centro criptológico nacional

Guía de Seguridad de las TIC

IMPLEMENTACIÓN DE SEGURIDAD SOBRE CENTOS 8 (CLIENTE INDEPENDIENTE)

SEPTIEMBRE 2020

MINISTERIO DE DEFENSA

Edita:

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES

NIPO: 083-20-180-6

Fecha de Edición: septiembre de 2020
Sidertia Solutions S.L. ha participado en la realización y modificación del presente documento y sus anexos.

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

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 y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del 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, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, 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 la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

septiembre de 2020

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

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 CentOS (**C**ommunity**ENT**erprise**O**perating**S**ystem) 8.1 Linux, 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 Linux CentOS 8.1 Linux (build 1911).

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 cliente, 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. Por lo tanto, 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 cliente con el sistema operativo “Linux CentOS”, instalado en español en su versión 8.1 (build 1911). 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 técnicas:

a) Implementación del ENS en un escenario con clientes independientes con el sistema operativo CentOS 8.1.

b) Implementación de plantillas de seguridad en función de los niveles de seguridad establecidos en el ENS para clientes CentOS 8.1 Linux independientes.

c) Implementación de seguridad en un escenario de red clasificada clientes independientes CentOS 8.1.

Este documento incluye:

a) **Descripción de versiones, opciones de mantenimiento** para todos aquellos operadores que tengan experiencia en versiones previas, se proporciona la información sobre las diferencias entre versiones y opciones de mantenimiento.

b) **Descripción de las nuevas funcionalidades** para todos aquellos operadores que tengan experiencia en las versiones anteriores de CentOS, se incluyen las nuevas características del producto.

c) **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 CentOS 8.1 Linux como puesto de trabajo independiente.

d) **Mecanismos para la implementación de la solución**. Se incorporan mecanismos para la implementación de la solución de forma automatizada.

e) **Mecanismos para la aplicación de configuraciones**. Se incorporan mecanismos para la implementación de forma automática de las configuraciones de seguridad susceptibles de ello.

f) **Guía paso a paso**. Va a permitir implantar y establecer las configuraciones de seguridad en clientes CentOS 7.4 Linux independientes.

g) **Lista de comprobación**. Permitirá verificar el grado de cumplimiento de los equipos cliente con respecto a las condiciones de seguridad que se establecen en esta guía.

h) **Configuración de cifrado de disco**. Establece los mecanismos para la configuración del cifrado que aporta CentOS 8.1 Linux.

i) **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 cliente CentOS 8.1 Linux 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 puesto cliente con Sistema Operativo CentOS 8.1 Linux 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 CentOS 8.1, 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 CentOS 8.1-x86_64-Everything (build 1911) con la opción de instalación “instalación mínima”.

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 CentOS 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, Yum/dnf puede usarse para agregar o eliminar paquetes.

Las imágenes MinimalCD contienen un mínimo de paquetes necesarios para una instalación funcional, sin comprometer la seguridad o la usabilidad de la red. Estas imágenes mínimas usan el instalador estándar de CentOS con todas sus características regulares menos la selección de paquetes. Yum se puede usar después de completar la instalación para agregar o eliminar paquetes.

La guía ha sido desarrollada y probada en entorno de uso de servicios Linux con la versión de CentOS 8.1-x86_64-Everything (build 1911).

La guía de seguridad ha sido elaborada utilizando un laboratorio basado en una plataforma de virtualización tipo Hyper-V sobre Windows Server 2019 Datacenter con las siguientes características técnicas:

a) Servidor Dell PowerEdge™ T320:
   i. Intel Pentium Xeon CPU ES 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 CentOS 8. Esto quiere decir que se requieren equipos con procesadores Intel o AMD de 64 o 32 bits (x64 o i386), con más de 1 GB 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.

A partir de la versión 7 de CentOS, el sistema solo es completamente compatible con arquitectura x86-64, por lo que las siguientes arquitecturas no son compatibles:

a) IA-32 en todas las variantes, tuvo soporte temporalmente en CentOS 7.0.
b) IA-32 sin extensión de dirección física (PAE), no compatible desde CentOS 6.
c) IA-64 (arquitectura Intel Itanium), fue compatible con CentOS 3 y 4.
d) PowerPC de 32 bits (Apple Macintosh y PowerMac con procesador PowerPC G3 o G4), el soporte beta estaba disponible en CentOS 4.
e) IBM Mainframe (eServer zSeries y S / 390), no compatible desde CentOS 5.
f) Alpha, el soporte estaba disponible en CentOS 4.
g) El soporte SPARC, beta estaba disponible en CentOS 4.

Nota: Puede comprobar los requisitos del sistema de CentOS en el siguiente enlace https://wiki.centos.org/About/Product.

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 recomendadas por el fabricante, disponibles a través del servicio “yum update --security “. Las actualizaciones por lo general están disponibles en los servidores espejo (servidores que replican los propios de RED-HAT), en las siguientes 72 horas después de su publicación por el equipo de RED-HAT. Normalmente estos paquetes están disponibles en 24 horas, no obstante, 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. Deberá tener en consideración que CentOS está basado en RED-HAT y ofrecen diferentes tiempos de implementación de actualizaciones. 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 Linux CentOS 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 Linux CentOS 8 Linux en la versión 8.1 (build 1911) 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 Linux CentOS 8 Linux en la versión 8.1 (build 1911) 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. 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.

6.1 CONFIGURACIÓN DE CONTRASEÑAS

Muchas contraseñas utilizadas por usuarios son bastante fáciles de adivinar. CentOS Linux proporciona diferentes maneras de proveer autentificación 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 autentificación, la seguridad de ese esquema estará por lo menos parcialmente a la merced de la complejidad de la contraseña elegida.

a) Una contraseña segura tiene que tener al menos estas características:

b) Tener una longitud mínima de 8 caracteres.

c) Mayúsculas y minúsculas alternadas.

d) Tantos signos de puntuación y números como sea posible.

e) Evitar palabras o frases comunes que puedan figurar en cualquier diccionario.

f) 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 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 debe seguir una serie de recomendaciones para ayudar a su correcta elección.

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

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 tercer 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	Journaled File System: fue introducido por IBM y aún se admite, pero ha sido sustituido por Ext4.
XFS	Linux/Red-HAT/CentOS	Sistema de archivos de 64 Bits, actualmente opción por defecto en Red Hat/CentOS Linux.
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.

Nota: Se optará por elegir XFS como sistema de archivos recomendado.

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

Partición	Tamaño
/	120 GiB xfs
/boot	500 MiB xfs
/boot/efi	Default MiB vfat
/var	50 GiB xfs
/tmp	25 GiB xfs
/var/log	35 GiB xfs
/home	200 GiB xfs
/var/log/audit	15 GiB xfs
/var/www	50 GiB xfs
swap	½ Memoria RAM Equipo

Nota: una vez instalado el sistema se recomienda cifrar las particiones aumentando la seguridad del mismo e impidiendo que personal no autorizado pueda acceder a datos críticos.

6.3 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 cargará 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 esta guía 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.

6.4 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.

6.4.1 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. Se montará con las opciones noauto, noexec, nodev, nosuid, ro.

b) **/boot/efi**. Se montará con los siguientes parámetros umask=0077, shortname=winnt <dump> 0 <pass> 0.

c) **/usr y /opt**. Contienen ficheros ejecutables del sistema. Se montará con las opciones nodev, ro.

d) **/var.** Contiene archivos muy variables del sistema (logs, BBDD, contenido web,etc.). Se montará con las opciones defaults, nosuid.

e) **/var/log.** Contiene los logs del sistema. Se montará con las opciones nodev, noexec, nosuid, rw.

f) **/var/log/audit.** Contiene información y logs de la herramienta Audit. Se montará con las opciones nodev, noexec, nosuid, rw.

g) **/var/www.** Contiene principalmente el contenido Web. Se montará con las opciones nodev, noexec, nosuid, rw.

h) **/home y /tmp.** Contienen los archivos del usuario y los temporales del sistema. Se montará con las opciones nodev, noexec, nosuid, rw y especialmente en /home se le asignará cuota de disco.

i) **/media/XXX.** Contiene montaje de particiones de dispositivos extraíbles. Se montará con las opciones noauto, nodev, nosuid, rw.

j) **/.** Contiene la partición raíz del sistema. Se montará con la opción de lectura y escritura (rw).

k) **Swap.** Se trata de la memoria de intercambio, memoria que usará el sistema cuando necesite espacio en memoria RAM. Se montará con la opción defaults, <dump> 0 <pass> 0.

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

a) **/boot.** Si se tuviera que actualizar el kernel, será necesario montar la partición temporalmente en lectura y escritura (rw).

b) **/usr y /opt.** Si se desea instalar una nueva aplicación o actualizar una ya existente, será necesario montar la partición correspondiente manualmente en modo de lectura y escritura(rw).

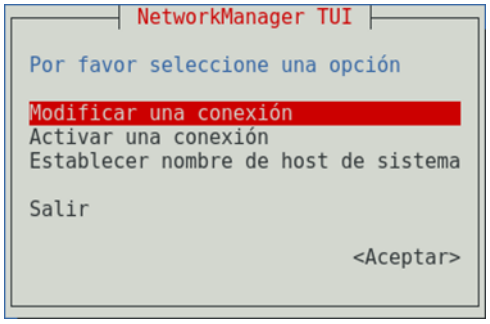
Nota: <dump> - Utilizado por el programa dump («volcado») para decidir cuándo hacer una copia de seguridad. Dump comprueba la entrada en el archivo fstab y el número de la misma le indica si un sistema de archivos debe ser respaldado o no. Las entradas posibles son 0 y 1. Si es 0, dump ignorará el sistema 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/centos-root/	xfs	defaults	1 1
UUID=xxxxxxxxxxxxxxxxxx/boot	xfs	noauto,noexec,nodev,nosuid,ro	1 2
UUID=xxxxxxxxxxxxxxxxx/boot/efi	xfs	umask=0077,shortname=winnt	0 0
/dev/mapper/centos-home/usr	xfs	nodev,ro	1 2
/dev/mapper/centos-home/opt	xfs	nodev,ro	1 2
/dev/mapper/centos-home/home	xfs	nodev,noexec,nosuid,rw	1 2
/dev/mapper/centos-tmp/tmp	xfs	nodev,noexec,nosuid,rw	1 2
/dev/mapper/centos-var/var	xfs	defaults,nosuid	1 2
/dev/mapper/centos-var_log/var/log	xfs	nodev,noexec,nosuid,rw	1 2
/dev/mapper/centos-var_log_audit/ var/log/audit	xfs	nodev,noexec,nosuid,rw	1 2
/dev/mapper/centos-var_www/var/ www	xfs	nodev,noexec,nosuid,rw	1 2
/dev/mapper/centos-swap swap	swap	defaults	0 0

6.4.2 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 **nmtui** (NetworkManager) 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 este 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.

6.4.3 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 ello, es conveniente 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 intentan explotar las debilidades del protocolo ICMP. Este se ha diseñado para comunicaciones unidireccionales que no requieren autentificación, 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 q 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.** La mayoría de las distribuciones Linux es 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 a trabajar en modo IPv6 en cualquier momento, y a veces en el menos inesperado, haciendo que sea víctima de algún ataque de red que afecte a IPv6, como son el de envenenamiento de vecinos - 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. Añadiendo la siguiente línea:

   i. net.ipv4.always_defrag = 1

6.4.4 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. CentOS Linux 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 deberá denegar 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. Más adelante, en esta guía, se explicará más detalladamente y con ejemplos ilustrativos la manera más segura de configurar los ficheros anteriores.

6.5 LIMITACIÓN DE RECURSOS DE USUARIO

Con el fin de limitar la utilización de recursos por parte de los usuarios del sistema y las acciones que los programas que ejecuta pueden llevar a cabo, es necesario aplicar ciertas configuraciones.

6.5.1 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 limitara "soft – core" y "hard – core" a 0.

6.5.2 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. A demás de los límites anteriores, se debe limitar las conexiones simultaneas 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".

6.5.3 BLOQUEAR EL USO DE ATAJOS CRÍTICOS

Para prevenir reinicios del sistema no deseados al utilizar la combinación de teclas Ctrl-Alt-Supr, se debe deshabilitar en los sistemas Core. 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.

6.5.4 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.

6.6 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.

6.6.1 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.

6.6.2 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.

6.6.3 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 almacenamiento, 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_faillock.so" pudiendo ser válido cualquier módulo que, siendo oficial del sistema operativo CentOS 8 Linux, realice la misma función:

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

6.6.4 LÍMITES DE INTENTO DE ACCESO AL SITEMA

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.

6.6.5 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 las distribuciones de Linux RHEL 8 y CentOS 8, 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 ntsysv 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.

La versión ntsysv 1.7.4 de Red Hat es la versión que viene por defecto en CentOS 8

6.7 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.

6.7.1 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. Se debe tener en cuenta que, al desinstalar el paquete padre (aplicación principal), no siempre se desinstalan las dependencias. Estas dependencias que quedan instaladas en el equipo, ocupando espacio en disco, son conocidos como paquetes huérfanos.

En este punto se hará hincapié en eliminar todos aquellos paquetes que se encuentren por defecto en la instalación propia de CentOS Linux o sean innecesarios para el correcto funcionamiento del sistema. Se procederá de la misma manera con todas sus correspondientes dependencias o paquetes huérfanos.

6.7.2 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.

6.8 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).

6.8.1 FICHEROS DE CONFIGURACIÓN

Los ficheros “/etc/profile” y “/etc/bashr”c 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 TMOUT.

   iii. Se restringe el tamaño del historial del intérprete de comandos al valor 1000 para los usuarios con la variable HISTSIZE.

b) /etc/bashrc:

   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.

6.8.2 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.

6.8.3 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".

7. CENTOS LINUX, NUEVAS FUNCIONALIDADES Y PRINCIPALES CAMBIOS

La versión 8 de CentOS 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 CentOS la distribución más idónea para entornos clasificados y ENS.

a) Estabilidad. CentOS 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. CentOS como solución corporativa basada en RHEL representa la mejor elección. Gracias a la detección proactiva de vulnerabilidades por parte del equipo de seguridad de Red Hat, su código fuente subyacente cuenta con un elevado nivel en seguridad. Además, a la hora de integrar nuevos programas o actualizar CentOS, la comprobación de la seguridad y de errores tienen prioridad.

c) Ciclos largos de mantenimiento y soporte. Desde la primera versión de CentOS, tanto los lanzamientos grandes como los pequeños han estado estrechamente vinculados a las publicaciones de RHEL. Para la adaptación del código, el equipo de desarrollo prevé un periodo de 2 a 6 semanas (o de unas pocas horas si se trata de pequeños cambios). Los números de cada versión se mantienen (por ejemplo, RHEL 6.2 a CentOS 6.2), aunque desde la versión 7 se añade una marca temporal (timestamp) que hace referencia a la publicación del código base. Así, por ejemplo, la fuente de la versión 7.0-1406 fue publicada en junio de 2014. Además del control de versiones, CentOS también se ha ocupado de las directrices para el periodo de soporte técnico: está previsto un soporte general de hasta 7 años y un suministro de hasta 10 años de actualizaciones de seguridad.

7.1 INSTALACIÓN

CentOS Linux 8 se instala utilizando imágenes ISO. Hay dos tipos de imágenes ISO disponibles para las arquitecturas AMD64, Intel 64-bit, ARM 64-bit, IBM Power Systems, e IBM Z:

a) DVD binario ISO: Una imagen de instalación completa que contiene los repositorios BaseOS y AppStream y le permite completar la instalación sin repositorios adicionales.

b) ISO de Arranque: Una imagen ISO de arranque mínimo que se utiliza para iniciar el programa de instalación. Esta opción requiere acceso a los repositorios BaseOS y AppStream para instalar paquetes de software. Los repositorios son parte de la imagen ISO del DVD Binario.

7.1.1 SOPORTE FORMATO DE ENCRIPTACIÓN LUKS2

El instalador de CentOS 8 Linux ahora usa el formato LUKS2 por defecto, pero se puede seleccionar una versión de LUKS desde la ventana de Particionado Personalizado de **Anaconda** o usando las nuevas opciones en los comandos logvol, part y RAID de Kickstart.

LUKS2 proporciona muchas mejoras y características, por ejemplo, amplía las capacidades del formato en disco y proporciona formas flexibles de almacenar metadatos.

7.1.2 PARÁMETROS DE ARRANQUE DEL KERNEL EN CENTOS 8

Anteriormente, sólo podía especificar un repositorio base desde los parámetros de arranque del núcleo. En CentOS 8 Linux, un nuevo parámetro de kernel (inst.addrepo=<name>,<url>) permite especificar un repositorio adicional durante la instalación.

Este parámetro tiene dos valores obligatorios: el nombre del repositorio y la URL que apunta al repositorio.

Nota: Para más información consulte el siguiente enlace.
https://anaconda-installer.readthedocs.io/en/latest/boot-options.html#inst-addrepo

7.1.3 ANACONDA SOPORTA ISOS UNIFICADAS EN CENTOS 8

En CentOS 8 Linux, se puede configurar una imagen en formato ISO que carga automáticamente los repositorios de origen de instalación de BaseOS y AppStream.

Esta característica funciona para el primer repositorio base que se carga durante la instalación. Por ejemplo, si arranca la instalación sin ningún repositorio configurado y se tiene la ISO unificada como repositorio base en la GUI, o si arranca la instalación usando la inst.repo=opción que apunta a la ISO unificada. Como resultado, el repositorio AppStream está habilitado en la sección Repositorios adicionales de la ventana de la GUI de origen de la instalación. No puede eliminar el repositorio de AppStream ni cambiar su configuración, pero puede desactivarlo en Fuente de instalación. Esta característica no funciona si arranca la instalación usando un repositorio base diferente y luego la cambia a la ISO unificada. Si lo hace, el repositorio base es reemplazado. Sin embargo, el repositorio de AppStream no se reemplaza y apunta al archivo original.

7.2 KERNEL

Los parches “en vivo” para el kernel ya están disponibles. Por medio de kpatch, se proporciona un mecanismo para parchear el núcleo en ejecución sin reiniciar ni reiniciar ningún proceso. Se proporcionarán parches de kernel “en vivo” para secuencias de actualizaciones menores de CentOS cubiertas por la política de Soporte de actualización extendida (EUS) para remediar CVE críticos e importantes.

7.2.1 COMPATIBLE CON EARLY KDUMP

La función early kdump permite que el kernel de bloqueo e initramfs se carguen lo suficientemente rápido como para capturar la información de vmcore incluso para fallos tempranos.

Para obtener más detalles sobre early kdump, se puede consultar el archivo /usr/share/doc/kexec-tools/early-kdump-howto.txt. dentro del sistema.

7.2.2 SOPORTE PARA IPCMNI_EXTEND

Se ha agregado un nuevo parámetro de línea de comando del kernel (ipcmni_extend) a CentOS 8 Linux. El parámetro amplía la cantidad de identificadores únicos de comunicación entre procesos del sistema V (IPC) y el máximo actual de 32 KB (15 bits) hasta 16 MB (24 bits). Como resultado, los usuarios cuyas aplicaciones producen muchos segmentos de memoria compartida pueden crear un identificador IPC mayor, sin exceder el límite de 32 KB.

Se debe de tener en cuenta que, en algunos casos, el uso de ipcmni_extend da como resultado una pequeña disminución de rendimiento y debe usarse solo si las aplicaciones necesitan más de 32 KB de identificador único de IPC.

7.2.3 LA GESTIÓN DE MEMORIA SOPORTA TABLAS DE PÁGINA DE 5 NIVELES

En CentOS 7, el bus de memoria existente tenía 48/46 bits de capacidad de direccionamiento de memoria física/virtual, y el núcleo de Linux implementó 4 niveles de tablas de página para gestionar estas direcciones virtuales a direcciones físicas. La línea de direccionamiento del bus físico sitúa el límite superior de capacidad de la memoria física en 64 TB.

Estos límites se han ampliado a 57/52 bits de direccionamiento de memoria virtual/física con 128 PiB de espacio de direcciones virtual y 4 PB de capacidad de memoria física.

Con el rango de direcciones extendido, la gestión de memoria en CentOS 8 Linux añade soporte para la implementación de tablas de páginas de 5 niveles, para poder manejar el rango de direcciones expandido.

7.3 GESTIÓN DE SOFTWARE

En CentOS 8 Linux, la instalación del software está garantizada por la nueva versión de la herramienta YUM, que se basa en la tecnología DNF.

YUM basado en DNF tiene las siguientes ventajas frente a la versión anterior (YUM v3) utilizado en CentOS 7:

a) Mayor rendimiento.

b) Soporte para contenido modular.

c) API estable y bien diseñada para la integración con herramientas.

Nota: Para más información de los cambios en YUM diríjase a la siguiente URL.
https://dnf.readthedocs.io/en/latest/cli_vs_yum.html

YUM basado en DNF es compatible con YUM v3 cuando se utiliza desde la línea de comandos, editando o creando archivos de configuración.

Para la instalación del software, se puede utilizar el comando yum y sus opciones particulares de la misma manera que en CentOS 7. Los paquetes se pueden instalar bajo los nombres anteriores usando “Provides”. Los paquetes también proporcionan enlaces simbólicos de compatibilidad, por lo que los binarios, archivos de configuración y directorios se pueden encontrar en las ubicaciones habituales.

Se debe de tener en cuenta que la “API Python” heredada proporcionada por YUM v3 y la “API Libdnf C“ son inestables y probablemente cambiarán durante el ciclo de vida de CentOS 8 Linux. Se aconseja a los usuarios migrar sus plugins y scripts a la nueva “API de DNF Python”, que es estable y totalmente compatible. La “API de DNF Python” está disponible en https://dnf.readthedocs.io/en/latest/api.html.

Algunas de las características del YUM v3 pueden comportarse de forma diferente en el YUM basado en DNF.

7.3.1 CARACTERÍSTICAS DESTACABLES DE RPM EN CENTOS 8

CentOS 8 Linux se distribuye con RPM 4.14. Esta versión introduce muchas mejoras con respecto a la RPM 4.11, que está disponible en CentOS 7. Las características más notables incluyen:

a) Los paquetes “debuginfo” se pueden instalar en paralelo.

b) Soporte para dependencias débiles.

c) Soporte para dependencias ricas o booleanas.

d) Compatibilidad con archivos de empaquetado de más de 4 GB de tamaño.

e) Compatibilidad con activadores de archivos.

f) Especificaciones más estrictas.

g) Comprobación simplificada de la firma de la salida en modo “no verbose”.

h) Adiciones y depreciación en las macros.

En CentOS 7, la utilidad RPM verificaba el contenido de la carga útil de los archivos individuales mientras se desempaquetaban. Sin embargo, esto es insuficiente por múltiples razones:

a) Si la carga útil está dañada, sólo se detecta después de ejecutar acciones de script, que son irreversibles.

b) Si la carga útil está dañada, la actualización de un paquete se interrumpe después de reemplazar algunos archivos de la versión anterior, lo que rompe una instalación en funcionamiento.

c) Los hashes de los archivos individuales se realizan sin comprimir, lo que hace que RPM sea vulnerable a las posibles vulnerabilidades de los descompresores.

En CentOS 8 Linux, el paquete completo es validado antes de la instalación en un paso separado, utilizando el mejor hash disponible.

Los paquetes construidos sobre CentOS 8 Linux utilizan un nuevo hash de SHA256 en la carga útil comprimida. En los paquetes firmados, el hash de la carga útil está adicionalmente protegido por la firma, y por lo tanto no puede ser alterado sin romper una firma y otros hashes en el encabezado del paquete. Los paquetes más antiguos utilizan el hash MD5 de la cabecera y la carga útil, a menos que esté deshabilitado por la configuración, como el modo FIPS.

La macro ”%_pkgverify_level” puede usarse para habilitar adicionalmente la verificación de firmas antes de la instalación o deshabilitar la verificación de la carga útil completamente. Además, la macro “%_pkgverify_flags” puede utilizarse para limitar qué hashes y firmas están permitidos. Por ejemplo, es posible desactivar el uso del hash MD5 débil a costa de la compatibilidad con paquetes más antiguos.

7.4 SERVICIOS DE INFRAESTRUCTURA

Se describen en esta sección los principales cambios en cuanto a servicios de infraestructura que se han modificado en la versión 8 de CentOS Linux.

7.4.1 GEOLITE 2

Las bases de datos “Geolite” que estaban presentes en CentOS 7 Linux fueron reemplazadas por las bases de datos Geolite2 en CentOS 8 Linux.

Las bases de datos “Geolite” fueron proporcionadas por el paquete “GeoIP”. Este paquete, junto con la base de datos heredada, ya no es compatible con la versión anterior.

Las bases de datos “Geolite2” son proporcionadas por múltiples paquetes. El paquete “libmaxminddb” incluye la biblioteca y la herramienta de línea de comandos “mmdblookup”, que permite la búsqueda manual de direcciones. El binario “geoipupdate” del paquete heredado “GeoIP” es ahora proporcionado por el paquete “geoipupdate”, y es capaz de descargar tanto las bases de datos heredadas como las nuevas bases de datos de “Geolite2”.

7.4.2 REGISTROS DE CUPS, JOURNALD

En CentOS 8, los registros CUPS ya no se almacenan en archivos específicos dentro del "/var/log/cups" que se utilizó en CentOS 7. En CentOS 8, todos los tipos de registros CUPS se registran de forma centralizada en el demonio systemd "journald" junto con los registros de otros programas. Para acceder a los registros CUPS, utilice el comando "journalctl -u cups".

7.5 SHELLS Y HERRAMIENTAS DE LÍNEA DE COMANDOS

El usuario "nobody" sustituye a "nfsnobody

En CentOS 7 Linux, había:

a) el par de usuarios nobody y grupos con el ID de 99

b) el par de usuario nfsnobody y grupo con el ID de 65534, que también es el ID de desbordamiento predeterminado del núcleo.

Ambos se han fusionado en el par de usuarios y grupos nobody, que utiliza el ID 65534 en CentOS 8 Linux. Las nuevas instalaciones ya no crean el nfsnobody.

Este cambio reduce la confusión sobre los archivos que son propiedad de NFS nobody pero no tienen nada que ver con NFS.

7.5.1 SISTEMAS DE CONTROL DE VERSIONES EN CENTOS 8

CentOS 8 ofrece los siguientes sistemas de control de versiones:

a) Git 2.18, un sistema de control de revisiones distribuido con una arquitectura descentralizada.

b) Mercurial 4.8, un sistema de control de versiones distribuido y ligero, diseñado para el manejo eficiente de grandes proyectos.

c) Subversion 1.10, un sistema de control de versiones centralizado.

Se debe tener en cuenta que el sistema de versiones simultáneas (CVS), disponible en CentOS 7, no se distribuye con CentOS 8.

7.5.1.1 CAMBIOS NOTABLES EN SUBVERSION 1.10

Subversion 1.10 introduce una serie de nuevas características desde la versión 1.7 distribuida en CentOS 7, así como los siguientes cambios de compatibilidad:

a) Debido a incompatibilidades en las librerías Subversion utilizadas para soportar los enlaces de lenguaje, los enlaces Python 3 para Subversion 1.10 no están disponibles. Como consecuencia, las aplicaciones que requieren fijaciones Python no están soportadas.

b) Ya no se soportan los repositorios basados en "Berkeley DB". Antes de migrar, se deberá realizar una copia de seguridad de los repositorios creados utilizando el comando "svnadmin dump" de Subversion 1.7. Después de instalar CentOS 8, Se deberán restaurar los repositorios utilizando el comando "svnadmin load".

c) Las copias de trabajo existentes obtenidas por el cliente Subversion 1.7 en CentOS 7 deben ser actualizadas al nuevo formato antes de que puedan ser utilizadas a partir de Subversion 1.10. Después de instalar CentOS 8, ejecute el comando “svn upgrade” en cada copia de trabajo.

d) Ya no se soporta la autenticación por tarjeta inteligente para acceder a los repositorios mediante el uso de repositorios “https://”.

7.6 ESCRITORIO

GNOME Shell, versión 3.28 está disponible en CentOS 8 Linux. Las mejoras notables incluyen:

a) Nuevas características de las cajas de GNOME

b) Nuevo teclado en pantalla

c) Compatibilidad con dispositivos extendidos, lo que es más importante, integración con la interfaz de Thunderbolt 3

d) Mejoras para el software GNOME, el editor de “dconf” y el terminal de GNOME.

7.6.1 WAYLAND COMO SERVIDOR DE VISUALIZACIÓN POR DEFECTO

la sesión de GNOME y el gestor de pantalla de GNOME (GDM) utilizan Wayland como su servidor de pantalla predeterminado en lugar del servidor X.org, que se utilizaba con la versión principal anterior de CentOS.

Wayland ofrece múltiples ventajas y mejoras sobre X.org:

a) Modelo de seguridad más sólido

b) Manejo mejorado de múltiples monitores

c) Escalado mejorado de la interfaz de usuario (UI)

d) El escritorio puede controlar directamente el manejo de ventanas.

Hay que tener en cuenta que las siguientes funciones no están disponibles actualmente o no funcionan como se espera:

a) En Wayland no se admiten configuraciones de varias GPUs.

b) El controlador binario de NVIDIA no funciona con Wayland.

c) La utilidad “xrandr” no funciona bajo Wayland debido a su diferente enfoque de manejo, resoluciones, rotaciones y diseño.

d) La grabación de pantalla, el escritorio remoto y la accesibilidad no siempre funcionan correctamente bajo Wayland.

e) No hay ningún administrador de portapapeles disponible.

f) Wayland ignora las capturas de teclado emitidas por las aplicaciones X11, como los visores de máquinas virtuales.

g) Wayland dentro de las máquinas virtuales huéspedes (VMs) tiene problemas de estabilidad y rendimiento, por lo que se recomienda utilizar la sesión X11 para entornos virtuales.

Si se actualiza a CentOS 8 desde un sistema CentOS 7 en el que utilizó la sesión de GNOME de X.org, su sistema seguirá utilizando X.org. El sistema también vuelve automáticamente a X.org cuando se utilizan los siguientes controladores de gráficos:

a) El controlador binario de NVIDIA

b) El conductor cirrus

c) El conductor mga

d) El conductor aspeed

Puede desactivar el uso de Wayland manualmente:

Para deshabilitar Wayland en GDM, establezca la opción de Wayland “Enable=false” en el fichero de configuración “/etc/gdm/custom.conf”.

Para desactivar Wayland en la sesión de GNOME, seleccione la opción X11 heredada utilizando el menú de rueda dentada en la pantalla de inicio de sesión después de introducir su nombre de usuario.

Nota: Para más detalles sobre Wayland, diríjase a la siguiente URL.
https://wayland.freedesktop.org/

7.6.2 LOCALIZACIÓN DE PAQUETES RPM QUE ESTÁN EN REPOSITORIOS NO HABILITADOS POR DEFECTO

Los repositorios adicionales para el escritorio no están habilitados de forma predeterminada. La desactivación se indica por la línea enabled=0 del archivo correspondiente “.repo”. Si se intenta instalar un paquete desde dicho repositorio usando “PackageKit”, éste muestra un mensaje de error anunciando que la aplicación no está disponible. Para que el paquete esté disponible, se deberá reemplazar la línea enabled=0 usada anteriormente en el archivo respectivo “.repo” con enabled=1.

7.6.3 SOFTWARE DE GNOME PARA LA GESTIÓN DE PAQUETES

El paquete gnome-packagekit que proporcionaba una colección de herramientas para la gestión de paquetes en un entorno gráfico en CentOS 7 Linux ya no está disponible. En CentOS 8 Linux, la utilidad del Software GNOME, que le permite instalar y actualizar aplicaciones y extensiones gnome-shell, proporciona una funcionalidad similar. El Software GNOME se distribuye en el paquete gnome-software.

7.7 GESTIÓN DE IDENTIDADES

Esta mejora añade nuevas comprobaciones de sintaxis de contraseñas al servidor de directorios. Los administradores pueden ahora, por ejemplo, habilitar las comprobaciones del diccionario, permitir o denegar el uso de secuencias de caracteres y palíndromos. Como resultado, si está habilitado, la comprobación de la sintaxis de la política de contraseñas en el Servidor de directorios hace que las contraseñas sean más seguras.

7.7.1 SERVIDOR DE DIRECTORIOS

El servidor de directorios ahora proporciona soporte mejorado para el registro de operaciones internas. Varias operaciones en el servidor de directorios, iniciadas por el servidor y los clientes, causan operaciones adicionales en segundo plano. Anteriormente, el servidor sólo registraba la palabra clave de conexión "Internal" para las operaciones internas, y el ID de la operación siempre se establecía en -1. Con esta mejora, el servidor de directorio registra el ID de conexión y operación real. Ahora puede rastrear la operación interna hasta la operación del servidor o cliente que causó esta operación.

Nota: Para más detalles sobre el registro de operaciones internas, diríjase al siguiente enlace: https://access.redhat.com/documentation/en-us/red_hat_directory_server/11/html-single/administration_guide/#logging_internal_operations.

7.7.2 DIRECTORY SERVER

Directory Server presenta nuevas utilidades de línea de comandos para gestionar instancias. CentOS Directory Server presenta "dscreate", "dsconf", y dsctl. Estas utilidades simplifican la gestión del servidor de directorios mediante la línea de comandos. Por ejemplo, ahora se puede utilizar un comando con parámetros para configurar una característica en lugar de enviar complejas instrucciones LDIF al servidor.

A continuación, se ofrece una descripción general del propósito de cada utilidad:

a) La utilidad dscreate crea nuevas instancias del servidor de directorios utilizando el modo interactivo o un archivo INF. Se debe tener en cuenta que el formato de archivo INF es diferente al que el instalador usaba en versiones anteriores del servidor de directorios.

b) La utilidad dsconf gestiona las instancias del servidor de directorios durante el tiempo de ejecución. Por ejemplo, se usa dsconf para:

   i. Configurar las opciones en la cn=configentrada

   ii. Configurar plug-ins

   iii. Configurar la replicación

   iv. Realizar una copia de seguridad y restaurar una instancia

c) La utilidad dsctl gestiona las instancias del servidor de directorios mientras están desconectadas. Por ejemplo, se usa dsctl para:

   i. Iniciar y detener una instancia

   ii. Re-indexar la base de datos del servidor

   iii. Realizar una copia de seguridad y restaurar una instancia

Estas utilidades sustituyen a los scripts Perl y shell marcados como obsoletos en Directory Server 10. Los scripts siguen estando disponibles en el paquete no soportado389-ds-base-legacy-tools, sin embargo, CentOS sólo soporta la gestión de Directory Server utilizando las nuevas utilidades.

Tenga en cuenta que la configuración del servidor de directorios mediante sentencias LDIF sigue siendo compatible, pero CentOS recomienda utilizar las nuevas utilidades.

7.7.3 SISTEMA DE CERTIFICADOS

El sistema de certificados ahora admite la renovación offline de los certificados del sistema. Con esta mejora, los administradores pueden utilizar la función de renovación offline para renovar los certificados de sistema configurados en el sistema de certificados. Cuando un certificado de sistema expira, el sistema de certificados no se inicia. Como resultado de la mejora, los administradores ya no necesitan soluciones adicionales para reemplazar un certificado de sistema caducado.

Además, el sistema de certificados admite la creación de una solicitud de firma de certificado (CSR) con la extensión Subject Key Identifier (SKI) para la firma de autoridad de certificación externa (CA). Algunas CA requieren esta extensión, ya sea con un valor particular o derivada de la clave pública de la CA. Como resultado, los administradores ahora pueden utilizar el parámetro “pki_req_ski” del archivo de configuración pasado a la utilidad “pkispawn” para crear una CSR con extensión SKI.

7.7.4 USUARIOS LOCALES Y SSSD

Los usuarios locales son almacenados en caché por SSSD y atendidos a través del módulo “nss_sss”. En CentOS 8, el demonio de servicios de seguridad del sistema (SSSD) sirve por defecto a usuarios y grupos desde los archivos “/etc/passwd” y “/etc/groups”. El módulo sss “nsswitch” precede a los archivos en el archivo “/etc/nsswitch.conf”.

La ventaja de servir a los usuarios locales a través de SSSD es que el módulo nss_sss tiene un cache “memory-mapped” que acelera las búsquedas de Name Service Switch (NSS) en comparación con el acceso al disco y la apertura de los archivos en cada solicitud NSS. Anteriormente, el demonio de caché del servicio Name (nscd) ayudó a acelerar el proceso de acceso al disco. Sin embargo, el uso nscd en paralelo con SSSD es engorroso, ya que, tanto SSSD como nsc hacen uso de su propio caché independiente. Por consiguiente, el uso nscd en configuraciones en las que los SSSD también sirven a usuarios de un dominio remoto, por ejemplo LDAP o Active Directory, puede causar un comportamiento impredecible.

Con esta actualización, la resolución de los usuarios y grupos locales es más rápida en CentOS 8. Tenga en cuenta que el usuario root nunca tiene acceso por SSSD, por lo tanto, la resolución root no puede verse afectada por un posible fallo en SSSD. Tenga en cuenta también que, si el SSSD no se está ejecutando, el módulo nss_sss resuelve la situación. No es necesario configurar los SSSD de ninguna manera, el dominio de los archivos se añade automáticamente.

7.7.5 KCM

KCM reemplaza a KEYRING como almacenamiento de caché de credenciales predeterminado. El almacenamiento de caché de credenciales predeterminado es el Kerberos Credential Manager (KCM), que está respaldado por el demonio sssd-kcm. KCM supera las limitaciones de la LLAVE utilizada anteriormente, como la dificultad de su uso en entornos basados en contenedores al no estar espaciada por nombres, así como para visualizar y gestionar cuotas.

Con esta actualización, CentOS 8 contiene una caché de credenciales que se adapta mejor a entornos basados en contenedores y que proporciona una base para crear más funciones en futuras versiones.

7.7.6 ACTIVE DIRECTORY Y GESTIÓN DE IDENTIDADES

CentOS 8 permite añadir una sustitución de ID de usuario para un usuario de Active Directory (AD) como miembro de un grupo de gestión de identidades (IdM). Una sustitución de ID es un registro que describe cómo deben verse las propiedades de un usuario o grupo de AD específico dentro de una vista de ID específica, en este caso la Vista de confianza predeterminada. Como consecuencia de la actualización, el servidor LDAP IdM puede aplicar reglas de control de acceso para el grupo IdM al usuario AD.

Los usuarios de AD ahora pueden utilizar las funciones de autoservicio de la interfaz IdM, por ejemplo, para cargar sus claves SSH o cambiar sus datos personales. Un administrador de AD puede administrar completamente la IdM sin tener dos cuentas y contraseñas diferentes. Tenga en cuenta que actualmente, las funciones seleccionadas en IdM pueden no estar disponibles para los usuarios de AD.

7.7.7 GRABACIÓN DE SESIONES

Se ha añadido una solución de grabación de sesiones a CentOS 8 Un nuevo paquete “tlog” y su reproductor de sesiones de consola web asociado permiten grabar y reproducir las sesiones del terminal de usuario. La grabación se puede configurar por un usuario o grupo de usuarios a través del servicio System Security Services Daemon (SSSD). Todas las entradas y salidas del terminal se capturan y almacenan en formato de texto en un diario del sistema. La entrada está inactiva por defecto por razones de seguridad para no interceptar contraseñas sin procesar y otra información sensible.

La solución puede utilizarse para auditar las sesiones de usuario en sistemas sensibles a la seguridad. En caso de una violación de la seguridad, las sesiones grabadas pueden ser revisadas como parte de un análisis forense. Los administradores del sistema pueden ahora configurar localmente la grabación de la sesión y ver el resultado desde la interfaz de la línea de comandos utilizando la utilidad tlog-play.

7.8 SISTEMAS DE ARCHIVOS Y ALMACENAMIENTO

El sistema de archivos XFS soporta la funcionalidad de extensión de datos de copia sobre escritura compartida. Esta función permite que dos o más archivos compartan un conjunto común de bloques de datos. Cuando cualquiera de los archivos que comparten bloques comunes cambia, XFS rompe el enlace con los bloques comunes y crea un nuevo archivo. Esto es similar a la funcionalidad de copia sobre escritura (COW) que se encuentra en otros sistemas de archivos.

Las nuevas funcionalidades son las siguientes:

a) Rapidez. La creación de copias compartidas no utiliza E/S de disco.

b) Eficiencia de espacio. Los bloques compartidos no consumen espacio de disco adicional.

c) Transparencia. Los archivos que comparten bloques comunes actúan como archivos normales.

Las utilidades del espacio de usuario pueden usar extensiones de datos de copia sobre escritura compartidas para:

a) Clonación eficiente de archivos, como con el comando “cp --reflink”.

b) Instantáneas por archivo.

Esta funcionalidad también es utilizada por subsistemas del núcleo como Overlayfs y NFS para una operación más eficiente.

Al crear un sistema de archivos XFS, las extensiones de datos de copia sobre escritura compartidas están habilitadas de forma predeterminada, comenzando con la versión del paquete "xfsprogs 4.17.0-2.el8".

Se debe tener en consideración que los dispositivos de acceso directo (DAX) actualmente no admiten XFS con extensiones de datos de copia sobre escritura compartidas. Para crear un sistema de archivos XFS sin esta función, utilice el siguiente comando:

```
# mkfs.xfs -m reflink=0 block-device
```

CentOS 7 Linux puede montar sistemas de archivos XFS con extensiones de datos de copia sobre escritura compartidas solamente en el modo de "read only".

Además, el tamaño máximo admitido de un sistema de archivos XFS se ha aumentado de 500 TiB a 1024 TiB. En CentOS 8, la utilidad "mkfs.xfs" crea sistemas de archivos que cumplen estos requisitos de forma predeterminada. No se admite el crecimiento de un sistema de archivos más pequeño que no cumpla estos requisitos a un tamaño superior a 500 TiB.

7.8.1 CIFRADO VOLÚMENES CON LUKS2

En CentOS 8 Linux, el formato LUKS versión 2 (LUKS2) sustituye al formato LUKS heredado (LUKS1). El subsistema "dm-crypt" y la herramienta "cryptsetup" utilizan ahora LUKS2 como formato predeterminado para los volúmenes cifrados. LUKS2 proporciona volúmenes cifrados con redundancia de metadatos y auto-recuperación en caso de un evento parcial de corrupción de metadatos.

Gracias a su diseño interno flexible, LUKS2 está pensado para futuras mejoras e implementaciones. Soporta el auto desbloqueo a través del token genérico de "kernel-keyring" incorporado en libcryptsetup que permite a los usuarios desbloquear volúmenes LUKS2 utilizando una frase de contraseña almacenada en el servicio de retención de "kernel-keyring".

Entre otras mejoras LUKS2 incluye:

a) La configuración de la clave protegida utiliza un nuevo esquema de cifrado.

b) Integración más fácil con el descifrado basado en políticas (Clevis).

c) Hasta 32 ranuras para llaves, LUKS1 proporciona sólo 8 ranuras para llaves.

7.9 FUNCIONALIDADES DE RED

La herramienta "Nftables" reemplaza a "iptables" como el marco de filtrado de paquetes de red predeterminado. La herramienta nftables proporciona instalaciones de clasificación de paquetes y es el sucesor designado de las herramientas iptables/ip6tables, arptables, y ebtables. Ofrece numerosas mejoras en comodidad, características y rendimiento en comparación con las herramientas de filtrado de paquetes anteriores:

a) Tablas de búsqueda en lugar de procesamiento lineal.

b) Un marco único tanto para los IPv6s, como para los protocolos IPv4.

c) Todas las reglas se aplican automáticamente en lugar de obtener, actualizar y almacenar un conjunto de reglas completo.

d) Soporte para depuración y rastreo en el conjunto de reglas (nftrace) y monitoreo de eventos de rastreo (en la herramienta nft).

e) Sintaxis más consistente y compacta, sin extensiones específicas de protocolo.

f) Una API de Netlink para aplicaciones de terceros.

Al igual que en el caso de las cadenas de almacenamiento iptables, nftables utiliza tablas para almacenarlas. Las cadenas contienen reglas individuales para realizar acciones. La herramienta nft reemplaza todas las herramientas de los marcos de trabajo de filtrado de paquetes anteriores. La librería libnftables se puede utilizar para la interacción de bajo nivel con la API de Netlink nftables a través de la librería libmnl.

Las herramientas iptables, ip6tables, ebtables y arptables se sustituyen por comandos basados en nftables con el mismo nombre. Mientras que el comportamiento externo es idéntico al de sus homólogos heredados, internamente utilizan nftables con módulos del núcleo netfilter heredados a través de una interfaz de compatibilidad cuando es necesario.

El efecto de los módulos sobre el conjunto de reglas nftables se puede observar usando el comando “nft list ruleset”. Dado que estas herramientas añaden tablas, cadenas y reglas al conjunto de reglas nftables, se ha de tener en cuenta que las operaciones de conjunto en nftables, como el comando “nft flush ruleset”, pueden afectar a las configuraciones implementadas utilizando los comandos heredados.

Para identificar rápidamente qué variante de la herramienta está presente, se ha actualizado la información de la versión para incluir el nombre del back-end. En CentOS 8, la herramienta basada en nftables/iptables imprime la siguiente información:

```
$ iptables --version
iptables v1.8.0 (nf_tables)
```

Para la comparación, se muestra la siguiente información de versión si la herramienta heredada iptables está presente:

```
$ iptables --version
iptables v1.8.0 (legacy)
```

7.9.1 FIREWALLD

Con motivo de la actualización de la herramienta nfstables, el demonio firewalld se actualiza, utilizando como “backend” predeterminado las funcionalidades de la misma. Para modificar el módulo de servicio, se deberá utilizar la opción “FirewallBackend” del archivo “/etc/firewalld.conf”.

Este cambio introduce las siguientes diferencias en el comportamiento cuando se utiliza nftables:

a) Las ejecuciones de reglas iptables siempre ocurren antes que las reglas de firewalld, de manera que:

   i. DROP en iptables significa que un paquete nunca es revisado por firewalld.

   ii. ACCEPT en iptables significa que un paquete sigue estando sujeto a revisión de las reglas de firewalld.

b) Las reglas directas de firewalld se siguen implementando a través de otras funciones propias, mientras que las de iptables utilizan nftables.

c) la ejecución directa de las reglas ocurre antes de la aprobación genérica de las conexiones establecidas por firewalld.

Además, esta actualización añade las herramientas iptables-translate e ip6tables-translate para convertir las reglas existentes en las equivalentes para nftables. Se ha de tener en cuenta que algunas extensiones carecen de soporte de traducción. Si existe tal extensión, la herramienta imprime la regla no traducida precedida por el signo "#". Por ejemplo:

```
| % iptables-translate -A INPUT -j CHECKSUM --checksum-fill
| nft # -A INPUT -j CHECKSUM --checksum-fill
```

Los usuarios pueden utilizar las herramientas iptables-restore-translate y ip6tables-restore-translate para traducir un volcado de reglas. Antes de eso, los usuarios pueden usar los comandos iptables-save o ip6tables-save para imprimir un volcado de las reglas actuales.

7.10 SEGURIDAD

Se han rediseñado varios complementos del sistema operativo CentOS 8 Linux para proporcionar un aumento en la seguridad global del sistema.

7.10.1 OPENSSH

Los paquetes openssh han sido actualizados a la versión 7.8p1. Los cambios incluyen:

a) Se ha eliminado el soporte para el protocolo SSH version 1.

b) Se ha eliminado el soporte para el código de autenticación de mensajes hmac-ripemd160.

c) Eliminado el soporte para RC4 (arcfour) cifrado.

d) Eliminado el soporte para el cifrado Blowfish.

e) Eliminado el soporte para el cifrado CAST.

f) Cambiado el valor por defecto de la opción UseDNS a no.

g) Algoritmos de clave pública DSA desactivados por defecto.

h) Cambiado el tamaño mínimo del módulo para los parámetros Diffie-Hellman a 2048 bits.

i) Cambiada la semántica de la opción de configuración ExposeAuthInfo.

j) La opción UsePrivilegeSeparation=sandbox es ahora obligatoria y no se puede desactivar.

k) Configure el tamaño mínimo aceptado de la clave RSA en 1024 bits.

7.10.2 CAMBIOS NOTABLES EN RSYSLOG

Los paquetes rsyslog han sido actualizados a la versión 8.37.0, que proporciona muchas correcciones y mejoras con respecto a las versiones anteriores. Los cambios incluyen:

a) Mejora del procesamiento de los mensajes internos de rsyslog; posibilidad de limitar la velocidad de los mensajes; se ha corregido un posible punto muerto.

b) Mejora de la limitación de la velocidad en general.

c) Administración mejorada de mensajes de gran tamaño, el usuario puede ahora establecer el modo de tratamiento, tanto en el núcleo como en ciertos módulos con acciones separadas.

d) Las bases de reglas “mmnormalize” ahora pueden ser incrustadas en el archivo de configuración en lugar de crear archivos separados para ellas.

e) El usuario ahora puede configurar la cadena de prioridad de “GnuTLS” para que “imtcp” permita un control detallado sobre el cifrado.

f) Todas variables de configuración, incluyendo las variables en JSON, son indiferentes a mayúsculas y minúsculas.

g) Varias mejoras en la salida de PostgreSQL.

h) Añadida la posibilidad de usar variables shell para controlar la configuración del procesamiento, como la carga condicional de archivos de configuración adicionales, la ejecución de sentencias o la inclusión de un texto en archivos “config”. Un uso excesivo de esta característica puede hacer que sea muy difícil depurar problemas con rsyslog.

i) Los modos de creación de archivos de 4 dígitos se pueden especificar ahora en “config”.

j) La entrada Relp (Relief Event Logging Protocol) ahora puede enlazar también sólo en una dirección específica.

k) El valor predeterminado de la opción “enable.body” de salida de correo ahora está alineada con la documentación.

l) El usuario puede ahora especificar códigos de error de inserción que deben ser ignorados en la salida de MongoDB.

m) La entrada paralela TCP (pTCP) tiene ahora el retraso configurable para un mejor balanceo de carga.

7.10.3 POLÍTICAS CRIPTOGRÁFICAS

Las políticas criptográficas de todo el sistema se aplican por defecto. Crypto-policies es un componente de CentOS 8 Linux, que configura los principales subsistemas criptográficos, cubriendo los protocolos TLS, IPSec, SSH, DNSSec y Kerberos. Proporciona un pequeño conjunto de políticas, que el administrador puede seleccionar utilizando el comando “update-crypto-policies”.

La política criptográfica “DEFAULT” de todo el sistema ofrece una configuración segura para los modelos de amenazas actuales. Permite los protocolos TLS 1.2 y 1.3, así como los protocolos IKEv2 y SSH2. Las claves RSA y los parámetros Diffie-Hellman se aceptan si son mayores de 2047 bits.

7.10.4 HERRAMIENTA AUDIT

Audit 3.0 reemplaza “audispd” con “auditd”. Con esta actualización, la funcionalidad de audispd se ha movido a auditd. Como resultado, las opciones de configuración audispd son ahora parte de auditd.conf. Además, el directorio plugins.d se ha movido a la ruta /etc/audit. El estado actual de los plug-ins auditd se puede comprobar ejecutando el comando “service auditd state”.