Administración de GPO

Transcribed on August 7, 2025 at 12:28 PM by Minutes AI

Speaker 1 (00:04)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar el tema de los objetos de directiva de grupo.

Vamos a hablar de los objetos de directiva de grupo, hablaremos cómo vamos a poder configurar tanto la parte de equipo como la parte de usuario, vamos a profundizar en el conocimiento de cómo funcionan realmente las configuraciones mediante directivas de grupo, hablaremos de la herencia, que es un elemento muy importante en las GPOs y veremos también cómo podemos generar informes de la actividad de las configuraciones mediante GPIO.

Los objetos de directiva de grupo van a centralizar la administración de la infraestructura de una organización y vamos a poder aplicarlas a través de sitio, a través de dominio o a través de unidades organizativas.

Es decir, nosotros vamos a hacer unas configuraciones, esas configuraciones van a estar dentro de la GPO y luego esa GPO la vamos a poder enlazar a una unidad organizativa, la podemos enlazar a nivel de dominio, a que les aplique a todo el dominio y la podemos enlazar también a un sitio donde tengamos, por ejemplo, varios zones.

El elemento más básico de un objeto de directiva de grupo es una configuración individual que va a definir una configuración específica.

Es decir, yo puedo tener una GPO que simplemente configure el fondo de escritorio o puedo tener una GPO que configure varios aspectos.

Puedo tener una GPO que configure el firewall, la configuración de la VPN, la configuración del adaptador de red.

Esos elementos pueden ser elementos que tengan que ver, es decir, de la parte de red o pueden ser diferentes elementos.

Puedo tener, por ejemplo, una GPO inicial que se utilice para configurar aquellos equipos que entran en el dominio y le aplique configuraciones en diferentes categorías.

Vamos a tener dos tipos de configuraciones disponibles, dos familias de configuraciones disponibleS en las GPOs, que serían las directivas para usuario, que van a configurar un usuario o las directivas para equipo.

Cuando nosotros aplicamos directivas a un usuario se van a aplicar a ese usuario independientemente del equipo donde inicie sesión.

Cuando nosotros aplicamos directivas a un equipo se van a aplicar las configuraciones a ese dispositivo independientemente de quién inicie sesión.

Las plantillas administrativas, que es el esquema de todas las posibles configuraciones que tenemos en las GPOs.

Es decir, yo en una GPO voy a tener todas las configuraciones disponibles y voy a activar dentro de esas configuraciones las que yo quiera utilizar.

Entonces, estas plantillas administrativas pueden tener tres el estado de no configurado, el estado de habilitado, es decir, que voy a utilizar esa característica, o el estado de deshabilitado, es decir, que voy a evitar que se utilice esa característica.

Esa característica.

Para poder administrar los objetos de directiva de grupo en Active Directory tenemos el Administrador de Directivas de grupo.

Para poder editar cada una de las GPOs, nosotros tenemos el editor de administrativas de directiva de grupo.

Las configuraciones que nosotros hacemos a través de GPOs se van a aplicar a intervalos regulares entre 90 y 120 minutos.

Se aplican también en el proceso de reinicio del equipo o de arranque del equipo, las configuraciones de equipo y cuando se inicia sesión, las configuraciones de usuario.

Por eso, cuando nosotros unimos un equipo al dominio, es necesario que ese equipo se reinicie para que, por ejemplo, entre otras cosas, se les apliquen las configuraciones de objetos de directiva de voz.

Vamos a tener dos categorías dentro de las configuraciones de directivas, que va a ser la parte de directivas y la parte de preferencias.

A su vez, cada una de estas categorías tiene otras categorías para ayudarnos a clasificar las posibles configuraciones.

En la parte de Directivas tendremos configuración de software, Configuración de Windows o Plantillas administrativas.

En la parte de Preferencias tendremos Configuración de Windows o la configuración del Panel de Control.

Es importante distinguir que hay una diferencia entre las directivas y las preferencias.

Las directivas son impositivas, es decir, cuando yo aplico directivas, esas directivas normalmente no las va a poder cambiar el usuario.

Cuando yo, por ejemplo, configuro el firewall, pues si el usuario luego trata de configurar el firewall, va a tener deshabilitados los paneles de control o al pulsar le va a aparecer un mensaje diciendo que esta característica está configurada a nivel de empresa.

Sin embargo, las preferencias, aunque podemos desplegarlas de la misma manera que las directivas, sí que puede cambiarlas posteriormente el usuario.

Entonces, normalmente en preferencias vamos a tener un conjunto de configuraciones habituales que es muy cómodo desplegar utilizando la estructura de objetos de directiva de grupo, pero que no van a ser impositivas.

Van a ser impositivas.

Una vez que estamos en Server Manager, si nos vamos a la parte de Tools, nos Vamos a la parte de Administrador de directivas de grupo y dentro del administrador de directivas de grupo nosotros ya tenemos siempre por defecto configuradas dos directivas.

Tenemos una directiva que es Default Domain Policy que se va a aplicar a toda la estructura del directorio activo, es decir, que se va a aplicar esas configuraciones a todos los elementos del dominio.

Y tenemos otra configuración que es Default Domain Controllers Policy.

Esta directiva se aplica a los equipos que son controladores de dominio.

Hemos visto que cuando yo promuevo un servidor a controlador de dominio, sale la cuenta de equipo del contenedor de Computers y se pone la unidad organizativa de controladores de dominio, automáticamente se le aplica las directivas de Default Domain Controllers Policy.

Entre ellas yo puedo iniciar sesión con un usuario sin privilegios en cualquier servidor, en cualquier equipo del dominio, en la configuración que hay por defecto y sin embargo no puedo iniciar sesión en un controlador de dominio y es precisamente porque lo que sucede es eso, Si nosotros nos vamos a ver la configuración de Default Domain Policy, nos vamos a la parte de Settings y vamos a ver la información que tenemos de todas las configuraciones que se aplican a través de esa directiva.

Como podéis ver, aparte de las directivas de cuenta, es decir, las directivas de contraseña y del ticket de Kerberos, en la Default Domain Policy apenas hay configuraciones.

Sin embargo, si nos vamos a Default Domain Controllers Policy y vamos a ver las configuraciones que se aplica, vemos que en este caso sí que se aplica una serie de configuraciones adicionales por estar en la unidad organizativa de Domain Control.

Todos los objetos de directiva de grupo que nosotros tengamos los vamos a tener aquí, es decir, tenemos un contenedor donde se almacenan estas gpos, Si yo selecciono el contenedor y doy a nuevo, puedo crear mi propia GPO, vamos a crear una GPO que se llama Firewall y esta GPO nosotros vamos a poder enlazarla en cualquier sitio que nosotros queramos, siempre y cuando sea o bien a nivel de dominio, a nivel de sitio o a nivel de unidad organizativa.

Recordar que aquí no aparece ni el contenedor de Computers ni el contenedor de Users, no podemos enlazar a ese tipo de contenedores.

Configuraciones mediante GPO Si yo doy botón derecho encima del dominio puedo enlazar una directiva y aquí aparecería la directiva de Firewall.

Sin embargo en una unidad organizativa puedo enlazar también la directiva y esta directiva no solo puedo enlazarla dentro de esa unidad organizativa, sino que además la puedo volver a emplear.

Es decir, si quiero aplicar estas configuraciones también a todos los equipos o a todos los usuarios que estén en esta GPO, pues simplemente vuelvo a enlazarla y de esta manera puedo reutilizar toda esa configuración.

Esto me da mucha potencia a la hora de hacer configuraciones, porque yo configuro una única vez el firewall en la GPO y después la aplico, perdón, a una unidad organizativa donde yo tengo 100 equipos y se va a aplicar esa configuración directamente a esos 100 equipos.

Pero es todavía mucho más potente, porque si yo después quiero esa misma configuración aplicarla a una nueva sucursal que está en otra ubicación, en otra unidad organizativa, simplemente la enlazo y automáticamente se le aplica toda esa configuración.

Si yo elimino la directiva, la directiva, yo puedo eliminar el enlace y va a permanecer ahí aunque va a dejar de tener efecto y va a permanecer ahí aunque va a dejar de tener efecto, o puedo eliminar la propia directiva, voy a borrar y borro esa GPO.

En ese caso la GPO no desaparece, es decir, deja de funcionar, deja de estar enlazada con ese contenedor, con esa brigada organizativa, pero sigo teniéndola en los demás sitios y sigo teniendo aquí ese objeto.

Si yo lo borro aquí en el contenedor de objetos de directiva de grupo, entonces sí que elimino la GPO.

Esta GPO que yo tengo aquí enlazada en la unidad organizativa de Boston, realmente no tiene ninguna configuración.

Si yo quisiera que tuviera alguna configuración tendría que editarla.

Entonces voy a editarla y aquí es donde yo voy a tener las plantillas administrativas.

Las plantillas administrativas que vemos que se dividen en dos categorías, la categoría de configuración de equipo y la categoría de configuración de usuario.

Vamos a tener directivas que están en ambas, es decir, vamos a tener las mismas configuraciones que se pueden aplicar a través de usuario y a través de equipo, y nosotros podemos hacer configuraciones dentro de una misma GPO en la que haya parte de configuraciones que estén en la parte de configuración de equipo y otras en la parte de configuración de usuario.

No hay ningún inconveniente dentro de las categorías vamos a tener directivas y vamos a tener preferencias.

Recordad que las preferencias no son impositivas y las directivas sí que son impositivas, son obligatorias.

Tendremos la configuración de software, tendríamos las plantillas administrativas, que dentro de las plantillas administrativas hay todo un mundo de configuraciones, es una cantidad de configuraciones inmensas.

Si abrimos por ejemplo la parte de System, podemos verificar que hay muchísimas configuraciones y luego cada una de estas categorías a su vez dentro tiene varias configuraciones.

Si nos vamos por ejemplo a la parte de componentes de Windows, nos va a suceder lo mismo, tenemos infinidad de configuraciones y dentro de cada una de estas categorías muchísimas configuraciones.

No es necesario memorizar ni saber todas las configuraciones o dónde están todas las configuraciones de objetos de directiva de grupo porque sería una locura, pero sí que es importante que nosotros tengamos una soltura a la hora de navegar, a la hora de desplazarnos por el esquema de configuraciones.

Dentro de la configuración de Windows vamos a tener aquí la configuración de seguridad, que va a ser un poco la que nos interesa en este curso.

Si nosotros nos vamos a la parte de configuración de seguridad, dentro de la parte de configuración de seguridad vamos a tener la configuración del firewall.

Tenemos aquí la configuración del firewall y dentro de la configuración de firewall podemos configurar por ejemplo una regla de entrada.

Generamos una regla de entrada, ejemplo para el protocolo ICMP y PV, vamos a personalizar que sea solo la solicitud de ECO, vamos a permitir que sea solo para el perfil de dominio y ya tendríamos hecha nuestra configuración.

Entonces nosotros ahora tenemos una configuración dentro de esa GPO.

Si nosotros nos vamos a la parte de Settings, vamos a tener aquí que tenemos una determinada configuración para esta GPU.

Por un lado vamos a utilizar el comando gpu day force, que es un comando que va a servir para obligar a aplicar los objetos de directiva de grupo, para obligar a que esas configuraciones se apliquen inmediatamente.

Las configuraciones mediante objetos de directivo de grupo pueden llegar a tardar en aplicarse un tiempo, dos horas, cuatro horas, incluso en algunos casos en entornos muy grandes puede incluso pasar más horas antes de que se aplique.

Normalmente nosotros queremos forzar los objetos de directiva de grupo y podemos hacerlo mediante el comando gpud force.

En algunos casos, a la hora de aplicar configuraciones sobre el equipo es obligatorio el reinicio del equipo para que se apliquen esas configuraciones.

Entonces hay que saberlo, hay que tener cuidado cuando forzamos una aplicación de directivas de grupo porque podemos provocar un reinicio del dispositivo.

Otro comando que nos es muy útil es el comando gpresolve r que va a servir para ver qué configuraciones mediante GPO se están aplicando tanto a nivel de equipo como a nivel de usuario.

Los objetos de directiva de grupo se administran a través de la consola de administración de objetos de directiva de grupo.

Como hemos visto se almacenan en el contenedor de objetos de directiva de grupo que va a contener todos los objetos.

Todas las GPOs van a contener una o más configuraciones.

Vamos a editarlas con el editor de directivas de grupo y después vamos a aplicarlas a un determinado nivel de la estructura del directorio activo.

También podemos utilizar comandos de Windows PowerShell para aplicar o para administrar objetos de directiva de grupo.

Vamos a tener un ámbito que se va a definir en función de una serie de elementos.

Por ejemplo, se va a definir en función de que la GPO esté enlazada a un determinado contenedor.

Se va a definir ese ámbito en función de filtros de seguridad.

Es decir que yo puedo aplicar una GPO a una determinada unidad organizativa, pero en vez de hacer que se aplique a todos los usuarios, puedo poner un grupo de seguridad y que se aplique solo a los usuarios que pertenecen a ese grupo.

Si yo tengo una GPO que configura el firewall y luego tengo otra GPO que configura el firewall, ahí sí se genera un conflicto.

Entonces va a prevalecer la última GPO que se aplica.

Es decir, que se va a aplicar una configuración y la siguiente GPO va a aplicar la otra configuración y va a sobreescribir.

Entonces nosotros el orden de aplicación de las GPOs es a nivel de equipo son las primeras que se aplican y después dentro de la estructura de dominio, a nivel de sitio, a nivel de dominio, a nivel de unidad organizativa y a nivel de unidad organizativa interna.

Cuando yo tengo una unidad organizativa dentro de otra, se aplica la de afuera y luego la de adentro a la que está en el contenedor dentro del otro contenedor.

Es decir que se van a aplicar de lo más general a lo más específico, de lo más grande a lo más pequeño.

Y tiene su lógica, porque si yo defino una configuración para una unidad organizativa, entiendo que eso tiene que prevalecer sobre lo general que tengo configurado para todo el dominio.

Otros elementos que influyen en la aplicación de las GPOs es el orden de enlazado, es decir, en un sitio donde yo tengo varias gpos puedo decidir cuál se aplica primero o cuál se aplica después, si esa GPO es forzosa, es obligatoria, entonces va a prevalecer incluso aunque se bloquee la herencia o podemos bloquear la herencia, que a nivel de unidad organizativa yo puedo decidir que aquellas GPOs que están fuera de la unidad organizativa no me afecten y después si el link está habilitado o no está habilitado.

Como podemos ver es un entorno complejo donde podemos llegar a tener muchas configuraciones y todas estas configuraciones pueden llegar a generar un conflicto y puede llegar un momento en el que no sabemos si un determinado usuario puede iniciar sesión o puede realizar una determinada tarea, o se le va a aplicar una configuración o no se le va a aplicar una configuración en esta estructura de GPOs.

Para ello nosotros tenemos una serie de elementos que nos van a ayudar en la verificación de todos estos resultantes, como puede ser el comando gpresolve que vimos anteriormente, pero también tenemos una serie de asistentes que van a permitirnos ver qué configuraciones se van a aplicar a un determinado usuario y a un determinado equipo, qué configuraciones se están aplicando a un determinado usuario en un determinado equipo.

Para ello tenemos el Group policy resolve, el asistente y tenemos el asistente de Group policy Model.

Aparte tenemos el comando, como hemos visto, gpresult, que nos va a permitir también ver que se está aplicando en un determinado equipo.

Todos estos asistentes nos pueden generar informes que después nosotros vamos a poder ver a través del propio asistente o podemos verlos a través de informes como HTML en la consola de administración de objetos de directiva de grupo.

Nos vamos aquí y vamos a crear una GPO directamente y enlazarla aquí.

Una vez que creamos esa GPO, si nos vamos por ejemplo a una unidad organizativa, dentro de la unidad organizativa nosotros vamos a ver las gpos que tenemos directamente enlazadas.

Podemos seleccionar el orden de qué GPO queremos que se aplique primero y vamos a ver aquí la herencia de esas GPOs, es decir, vamos a ver cómo esas GPOs se aplican dentro de este contenedor.

Si yo por ejemplo aquí desactivo Security, si ahora vuelvo aquí, vemos que desaparece, si yo activo, vuelvo a habilitar el enlace, entonces vuelvo a tenerla aquí aplicándose, yo puedo bloquear la herencia de tal forma que las GPOs que no pertenecen a la unidad organizativa dejan de tener efecto.

Si yo una de estas gpos la pongo como obligatoria, automáticamente no solo elimina o se salta el bloqueo de herencia, sino que además se pone la primera, de tal forma que sabemos que va a prevalecer las configuraciones de esa GPO que nosotros estamos marcando aquí como obligatoria.

Si quitamos este check vuelve a desaparecer y si aquí quitamos el bloqueo de herencia, pues nos vuelven a aparecer todas las configuraciones de todas las GPOs que sean globales, que están fuera de ese contenedor y todas las configuraciones de las GPOs que están directamente enlazadas a este contenedor.

Si yo selecciono cualquier directiva, cualquier GPO, voy a tener la posibilidad de ver el ámbito de esa GPO y aquí voy a poder aplicar filtros de seguridad.

Yo puedo poner aquí que esto se aplique a un determinado grupo, en este caso por ejemplo el grupo auditores y puedo eliminar los usuarios autenticados y de esta manera se aplicaría esa configuración específicamente a ese grupo de seguridad.

Lo mismo me pasaría si yo aplico filtros WMI.

Además nosotros en la parte de detalles podemos también deshabilitar todas las configuraciones, podemos deshabilitar solo las configuraciones de equipo o podemos deshabilitar las configuraciones de usuario o qué configuraciones se le aplica a un usuario cuando inicia sesión en un determinado equipo.

Para eso tenemos el Group Policy Modeling y tenemos el Group Policy Resub.

Si nosotros lanzamos el asistente nos va a guiar durante el proceso de consulta, por ejemplo en este equipo o en otro determinado equipo, en este usuario o podemos seleccionar un usuario específico, daríamos a siguiente y entonces nos va a generar un informe de todas las configuraciones que se van a aplicar mediante GPOs a este usuario o el usuario elegido.

Entonces iríamos a la parte de ver las configuraciones y nosotros vamos a tener aquí un listado con todas las configuraciones que se van a aplicar a este usuario cuando inicia sesión en este equipo.

Como conclusión, hemos visto que tenemos los objetos de directiva de grupo que nos van a permitir hacer una serie de configuraciones que van a ser muy eficientes porque nos permiten, haciendo la configuración una única vez, después aplicarla de forma muy específica o de forma muy general y poder reutilizarla para que se aplique a un amplio número de usuarios o a un amplio número de equipos.

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