Universidad del Quindío
Área de Soporte Técnico

Delegación de autoridad en Directorio Activo

Basado en artículo: Delegación de autoridad en Active Directory por Joel Yoker and Rob Campbell. Technet Magazine. © 2011 Microsoft. Reservados todos los derechos.

Las capacidades de delegación en Directorio Activo son bastante eficaces; responden a una serie de problemas de seguridad y simplifican las tareas de administración. Mediante una delegación correcta de derechos en Directorio Activo®[1], puede aplicar funciones especificadas en el entorno, limitar la repercusión y la probabilidad de errores administrativos, y aplicar el principio de privilegio mínimo en la infraestructura. Todavía hay muchas organizaciones que dependen de Directorio Activo y aún no han aprovechado la eficacia de la delegación. En parte, esto se debe a que, a simple vista, el desarrollo de un modelo de delegación de Directorio Activo para la empresa parece ser bastante complejo. Mientras que el principal obstáculo es desarrollar un modelo de la delegación que satisfaga las necesidades exclusivas de la organización, lo cierto es que hay modelos muy sencillos que se pueden aplicar a la mayoría de infraestructuras de TI con pequeñas modificaciones.

Aunque cada entorno es diferente en algo, la realidad es que la mayoría de las empresas grandes son semejantes en muchos sentidos y encaran los mismos desafíos de TI. Por ejemplo, muchas organizaciones están divididas en regiones geográficas, han evolucionado a partir de una ingeniería de TI o unos equipos de soporte técnico de funcionamiento distintos, y tienen unidades de negocio independientes. Y muchas organizaciones grandes deben tratar estos asuntos en términos de aumento de privilegios, abuso de cuentas de servicios y "confianza".

La confianza es un término interesante y a menudo se convierte en la justificación para tener varios bosques de Directorio Activo. Los problemas de confianza provienen con frecuencia de la capacidad de una división o región para influir en la disponibilidad del sistema de otra división o región. Es habitual en los niveles de habilidades que se diferencie entre los límites de la organización y que haya una falta de conocimiento exhaustivo de sistemas específicos necesarios para ofrecer soporte a una región o unidad de negocio concretas. Así, las divisiones suelen no querer renunciar a sus derechos administrativos en favor de un grupo central.

Mientras tanto, para cualquier implementación de Directorio Activo, los administradores deben definir las reglas de compromiso de las aplicaciones que usan la infraestructura de Directorio Activo. Desgraciadamente, un enfoque común (que a menudo se cita en las guías de instalación) es hacer que una cuenta de servicio sea un miembro del grupo ***Admins. de dominio***. El problema de este enfoque es que las cuentas de servicio son cuentas genéricas fundamentalmente. Al conceder a estas cuentas los derechos de un administrador de dominio, se introduce una amenaza considerable para el entorno de TI. Las cuentas de servicio pueden caer fácilmente en manos de administradores malintencionados o descuidados, o bien ser usadas por atacantes que aprovechen problemas de seguridad subyacentes de una aplicación.

Aunque estos obstáculos parecen ser insuperables, representan el escenario principal para implementar un modelo de delegación de Directorio Activo. El desarrollo de un modelo de la delegación es un proceso de diseño iterativo y se recomienda que se

realicen estos pasos:

[1]

1. Defina las funciones administrativas de TI de la organización.
2. Desarrolle un modelo de unidad organizativa y grupo de seguridad.
3. Establezca cuentas secundarias para administradores de TI.
4. Delegue derechos.

Observemos con mayor detenimiento estos pasos.

1. Definición de funciones

El proceso de definición de funciones comienza con una descripción completa de la administración de servicios y la administración de datos. Estos conceptos son la piedra angular de cualquier modelo de delegación de Directorio Activo.

En esencia, la administración de servicios es la administración de los componentes de infraestructura de servicio de directorios fundamentales, tales como los servidores Exchange y los controladores de dominio. La administración de datos es la administración de objetos, tales como buzones de correo y cuentas de usuario que residen en los servicios. Dentro del ámbito de Directorio Activo, los administradores de servicios son responsables en última instancia de la entrega y la disponibilidad de los servicios de directorio, mientras que los administradores de datos administran cuentas de usuario y servidor, grupos y otros recursos del dominio.

Directorio Activo es compatible con la delegación granular de autoridad a través de unidades organizativas (OU). Las unidades organizativas pueden adaptarse con frecuencia para ofrecer el mismo nivel de autoridad que está disponible para los administradores dentro del servicio de directorio o los modelos de dominio existentes. Pero es importante entender que algunas funciones simplemente no pueden delegarse y deben administrarse mediante un grupo o entidad únicos y de confianza.

El análisis de tareas también es fundamental. Necesita saber qué tareas de Directorio Activo llevan a cabo los administradores y cómo se asignan esas tareas a funciones. Por ejemplo, la creación de sitios de Directorio Activo es una tarea de administración de servicios, mientras que la modificación de la pertenencia a grupos de seguridad generalmente está dentro de la administración de datos. Se debe evaluar la frecuencia, la importancia y la dificultad de cada tarea. Éstos son aspectos esenciales de la definición de tareas, porque determinan si se debe delegar un derecho. Las tareas que se realizan de forma rutinaria, tienen un riesgo limitado y cuya finalización no es importante, son candidatas excelentes para la delegación. Por otro lado, las tareas que no se realizan casi nunca, tienen una gran repercusión en la organización y requieren niveles altos de habilidad, son malas candidatas para la delegación. En su lugar, la extensión (elevación temporal de una cuenta a la función necesaria o reasignación de la tarea) es la ruta adecuada para estas tareas.

Puesto que muchas de las características de organizaciones grandes son semejantes, se puede asumir con seguridad la implementación de un modelo de delegación común. Tenga en cuenta que este modelo es apenas un ejemplo; se trata de un punto de partida ideal para hablar de las funciones en la organización.

Algunas funciones ya las define Directorio Activo y otras se deben crear desde cero para completar el modelo de delegación. Un conjunto de muestra de funciones que se ajustaría a muchos entornos grandes de Directorio Activo quizás incluya Administradores de organización, Admins. de dominio y Tier4 Admins (Admins. de nivel4) para la administración de servicios, y Tier3 Admins (Admins. de nivel3), Regional Admins (Admins. regionales), Tier2 Admins (Admins. de nivel2) y Tier1 Admins (Admins. de nivel1) para la administración de datos.

Administradores de servicios	Descripción
Administradores de organización	Responsable de la administración de servicios de nivel superior en la empresa. No debe contener ningún miembro permanente.
Administradores del dominio	Responsable de la administración de servicios de nivel superior en el dominio. Debe contener sólo un número pequeño y controlable de administradores de confianza.
Tier4 Admins (Admins. de nivel4)	Responsable de la administración de servicios en el dominio. Concede sólo los derechos necesarios para administrar los servicios correspondientes. Sirve también como un punto de extensión para administradores de datos.
Administradores de datos	Descripción
Tier1 Admins (Admins. de nivel1)	Responsable de la administración general de objetos de directorio, realiza tareas tales como el restablecimiento de contraseñas, la modificación de propiedades de cuenta de usuario, etc.
Tier3 Admins (Admins. de nivel3)	Responsable de la creación y/o eliminación selectivas de cuentas de usuario y equipo en la configuración regional o la organización.
Regional Admins (Admins. regionales)	Responsable de la administración de la estructura de unidades organizativas local. Concede permisos para crear la mayoría de los objetos de una unidad organizativa.
Tier3 Admins (Admins. de nivel3)	Responsable de la administración de todos los administradores de datos. Sirve como departamento de soporte técnico y punto de extensión de nivel superior para todos los administradores regionales.

2. Administradores de servicios

Observemos con mayor detenimiento las funciones del administrador de servicio. Los administradores de servicios administran componentes de infraestructura esenciales y todos los que se incluyen esta categoría tienen muchos privilegios. Por lo tanto, una estrategia de privilegio mínimo, que significa que sólo se concede el conjunto mínimo de permisos necesario para realizar las tareas correspondientes, es muy recomendable en

este caso.

Los administradores de organización y dominio de Directorio Activo representan dos grupos de administradores especiales cuyo contexto de seguridad es necesario para funciones críticas dentro del directorio. Estos grupos, Administradores de organización y Admins. de dominio, son responsables de la administración de servicios de nivel superior. Para mitigar los riesgos inherentes en dichos grupos con muchos privilegios, recomendamos encarecidamente que se restrinja la pertenencia a los mismos. De hecho, el grupo Administradores de organización no debe tener miembros permanentes y los grupos de Admins. de dominio deben contener sólo un número pequeño y controlable de individuos de confianza que trabajen para la organización a tiempo completo.

Cuando sea necesario realizar tareas de administración de empresa como la autorización de servidor DHCP o la creación de sitios de Directorio Activo, el grupo Admins. de dominio del dominio raíz del bosque de Directorio Activo puede aumentar los privilegios administrando la pertenencia del grupo Administradores de organización. Estos privilegios sólo deben concederse por espacios de tiempo cortos para evitar la creación de miembros permanentes en el grupo Administradores de organización. Por supuesto, todos los miembros de un grupo Admins. de dominio de un bosque de Directorio Activo determinado deben tener la misma confianza.

Un error común que suelen cometer la mayoría de las organizaciones al desarrollar un modelo de delegación, es deshabilitar o paralizar estas funciones integradas. La modificación de las funciones predeterminadas puede causar resultados imprevisibles y no hay garantía de que las revisiones de service pack ni las actualizaciones de producto conserven esta configuración. Además, este tipo de modificación crea un entorno no compatible fuera de la organización. Un enfoque práctico consiste en usar las funciones y los grupos integrados, pero limitando la pertenencia. Para ello, tendrá probablemente que crear funciones nuevas para los administradores que anteriormente pertenecían a grupos como Adminis. de domino.

Tier4 Admins (Admins. de nivel4) El grupo Tier4 Admins (Admins. de nivel4) debe consistir en administradores de servicios centralizados que ofrecen soporte técnico para todos los servicios de empresa. Puesto que se trata de una función creada, los permisos de servicio de directorio y acceso al sistema se pueden adaptar a los requisitos específicos de la organización. Aunque los miembros de este grupo son administradores de servicio, pueden realizar también tareas de administración de datos en todo el bosque. Debido a que hay muchas clases de sistemas y áreas diferentes de responsabilidad, las funciones del nivel4 se dividen en varios subgrupos dentro del directorio. Por ejemplo, se deben crear grupos independientes del nivel4 para ofrecer una administración distinta de sistemas específicos, tales como los servidores Exchange. Este grupo sirve también como un punto de extensión para administradores de datos.

Una de las razones por las que a menudo la gente desea que se le conceda la pertenencia al grupo Admins. de dominio es conseguir derechos administrativos de todo el sistema en un dominio determinado. El truco para que estos administradores de servicio trabajen en el modo de privilegio mínimo es conceder el control de Tier4 Admins (Admins. de nivel4) de los servidores de empresa sin hacerlos administradores de dominio. Para evitar la extensión de privilegios, no se debe conceder a los administradores de Tier4 Admins (Admins. de nivel4) la pertenencia al grupo BUILTIN\Administradores en controladores de dominio, ya que ese grupo tiene muchos derechos subyacentes para el servicio de directorio que no se pueden separar. Por ejemplo, un miembro del grupo BUILTIN\Administradores de un dominio determinado puede administrar la pertenencia al grupo Admins. de dominio, permitiendo que ciertos miembros aumenten sus privilegios sin realizar comprobaciones ni equilibrios.

Recordando nuestra regla de no paralizar permisos predeterminados, podemos mitigar este riesgo haciendo que los grupos del nivel4 sean miembros anidados de los grupos de dominio integrados Opers. de servidores y DNS Admins (Admins. de DNS). De esta forma, se permite la administración local de controladores de dominio a la vez que se limita la capacidad de Tier4 Admins (Admins. de nivel4) de aumentar los privilegios. Para la mayoría de los sistemas (que no sean controladores de dominio, servidores de certificados, etc.), debe hacer que el grupo Tier4 Admins (Admins. de nivel4) sea miembro del grupo Administradores local. La automatización de la pertenencia anidada a grupos locales se puede lograr mediante la funcionalidad Grupos restringidos de directiva de grupo.

3. Administradores de datos

Ahora centrémonos en las funciones de administración de datos. Deben estar diseñadas con derechos acumulativos, lo que significa que un administrador de Tier2 Admins (Admins. de nivel2) debe tener los mismos derechos que un administrador de Tier1 Admins (Admins. de nivel1) junto con algunos privilegios adicionales, etc. Por ello, nos centraremos en estos grupos y seguiremos un orden de abajo a arriba.

Tier1 Admins (Admins. de nivel1) El grupo Tier1 Admins (Admins. de nivel1) debe ofrecer la administración general de objetos de directorio anteriormente creados. Este grupo es para los administradores con un aprendizaje mínimo o para aquéllos que realicen tareas aisladas, tales como restablecimientos de contraseñas. Conceda a este grupo los derechos de la unidad organizativa para modificar propiedades de cuenta de usuario, restablecer contraseñas de cuenta de usuario, desbloquear cuentas, activar/desactivar cuentas de usuario, agregar y restablecer cuentas de equipos de estación de trabajo y modificar la pertenencia de objetos de grupos que no sean administrativos.

Tier2 Admins (Admins. de nivel2) Este grupo debe permitir la administración y la creación selectiva de objetos, permitiendo que sólo se creen los objetos que pueda administrar Tier1 Admins (Admins. de nivel1). Por ejemplo, los grupos de seguridad sólo se pueden crear en la unidad organizativa de grupos. Los administradores de Tier2 Admins (Admins. de nivel2) pueden agregar y modificar cuentas de Tier1 Admins (Admins. de nivel1); agregar, modificar y eliminar cuentas de usuario de una unidad organizativa; eliminar objetos de equipos de estación de trabajo; y agregar, modificar y eliminar objetos de servidor, contacto y carpetas compartidas.

Regional Admins (Admins. regionales) A este grupo se le conceden derechos exclusivos sobre su estructura de unidades organizativas regionales. Sin embargo, sus administradores no pueden administrar otras estructuras de unidades organizativas regionales del directorio. Las cuentas de este grupo se deben considerar con muchos privilegios y, como resultado, se almacenan en una jerarquía de unidad organizativa independiente y están administradas por los administradores de servicios de Tier4 Admins (Admins. de nivel4). A los administradores de Regional Admins (Admins. regionales) se les permite crear la mayoría de los objetos sin restricciones dentro de su estructura de unidades organizativas (una excepción notable es la creación de otras unidades organizativas), que conlleva el riesgo adicional de crear objetos que no se puedan administrar en niveles inferiores.

Tier3 Admins (Admins. de nivel3) Muchas organizaciones tienen un departamento de soporte técnico centralizado o de nivel superior. Esta función llena la lista de administradores de datos y ofrece un grupo de administradores de datos por encima de todos los administradores regionales. Los derechos no se delegan a estos grupos específicamente dentro del directorio; en su lugar, se delegan a través de la pertenencia anidada de cada grupo Regional Admins (Admins. regionales). Esto ofrece un punto de extensión de nivel superior para todos los administradores de datos así como un punto de entrada de problemas que pasarán a los grupos de administración de servicios.

4. Creación de un modelo de unidad organizativa y grupo de seguridad

Una vez que las funciones están definidas en la organización, se debe definir un modelo de unidad organizativa y grupo de seguridad. Hay dos razones principales para crear una unidad organizativa en Directorio Activo: la delegación de derechos y la creación de un punto donde se puedan vincular los objetos de directiva de grupo. Las unidades organizativas definen un ámbito de administración (SOM) dentro del directorio y se pueden usar para limitar los derechos a objetos de varios niveles. Como resultado, el modo en que elija delegar la autoridad debe ser un factor principal en la implementación de la estructura de unidades organizativas.

Teniendo esto en cuenta, se debe crear una unidad organizativa de nivel superior (o una serie de unidades organizativas) directamente bajo el dominio para albergar todos los objetos. Esta unidad organizativa sirve para el propósito específico de definir el SOM de nivel superior de Tier4 Admins (Admins. de nivel4). Al crear una unidad organizativa de nivel superior, los derechos sobre el servicio de directorio pueden comenzar explícitamente en el nivel de unidad organizativa en lugar de en el nivel de dominio. La delegación desde una unidad organizativa de nivel superior en lugar de un dominio mitiga el riesgo observado anteriormente de que los usuarios tengan la capacidad de aumentar los privilegios mediante la manipulación de los grupos del dominio integrados.

Debajo de las unidades organizativas de nivel superior, debe crear jerarquías independientes de unidades organizativas inferiores para representar cada región o unidad de negocio que tiene un equipo de administración de datos específico. Cada unidad organizativa inferior regional debe tener una jerarquía de unidades organizativas común y no extensible para la administración de objetos de directorio. La uniformidad es fundamental para la administración progresiva, ya que gran parte de la delegación de derechos será automática. Éste es un orden de gran tamaño, ya que es posible que cada región desee unidades organizativas únicas. Sin embargo, los administradores de TI deben mantenerse firmes, y si una extensión es requerida para una región, la estructura de unidades organizativas inferiores debe extenderse para todas las regiones. Esto puede parecer difícil al principio, pero si la organización ofrece un alojamiento genérico para los objetos, las situaciones aisladas acaban produciéndose con el tiempo.

Finalmente, cree grupos y cuentas de subadministradores independientes para eliminar a la capacidad de los administradores de aumentar los privilegios (un grupo Tier1 Admins (Admins. de nivel1), Tier2 Admins (Admins. de nivel2) y Regional Admins (Admins. regionales) para cada jerarquía de unidad organizativa inferior). Al colocar estas cuentas en unidades organizativas independientes, se permite la restricción de la administración a ese nivel o a uno inferior. Así, si todas las cuentas de Tier1 Admins (Admins. de nivel1) y el grupo de seguridad asociado residen en una unidad organizativa donde no tienen derechos, los administradores no podrán apropiarse de otras cuentas de administrador ni aumentar los privilegios de otros administradores a su nivel. Cualquier miembro del grupo Admins. de dominio, por ejemplo, puede convertir cualquier otra cuenta de usuario del dominio en un administrador de dominio. Sin embargo, con este modelo de unidad organizativa aplicado, se mitiga ese riesgo. En la Figura se muestra una estructura de unidad organizativa de ejemplo con grupos de seguridad asociados.

Estructura de unidad organizativa y grupos de seguridad asociados

5. Establecimiento de cuentas secundarias

La clave para conseguir un modelo satisfactorio de delegación consiste en aplicar el principio de privilegio mínimo. En la práctica, esto significa que una entidad de seguridad debe tener sólo la capacidad de realizar las tareas necesarias para su función y nada más. Desgraciadamente, muchos administradores de TI usan la misma entidad de seguridad para la administración de directorios y para tareas diarias como la exploración de la Web y la lectura del correo electrónico. Tener cuentas separadas disminuye la probabilidad de que un administrador con niveles dañe el servicio de directorios por error o sea víctima de un ataque enviado a través de aplicaciones diarias y dirigido al administrador de directorios.

Para alcanzar esto sin requerir que el usuario cierre sesión y vuelva a abrirla, se usa el servicio de inicio de sesión secundario (Runas.exe). Éste permite a los usuarios aumentar sus privilegios mediante un conjunto alternativo de credenciales al ejecutar scripts o archivos ejecutables en servidores y estaciones de trabajo.

Mientras el concepto del uso de cuentas de privilegio mínimo es relativamente sencillo, las organizaciones a veces lo encuentran difícil de implantar, ya que puede que los hábitos de TI anteriores sean bastante difíciles de quebrantar. Un método directo para evitar el uso de cuentas con privilegios en tareas diarias es no ofrecer acceso al correo a dichas cuentas en Exchange Server, reforzando este principio mediante una directiva administrativa en la organización. Este enfoque relativamente sencillo reduce apreciablemente la probabilidad de que se usen dichas cuentas para tareas rutinarias no administrativas.

6. Delegación de derechos

El paso final para desarrollar un modelo de delegación es la delegación real de derechos en Directorio Activo. Esto trae consigo la manipulación de entradas de control de acceso (ACE) y de listas de control de acceso (ACL) en los datos almacenados en el directorio. Las ACL de contenedores de Directorio Activo definen qué objetos se pueden crear y cómo se administran dichos objetos. La delegación de derechos implica operaciones básicas en objetos, como la capacidad de ver un objeto, de crear un objeto secundario de una clase especificada o de leer información de atributos y seguridad en objetos de una clase especificada. Aparte de estas operaciones básicas, Directorio Activo define derechos extendidos, que permiten operaciones tales como Enviar como y Administrar topología de réplica.

En pasos anteriores, hemos tratado la creación de grupos de seguridad que se asignan a funciones definidas de la organización. Esto significa que para cada función hay un grupo de seguridad asociado por estructura de unidades organizativas inferiores. Para implementar el modelo de delegación, se deben asignar permisos a estos grupos sobre los objetos del directorio. En este punto del proceso, no desea grandes descubrimientos ni tener que crear un entorno sumamente personalizado. En su lugar, pruebe a aprovechar los grupos y los derechos integrados en la medida de lo posible. Supongamos que una función concreta necesita administrar registros DNS para el bosque. No intente delegar los derechos sobre los contenedores y los contextos de nomenclatura a DNS integrado de Directorio Activo; en vez de eso, simplemente aproveche el grupo BUILTIN\DNS Admins (BUILTIN\Admins. de DNS) del dominio. Además, los derechos de usuario y otros permisos se pueden extender a través de la directiva de grupo para ofrecer los derechos adicionales necesarios para administrar una clase específica de sistema mediante una función determinada.

Al asignar permisos mediante la delegación, debe limitar o incluso eliminar

completamente el uso de ACE de denegación en el directorio. Pueden resultar delicadas a la hora de solucionar problemas. Un mejor enfoque es usar ACE de admisión para conceder derechos a los grupos personalizados que representan las funciones. Recuerde que las funciones definidas por el usuario, tal como Tier4 Admins (Admins. de nivel4), sólo tendrán los derechos explícitos definidos por esa función.

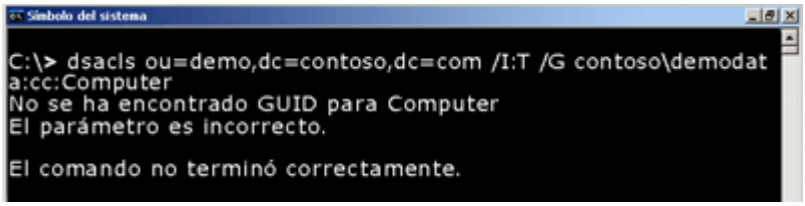
La herencia resulta fundamental para la seguridad de Directorio Activo y define como una ACL concreta se aplica a objetos secundarios en un contenedor o sub-contenedor determinado. Sea siempre específico acerca del ámbito de herencia, asegurándose de que las ACE heredables se aplican tan próximas a los objetos de destino como sea posible. Los permisos de denegación heredables aplicados en el objeto primario tendrán prioridad frente a permisos de denegación heredables aplicados en el objeto primario principal; ésta es una de las razones principales por las que no se recomiendan las ACE de denegación para la delegación práctica. Además, los permisos heredables no pueden invalidar ninguna ACE explícita de un objeto. Por ello, se recomienda que limite o elimine la capacidad de los administradores con niveles para modificar la lista de control de acceso discrecional (eliminando el privilegio de escritura en DACL) en objetos de directorio. Tenga en cuenta que el creador del objeto posee estos derechos de manera implícita. La regla general es que si un administrador tiene la capacidad de cambiar la DACL de un objeto, probablemente lo hará. No permita que el duro trabajo que la organización ha encomendado al modelo de delegación se pierda al introducir la elección y un posible error administrativo.

Hay varias herramientas que deberá usar para implementar correctamente un modelo de delegación de Directorio Activo. Para la mayoría de las organizaciones grandes, el uso del asistente de delegación integrado para asignar permisos en el directorio es una tarea desalentadora en la que prima la posibilidad de un error administrativo. En su lugar, siempre se debe usar la automatización para garantizar que el modelo de delegación está bien documentado, es compatible y ofrece una opción de recuperación en caso de que se pierda o se cambie la configuración de algún modo sin querer.

La herramienta principal necesaria para implementar la delegación es DSACLS.EXE, una herramienta de línea de comandos usada para manipular las ACL de servicio de directorio en objetos. Esta herramienta también permite especificar los indicadores de herencia para una DACL en el objeto primario. (Los indicadores de herencia incluyen este objeto y subobjetos, sólo subobjetos y propagan los permisos heredables sólo en un nivel). Los comandos de DSACLS no funcionarán correctamente en última instancia si un indicador de herencia está establecido incorrectamente, de modo que es esencial realizar pruebas al usar esta herramienta. Aquí tiene un ejemplo de la sintaxis de DSACLS para delegar la capacidad de crear objetos de equipo en la unidad organizativa de demostración de destino:

```
dsacls.exe ou=demo,dc=contoso,dc=com /I:T /G contoso\dataadmin:CC;computer
```

DSACLS distingue mayúsculas y minúsculas con respecto a los tipos de objeto. Esto significa que si intenta delegar permisos para la clase de objeto "cn=Computer" en "cn=computer", no funcionará (consulte la Figura 3).




```
dsacls ou=demo,dc=contoso,dc=com /I:T /G contoso\demodata:CC;user
```

Error debido a distinción de mayúsculas y minúsculas (Hacer clic en la imagen para ampliarla)

Es necesario contar con un conjunto específico de derechos para crear algunos objetos. Esto tiene que ver con los atributos "obligatorios" y "opcionales" de los objetos. La mejor metáfora que he conocido para explicar este concepto es el modelo de la hamburguesa. Las hamburguesas deben estar compuestas por una hamburguesa de carne y un bollo para ser consideradas hamburguesas. Estos son los atributos obligatorios de la clase de objeto hamburguesa. Los elementos como pepinillos, ketchup, lechuga, etc. son los atributos opcionales. Si extendemos la clase de objeto para definir una hamburguesa con queso, agregaremos el queso a la lista de atributos obligatorios.

Los objetos de usuario funcionan de la misma manera. Digamos que vamos a seguir este

```
dsacls ou=demo,dc=contoso,dc=com /I:S /G contoso\demodata:GRGW;;user
```

```
dsacls ou=demo,dc=contoso,dc=com /I:S /G contoso\demodata:CA;"Reset Password";user
```

El administrador se enfrentará a varios errores durante la creación de objetos de usuario. Necesitamos conceder los privilegios necesarios para establecer los atributos correspondientes de objeto de usuario, incluida la configuración de la contraseña. Todo esto se muestra en la siguiente sintaxis de DSACLS adicional.

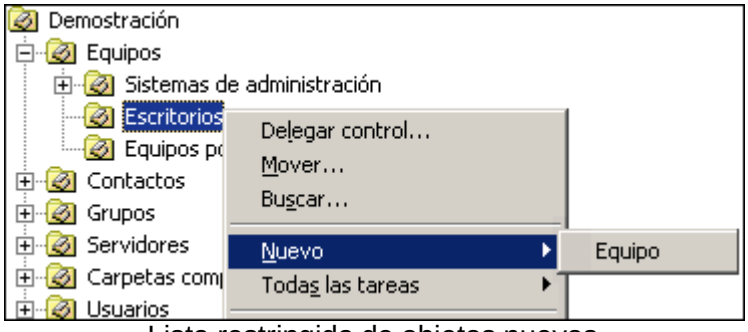
Para el primer paso, conceda el privilegio para escribir atributos obligatorios mediante la concesión de los concediendo la Lectura genérica/Escritura genérica a todos los atributos de la clase de usuario:

Para el paso siguiente, conceda el derecho extendido para cambiar la contraseña:

Para el paso final, conceda el privilegio de Propiedad de lectura y escritura del atributo Último cambio de contraseña:

```
dsacls ou=demo,dc=contoso,dc=com /I:S /G contoso\demodata:RPWP;pwdLastSet;user
```

Una vez que se hayan delegado los derechos correspondientes, las funciones definidas se limitarán sólo a la administración de las clases de objeto definidas en la DACL del contenedor. Mediante el ejemplo de objeto de equipo anterior, el menú contextual de Usuarios y equipos de Directorio Activo restringe la lista de objetos nuevos que puede crear el usuario al que se delegan dichos derechos.



Lista restringida de objetos nuevos

El valor de DSACLS también se puede automatizar para ofrecer una implementación compleja de derechos. Aquí se muestran algunos de los comandos de DSACLS que se pueden usar para delegar derechos de manipulación de atributos de dirección comunes a objetos de usuario de un contenedor determinado:

```
dsacls ou=demo,dc=contoso,dc=com /I:S /G contoso\demodata:RPWP;c;user
dsacls ou=demo,dc=contoso,dc=com /I:S /G contoso\demodata:RPWP;co;user
dsacls ou=demo,dc=contoso,dc=com /I:S /G contoso\demodata:RPWP;l;user
dsacls ou=demo,dc=contoso,dc=com /I:S /G contoso\demodata:RPWP;postalCode;user
```

Ejemplos como éstos son comunes para la mayoría de los modelos de delegación y se pueden usar junto con las funciones definidas anteriormente.

Otra herramienta usada para implementar la delegación es DSREVOKE.EXE, que permite a los administradores localizar y eliminar derechos delegados para entidades de seguridad específicas de objetos del directorio. Aunque esta herramienta puede ser muy útil, es específica de una entidad de seguridad y no evalúa la pertenencia anidada de los grupos de seguridad.

Además de estas herramientas de línea de comandos, recomendamos el uso de la asignación de derechos de usuario y los grupos restringidos con directiva de grupo. Como hemos indicado anteriormente, la asignación de derechos de usuario permite a los administradores de TI extender o eliminar derechos de nivel inferior (tales como el derecho de obtener acceso y reiniciar el sistema de forma remota) para varios grupos de usuarios de sistemas de destino específicos. Los grupos restringidos se pueden usar para especificar y aplicar la pertenencia local y de dominio en el bosque. Juntas, estas herramientas ofrecen todo lo que necesita para automatizar e implementar un modelo de delegación de Directorio Activo.

Resumen

Aunque la tarea de desarrollo de un modelo de delegación de Directorio Activo puede parecer compleja, lo cierto es que se pueden aplicar modelos muy sencillos a la mayoría de infraestructuras de TI. Uno de los pasos más importantes a la hora de implementar un modelo práctico de delegación es definir funciones claras. Debe limitar las funciones definidas a un número pequeño y controlable. El equilibrio es complicado, ya que si se cuenta con demasiadas funciones, habrá algunas que no se usen, mientras que tener muy pocas funciones no permitirá la separación de las mismas.

Al definir las tareas, recuerde clasificarlas por frecuencia, importancia y dificultad. Una vez que defina las funciones, desarrolle un conjunto de casos de uso para ayudar a identificar lo que cada función puede o no puede hacer y poder automatizar el proceso de prueba.

Los casos de uso bien preparados ayudarán a explicar estas funciones a sus poseedores en la organización y a mitigar cualquier sorpresa debido a errores de automatización.

Finalmente, siempre es una buena idea tomar un enfoque práctico al desarrollar un modelo de delegación. Recuerde, la sencillez se equipara a la compatibilidad y un modelo de delegación sostenible reportará grandes beneficios a la hora de controlar los derechos administrativos en el entorno de Directorio Activo.