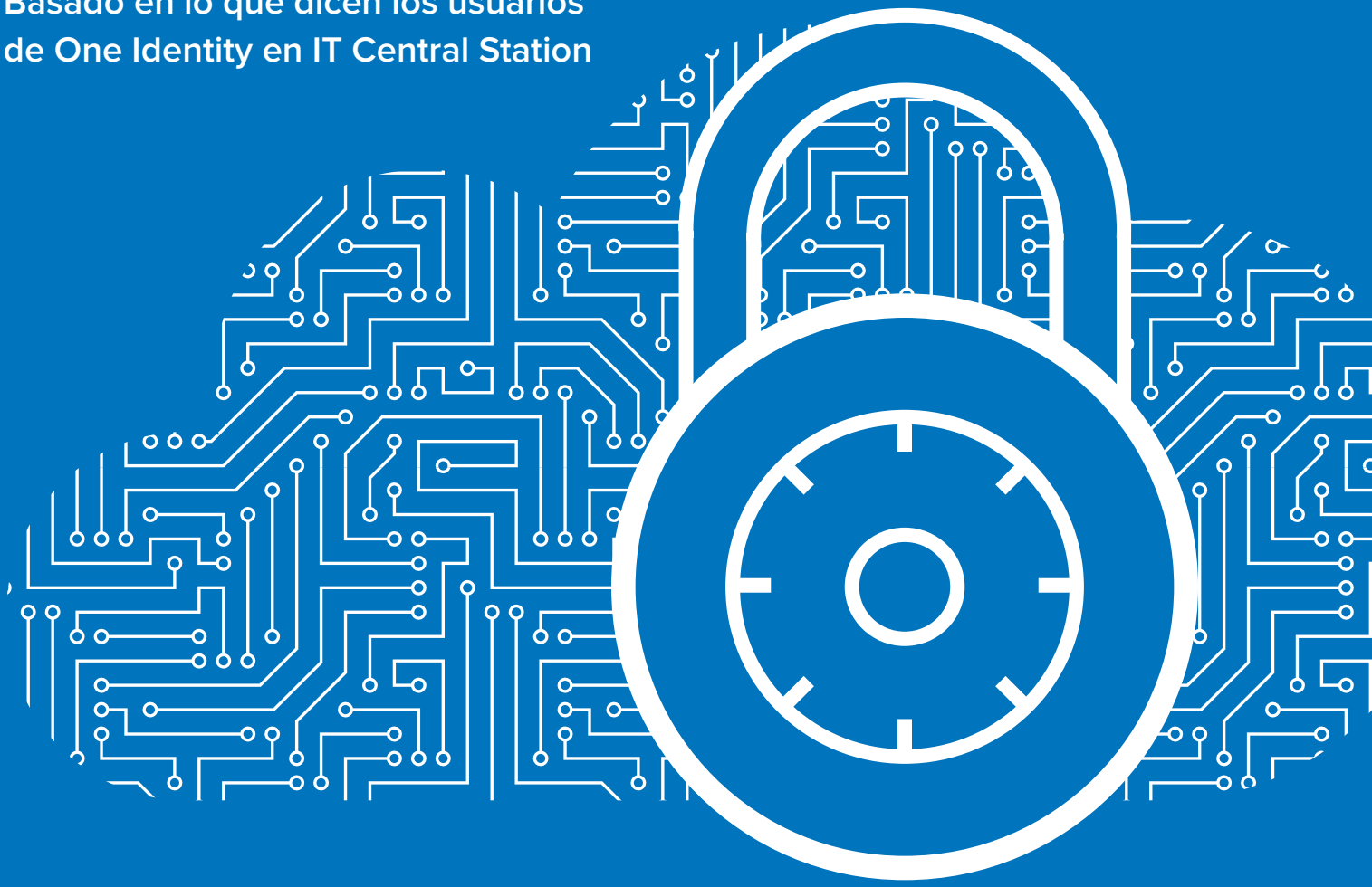
Informe PeerPaper™ 2021

10 prácticas recomendadas para administrar y proteger Microsoft Active Directory en un mundo de TI en evolución

Basado en lo que dicen los usuarios de One Identity en IT Central Station



IT Central Station
Unbiased reviews from the tech community

CSO
FROM IDG

RESUMEN

La mayoría de los programas de administración de identidades y accesos (IAM) se centran de forma confiable en Microsoft Active Directory (AD) y Azure AD (AAD) como su base. Sin embargo, a medida que los entornos de IAM se trasladan a la nube, se modernizan y se extienden hacia la gobernanza, los responsables de TI se ven perjudicados por las lagunas de seguridad y eficiencia del AD nativo, por lo que buscan soluciones para aumentar las capacidades de AD, que a menudo no son suficientes. Las empresas líderes están definiendo enfoques viables para asegurar y administrar los entornos de AD híbridos a medida que las identidades y la gobernanza de cuentas evolucionan mediante la adopción de la nube y mucho más. En este documento se exploran estas prácticas recomendadas emergentes, basadas en las experiencias de usuarios reales con la solución One Identity Active Roles, tal y como se describe en las reseñas de IT Central Station.

CONTENIDO

INTRODUCCIÓN

Dado que la seguridad es lo más importante para todos los CISO y líderes del área de TI, un marco de administración de identidades y accesos (IAM) seguro y correctamente administrado es un pilar fundamental de la estrategia de ciberseguridad. En efecto, los principales marcos de seguridad, como los del NIST, consideran que el control efectivo de las identidades de los usuarios y de los privilegios de acceso es el factor clave que posibilita numerosas contramedidas. En este ámbito, Microsoft Active Directory (AD) y Azure AD (AAD) siguen siendo el núcleo de la mayoría de los programas de IAM. No obstante, los responsables de seguridad suelen tener problemas con AD, ya que el entorno de TI se expande para ser híbrido y cada vez más complejo. Pretenden aumentar la funcionalidad limitada e ineficiente de las herramientas nativas de AD. Han surgido soluciones innovadoras como enfoques prácticos para mantener la viabilidad de AD a medida que la gestión de identidades evoluciona a través de la adopción de la nube y mucho más.

Excepto cuando se indica, todas las empresas que se mencionan en este informe tienen más de 10 000 empleados.

IAM en un mundo cambiante de TI y seguridad

A medida que las empresas trasladan los activos digitales a la nube y modernizan sus operaciones, se encuentran con nuevos retos de IAM. Sus casos de uso de One Identity Active Roles muestran cómo los administradores de identidades están adaptando la IAM a la nube. Por ejemplo, un responsable de TI de los servicios de seguridad de una empresa aeroespacial/de defensa utiliza Active Roles para su Active Directory local. Pese a ello, los propios servidores están alojados en Azure.

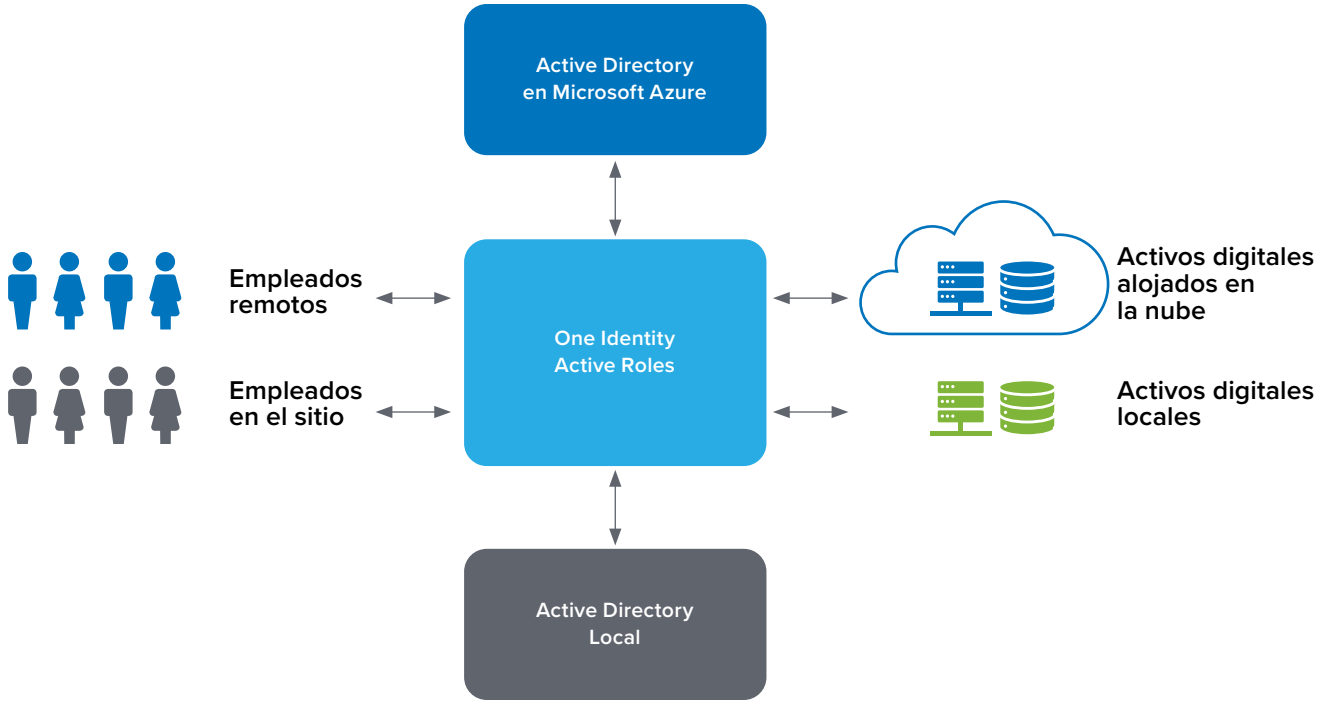


Imagen 1: La migración a la nube crea la necesidad de una IAM centralizada para administrar el acceso a los activos digitales, dondequiera que estén alojados.

Una analista de negocios sénior de la Universidad George Washington (GWU) utiliza Active Roles para muchos propósitos de administración de AD, que incluyen una capacidad central de creación de cuentas. Explicó: "Exponemos las propiedades nativas de los grupos de usuarios de Azure AD para ayudar a aumentar la asistencia. Aprovisionamos y desaprovisionamos las aplicaciones, y creamos los informes necesarios". La figura 1 ofrece una arquitectura de referencia sencilla que muestra cómo los activos digitales y las instancias de AD se distribuyen ahora entre el alojamiento cercano y el local.

Problemas con AD y otros sistemas heredados

El movimiento hacia las soluciones IAM aumentadas, como Active Roles, está impulsado por los problemas a los que se enfrentan los usuarios de AD y otros sistemas heredados y su necesidad de llenar las brechas inherentes a las herramientas nativas de AD. Como explicó un director técnico de seguridad de Liberty Global, un proveedor de servicios de comunicaciones, "La razón por la que optamos por esta solución [Active Roles] (y fue hace diez o quince años) fue la delegación de Active Directory. No podíamos permitir que todos tuvieran acceso nativo a nuestro Active Directory. Nos planteamos utilizar la solución de Microsoft porque es gratuita y está incorporada, y ya existe. Pero cuando se supera un determinado tamaño, se descubre que ya no es suficiente. Las funciones de gestión de AD y AAD de esta solución son realmente buenas. Son mejores que las herramientas nativas".

Un director de seguridad de la información de una empresa manufacturera con más de 5.000 empleados dijo: "Al principio utilizábamos las herramientas nativas de Microsoft. Cambiamos a Active Roles porque las herramientas nativas de Microsoft servían realmente para administrar los componentes principales y no tenían todas las capacidades de aprovisionamiento, desaprovisionamiento, control de accesos basado en roles e historial de cambios. No tenían el enfoque de proxy para administrar Active Directory de forma centralizada. Con Microsoft, Active Directory se distribuye por naturaleza, en comparación con Active Roles que lo centraliza".

"Antes de Active Roles, teníamos una solución de secuencias de comandos interna", señaló un director superior de TI de la Junta Escolar del Distrito de Toronto. "Cambiamos debido a su mejor soporte y a la sucesión de scripts de construcción manual antiguos y sin soporte. Así tenemos un producto que sabemos que tiene futuro y contamos con la asistencia adecuada. En comparación, las herramientas nativas de Microsoft son básicamente inexistentes para lo que estamos utilizando; los conectores para la federación de usuarios y la sincronización con las otras soluciones son inexistentes".

Para la analista de negocios sénior de GWU, Active Roles permitió a su equipo eliminar Oracle Identity Manager (OIM). Dijo: "Lamentablemente, la OIM se puso en marcha hace unos nueve años, pero demostró requerir un largo ciclo de vida para incorporar las aplicaciones y pasar a la provisión basada en roles, por lo que nunca pasamos de la primera fase. Hemos sacado todo de ese sistema y hemos creado, por así decirlo, un nuevo Active Roles para administrar todo lo que había allí. Si la OIM se ahogara, deberíamos hacer constantes reinicios. Ya no tenemos nada de eso ahora que estamos en Active Roles. No hemos puesto un ticket para un reinicio en más de un año desde que migramos".

> **“Cambiamos debido a su mejor soporte y a la sucesión de scripts de construcción manual antiguos y sin soporte.**

La necesidad de reforzar la seguridad mediante una mejor IAM

Una mejor IAM (es decir, una IAM más segura, más fácil de administrar y más eficiente) es un elemento clave para mejorar la postura de seguridad general de una empresa y establecer un enfoque sólido para la gestión y la administración de AD/AAD (AGA). Sin embargo, poner en práctica esta idea no siempre es sencillo. Están surgiendo diez prácticas recomendadas de IAM para un enfoque más sólido, más seguro y más eficiente.
La solución de IAM debe dificultar que los usuarios realicen cambios no autorizados.
La carga administrativa también puede ser elevada, así que los usuarios prefieren soluciones que permitan la automatización y la integración con otros sistemas.
La delegación del control también es fundamental para una IAM eficiente y eficaz. Lo ideal es que las soluciones de IAM también posibiliten la adopción del modelo de control de acceso de privilegios mínimos, lo que allana el camino hacia la confianza cero.

1. Reducir los cambios no autorizados mitiga el riesgo

Los cambios no autorizados en los controles de identidades y accesos son una fuente de exposición al riesgo, ya que usuarios desconocidos pueden obtener acceso sin que los administradores sean plenamente conscientes de lo que está sucediendo. La capacidad de Active Roles de complementar AD ayuda a reducir el impacto de este comportamiento. Como explicó el responsable de seguridad de la información de la empresa manufacturera, "al poder eliminar los derechos de administrador principal, hay menos cambios sin controlar, y cuando se producen menos cambios sin controlar, se tiene una mayor disponibilidad del servicio, en general, y menos resultados de auditoría". Y agregó: "La solución [Active Roles] definitivamente reduce el riesgo para nuestra empresa. Al evitar los cambios en la seguridad nativa de Active Directory, y el hecho de que exista un control de accesos basado en roles para administrar el propio Active Directory mediante la aplicación, se ha producido una reducción significativa del riesgo".

> **Nuestra decisión de optar por esta solución se enmarca en la necesidad de bloquear las cosas, de hacerlas más seguras.**

El director técnico de seguridad de Liberty Global puso el asunto en perspectiva cuando dijo: "El ROI de [Active Roles] está en la mitigación de los riesgos: El riesgo de dejar atrás el acceso no autorizado, el riesgo de tener la contaminación de Active Directory". En su opinión, "eso conlleva el riesgo de que la gente tenga un acceso que no debería tener. Existe el riesgo de tener múltiples cuentas para lo mismo".

"Ha mejorado las cosas porque no tenemos 'cambios descontrolados' que se hacen en AD sin que lo sepamos", comentó un analista sénior de identidades en una empresa de bienes de consumo. "La gente sigue teniendo que hacer las cosas que tiene que hacer, pero ahora podemos asegurarnos de que no haga algo que no debería sin saberlo. Antes la gente podía actualizar AD directamente. Hemos reducido eso impulsando todo mediante Active Roles. Nuestra decisión de optar por esta solución se enmarca en la necesidad de bloquear las cosas, de hacerlas más seguras".

2. Integración de IAM en los sistemas de seguridad

IAM es un área de TI y seguridad que funciona mejor cuando puede integrarse con relativa facilidad con otros sistemas de la empresa. En el caso del gestor de seguridad de la información de la empresa de fabricación, por ejemplo, esto significa utilizar Active Roles para suministrar objetos de Active Directory. Al mismo tiempo, lo está utilizando para conectarse, mediante el Servicio de Sincronización de Active Roles, a un sistema de RR. HH. y para suministrar y retirar empleados. En general, lo utilizamos para aprovisionar cualquier objeto: grupos de seguridad y objetos informáticos, de forma delegada. El servidor de Active Roles permite cambiar la seguridad de Active Directory para delegar el acceso de provisión a diferentes equipos de TI, sin cambiar la seguridad real de Active Directory".

> **... lo utilizamos para aprovisionar cualquier objeto: grupos de seguridad y objetos informáticos, de forma delegada.**

El responsable del área de TI del sector aeroespacial utiliza la interfaz PowerShell de Active Roles para permitir que otras partes de su entorno y otras aplicaciones, que podrían necesitar interactuar con él, realicen cambios en Active Directory utilizando comandos de PowerShell. Como señaló, "podemos aplicar el mismo principio que nuestros derechos de seguridad para que deban utilizar Active Roles, lo que reduce nuestro riesgo desde el punto de vista de la seguridad".

3. Delegación para mejorar la seguridad

Los miembros de IT Central Station debatieron sobre su preferencia de poder delegar el acceso a los procesos de AD. Por ejemplo, BeClever IT Solutions, una pequeña empresa de servicios tecnológicos, está trabajando con un cliente que tiene un problema con sus permisos y delegaciones. Muchos de los usuarios de esta empresa deben realizar actividades de administración en AD. Esto resultaba problemático por la posibilidad de que estos usuarios cometieran errores. Ahora, con Active Roles, pueden omitir a los administradores de dominio y mantener a sus usuarios habituales. Pueden rellenar previamente los valores de determinados campos.

Según dijo, "esto es fantástico para ellos porque parte del personal son técnicos informáticos de nivel básico sin conocimientos de las funciones avanzadas de AD". Esta solución eliminó las tediosas tareas de TI con el aprovisionamiento". El director de seguridad de la información de la empresa manufacturera también agregó: "El acceso delegado a Active Directory nos permite revocar muchos de los derechos de administración. Nos da un mejor cierre y un entorno más seguro que el que teníamos antes".

4. Adoptar el modelo de privilegios mínimos y habilitar la confianza cero

Algunos usuarios de Active Roles en IT Central Station están aprovechando la solución para implementar el modelo de administración de acceso de privilegios mínimos. Este enfoque está ganando cada vez más adeptos, sobre todo a medida que el perímetro de seguridad tradicional se desvanece y las empresas planean pasar al modelo de confianza cero. Tal y como describió el responsable de TI del sector aeroespacial, "somos muy partidarios de utilizar el modelo con privilegios mínimos y de tener la menor cantidad posible de derechos nativos de Active Directory, ya que así se reducen los problemas posteriores". Teniendo menos personas con derechos nativos de Active Directory, se reducen los posibles problemas que debemos solucionar". La imagen 2 muestra una representación del modelo de privilegios mínimos utilizando la imagen de "anillos" de privilegio creciente, con el privilegio mínimo en el anillo exterior.

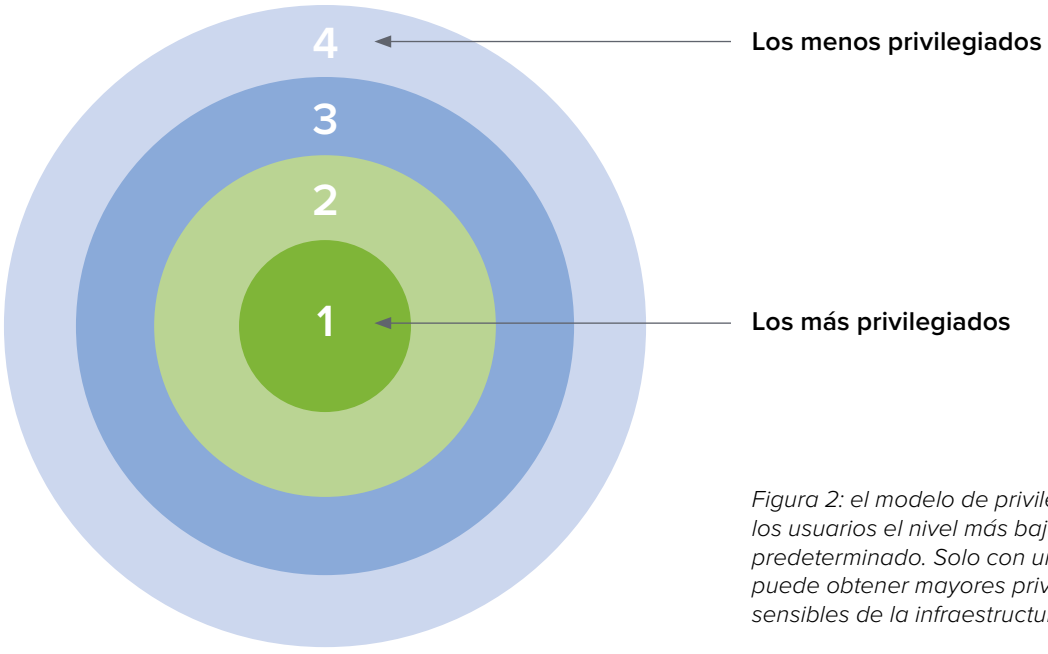
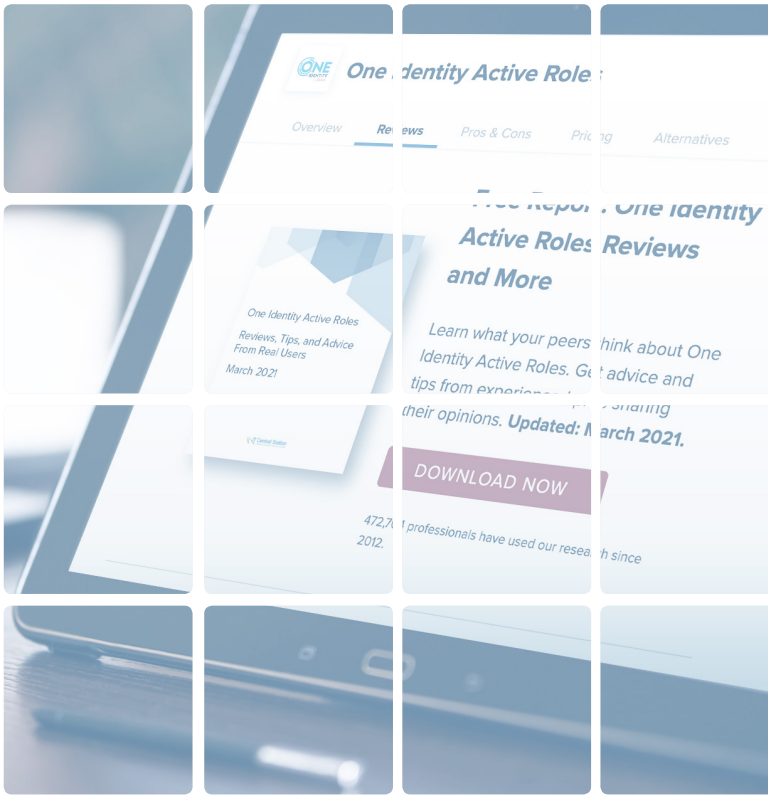


Figura 2: el modelo de privilegios mínimos asigna a los usuarios el nivel más bajo de privilegio de acceso predeterminado. Solo con un permiso específico, un usuario puede obtener mayores privilegios y acceder a zonas más sensibles de la infraestructura, los datos, entre otros.

Mejora del proceso de administración de identidades

Dada la importancia de reforzar la seguridad mediante una mejor IAM, ¿qué se necesita para mejorar el proceso de administración de identidades? Los miembros de IT Central Station opinaron, destacando la importancia de tener un punto de control unificado, pero acompañado de granularidad de control. Ahorrar tiempo es importante, al igual que tener un proceso de incorporación eficiente. También es esencial poder automatizar los flujos de trabajo de administración de identidades, utilizando políticas y plantillas, y aprovechando los grupos dinámicos para lograr el mayor impacto posible.



5. Unificar la administración con una única consola

Los usuarios de Active Roles, como el responsable de TI del sector aeroespacial, se mostraron complacidos de poder administrar múltiples Active Directories desde una sola consola y tener una "única consola" local. Indicó: "Contamos con muchos entornos de Active Directory, por lo que podemos administrarlos y verlos todos en un solo lugar". La analista de negocios sénior de GWU hizo eco de este sentimiento, afirmando: "La flexibilidad y la extensibilidad de esta plataforma nos permitieron lograr mucha más eficiencia de la que esperábamos. Active Roles también le ofrece una única consola para administrar AD y Azure AD. Una de las cosas que más nos gusta es que podemos acceder a todo desde Active Roles si lo necesitamos".

Un empleado de Marriott Phoenix se refirió a la cuestión del control. Según él, "Active Roles nos da la capacidad de proporcionar un control granular que AD no ofrece. Disponer de una herramienta para administrar todos los cambios de AD desde una sola consola es impresionante. También permite al personal del servicio de asistencia técnica ponerse al día muy rápidamente sin tener una gran formación técnica".

6. Mejorar la incorporación y la administración del ciclo de vida de los usuarios

La administración de los aspectos de identidades y accesos del ciclo de vida de los empleados es una posible pérdida de tiempo, pero también es un punto de vulnerabilidad. Por ejemplo, los antiguos empleados que conservan el acceso a los datos de inicio de sesión suponen una amenaza para la seguridad. Para mitigar los riesgos asociados, una solución de IAM debe permitir controles eficientes y eficaces del ciclo de vida de los usuarios. Por ejemplo, el director de seguridad de la información de una empresa manufacturera compartió que su solución automatiza la el aprovisionamiento. Y añadió: "En nuestro sistema de RR. HH., estamos automatizando la creación, el cese y la administración continua de toda nuestra base de empleados. Tenemos entre 5.000 y 6.000 empleados, y todos esos procesos están totalmente automatizados sin que la informática intervenga. Ahorra muchas horas fácilmente de alrededor de cientos de horas al año".

Este usuario comentó entonces que "One Identity Active Roles también ha mejorado la precisión de nuestro proceso de incorporación. Como empresa, nuestro proceso de incorporación de personal está sometido a auditorías SOX [Ley Sarbanes Oxley]. Hace diez años, nos encontrábamos en una situación en la que teníamos cientos de disconformidades. En la actualidad, tenemos básicamente cero disconformidades". El director superior de TI del Consejo Escolar de Toronto coincidió con esta afirmación: "Active Roles ha mejorado la precisión de nuestro proceso de incorporación. Hay menos errores durante la sincronización".

7. Automatización de los flujos de trabajo de administración de identidades

La excesiva dependencia en los procesos manuales para administrar la IAM es ineficaz y propensa a errores. Por lo tanto, los administradores están a favor de las soluciones de IAM que permitan la automatización de los procesos de seguridad. Según el responsable de TI del sector aeroespacial, "entre la automatización del uso de Active Roles para realizar nuestra incorporación, las políticas y los flujos de trabajo, podemos garantizar que los datos que se introducen en Active Directory durante la incorporación de cualquier tipo de objeto para Active Directory son precisos y cumplen nuestros estándares, de modo que no se introduce basura. Esto ha ayudado a agilizar las cosas".

> “
>
> **Ahorra muchas horas, fácilmente del orden de cientos de horas al año"**

Como también explicó, "una de las cosas más difíciles desde la perspectiva de la administración de Active Directory, sin una herramienta como Active Roles, es controlar cómo la gente hace algo. La forma en que yo querría instalar o configurar un nuevo usuario podría ser diferente a la de la persona que está a mi lado. Por ejemplo, se puede dar a alguien un conjunto de políticas para seguir cuando no se está utilizando un producto como Active Roles, entonces depende de esa persona interpretarlas y seguirlas. Active Roles nos permite aplicar esas políticas para que los datos que se introduzcan en Active Directory sean más limpios y consistentes. Disponer de datos consistentes nos permite hacer muchas más automatizaciones y asegurarnos de que las personas y los objetos estén correctamente configurados".

Otros comentarios notables sobre la automatización incluyen lo siguiente:

- "También ha mejorado nuestra automatización. Ya estaba automatizado, pero lo ha mejorado. Fue capaz de capturar más datos de Trillium y SAP, y poblar Active Directory de forma abierta. Tenemos dos miembros del personal y; por consiguiente, por cada miembro del personal, Active Roles nos ahorra 0,2 ETC". - Director superior de TI de la Junta Escolar del Distrito de Toronto

- "Ha eliminado tareas que estaban atascando nuestro departamento de TI, en especial en algunas automatizaciones del flujo de trabajo. A través del Servicio de sincronización de Active Roles, podemos procesar los datos procedentes de RR. HH. y actualizar de manera automática esos atributos y campos de datos directamente en Active Directory, frente a hacerlo de forma manual o mediante importaciones masivas". - Director de seguridad de la información en una empresa de fabricación con más de 5.000 empleados

- "Logramos introducir el aprovisionamiento automatizado basado por primera vez, porque teníamos Active Roles. Además, con el uso de los flujos de trabajo y las tareas programadas, pudimos automatizar y administrar de forma centralizada varios de los procesos, así como utilizarlos para sortear las limitaciones de otros productos. Estos incluyen, entre otros, la sincronización con Azure AD de los grupos más grandes, que tienen más de 50 000 miembros". - Director gerente Analista de negocios en la Universidad George Washington

8. Ahorro de tiempo y aumento de la eficacia

La solución de IAM adecuada ayudará al personal de TI y de seguridad a ahorrar tiempo. Este fue el caso de la analista de negocios sénior de GWU, que descubrió que Active Roles permitía a su equipo hacer más y ser más eficiente. El director técnico de seguridad de Liberty Global tuvo una experiencia similar, ya que consideró que la solución ha eliminado numerosas tareas informáticas tediosas, sobre todo cuando el personal deja la empresa.

Este usuario explicó que "hay diez o quince acciones con script que hace Active Roles, siempre de la misma manera y a la misma hora. Antes, había literalmente una lista de cosas que el administrador debía hacer, como ocultar el buzón de correo, deshabilitar el usuario, eliminar los grupos, entre otros. Además, el historial de auditorías que guarda nos resulta muy útil. Nos proporciona un registro de cambios de lo que se ha hecho a un usuario, quién lo hizo, cuándo lo hizo, y eso realmente ayuda. Y ahora que estamos subcontratando muchas actividades, nos enfrentamos a un público cambiante. Herramientas como esta garantizan que todo se haga de forma estructurada, que todos hagan lo mismo a la vez".

> **"La solución ha ahorrado tiempo a nuestros clientes al automatizar tareas que podían llevar de media hora a 45 minutos"**

Algunos usuarios pudieron calcular su ahorro de tiempo. El director de tecnología de BeClever IT Solutions reveló que "la solución ha ahorrado tiempo a nuestros clientes automatizando tareas que podían llevar de media hora a 45 minutos". El responsable de TI del sector aeroespacial comentó que, en su empresa de 55 000 personas, "la gente entra a la empresa y sale de ella todos los días". En este entorno, "Active Roles quizás nos ahorra más de 500 solicitudes a la semana. La solución ha eliminado las tareas de administración que estaban atascando a nuestro departamento de TI. Ahora, nadie de TI tiene que tomar medidas para actualizar el grupo en los casos en que alguien se incorpore a la empresa o se desvincule de ella". La analista de negocios sénior de GWU dijo: "Active Roles tal vez nos ahorra al menos dos semanas de cada mes. Ha reducido nuestra carga de trabajo en un 50 %, fácilmente".

9. Uso de políticas y plantillas para mejorar el control basado en roles

Las políticas y plantillas basadas en roles ayudan a mejorar el control de acceso, ahorrar tiempo y aumentar la precisión para la gestión y la administración de AD. En palabras del empleado del Marriott Phoenix, "las plantillas integradas

en Active Roles permiten crear grupos de seguridad sin tener que construirlos por cuenta propia. Simplifica enormemente el proceso y también facilita mucho la revisión si alguna vez hay que hacer cambios". El director técnico de seguridad de Liberty Global comentó que "Active Roles permite la aplicación de políticas y hay un montón de ejemplos de políticas que vienen con él". Y agregó: "Tiene plantillas de acceso y hay muchos ejemplos de plantillas de acceso en él. También tiene flujos de trabajo y estos son realmente potentes".

10. Aprovechar los grupos dinámicos para reducir el riesgo y automatizar las actualizaciones

"Mi característica favorita [de Active Roles] tal vez sean los Grupos Dinámicos y el hecho de que los Grupos Dinámicos se crean prácticamente sobre la marcha y se mantienen actualizados. Eso es muy importante para nosotros", afirmó el responsable de TI del sector aeroespacial. A continuación, dijo: "Recibimos de forma habitual solicitudes de nuestra empresa, que dicen 'Necesitamos un grupo que contenga a todo el mundo en este departamento en particular', ya sea una lista de distribución solo para correos electrónicos, un grupo para asegurar un servidor de archivos, entre otros. Con Active Roles, podemos crear este grupo y decirle a Active Roles: "Cada cuenta de usuario que encuentre que tenga un departamento igual a 'esto' ponla en este grupo".

> **“No tenemos que esperar a que un ser humano vaya a mirar en cada grupo para ver si esa persona está allí.**

Para la analista de negocios sénior de GWU, el uso de grupos dinámicos reduce el riesgo y mejora la seguridad eliminando las cuentas huérfanas, que es una vulnerabilidad importante. Dijo: "Con un grupo dinámico, si la persona ya no está en la fuente proveniente del sistema de RR. HH., entonces se la quita inmediata y automáticamente del grupo. No tenemos que esperar a que un ser humano vaya a mirar en cada grupo para ver si esa persona está allí. Es una cuestión de llevar a cabo las prácticas recomendadas e internas, asegurándonos de que cumplimos el requisito de tener el menor acceso posible".

CONCLUSIÓN

La IAM es cada vez más compleja a medida que los entornos de TI se vuelven más complejos y migran, al menos en parte, a la nube. Microsoft Active Directory funciona bien para las funciones básicas de IAM, pero la realidad de la administración de las identidades y el control de accesos crea la necesidad de soluciones más sofisticadas y automatizadas que puedan construirse sobre AD. Como explican los usuarios de One Identity Active Roles en los comentarios de IT Central Station, la solución adecuada puede aumentar la eficiencia de IAM y ahorrar tiempo. Puede conducir a una reducción de los cambios no autorizados y a una mejora de la postura de seguridad mediante la delegación, los grupos dinámicos, las políticas y las plantillas. Un punto de control unificado permite aumentar la eficiencia. En última instancia, las soluciones como Active Roles, que pueden funcionar tanto en la nube como de forma local y en modo híbrido, proporcionan la base para las mejoras continuas en IAM (y la postura de seguridad más amplia de una empresa) a medida que la TI y la seguridad siguen evolucionando.

SOBRE IT CENTRAL STATION

Opiniones de usuarios, debates sinceros y más para los profesionales de la tecnología empresarial.

Internet ha cambiado por completo la forma de tomar decisiones de compra. Ahora utilizamos sitios de valoraciones y reseñas para ver lo que piensan otros usuarios reales antes de comprar productos electrónicos, reservar un hotel, visitar a un médico o elegir un restaurante. Pero en el mundo de la tecnología empresarial, la mayor parte de la información en línea y en su bandeja de entrada proviene de los proveedores. Lo que realmente desea es información objetiva de otros usuarios. IT Central Station ofrece a los profesionales de la tecnología una plataforma comunitaria para compartir información sobre soluciones empresariales.

IT Central Station se compromete a ofrecer información que aportan los usuarios y que es valiosa, objetiva y relevante. Validamos a todos los revisores con un triple proceso de autenticación, y protegemos su privacidad proporcionando un entorno en el que puede publicar de forma anónima y expresar libremente sus opiniones. Como resultado, la comunidad se convierte en un recurso valioso, que le garantiza el acceso a la información correcta y la conexión con las personas adecuadas, siempre que lo necesite.

www.itcentralstation.com

IT Central Station no respalda ni recomienda ningún producto o servicio. Los puntos de vista y las opiniones de los revisores citados en este documento, los sitios web de IT Central Station y sus materiales no reflejan las opiniones de IT Central Station.

ACERCA DE ONE IDENTITY

One Identity, una empresa de Quest Software, 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 con privilegios 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