Cuentas de Servicio

Transcribed on August 8, 2025 at 12:38 PM by Minutes AI

Speaker 1 (00:04)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar el tema de las cuentas de servicio administradas.

Hablaremos de las cuentas de servicio administradas de Microsoft.

Vamos a ver un paso a paso qué tenemos que hacer para poder desplegar este tipo de cuentas y vamos a ver qué ventajas tiene utilizar esta tecnología.

En entornos empresariales es habitual la necesidad de emplear identidades que están asociadas al funcionamiento de un rol, de un servicio o de una aplicación.

Es decir, cuando yo estoy ejecutando un servidor web o una aplicación que yo tengo en un servidor y que está trabajando 24 7, hay una identidad relacionada con el funcionamiento de ese servicio.

Esa identidad al final es una cuenta de usuario y como todas las cuentas de usuario, pues en un momento determinado tiene que renovar el password.

Por ejemplo, en muchos casos los administradores terminan utilizando cuentas de usuario con contraseñas que nunca caducan para no tener que estar manteniendo o cambiando esa contraseña, porque si en un momento determinado se cambia esa contraseña, pues podría dejar de funcionar el servicio.

En algunos equipos, en algunos dispositivos, la administración sería un poco más compleja.

Entonces, una práctica habitual para las cuentas de servicio, para las cuentas de aplicaciones, es crear un usuario cuya contraseña no cambia y no expira.

Cuando nosotros utilizamos una determinada cuenta para abrir una aplicación, por ejemplo, cuando yo quiero abrir un documento de Word, lo que sucede es que ese documento de Word se está ejecutando con los mismos privilegios que tiene mi usuario.

Si ese documento de Word contiene un malware, lo que va a hacer ese malware es que va a tener los mismos privilegios de ejecución para poder funcional que tengan identidad.

Por eso se recomienda que nosotros utilicemos usuarios que sean usuarios estándar y que tengan siempre pocos privilegios, porque en el caso de que ejecutemos un software malicioso o algún programa que contenga un determinado malware, pues va a tener minimizado el impacto porque va a tener menos privilegios, va a tener menos campo de malware.

Este mismo malware puede hacerse con una cuenta de servicio, es decir, con un usuario que sea el que se utiliza para que funcione una aplicación o un usuario que sea el que se utiliza para un servicio web, por ejemplo, y va a pasar muy desapercibido porque esa cuenta de servicio puede estar funcionando 24 7, es decir, puede estar funcionando todos los días del año a cualquier hora, con lo cual ese malware puede estar haciendo una actividad constante y va a pasar desapercibido.

Es más, si esa cuenta está configurada para que la contraseña nunca caduque automáticamente ese malware va a tener un acceso indefinido a los recursos del sistema.

Microsoft lo que hace es proporcionar la utilización de cuentas de servicio administradas para solucionar los desafíos en este tipo de escenarios.

La principal ventaja de estas identidades es que Windows se va a encargar del mantenimiento y la actualización de las propiedades de estas cuentas, incluida la renovación periódica de contraseña de la identidad.

Es decir, el controlador de dominio lo que va a hacer es generar un password complejo y además va a renovar ese password a intervalos regulares.

De esta manera vamos a tener una cuenta que después es la que va a utilizar la aplicación, es la que va a utilizar el servicio, servicio web, servicio DNS, cualquier servicio con el que nosotros estemos trabajando y esa cuenta va a tener una administración segura y automatizada desde el controlador de dominio.

Los requisitos para utilizar las cuentas de servicio administrados son que el esquema del directorio activo en el bosque del dominio debe actualizarse por lo menos a Windows Server 2000, lo que hoy en día no sería ningún inconveniente.

Luego el valor del atributo CNESquema CN configuration SEXcom debe ser 52, un grupo de seguridad para la nueva cuenta MSA aprovisionada, es decir que tenemos que crear un grupo para y después CFIS master para el directorio activo no se implementa en el dominio o no se ha creado, se debe crear.

El resultado lo vamos a poder verificar con el registro de KDS Service con el evento coidentificador 4004.

Bueno, el paso a paso para poder trabajar con estas cuentas de servicio administrado sería un poco el que tenemos definido en esta diapositiva.

Tenemos que ejecutar una serie de comandos en el que tenemos que crear esa roofkey.

Una vez que nosotros creamos esa roofkey vamos a crear el nombre de las cuentas que vamos a utilizar.

En los siguientes comandos vemos cómo creamos una cuenta que se llama Datos compartidos y creamos otra cuenta que se llama Servicio web.

Esas dos cuentas después se van a añadir como cuentas de servicio, es decir que por un lado creamos la cuenta con un comando que es new AD service account y después añadimos esa cuenta cuenta de servicio con el comando add computer service account.

Una vez que tenemos creadas esas dos cuentas, podemos verlas con un comando como por ejemplo get a desarvisaconfilter nos va a mostrar todas las cuentas de servicio y después podemos instalarlas.

Para instalarlas vamos a utilizar el comando installade serviceaccount y el nombre de la cuenta.

Una vez que nosotros tenemos hecho eso, si queremos por ejemplo utilizar esas cuentas, pues podemos probar a utilizar esa cuenta para el servicio web de Microsoft.

En el caso de Microsoft, el servidor web es Internet Information Service IDIS.

Entonces seguiríamos los pasos que tenemos en la diapositiva, iríamos a la parte de Pools de aplicaciones, en la parte de detalles, iríamos a la parte de configuración avanzada y en la parte de configuración avanzada seleccionaríamos la parte de identidad y ahí nosotros lo que haríamos sería la parte de personalizar la cuenta, añadiríamos la cuenta de servicio, siempre terminándola en dólar y después en la cuenta del servidor.

Vamos a ver esto en la parte práctica y lo primero que vamos a hacer, vamos a ir a la parte de herramientas, vamos a ir al módulo de Windows PowerShell para Active Directory, vamos a lanzar este módulo y lo primero que tenemos que hacer es crear esa seleccionamos el comando para crear esa rootkey, nos va a aparecer un identificador asociado a esa rootkey y luego podemos empezar a crear las diferentes aplicaciones y la añadimos como cuenta de servicio.

Ahora vamos a crear otra cuenta que la vamos a llamar webservice y vamos a añadir esa cuenta también como cuenta de servicio.

Y ahora vamos a verificar que esas cuentas de servicio están correctamente creadas.

Vemos que tenemos aquí una cuenta que es la de datos compartidos, la tenemos habilitada, tenemos otra que es la cuenta de webservice.

Vamos a instalar esas cuentas como servicio.

Una vez que tenemos instaladas esas cuentas ya podríamos utilizarlas en los servidores correspondientes.

En este caso vamos a hacerlo desde la misma máquina y por ejemplo podemos ir a la consola de servicios y dentro de la consola de servicios podríamos buscar en este caso el servicio de compartición de datos.

Vamos a la parte de propiedades, vamos a la parte de inicio y aquí seleccionaríamos la cuenta que queremos utilizar.

En este caso buscaríamos la cuenta, daríamos a OK, verificamos que la cuenta termine en el símbolo dólar, eliminaríamos los password porque de esta parte se va a encargar el controlador de dominio de generar y renovar esos passwords y daríamos a OK y nosotros tendríamos funcionando esa cuenta de servicio asociada, Tendríamos esa cuenta de servicio asociada al funcionamiento de este servicio.

También podemos configurarla dentro de Internet Information Service, por ejemplo, vamos a la parte de Tools, nos vamos a la consola de Internet, dentro de la consola nos iríamos a la parte de configuración, vamos a los Pool de aplicaciones, seleccionamos el Pool por defecto, damos a la configuración avanzada y dentro de la parte de configuración, configuración avanzada, vamos a la parte de identidad y seleccionamos que queremos que funcione con esta determinada cuenta.

En este caso ponemos la cuenta, ponemos seguridad, Jabal, webservice que termine en dólar, daríamos OK, daríamos OK y daríamos a OK, Pararíamos el servicio, iniciaríamos el servicio y tendríamos la identidad, tendríamos la identidad de Web Service funcionando en este caso con el pool de aplicaciones de Internet Information Service.

De esta manera nosotros lo que vamos a hacer es que vamos a asociar las cuentas de servicio y esas cuentas de servicio las van a gestionar, las van a configurar los controladores de dominio para que nosotros no tengamos que encargarnos del mantenimiento de estas cuentas.

También podemos trabajar con cuentas de servicio administradas, por ejemplo para los servicios, por ejemplo de Web Application Proxy, Active Directory, Federation Service, ADFS, para los servicios de autenticación de esos de funcionamiento de esas configuraciones o de esos servicios.

Resaltar también que para el correcto funcionamiento de las cuentas de servicio en función de la aplicación o el rol que nosotros queramos configurar en esas cuentas de servicio, pues a veces es necesario aplicar configuraciones adicionales.

Por ejemplo, para trabajar con servicios de autenticación mediante Federation Service, es necesario incluir esas cuentas de servicio dentro de una serie de grupos de administración local y dentro de una serie de grupos que permiten a esas cuentas funcionar como servicio, que podemos hacerlo mediante objetos de directiva de grupo.

Si no, puede darse el caso de que en un proceso de reinicio de esa máquina o de reinicio de ese servicio, esa cuenta no pueda arrancar o no pueda iniciarse y nos va a generar un error.

Si verificamos el código de ese error, vamos a ver rápidamente que nos van a aparecer diferentes sitios donde nos van a indicar que esa cuenta tiene que estar incluida dentro de una serie de grupos de administración y de funcionamiento como cuentas de servicio.

Entonces podemos aplicarle esa configuración a esas cuentas de servicio mediante configuraciones, mediante objetos de directiva de grupo, mediante GPOs, que aplicaríamos en el lugar correspondiente para que esas cuentas de servicio tuvieran los privilegios para poder funcionar correctamente dentro de una estructura, por ejemplo, de Federation Server.

Como conclusión, las cuentas de servicio administrados son una opción excelente para mantener la administración de las cuentas de servicio a lo largo del tiempo.

Vamos a delegar el mantenimiento y la renovación de credenciales en los controladores de dominio que van a realizar la tarea de forma periódica y automatizada.

Llegamos al final de la sesión, os esperamos en el siguiente vídeo.