación de permisos inicial se ha realizado correctamente, las operaciones de lectura y escritura se permiten de forma indefinida sin más comprobaciones, incluso si los derechos de acceso al objeto se cambian o se revocan.

195. Si esta revocación diferida no es aceptable en su caso y necesita asegurarse de que ningún proceso de usuario acceda a un objeto después de haber cambiado los derechos de acceso a ese objeto, DEBE rearrancar el sistema. Esto garantiza que ningún proceso tenga descriptores abiertos que permitan un acceso continuo.

6.5.2 MEMORIA COMPARTIDA *SYSV* Y OBJETOS *IPC*

196. El sistema admite el uso de memoria compartida compatible con *SYSV*, objetos *IPC* y colas de mensajes. Si los programas no pueden liberar los recursos que han utilizado (por ejemplo, debido a un fallo), el administrador PUEDE utilizar la utilidad *ipcs*(8) para mostrar información sobre esos recursos, e *ipcrm*(8) para forzar la supresión de objetos innecesarios. Estos recursos también se liberan cuando se rearranca el sistema.

197. Para obtener información adicional, consulte la página *man* de *ipc*(2).

6.5.3 COLAS DE MENSAJES POSIX

198. Las colas de mensajes *POSIX* se admiten como alternativa a las colas de mensajes *SYSV*. Los usuarios y administradores PUEDEN utilizar las llamadas al sistema y las funciones de biblioteca correspondientes descritas en la página *man* de *mq_overview*(7), como *mq_open*(2) y *mq_unlink*(2).

199. El sistema de archivos de cola de mensajes (tipo *mqueue*) PUEDE estar montado en caso de que se solicite el acceso basado en el sistema de archivos a las colas de mensajes POSIX.

6.5.4 CONFIGURACIÓN DE DERECHOS DE ACCESO A OBJETOS

200. Los administradores PUEDEN utilizar las herramientas *chown*(1), *chgrp*(1) y *chmod*(1) para configurar los derechos de acceso de DAC. NO DEBE otorgar acceso adicional a los objetos que forman parte de la configuración evaluada.

201. Consulte las páginas *man* correspondientes para obtener más información acerca de estas herramientas.

6.6 PROGRAMACIÓN DE PROCESOS MEDIANTE CRON

202. *cron*(8) planifica la ejecución de programas a intervalos regulares. Las entradas se pueden modificar mediante el programa

203. *crontab*(1): el formato de archivo se documenta en la página *man* de *crontab*(5).

204. DEBE seguir las reglas especificadas para la instalación de programas adicionales para todas las entradas que ejecutará el usuario *root*. Utilice entradas *crontab* que no sean de usuario *root* en todos los casos en los que los privilegios de *root* no sean absolutamente necesarios.

205. Los errores en las tareas no interactivas ejecutadas por *cron* se notifican en los archivos de registro del sistema en */var/log/* y, además, por correo electrónico al usuario que las haya programado.

206. El permiso para que los usuarios puedan programar tareas con *cron* se controla mediante los siguientes archivos *allow* y *deny*:

    /etc/cron.allow
    /etc/cron.deny

207. El archivo *allow*, si existe, tiene prioridad. Solo pueden utilizar el servicio los usuarios cuyos nombres de usuario aparecen en ese archivo. Si no existe, se utiliza el archivo *deny* en su lugar, y todos los usuarios que *no* aparecen en ese archivo pueden utilizar el servicio. El contenido de estos archivos solo es relevante cuando se ejecutan los comandos de programación; los cambios no tienen efecto en los comandos ya programados.

208. En la distribución de SLES, no existen archivos *allow*, y los archivos *deny* se utilizan para impedir que los ID internos del sistema o los usuarios invitados utilicen estos servicios. Por defecto, la configuración evaluada permite que todos los usuarios que no pertenezcan al sistema utilicen *cron* y *at*.

209. Se RECOMIENDA restringir el uso de *cron* a usuarios humanos y no permitir que las cuentas del sistema utilicen estos mecanismos. Por ejemplo, los siguientes comandos añaden todas las cuentas del sistema que no sean de usuarios *root* a los archivos *deny*:

    awk -F: '{if ($3>0 && $3<1000) print $1}' /etc/passwd >/etc/cron.deny chmod 600 /etc/cron.deny

210. Los administradores PUEDEN programar tareas que se ejecutarán con los privilegios de un usuario especificado editando el archivo */etc/crontab* con un nombre de usuario adecuado en el sexto campo. Las entradas de */etc/crontab* no se restringen por el contenido de los archivos *allow* y *deny*.

211. PUEDE crear */etc/cron.allow* para mostrar explícitamente a los usuarios que tienen permiso para utilizar estos servicios. Si crea estos archivos, DEBEN ser propiedad del usuario *root* y tener permisos de archivo 0600 (sin acceso para grupos u otros).

212. El ID de inicio de sesión no se conserva en el siguiente caso especial:
    - El usuario A inicia sesión en el sistema.
    - El usuario A utiliza "su" para cambiar al usuario B.
    - El usuario B ahora edita la cola cron o at para añadir nuevas tareas. Esta operación se audita adecuadamente con el ID de inicio de sesión adecuado.
    - Ahora, cuando se ejecutan las nuevas tareas como usuario B, el sistema no proporciona la información de auditoría de que las tareas las ha creado el usuario A.

6.7 MONTAJE DE SISTEMAS DE ARCHIVOS

213. Si es necesario montar algún sistema de archivos además de los que se configuran durante la instalación, se DEBEN usar las opciones adecuadas para garantizar que no se introducen funciones que puedan infringir la directiva de seguridad.

214. Estos sistemas de archivos con propósitos especiales forman parte de la configuración evaluada: *proc*, *sysfs*, *devpts*, *securityfs*, *cgroups*, *binfmt_misc*, *devtmpfs*, *mqueue* y *tmpfs*. Estos son sistemas de archivos virtuales sin almacenamiento físico subyacente y representan estructuras de datos de la memoria del kernel. El acceso al contenido de

estos sistemas de archivos especiales está protegido por la directiva de control de acceso discrecional normal y por comprobaciones de permisos adicionales.

215. Por lo general, NO se admite el cambio de la propiedad o de los permisos de los archivos y directorios virtuales para los sistemas de archivos *proc* y *sysfs* (correspondientes a los directorios */proc/* y */sys/*). Cualquier intento de hacerlo se ignorará y se producirá un mensaje de error.

216. Es posible integrar un nuevo sistema de archivos como parte de la configuración evaluada, por ejemplo, mediante la instalación de un disco duro adicional, con las siguientes condiciones:

    - El dispositivo debe estar protegido contra robo o manipulación de la misma manera que el propio servidor; por ejemplo, debe estar instalado dentro del servidor.
    - Se deben crear uno o varios sistemas de archivos nuevos y vacíos con los formatos de sistema de archivos indicados en la sección 5.1.1 "PROCESO DE INSTALACIÓN".
    - Los sistemas de archivos EXT3, EXT4. BtrfFS o XFS se deben montar mediante la opción acl; por ejemplo, con el siguiente ajuste en el archivo */etc/fstab*:

      /dev/sdc1 /home2 ext3 acl 1 2

217. Los archivos y directorios existentes PUEDEN trasladarse a los nuevos sistemas de archivos.

    - Si un dispositivo que contiene un sistema de archivos se elimina alguna vez del sistema, el dispositivo DEBE almacenarse dentro de las instalaciones del servidor seguro o, alternativamente, DEBE destruirse de forma que los datos que contiene se borren de forma fiable.

218. Como alternativa, se PUEDE acceder a medios si no se integran en la configuración evaluada; por ejemplo, a unidades de memoria USB.

219. Para acceder a dispositivos USB, se DEBE utilizar el tipo de sistema de archivos iso9660.

220. DEBEN utilizarse las siguientes opciones de montaje si los sistemas de archivos contienen datos que no forman parte de la configuración evaluada:

      nodev,nosuid

    - Modificación por parte de usuarios no autorizados: tenga en cuenta que los datos importados pueden haberse creado con nombres de usuario y permisos que no coincidan con las directivas de seguridad del sistema.

221. NO DEBE escribir datos en sistemas de archivos extraíbles, como disquetes, ya que los mecanismos de control de acceso del sistema no pueden protegerlos adecuadamente después de que se extraigan del sistema. Consulte la sección 6.1.2 INSTALACIÓN DE SOFTWARE ADICIONAL.

222. Cada nuevo sistema de archivos DEBE montarse en un directorio vacío que no se utilice para ningún otro propósito. Se RECOMIENDA utilizar los subdirectorios de */mnt* para montar discos temporales y medios de almacenamiento extraíbles. Por ejemplo:

      # mount /dev/cdrom /media/cdrom -t iso9660 -o ro,nodev,nosuid,noexec

223. También PUEDE añadir una configuración equivalente a */etc/fstab*, por ejemplo:

    /dev/cdrom /media/cdrom iso9660 ro,noauto,nodev,nosuid,noexec 0 0

224. NO DEBE incluir el indicador *user*, ya que los usuarios normales no pueden montar sistemas de archivos. Esto también se aplica cuando se suprime el bit *SUID* en el comando *mount*.

6.8 CIFRADO DE PARTICIONES

225. SLES proporciona el mecanismo *dm-crypt* para configurar particiones en las que todos los datos que se almacenen en ellas se cifren sobre la marcha. Cuando se leen datos de esas particiones, esos datos se descifran sin intervención de ningún usuario.

226. Dado que el dispositivo de bloques de la partición está sujeto a la operación de cifrado, no existe ninguna restricción sobre qué sistema de archivos se utilizará junto con el dispositivo de bloques cifrado. Si ha seleccionado el cifrado de disco completo o ha configurado el cifrado para distintas particiones durante la instalación inicial, tal y como se describe en la sección 5.1.1 "PROCESO DE INSTALACIÓN", ya habrá almacenado los datos en discos duros protegidos por *dm-crypt*.

227. PUEDE configurar discos duros o particiones recién añadidos o que aún no se han utilizado mediante *dm-crypt* antes de crear un sistema de archivos en ellos. Para configurar una partición protegida por *dm-crypt* se utiliza la aplicación *cryptsetup*. Consulte la página *man* de *cryptsetup*(8) para descubrir cómo se usa *dm-crypt*.

228. Si la aplicación *cryptsetup* no está disponible en el sistema, debe instalarse mediante el comando *zypper*:

    zypper en cryptsetup-2.4.3-150400.1.110

229. Si se usa *cryptsetup* manualmente, DEBE usar la extensión LUKS y, por lo tanto, los comandos LUKS especificados en *cryptsetup*(8). La clave criptográfica que cifra todos los datos está protegida con una contraseña codificada proporcionada en el momento de la creación. La contraseña codificada debe ser lo suficientemente segura para proteger la clave de cifrado.

230. Para configurar una partición protegida por *dm-crypt* se utiliza el comando *luksFormat* en la aplicación *cryptsetup*.

231. Si no desea utilizar el cifrado por defecto con *luksFormat* (consulte *cryptsetup --help*), DEBE asegurarse de que se cumplen los siguientes requisitos al especificar el cifrado:

    - AES en modo CBC con 256 bits
    - AES en modo XTS con 512 bits

232. Después del formateo, se debe utilizar el comando *luksOpen* para configurar el mecanismo de cifrado; es decir, para informar al kernel de que cualquier operación de lectura y escritura se cifrará y descifrará sobre la marcha. El archivo de dispositivo creado con el comando *luksOpen* se puede usar ahora para crear un sistema de archivos que también se puede montar.

233. Para que el funcionamiento sea normal, el comando *luksOpen* debe ir seguido de un comando *mount* con el archivo de dispositivo creado por *luksOpen*.

6.9 BORRADO SEGURO

234. Para borrar el material clave de los archivos, como los certificados o claves de TLS y los pares de claves SSH, DEBE suprimirse el archivo que contiene ese material clave y, por lo tanto, **DEBE utilizarse el comando *shred***. Pero tenga en cuenta que *shred* no es eficaz en todos los sistemas de archivos. Encontrará más información en la página *man* de *shred*(1). Es más**, para las unidades SSD se DEBE invocar el comando */usr/sbin/fstrim* después de que se haya suprimido el archivo de claves con el material clave, a fin de informar a la unidad SSD subyacente de que debe descartar los bloques suprimidos**. Un ejemplo es el uso del comando

    fstrim -a

235. para recortar todos los dispositivos de bloques, incluido el dispositivo de bloques que solía contener los datos confidenciales. Para obtener más información, consulte la página *man* de *fstrim*(8).

236. Además, el disco DEBE sobrescribirse varias veces con números aleatorios antes de desecharse. También se RECOMIENDA utilizar particiones cifradas (consulte 6.8 "CIFRADO DE PARTICIONES"), así como destruir físicamente el disco al desecharlo.

6.10 CONFIGURACIÓN DE LA RED

237. Para configurar las interfaces de red, modifique los archivos *config* o utilice la herramienta *wicked*. para obtener información detallada acerca de *wicked* y sobre la configuración manual para habilitar o inhabilitar interfaces de red y configurar interfaces wifi, consulte la sección 23.5, "configuración manual de una conexión de red", en la guía de administración de suse linux enterprise server 15 sp4, disponible en https://documentation.suse.com/sles/15-sp4/.

6.11 USO DE TERMINALES EN SERIE

238. PUEDE conectar terminales en serie al sistema para que los utilicen los administradores del sistema.

239. Los terminales en serie se activan automáticamente mediante *systemd* cuando se utiliza la opción de línea de comandos del kernel *console* para habilitar una consola en serie. Por ejemplo:

    console=ttyS0,115200n8

6.12 REENVÍO DE AGENTES SSH

240. El uso del reenvío del agente ssh en el sistema no está permitido y, por lo tanto, DEBE inhabilitarse. El archivo */etc/ssh/ssh_config* DEBE modificarse de la siguiente manera:

    *Host **
        ForwardAgent no

6.13 BACKUP

241. Siempre que realice cambios en archivos críticos para la seguridad, PUEDE ser necesario realizar un seguimiento de los cambios realizados y revertir a versiones anteriores, pero no es obligatorio para cumplir con la configuración evaluada.

242. Se RECOMIENDA utilizar el archivador *tar*(1) para realizar copias de seguridad de todo el contenido del directorio. Consulte la sección 7.3.6 "IMPORTACIÓN/EXPORTACIÓN DE DATOS" en esta guía. Se RECOMIENDA realizar copias de seguridad periódicas de los siguientes archivos y directorios (en medios extraíbles, como una memoria USB o en un host independiente):

    /etc/
    /var/spool/cron/

243. DEBE utilizar la opción *--acl* para *tar* si desea guardar o restaurar las ACL.

244. Dependiendo de los requisitos de auditoría de su sitio, incluya también el contenido de */var/log/* en el plan de copia de seguridad. En ese caso, la rotación automática diaria de archivos de registro debe inhabilitarse o sincronizarse con el mecanismo de copia de seguridad. Consulte las secciones 7.1.2 "REGISTRO Y CONTABILIDAD DEL SISTEMA" y 6.19 "CONFIGURACIÓN DEL SUBSISTEMA DE AUDITORÍA" de esta guía para obtener más información.

245. DEBE proteger los medios de copia de seguridad contra al acceso no autorizado, ya que los datos copiados no cuentan con los mecanismos de control de acceso del sistema de archivos original. Entre otros datos críticos, contienen las claves secretas utilizadas por los servidores *SSH* y *charon*, así como la base de datos de contraseñas */etc/shadow*. Almacene los medios de copia de seguridad al menos con la misma seguridad que el propio servidor.

6.14 SINCRONIZACIÓN

6.14.1 CONFIGURACIÓN DE LA FECHA Y LA HORA DEL SISTEMA

246. **DEBE verificar periódicamente que el reloj del sistema sea lo suficientemente preciso**; de lo contrario, los archivos de registro y de auditoría contendrán información engañosa. Al iniciar el sistema, la fecha y la hora se copian del reloj de *hardware* del equipo al reloj de *software* del kernel. Cuando se apaga el sistema, se vuelven a escribir en el reloj de *hardware*.

247. Todas las fechas y horas internas utilizadas por el kernel, como las marcas de modificación de archivos, utilizan la hora universal (UTC) y no dependen de los ajustes de la zona horaria actual. Las utilidades de espacio de usuario normalmente ajustan estos valores a la zona horaria activa para mostrarlos. Los archivos de registro de texto contendrán representaciones ASCII de la fecha y la hora en la hora local, a menudo sin especificar explícitamente la zona horaria.

248. El comando *date*(1) muestra la fecha y hora actuales. Los administradores pueden utilizarlo para ajustar el reloj del *software* con el argumento *mmddHHMMaaaa* para especificar el mes, el día, la hora, el minuto y el año numéricos, respectivamente. Por

ejemplo, el siguiente comando establece el reloj en el 1 de mayo de 2004 a la 13:00 en la zona horaria local:

date 050113002004

249. El comando *hwclock*(8) puede consultar y modificar el reloj de *hardware* en las plataformas compatibles, pero no está disponible en entornos virtuales como *z/VM* o *LPAR*. Su uso habitual es copiar el valor actual del reloj del software en el reloj del *hardware*. El reloj de *hardware* PUEDE ejecutarse en la hora local o en la hora universal, como indica el ajuste *UTC* del archivo */etc/sysconfig/clock*. El siguiente comando ajusta el reloj de *hardware* a la hora actual UTC:

hwclock -u -w

250. Utilice el comando *tzselect*(8) para cambiar la zona horaria por defecto para todo el sistema. Los usuarios PUEDEN configurar individualmente una zona horaria diferente estableciendo la variable de entorno *TZ* como deseen en su perfil de *shell*, por ejemplo en el archivo *$HOME/.bashrc*.

6.14.2 CONFIGURACIÓN DE LA SINCRONIZACIÓN HORARIA CON NTP

251. Para configurar los servidores horarios, *chrony*(1) lee su configuración de */etc/chrony.conf*. Por lo tanto, es necesario actualizar */etc/chrony.conf*. Para ello, nombres de servidores específicos o direcciones IP como

0.suse.pool.ntp.org
1.suse.pool.ntp.org

252. o un nombre de repositorio como

pool pool.ntp.org

253. pueden especificarse. El nombre del repositorio se resuelve en varias direcciones IP. Consulte *chrony.conf*(5) para obtener más información.

254. Posteriormente, es necesario ejecutar *chrony* mediante

systemctl start chronyd.service

255. Puede llevar algún tiempo que la hora del sistema sea estable. Para iniciar *chrony* en el momento del arranque, se debe usar

systemctl enable chronyd.service

256. Dado que solo se puede ejecutar una instancia de *chronyd* a la vez, no debe habilitar ni iniciar *yast-timesync.service*.

257. Recuerde también que *chronyc*(1) se puede usar para ver informes de estado sobre el funcionamiento de *chronyd*. Para obtener más información, consulte la página man de *chronyc*(1).

6.15 CONFIGURACIÓN DEL CORTAFUEGOS

258. PUEDE habilitar, reconfigurar o inhabilitar el cortafuegos de red integrado según sea necesario. SLES permite los siguientes tipos de configuración de cortafuegos para controlar el tráfico:

    - El filtrado de paquetes de los protocolos IP, TCP, UDP e ICMP se implementa con *firewalld*, que se puede utilizar con la utilidad de línea de comandos *firewall-cmd* o la interfaz gráfica de usuario *firewall-config*. *firewalld* se usa para configurar reglas de filtro de paquetes muy pequeñas y ajustadas, así como reglas de filtrado complejas y sofisticadas, según las necesidades del administrador. Consulte la sección 23.4 de "*SUSE Linux Enterprise Security and Hardening Guide*" (Guía de seguridad y protección de SUSE Linux Enterprise), así como *firewall-cmd*(1) para obtener más datos sobre el uso de la aplicación.
    - SLES permite la configuración de máquinas virtuales mediante la función KVM y conecta el *software* invitado con redes externas mediante la función de puente del kernel de Linux. Dado que la función de puente se aplica en la capa *Ethernet*, el kernel de Linux no activa su pila TCP/IP para los paquetes que viajan a través del puente y que reciben algún *software* invitado de KVM o sistemas remotos. SLES proporciona un mecanismo de filtro de paquetes para filtrar paquetes en la capa *Ethernet* mediante la función *ebtables*. La página *man* de *ebtables*(8) describe el concepto, así como el uso del filtro de paquetes.

6.15.1 AUDITORÍA DE FIREWALLD DE OPERACIONES DE FILTRO DE PAQUETES

259. *firewalld* contiene la declaración *set-log-denied*, que está documentada en *firewall-cmd*(1).

260. Esto permite el registro de los paquetes denegados. Cuando se define esta opción, el kernel de Linux generará una entrada de auditoría para cada paquete denegado (rechazado o descartado).

261. Consulte *firewall-cmd*(1) para obtener más información.

6.16 CONFIGURACIÓN DEL PROTECTOR DE PANTALLA

262. La aplicación *screen* se utiliza para proporcionar un mecanismo de bloqueo del terminal actual para cada usuario. En la configuración por defecto, *screen* no está habilitada. **PUEDE habilitar screen ejecutando el guion**:

    /usr/share/doc/packages/certification-sles-eal4/ screen-script-screensaver

263. Este guión modifica */etc/profile* para permitir que *screen* se inicie en el momento del inicio de sesión. La siguiente descripción solo se aplica cuando se ha ejecutado el guion mencionado. Independientemente de si habilita *screen* con el guion mencionado, el *buffer* de retroceso del terminal se inhabilita mediante una línea de comandos del kernel. Se habla sobre esta línea de comandos en los párrafos siguientes.

264. El bloqueo de pantalla se invoca por los siguientes medios:

    - El bloqueo se ejecuta automáticamente después de un período de inactividad en el terminal definido por un tiempo límite en */etc/screenrc* o en *~/.screenrc* mediante el

valor de configuración *idle X lockscreen*, donde X es un número entero que indica el tiempo de inactividad en segundos antes de que se bloquee la pantalla.

- Todos los usuarios pueden bloquear su pantalla ejecutando la combinación de teclas de pantalla "*C+a C+x*".

265. PUEDE cambiar el valor de tiempo límite para bloquear la sesión en */etc/screenrc* con el valor de *lockscreen*.

266. Los usuarios pueden modificar el tiempo límite proporcionando su propio archivo *~/.screenrc*. Puede inhabilitar la compatibilidad con los archivos de configuración de los usuarios invocando *screen* con la opción *-c/dev/null*.

267. **ADVERTENCIA:** si un usuario accede al sistema de forma remota y la función del protector de pantalla se activa, el TOE se asegura de que la sesión se bloquee. Sin embargo, es posible que el terminal remoto implemente un *buffer* de retroceso que no esté bajo control del TOE. Por lo tanto, es posible que el terminal remoto tenga la sesión bloqueada, pero que un usuario pueda desplazarse hacia atrás y mostrar el historial de acciones. Si el usuario no debe tener permiso para utilizar el buffer de retroceso del terminal remoto, dicho terminal debe configurarse en consecuencia, ya que este buffer no está bajo el control del TOE. El buffer de retroceso local se inhabilita con esta entrada de la línea de comandos del kernel:

    no-scroll fbcon=scrollback:0

268. Para invocar *screen* automáticamente al iniciar la sesión, PUEDE introducir las siguientes líneas en */etc/bash_profile* para que se aplique en todo el sistema o en *~/.bash_profile* para que se aplique por usuario. Tenga en cuenta que un usuario puede cambiar *~/.bash_profile.*

    exec screen

6.17 CONFIGURACIÓN DE LAS ACTUALIZACIONES

269. COMO REQUISITO PREVIO PARA RECIBIR ACTUALIZACIONES CONTINUAS, DEBE REGISTRAR EL SISTEMA EN EL CENTRO DE SERVICIOS AL CLIENTE DE SUSE (SCC) COMO SE DESCRIBE EN LA SECCIÓN 5.1.1 "PROCESO DE INSTALACIÓN".

270. Para instalar las actualizaciones, se utiliza YaST. Está en línea con la configuración evaluada.

6.17.1 ACTUALIZACIÓN MANUAL

271. Para abrir el recuadro de diálogo de actualización en línea, inicie YaST y seleccione Software › Actualización en línea o, alternativamente, inícielo desde la línea de comandos con *yast2 online_update*.

272. La aplicación mostrará ahora los parches disponibles ordenados por relevancia de seguridad: seguridad, recomendado y opcional. Ahora puede seleccionar una entrada en la sección Resumen para ver una breve descripción del parche en la esquina inferior izquierda del recuadro de diálogo. La sección superior derecha muestra los paquetes incluidos en el parche seleccionado.

273. Por defecto, todos los parches nuevos (excepto los opcionales) que están actualmente disponibles para el sistema ya están marcados para su instalación. Se aplicarán automáticamente cuando se haga clic en Aceptar o Aplicar. Si uno o varios parches requieren que se reinicie el sistema, esto se mostrará antes de que comience la instalación del parche. Una vez completada la instalación, haga clic en Finalizar para salir de la actualización en línea de YaST. Su sistema está ahora actualizado.

6.17.2 ACTUALIZACIÓN AUTOMÁTICA

274. Para abrir el recuadro de diálogo de actualización automática en línea, inicie YaST y seleccione Software › Actualización en línea > Configuración > Actualización en línea o, alternativamente, inícielo desde la línea de comandos con yast2 *online_update_configuration*.

275. Ahora, el intervalo de actualización se puede establecer en Diariamente, Semanalmente o Mensualmente.

276. A veces, los parches pueden requerir la atención del administrador. Antes de instalar estos parches, se informa al usuario de las consecuencias y se le pide que confirme la instalación del parche. Estos parches se denominan "parches interactivos". Cuando se instalan parches automáticamente, se presupone que ha aceptado la instalación de parches interactivos. Si prefiere revisar estos parches antes de instalarlos, seleccione Omitir parches interactivos. En tal caso, los parches interactivos se omitirán durante la aplicación automática de parches. Asegúrese de ejecutar periódicamente una actualización manual en línea para comprobar si hay parches interactivos a la espera de ser instalados.

277. Para aceptar automáticamente cualquier acuerdo de licencia, active Aceptar con licencias. Active Incluir paquetes recomendados para instalar automáticamente todos los paquetes recomendados por los paquetes actualizados. Para inhabilitar el uso de RPM delta (por motivos de rendimiento), desmarque Usar RPM delta.

278. Para filtrar los parches por categoría (por ejemplo, seguridad o recomendado), seleccione Filtrar por categoría y añada las categorías de parches adecuadas de la lista. Solo se instalarán los parches de las categorías seleccionadas. Es recomendable habilitar solo las actualizaciones de seguridad automáticas y revisar manualmente todas las demás. La aplicación de parches suele ser fiable, pero es posible que desee probar los parches que no son de seguridad y revertirlos si encuentra algún problema.

279. Como último paso, confirme la configuración haciendo clic en Aceptar.

280. Nota: la actualización automática en línea no reinicia automáticamente el sistema. Si hay actualizaciones de paquetes que requieren un reinicio del sistema, este debe realizarse manualmente.

281. Nota: para inhabilitar las actualizaciones automáticas, desmarque Actualización automática en línea y haga clic en Aceptar para confirmar.

6.18 COMPATIBILIDAD CON CIFRADO

6.18.1 OPENSSL EN ARQUITECTURA X86

282. Por defecto, OpenSSL utiliza el conjunto de instrucciones AES-NI si la CPU x86 subyacente lo proporciona. Si el administrador desea volver a la implementación de software de AES, en lugar de usar AES-NI, a medida que revisa la implementación de software, se DEBE definir la siguiente variable de entorno para las aplicaciones que utilizan OpenSSL:

    OPENSSL_ia32cap="~0x200000200000000"

283. Tenga en cuenta que en la configuración evaluada, AES- NI DEBE estar desactivado. Por lo tanto, para cumplir con el resultado de la evaluación, DEBE aplicar la variable de entorno para OpenSSH y la aplicación openssl.

284. Esta variable de entorno garantiza que tanto AES-NI como la compatibilidad con PCLMULQDQ en la CPU x86 subyacente estén inhabilitadas.

6.18.2 OPENSSL EN LA ARQUITECTURA DE IBM POWER SYSTEM

285. Por defecto, OpenSSL utiliza el conjunto de instrucciones VMX si la CPU de IBM POWER System lo proporciona. Si el administrador desea volver a la implementación de software de AES, en lugar de usar VMX, a medida que revisa la implementación de software, se DEBE definir la siguiente variable de entorno para las aplicaciones que utilizan OpenSSL:

    OPENSSL_ppccap="0b01011"

286. Tenga en cuenta que en la configuración evaluada, VMX DEBE estar desactivado. Por lo tanto, para cumplir con el resultado de la evaluación, DEBE aplicar la variable de entorno para OpenSSH y la aplicación *openssl*.

6.18.3 OPENSSL EN ARQUITECTURA ARM

287. Por defecto, OpenSSL utiliza el conjunto de instrucciones CE si la CPU de ARM subyacente lo proporciona. Si el administrador desea volver a la implementación de software de AES, en lugar de usar CE, a medida que revisa la implementación de software, se DEBE definir la siguiente variable de entorno para las aplicaciones que utilizan OpenSSL:

    OPENSSL_armcap_P=1

288. Tenga en cuenta que en la configuración evaluada, CE DEBE estar desactivado. Por lo tanto, para cumplir con el resultado de la evaluación, DEBE aplicar la variable de entorno para OpenSSH y la aplicación *openssl*.

6.18.4 CONFIGURACIÓN DEL CLIENTE SSH

289. La configuración evaluada requiere que las claves generadas para las aplicaciones OpenSSH, incluido el *daemon sshd*, la aplicación cliente *ssh* y *ssh-keygen*, deben generarse mediante un generador de números aleatorios que se inicializa con al menos 256 bits de entropía.

290. OpenSSH utiliza el generador de números aleatorios determinista de OpenSSL para generar claves. Este generador se inicializa leyendo la propagación de la llamada al sistema *getrandom*.

291. Para la protección del cliente OpenSSH, DEBE añadir la siguiente opción al archivo */etc/ssh/ssh_config*:

    UseRoaming no

6.18.5 CONFIGURACIÓN DEL SERVIDOR SSH

292. La configuración evaluada requiere que el archivo */etc/ssh/sshd_config(5)* DEBA modificarse de la siguiente manera, independientemente de si el archivo de configuración contiene un comentario de que sea compatible con la configuración de CC:

    - La opción ssh-ed25519 DEBE eliminarse de HostbasedAcceptedKeyTypes.
    - La opción RekeyLimit DEBE definirse en 1G 1h.
    - Solo se permite habilitar PubkeyAuthentication y PasswordAuthentication.

6.18.6 GESTIÓN DE CLAVES CRIPTOGRÁFICAS

293. Los protocolos de red de cifrado de SSH y TLS proporcionan un canal seguro para proteger la integridad y confidencialidad de los datos. Durante el establecimiento del canal seguro, los protocolos utilizan certificados y claves privadas para admitir la autenticación mutua. Para que la seguridad sea de total confianza, también debe haber una autenticación adecuada para establecer la identidad y la autenticidad del par remoto. Para configurar SSH y TLS consulte la siguiente documentación:

    man 5 sshd_config

    man 7 crypto-policies

294. Por lo tanto, DEBE asegurarse de que la generación y el uso de los certificados, las listas de revocación de certificados (CRL) utilizadas para la validación de certificados y las claves públicas y privadas utilizadas para estos protocolos de red cumplen los estándares correspondientes y proporcionan suficiente seguridad mediante el uso de claves con la longitud adecuada y de algoritmos de resumen de mensajes.

295. También DEBE verificar la integridad y autenticidad de los certificados digitales y del material clave antes de importarlos al TOE, así como verificar que los certificados estén firmados mediante algoritmos hash seguros.

296. Las claves de cifrado almacenadas en la memoria volátil se borran completamente solo después de un ciclo de alimentación completo.

297. Los siguientes mecanismos de cifrado DEBEN utilizarse para SSH:

Algoritmos de cifrado

AES128-CBC, AES256-CBC, AES128-GCM@openssh.com y AES256-GCM@openssh.com

Algoritmos de clave pública

RSA-SHA2-256, RSA-SHA2-512, ECDSA-SHA2-NISTP384 o ECDSA-SHA2-NISTP521

Algoritmos de MAC

HMAC-SHA2-256, HMAC-SHA2-512, AES128-GCM@openssh.com, AES256-GCM@openssh.com

Intercambio de claves

Diffie-Hellman-group14-SHA256, Diffie-Hellman-group16-SHA512, Diffie-Hellman-group18-SHA512, ECDH-SHA2-NISTP256, ECDH-SHA2-NISTP384 o ECDH-SHA2-NISTP521

298. La compatibilidad con el cliente TLS se implementa en OpenSSL. La autenticación del certificado del servidor TLS se realiza mediante el nombre completo del *host* o la dirección IP. Se admiten otros comodines para la resolución del identificador del servidor. Sin embargo, no se admite la fijación de certificados. DEBEN utilizarse los siguientes paquetes de cifrado:

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

299. Las extensiones de grupos admitidos permitidas en el saludo de cliente para TLS son:

- secp256r1
- secp384r1
- secp521r1

300. Además, al configurar las configuraciones de cifrado de disco, la contraseña codificada protege la clave de volumen maestra utilizada para cifrar los datos que se almacenarán en el disco. Para garantizar que la protección de esa clave de volumen maestra sea adecuada, DEBE utilizar una contraseña codificada suficientemente segura. Para el cifrado de disco, DEBE utilizar los cifrados permitidos y los modos de encadenamiento de bloques permitidos, tal como se especifica en 6.8 "CIFRADO DE PARTICIONES".

6.18.7 GENERACIÓN Y ESTABLECIMIENTO DE CLAVES CRIPTOGRÁFICAS

301. Las claves criptográficas asimétricas DEBEN generarse utilizando uno de los siguientes algoritmos de generación de claves criptográficas:
    - RSA con tamaños de clave de 2048 bits, 3072 bits y 4096 bits
    - Cifrado de curva elíptica (ECC) con la curvas NIST P-256, NIST P-384 o NIST P-521
    - Cifrado de campo finito (FFC) con grupos Safe-Prime aprobados como se especifica en la publicación especial NIST 800-56A Revisión 3
302. El establecimiento de la clave criptográfica DEBE implementarse mediante uno de los siguientes métodos:
    - Cifrado de curva elíptica (ECC) con ECC CDH
    - Cifrado de campo finito (FFC) con FFC DH

6.19 CONFIGURACIÓN DEL SUBSISTEMA DE AUDITORÍA

303. El subsistema de auditoría implementa una solución de supervisión central para realizar un seguimiento de los eventos relevantes para la seguridad, como los cambios y los intentos de cambio de los archivos críticos para la seguridad.
304. Esto se consigue con dos mecanismos independientes. Todas las llamadas al sistema se interceptan y el kernel escribe los parámetros y el valor devuelto en el registro de auditoría para las llamadas que se marcan como relevantes para la seguridad en la configuración del filtro. Además, algunos programas de confianza contienen código específico de auditoría para escribir seguimientos de auditoría de las acciones que deben realizar.
305. Consulte las páginas man de *auditd*(8), *auditd.conf*(5) y *auditctl*(8) para obtener más información.
306. Para obtener más información sobre la auditoría remota, consulte *audisp-remote*(8) y *audisp-remote.conf*(5).

6.19.1 USO PREVISTO DEL SUBSISTEMA DE AUDITORÍA

307. El perfil de protección del sistema operativo (OSPP) especifica las capacidades de auditoría que debe admitir un sistema compatible. La configuración evaluada que se describe aquí se basa en estos requisitos.
308. **ADVERTENCIA:** algunos de los requisitos del perfil de protección pueden entrar en conflicto con los requisitos específicos del sistema. Por ejemplo, un sistema compatible con OSPP DEBE inhabilitar las entradas al sistema si el subsistema de auditoría no funciona. Asegúrese de que conoce las consecuencias si habilita la auditoría.
309. OSPP está diseñado para sistemas multiusuario, con varios usuarios únicos que mantienen recursos compartidos y privados. Las funciones de auditoría están diseñadas para admitir este modo de funcionamiento con un seguimiento confiable de las operaciones relevantes para la seguridad. Es menos útil para un servidor de aplicaciones puro sin usuarios interactivos.

310. Tenga en cuenta que el subsistema de auditoría, cuando se activa, ralentiza las aplicaciones del servidor. El impacto depende de lo que esté haciendo la aplicación y de cómo esté configurado el subsistema de auditoría. Como regla general, las aplicaciones que abren un gran número de archivos independientes son las más afectadas, y los programas asociados a la CPU no deberían verse afectados de forma apreciable. Deberá encontrar un equilibrio entre requisitos de rendimiento y sus necesidades de seguridad a la hora de decidir si desea utilizar la auditoría y cómo desea hacerlo.

6.19.2 SELECCIONAR LOS EVENTOS A AUDITAR

311. PUEDE realizar cambios en el conjunto de llamadas y eventos del sistema que se van a auditar. OSPP requiere que el sistema tenga la capacidad de auditar eventos relevantes para la seguridad, pero depende de usted elegir cómo desea utilizar esas capacidades. Es aceptable desactivar completamente la auditoría de llamadas al sistema incluso en una configuración evaluada, por ejemplo, en un servidor de aplicaciones puro sin usuarios interactivos en el sistema.

312. El paquete de auditoría proporciona varios archivos de configuración de auditoría sugeridos; por ejemplo, el archivo */usr/share/doc/packages/audit/capp.rules* para sistemas que cubren la funcionalidad básica del sistema. Contiene una configuración sugerida para un sistema multiusuario típico, todo el acceso a los archivos relevantes para la seguridad se audita, junto con otros eventos relevantes para la seguridad, como la reconfiguración del sistema. PUEDE copiar uno de los archivos de reglas de ejemplo en */etc/audit/audit.rules* y modificar la configuración según los requisitos locales, incluida la opción de utilizar un archivo de reglas de auditoría vacío para inhabilitar la auditoría si no es necesaria.

313. La página man de *auditctl*(8) proporciona una descripción de las reglas de auditoría.

6.19.3 LECTURA Y BÚSQUEDA DE REGISTROS DE AUDITORÍA

314. Utilice la herramienta *ausearch*(8) para recuperar información de los registros de auditoría. La información disponible para recuperar depende de la configuración del filtro activo. Si modifica la configuración del filtro, se RECOMIENDA que conserve una copia con marca de fecha de la configuración aplicable con los archivos de registro como referencia para el futuro.

315. Por ejemplo:

```
# busca eventos con un UID de entrada específico
ausearch -ul jdoe

# busca eventos por ID de proceso
ausearch -p 4690
```

316. Consulte la página *man* de *ausearch*(8) para obtener más información.

317. Para algunas llamadas al sistema en algunas plataformas, los argumentos de llamada al sistema del registro de auditoría pueden ser ligeramente diferentes de lo que se puede esperar del código fuente del programa debido a las modificaciones de los argumentos en la biblioteca C o en las funciones del contenedor del kernel. Por ejemplo, la función de biblioteca glibc *mq_open*(3) elimina el carácter "/" inicial del argumento de vía antes de

pasarlo a la llamada al sistema *mq_open*(2), lo que provoca una diferencia de un carácter en los datos del registro de auditoría. Del mismo modo, algunas llamadas al sistema como *semctl*(2), *getxattr*(2) y *mknodat*(2) pueden tener indicadores internos adicionales añadidos automáticamente al argumento indicador. Estas pequeñas modificaciones no cambian la información relevante de seguridad del registro de auditoría.

318. Por supuesto, puede utilizar otras herramientas como *grep*(1) o lenguajes de guiones como *awk*(1), *python*(1) o *perl*(1) para analizar más a fondo el archivo de registro de auditoría de texto o la salida generada por la herramienta de bajo nivel *ausearch*.

6.19.4 INICIAR Y DETENER EL SUBSISTEMA DE AUDITORÍA

319. Si el *daemon* de auditoría se interrumpe, no se guarda ningún evento de auditoría hasta que se reinicia. Para evitar la pérdida de registros de auditoría cuando se modifica la configuración del filtro, DEBE utilizar el comando **service auditd reload** para volver a cargar los filtros.

320. NO DEBE utilizar la señal *KILL* (-9) para detener el *daemon* de auditoría, ya que impediría que se apagara correctamente.

321. **Se RECOMIENDA que añada el parámetro del kernel *audit=1* al archivo de configuración del cargador de arranque** para garantizar que todos los procesos, incluidos los iniciados antes del servicio *auditd*, estén correctamente conectados al subsistema de auditoría. Consulte la documentación del cargador de arranque para obtener más información sobre cómo modificar la línea de comandos del kernel.

6.19.5 ALMACENAMIENTO DE REGISTROS DE AUDITORÍA

322. La configuración de auditoría por defecto almacena los registros de auditoría en el archivo */var/log/audit/audit.log*. Esto se configura en el archivo */etc/audit/auditd.conf*. PUEDE cambiar el archivo *auditd.conf* para adaptarlo a sus requisitos locales.

323. Se RECOMIENDA que configure los ajustes del daemon de auditoría de forma adecuada para sus requisitos locales; por ejemplo, cambiando la directiva de retención de archivos de registro para no suprimir nunca los registros de auditoría antiguos con el siguiente ajuste en el archivo */etc/audit/auditd.conf*:

    max_log_file_action = KEEP_LOGS

324. Los ajustes más importantes se refieren a situaciones en las que el sistema de auditoría corre el riesgo de perder información de auditoría; por ejemplo, debido a la falta de espacio en disco u otras condiciones de error. PUEDE elegir las acciones apropiadas para su entorno, como cambiar al modo de usuario único (acción *single*) o apagar el sistema (acción *halt*) para evitar acciones auditables si los registros de auditoría no se pueden almacenar.

325. **ADVERTENCIA:** el cambio al modo de usuario único no elimina automáticamente todos los procesos de usuario si se utiliza el procedimiento por defecto del sistema. PUEDE eliminar procesos de usuarios utilizando *killall -u*. Tenga en cuenta que los servicios del sistema NO DEBERÍAN interrumpirse.

326. Se RECOMIENDA detener el sistema, y es la forma más segura de garantizar que se detengan todos los procesos de usuario. Si se requiere un sistema de auditoría a prueba de fallos, se RECOMIENDA usar los siguientes ajustes en el archivo */etc/audit/auditd.conf*:

    admin_space_left_action = SINGLE
    disk_full_action = HALT
    disk_error_action = HALT

327. Se RECOMIENDA configurar los umbrales de espacio de disco y los métodos de notificación oportunos para poder recibir una advertencia anticipada si se está agotando el espacio para los registros de auditoría.

328. Se RECOMIENDA que utilice una partición dedicada para el directorio */var/log/audit/* para asegurarse de que *auditd* tenga control total sobre el uso del espacio en disco sin que otros procesos interfieran.

329. Consulte la página *man* de *auditd.conf*(5) para obtener más información sobre el almacenamiento y la gestión de los registros de auditoría.

6.19.6 FIABILIDAD DE LOS DATOS DE AUDITORÍA

330. PUEDE buscar el equilibrio adecuado entre la disponibilidad del sistema y el modo de fallo seguro en caso de que el sistema de auditoría funcione incorrectamente con sus requisitos locales.

331. PUEDE configurar el sistema para detener todos los procesos de inmediato en caso de que se produzcan errores críticos en el sistema de auditoría. Cuando se detecte un error de este tipo, el sistema entrará inmediatamente en modo "pánico" y deberá rearrancarse manualmente. Para utilizar este modo, añada la siguiente línea al archivo */etc/audit/audit.rules*:

    -f 2

332. Consulte la página *man* de *auditctl*(8) para obtener más información sobre los modos de gestión de fallos.

333. PUEDE editar el archivo */etc/libaudit.conf* para configurar la acción deseada para las aplicaciones que no pueden comunicarse con el sistema de auditoría. Consulte la página *man* de *get_auditfail_action*(3) para obtener más información.

334. *auditd* escribe registros de auditoría utilizando el almacenamiento en búfer normal del sistema de archivos de Linux, lo que significa que la información se puede perder en caso de fallo porque aún no se ha escrito en el disco físico. Las opciones de configuración controlan el modo en que *auditd* gestiona las escrituras en disco y permiten al administrador elegir un equilibrio adecuado entre rendimiento y fiabilidad.

335. Cualquier aplicación que lea los registros mientras el sistema se está ejecutando obtendrá siempre los datos más recientes del caché del *buffer*, incluso si aún no se han confirmado en el disco, por lo que los ajustes de *buffering* no afectan al funcionamiento normal.

336. El ajuste por defecto es *flush = DATA*, lo que garantiza que los datos de registro se escriban en el disco, pero los metadatos, como la hora del último archivo, pueden ser incoherentes.

337. El modo de rendimiento más alto es *flush = none*, pero tenga en cuenta que esto puede provocar la pérdida de registros de auditoría en caso de fallo del sistema.

338. Si desea asegurarse de que *auditd* fuerce siempre una escritura en disco para cada registro, PUEDE definir la opción ***flush = SYNC*** en */etc/audit/auditd.conf*, pero tenga en cuenta que esto dará como resultado una reducción significativa del rendimiento y una gran carga en el disco.

339. Un compromiso entre la confiabilidad y el rendimiento es garantizar la sincronización del disco después de escribir un número específico de registros a fin de proporcionar un límite superior para el número de registros perdidos en un bloqueo. Para ello, utilice una combinación de *flush = INCREMENTAL* y un valor numérico para el parámetro *freq*, por ejemplo:

    flush = INCREMENTAL
    freq = 100

340. Los archivos de registro de auditoría *no* están protegidos contra administradores malintencionados y no están diseñados para entornos en los que los administradores no sean de confianza.

7 FASE DE OPERACIÓN

7.1 MONITOREO, REGISTRO Y AUDITORÍA

7.1.1 REVISAR LA CONFIGURACIÓN DEL SISTEMA

341. Se RECOMIENDA que revise la configuración del sistema a intervalos regulares para verificar si aún coincide con la configuración evaluada. Esto afecta principalmente a los procesos que pueden ejecutarse con privilegios de usuario *root*.

342. Los permisos de los archivos de dispositivo */dev/** NO DEBEN modificarse.

343. En concreto, revise los ajustes de los siguientes archivos y directorios para asegurarse de que el contenido y los permisos no se han modificado:

*/etc/apparmor/**
*/etc/audit/**
/etc/cron.allow
*/etc/cron.d/**
/etc/cron.deny
*/etc/cron.daily/**
*/etc/cron.hourly/**
*/etc/cron.monthly/**
*/etc/cron.weekly/**
/etc/crontab
/etc/group
/etc/gshadow
/etc/hosts
*/etc/systemd/**
/etc/ld.so.conf
*/etc/libvirt/**
/etc/localtime
/etc/login.defs
/etc/modprobe.conf
*/etc/pam.d/**
/etc/passwd
/etc/securetty
/etc/security/opasswd
*/etc/security/**
/etc/shadow
/etc/ssh/ssh_config
/etc/ssh/sshd_config
*/etc/sysconfig/**
*/var/log/audit.d/**
/var/log/faillog
/var/log/lastlog
*/var/spool/cron/**

344. Utilice el comando *lastlog* para detectar patrones inusuales de inicios de sesión.

345. Verifique también la salida de los siguientes comandos (ejecutados como *root*) para analizar que no se muestra ninguna aplicación ni comando desconocidos, ya que eso podría indicar una brecha de seguridad del sistema:

```
# lista de comandos ejecutados como root por cron
crontab -l

# lista de archivos con el conjunto de bits de SUID/SGID
find / \( -perm -4000 -o -perm -2000 \) -ls

# lista de archivos, directorios o archivos de dispositivos de bloques de escritura universal
find / \( -type f -o -type d -o -type b \) -perm -0002 -ls

# lista de archivos en directorios del sistema que no son propiedad del root
find / bin / boot / etc / lib / sbin / usr \
! -type l \( !  -uid 0 -o -perm +022 \)
```

7.1.2 REGISTRO Y CONTABILIDAD DEL SISTEMA

346. Los mensajes de registro del sistema se almacenan en el árbol de directorio */var/log/* en formato de texto sin formato. La mayoría se registra a través de *syslogd*(8) y *klogd*(8), que PUEDEN configurarse mediante el archivo */etc/syslog.conf*.

347. La utilidad *logrotate*(8), lanzada desde */etc/cron.daily/logrotate*, inicia un nuevo archivo de registro cada semana o cuando alcanza un tamaño máximo y elimina o archiva automáticamente los archivos de registro antiguos. PUEDE cambiar los archivos de configuración */etc/logrotate.conf* y */etc/logrotate.d/** según sea necesario.

348. Además de los mensajes de syslog, otros programas generan distintos archivos de registro y de estado en */var/log*:

```
Archivo        Origen
-------------+------------------------------------------------------------
YaST2          Directorio para archivos de registro de YaST2
audit.d        Directorio para registros de LAF
boot.msg       Mensajes del inicio del sistema
lastlog        Último inicio de sesión correcto (consulte lastlog(8))
libvirt        Registro mantenido por libvirtd
localmessages  Escrito por syslog
mail           Escrito por syslog, contiene mensajes del MTA (postfix)
messages       Escrito por syslog, contiene mensajes de su y ssh
news/          noticias de syslog (no se utilizan en la configuración
               evaluada)
warn           Escrito por syslog
wtmp           Escrito por el subsistema PAM, consulte who(1)
```

349. Consulte las páginas *man* de *syslog*(3), *syslog.conf*(5) y *syslogd*(8) para obtener información detallada sobre la configuración de syslog.

350. El comando *ps*(1) se puede utilizar para supervisar los procesos en ejecución. El uso de *ps faux* mostrará todos los procesos e hilos en ejecución.

7.1.3 VARIABLES DE CONFIGURACIÓN DEL SISTEMA EN /ETC/SYSCONFIG

351. El sistema utiliza varios archivos en */etc/sysconfig* para configurar el sistema. La mayoría de los archivos de este árbol de directorios contienen definiciones de variables en forma de variables de *shell* que los guiones *rc* leen durante el arranque del sistema, o que el comando *SuSEconfig* evalúa o que se utiliza como entrada para volver a escribir otros archivos de configuración en el sistema.

352. En la configuración evaluada, no se permiten cambios que requieran ejecutar el comando *SuSEconfig* para volver a escribir otros archivos de configuración. PUEDE ejecutar *SuSEconfig*, pero no tendrá ningún efecto en la configuración evaluada.

7.2 DESARROLLADORES DE APLICACIONES

353. Cuando crean aplicaciones que se ejecutan en SLES, los desarrolladores pueden utilizar el compilador y enlazador *gcc* incluido. Cuando se invoca gcc, los desarrolladores deben seguir las prácticas recomendadas para el desarrollo seguro:

    - Incluir la habilitación de protecciones contra la rotura de la pila mediante los siguientes indicadores del compilador:

      -fstack-protector-strong --param=ssp-buffer-size=4

    - Incluir la habilitación de ASLR mediante los siguientes indicadores del compilador y enlazador:

      -fpie -Wl,-pie

7.3 PAUTAS DE SEGURIDAD PARA LOS USUARIOS

7.3.1 DOCUMENTACIÓN EN LÍNEA

354. El sistema proporciona una gran cantidad de documentación en línea, normalmente en formato de texto. Utilice el programa "man" para leer las entradas del manual en línea, por ejemplo:

    man ls
    man man

355. para leer información acerca de los comandos *ls* y *man*, respectivamente. Puede buscar palabras clave en el manual en línea con la utilidad *apropos*(1), por ejemplo:

    apropos contraseña

356. Cuando esta guía hace referencia a páginas de manual (páginas *man*), utiliza la sintaxis ENTRADA(SECCIÓN), por ejemplo *ls*(1). Normalmente no es necesario proporcionar el número de sección, pero si hay varias entradas en diferentes secciones, puede utilizar el conmutador -S opcional y seleccionar una específica.

357. Algunos programas proporcionan información adicional en formato GNU "*texinfo*". Utilice el programa *info* para leerla, por ejemplo:

info diff

358. En los directorios */usr/share/doc/*/* se puede encontrar información adicional, ordenada por paquetes de *software*. Utilice el paginador *less*(1) para leerla, por ejemplo:

less /usr/share/doc/packages/bash/FAQ

359. Muchos programas también admiten el comando *--help*, *-?* o *-h*, que puede utilizar para obtener un resumen de uso de los parámetros admitidos de la línea de comandos.

360. Esta Guía de configuración tiene prioridad sobre otros documentos en caso de que las recomendaciones se contradigan.

7.3.2 AUTENTICACIÓN

361. DEBE autenticarse (demostrar su identidad) antes de que se le permita utilizar el sistema. Cuando el administrador haya creado su cuenta de usuario, le habrá asignado un nombre de usuario y una contraseña por defecto, y le habrá proporcionado esa información junto con instrucciones para acceder al sistema.

362. Tenga en cuenta que, junto a la autenticación de contraseña, también se permite la autenticación basada en clave, como se describe en el apartado 7.3.4 "AUTENTICACIÓN BASADA EN CLAVES SSH". Sin embargo, estos son los dos únicos métodos de autenticación permitidos en la configuración evaluada y uno de ellos DEBE utilizarse.

363. Normalmente, la entrada al sistema se realiza mediante el protocolo Secure Shell (SSH), o bien puede haber disponible un terminal en serie. Utilice el comando *ssh* para conectarse al sistema a menos que el administrador indique lo contrario, por ejemplo:

ssh jdoe@172.16.0.1

364. La página *man* de *ssh*(1) proporciona más información sobre las opciones disponibles. Si necesita transferir archivos de un sistema a otro, utilice las herramientas *scp*(1) o *sftp*(1).

365. Si es la primera vez que se conecta al sistema de destino, se le preguntará si desea aceptar la clave de *host*. Si el administrador ha proporcionado una huella digital clave para comparar, verifique que coincidan; de lo contrario, escriba "sí" para continuar. **DEBE cambiar de inmediato la contraseña asignada inicialmente** con la utilidad *passwd*(1).

366. NO DEBE, bajo ninguna circunstancia, intentar entrar desde un dispositivo que no sea seguro, como un terminal público o un equipo que pertenezca a un amigo. Incluso si la *persona* propietaria del equipo es de confianza, es posible que el *equipo* haya sido infectado con código dañino. Recuerde siempre que el dispositivo en el que está escribiendo su contraseña tiene la capacidad de guardar y reutilizar su información de autenticación, por lo que está otorgando a ese equipo el derecho de realizar cualquier acción en su nombre. El manejo de la información de autenticación de una forma no segura es la causa principal de las vulnerabilidades de los sistemas que, de otro modo, serían seguros. SSH solo puede proteger la información durante el tránsito y no ofrece protección alguna contra un endpoint inseguro.

367. Cuando salga del sistema y deje el dispositivo que ha utilizado para acceder (como un terminal o una estación de trabajo con emulación de terminal), DEBE asegurarse de que no ha dejado información en la pantalla o en un buffer interno al que no debería poder

acceder otro usuario. Algunos terminales también almacenan información que no se muestra en el terminal (como contraseñas o el contenido de un buffer de retroceso). Sin embargo, esta información puede ser extraída por el siguiente usuario, a menos que se haya borrado el buffer del terminal. **Las opciones seguras incluyen apagar por completo el *software* cliente utilizado para acceder, apagar un terminal de *hardware* o borrar el *buffer* de retroceso pasado de un terminal virtual a otro, además de borrar el área de pantalla visible.**

368. Si olvida su contraseña, póngase en contacto con el administrador, que podrá asignarle una nueva.

369. PUEDE utilizar los programas *chsh*(1) y *chfn*(1) para actualizar la shell de entrada y la información personal si fuera necesario. No todos los ajustes se pueden cambiar de esta forma. Póngase en contacto con el administrador si necesita cambiar ajustes que requieran privilegios adicionales.

7.3.3 POLÍTICA DE CONTRASEÑAS

370. Todos los usuarios, incluidos los administradores, DEBEN asegurarse de que sus contraseñas de autenticación sean seguras (difíciles de adivinar) y de que se gestionen con las precauciones de seguridad adecuadas. La directiva de contraseñas descrita aquí está diseñada para cumplir los requisitos de la configuración evaluada. Si su organización ya tiene una directiva de contraseñas definida, el administrador PUEDE remitirlo a esa directiva si es equivalente en materia de seguridad.

371. **DEBE cambiar la contraseña inicial definida por el administrador cuando entre por primera vez al sistema.** DEBE seleccionar su propia contraseña de acuerdo con las reglas definidas aquí. También DEBE cambiar la contraseña si el administrador define una contraseña nueva; por ejemplo, si ha olvidado la contraseña y ha solicitado al administrador que la restablezca.

372. Utilice el programa *passwd*(1) para cambiar la contraseña. Primero, le pedirá la contraseña anterior para confirmar su identidad y, a continuación, la contraseña nueva. Se le pedirá que introduzca la contraseña nueva dos veces para comprobar que no se ha escrito erróneamente.

373. El programa *passwd*(1) realizará automáticamente algunas comprobaciones en la contraseña nueva para garantizar que no sea fácil de adivinar, pero DEBE seguir los requisitos de este capítulo.

374. Los administradores DEBEN asegurarse de que sus propias contraseñas cumplan con esta directiva de contraseñas, incluso en los casos en los que no se realice una comprobación automática, como cuando se instala el sistema por primera vez.

- La contraseña DEBE tener un mínimo de 8 caracteres. PUEDEN utilizarse más de 12 caracteres (se RECOMIENDA utilizar más de 12, lo mejor es utilizar contraseñas codificadas) y todos los caracteres son significativos.
- Combine diferentes clases de caracteres para crear una contraseña suficientemente segura con 12 caracteres que contengan al menos un carácter de cada clase. Las clases de caracteres se definen de la siguiente manera:

  Letras minúsculas: abcdefghijklmnopqrstuvwxyz
  Letras mayúsculas: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Dígitos: 0123456789
Puntuación:!"#$%&'()+,-./:;<=>?[\]^_'{|}~*
Para las contraseñas PUEDEN utilizarse caracteres ASCII que no sean de 7 bits.

- **NO DEBE basar la contraseña en una palabra del diccionario**, su nombre real, su nombre de usuario u otros datos personales (como fechas, nombres de parientes o mascotas), nombres de personas reales ni personajes ficticios.
- En lugar de una contraseña, PUEDE utilizar una contraseña codificada formada por varias palabras no relacionadas (al menos tres) unidas con caracteres de puntuación aleatorios. Dicha contraseña codificada DEBE tener una longitud de al menos 16 caracteres. Esto corresponde a contraseñas codificadas generadas automáticamente al elegir 3 palabras de un diccionario de 4096 palabras y añadir dos caracteres de puntuación de un conjunto de 8, lo que equivale a 42 bits de entropía.
- **NO DEBE utilizar una cadena alfabética simple**, palíndromos ni combinaciones de teclas adyacentes.
- Cuando elija una contraseña nueva, NO DEBE ser una simple variación o permutación de una contraseña utilizada anteriormente.
- **NO DEBE escribir la contraseña en papel ni almacenarla en dispositivos electrónicos sin protección.** El almacenamiento en una ubicación segura (como un sobre en una caja de seguridad o un almacenamiento cifrado en un dispositivo electrónico) PUEDE ser aceptable. Póngase en contacto primero con el administrador para asegurarse de que la protección es lo suficientemente sólida como para que la recuperación de contraseñas no sea viable para los tipos de atacantes contra los que el sistema está diseñado para proteger.
- La contraseña es exclusiva para usted. Una contraseña es como un cepillo de dientes: no quiere compartirla con nadie, ni siquiera con su mejor amigo. NO DEBE revelar su contraseña a nadie, ni permitir que nadie más utilice el sistema utilizando su identidad.
- Tenga en cuenta que los administradores nunca le pedirán su contraseña, ya que no la necesitan aunque tengan que modificar los ajustes que afectan a su cuenta de usuario.
- NO DEBE utilizar la misma contraseña para acceder a ningún sistema bajo administración externa, incluidos los sitios de Internet. No obstante, PUEDE utilizar la misma contraseña para las cuentas de varios equipos de una unidad administrativa, siempre que todos tengan un nivel de seguridad equivalente y estén bajo el control de los mismos administradores.
- DEBE informar al administrador y seleccionar una nueva contraseña si tiene motivos para creer que su contraseña se ha revelado accidentalmente a un tercero.
- Si el sistema le notifica que su contraseña caducará pronto o que ha caducado, elija una nueva según las instrucciones. Póngase en contacto con su administrador en caso de dificultad.

375. Un método RECOMENDADO para generar contraseñas que se ajustan a estos criterios sin dejar de ser fáciles de memorizar es basarlas en letras de palabras de una oración (NO de una cita famosa), incluidas las mayúsculas y la puntuación, con una o dos variaciones. Ejemplo:

"Piensa cuántas palabras tiene una oración como esta".
=> Pcpt1oce.

"La contraseña 'Lc'9nes;sie1d' no es segura; se incluye en un documento"
=> Lc'9nes;sie1d

7.3.4 AUTENTICACIÓN BASADA EN CLAVES SSH

376. PUEDE usar la autenticación basada en clave SSH que se describe en la sección *sshd*(8) "AUTHORIZED_KEYS FILE FORMAT". Antes de poder utilizar la autenticación basada en clave SSH, debe generar un par de claves.

377. Dado que solo la utilidad *ssh-keygen*(1) proporcionada con el TOE ha estado sujeta a la evaluación de seguridad, incluida la compatibilidad con la generación de claves adecuada, se RECOMIENDA encarecidamente que utilice esta herramienta del TOE.

378. DEBE generar pares de claves para SSHv2 mediante el conmutador de línea de comandos *-t rsa* o *-t ecdsa*.

379. La utilidad *ssh-keygen* permite especificar el tamaño de clave para RSA, con un valor por defecto de 2048 bits. Si selecciona un tamaño de clave diferente, DEBE utilizar tamaños de clave de más de 2048 bits. Se permiten todos los tamaños de clave admitidos para ECDSA.

380. DEBE mantener la parte de la clave privada almacenada en *~/.ssh/* inaccesible para cualquier otro usuario. Este archivo debe tratarse de forma similar a una contraseña. Se RECOMIENDA encarecidamente que proteja esta clave con una contraseña codificada **ssh-keygen**.

381. La siguiente línea de comandos es un ejemplo que genera una clave ECDSA:

    sh-keygen -t ecdsa -C "clave de John Doe"

382. El comando solicita una contraseña donde DEBERÍA proporcionarse una contraseña segura.

383. Después de generar el par de claves, PUEDE copiar el archivo aplicable de los archivos *~/.ssh/*.pub* al sistema del servidor y añadirlo al archivo *~/.ssh/authorized_keys*. Cree ese archivo si no existe y asegúrese de que su permiso impide que otros usuarios accedan a él. Encontrará más información en la sección *sshd*(8) "*AUTHORIZED_KEYS FILE FORMAT*".

384. En caso de que no cumpla los requisitos mencionados anteriormente, la protección de su cuenta puede verse debilitada. Esto puede considerarse similar a elegir una contraseña débil o a no mantener la confidencialidad de la contraseña.

385. El uso de la autenticación basada en clave no está sujeto al mecanismo de bloqueo de cuenta aplicado para las contraseñas.

7.3.5 CONTROL DE ACCESO A ARCHIVOS Y DIRECTORIOS

386. Linux es un sistema operativo multiusuario. Puede controlar qué otros usuarios podrán leer o modificar sus archivos estableciendo los bits de permiso de Unix y los ID de usuario/grupo, o (si se necesita un control más preciso) mediante listas de control de acceso (ACL) de estilo POSIX.

387. Los administradores (usuarios root) pueden anular estos permisos y acceder a todos los archivos del sistema. **Se RECOMIENDA el uso de cifrado para proteger adicionalmente los datos confidenciales.**

CONTROL DE ACCESO DISCRECIONAL

388. Puede controlar qué otros usuarios podrán leer o modificar sus archivos estableciendo los bits de permiso de Unix y los ID de usuario/grupo, o (si se necesita un control más preciso) mediante listas de control de acceso (ACL) de estilo POSIX. Esto se conoce como control de acceso discrecional (DAC).

389. El ajuste "*umask*" controla los permisos de los archivos y directorios recién creados y especifica los *bits* de acceso que se *eliminarán* de los objetos nuevos. **Asegúrese de que el ajuste sea adecuado y nunca otorgue acceso de escritura a otros usuarios por defecto.** El ajuste *umask* DEBE incluir al menos el bit 002 (sin acceso de escritura para los demás) y el valor RECOMENDADO es 027 (acceso de solo lectura y ejecución para el grupo, sin acceso para los demás). La configuración por defecto es aún más estricta, ya que establece el valor 077 (accesible solo para el propietario).

390. No configure áreas de escritura universal en el sistema de archivos: si desea compartir archivos de forma controlada con un grupo fijo de otros usuarios (como un grupo de proyecto), póngase en contacto con el administrador y solicite la creación de un grupo de usuarios para ese propósito.

391. Recuerde siempre que usted es responsable de la seguridad de los datos que cree y utilice. Elija permisos que coincidan con los objetivos de protección adecuados para el contenido y que correspondan a la directiva de seguridad de su organización. **El acceso a los datos confidenciales DEBE realizarse según una base "need-to-know" (la información justa a las personas justas)**, no haga que los datos sean legibles a menos que la información esté destinada a ser pública.

392. Siempre que inicie un programa o guion, se ejecutará con sus derechos de acceso. Esto implica que un programa malintencionado podría leer y modificar todos los archivos a los que tiene acceso. **Nunca ejecute ningún código que haya recibido de fuentes no fiables y no ejecute comandos que no comprenda.** Tenga en cuenta que las manipulaciones en el entorno en el que se ejecuta un programa también pueden provocar fallos de seguridad, como la filtración de información confidencial. No utilice las variables de *shell* *LD_LIBRARY_PATH* ni *LD_PRELOAD* que modifiquen la configuración de la biblioteca compartida utilizada por los programas enlazados dinámicamente.

393. Los programas se pueden configurar para ejecutarse con los derechos de acceso del propietario o el grupo del archivo de programa, en lugar de los derechos del usuario que realiza la llamada. Se trata del mecanismo SUID/SGID, que utilizan las utilidades como *passwd*(1) para poder acceder a archivos críticos para la seguridad. También puede crear sus propios programas SUID/SGID mediante *chmod*(1), pero NO lo haga a menos que comprenda completamente las implicaciones de seguridad; estaría cediendo *sus*

privilegios de acceso a cualquiera que lance el programa SUID. En el improbable caso de que necesite crear un programa de este tipo, consulte el documento "*Secure Programming HOWTO*" (Guía de programación segura). En él encontrará explicaciones de los diversos aspectos que se deben tener en cuenta, como el riesgo de que se produzcan fugas de *shell* no previstas, sobrecargas del buffer, ataques de agotamiento de recursos y muchos más. Los programas SUID de usuario *root* NO DEBEN añadirse a la configuración evaluada. El único uso permitido del bit SUID es para definir ID de usuarios que no sean *root*.

394. Consulte las páginas *man* de *chmod*(1), *umask*(2), *chown*(1), *chgrp*(1), *acl*(5), *getfacl*(1) y *setfacl*(1) para obtener información, o cualquiera de los muchos libros disponibles sobre la seguridad de Linux (consulte el Apéndice "Literatura") o pídale consejo al administrador del sistema.

7.3.6 IMPORTACIÓN/EXPORTACIÓN DE DATOS

395. El sistema incluye varias herramientas para archivar datos (*tar*, *star*, *cpio*). Si se utilizan ACL, solo se DEBE utilizar *star* para gestionar los archivos y directorios, ya que los demás comandos no admiten ACL. Las opciones *-H=exustar -acl* deben utilizarse con *star*.

396. Consulte la página man de *star*(1) para obtener más información.

7.3.7 PROTECTOR DE PANTALLA

397. El sistema ofrece la posibilidad de bloquear el terminal. Para desbloquearlo, DEBE proporcionar su contraseña.

398. El bloqueo se establece mediante la aplicación *screen*. Dependiendo de la configuración del sistema, PUEDE que *screen* ya se haya iniciado al entrar a la sesión. Si la aplicación *screen* no se inicia, puede hacerlo manualmente.

399. La aplicación *screen* permite los dos tipos de bloqueo de pantalla siguientes:

400. Bloqueo automático de la pantalla después de un período de inactividad del terminal definido por un tiempo límite en */etc/screenrc* o *~/.screenrc* mediante el valor de configuración *lockscreen*.

401. Bloqueo manual ejecutando la combinación de teclas de pantalla "*C+a C+x*".

402. PUEDE cambiar el valor de tiempo límite para bloquear la sesión en *~/.screenrc* con el valor de *lockscreen*. Tenga en cuenta que el administrador PUEDE inhabilitar la capacidad de utilizar el archivo de configuración *~/.screenrc*.

403. **ADVERTENCIA:** si un usuario accede al sistema de forma remota y la función del protector de pantalla se activa, el TOE se asegura de que la sesión se bloquea. Sin embargo, es posible que el terminal remoto implemente un buffer de retroceso que no esté bajo control del TOE. Por lo tanto, es posible que el terminal remoto tenga la sesión bloqueada, pero que un usuario pueda desplazarse hacia atrás y mostrar el historial de acciones. Si el usuario no debe tener permiso para utilizar el *buffer* de retroceso del terminal remoto, dicho terminal debe configurarse en consecuencia, ya que este *buffer* no está bajo el control del TOE. El *buffer* de retroceso local está inhabilitado.

no-scroll fbcon=scrollback:0

404. Si *screen* no se invoca automáticamente durante el inicio, PUEDE introducir la línea siguiente en *~/.bash_profile*.

exec screen

8 REFERENCIAS

405. Si hay recomendaciones contradictorias en esta guía o en alguna de las fuentes de información incluidas, la Guía de configuración tiene prioridad con respecto a la configuración evaluada.

REF1 GUIA DE SUSE LINUX ENTERPRISE SERVER: HTTPS://DOCUMENTATION.SUSE.COM/SLES/15-SP4/

9 ABREVIATURAS

AES	Advanced Encryption Standard
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación
CPU	Central Processing Unit
CRL	Certificate Revocation List
DAC	Discretionary Access Control
DHCP	Dynamic Host Configuration Protocol
ECC	Elliptic Curve Cryptography
ECC CDH	Elliptic Curve Cryptography Cofactor Diffie-Hellman
ENS	Esquema Nacional de Seguridad.
FFC	Finite Field Cryptography
FFC DH	Finite Field Cryptography Diffie-Hellman
HTTP	Hypertext Transfer Protocol
IBM	International Business Machines
IKE	Internet Key Exchange
IP	Internet Protocol
IPC	Inter-Process Communication
IPSEC	Internet Protocol Security
ISO	International Organization for Standardization (used here in the context of ISO disk images)
KVM	Kernel-based Virtual Machine
LPAR	Logical Partition
MAC	Message Authentication Code
NAT	Network Address Translation
NFS	Network File System
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OSI	Open Systems Interconnection
OSPP	Operating System Protection Profile
PAM	Pluggable Authentication Modules
RFC	Request for Comments
rpm	RPM Package Manager (originally Red Hat Package Manager)
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SCC	SUSE Customer Center
SHA	Secure Hash Algorithm
SLES	SUSE Linux Enterprise Server
SSH	Secure Shell
SSL	Secure Sockets Layer
SYSV	System V (UNIX variant)
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol

USB	Universal Serial Bus
UTC	Coordinated Universal Time
VMX	Vector Multimedia Extension
VPN	Virtual Private Network
WAN	Wide Area Network
z/VM	z Virtual Machine (IBM mainframe operating system)

PUBLICACIONES DE DEFENSA

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