Seguridad Informática

Transcribed on August 7, 2025 at 2:29 PM by Minutes AI

Speaker 1 (00:07)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar el tema de las directivas de configuración de seguridad.

Hemos visto los objetos de directiva de grupo, vamos a ver qué repercusión tienen esos objetos de directiva de grupo en la configuración de seguridad.

Veremos las directivas de configuración de seguridad, cómo podemos importar plantillas de seguridad, vamos a ver las directivas de cuenta, las directivas locales, los derechos de usuario, las directivas de auditoría y las directivas avanzadas de auditoría.

Todo esto con una serie de demostraciones para aprender a tener una soltura en la administración de todos estos dispositivos.

Las plantillas administrativas hacen modificaciones en claves específicas del registro, tanto en la parte del registro del usuario como la parte del registro del equipo en Local Machine o Current User.

Las plantillas administrativas se van a almacenar como un archivo ADMX o en formatos antiguos AEDM en Windows Server 2003 y versiones anteriores.

Y podemos crear un repositorio central de plantillas administrativas.

Es decir, cuando yo abro una configuración de una GPO se va a basar en una serie de plantillas previas que tiene ese dispositivo, en este caso un controlador de dominio.

Cuando yo tengo varios controladores de dominio en el mismo dominio, cada controlador de dominio va a tener sus plantillas administrativas, normalmente van a ser las mismas, pero puede darse el caso de que alguien descargue o añada plantillas administrativas adicionales, y si lo haces solo en un controlador de dominio, estarían específicamente en ese controlador de dominio.

Entonces esas configuraciones sólo se podrían hacer desde ese controlador de dominio.

Cuando yo en un dominio tengo varios controladores de dominio, lo normal es hacer un repositorio central para las plantillas administrativas y tenemos que hacerlo de forma manual.

Para eso hay que definir una carpeta, para eso hay que definir una carpeta en recursos compartidos con la ruta que tenéis en la diapositiva, por ejemplo BAR, el nombre de dominio SYSWOL, el nombre del dominio póisis.

Automáticamente todos los controladores de dominio que hay en ese dominio van a detectar ese repositorio central para las plantillas administrativas y lo van a utilizar.

Las plantillas administrativas también pueden ser administradas o importadas mediante SCDI.

EXE, mediante la consola de administración de directivas de grupo o mediante Security Complianied Manager.

Dentro de las directivas vamos a tener una serie de directivas específicas de seguridad.

Estas directivas nos van a permitir generar una línea base de seguridad que nos va a ayudar en el proceso de fortificación de la infraestructura.

Entre las directivas de seguridad que tenemos tenemos las directivas de cuenta, las directivas locales, los grupos restringidos, sistemas y servicios, parte del registro, sistemas de archivos, la parte para la administración de directivas de red, la parte por supuesto para configurar todo lo que es la seguridad del software anti malware de Microsoft.

Tendríamos también en directivas para las redes inalámbricas, para las claves públicas de los certificados, para la restricción de software, para el control de aplicaciones que viene a ser más o menos lo mismo que el restricción de software y después tendríamos unas específicas para la configuración de directivas de auditoría avanzzaal.

Es posible importar configuraciones de seguridad mediante plantillas administrativas.

Para eso tenemos que seguir el procedimiento que tenemos en la diapositiva en la consola de administración de directivas de grupo crearíamos un FPO, daríamos a editar la directiva y luego en el editor, en la ruta que tenéis en la diapositiva dentro de configuraciones de seguridad, daríamos botón derecho y seleccionaríamos la opción de importar directiva.

Entonces podemos importar un archivo con una serie de plantillas de seguridad específica.

Microsoft tiene publicadas diferentes plantillas para diferentes escenarios, para securizar estructuras de fileover, cluster de Active Directory, de servidores web.

Las primeras directivas que vamos a ver en lo que se refiere a la parte de seguridad son las directivas de control de cuenta.

Las directivas de control de cuenta nos van a permitir configurar tanto lo que es la parte de contraseña, como lo que es la parte de los tickets TGT de Kerberos, como lo que sería toda la parte de bloqueo de cuenta.

Desde Server Manager nos vamos a ir a la parte de Tools, nos vamos a ir a la consola de administración de directivas y vamos a editar la de Folgo MD Policy, damos a editar, vamos a la parte de equipo, dentro de la parte de equipo nos vamos a la parte de directivas, nos vamos a la parte de configuración de Windows y dentro de la parte de configuración de Windows vamos a tener la parte de configuración de seguridad.

Aquí vamos a tener las directivas relacionadas con todos aquellos elementos de seguridad, certificados digitales, el firewall de windowswsdows, Defender, Etcéter, etc.

Si nos vamos a la parte de directivas de cuenta.

Dentro de la parte de directivas de cuenta vamos a tener tres categorías.

La primera categoría es la directiva de contraseñas, aquí es donde nosotros vamos a poder definir las contraseñas para todo el dominio.

Es importante recordar que las directivas de contraseñas sólo se pueden definir en la defauldo mind POLICY y que van a ser únicas para toda la estructura del domio.

Igual que yo puedo tener configuraciones para otras cosas, para el firewall o para Windo Defender o para el control de cuentas de usuario y puedo hacer diferentes gpos y puedo enlazarlas en diferentes unidades organizativas para que unas unidades organizativas tengan una configuración del control de cuenta de usuarios y otras tengan otra configuración diferente.

En lo que se refiere a la parte de configuración de contraseñas se definen para todo el dominio en la defdo mind policy.

Si luego yo quiero que un determinado grupo de usuarios tenga una directiva de contraseñas distinta, tengo una configuración diferente para el password, lo voy a hacer con otro objeto que no tiene nada que ver con las GPOs, que son las PSSOO, son los objetos de password que vamos a ver posteriormente cómo se configuran o en otros vídeos vamos a ver cómo se definen estas características, pero no tienen nada que ver con las configuraciones VROS objetos de dirección.

Entonces cuando vamos a definir en una organización los password lo vamos a hacer aquíuerdo MD POLICY y aquí podemos decidir el histórico de password, es decir, cuántos passwords se van a recordar, sí que se pueden repetir, vamos a ver la vigencia de ese password, vamos a ver características como por ejemplo que el password deja requerimiento de complejidad, si nosotros queremos habilitar una directiva, pues la dejamos en habilitado, o si está deshabilitada la ponemos inhailitado, o si queremos deshabilitarla pues simplemente la marcamos aquí y dejaría de estar activa esa directiva.

Si queremos que esa configuración no se pueda habilitar, entonces la pondríamos en nuestra web de deshabilitar.

Nosotros vamos a tener la explicación de qué es lo que hace cualquiera de las configuraciones mediante una GPO, entonces simplemente nos iríamos a la parte de la explicación y nosotros aquí podríamos ver lo que Microsoft entiende por un requerimiento de complejidad de password, que quiere decir que tenga al menos 6 caracteres, que no tenga coincidencia con el nombre de usuario, que entre mayúsculas, minúsculas, números y caracteres especiales tiene que estar compuesto de tres de esos cuatro elementos etcter.

Otro elemento que tenemos en la parte de directivas de cuenta son los bloqueos.

Los bloqueos de cuenta va a ser la configuración del número de intentos que tiene un usuario para poder iniciar sesión antes de que se bloquee la cuenta.

Yo lo pongo en 5.

Si el usuario se equivoca 6 veces a la hora de introducir la contraseña se va a bloquear la cuenta por un determinado periodo de tiempo o incluso podríamos hacer que se la tuviera que desbloquear manualmente un administrador.

Es una configuración que viene por defecto deshabilitada.

Si os fijáis en esta máquina virtual que está creada tenemos esto sin definir y es una configuración muy interesante porque Si yo dejo 5 intentos y bloqueo la cuenta por un periodo de 3 minutos, para el usuario no va a ser ningún perjuicio.

Un trabajador que se equivoca cinco veces a la hora de introducir la contraseña y luego Tiene que esperar 3 minutos, si sabe que funciona de esa manera, espera 3 minutos y luego puede volver a iniciarse si 1 y vuelva a tener otros 5 intentos.

Sin embargo, si alguien está haciendo un ataque de fuerza bruta sobre esa identidad, le voy a obligar a probar cinco contraseñas cada tres minutos, en vez de utilizar un software que puede probar 10.000 contraseñas en un minuto, pues va a poder probar 5 combinaciones, espero 3 minutos, 5 combinaciones, Espero 3 minutos.

Esto hace o dificulta que los ataques de fuerza bruta contra las identidades sean mucho más dificultosos.

Y luego tendríamos la configuración de Kerberos, los tickets TGT, que son esos tickets que el controlador de dominio le entrega al usuario cuando éste hace un proceso de autenticación y después son los que se utilizan para comprobar si tenemos derecho acceder a los diferentes recursos.

Entonces la configuración del tiempo y los valores de los ticks de Kervelos la haríamos aquí.

Tenemos otras categorías que están relacionadas directamente como el uso de las cuentas, también con la gestión de cuentas, que son las directivas locales.

Las directivas locales van a tener tres secciones diferenciadas, uno lo que sería la parte de directivas de auditoría, lo que sería la parte de derechos de usuario y lo que sería la parte de opciones de seguridad.

Todas estas directivas tienen una especial importancia en la administración de seguridad de una infraestructura y son muy importantes para algunas configuraciones de seguridad dentro de Active Director.

Por ejemplo, administrar la cuenta del administrador de dominio o cambiar el nombre de esa cuenta, pues puede ayudarnos a proteger la identidad del administrador de dominio, que es un recurso crítico dentro de la organización.

Los derechos de usuario son aquellos privilegios que tienen un usuario simplemente por el mero hecho de serie.

Por ejemplo, en la configuración que nosotros tenemos por defecto, un usuario sin privilegios, un usuario estándar, es capaz de unir un equipo al dominio.

Si nosotros no queremos que cualquier usuario pueda unir equipos al dominio, que se generen esas cuentas de equipo en el dominio, tenemos que limitarlo a través de la configuración de derechos de usuario a través de objetos de directiva de grupo.

Por ejemplo, algunos ejemplos de derecho de usuario es unir un equipo al dominio, iniciar sesión localmente, conectarse por escritorio remoto, cambiar la OBA del sistema, realizar en operaciones de backcaup de archivos o directorios o apagar un i.

Como podéis ver algunas de estas opciones es muy interesante que en ciertas partes de la organización estén desactivadas, que un usuario no pueda hacer eso.

Por ejemplo, si yo tengo una unidad organizativa donde tengo dos servidores, pues a lo mejor no me interesa que un usuarioidenntes tenga la capacidad de ap paar un servidor, que tenga que ser un usuario determinado, que tenga determinados privilegios, que sea capaz por tenga la capacidad de poder apagar los servidores.

Luego tenemos las opciones de seguridad.

Las opciones de seguridad son una serie de configuraciones básicas con elementos que pueden tener un impacto grave en la seguridad del entorno de Active Directo.

Algunas opciones por ejemplo son relacionadas con el nombre de las cuentas de usuario, con los dispositivos extraíbles, instalación de drwivers o con el control de cuentas de usuario.

Por ejemplo, no mostrar el nombre del último usuario que inició sesión, o que el usuario pueda cambiar el password antes de que éste expire, o renombrar la cuenta de administrador de tal forma que si luego alguien quiere hacer un ataque sobre la cuenta de administrador, no sólo tiene que conocer la contraseña, sino que para empezar tiene que conocer el nombre o el alias que le hemos dado a esa cuenta administra.

Finalmente en esta categoría tenemos las directivas de auditoría.

Las directivas de auditoría nos van a permitir habilitar una serie de registros que se van a generar en un momento determinado, por ejemplo a la hora de iniciar sesión un usuario o por ejemplo a la hora de acceder a un determinado objeto, por ejemplo una carpeta o un archiv.

Dentro de las opciones de auditoría, en las últimas versiones de Microsoft del sistema operativo Windows, se generaron unas directivas de auditoría avanzadas que son más específicas que las directivas de auditoría convencionales.

Cuando nosotros utilizamos estas directivas de auditoría avanzada se van a generar registros más específicos, es decir, cuando yo habilito en auditoría de inicio de sesión se me van a disparar varios registros y se van a generar en varios registros que puedo tener o que puedo ver en el visor de eventos.

Con las directivas de auditoría avanzada puedo ser más específico en qué tipo de registros sobre el inicio de sesión de un usuario quiero que se genere.

Esto va a hacer que tenga menos impacto en el sistema y ser mucho más específico a la hora de generar registros.

El problema que tenemos con las directivas de auditorio avanzada es que que no son compatibles con las directivas convencionales de auditoría.

Entonces cuando vamos a utilizar estas últimas, las directivas de auditoría avanzada, tenemos que realizar los pasos que vemos en la diapositiva.

Tenemos que configurar dentro de las directivas de configuración en directivas locales las opciones de seguridad y tenemos que configurar audit con la opción que tenéis en la diapositiva Forte AU policiy category settings Tober right AU policy category settings Dentro de las directivas de seguridad tenemos las directivas locales que van a tener tres categorías.

Si vamos a la parte de derechos de usuario, nosotros vamos a tener aquí el listado de aquellos elementos que van a tener disponibles un usuario, todas las operaciones que un usuario va a poder hacer.

Tener en cuenta que la mayor parte de estas directivas no vienen definidas, esto quiere decir que el usuario en principio va a poder realizar esa función.

Entonces por ejemplo vemos que un usuario puede cambiar la hora del sistema, vemos que un usuario puede crear un objeto tipo token o enlace simbólico, puede hacerteun de programas, podemos habilitar la directiva para denegar que inicie sesión una cuenta de un usuario como servicio o denegar para que inicies sesión de forma local.

Tendríamos también procesos de autenticación en lo que se refiere a la fortificación de los procesos de autenticación y el manejo de tokens.

Tendríamos también la posibilidad de configurar quién puede cargar drivers de dispositivo.

Entonces si cualquiera de estas nosotros venimos aquí a definirla, vendríamos aquí a definirla, seleccionaríamos aquí qué usuarios o qué grupos van a poder realizar esas tareas y de esta manera nosotros vamos a controlar quién puede realizar esas funciones específicamente pues esos usuarios o esos grupos que nosotros vamos a definir aquí.

Si queremos saber qué es exactamente lo que hace esa configuración, igualmente que las directivas que vimos anteriormente, nos vamos a la parte de explicación y vamos a tener aquí información detallada de qué es lo que hace específicamente esa directiva.

Lo siguiente que tendríamos que revisar serían las opciones de seguridad.

Dentro de las opciones de seguridad vamos a tener lass divididas por categoría, lo que sería la parte de cuentas, por ejemplo el estatus de la cuenta de administrador, renombrar la cuenta de invitado, renombrar la cuenta de entonces todos estos elementos nosotros vendríamos aquí, vendríamos a definirlos y definiríamos pues el valor correspondiente para esta configuración.

Si tenemos dudas nos vamos a la parte de explicación y vemos lo que quiere o para lo que sirve esa directiva.

Veis que tenemos una serie de directivas relacionadas con los inicios de sesión, la pertenencia al doc domio en la parte de red, acceso a la red, seguridad de red y después tenemos una serie de directivas también que nos pueden servir para los objetos de sistema y la configuración del control de cuentas de usuario.

De tal forma que nosotros podemos hacer mediante configuraciones de GPO una configuración para el control de cutas de ##uario que sea mucho más potente, que esté mucho más personalizada y sea mucho más fuerte, mucho más estricta para el tema de seguridad y luego desplegarla en todo el dominio o desplegarla en una parte del dominio donde por ejemplo haya una serie de equipos críticos, bien porque sean servidores, bien porque los estemos utilizando pues usuarios con privilegios o usuarios que tienen hacer esa información confidencial.

Otro elemento que nosotros debemos tener en cuenta son las políticas de auditoría, cuando nosotros vimos la parte del visor de eventos, en el visor de eventos nosotros vamos a ver una serie de registros, pero no están todos los registros que el sistema operativo puede crear, lógicamente si el sistema operativo generará todos los registros tendría un impacto en la carga de trabajo que sería muy grande, entonces no tiene ninguna lógica cuando nosotros queremos que ciertos registros se generen en lo que se refiere a la parte de seguridad, como por ejemplo lo que sería la parte de los eventos de inicio de sesión, pues nosotros simplemente vamos aquí y definimos esta directiva.

Cuando nosotros definimos estas directivas podemos definir el éxito, podemos definir el fallo o podemos definir ambas cosas.

¿Qué es el éxito o qué es el fallo?

Cuando yo estoy auditando el éxito es cuando un usuario quiere iniciar sesión e inicia sesión correctamente.

Voy a tener un registro en el visor de eventos que demuestra que un día a una determinada hora el usuario X inició sesión en tal equipo.

Cuando yo estoy auditando el fallo es cuando alguien trata de iniciar sesión y se equivoca en la contraseña.

Para finalizar podemos ver que mediante los objetos de directiva de grupo nosotros vamos a tener una serie de herramientas que nos van a servir para la configuración de diferentes elementos dentro de una organización, pero además tienen especial incidencia en lo que se refiere a la parte de seguridad.

Tenemos unas configuraciones específicas dentro de las GPOs para la parte de seguridad.

Muchas de las tecnologías que en Microsoft va incorporando de seguridad a las versiones nuevas del sistema operativo se despliegan mediante objetos de directiva de group.

Entonces es importante entender cómo funcionan correctamente los objetos de directiva de grupo para poder desplegar estas nuevas tecnologías de seguridad.

En la propuesta de ejercicio se os va a pedir que configuréis una directiva de bloqueo de cuenta que veis que vienen sin configurar por defecto, de tal forma que dejemos 5 intentos al usuario y bloqueemos la cuenta por un periodo de 30 minutos.

Después vamos a configurar las auditorías de inicio de sesión y vamos a configurar las auditorías de acceso a objetos y después vamos a verificar en el visor de eventos como esas auditorías nos van a generar los registros.

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

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar el tema de la resolución del ejercicio del vídeo anterior en el que se pedía configurar mediante objetos de directiva del grupo las opciones de seguridad de bloqueo de cuenta y después las opciones de auditoría de los inicios de sesión ylaceso a objetos.

Posteriormente vamos a verificar cómo se generan los registros y podemos verlos en el visor de eventos desde Server Manager nos vamos a la parte de Tools, nos vamos a la consolada administración de dirección de grupo y en la consola de administración de directivas del grupo vamos editar the worder my policy y nos vamos a la parte de directivas, nos vamos a la parte de configuración de Windows, nos vamos a la parte configuración de seguridad y nos vamos a la parte de directivas de cuenta.

Dentro de la parte de directiva de cuenta nos vamos a la parte de directivas del bloqueo de cuenta y nosotros lo que vamos a definir aquí es el número de intentos que vamos a permitir, habíamos dicho 5 intentos, damos OK y automáticamente nos va a definir las otras dos directivas, es decir que después de cinco intentos nos va a bloquear la cuenta por un periodo de 30 minutos, nosotros podemos definir esto y podemos decidir que el bloqueo sea por un periodo de 3 minut entonces vamos a evitar estos valores, lo vamos a poner en el periodo que nosotros queremos y ya tendríamos configurado este element, esto nos va a ayudar a evitar o a dificultar los ataques de fuerza bruta con ciertas técnicas sobre las identidades que tenemos en el domin Después nos vamos a la parte de directivas locales, vamos a la parte de directivas de auditoría y vamos a habilitar tanto el éxito como el fallo de las auditorías de inicio de sesión y de acceso a objetos.

Vamos a seleccionar todas las auditorías y las vamos a tener aquí marcadas.

Bueno una vez que hemos definido las configuraciones en la GPO que queríamos definir, podemos cerrar esta parte y ahora lo que voy a hacer es crear una carpeta aquí en el escritorio, esta carpeta va a ser la carpeta confidencial y vamos a generar una serie de documentos en la carpeta y lo que vamos a hacer es que vamos a habilitar la auditoría de acceso objetos de esta carpeta, Nos vamos a la parte de propiedades, a la parte de propiedades nos vamos a la parte de seguridad, nos vamos a la parte de avanzado y dentro de la parte de avanzado nos vamos la parte de auditoría y vamos a dar a añadir, seleccionamos los usuaruarios que queremos, en este caso vamos a poner todos los usuarios autenticados, damos OK y vamos a seleccionar en este caso los procesos de o los permisos que vamos a aplicar OK y damos OK.

Vamos a asegurarnos de que se aplican las configuraciones y para ello vamos a abrir una consola y vamos a aplicar el comando GPU da párrafos, vemos que va a actualizar las configuraciones de directivas de grupo y una vez que finalice el proceso de actualización de estas directivas, vamos a reiniciar el equipo para asegurarnos que se vaga a aplicar.

Una vez que el equipo reinicia, vamos a introducir la clave de forma incorrecta a propósito un par de veces, vamos a minimizar Server Manager en la carpeta en la que estamos auditando, vamos a acceder a la carpeta, vamos a acceder al documento, vamos a hacer cambios en el documento y ahora nuevamente desde Server Manager nos vamos a ir a la parte de Tools, nos vamos a ir a la parte del visor de eventos y en la parte del visor de eventos nos vamos a ir a la parte de seguridad.

Ahora dentro de la parte de seguridad vamos a ver que se han creado los registros correspondientes.

Vemos que tenemos aquí los registros de auditoría relacionados con el sistema de archivos.

Tenemos aquí tanto el éxito como los errores en el manejo del objeto que estamos auditando y después tendríamos que tener también información en lo que corresponde con la parte del inicio de sesión.

Vemos que aquí estaría el sistema de archivos, que son los registros más recientes y aquí tenemos los registros relacionados con el inicio de sesión.

Vemos que tenemos aquí el fallo del intento de inicio de sesión, la petición de queberos, la parte del intento fallido de ese inicio de sesión y si nos vamos a la parte de detalles, vemos que es respecto a la cuenta de administrador, de tal manera que sabemos los datos relacionados con ese determinado evento.

Entonces tendríamos ahí aquellos datos relacionados con este registro de un intento de inicio de sesión fallir.

Si nosotros vamos aquí a la parte de anclar una tarea a este registro, que sabemos que es el registro 4771, podemos seleccionar que cuando se genere este registro nos envíe un correo, de tal forma que cuando el administrador de dominio alguien trata de iniciar sesión y lo hace de forma incorrecta, pues nos va a enviar un correo.

Si nosotros recibimos dos correos, pues es que algún administrador del dominio se ha equivocado a la hora de introducir el password.

Sin embargo, si empezamos a recibir 15 correos, podemos entender que alguien está tratando de acceder a la cuenta de administrador de dominio y que no tiene esas credenciales.

Después tendríamos en la parte de arriba el éxito de ese inicio de sesión, en este caso con la cuenta de administrador del dominio y lo tendríamos registrado aquí.

De la misma manera, como podemos ver, los objetos de directiva de grupo nos permiten configuraciones específicas de seguridad que pueden marcar una diferencia en la línea base del proceso de fortificación de la estructura de una organización, especialmente en todo lo que se refiere a la administración de Active Directo.

Llegamos al final de la sesión.

Os esperamos en el siguiente V.