

|  |
| --- |
| SERVICIO DE DIRECTORIO:  ACTIVE DIRECTORY |
|  |
| Sistemas Operativos en Red  Juan Carlos Navidad García |



SISTEMAS OPERATIVOS EN RED

JUAN CARLOS NAVIDAD GARCÍA

CASO PRACTICO: RECURSOS COMPARTIDOS EN AD

PARTIREMOS DEL SIGUENTE ESQUEMA

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| EQUIPOS DEL DOMINIO (red nat) | | | | | |
| Nombre equipo | Nombre FQDN en el dominio | IP | Mascara | Puerta de enlace | DNS |
| dc01 | dc01.empresa.es | 192.168.1.254 | 255.255.255.0 | 192.168.1.1 | 192.168.1.254 |
| pc01 | pc01.empresa.es | 192.168.1.20 | 255.255.255.0 | 192.168.1.1 | 192.168.1.254 |

Pc01 tendrá que estar unido al dominio empresa.es

|  |  |  |
| --- | --- | --- |
| USUARIOS Y GRUPOS | | |
| GRUPO | TIPO |  |
| Contabilidad | Grupo seguridad- global | Corresponde con el departamento contabilidad de la empresa |
| Usuarios: Alberto Gómez |
| sistemas | Grupo seguridad- global | Corresponde con el departamento sistemas de la empresa |
| Usuarios: Carmen martinez, Laura jarcia, Marisa Fernández |

Directorios: c:\empresa

\empresa\almacen

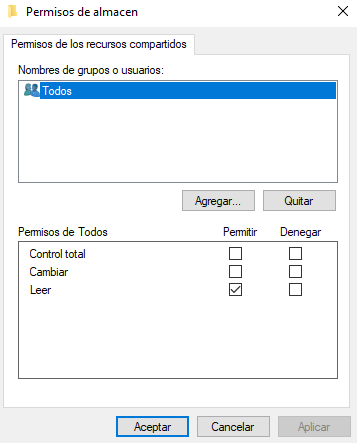
\empresa\contabilidad

\empresa\proyectos

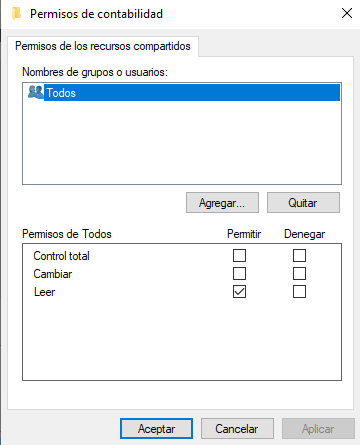
COMPARTIR DIRECTORIOS EN RED

Queremos compartir la siguiente estructura de directorios de la siguiente forma

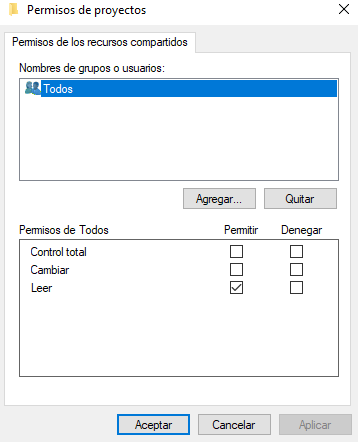
c/empresa/almacen: todos los usuarios del dominio podrán leer



c/empresa/contabilidad: todos los usuarios del dominio podrán leer



c/empresa/proyectos: todos los usuarios tienen acceso de lectura



No solo serviría para windows server

Podemos trabajar desde

* El explorador de windows:
* Administración de equipos/carpetas comartidas

Para compartir almacén usaremos el explorador de windows:

1. Botón derecho sobre la carpeta a compartir (almacen)/compartir con/usuarios específicos
2. Agregamos usuarios del dominio
3. Le damos permisos de lectura
4. Nos mostrara la dirección del recurso [\\dc01\almacen](file:///\\dc01\almacen)
5. Observa que desde esta opción no se podrá cambiar el nombre con el que se compartir el recurso

Explorador de windows

Para compartir contabilidad usaremos el explorador de windows y las propiedades de la carpeta

1. Botón derecho sobre la carpeta a compartir (contabilidad)/propiedades/compartir
   1. Desde compartir: nos saldría el asistente anterior, con el que hemos compartido almacén
   2. Desde uso compartido avanzado:
      1. Cambiar el nombre de la carpeta compartida: conta
      2. Establecer el límite de usuarios simultáneos
      3. Añadimos un comentario
      4. Agregamos usuarios del dominio
      5. Le damos permisos de lectura
      6. Nos mostrara la dirección del recurso [\\dc01\conta](file:///\\dc01\conta)
2. Cambiar el nombre del recurso compartido Almacen por storage.
   1. Accedo a las propiedades/compartir
   2. Quito los permisos
   3. Cambio el nombre
   4. Agregamos los usuarios del dominio

Herramientas administrativas/administración de equipos

En Carpetas compartidas/recursos compartidos veremos nuestros recursos compartidos

Los recursos compartidos en el que su nombre aparece al final un $ significa que el recurso esta oculto para el cliente que accede de forma remota

Para compartir desde aquí:

* Botón derecho/nuevo recurso compartido: aparecerá un asistente
  + Nombre del equipo donde se encuentra el recurso a compartir: dc01
  + Ruta de la carpeta: buscamos proyectos
  + Nombre del recurso compartido: Trabajos
  + Descripción: proyectos y trabajos de la empresa
  + Tipo de permisos: todos los usuarios tienen acceso de lectura
* Verifica que el recurso aparece como recurso compartido en el administrador de equipos/carpetas compartidas/recursos compartidos

Nota: utilizar la herramienta recursos compartidos nos proporciona unos beneficios que no se pueden utilizar el el explorador de windows:

Conectar una unidad de red en un SOR Cliente de Microsoft, a un directorio compartido en Windows Server 2016.

1. Conectamos con una cuenta del dominio en el cliente
2. Desde el explorador de Windows podemos conectarnos a un Directorio compartido:
   1. Mediante Red: accediendo al directorio compartido
      1. Activaremos detección de redes
      2. Credenciales
   2. Desde red: botón derecho conectar a una unidad de red
   3. Desde la barra de direcciones poniendo la ruta
3. Conectar la carpeta conta a una unidad de red
   1. Accedemos a la carpeta o bien mediante la red o la barra de direcciones y sobre la carpeta conta botón derecho conectar a una unidad de red
      1. Le damos la letra
      2. Conectar de nuevo al iniciar sesión
      3. Verificar que en Este equipo está la unidad
      4. Verificar si puedo crear archivos o carpetas
4. Conectar a la unidad Y la carpeta storage desde red
   1. Botón derecho sobre Red
   2. Conectar a unidad de red
   3. Asignar la letra Y
   4. Poner la dirección del recurso [\\dc01\storage](file:///\\dc01\storage)
5. Verificad si se puede modificar dichos recursos creando nuevos directorios

PUBLICAR RECURSOS COMPARTIDOS EN ACTIVE DIRECTORY.

Va a permitir al cliente buscar recursos compartidos del directorio activo. Útil cuando los recursos están repartidos en diferentes equipos y no sabemos donde.

1. Publicar el directorio compartidos conta y trabajos
   1. Desde el servidor en recursos compartidos
   2. Botón derecho sobre conta/propiedades/publicar
      1. Activamos la casilla de verificación publicar
      2. Palabras claves de búsqueda:
         1. 2016
   3. Lo mismo para trabajos
2. Verificar la búsqueda de los recursos conta y trabajos desde el cliente
   1. Desde Red
   2. Búsqueda en active directory
      1. Buscar: Carpetas compartidas
      2. En: todo el directorio
   3. Con el botón derecho sobre el recurso encontrado podremos:
      1. Acceder al recurso: explorar
      2. Buscar
      3. Conectar a una unidad
      4. Propiedades

RECURSOS COMPARTIDOS OCULTOS

Al compartir un recurso, en este caso un directorio, de forma oculta el nombre del recurso no se mostrará en los clientes en red que se conecten al equipo en el que se comparten dichos recursos.

Tan solo se podrán conectar a estos recursos ocultos aquellos usuarios que conozcan el nombre del recurso compartido, puesto que no se muestran en el navegador de ficheros al conectarse al equipo que comparte los recursos ocultos.

Para crear un recurso compartido de forma oculta hay que ponerle un $ al final del nombre del recurso compartido

Crear dos directorios compartidos ocultos llamados música y videos en C del servidor dc01

1. Creo las carpetas desde el explorador
   1. Comparto Música de forma oculta desde el explorador:
      1. propiedades compartir/uso compartido avanzado compartir carpeta
         1. Nombre: música$
         2. Comentario: directoria de música para proyectos
      2. Verifica la ruta de acceso
         1. \\dc01\musica$
   2. Comparto video de forma oculta desde recursos compartidos:
      1. Botón derecho/recurso compartido nuevo. Aparece asistente
         1. Ruta de la carpeta: Examinar: nombre del recurso:**video$**
         2. Verifica la ruta de acceso: \\dc01\video$
2. Desde el cliente verifica que no aparen los recurso video y música
3. Accede con la ruta de acceso en la barra de direcciones:
   1. \\dc01\musica$
   2. [\\dc01\video$](file:///\\dc01\video$)
4. Conectar una unidad de red a música y otra a video
5. Publica los directorios música y video. ¿Qué ocurre? No se puede, no tiene sentido
6. Verifica desde el cliente si se puede acceder al directorio oculto C$ sabiendo su ruta. ¿que ocurre? Nos pide credenciales

PERMISOS LOCALES A DIRECTORIOS QUE ESTÁN COMPARTIDOS COMO RECURSOS COMPARTIDOS EN RED.

Lo que vamos a hacer es configurar los permisos NTFS (ACLs) de los directorios compartidos.

Cuando se accede a un directorio compartido de forma remota, a través de la red, el sistema operativo aplicará tanto los permisos establecidos en compartir como los permisos locales aplicados sobre el directorio. La composición de los permisos que se aplicará será la más restrictiva de ambos permisos.

En realidad, los permisos configurados en el directorio en sistema de ficheros NTFS son los que siempre se aplicarán, sea el acceso local o remoto.

Los permisos configurados en compartir solo se comprobarán cuando el acceso al directorio compartido se haga a través de la red. Primero se comprueban estos permisos y después se trata de acceder con los permisos aplicados sobre el directorio. Se trata, por tanto, de un doble filtro que establece qué operaciones se podrán hacer sobre un directorio tanto en local como en remoto.

Como simplificación, podemos pensar que cuando se comparte un directorio en red, el sistema operativo aplicará la composición más restrictiva de ambos permisos, los locales y los remotos, cuando un usuario trate de acceder de forma remota.

Si el acceso es local, como ya se ha comentado, entonces el sistema operativo tan solo aplicará los permisos establecidos sobre el directorio a través de la pestaña seguridad (ACLs sobre el directorio en sistema de ficheros NTFS).

1. Ver permisos locales y de red de la carpeta video: En el servidor sobre videos$/propiedades/
   1. Permisos de red: compartir/ uso compartido avanzado/permisos: Verificamos los permisos que tienen
      1. Todos: leer
   2. Permisos locales: seguridad
      1. Creator ower
      2. System
      3. Administradores
      4. Usuarios:
2. Cambiar el propietario de la carpeta video:
   1. Accedemos a las propiedades de seguridad de la carpeta videos:
      1. Opciones avanzadas
      2. Propietario: cambiar
3. Intentad cambiar los permisos locales de video$

Cuando se crea un directorio o fichero el sistema de archivos (NTF) por deficto le asigna los permisos heredados del directorio padre. Esto implica que estos permisos no se pueden cambiar (aparecen con un tic gris) porque son permisos heredados, lo que si podríamos es añadir nuevos permisos. Para poder modificar los permisos heredados debemos deshabilitar la herencia.

Al deshabilitar la herencia ¿Qué permisos le pondremos?:

* Convertir los permisos heredados en permisos explícitos en este objeto
  + De esta manera mantendrá los permisos padres, pero podremos cambiarlos
* Quitar todos los permisos heredados de este objeto. Ojo, debemos añadir el creator owner y system

1. Modificar los permisos locales de video$ para que solo los administradores tengan permisos (además de creator owner y system para que no me de problemas)
   1. Accedemos a las propiedades de seguridad de la carpeta videos:
      1. Opciones avanzadas
      2. Deshabilitar herencia
      3. Eliminar los permisos que no sean system, creaor owner y administradores.

COMPARTIR RECURSO CON AGLDP

Queremos Compartir el recurso videos [\\dc01\empresa\videos](file:///\\dc01\empresa\videos) de forma que

1. Puedan gestionar (administrar) el recurso video los usuarios de sistemas
2. Puedan tener solo acceso los usuarios de sistema que pertenecen a contabilidad.

Análisis de la Solución:

En este caso, tenemos dos tipos de acceso.

1. **Solo lectura**. Usuarios que podrán acceder a este recurso compartido para descargar documentos (según el enunciado).
2. **Control total**. Usuarios que gestionarán el contenido de este recurso compartido a través de la red.

crearemos un grupo para cada uno de estos tipos de acceso:

En este caso, tenemos dos tipos de acceso.

1. **Solo lectura**. DL\_GestorVideos
2. **Control total**. DL\_visoresVideos

Ahora solo tenemos que crear tantos grupos de Dominio Local( DL ) en nuestro dominio Active Directory, como tipos de acceso tengamos. En este caso 2 grupos:

* Dl\_gestorVideos
* Dl-visoresVideos

Esta estructura nos permitirá gestionar los permisos usando solo los grupos de seguridad de dominio local

Esta estrategia de asignación de permisos se le denomina AGLPD

Quedando así nuestros usuarios y grupos

|  |  |  |
| --- | --- | --- |
| USUARIOS Y GRUPOS | | |
| GRUPO | TIPO |  |
| Dl\_gestorVideos | Grupo seguridad- dominio local | Para dar permisos de gestión a videos |
| Miembros: sistemas |
| Dl-visoresVideos | Grupo seguridad- dominio local | Para dar permiso de acceso (lectura) a videos |
| Miembros: contabilidad y sistemas |
| contabilidad | Grupo seguridad- global | Corresponde con el departamento contabilidad de la empresa |
| Usuarios: Alberto Gómez |
| sistemas | Grupo seguridad- global | Corresponde con el departamento sistemas de la empresa |
| Usuarios: Carmen martinez, Laura jarcia, Marisa Fernández |

Solución practica:

1. Herramienta/usuarios y equipos
   1. Videos/propiedades/opciones avanzadas/agregar/seleccinar entidad de seguridad
      1. Dl-gestoresVideo: contral total solo al contenedor. Este permiso no es heredado lo acabamos de crear
      2. Dl\_visoresVideo: lectura y ejecución, mostrar el contenido y lectura
2. Accesos efectivos:
   1. verificar los accesos que tiene el usuario marisa fernandez sobre el recurso videos
      1. Desde Videos/propiedades/opciones avanzadas/accesos efectivos
         1. seleccionar un usuario: mfernandez(cuenta de marisa fernansdez) y **vemos que no tiene control total**
         2. **la razón es, que aunque pertenece a sistemas y sistemas es miembro de visores y gestores de video**