Gestión de Identidades

Transcribed on August 7, 2025 at 3:55 PM by Minutes AI

Speaker 1 (00:05)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar el tema de la administración de identidades.

Hablaremos de la administración de identidades y qué herramientas tenemos en Windows para securizar todo lo que es la parte de gestión de identidades.

Hablaremos de los grupos restringidos, hablaremos del grupo de usuarios protegidos, hablaremos de los objetos de configuración de password y hablaremos de Local Administrator Password Solution, caso solución de Microsoft de libre descarga para la administración de password en las cuentas o en las identidades de equipos locales.

La administración de identidades es uno de los desafíos más importantes en la infraestructura de las organizaciones hoy en día.

Administrar de forma adecuada los procesos de autorización y gestión de credenciales es un paso básico para evitar riesgos de accesos no autorizados o que un malware o un determinado atacante sea capaz de utilizar esa identidad o algún complemento relacionado con esa identidad, un token relacionado con un usuario o un ticket TGT para poder ejecutar o poder acceder a servicios a los que no tendría permiso.

Hay una serie de recomendaciones que nos van a ayudar a mitigar algunos ataques conocidos como Securizar las cuentas de usuario y las contraseñas.

Administrar de forma adecuada los grupos con privilegios, auditar los cambios en los recursos críticos de una organización, desplegar autenticaciones de forma segura y utilizar segundos factores de autenticación.

Securizar la actividad de la red y monitorizar la actividad de la red en búsqueda de tráfico inusual o de tráfico paquetes de red que puedan ser maliciosos para descubrimiento de redes u otro tipo de actividades no autorizadas.

Establecer una administración de cuentas para aprovisionar de forma segura y de forma adecuada a lo largo del tiempo las diferentes identidades y las cuentas de equipo y usuario.

¿Es decir, no sólo tenemos que tener desplegado la planificación cuando un usuario inicia sesión en una organización y se le asigna una determinada identidad, sino que hay que planificar cuando ese usuario cesa una actividad qué es lo que pasa con esa identidad si se destruye esa cuenta?

¿Se elimina?

¿Se deja inactiva?

¿Va a ser utilizada por otro usuario?

Y después tener siempre en cuenta la parte de la seguridad física de los dispositivos.

Entre las tecnologías que tenemos disponibles dentro de Microsoft para la securización de identidades tenemos una herramienta que se llama grupos restringidos.

Los grupos restringidos van a controlar la pertenencia a los grupos de administración local de los equipos.

Y quiero hacer especial hincapié en esta parte.

Hay muchos tutoriales, hay mucha información de Internet en el que se administra la pertenencia a grupos de dominio.

Microsoft es muy claro en este aspecto.

Grupos restringidos funciona para controlar o para administrar qué grupos, qué usuarios pueden pertenecer a grupos locales de equipos.

No funciona para grupos de dominio.

Vamos a tener dos maneras de poder configurar Vamos a poder configurar en la parte de arriba los miembros de este grupo y si seleccionamos esa opción, lo que vamos a hacer es que cuando añadimos un grupo o añadimos un usuario, automáticamente el resto de grupos o de usuarios que tuvieran privilegios de administración local en los equipos dejan de tenerlos, a excepción del grupo de administradores de dominio.

Si utilizamos la parte de abajo de la configuración que sería miembros en esa parte, si nosotros añadimos un determinado grupo, por ejemplo el grupo Auditores o el grupo Departamento IT, vamos a añadir ese grupo como administrador local de los equipos, pero no vamos a excluir aquellos usuarios o aquellos grupos que ya fueran administradores locales de los equipos del dominio.

Recordar específicamente que grupos restringidos no se utiliza para administrar la pertenencia a grupos de dominio, solo la pertenencia a grupos locales de equipo.

Tenemos otro elemento disponible desde la versión de Windows Server R, que es el grupo Usuarios protegidos.

El grupo Usuarios protegidos está creado por defecto, no necesitamos crear este grupo.

Cuando nosotros añadimos un usuario o añadimos un grupo dentro del grupo Usuarios protegidos se le van a aplicar una serie de medidas de seguridad adicionales en lo que se refiere a la parte de gestión de tokens, de autenticación, de modelos de autenticación y de diferentes secretos o diferentes protocolos o tecnologías que va a poder utilizar el dominio.

Tiene que soportar cifrado mediante AES, no va a poder utilizar ni DES ni RC para la parte de cifrado y no va a soportar tampoco delegaciones de Kerberos, Autenticación con NTLM, Digest Authentication o CredSSP no van a estar permitidas.

Es decir, hay una serie de tecnologías de manejo y cacheo de credenciales que se sabe que son inseguras, que hay ataques conocidos y entonces todos los usuarios o grupos que pertenezcan al grupo Usuarios protegidos pues no van a poder utilizar todas esas tecnologías de esta manera van a estar mucho más seguros porque no se va a poder atacar las credenciales de ese usuario, no se va a poder atacar el cacheo de tokens o de credenciales o de secretos que utilice ese usuario, ese grupo, porque esos protocolos inseguros no van a funcionar.

El ticket de Kerberos va a tener un valor por defecto de cuatro horas, aunque va a poder modificarse mediante polisilos o directivas de autenticación.

Vamos a ver cómo sería la configuración de estas tecnologías.

Estamos en Server Manager, nos vamos a la parte de Pools, nos vamos a la consola de administración de directivas de grupo, vamos a seleccionar la política que tenemos por defecto en el dominio que se llama Seguridad y en esta política nos vamos a ir a la configuración de Equipo, nos vamos a Directivas, Configuración de Windows, nos vamos a la parte de Configuración de seguridad y tendremos aquí Restricted Groups, vamos a seleccionar aquí el grupo de administradores, nos vamos a la parte de Propiedades y vamos a dar aquí a la parte de Añadir y vamos a seleccionar un grupo.

Seleccionamos el grupo IT, damos a OK, damos Aplicar y lo que estamos haciendo ahora es añadir a todos los miembros del grupo italiano al grupo de administradores locales de los equipos del domingo.

Si nosotros lo hacemos de esta manera, cualquier usuario que pertenezca al grupo de administradores locales de los equipos, cualquier grupo que pertenezca al grupo de administradores locales de los equipos va a permanecer.

Si nosotros lo hiciéramos en la parte de arriba, el grupo IT formaría parte del grupo de administradores de los equipos locales y cualquier otro grupo, excepto el grupo Administradores de dominio y Administradores del dominio, dejaría de pertenecer al grupo de administradores locales de los dispositivos.

Como ya os digo, es una característica muy interesante para la administración de la pertenencia a grupos de administración local de los equipos.

Nos sirve para grupos o cuentas de dominio.

Si nos vamos a la parte del centro administrativo de Active Directory, nos vamos a la parte del dominio, dentro de la parte del dominio nos vamos a la parte de Users y dentro de la parte de Users vamos a tener el grupo que ya está creado por defecto, no necesitamos crearlo, que se llama Usuarios protegidos.

Si nosotros vemos las características de este grupo en la parte de descripción, nos indica que tiene una serie de medidas adicionales para la restricción de no utilizar protocolos que se sabe que son vulnerables.

Seleccionamos Miembros y en la parte de miembros damos Añadir, en este caso seleccionamos el grupo IT, damos a OK y ya tendríamos el grupo IT dentro del grupo de usuarios protegidos aplicándosele todas esas medidas.

Si nos vamos a la parte de Usuarios pueite y si vamos a la parte de Miembro D vemos que pertenece al grupo de usuarios protegidos.

Esto lo que va a hacer es que va a evitar que se utilicen todos estos protocolos inseguros.

Hay que tener en cuenta que si nosotros necesitamos utilizar alguna tecnología, una VPN, un acceso a una aplicación, un acceso a un servidor que negocie las credenciales o que necesite cachear credenciales o que necesite utilizar un determinado protocolo, creo CSSP, etc.

Etc.

No vamos a poder utilizar esa aplicación o esa VPN o no vamos a poder acceder a ese servicio.

Entonces usuarios protegidos no está pensado para desplegar a nivel de todos los usuarios todos los grupos de la organización, sino para una serie de cuentas específicas que nosotros queremos securizar o bien porque tienen muchos privilegios o bien porque tienen acceso a información confidencial, a información importante dentro de una organización.

Tenemos otro elemento para la gestión de credenciales que son los objetos de configuración de password.

Desde Windows Server 2008 es una característica que nos va a permitir configurar una segunda política de contraseñas.

Habíamos visto cuando vimos los objetos de directiva de grupo, las GPOs, que nosotros sólo podemos definir una única directiva de contraseñas para todo el dominio.

Normalmente vamos a Default Domain Policy y definimos ahí la directiva de contraseñas, qué longitud quiere, si queremos que tenga un grado de complejidad, requisito de complejidad, si queremos que tenga un histórico y recuerde X contraseñas, etc.

Pero sólo lo podemos hacer de una forma genérica para todo el dominio.

En los entornos actuales puede darse el caso de que nosotros queramos que un determinado grupo o que un determinado usuario tenga una política de contraseñas que sea más estricta, por ejemplo los directivos o por ejemplo el grupo del departamento IT.

Entonces para eso nosotros podemos utilizar los objetos de configuración del password para después de crear esas condiciones de contraseña poder asignar esas direcciones de contraseña a un grupo de seguridad.

No funciona con la infraestructura de objetos de directiva de grupo, es una tecnología diferente que después no se va a asignar a una unidad organizativa ni se asigna a nivel de dominio, sino que se va a enlazar con un grupo de seguridad global.

Los objetos de directiva de contraseña van a utilizar dos elementos, un contenedor que es el que va a almacenar las psos y que va a permitir a los usuarios o grupos de seguridad global enlazar esas psos y después estos objetos de contraseña, las psos que sólo los administradores de dominio van a poder crear o van a poder enlazar.

Fine Grained Password Policy sólo se aplica a objetos de usuario y Network Person o grupos de seguridad global.

Cuando nosotros enlazamos una PSO, un atributo por defecto vacío que se llama MSDS PSOapplied es modificado y se le asigna el valor de la PSOE.

Tenemos dos maneras de poder aplicar objetos de contraseña estas PCO primeramente mediante Windows PowerShell, en el que primero crearíamos la PSO, tenéis un ejemplo de la sintaxis en la diapositiva, y después tendríamos que asignar esa PSO a un determinado grupo, en este caso al grupo de auditores, o podemos hacerlo mediante el entorno gráfico en el centro administrativo de Active Directory.

Vamos a tenerlo dentro del dominio, en la parte de System, tendremos Password Settings Container y ahí vamos a poder crear un nuevo objeto de contraseña y después vamos a poder asignarlo dentro de las características del grupo, dentro de las características del usuario o directamente a través de PSO, independientemente de cómo lo asignemos nosotros.

Vamos a tener que definir también un valor de precedencia, que es un atributo que va a indicar en caso de conflicto qué política de contraseña se va a aplicar, teniendo en cuenta que el valor más bajo va a indicar la prioridad de preferencia, es decir, si yo tengo una pso de valor 15 de precedencia 15 de una pso de precedencia 3, si se aplican las dos, la que tenga el valor 3, el valor menor, es la que va a prevalecer.

Esto puede darse de forma habitual porque un usuario puede pertenecer a varios grupos, yo puedo tener aplicada una PSO a un determinado grupo y otra PSO a otro grupo, entonces como un usuario pertenece a los dos grupos, se le puede tratar de aplicar las dos directivas de contraseña, pues aquella que tenga el número de precedencia más bajo es la que va a prevalecer dentro de la parte del dominio.

Nos vamos a ir a la parte de System, simplemente vamos a dar a Nuevo Password Settings y nos va a aparecer un panel de configuración para seleccionar cómo queremos poner la contraseña.

Vamos a hacer una que sea para el departamento IT, que tenga una precedencia por ejemplo de 5.

Aquí tendríamos los valores para indicar cómo queremos que se configure la contraseña, longitud de la contraseña, contraseña histórico, incluso podemos habilitar también desde aquí la parte de bloqueo de cuenta e incluso desde aquí nosotros podríamos añadir eso a el grupo al que queremos asignar, en este caso la directiva de contraseñas al grupo IT.

Al grupo IT damos OK, damos a OK y ya tendríamos el Password setting asignado en este caso al grupo IT.

Si nos vamos a la parte de Users vamos a ir en este caso al grupo IT y dentro de la parte del grupo IT, si nos vamos a la parte de configuración de contraseñas vemos que está asignada a esta contraseña.

Nosotros desde aquí podríamos eliminar la contraseña o incluso desde el propio grupo podríamos seleccionar entre todas las PSO que tuviéramos disponibles para asignarla.

Aquí como podéis ver la administración de los objetos de directiva de contraseña, de configuración de contraseña son muy intuitivos y muy fáciles de administrar.

Además de las diferentes opciones que nosotros tenemos dentro de los sistemas operativos para la gestión de identidades en entornos de dominio, podemos descargar una herramienta adicional para la administración de identidades locales de los equipos que se llama Labs.

Las características de Labs es que vamos a administrar contraseñas únicas para cada uno de los equipos.

Labs va a generar contraseñas de forma aleatoria para los administradores locales y va a almacenar esas contraseñas y todos los secretos relacionados con las identidades locales en los controladores de dominio, de tal forma que los ataques conocidos sobre el dispositivo, accediendo al disco duro y al archivo SAM para extraer contraseñas, activar usuarios, etc.

No nos funcionaría.

Después podemos recuperar esas contraseñas desde la propia herramienta, desde el controlador de dominio y va a intervalos regulares a cambiar esa contraseña.

Los requerimientos de Labs son equipos Windows, tanto versiones 86 como 64 que pertenezcan al dominio en un nivel funcional de dominio de al menos Windows Server 2003 y Labs VA a extender el esquema de Active Directory, es decir, que va a aumentar el número de atributos de Active Directory.

Tenemos que instalar Labs en los equipos cliente que vamos a administrar y requiere.

NET Framework 4.0 y PowerShell 2 o versiones posteriores.

Como veis, a nivel de compatibilidad es muy fácil que se pueda desplegar.

¿Cómo trabaja Labs?

Bueno, pues va a determinar si la cuenta de administrador local ha expirado.

Si esa cuenta ha expirado va a realizar los siguientes va a cambiar la contraseña a una nueva contraseña aleatoria, además va a utilizar una serie de contraseñas aleatorias muy largas, muy, muy seguras y va a transmitir la nueva contraseña y la fecha de expiración al directorio activo donde va a almacenarse junto con aquellos elementos que sean sensibles relacionados con la cuenta de equipo de ese dispositivo.

Como hemos podido ver, Windows Server tiene una serie de herramientas que nos ayudan a proteger usuarios y servicios y administrar las directivas de contraseña y poder adaptarlas de una forma específica a las necesidades de la organización.

Tenemos una propuesta de ejercicio que es crear un grupo de seguridad global que se llame Auditores, asignar ese grupo al grupo Usuarios protegidos y después crear Password Setting Audit, es decir, un objeto de configuración de password específico para ese grupo de auditores y asignárselo a ese grupo de auditores.

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar el tema de la administración de identidades.

Vamos a resolver el ejercicio que se pedía en el vídeo anterior en el que había que crear un grupo de seguridad global llamado Auditores, asignar ese grupo al grupo Usuarios protegidos para que se aplicarán todas las medidas de seguridad relacionadas con el grupo Usuarios protegidos.

Después crear un objeto de configuración de password específico para ese determinado grupo y asignarlo al grupo de auditores.

En la consola de Server Manager vamos a la parte de Tools, nos vamos a Usuarios y Equipos del directorio activo y desde la consola de usuarios Equipos del directorio activo.

Nos vamos a la parte de Usuarios, vamos a crear un nuevo usuario que se va a llamar Tom, ponemos el nombre de UPN para que inicie sesión, damos a Siguiente, ponemos la contraseña, seleccionamos las opciones de contraseña, damos a Siguiente y damos a Finalizar.

Vamos a crear también un grupo nuevo, grupo llamar Auditores.

Este grupo tiene que ser un grupo de seguridad global.

Es importante que sea un grupo de seguridad global porque si no luego no vamos a poder asignarle la PSOE.

Si es un grupo, por ejemplo, de seguridad universal, no le podemos asignar una PSU.

Ya tenemos el grupo y en este caso vamos a buscar el usuario Tom.

Vamos a añadirlo al grupo de Auditores, seleccionamos el grupo de auditores y ya lo tenemos.

Dentro del grupo de auditores vamos a ir ahora al Centro administrativo de Active Directory.

Dentro del centro administrativo de Active Directory nos vamos a la parte de Users, dentro de la parte de Users vamos a buscar Protected Users y dentro de la parte de Protected Users nos vamos a la parte de Members y vamos a añadir aquí el grupo Auditores.

Seleccionamos el grupo, damos a OK, damos OK y damos OK.

De esta manera ya tenemos al grupo Auditores.

Dentro del grupo de Usuarios protegidos nos vamos a ir ahora a la parte de System y dentro de la parte de System vamos a Password Settings Container, Vamos a crear una nueva configuración de contraseña que va a ser específica para el grupo de auditores.

Seleccionamos Auditors, le damos una precedencia de 7, le damos los valores de contraseña, vamos a personalizar estos valores como nosotros queramos, seleccionamos el bloqueo de cuenta, vamos a poner los valores para el bloqueo de cuenta y desde aquí vamos a seleccionar el grupo Auditores para añadirlo o para enlazarlo a esta PSU.

Damos OK.

Damos OK y si ahora nos vamos a la parte de Users, nos vamos al grupo de Auditores y dentro del grupo de Auditores, si nos vamos a la parte de Miembros, tenemos que ver que pertenece, perdón, Miembros de.

Tenemos que ver que pertenece a usuarios protegidos.

En la parte de configuración de Password vemos que pertenece a la PSO de Auditores.

Si nos vamos al usuario Tom, dentro del usuario Tom, en la parte de Características nos iríamos a la parte de Miembros y dentro de la parte de Miembros de.

Vemos que pertenece al grupo de auditores, por lo tanto se le van a aplicar esos elementos.

Y luego la parte de Password Setting vemos que no nos aparece, pero sí que recibiríamos esa configuración porque pertenecemos a un grupo de auditores, aunque no nos veamos refleja aquí lo veríamos igualmente o haría efecto igualmente.

Como hemos visto, tenemos algunas características de seguridad que cambian el impacto de la gestión de identidades y de la protección de usuarios y grupos de una forma radical y con una aplicación muy sencilla, muy intuitiva.

Entre ellos el grupo Usuarios protegidos o la posibilidad de personalizar configuraciones de contraseñas específicas para usuarios o para grupos en concreto.

Llegamos al final de la sesión.

Os esperamos en el siguiente vídeo.