BeyondTrust

SOLUTION BRIEF

15 Casos de Uso de la Gestión de Privilegios en Servidores Unix & Linux

Esta guía ha sido preparada para que los administradores de TI y seguridad puedan comprender rápidamente cómo las soluciones de gestión de privilegios en terminales (Endpoint Privilege Management for Unix & Linux) y Active Directory Bridge, de BeyondTrust pueden ayudarlos a madurar progresivamente los controles de seguridad de accesos privilegiados y eliminar el sudo, al tiempo que centraliza la administración, la auditoría y los informes.

Tabla de contenido

Resumen Ejecutivo

El concepto de privilegio mínimo establece que todos los usuarios deben tener el nivel más bajo de privilegios de acceso necesarios para realizar sus trabajos de manera efectiva. Sin embargo, muchas funciones básicas de sistema operativo, administración, aplicación y software (por ejemplo, utilidades de configuración) requieren más que solo privilegios básicos. En consecuencia, los usuarios necesitan tener privilegios elevados en forma de nombres de usuario y contraseñas de administrador, o *root*. Para superar este riesgo inherente de seguridad de privilegios excesivos, las organizaciones deben eliminar la necesidad de distribuir y mantener credenciales root y administrativas, o incluso revelar estas credenciales a los usuarios, pero sin afectar la productividad.

La solución BeyondTrust Endpoint Privilege Management permite a los equipos de TI ejercer un control granular sobre quién puede acceder a los servidores Unix, Linux y Windows, y qué pueden hacer esos usuarios con ese acceso. De esta forma, las organizaciones mejoran la seguridad del sistema del servidor, al tiempo que simplifican las implementaciones de administración de accesos privilegiados y garantizan la productividad.

BeyondTrust Endpoint Privilege Management incluye recursos para:

- Descubrir, administrar y monitorear el acceso a root, admin y otras contraseñas privilegiadas y claves SSH automaticamente;
- Elevar los comandos y delegar privilegios con controles de política específicos, proporcionando una gestión sólida sobre lo que los usuarios de Windows, Unix y Linux pueden hacer una vez que inician sesión en un sistema;
- Habilitar el inicio de sesión único (SSO) y la política simplificada mediante la consolidación de cuentas en múltiples plataformas en un solo conjunto de políticas de control de acceso;
- Proporcionar visibilidad del riesgo en las aplicaciones destinadas a la elevación de privilegios;
- Análisis, registro e informes sobre contraseñas privilegiadas, usuarios y comportamiento de las cuentas.

Esta guía explica casos de uso comunes para la gestión de privilegios en servidores Unix/Linux, incluidos los recursos disponibles en Privilege Management for Unix & Linux y BeyondTrust Active Directory Bridge (AD Bridge), que forman parte de la solución de gestión de privilegios en terminales de BeyondTrust. Estos casos de uso son progresivos, con los más directos enumerados primero, seguidos por los de mayor nivel de complejidad.

15 Casos de Uso de la Gestión de Privilegios en Servidores Unix & Linux

1. Eliminando la Necesidad de Iniciar Sesión Como root

Muchos usuarios de sistemas y aplicaciones Unix y Linux usan la frase "Necesito root", lo que indica que solo pueden realizar sus funciones diarias de trabajo si iniciaren sesión con el usuario más poderoso del sistema, "root". Root, a menudo, se conoce como el usuario "Dios", ya que prácticamente no hay nada que el usuario root no pueda hacer.

El uso de la cuenta root elimina la capacidad de auditar las acciones de un individuo (esencialmente promoviendo el uso compartido de la cuenta) e inhibe el uso de una contraseña segura y modificable para la cuenta root debido a la necesidad de que varias personas usen la cuenta y aprovechen sus privilegios en cualquier momento. El uso de la cuenta root y prácticas como el uso compartido de cuentas aumentan drásticamente el riesgo de amenazas internas a través de comportamientos maliciosos y accidentales, así como las amenazas externas.

Privilege Management for Unix & Linux implementa un verdadero modelo de delegación con menos privilegios que puede eliminar o restringir en gran medida el uso de la cuenta root, sin obstaculizar los flujos de trabajo de los usuarios. Con la solución BeyondTrust, puede permitir que los usuarios ejecuten cualquier comando en un nivel de privilegio más alto según lo dicte su política centralizada. Al eliminar la necesidad de que los usuarios inicien sesión como root, la cuenta de usuario root puede tener controles de seguridad mucho más estrictos o pasar a un sistema de gestión de contraseñas, como BeyondTrust Password Safe.

2. Lograr el Cumplimiento de la Cuenta Root

Los administradores de sistemas pueden, de vez en cuando, tener una necesidad legítima de usar la cuenta root debido a los tipos de cambios a nivel del sistema que se realizan, o simplemente debido a la naturaleza *ad-hoc* de los comandos que necesitan ejecutar.

Sin embargo, el equipo de cumplimiento debe monitorear TODAS las actividades y garantizar la responsabilidad de las acciones. Para permitir que los administradores del sistema accedan a una cuenta privilegiada, los equipos de cumplimiento necesitan las herramientas y los procesos correctos para poder identificar quién estaba usando la cuenta root, cuándo y qué cambios fueron realizados por ese usuario con esta cuenta. Además, es imprescindible que los archivos de registro sean inmunes a cualquier tipo de manipulación.

Privilege Management for Unix & Linux permite que las cuentas estándar se eleven a un nivel root con un registro de sesión completo, proporcionando una pista de auditoría centralizada y de forma transparente para cada administrador de sistema.

3. Cuando Sudo ya no es Suficiente

Sudo ha existido durante mucho tiempo, pero a medida que la cantidad de sistemas y usuarios ha crecido, la administración de sudo se ha vuelto demasiado lenta. Junto con las limitaciones de los controles disponibles en sudo, los sistemas ahora parecen expuestos a un número creciente de amenazas de seguridad internas y externas.

Privilege Management for Unix & Linux proporciona un lenguaje de políticas mucho más flexible, lo que permite crear políticas más granulares tanto a nivel de comando como de sistema. La herramienta aumenta la seguridad de varias maneras, que incluyen mover la

política y los datos de registro de la estación de trabajo o servidor de los usuarios, y utilizar la última tecnología de cifrado para datos tanto en tránsito como en reposo.

4. Control de Permisos y Acceso al Sistema de Archivos

Los sistemas de archivos permiten la configuración de permisos de archivos y carpetas, como leer, escribir, ejecutar, etc. Sin embargo, los permisos de archivos y carpetas son de naturaleza muy estática y deben establecerse en cada host. También existen riesgos al permitir el acceso de cuentas altamente privilegiadas (como la root) a un servidor o estación de trabajo, ya que una cuenta con ese tipo de privilegio puede manipular fácilmente los permisos y la configuración de propiedad utilizando comandos como "chmod" y "chown". Dar a una cuenta acceso ilimitado a archivos y datos representa un riesgo significativo.

Privilege Management for Unix & Linux resuelve este desafío al permitir la aplicación de configuraciones de seguridad de tiempo de ejecución sean controladas centralmente, protegendo las cuentas privilegiadas. El recurso Advanced Control and Audit (ACA) de Privilege Management for Unix & Linux se puede aplicar dinámicamente, lo que permite la aplicación de las reglas de permisos del sistema de archivos durante ciertos momentos, o permite el acceso solo si se cumplen ciertas condiciones, como la entrada de un autenticación de factor o proporcionando un número de incidente válido del sistema de tickets.

Con esta capacidad, las organizaciones pueden otorgar una estructura de nivel 'root' completa, pero al mismo tiempo, impedir que ese usuario root pueda acceder a los archivos de usuario almacenados en '/ home', o al permitir que se ejecuten scripts, pero no visto o editado.

5. Control de Acceso a Scripts y Auditoría de Acciones de Scripts

Los administradores de Unix y Linux dependen en gran medida del uso de scripts para realizar tareas diarias de administración del sistema. Muchos de estos scripts deben ejecutarse como usuario privilegiado, como "root", o funciones de llamada que a su vez requieren altos niveles de privilegio. El uso de una solución de privilegios mínimos es esencial a los usuarios que necesitan de privilegios elevados. Tradicionalmente, la mejor manera de auditar las actividades de estos usuarios seria habilitar alguna forma de grabación de sesión, es decir, grabar stdin y stdout, o registrar todo lo que el usuario escribe y todo lo que el usuario ve en la pantalla. El problema con este enfoque es que, al registrar estas acciones, no hay forma de ver qué acciones se realizaron dentro del script, qué datos pueden haber sido afectados o cómo el sistema puede haber sido manipulado.

Al usar Privilege Management for Unix & Linux y el recurso Advanced Control and Audit (ACA), no solo los scripts pueden controlarse más estrictamente (es decir, los scripts pueden ejecutarse y visualizarse, pero no modificarse, incluso desde la root), sino que los equipos de TI también pueden iniciar sesión y registrar todas las llamadas a nivel del sistema que se realizan, independientemente de su origen, durante la sesión.

Esta capacidad permite que se registren acciones, como la ejecución de un script, junto con cada llamada que realiza el script (es decir, lee, escribe, ejecuta, etc.). Además de registrar todas las actividades del script, Privilege Management for Unix & Linux también tiene la capacidad de controlar acciones individuales en el script y permitir o bloquear selectivamente esas acciones sin detener el procesamiento general del script.

6. Control de Acceso al Nivel del Sistema

Las herramientas tradicionales de restricción de privilegios, como sudo, se centran en controlar lo que el usuario escribe en la línea de comandos en lugar de lo que el sistema realmente intenta procesar. Las reglas definidas en tales herramientas se centran en lo que el usuario está escribiendo y no en lo que el sistema realmente va a hacer. Sin embargo, en la mayoría de los sistemas operativos modernos, estas dos acciones pueden ser muy diferentes.

Por ejemplo, en Windows, es simple crear un acceso directo a un elemento, como "notepad.exe", y nombrar ese acceso directo "My Fav Text Editor.lnk". Si una organización tiene una política que impide que alguien haga clic en un icono llamado Notepad.exe, ¿qué sucederá cuando alguien haga doble clic en el nuevo acceso directo que acaba de crear?

El mismo tipo de escenario se desarrolla en el mundo de Unix y Linux. Siendo un sistema operativo de línea de comandos, las políticas de seguridad se centran principalmente en lo que el usuario escribe en el prompt del sistema. El problema es que los atajos (conocidos como enlaces simbólicos y fisicos) también se pueden usar para llamar a binarios (ejecutables) y scripts, o archivos de referencia. Además, los archivos binarios (ejecutables) también se pueden renombrar para eludir las políticas de seguridad. Imagine si alguien copiara el binario de "shutdown" y lo llamara "ping". Sudo puede bloquear el shutdown, pero no el ping. Un administrador astuto ejecuta "sudo ping" y el sistema se apagará sin que nadie pueda descubrir lo que acaba de suceder.

Las reglas de política de Advanced Control and Audit (ACA) permiten colocar controles de una línea alrededor de archivos, carpetas y subcarpetas. Estos controles permiten establecer permisos granulares contra el destino, pero lo más importante es que ACA opera en el nivel del sistema y no en el nivel de la línea de comandos. Independientemente de cómo se llame el comando 'shutdown', ya sea directamente '/ usr / sbin / shutdown', un enlace fijo o suave a '/ usr / sbin / shutdown' o uno copia renombrado del comando shutdown, ACA es inteligente suficiente para bloquear la ejecución del comando emitido.

7. Consolidación de Registros de Eventos, Informes y Análisis

Por su naturaleza de línea de comandos, los sistemas Unix y Linux no son los más amables cuando se trata de generar informes. Sin embargo, la presentación de reportes es esencial, especialmente cuando se realizan investigaciones forenses en registros o se detectan anomalías.

BeyondTrust resuelve este problema con la integración entre Privilege Management for Unix & Linux y la plataforma central, BeyondInsight. La herramienta envía datos de registro de eventos a BeyondInsight para su presentación en el *dashboard*; específicamente, quién, qué, dónde y cuándo de los eventos. Estos datos se pueden presentar en informes fáciles de consumer y, con una herramienta de inteligencia de negocios, pueden ser usados para crear informes personalizados. Además, pueden correlacionarse con otros datos, utilizando Auditor de BeyondInsight para la detección y reporte de anomalías.

Esta integración hace que la presentación de informes sobre eventos de Unix y Linux sea más simple, más rápida y más fácil de leer para que los interesados puedan tener una idea más clara de sus riesgos de privilegios.

8. Forense: El Tiempo es Esencial

Registrar todas las actividades de los usuarios Unix/Linux puede volverse abrumador rápidamente. Cuando se necesita realizar una investigación forense, las organizaciones pueden perder tiempo y mano de obra realizando investigaciones.

Con Privilege Management for Unix & Linux, los registros de eventos pueden nombrarse dinámicamente, ubicarse centralmente y controlarse el acceso en la consola central BeyondInsight. Privilege Management for Unix & Linux utiliza SOLR para indexar todas las sesiones grabadas, con toda la información accesible a través de la línea de comandos o la API REST.

9. Grabación de la Sesión (El escrito és visto)

El privilegio mínimo es un estado ideal para la mayoría de los grupos de seguridad, pero a veces solo necesita activar un shell privilegiado, como a de nivel root. Por lo tanto, para los administradores de confianza, una estructura root completa a menudo no presenta ningún problema siempre que la actividad del administrador se registre de forma segura. Este nivel de supervisión ayuda a garantizar que los administradores no abusen de sus derechos, al tiempo que ayuda a una organización a cumplir con los requisitos de cumplimiento relacionados con los accesos privilegiados.

Una línea simple en la política de Privilege Management for Unix y Linux activa la grabación de sesión completa, que luego se nombra dinámicamente y se indexa automáticamente usando SOLR. Esta capacidad permite a las organizaciones ver la sesión de muchas maneras diferentes: mediante reproducción interactiva, reproducción por video, ver la transcripción de la sesión, el historial de comandos o en un índice de búsqueda. Esta capacidad proporciona flexibilidad para activar y buscar rápidamente la actividad de uso, ayudándole a gestionar mejor el riesgo.

10. Lograr la Gestión de Contraseñas y el Menor Privilegio

Para que funcione una solución de almacenamiento de contraseñas, se requiere una cuenta de segundo nivel (cuenta funcional) para que la contraseña segura pueda manejar los cambios de contraseña, si la contraseña de la cuenta administrada no está sincronizada o es desconocida para la bóveda. Esto también es cierto para cualquier aplicación que necesite mayores privilegios, como herramientas de escaneo, administración remota automatizada, etc. Estas cuentas representan un riesgo para el sistema de destino debido a su nivel de privilegio requerido de "administrador de contraseña de usuario".

Al instalar Privilege Management for Unix & Linux con BeyondTrust Password Safe y agregar una política simple, cualquier cuenta de usuario, incluso una con derechos extremadamente limitados en el sistema de destino, puede recibir los privilegios necesarios para que Password Safe funcione. Esto garantiza una mayor seguridad y un cumplimiento más estricto (al no tener cuentas con los privilegios normalmente necesarios para que funcionen las cuentas funcionales), al tiempo que se reduce la superficie de ataque del host.

11. Integración de la Gestión de Contraseñas Privilegiadas con la Ejecución de Comandos

A veces, los administradores deben realizar una acción en un host de destino que requiere el uso de una cuenta/contraseña, que puede no residir en el host en sí. Al ejecutar un comando a través de Privilege Management for Unix & Linux, es decir, pbrun sqlplus, la herramienta puede recuperar credenciales de una solución de almacenamiento de contraseñas para usar en la ejecución del comando solicitado. Esta integración asegura que las organizaciones no solo pueden controlar sus credenciales privilegiadas, sino que también permiten el control de comandos muy granular en los sistemas de destino una vez que se recupera la credencial.

12. Gestión Centralizada de Controles de Políticas Sudo

Incluso para los usuarios de herramientas de privilegios mínimos, casi siempre habrá algunas máquinas que todavía tengan acceso a sudo. Con tantas iteraciones diferentes del archivo de políticas sudoers utilizado por los diversos grupos dentro de la organización, la necesidad de controlar y rastrear los cambios realizados en cada sudoers se convierte rápidamente en una tarea inmanejable. Casi todos los usuarios sudo pronto se enfrentan al desafío de administrar adecuadamente los archivos sudoers individuales que se crean en cada host Unix o Linux.

Las herramientas de sincronización manual y las soluciones de bases de datos/LDAP locales pueden parecer atractivas al principio, pero la confiabilidad, la complejidad y los controles de

seguridad terminan reduciendo drásticamente la efectividad de tales configuraciones, lo que a menudo causa más problemas de los que resuelven. No hay una manera efectiva de deshacer los cambios en uno o más archivos sudoers, o volver a un cierto tiempo/versión de un archivo de política sudoers.

Privilege Management for Unix & Linux proporciona una forma de centralizar rápidamente uno o más archivos sudoers, permitiendo la gestión de cambios y el control de versiones. Los cambios de política pueden validarse antes de realizar cambios en el archivo de política en vivo, o compararse rápidamente con las diferencias resaltadas entre dos versiones de un archivo sudoers. La funcionalidad de retroceso/avance permite un cambio rápido entre dos versiones guardadas del archivo sudoers que PMUL administra. Los hosts de conexión se pueden agrupar o ejecutar opcionalmente en un híbrido de hosts agrupados uno a uno. Esto permite un acceso simple y controlado a archivos sudoers específicos ubicados en uno o más servidores centralizados, en función de la membresía de grupo del host solicitante.

13. Almacenamiento Centralizado de Datos de Auditoría Sudo

Usar sudo significa colocar datos de registro de diferentes ubicaciones en diferentes sistemas. Dependiendo de la versión de Unix o Linux, los datos de eventos terminan en diferentes archivos de syslog y también se mezclan con otros datos de eventos del sistema. Es claramente necesaria una mejor manera de mover y almacenar de forma segura los datos de registro y los de registro de sesión de sudo.

Privilege Management for Unix & Linux proporciona una conexión de red segura a un servidor centralizado que almacena datos de eventos y sesiones (cifrados si lo desea) en una ubicación centralizada y segura a medida que se escriben los datos de registro, eliminando la capacidad de enviar a los usuarios para manipular los registros, y permitiendo una revisión de registros y análisis forenses mucho más rápidos cuando sea necesario.

14. Consolidando Cuentas y Directorios

Cuando los usuarios y administradores requieren acceso a un sistema, se debe crear una cuenta de usuario en cada host para proporcionarle acceso al sistema. Los derechos para estas cuentas de usuario a menudo están inflados, y la limpieza de las cuentas, con sus derechos asociados, a menudo no se verifica cuando un empleado cambia de roles o abandona la empresa. Las organizaciones necesitan una forma de reducir la cantidad de cuentas que se crean, controlar qué servidor ellas pueden iniciar sesión y ejercer control sobre qué privilegios tiene el usuario después de haber sido autenticado.

BeyondTrust Active Directory Bridge (AD Bridge), con Privilege Management for Unix & Linux, proporciona consolidación de cuentas con privilegios de acceso al sistema consolidados y un sistema de privilegios mínimos para controlar los privilegios del usuario, después del inicio de sesión. La pertenencia a un grupo de Active Directory de un usuario puede controlar a qué servidores accede ese usuario, y una política centralizada controlará y auditará estrictamente sus actividades durante cada sesión autenticada.

Como beneficio adicional, AD Bridge permite a los usuarios iniciar sesión en sistemas Unix, Linux o Mac utilizando sus nombres de usuario y contraseñas de Active Directory (AD), sin necesidad de infraestructura adicional o sincronización de contraseña.

Con esta solución integrada, puede facilitar la migración desde múltiples mecanismos de autenticación, identidades y directorios a una única infraestructura basada en Active Directory para todos los sistemas y usuarios. Esto centraliza el control y acelera el acceso del usuario.

15. Ampliación de la Política de Grupo a Sistemas non Windows

Algunas organizaciones optan por administrar de manera centralizada sus sistemas Windows, Unix y Linux para obtener beneficios de seguridad, cumplimiento y eficiencia, pero pueden tener dificultades para garantizar que las políticas de configuración se apliquen de manera consistente a nivel empresarial.

BeyondTrust Active Directory Bridge (AD Bridge) y Privilege Management for Unix & Linux permiten una configuración consistente en toda la empresa al extender las herramientas nativas de administración de Politicas de Grupo para incluir configuraciones específicas para Unix, Linux y Mac. Esta capacidad admite el cumplimiento de SOX, PCI, HIPAA y otras regulaciones en todos los sistemas al reemplazar NIS con una infraestructura de Active Directory.

La plataforma de Gestión de Accesos Privilegiados BeyondTrust

Privilege Management for Unix & Linux y Active Directory Bridge (AD Bridge) son parte de las soluciones de BeyondTrust para la gestión de privilegios en terminales, e se integran con otras soluciones de administración de accesos privilegiados en la plataforma BeyondTrust Privileged Access Management. La plataforma es una solución integrada para proporcionar control y visibilidad sobre todas las cuentas y usuarios privilegiados.

Próximos pasos

Este documento presentó casos de uso comunes para la gestión de privilegios basada en políticas y la elevación de comandos para servidores Unix y Linux. Para obtener más información sobre cómo BeyondTrust puede ayudar, visite beyondtrust.com/endpoint-privilege-management.