

TAREA REVISIÓN UT7

Realiza los siguientes ejercicios según las indicaciones:

MG: Modo gráfico, **CMD,** **PW:** Powershell

1. Agrega un equipo cliente al dominio: **MG**

Desde el cliente

Propiedades del sistema

Cambios en el dominio o el nombre del equipo

Puede cambiar el nombre y la pertenencia de este equipo. Los cambios podrían afectar al acceso a los recursos de red.

Nombre de equipo: Cliente_7

Nombre completo de equipo: Cliente_7.Asir7.com

Miembro del

☒ Dominio: Asir7.com

☐ Grupo de trabajo:

Aceptar Cancelar Aplicar

Usuarios

Archivo Inicio Compartir Vista

Este equipo > Disco local (C:) > Usuarios >

	Nombre	Fecha de modificación	Tipo
Acceso rápido	Acceso público	15/01/2022 21:53	Carpeta de archivos
Escritorio	Administrador	22/01/2022 10:18	Carpeta de archivos
Descargas	Cliente_7	21/01/2022 14:20	Carpeta de archivos

Desde el servidor

Nuevo objeto: Equipo

Crear en: Asir7.com/Computers

Nombre de equipo: Cliente_7

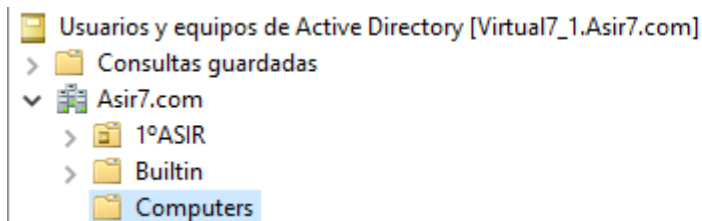
Nombre del equipo (anterior a Windows 2000): CLIENTE_7

El siguiente usuario o grupo puede unir este equipo a un dominio.

Usuario o grupo: Predeterminado: Admins. del dominio

☐ Asignar la cuenta de este equipo como un equipo anterior a Windows 2000

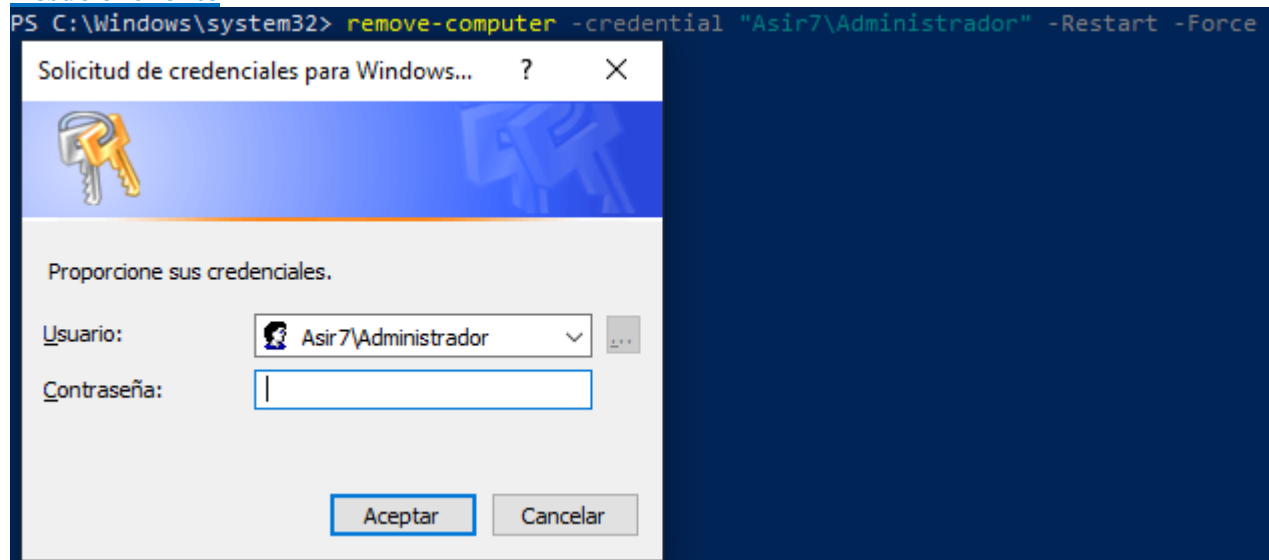
Aceptar Cancelar Ayuda



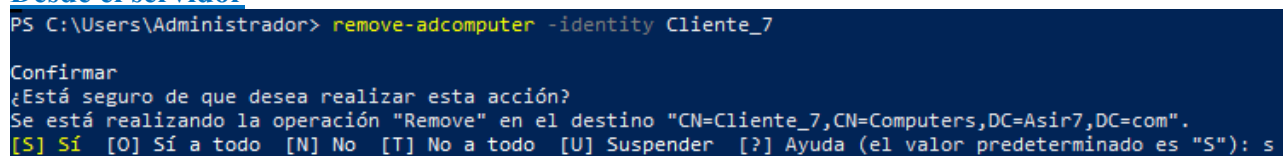
Nombre	Tipo
CLIENTE_7	Equipo
VIRTUAL7_2	Equipo
VIRTUAL7_3	Equipo

2. Elimina un equipo cliente del dominio: **PW**

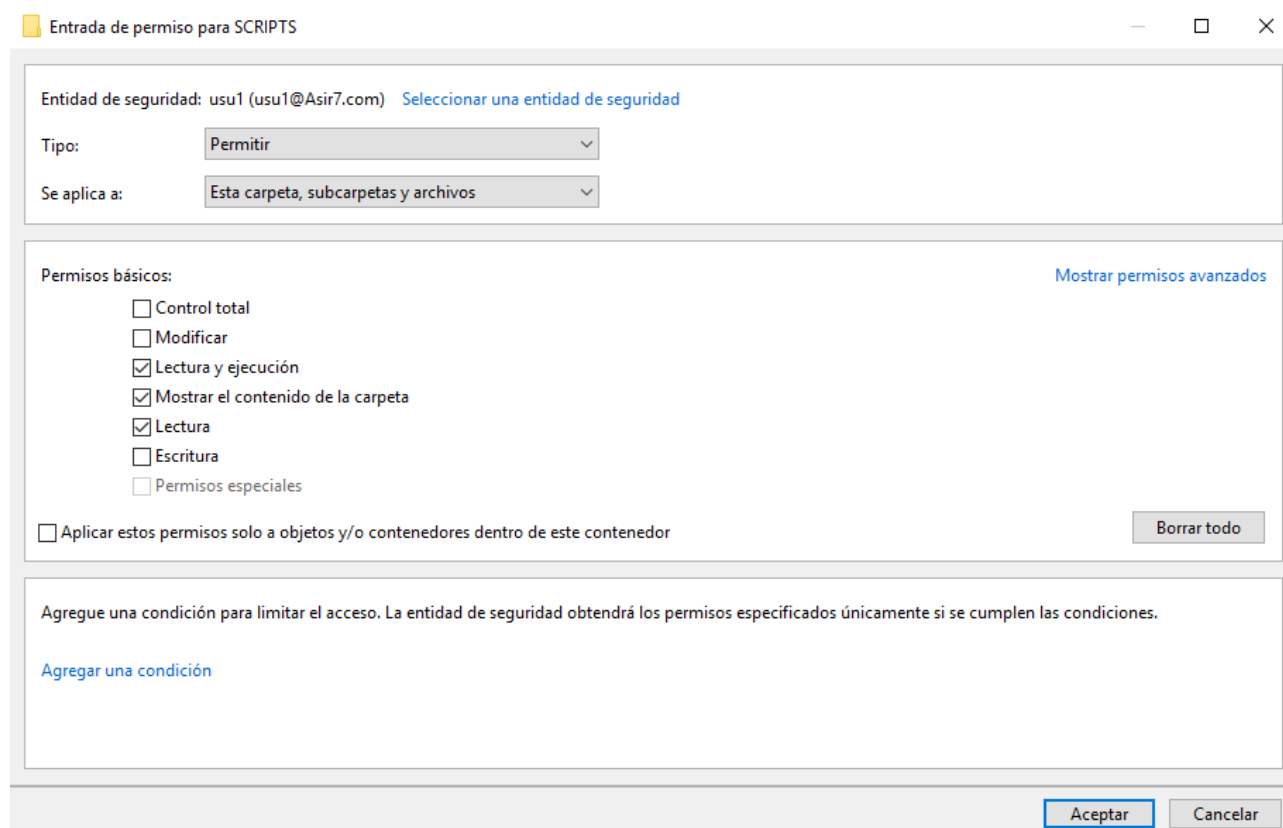
Desde el cliente



Desde el servidor



3. **Visualiza** los permisos básicos y avanzados de los distintos usuarios: **MG**



Entrada de permiso para SCRIPTS

Entidad de seguridad: usu1(usu1@Asir7.com) [Seleccionar una entidad de seguridad](#)

Tipo: Permitir

Se aplica a: Esta carpeta, subcarpetas y archivos

Permisos avanzados: [Mostrar permisos básicos](#)

<input type="checkbox"/> Control total	<input type="checkbox"/> Escribir atributos
<input checked="" type="checkbox"/> Atravesar carpeta / ejecutar archivo	<input type="checkbox"/> Escribir atributos extendidos
<input checked="" type="checkbox"/> Mostrar carpeta / leer datos	<input type="checkbox"/> Eliminar subcarpetas y archivos
<input checked="" type="checkbox"/> Leer atributos	<input type="checkbox"/> Eliminar
<input checked="" type="checkbox"/> Leer atributos extendidos	<input checked="" type="checkbox"/> Permisos de lectura
<input type="checkbox"/> Crear archivos / escribir datos	<input type="checkbox"/> Cambiar permisos
<input type="checkbox"/> Crear carpetas / anexas datos	<input type="checkbox"/> 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](#)

4. **Agrega permisos a un usuario. CMD**

Con el comando cacs sobre un archivo

```
C:\Users\Administrador\Desktop\SCRIPTS>cacs "EXAMEN -UT5-UT6-PART2-JOSE MARIA.ps1" /g usu1:W
¿Está seguro (S/N)?s
```

Con el comando attrib sobre una carpeta

```
C:\Users\Administrador\Desktop\SCRIPTS>attrib +R "EXAMEN -UT5-UT6-PART2-JOSE MARIA.ps1"
```

5. **Deniega permisos a un usuario. PW**

Con el comando cacs sobre un archivo

```
C:\Users\Administrador\Desktop\SCRIPTS>cacs "EXAMEN -UT5-UT6-PART2-JOSE MARIA.ps1" /d usu1
¿Está seguro (S/N)?s
```

Con el comando attrib sobre una carpeta

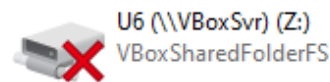
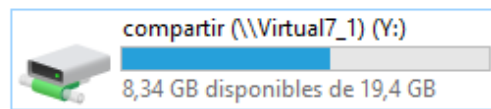
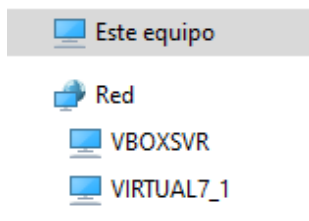
```
C:\Users\Administrador\Desktop\SCRIPTS>attrib -R "EXAMEN -UT5-UT6-PART2-JOSE MARIA.ps1"
```

6. **Realiza un SCRIPT que permita realizar la gestión de recursos compartidos:**

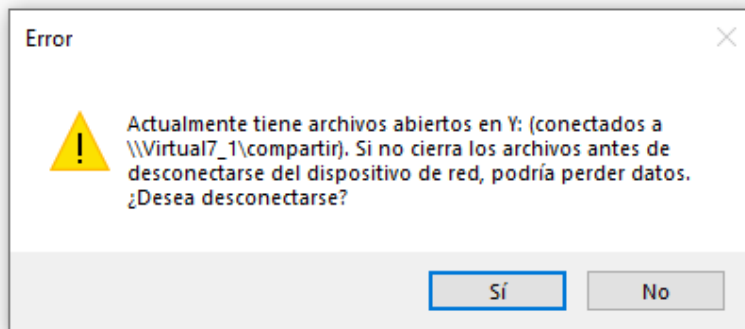
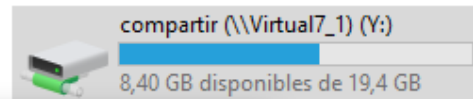
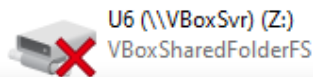
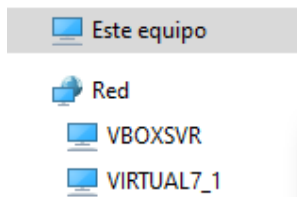
1. Mostrar información de los recursos compartidos.
2. Crear un recurso compartido.
3. Modificar un recurso compartido.
4. Administrar (ver, añadir, eliminar) los permisos de un recurso compartido.
5. Eliminar un recurso compartido.

7. Realiza en **MG**:

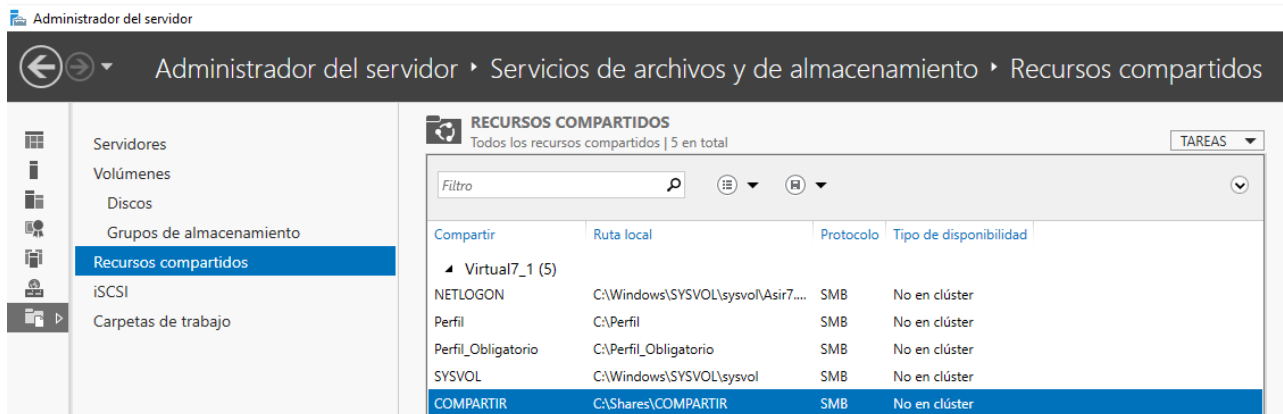
1. Crear **unidad de red**.



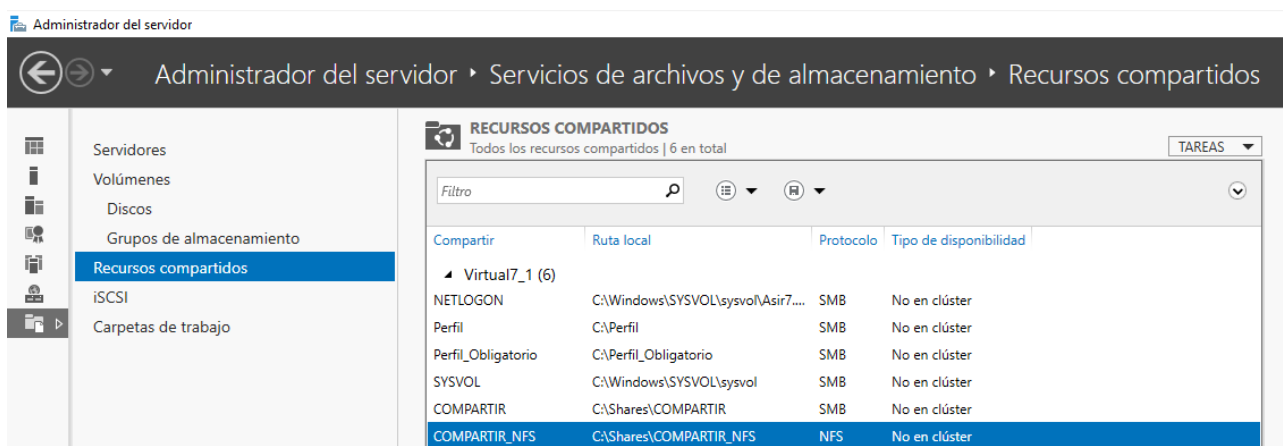
2. Eliminar unidad de red.



3. Crea un recurso compartido de tipo SMB.



4. Crea un recurso NFS.



5. En equipo cliente de dominio crea una directiva de grupo para ocultar las notificaciones.

Ocultar el área de notificación

Ocultar el área de notificación

Valor anterior Valor siguiente

☐ No configurada
 ☒ Habilitada
 ☐ Deshabilitada

Comentario:

Compatible con: Al menos sistemas operativos Windows Server 2003 o Windows XP Professional

Opciones:

Ayuda:

Esta opción afecta al área de notificación (denominada anteriormente "bandeja del sistema") de la barra de tareas.

Descripción: el área de notificación está ubicada en el extremo derecho de la barra de tareas e incluye los iconos de notificaciones actuales y el reloj del sistema.

Si se habilita esta opción, se ocultará el área de notificación del usuario, incluidos los iconos de notificación. La barra de tareas mostrará solo el botón Inicio, los botones de la barra de tareas, las barras de herramientas personalizadas (si hay alguna) y el reloj del sistema.

Si esta opción está deshabilitada o no está configurada, se mostrará el área de notificación en la barra de tareas del usuario.

Nota: al habilitar esta opción, se invalida la opción "Desactivar limpieza de área de notificación" porque, si el área de notificación está oculta, no es necesario limpiar los iconos.

Aceptar Cancelar Aplicar

6. En equipo **servidor de dominio** establece una directiva de grupo para **impedir el acceso a Google Chrome**.

Mostrar contenido

Lista de aplicaciones no permitidas

	Valor
▶	chrome.exe
*	

Aceptar Cancelar

No ejecutar aplicaciones de Windows especificadas

No ejecutar aplicaciones de Windows especificadas

Valor anterior Valor siguiente

☐ No configurada Comentario:

☒ Habilitada

☐ Deshabilitada

Compatible con: Al menos Windows 2000

Opciones:

Ayuda:

Lista de aplicaciones no permitidas

Mostrar...

Impide que Windows ejecute los programas que usted especifique en esta configuración de directiva.

Si habilita esta configuración de directiva, los usuarios no podrán ejecutar los programas que agregue a la lista de aplicaciones no permitidas.

Si deshabilita o no define esta configuración de directiva, los usuarios podrán ejecutar cualquier programa.

Esta configuración de directiva solo impide que los usuarios ejecuten programas iniciados por un proceso del Explorador de archivos. No impide que los usuarios ejecuten programas como el Administrador de tareas, que se inician mediante procesos del sistema y otros procesos. Además, si los usuarios tienen acceso al símbolo del sistema (Cmd.exe), esta configuración de directiva no les impide iniciar programas en la ventana de comandos aunque no podrán hacerlo mediante el Explorador de archivos.

Nota: se requieren aplicaciones de terceros con certificaciones de Windows 2000 o posteriores para cumplir con esta configuración

Aceptar Cancelar Aplicar

7. **Audite** el acceso a una carpeta para un grupo de usuarios.

Entrada de auditoría para EXAMEN

Entidad de seguridad: GrupoExamen (ASIR7\GrupoExamen)
[Seleccionar una entidad de seguridad](#)

Tipo:

Correcto

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 esta configuración de auditoría solo a objetos y/o contenedores dentro de este contenedor

Borrar todo

Agregue una condición para limitar el ámbito de esta entrada de auditoría. Los eventos de seguridad se registrarán únicamente si se cumplen las condiciones.

[Agregar una condición](#)

Aceptar

Cancelar

Configuración de seguridad avanzada para EXAMEN

Nombre: C:\Users\Administrador\Desktop\EXAMEN

Propietario: usu1 (usu1@Asir7.com)

Cambiar

Permisos

Compartir

Auditoría

Acceso efectivo

Para obtener información adicional, haga doble clic en una entrada de auditoría. Para modificar una entrada de auditoría, seleccione la entrada y haga clic en Editar (si está disponible).

Entradas de auditoría:

Tipo	Entidad de seguridad	Acceso	Heredada de	Se aplica a
Corre...	GrupoExamen (ASIR7\GrupoE...	Control total	Ninguno	Esta carpeta, subcarpetas y arc...

Agregar

Quitar

Editar

Habilitar herencia

☐ Reemplazar todas las entradas de auditoría de objetos secundarios por entradas de auditoría heredables de este objeto

Aceptar

Cancelar

Aplicar

8. **Visualiza los eventos** generados por las auditorías.

Visor de eventos

Archivo Acción Ver Ayuda

Visor de eventos (local)

- Vistas personalizadas
- Registros de Windows
 - Aplicación
 - Seguridad**
 - Instalación
 - Sistema
 - Eventos reenviados
 - Registros de aplicaciones y suscripciones

Palabras clave	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Auditoria correcta	18/02/2022 14:08:46	Microsoft Windows security auditing.	5156	Filtering Platform Connection
Auditoria correcta	18/02/2022 14:08:46	Microsoft Windows security auditing.	5158	Filtering Platform Connection
Auditoria correcta	18/02/2022 14:08:46	Microsoft Windows security auditing.	5158	Filtering Platform Connection
Auditoria correcta	18/02/2022 14:08:46	Microsoft Windows security auditing.	5156	Filtering Platform Connection
Auditoria correcta	18/02/2022 14:08:46	Microsoft Windows security auditing.	5156	Filtering Platform Connection
Auditoria correcta	18/02/2022 14:08:46	Microsoft Windows security auditing.	5156	Filtering Platform Connection
Auditoria correcta	18/02/2022 14:08:46	Microsoft Windows security auditing.	5158	Filtering Platform Connection
Auditoria correcta	18/02/2022 14:08:46	Microsoft Windows security auditing.	5158	Filtering Platform Connection
Auditoria correcta	18/02/2022 14:08:43	Microsoft Windows security auditing.	4672	Special Logon
Auditoria correcta	18/02/2022 14:08:43	Microsoft Windows security auditing.	4624	Logon
Auditoria correcta	18/02/2022 14:08:40	Microsoft Windows security auditing.	4634	Logoff
Auditoria correcta	18/02/2022 14:08:39	Microsoft Windows security auditing.	4672	Special Logon
Auditoria correcta	18/02/2022 14:08:39	Microsoft Windows security auditing.	4624	Logon

Evento 5156, Microsoft Windows security auditing.

General Detalles

La Plataforma de filtrado de Windows permitió una conexión.

Información de aplicación:
 Id. de proceso: 108
 Nombre de aplicación: \device\harddiskvolume2\windows\system32\svchost.exe

Información de red:
 Dirección: Enlace externo
 Dirección de origen: 10.0.3.15
 Puerto de origen: 55918
 Dirección de destino: 192.168.2.1
 Puerto de destino: 53
 Protocolo: 17

Información de filtro:

Nombre de registro: Seguridad
 Origen: Microsoft Windows security Registrado: 18/02/2022 14:08:46
 Id. del: 5156 Categoría de tareas: Filtering Platform Connection
 Nivel: Información Palabras clave: Auditoria correcta
 Usuario: No disponible Equipo: Virtual7_1.Asir7.com
 Código de operación: Información
 Más información: [Ayuda Registro de eventos](#)

Propiedades de evento: Evento 5156, Microsoft Windows security auditing.

General Detalles

La Plataforma de filtrado de Windows permitió una conexión.

Información de aplicación:
 Id. de proceso: 108
 Nombre de aplicación: \device\harddiskvolume2\windows\system32\svchost.exe

Nombre de registro: Seguridad
 Origen: Microsoft Windows security Registrado: 18/02/2022 14:08:46
 Id. del: 5156 Categoría de tareas: Filtering Platform Connect
 Nivel: Información Palabras clave: Auditoria correcta
 Usuario: No disponible Equipo: Virtual7_1.Asir7.com
 Código de operación: Información
 Más información: [Ayuda Registro de eventos](#)

Copiar Cerrar