UD 07_04 – Administración centralizada de redes con Windows Server 2016
Permisos y directivas de grupo.

(Del curso "Administración centralizada de redes con Windows Server 2016" del profesor Alberto Aparicio Vila)

Contenido

Permisos de recursos compartidos **2**
Acceso a los recursos compartidos 2
Establecer permisos en recursos compartidos 6
Permisos NTFS **9**
Tipos de permisos NTFS 9
Asignación de permisos NTFS 12
Permisos implícitos y permisos explícitos 15
Herencia de permisos 18
Eliminación de herencia del recurso de nivel superior 19
Cambio de los permisos de un objeto hijo 20
Directivas de Grupo (GPO) **22**
Acumulación de directivas de grupo 22
Edición de las directivas de grupo predeterminadas 22
Bloqueo de cuenta al introducir una contraseña 3 veces una contraseña errónea 26
Longitud de la contraseña 28
Historial de contraseñas 30
Vigencia máxima de la contraseña 30
Creación de directivas de grupo 31
Fondo de escritorio obligatorio 32
Bloqueo de la línea de comandos 35
Comprobación de las directivas establecidas 36
Bloqueo de cuenta 36
Longitud de la contraseña 37
Fondo de escritorio obligatorio 37
Bloqueo de la línea de comandos 37
Ficha perfil 38
Carpetas Personales 38
Comandos de inicio de sesión 41
Ejemplos de scripts de inicio de sesión: Asignación de unidad de red 42
Ejemplos de scripts de inicio de sesión: Asignación de unidad de red 44
Actividades tema 4 ..... **44**
Actividad 4.1 44

Permisos de recursos compartidos

Los sistemas operativos de la familia Windows poseen dos niveles de permisos para los recursos compartidos:

- Permisos para carpetas compartidas: se aplican cada vez que un usuario quiere acceder a un archivo o carpeta de la red.
- Permisos para archivos y carpetas (NTFS): se aplican sobre dispositivos con formato NTFS para definir en mayor detalle las acciones permitidas.

De lo anterior se extrae que cuando se accede en modo local a los archivos o carpetas sólo intervienen los permisos asociados al sistema de ficheros, en este caso NTFS, sin embargo, si se accede a través de la red se aplican los dos niveles de permisos: en primer lugar, se aplican los permisos de carpetas compartidas y posteriormente los permisos NTFS.

Permisos NTFS y compartidos

Acceso a los recursos compartidos

Para acceder a la gestión de recursos compartidos, lo podemos hacer a través de la opción servicios de archivo y almacenamiento, desde el Panel del Administrador del Servidor.

Recursos compartidos

Después accedemos a la opción recursos compartidos:

Recursos compartidos

En la parte central de la consola de administración del almacenamiento aparecen los recursos compartidos en el servidor. Para visualizar los permisos de cada recurso compartido, basta con hacer clic con el botón secundario del ratón sobre el recurso cuyos permisos se quieren consultar y se selecciona 'Propiedades':

Propiedades Recursos Compartidos

Veremos que aparece un cuadro de dialogo donde podemos ver en la parte de la izquierda la opción permisos. Y bajo Personalizar Permisos:

Nos aparece después el cuadro de permisos completo del recurso seleccionado:

Recursos compartidos

Si accedemos a la pestaña compartir, podremos ver los permisos del recurso compartido. En este caso, el recurso compartido netlogon tiene los permisos:

Estos pueden ser de tres tipos:

- Control total: no solo permite cambiar y leer, sino modificar los permisos sobre el recurso compartido
- Cambiar: se permite crear carpetas y archivos además de modificar y borrar los archivos y directorios existentes.
- Lectura: únicamente permite la lectura de archivos y la ejecución de archivos ejecutables que se hallen dentro del recurso compartido.

Permisos de NETLOGON

Como se puede comprobar en la siguiente figura, existen dos tipos de directivas: 'Permitir' y 'Denegar'. Es importante destacar que la opción '**Denegar' tiene prioridad sobre otros permisos asignados sobre el recurso compartido**.

Tipos de directivas

Establecer permisos en recursos compartidos

Establecer permisos de recursos compartidos se puede hacer de varias maneras. Probablemente la más sencilla sea seleccionar el recurso sobre el cual se desean configurar los permisos, y haciendo clic con el botón secundario 'Compartir con…' y usuarios específicos. Por ejemplo, vamos a crear una carpeta en C: llamada Empresa_users y la vamos a compartir:

Compartir recursos

Y agregamos el grupo Empresa con lectura y escritura:

Agregar permisos

Agregar Permisos recurso compartido

Agregar Permisos recurso compartido

Por último, accedemos a la pestaña Compartir. En lugar de hacer uso de este asistente, vamos a compartir mediante el **uso compartido avanzado**, que nos da más opciones para asignar los permisos. Para ello, seleccionaremos la carpeta y con el botón de la derecha del ratón propiedades y pestaña compartir:

Uso compartido avanzado

Uso compartido avanzado

En la medida de lo posible, habrá que asignar permisos a grupos y eliminar grupos que no tengan ninguna relación con la carpeta que queremos compartir. Se debe evitar el uso de grupo Todos y en su lugar crearemos los grupos correspondientes.

Permisos NTFS

Como se ha comentado anteriormente, los permisos NTFS complementan y amplían los permisos de recursos compartidos, siendo efectivo el más restrictivo.

Todos los archivos y carpetas de un volumen NTFS tienen asociada una ACL o lista de control de acceso que fija el nivel de acceso de un usuario o grupo que pretenda acceder al recurso. Además, los permisos NTFS pueden ser aplicados a nivel de archivo, a diferencia de los permisos de recursos compartidos, los cuales únicamente pueden aplicarse a nivel de carpeta.

Por otra parte, surge un nuevo concepto al aplicar los permisos NTFS que los hace más complejos, aunque también más potentes: la herencia, la cual determinará los permisos que se reciben sobre un determinado recurso provenientes de un nivel superior, aunque esto lo veremos detalladamente más adelante.

Tipos de permisos NTFS

Tal y como se muestra en la figura siguiente (para abrir ese cuadro de diálogo hacer clic con el botón secundario sobre el recurso compartido y hacer clic en la pestaña 'Seguridad'), los permisos (predeterminados) que pueden aplicarse sobre archivos y carpetas son:

- Control total.
- Cambiar.
- Leer y ejecutar.
- Mostrar el contenido de la carpeta.
- Leer.
- Escribir.

Permisos estándar

No obstante, estos permisos en realidad representan varios aspectos mucho más concretos. Para tratar de clarificar esta cuestión, la tabla 1 resume qué tareas pueden realizarse con cada tipo de permiso.

	Control total	Cambiar	Leer y ejecutar	Mostrar el contenido de la carpeta	Leer	Escribir
Recorrer por carpeta/ejecutar archivo	☑	☑	☑	☑		
Mostrar carpeta/leer datos	☑	☑	☑	☑	☑	
Atributos de lectura	☑	☑	☑	☑	☑	
Atributos extendidos de lectura	☑	☑	☑	☑	☑	
Crear archivos/escribir datos	☑	☑				☑
Crear carpetas/agregar datos	☑	☑				☑
Atributos de escritura	☑	☑				☑
Atributos extendidos de escritura	☑	☑				☑
Eliminar subcarpetas y archivos	☑					
Eliminar	☑	☑				
Permisos de lectura	☑	☑	☑	☑	☑	☑
Cambiar permisos	☑					
Tomar posesión	☑					

Permisos para carpetas y archivos

Para poder acceder a estos permisos especiales, lo haremos a través de las propiedades, pestaña de Seguridad y opciones avanzadas:

Acceso a permisos especiales

Acceso a permisos especiales

Acceso a permisos especiales

Acceso a permisos especiales

Es importante entender que los permisos predeterminados estándar, en realidad corresponden a unas combinaciones de permisos específicos, siendo estos últimos con los que trabajaremos más adelante cuando gestionemos las listas de control de acceso por línea de comandos.

Asignación de permisos NTFS

Al definir un permiso NTFS este puede ser un permiso o una denegación:

Permisos NTFS

Permisos NTFS

Los permisos NTFS son acumulativos: se evalúan los permisos otorgados al usuario y a los grupos a los que pertenece el usuario. En el caso de que haya una incompatibilidad entre los permisos asignados a un usuario y los asignados a un grupo del cual sea miembro, prevalecerá la opción más restrictiva: Denegar (si está definido **explícitamente).**

Para asignar permisos NTFS a un recurso compartido bastará con hacer clic con el botón secundario sobre el recurso y acceder a la pestaña 'Seguridad'. A continuación, pulsaremos el botón 'Opciones Avanzadas', como se muestra a continuación:

Permisos NTFS

Permisos NTFS

Entrada de permiso para Empresa_users
Entidad de seguridad: Seleccionar una entidad de seguridad
Tipo: Permitir
Se aplica a: Esta carpeta, subcarpetas y archivos
Permisos básicos:
Mostrar permisos avanzados
Control total
Modificar
Lectura y ejecución
Mostrar el contenido de la carpeta
Lectura
Escritura
Permisos especiales
Aplicar estos permisos solo a objetos y/o contenedores dentro de este contenedor
Borrar todo
Agregue una condición para limitar el acceso. La entidad de seguridad obtendrá los permisos especificados únicamente si se cumplen las condiciones.
Agregar una condición
Aceptar
Cancelar

Seleccionar Usuario, Equipo, Cuenta de servicio o Grupo
Seleccionar este tipo de objeto:
Usuario, Grupo, o Entidad de seguridad integrada
Tipos de objeto...
Desde esta ubicación:
CEFIRE2017.LOCAL
Ubicaciones...
Escriba el nombre de objeto para seleccionar (ejemplos):
Empresa
Comprobar nombres
Opciones avanzadas...
Aceptar
Cancelar

Entrada de permiso para Empresa_users
Entidad de seguridad: Empresa (CEFIRE2017\Empresa) Seleccionar una entidad de seguridad
Tipo: Permitir
1
Se aplica a: Esta carpeta, subcarpetas y archivos
2
Permisos avanzados:
3
Mostrar permisos básicos
Control total
Atravesar carpeta / ejecutar archivo
Mostrar carpeta / leer datos
Leer atributos
Leer atributos extendidos
Crear archivos / escribir datos
Crear carpetas / anexar datos
Escribir atributos
Escribir atributos extendidos
Eliminar subcarpetas y archivos
Eliminar
Permisos de lectura
Cambiar permisos
Tomar posesión
Aplicar estos permisos solo a objetos y/o contenedores dentro de este contenedor
Borrar todo
Agregue una condición para limitar el acceso. La entidad de seguridad obtendrá los permisos especificados únicamente si se cumplen las condiciones.
Agregar una condición
Aceptar
Cancelar

Grupo Usuarios (del dominio)

Cuidado con el **grupo Usuarios (del dominio)** porque aparece por defecto en los permisos NTFS (con permisos de lectura), y puede provocar que se produzcan accesos diferentes a nuestra planificación. Como norma general, si queremos limitar el acceso a un recurso compartido, eliminaremos el grupo Usuarios de los permisos NTFS y explicitaremos únicamente aquellos grupos o usuarios que efectivamente queramos que tengan acceso al recurso

Permisos implícitos y permisos explícitos

Los permisos otorgados de manera implícita o explícita son una cuestión sencilla, pero si no los modificamos con atención, podemos hacer que los accesos a los recursos no funcionen como teníamos previsto. Para evitar problemas tendremos en cuenta que:

1. Un permiso definido de manera explícita siempre prevalecerá sobre un permiso definido de manera implícita.
2. Denegar un permiso siempre prevalece sobre otorgar ese permiso, siempre y cuando ambos estén definidos de la misma manera (implícita o explícitamente).

¿Cómo se define un permiso de manera explícita? Si nos fijamos en la siguiente figura, el grupo Compras no tiene (aparentemente) definidos permisos de escritura. Sin embargo, esa aparente indefinición, en realidad indica que el permiso de escritura está denegado implícitamente. Si un usuario del grupo Ventas intenta escribir en la carpeta, se producirá un mensaje de error como muestra la siguiente figura:

Permisos explícitos

Error al crear archivo en recurso compartido

Sin embargo, si le otorgamos el permiso explícito de escritura, veremos que efectivamente puede escribir en el recurso, ya que la definición explícita del permiso para escribir prevalece sobre la denegación implícita del permiso escribir:

Permisos de escritura

Permisos de escritura

Si explicitamos la denegación del permiso de escritura para los miembros del grupo Compras, podremos comprobar que efectivamente el usuario usucomp1 no puede escribir en la carpeta:

Denegación explicita

Denegación explícita

Herencia de permisos

Al crear un archivo o carpeta en un volumen NTFS ese objeto hereda automáticamente los permisos de su carpeta contenedora, y a la inversa: cuando asignamos permisos a una carpeta contenedora, los permisos se propagan automáticamente hacia los archivos y subcarpetas contenidas en el recurso.

Sin embargo, pueden darse ocasiones en las que queramos eliminar esa herencia de permisos. Esto puede ejecutarse de tres maneras diferentes:

- Eliminar la herencia a nivel de la carpeta de nivel superior, los objetos contenidos en ella dejan de heredar los permisos.
- Eliminar la herencia a nivel de subcarpeta o archivo contenido dentro del recurso principal.
- Permitir o denegar explícitamente un permiso de manera diferente a como está definido en el recurso contenedor.

¿Qué utilidad práctica puede tener la herencia de permisos?

Fundamentalmente son dos las utilidades principales.

- La primera radica en que el administrador no tiene que asignar manualmente los permisos a los archivos y subcarpetas que haya contenidas dentro del recurso principal, y que fácilmente pueden ser miles.
- Relacionado con este aspecto, también encontramos una segunda utilidad práctica que es el aumento de la seguridad al descartar posibles errores de asignación de permisos realizados manualmente.

Eliminación de herencia del recurso de nivel superior

Para eliminar la herencia de los permisos establecidos en la carpeta de nivel superior, se debe acceder a la ficha 'Seguridad' del cuadro de diálogo 'Permisos' y a continuación se hace clic en 'Opciones Avanzadas' :

Deshabilitar herencia

En este caso vemos que la carpeta c:\pistonazo_users hereda los permisos de la unidad c:\. Para eliminar la herencia, debemos hacer clic en Deshabilitar herencia y nos aparecerá un diálogo para dejar los permisos explícitos o bien para eliminar todos los permisos:

Deshabilitar herencia

Tenemos dos opciones:

- Convertir los permisos heredados en permisos explícitos: mantiene los permisos de todos los archivos y subcarpetas, pero no están vinculados a los del nivel superior.
- Quitar todos los permisos: elimina todos los permisos heredados

Como norma general marcaremos la primera opción, convertir los permisos en permisos explícitos:

Deshabilitar herencia: Permisos explícitos

Cambio de los permisos de un objeto hijo

Si observamos los permisos de un objeto que está heredando permisos, veremos que las casillas de verificación están (completa o parcialmente) inaccesibles. En este caso la carpeta Compras que hereda los permisos de la carpeta Administración, hereda también los permisos del grupo administración:

Herencia de permisos

En primer lugar, podemos interrumpir la herencia, denegando explícitamente los permisos. Si el permiso heredado es de concesión, la denegación está habilitada.

Interrupción de herencia

Para este caso, podemos denegar el permiso heredado de escritura.

Directivas de Grupo (GPO)

Las directivas de grupo (Group Policy) son una serie de configuraciones creadas por el administrador que se aplican a objetos del dominio. Por medio de estas directivas, el administrador controla los entornos de trabajo de los usuarios del dominio, los equipos y el comportamiento de distintos objetos. Son en definitiva un conjunto de reglas que facilitan las labores de administración de los usuarios y equipos.

Algunos de los aspectos más útiles que se pueden definir por parte del administrador mediante las directivas son:

- Los comandos de inicio de sesión.
- Características de las directivas de seguridad de las cuentas de usuario.
- Configuración de la apariencia de la sesión de usuario.
- Redirección del acceso a ciertas carpetas o archivos centralizados Distribución de software a los equipos clientes.
- Permisos otorgados a las cuentas de usuarios y grupos, etc.

Acumulación de directivas de grupo

Al existir diferentes niveles de directivas de grupo, estas pueden entrar en conflicto, haciendo que aparezcan efectos no deseados en la gestión del dominio. Al establecer directivas de grupo hay que tener en cuenta el orden de aplicación de las mismas:

- Directiva de grupo local.
- Directiva de grupo de sitio.
- Directiva de grupo de dominio.
- Directiva de grupo de unidad organizativa.

De manera predeterminada cuando existe una contradicción entre las directivas, la que prevalece será la que está en un nivel inferior de la lista anterior. Obviamente, en caso de no existir contradicciones, se aplican todas las directivas.

Directivas de usuario o equipo

Si queremos saber las directivas que están aplicandose a un usuario o equipo, ejecutaremos rsop.msc:

-->

Cuando se pone en marcha un dominio se crean dos directivas de grupo llamadas:

- Default Domain Controllers.
- Default Domain Policy.

GPOs predefinidos

Estas dos directivas establecen la configuración básica de los objetos del dominio, y están vinculadas respectivamente a:

- La unidad organizativa Domain
- Controllers . El dominio.

Estos dos GPO se componen de un conjunto muy amplio de directivas, como se puede ver al abrir el editor de directivas:

GPOs predeterminadas Default Domain Policy

Supongamos que queremos cambiar la configuración de la directiva que aplica sobre el permiso para apagar el equipo. En ese caso la buscaríamos entre todo el conjunto de directivas dentro del GPO Default Domain Policy y haríamos doble clic sobre ella:

GPO Apagar el sistema

Vemos que la directiva 'Apagar el Sistema' no está habilitada. Si la habilitamos y únicamente otorgamos permiso a los administradores del dominio, podremos comprobar que efectivamente un usuario del dominio que inicia sesión en un equipo cliente no puede apagarlo, solamente podría un usuario con privilegios de administración.

Para evitar generar un tráfico de gestión excesivo en la red, las directivas de grupo no se actualizan inmediatamente tras su modificación, sino que está establecido un intervalo de 5 minutos entre actualizaciones automáticas. No obstante, este intervalo se puede modificar en las propias directivas de grupo. De todas maneras, no es necesario modificar este intervalo para comprobar la correcta aplicación de las directivas de grupo, basta con escribir en la consola cmd el comando gpupdate:

```
Administrador: C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 10.0.14393]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Administrador>gpupdate
Actualizando directiva...

La actualización de la directiva de equipo se completó correctamente.
Se completó correctamente la Actualización de directiva de usuario.


C:\Users\Administrador>
```

gpupdate

Y ahora iniciamos una sesión con un usuario en la máquina cliente y comprobamos que efectivamente no se puede apagar la máquina:

Denegar apagado del sistema

Las tareas más comunes que se realizan con las GPOs son aquellas relativas a las directivas de contraseñas, de inicios de sesión y bloqueos entre otros. Para ejemplificar todo lo anterior vamos a modificar la Default Domain Policy para implementar las siguientes configuraciones en el dominio:

1. Si el usuario se equivoca tres veces al introducir su contraseña, su cuenta queda bloqueada (solo la podrá desbloquear el administrador). Esto protege el sistema de posibles ataques.
2. La contraseña deberá tener un mínimo de 5 caracteres, pero no es necesario obligatoriamente que sean mayúsculas, minúsculas, caracteres alfanuméricos, obligatoriamente, etc.
3. La contraseña que se haya utilizado ya, no podrá volverse a utilizar hasta pasados al menos 10 cambios de contraseña (de esta manera forzamos al usuario a que no 'recicle' contraseñas antiguas, incrementando la seguridad del sistema).
4. El usuario debe cambiar la contraseña cada seis meses, al establecer una 'vida útil' de las contraseñas tenemos un sistema más seguro, ya que en caso de que alguien haya averiguado la contraseña del usuario, y no se haya detectado, como tarde a los seis meses, perderá el acceso a la cuenta.

En las siguientes subsecciones se examina la manera de proceder para llevar a cabo estas configuraciones del sistema.

Bloqueo de cuenta al introducir una contraseña 3 veces una contraseña errónea

En primer lugar editaremos el GPO 'Default Domain Policy' para configurar la directiva de bloqueo de cuenta. Esta se halla en 'Configuración del equipo'→'Directivas'→'Configuración de Windows'→'Directiva de bloqueo de cuenta'→'Umbral de bloqueo de cuenta':

Acceso a GPOs Default Domain Policy

Acceso directiva bloqueo de cuenta

Modificamos la directiva Umbral de bloqueo de cuenta a '3 intentos' de inicio de sesión erróneos:

Umbral de bloqueo de cuenta

Además, configuraremos la duración del bloqueo, donde un valor de 0 indica que la cuenta deberá ser desbloqueada manualmente por el administrador:

Duración de bloqueo de cuenta

Finalmente, también configuraremos el tiempo que debe transcurrir entre intentos para que el contador de fallos de inicio de sesión vuelva a cero antes de que se bloquee la cuenta. Pondremos el máximo valor permitido:

Restablecer el bloqueo

Longitud de la contraseña

Como en el caso anterior editaremos el GPO 'Default Domain Policy' para configurar la longitud y complejidad de las contraseñas:

Directivas de contraseñas

Modificamos el valor de la longitud a 5 caracteres:

Longitud de la contraseña

A continuación, deshabilitamos los requisitos de complejidad de las contraseñas. En la siguiente figura aparecen las características de complejidad que aplica esta directiva cuando está habilitada:

Deshabilitar complejidad de contraseñas

Historial de contraseñas

Editamos de nuevo el GPO 'Default Domain Policy' y accedemos a las directivas de contraseñas:

Historial de contraseñas

Vigencia máxima de la contraseña

Como en casos anteriores accedemos a las directivas de contraseña:

Cambiamos la duración máxima de las contraseñas a 180 días -6 meses-

El resultado de cada una de las directivas de la sección Directivas de contraseñas sería:

Directiva	Configuración de directiva
Almacenar contraseñas con cifrado reversible	Deshabilitada
Exigir historial de contraseñas	10 contraseñas recordadas
La contraseña debe cumplir los requisitos de complejidad	Deshabilitada
Longitud mínima de la contraseña	5 caracteres
Vigencia máxima de la contraseña	180 días
Vigencia mínima de la contraseña	1 días

Directivas de contraseñas

Creación de directivas de grupo

Vamos a modificar ciertas directivas de la organización Pistonazo, para ello accederemos ('Panel del administrador'→'Herramientas administrativas'→'Administración de directivas de grupo').

Supongamos que queremos crear una Directiva de Grupo sobre la unidad organizativa 'Pistonazo' que creamos en el tema anterior. Hacemos clic con el botón secundario y escogemos la opción 'Crear un GPO en este dominio y vincularlo aquí'

Directivas de grupo

Aparecerá el cuadro de diálogo e introduciremos el nombre que le queremos dar, por ejemplo 'Entorno de trabajo', ya que posteriormente utilizaremos esta directiva para configurar un entorno de trabajo homogéneo en todos los usuarios que pertenecen a la Unidad Organizativa 'Pistonazo'.

Nueva GPO

La nueva directiva aparecerá en el panel de detalles:

Nueva GPO

Seleccionamos el GPO y hacemos clic con el botón derecho, escogiendo la opción 'Editar'. Con la nueva directiva vamos a establecer las siguientes configuraciones:

1. Todos los miembros de la unidad organizativa 'Pistonazo' tendrán un fondo de escritorio 'corporativo' que se instalará de manera automática y que no podrá ser modificado.
2. Los miembros de la unidad organizativa 'Trabajadores' no pueden abrir la consola de comandos.

En las siguientes subsecciones se examina la manera de proceder para llevar a cabo estas configuraciones del sistema.

Fondo de escritorio obligatorio

Para modificar de una manera centralizada el fondo de escritorio de los usuarios de la unidad organizativa 'Pistonazo' debemos editar la directiva 'Entorno de Trabajo' y acceder a 'Configuración del usuario'→'Plantillas administrativas'→'Active Desktop'→'Active Desktop'

GPO Pistonazo

Personalizar Active Desktop

Habilitamos el Active Desktop:

Active Desktop

Vamos a impedir también que los usuarios puedan modificar el fondo de escritorio:

No permitir cambios

Indicamos la ruta en la que se halla la imagen que queremos poner como fondo de escritorio. En este caso se llama fondopisto.jpg y hay que añadirla a una carpeta compartida que se encuentre en el servidor. En nuestro caso, la añadiremos a la carpeta Pistonazo:

Tapiz de escritorio

La imagen debe hallarse en una carpeta compartida en red (preferiblemente en el servidor por cuestiones de disponibilidad) donde todos los usuarios del dominio tengan permiso de lectura. Además, se recomienda que la ruta se introduzca en formato UNC del tipo:

\\server 1\gestion\fondocorp.jpg no en formato \\192.168.0.100\gestion\fondocorp.jpg

Bloqueo de la línea de comandos

Para bloquear la línea de comandos editaremos el GPO correspondiente accediendo a 'Configuración del usuario'→'Plantillas administrativas'→'Sistema'

Bloqueo consola

Y habilitamos el bloqueo:

Habilitar el bloqueo

Comprobación de las directivas establecidas

Ahora comprobaremos que las directivas se han aplicado correctamente. Para ello utilizaremos un usuario cualquiera dentro de la unidad organizativa 'Pistonazo' que es sobre la que se aplican el GPO creado 'Entorno de Trabajo', y obviamente el GPO Default Domain Policy, que hemos editado.

Bloqueo de cuenta

La primera directiva que hemos aplicado consistía en bloquear la cuenta indefinidamente al introducir en tres ocasiones la contraseña incorrectamente. Nos equivocamos voluntariamente al iniciar sesión en un equipo cliente y la cuenta se acaba bloqueando. Por ejemplo, vamos a iniciar sesión con usuario usucomp1 e introduciremos 3 veces de manera incorrecta la contraseña:

Cuenta usucomp1 bloqueada

Comprobamos en el controlador de dominio que efectivamente está bloqueada y la desbloqueamos:

Cuenta bloqueada.

Longitud de la contraseña

Para comprobar la longitud de la contraseña, vamos a cambiar la contraseña del usuario usucomp1 y vamos a poner una contraseña que tenga 5 caracteres, por ejemplo 12345.

Restablecer contraseña

Así también hemos visto que podemos introducir una contraseña sin requisitos de complejidad.

Fondo de escritorio obligatorio

Al iniciar sesión se carga el fondo de escritorio definido con la directiva de grupo, y además el usuario no puede modificarlo. Por ejemplo, iniciamos sesión con el usuario usucomp2:

Bloqueo de la línea de comandos

Una vez iniciada la sesión, si se intenta ejecutar cmd aparece el siguiente mensaje:

Acceso a cmd

Ficha perfil

Carpetas Personales

Una de las opciones más utilizadas que puede configurarse en la ficha 'Perfiles' de las propiedades de la cuenta de usuario es el establecimiento de una unidad en red personal para cada usuario a la que únicamente él tiene acceso:

Carpeta particular

Para configurarla, basta crear una carpeta a la que se tenga acceso desde la red. Esta carpeta la tenemos creada en el disco c:\Pistonazo_users y dentro de esta carpeta están las carpetas de cada uno de los usuarios. Bastará asignar la ruta de esa carpeta a cada uno de los usuarios. Por ejemplo, vamos a asignar la unidad Z: a la carpeta personal de cada uno de los usuarios de nuestra organización Pistonazo:

Carpetas particulares

Asignaremos estas carpetas a cada uno de los usuarios. Para ello desde la pestaña perfil:

Carpetas particulares

La carpeta del usuario debe ser una carpeta compartida y con permisos de escritura. En nuestro caso utilizaremos las carpetas que creamos en la sección de Permisos NTFS por línea de comandos. Creamos una carpeta en C:\Pistonazo_Users, esta carpeta tiene permisos de acceso el grupo Pistonazo y los Administradores. Por tanto, el recurso **\\192.168.100.1\Pistonazo_users\%username%** será la carpeta de cada uno de los usuarios.
La variable %username% sustituye el valor por el identificador de usuario.

Carpetas personales ocultas

Si quisiéramos que las carpetas personales estuvieran ocultas, bastaría con añadir un $ al final del nombre del recurso compartido. En nuestro caso, podíamos haber compartido el recurso Pistonazo_Users con un $ al final y así ocultar las carpetas de usuarios.

Carpeta personal asignada a Z:

Al añadir las carpetas personales de los usuarios, cuando iniciamos sesión, veremos que tenemos una nueva conexión de red asociado a la unidad Z: que conectará con el recurso compartido que serán las carpetas personales de los usuarios. Si iniciamos sesión con usucomp1:

Carpeta personal montada como recurso de red en Z

Si accedemos a los recursos del servidor, veremos como no aparecen las carpetas personales de los usuarios, ya que se encuentran ocultas:

Carpetas de usuarios ocultas en DC

Comandos de inicio de sesión

Otra opción que podemos configurar dentro de la ficha perfil consiste en indicar un script que se ejecutará en cada inicio de sesión de manera automática y transparente al usuario. Para ello desde la pestaña perfil del usuario accedemos a Script de inicio de sesión:

Script de inicio de sesión

Estos scripts deben hallarse en la carpeta compartida NETLOGON, cuya dirección local en el controlador de dominio es: C:\Windows\SYSVOL\sysvolCEFIRE2017.LOCAL\scripts . En este caso concreto, la dirección local y la dirección en red serían respectivamente:

Ruta Netlogon

Crearemos en esta carpeta un fichero llamado pistonazo.bat. Que será donde añadamos los comandos que queremos que se ejecuten cuando un usuario inicie la sesión:

Fichero pistonazo.bat

Hay que tener en cuenta que por defecto las extensiones de archivo están ocultas. Para evitar confusiones con los archivos, vamos a marcar que nos muestre las extensiones de los archivos. Para ello seleccionamos Vista y marcamos extensiones de archivo:

Marcar extensiones de archivos en Netlogon

Ejemplos de scripts de inicio de sesión: Asignación de unidad de red

Vamos a hacer que se monte de manera automática la unidad P: que será la unidad donde se encuentren las carpetas de los departamentos de los usuarios de la organización Pistonazo. Para ello, añadiremos a nuestro script, el comando Net Use P: \\192.168.100.1\Pistonazo

Pistonazo.bat

Script de inicio de sesión

Y ahora si iniciamos sesión con alguno de los usuarios de Pistonazo, veremos que nos habrá añadido una nueva unidad de red, la unidad P: que conectará a la estructura de Pistonazo que se encuentra en el servidor:

Unidad de red Pistonazo

Ejemplos de scripts de inicio de sesión: Asignación de unidad de red

Supongamos que queremos enviar un mensaje a los usuarios cuando se conecten al sistema. Suele ser habitual enviar mensajes del tipo 'Guarda los datos en red' o 'No instales software sin permiso del administrador', o simplemente avisar de paradas planeadas en el sistema. Para enviar este tipo de mensajes automáticamente cuando el usuario inicia sesión podemos utilizar el comando msg dentro del fichero de comandos de inicio de sesión que hemos creado en el punto anterior:

```
if NOT EXIST P: net use P: \\192.168.100.1\Pistonazo msg %username% Recuerda guardar
los datos en  las unidades Z: o P:
```

Mensajes de aviso a usuarios

Actividades tema 4

Actividad 4.1

Comparte una carpeta donde puedan leer y escribir los usuarios del grupo finanzas y puedan simplemente leer los usuarios de ventas. Haz una captura de pantalla donde se muestren los recursos compartidos en el servidor y otra captura donde se vean los permisos de la carpeta que acabas de compartir.

Configura el **perfil** de uno de los usuarios para que le aparezca automáticamente como una unidad de red cuando inicie sesión.

Modifica las siguientes **directivas** para conseguir:

1. Los usuarios deben cambiar la contraseña cada 90 días y guardar el historial de 5 contraseñas. Para facilitar la gestión no será necesaria tener una restricción en cuánto a la complejidad de la contraseña y el número mínimo de caracteres será de 4.
2. Para evitar posibles robos de contraseña y ataques mal intencionados, cuando un usuario intenta 4 veces introducir de manera incorrecta su contraseña, la cuenta se bloqueará hasta que el administrador la desbloquee. Se reestablecerá el contador de inicios de sesión erróneos a los 10minutos.

Haz una captura de pantalla de las directivas de contraseña y de inicios de sesión.

Obra publicada con Licencia Creative Commons Reconocimiento Compartir igual 4.0