DOCUMENTACIÓN TÉCNICA

Juntos es mejor: 10 formas de acelerar Active Directory con One Identity Active Roles

Acerca de este documento

En este documento se detallan 10 pasos para solucionar y evitar problemas de cuentas de usuario en AD. Estos pasos utilizan características nativas de AD y tecnología de flujo de trabajo habitual, como Microsoft SharePoint, lo que significa que hay una curva de aprendizaje muy pequeña para implementar las recomendaciones en este documento.

Sin embargo, aunque siga todas las recomendaciones de este documento, sin herramientas adicionales que le ayuden a administrar y automatizar sus procesos, gran parte de la carga administrativa y de confirmación manual seguirá recayendo en sus administradores de línea de negocio, representantes de RR. HH. y personal de TI.

La buena noticia es que puede reducir casi todos estos problemas con One Identity Active Roles de Quest. Active Roles proporciona una gran cantidad de funciones para eliminar la dependencia de los usuarios finales, los administradores y el personal de RR. HH. Siga leyendo para ver cómo Active Roles facilita cada uno de los 10 pasos.

Información general

Microsoft Active Directory (AD) y Azure AD (AAD) aportan organización y estándares a la forma en que se administran y almacenan los datos de identidad y cuentas. One Identity Active Roles aporta agilidad, seguridad, rapidez y unidad a la administración de AD/Azure AD. Con Active Roles y AD/AAD, los responsables de la administración de TI disponen de una solución que mejora notablemente la seguridad y la eficacia de sus entornos AD, lo que reduce la vulnerabilidad. Utilizar una analogía es como si se tomara una versión de producción potente de un coche deportivo y se le agregara una suspensión de carreras, un turbocompresor y un panel de control conectado a la nube y un sistema de supervisión de rendimiento ampliamente mejorados, además de proteger todo con un mando de acceso remoto, programable y de gran seguridad.

Si bien el vehículo en exhibición es excelente, la versión mejorada por el mercado de accesorios le permite ocuparse de todo lo que el camino le depare, incluidos los cambios y las amenazas masivas. Es más rápido, más seguro, dobla como una gacela, necesita menos mantenimiento continuo y es más eficiente en cuanto al consumo de combustible. Su inversión adicional se recupera con rapidez y lo prepara para emprender con seguridad viajes que antes eran impensables. Simplemente es mejor.

Lo mismo ocurre con Active Roles y One Identity Active Roles. Juntos son mejores.

Si usted es como el 95 % de las empresas de la lista Fortune 1000, ya dispone del auto en exhibición: utiliza Microsoft Active Directory como su conductor diario para la provisión y eliminación de los permisos de los usuarios. No obstante, el mundo se mueve más rápido, los recursos que AD y Azure AD (así como AD LDS) administran continúan diversificándose. Además, otras tendencias aumentan la complejidad que rodea a AD/AAD, como la seguridad de las identidades, la migración a la nube y el papel fundamental que AD/AAD desempeña en la administración de accesos con privilegios (PAM). Últimamente, la implementación de una arquitectura de seguridad de confianza cero (o privilegio permanente cero) para prevenir y limitar los daños de una infracción está impulsando la necesidad de ampliar y mejorar las capacidades nativas de AD/AAD. Aquí es donde Active Roles de One Identity puede automatizar y potenciar los servicios de AD/AAD.

En este documento, le mostraremos 10 pasos para limpiar los datos de las cuentas de usuario de Microsoft AD/AAD. Este proceso es clave para la eficiencia y la seguridad. A medida que vayamos desglosando cada uno de los diez pasos, le iremos explicando cada uno de ellos, demostrando por qué es importante y cómo One Identity Active Roles permite o acelera ese paso. Muchos de los pasos son de sentido común (como eliminar las cuentas que no se utilizan y revocar el acceso a las aplicaciones y otros recursos), pero como todos sabemos, en el fragor de la batalla diaria, resulta difícil priorizar las tareas manuales de mantenimiento de cuentas frente a las situaciones graves relacionadas con la tecnología y los datos. Vea cómo One Identity Active Roles puede automatizar y asegurar esas tareas y, junto con One Identity CertAccess, puede garantizar que se sigan y registren los procesos de autorización, aprobación y certificación.

Active Roles proporciona una gran cantidad de funciones para eliminar la dependencia de los usuarios finales, los administradores y el personal de RR. HH.

Estos 10 pasos utilizan características nativas de AD y tecnología de flujo de trabajo habitual, como Microsoft SharePoint, lo que significa que hay una curva de aprendizaje muy pequeña para implementar las recomendaciones en este documento.

Sin embargo, aunque siga todas las recomendaciones de este documento, sin herramientas adicionales que le ayuden a administrar y automatizar sus procesos, gran parte de la carga administrativa y de confirmación manual seguirá recayendo en sus administradores de línea de negocio, representantes de RR. HH. y personal de TI.

La buena noticia es que puede reducir casi todos estos problemas con One Identity Active Roles de Quest. Active Roles proporciona una gran cantidad de funciones para eliminar la dependencia de los usuarios finales, los administradores y el personal de RR. HH.

Siga leyendo para saber cómo y por qué Active Directory y One Identity Active Roles son mejores juntos.

Active Directory es crucial para controlar el riesgo y garantizar el cumplimiento de la normativa

Active Directory (AD) es la base de la administración de identidades y accesos (IAM) en la mayoría de las empresas y, como tal, es posible que sea la tecnología más importante de la red. Cada vez más sistemas y aplicaciones utilizan AD y Azure Active Directory (AAD) para la autenticación, las políticas, los permisos y la administración de la configuración. Si AD no es seguro, nada es seguro.

Las cuentas de usuario son importantes para la seguridad, pero son difíciles de mantener

Asegurar Active Directory/Azure AD es crucial para controlar el riesgo y lograr el cumplimento de la normativa. Pese a ello, mantener AD en un estado limpio, organizado y seguro es un desafío, en particular para las cuentas de usuario.

Las cuentas de usuario son la base de la autenticación y el acceso a las redes, sistemas y aplicaciones. Son difíciles de mantener sin las herramientas adecuadas para dar soporte al seguimiento de todos los permisos de un usuario en múltiples plataformas. Cuando se contrata a un empleado, se crea una cuenta de usuario. A medida que cambian el trabajo y las asignaciones del usuario, la cuenta de AD del usuario (como el puesto de trabajo, el departamento y el número de teléfono) se actualiza, incluso cuando el usuario abandona grupos o se une a ellos. En última instancia, cuando el usuario abandona la empresa por completo, los permisos de acceso de la cuenta deben eliminarse de forma adecuada.

Este proceso parece sencillo y sin complicaciones. No obstante, muchas empresas funcionan con una cantidad importante de cuentas de usuario con permisos inadecuados u obsoletos, y que no cumplen con la política de seguridad de la empresa. Y lo que es más importante, exponen a la empresa a riesgos de seguridad.

La causa de estos problemas es la debilidad de las prácticas del ciclo de vida de las cuentas de usuario. Tradicionalmente, las empresas confían en los usuarios finales, los administradores y el personal de RR. HH. para reconocer los eventos que afectan a la cuenta de AD de un usuario. Luego se espera que estas personas ocupadas informen a su sobrecargado equipo de TI para que realice los cambios en AD con el fin de mantener las cuentas de los usuarios actualizadas. Cuando se sirve exclusivamente de procesos manuales, estos cambios no se ejecutan con demasiada frecuencia, lo que da lugar a cuentas fantasma y permisos inadecuados que pueden ser el objetivo de los actores con malas intenciones para causar problemas en una empresa.

10 pasos para mejorar la agilidad, la seguridad y el rendimiento de Active Directory

Paso 1. Realizar un análisis periódico de la cuenta

La forma más eficaz de mantener un AD/AAD limpio y seguro es revisar de forma periódica las cuentas de los usuarios. Si revisa las propiedades de la cuenta antes de una auditoría, podrá encontrar y corregir rápidamente muchos puntos con los que los auditores tienen problemas.

Obtener una lista de cuentas de usuarios es fácil

Hubo un momento en que obtener una lista de cuentas de usuario no era tarea sencilla. Ahora es una simple cuestión de ejecutar un script de Windows PowerShell e importar los resultados a Microsoft Excel. Vea este script (Output-ADUsersAsCSV) disponible en http://www.ultimatewindowssecurity.com/tools/Output-ADUsersAsCSV. El resultado será una hoja de cálculo, como la que se muestra a continuación.

	A	B	C	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	Distinguished Name	Display Name	SAM ID	Description	Office	Phone	E-mail Address	Job Title	Dept	Org	Company	Manager	Can user change password ?	Does password expire?	Is account disabled?	Account Expiration Date	Last Log-on Date	Has user ever logged on?
2	CN=Administrator,CN=Users,DC=mt		Administrat	Built-in account for administering the computer/domain									Yes	Yes	No		10/13/12	Yes
3	CN=Guest,CN=Users,DC=mtg,DC=lo		Guest	Built-in account for guest access to the computer/domain									Yes	No	Yes			No
4	CN=krbtgt,CN=Users,DC=mtg,DC=lo		krbtgt	Key Distribution Center Service Account									Yes	Yes	Yes			No

Filtrar la hoja de cálculo para encontrar cuentas con incumplimientos

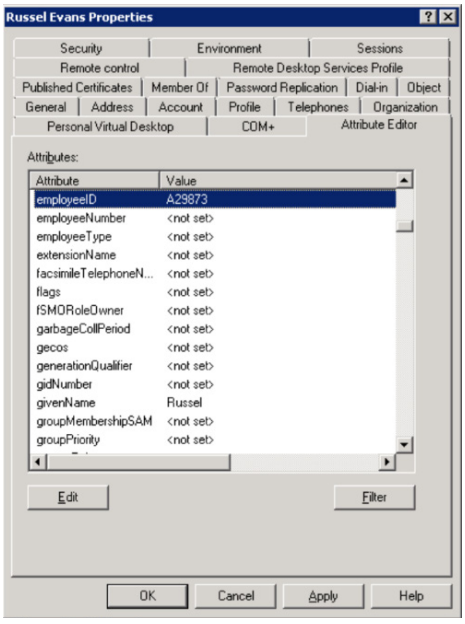
Con un script y la hoja de cálculo resultante, se puede filtrar por varias propiedades de los usuarios para encontrar las cuentas con incumplimiento. Comience por identificar las cuentas con problemas fáciles de encontrar, como una contraseña que nunca caduca. A continuación, incluya criterios de filtrado en otras columnas, como el ID de SAM o la descripción, para eliminar las cuentas de servicios, aplicaciones y otras que sepa que son excepciones.

Se trata de problemas fáciles de solucionar antes de que llegue el auditor y que reducirán la cantidad de hallazgos de riesgo en su auditoría. Un problema obvio que hay que buscar son las cuentas inactivas, hay todo un paso que se centra en este tema más adelante.

Hay otros problemas, como las cuentas que nunca debieron crearse en primer lugar o que no contaron con las normas de nomenclatura u otros controles de creación de cuentas.

Por ejemplo: La norma de nomenclatura de Acme Corp exige que todas las cuentas de usuario final empiecen por "u-", las de administrador por "p-" (de privilegio) y las de servicio por "s-". En primer lugar, filtre todas las cuentas que empiecen por esos prefijos para encontrar el resto de cuentas dudosas. Algunas de esas cuentas restantes podrían ser excepciones legítimas, que se pueden abordar en un paso posterior. Muchas de estas cuentas resultarán ser cuentas misteriosas que deberá localizar para determinar el propósito y el estado.

Sin duda, es conveniente realizar este paso antes de una auditoría. Sin embargo, esto debería hacerse cada mes para estar al tanto de su AD. Al fin y al cabo, es probable que no esté contratado solo para pasar auditorías, sino que el objetivo debe ser mantener la seguridad y la organización de AD en todo momento.



Existen muchas formas de vincular las cuentas de AD a los registros de los empleados: (1) Utilizando el atributo ID de empleado o Número de empleado en AD; (2) A través de la pestaña "Attribute Editor" (editor de atributos), como se muestra en la imagen anterior; (3) Ingresando el ID del empleado en el campo Description o Notes; (4) Incorporando el número de empleado en el nombre de inicio de sesión.

Tenga en cuenta que este paso es un control de detección o reactivo, no un control preventivo o proactivo. Su objetivo debe ser evitar que se produzcan los problemas. El paso 2 es la primera forma de lograr ese objetivo.

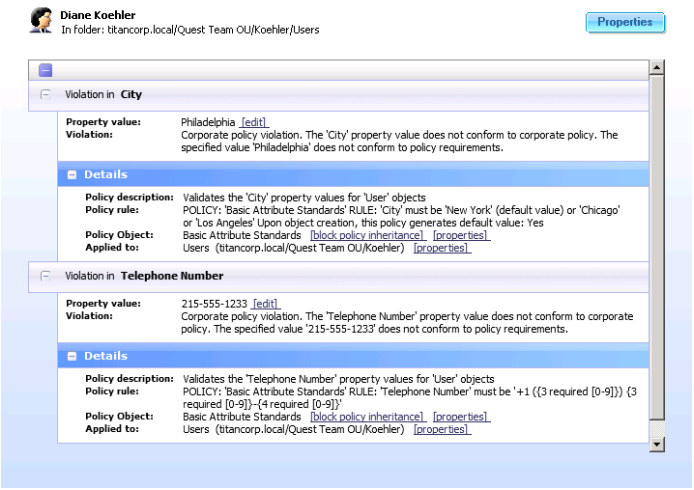
Cómo ayuda Active Roles

Active Roles tiene la capacidad de comparar sus estándares de objetos AD previstos (llamados políticas) con sus objetos AD reales. Los resultados de esta comparación (llamada Solicitud de política de verificación) se entregan ad hoc, en pantalla con dos clics o mediante informes programados cada cierto tiempo. Esta funcionalidad puede ayudar a una empresa a poner el hogar en orden.

Con una inversión administrativa relativamente pequeña en la creación de políticas, se puede iniciar el proceso para recuperar el control.

Paso 2. Vincular las cuentas a los registros de los empleados

La forma más importante de mantener las cuentas de AD limpias y seguras es vincular todas las cuentas a un usuario real. Esto incluye las cuentas no humanas, como las creadas para servicios y aplicaciones, que se explicarán más adelante en el paso 7. En primer lugar, se debe centrar en las cuentas creadas para personas, incluidos los usuarios finales, contratistas, administradores y otros.



Active Roles tiene la capacidad de comparar sus estándares de objetos AD previstos (llamados políticas) con sus objetos AD reales.

Lo más importante es que cualquier cuenta de empleado debe estar vinculada al registro maestro del empleado en su sistema de RR. HH.

Este nexo es fundamental porque el acceso de los empleados a la red debe estar vinculado a su estatus y función dentro de la empresa. El registro oficial de esto es el registro maestro en RR. HH., que también tiene la mayor probabilidad de estar actualizado.

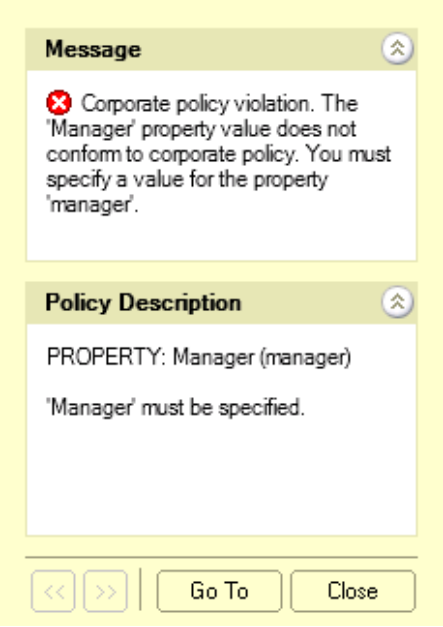
Cuando el estatus o la función de un empleado cambia, debe poder encontrar las cuentas del empleado y en consecuencia cambiar el estatus o los permisos. La clave es documentar el ID del empleado en las cuentas de AD. Por supuesto, también se deben poner en marcha procedimientos para facilitar la respuesta a estos eventos, lo que se trata en un paso posterior.

Cómo ayuda Active Roles

Usando las políticas de creación de cuentas, Active Roles puede ordenar que todas las cuentas no humanas sean creadas con un valor Manager o EmployeeID. De hecho, Active Roles puede administrar la provisión de cuentas y el formato de cualquier atributo.

Paso 3. Controlar las cuentas nuevas

En las auditorías de TI de AD, es frecuente encontrar cuentas inservibles y no estándares, incluidas aquellas que se alejan de las convenciones de nomenclatura corporativa. Esto sucede cuando demasiadas personas en el departamento de TI tienen autoridad para crear cuentas. Esto se abordará en un paso posterior.



Los intrusos que consiguen su objetivo, tanto humanos como automatizados, suelen crear cuentas secretas para asegurarse un acceso continuado y enmascarar su actividad.

Los intrusos suelen crear cuentas secretas

Los intrusos que consiguen su objetivo, tanto humanos como automatizados, suelen crear cuentas secretas para asegurarse un acceso continuado y enmascarar su actividad. Flame, un reciente malware armado, intentaba específicamente crear una cuenta de este tipo cuando descubría que se ejecutaba bajo la autoridad de un administrador de dominio.

Deténgalos cuando se cree la cuenta

Por lo tanto, la localización de cuentas nuevas es esencial, pero también requiere mucho tiempo y a menudo no es concluyente. El mejor momento para localizar una cuenta con incumplimientos es cuando se crea:

- Identifique quién creó la cuenta
- ¿Sigue trabajando en su empresa?
- ¿Por qué se creó la cuenta?

Cómo monitorear y revisar las cuentas nuevas

Existen dos maneras de revisar y responder a las cuentas nuevas:

- Monitoree los registros de seguridad del controlador de dominio de AD en busca del ID de evento 4720 (debe habilitar la subcategoría de auditoría de administración de cuentas de usuario).
- Ejecute el script Output-ADUsersAsCSV y ordene la columna When Created.

Al revisar cada cuenta, haga lo posible por responder a las siguientes preguntas:

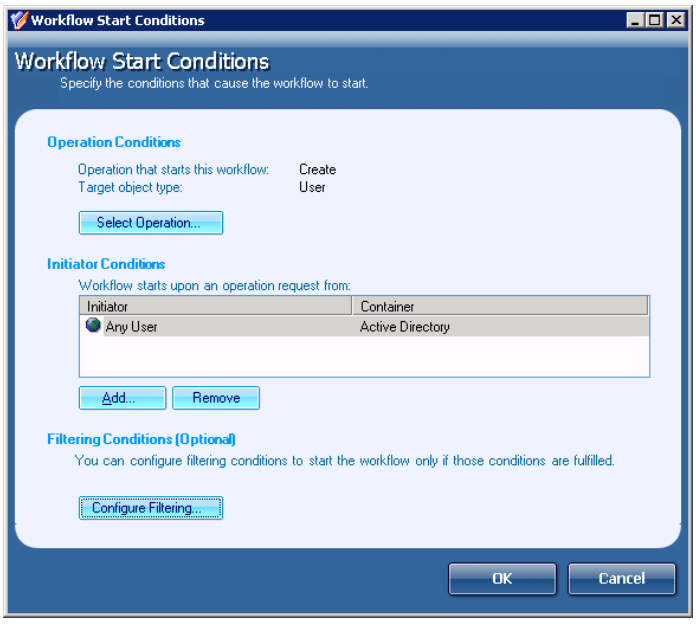
- ¿Existe un ticket de trabajo u otra documentación que corrobore esta cuenta?
- ¿Coincide la cuenta con las convenciones de nomenclatura establecidas?
- ¿Cumple la cuenta con las demás normas y políticas de creación de cuentas de su empresa?

```
Evento ID 4720: Se ha creado una cuenta de usuario

Asunto:

     ID de seguridad: ACME-FR\administrador

     Nombre de la cuenta: administrador

     Dominio de la cuenta: ACME-FR

        ID de inicio de sesión:

0x20f9d Cuenta nueva:

     ID de seguridad: ACME-FR\John.Locke

     Nombre de la cuenta: John.Locke

     Dominio de la cuenta: ACME-FR

Atributos:

     Nombre de la cuenta SAM: John.Locke

     Mostrar nombre: John Locke

     Nombre principal del usuario: John.Locke@acme-
     fr.local
```

Si la cuenta resulta no estar autorizada o no cumplir con los requisitos, deberá hacer un seguimiento con quien la creó. La ventaja de utilizar el primer método es que el evento de registro de seguridad 4720 le indica quién creó la cuenta.

Cómo ayuda Active Roles

Active Roles actúa como un servidor de seguridad virtual alrededor de Active Directory y garantiza que se aplique el acceso basado en el modelo de privilegios mínimos. La posibilidad de utilizar flujos de trabajo para cualquier operación, como la creación, modificación o eliminación de cualquier cuenta en el dominio, significa que todos los procesos que normalmente se realizan de forma manual pueden ser automatizados. Esto significa que esas acciones tan importantes realmente se llevan a cabo, de forma inmediata, íntegra y con una auditoría completa.



Paso 4. Automatizar el mantenimiento de la cuenta

Pasos para crear una cuenta nueva

Para asegurarse de que las nuevas cuentas se creen de acuerdo con sus normas, automatice todo lo posible el proceso de creación de cuentas a fin de reducir las posibilidades de error humano. La creación de la cuenta incluye los siguientes pasos:

1. Crear la cuenta en AD
2. Establecer atributos de identidad (puesto laboral, números de teléfono, entre otros)
3. Crear el buzón de correo de la cuenta en Microsoft Exchange/ O365
4. Agregar la cuenta a los grupos que son apropiados para el rol del usuario
5. Registrar la cuenta de AD en otras aplicaciones, según sea necesario

Automatizar con PowerShell Scripts

Muchos de estos pasos pueden automatizarse con scripts de PowerShell. El siguiente script realiza los pasos 1 a 4. El siguiente script realiza los pasos 1 a 4.

```
Nuevo-ADUser: Nombre "randyjones"

-SamAccountName randyjones: AccountExpirationDate
01/01/2014

-Nombre "Randy" -Apellido

"Jones"

-DisplayName 'RandyJones' -Path
'CN=Users,DC=acme,DC=local' - EmployeeID '93299'
-OfficePhone

"27884". Cargo "CEO"

Enable-Mailbox -Identity acme\ randyjones -Database
Database01

Add-ADGroupMember Group1 acme\randyjones

Add-ADGroupMember Group2 acme\randyjones
```

Puede hacer una versión personalizada de este script para los roles de su empresa que tienen una elevada rotación. También puede mejorar esta secuencia de comandos para que acepte entradas y construya la cuenta de acuerdo con las elecciones realizadas en el momento de la ejecución.

Cómo ayuda Active Roles

Active Roles ofrece numerosas interfaces, como PowerShell, ADSI scripting, SPML, SCIM, MMC y Web. Lo importante es que puede aplicar normas (denominadas políticas) a cualquier operación CRUD de objetos de AD, independientemente de la interfaz. Esta instancia de administración le permite asegurar que las normas pueden controlar por completo toda la actividad dentro de su entorno de AD. El incumplimiento de sus normas puede dar lugar a una infracción permitida (notificable) o provocar una respuesta de error; la elección es suya.

Paso 5. Manejar los usuarios salientes y los cambios de rol

Para las empresas que utilizan herramientas tradicionales de administración de AD, las cuentas de usuario fantasma o huérfanas son una fuente continua de riesgo. Sin la automatización o una única fuente de verdad de las identidades y los permisos, es probable que en sus datos de identidad haya personas que la empresa ya no tenga empleadas o contratadas. Es crucial para quien sea responsable de actualizar el estatus (ya sea de RR. HH. o de TI) que se le notifique cuando alguien deja la empresa o cambia de función.

La búsqueda de cuentas inactivas no resuelve este problema

Si bien esto puede parecer sencillo, las empresas no suelen desactivar las cuentas de los usuarios o no cambian los derechos cuando se modifica el estado de un usuario. Una respuesta frecuente a las preguntas de auditoría sobre cómo una empresa se encarga de desactivar a los usuarios que se han ido: por lo general, buscan las cuentas inactivas, mediante la búsqueda de cuentas que no se han conectado recientemente. Este enfoque es erróneo, ya que si una persona dada de baja sigue accediendo a la red, su cuenta no aparecerá como inactiva y no se incluirá en el informe de cuentas inactivas.

Buscar cuentas inactivas es tratar los síntomas en lugar de la causa. Con un enfoque que considere todo el ciclo de vida de una cuenta de AD, desde la contratación hasta la salida y todos los pasos intermedios, se puede eliminar este problema.

Lo mismo podría aplicarse a los datos redundantes. Esto es tan importante como la creación precisa de nuevas entradas. Si no depura los datos redundantes y no deseados, su AD se llenará de datos desordenados.

Formas eficaces de abordar la salida de usuarios y los cambios de funciones

A continuación se exponen tres formas de abordar eficazmente los cambios de estado, en orden descendente de preferencia:

- La mayoría de las empresas tienen un proceso claramente definido y ejecutado de forma estricta para eliminar el acceso físico de un usuario al edificio, haga que la desactivación de la cuenta de AD sea parte de este proceso.
- Si su aplicación de RR. HH. incluye un flujo de trabajo, automatícelo para que envíe un correo electrónico a los administradores cuando un usuario sea despedido, cambie de función o dependa de un supervisor diferente.
- La mayoría de las aplicaciones de RR. HH. le permiten programar la entrega automática de informes, programar un informe diario de bajas y cambios de trabajo que se entrega a los administradores de cuentas.

La conclusión es que la desactivación de cuentas y la actualización del estado de los permisos son necesarias para cumplir con los requisitos de la industria y del gobierno. Sea cual fuere su proceso, la administración debe comprender su importancia y la responsabilidad debe estar claramente definida.

Cómo ayuda Active Roles

Las capacidades de flujo de trabajo de Active Roles incluyen tareas y procesos completos activados por cambios en el directorio. Esto incluye políticas de cierre de cuentas que permiten a su empresa designar con exactitud lo que ocurre con una cuenta de usuario cuando una persona ha sido dada de baja.

Las opciones pueden incluir la desactivación de la cuenta, el cambio de ubicación de la OU, la codificación de la contraseña y la alteración del nombre de inicio de sesión, el cambio de nombre con variables de operación, la asignación de delegados para el correo y las carpetas de inicio, entre otras.

Y lo que es más importante, Active Roles puede eliminar al usuario de todos los grupos de seguridad, volver a autorizar el directorio principal del usuario, liberar las licencias de O365 asignadas y mucho más. Es importante señalar que estas políticas pueden activarse de forma manual, programada o automática.

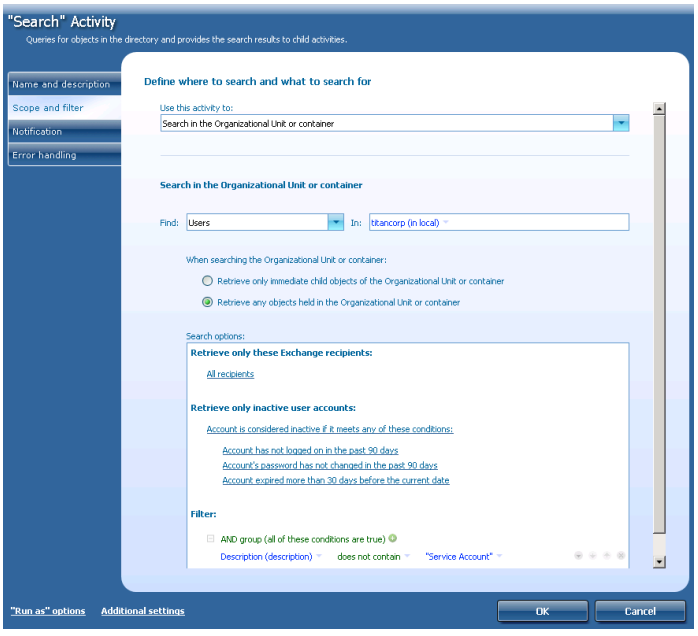
Paso 6. Abordar las cuentas inactivas

El siguiente paso es comprobar de forma periódica si hay cuentas inactivas (es decir, cuentas de usuario que no se han conectado recientemente). De nuevo, tenga en cuenta que este paso no sustituye al paso 5.

Encontrar cuentas inactivas es fácil

Antes de Windows 2003, era difícil encontrar cuentas inactivas. Gracias al atributo lastLogonTimestamp, es relativamente fácil. Esta replicación (cada siete días) le permite consultar los controladores de dominio y ver las últimas horas de inicio de sesión, lo que ayuda a identificar a los usuarios inactivos.

LastLogonTimestamp se expone mediante Get-ADUser con la propiedad LastLogonDate, como se muestra en el script OutputADUsersAsCSV del paso 1. Con ese script, solo debe ordenar la columna Last Logon en orden descendente para identificar con facilidad las cuentas que no se han conectado recientemente.



También debe comprobar si hay cuentas de usuario que nunca se han conectado. En las hojas de cálculo producidas a partir de Output-ADUsersAsCSV, estas cuentas se indican mediante filas en las que la columna Last Logon está en blanco.

Cómo ayuda Active Roles

Active Roles automatiza los procesos que identifican y administran las cuentas inactivas, incluidas la clasificación, la detección y la corrección. Esto facilita el proceso de limpieza de la cuenta. Cuando se utiliza junto con las políticas adecuadas en torno a la administración del ciclo de vida de las cuentas (como la reducción de provisión), no solo se pueden resolver los problemas heredados, sino que se pueden evitar los problemas futuros.

Paso 7. Administrar las cuentas no humanas

No todas las cuentas corresponden directamente a una persona. Por ejemplo, muchas aplicaciones requieren una o más cuentas para que los servicios se conecten. Estas cuentas suelen tener acceso privilegiado a los servidores y a los datos, por lo que deben estar protegidas.

Por qué están en riesgo las cuentas con altos privilegios

No obstante, la aplicación y otras cuentas no humanas son difíciles de localizar. En las auditorías de TI, no es raro descubrir cuentas con privilegios que están en riesgo por las siguientes razones:

- Nadie sabe con certeza el propósito de una cuenta o por qué existe
- A pesar de la salida de muchos administradores, la contraseña de una cuenta no se ha actualizado, por temor a dañar una aplicación en algún lugar de la red
- La cuenta tiene autoridad para conectarse de forma interactiva.
    - Debe prohibirse que las cuentas no humanas se conecten de forma interactiva (en la consola o mediante el escritorio remoto) para evitar que los administradores (que conocen la contraseña de la cuenta) se conecten de forma anónima como esa cuenta y sin responsabilidad individual

Identifique las cuentas no humanas

El primer paso en la administración de las cuentas no humanas es identificar todas las cuentas de este tipo. Puede hacerlo utilizando un prefijo en la convención de nomenclatura del nombre de inicio de sesión, colocando las cuentas en una unidad organizativa (OU) específica de cuentas no humanas o etiquetándolas como tales mediante algún otro atributo en AD.

Documente la finalidad y el titular de cada cuenta

A continuación, la finalidad de la cuenta y los sistemas en los que se utiliza deben documentarse en los campos Description o Notes de la cuenta.

Active Roles automatiza los procesos que identifican y administran las cuentas inactivas, incluidas la clasificación, la detección y la corrección.

Designe un titular para cada cuenta no humana y documéntelo en AD. El titular puede ser una cuenta de usuario humano individual, pero normalmente es mejor seleccionar un grupo que corresponda al equipo responsable de la aplicación u otra tecnología que utiliza la cuenta. El titular también puede documentarse en el campo Description o Notes.

El uso de las cuentas de servicio administradas (MSA) se presentó en Windows Server 2008 R2 (y posteriormente las cuentas de servicio administradas en grupo) para administrar (cambiar) de forma automática las contraseñas de las cuentas de servicio. Utilizando MSA/gMSA, puede reducir considerablemente el riesgo de que las cuentas del sistema se vean comprometidas.

Mantenimiento de contraseñas

Uno de los mayores desafíos de las cuentas no humanas es el mantenimiento de las contraseñas. La contraseña de una cuenta no humana debe cambiarse siempre que un administrador (que conoce la contraseña) abandone la empresa. A menos que las cuentas se documenten correctamente, es difícil determinar a qué cuentas no humanas tenía acceso un administrador. Sin embargo, cambiar la contraseña de una cuenta conlleva un riesgo, ya que cualquier servicio o tarea programada que se ejecute como esa cuenta, o las aplicaciones que almacenan la contraseña de esa cuenta, deben actualizarse o se dañarán la próxima vez que se inicien o intenten iniciar sesión.

Determine en qué sistemas se utiliza una cuenta

Si está intentando limpiar un conjunto existente de cuentas no humanas, puede determinar los sistemas en los que se está utilizando una cuenta consultando el registro de seguridad de Windows. Suponiendo que haya habilitado la subcategoría de auditoría Operaciones de tickets de servicio de Kerberos en su objeto de política de grupo (GPO) de la política del controlador de dominio predeterminado, sus controladores de dominio registrarán el ID de evento 4769. Si busca en los registros de seguridad del controlador de dominio todas las apariciones de 4769 donde Account Name es la cuenta de servicio en cuestión, puede obtener una lista de todos los equipos en los que se está utilizando esa cuenta. Mire el campo Service Name en esos eventos. El campo Service Name en el ID de evento 4769 identifica el equipo para el cual la cuenta de usuario está solicitando la autenticación.

Limite los permisos de inicio de sesión de las cuentas no humanas

Un último paso para asegurar las cuentas no humanas es limitar los permisos de inicio de sesión en los equipos de todo el dominio. Esto ayuda a evitar que alguien abuse de las cuentas no humanas iniciando sesión con la cuenta de forma interactiva en la consola de un equipo o mediante el Escritorio Remoto. Este paso sirve como medida de defensa exhaustiva en caso de que los cambios de contraseña se pierdan cuando un administrador se vaya. Cinco tipos de inicio de sesión en Windows cuentan con ambos y pueden permitir y denegar permisos:

Para conectarse de una manera determinada, debe tener el permiso de inicio de sesión correspondiente. Incluso en ese caso, si también se le ha asignado el permiso de negación de acceso, no se le permitirá iniciar la sesión, ya que el permiso de negación de acceso anula el derecho de permiso. Puede encontrar estos permisos en un GPO en Configuración del equipo\Configuración de Windows

Configuración de seguridad\Políticas locales\Asignación de permisos de usuario.

Por lo general, las cuentas no humanas deberían tener solo el permiso de "Iniciar sesión como servicio". Es aconsejable denegar de forma explícita los permisos de inicio de sesión de Escritorio Interactivo y Remoto para evitar que la cuenta se utilice de forma indebida. Si agrega todas las cuentas no humanas a un grupo específico para ese fin, puede asignar a ese grupo los permisos "Denegar el inicio de sesión localmente" y "Denegar el inicio de sesión mediante servicios de Escritorio Remoto" en un GPO, como la Política de dominio predeterminada, que se aplica a todos los equipos del dominio.

Tenga cuidado al negar el permiso de acceso a la red. La aplicación que utiliza la cuenta puede necesitar acceder a recursos en otras redes.

Cómo ayuda Active Roles

Active Roles puede exigir y validar (mediante informes de comparación) que todas las cuentas no humanas estén configuradas con la convención de nomenclatura, la configuración de atributos, la ubicación de los objetos y la pertenencia a grupos (vinculada a GPO) que cumplen con los estándares de su empresa. Además, se pueden habilitar flujos de trabajo if-then (si-cuando) para forzar la aprobación (por niveles) de todas las cuentas (de servicio) creadas en una determinada ubicación de la OU o para aquellas cuentas con un prefijo de nombre concreto, entre otros, con todas estas acciones totalmente auditadas y vinculadas a la persona responsable y real.

Paso 8. Controlar las excepciones

Documente las excepciones legítimas y aprobadas

El viejo refrán dice que "las reglas están hechas para romperse". Definitivamente hay excepciones legítimas a las normas para las cuentas de usuario. Por ejemplo, puede tener una aplicación que requiere una cuenta de usuario con un nombre específico que incumple su convención de nomenclatura normal. Para situaciones como esta, se necesita una forma de documentar las excepciones legítimas y aprobadas. El mejor modo de hacerlo es con una OU llamada Excepciones o marcando las cuentas de excepción en los campos Description o Notes.

Pero no basta con etiquetar una cuenta como excepción, sino que se debe documentar la finalidad y el propietario de la cuenta, como se describe en el paso 7.

Tipo de inicio de sesión	Permisos de inicio de sesión
Interactivo	Permitir el inicio de sesión localmente Denegar el inicio de sesión localmente
Escritorio remoto	Permitir el inicio de sesión mediante los Servicios de Escritorio Remoto Denegar el inicio de sesión mediante los Servicios de Escritorio Remoto
Servicio	Iniciar sesión como servicio Denegar el inicio de sesión como servicio
Tarea programada	Iniciar sesión como servicio Denegar el inicio de sesión como servicio
Red (por ejemplo, acceso a carpetas compartidas)	Iniciar sesión como trabajo por lotes Denegar el inicio de sesión como trabajo por lotes
Cifrado de transporte RDP FIPS 140-2	Acceder a este equipo desde la red Denegar el inicio de sesión a través de los Servicios de Escritorio Remoto

El viejo refrán dice que "las reglas están hechas para romperse". Definitivamente hay excepciones legítimas a las normas para las cuentas de usuario.

No permita que las excepciones se conviertan en algo común

Una advertencia: Las implementaciones de AD en las que un gran porcentaje de cuentas eran excepciones. El personal se había acostumbrado a marcar una cuenta como excepción cada vez que resultaba inconveniente seguir las normas y procedimientos de mantenimiento de cuentas. No se debe abusar de la previsión de excepciones.

Cómo ayuda Active Roles

Puede acomodar y controlar las excepciones mediante políticas que garanticen que las cuentas de excepción solo se permitan en determinadas ubicaciones. Cuando se crea una excepción en la ubicación de la excepción, Active Roles se asegura de que se cumplan y apliquen todas las normas de configuración, atributos u otras restricciones de política necesarias.

Además, se pueden emplear flujos de trabajo de aprobación en los que el escalamiento se produce cuando se realiza una solicitud de creación (manual o programada) de un nuevo intento de excepción, para evitar que las excepciones se conviertan en la norma.

Paso 9. Controlar la autoridad de administración

Limite quién puede crear cuentas

Una de las razones por las que AD suele estar plagado de cuentas innecesarias o misteriosas es porque demasiadas personas tienen autoridad para crear cuentas de usuario.

Para aplicar los controles de creación de cuentas nuevas, cruciales para la seguridad y el cumplimiento de la normativa, la cantidad de personas que pueden crear cuentas debe limitarse a unas pocas personas capacitadas.

Utilice el Asistente de Delegación de Control

AD da soporte a los privilegios mínimos permitiendo a los administradores de dominio delegar permisos seleccionados sobre OU específicas. Cuando se aplica correctamente, la capacidad de delegación de control de AD permite que las personas hagan su trabajo sin darles más autoridad de la necesaria. Por ejemplo,

> *Active Roles incluye más de 300 plantillas de acceso comúnmente utilizadas y probadas, lo que hace de Active Roles una de las herramientas más rápidas de poner en marcha.*

en vez de hacer que el servicio de asistencia sea miembro de los administradores de dominio, podría conceder a dicho servicio el permiso de restablecer la contraseña en la OU que contiene las cuentas de los usuarios finales.

Para iniciar el Asistente de Delegación de Control, solo haga clic con el botón derecho en la OU que desee y seleccione "Delegar control". La siguiente imagen muestra la autoridad de restablecimiento de contraseñas delegada en el grupo de servicio de asistencia.

Cómo ayuda Active Roles

Los "roles" en Active Roles se conocen como Plantillas de acceso. Representan conjuntos de permisos con un alto grado de granularidad, que se pueden aplicar a cualquier ubicación de su infraestructura de Active Directory. Incluso es posible aplicarlos a ubicaciones virtuales que se pueden personalizar y mantener de forma dinámica dentro de la herramienta.

Las plantillas de acceso son un conjunto de permisos de AD, clasificados por objeto de destino, que le permiten delegar fácilmente los permisos de administración basándose en un modelo de privilegios mínimos. Estos conjuntos de permisos pueden ser tan simples como "restablecer la contraseña" o tan detallados como los permisos de lectura/escritura/lista de cualquier/todos los atributos de los objetos de AD. Active Roles incluye más de 300 plantillas de acceso comúnmente utilizadas y probadas, lo que hace que Active Roles sea una de las herramientas más rápidas de poner en marcha, y de obtener un retorno de la inversión (ROI). Y crear nuevas plantillas es sencillo y rápido.

Paso 10. Aprovechar la tecnología del flujo de trabajo

SharePoint es mejor que el correo electrónico para la administración de cuentas

Muchas empresas intentan administrar las solicitudes de cuentas nuevas, las bajas laborales, los cambios de trabajo y las distintas aprobaciones utilizando únicamente el correo electrónico. Este enfoque dificulta el seguimiento de las normas de administración de cuentas o la demostración de su cumplimiento. La tecnología de flujos de trabajo, como las listas en SharePoint, nunca será una opción de automatización completa para la administración de cuentas, pero sin dudas una mejora respecto al correo electrónico por sí solo. SharePoint, como ejemplo de tecnología de flujo de trabajo, le permite dar a las listas de anuncios una dirección de correo electrónico que convierte los correos electrónicos entrantes en nuevos elementos de la lista y traslada cualquier documento

adjunto a los archivos adjuntos de los elementos de la lista. Puede personalizar la lista con campos Status para seguir los pasos de procesamiento del elemento de la lista.

Ejemplo: Utilización de SharePoint para administrar los cambios de cuenta relacionados con las bajas

Por ejemplo, puede utilizar una lista de SharePoint habilitada para el correo electrónico para organizar las notificaciones de desvinculación laboral y para documentar que se cumpla el procedimiento de salida de usuarios. Si utiliza la opción 2 o 3 del paso 5, configure la aplicación de RR. HH. para que envíe sus correos electrónicos a su lista de SharePoint y agregue las columnas Status y Notes a la lista. A medida que se envían a la lista nuevas notificaciones de desvinculación laboral o informes, puede desactivar las cuentas asociadas en AD y editar el elemento de la lista para documentar que se ha procesado y qué cuentas se han desactivado como respuesta. Incluso puede suscribirse a las alertas de la lista para saber apenas se cree un artículo. Se pueden crear listas similares para las solicitudes de cuentas nuevas y las notificaciones de cambios laborales. La cuestión es que debe aprovechar la tecnología de los flujos de trabajo para reducir la carga burocrática que recae en los administradores y, al mismo tiempo, mejorar el cumplimiento.

Cómo ayuda Active Roles

La arquitectura de Active Roles permite aplicar las capacidades de información y auditoría a todas las operaciones CRUD. Esto significa que los informes están disponibles para todas las creaciones o modificaciones de cuentas nuevas, todas las creaciones de grupos, las modificaciones y la eliminación de cuentas. En efecto, todo lo que ocurre a través de Active Roles se audita.

Los informes incluyen las cinco preguntas (quién, qué, cuándo, dónde y por qué) y pueden enviarse a los auditores automáticamente. Además, se puede acceder a los informes en línea a través de un portal web.

Un subproducto útil del alto nivel de auditoría es la capacidad de deshacer acciones de forma segura. Una acción errónea de eliminación, por ejemplo, puede revertirse con un par de clics y sin perder la continuidad de la actividad empresarial.

Mantenga un AD limpio y seguro, de forma automática

Ampliar y automatizar las capacidades de las herramientas nativas para reducir el riesgo

Las 10 recomendaciones de este documento le ayudarán a limpiar las cuentas de usuario de su AD, así como a evitar que se repitan los problemas. Sin embargo, si se limita a seguir las recomendaciones sin invertir en herramientas adicionales, se conservará gran parte de la carga de confirmación administrativa y manual del personal de TI, junto con la dependencia de los usuarios finales, los administradores y el personal de RR. HH. para la notificación y la información sobre los eventos importantes del ciclo de vida del usuario.

En el área de TI, la mayoría de las empresas dedican demasiado tiempo a crear y eliminar cuentas de usuario en AD. Las herramientas nativas son ineficientes y consumen mucho tiempo. Los procesos manuales que requieren presentan la posibilidad de errores humanos que pueden comprometer la seguridad y la estabilidad de su entorno de Windows. Además, muchas empresas tienen procesos igualmente ineficientes pero separados del todo para crear cuentas en sus sistemas que no son Windows, lo que aumenta la carga administrativa a la vez que presenta aún más riesgos de seguridad.

Active Roles automatiza el mantenimiento de las cuentas de usuario, reduce el trabajo y mejora la seguridad

Como ha visto en la sección "Cómo ayuda Active Roles" en cada paso, Active Roles automatiza la mayor parte del mantenimiento de AD y proporciona una gran cantidad de funciones para eliminar la dependencia de los usuarios finales, los administradores y el personal de RR. HH. Active Roles le ayuda a realizar cada uno de los pasos de este documento.

Active Roles permite que AD se sincronice con bases de datos y directorios externos, incluyendo SharePoint Server, aplicaciones de línea de negocio y muchas más. Todos los sistemas de casi cualquier sistema operativo moderno pueden gozar ahora de una sincronización de identidades en dos direcciones, ya sea local o en la nube. Lo mejor de todo es que, integrándose con su aplicación de RR. HH., la creación de cuentas de identidad puede utilizarse para impulsar la administración automatizada de los accesos.

Active Roles automatiza la creación y administración de cuentas basadas en AD. Los usuarios se asignan a funciones de trabajo que se corresponden con sus responsabilidades, lo que garantiza que tienen exactamente los permisos adecuados para los recursos adecuados, nada más y nada menos. Los usuarios están más satisfechos porque pueden acceder a los recursos que necesitan para hacer su trabajo, y los administradores están más complacidos porque todo está automatizado, lo que reduce al mínimo el tiempo dedicado a ejecutar tareas tediosas de presionar botones.

Active Roles proporciona una administración de cuentas de usuario y de grupo inmediata, una seguridad basada en roles estrictamente aplicada, una administración de identidades diaria y una auditoría e informes integrados para entornos centrados en Windows.

Active Roles incluye estas características:

- **Acceso seguro**: Active Roles actúa como un servidor de seguridad virtual alrededor de Active Directory, lo que le permite controlar el acceso mediante la delegación con un modelo menos privilegiado. Según las políticas administrativas definidas y los permisos asociados, genera y hace cumplir estrictamente las reglas de acceso, lo que elimina los errores y las inconsistencias comunes con perspectivas nativas a la administración de AD. Además, los procedimientos de aprobación sólidos y personalizados establecen un proceso del área de TI y supervisión coherente con los requisitos de la empresa, con cadenas de responsabilidad que complementan la administración automatizada de datos del directorio.
- **Creación automática de cuentas** Automatiza una gran variedad de tareas, entre ellas las siguientes:
- Crear cuentas de grupo y usuarios en AD/AAD.
- Crear buzones de correo en Exchange/Exchange Online
- Completar grupos
- Asignar recursos en Windows

Active Roles también automatiza el proceso de reasignación y eliminación de permisos de acceso del usuario en los sistemas AD/AAD y los sistemas unidos a AD (que incluyen las terminaciones de usuarios y grupos) para asegurar un proceso administrativo seguro y eficiente de los tiempos de vida de grupo y usuario. Cuando se deben modificar o eliminar las necesidades de acceso de un usuario, las actualizaciones se realizan automáticamente en AD, Exchange, SharePoint, OCS, Lync y Windows, así como también en cualquier sistema unido a AD como UNIX, Linux y Mac OS X.

- **Administración diaria del directorio:** le permite gestionar con facilidad todo lo que se indica a continuación:
- Destinatarios de Exchange y Exchange Online, incluidos la administración de listas de distribución y permisos, eliminación, movimiento, creación y asignación de OCS o buzones de correo
- Grupos
- Equipos, incluidos los recursos compartidos, impresoras, usuarios y grupos locales
- Active Directory, incluido AD LDS
- También incluye interfaces intuitivas para mejorar la administración diaria y las operaciones del servicio de asistencia mediante un complemento MMC y una interfaz web
- **Administrar grupos y usuarios en un entorno alojado:** Active Roles funciona en un entorno alojado en el que las cuentas del dominio AD del cliente se sincronizan con un dominio AD alojado. Permite la administración de cuentas de usuarios y de grupo desde el dominio del cliente al dominio alojado, a la vez que sincroniza los atributos y las contraseñas. Utilice conectores listos para usar con el fin de sincronizar sus cuentas AD locales con otras plataformas y aplicaciones. Aproveche una variedad en rápido crecimiento de más de 30 conectores (https://www.cloud.oneidentity.com/products/connect/connectors) a múltiples servicios y aplicaciones basados en la nube, como Salesforce, G-Suite y ServiceNow mediante One Identity Starling Connect.
- **Consolide los puntos de administración mediante la integración:** Active Roles complementa la tecnología existente y la estrategia de IAM. Amplía todas las funciones, simplifica y consolida los puntos de administración asegurando una integración sencilla en muchos productos de One Identity, que incluyen Identity Manager, Privilege Password Manager, Desktop Virtualization, Authentication Services, Defender, Password Manager y Quest Change Auditor. Active Roles también automatiza y extiende las capacidades de PowerShell, ADSI, SPML y las interfaces web personalizables.

10 pasos para lograr el rendimiento, la agilidad y la seguridad

Paso 1. Realizar un análisis periódico de la cuenta

Paso 2. Vincular las cuentas a los registros de los empleados

Paso 3. Controlar las cuentas nuevas

Paso 4. Automatizar el mantenimiento de la cuenta

Paso 5. Manejar los usuarios salientes y los cambios de rol

Paso 6. Abordar las cuentas inactivas

Paso 7. Administrar las cuentas no humanas

Paso 8. Controlar las excepciones

Paso 9. Controlar la autoridad de administración

Paso 10. Aprovechar la tecnología del flujo de trabajo

Estos 10 pasos pueden limpiar los datos de AD/Azure AD, que son fundamentales para el rendimiento y la seguridad. One Identity Active Roles ayuda a ejecutar estos pasos y mantendrá sus datos limpios en el futuro. Por lo tanto, tome ese auto en exhibición, aliméntelo con datos limpios y disfrute del rendimiento, la velocidad y el manejo que Active Roles puede instalar en su estrategia AD/AAD.

Microsoft Active Directory y One Identity Active Roles: son mejores juntos

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 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

Whitepaper_2021_MicrosoftBetterTogetherwithOIDActiveRoles_PG_es_LX-WL-67415