Prácticas de Infraestructura Informática

Bloque 2: Gestión de equipos mediante Directorio Activo

Sesión 3 - Gestión centralizada de equipos mediante directivas de grupo: casos prácticos

Objetivos

Practicar el uso de las directivas de grupo para la administración centralizada de equipos gestionados mediante una infraestructura de Directorio Activo.

Desarrollo

En esta práctica se plantean 4 casos de gestión de equipos. Cada caso persigue cumplir unos objetivos diferentes.

- **Actuaciones preliminares**

  - COMPROBACIÓN INICIAL: al igual que en sesiones anteriores, siempre que no sea necesario, es conveniente que los clientes Win11 no tengan acceso a la red externa para que no se actualicen. Este es el caso de esta sesión de prácticas. En el sistema anfitrión, *Herramientas administrativas -> Enrutamiento y acceso remoto*. Entonces, comprueba que el servicio de enrutamiento está detenido. Si no es así, detenlo.

    En dos de los casos prácticos planteados en esta sesión se requiere que los equipos del dominio accedan a determinados paquetes de software para su instalación. Debido a ello, se requiere disponer de un recurso de distribución de software para los equipos del dominio. Si bien en la sesión de prácticas anterior se creó un recurso de distribución en el servidor de dominio para la distribución de scripts, en el caso de la distribución de software a todo el dominio, lo más lógico es utilizar el servidor de ficheros disponible en el dominio (PLX-S-FS). En este apartado de actuaciones preliminares se preparará un recurso de distribución de software en el servidor de ficheros del dominio.

    - Arranca el servidor de dominio (PLX-S-DC) e inicia sesión con el *Administrador*. Es aconsejable esperar a que arranque completamente antes de arrancar otras máquinas del dominio.
    - Arranca el servidor de ficheros (PLX-S-FS) e inicia sesión con el *Administrador* local.
    - En el servidor de ficheros, crea la carpeta *RDS* en el volumen D. *RDS* significa Recurso de Distribución de Software. Asimismo, recuerda que el volumen D corresponde al disco de datos del servidor.
    - Botón derecho sobre *RDS* -> *Propiedades* -> ficha *Compartir* -> botón *Compartir*. En este punto hay que elegir los usuarios que tendrán autorización de acceso a este recurso. Para poder escribir en el recurso (por ejemplo, para copiar en él paquetes de software) se va a autorizar al usuario local *Pruebas* (este usuario se creó en este servidor en una sesión de prácticas anterior). En el campo *Agregar*, escribe *Pruebas*. Por defecto, solo se le otorga permiso de lectura. Añádele también permiso de escritura. Por otra parte, también se requiere que los usuarios del dominio puedan acceder a este recurso. Para ello, selecciona Buscar personas -> botón *Opciones avanzadas*. Entonces, autentícate en el dominio con el *Administrador*. Botón *Buscar ahora*. Entonces, selecciona el grupo *Usuarios autentificados*. Por defecto, se otorga acceso de *Lectura*. Esto es correcto, ya que los usuarios del dominio solo necesitan leer de este recurso compartido. Pulsa *Compartir* para completar la operación.
    - Para comprobar que puedes acceder a RDS correctamente, vas a copiar en él un paquete de software que se utilizará en el primer caso de trabajo. Se trata del software de compresión de

archivos 7-Zip. Para obtener este paquete de software utilizarás el sistema anfitrión, que sí tiene conexión de la red externa.

- En el sistema anfitrión, utilizando el Internet Explorer, accede a la página de descarga de 7-Zip. El paquete que debes descargar debe ser de tipo "`.msi`" y de 64-bit para Windows x64. Descarga este paquete en la carpeta estándar (*Descargas*).
- En el sistema anfitrión, conéctate al recuso compartido RDS. Utiliza las credenciales del usuario *Pruebas* para conectarte. Entonces, copia el fichero `.msi` desde *Descargas* a *RDS*.
- En este punto, el paquete de software que utilizarás en el primer caso de trabajo, ya está disponible en *RDS*.

Caso 1: Creación de un entorno restrictivo para los equipos de los empleados de la organización de ejemplo

Es habitual que los empleados de una organización utilicen usuarios locales con privilegios de administración para trabajar en sus equipos personales. Esto les proporcionaría, en principio, control total sobre sus equipos. Sin embargo, mediante las directivas de grupo, se pueden establecer configuraciones obligatorias para todos los usuarios, orientadas, por ejemplo, a mejorar la seguridad de los equipos, o a restringir el uso de características que no se consideren apropiadas para el puesto de trabajo. En este Caso 1 se plantea la utilización de directivas de grupo para establecer un conjunto de restricciones en la configuración de los equipos de los empleados de la organización de ejemplo.

Especificaciones del caso

- Equipos objetivo
  - PLX-C-53
  - PLX-C-54
- Configuraciones obligatorias requeridas para los equipos
  - *Configuración 1*: El firewall debe estar activo en todas las posibles ubicaciones de red (red de dominio, red doméstica o de trabajo y red pública). Además, el usuario local no podrá cambiar esta configuración del firewall.
  - *Configuración 2*: El firewall debe estar abierto al protocolo ICMPv4 mediante una regla de entrada. El usuario local no podrá cambiar esta regla. La apertura de este protocolo permitirá a los administradores de red comprobar el estado de los equipos.
  - *Configuración 3*: Los usuarios, incluidos los usuarios locales, no tendrán la capacidad de instalar software en el los equipos mediante la herramienta Windows Installer. Esta herramienta es la que utiliza el sistema para instalar paquetes `.msi`.
  - *Configuración 4*: La capacidad del usuario local para activar el escritorio remoto de su equipo debe estar deshabilitada.

Operaciones previas

- Arranca los equipos PLX-C-53 y PLX-C-54.
- Ambos equipos deben encontrarse integrados en el dominio *practicas.local*. Sin embargo, en este momento, solo PLX-C-53 se encuentra integrado en el dominio. Debido a ello, agrega también PLX-C-54 al dominio.

  El usuario local *Alumno* no refleja apropiadamente el cometido asignado a los ordenadores PLX-C-53 y PLX-C-54 en este caso de trabajo. Debido a ello, será necesario crear un nuevo usuario acorde al caso de trabajo y eliminar el usuario *Alumno*, que dejará de tener sentido en estos equipos.

- En PLX-C-53 crea un nuevo usuario local llamado *Empleado*. Asígnale la contraseña *MVclave00*. En opciones de contraseña deja solo la opción *La contraseña nunca expira*. Agrégalo al grupo de administradores locales. Quítalo del grupo de usuarios locales. Cierra

sesión e inicia una nueva con el usuario *Empleado*. Al iniciar sesión por primera vez se crea su perfil y es necesario contestar a las preguntas del asistente que establece la configuración inicial del usuario. Contesta a todo NO. Una vez iniciada la sesión, elimina el usuario *Alumno* y borra su perfil.

- Repite el mismo proceso en PLX-C-54.

Procedimiento de resolución del caso

- Paso 1. En el controlador de dominio, mueve las cuentas de PLX-C-53 y PLX-C-54 a *Cientes-Admin*.
- Paso 2. En el controlador de dominio, crea el GPO *Caso-1* y vincúlalo a *Clientes-Admin*.
- Paso 3. Establecimiento de la *Configuración 1*.
  - Antes de aplicar las directivas necesarias, debes comprobar que el usuario *Empleado* tiene la capacidad de activar y desactivar el Firewall en todas las ubicaciones de red. Para ello, en cada equipo cliente, *Panel de control -> Sistemas y seguridad -> Firewall de Windows Defender -> Activar o desactivar el Firewall de Windows Defender*. NO CAMBIES NADA, simplemente, comprueba que puedes hacer cambios.
  - En la edición del GPO *Caso-1*, podrás encontrar las directivas requeridas en *Configuración del equipo -> Directivas -> Plantillas administrativas -> Red -> Conexiones de red -> Firewall de Windows*.

    (1) PREGUNTA. ¿Qué directivas son necesarias para aplicar la *Configuración 1*?

    ```
    Nombre de la directiva:
    Ruta desde Plantillas admin.:

    Nombre de la directiva:
    Ruta desde Plantillas admin.:
    ```

  - Configura en el GPO *Caso-1* las directivas pertinentes.
  - En PLX-C-53, ejecuta `gpupdate /force`. Comprueba que la directiva se ha aplicado y el comportamiento del firewall es el esperado.
  - Cuando todo esté comprobado en PLX-C-53, repite el proceso en PLX-C-54.
- Paso 4. Establecimiento de la *Configuración 2*.
  - Antes de aplicar las directivas necesarias, debes comprobar que ni PLX-C-53, ni PLX-C-54 responden al comando *ping*, realizado, por ejemplo, desde el equipo anfitrión. Comprueba también que en la herramienta *Windows Defender Firewall con seguridad avanzada* de estos equipos, en el apartado *Reglas de entrada*, no existe la regla *Permitir ICMPv4*.
  - En la edición del GPO *Caso-1*, para abrir el firewall al protocolo ICMPv4, debes buscar la herramienta necesaria en la ruta siguiente:

    Configuración del equipo -> Directivas -> Configuración de Windows -> Configuración de seguridad -> Windows Defender Firewall con seguridad avanzada.
  - Configura en el GPO *Caso-1* la regla *Permitir ICMPv4*.
  - En PLX-C-53, ejecuta `gpupdate /force`. Comprurba que la directiva se ha aplicado. Para ello, busca la regla *Permitir ICMPv4* en la herramienta *Windows Defender Firewall con seguridad avanzada* de este equipo. Comprueba que el equipo responde al comando *ping* realizado desde el anfitrión.
  - Cuando todo esté comprobado en PLX-C-53, repite el proceso en PLX-C-54.
- Paso 5. Establecimiento de la *Configuración 3*.
  - Antes de aplicar las directivas necesarias, debes comprobar que el usuario *Empleado* tiene la capacidad de instalar paquetes software `.msi` en ambos equipos. Para ello, sigue las instrucciones que se indican en los puntos siguientes.

- En PLX-C-53, primero, debes conectarte al recurso de distribución de software. Sin embargo, para establecer la conexión no debes utilizar el nombre UNC del recurso (\\192.168.0.1\RDS), ya que la conexión fallaría. El problema ocurre porque en PLX-C-53 estás utilizando un usuario local (*Empleado*), pero en un equipo que pertenece a un dominio. Por el hecho de pertenecer PLX-C-53 al dominio, el recurso RDS se trata como un recurso del dominio, y las solicitudes de acceso al recurso son redirigidas por el servidor de ficheros al controlador de dominio. Sin embargo, como el usuario activo en PLX-C-53 es local, las credenciales que se presentan el controlador de dominio no son válidas y la conexión no se establece. El fallo se produce entre el servidor de ficheros y el servidor de dominio, y en el ordenador cliente, lo único que se percibe es que no es establece la conexión. La SOLUCIÓN es establecer la conexión al servidor de ficheros sin especificar el nombre del recurso, o sea, utilizar el identificador UNC *\\192.168.0.1*, en vez de *\\192.168.0.1\RDS*. De esta forma, se fuerza al servidor de ficheros a solicitar credenciales al cliente. En este punto, de nuevo, la autenticación ocurre a nivel de dominio. Debido a ello, para establecer la conexión, hay que proporcionar las credenciales de un usuario del demonio (recuerda que en el recuro RDS se ha autorizado el acceso de lectura a los *Usuarios autentificados* en el dominio). Puedes suponer que el usuario que está utilizando PLX-C-53 posee las credenciales del usuario PAS1 en el dominio. Siguiendo las indicaciones anteriores, establece una conexión don el servidor de ficheros. Después, entra en la carpeta RDS y copia el paquete `.msi` en el escritorio de PLX-C-53.
- Procede a la instalación del paquete. En el caso de que se muestre alguna advertencia de seguridad, óbviala. Completa la instalación. Ésta ha sido llevada a cabo por Windows Installer.
- Ahora se procederá a la desinstalación del paquete. Para ello, *Panel de control -> Programas -> Desinstalar un programa*. Selecciona el paquete de 7-Zip instalado y desinstálalo.
- Ahora se requiere configurar la directiva que impide la instalación de paquetes `.msi`. En la edición del GPO *Caso-1*, puedes encontrar la directiva requerida en la ruta siguiente:

  Configuración del equipo -> Directivas -> Plantillas administrativas -> Componentes de Windows -> Windows Installer.

  (2) PREGUNTA. Indica el nombre de la directiva requerida para aplicar la *Configuración 3*.

- Esta directiva requiere especificar un campo de *Opciones*. Lee atentamente la información de ayuda proporcionada en la ventana de configuración de la directiva. Según esta información,

  (3) PREGUNTA. ¿Qué opción debes especificar en el campo *Opciones*?

- Configura en el GPO *Caso-1* la directiva pertinente, configurada de la forma apropiada.
- En PLX-C-53, ejecuta `gpupdate /force`.
- Para comprobar la aplicación de la directiva, trata de volver a instalar el paquete `.msi`. Debes comprobar que no es posible.

  (4) PREGUNTA. ¿Qué mensaje muestra Windows Installer?

- Cuando todo esté comprobado en PLX-C-53, repite el proceso en PLX-C-54.

o Paso 6. Establecimiento de la *Configuración 4*.

- Antes de aplicar las directivas necesarias, debes comprobar que el usuario *Empleado* tiene la capacidad de activar y desactivar el acceso remoto en PLX-C-53. Para acceder a la

configuración del acceso remoto, *Panel de control -> Sistema y seguridad -> Sistema*. Entonces, en el apartado *Vínculos relacionados*, pulsa sobre *Configuración avanzada del sistema*. Comprueba que tienes la capacidad de permitir o no el acceso remoto. No obstante, deja la configuración en su estado por defecto (*No permitir las conexiones remotas a este equipo*).

– En la edición del GPO *Caso-1*, podrás encontrar la directiva requerida para establecer la *Configuración 4* en la ruta siguiente:

Configuración del equipo -> Directivas -> Plantillas administrativas -> Componentes de Windows -> Servicios de escritorio remoto-> Host de sesión de escritorio remoto.

(5) PREGUNTA. ¿Qué directiva se requiere para aplicar la *Configuración 4*?

Nombre de la directiva: **Ruta desde Plantillas admin.:**

– Configura en el GPO *Caso-1* la directiva pertinente.

– En PLX-C-53, ejecuta `gpupdate /force`. Comprueba que la directiva se ha aplicado, es decir, el usuario *Empleado* ya no tiene la capacidad de habilitar la conexión remota al equipo.

– Cuando todo esté comprobado en PLX-C-53, repite el proceso en PLX-C-54.

- **Caso 2: Creación de un recurso compartido para los profesores de la organización y mapeo automático del recurso mediante unidad de red**

En las organizaciones resulta muy habitual el uso de recursos compartidos para la realización de trabajo colaborativo entre los usuarios de un determinado grupo. En este ejemplo se creará un espacio de colaboración para todos los profesores de la organización. Adicionalmente, para facilitar el uso de este espacio se mapeará automáticamente en el escritorio de los profesores una unidad de red correspondiente a dicho espacio.

Este ejercicio se abordará en tres fases. En la primera fase se configurará de la forma apropiada el recurso compartido. En la segunda fase se analizará cómo mapear automáticamente el recurso compartido en el escritorio de los usuarios. Y en la tercera fase se afinarán las unidades organizativas para tener el control necesario de los usuarios objetivo de las directivas.

Fase 1: Creación y configuración del recurso compartido

Este recurso se creará en el servidor de ficheros (PLX-S-FS).

- En este punto PLX-S-FS ya debe estar arrancado.
- En el servidor de ficheros, en la unidad D, crea una carpeta llamada *Compartida2*.
- Comparte *Compartida2* y configúrala para que solamente puedan acceder a ella los profesores de la organización, además de los administradores. Los usuarios profesores debe tener permisos de lectura y escritura en esta carpeta.
- Utiliza PLX-C-53 para comprobar la correcta configuración de *Compartida2*. Inicia sesión con un profesor del dominio y comprueba que puedes acceder a *Compartida2*, tanto para escritura como para lectura. Después inicia sesión con un alumno del dominio y comprueba que no puedes acceder a la carpeta ni para escritura ni para lectura.

Fase 2: Mapeo del recurso compartido mediante unidad de red

Mapeo manual

Cuando un recurso de red siempre está accesible para un usuario, éste puede facilitar su acceso al recurso mapeándolo como unidad de red. Entonces cuando el usuario inicia sesión, tiene el recurso disponible automáticamente.

- En PLX-C-53 inicia sesión con un profesor del dominio.

- Abre el *Explorador de archivos*. Botón derecho sobre *Este equipo -> Mostrar más opciones - > Conectar a unidad de red*. Utiliza como nombre de unidad la Z. Proporciona la ruta apropiada y deja seleccionada la opción *Conectar de nuevo al iniciar sesión*. Esto hará que la unidad esté disponible cada vez que el usuario inicia sesión. Comprueba que se crea la unidad Z y que es accesible.
- Cierra sesión e inicia una nueva con el mismo usuario. Comprueba que la unidad Z se encuentra mapeada y es accesible.
- Elimina el mapeo de la unidad Z. Para ello, botón derecho -> *Mostrar más opciones –> Desconectar*.

Mapeo automático

Se pretende proporcionar a los profesores el servicio de mapear automáticamente el área de trabajo correspondiente a *Compartida2*. Obsérvese que no es en absoluto habitual para usuarios que no sean del ámbito de la informática acceder a un recurso compartido utilizando *\\IP\RecursoCompartido* desde el menú *Inicio*. Para el usuario resultará mucho más natural tener mapeada automáticamente una unidad de red. La característica de mapear unidades de red es proporcionada por las preferencias de los objetos GPO.

- Para aplicar esta preferencia, en el servidor de dominio debes crear un objeto GPO llamado *Caso-2*. Crea este GPO ahora.

  (6) PREGUNTA. ¿A qué unidad organizativa debes vincular el GPO *Caso-2*? ¿Por qué? Si tienes dudas pregúntale a tu profesor.

- Vincula el GPO *Caso-2* a la unidad organizativa que acabas de indicar.
- Para mapear una unidad de red mediante el GPO *Caso-2*, edita el GPO. Entonces navega hasta *Configuración de usuario -> Preferencias -> Configuración de Windows -> Asignación de unidades*. Para abrir el asistente que genera la asignación, *botón derecho -> Nuevo -> Unidad asignada*. A continuación, se indican los campos que debes rellenar:
  - Campo *Acción*: vale cualquier valor salvo *Eliminar*. Puedes dejar *Actualizar*, que es el valor por defecto.
  - Campo *Ubicación*: debes indicar el identificador UNC del recuro compartido.

    (7) PREGUNTA. Indica el identificador UNC utilizado.

  - Casilla de verificación *Reconectar*: debes marcarla (esta configuración establece que la unidad de red se conecte cada vez que el usuario inicia sesión).
  - Opción *Letra de unidad*: elige Z.
- Una vez configurada y salvada la preferencia, en PLX-C-53, cierra la sesión abierta, e inicia una nueva sesión con *Prof1*. Comprueba que este usuario tiene mapeada la unidad Z y que tiene acceso a ella en lectura y escritura.
- Cierra la sesión de *Prof1* e inicia sesión con *Prof2*. Comprueba que este usuario también tiene asignada la unidad Z:

  (8) PREGUNTA. Si inicias sesión con el administrador del dominio, ¿tendrá este usuario mapeada la unidad Z? ¿Por qué?

- Comprueba tu respuesta iniciando sesión con dicho usuario. (NOTA: en el campo *Nombre de usuario*, cuando se escribe *Administrador*, el inicio de sesión cambia automáticamente al

ordenador local. Debido a ello, para iniciar sesión con el administrador del dominio, en el campo *Nombre de usuario* debes introducir *PRACTICAS\Administrador*.)

Fase 3: Reorganización de las unidades organizativas

En el esquema organizativo de este caso de trabajo se plantea un problema: hay un grupo de usuarios que reciben el mapeo de la unidad Z, sin que dicha unidad vaya orientada a ellos.

(9) PREGUNTA. ¿Cuál es este grupo de usuarios?

- Comprueba tu respuesta iniciando sesión con un usuario perteneciente a este grupo en PLX-C-53.

  (10) PREGUNTA. A pesar de tener mapeada la unidad Z, ¿tiene este grupo de usuarios acceso a la misma? ¿Por qué?

- Elimina la unidad Z mapeada para este usuario y cierra sesión.

  No es admisible que un grupo de usuarios reciba el mapeo de una unidad a la que no tienen acceso. El problema planteado tiene su origen en un refinamiento insuficiente de las unidades organizativas. Para solucionar el problema, el administrador del dominio debe reorganizar dichas unidades con el objetivo de tener un control más fino de los ámbitos de aplicación de las directivas. En este caso de trabajo la solución será separar los usuarios *PAS* y *Profesores* en unidades organizativas diferentes.

- En el controlador de dominio, crea una nueva unidad organizativa llamada *Profesores*. Mueve a los usuarios y al grupo correspondientes a este colectivo de la OU *Empleados* a la OU *Profesores*.
- Cambia la vinculación del GPO *Caso-2* de la forma apropiada.
- Utilizando PLX-C-53, inicia sesión sucesivamente con un usuario profesor y con un usuario PAS. Comprueba que el usuario del grupo profesores recibe el mapeo de la unidad Z, mientras que el usuario del grupo PAS, no lo recibe.
- En los casos de trabajo siguientes, ya no se requieren los equipos PLX-C-53 y PLX-C-54. Apágalos, con objeto de evitar un número excesivo de máquinas virtuales en ejecución.

Caso 3: Distribución de software mediante directivas de grupo

Las directivas de grupo tienen la capacidad de distribuir software a los equipos del dominio. En este caso de trabajo se plantea la distribución de un paquete de software a los equipos dedicados al soporte de la actividad docente en la organización de ejemplo. A modo de ejemplo, se supone que esos equipos son el PLX-C-51 y el PLX-C-52.

Especificaciones del caso

- Equipos objetivo
  - PLX-C-51
  - PLX-C-52
- Paquete de software a distribuir:
  - 7-Zip de tipo ".msi" y de 64-bit para Windows x64.
  - Ubicación del fichero: \\192.168.0.1\RDS. El paquete ya fue copiado a este recurso durante el desarrollo del Caso 1.

Procedimiento de resolución del caso

Preparación de un recurso de distribución de software

Para distribuir software mediante directivas de grupo es necesario disponer de un recurso de distribución de software que sea accesible para todos los ordenadores del dominio. Dicho recurso se implementa mediante una carpeta compartida. En el apartado *Actuaciones preliminares*, ya se configuró un recurso de distribución de software. Ese recurso se utilizará también en la resolución de este caso práctico.

(11) PREGUNTA. Indica el identificador UNC del recurso de distribución de software desplegado en el apartado *Actuaciones preliminares*.

Preparación de las unidades organizativas

En el momento actual, PLX-C-51 y PLX-C-52 no se encuentran asignados a ninguna unidad organizativa. En este caso de trabajo, estos equipos asumen el rol de equipos dedicados al soporte de la actividad docente. Debido a ello, su ubicación debe ser la unidad organizativa *Clientes-Docencia*.

- En el controlador de dominio, mueve las cuentas de los equipos PLX-C-51 y PLX-C-52 a la unidad organizativa *Clientes-Docencia*.

Configuración de un GPO para la instalación del software

- Antes de crear y configurar el GPO requerido, con el objetivo de facilitar el manejo del recurso de distribución de software en el controlador de dominio, la mejor opción es mapear dicho recurso mediante una unidad de red. Para ello, en el controlador de dominio, abre el *Explorador de archivos* -> botón derecho sobre *Este equipo* -> *Conectar a unidad de red*. Utiliza S: como nombre de unidad y mapea el recurso *RDS* en la forma apropiada.
- Crea el GPO *Caso-3* y vincúlalo a la unidad organizativa *Clientes-Docencia*.
- Edita el GPO. Navega hasta *Configuración del equipo -> Directivas -> Configuración de software -> Instalación de software*. Entonces *Botón derecho* sobre *Instalación de software -> Nuevo -> Paquete*. Utilizando la unidad S, selecciona el paquete `.msi`. En la ventana *Implementar software*, selecciona *Asignada* como método de implementación. En este momento el software está listo para desplegarse.

Instalación del software

- Arranca PLX-C-51, e inicia sesión con el *Administrador* del dominio. Entonces *Panel de control -> Programas -> Programas y características*. Comprueba que *7-Zip* no se encuentra instalado.
- Con objeto de que la directiva de instalación de software se aplique, abre una consola y ejecuta `gpupdate /force`. Comprobarás que la directiva de instalación de software requiere el reinicio del equipo para su completa aplicación. Reinicia el equipo, tardará un poco en iniciarse, ya que durante el inicio se realizará la instalación del software. Inicia sesión con el *Administrador* del dominio. Abre el menú *Inicio -> Todas las aplicaciones*, y comprueba que *7-Zip* se ha instalado satisfactoriamente y que tienes la capacidad de ejecutarlo.
- Repite todo el proceso PLX-C-52.

  En un entorno de producción, los clientes detectarían la aplicación de la directiva en un proceso de segundo plano. Sin embargo, el software no se instalaría hasta que ocurriese el próximo reinicio en el equipo.

  La capacidad de las directivas de grupo para la distribución de software resulta de gran utilidad. No obstante, Microsoft dispone de herramientas mucho más evolucionadas para este cometido, como por ejemplo, la infraestructura de distribución de aplicaciones virtualizadas, o los servicios de implementación de Windows (WDS).

- Una vez completado este caso, ya no son necesarias las máquinas PLX-C-51 y PLX-C-52. Apágalas.

• Caso 4: Preparación de entorno de trabajo para una asignatura

Un profesor de la organización desea preparar un entorno de trabajo para impartir una asignatura de programación de servicios. Los estudiantes deben desarrollar un trabajo de programación en grupo. Se establece que la mejor opción para el entorno de trabajo de los estudiantes es desplegar una MV para cada grupo, en la que los miembros del grupo puedan desarrollar el trabajo de forma colaborativa.

Para establecer el control de acceso a las MV de los alumnos, así como las "autorizaciones de acceso a recursos" requeridas, se establece que la mejor opción es utilizar la infraestructura de directorio activo de la organización. En este caso de trabajo se plantea cómo utilizar esta infraestructura para gestionar las MV de los alumnos. Asimismo, se establecen algunas directivas de grupo para distribuir información y proporcionar acceso a algunos recursos requeridos para la asignatura. En la resolución de este caso de trabajo se utilizará también el servidor de ficheros como repositorio para almacenamiento y distribución de material.

Con objeto de no desplegar nuevas máquinas virtuales, que consumen recursos de disco, en este caso de trabajo se utilizará una máquina ya desplegada. Se trata de PLX-S-PRUEBAS-YYY. Se utilizará esta máquina como ejemplo de la MV a utilizar por un grupo de alumnos.

Este caso de trabajo es más amplio que los anteriores y platea el uso de diversas técnicas de gestión utilizadas en el ámbito del directorio activo, incluyendo la gestión de recursos compartidos, la gestión de derechos de usuario y la aplicación de políticas administrativas.

Procedimiento de resolución del caso

Preparación de la máquina virtual

- Adecúa la identificación de la MV para reflejar apropiadamente su cometido en el dominio.
  - Nombre de la MV: A01-G1 (los identificadores significan *Asignatura_Grupo*)
  - Nombre del disco virtual: A01-G1.vhdx
- Conecta la MV a *Red virtual interna*
- Arranca la MV y realiza las configuraciones siguientes:
  - Nombre del sistema: A01-G1
  - Configuración IP: La MV se configura en la subred del dominio, asignándole la IP 201.

    (12) PREGUNTA. ¿Qué valores has utilizado en la configuración IP de la MV?

    ```
    Dirección IP:
    Puerta de enlace:
    DNS:
    ```

  - Comprueba que puedes hacer ping desde la MV a la puerta de enlace y al DNS de la red.
  - Agrega la MV al dominio *practicas.local*. Reiníciala para que el cambio tenga efecto.

Configuración de unidades organizativas

Para la gestión de las MV de los alumnos, se requiere desplegar un conjunto de unidades organizativas que permitan aplicar las políticas adecuadas a las MV y a los usuarios de los alumnos y del profesor de la asignatura.

- En el controlador de dominio, crea la unidad organizativa *Asignaturas* debajo del dominio.
- Dentro de *Asignaturas*, crea las unidades organizativas A01-C y A01-U. A01 representa el identificador de la asignatura, la C indica *Computer*, y la U, *User*. Así, A01-C está orientada a contener las cuentas de las MV (*computers*), y A01-U, las cuentas de los usuarios.
- En la unidad organizativa A01-U, crea los usuarios A01-Alu1, A01-Alu2 y A01-Prof.

- Para asignar derechos a todos los alumnos del grupo, en la unidad organizativa A01-U, crea el grupo de seguridad A01-AluG1 y agrégale los usuarios A01-Alu1 y A01-Alu2.
- Mueve la cuenta de equipo A01-G1 a la unidad organizativa A01-C.

Creación y configuración de un recurso de almacenamiento

La asignatura necesita un recurso de almacenamiento con un doble cometido: 1) distribución de material a los alumnos (paquetes de software, imágenes ISO, documentación, etc.), y 2) especio de escritura para los alumnos, para que puedan almacenar sus desarrollos en una ubicación accesible para el profesor, para su seguimiento.

- En el servidor de ficheros, en la unidad D, crea la siguiente estructura de carpetas:

```
Asignaturas
 └─ A01
     └─ A01AluG1
     └─ A01RD
```

- La carpeta *A01AluG1* es el espacio de escritura para los alumnos del grupo G1. Comparte esta carpeta y asigna los derechos adecuados a los alumnos y al profesor.

  (13) PREGUNTA. Al compartir esta carpeta, además de *Administrador* y *Administradores*, debes agregar un usuario y un grupo. Señálalos a continuación, indicando también el nivel de permiso que les has asignado.

- La carpeta *A01ARD* es el recurso de distribución para distribuir material a los alumnos. Comparte esta carpeta y asigna los derechos adecuados a los alumnos y al profesor.

  (14) PREGUNTA. Al compartir esta carpeta, además de *Administrador* y *Administradores*, debes agregar un usuario y un grupo. Señálalos a continuación, indicando también el nivel de permiso que les has asignado.

Asignación de derechos de administración a los alumnos en la MV

Los usuarios pertenecientes a un grupo de prácticas, necesitan tener el control total de su MV, ya que, por ejemplo, necesitarán instalar y desinstalar software, así como llevar a cabo otras configuraciones en el sistema. Para ello, es necesario que el grupo de alumnos creado en el dominio se agregue al grupo de *Administradores* locales de la MV.

- En A01-G1, utilizando *Administración de equipos -> Usuarios y grupos locales*, agrega al grupo *Administradores* (que son administradores locales) el grupo del dominio *A01-AluG1*.

Aplicación de políticas administrativas

Como ejemplos de aplicación de políticas administrativas, se aplicarán dos directivas, una de ellas a los usuarios del grupo de alumnos, y otra, a la MV (o sea, al equipo).

Creación de objetos GPO

- En el servidor de dominio, para aplicar las políticas orientadas a los usuarios, crea un GPO denominado *A01-Politicas-Usuarios*. Entonces, vincúlalo a la unidad organizativa *A01-U*.
- Para aplicar las políticas orientadas a la MV (o sea, al equipo), crea un GPO denominado *A01-Politicas-MV*. Entonces, vincúlalo a la unidad organizativa *A01-C*.

Directiva 1 (orientada a usuarios)

- El administrador del dominio desea ubicar de forma automática un fichero con información esencial del entorno de trabajo en el escritorio de los alumnos. Para hacer accesible el fichero informativo a la MV de los alumnos, el administrador del dominio decide utilizar un recurso de distribución ya configurado en el controlador del dominio. Se trata del recurso compartid ZZRD (ubicado en el volumen C), que se utilizó en la sesión anterior para distribuir *Script-Inicio.vbs*.
- En el controlador de dominio, en la carpeta *C:\ZZRD*, crea la carpeta A01, y dentro de ella, un fichero de texto llamado *Leeme-A01-G1.txt*. A modo de ejemplo, escribe en el fichero el texto siguiente: "MV para uso del grupo G1 de la asignatura A01".
- En el servidor de dominio, en el GPO *A01-Politicas-Usuarios*, *Edita* y navega hasta la preferencia siguiente:

  Configuración de usuario -> Preferencias -> Configuración de Windows -> Archivos

  Crea una nueva preferencia de archivo. Utiliza los parámetros siguientes:

  – Campo *Acción*: *Actualizar*
  – Archivos de origen: *\\192.168.0.25\ZZRD\A01\Leeme-A01-G1.txt*
  – Archivo destino: *%DesktopDir%\Leeme.txt* (NOTA: %DesktopDir% es una variable de entorno que significa "la carpeta del escritorio del usuario actual".

Directiva 2 (orientada a usuarios)

- Se desea mapear, de forma automática, los recursos compartidos *A01AluG1* y *A01RD*, como unidades de red, accesibles para los alumnos, en la MV *A01-G1*.
- En el GPO *A01-Politicas-Usuarios*, *Edita* y navega hasta la preferencia siguiente:

  Configuración de usuario -> Preferencias -> Configuración de Windows -> Asignación de unidades

  Crea una preferencia de asignación de unidades. Utiliza los parámetros siguientes:

  – Campo *Acción*: *Actualizar*
  – Campo *Ubicación*: *\\192.168.0.1\A01AluG1*
  – Casilla de verificación *Reconectar*: Marcada
  – Letra de unidad: Y

  Crea una segunda preferencia de asignación de unidades. Utiliza los parámetros siguientes:

  – Campo *Acción*: *Actualizar*
  – Campo *Ubicación*: *\\192.168.0.1\A01RD*
  – Casilla de verificación *Reconectar*: Marcada
  – Letra de unidad: Z

Directiva 3 (orientada a las MV)

- Se considera esencial que el *firewall* de las MV esté activado y que no se permita a los usuarios desactivarlo.
- En el GPO *A01-Politicas-MV*, *Edita* y navega hasta la directiva siguiente:

  Configuración del equipo -> Directivas -> Plantillas administrativas -> Red -> Conexiones de red -> Firewall de Windows.

  Entonces, tanto en *Perfil de dominio* como en *Perfil estándar*, Habilita la directiva *Firewall de Windows Defender: proteger todas las conexiones de red*.

Pruebas

Pruebas con un usuario de la asignatura

- Primero, vas iniciar sesión con un usuario de la asignatura. Entonces comprobarás que dicho usuario tiene acceso a los diferentes recursos desplegados para la asignatura. Asimismo, el

usuario tendrá la capacidad de realizar cualquier operación administrativa en la MV, como por ejemplo, cambiar la configuración de la red o instalar un paquete de software.

- En A01-G1, cierra la sesión que tienes abierta con el *Administrador* local (se supone que los alumnos de la asignatura no tienen las credenciales de este usuario). Entonces, inicia una nueva sesión con el usuario *A01-Alu1*.
- Como es la primera vez que se inicia sesión con este usuario se crea su perfil. El Administrador del servidor arranca automáticamente. Para inhabilitar este comportamiento, menú *Administrar -> Propiedades del administrador del servidor*. Entonces, marca la casilla de verificación *No iniciar el Administrador del servidor automáticamente al iniciar sesión*.
- Cierra el *Administrador del servidor*.
- Observa que el escritorio tiene tono azul, en vez de verde. Eso se debe a que se aplica el perfil por defecto al nuevo usuario (*A01-Alu1*), y en el perfil por defecto el escritorio es azul.
- Para que se apliquen las directivas de equipo, además de las de usuario, ejecuta el comando *gpupdate /force*.
- Con objeto de disponer de un paquete de software en el recuso de distribución de la asignatura, copia el paquete del 7-Zip en el recurso compartido *A01RD*.
- Realiza las siguientes comprobaciones:
  - Se ha copiado al escritorio del usuario un fichero.

    (15) PREGUNTA. ¿Cuál es?

  - El usuario tiene mapeadas las unidades Y y Z. Comprueba que en una de las unidades el usuario tiene acceso de lectura y escritura, y en la otra, solo de lectura.

    (16) PREGUNTA. Indica el tipo de acceso que tiene en cada una de ellas.

Y:
Z:

  - El *Firewall de Windows Defender* está habilitado en todos los perfiles de red (dominio, privada y pública) y el usuario no tiene la capacidad de modificar esta configuración.
  - El usuario tiene la capacidad de realizar tareas administrativas privilegiadas, como por ejemplo, modificar la configuración IP del sistema.
  - El usuario tiene la capacidad de instalar software en el sistema. Utiliza para ello el paquete de software del 7-Zip. Para hacer esta comprobación, instala el paquete. Después, desinstálalo, usando la utilidad *Programas* del *Panel de control*.

Pruebas con un usuario no perteneciente a la asignatura

- En este caso, vas a iniciar sesión con un usuario ajeno a la asignatura A01. Entonces comprobarás que dicho usuario no tiene acceso a los diferentes recursos desplegados para la asignatura, y sus capacidades administrativas están restringidas a las de un usuario normal, sin privilegios de administración.
- En A01-G1, cierra la sesión que tienes abierta con *A01-Alu1*. Entonces, inicia una nueva sesión con el usuario *Alu1*. Se trata de un usuario del dominio no perteneciente a la asignatura A01.
- Para que se apliquen las directivas de equipo, además de las de usuario, ejecuta el comando *gpupdate /force*.
- Realiza las siguientes comprobaciones:
  - No se ha copiado al escritorio del usuario el fichero *Léeme.txt*.
  - No se han mapeado las unidades Y y Z.

(17) PREGUNTA. Indica cómo se encuentra el *Firewall de Windows Defender* y porqué.

(18) PREGUNTA. ¿Qué ocurre si tratas de modificar la configuración IP del equipo?

Lo ocurrido al tratar de modificar la dirección IP se debe a que el usuario *Alu1* no pertenece al grupo de *Administradores* del equipo.

- Establece una conexión con el servidor de ficheros mediante *\\192.168.0.1*. Entonces abre el recurso de distribución de software, RDS, y copia el paquete del 7-Zip en el escritorio. Ejecuta el instalador hasta que llegues a la ventana *Ready to Install*. Entonces, pulsa *Install*.

(19) PREGUNTA. ¿Qué ocurre?

De la misma forma que al tratar de modificar la configuración de la IP, lo ocurrido al instalar software se debe a que *Alu1* no pertenece al grupo *Administradores* del equipo.