DOCUMENTACIÓN TÉCNICA

Seguridad con privilegios para Active Directory (AD)

Resumen ejecutivo

Con la proliferación de Microsoft Active Directory (AD) y Azure AD (AAD) en el 95 % de las empresas de la lista Fortune 1000 global, AD es a menudo el objetivo principal de la mayoría de los ataques de ciberseguridad. Además, dado que el acceso con privilegios se está convirtiendo en un elemento cada vez más integrado de lo que controlan AD y AAD, es fundamental que el entorno híbrido sea seguro. Desafortunadamente, a menudo se gestiona de forma inadecuada. El resultado: cuentas explotadas, activos expuestos, daños costosos, efectos a largo plazo y difícil corrección y recuperación.

Es fundamental protegerse contra las amenazas dirigidas a AD/AAD y proporcionar visibilidad y control sobre el acceso con privilegios, lo que también satisface la necesidad de mejorar la eficiencia administrativa híbrida y reducir los errores. La solución ideal le dirá lo que sucedió, lo ayudará a remediar los efectos y lo ayudará a evitar que vuelva a suceder. Establecer una confianza cero y un acceso con privilegios mínimos, según lo recomendado por NIST SP 800-207, es clave para proteger las cuentas con privilegios para entornos AD híbridos. También es una forma importante y eficaz de simplificar el cumplimiento de su empresa con las regulaciones gubernamentales y de la industria.

Desafíos inherentes al panorama

Dado que el 95 % de las empresas de la lista Fortune 1000 global dependen de AD y Azure AD para los permisos y el acceso de los usuarios, es uno de los primeros lugares que los atacantes buscan poner en riesgo. Lo que lo hace peor es que las herramientas nativas carecen de una gestión adecuada de las cuentas de administración de AD y AAD. Microsoft nos dice que 95 millones de cuentas de AD son el objetivo de ciberataques todos los días.[1]

Forrester estima que el 80 % de todas las filtraciones de datos involucran el uso indebido de privilegios administrativos[2]. Esto significa que administrar la seguridad con privilegios en su entorno híbrido de AD es esencial para proteger a sus usuarios e infraestructura. Además, la encuesta global de One Identity[3] de prácticas de accesos con privilegios reveló:

- El 88 % de los encuestados considera que administrar contraseñas con privilegios es un desafío
- El 86 % no cambia las contraseñas con privilegios después de cada uso
- El 40 % no cambia las contraseñas de administración predeterminadas en sistemas críticos

Todo esto se suma para facilitar que los actores maliciosos pongan en riesgo sus cuentas con privilegios.

Complicaciones en la nube

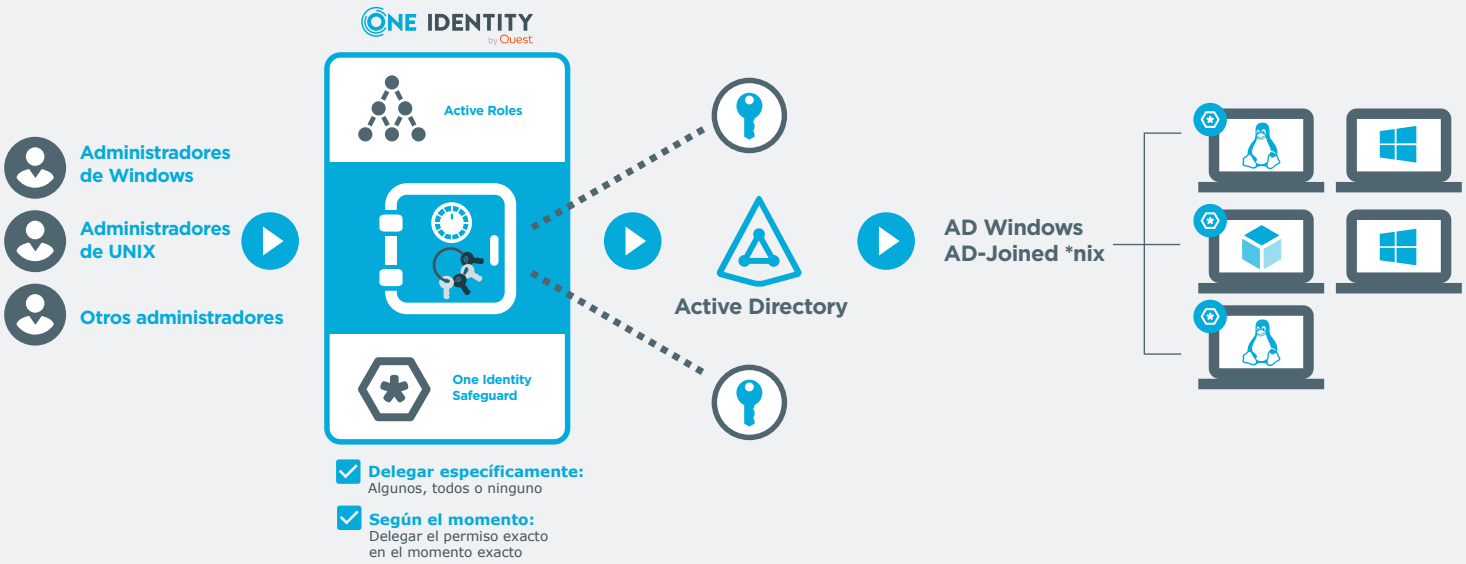
Si bien proteger AD en las instalaciones es complejo por sí solo, con Office 365 y Azure AD, la superficie de ataque ha aumentado drásticamente. Lo que esto significa desde una perspectiva de seguridad es que cualquier actor malicioso que busque poner en riesgo AD podría tener un efecto más amplio a través de Azure AD, a menos que se tomen ciertas medidas.

Dado que los ciberdelincuentes apuntan a AD y AAD, los equipos de TI deben poder otorgar acceso de administrador de manera efectiva y segura. Si no tienen éxito, exponen a las empresas a riesgos de seguridad y cumplimiento. Con este panorama de amenazas en constante cambio, faltan la visibilidad y el control necesarios para combatirlo sin las herramientas adecuadas. Las complicaciones comunes incluyen a los administradores frustrados por todos los obstáculos que tienen que superar para trabajar de forma segura y la enorme cantidad de gastos generales que se necesitan para construir y mantener el cumplimiento.

Responsabilidad de los administradores

Las cuentas de administrador de Active Directory (y Azure AD) son todopoderosas y deben usarse cada vez que alguien necesite mantener, actualizar y administrar los directorios o las cuentas de usuario que contienen. Estas cuentas de administrador utilizan credenciales compartidas y, por lo tanto, son anónimas y sin responsabilidad

Habilitar la confianza cero



individual. Por lo tanto, cualquier persona que necesite hacer algo en los sistemas debe usar la credencial de administrador para AD local y otra para Azure AD basado en la nube.

Modelos de confianza cero y privilegios mínimos

Sin embargo, hay esperanza. Es posible proteger las cuentas con privilegios de AD y AAD con un enfoque holístico. Hay dos métodos comprobados para implementar la gestión de accesos con privilegios (PAM) en entornos AD híbridos: Confianza cero y Privilegios mínimos.

- **Implementar el modelo de confianza cero** implica eliminar la posibilidad de compartir contraseñas de administrador. Los usuarios se autentican de forma individual y dinámica para cada acción administrativa. La credencial se activa cuando es necesario solo después de que se obtienen todas las aprobaciones correctas, solo para un propósito específico o un período de tiempo específico.
- **Establecer privilegios mínimos** implica emitir solo los permisos que un administrador requiere para hacer su trabajo, ni más ni menos. De esta manera, pueden realizar su trabajo diario sin intervención y eliminar la demora y el tedio de solicitar derechos de administrador completos para todo lo que necesitan hacer.

Combinar PAM con acceso a AD – PAMOps

La gestión de accesos con privilegios (PAM) se ha convertido en una parte integral de las estrategias de ciberseguridad de las empresas y se ha incorporado a los programas de seguridad para garantizar que los privilegios elevados se controlen y auditen. El concepto de integrar PAM en los procesos comerciales se está volviendo la norma (ahora llamado PAMOps) a medida que crece concepto. Si bien la mayoría de las empresas ven el valor de controlar las cuentas con privilegios, algunas han separado AD de la estrategia PAMOps.

Si bien pueden controlar algunas cuentas con privilegios que viven en AD, ¿han "cruzado por completo las corrientes" y han combinado la administración de cuentas de AD y PAM?

Algunas pueden haber dejado el acceso con privilegios a AD fuera de la estrategia PAMOps ya que AD proporciona un modelo de delegación básico. Sin embargo, las herramientas nativas proporcionan una delegación básica con algunas limitaciones importantes para la mayoría de las grandes empresas.

- Los permisos asignados son generales y estáticos. Asignar permisos de forma nativa es simple, pero no hay muchas opciones para cumplir con los requisitos de delegación. Esto generalmente da como resultado un exceso de permisos. Además, los permisos se asignan de forma estática o permanente, no se otorgan cuando se necesitan y se eliminan cuando no se utilizan.
- Los permisos solo se otorgan dentro de la estructura OU de AD. Esto también da como resultado un exceso de permisos, ya que los administradores a menudo necesitan acceso en muchas ubicaciones en diferentes niveles. Es mucho más fácil delegar en el nivel superior o agregar al grupo de administradores de dominio.

El Instituto Nacional de Estándares y Tecnología (NIST) establece SP 800-207, *Arquitectura de confianza cero*, para orientar a las empresas en los conceptos para reducir los permisos vulnerables. La implementación de la arquitectura de confianza cero en Active Directory presenta algunos desafíos, ya que las herramientas nativas solo permiten permisos estáticos. El concepto de aprovisionamiento "Just-In-Time" (justo a tiempo, en inglés) permite que los usuarios se agreguen a grupos con privilegios cuando sea necesario y luego se eliminen cuando no estén en uso. El NIST también establece una guía general para administrar cuentas con privilegios, y muchas de estas recomendaciones se aplican directamente a AD. Las recomendaciones del NIST incluyen:

Eliminar accesos innecesarios

Elimine todos los accesos con privilegios a las cuentas de los usuarios que ya no necesitan acceso para realizar sus tareas asignadas. Si no lo necesitan, ¿por qué tenerlo?

- **Delegación de la cuenta de administrador de AD:** para hacer esto de manera efectiva, su herramienta de gestión de AD debe permitir un modelo de acceso con privilegios mínimos. Esto significa que los permisos para empleados individuales les permiten acceder a los recursos que necesitan para hacer su trabajo, pero nada más. Este modelo incluye la gestión limitada de cuentas y grupos elevados (como administradores de dominio, administradores de empresas y operadores de cuentas) sin otorgar privilegios ilimitados a personas individuales.
- **Pertenencia temporal a grupos (gestión de sesiones):** esto significa que la elevación de privilegios no es permanente y no se arrastra cuando un usuario con privilegios cambia de puesto de trabajo. Los usuarios solo serán parte de un grupo con privilegios durante un tiempo específico para realizar tareas específicas. Se agregan al grupo en el momento de inicio y luego se eliminan cuando ese permiso expira o la tarea se completa. Entonces, si una cuenta con privilegios es un objetivo de ataque, el impacto de ese ataque se limita a los privilegios normales del usuario.
- **Integre PAMOps y elevación de privilegios Just-In-Time:** esto implica automatizar las membresías a grupos privilegiados cuando sea necesario y eliminarlas cuando se completen las tareas con privilegios. Esta capacidad por sí sola reduce significativamente la superficie de ataque y la vulnerabilidad de las cuentas con privilegios en AD y Azure AD.
- **Administración controlada:** es un servicio administrativo que actúa como un firewall alrededor de AD. Esto proporciona un control de accesos mejorado a cuentas con privilegios mediante la definición de roles administrativos y permisos asociados y permite que las reglas se apliquen estrictamente. Es la única forma de mantener de manera efectiva el cumplimiento de las políticas y regulaciones de seguridad.

Eliminar cuentas innecesarias

Si la cuenta ya no es necesaria, ¿por qué sigue ahí? Una vez más, ¿quién la necesita?

Las cuentas que viven en AD que ya no se necesitan o ya no se usan son vulnerables verse comprometidas, más que una cuenta con actividad regular. Necesita una solución que brinde la capacidad de eliminar esta vulnerabilidad de manera programada a través de una política respaldada por un proceso. Por ejemplo, una solución eficaz puede inhabilitar automáticamente las cuentas que no se han utilizado en una determinada cantidad de días. Las soluciones eficaces también deben venir con políticas predeterminadas para automatizar las tareas de desaprovisionamiento comúnmente programadas y permitir que todas las políticas de aprovisionamiento se adapten a las necesidades específicas de una empresa.

Active Roles y Safeguard de One Identity permiten a las empresas con grandes entornos de AD híbridos implementar políticas mucho más sólidas para el control y la delegación.

Eliminar excesos de accesos

No permita que el "arrastre de roles" en su entorno de AD. Por lo general, aquí es donde un administrador cambia de puesto de trabajo y mantiene los permisos de una posición anterior o simplemente se eleva al rol de administrador de nivel superior con acceso a todo. ¿Cómose puede prevenir el arrastre de roles?

- **Delegación adecuada en AD:** debe buscar una solución que pueda garantizar que el administrador tenga los permisos necesarios para hacer su trabajo. Funciones como la pertenencia a un grupo dinámico pueden evitar el arrastre de roles, ya que pueden emitir y eliminar automáticamente permisos (o roles) cuando un administrador (o incluso un usuario de línea de negocio habitual) cambia de posición.
- **Aprovisionamiento automatizado:** automatiza el aprovisionamiento de usuarios y grupos, incluida la creación de cuentas en AD, la creación de buzones de correo en Office 365 o Exchange local, la población de grupos y el aprovisionamiento de recursos en Windows, lo que le ayuda a ahorrar un valioso tiempo administrativo y garantiza la precisión. La solución que seleccione debe automatizar el reaprovisionamiento y el desaprovisionamiento para lograr un proceso administrativo eficiente durante la vida útil de una cuenta de usuario o grupo.
- **Grupos con privilegios temporales:** colocar cuentas de usuarios con privilegios en grupos con privilegios permanentes es una vulnerabilidad crítica. Se beneficiará mejor si su solución puede poblar temporalmente grupos con privilegios para que un usuario sea miembro solo mientras realiza tareas con privilegios, y luego se eliminan cuando la tarea se completa. Si la cuenta de usuario se ve comprometida fuera de la ventana con privilegios, no tendrá ningún privilegio elevado, por lo que cualquier forma en la que se vea comprometida sería insignificante.

Eliminar permisos innecesarios

Elimine todos los permisos innecesarios de las cuentas con privilegios. Si no necesitan acceso, no se los dé. Cuando se lanzó AD por primera vez, supuso una gran mejora con respecto al directorio de Windows NT 4.0, ya que tenía un modelo de delegación. No ha cambiado mucho desde entonces. Las necesidades de delegación de las grandes empresas son significativamente más complejas de lo que posiblemente pueda proporcionar la herramienta de AD nativa.

- **Proporcione delegación granular:** la delegación de derechos granulares nativos en AD (particularmente los derechos de administrador de AD) es difícil, requiere mucho tiempo y es propensa a errores. Las soluciones eficaces proporcionan automatización, flujos de trabajo prediseñados e informes que permiten una alta granularidad en el aprovisionamiento de derechos de acceso.
- **Busque una solución que permita que las tareas de AD,** o grupos de tareas, se deleguen fácilmente a cualquier nivel, e incluso fuera de la estructura de OU de AD. Esto permite flexibilidad en el diseño de sus permisos y modelo de delegación, e incluso permite la superposición de la delegación sin exceso de permisos.

Las recomendaciones del NIST son principios generales diseñados para aplicarse a la amplia variedad de sistemas de información existentes. Afortunadamente, enfocar algunas de esas recomendaciones directamente en el entorno de AD híbrido proporciona un alto valor. AD, como lo conocemos, se encuentra en un estado de transición. Mientras trabajan para proteger el entorno AD local tradicional, muchas iniciativas empresariales están examinando la viabilidad de trasladar este servicio crítico a la nube. Si su empresa usa Office 365, entonces ya está utilizando AD en la nube. Con la mayoría de las empresas que ya han completado estudios sobre la viabilidad de Azure AD, vemos que concluyen que AD híbrido es el siguiente paso inevitable.

Presentación de Active Roles -local o en la nube- Active Directory híbrido, simple y seguro

Con los entornos de AD híbridos actuales y las capacidades limitadas de las herramientas nativas, los administradores luchan por mantenerse al día con las solicitudes para crear, cambiar o eliminar accesos. Afortunadamente, la ayuda está aquí. Con One Identity Active Roles, puede resolver sus problemas de seguridad y satisfacer los requisitos de cumplimiento interminables al asegurar y proteger los recursos de AD locales y en la nube, de manera simple y eficaz. Active Roles:

- Supera las limitaciones de las herramientas nativas
- Administra las cuentas para Exchange Online, Lync, SharePoint Online, Office 365 y mucho más
- Ofrece una herramienta de seguridad y administración simple e intuitiva para entornos híbridos de AD
- Se integra con One Identity Safeguard para el acceso privilegiado Just-In-Time para seguir las pautas de NIST ZTA

La nube plantea cuestiones de seguridad. Si Active Roles administra su AD local, así como su Azure AD, podrá hacer lo siguiente:

- Aplicar políticas sólidas y flexibles para la administración y la estructura, incluso el control de atributos
- Sincronizar AD local con AAD a través de conectores simples y fáciles de controlar
- Administrar entornos de AD en las instalaciones y en la nube con una única interfaz (MMC o interfaz de usuario web)
- Proporcionar a los administradores de nivel superior una herramienta familiar
- Permitir un acceso de administrador detallado en todo su entorno de AD híbrido

Almacenar, administrar, autenticar, grabar y analizar de forma segura el acceso con privilegios

La pieza complementaria crítica de este modelo de confianza cero y privilegios mínimos es el componente PAM que se integra a la perfección con su entorno híbrido de AD. Presentación de la familia de soluciones PAM de One Identity Safeguard. Estos son:

- Dispositivos virtuales o físicos reforzados, autónomos, listos para enchufar y usar, ya sea en las instalaciones o en su plataforma de nube preferida
- Soluciones modulares, pero integradas, para que solo use lo que necesita
- Fáciles y asequibles de expandir para respaldar su crecimiento y sus necesidades crecientes
- Familiares para los usuarios, lo que les permite seguir trabajando con las herramientas y los procesos que conocen, pero con una seguridad mejorada y casi sin fricciones.
- Se actualizan fácilmente para garantizar que siempre tenga las funciones y capacidades más recientes

Resumen

La creación de prácticas bien pensadas para proteger y administrar AD puede ser una tarea muy compleja, pero la parte fundamental de la seguridad es la implementación. Escribirlas y esperar que los administradores de todos los niveles las cumplan y hagan cumplir simplemente no es razonable.

Active Roles y Safeguard de One Identity permiten a las empresas con entornos de AD híbridos implementar políticas mucho más sólidas para el control y la delegación, así como mejorar la seguridad a través de la automatización, como la elevación de privilegios Just-In-Time para cumplir con la arquitectura de confianza cero del NIST. El NIST nos ha equipado con algunos buenos conceptos de tecnología para lograr avances significativos en la seguridad de la información crítica. Si bien no abordan específicamente la protección de AD en las instalaciones o en la nube, es fundamental que traduzcamos los conceptos y los apliquemos al sistema que brinda millones de decisiones de acceso todos los días para todas las empresas.

Acerca de One Identity

One Identity de Quest permite que las empresas implementen una estrategia de seguridad centrada en las identidades, ya sea localmente, en la nube o en un entorno híbrido. Con nuestro portafolio exclusivamente amplio e integrado de propuestas de gestión de identidades que incluyen administración de cuentas, gobernanza de identidades y gestión de accesos privilegiados y administración, las empresas son capaces de alcanzar su máximo potencial donde la seguridad se logra al ubicar las identidades en el centro del programa, lo que posibilita un acceso adecuado desde todos los tipos de usuarios, sistemas y datos. Obtenga más información en OneIdentity.com

Whitepaper_PrivilegedSecurityforAD_RS_63758