FORTRA

GUÍA (Powertech)

# PIM, PAM y PUM: Mejores Prácticas para la Gestión de Accesos y Permisos Privilegiados en Linux/UNIX

PIM, PAM y PUM pueden tener significados e interpretaciones diferentes, según la persona a la que se consulte. Sin embargo, son conceptos que se cruzan y hacen referencia a lo mismo:

- **PIM:** Gestión de Permisos Privilegiados (Privileged Identity Management);
- **PAM:** Gestión de Cuentas o Accesos Privilegiados (Privileged Account Management o Privileged Access Management); y
- **PUM:** Gestión de Usuarios Privilegiados (Privileged User Management).

Estos tres acrónimos giran alrededor de algunos conceptos simples: quién puede acceder a un servidor, máquina virtual o imagen de sistema, cómo pueden ingresar al Sistema Operativo, y qué pueden hacer una vez dentro de él.

## Gestión de Cuentas

Si queremos hablar sobre control de accesos y gestión de permisos, debemos comenzar con las cuentas que están configuradas para permitir el uso de un sistema. En general, crear cuentas es una tarea bastante sencilla, pero deshabilitar o eliminar cuentas que ya no son requeridas, ha sido un desafío para las empresas durante muchos años, y lo seguirá siendo. El riesgo que conlleva dejar cuentas activas que no deberían estarlo ha producido distintas consecuencias. Un ejemplo histórico es una bomba lógica configurada por un empleado que ese mismo día había sido notificado de su despido y continuó trabajando durante la jornada con los permisos de acceso total que había necesitado en sus funciones como administrador. Ese es un ejemplo de una cuenta de tipo “persona”.

Los sistemas Linux y el legacy UNIX requieren siempre, de alguna manera, una cuenta para que alguien tenga acceso al sistema. Normalmente, las personas acceden a los sistemas Linux/UNIX de manera directa cuando están ejecutando una tarea administrativa en el Sistema Operativo, en aplicaciones o con datos críticos.

Sin embargo, "persona" es solo uno de los tipos de cuenta que se requieren en estos sistemas. Los sistemas por sí mismos, necesitan de otras cuentas determinadas para funcionar, como la potente cuenta “root”. Por su parte, las aplicaciones también necesitan algunos otros tipos de cuenta en un servidor para funcionar de manera apropiada.

Cuando se piensa en la administración de cuentas de usuario, en general se piensa solo en la administración de cuentas tipo “persona”, dejando fuera todos los otros tipos de cuentas que el sistema usa y requiere.

Esta mirada parcial de la administración de cuentas de usuario conlleva una brecha de Seguridad importante en muchas empresas.

## Implemente el mínimo de privilegios

Las acciones que una cuenta está autorizada a realizar una vez iniciada la sesión son, probablemente, más importantes que controlar quién ingresa. Imagine que todos en la empresa pudieran ingresar a un sistema, pero que solo pudieran realizar las tareas que son necesarias para su función. Muchas personas directamente no podrían hacer nada. El riesgo de habilitar accesos es -en general- menos grave que controlar lo que las personas pueden hacer.

Considere lo siguiente:

- ¿Todos los administradores de sistemas necesitan estar registrados como “root”?
- ¿Necesitan poder ejecutar cada comando sobre el que “root” tiene el permiso de ejecución?
- ¿Los administradores de bases de datos necesitan accesos "root" o deben ser prevenidos de ejecutar comandos de sistemas que no son parte de su función?
- ¿Qué pasa con las cuentas utilizadas para la comunicación entre aplicaciones?
- ¿Una computadora que se comunica con otra requiere acceso a todos los comandos que pueden ser ejecutados o existe un conjunto reducido de comandos que requieren estos procesos automatizados?

## Gestión de contraseñas

Más allá de que se recomienda una autenticación robusta para el inicio de sesión de “personas”, existen casos y lugares en los que las contraseñas todavía son, y deben ser, utilizadas. Donde existan las contraseñas, hay una necesidad de gestionarlas. La mayoría de las personas ya cuenta con alguna experiencia en este sentido, ya sean técnicos o no. Gestionar contraseñas incluye lo básico: que la contraseña sea modificada periódicamente, prohibir la reutilización de antiguas contraseñas, o requerir cierto nivel de complejidad en ellas. Estas son algunas de las reglas básicas de la gestión de contraseñas.

La administración de contraseñas debe hacer referencia a TODAS las contraseñas: de usuarios, de cuentas de aplicaciones / funcionales / de servicios, y a las de la poderosa cuenta "root".

## Elimine el uso de cuentas compartidas

Esto es especialmente importante para las personas que acceden al sistema. Dos administradores de un sistema no deben compartir una cuenta, ya que ésta es la que registra y contabiliza las acciones realizadas. Esto no aplica solo a los administradores del Sistema Operativo, sino para todo aquel que acceda al sistema para trabajar en aplicaciones o datos. Para algunas organizaciones eso puede significar muchas cuentas a gestionar a través de muchos servidores, pero el objetivo de no tener a dos personas compartiendo una cuenta para el acceso a un sistema debería motivar la planificación y el proceso de requerimientos previos a la implementación de PIM/ PAM/PUM.

Existen algunas cuentas que simplemente no se pueden eliminar. Cada sistema Linux/UNIX tiene una cuenta "root" y muchas aplicaciones tienen una configuración de cuenta para asociar sus procesos y limitar los permisos de la aplicación en el sistema, y, a veces, una aplicación del Sistema Operativo o un administrador de datos necesitará realizar algunas actividades con los privilegios del Sistema Operativo, de la aplicación o del servicio de datos.

Implemente un sistema donde una persona pueda ejecutar comandos como otra cuenta, sin tener que iniciar sesión como esa cuenta ni convertirse en esa identidad. Utilizando el comando tradicional de Linux/UNIX "sudo", un usuario puede elevar los permisos o cambiar la identidad, y ejecutar un comando con el permiso o la identidad que haya seleccionado. Ese tipo de modelo elimina la necesidad de tener una cuenta compartida y permite registrar y contabilizar las actividades realizadas en el sistema.

Sin embargo, las cuentas de personas no son las únicas. Existe al menos una cuenta ("root") que los administradores de sistemas pueden necesitar, pero puede haber otras más. Cuando iniciar sesión con el usuario "root" (u otra cuenta) es la única opción posible, se requiere un modelo que proporcione a una persona el atributo de uso sobre la cuenta "root" dejando pistas de auditoría claras de su uso.

## Accesos de control

No todas las cuentas son iguales, ni todas las cuentas disponibles en un sistema necesitan acceder a él a través de la red. Si ha implementado de forma apropiada el control de permisos, entonces nadie necesitará iniciar sesión como "root" cuando se conectan vía SSH para hacer mantenimiento. Pero, la cuenta “root” seguirá necesitando ser capaz de iniciar sesión en una consola para una ocasión específica en la que algo haya salido terriblemente mal y un administrador necesite entrar en el datacenter e investigar.

No todas las cuentas necesitan acceso a todos los servidores desde todas las computadoras de la red. Las autenticaciones automatizadas desde una aplicación a otra, o de un sistema a otro, no necesitan estar disponibles desde cualquier lugar. De hecho, casi por definición, solo deberían estar permitidas desde el sistema que esté ejecutando la tarea, de modo que el objetivo solo permita a esa cuenta conectar de ese modo y realizar esa tarea, desde una locación definida.

También los administradores deberían tener algunas limitaciones. Un administrador en una locación segura, en una red segura y en un sistema seguro, debería estar autorizado a hacer mucho más que si iniciara sesión desde su laptop, a través de una VPN en una habitación de hotel.

El control de accesos debería ser granular y el contexto de acceso debe alimentar las decisiones de autorización. Dónde, cuándo y cómo una cuenta accede al sistema debería ser determinante en la decisión sobre qué es lo que la cuenta puede hacer una vez que llegue allí.

## Log, Log, Log, Log

Registre cambios, registre accesos, registre permisos y registre fallas. Los registros son una buena idea, y la mayoría de los equipos de Seguridad, Cumplimiento y auditores lo entienden. Pero también requiere tiempo y recursos para almacenar y analizar todos esos mensajes, que pueden llegar a ser cientos de miles cada día.

Usted debe ser capaz de generar reportes sobre quién ha accedido a qué y cuándo, algo requerido por muchas normativas y regulaciones tales como PCI (el estándar de Seguridad para la industria de tarjetas de crédito), SOX, o las nuevas leyes sobre protección de datos personales, como GDPR. Sin embargo, generar reportes sobre las políticas implementadas, no es un registro de auditoría.

Grabar y registrar cualquier cambio en las cuentas o en su titularidad, como la incorporación, eliminación u otras actividades referidas a las reglas que afectan a quién puede acceder a qué, desde dónde y cuándo, es un registro de auditoría. Todos los cambios a las cuentas, niveles de acceso y otras reglas deben ser registrados para que el administrador que haya modificado las reglas pueda ser identificado.

El registro de accesos es casi una obviedad. Al registrar quién inicia sesión, debe conocer qué cuenta está siendo utilizada, cómo ha sido autenticada, de dónde proviene y cómo se conecta. Esto es un syslog típico (pero debe tener en cuenta que esto es considerado el nivel VERBOSE de registro en una instalación OpenSSH out-of-the-box).

Cuando una cuenta necesite ejecutar comandos con un nivel diferente de permisos, eso debe ser registrado. Esto vuelve al punto de “quién hace qué y cuándo” y es más que importante por diversas razones. Las operaciones privilegiadas tienen la capacidad de acceder potencialmente a cualquier dato disponible en el sistema y de destruir o dañar la capacidad del sistema de ejecutar sus funciones. ¡Esto puede ser fatal para su empresa! Por lo tanto, debe tener en cuenta dos cuestiones. Primero, al ocurrir un problema, usted necesita saber exactamente quién lo ocasionó. Segundo, si los usuarios saben que sus acciones son vigiladas, es más probable que no realicen ninguna actividad dañina.

Por último, pero no por eso menos importante: los inicios de sesión fallidos. Si una cuenta ejecuta autenticación automática por medio de una llave SSH y, de repente, esa cuenta está intentando acceder con la misma llave, pero desde un host que no debería, ese es un problema del que usted quisiera enterarse. Obviamente, lo mejor sería bloquear el acceso y enviar una notificación. Este y cualquier tipo de fallos en relación con las reglas implementadas manifestarán una de dos cosas: o sus reglas están mal o algo está pasando que no debería.

## Gestione y registre la actividad privilegiada

Está bien saber quién accede a qué host, cuándo, desde dónde y cómo. También saber que determinada cuenta elevó sus permisos para acceder a un comando adicional. Pero, a veces, más es mejor.

Si algo malo ocurre, lo mejor es tener la capacidad de analizar los datos y entender quién lo hizo. Sin embargo, el registro a nivel de pulsación de teclas le permite ver exactamente qué hicieron. Cuando algo malo ocurre, los detalles importan.

Gestionar quién tiene los derechos a qué, a dónde y cuándo, es una herramienta potente. Generalmente, los administradores necesitan ejecutar comandos con otros permisos que los asignados a su propia cuenta. Estos pueden ser administradores de aplicaciones o de bases de datos que deben realizar mantenimiento o configurar operaciones, o pueden ser administradores de sistemas. En el pasado, todos estos administradores querían que se les concediera un control total, con acceso "root". Sin embargo, esto no es necesario. El acceso "root" es solo un atajo y una solución sencilla. Garantiza que la Gestión de Permisos no se convierta en un impedimento a la productividad, pero también es una receta para un próximo desastre.

***"El acceso root es un atajo y una solución sencilla. Garantiza que la Gestión de Permisos no se convierta en un impedimento para la productividad, pero también es una receta para un próximo desastre".***

Existen dos formas en la que los permisos excesivos pueden causar tremendos problemas a la organización. Primero, el abuso de la cuenta por un actor de confianza. Podemos pensar en episodios como el caso Snowden, donde un administrador convertido en delincuente abusó de sus permisos y accesos en detrimento de la empresa. Incluso hoy, luego de ejemplos como estos, es difícil para muchas empresas ser escépticos en relación a quienes deberían ser personas de máxima confianza encargadas de administrar la tecnología. Es deprimente no poder confiar en las personas contratadas, y vigilarlas de cerca puede ser un golpe para la moral; nadie quiere sentir que no es de confianza o que es controlado.

De todas formas, incluso con un staff de máxima confianza, las cuentas no deben ser confiadas a nadie.

Las credenciales de los administradores, no los datos, son la joya de la corona para quienes están planeando atacarlo. Una vez que se roban las credenciales de los sistemas, todo lo demás cae. Los atacantes no buscan datos, al menos al principio. Las cuentas privilegiadas son la puerta de acceso a todo lo demás: emails, datos, bases de datos, archivos, configuraciones de sistemas, aplicaciones… Todo queda expuesto una vez que las cuentas privilegiadas son violadas. En base a esto, las cuentas internas deben ser tratadas con sospecha. No a causa de las personas a las que están asignadas, sino porque son el activo más valioso para quienes buscan atacar a su organización.

## Alerte y notifique

Esto es simplemente un aspecto natural de cualquier sistema de registro y auditoría bien implementado.
No cualquier ataque necesita despertar a su administrador de Seguridad a las 2 de la mañana, pero existen algunos que sí deberían:

- ¿El intento de acceso a una cuenta se produce desde un host del cual no debería?
- ¿Se utiliza una clave SSH desde un lugar del cual no se debería?
- ¿Una cuenta de administrador está intentando ejecutar comandos privilegiados que no le corresponden?

Un sistema bien implementado, con reglas bien definidas, debería detener las acciones maliciosas. Después de todo, si podemos analizar logs y saber qué no debería estar sucediendo, eso también quiere decir que podemos definir reglas para prevenir que ocurra. La diferencia reside en detectar una alerta de manera proactiva y no reactiva. Este es el concepto de detección a través de la aplicación. Las mismas reglas que pueden ser escritas para detectar un mal comportamiento, deben ser utilizadas para prevenirlo. La defensa y la detección se funden en un único esfuerzo.

## Centralice, unifique y sea eficiente

Casi todas estas valiosas funcionalidades están disponibles de forma nativa en Linux y UNIX.

- SSH permite a la configuración local controlar quién puede acceder, desde dónde, cómo y qué puede hacer una vez conectado.
- Las cuentas pueden ser creadas o eliminadas en un sistema local con los comandos "adduser" y "userdel", y existen varias técnicas para mantener una cuenta, sin bloquear su acceso.
- Los permisos pueden ser administrados utilizando el comando "sudo" y archivos de configuración local.
- Todo lo que puede ser realizado, puede hacerse en la configuración del sistema local.

El estricto control de accesos y la gestión de permisos tiene ventajas distintivas en comparación a intentar administrarlas en forma separada, y en el mundo Linux/UNIX, el control de accesos está estrechamente unido al control de cuentas. Por eso, usted necesita una herramienta que le permita administrar de forma centralizada estos tres aspectos fundamentales: gestión de cuentas, control de accesos, y gestión de permisos.

Sin embargo, operativamente puede representar un gran desafío.

**En infraestructuras pequeñas:** Para un sistema y unos pocos usuarios, usted deberá administrar esas pocas cuentas, la configuración y las reglas de acceso de SSH, los permisos sudo, y más. Cada servidor adicional aumenta el esfuerzo de mantener la configuración apropiada de manera exponencial. Para uno o pocos servidores, puede ser un desafío tedioso, pero posible de hacer. Para que tenga en cuenta: el "451 Group" -ente que se ocupa de calcular métricas acerca de cuándo las herramientas de automatización se vuelven muy útiles y rentables- en sus resultados de 2018 indicó que un administrador de sistemas es capaz de administrar no más de 500 sistemas operativos en simultáneo, utilizando scripts y procesos manuales.

**En infraestructuras mixtas**: Linux y las variaciones del Sistema Operativo UNIX, como IBM AIX, Oracle Solaris y el HP-UX de HPE, manipulan usuarios, grupos, permisos, contraseñas, sudo y claves SSH. Desafortunadamente, debido a razones históricas que nos transportan décadas atrás, los proveedores de cada plataforma tomaron distintas decisiones sobre cómo se configura y se mantiene la seguridad de los Sistemas Operativos. Por ejemplo:

- Cada plataforma tiene una forma diferente de definir la extensión de las contraseñas y sus reglas de complejidad, utilizando sus propias herramientas administrativas.
- Solaris almacena las claves SSH en un formato técnico completamente diferente al resto de las plataformas.

Intentar gestionar estas diferencias con scripts o configuraciones de administración puede ser problemático, y las plataformas continúan teniendo problemas logarítmicos o de implementación (por ejemplo, la distribución de archivos de configuración sudo, o claves SSH de usuarios). Como resultado, se pierde demasiado tiempo en generar scripts o utilizar herramientas de gestión de cambios, para realizar comparaciones básicas de archivos en cada uno de los nodos y así verificar si algo ha cambiado. Lo que, además, demanda mucha capacidad de CPU y carga el tráfico de lared, para intentar mantener todo sincronizado.

Estos problemas operativos no desaparecen incluso si usted actualmente gestiona una mono-cultura de sistemas, con una plataforma única y "limpia". En una cultura de negocio de fusiones y adquisiciones internacionales, nunca se sabe qué Sistema Operativo puede necesitar controlar o qué plataformas técnicas heredará en el futuro.

BoKS ServerControl, de Fortra, fue diseñado para operar a través de múltiples plataformas, manteniendo la Seguridad en la forma requerida por los distintos Sistemas Operativos, administrados desde un punto de control central. Además, el administrador de Seguridad no necesita preocuparse sobre si trata de un sistema AIX, Linux, PowerLinux o Solaris. Nuestro software se encarga de eso.

**Grandes infraestructuras:** Para cientos o miles de servidores, y decenas o cientos de usuarios, mantener los servidores configurados apropiadamente se convierte en una enorme tarea, casi imposible de lograr sin un ejército de administradores. La respuesta por defecto es implementar un software de configuración de administración como Puppet, Ansible, o Chef. Sin embargo, las últimas métricas del 451 Group indican que utilizar estas herramientas de configuración solo duplican la productividad de un solo administrador a no más de 1000 Sistemas Operativos concurrentes.

**Infraestructuras de escala web:** Si usted tiene infraestructura worldwide o net facing en decenas de miles de nodos, necesita otro enfoque de herramientas de administración, y es ahí donde BoKS ServerControl le permite ahorrar gran cantidad de tiempo y trabajo de su equipo de administración.

## Sobre BoKS ServerControl

BoKS® ServerControl transforma su entorno híbrido de servidores Linux y UNIX en un dominio seguro, gestionado centralmente. Simplifica la capacidad de su empresa de potenciar las políticas de Seguridad y controla el acceso a sistemas e información críticos. Con un control completo sobre las cuentas, accesos y permisos, los equipos de IT y

Seguridad pueden prevenir en forma proactiva ataques críticos, tanto internos como externos, antes de que comiencen.

BoKS protege sus sistemas y datos críticos para que pueda enfocarse en lo más importante: acelerar el crecimiento de su negocio. Visite www.fortra.com/es/BoKS para conocer más o solicitar una demostración.

FORTRA

Fortra.com

**Sobre Fortra**

Fortra es una compañía de Ciberseguridad como ninguna otra. Hemos creado un futuro más simple y sólido para nuestros clientes. Nuestro equipo de expertos junto con el mejor portfolio de soluciones integradas y escalables aportan equilibrio y control a organizaciones en todo el mundo. Somos impulsores del cambio positivo y su aliado de confianza para darle tranquilidad en cada paso de su camino de Ciberseguridad. Conozca más en fortra.com/es.

 (fta-ptx-gd-es-1122-r1-79d)