

Procedimiento de Empleo Seguro

SUSE 15 SP2



Junio de 2022



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

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2022
NIPO: Pendiente de asignación.

Fecha de Edición: junio de 2022

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

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. INTRODUCCIÓN	4
1.1 OBJETIVO DE ESTE DOCUMENTO.....	4
1.2 CÓMO UTILIZAR ESTE DOCUMENTO.....	4
2. OBJETO Y ALCANCE	5
2.1 REQUISITOS <i>HARDWARE</i>	5
2.2 REQUISITOS <i>SOFTWARE</i>	5
3. ORGANIZACIÓN DEL DOCUMENTO	6
4. FASE DE DESPLIEGUE E INSTALACIÓN	7
4.1 ENTREGA SEGURA DEL PRODUCTO	7
4.1.1 OBTENCIÓN DE IMÁGENES DE INSTALACIÓN	7
4.2 ENTORNO DE INSTALACIÓN SEGURO	7
4.2.1 REQUISITOS DEL ENTORNO DEL SISTEMA.....	7
4.2.2 REQUISITOS PARA LOS USUARIOS DEL SISTEMA	10
4.3 CONSIDERACIONES PREVIAS	11
4.3.1 REQUISITOS PREVIOS PARA LA INSTALACIÓN.....	11
4.4 INSTALACIÓN.....	11
4.4.1 <i>HARDWARE</i> ADMITIDO	12
4.4.2 PROCESO DE INSTALACIÓN AUTOMATIZADO	12
4.4.3 INSTALACIÓN DE RPM ADICIONAL	21
4.4.4 CONFIGURACIÓN INICIAL	21
4.4.5 CONFIGURACIÓN DEL SISTEMA X86.....	24
4.4.6 CONFIGURACIÓN DEL SISTEMA ARM64.....	24
4.4.7 CONFIGURACIÓN DEL SISTEMA IBM Z	25
5. FASE DE CONFIGURACIÓN	26
5.1 MODO DE OPERACIÓN SEGURO	26
5.1.1 INICIO, APAGADO Y RECUPERACIÓN TRAS FALLOS DEL SISTEMA	26
5.1.2 SECURIZACIÓN DE LOS PARÁMETROS DEL KERNEL	26
5.1.3 OBTENCIÓN DE ACCESO ADMINISTRATIVO	27
5.1.4 INSTALACIÓN DE SOFTWARE ADICIONAL	28
5.1.5 PROGRAMACIÓN DE PROCESOS MEDIANTE <i>CRON</i>	30
5.1.6 MONTAJE DE SISTEMAS DE ARCHIVOS	31
5.1.7 PROTECCIÓN DE LAS PARTICIONES	33
5.1.8 CIFRADO DE PARTICIONES	35
5.1.9 BORRADO SEGURO	36
5.1.10 ELEMENTOS INNECESARIOS DEL SISTEMA.....	36
5.2 AUTENTICACIÓN.....	37
5.2.1 GESTIÓN DE CUENTAS DE USUARIO.....	37
5.2.2 USO DE TERMINALES EN SERIE.....	41
5.2.3 GESTIÓN DE OBJETOS DE DATOS	41
5.2.4 CONFIGURACIÓN DE DERECHOS DE ACCESO A OBJETOS	41
5.3 ADMINISTRACIÓN DEL PRODUCTO.....	42
5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA.....	42
5.3.2 CONFIGURACIÓN DE ADMINISTRADORES	42

5.4 CONFIGURACIÓN DE PROTOCOLOS SEGUROS	43
5.4.1 COMPATIBILIDAD CON CIFRADO.....	43
5.5 SINCRONIZACIÓN HORARIA	44
5.5.1 CONFIGURACIÓN DE LA FECHA Y LA HORA DEL SISTEMA	44
5.6 ACTUALIZACIONES	45
5.7 CONFIGURACIÓN DEL CORTAFUEGOS	45
5.8 CONFIGURACIÓN DEL PROTECTOR DE PANTALLA.....	46
5.9 AUDITORÍA	47
5.9.1 REGISTRO DE EVENTOS	47
5.9.2 ALMACENAMIENTO LOCAL	51
5.10 <i>BACKUP</i>	52
5.10.1 COPIA DE SEGURIDAD Y RESTAURACIÓN	52
5.11 SERVICIOS DE SEGURIDAD	53
5.11.1 DOCUMENTACIÓN EN LÍNEA.....	53
5.11.2 AUTENTICACIÓN	53
5.11.3 DIRECTIVA DE CONTRASEÑAS	54
5.11.4 AUTENTICACIÓN BASADA EN CLAVE SSH.....	55
5.11.5 CONTROL DE ACCESO A ARCHIVOS Y DIRECTORIOS	56
5.11.6 PROTECTOR DE PANTALLA	57
5.12 GESTIÓN DE MÁQUINAS VIRTUALES BASADAS EN EL NÚCLEO (KVM).....	58
5.12.1 CONFIGURACIÓN <i>HARDWARE</i>	58
5.12.2 CONFIGURACIÓN DE MÁQUINAS VIRTUALES BASADAS EN EL NÚCLEO (KVM).....	59
5.12.3 MÁQUINAS VIRTUALES INICIADAS FUERA DE <i>LIBVIRT</i>	61
5.12.4 SEPARACIÓN DE MÁQUINAS VIRTUALES	62
5.12.5 ID DE USUARIO Y GRUPO SIN PRIVILEGIOS	62
5.12.6 COMPATIBILIDAD CON SVIRT DE APPARMOR	62
5.12.7 USO COMPARTIDO DE RECURSOS.....	63
5.12.8 CONSIDERACIONES SOBRE CONECTIVIDAD	64
6. FASE DE OPERACIÓN	66
6.1 REVISIÓN DE LA CONFIGURACIÓN DEL SISTEMA.....	66
7. DESARROLLADORES DE APLICACIONES.....	68
8. <i>CHECKLIST</i>.....	69
9. REFERENCIAS	71
10. ABREVIATURAS	72

1. INTRODUCCIÓN

1.1 OBJETIVO DE ESTE DOCUMENTO

La distribución **SUSE LINUX Enterprise Server (SLES) 15 SP2** está diseñada para proporcionar un sistema operativo de propósito general seguro y fiable.

Este documento es una guía de seguridad que recoge las consideraciones necesarias para hacer uso del sistema operativo de forma segura, según una configuración evaluada y certificada.

Proporciona información a los administradores y usuarios para garantizar el principio de máxima seguridad, y mínima exposición. Abarca consideraciones de seguridad a nivel general e incluye referencias a otra documentación complementaria en caso de requerirse detalles adicionales.

1.2 CÓMO UTILIZAR ESTE DOCUMENTO

Si se siguen los requisitos de este documento al instalar y utilizar el sistema, la configuración resultante será la configuración que ha sido certificada. Algunas opciones de configuración se marcan como opcionales y pueden ser modificadas según sea necesario. Sin embargo, los administradores deben tener cuidado al cambiar el sistema para evitar que salga del estado certificado. Consultar la sección [2.2 REQUISITOS SOFTWARE](#) para obtener más información sobre cómo mantener la configuración certificada.

Por supuesto, siempre se debe utilizar el sentido común. Este documento no es una especificación formal y pueden existir razones legítimas para modificar la configuración del sistema de formas no descritas aquí si es necesario para que el sistema cumpla su propósito previsto. Específicamente, **se deben aplicar los parches de seguridad publicados por el proveedor**, aunque ello provoque una desviación de la configuración evaluada.

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 este Procedimiento de Empleo Seguro tiene mayor prioridad junto con la guía de configuración [REF1]. Se debe seguir los pasos descritos para llegar a la configuración evaluada, incluso si otra documentación describe métodos diferentes.

En esta guía se usan las convenciones habituales cuando se hace referencia a las páginas de manual que se incluyen en la distribución del *software*. Por ejemplo, la notación *ls* 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

2.1 REQUISITOS *HARDWARE*

El *hardware* sobre el que se despliegue el sistema operativo debe ser uno de los siguientes componentes:

- **Procesadores Intel Xeon x86 de 64 bits**
Delta D20x-M1-PC-32-8-96GB-1TB-2x1G
- **Procesadores AMD EPYC**
AMD EPYC DP Server R181-Z90
- **SLES en IBM System Z basado en procesadores z/Architecture**
IBM Z System z15
- **Sistema basado en procesadores ARM:**
Gigabyte R181-T90

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.

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.

2.2 REQUISITOS *SOFTWARE*

El *software* debe coincidir con la configuración evaluada. En el caso de un sistema operativo, también se requiere que el núcleo 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*).

Como norma general, para mantener la configuración evaluada, deben tenerse en cuenta las siguientes reglas:

- a) Todas las configuraciones indicadas en este documento deben seguirse estrictamente.
- b) Se pueden instalar nuevos paquetes en el sistema si:
 - Los ejecutables instalados no se ejecutan como *root* (o con un permiso equivalente).
 - Los ejecutables instalados no tienen SUID/SGID.
 - Los ejecutables instalados no tienen un nivel administrativo de permiso para cambiar el sistema de archivos (es decir, no hay cambios en las particiones ni se modifican las configuraciones existentes del sistema de archivos).
 - No hay módulos del kernel instalados.

3. ORGANIZACIÓN DEL DOCUMENTO

Este documento se estructura en los siguientes apartados:

- a) **Apartado 4.** En este apartado se recogen recomendaciones a tener en cuenta durante la fase de despliegue e instalación del producto.
- b) **Apartado 5.** En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.
- c) **Apartado 6.** En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.
- d) **Apartado 7.** En este apartado se incluyen recomendaciones para el desarrollo de aplicaciones.
- e) **Apartado 8.** En este apartado se recoge la lista de verificación de las actividades de bastionado recogidas en este documento.
- f) **Apartado 9.** En este apartado se incluyen las referencias a los documentos de interés mencionados a lo largo del documento.
- g) **Apartado 10.** En este apartado se incluyen las abreviaturas.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

4.1.1 OBTENCIÓN DE IMÁGENES DE INSTALACIÓN

Se deben descargar las imágenes ISO estándares del sitio Web de SUSE en un equipo independiente conectado a Internet y grabar los DVD-R a partir de esas imágenes, o bien hacer que el contenido esté disponible como se describe en la guía de distribución de SLES 15 SP2 en <https://documentation.suse.com/es-es/sles/15-SP2/>. Se pueden descargar las siguientes imágenes específicas de cada plataforma de <https://www.suse.com/download/sles/>.

Si la imagen que se desea descargar no aparece en la página, se debe iniciar sesión.

SUSE Linux Enterprise Server 15 SP2 para IBM Z System

- Nombre de archivo: SLE-15-SP2-Full-s390x-QU1-Media1.iso
- Suma de comprobación SHA256:
00f6d37fcf910ebf039bf9b13ef85243610443a4183a3817a9ede8d389f0cee9

SUSE Linux Enterprise Server 15 SP2 para Intel 64/AMD64

- Nombre de archivo: SLE-15-SP2-Full-x86_64-QU1-Media1.iso
- Suma de comprobación SHA256:
64aea562b5f51381b57f0c295fdd96c49b64c5f0760f2b62752fca54f4d999fd

SUSE Linux Enterprise Server 15 SP2 para ARM64

- Nombre de archivo: SLE-15-SP2-Full-aarch64-QU1-Media1.iso
- Suma de comprobación SHA256:
f04da5cf32448d2fafb5920175add0a42bfbacd0b6ff20303c793d46ee07dd4b

Se debe desplegar SUSE Linux Enterprise Server 15 SP2 y asegurarse de usar la versión adecuada para su plataforma; consultar la sección [2.1 REQUISITOS HARDWARE](#) de esta guía para obtener la lista de *hardware* compatible y la versión correspondiente necesaria.

Se debe verificar que las sumas de comprobación SHA256, incluida la firma, de los archivos de imagen ISO de SLES 15 SP2 sean correctas, realizando los pasos descritos en la página Web de seguridad: <http://www.suse.com/security/download-verification.html>.

4.2 ENTORNO DE INSTALACIÓN SEGURO

4.2.1 REQUISITOS DEL ENTORNO DEL SISTEMA

El objetivo de seguridad cubre uno o varios sistemas que ejecutan SLES, conectados en red en una red no hostil, con una comunidad de usuarios bien gestionada. 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.

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.

Se 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.

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 SSHv2 o TLS se considera protección suficiente para las conexiones de red. **Todas las demás conexiones deben permanecer completamente dentro del entorno del servidor físicamente seguro.**

4.2.1.1 REQUISITOS DE CONECTIVIDAD

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.

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

Se debe tener 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 este Procedimiento de Empleo Seguro (PES). Si se configura un enlace de comunicación con un sistema no controlado, se debe tener 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).

Al configurar un sistema KVM invitado, KVM permite que los adaptadores de red físicos se compartan entre distintos sistemas invitados. El uso compartido se basa en direcciones IP en las que KVM asigna una dirección IP única a cada invitado. Configurar adaptadores de red compartidos es similar a utilizar conmutadores físicos en la red. Si se desea lograr una separación más segura entre las máquinas virtuales, a cada dominio invitado se le debe asignar una interfaz de red física dedicada.

4.2.1.2 REQUISITOS PARA LOS ADMINISTRADORES

Se debe disponer de una o más personas formadas y concienciadas 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, junto con los propietarios de objetos, tendrán la capacidad de asignar y revocar derechos de acceso a los objetos a los roles.

Los administradores del sistema no deben ser descuidados, negligentes ni hostiles, y deben seguir y acatar las instrucciones proporcionadas en la documentación de seguridad de referencia.

Toda persona que tenga la capacidad de realizar acciones de administración, 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. Este Procedimiento de Empleo Seguro 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 administre Linux de forma segura.

En este documento se presupone que los administradores tienen un buen conocimiento y comprensión de los principios de seguridad operativos en general, de los comandos administrativos de Linux y de 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.

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. Este PES 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.

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.

Para garantizar la integridad del sistema, **se deben 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 para validar la integridad del sistema es el uso de *aide*. Esta funcionalidad se emplea principalmente para detectar cambios en los ficheros de configuración y binarios importantes, generalmente generando un resumen cifrado único de los ficheros a ser verificados, y almacenándolos en un lugar seguro. Con un procedimiento regular (mediante el planificador *cron*), los resúmenes originales se comparan con los generados a partir de la copia actual de cada fichero, para determinar si el fichero ha cambiado. Se le proporcionará a *aide* parámetros, para controlar al menos los siguientes puntos:

- a) La información referente a permisos (parámetro *p*).

- b) La información de los *inodos* (parámetro *i*).
- c) La cantidad de enlaces (duros y blandos) a cada fichero y al directorio (parámetro *n*).
- d) El propietario de cada fichero (parámetro *u*).
- e) El grupo propietario de cada fichero (parámetro *g*).
- f) El tamaño de cada fichero (parámetro *s*).
- g) La cantidad de bloques utilizados por cada fichero (parámetro *b*).
- h) Las fechas de modificación (parámetro *m*) y creación (parámetro *c*) de cada fichero.
- i) El tipo de fichero (parámetro *f**type*).
- j) Las listas de control de acceso (parámetro *acl*).
- k) Las modificaciones en *SELinux* (parámetro *selinux*).
- l) Los atributos extendidos de ficheros (parámetro *xattrs*).
- m) Además, se generará un resumen en sha512 por medio del parámetro *sha512*.

El administrador no debe poder leer el contenido del archivo que contiene la información de inicialización en */var/lib/misc/random-seed*. Esto garantiza que, si un administrador queda relevado de sus funciones y, por lo tanto, la relación de confianza se interrumpe, el administrador no podrá obtener ni aplicar el conocimiento (parcial) del estado de */dev/random* o de */dev/urandom*.

4.2.2 REQUISITOS PARA LOS USUARIOS DEL SISTEMA

Los requisitos específicos para los usuarios son:

- 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.
- Los usuarios deben realizar algunas tareas o grupos de tareas dentro de un entorno de TI seguro mediante el control total de sus datos.
- Todos los usuarios del sistema deben tener la capacidad suficiente para comprender las implicaciones de seguridad de sus acciones y seguir los requisitos de seguridad establecidos. Se les debe proporcionar la formación adecuada para garantizarlo.

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.

4.3 CONSIDERACIONES PREVIAS

4.3.1 REQUISITOS PREVIOS PARA LA INSTALACIÓN

Se recomienda desconectar todas las conexiones de red hasta que finalice la configuración del sistema. Se 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 se utiliza una red, se debe garantizar que sea segura; por ejemplo, conectando directamente el nuevo sistema a un servidor NFS independiente sin otras conexiones de red.

Se necesitarán los siguientes componentes para instalar un sistema en la configuración evaluada como se explica en las siguientes secciones:

- El sistema de destino en el que se instalará el sistema operativo (consultar la sección [2.1 REQUISITOS 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 SP2 aplicable al sistema *hardware* seleccionado debe estar disponible. Si se utiliza *hardware* basado en Intel, se 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.
- Una dirección IP estática si se 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 se 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.

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 la 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 **[REF2]**.

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 INSTALACIÓN

Para asegurar de forma correcta cualquier sistema operativo, es recomendable seguir una serie de pautas de configuración desde el inicio. Por ello, se tendrán en cuenta configuraciones iniciales de instalación tales como el particionado, el sistema de archivos a utilizar o la complejidad de contraseñas entre otros.

El sistema operativo certificado cubre una instalación nueva de SLES 15 en una de las plataformas *hardware* compatibles, como se define en la sección [2.1 REQUISITOS HARDWARE](#) de esta guía.

En las plataformas que admiten virtualización (VM) o particionamiento lógico seguro (LPAR), puede haber otros sistemas operativos instalados y activos al mismo tiempo que la configuración evaluada. Esto podría darse si (y solo si) la configuración de la máquina virtual o el LPAR garantiza que los demás sistemas operativos no puedan acceder a los datos que pertenecen a la configuración evaluada y que no puedan interferir con su funcionamiento de ninguna otra forma. La preparación de este tipo de configuración se considera parte del entorno operativo y no se trata en esta guía.

En las demás plataformas, la configuración evaluada y certificada debe ser el único sistema operativo instalado en el servidor.

4.4.1 HARDWARE ADMITIDO

Se pueden conectar los siguientes periféricos sin invalidar la certificación del sistema operativo. No deben 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, se pueden conectar directamente terminales en serie compatibles (consultar la sección [5.2.2 USO DE TERMINALES EN SERIE](#) de esta guía), pero no módems, tarjetas RDSI ni otros terminales de acceso remoto.

No deben instalarse ni asignarse a la máquina virtual tarjetas *IBM Crypto Express*. Esta restricción se debe a la limitación de los recursos durante la evaluación y de ninguna manera es una indicación de que el *hardware* o los controladores de *software* asociados se hayan implementado incorrectamente.

4.4.2 PROCESO DE INSTALACIÓN AUTOMATIZADO

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

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

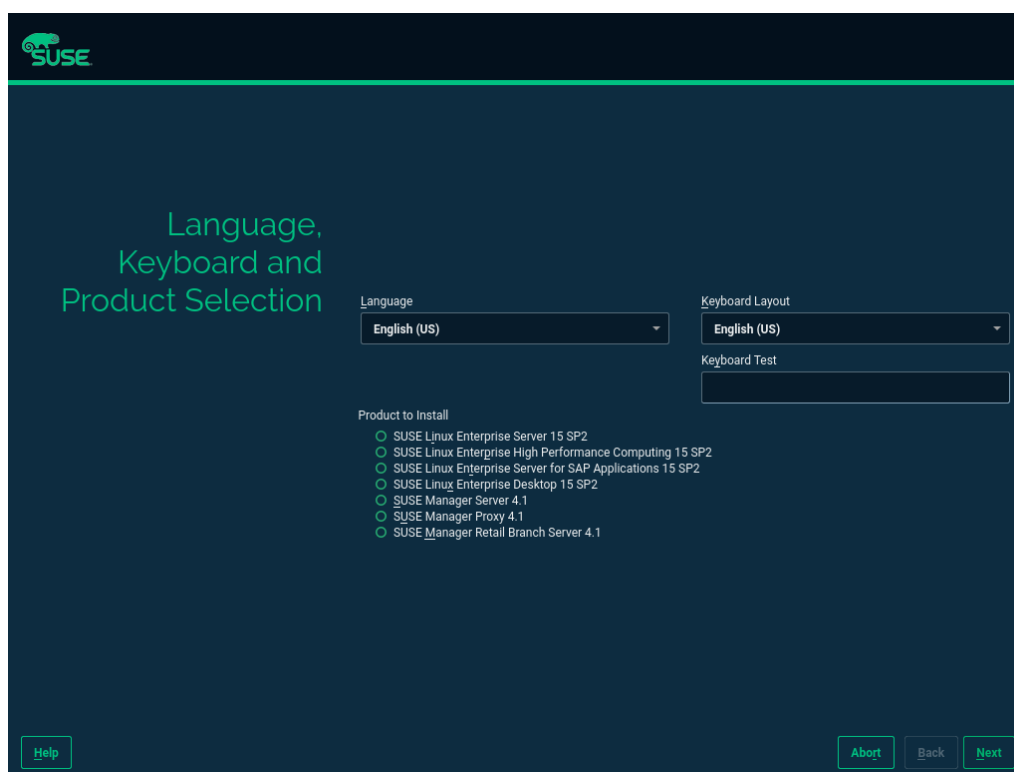
Todos los ajustes indicados aquí son necesarios a menos que se indique específicamente lo contrario.

4.4.2.1 PROCESO DE INSTALACIÓN

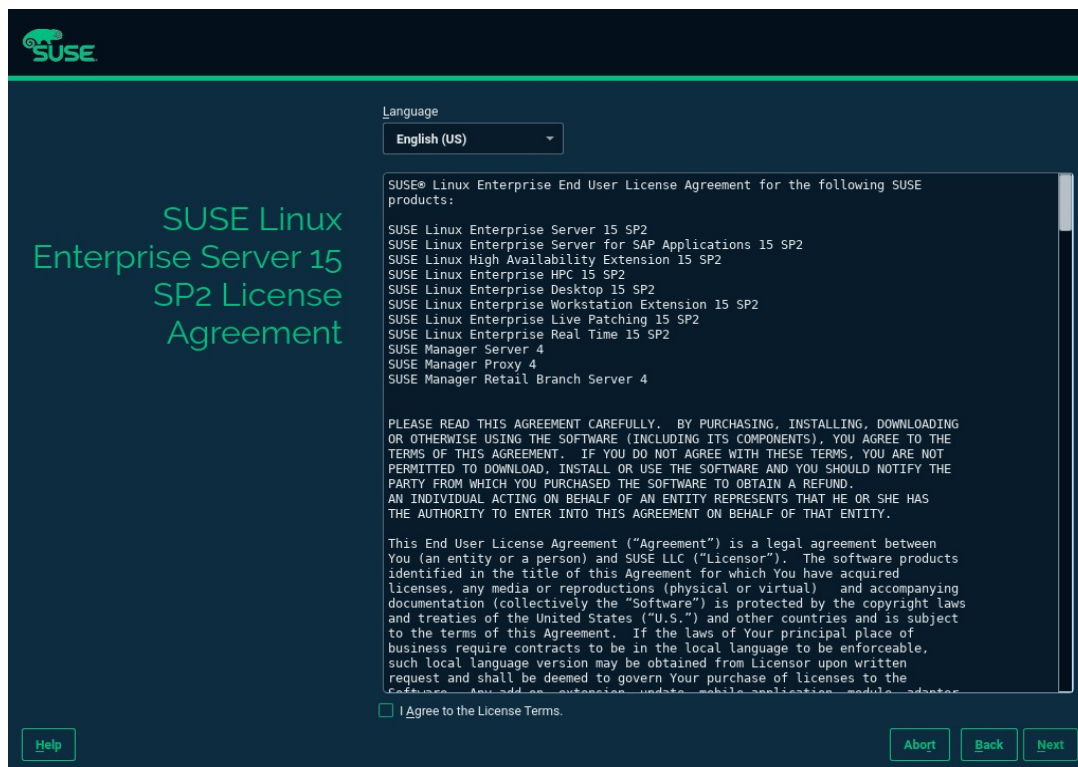
La preparación del arranque inicial y el modo en que se accede al indicador de arranque dependen del *hardware* y de la configuración elegidos. Se recomienda consultar la documentación de SLES específica de la arquitectura para configurar el entorno de arranque.

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

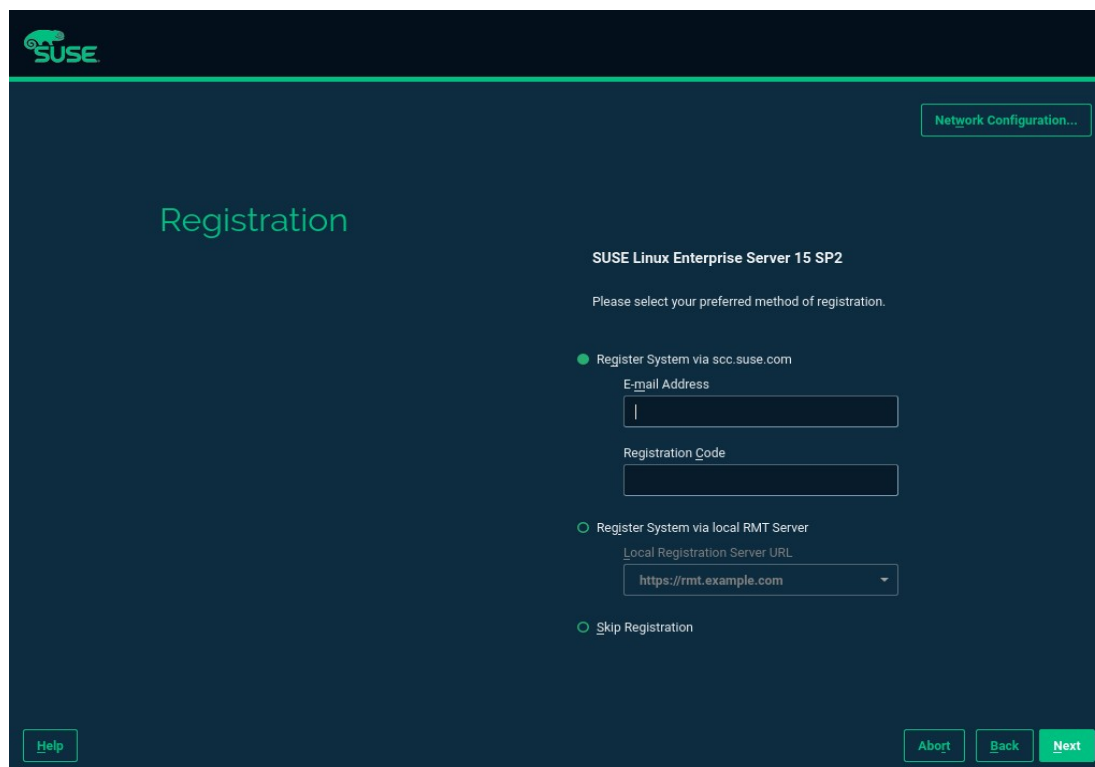
En la siguiente ilustración se muestra un ejemplo de cómo arrancar directamente desde el DVD de SLES. Si se utiliza un mecanismo de arranque distinto, esta ilustración puede no ser aplicable.



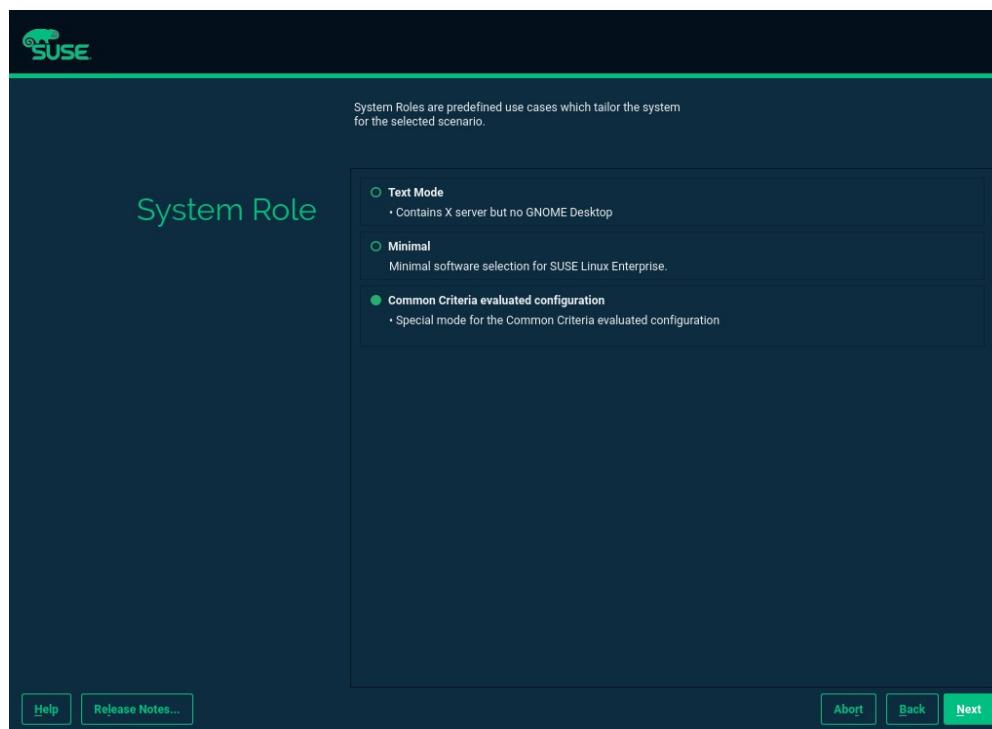
Cuando el instalador pregunte el idioma de instalación, se debe seleccionar "*English*", ya que es el único idioma admitido para la configuración evaluada. También se puede seleccionar la distribución del teclado que mejor le convenga y se debe leer atentamente el acuerdo de licencia y marcar la casilla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



Después de aceptar el acuerdo de licencia, se recomienda que registre el producto en scc.suse.com o en un servidor RMT local. Si se omite el registro en este punto, se debería registrar el producto después de finalizar la configuración del sistema posterior a la instalación.



En el paso siguiente se debe seleccionar "*Common Criteria evaluated configuration*" para instalar SUSE Linux Enterprise Server en la configuración evaluada. Esta configuración contiene algunas restricciones a las opciones disponibles.

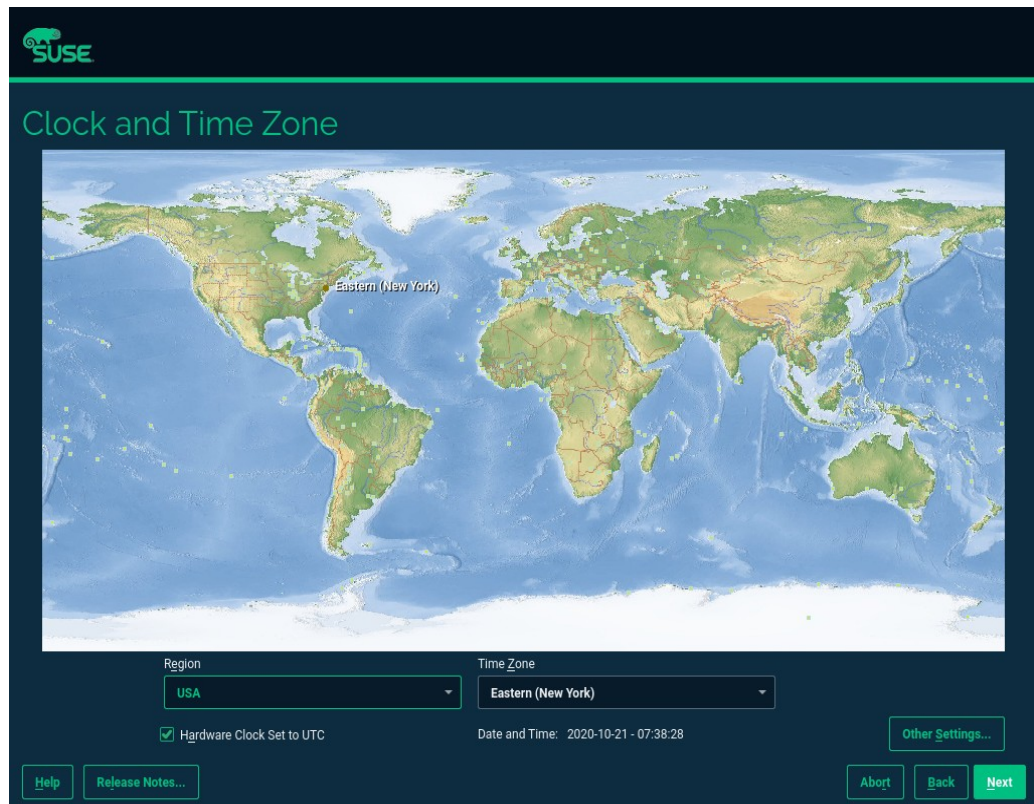


El siguiente paso es la partición. Se pueden modificar los siguientes ajustes en este punto; sin embargo, **el cifrado de disco debe estar habilitado**.

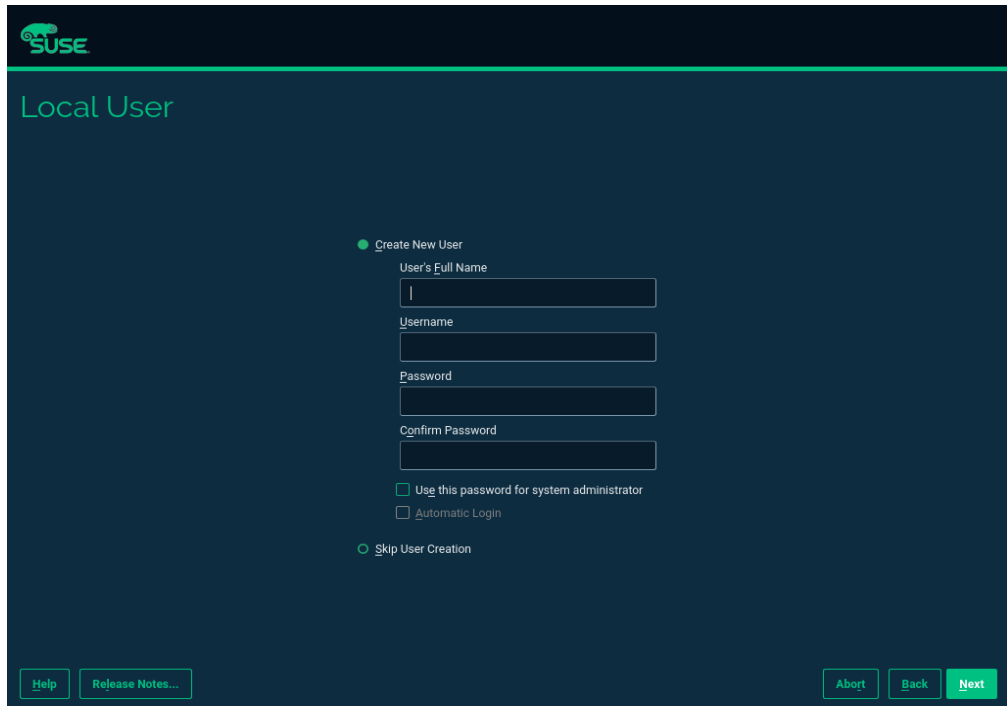
- El diseño de las particiones puede adaptarse a las necesidades de la organización. En particular, puede cambiar las particiones; sin embargo, no se debe cambiar la configuración de la partición `/boot`. Además, se pueden cambiar los sistemas de archivos utilizados a EXT3, EXT4, BTRFS o XFS. La elección del sistema de archivos adecuado depende del propósito de la máquina que se está configurando. Consultar el siguiente link <https://documentation.suse.com/sles/15-SP2/single-html/SLES-storage/#cha-filesystems> para obtener información que ayude a decidir el sistema de archivos más adecuado. No se 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, se debe estar seguro de que se formatean las particiones; el valor por defecto garantiza que las particiones se formatean. La sección **5.1.7 PROTECCIÓN DE LAS PARTICIONES** proporciona ejemplos de esquema de partición y recomienda sistemas de archivos para el caso genérico.
- 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. Se 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 especificar las opciones de montaje de *nosuid* y *nodev* para las particiones montadas en */tmp* o */var/tmp*.

- Se 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.
- Se recomienda, en este punto, reservar espacio para los discos de las máquinas virtuales, creando sus archivos de imagen, porque estos archivos son potencialmente muy grandes. La ubicación por defecto elegida por *libvirt* es */var/lib/libvirt/images/*. Se puede modificar el diseño de particiones para otorgar espacio a los archivos utilizados como *backends* de dispositivos de disco para las máquinas virtuales.
- Se pueden también modificar las opciones del cargador de arranque; por ejemplo, se puede establecer una contraseña. Sin embargo, no se debe modificar el tipo de cargador de arranque, la ubicación del cargador de arranque ni la sección del cargador de arranque de "*Linux - CC evaluated configuration*", que debe ser la opción por defecto. Las contraseñas deben ser lo más seguras posibles para evitar inicios de sesión no autorizados. Para ello, se deben seguir las indicaciones del apartado 5.11.3 DIRECTIVA DE CONTRASEÑAS.
- En este momento, la instalación pedirá la zona horaria aplicable al sistema. Se puede seleccionar la zona horaria que se quiera. Además, se puede configurar un servidor NTP en este punto seleccionando "*Change*" en el recuadro "*Date and Time*".



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

The image shows a window titled "Local User" with the SUSE logo in the top left. It contains a "Create New User" section with four text input fields: "User's Full Name", "Username", "Password", and "Confirm Password". Below these fields are two checkboxes: "Use this password for system administrator" and "Automatic Login". At the bottom of the form is a radio button labeled "Skip User Creation". At the very bottom of the window are three buttons: "Help", "Release Notes...", and a group of "Abort", "Back", and "Next" buttons.

- Después de configurar todas las opciones, se invoca el proceso de instalación haciendo clic en "*Install*". 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.
- Se debe verificar que se muestre una configuración correcta como resultado. Si falla algún paso de la configuración, no se 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 añadirlo. <USUARIO> es el nombre del usuario añadido anteriormente:

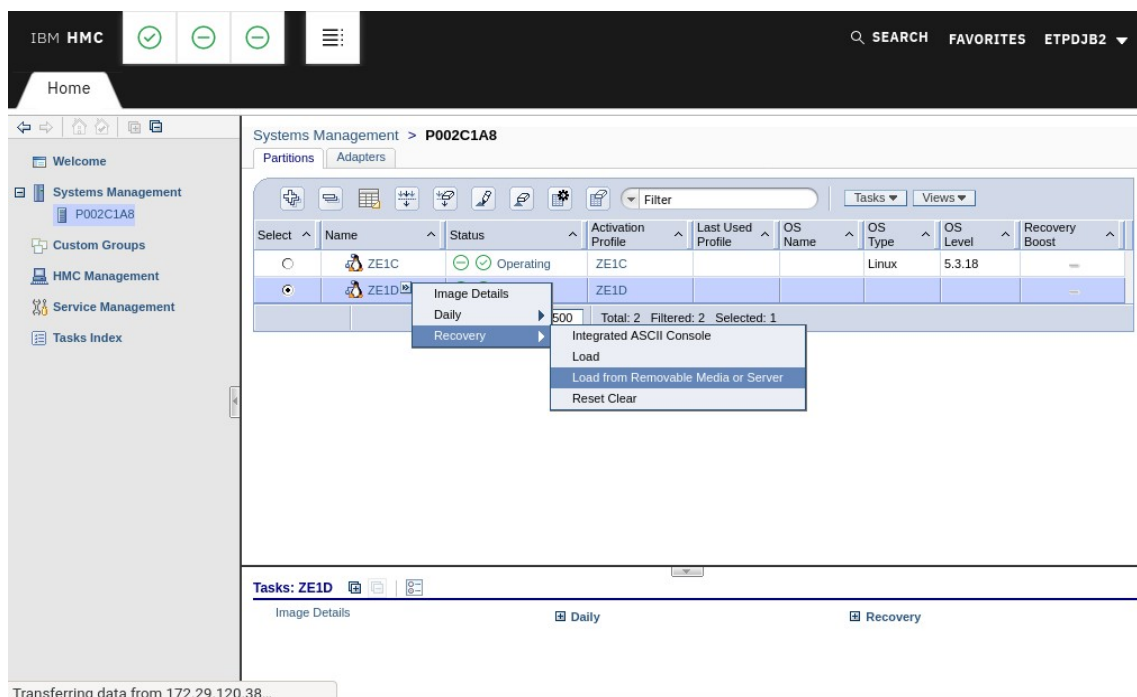
`usermod -G trusted -a <USUARIO>`

En la configuración posterior no debe utilizarse la herramienta YaST, ya que puede interferir y deshacer la anterior configuración manual. (YaST es una herramienta disponible en las distribuciones de SUSE que facilita la administración del sistema y la instalación de software. Para más detalle consultar <https://documentation.suse.com/sles/15-SP2/single-html/SLES-administration/#cha-yast-gui>).

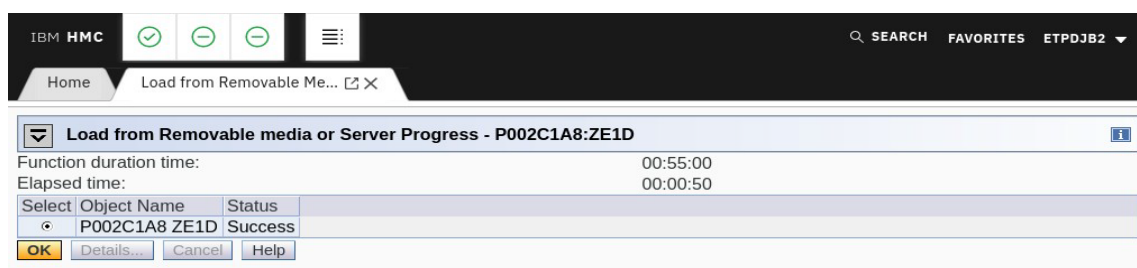
Instalación en IBM Z System

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 de forma remota a la consola z/VM. 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, ya que el instalador de HMC parece no funcionar con entradas anónimas.

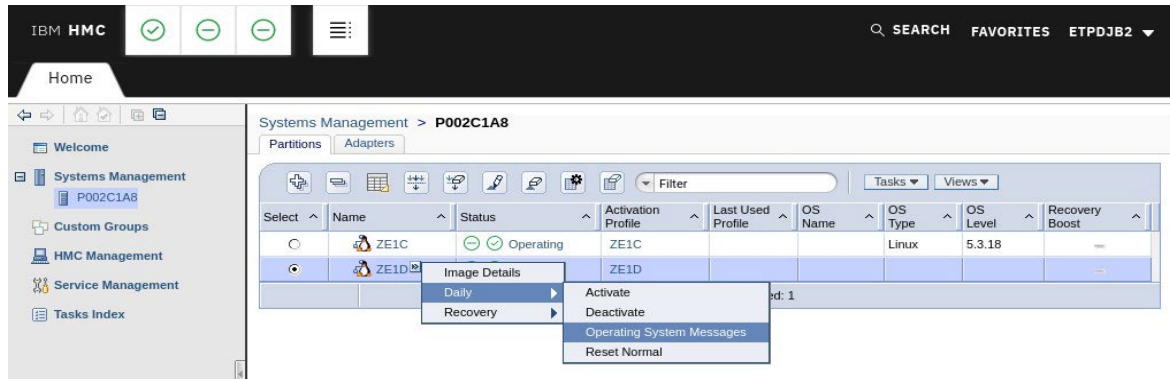
El primer paso para instalar SUSE Linux Enterprise 15 SP2 es la recuperación desde un medio remoto, como se muestra en la siguiente ilustración.



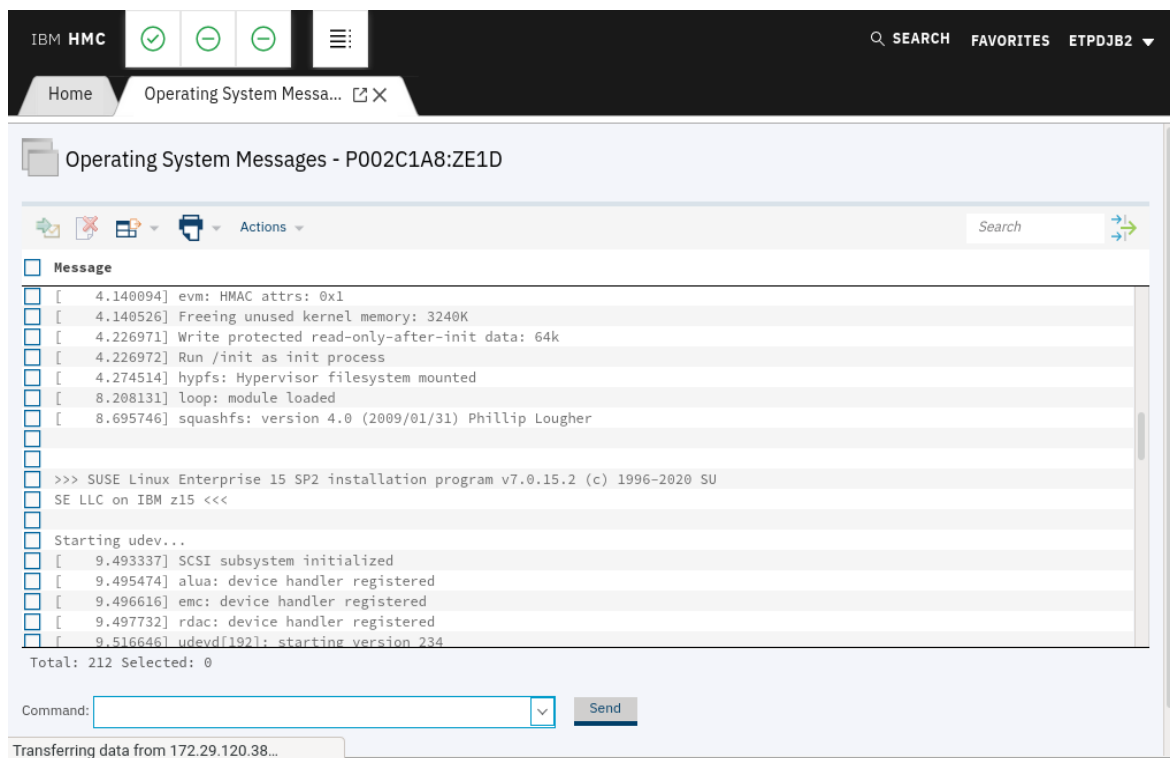
Posteriormente, se deben introducir las credenciales de FTP, incluido el nombre de *host* y la vía del archivo. En el siguiente paso, seleccionar *[...]/suse.ins* (no *[...]/susehmc.ins*) y continuar. Después de proporcionar la contraseña del usuario, la imagen se cargará y el proceso continuará correctamente.



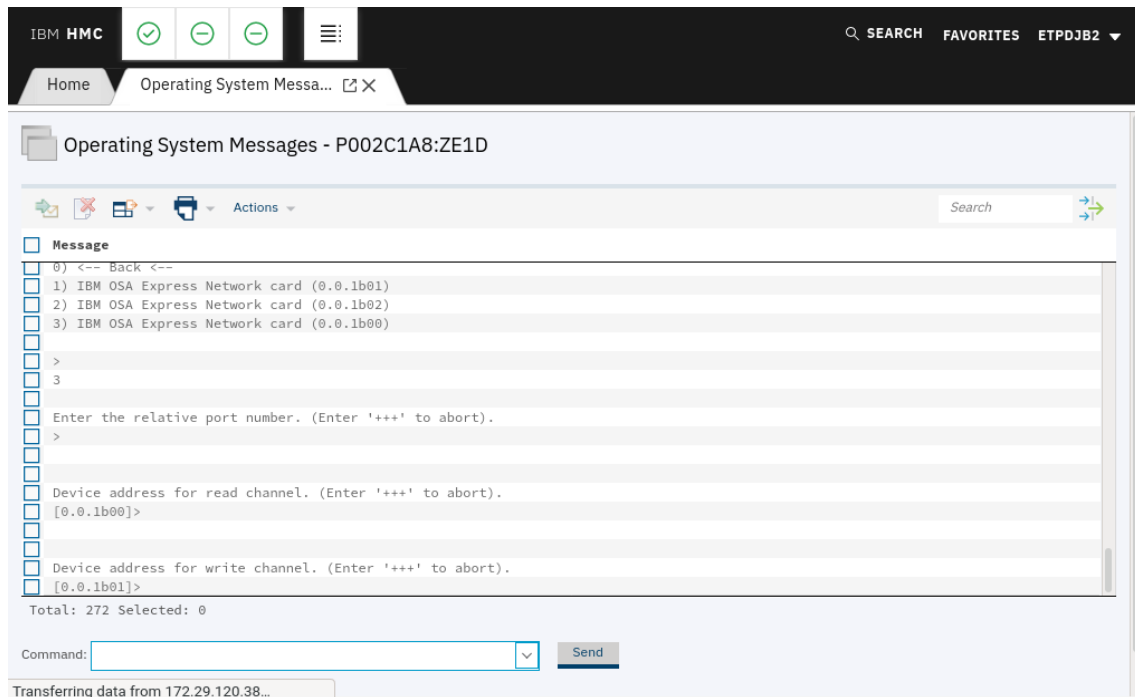
Acceder ahora a la salida del sistema operativo de HMC, como se muestra en la siguiente ilustración.



Debería mostrarse "SUSE Linux Enterprise 15 SP2 installation program" para "SUSE LLC on IBM z15".

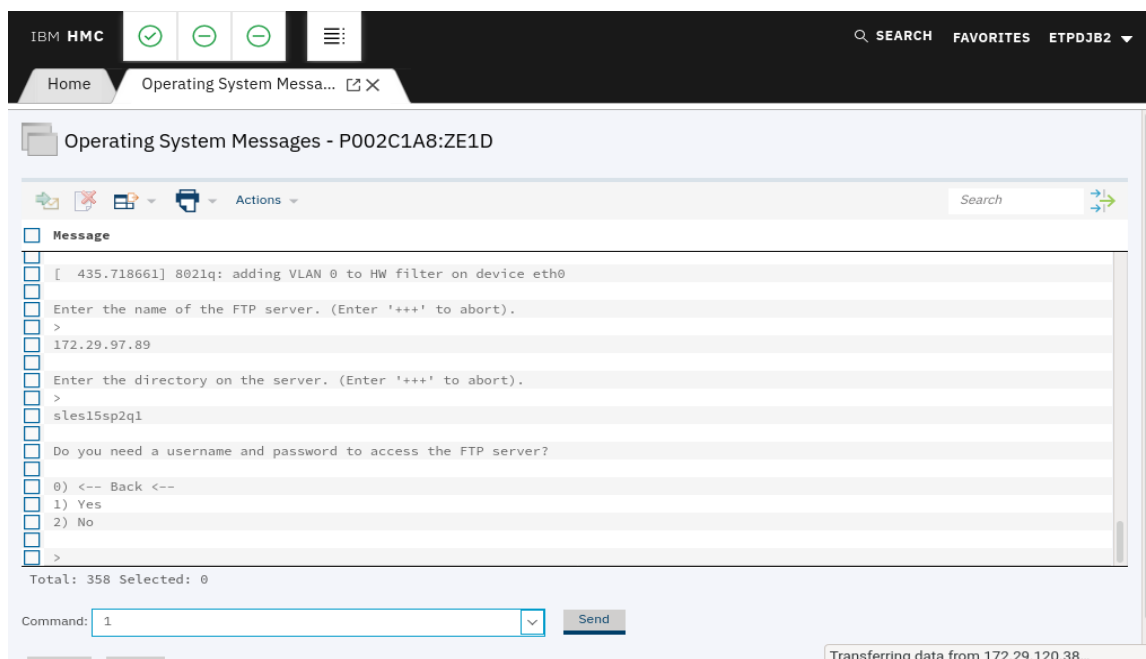


Se debe iniciar la instalación, elegir como red de origen y como protocolo FTP. Elegir la primera tarjeta de red dentro de la máquina virtual de System Z, que siempre debe ser 0.0.1.b00, y utilizar los valores por defecto. No utilizar compatibilidad con OSI Layer 2.



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.

A continuación, es necesario introducir la dirección IP del servidor FTP y el directorio de medios. Se debe indicar que se necesita una contraseña para acceder al servidor FTP e introducir el nombre de usuario y la contraseña.



Seleccionar que no se necesita proxy. El sistema de instalación ya está cargado. Seleccionar la instalación SSH y definir 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. Se debe conectar por VPN a través de SSH al sistema de instalación.

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.

```
~> ssh root@172.29.129.33
The authenticity of host '172.29.129.33 (172.29.129.33)' can't be established.
ECDSA key fingerprint is SHA256:AA6jLtJnq+IsLxZtuhgJWksSfRLTqt3rqK0blhk802g.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.29.129.33' (ECDSA) to the list of known hosts.
Password:

SUSE Linux Enterprise 15 SP2 Installation

Run yast.ssh to start the installation.

0:install:~ #
```

Después de seleccionar SUSE Linux Enterprise Server 15 SP2 y aceptar el acuerdo de licencia, seleccionar "Configure ZFCP Disks" (Configurar discos ZFCP) y seguir los pasos descritos en [4.1.1 OBTENCIÓN DE IMÁGENES DE INSTALACIÓN](#). Después, se podrá conectar al sistema a través de SSH.

En los pasos de configuración posteriores no se debe utilizar la herramienta YaST.

4.4.3 INSTALACIÓN DE RPM ADICIONAL

Después de finalizar el proceso de instalación como se describe en el capítulo anterior, **se deben instalar los siguientes paquetes** mediante el comando `zypper`:

```
zypper install openssh-8.1p1-5.18.1 openssh-helpers-8.1p1-5.18.1
openssh-fips-8.1p1-5.18.1 openssl-1_1-1.1.1d-11.20.1
sudo-1.8.22-4.15.1 dnsmasq-2.78-7.6.1
permissions-20181224-23.3.1 kernel-default-5.3.18-24.78.1
audit-2.8.1-12.3.1 libaudit1-2.8.1-12.3.1 libauparse0-2.8.1-12.3.1
python3-audit-2.8.1-12.3.1 audit-audispd-plugins-2.8.1-12.3.1
screen-4.6.2-5.3.1 libxml2-tools-2.9.7-3.34.1
libxml2-2-2.9.7-3.34.1 python3-libxml2-python-2.9.7-3.34.1
grub2-2.04-9.45.2 grub2-systemd-sleep-plugin-2.04-9.45.2
grub2-snapper-plugin-2.04-9.45.2 cpio-2.12-3.9.1
polkit-0.116-3.3.1
```

4.4.4 CONFIGURACIÓN INICIAL

Por defecto el sistema operativo, crea ciertas configuraciones para facilitar el acceso al usuario, habilitando la mayor parte de funcionalidades y aumentando la velocidad de instalación del

mismo. Estas configuraciones en muchas ocasiones pueden ser motivo de posibles brechas de seguridad.

Para evitar brechas innecesarias, se configurarán ciertos parámetros de manera correcta:

- a) **GRUB.** GNU *Grand Unified Boot loader* (GRUB) es un gestor de arranque múltiple desarrollado inicialmente para el sistema GNU Hurd. El gestor de arranque grub tiene varias funciones, pero sin duda su misión principal es seleccionar qué sistema operativo instalado o *kernel* cargar en el momento de arranque del sistema. Permite también que el usuario transmita argumentos al kernel. Por estos motivos Grub solo tiene que ser accesible por *root* y mediante contraseña y se deberá:

- i. Bloquear el acceso a la línea de comandos del Grub.
- ii. Bloquear la posibilidad de edición de las entradas del Grub.

Para ello, se deberá:

- Crear una contraseña para grub2 usando *grub2-mkpasswd-pbkdf2*.
- Escribir la contraseña y su confirmación. El programa genera una línea comenzando con: *"PBKDF2 hash of your password is grub.pbkdf2.sha512.10000..."*
- Copiar la línea generada comenzando en *"grub.pbkdf2.sha512.10000..."* hasta el final de la línea
- Crear el fichero */etc/grub.d/42_password* el cual contendrá lo siguiente (hasta la línea de #####):

```
#!/bin/sh
exec tail -n +2 $0
set superusers="root"
password_pbkdf2 root <SUSTITUIR grub.pbkdf2.sha512.10000...>
export superusers
set unrestricted_menu="y"
export unrestricted_menu
#####
```

- Sustituir la línea *<SUSTITUIR grub.pbkdf2.sha512.10000...>* en el fichero */etc/grub.d/42_password* con la línea que has obtenido del programa *grub2-mkpasswd-pbkdf2*.
- Guardar el fichero y cambiar su permiso de ejecución con el siguiente comando:
- Entonces ejecutar el siguiente comando para actualizar grub2:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

- b) **Contraseña segura para Root.** Cuando se habla de *root*, se refiere a la cuenta superusuario en Linux, aquella que posee todos los privilegios y permisos para realizar acciones sobre el sistema. Para ciertas acciones que afectan al sistema de archivos, se

requiere tener acceso *root*. Sin embargo, se debe tener un conocimiento sobre las acciones que se realizan, ya que una acción realizada de manera errónea podría ocasionar daños importantes en el sistema. Para evitar el uso de instrucciones con privilegios de superusuario la cuenta *root* tiene que estar dotada con una contraseña segura que evite que cualquier usuario malintencionado pueda comprometer de algún modo el sistema. Para cambiar la contraseña de *root* es necesario usar el siguiente comando: *\$sudo passwd root*.

- c) **Usuarios UID 0.** En el fichero */etc/passwd/* existe un campo UID por cada usuario, que corresponde al identificador de cada usuario. Algunas distribuciones de Linux por defecto, crean varios usuarios con UID 0 que corresponde al identificador de superusuario. Si existen varios superusuarios en el sistema la probabilidad de vulnerar el mismo es mayor, por este motivo se deben limitar los usuarios con UID 0 únicamente a *root*, siendo el único usuario habilitado para tener control total sobre el sistema. Para saber el número de superusuarios que existen se deberá utilizar el siguiente comando:

```
sudo cat /etc/passwd | cut -d":" -f1,3 | grep -w 0 | cut -d":" -f1.
```

El comando deberá devolver “*root*” como resultado por pantalla, pero si, por el contrario, sale algún resultado que no sea *root*, significará que esos usuarios tienen “UID” 0 y por ende permisos demasiado elevados y deben ser eliminados.

- d) **Cuentas sin contraseñas.** En Linux existe la opción de configurar una cuenta de usuario sin contraseña, aunque ese usuario no pertenezca a los denominados “sudores” (administradores). En el sistema no debe de haber ningún usuario sin contraseña, esto supondría una vulnerabilidad, ya que cualquier usuario podría acceder a información sensible sin necesidad de estar autorizado para ello.
- e) **Instalación por defecto.** Utilizar el módulo de gestión de software de YaST para buscar los componentes de software que desee añadir o eliminar. YaST resuelve todas las dependencias automáticamente. Para instalar paquetes no incluidos con el medio de instalación, añada repositorios adicionales de software a la configuración y deje que YaST los gestione. El applet de actualización le permite mantener el sistema actualizado gestionando las actualizaciones de software.
- f) **Aplicación de la configuración evaluada.** Es necesario modificar el archivo *55-common-criteria.conf*, ubicado en */usr/lib/sysctl.d/* añadiendo la siguiente línea:

```
kernel.unprivileged_bpf_disabled = 1
```

- g) **Configuración de cifrado.** El archivo *sshd_config* ubicado en */etc/ssh/sshd_config* debe modificarse para cumplir con la configuración evaluada. Por lo tanto, el límite de *rekey* debe establecerse en:

```
RekeyLimit 4G none
```

Esta configuración limitará la cantidad máxima de datos transmitidos antes de que se configure una nueva clave simétrica. Transmitir por encima de ese límite puede debilitar la seguridad de algunos algoritmos simétricos.

Además, los siguientes algoritmos criptográficos deben estar restringidos en el mismo fichero mencionado:

Ciphers AES128-CTR, AES256-CTR

KexAlgorithms ECDH-SHA2-NISTP256, ECDH-SHA2-NISTP384 o ECDH-SHA2-NISTP521

MACs HMAC-SHA2-256, HMAC-SHA2-512

HostbasedAcceptedKeyTypes (HostbasedAcceptedAlgorithms) ECDSA-SHA2-NISTP256 o ECDSA-SHA2-NISTP384

Adicionalmente, las siguientes configuraciones deben añadirse en el mismo fichero:

X11Forwarding *yes*

Desactivar el envío de aplicaciones X11 a través de la conexión ssh:

LoginGraceTime *2m*

Establecer un tiempo máximo para el inicio de sesión, antes de abandonar la conexión:

HostbasedAuthentication *no* **IgnoreRhosts** *yes*

Desactivar la autenticación basada en el host ya que no es segura:

PermitUserEnvironment *no*

No permitir el uso de variables de entorno del host de conexión en el servidor conectado:

PermitEmptyPasswords *no*

Denegar el acceso remoto a los usuarios que no tienen contraseña:

ClientAliveInterval *60*

ClientAliveMaxIntervals *3*

Esto establecerá un máximo de 180 segundos (3 minutos) de inactividad para la conexión. Si expira, la conexión se interrumpe.

4.4.5 CONFIGURACIÓN DEL SISTEMA X86

Se debe utilizar el siguiente comando *zypper* para actualizar los paquetes *audit*, *grub2* y *ship* después del primer arranque:

```
zypper install libaudit1-32bit-2.8.1-12.3.1 shim-15.4-3.20.1
```

```
grub2-x86_64-efi-2.04-9.45.2 grub2-i386-pc-2.04-9.45.2
```

4.4.6 CONFIGURACIÓN DEL SISTEMA ARM64

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.

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.

Después del primer arranque, debe **inhabilitar los módulos del núcleo de CE Linux para evitar que se utilicen**. Para ello, se debe crear el siguiente archivo con este contenido:

/etc/modprobe.d/aes_ce.conf

```
install aes_ce_cipher /bin/true
```

```
install aes_ce_blk /bin/true
```

```
install sha2_ce /bin/true
```

```
install sha1_ce /bin/true
```

```
install ghash_ce /bin/true
```

```
install crct10dif_ce /bin/true
```

Además, para que la configuración evaluada esté conforme, **se debe actualizar el paquete grub2** mediante el siguiente comando *zypper*:

```
zypper install grub2-arm64-efi-2.04-9.45.2
```

4.4.7 CONFIGURACIÓN DEL SISTEMA IBM Z

SE debe utilizar el siguiente comando *zypper* para actualizar el paquete s390-tools después del primer arranque:

```
zypper install s390-tools-2.11.0-9.31.1
```

```
grub2-s390x-emu-2.04-9.45.2
```

5. FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

5.1.1 INICIO, APAGADO Y RECUPERACIÓN TRAS FALLOS DEL SISTEMA

Se deben utilizar los programas *shutdown*, *halt* o *reboot* según sea necesario para apagar o rearrancar el sistema.

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. Se recomienda consultar la documentación de *fsck* y *debugfs* para obtener más información.

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, puede ser útil el argumento de la línea de comandos del núcleo para arrancar en el modo de emergencia:

```
systemd.unit=emergency.target
```

Además, el destino de rescate proporciona un entorno útil:

```
systemd.unit=rescue.target
```

Para obtener más información, consultar la documentación pertinente del cargador de arranque, así como la guía del administrador de SLES [REF2].

5.1.2 SECURIZACIÓN DE LOS PARÁMETROS DEL KERNEL

Los parámetros `sysctl` del *kernel* pueden ser manipulados para proporcionar seguridad adicional, especialmente para el subsistema de red. Los siguientes parámetros deberían ser añadidos en el fichero `/etc/sysctl.d/CCN-STIC-1615.conf` (se debe crear si no existe para mejorar la seguridad del Kernel):

```
# Evitar la modificación de tablas de encaminamiento
#
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.default.secure_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
#
# Deshabilitar el source routing
```

```
#  
net.ipv4.conf.all.accept_source_route = 0  
net.ipv4.conf.default.accept_source_route = 0  
#  
# Activa los logs para paquetes anormales o excepcionales  
#  
net.ipv4.conf.all.log_martians = 1  
net.ipv4.conf.default.log_martians = 1  
#  
# Ignorar peticiones broadcast  
#  
net.ipv4.icmp_echo_ignore_broadcasts = 1  
#  
# Ignorar mensajes de error mal formados  
#  
net.ipv4.icmp_ignore_bogus_error_responses = 1  
#  
# Protegerse ante ataques tcp syn  
#  
net.ipv4.tcp_syncookies = 1  
#  
#Bloqueo de core dumps de programas con SUID  
#  
fs.suid_dumpable = 0
```

5.1.3 OBTENCIÓN DE ACCESO ADMINISTRATIVO

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 se debe autenticar utilizando un ID de usuario sin privilegios y, a continuación, utilizar el comando *su* o *sudo* para cambiar de identidad. Solo se deben utilizar los derechos de usuario *root* para tareas administrativas que requieran estos privilegios; todas las demás tareas deben realizarse utilizando su ID de usuario normal (no *root*).

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*.

5.1.3.1 USO DE *SU*

El comando *su* permite un cambio permanente del ID de usuario para la sesión actual.

Debe utilizarse exactamente la siguiente línea de comando de *su* para obtener acceso de superusuario:

```
/usr/bin/su -
```

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.

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. 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.

5.1.3.2 USO DE *SUDO*

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.

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*.

La configuración siguiente permite que todos los usuarios asociados al grupo *trusted* utilicen todos los comandos con privilegios:

```
%trusted ALL=(ALL) ALL
```

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

5.1.4 INSTALACIÓN DE SOFTWARE ADICIONAL

Se pueden instalar paquetes de software adicionales según sea necesario, siempre que no entren en conflicto con los requisitos de seguridad.

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

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.

Los requisitos de seguridad para el *software* adicional son:

- **No se debe instalar ni cargar módulos del núcleo distintos de los proporcionados como parte de la configuración evaluada.** No se debe cargar el módulo del núcleo *tux* (el servidor Web del núcleo no es compatible). No se 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 se debe activar *knfsd* ni exportar sistemas de archivos NFS.
- No se debe añadir al sistema nodos especiales del dispositivo.
- No se debe añadir al sistema programas de *root* de SUID, programas de *root* de SGID ni programas con capacidades de sistema de archivos. Se pueden 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*". Para información adicional sobre el propósito del */etc/login.defs*, usar el comando *man 5 login.defs*.
- **No se 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. Se pueden añadir archivos y directorios a directorios existentes siempre que esto no infrinja ningún otro requisito.
- **No se deben 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*, *setgid* y *setuid* en un binario. Las llamadas *seteuid* y similares no son suficientes: **si el administrador no puede identificar cuándo y cómo se eliminan los privilegios, la aplicación no debe instalarse.**

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 que se inician mediante el sistema *DBUS*, que se configura mediante */etc/dbus-1/system.d/*.
- Aplicaciones especificadas en */etc/sudoers* o con reglas ubicadas en un archivo del directorio */etc/sudoers.d*. Ese archivo puede contener la palabra clave *ALL* como espacio reservado para un comando. En ese caso, el usuario autorizado para 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*.

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.

5.1.5 PROGRAMACIÓN DE PROCESOS MEDIANTE *CRON*

Cron es una herramienta que se usa para automatizar procesos. Es un administrador regular de procesos en segundo plano (demonio) que ejecuta procesos o guiones a intervalos regulares (por ejemplo, cada minuto, día, semana o mes).

Sus entradas se pueden modificar mediante el programa *crontab*. El formato de archivo se describe en la página *man* de *crontab*.

Dado que *cron* permite elegir qué usuario ejecutará un determinado proceso, tiene un gran potencial de abuso de seguridad. Se deben seguir las reglas especificadas para la instalación de programas adicionales para todas las entradas que ejecutará el usuario *root*. Se deben utilizar entradas *crontab* que no sean de usuario *root* en todos los casos en los que los privilegios de *root* no sean absolutamente necesarios.

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.

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

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.

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*.

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
```

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*.

Se 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).

El ID de entrada a la sesión no se conserva en el siguiente caso especial:

- a) El usuario A entra en el sistema.
- b) El usuario A utiliza su para cambiar a usuario B.
- c) El usuario B ahora edita la cola cron o at para añadir nuevas tareas. Esta operación se audita adecuadamente con el ID de entrada a la sesión adecuado.
- d) 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.

5.1.6 MONTAJE DE SISTEMAS DE ARCHIVOS

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 no se introducen funciones que puedan infringir la directiva de seguridad.

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 núcleo. 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.

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.

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 [4.1.1 OBTENCIÓN DE IMÁGENES DE INSTALACIÓN](#).
- Los sistemas de archivos EXT2, EXT3 o EXT4 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`

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.

Como alternativa, se puede acceder a medios si no se integran en la configuración evaluada; por ejemplo, a un CD-ROM o DVD. Para ello, se debe utilizar el tipo de sistema de archivos iso9660.

Se deben utilizar las siguientes opciones de montaje si los sistemas de archivos contienen datos que no forman parte de la configuración evaluada: *nodev* y *nosuid*.

Se recomienda añadir la opción de montaje *noexec* para evitar que se ejecuten de forma accidental archivos o guiones en sistemas de archivos adicionales montados.

Estos ajustes no protegen por completo contra código y datos dañinos, por lo que **se debe verificar que los datos proceden de una fuente de confianza y no ponen en peligro la seguridad del servidor**. En concreto, se deben tener 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 que usuarios no autorizados los puedan divulgar o modificar. Los datos importados pueden haberse creado con nombres de usuario y permisos que no coincidan con las directivas de seguridad del sistema.
- No se deben 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. Consultar la sección [5.10.1 COPIA DE SEGURIDAD Y RESTAURACIÓN](#) de esta guía para obtener más información acerca de la copia de seguridad no basada en sistemas de archivos.

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
```

También puede añadir una configuración equivalente a */etc/fstab*, por ejemplo:

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

No se 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*.

5.1.7 PROTECCIÓN DE LAS PARTICIONES

Para proteger el uso indebido de las diferentes particiones y los ficheros alojados en ellas, se deberá analizar cuál es el uso principal de cada partición, y así determinar las opciones que se utilizarán para montarlas. Estas opciones se reflejarán en el fichero */etc/fstab*.

Las opciones que se configuren en el fichero */etc/fstab* se aplicarán de forma automática en el inicio de montaje de cada partición.

Las particiones se pueden montar de distintas formas para que limiten determinados permisos:

- a) *Noauto*: La partición no se montará automáticamente.
- b) *Noexec*: La partición no admitirá la ejecución de ficheros desde la misma.
- c) *Nodev*: La partición no admitirá la instalación de dispositivos.
- d) Permisos (ro), (rw): La partición se configurará con permisos *read-only* (ro, solo lectura), *read-write* (rw, lectura y escritura).

NOTA: Hay que tener en cuenta que la opción default monta la partición con las opciones *rw*, *suid*, *dev*, *exec*, *auto*, *nouser*, *async*.

A continuación, se listan las particiones más importantes y las recomendaciones seguras de montaje:

- a) */boot*. Contiene información sobre el arranque del sistema.
Se montará con las opciones *noauto*, *noexec*, *nodev*, *nosuid*, *ro*.
- b) */boot/efi*. Contiene información sobre el arranque del sistema UEFI.
Se montará con los siguientes parámetros *umask=0077*, *shortname=winnt <dump> 0 <pass> 0*.
- c) */usr* y */opt*: Contienen ficheros ejecutables del sistema.
Se montará con las opciones *nodev*, *ro*.
- d) */var*: Contiene archivos muy variables del sistema (*logs*, *BBDD*, contenido *web*, etc.)
Se montará con las opciones *defaults*, *nosuid*.
- e) */var/log*: Contiene los logs del sistema.
Se montará con las opciones *nodev*, *noexec*, *nosuid*, *rw*.
- f) */var/log/audit*: Contiene información y *logs* de la herramienta *Audit*.
Se montará con las opciones *nodev*, *noexec*, *nosuid*, *rw*.
- g) */var/www*: Contiene principalmente el contenido Web.
Se montará con las opciones *nodev*, *noexec*, *nosuid*, *rw*.
- h) */home* y */tmp*: Contienen los archivos del usuario y los temporales del sistema.
Se montará con las opciones *nodev*, *noexec*, *nosuid*, *rw* y especialmente en */home* se le asignará cuota de disco.
- i) */media/XXX*: Contiene montaje de particiones de dispositivos extraíbles.

Se montará con las opciones *noauto*, *nodev*, *nosuid*, *rw*.

- j) */*: Contiene la partición raíz del sistema.

Se montará con la opción de lectura y escritura (*rw*).

- k) *Swap*: Se trata de la memoria de intercambio, memoria que usará el sistema cuando necesite espacio en memoria RAM.

Se montará con la opción *defaults*, *<dump> 0 <pass> 0*.

Excepciones.

Para realizar ciertas acciones en determinados momentos se modificará la forma de montaje.

- a) */boot*: Si se tuviera que actualizar el kernel, será necesario montar la partición temporalmente en lectura y escritura (*rw*).
- b) */usr* y */opt*: Si se desea instalar una nueva aplicación o actualizar una ya existente, será necesario montar la partición correspondiente manualmente en modo de lectura y escritura (*rw*).

NOTA:

- Utilizado por el programa *dump* («volcado») para decidir cuándo hacer una copia de seguridad. *Dump* comprueba la entrada en el archivo *fstab* y el número de la misma le indica si un sistema de archivos debe ser respaldado o no. Las entradas posibles son 0 y 1. Si es 0, *dump* ignorará el sistema de archivos, mientras que, si el valor es 1, *dump* realizará una copia de seguridad. La mayoría de los usuarios no tendrán *dump* instalado, por lo que deben poner el valor 0 para la entrada.
- Utilizado por *fsck* para decidir el orden en el que los sistemas de archivos serán comprobados. Las entradas posibles son 0, 1 y 2. El sistema de archivos raíz («root») debe tener la más alta prioridad: 1 - todos los demás sistemas de archivos que desea comprobar deben tener un 2-. La utilidad *fsck* no comprobará los sistemas de archivos que vengan ajustados con un valor 0.

Una vez realizadas todas las modificaciones debe quedar el fichero */etc/fstab* de esta manera:

Particiones	Sistema de archivos	Permisos
<i>/dev/mapper/cr ROOT /</i>	Btrfs	<i>defaults,nofail</i> 1 1
UUID=xxxxxxxxxxxxxxxx swap swap	swap	<i>defaults</i> 0 0
UUID=xxxxxxxxxxxxxxxx/boot	xfs	<i>noauto,noexec,nodev,nosuid,ro</i> 1 2
UUID=xxxxxxxxxxxxxxxx/opt	xfs	<i>exec,nodev,auto,nouser,async,ro</i> 1 2
UUID=xxxxxxxxxxxxxxxx/svr	xfs	<i>defaults</i> 1 2
UUID=xxxxxxxxxxxxxxxx/home	xfs	<i>nodev,noexec,nosuid,rw</i> 1 2

Particiones	Sistema de archivos	Permisos
UUID=xxxxxxxxxxxxxxxxxxxx /tmp	xfs	nodev,noexec,nosuid,rw 1 2
UUID=xxxxxxxxxxxxxxxxxxxx /var	xfs	dev,nosuid,exec,auto,nouser, async,rw 1 2
UUID=xxxxxxxxxxxxxxxxxxxx /var/log	xfs	nodev,noexec,nosuid,rw 1 2
UUID=xxxxxxxxxxxxxxxxxxxx /var/log/audit	xfs	nodev,noexec,nosuid,rw 1 2

La tabla anterior es un ejemplo de organización posible, ya que no se fuerza a una partición específica y/o a una configuración del sistema de archivos durante la instalación.

5.1.8 CIFRADO DE PARTICIONES

Se deben cifrar las particiones para aumentar la seguridad de las mismas e impedir que personal no autorizado pueda acceder a datos críticos. Recomendamos que se realice este cifrado durante el proceso de instalación y, por tanto, **no se recomienda cifrar una partición en un sistema ya instalado**. Se requiere mucho cuidado y cualquier error puede llevar a la pérdida de datos.

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.

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 se ha seleccionado el cifrado de disco completo o se ha configurado el cifrado para distintas particiones durante la instalación inicial, tal y como se describe en la sección [4.1.1 OBTENCIÓN DE IMÁGENES DE INSTALACIÓN](#), ya se habrán almacenado los datos en discos duros protegidos por *dm-crypt*.

Se pueden 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*. Se puede consultar la página man de *cryptsetup* para descubrir cómo se usa *dm-crypt*.

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

```
zypper install cryptsetup-2.0.6-4.3.1
```

Si se usa *cryptsetup* manualmente, debe usar la extensión LUKS y, por lo tanto, los comandos LUKS especificados en *cryptsetup*. Una contraseña se utiliza para recuperar la clave que cifra todos los datos encriptados en el disco, por lo que recomendamos el uso de contraseñas suficientemente seguras.

Para configurar una partición protegida por *dm-crypt* se utiliza el comando *luksFormat* en la aplicación *cryptsetup*. Si no desea utilizar el cifrado por defecto con *luksFormat* (consultar *cryptsetup --help*), se debe verificar que se cumplen los siguientes requisitos al especificar el cifrado:

Cifrados permitidos:

- AES (128 bits, 256 bits)

Modos de encadenamiento de bloques permitidos:

- XTS (como se define en NIST SP 800-38E)

Después del formateo, se debe utilizar el comando *luksOpen* para configurar el mecanismo de cifrado; es decir, para informar al núcleo de que cualquier operación de lectura y escritura se cifrará y descifrá 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.

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

5.1.9 BORRADO SEGURO

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 y, por lo tanto, **debe utilizarse el comando *shred***. Sin embargo, *shred* no es eficaz en todos los sistemas de archivos (más información en la página *man* de *shred*). 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 utilizar el comando:

```
fstrim -a
```

para recortar todos los dispositivos de bloques, incluido el dispositivo de bloques que solía contener los datos confidenciales. Para obtener más información acerca de *fstrim*, consultar la página *man* de *fstrim*.

Además, el disco debe sobrescribirse varias veces con números aleatorios antes de desecharse. También se recomienda utilizar particiones cifradas (consultar [5.1.8 CIFRADO DE PARTICIONES](#)), así como destruir físicamente el disco al desecharlo.

5.1.10 ELEMENTOS INNECESARIOS DEL SISTEMA

En este punto es necesario tratar siempre de deshabilitar todos aquellos elementos del sistema que no sean necesarios, minimizando la superficie de posibles ataques al mismo.

5.1.10.1 PAQUETES INNECESARIOS

Una de las características del *software* libre es su carácter colaborativo. De esta manera existen cientos de miles de librerías disponibles, que permiten a los desarrolladores crear una aplicación sin tener que empezar de cero. Disponiendo de componentes de diferentes tamaños con un objetivo o funcionalidad específica y que permiten hacer la aplicación más robusta.

De esta característica se nutren las distribuciones Linux. Para que esas aplicaciones se ejecuten correctamente, se necesita que estén instalados el resto de paquetes. De esta forma, cuando se

instala una aplicación, también se instalan aquellos paquetes necesarios para su funcionamiento.

Estos paquetes necesarios son los que se conocen como dependencias. Sin embargo, hay que tener en cuenta el momento de en la desinstalación de una aplicación, puesto que al desinstalar el paquete padre (aplicación principal) no siempre se desinstalan las dependencias. Al contrario, esas dependencias quedan instaladas en el equipo ocupando un espacio innecesario. Estos paquetes son los que se conoce como paquetes huérfanos.

5.1.10.2 USUARIOS INNECESARIOS

Como se ha comentado anteriormente, por defecto el sistema operativo, crea configuraciones para facilitar el uso del mismo, una de esas configuraciones, son los usuarios predefinidos como *ftp*, *games*, etc. Estos usuarios tienen permisos y configuraciones para ciertas partes del sistema operativo. El tener usuarios predefinidos en el S.O puede ser motivo de posibles brechas de seguridad.

Por esto, los usuarios de un sistema operativo tienen que ser los mínimos necesarios e indispensables, eliminando los que no sean necesarios y restringiendo ciertos permisos a los que por necesidad deban mantenerse. Para ello, se debe seguir lo indicado en el apartado [5.2.1.6 ELIMINACIÓN DE USUARIOS](#).

5.2 AUTENTICACIÓN

5.2.1 GESTIÓN DE CUENTAS DE USUARIO

5.2.1.1 CREACIÓN DE USUARIOS

Se puede utilizar el comando *useradd* para crear nuevas cuentas de usuario y, a continuación, el comando *passwd* para asignar una contraseña inicial al usuario. Se puede consultar las páginas *man* de *useradd* y *passwd* para obtener más información.

Si se asigna una contraseña inicial para un nuevo usuario, esta debe ser transferida de forma segura al usuario, asegurándose de que ningún tercero obtenga la información. Esto debe 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. Se debe informar al usuario de que debe cambiar esta contraseña inicial cuando entre por primera vez en el sistema y seleccionar su propia contraseña de acuerdo con las reglas definidas en la sección [5.11.3 DIRECTIVA DE CONTRASEÑAS](#) de esta guía.

No se debe utilizar la opción *-p* para *useradd* ya que, si especifica una contraseña de ese modo, se omitirá el mecanismo de comprobación de la calidad de la contraseña.

El usuario debe cambiar la contraseña temporal definida por el administrador lo antes posible. Se puede utilizar el comando *chage* 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*.

Ejemplo:

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

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

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

5.2.1.2 CAMBIO DE CONTRASEÑAS DE USUARIO

Si es necesario, se 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.

5.2.1.3 AUTENTICACIÓN BASADA EN CLAVE SSH

El sistema operativo permite configurar la autenticación basada en clave para SSH. 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, consultar `sshd`.

Para generar las claves usadas en la autenticación, se proporciona la herramienta `ssh-keygen`, cuyo uso se recomienda, ya que esta utilidad ha formado parte de la evaluación de seguridad. Dado que el `daemon` de SSH solo acepta la versión 2 del protocolo SSH, únicamente se admiten las claves del protocolo 2. Por lo tanto, solo se utiliza la opción `-t rsa` o `-t ecdsa` cuando se genere una clave con `ssh-keygen`.

La utilidad `ssh-keygen` permite especificar el tamaño de clave para RSA, con un valor por defecto de 2048 bits. Sin embargo, **se deben utilizar tamaños de clave de más de 2048 bits**. Se permiten todos los tamaños de clave admitidos para ECDSA.

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`.

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

```
ssh-keygen -t ecdsa -C "Clave de John Doe"
```

El comando solicita una contraseña codificada donde se debería proporcionar una contraseña codificada segura.

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

5.2.1.4 CAMBIO DE LAS PROPIEDADES DEL USUARIO

Se puede utilizar el comando *usermod* para cambiar las propiedades del usuario.

5.2.1.5 BLOQUEO Y DESBLOQUEO DE CUENTAS DE USUARIO

Se puede bloquear (inhabilitar) a los usuarios mediante *passwd -l USUARIO* y volver a habilitarlos mediante *passwd -u USUARIO*. 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 entradas basadas en clave SSH, se debe eliminar el archivo *.ssh/authorized_keys* ubicado en el directorio personal del usuario.

El módulo PAM *pam_tally2.so* aplica un bloqueo automático después de que se supere un número de intentos de autenticación fallidos. Se puede utilizar el programa *pam_tally2* para ver y restablecer el contador si es necesario, como se indica en la página man de *pam_tally2*. 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, se 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
passwd jdoe
pam_tally2 --user jdoe --reset
```

La utilidad *chage* 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.

5.2.1.6 ELIMINACIÓN DE USUARIOS

La utilidad *userdel* 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. Se puede utilizar *kill* (o re arranque el sistema) y *find* para hacerlo manualmente si es necesario, por ejemplo:

```
# ¿Qué usuario desea 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 re arrancar)
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
```

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.

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.

Puede encontrar una explicación de lo que son las ACL en:

<https://documentation.suse.com/sles/15-SP1/html/SLES-all/cha-security-acls.html>.

Si se necesitan crear grupos adicionales o modificar grupos existentes, se pueden utilizar los comandos *groupadd*, *groupmod* y *groupdel*.

En la configuración evaluada no se admiten contraseñas de grupo. Se han inhabilitado eliminando el bit de SUID del programa *newgrp*. No se debe volver a habilitar esta función y no se debe utilizar *passwd* con el conmutador *-g* ni el comando *gpasswd* para definir contraseñas de grupo.

5.2.1.7 DEFINICIÓN DE CUENTAS ADMINISTRATIVAS

Los usuarios administrativos deben ser miembros del grupo *trusted*. Se debe especificar la opción *-G trusted* para el comando *useradd* al crear usuarios administrativos.

También se puede utilizar el comando *usermod* para cambiar la pertenencia a grupos. Por ejemplo, si desea añadir el usuario *jdoe* al grupo *trusted*, se 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
```

5.2.2 USO DE TERMINALES EN SERIE

Se pueden conectar terminales en serie al sistema para que los utilicen los administradores del sistema. Los terminales en serie se activan automáticamente mediante *systemd* cuando se utiliza la opción de línea de comandos del núcleo *console* para habilitar una consola en serie. Por ejemplo:

```
console=ttyS0,115200n8
```

5.2.3 GESTIÓN DE OBJETOS DE DATOS

5.2.3.1 REVOCACIÓN DEL ACCESO

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.

Si esta revocación diferida no es aceptable y es necesario asegurarse de que ningún proceso de usuario acceda a un objeto después de haber cambiado los derechos de acceso a ese objeto, se debe reorganizar el sistema. Esto garantiza que ningún proceso tenga descriptores abiertos que permitan un acceso continuo.

5.2.3.2 MEMORIA COMPARTIDA SYSV Y OBJETOS IPC

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* para mostrar información sobre esos recursos e *ipcrm* para forzar la supresión de objetos innecesarios. Estos recursos también se liberan cuando se reorganiza el sistema.

Para obtener información adicional, se puede consultar la página *man* de *ipc*.

5.2.3.3 COLAS DE MENSAJES POSIX

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 mq_overview*, como *mq_open* y *mq_unlink*.

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*.

5.2.4 CONFIGURACIÓN DE DERECHOS DE ACCESO A OBJETOS

Los administradores pueden utilizar las herramientas *chown*, *chgrp* y *chmod* para configurar los derechos de acceso a objetos. No se debe otorgar acceso adicional a los objetos que forman parte de la configuración evaluada.

Se puede consultar las correspondientes páginas *man* para obtener más información acerca de estas herramientas.

5.3 ADMINISTRACIÓN DEL PRODUCTO

5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

5.3.1.1 CONFIGURACIÓN DE RED

Para configurar las interfaces de red, se deben modificar los archivos *config* y utilizar 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, se puede consultar la sección 19.5 "*Configuración manual de una conexión de red*", en la Guía de administración de SUSE Linux Enterprise Server 15 SP2 [REF2].

5.3.2 CONFIGURACIÓN DE ADMINISTRADORES

5.3.2.1 CONFIGURACIÓN DE LA DIRECTIVA DE CONTRASEÑAS

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*:

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.

Se debe tener en cuenta la directiva de contraseñas del apartado 5.3.2.1 CONFIGURACIÓN DE LA DIRECTIVA DE CONTRASEÑAS.

5.4 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

5.4.1 COMPATIBILIDAD CON CIFRADO

5.4.1.1 CONFIGURACIÓN DE OPENSSH

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.

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*.

Para la protección del cliente OpenSSH, se debe añadir la siguiente opción al archivo */etc/ssh/ssh_config*:

UseRoaming no

Esta opción está relacionada con dos problemas de seguridad: CVE-0216-0777 y CVE-0216-0778.

5.4.1.2 GESTIÓN DE CLAVES CRIPTOGRÁFICAS

Los protocolos de red de cifrado SSH y TLS proporcionan un canal seguro para proteger 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.

Por lo tanto, se debe verificar 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.

También se 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.

Se deben utilizar los siguientes mecanismos de cifrado para SSH:

Algoritmos de cifrado

AES128-CTR o AES256-CTR

Algoritmos de clave pública

ecdsa-sha2-nistp256 o ecdsa-sha2-nistp384

Intercambio de claves

ecdh-sha2-nistp256, ecdh-sha2-nistp384 o ecdh-sha2-nistp521.

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. Deben usarse alguno de los siguientes conjuntos de cifrado:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Las extensiones de grupos admitidos que se permiten en el *Hello* del cliente son estas:

- secp256r1
- secp384r1
- secp521r1

Además, al configurar el 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 [5.1.8 CIFRADO DE PARTICIONES](#).

5.4.1.3 GENERACIÓN Y ESTABLECIMIENTO DE CLAVES CRIPTOGRÁFICAS

Las claves criptográficas asimétricas deben generarse utilizando uno de los siguientes algoritmos de generación de claves criptográficas:

- Claves RSA con longitud mínima de 3072.
- Cifrado de curva elíptica (ECC) con las curvas NIST P-256, NIST P-384 o NIST P-521.
- Cifrado de campo finito (FFC) con tamaños de clave de 3072 bits o más

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

En cualquier caso, se debe garantizar que se cumplen los requisitos de fortaleza mínima definidos en la guía CCN-SIC- 807 Criptología de empleo en el ENS.

5.5 SINCRONIZACIÓN HORARIA

5.5.1 CONFIGURACIÓN DE LA FECHA Y LA HORA DEL SISTEMA

Se debe verificar periódicamente que el reloj del sistema es 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 núcleo. Cuando se apaga el sistema, se vuelven a escribir en el reloj de *hardware*.

Todas las fechas y horas internas utilizadas por el núcleo, 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.

El comando *date* 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 las 13:00 en la zona horaria local:

```
date 050113002004
```

El comando *hwclock* puede consultar y modificar el reloj *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 del *hardware* puede ejecutarse en la hora local o en la hora universal, como indica el ajuste *UTC* del archivo */etc/sysconfig/clock*. El comando siguiente ajusta el reloj de *hardware* a la hora actual UTC:

```
hwclock -u -w
```

Utilice el comando *tzselect* 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*.

5.6 ACTUALIZACIONES

La gestión de *software* del sistema proporcionada por la herramienta *zypper* obtiene una lista de actualizaciones periódicamente de SUSE. La lista se compara con el conjunto instalado de RPM. Si se encuentra una actualización para un RPM instalado, se notifica al administrador.

Durante la instalación, el sistema operativo recibe un certificado que se almacena en la base de datos de RPM. Ese certificado se utiliza para validar cada RPM que se instala. Si falta una firma de un paquete de RPM o hay alguna incorrecta, el paquete no se instalará. El sistema operativo y sus actualizaciones se distribuyen como RPM.

SUSE ofrece un flujo continuo de parches de seguridad de software para su producto, que deben ser instalados para proteger el producto de ataques.

5.7 CONFIGURACIÓN DEL CORTAFUEGOS

Se 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 el comando *iptables*, que utiliza la compatibilidad del núcleo para controlar el tráfico. *iptables* se puede utilizar para configurar reglas de filtrado de paquetes muy reducidas y sencillas. Por otro lado, también se pueden configurar reglas de filtrado muy complejas y sofisticadas para satisfacer las necesidades del administrador. En el capítulo 25 de la guía *SUSE Linux Enterprise Security and Hardening Guide* (Guía de

seguridad y protección de SUSE Linux Enterprise), disponible en [REF2], se incluye una introducción detallada. También, en *iptables* se describe 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 núcleo de Linux. Dado que la función de puente se aplica en la capa *Ethernet*, el núcleo 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 *etables*. La página *man* de *etables* describe el concepto, así como el uso del filtro de paquetes.

5.8 CONFIGURACIÓN DEL PROTECTOR DE PANTALLA

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 habilitado. **Se debe habilitar *screen* ejecutando el guion:**

```
/usr/share/doc/packages/certification-sles-eal4/
```

```
screen-script-screensaver
```

Este guion 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 núcleo. El bloqueo de *screen* se invoca de las siguientes formas:

- 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*.

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

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 sistema operativo. 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. Para inhabilitar el *buffer* de retroceso local se puede utilizar esta entrada de la línea de comandos del núcleo:

```
no-scroll fbcon=scrollback:0
```

Para invocar *screen* automáticamente al entrar a la sesión, se 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
```

5.9 AUDITORÍA

5.9.1 REGISTRO DE EVENTOS

El encargado principal de recoger todos los logs para tener una visión global del sistema en SUSE Enterprise server 15 será la herramienta *Audit*.

El sistema *Audit* de Linux proporciona una forma de rastrear información relevante para la seguridad en su sistema. Según las reglas pre configuradas, *Audit* genera entradas de registro para registrar la mayor cantidad posible de información sobre los eventos que suceden en su sistema. Esta información es crucial en entornos de misión crítica para determinar quién viola las políticas de seguridad y cuáles son las acciones se han realizaron. La auditoría no proporciona seguridad adicional al sistema; más bien, se puede usar para descubrir infracciones de las políticas de seguridad utilizadas en su sistema. Estas violaciones pueden evitarse con medidas de seguridad adicionales como SELinux.

La página *man* de *auditctl* proporciona una descripción de las reglas de auditoría.

5.9.1.1 REGISTRO Y CONTABILIDAD DEL SISTEMA

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* y *klogd*, que pueden configurarse mediante el archivo */etc/syslog.conf*.

La utilidad *logrotate*, 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. Se pueden cambiar los archivos de configuración */etc/logrotate.conf* y */etc/logrotate.d/**, según sea necesario.

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

Archivo Origen

----- + -----

YaST2 Directorio YaST2 para archivos de registro de YaST2

audit.d Directorio para registros de LAF

boot.msg Mensajes del inicio del sistema

lastlog Última entrada correcta (consulte *lastlog*)

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

wtmpt Escrito por el subsistema PAM, consulte *who*

Se recomienda consultar las páginas *man* de *syslog*, *syslog.conf* y *syslogd* para obtener información detallada sobre la configuración de *syslog*.

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

5.9.1.2 CONFIGURACIÓN DEL SUBSISTEMA DE AUDITORÍA

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.

Esto se consigue con dos (2) mecanismos independientes. Todas las llamadas al sistema se interceptan y el núcleo 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.

Se recomienda consultar las páginas *man* de *auditd*, *auditd.conf* y *auditctl* para obtener más información y *audisp-remote* para obtener más información sobre la auditoría remota.

5.9.1.3 USO PREVISTO DEL SUBSISTEMA DE AUDITORÍA

Es necesario tener 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. Se recomienda encontrar un equilibrio entre requisitos de rendimiento y sus necesidades de seguridad a la hora de decidir si se desea utilizar la auditoría y cómo hacerlo.

Se pueden realizar cambios en el conjunto de llamadas al sistema y eventos que se van a auditar. La certificación del sistema operativo requiere que el sistema tenga la capacidad de auditar eventos relevantes para la seguridad, pero depende del usuario elegir cómo desea utilizar estas 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.

El paquete de auditoría proporciona varios archivos de configuración de auditoría sugeridos, por ejemplo, el archivo */usr/share/doc/packages/audit/capp.rules* para los 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 de seguridad, como la reconfiguración del sistema. Se puede copiar uno de los archivos de reglas de ejemplo en `/etc/audit/audit.rules` y modificar la configuración.

SLES genera registros de auditoría con la fecha y la hora del evento, el tipo de evento, la identidad del sujeto (si corresponde) y el resultado (correcto o incorrecto) del evento para los siguientes eventos:

- Inicio de la función de auditoría
- Apagado de la función de auditoría
- Eventos de autenticación
- Uso de eventos de derechos con privilegios/especiales (cambios de seguridad, auditoría y configuración realizados correctamente y que no se han podido realizar)
- Eventos de derivación de funciones o privilegios
- Eventos de archivos y objetos (intentos correctos y no correctos de crear, acceder, suprimir, editar y modificar permisos)
- Eventos de gestión de usuarios y grupos (adición, supresión, modificación, inhabilitación, habilitación y cambio de credenciales correctos y no correctos)
- Intentos de invocación de aplicaciones con argumentos (correctos o incorrectos, por ejemplo, debido a una directiva de restricción de software)
- Eventos de arranque, reinicio y apagado del sistema
- Eventos de carga y descarga del módulo del núcleo
- Eventos de acceso a nivel de administrador o usuario root

5.9.1.4 LECTURA Y BÚSQUEDA DE REGISTROS DE AUDITORÍA

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

Por ejemplo:

busca eventos con un UID de entrada específico

ausearch -ul jdoe

busca eventos por ID de proceso

ausearch -p 4690

Se recomienda consultar la página *man* de *ausearch* para obtener más información.

Se pueden utilizar también otras herramientas como *grep* o lenguajes de guiones como *awk*, *python* o *perl* para analizar más a fondo el archivo de registro de auditoría de texto o la salida generada por la herramienta de bajo nivel *ausearch*.

5.9.1.5 INICIO Y DETENCIÓN DEL SUBSISTEMA DE AUDITORÍA

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, se debe utilizar el comando ***service auditd reload*** para volver a cargar los filtros.

No se debe utilizar la señal *kill* para detener el *daemon* de auditoría, ya que impediría que se apagara correctamente.

Se recomienda añadir el parámetro del núcleo *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. Se recomienda la documentación del cargador de arranque para obtener más información sobre cómo modificar la línea de comandos del núcleo.

5.9.1.6 FIABILIDAD DE LOS DATOS DE AUDITORÍA

Se recomienda 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.

Se 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

Se recomienda consultar la página *man* de *auditctl* para obtener más información acerca de los modos de gestión de fallos.

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

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.

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.

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.

El modo de rendimiento más alto es *flush = none*, pero no se recomienda dado que esto puede provocar la pérdida de registros de auditoría en caso de fallo del sistema.

Para asegurar que *auditd* siempre fuerza una escritura en disco para cada registro, se debe definir la opción ***flush = SYNC*** en */etc/audit/auditd.conf*, pero habrá una reducción significativa del rendimiento y una gran carga en el disco.

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, se puede utilizar una combinación de *flush = INCREMENTAL* y un valor numérico para el parámetro *freq*, por ejemplo:

flush = INCREMENTAL

freq = 100

5.9.1.7 VARIABLES DE CONFIGURACIÓN DEL SISTEMA EN */ETC/SYSCONFIG*

El sistema utiliza varios archivos en */etc/sysconfig* para su configuración. 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 utiliza como entrada para volver a escribir otros archivos de configuración en el sistema.

En la configuración evaluada, no se permiten cambios que requieran ejecutar el comando *SuSEconfig* para volver a escribir otros archivos de configuración.

5.9.2 ALMACENAMIENTO LOCAL

5.9.2.1 ALMACENAMIENTO DE REGISTROS DE AUDITORÍA

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*, que puede ser actualizado en función de las necesidades.

Se recomienda configurar los ajustes del *daemon* de auditoría de forma adecuada; por ejemplo, cambiando la directiva de retención del archivo de registro para que no se supriman nunca los registros de auditoría antiguos con el siguiente ajuste en el archivo */etc/audit/auditd.conf*:

max_log_file_action = KEEP_LOGS

Los ajustes más importantes se refieren a la gestión de 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 el disco u otras condiciones de error. Se pueden 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 auditable si los registros de auditoría no se pueden almacenar.

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. Se pueden eliminar procesos de usuarios utilizando *killall -u*, pero los servicios del sistema no deberían interrumpirse. Dependiendo de la directiva local, puede ser necesario apagar los invitados de KVM. Dado que estos invitados de KVM actúan como procesos normales en el sistema *host* de Linux, se pueden utilizar los mismos comandos para interrumpir esos procesos.

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
```

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.

Se recomienda utilizar una partición dedicada para el directorio `/var/log/audit/` y así asegurarse de que *auditd* tenga control total sobre el uso del espacio en disco sin que otros procesos interfieran.

Se recomienda consultar la página *man* de *auditd.conf* para obtener más información sobre el almacenamiento y la gestión de los registros de auditoría.

5.10 BACKUP

5.10.1 COPIA DE SEGURIDAD Y RESTAURACIÓN

La realización de copias de seguridad debe responder a una política definida y preestablecida que determine claramente:

- Qué información es importante incluir en la copia de seguridad: documentos de usuarios, ficheros de configuración, registros de log, etc. Siempre que se realicen cambios en archivos críticos para la seguridad, puede ser necesario realizar un seguimiento de los cambios realizados y revertir a versiones anteriores.
- Cuál será la política de nombrado de los ficheros de copias de seguridad, para su rápida localización en caso de necesidad. Dicha política debe permitir la rápida localización por parte de los administradores del sistema, pero sin dar excesiva información a alguien externo acerca del contenido de las copias de seguridad.
- La periodicidad de realización de estas copias de seguridad y el modo de copia (total, incremental, etc.).
- El soporte, sistema, localización física, etc. en la que se almacenará la copia de seguridad. Siempre que sea posible, deberán almacenarse dos copias de seguridad, una de fácil acceso para ser utilizada en caso de pérdida de datos, y otra en una localización diferente para prevenir posibles desastres en la localización original de los datos.
- Las medidas de protección a aplicar a cada copia de seguridad: control de integridad, confidencialidad, etc. No hay que olvidar que los datos en las copias de seguridad tienen los mismos requisitos de seguridad que los archivos originales.

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/

Se debe utilizar la opción *--acl* para *tar* si se desea guardar o restaurar las listas de control de acceso (ACL).

Se recomienda también incluir 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. Consultar, para obtener más información, las secciones [5.9.1.1 REGISTRO Y CONTABILIDAD DEL SISTEMA](#) y [5.9.1.2 CONFIGURACIÓN DEL SUBSISTEMA DE AUDITORÍA](#) de esta guía para obtener más información.

5.11 SERVICIOS DE SEGURIDAD

5.11.1 DOCUMENTACIÓN EN LÍNEA

El sistema proporciona una gran cantidad de documentación en línea, normalmente en formato de texto, a través del programa *man* para leer las entradas del manual en línea, por ejemplo:

man ls

man man

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

apropos contraseña

Algunos programas proporcionan información adicional en formato GNU *'texinfo'*. Se puede utilizar el programa *info* para leerla, por ejemplo:

info diff

En los directorios */usr/share/doc/*/* se puede encontrar información adicional, ordenada por paquetes de *software*. Se puede utilizar el paginador *less* para realizar la consulta. Por ejemplo:

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

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

5.11.2 AUTENTICACIÓN

Todos los usuarios deben autenticarse antes de poder acceder al sistema operativo. Cuando el administrador crea una cuenta de usuario, asigna un nombre de usuario y una contraseña por defecto, que son proporcionadas al usuario, junto con las instrucciones para acceder al sistema.

Normalmente, la entrada al sistema se realiza mediante el protocolo Secure Shell (SSH), o bien a través de un terminal en serie. Se puede usar el comando *ssh* para conectarse al sistema. Por ejemplo:

ssh jdoe@172.16.0.1

La página *man* de *ssh* incluye más información sobre las opciones disponibles. Si se necesita transferir archivos de un sistema a otro, se pueden utilizar las herramientas *scp* o *sftp*.

Si es la primera vez que se accede al sistema de destino, este preguntará si se desea aceptar la clave de *host*. Si se conoce previamente la clave del *host* (alguien la ha compartido a través de un canal seguro), entonces **se debe comprobar si la clave del host coincide**. En caso contrario, no debe conectarse al *host*, ya que se está produciendo una posible suplantación de *host*. **Se debe cambiar de inmediato la contraseña asignada inicialmente** con la utilidad *passwd*.

No se debe, bajo ninguna circunstancia, acceder desde un dispositivo no controlado o inseguro. SSH solo puede proteger la información durante el tránsito y no ofrece protección alguna contra un punto final inseguro. Se deberá, por tanto, no dejar información en la pantalla o en un buffer interno al que podría 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) que puede ser extraída por el siguiente usuario, salvo 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, borrar el buffer de retroceso pasado de un terminal virtual a otro y borrar el área de pantalla visible.**

5.11.3 DIRECTIVA DE CONTRASEÑAS

Todos los usuarios, incluidos los administradores, deben asegurarse de que sus contraseñas de autenticación sean seguras y de que se gestionen con las precauciones de seguridad adecuadas.

Se debe cambiar la contraseña inicial definida por el administrador cuando se entre por primera vez al sistema. Para cambiar la contraseña, se puede hacer uso de *passwd*. Primero, se pedirá la contraseña anterior para confirmar su identidad y, a continuación, la contraseña nueva. Pedirá introducir la contraseña nueva dos (2) veces para comprobar que no se ha escrito erróneamente.

El programa *passwd* realizará automáticamente algunas comprobaciones de fortaleza en la contraseña. En cualquier caso, se deben seguir las recomendaciones contenidas en este capítulo. Es decir, los administradores deben asegurarse de que las contraseñas cumplan con la directiva de contraseñas establecida, incluso en los casos en los que no se realice una comprobación automática, como cuando se instala el sistema por primera vez.

Además, el administrador puede cambiar la comprobación automática de contraseñas como se describe en la sección [5.3.2.1 CONFIGURACIÓN DE LA DIRECTIVA DE CONTRASEÑAS](#).

- La contraseña debe tener un mínimo de 12 caracteres.
- Debe contener un carácter de, al menos, tres de las cuatro clases. Las clases de caracteres se definen de la siguiente manera:

Letras minúsculas: *abcdefghijklmnopqrstuvwxyz*

Letras mayúsculas: *ABCDEFGHIJKLMNOPQRSTUVWXYZ*

Dígitos: *0123456789*

Puntuación: *!"#\$%&'()*+,-./:;<=>?[\]^_`{|}~*

- **No se deben utilizar palabra del diccionario**, nombres de personas u otros datos personales, como fechas.
- **No se debe utilizar una cadena alfabética simple**, palíndromos ni combinaciones de teclas adyacentes.
- Cuando se 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.
- **Se debe establecer una caducidad de contraseñas. Estas deben ser actualizadas, como máximo, cada 60 días**. Para esto, puede ser útil el comando *chage* el cual es usado para modificar la información de caducidad de la contraseña de un usuario específica, permite ver la información de antigüedad de la cuenta de un usuario o cambiar el número de días entre los cambios de contraseña y la fecha de la última contraseña.
- La contraseña no debe compartirse con nadie.
- No se debe utilizar la misma contraseña para acceder a ningún sistema bajo administración externa, especialmente 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.
- Se debe actualizar la contraseña si se sospecha que ha podido ser revelada a un tercero.

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;sieed' no es segura; se incluye en un documento"

=> *Lc'9nes;sie1d*

5.11.4 AUTENTICACIÓN BASADA EN CLAVE SSH

La autenticación puede también realizarse a partir de claves SSH. Antes de poder utilizar este método, se deben generar un par de claves. Para ello, se recomienda hacer uso de la utilidad *ssh-keygen*, dado que ha sido el método incluido en la evaluación de seguridad.

Se deben generar pares de claves para SSHv2 mediante el conmutador de línea de comandos *-t rsa* o *-t ecdsa*. La utilidad *ssh-keygen* permite especificar el tamaño de clave RSA, con un valor

por defecto de 2048 bits. Sin embargo, **el tamaño de la clave debe tener, al menos, una longitud de 3072 bits.**

Se 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 debe proteger esta clave con una contraseña codificada mediante ***ssh-keygen***.

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

```
ssh-keygen -t ecdsa -C "Clave de John Doe"
```

El comando solicita una contraseña. Debe proporcionarse una contraseña segura, acorde a los requisitos indicados en el apartado anterior.

Después de generar el par de claves, se puede copiar el archivo de los archivos `~/.ssh/*.pub` al sistema del servidor y añadirlo al archivo `~/.ssh/authorized_keys`. Se debe crear el archivo si no existe y asegurarse de que su permiso impide que otros usuarios accedan a él. Se puede obtener más información en la sección `sshd "AUTHORIZED_KEYS FILE FORMAT"`.

Se destaca que el uso de la autenticación basada en clave no está sujeto al mecanismo de bloqueo de cuenta aplicado para las contraseñas y, además, se debe borrar de forma segura la clave SSH, tal y como se describe en [5.1.9 BORRADO SEGURO](#).

5.11.5 CONTROL DE ACCESO A ARCHIVOS Y DIRECTORIOS

Linux es un sistema operativo multiusuario. Se 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.

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.**

5.11.5.1 CONTROL DE ACCESO DISCRECIONAL

El sistema operativo permite controlar qué otros usuarios podrán leer o modificar 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).

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. **Se debe verificar que el ajuste sea adecuado y nunca se otorgue acceso de escritura a otros usuarios por defecto.** La configuración por defecto es estricta, ya que establece el valor 077 (accesible solo para el propietario).

No se deben configurar áreas de escritura universal en el sistema de archivos. Si se desea compartir archivos de forma controlada con un grupo fijo de otros usuarios (como un grupo de proyecto), el administrador puede crear un grupo de usuarios para ese propósito.

Se deben elegir permisos que coincidan con los objetivos de protección adecuados para el contenido y que correspondan a la directiva de seguridad de la organización. **El acceso a los datos debe realizarse según una base "need-to-know".**

Siempre que se inicie un programa o guion, se ejecutará con los derechos de acceso del usuario. Esto implica que un programa malintencionado podría leer y modificar todos los archivos a los que se tiene acceso. **Nunca se debe ejecutar código de fuentes no fiables y no se deben ejecutar comandos desconocidos.**

Las manipulaciones en el entorno en el que se ejecuta un programa también pueden provocar fallos de seguridad, como la filtración de información. No se deben utilizar las variables de *shell* `LD_LIBRARY_PATH` ni `LD_PRELOAD`, que modifiquen la configuración de la biblioteca compartida utilizada por los programas enlazados dinámicamente.

Se recomienda consultar las páginas *man* de *chmod*, *umask*, *chown*, *chgrp*, *acl*, *getfacl* y *setfacl* para obtener más información.

5.11.6 PROTECTOR DE PANTALLA

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

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, se puede hacer manualmente.

La aplicación *screen* permite dos (2) tipos de bloqueo de pantalla:

- 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*.
- Bloqueo manual ejecutando la combinación de teclas de pantalla *C-a C-x*.

Se puede cambiar el valor de tiempo límite para bloquear la sesión en `~/screenrc` con el valor de *lockscreen*. El administrador puede inhabilitar la capacidad de utilizar el archivo de configuración `~/screenrc`.

Advertencia: si un usuario accede al sistema de forma remota y la función del protector de pantalla se activa, el sistema operativo se asegura de que la sesión esté bloqueada. Sin embargo, es posible que el terminal remoto implemente un buffer de retroceso que no esté bajo control del sistema. 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 sistema operativo. El *buffer* de retroceso local está inhabilitado.

no-scroll fbcon=scrollback:0

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

exec screen

5.12 GESTIÓN DE MÁQUINAS VIRTUALES BASADAS EN EL NÚCLEO (KVM)

Cuando se utiliza SLES como sistema *host* para máquinas virtuales, se usan distintos *UID* y *GID* para separar los distintos usuarios, servicios o máquinas virtuales proporcionados por el sistema. En este caso, se presupone que estos procesos son responsables de la protección de sus datos.

Nota: la configuración evaluada permite que los usuarios normales puedan usar el sistema *host* para el funcionamiento regular al mismo tiempo que se ejecutan las máquinas virtuales. Dependerá de las directivas definidas por el administrador que se permita o no dicho uso dual.

Alojar máquinas virtuales con sistemas operativos invitados aumenta los requisitos de disponibilidad en el sistema *host*. Si no hay sistemas invitados, cuando un sistema falla, procesa sin conexión los servicios que ofrece. Sin embargo, si el sistema tiene varios sistemas invitados y falla, interrumpe los servicios ofrecidos por el *host* y por todos los sistemas invitados alojados. El impacto de esa interrupción es varios órdenes de magnitud mayor. Por lo tanto, debe planificar cuidadosamente la distribución de un sistema *host* para otros sistemas operativos a fin de evitar interrupciones en el servicio que afecten a los objetivos generales de su infraestructura de TI.

En las siguientes secciones se describe la configuración de las máquinas virtuales y sus recursos. Para información general adicional sobre KVM consultar el apartado 4 de [REF1]).

5.12.1 CONFIGURACIÓN *HARDWARE*

Se debe verificar que los mecanismos *hardware* de virtualización están habilitados. Se pueden inhabilitar/habilitar en los ajustes de BIOS. Se recomienda consultar los manuales del *hardware* o preguntar al proveedor para asegurarse de que la compatibilidad con el hardware siguiente está habilitada:

Sistemas basados en Intel x86_64 bits

- La compatibilidad con las extensiones de tecnología de virtualización (VT-x) del procesador debe estar habilitada. Si es así, el comando siguiente devuelve una lista de las capacidades del procesador:

```
cat /proc/cpuinfo | grep vmx
```

- La compatibilidad con las tablas de página mejoradas (EPT) del procesador debe estar habilitada. Si es así, el comando siguiente devuelve una lista de las capacidades del procesador:

```
cat /proc/cpuinfo | grep ept
```

Sistemas basados en AMD Opteron

- La compatibilidad del procesador AMD-V con máquinas virtuales debe estar habilitada. Si es así, el comando siguiente devuelve una lista de las capacidades del procesador:

```
cat /proc/cpuinfo | grep svm
```

- La compatibilidad con tablas de páginas anidadas (NPT) del procesador debe estar habilitada. Si esa así, el comando siguiente devuelve una lista de las capacidades del procesador:

```
cat /proc/cpuinfo | grep npt
```

Sistemas basados en ARM64

Las extensiones de virtualización DE ARM deben estar disponibles.

Sistemas basados en IBM Z System

La virtualización basada en instrucciones de IBM SIE debe estar disponible.

5.12.2 CONFIGURACIÓN DE MÁQUINAS VIRTUALES BASADAS EN EL NÚCLEO (KVM)

La configuración evaluada y certificada permite la administración de máquinas virtuales. Para acceder al *daemon* de gestión *libvirt* y a la consola de una máquina virtual se utiliza SSH.

El *daemon* de gestión de máquinas virtuales *libvirt* permite especificar máquinas virtuales y asignarles recursos. Después de configurar una máquina virtual, este *daemon* también permite iniciar y detener una máquina virtual.

Otro aspecto de *libvirt* es la configuración del sistema *host* y sus recursos que están disponibles para las máquinas virtuales, incluida la configuración de redes y áreas de almacenamiento.

La funcionalidad mencionada para *libvirt* permite a los usuarios definir e iniciar máquinas virtuales. Sin embargo, el acceso a la consola de la máquina virtual se establece por separado. Las instancias de las máquinas virtuales se crean como un proceso de Linux mediante la compatibilidad con la virtualización *QEMU*. *QEMU* emula varios dispositivos para una máquina virtual, incluidos los dispositivos de consola con teclado, ratón y pantalla. Estos dispositivos simulados se convierten en un servidor VNC al que puede conectarse el propietario de la máquina virtual.

El acceso al *daemon* de gestión *libvirt* la instancia del servidor VNC para una máquina virtual por *QEMU* se establece mediante SSH. Las aplicaciones cliente de gestión de máquinas virtuales distribuidas por el *host* se pueden utilizar para acceder tanto al *daemon* de gestión *libvirt* como al servidor VNC. Por ejemplo, las aplicaciones cliente de *virsh* o *virt-manager* permiten el acceso de ambos componentes mediante SSH. Ninguna de estas dos aplicaciones cliente está cubierta por la evaluación.

Los usuarios que gestionan máquinas virtuales y tienen permiso para acceder a los servidores VNC deben tener una cuenta local en el TOE y deben ser miembros del grupo *libvirt*. Estos usuarios no necesitan ningún otro privilegio, como acceso de *root*. Antes de que estos usuarios puedan acceder a *libvirt* y a los servidores VNC, deben autenticarse mediante SSH utilizando sus cuentas. Para acceder al *daemon* de gestión de máquinas virtuales *libvirt* de forma remota mediante SSH, utilice el comando siguiente:

```
virsh connect qemu+ssh://USUARIO@HOST/system
```

Sustituya USUARIO por el ID de usuario con el que desea autenticarse y *HOST* por el nombre de host o dirección IP del sistema que ejecuta el *daemon* de gestión *libvirt*.

Para acceder a *libvirt* de forma local en el sistema TOE, puede utilizar el siguiente comando:

```
virsh connect qemu:///system
```

En este caso, el comando *virsh* accede directamente a los zócalos de dominio Unix proporcionados por *libvirt* en */var/run/libvirt/*.

Para gestionar máquinas virtuales y asignaciones de recursos, consultar la página *man* de *virsh*. Este comando permite administrar máquinas virtuales y sus recursos, así como mantener el ciclo de vida de las máquinas virtuales.

Si es necesario restringir el acceso de los administradores de máquinas virtuales que acceden a *libvirt* de forma remota para que solo lo puedan hacer sin la capacidad de invocar comandos en el *host*, puede añadir las siguientes opciones al archivo *~/.ssh/authorized_keys*. En este archivo, todas las opciones deben encontrarse en una línea justo delante de la clave pública aplicable. Consultar *sshd* para obtener más información sobre las opciones que se deben proporcionar en el archivo *authorized_keys*.

```
no-agent-forwarding,no-pty,no-port-forwarding,no-user-rc,no-X11-forwarding,  
no-agent-forwarding,command="/usr/local/bin/libvirt-access.sh"
```

Además de la configuración anterior, debe generar el archivo */usr/local/bin/libvirt-access.sh* con los permisos de 755 con el siguiente contenido:

```
#!/bin/bash  
if (echo $SSH_ORIGINAL_COMMAND | grep -q "127")  
then  
sh -c nc -q 2>&1 | grep "necesita un argumento" >/dev/null  
if [ $? -eq 0 ]  
then  
CMD="nc -q 0 127.0.0.1 5900"  
else  
CMD="nc 127.0.0.1 5900"  
fi  
eval "$CMD";  
else  
sh -c nc -q 2>&1 | grep "necesita un argumento" >/dev/null  
if [ $? -eq 0 ]  
then  
CMD="nc -q 0 -U /var/run/libvirt/libvirt-sock"  
else  
CMD="nc -U /var/run/libvirt/libvirt-sock"  
fi  
eval "$CMD"  
fi
```

Estas opciones garantizan que solo se pueda abrir el túnel a los zócalos del dominio Unix de *libvirtd* sin provocar ninguna otra operación en el host.

Nota: esta configuración impide que un administrador de la máquina virtual pueda acceder a la consola local. Sin embargo, un administrador de máquina virtual aún puede acceder a cualquier dispositivo si lo desea. Por ejemplo, un administrador de máquina virtual puede asignar todo el disco duro que contiene el sistema host a una máquina virtual. De esa forma, el administrador de la máquina virtual puede leer todo el contenido del espacio de disco del host mediante la funcionalidad de la máquina virtual, omitiendo cualquier DAC u otras restricciones impuestas por el sistema host.

No se permite cambiar la directiva de *AppArmor* que cubre la funcionalidad *sVirt* para separar máquinas virtuales entre sí.

5.12.3 MÁQUINAS VIRTUALES INICIADAS FUERA DE *LIBVIRT*D

En la versión del TOE, solo las instancias de máquinas virtuales creadas con el *daemon* de gestión de máquinas virtuales *libvirtd* están cubiertas por los mecanismos de separación sujetos a evaluación. Las máquinas virtuales PUEDEN iniciarse fuera de *libvirtd* accediendo directamente a */dev/kvm*; por ejemplo, distribuyendo QEMU mediante la línea de comandos. Estas máquinas virtuales tienen los mismos privilegios en el sistema host que el usuario que las inició.

Los usuarios pueden invocar la aplicación QEMU con opciones de línea de comandos similares a las del *daemon libvirtd*. En este caso, se inicia el entorno de virtualización y el sistema operativo invitado puede activarse. Sin embargo, esta forma de puesta en marcha no ofrece ninguna garantía de que la evaluación esté conforme con los CC. En particular, falta la siguiente compatibilidad para las máquinas virtuales, lo que hace que la ejecución de dichas máquinas virtuales sea menos efectiva:

- PUEDE que no se utilice la compatibilidad con la virtualización de hardware, ya que la interfaz del núcleo de Linux que permite al espacio del usuario utilizar la compatibilidad de hardware puede que no sea accesible para los usuarios normales. El archivo de dispositivo */dev/kvm* proporciona acceso a la compatibilidad del hardware.
- El mecanismo de separación entre varias instancias de máquinas virtuales, como se describe en [5.12.6 COMPATIBILIDAD CON SVIRT DE APPARMOR](#), no está configurado ni aplicado.

Para garantizar que se emplean todos los mecanismos de compatibilidad para el funcionamiento correcto y la separación de las máquinas virtuales, las máquinas virtuales deben configurarse y gestionarse mediante el *daemon* de gestión de máquinas virtuales *libvirtd*.

5.12.3.1 INSTANCIAS DE SISTEMA FRENTE A INSTANCIAS DE SESIÓN DE *LIBVIRT*D

El *daemon* de gestión de máquinas virtuales *libvirtd* tiene la capacidad de proporcionar a los usuarios sin privilegios (es decir, a los usuarios que no forman parte del grupo *libvirt*) la posibilidad de gestionar máquinas virtuales. En este escenario, se ejecuta una instancia de *libvirtd* con el ID del usuario. Este modo operativo se denomina modo *session* (de sesión).

Por el contrario, la instancia de *libvirtd* con privilegios que se inició durante el arranque se conoce como instancia *system* (de sistema).

Cuando se conecta a *libvirtd*, el modo operativo al que desea acceder el usuario que se conecta se proporciona junto con el URI. El URI que aparece en [5.12.2 CONFIGURACIÓN DE MÁQUINAS VIRTUALES BASADAS EN EL NÚCLEO \(KVM\)](#) contiene la cadena *system* y, por lo tanto, se conecta a la instancia de *libvirtd* con privilegios.

Las máquinas virtuales iniciadas desde la instancia *session* del *daemon* de gestión de máquinas virtuales *libvirtd* carecen de las mismas capacidades que las que se inician completamente fuera del *daemon libvirtd*. Por lo tanto, las capacidades indicadas en la sección [5.12.3 MÁQUINAS VIRTUALES INICIADAS FUERA DE LIBVIRT](#) tampoco están presentes para las máquinas virtuales que se inician desde una instancia *session* de *libvirtd*.

Todas las capacidades de máquinas virtuales descritas en este documento únicamente se aplican a las máquinas virtuales controladas por instancias *system* de *libvirtd*.

5.12.4 SEPARACIÓN DE MÁQUINAS VIRTUALES

El *daemon* de gestión de máquinas virtuales *libvirtd* garantiza que el entorno de ejecución y los recursos asignados a una máquina virtual específica estén separados de otras instancias de máquinas virtuales, así como del sistema host. Esta configuración transparente ayuda al administrador a mantener una configuración segura para el sistema host y para las máquinas virtuales.

5.12.5 ID DE USUARIO Y GRUPO SIN PRIVILEGIOS

El sistema host protege su funcionamiento frente a las máquinas virtuales ejecutándolas con un ID de usuario y grupo sin privilegios, el ID *qemu*. Este ID de usuario tiene derechos equivalentes a los de los usuarios normales sin privilegios y, por lo tanto, no puede dañar el sistema host, incluso si el sistema operativo invitado fuera capaz de aprovechar cualquier vulnerabilidad en el código de emulación de hardware proporcionado con la aplicación QEMU. El *daemon* de gestión de máquinas virtuales *libvirtd* garantiza que los procesos que implementan el entorno de máquinas virtuales se inician con el ID de usuario y grupo *qemu*. Estos ID se especifican en */etc/libvirt/qemu.conf*.

La opción de configuración que permite el inicio de una máquina virtual con el ID de usuario configurado y la modificación de la propiedad de los recursos del sistema de archivos se encuentra en */etc/libvirt/qemu.conf* estableciendo el valor de configuración *dynamic_ownership* en 1.

5.12.6 COMPATIBILIDAD CON SVIRT DE APPARMOR

Además de la protección frente a las máquinas virtuales, el sistema host utiliza otro mecanismo para garantizar la separación completa entre las máquinas virtuales. Dado que todas las máquinas virtuales se ejecutan con el mismo ID de usuario y el mismo ID de grupo, en teoría es posible que estos procesos de máquina virtual interfieran entre sí. La plantilla de directiva de

AppArmor aplicada con *libvirt* implementa una separación estricta entre las máquinas virtuales y sus recursos.

Si se implementa el mecanismo *sVirt* implementado con el *daemon* de gestión de máquinas virtuales *libvirt*, se genera automáticamente una etiqueta de *AppArmor*. Estas etiquetas de *AppArmor* únicas generadas por *sVirt* se asignan a cada máquina virtual y a sus recursos. Las directivas de *AppArmor* impiden cualquier petición de acceso de una máquina virtual a un recurso que *libvirt* no haya asignado a la máquina virtual. En la configuración evaluada, el *daemon* de gestión de máquinas virtuales *libvirt* deriva automáticamente las etiquetas únicas de *AppArmor* para cada máquina virtual durante el inicio de la máquina virtual.

El proceso de la máquina virtual recibe su etiqueta de *AppArmor* cuando *libvirt* invoca la máquina virtual.

Encontrará más información sobre el etiquetado dinámico en <http://libvirt.org/drvqemu.html#securitysvirt>.

5.12.7 USO COMPARTIDO DE RECURSOS

La función *sVirt* descrita en la sección [5.12.6 COMPATIBILIDAD CON SVIRT DE APPARMOR](#) garantiza que las máquinas virtuales estén aisladas unas de otras. Este aislamiento cubre los recursos utilizados por las máquinas virtuales, como los dispositivos USB o PCI asignados a las máquinas virtuales, los *backends* del disco, etc. Los perfiles de *AppArmor* solo permiten el acceso a los dispositivos configurados a los que hacen referencia los objetos del sistema de archivos, como los archivos de dispositivo o los archivos normales, y deniegan el acceso a cualquier otro dispositivo.

El administrador de la máquina virtual puede asignar el mismo archivo de dispositivo o de *backend* de disco a varias máquinas virtuales. Este tipo de uso compartido de recursos es lo deseable. Por ejemplo, si una imagen ISO se va a asignar a varias máquinas virtuales como *backend* de CD-ROM. Por ejemplo, si se van a instalar varias máquinas virtuales que ejecutan SLES15, se puede asignar una imagen ISO de instalación de SLES15 a todas estas máquinas virtuales al mismo tiempo. Otros ejemplos incluyen las configuraciones de alta disponibilidad en las que se debe configurar un dispositivo de disco compartido común.

La función *sVirt* permite asignar así un recurso a varias máquinas virtuales infringiendo la directiva de aislamiento. Los administradores de máquinas virtuales deben prever que el aislamiento de la máquina virtual no se aplica a estos recursos compartidos.

Si una máquina virtual debe estar completamente aislada de otras máquinas virtuales, el administrador de la máquina virtual debe asegurarse de que todos los dispositivos y los recursos de *backend* de disco asignados a esta máquina virtual totalmente aislada no se compartan con otras máquinas virtuales.

Tenga en cuenta que los archivos de *backend* de disco PUEDEN asignarse a máquinas virtuales en modo de solo lectura. En ese caso, el perfil de *AppArmor* solo permite el acceso de lectura y deniega el acceso de escritura al archivo de *backend* de disco. Este modo de solo lectura se utiliza normalmente para imágenes ISO configuradas como dispositivos de CD-ROM para máquinas virtuales.

5.12.8 CONSIDERACIONES SOBRE CONECTIVIDAD

Las máquinas virtuales PUEDEN configurarse con una o más interfaces de red. El *daemon* de gestión de máquinas virtuales *libvirt* permite configurar las funciones de red de las máquinas virtuales.

Se deben configurar dos aspectos para establecer la conectividad de red para las máquinas virtuales:

- *Libvirt* debe configurarse con una o más redes. Cada configuración de red da como resultado una configuración automatizada de una interfaz de red de puente en el sistema host. A esa interfaz de puente se le asigna una interfaz de red física en el host. Para lograr la separación entre estas redes, cada red debe estar asignada a una interfaz de red física individual.
- Debe asignarse cada configuración de red de máquina virtual para que pertenezca a una red definida para *libvirt*. Con este enlace, la máquina virtual pasa a formar parte del puente definido para la interfaz de red.

Se puede considerar que un puente de red proporcionado con el sistema host se parece a un conmutador de red. Cada miembro del puente puede comunicarse directamente entre sí. Por lo tanto, si se necesita configurar máquinas virtuales que no deben comunicarse entre sí, se deben especificar redes independientes con *libvirt*. Estas redes deben tener asignadas diferentes interfaces de red físicas en el host. Las interfaces de red de las máquinas virtuales que se aislarán deben tener asignadas redes diferentes.

Cuando *libvirt* crea una instancia de una máquina virtual, configura un dispositivo TAP conectado al puente para el que la máquina virtual configurada tiene acceso. El *daemon* de gestión de máquinas virtuales *libvirt* transfiere el descriptor de archivo de ese dispositivo TAP al proceso QEMU, ya que el QEMU sin privilegios no tiene permiso para abrir el dispositivo TAP. Con este descriptor de archivo, el proceso de la máquina virtual ahora puede implementar todos los protocolos de red a partir de la capa 2 de OSI.

Dado que *libvirt* proporciona a los procesos de máquina virtual un dispositivo TAP a la interfaz de puente del sistema *host*, una máquina virtual puede generar comunicación Ethernet completa, incluida la detección de la red o la saturación de datos. Esto implica que, aunque el sistema host aísla completamente las máquinas virtuales del sistema host, así como entre sí, las máquinas virtuales tienen las mismas capacidades de red para la red asignada que los sistemas completos conectados a la misma red. Por lo tanto, el software invitado que se ejecuta en las máquinas virtuales debe ser tan fiable como los equipos físicos individuales de la misma red. KVM no puede impedir que un software invitado malicioso haga un mal uso del acceso a las redes a las que puede acceder, y tampoco está diseñado para ello.

5.12.8.1 ASIGNACIÓN DE DISPOSITIVOS

Además de la compatibilidad con el *daemon* de gestión *libvirt*, KVM permite asignar dispositivos PCI y USB a máquinas virtuales para su uso exclusivo. Solo se puede usar este mecanismo para asignar un dispositivo a una máquina virtual.

En las siguientes secciones se describen los mecanismos de asignación de dispositivos por separado para dispositivos PCI y USB.

5.12.8.2 ASIGNACIÓN DE DISPOSITIVOS PCI

NO se debe configurar la asignación de dispositivos PCI, ya que se considera que no es segura en entornos seguros.

5.12.8.3 ASIGNACIÓN DE DISPOSITIVOS USB

A diferencia de la asignación de dispositivos PCI, para asignar dispositivos USB no se requieren consideraciones especiales. Si se asigna un dispositivo USB a una máquina virtual, el acceso se realiza mediante QEMU a través del archivo de dispositivo USB. Para restringir los permisos de acceso en el archivo de dispositivo USB se usa *libvirtd*. Para ello, se modifica la propiedad del archivo de dispositivo y su permiso de acceso de *AppArmor*, de modo que solo la máquina virtual que tiene acceso al dispositivo puede acceder al archivo de dispositivo.

ADVERTENCIA: ni el *daemon* de gestión *libvirtd* ni la funcionalidad KVM implementan restricción alguna sobre qué dispositivos USB se puedan asignar a una máquina virtual. Los administradores de las máquinas virtuales pueden asignar cualquier dispositivo que aparezca en la salida *lsusb* a una máquina virtual. Esto incluye los dispositivos que necesita el sistema host. Los administradores de las máquinas virtuales tienen la capacidad de interrumpir el funcionamiento del host. La configuración evaluada no impone ninguna restricción sobre los dispositivos USB que se asignan a las máquinas virtuales. Esto proporciona al administrador de las máquinas virtuales total flexibilidad a la hora de configurar la asignación de dispositivos USB. Sin embargo, el administrador debe tener mucho cuidado con los dispositivos USB asignados.

5.12.8.4 GESTIÓN DEL ESPACIO EN DISCO

La configuración evaluada permite a los administradores de máquinas virtuales configurar varios *backends* de almacenamiento que se pasan a las máquinas virtuales como dispositivos de disco. Se permiten todas las configuraciones ofrecidas por *libvirtd*.

6. FASE DE OPERACIÓN

6.1 REVISIÓN DE LA CONFIGURACIÓN DEL SISTEMA

Se recomienda revisar periódicamente la configuración del sistema para verificar si aún coincide con la configuración evaluada. Esto afecta principalmente a los procesos que pueden ejecutarse con privilegios de usuario *root*.

Los permisos de los archivos de dispositivo */dev/** no deben modificarse.

En concreto, se deben revisar 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/*
```

Se debe usar el comando lastlog para detectar patrones de entrada a la sesión inusuales y verificar 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. DESARROLLADORES DE APLICACIONES

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 siguientes recomendaciones de 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

8. CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Instalación en un entorno seguro	☐	☐	
Registro de los equipos	☐	☐	
Registro de las licencias	☐	☐	
Actualización de <i>firmware</i>	☐	☐	
Instalación	☐	☐	
Instalación de RPM Adicional	☐	☐	
Configuración inicial: GRUB	☐	☐	
Configuración inicial: Contraseña segura para Root	☐	☐	
Configuración inicial: Aplicación de la configuración evaluada	☐	☐	
Configuración inicial: Configuración de cifrado	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Modo de Operación seguro activado (FIPS-CC)	☐	☐	
Securización de los Parámetros del Kernel	☐	☐	
Uso de SUDO	☐	☐	
Programación de procesos mediante CRON	☐	☐	
Protección de las particiones	☐	☐	
Creación de usuarios	☐	☐	
Eliminación de usuarios	☐	☐	
Definición de cuentas administrativas	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
Configuración de La Directiva de Contraseñas	☐	☐	
Configuración de <i>Openssh</i>	☐	☐	
Sincronización Horaria	☐	☐	
Configuración del cortafuegos	☐	☐	
Configuración del protector de pantalla	☐	☐	
Configuración del sistema de auditoria	☐	☐	
Configuración de máquinas virtuales	☐	☐	

9. REFERENCIAS

[REF1] Guía de configuración evaluada de Criterios Comunes para SUSE LINUX Enterprise Server 15 SP2

<https://links.imagerelay.com/cdn/3404/ql/816857783fe246caa4e56360c7da38bc/common-criteria-evaluated-configuration-guide-for-suse-linux-enterprise-server-15-sp2-niap.pdf>

[REF2] Guía de SUSE Linux Enterprise Server:

<https://documentation.suse.com/sles/15-SP2/>

10.ABREVIATURAS

ACL	<i>Access Control List</i>
AES	<i>Advanced Encryption Standard</i>
CC	<i>Common Criteria</i>
CTR	<i>AES Counter Mode</i>
DHCP	<i>Dynamic Host Configuration Protocol</i>
DNS	<i>Domain Name System</i>
ECC	<i>Elliptical Curve</i>
ENS	<i>Esquema Nacional de Seguridad.</i>
FAQ	<i>Frequently Asked Questions</i>
FS	<i>Filesystem</i>
FTP	<i>File Transfer Protocol</i>
GID	<i>Group ID</i>
GRUB	<i>Grand Unified Boot loader</i>
HMC	<i>Hardware Management Console</i>
IPC	<i>Interprocess Communication</i>
ISO	<i>ISO9660 – a disc image format</i>
KVM	<i>Linux Kernel-based Virtual Machine</i>
LPAR	<i>Logical Partition</i>
LUKS	<i>Linux Unified Key Setup</i>
NTP	<i>Network Time Protocol</i>
PAM	<i>Linux Pluggable Authentication Modules</i>
PES	<i>Procedimiento de Empleo Seguro</i>
QEMU	<i>Open Source Emulator</i>
RPM	<i>RPM Package Manager</i>
SGID	<i>Set Groud ID on execution</i>
SLES	<i>SUSE LINUX Enterprise Server</i>
SSH	<i>Secure Shell</i>
SUID	<i>Set User ID on execution</i>
SYSV	<i>System V</i>
UID	<i>User ID</i>
UTC	<i>Coordinated Universal Time</i>
VM	<i>Virtual Machine - Máquina virtual</i>
WAN	<i>Wide Area Network</i>

XTS*AES XTS block mode*

