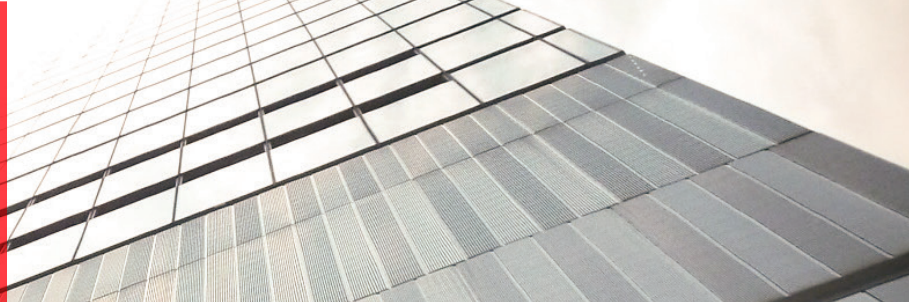

Servicio de elevación de privilegios de Centrify

Establecer el acceso con los mínimos privilegios para reducir la superficie expuesta a ataques

En los años recientes, ha quedado patente que los atacantes ya no «hackean» para acceder a los datos mediante brechas de seguridad. Simplemente inician sesión utilizando credenciales con privilegios robadas, débiles o reveladas de alguna manera. Una vez dentro, se aprovechan de que muchas organizaciones asignan demasiados privilegios a los usuarios administrativos. Esto permite a los *hackers* campar a sus anchas y desplazarse lateralmente por la red para apropiarse de más cuentas y credenciales con privilegios que les ayudan a obtener acceso a la infraestructura más crítica y a los datos sensibles de una organización. Zero Trust Privilege prescribe que se concedan los privilegios estrictamente necesarios durante el tiempo justo con el fin de limitar el desplazamiento lateral por la red.

Zona peligrosa: demasiados privilegios

El concepto de mínimos privilegios es más común de lo que parece. Piense en el control de acceso físico a su oficina: los usuarios con diferentes responsabilidades tienen derechos de acceso distintos y el acceso a ciertas áreas tiene que solicitarse y ser aprobado. Estas prácticas son bien conocidas y aceptadas en el espacio físico de seguridad. La misma lógica se aplica a la seguridad informática, por ejemplo, cuando se concede acceso granular según el rol a los recursos con privilegios.

Otro objetivo de conceder los mínimos privilegios es limitar el desplazamiento lateral por la red. Esta es la manera principal en que los atacantes obtienen acceso a datos sensibles: empiezan en una ubicación y se desplazan lateralmente hasta que encuentran lo que están buscando. Si desactivamos las zonas a las que pueden acceder, podemos detener el desplazamiento lateral. De la misma manera que a nadie se le ocurriría entregar una clave o distintivo que conceda acceso a todo, tampoco es deseable utilizar la cuenta raíz de un servidor, ya que concede demasiado acceso y no se puede atribuir al usuario real. Por poner otro ejemplo, tenemos un usuario real al que llamaremos Bob. Con los privilegios que se le han concedido, Bob debe iniciar sesión directamente en el sistema de destino con sus propios derechos administrativos, que le conceden acceso para reiniciar únicamente un conjunto determinado de servidores. Si Bob necesita cambiar la configuración o acceder a otro sistema de destino, tiene que solicitar acceso durante un período de tiempo específico. El acceso se puede conceder de forma automática o mediante algún servicio como ServiceNow® o SailPoint Technologies®. Además, se le puede pedir a Bob la autenticación multifactorial (MFA). En cuanto termine, los derechos de Bob volverán a ser los estrictamente necesarios.

Establecer el acceso con los mínimos privilegios para reducir la superficie expuesta a ataques

El Servicio de elevación de privilegios de Centrify minimiza la exposición al riesgo de ataques cibernéticos causados por personas con demasiados privilegios. El servicio permite a los clientes implementar las prácticas recomendadas de acceso con los privilegios estrictamente necesarios durante el tiempo justo y, por consiguiente, limitar los daños potenciales debidos a brechas de seguridad.

ELEVACIÓN DE PRIVILEGIOS

Proteja y gestione los privilegios de fina granularidad en los sistemas Windows, Linux y UNIX para limitar así los daños potenciales debidos a brechas de seguridad. Requiera que los usuarios inicien sus propias sesiones por responsabilidad y eleven los privilegios en función de su rol en la organización.

ASIGNACIÓN DE ROLES EN FUNCIÓN DEL TIEMPO

Minimice el riesgo de seguridad haciendo que los administradores soliciten sistemáticamente un nuevo rol para obtener los derechos que necesitan para llevar a cabo sus tareas. La solicitud de acceso a roles con privilegios permite a las organizaciones conceder privilegios y roles provisionales o durante un período prolongado, mediante un modelo flexible que se aplica durante el tiempo justo y se adapta a las necesidades variables del negocio.

GESTIÓN DE POLÍTICAS Y ROLES CON PRIVILEGIOS DELEGADOS

Los roles, derechos y políticas de privilegios centralizados facilitan la gestión en entornos heterogéneos (UNIX, Linux y Windows). Las políticas se almacenan en Active Directory en directorios independientes de los de objetos comunes para dar soporte a la delegación de funciones de administrador de servidor y a la separación de deberes de los administradores de Active Directory. De este modo, se evita que los administradores de servidores gestionen objetos de Active Directory a los que no deberían tener acceso. Todo esto se hace sin modificar el esquema de Active Directory.

MFA EN LA ELEVACIÓN DE PRIVILEGIOS

Utilizar la MFA en el inicio de sesión es una práctica recomendada excelente, especialmente para los administradores. No obstante, debe reforzarse utilizándola también en la elevación de privilegios para protegerse de personas con malas intenciones y asegurarse de que solo las personas autorizadas puedan iniciar comandos con privilegios mediante una validación de MFA anterior a la ejecución del comando con privilegios.

Conceder los privilegios estrictamente necesarios en Windows, Linux y Unix

Reduzca el riesgo de ataque a través de personas con demasiados privilegios y por el uso rutinario de cuentas con privilegios compartidas. Implementar el acceso con los mínimos privilegios limita los daños potenciales debidos a brechas de seguridad. De esta manera, la flexibilidad y la granularidad del Servicio de elevación de privilegios de Centrify permiten que los usuarios hagan su trabajo, reducen el riesgo y simplifican la implementación del modelo de privilegios mínimos durante el tiempo justo gracias a los controles de acceso según el rol.

- Los controles de acceso según el rol facilitan la concesión de privilegios mínimos. La tecnología Zones patentada por Centrify proporciona controles de acceso de alta granularidad según el rol que se encargan de simplificar la implementación del modelo de mínimos privilegios en los sistemas Windows, Linux y UNIX.
- Proteja sus sistemas Windows, Linux y UNIX controlando exactamente quién puede acceder a qué y cuándo. A diferencia de las herramientas descentralizadas para un solo propósito, como SUDO (acrónimo en inglés de Super User Do, acciones de superusuario), Centrify habilita la configuración de privilegios dinámicos. De este modo, los usuarios solo pueden elevar sus privilegios en momentos concretos, durante un tiempo limitado y en ciertos servidores. También se pueden aislar los servidores en función del tiempo y de las relaciones de confianza para proteger más los datos sensibles. Esto ayuda a limitar aún más el desplazamiento lateral.
- Centrify ofrece un conjunto potente de herramientas que simplifican la adopción y la gestión del modelo de acceso con mínimos privilegios.

Simplificar la gestión de entornos heterogéneos

Los roles, derechos y políticas de privilegios centralizados facilitan la gestión en entornos heterogéneos (UNIX, Linux y Windows). Las políticas de los servicios Zero Trust Privilege de Centrify se almacenan en Active Directory en directorios independientes de los de objetos comunes para dar soporte a la delegación de funciones de administrador de servidor y a la separación de deberes de los administradores de Active Directory. De este modo, se evita que los administradores de servidor gestionen objetos de AD a los que no deberían tener acceso. Además, Centrify facilita un modelo jerárquico de políticas diseñadas para dar soporte a los modelos típicos de gestión empresarial con roles y derechos comunes que se controlan y gestionan de forma centralizada. Al mismo tiempo, da soporte a la delegación en equipos administrativos subordinados, por departamento según el rol y el ordenador, para asignar derechos de acceso a sistemas.

- Un modelo de políticas coherente y estructurado para Windows, Linux y UNIX facilita el cumplimiento y reduce los costes de mantenimiento.
- La gestión de políticas de Windows, Linux y UNIX en Active Directory aplica un método coherente de seguridad del acceso con privilegios y crea además la separación de deberes adecuada entre los propietarios de las políticas y los administradores de los sistemas. Utilizar este método homogéneo para la gestión de entornos heterogéneos abrevia las auditorías y simplifica el cumplimiento.

Autoservicio de solicitudes de rol para obtener privilegios durante el tiempo justo

Minimice el riesgo de seguridad haciendo que los administradores soliciten sistemáticamente un nuevo rol para obtener los derechos que necesitan para llevar a cabo sus tareas. La solicitud de acceso a roles con privilegios permite a las organizaciones conceder privilegios y roles provisionales durante el tiempo justo, mediante un modelo flexible que se adapta a las necesidades variables del negocio.

- Requiera que los administradores inicien sus propias sesiones y que eleven los privilegios mediante solicitudes sistemáticas de nuevas asignaciones de rol que les otorguen los derechos necesarios para llevar a cabo sus tareas. Un sistema de autoservicio facilita la solicitud del rol y el período de tiempo especificados. Si se aprueba la solicitud, el derecho se revocará automáticamente en cuanto expire.
- Minimice la superficie expuesta a ataques al habilitar el acceso provisional por tiempo limitado a las cuentas y los roles con privilegios. Conceda el acceso de administrador de TI a las credenciales de cuenta con privilegios, a las sesiones de gestión remota o cuando sea necesario modificar provisionalmente la asignación de roles para realizar tareas administrativas adicionales.
- Reduzca el riesgo de brechas de seguridad en los datos al requerir aprobación para los usuarios de TI que necesiten acceso a sistemas con roles con privilegios. Los usuarios de TI que utilizan la gestión de activos y la base de datos de gestión de configuración (CMDB) de ServiceNow® o las soluciones de administración y control de identidades de SailPoint Technologies® pueden solicitar un rol con privilegios para acceder a servidores concretos durante un período de tiempo específico. Las aprobaciones se conceden o se deniegan a través de un proceso de gestión basado en el flujo de trabajo.

Comprobar que los comandos con privilegios son iniciados por el usuario con privilegios adecuado

La ejecución de un comando con privilegios siempre debe protegerse de las personas con malas intenciones. Es necesario asegurarse de que solo las personas autorizadas o las aplicaciones y servicios que tengan los derechos adecuados puedan llevar a cabo una actividad con privilegios. Centrify proporciona tecnología basada en host, que no se puede burlar, para aplicar la MFA a la ejecución de tareas con privilegios en servidores Linux, UNIX y Windows.

- Tanto si aplica la MFA en el inicio de sesión del sistema o de la bóveda, como si lo hace durante la elevación de privilegios, la integración con el Servicio de acceso con privilegios de Centrify brinda un servicio de MFA coherente y de fácil mantenimiento para cualquier acceso con privilegios. También cuenta con la mayor variedad de autenticadores y compatibilidad predefinida con los niveles de garantía 2 y 3 de NIST.
- Un método Zero Trust Privilege exige que se verifique siempre quién solicita el acceso con privilegios. El inicio de sesión de los administradores de UNIX y Linux para comprobar el sistema no se considera peligroso y no requiere la MFA. No obstante, la ejecución de cualquier comando con privilegios debe configurarse de modo que requiera la MFA previamente a través de los servicios centralizados de MFA de Centrify.
- Un método Zero Trust Privilege exige que se verifique siempre quién solicita el acceso con privilegios. A los administradores de Windows que necesitan ejecutar comandos con privilegios se les puede requerir la MFA, que vuelvan a autenticarse con su contraseña de AD o que validen su identidad con una tarjeta inteligente.

Nuestra misión es impedir la principal causa de las brechas de seguridad: el uso indebido del acceso con privilegios. Centrify facilita a sus clientes un método Cloud Ready Zero Trust Privilege para proteger el acceso a la infraestructura, a DevOps, a la nube, a los contenedores, al Big Data y a otras superficies de la empresa actual expuestas a ataques. Para obtener más información, visite www.centrify.com.

Sede central en EE. UU. +1 (669) 444 5200
EMEA +44 (0) 1344 317950
Asia-Pacífico +61 1300 795 789
Brasil +55 11 3958 4876
Latinoamérica +1 305 900 5354
sales@centrify.com

www.centrify.com