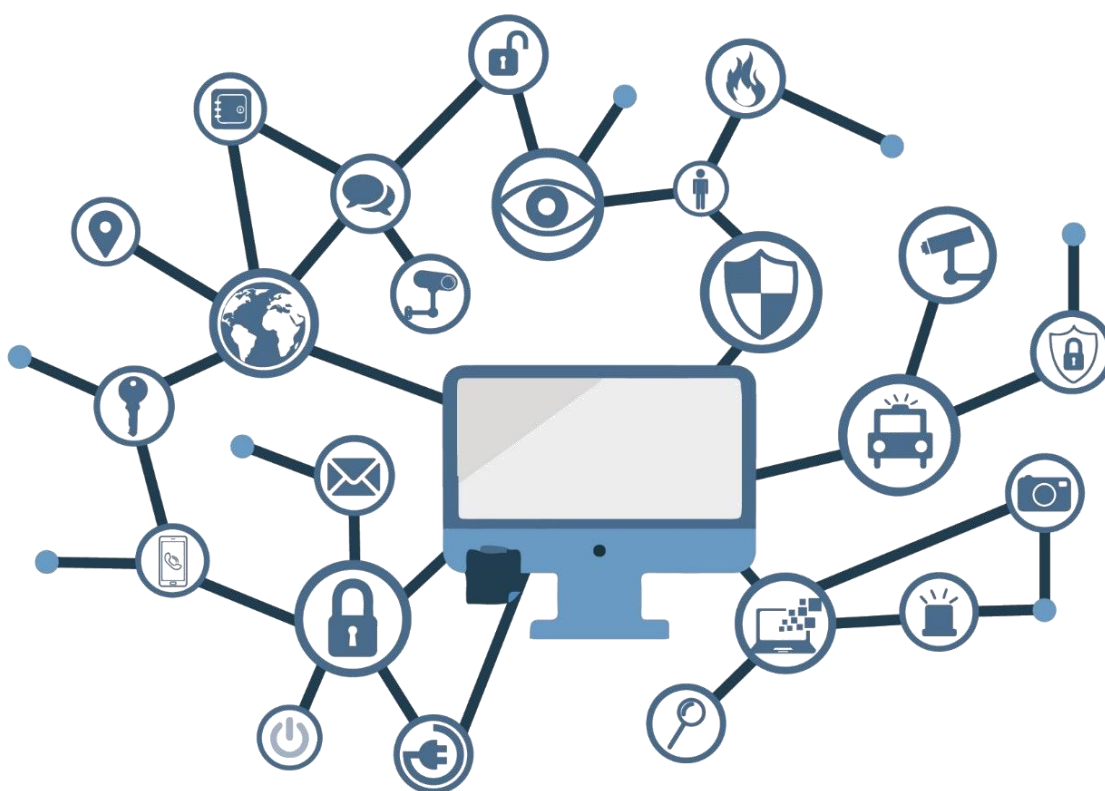


Guía de Seguridad de las TIC

IMPLEMENTACIÓN DE SEGURIDAD SOBRE SUSE LINUX ENTERPRISE 12 (SERVIDOR INDEPENDIENTE)



ABRIL 2019

Edita:



© Centro Criptológico Nacional, 2019

NIPO: 083-19-155-8

Fecha de Edición: abril de 2019

La Jefatura de Servicios Técnicos y CIS del Ejército del Aire, junto con las empresas Sellcom Solutions y Sidertia Solutions S.L. han participado en la realización del presente documento, siendo esta última, la que ha realizado los anexos y la modificación del documento original.

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.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

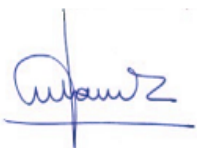
Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, actualizado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

abril de 2019



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL	6
2. INTRODUCCIÓN	6
3. OBJETO	6
4. ALCANCE	7
5. DESCRIPCIÓN DEL USO DE ESTA GUÍA.....	8
5.1 AVISOS IMPORTANTES A LOS USUARIOS DE ESTA GUÍA	8
5.2 ESTRUCTURA DE LA GUÍA	10
6. SUSE LINUX ENTERPRISE SERVER 12 (SP3)	10
6.1 INSTALACIÓN	10
6.1.1 DEFINICIÓN DE TÉRMINOS	11
6.1.2 DESTINO DE LA INSTALACIÓN	12
6.1.3 MÉTODOS DE INSTALACIÓN	12
6.1.4 REQUISITOS DE ESPACIO EN DISCO	13
6.2 SEGURIDAD INICIAL	13
6.2.1 CONFIGURACIÓN DE CONTRASEÑAS	13
6.2.2 PARTICIONADO Y SISTEMA DE ARCHIVOS	14
6.2.3 CONFIGURACIÓN INICIAL	16
6.2.4 PROTECCIÓN DEL SISTEMA	17
6.2.4.1 PROTECCIÓN DE LAS PARTICIONES	17
6.2.4.2 CONFIGURACIÓN SEGURA DE RED	19
6.2.4.3 CONFIGURACIÓN SEGURA DE PARÁMETROS DEL KERNEL	20
6.2.4.4 CONFIGURACIÓN DE TCP-WRAPPERS	21
6.2.5 LIMITACIÓN DE RECURSOS DE USUARIO	21
6.2.5.1 BLOQUEAR LA GENERACIÓN DE VOLCADOS DE MEMORIA	22
6.2.5.2 LÍMITE DE LOS RECURSOS DISPONIBLES PARA CADA USUARIO	22
6.2.5.3 BLOQUEAR EL USO DE ATAJOES CRÍTICOS.....	22
6.2.5.4 ESTABLECIMIENTO DE CUOTAS DE DISCO	22
6.2.6 LIMITE DE ACCESO AL SISTEMA.....	23
6.2.6.1 CONTROL DE INFORMACIÓN DIVULGADA POR EL SISTEMA	23
6.2.6.2 CONFIGURACIÓN SEGURA DE SSH	23
6.2.6.3 MÓDULOS PAM DE AUTENTICACIÓN	23
6.2.6.4 LÍMITES DE INTENTO DE ACCESO AL SISTEMA	24
6.2.6.5 LÍMITE DE SERVICIOS DEL SISTEMA	24
6.2.7 ELEMENTOS INNECESARIOS DEL SISTEMA	25
6.2.7.1 PAQUETES INNECESARIOS	25

6.2.7.2	USUARIOS INNECESARIOS.....	25
6.2.8	PERMISOS Y VARIABLES DE ENTORNO.....	26
6.2.8.1	FICHEROS DE CONFIGURACIÓN	26
6.2.8.2	DIRECTORIO DE USUARIOS	26
6.2.8.3	PERMISOS EN FICHEROS Y DIRECTORIOS IMPORTANTES.....	26
6.3	SISTEMA.....	27
6.3.1	ACTUALIZACIÓN DEL SISTEMA	27
6.3.1.1	ONLINE	27
6.3.1.2	OFFLINE	27
6.3.2	SISTEMA Y SERVICIOS	27
6.3.3	ADMINISTRACIÓN DE RECURSOS	28
6.3.4	ALMACENAMIENTO.....	30
6.3.5	SISTEMA DE ARCHIVOS.....	30
6.3.6	ADMINISTRACIÓN Y MANTENIMIENTO	31
6.3.6.1	AUTOMATIZACIÓN DE TAREAS	31
6.3.6.2	LOGS DE SISTEMA	32
6.3.6.3	CONTROL DE INTEGRIDAD DE HARDWARE	32
6.3.6.4	CONTROL DE DISPOSITIVOS EXTRAIBLES	33
6.3.6.5	COPIAS DE SEGURIDAD	33
7.	NUEVAS FUNCIONALIDADES Y PRINCIPALES CAMBIOS	33
7.1	ESCRITORIO.....	34
7.2	SEGURIDAD	34
7.2.1	APPARMOR.....	35
7.2.2	INSTALACIÓN O ELIMINACIÓN DE SOFTWARE.....	35
7.2.3	MANTENIMIENTO DEL SISTEMA ACTUALIZADO	36
7.3	INTEROPERABILIDAD Y SOPORTE DE HARDWARE.....	37
7.4	CONFIGURACIÓN DE SUSEFIREWALL2.....	37

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. INTRODUCCIÓN

Este documento forma parte del conjunto de normas desarrolladas por el Centro Criptológico Nacional para entornos basados en los productos y sistemas operativos de Linux (CCN STIC 600), siendo de aplicación para la Administración pública en el cumplimiento del Esquema Nacional de Seguridad (ENS) y de obligado cumplimiento para los sistemas que manejen información clasificada nacional.

3. OBJETO

El presente documento contiene una guía para la configuración segura del sistema operativo SUSE "*Software und Systementwicklung*" (Desarrollo de Sistemas y de Software) Enterprise Linux 12, en máquinas en las que posteriormente se instala aplicaciones que requieren un nivel óptimo de seguridad.

La configuración deberá realizarse en máquinas con el sistema operativo recién instalado, si bien también se deben llevar a cabo periódicamente sobre cualquier máquina para comprobar el estado de seguridad de la misma. En un anexo final se incluye un cuadro con cada uno de los chequeos que deben realizarse.

Para manejar información clasificada, la única versión del sistema operativo permitida es SUSE Enterprise server 12 SP3.

La configuración que se aplica a través de la presente guía se ha diseñado para ser lo más restrictiva posible, minimizando la superficie de ataque y, por lo tanto, los riesgos que pudieran existir. En algunos casos y dependiendo de la funcionalidad requerida del servidor, podría ser necesario modificar la configuración, que aquí se plantea, para permitir que el equipo proporcione los servicios adicionales.

No obstante, se tiene en consideración que los ámbitos de aplicación son muy variados y por lo tanto dependerán de su aplicación, las peculiaridades y funcionalidades de los servicios prestados por las diferentes organizaciones. Las plantillas y normas de seguridad se han generado definiendo unas pautas generales de seguridad que permitan el cumplimiento de los mínimos establecidos en el ENS y las condiciones de seguridad necesarias en un entorno clasificado.

4. ALCANCE

La guía se ha elaborado para proporcionar información específica con objeto de asegurar un servidor con el sistema operativo “SUSE Linux Enterprise Server”, instalado en español en su versión 12 (SP3). Se incluyen, además, operaciones básicas de administración para la aplicación de las mismas, así como una serie de recomendaciones para su uso.

El escenario en el cual está basada la presente guía tiene las siguientes características:

- a) Implementación del ENS en un escenario con servidores independientes con el sistema SUSE Linux Enterprise Server 12.
- b) Implementación de plantillas de seguridad en función de los niveles de seguridad establecidos en el ENS para servidores SUSE Linux Enterprise Server 12 independientes.
- c) Implementación de seguridad en un escenario de red clasificada servidores independientes SUSE Linux Enterprise Server 12 (SP3).

Este documento incluye:

- a) **Descripción de versiones** para todos aquellos operadores que tengan experiencia en versiones previas, se proporciona la información sobre las diferentes opciones y versiones de las que dispone el sistema.
- d) **Descripción de las nuevas funcionalidades** para todos aquellos operadores que tengan experiencia en las versiones anteriores de SUSE Linux Enterprise Server, se incluyen las nuevas características del producto.
- e) **Funcionalidades de seguridad local adicionales.** Completa descripción de aquellas características y servicios que, no encontrándose definidos por defecto, agregan seguridad adicional a una infraestructura de SUSE Linux Enterprise Server 12 como servidor independiente.
- f) **Mecanismos para la implementación de la solución.** Se incorporan mecanismos para la implementación de la solución de forma automatizada.
- g) **Mecanismos para la aplicación de configuraciones.** Se incorporan mecanismos para la implementación de forma automática de las configuraciones de seguridad.
- h) **Guía paso a paso.** Va a permitir implantar y establecer las configuraciones de seguridad en servidores SUSE Linux Enterprise Server independientes.
- i) **Lista de comprobación.** Permitirá verificar el grado de cumplimiento de los equipos servidor con respecto a las condiciones de seguridad que se establecen en esta guía.
- j) **Configuración de cifrado de disco.** Establece los mecanismos para la configuración del cifrado que aporta SUSE Linux Enterprise Server 12.
- k) **Solucionarios adicionales.** Guías paso a paso para la comprobación de la configuración de operativas sobre el puesto de trabajo.

5. DESCRIPCIÓN DEL USO DE ESTA GUÍA

Para entender esta guía de seguridad, es conveniente explicar el proceso de securización que describe y los recursos que proporciona. Este proceso constará de los siguientes pasos:

- a) Implementación de un escenario con servidor SUSE Linux Enterprise Server independiente.
- b) Deberá implementar la presente guía en función del entorno que requiera su organización.

5.1 AVISOS IMPORTANTES A LOS USUARIOS DE ESTA GUÍA

Los contenidos de esta guía son de aplicación a equipos tipo servidor con Sistema Operativo SUSE Linux Enterprise Server 12 en castellano, con el objetivo de reducir la superficie de exposición a ataques posibles con una instalación por defecto, manteniendo los principios de máxima seguridad, mínima exposición y servicios y mínimos privilegios que emanan de la CCN-STIC-301. En el caso de llevar a cabo la aplicación de esta guía sobre el Sistema Operativo con una configuración de idioma diferente al castellano, es posible que deba incorporar nuevos recursos y/o realizar ciertas modificaciones sobre los recursos que se adjuntan con este documento para permitir la correcta aplicación y uso del documento.

Para los entornos de ENS se podrá utilizar la versión de SUSE Linux Enterprise Server 12, con la opción de instalación deseada, que más se adapte a las necesidades de cada organización.

En un entorno de red clasificada donde se maneja información clasificada la única versión autorizada del Sistema Operativo SUSE Linux Enterprise Server 12 con la opción de instalación "Sistema por Defecto".

Las imágenes LiveCD y LiveDVD contienen un sistema de archivos comprimido de arranque, creado por un conjunto de scripts personalizados utilizan un archivo de configuración kickstart. Estas imágenes en vivo también se pueden instalar en el disco duro, obteniendo así una instalación de SUSE Linux Enterprise Server totalmente funcional. El conjunto de paquetes instalados de esa manera en un disco duro no se puede ajustar durante la instalación, ya que es una transferencia simple de la imagen existente en CD / DVD a un disco duro. Después de arrancar desde el disco duro, Zypper puede usarse para agregar o eliminar paquetes.

La guía ha sido desarrollada y probada en entorno de uso de servicios Linux con la versión de SUSE Linux Enterprise Server 12 (SP3).

La guía de seguridad ha sido elaborada utilizando un laboratorio basado en una plataforma de virtualización tipo Hyper-V sobre Windows Server 2012 R2 Datacenter con las siguientes características técnicas:

- a) Servidor Dell PowerEdge™ T320:
 - i. Intel Pentium Xeon CPU E5 2430 2.20GHz.
 - ii. HDD 1 TB.
 - iii. 64 GB de RAM.
 - iv. Interfaz de Red 1 Gbit/s.

Esta guía de seguridad no funcionará con hardware que no cumpla con los requisitos de seguridad mínimos de SUSE Linux Enterprise Server 12. Esto quiere decir que se requieren equipos con procesadores Intel o AMD de 64 o 32 bits (x64 o i386), con más de 512 MiB de memoria RAM ambas versiones.

Se aconseja, no obstante, por seguridad y rendimiento, la implementación de versiones de 64 bits frente a las de 32 bits.

La versión SUSE Linux Enterprise Server 12 tiene ciertas limitaciones de arquitectura que se expresan en el siguiente cuadro.

SUSE 12 (SP3)	x86_64	s390x	ppc64le
CPU bits	64	64	64
Máximas CPUs lógicas	8192	256	2048
Máxima memoria RAM (teórica/certificada)	> 1 PiB/64 TiB	4 TiB/256 GiB	1 PiB/64 TiB
usuarios/espaciokernel máximo	128 TiB/128 TiB	ϕ/ϕ	2 TiB/2 EiB
Capacidad swap máxima	29 * 64 GB	30 * 64 GB	
Procesos máximos	1048576		
Hilos máximos por proceso	El límite máximo depende de la memoria y de otros parámetros (testado con más de 120000).		
Máximo tamaño por bloque de dispositivo	Hasta 8 EiB en todas las arquitecturas de 64 bits		
FD_SETSIZE	1024		

Nota: Puede comprobar los requisitos del sistema de SUSE Linux Enterprise Server 12 en el siguiente enlace.

https://www.suse.com/releasenotes/x86_64/SUSE-SLES/12/#TechInfo.Kernel

La guía ha sido desarrollada con el objetivo de dotar a las infraestructuras con la seguridad adecuada dependiendo del entorno sobre el que se aplique. Es posible que algunas de las funcionalidades esperadas hayan sido desactivadas y, por lo tanto, pueda ser necesario aplicar acciones adicionales para habilitar servicios, demonios o características deseadas.

Para garantizar la seguridad de los puestos de trabajo, deberán instalarse las actualizaciones de seguridad recomendadas por el fabricante, disponibles a través del servicio “zypper patch --category security”. Hay que tener en cuenta que las actualizaciones de arquitecturas cruzadas, como actualizar de una versión 32 bits de SUSE Linux Enterprise Server a la versión 64 bits, o actualizar de big-endian a little-endian, no se admiten, así mismo, hay que tener presente que determinadas actualizaciones por su criticidad pueden ser liberadas en cualquier momento. Se deberá tener en cuenta la implementación de las actualizaciones tanto para el sistema operativo como para los diferentes servicios instalados. En líneas posteriores de la presente guía se tratarán las consideraciones oportunas.

Dependiendo de la naturaleza de estas actualizaciones, el lector podrá encontrarse con algunas diferencias respecto a lo descrito en esta guía. Esto viene motivado por los cambios que, en ocasiones, se realizan para las distintas actualizaciones de seguridad.

Antes de aplicar esta guía en producción, deberá asegurarse el hecho de haber probado su configuración y comportamiento en un entorno aislado y controlado, en el cual se habrán aplicado las pruebas y posteriores cambios en la configuración que se ajusten a los criterios específicos de cada organización.

Si estuviera aplicando la presente configuración de seguridad en un sistema ya configurado con una versión previa de esta guía, tenga en cuenta los cambios personalizados que hubiera realizado. La aplicación nuevamente

de la seguridad a través de los paso a paso correspondientes, puede implicar que tenga que ajustar de nuevo los valores que ya hubiera personalizado.

El espíritu de estas guías no está dirigido a remplazar políticas consolidadas y probadas de las organizaciones sino a servir como línea base de seguridad. Esta línea deberá ser adaptada a las necesidades propias de cada organización.

5.2 ESTRUCTURA DE LA GUÍA

Esta guía dispone de una estructura que diferencia la implementación del sistema SUSE Linux Enterprise Server dependiendo del entorno sobre el que vaya a ser aplicado, así como una diferenciación de la versión a utilizar.

La guía dispone de las siguientes configuraciones divididas en dos grandes anexos, los cuales se definen a continuación:

- a) **Anexo A:** En este anexo se define la configuración necesaria para adaptar los sistemas SUSE Linux Enterprise Server 12 (SP3) a las necesidades requeridas por el Esquema Nacional de Seguridad (ENS).
- b) **Anexo B:** En este anexo se define la configuración necesaria para adaptar los sistemas SUSE Linux Enterprise Server 12 (SP3) a las necesidades requeridas en los entornos clasificados.

Cabe remarcar que en sus respectivos anexos se dotara de la información necesaria y concreta para cada tipo de implementación.

6. SUSE LINUX ENTERPRISE SERVER 12 (SP3)

La versión Enterprise Server 12 (SP3) de SUSE incorpora nuevas funcionalidades con respecto a sus antecesoras.

Se enumerarán y se dará una breve descripción sobre las mismas, completando, posteriormente, con un detalle más significativo de aquellos elementos más críticos. No obstante, se debe tener en consideración que algunas de las funcionalidades y/o componentes citados no se encontrarán disponibles por defecto en la instalación o bien se encontrarán deshabilitados o limitados con las funcionalidades de seguridad que se aplican tras la fortificación del sistema a través de la presente guía.

Se describen a continuación las partes del sistema que hacen de SUSE Linux Enterprise Server 12 (SP3) la distribución más idónea para entornos clasificados y ENS.

- a) **Estabilidad.** SUSE® se desarrolla de forma continua con el fin de ofrecer la plataforma perfecta para el software más reciente. En este proceso no se pierde de vista al aspecto de la compatibilidad con las aplicaciones más antiguas. Cada paso en el desarrollo orientado al futuro siempre se hace pensando en garantizar la estabilidad de los componentes activos. Además, este sistema convence con un gran rendimiento en cuanto a la virtualización (basada en KVM o máquina virtual basada en el núcleo) y con una alta disponibilidad.
- b) **Seguridad.** SUSE® presenta un amplio historial en materia de seguridad de TI para sistemas operativos de Linux y ofrece un amplio paquete de seguridad para SUSE® Linux Enterprise Server que protege los sistemas frente a todo tipo de incidentes de seguridad.
- c) **Ciclos largos de mantenimiento y soporte.** SUSE® se ha ocupado de las directrices para el periodo de soporte técnico: Parches y herramientas para mejorar la seguridad y el cumplimiento normativo y hasta 5 años de asistencia en los paquetes de servicio además de un ciclo de vida de 13 años.

6.1 INSTALACIÓN

Para asegurarse de que el sistema funcionará sin errores, emplee siempre hardware certificado. El proceso de certificación de hardware es continuo y la base de datos correspondiente se actualiza con regularidad.

Nota: Consulte el formulario de búsqueda de hardware certificado en:
<http://www.suse.com/yessearch/Search.jsp>

SUSE Linux Enterprise Server proporciona una amplia variedad de servicios. La mayor parte de las configuraciones necesarias se pueden definir con YaST, la utilidad de configuración de SUSE. Además, los numerosos procesos de configuración y manuales necesarios se describen de manera más extendida en el siguiente enlace:

<https://www.suse.com/es-es/documentation/sles-12/index.html>

6.1.1 DEFINICIÓN DE TÉRMINOS

- a) **Repositorio.** Directorio local o remoto que contiene paquetes, actualizaciones de sistema y aplicaciones que se instalan a través de gestores, para mantener actualizado el sistema y su software.
- b) **Alias/Nombre del repositorio.** Un nombre breve para el repositorio (denominado Alias en Zypper y Nombre del repositorio en YaST). El usuario puede seleccionarlo al añadir el repositorio, sin olvidar que el nombre debe ser exclusivo.
- c) **Archivos de descripción del repositorio.** Cada repositorio proporciona archivos que describen su contenido (nombres de paquetes, versiones, etc.). Estos archivos de descripción de los repositorios se descargan a un caché local que utiliza YaST.
- d) **Producto.** Representa un producto completo, por ejemplo, SUSE® Linux Enterprise Server.
- e) **Patrón.** Un patrón es un grupo instalable de paquetes dedicado a un fin concreto. Por ejemplo, el patrón Portátil contiene todos los paquetes necesarios en un entorno informático móvil. Los patrones definen las dependencias de paquetes (como los paquetes necesarios o recomendados) y vienen con una selección previa de paquetes marcados para su instalación. Esto garantiza que los paquetes más importantes necesarios para un fin concreto estén disponibles en el sistema una vez instalado el patrón. Sin embargo, no es necesario que todos los paquetes de un patrón estén preseleccionados para la instalación. Puede seleccionar o deseleccionar manualmente los paquetes de un patrón según sus necesidades y preferencias.
- f) **Paquete.** Un paquete es un archivo comprimido en formato rpm que contiene los archivos de un programa concreto.
- g) **Parche.** Un parche está formado por uno o más paquetes y puede aplicarse mediante paquetes RPM delta. También puede introducir dependencias de paquetes que aún no estén instalados.
- h) **Resolución.** Término genérico con el que se hace referencia a los productos, patrones, paquetes o parches. El tipo de resolución que más se utiliza es el paquete o el parche.
- i) **RPM delta.** Un paquete RPM delta está compuesto únicamente por los archivos binarios que no tienen en común dos versiones definidas de un mismo paquete, por lo que presenta el tamaño de descarga más pequeño. Antes de la instalación, el paquete RPM completo se reconstruye en el equipo local.
- j) **Dependencias de paquetes.** Ciertos paquetes dependen de otros, por ejemplo, las bibliotecas compartidas. En otras palabras, un paquete puede requerir otros paquetes. Si los paquetes necesarios no están disponibles, no es posible instalar el paquete. Además de las dependencias (requisitos de paquetes) que deben cumplirse, algunos paquetes recomiendan otros paquetes. Estos paquetes recomendados solo se instalan si están realmente disponibles. De lo contrario, se hace caso omiso de ellos y el paquete que los recomienda se instala de todos modos.

6.1.2 DESTINO DE LA INSTALACIÓN

La mayoría de instalaciones se realizan en un disco duro local. Por lo tanto, es necesario que los controladores de disco duro estén disponibles para el sistema de instalación. Si un controlador especial, como un controlador RAID, necesita un módulo de núcleo adicional, proporcione un disco de actualización de módulos del núcleo al sistema de instalación.

Otros destinos de instalación pueden ser de varios tipos de dispositivos de bloques que proporcionen el suficiente espacio en disco y la velocidad necesaria para ejecutar un sistema operativo. Esto incluye los dispositivos de bloques de red como iSCSI o SAN.

6.1.3 MÉTODOS DE INSTALACIÓN

SUSE Linux Enterprise Server ofrece varios métodos para controlar la instalación:

- a) Instalación en la consola
- b) Instalación mediante la consola en serie
- c) Instalación con AutoYaST
- d) Instalación con imágenes KIWI
- e) Instalación mediante SSH
- f) Instalación con VNC

Por defecto, se utiliza la consola gráfica. Si desea realizar la instalación en muchos equipos similares, conviene crear un archivo de configuración de AutoYaST o una imagen de precarga de KIWI y hacer que estén disponibles para el proceso de instalación.

6.1.4 REQUISITOS DE ESPACIO EN DISCO

Los requisitos del disco duro dependen en gran medida de la instalación. Por lo general, se necesita más espacio del que requiere el software de instalación en sí para que el sistema funcione correctamente. Los requisitos mínimos para las distintas combinaciones posibles son:

CAPACIDAD	TIPO DE INSTALACIÓN
3.5 GB	Instalación por defecto
4 GB	Recomendado más de 4Gb (con escritorio gráfico, paquetes de desarrollo y Java).

6.2 SEGURIDAD INICIAL

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.

Las contraseñas son las llaves del sistema. Deben ser lo más seguras posibles para evitar inicios de sesión no autorizados, que es el primer paso hacia problemas de seguridad mayores. El uso de contraseñas lo suficientemente fuertes como para amortizar un ataque es un paso decisivo y a la vez sencillo que ahorrará muchos problemas en el futuro.

6.2.1 CONFIGURACIÓN DE CONTRASEÑAS

Muchas contraseñas utilizadas por usuarios son bastante fáciles de adivinar. SUSE Linux Enterprise Server 12 proporciona diferentes maneras de proveer autenticación al sistema, incluyendo contraseñas encriptadas con el comando **crypt**, las contraseñas **shadow**, **Kerberos**... Etc. En cualquier situación en la cual se elija una contraseña como parte de un esquema de autenticación, la seguridad de ese esquema estará por lo menos parcialmente a la merced de la complejidad de la contraseña elegida.

Una contraseña segura tiene que tener al menos estas características:

- Tener una longitud mínima de 8 caracteres.
- Mayúsculas y minúsculas alternadas.
- Tantos signos de puntuación y números como sea posible.
- Evitar palabras o frases comunes que puedan figurar en cualquier diccionario.
- No tener relación evidente con datos personales del usuario: Nombre, fecha de nacimiento, etc.

Otro factor a tener en cuenta es la **caducidad de contraseñas**. Dentro de las tareas frecuentes que se realizan en Linux, se encuentra la de administrador de cuentas de usuario, tanto en su creación y edición, como en establecimiento o modificación de la caducidad y el vencimiento de las contraseñas de los usuarios, siendo política de seguridad modificar regularmente la misma.

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.

En esta guía se configurará de manera permanente una caducidad de contraseña para nuevos usuarios y modificará la política de seguridad de los usuarios ya existentes para que cumplan estos requisitos de seguridad establecidos. Las recomendaciones de configuración en cuanto a la caducidad de las contraseñas se configurarán en el fichero **/etc/login.defs** y serán las siguientes:

- a) El periodo máximo durante el que se puede mantener una contraseña será de 60 días.
- b) La longitud mínima de la contraseña será de 8 caracteres.
- c) El período mínimo durante el que se debe mantener una contraseña será de 15 días.
- d) El período durante el que el sistema avisará de una futura caducidad de la contraseña será de 15 días.

6.2.2 PARTICIONADO Y SISTEMA DE ARCHIVOS

Se debe establecer la cantidad y tamaño de las particiones, así como el sistema de archivos a utilizar. Aunque estos factores dependen en gran medida del uso que se vaya a hacer del sistema, se van a dar una serie de recomendaciones para ayudar a su correcta elección.

Para realizar una correcta elección del sistema de archivos hay que tener en cuenta los tipos de archivos más comunes que existen en Linux.

Se optará por elegir **XFS** como sistema de archivos recomendado excepto en el punto de montaje "/" que se utilizará Btrfs.

Sistema de archivos	Sistema operativo	Descripción
FAT	Heredado	Sistema de archivos heredado que se ha adoptado universalmente. FAT12, FAT16 y FAT32.
Ext2	Linux	El segundo Filesystem: Sigla de "Extended Graphics Array" utilizado por muchas distribuciones Linux.
Ext3	Linux	El tercero Filesystem: Se añadió registro diario (journaling), utilizado por muchas distribuciones Linux.
Ext4	Linux	El cuarto Filesystem: utilizado por muchas distribuciones Linux. "Extiende los límites de almacenamiento."
JFS	Linux	Journalized File System: fue introducido por IBM y aún se admite, pero ha sido sustituido por Ext4.
XFS	Linux/Red-HAT	Sistema de archivos de 64 Bits, actualmente opción por defecto en Red Hat.
ReiserFS	Linux/SUSE	Se trataba de un formato de archivo que estaba en uso en varias distribuciones, pero ha sido reemplazado por Ext3.
Btrfs	Linux/SUSE	CentOS/Red-Hat tienen soporte para este sistema de archivos, SUSE ofrece este sistema por defecto , recomendándolo para particiones críticas del sistema.

A continuación, Se muestra una organización de las particiones como ejemplo, siendo viables alternativas en función de los usos del sistema.

PARTICIÓN	TAMAÑO
/	50 GB Btrfs
/home	20 GB XFS
/var	10 GB XFS
/var/log	10 GB XFS
/var/log/audit	10 GB XFS
/opt	20 GB XFS
/srv	25 GB XFS
/usr/local	25 GB XFS
/boot	1 GB XFS
/tmp	10 GB XFS
SWAP	½ Memoria total del servidor

Inicialmente se recomienda cifrar las particiones aumentando la seguridad de la misma e impidiendo que personal no autorizado pueda acceder a datos críticos.

Hay que tener en cuenta que la elección del sistema de archivos Btrfs conlleva conocer ciertas particularidades y funcionalidades, las cuales, se nombran a continuación:

- a) Es posible crear instantáneas de subvolumenes Btrfs, ya sea manual o automáticamente a partir de eventos del sistema. Por ejemplo, al realizar cambios en el sistema de archivos, zypper invoca al comando snapper para crear instantáneas antes y después del cambio. Esto resulta útil si no queda satisfecho con el cambio que ha realizado zypper y quiere volver al estado anterior. Como el comando snapper invocado por zypper crea las instantáneas por defecto en el sistema de archivos raíz, es buena idea excluir ciertos directorios de las instantáneas. Por eso YaST sugiere crear los siguientes subvolumenes independientes.
 - i. **/boot/grub2/i386-pc, /boot/grub2/x86_64-efi, /boot/grub2/powerpc-ieee1275, /boot/grub2/s390x-emu**

Nota: No se admite la reversión de la configuración del cargador de arranque. Los directorios mostrados anteriormente son específicos de la arquitectura. Los dos primeros directorios están presentes en equipos AMD64 e Intel 64, los dos últimos en IBM POWER y IBM z Systems, respectivamente.

- ii. **/home:** Si /home no se encuentra en una partición independiente, se excluye para evitar la pérdida de datos cuando se produce una reversión.
- iii. **/opt, /var/opt:** Normalmente, los productos de otros fabricantes se instalan en /opt. Se excluye para evitar la desinstalación de estas aplicaciones cuando se produce una reversión.
- iv. **/srv:** Contiene datos de los servidores Web y FTP. Se excluye para evitar la pérdida de datos cuando se produce una reversión.
- v. **/tmp, /var/tmp, /var/cache, /var/crash:** Todos los directorios que contienen archivos temporales y cachés se excluyen de las instantáneas.
- vi. **/usr/local:** Este directorio se usa cuando se instala manualmente el software. Se excluye para evitar la desinstalación de estas instalaciones cuando se produce una reversión.

- vii. **/var/lib/libvirt/images:** La ubicación por defecto de las imágenes de máquina virtual gestionadas con libvirt. Se excluye para garantizar que las imágenes de máquina virtual no se sustituyen con las versiones anteriores durante una operación de reversión. Por defecto, este subvolumen se crea con la opción sin copia al escribir.
- viii. **/var/lib/mailman, /var/spool:** Para evitar la pérdida de correos después de una operación de reversión, los directorios que contienen mensajes de correo o colas de correo se excluyen.
- ix. **/var/lib/named:** Contiene datos de la zona para el servidor DNS. Se excluye de las instantáneas para garantizar que un servidor de nombres pueda funcionar tras una operación de reversión.
- x. **/var/lib/mariadb, /var/lib/mysql, /var/lib/pgqsl:** Estos directorios contienen datos de la base de datos. Por defecto, estos subvolúmenes se crean con la opción sin copia al escribir.
- xi. **/var/log:** Ubicación del archivo de registro. Se excluye de las instantáneas para permitir el análisis del archivo de registro después de la restauración de un sistema dañado.

Nota: Dado que las instantáneas guardadas requieren más espacio en disco, se recomienda reservar suficiente espacio para Btrfs. El tamaño recomendado para una partición Btrfs raíz con los subvolúmenes por defecto es de 20GB.

6.2.3 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, aplicando los pasos de esta guía que se describirán posteriormente conseguiremos:
 - i. Bloquear el acceso a la línea de comandos del Grub.
 - ii. Bloquear la posibilidad de edición de las entradas del Grub.
 - iii. Bloquear la posibilidad de ejecución de todas las entradas del Grub.
- 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.
- 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.
- 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.** Utilice 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.

6.2.4 PROTECCIÓN DEL SISTEMA

En la actualidad, al menos en algún momento, Importantes organizaciones, tanto públicas como privadas, han sufrido ataques a sus sistemas informáticos. Estos ciberataques no sólo afectan a ciertas compañías, sino que pueden llegar a afectar a la seguridad nacional.

Por esta y por muchas razones es prioritario proteger cualquier sistema que tenga cierta criticidad. Esta parte se centrará en la protección de las partes más vulnerables del sistema, evitando dejar configuraciones por defecto y permisos innecesarios.

6.2.4.1 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.
 - i. Se montará con las opciones **noauto, noexec, nodev, nosuid, ro**.
- b) **/boot/efi.** Contiene información sobre el arranque del sistema UEFI.
 - i. Se montará con los siguientes parámetros **umask=0077, shortname=winnt <dump> 0 <pass> 0**.
- c) **/usr y /opt:** Contienen ficheros ejecutables del sistema.
 - i. Se montará con las opciones **nodev, ro**.
- d) **/var:** Contiene archivos muy variables del sistema (logs, BBDD, contenido web, etc.)
 - i. Se montará con las opciones **defaults, nosuid**.
- e) **/var/log:** Contiene los logs del sistema.

- i. Se montará con las opciones **nodev, noexec, nosuid, rw**.
- f) **/var/log/audit**: Contiene información y logs de la herramienta Audit.
 - i. Se montará con las opciones **nodev, noexec, nosuid, rw**.
- g) **/var/www**: Contiene principalmente el contenido Web.
 - i. Se montará con las opciones **nodev, noexec, nosuid, rw**.
- h) **/home y /tmp**: Contienen los archivos del usuario y los temporales del sistema.
 - i. 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.
 - i. Se montará con las opciones **noauto, nodev, nosuid, rw**.
- j) **/**: Contiene la partición raíz del sistema.
 - i. 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.
 - i. 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: <dump> - 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 <dump>.

<pass> - 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 en <pass>.

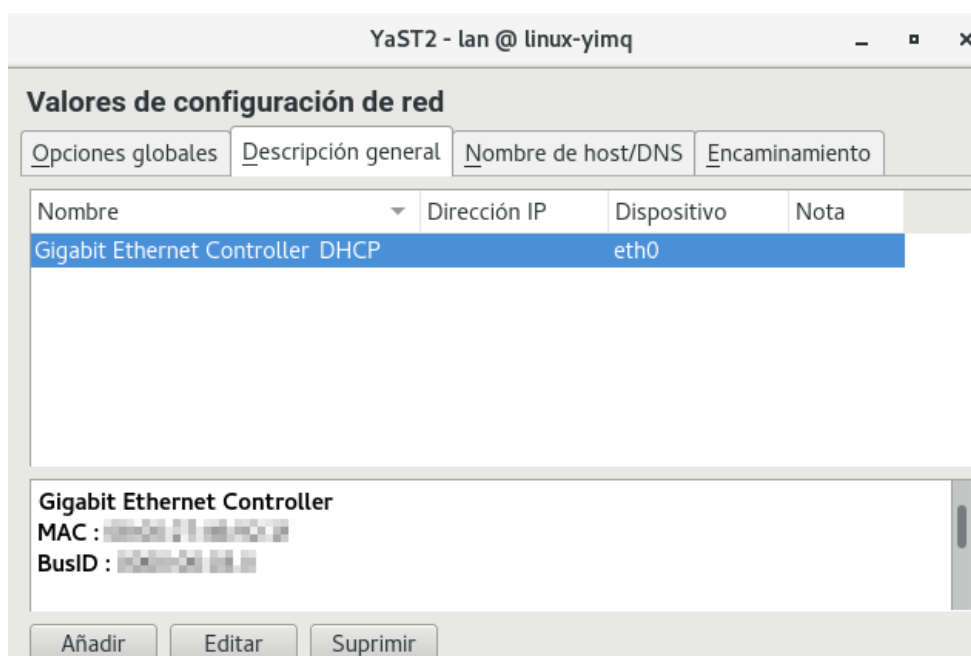
Una vez realizadas todas las modificaciones debe quedar el fichero **/etc/fstab** de esta manera:

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

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

6.2.4.2 CONFIGURACIÓN SEGURA DE RED

Siempre que sea posible deberá configurarse la red de forma estática, asignando direcciones IP de forma manual a cada sistema en lugar de utilizar los protocolos DHCP o BOOTP. Para ello podrá utilizarse el asistente **YaST** o se podrán realizar manualmente los cambios en los ficheros **/etc/sysconfig/network-scripts/ifcfg-enpXXX** (configuración de los interfaces), y **/etc/resolv.conf** (servidores de resolución de nombres).



Es recomendable deshabilitar ciertos protocolos que pueden afectar a la vulnerabilidad del sistema y que están orientados a usuarios sin conocimientos de administración de redes, uno de estos protocolos es el protocolo **Zeroconf**.

Zeroconf o APIPA (Automatic Private Ip Address), es un protocolo que se encarga de la asignación automática por parte del sistema operativo de una ip tipo 169.254.X.X con máscara 255.255.0.0. De éste modo, dos equipos sin configuración de red, podrían comunicarse entre sí por medio de este protocolo.

Del mismo modo, el protocolo de enrutamiento **IPv6** está diseñado para resolver muchos de los problemas que se producen en la versión actual del conjunto de protocolo de Internet (conocido como IPv4) en relación con el agotamiento de direcciones, la configuración automática, la extensibilidad, etc. Este protocolo debe de ser desactivado en caso de que no sea necesaria su utilización para el buen funcionamiento de la red.

Al igual que el protocolo **RPC** (Remote Procedure Call) para IPv6 debe ser deshabilitado si no se contempla administración remota del sistema por medio de redes IPv6.

Para prevenir ataques a las posibles vulnerabilidades en la implementación de algunos protocolos de la pila de red de Linux (dccp, sctp, rds, tipc) se añaden archivos **.conf** al directorio **/etc/modprobe.d** para que se ejecute la shell **/bin/false** en lugar de cargar el módulo del protocolo indicado.

6.2.4.3 CONFIGURACIÓN SEGURA DE PARÁMETROS DEL KERNEL

El kernel Linux permite modificar una gran cantidad de parámetros sin necesidad de volverlo a compilar. Estos parámetros afectan al funcionamiento del sistema en mayor o menor medida así que conviene tener conocimiento de cómo modificarlos. El comando **sysctl** suele ser la forma más común de hacerlo. Los valores se almacenan en el directorio **/proc/sys**.

Hay que tener en cuenta que cuando se modifican los parámetros del kernel vía **sysctl** los cambios surten efecto al instante, pero estos cambios se perderán en el momento que el equipo se reinicie, por eso conviene guardar los cambios en el fichero de configuración de sysctl **/etc/sysctl.conf**.

En esta guía se verá como configurar el sistema con ciertos parámetros que afectan a la seguridad ya sea directa o indirectamente.

- a) **No responder a peticiones icmp.** Los mensajes ICMP pueden ser utilizados por atacantes remotos, ya sea para identificar ciertas máquinas activas o para intentar explotar las debilidades del protocolo ICMP. Este se ha diseñado para comunicaciones unidireccionales que no requieren autenticación, lo cual habilita a los atacantes a desencadenar ataques DoS o ataques que brindan acceso a los paquetes entrantes y salientes a individuos desautorizados como pueden ser ataques por flujo de ping, por flujo ICMP_ECHO y ataques "smurf".
- b) **No responder a peticiones broadcast.** Cuando una máquina envía un paquete a la dirección de broadcast (por ejemplo, 192.168.1.255), éste es entregado a todas las máquinas existentes en la red local. A continuación, todas las máquinas deben enviar un mensaje ECHO del protocolo ICMP. Esto puede provocar una congestión de la red, a la vez que permite determinar que sistemas están activos en la red.
- c) **Deshabilitar source routing.** El source routing (o encaminamiento en origen) es una funcionalidad propia del protocolo IP que permite enviar dentro del mismo paquete de datos la información necesaria para su enrutamiento, es decir, la dirección IP de cada uno de los dispositivos de red intermedios que deben cruzarse hasta llegar al destino final. Esto permite al emisor de un paquete dictar la ruta por la que deberá transmitirse a lo largo de la red. Esta característica presenta un grave riesgo de seguridad. De hecho, la mayoría de los routers ignoran ya por defecto esta opción.
- d) **Protegerse ante ataques tcp syn.** El "ataque SYN" (también denominado "inundación TCP/SYN") consiste en saturar el tráfico de la red aprovechando el mecanismo de negociación de tres vías del protocolo TCP comenzando varias veces el proceso de establecimiento de conexión a una máquina, sin llegar a completarlo.
- e) **Deshabilitar la redirección icmp.** Si un host envía un paquete por una ruta no válida, los routers utilizarán los mensajes de redireccionamiento ICMP para informarle a los hosts en el link de datos que está disponible una ruta mejor para el destino en particular. Dicho mensaje origina que el host modifique sus tablas de enrutamiento. Sin embargo, si un atacante tiene la capacidad de enviar este tipo de mensajes de redirección, podría modificar las tablas de enrutamiento a voluntad, pudiendo conseguir que todo su tráfico saliente se enrutara a otra máquina controlada por el atacante. Por lo tanto, y a pesar de las ventajas que supone en sí mismo este tipo de redirección, podría ser interesante ignorarla a fin de evitar una posible vía de ataque.
- f) **Deshabilitar la redirección ip.** La redirección IP se refiere a la capacidad que dispone un sistema de varias interfaces de conexión a distintas subredes, de recibir por una los paquetes destinados a cualquier otra. Este comportamiento es correcto en equipos o dispositivos que actúen como routers o cortafuegos, pero no en un equipo ordinario.

- g) **Ignorar los mensajes de error mal formados.** El protocolo ICMP, dispone de mensajes de error para notificar alguna situación anormal en la red. Sin embargo, esta característica se puede utilizar para atacar a los equipos, ya que se les puede inducir a pensar que la red está en un estado distinto al real. En muchas ocasiones, un mensaje de error mal formado indica que se está cometiendo un ataque.
- h) **Protección frente a ip spoofing.** Esta protección impide que el sistema sea utilizado para el envío de paquetes IP cuya dirección de destino sea inválida, lo que puede ser indicativo de que se está cometiendo un ataque con el fin de saturar los recursos de comunicación suplantando una dirección IP válida.
- i) **Logging de actividades sospechosas.** Mediante esta protección se consigue que el sistema anote en sus registros (logs) la ocurrencia de paquetes con dirección IP inválida (conocido como ataque “IP spoofing”), paquetes que indiquen cambios de rutas (por ejemplo, por haberse activado en el origen el “source routing”) y la ocurrencia de otros paquetes anormales o excepcionales.
- j) **Protección frente a buffer overflow.** ASLR (Address Space Layout Randomization) es una técnica de seguridad implicada en la protección de los ataques de desbordamiento de la pila.
- k) **Bloqueo IPv6.** En la mayoría de las distribuciones *Linux* es común que *IPv6* venga configurado por defecto. Sin embargo, no son muchos los usuarios que, aun teniendo esta configuración, hagan uso de alguna aplicación o servicio sobre *IPv6*, al menos conscientemente. Sus equipos pueden cambiar el modo de trabajo a *IPv6* en cualquier momento, haciendo que sea víctima de algún ataque de red que afecte a *IPv6*, como algo similar al ARP-Spoofing, pero con paquetes ICMPv6 spoofeados que realizan aplicaciones como *insane6*, *parasite6* o *Scapy*, a un ataque de Rogue DHCPv6 que configure un servicio de DNS o una puerta de enlace maliciosa o a un ataque de Man in the middle por medio del protocolo SLAAC.
- l) **Activar la protección “DEFRAGGING”.** Esta protección se debería aplicar en equipos que actúen como Gateway y que se dediquen a enmascarar tráfico interno (conocido como “IP-masquerading”). A través de este parámetro se le permitiría dividir los paquetes que lo atraviesan, a fin de evitar un consumo excesivo de recursos.

6.2.4.4 CONFIGURACIÓN DE TCP-WRAPPERS

Para restringir un servicio a pesar de que éste esté abierto, de forma que sólo las máquinas que deban usarlo puedan acceder se emplearán los TCP-wrapper. SUSE Linux Enterprise Server 12 (SP3) ya tiene instalado el TCP-wrapper, pero está sin configurar y permite el acceso a todos los usuarios. Su configuración es muy sencilla, consta de dos archivos que están en el directorio **/etc: hosts.allow** y **hosts.deny**.

- a) Dentro del archivo **/etc/hosts.allow** se indicará los equipos que tienen permiso para acceder a nuestros servicios.
- b) Dentro del archivo **/etc/hosts.deny** se indicará los equipos que no tienen permiso para acceder a nuestros servicios.

La sintaxis es la siguiente: **<demonio>:<equipo o grupo de equipos>**. En un principio, se denegará el acceso a todos los equipos, para después otorgárselo a los que sea necesario. Para ello en el **/etc/hosts.deny** se indicará **'ALL : ALL'**, lo que deniega todo lo que no se permita explícitamente en el fichero **hosts.allow**.

A continuación, en el archivo **/etc/hosts.allow** se otorgarán permiso a todos aquellos equipos que lo requieran. Posteriormente se explicará más detalladamente y con ejemplos ilustrativos la manera más segura de configurar los ficheros anteriores.

6.2.5 LIMITACIÓN DE RECURSOS DE USUARIO

Con el fin de limitar los recursos que puede utilizar un usuario en el sistema y las acciones que los programas que ejecuta pueden llevar a cabo, es necesario aplicar ciertas configuraciones.

6.2.5.1 BLOQUEAR LA GENERACIÓN DE VOLCADOS DE MEMORIA

Para prevenir la creación de volcados de memoria (core dumps) de programas que abortan su ejecución (ya que esta información puede revelar datos confidenciales, y únicamente tiene valor para desarrolladores), se limitará **soft - core** y **hard - core** a 0.

6.2.5.2 LÍMITE DE LOS RECURSOS DISPONIBLES PARA CADA USUARIO

Se debe limitar la cantidad de **procesos** que un usuario puede tener simultáneamente en el sistema. Del mismo modo se debe limitar la cantidad de **memoria** residente de la que hace uso un usuario. Además de los límites anteriores, se debe limitar las **conexiones** simultáneas al sistema que cada usuario puede realizar. Todos estos parámetros se configuran en el siguiente fichero de configuración **/etc/security/limits.conf**.

Por último, hay que limitar la cantidad de hilos concurrentes que se ejecutan en el sistema, evitando que cualquier programa que se ejecute aumente hasta provocar una denegación de servicio, esta configuración se realizará en **/etc/sysctl.conf**.

6.2.5.3 BLOQUEAR EL USO DE ATAJO CRÍTICOS

Para prevenir reinicios del sistema no deseados al utilizar la combinación de teclas **Ctrl-Alt-Supr**, se debe deshabilitar. Para distribuciones de GNU/Linux que utilizan **Systemd** como sistema de gestión de tareas y servicios durante el inicio, el comportamiento de teclas Ctrl-Alt-Supr se determina por un enlace simbólico denominado **/usr/lib/systemd/system/ctrl-alt-del.target** que apunta hacia el archivo **reboot.target**, localizado dentro del mismo directorio. Del mismo modo se deshabilitará el reinicio a usuarios no autorizados, por medio de las herramientas que implementa Gnome3.

6.2.5.4 ESTABLECIMIENTO DE CUOTAS DE DISCO

El uso de cuotas de disco permite limitar la cantidad de espacio en disco que utiliza un usuario. La diferencia respecto a los sistemas de archivos extendidos (extended file system o ext) es que XFS requiere habilitar las cuotas a través del parámetro de kernel "rootflags" en tiempo de arranque (boot). Se debe entonces añadir el parámetro de kernel en la configuración de grub. La variable que contiene los parámetros es "GRUB_CMDLINE_LINUX".

Una vez activada la característica, se debe de asignar parámetros de cuotas a la partición que se requiera limitar por usuarios, comúnmente se suele asignar cuotas a la partición **/home**, puesto que en ella suelen estar los archivos personales de cada usuario.

6.2.6 LIMITE DE ACCESO AL SISTEMA

Esta guía se basa en la asunción de que no puede haber ningún sistema perfecto, libre de bugs o errores. Dado que cada entorno cuenta con millones de líneas de código e interacciones software/hardware. Un error crítico en cualquiera de estas interacciones puede ser suficiente para que un software malicioso pueda tomar el control de un sistema.

Por esto mismo se debe limitar al máximo los accesos al sistema, así como los permisos, evitando en la medida de lo posible los automatismos y las posibles formas de intrusión. Reduciendo las consecuencias e incluso previniendo los problemas legales.

6.2.6.1 CONTROL DE INFORMACIÓN DIVULGADA POR EL SISTEMA

Ciertos ficheros del sistema contienen información que se muestra a los usuarios que intentan acceder al sistema. Esta información deberá revisarse para comprobar que no se está divulgando información confidencial. Así mismo, se sustituirá esa información por avisos legales previniendo las consecuencias del acceso no autorizado al sistema.

6.2.6.2 CONFIGURACIÓN SEGURA DE SSH

Para evitar el uso de versiones inseguras del protocolo SSH se comprobará que la configuración del cliente SSH fuerza la versión 2 del protocolo modificando en el fichero de configuración `/etc/ssh/ssh_config` la línea correspondiente al protocolo. Por parte del servidor de SSH se requerirán más directrices que se configurarán en el fichero de configuración `/etc/ssh/sshd_config`.

- a) Se forzará el uso de la versión 2 del protocolo.
- b) Se denegará el uso de aplicaciones gráficas de modo remoto por medio de X11.
- c) Se configurarán los usuarios no administradores como acceso denegado.
- d) Se limitará el tiempo total para hacer login en 120 segundos.
- e) Se establecerá el tiempo mínimo de inactividad antes de la desconexión.
- f) SSH puede emular el comportamiento del comando rsh obsoleto al permitir a los usuarios habilitar el acceso inseguro a sus cuentas a través de archivos `.rhosts`. por lo que se procederá a eliminar este comportamiento.
- g) La autenticación criptográfica basada en host de SSH es más segura que la autenticación `.rhosts`. Sin embargo, no se recomienda que los hosts confíen unilateralmente entre sí, incluso dentro de una organización. Por lo que se procederá a eliminar esta característica.
- h) Se denegarán los inicios de sesión root por medio de SSH.
- i) Se denegarán los accesos por medio de usuarios sin contraseña.
- j) Se configurará correctamente un banner que disuada a los posibles atacantes.
- k) Se garantizará que los usuarios no puedan usar variables de entorno al demonio SSH.
- l) Se configurará el uso únicamente del protocolo SSH con los algoritmos de cifrado permitidos.

6.2.6.3 MÓDULOS PAM DE AUTENTICACIÓN

Los administradores de sistemas de una organización deben decidir cuánto acceso administrativo se les otorga a los usuarios dentro de la organización a sus máquinas. A través de un módulo PAM llamado **pam_console.so**, se permiten algunas actividades normalmente reservadas para superusuarios, tales como el reinicio o el montaje de medios removibles, al primer usuario que se conecte en la consola física. Sin embargo, otras tareas importantes de administración de sistemas, tales como la modificación de las configuraciones de la red, configurar un nuevo ratón

o montar dispositivos de red, son imposibles sin privilegios administrativos. En consecuencia, los administradores deben decidir cuánto acceso administrativo deberían recibir los usuarios en su sistema.

En el siguiente apartado se definen las acciones recomendadas para el módulo "**pam_tally2.so**":

- a) Se contabilizarán los intentos fallidos de acceso o cambio de privilegios mediante "su".
- b) Se bloquearán aquellas cuentas que superen 5 intentos fallidos.
- c) Para evitar que la cuenta root se bloquee intencionadamente se fijará manualmente un máximo de intentos fallidos.
- d) Se recordarán las 7 últimas contraseñas utilizadas por cada usuario y no permitirá su repetición.
- e) Se limitará el acceso de usuarios wheel a cuentas administrativas.

6.2.6.4 LÍMITES DE INTENTO DE ACCESO AL SISTEMA

En este apartado se configurarán limitaciones al sistema mediante el componente shadow-utils, evitando ataques por fuerza bruta y logrando tener un mayor control sobre los intentos de acceso al mismo.

Hay que tener en cuenta que los parámetros que se configurarán en el archivo de configuración **/etc/login.defs** controlan el comportamiento de las herramientas del componente **shadow-utils**. Ninguna de estas herramientas utiliza el mecanismo PAM, y las utilidades que usan PAM (como el comando **passwd**) deben configurarse en lugar correspondiente.

Se procederá a seguir las siguientes recomendaciones:

- a) Número máximo de intentos de acceso fallidos conste de 3 intentos.
- b) El tiempo máximo permitido para acceder al sistema sea de 60 segundos.
- c) Evitar que el sistema indique cuando el usuario es desconocido para el mismo.
- d) El tiempo de retardo tras un intento fallido será de 10 segundos.
- e) Se registrarán los intentos fallidos de acceso al sistema.

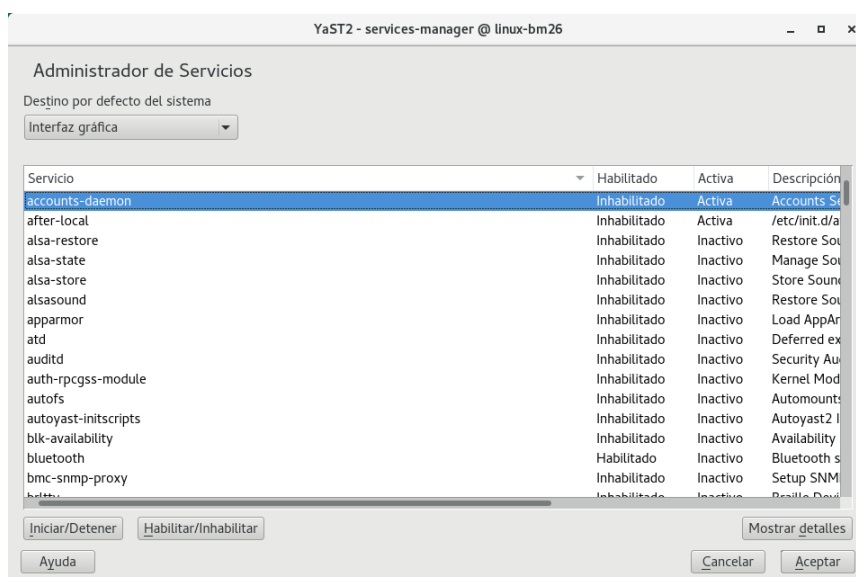
6.2.6.5 LÍMITE DE SERVICIOS DEL SISTEMA

Como se comentó en otras partes de la guía se necesita minimizar la superficie de ataque, eliminando elementos innecesarios. Por ello no se deben mantener servicios activos que no son necesarios para el correcto funcionamiento del sistema.

En la distribución SUSE Linux Enterprise Server 12, la forma de controlar los servicios del sistema cambia con respecto a sus antecesoras. Se pasa del uso del comando "service" y del control de servicios a través de **/etc/init.d** a la gestión a través del service manager **systemctl**.

Se pueden listar fácilmente todos los servicios del sistema que corren al inicio mediante el comando **systemctl list-unit-files**. Procediendo a deshabilitar los que no sean necesarios.

Es posible usar el asistente **YaST** que muestra de manera más gráfica una lista de servicios disponibles los cuales se pueden seleccionar y definir para que arranquen automáticamente junto con el sistema.



6.2.7 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.

6.2.7.1 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**.

En este punto se hará hincapié en eliminar todos aquellos paquetes que se encuentren por defecto en la instalación propia de SUSE Linux Enterprise Server 12 (SP3) o sean innecesarios para el correcto funcionamiento del sistema. Así mismo se procederá con sus correspondientes dependencias.

6.2.7.2 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.

6.2.8 PERMISOS Y VARIABLES DE ENTORNO

Las variables de entorno forman un conjunto de valores dinámicos que normalmente afectan al comportamiento de los procesos en un sistema. Las variables de entorno contienen información a la que se accede a través del nombre de la variable (al igual que ocurre en los lenguajes de programación).

6.2.8.1 FICHEROS DE CONFIGURACIÓN

Los ficheros **/etc/profile** y **/etc/csh.login** contienen las variables de entorno generales para todos los usuarios del sistema. Aunque su revisión está recomendada, hay que prestar especial atención a los siguientes puntos:

- a) **/etc/profile**:
 - i. En el PATH no debe figurar el directorio actual (**.**). Para validar que esto también se cumple en el caso de root, se comprueba la salida del comando “echo \$PATH”.
 - ii. Se restringe el tiempo máximo de inactividad en el sistema estableciendo el valor 600 para la variable TMOU.
 - iii. Se restringe el tamaño del historial del intérprete de comandos al valor 1000 para los usuarios con la variable HISTSIZE.
- b) **/etc/csh.login**:
 - i. Se comprueba que la máscara por defecto de los usuarios es restrictiva comprobando que la directiva **umask** tiene el valor **027**.

Nota: Otros ficheros de entorno que puedan existir en los directorios de los usuarios deberán ser revisados para evaluar su potencial peligrosidad. Por ejemplo, los ficheros **.netrc** deberán ser eliminados, ya que suponen un riesgo para el sistema.

6.2.8.2 DIRECTORIO DE USUARIOS

Se comprobará que los directorios **/home** de los usuarios no permiten a otros usuarios acceder ni modificar su contenido. Para ello será necesario que estos directorios cuenten con permisos **740** o más restrictivos.

6.2.8.3 PERMISOS EN FICHEROS Y DIRECTORIOS IMPORTANTES

Ciertos ficheros y directorios contienen información de carácter crítico, por lo que sus permisos deben ser revisados cuidadosamente para evitar problemas. Los ficheros más importantes son **/etc/passwd**, **/etc/group** y **/etc/shadow**. Por ello, se deben de tomar ciertas medidas para evitar el acceso a la lectura o la modificación de los mismos por personal no autorizado.

El propietario de los tres debe ser **root**, con grupo **root**; los permisos de los dos primeros deben permitir la lectura por parte de todos los usuarios del sistema y la modificación únicamente por root, mientras que el fichero de contraseñas shadow únicamente debe ser leído por root.

En cuanto a los directorios, todos aquellos en los que los usuarios del sistema tengan permisos de escritura deberán proteger sus contenidos utilizando el “**sticky bit**”, que previene que usuarios del sistema borren contenidos creados por otros usuarios.

También será necesario identificar ficheros cuyos permisos puedan representar un riesgo para el sistema. En especial será necesario identificar aquellos ficheros que puedan ser modificados por todos los usuarios, independientemente de los permisos que posean. A demás de aquellos ficheros que tengan activado el bit de **SUID** o de **SGID**.

6.3 SISTEMA

6.3.1 ACTUALIZACIÓN DEL SISTEMA

Las actualizaciones del sistema son mejoras que se realizan al núcleo del sistema operativo y a diversas aplicaciones que se ejecutan en este sistema, con la finalidad de mantener su funcionamiento óptimo y reparar en la medida de lo posible fallos, errores y vulnerabilidades que se puedan presentar.

Todo sistema debe de estar actualizado, pero dependiendo de la criticidad del sistema que se deba actualizar, es posible que se necesite aislar del resto de sistemas o aislar su comunicación con redes externas e internet. Por este motivo ciertos sistemas necesitarán una actualización fuera de línea.

En esta guía se diferenciará la actualización por parte del fabricante de manera “online” y mediante parches y actualizaciones de manera “offline”.

6.3.1.1 ONLINE

SUSE Linux es una de las distribuciones Linux existentes a nivel mundial, se basó en sus orígenes en Slackware. Entre las principales virtudes de esta distribución se encuentra el que sea una de las más sencillas de instalar y administrar, ya que cuenta con varios asistentes gráficos para completar diversas tareas en especial por su gran herramienta de instalación y configuración YaST.

6.3.1.2 OFFLINE

Para actualizar el sistema, arranque desde un origen de instalación, como haría en el caso de una instalación nueva. Sin embargo, cuando aparece la pantalla de arranque, debe seleccionar la opción Actualizar (en lugar de Instalación). La actualización se puede iniciar desde:

- a) **Medios extraíbles.** Esto incluye medios como los CD, DVD o dispositivos USB de almacenamiento masivo.
- b) **Recursos de red.** Puede arrancar desde el medio local y después seleccionar el tipo de instalación de red correspondiente, o bien arrancar mediante PXE.
- c) **Discos duros.** Puede copiar el nuevo núcleo y la imagen initrd desde la imagen del disco duro que contiene la instalación de SUSE Linux Enterprise y ajustar el menú de arranque.

Nota: Para obtener más información, consulte el siguiente enlace: https://www.suse.com/es-es/documentation/sles-12/book_sle_deployment/data/sec_update_offline_conceptual-overview.html

6.3.2 SISTEMA Y SERVICIOS

Linux ofrece multitud de servicios, estos pueden iniciar o arrancar junto con la carga del sistema o pueden arrancar a petición del usuario, lo que para muchos servicios será lo recomendable. Parte esencial de la administración de sistemas Linux es continuamente trabajar con los servicios que este proporciona.

SYSTEMD es un gestor de sistema y servicios para Linux, el cual reemplaza SysV utilizado en lanzamientos anteriores de SUSE Enterprise Linux. Systemd es compatible con SysV y scripts init de Linux Standard Base.

Systemd ofrece, entre otras, las siguientes capacidades:

- a) Capacidades de paralelización agresiva
- b) Uso de activación de socket y D-Bus para servicios de inicio.
- c) Inicios On-demand de demonios.
- d) Manejo de grupos de control

- e) Creación de instantáneas de estado del sistema y restauración de estado del sistema.

6.3.3 ADMINISTRACIÓN DE RECURSOS

SUSE Enterprise Linux 12 SP3 introduce los grupos de control, un concepto para procesos de organización en un árbol de grupos nominados para propósitos de administración de recursos. Los grupos de control proporcionan una forma de agrupar por jerarquías y procesos de etiquetas y una forma de aplicar límites de recursos a estos grupos. En SUSE Enterprise Linux 12 SP3, los grupos de control se manejan de forma exclusiva a través de **systemd**.

Los grupos de control, abreviados como **cgroups**, son una función de kernel de Linux que le permite asignar recursos, como tiempo de CPU, memoria del sistema, ancho de banda de red o combinaciones de estos recursos, entre grupos ordenados jerárquicamente de procesos que se ejecutan en un sistema. Mediante el uso de cgroups, los administradores del sistema obtienen un control detallado sobre la asignación, priorización, denegación, administración y supervisión de los recursos del sistema.

Los recursos de hardware se pueden dividir inteligentemente entre aplicaciones y usuarios, aumentando la eficiencia general. Cgroups se configuran en archivos de unidades de systemd y se manejan con las herramientas de la interfaz de línea de comandos(CLI).

SUSE Enterprise Linux 12 SP3 traslada la configuración de administración de recursos del nivel de proceso al nivel de aplicación vinculando el sistema de jerarquías de cgroup con el árbol de unidades systemd. Por lo tanto, puede administrar los recursos del sistema con los comandos **systemctl**, o modificando los archivos de la unidad **systemd**.

En versiones anteriores de SUSE Enterprise Linux 12 SP3, los administradores del sistema creaban jerarquías de cgroup personalizadas con el uso del comando **cgconfig** del paquete **libcgroup**. Este paquete ahora está en desuso, y no se recomienda su uso ya que puede crear conflictos con la jerarquía predeterminada de cgroup. Sin embargo, libcgroup todavía está disponible para cubrir ciertos casos específicos, donde systemd aún no fuera aplicable.

Las herramientas mencionadas proporcionan una interfaz de alto nivel para interactuar con los controladores cgroup (también conocidos como subsistemas) en el kernel de Linux. Los controladores principales de cgroup para la gestión de recursos son cpu, memory y blkio.

Un controlador de recursos, también llamado subsistema cgroup, representa un único recurso, como el tiempo de CPU o la memoria. El kernel de Linux proporciona una gama de controladores de recursos, que systemd monta automáticamente. la lista de controladores de recursos actualmente se encuentra en /proc/cgroups, otra opción es usar la herramienta de supervisión **lssubsys**. SUSE Enterprise Linux 12 SP3, systemd monta los siguientes controladores por defecto:

- a) **blkio**: establece límites en el acceso de entrada / salida hacia y desde dispositivos de bloque.
- b) **CPU**: utiliza el programador de la CPU para proporcionar acceso a las tareas de cgroup a la CPU. Se monta junto con el controlador cpuacct en el mismo soporte.
- c) **cpuacct**: crea informes automáticos sobre los recursos de la CPU utilizados por las tareas en un cgroup. Se monta junto con el controlador de la CPU en el mismo soporte.
- d) **cpuset**: asigna CPU individuales (en un sistema multinúcleo) y nodos de memoria a tareas en un cgroup.
- e) **devices**: permite o deniega el acceso a dispositivos para tareas en un cgroup.
- f) **freezer**: suspende o reanuda tareas en un grupo cg.
- g) **memory**: establece límites en el uso de memoria por tareas en un grupo de cg y genera informes automáticos sobre los recursos de memoria utilizados por esas tareas.
- h) **net_cls**: etiqueta paquetes de red con un identificador de clase (classid) que permite que el controlador de tráfico de Linux (el comando tc) identifique los paquetes que se originan de una tarea particular de cgroup.

Un subsistema de `net_cls`, `net_filter` (iptables) también puede usar esta etiqueta para realizar acciones en dichos paquetes. `Net_filter` etiqueta los sockets de red con un identificador de firewall (fwid) que permite que el firewall de Linux (el comando iptables) identifique los paquetes (skb → sk) que se originan de una tarea particular de cgroup.

- i) **perf_event**: habilita la supervisión de cgroups con la herramienta perf.
- j) **hugetlb**: permite utilizar páginas de memoria virtual de gran tamaño y aplicar límites de recursos en estas páginas.

6.3.4 ALMACENAMIENTO

En Linux, casi todo está representado por un archivo. Esto incluye hardware como unidades de almacenamiento, que se representan en el sistema como archivos en el directorio **/dev**. Normalmente, los archivos que representan dispositivos de almacenamiento comienzan con **sd** o **hd** seguido de una letra. Por ejemplo, la primera unidad en un servidor suele ser algo así como **/dev/sda**.

Las particiones en estas unidades también tienen archivos dentro de **/dev**, representados al agregar el número de partición al final del nombre de la unidad. Por ejemplo, la primera partición en el disco del ejemplo anterior sería **/dev/sda1**.

Mientras que los archivos del dispositivo **/dev/sd*** y **/dev/hd*** representan la forma tradicional de referirse a unidades y particiones, existe una desventaja significativa al usar estos valores por sí mismos. El kernel de Linux decide qué dispositivo obtiene qué nombre en cada arranque, por lo que esto puede generar escenarios confusos en los que los dispositivos cambian los nodos del dispositivo.

Para evitar este problema, el directorio **/dev/disk** contiene subdirectorios correspondientes con formas diferentes y más persistentes para identificar discos y particiones en el sistema. Estos contienen enlaces simbólicos que se crean en el inicio de los archivos correctos **/dev/[s,h]da***. Los enlaces se nombran de acuerdo con el rasgo de identificación del directorio (por ejemplo, mediante la etiqueta de partición en el directorio **/dev/disk/by-partlabel**). Estos enlaces siempre apuntan a los dispositivos correctos, por lo que pueden usarse como identificadores estáticos para espacios de almacenamiento.

6.3.5 SISTEMA DE ARCHIVOS

Un sistema de archivos es el sistema que estructura los datos, controla cómo se escribe y recupera la información del disco subyacente. Sin un sistema de archivos, no podría usar el dispositivo de almacenamiento para ninguna operación relacionada con archivos.

El sistema de archivos para una instalación en SUSE Enterprise server 12 SP3 por defecto es Btrfs (B-Tree), el cual reemplaza el Cuarto sistema de archivos extendido (ext4) utilizado como predeterminado en versiones anteriores. El sistema de archivos ext4 y el sistema de archivos XFS pueden utilizarse como alternativos para Btrfs.

Se optará por el uso del sistema de archivos XFS. XFS es un sistema de archivos escalable de alta disponibilidad, el cual fue diseñado originalmente en Silicon Graphics, Inc. Fue creado para soportar sistemas de archivos de hasta 16 Exabytes (aproximadamente 16 millones de terabytes), y estructuras de directorios que contienen decenas de millones de entradas. XFS soporta diario de metadatos, lo cual facilita recuperación de daños de una forma más rápida. Los sistemas de archivos XFS también se pueden desfragmentar y expandir cuando están montados y activos.

Tabla de comandos de referencia para ext4 y XFS:

Tarea	Ext4	XFS
Creación de un sistema de Archivos	mkfs.ext4	mkfs.xfs
Montaje de un sistema de Archivos	mount	mount
Cambiar el tamaño de un sistema de Archivos	resize2fs	xfs_growfs ¹
Reparar un sistema de archivos	e2fsck	xfs_repair
Cambiar la etiqueta en un sistema de archivos	e2label	xfs_admin -L
Informes sobre el espacio en disco y el uso de archivos	quota	quota
Depuración de un sistema de archivos	debugfs	xfs_db
Guardar metadatos críticos del sistema de archivos	e2image	xfs_metadump

Por otra parte, el sistema de archivos **Btrfs** es uno de los sistemas de archivos más nuevo que hay disponibles en Linux. La meta de Btrfs es implementar algunas características importantes que faltan en los sistemas de archivos en Linux, tales como pooling, snapshots y checksums, entre otras. Una de las motivaciones principales es proveer de soporte confiable para sistemas de archivos grandes, por lo cual puede ser de interés para cualquier organización que tenga muchos usuarios y/o que posea un almacenamiento grande.

6.3.6 ADMINISTRACIÓN Y MANTENIMIENTO

Tanto la Administración como el mantenimiento de servidores o equipos Linux es una tarea que necesita una vigilancia constante para asegurar la estabilidad del sistema.

El mantenimiento de servidores debe realizarse desde el primer momento en que estos comienzan a funcionar. Y es que, aunque en un primer momento parezca que el mantenimiento no es una tarea demasiado relevante, es importante sentar las bases para el medio y largo plazo, cuando el tráfico sea más elevado y los recursos almacenados en el servidor sean mayores.

6.3.6.1 AUTOMATIZACIÓN DE TAREAS

En un sistema cualquier tarea automatizada puede ser motivo de fallo de seguridad, por lo que hay que tener identificadas las tareas automatizadas que suceden en nuestro sistema, además de tener protegidos los programas y servicios que las crean.

La herramienta que se usa para automatizar procesos es **cron**. Esta herramienta no es más que 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). Los procesos que deben ejecutarse y la hora en la que deben hacerlo se especifican en el fichero **Crontab**.

A demás existe el comando **"at"**. Esta herramienta permite programar tareas que se ejecutarán una única vez.

Para limitar la generación de tareas periódicas a usuarios que no estén autorizados (generalmente se considerará únicamente el usuario root como usuario autorizado para tal efecto) se crearán los ficheros **/etc/cron.allow** y **/etc/at.allow** en los que se incorporarán los nombres de los usuarios que pueden utilizar estos servicios.

Se puede establecer esto mismo mediante lista negra en lugar de lista blanca, si es así se crearán los ficheros **/etc/cron.deny** y **/etc/at.deny**, en los que aparecerán los nombres de los usuarios que no pueden utilizar los servicios de los planificadores de tareas.

Nota: Tanto en **CRON** como en **AT** los usuarios incluidos en los ficheros **.allow** tienen preferencia con respecto a los usuarios incluidos en el fichero **.deny**.

¹ El tamaño de los sistemas de archivos XFS no se puede reducir; el comando se usa solo para aumentar el tamaño.

6.3.6.2 LOGS DE SISTEMA

El encargado principal de recoger todos los logs para tener una visión global del sistema en SUSE Enterprise server 12 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 que se han realizado. La auditoría no proporciona seguridad adicional a su 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.

Entre las partes del sistema que Audit es capaz de recoger información se encuentran las siguientes:

- a) Fecha y hora, tipo y resultado de un evento.
- b) Etiquetas más detalladas de sujetos y objetos.
- c) Asociación de un evento con la identidad del usuario que activó el evento.
- d) Todas las modificaciones a la configuración de auditoría e intentos de acceso a los archivos de registro de auditoría.
- e) Todos los usos de los mecanismos de autenticación, como SSH, Kerberos y otros.
- f) Cambios en cualquier base de datos confiable, como `/etc/passwd`.
- g) Intentos de importación o exportación de información hacia o desde el sistema.
- h) Incluir o excluir eventos en función de la identidad del usuario, las etiquetas de tema y objeto, y otros atributos.
- i) Por la criticidad de los datos que contiene esta aplicación, se procederá a configurar los accesos a la misma de forma segura. Además se hará hincapié en la creación de reglas que proporcionen la mayor información posible sobre lo que pueda ocurrir en el sistema.

6.3.6.3 CONTROL DE INTEGRIDAD DE HARDWARE

AIDE es una alternativa libre a Tripwire, que 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 ftype).
- 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.

6.3.6.4 CONTROL DE DISPOSITIVOS EXTRAIBLES

En la actualidad el volumen de datos que se puede copiar rápidamente a dispositivos de almacenamiento extraíbles es más que notorio. Aunque este tipo de dispositivos puede fomentar en gran medida la productividad, su potencial para minar la seguridad de los datos y las directivas de control también es muy grande. Entre las amenazas que entrañan estos dispositivos destacan las siguientes:

- a) Usuarios malintencionados que copian grandes cantidades de información sin que se refleje en el seguimiento de la auditoría.
- b) Usuarios de buena fe que desechan o extravían dispositivos con información confidencial.
- c) Malware y códigos nocivos que se infiltran en la red por medio de dispositivos infectados.
- d) Infracciones de normativas como HIPAA, SOX, GLBA y otras regulaciones como consecuencia de la copia y el transporte de datos confidenciales que no se han cifrado.

Por este motivo, se limitarán los dispositivos extraíbles que tienen acceso al sistema, siendo los usuarios con permiso de administración los habilitados con privilegios para la activación de esta característica.

En esta guía se recomienda la instalación del software **USBGUARD**, añadiendo mayor seguridad y control sobre los dispositivos extraíbles que se introduzcan en el sistema.

6.3.6.5 COPIAS DE SEGURIDAD

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

- a) Qué información es importante incluir en la copia de seguridad: documentos de usuarios, ficheros de configuración, registros de log, etc.
- b)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.
- c) La periodicidad de realización de estas copias de seguridad y el modo de copia (total, incremental, etc.).
- d) 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.
- e) 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.

7. NUEVAS FUNCIONALIDADES Y PRINCIPALES CAMBIOS

SUSE Linux Enterprise Server es un sistema operativo de servidor altamente confiable, escalable y seguro, creado para alimentar cargas de trabajo críticas en entornos físicos y virtuales. Es una base de código abierto asequible, interoperable y manejable. Con ello, las empresas pueden habilitar redes seguras y simplificar la administración de su infraestructura de TI heterogénea, maximizando la eficiencia y el valor.

SUSE Linux Enterprise Server, el único Linux empresarial recomendado por Microsoft y SAP, está optimizado para ofrecer servicios de misión crítica de alto rendimiento, así como cargas de trabajo de infraestructura web y borde de red.

Diseñado para la interoperabilidad, SUSE Linux Enterprise Server se integra en Unix clásico y en entornos de Windows, admite interfaces estándar abiertas para la administración de sistemas y ha sido certificado para la compatibilidad con IPv6.

Este sistema operativo modular de propósito general se ejecuta en tres arquitecturas de procesador y está disponible con extensiones opcionales que brindan capacidades avanzadas para tareas como la computación en tiempo real y la agrupación en clústeres de alta disponibilidad.

SUSE Linux Enterprise Server está optimizado para ejecutarse como un invitado de alto rendimiento en hipervisores líderes y admite un número ilimitado de máquinas virtuales por sistema físico con una sola suscripción, lo que lo convierte en el sistema operativo invitado perfecto para la computación virtual.

SUSE Linux Enterprise Server está respaldado por el galardonado soporte de SUSE, un líder tecnológico establecido con un historial comprobado de prestación de servicios de soporte de calidad empresarial.

7.1 ESCRITORIO

SUSE Linux Enterprise Server 12 provee una interfaz Gui (escritorio) que interactúa entre el software instalado en el equipo, los dispositivos hardware y el usuario. Linux ofrece muchas alternativas. Los entornos de escritorio más populares son GNOME, KDE, XFCE, MATE y Cinnamon.

a) GNOME 3

- i. La experiencia del usuario de GNOME 3 es definida ampliamente por GNOME Shell, el cual reemplaza el Shell de escritorio de GNOME 2. Aparte de la administración de ventanas, GNOME Shell proporciona la barra superior en la pantalla, la cual alberga el área de “estatus del sistema” en la parte superior derecha, un reloj y una esquina que cambia a Vista de actividades, la cual proporciona fácil acceso a aplicaciones y ventanas.
- ii. La interfaz predeterminada de GNOME Shell en SUSE Linux Enterprise Server 12 es GNOME Classic, el cual presenta una lista de ventana en la parte inferior de la pantalla, y los menús de las Aplicaciones y los Sitios tradicionales.

Para obtener más información sobre GNOME 3, consulte la ayuda de GNOME.

<https://help.gnome.org/users/gnome-help/stable/index.html.es>

7.2 SEGURIDAD

Linux es un sistema operativo multiusuario, lo que significa que puede tener más de un usuario trabajando al mismo tiempo desde sus diferentes estaciones de trabajo. A raíz de esto, el sistema debe proteger a unos usuarios frente a otros y a sí mismo.

En Linux se adopta como norma básica de seguridad, asignarle a cada uno de los usuarios, sólo los permisos mínimos y necesarios para que este pueda realizar su trabajo, sin comprometer el de los demás y la integridad del sistema.

El sistema de archivos de Linux sigue el estándar de Unix, posee una estructura determinada y compatible con los demás sistemas Unix. Estos tienen su origen en la denominada “raíz” que es representado por “/”. De este directorio se desprenden todos los Archivos (Archivos ordinarios - Directorios - Archivos Especiales) a los que el sistema operativo tiene acceso.

Estos son los cambios realizados en las herramientas de SUSE Linux Enterprise Server 12 que abordan el tema de la seguridad:

7.2.1 APPARMOR

AppArmor es una aplicación y herramienta de seguridad incluida en el paquete SUSE Enterprise Linux diseñada para proveer una protección de fácil uso para tus aplicaciones. AppArmor protege proactivamente el sistema operativo y las aplicaciones de amenazas externas o internas inclusive ataques "zeroday" implementando un buen funcionamiento e impidiendo inclusive fallos desconocidos de ser explotados. Las políticas de seguridad de AppArmor (Perfiles) definen que recursos del sistema y privilegios pueden acceder las aplicaciones. AppArmor incluye perfiles predeterminados que usan una combinación de análisis estático avanzado y herramientas basadas en aprendizaje; por esta razón pueden colocarse en las aplicaciones más complejas en cuestión de horas.

AppArmor está formado por:

- a) Un módulo de kernel comunicado con el kernel de SUSE Enterprise Linux que implementa los perfiles de seguridad.
- b) Un conjunto de perfiles de AppArmor para numerosos programas que se comunican con SUSE Enterprise Linux.
- c) Herramientas para crear y operar nuevos perfiles
- d) Una interfaz de usuario YaST para operar reportes y notificaciones de eventos de seguridad.
- e) Documentación acerca de las herramientas.

7.2.2 INSTALACIÓN O ELIMINACIÓN DE SOFTWARE

Utilice 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.

Modifique la colección de software del sistema mediante el Gestor de software de YaST. Hay dos versiones de este módulo de YaST: una variante gráfica para X Window y una basada en texto para usar en la línea de comandos.

Nota: Al instalar, actualizar o eliminar paquetes, cualquier cambio en el Gestor de software no se aplica de inmediato, sino después de confirmarlo con Aceptar o Aplicar respectivamente. YaST mantiene una lista de todas las acciones, de modo que permite revisar y modificar los cambios antes de aplicarlos al sistema.

- a) **Instalación de módulos, extensiones y productos adicionales de otros fabricantes.** Los módulos y extensiones añaden partes o funcionalidades al sistema. Los módulos son partes totalmente compatibles de SUSE Linux Enterprise Server con un ciclo de vida y una periodicidad de actualizaciones distintos. Son un conjunto de paquetes con un objetivo claramente definido y se proporcionan solo a través del canal en línea. Las extensiones, como la de estación de trabajo o la "High Availability Extension", aportan funciones adicionales al sistema y requieren una clave de registro de pago propia. Las extensiones se proporcionan a través del canal en línea o de un medio físico. Para suscribirse a los canales en línea, es imprescindible haberse registrado previamente en el Centro de servicios al cliente de SUSE o en un servidor de registro local. Las extensiones Package Hub y SUSE Software Development Kit son excepciones que no requieren una clave de registro y no están cubiertas por los acuerdos de asistencia de SUSE.

Cuando registre el sistema en el Centro de servicios al cliente de SUSE o en un servidor de registro local, tendrá a su disposición una lista de módulos y extensiones para el producto. Si omitió el paso de registro

durante la instalación, puede registrar el sistema en cualquier momento mediante el módulo Configuración del Centro de servicios al cliente de SUSE en YaST.

Algunos productos adicionales también provienen de otros fabricantes; por ejemplo, los controladores solo binarios necesarios para que cierto hardware funcione correctamente. Si dispone de hardware de este tipo, consulte las notas de la versión para obtener más información acerca de si hay controladores binarios disponibles para su sistema. Las notas de la versión están disponibles en <http://www.suse.com/releasesnotes>, en YaST o en `/usr/share/doc/release-notes/SUSE_Linux_Enterprise_Server_12/` en el sistema instalado.

- b) **Instalación de varias versiones del núcleo.** SUSE Linux Enterprise Server admite la instalación en paralelo de varias versiones del núcleo. Al instalar un segundo núcleo, se crean automáticamente una entrada de arranque y un `initrd`, por lo que no es necesaria realizar más configuración manual. Al rearrancar el equipo, el núcleo recién añadido estará disponible como opción de arranque adicional.

Mediante esta función, es posible probar con seguridad las actualizaciones del núcleo y volver en cualquier momento al núcleo anterior. Para ello, no debe usar las herramientas de actualización (como YaST Online Update o el applet de actualización).

7.2.3 MANTENIMIENTO DEL SISTEMA ACTUALIZADO

SUSE ofrece un flujo continuo de parches de seguridad de software para su producto. Se pueden instalar mediante el módulo “YaST Online Update”. También ofrece funciones avanzadas para personalizar la instalación de parches.

El escritorio GNOME proporciona además una herramienta para instalar parches y para instalar actualizaciones de paquetes que ya están instalados. A diferencia de un Parche, una actualización de paquete solo está relacionada con un paquete y proporciona una versión más reciente de este. La herramienta GNOME permite instalar parches y actualizaciones de paquetes en pocos pasos.

Vías de actualización a SLE 12 SP3 admitidas:

- a) **Actualizar de SUSE Linux Enterprise 10** (cualquier paquete de servicio o Service Pack). No se admite ninguna vía de migración directa a SUSE Linux Enterprise 12. En este caso, se recomienda realizar una instalación nueva.
- b) **Actualización desde SUSE Linux Enterprise 11 GA, SP1 o SP2.** No se admite ninguna vía de migración directa a SUSE Linux Enterprise 12. Debe tener instalado al menos SLE 11 SP4 para poder continuar a SLE 12 SP3. Si no es posible realizar una instalación nueva, actualice primero el paquete de servicios de SLE 11 instalado a SLE 11 SP4. Estos pasos se describen en la Guía de distribución de SUSE Linux Enterprise 11.
- c) **Actualización desde SUSE Linux Enterprise 11 SP4.** La actualización de SLE 11 a SLE 12 SP3 solo se admite a través de una actualización sin conexión. Consulte la Sección 18.5.2, Actualización con conexión y sin conexión para obtener más detalles.
https://www.suse.com/es-es/documentation/sles-12/book_sle_deployment/data/sec_update_sle12_manual.html
- d) **Actualización desde SUSE Linux Enterprise 12 GA a SP3.** No se admite la actualización directa de SLE 12 GA a SP3. Actualice primero a SLE 12 SP2.
- e) **Actualización desde SUSE Linux Enterprise 12 SP1 o SP2 a SP3.** Se admite la actualización desde SUSE Linux Enterprise 12 SP1 o SP2 a SP3
- f) **Actualización desde SUSE Linux Enterprise 12 LTSS GA, SP1 o SP2 a SP3.** Se admite la actualización de cualquier versión anterior de SLE 12 LTSS a SP3.

7.3 INTEROPERABILIDAD Y SOPORTE DE HARDWARE

Viene con las últimas versiones de aplicaciones líderes como el paquete de productividad de oficina LibreOffice, el navegador web Mozilla Firefox y el paquete de correo electrónico y calendario Evolution. Además, se integra con Microsoft SharePoint para la colaboración grupal y es compatible con una amplia gama de formatos de archivos multimedia, estándares de redes inalámbricas y dispositivos plug-and-play.

A través de las últimas mejoras en administración de energía y seguridad, SUSE Linux Enterprise Desktop también brinda una experiencia de TI respetuosa con el medio ambiente (TI verde) y un escritorio a prueba de errores. Finalmente, SUSE Linux Enterprise Desktop ofrece una flexibilidad sin igual. Puede implementarlo en una amplia gama de dispositivos de cliente grueso (incluidos equipos de escritorio, portátiles, notebooks y estaciones de trabajo), en dispositivos de cliente ligero o como un escritorio virtual.

Robustez en los errores administrativos y capacidades de administración mejoradas con reversión total del sistema basada en Btrfs como el sistema de archivos predeterminado para la partición del sistema operativo y la tecnología de pago de SUSE.

Una revisión del instalador introduce un nuevo flujo de trabajo que le permite registrar su sistema y recibir todas las actualizaciones de mantenimiento disponibles como parte de la instalación.

Los módulos de servidor empresarial de SUSE Linux ofrecen una variedad de paquetes complementarios, que van desde herramientas para desarrollo web y secuencias de comandos, a través de un módulo de gestión de la nube, hasta una vista previa del próximo conjunto de herramientas de gestión de SUSE, llamada Advanced Systems Management. Los módulos forman parte de su suscripción a SUSE Linux Enterprise Server, se entregan técnicamente como repositorios en línea y difieren de la base de SUSE Linux Enterprise Server solo por su ciclo de vida.

Nuevas tecnologías básicas, como systemd (que reemplaza el proceso inicial basado en System V) que introduce una infraestructura de configuración de red moderna y dinámica.

El sistema de base de datos de código abierto MariaDB es totalmente compatible.

Soporte para las herramientas open-vm junto con VMware para una mejor integración en entornos de hipervisor basados en VMware.

Los contenedores de Linux están integrados en la infraestructura de gestión de virtualización (lib-virt). Docker es totalmente compatible ahora.

Soporte para la variante Little-Endian de 64 bits de la arquitectura POWER de IBM, además del soporte continuo para las arquitecturas Intel 64 / AMD64 e IBM System z.

GNOME 3.10 (o simplemente GNOME 3), que ofrece a los usuarios un entorno de escritorio moderno con una selección de diferentes opciones de apariencia, incluido un modo clásico de SUSE Linux Enterprise para una migración más sencilla desde los entornos de escritorio anteriores de SUSE Linux Enterprise.

Integración con el nuevo Centro de servicios al cliente de SUSE, el portal web central de SUSE para gestionar las suscripciones, los derechos y proporcionar acceso al soporte.

7.4 CONFIGURACIÓN DE SUSEFIREWALL2

SuSEFirewall2 es un script que lee las variables establecidas en `/etc/sysconfig/SuSEfirewall2` para generar un conjunto de reglas de iptables. Define tres zonas de seguridad:

- a) **Zona externa.** Dado que no hay forma de controlar lo que está sucediendo en la red externa, el host debe estar protegido de ella. Por lo general, la red externa es Internet, pero podría ser otra red insegura, como una conexión Wi-Fi.

- b) **Zona interna.** Esto se refiere a la red privada, generalmente la LAN. Si los hosts de esta red utilizan direcciones IP del rango privado habilite la traducción de direcciones de red (NAT), de modo que los hosts de la red interna puedan acceder al servidor externo. Todos los puertos están abiertos en la zona interna. La principal ventaja de poner interfaces en la zona interna (en lugar de detener el firewall) es que el firewall aún se ejecuta, por lo que cuando agrega nuevas interfaces, se colocarán en la zona externa de manera predeterminada. De esa manera, una interfaz no se abre accidentalmente de forma predeterminada.
- c) **Zona desmilitarizada (DMZ).** Si bien se puede acceder a los hosts ubicados en esta zona tanto desde la red externa como desde la interna, no pueden acceder a la red interna por sí mismos. Esta configuración se puede usar para colocar una línea de defensa adicional frente a la red interna, ya que los sistemas DMZ están aislados de la red interna.

Después de la instalación, YaST inicia automáticamente un firewall en todas las interfaces configuradas. Si un servidor está configurado y activado en el sistema, YaST puede modificar la configuración del cortafuegos generado automáticamente con las opciones “Abrir puertos en la interfaz seleccionada del Cortafuegos” o “Abrir puertos en el Cortafuegos” en los módulos de configuración del servidor. Algunos cuadros de diálogo del módulo del servidor incluyen un botón “Detalles del servidor de seguridad” para activar puertos y servicios adicionales. El módulo de configuración del firewall de YaST se puede usar para activar, desactivar o reconfigurar el firewall.