I.E.S. Fernando Aguilar Quignon
C/Conil de la Frontera, 3
CP 11010, Cádiz

Administración de Sistemas Operativos - 2ª Evaluación (RA 1 – CE a,b,c,d,e,f,g,h,i,j)

Unidad Didáctica 7. Implantación de dominios

La empresa **TechNet Solutions**, especializada en consultoría IT y desarrollo de software, ha decidido optimizar su infraestructura de red debido al crecimiento de su plantilla y a la necesidad de mejorar la seguridad y administración de sus recursos informáticos.

Actualmente, la organización presenta los siguientes problemas en su red:

- **Falta de un sistema de autenticación centralizado**, lo que dificulta la gestión de usuarios y permisos.
- **Asignación manual de direcciones IP**, lo que genera conflictos de red y dificultades en la administración.
- **Falta de redundancia en los datos**, lo que podría provocar pérdida de información en caso de fallo de hardware.
- **Gestión ineficiente del almacenamiento**, con empleados que ocupan espacio sin restricciones.
- **Accesos no controlados a recursos compartidos**, lo que compromete la seguridad de la información.
- **Ausencia de copias de seguridad automatizadas**, lo que expone la empresa a riesgos ante fallos o ataques.

Para solucionar estos problemas, el departamento de TI ha propuesto la implementación de un **dominio en Windows Server 2016 con Active Directory**, asegurando que todos los empleados tengan acceso seguro y controlado a los recursos. A lo largo de este proyecto, el equipo técnico deberá desplegar los siguientes servicios y configuraciones en un entorno corporativo realista.

Apartados a Desarrollar

1. Instalación y configuración de Active Directory

TechNet Solutions necesita una **infraestructura de dominio** que permita la administración centralizada de **usuarios, equipos y políticas de seguridad**. Para ello, el equipo técnico deberá desplegar un **entorno de Active Directory en Windows Server 2016** con una estructura lógica bien definida.

Las tareas a desarrollar incluyen:

- **Instalación y configuración de Active Directory** en un servidor Windows Server 2016.
- **Definición del nombre de dominio** corporativo (technet.local) que identificará la organización dentro de la red.
- **Creación de Unidades Organizativas (OUs)** que representen la jerarquía y estructura de la empresa. Estas OUs permitirán la correcta administración de usuarios, equipos y políticas.
- **Establecimiento de cuentas de usuario** con roles diferenciados y permisos adecuados según el departamento al que pertenezcan.
- **Creación de plantillas de usuario para agilizar la gestión de cuentas en Active Directory y garantizar una administración eficiente.** Para garantizar una administración uniforme y simplificar la creación de nuevos usuarios, se implementarán **plantillas de usuario en Active Directory**. Estas plantillas facilitarán la incorporación de nuevos empleados al dominio al permitir la asignación rápida y estandarizada de permisos y configuraciones específicas para cada departamento.

  El uso de plantillas de usuario **evitará errores manuales** y asegurará que los nuevos empleados tengan los mismos accesos y restricciones que los demás miembros de su equipo. En lugar de crear cada cuenta desde cero, el equipo de TI podrá copiar la configuración de una cuenta predefinida y asignarla a un nuevo usuario, garantizando así coherencia en la gestión de accesos.

La estructura de **Unidades Organizativas (OUs) en Active Directory** de TechNet Solutions se diseñará para facilitar la administración centralizada de usuarios, equipos, permisos y recursos dentro del dominio technet.local.

Para ello, se definirán las siguientes unidades organizativas:

- **Usuarios**, donde se organizarán las cuentas de los empleados según su departamento. Dentro de esta OU, se crearán subunidades para cada área de la empresa:
    - **Desarrollo**, que incluirá a los programadores y técnicos encargados del desarrollo de software.
    - **Soporte**, donde estarán los técnicos responsables del mantenimiento y la asistencia a clientes internos y externos.
    - **Ventas**, que agrupará a los comerciales y encargados de gestión de clientes.
    - **Administración**, donde se gestionarán los empleados dedicados a la contabilidad y gestión financiera.
    - **Recursos Humanos**, encargados de la gestión de personal y contratación.
- **Equipos**, que contendrá las estaciones de trabajo y dispositivos de los empleados, organizados por departamentos:
    - **PCs Desarrollo**, donde se incluirán los equipos utilizados por el departamento de desarrollo.
    - **PCs Administración**, que agrupará los ordenadores de la administración y contabilidad.
    - **PCs Soporte**, con los equipos utilizados por los técnicos de soporte.
- **Grupos de Seguridad**, que permitirán asignar permisos de acceso a recursos y configuraciones específicas. Los principales grupos de seguridad serán:
    - **Grupo_Desarrollo**, que tendrá acceso a los proyectos internos de software.

- **Grupo_Soporte**, con permisos para acceder a la documentación técnica y herramientas de asistencia.
- **Grupo_Ventas**, que dispondrá de acceso a la base de datos de clientes y herramientas de CRM.
- **Grupo_Administración**, con permisos sobre la contabilidad y documentos financieros de la empresa.
- **Grupo_TI**, que tendrá privilegios avanzados para la administración de los servidores y sistemas críticos.

- **Recursos Compartidos**, donde se gestionarán las carpetas y archivos accesibles para cada departamento. Se definirán carpetas con permisos específicos para cada grupo:
  - **\server\Desarrollo**, accesible exclusivamente para el equipo de desarrollo.
  - **\server\Soporte**, donde se almacenará documentación y herramientas del departamento de soporte.
  - **\server\Administración**, que contendrá información financiera y documentos administrativos, accesible solo para el grupo de administración.
- **Recursos Publicados en Active Directory**, que facilitarán el acceso a dispositivos y archivos compartidos en la red:
  - **\server\ImpresoraOficina**, una impresora de red accesible desde cualquier equipo de la empresa.
  - **\server\Plantillas**, una carpeta compartida con documentos estándar de la organización.

Esta estructura permitirá gestionar de manera eficiente el acceso a los recursos de la empresa, garantizando que cada usuario disponga de los permisos adecuados según su rol, además de facilitar la administración de políticas de seguridad y organización de los dispositivos de la red.

2. Integración con los servicios DNS, DHCP e impresión

Para garantizar el correcto funcionamiento del dominio, es necesario integrar Active Directory con otros servicios clave:

- **DNS:** Se debe configurar un servidor DNS para la resolución de nombres dentro del dominio, asegurando que los clientes puedan localizar el controlador de dominio.
- **DHCP:** Se debe configurar un servidor DHCP para la asignación automática de direcciones IP a los dispositivos de la red, evitando conflictos y optimizando la gestión de direcciones.
- **Impresión:** Se deben **publicar las impresoras de oficina en Active Directory**, permitiendo que los empleados accedan a ellas de manera centralizada según su departamento.

El éxito de esta integración garantizará la estabilidad y eficiencia de la infraestructura de red.

3. Configuración de almacenamiento redundante en RAID 5

Para proteger la información de la empresa y evitar pérdidas de datos en caso de fallo de hardware, se implementará un sistema de almacenamiento redundante en **RAID 5**, que proporcionará tolerancia a fallos y un equilibrio entre rendimiento y seguridad.

El equipo técnico deberá:

- **Configurar tres discos en el servidor** y establecer un volumen **RAID 5** para mejorar la seguridad y el rendimiento del almacenamiento.
- **Asignar este volumen** para el almacenamiento de **perfiles móviles, carpetas compartidas y backups**, asegurando que los datos críticos de la empresa estén protegidos ante fallos de disco.

- **Simular un fallo de disco** en el entorno RAID 5 para verificar la capacidad de recuperación del sistema. Durante esta prueba, se deberá retirar uno de los discos del RAID y comprobar que el sistema sigue funcionando sin pérdida de datos.
- **Añadir un nuevo disco al RAID 5** y proceder con la **reconstrucción del volumen**, asegurando que toda la información almacenada se restaure sin afectar la operativa de la empresa.
- **Verificar el estado de RAID** tras la reconstrucción, comprobando que el nuevo disco ha sido correctamente integrado y que el sistema vuelve a contar con la redundancia establecida.

Este proceso garantizará que la empresa pueda continuar operando sin interrupciones en caso de fallo de hardware y que la infraestructura de almacenamiento sea capaz de recuperar datos de manera automática y eficiente.

4. Implementación de perfiles móviles y asignación de cuotas de almacenamiento

Dado que muchos empleados trabajan desde diferentes estaciones de trabajo dentro de la empresa, es necesario configurar **perfiles móviles**, permitiendo que sus configuraciones y documentos los acompañen en cualquier equipo donde inicien sesión.

Además, para evitar un uso descontrolado del almacenamiento, se deben definir **cuotas de disco** que limiten el espacio asignado a cada usuario, optimizando así los recursos del servidor.

Este apartado garantizará una gestión eficiente del espacio y mejorará la movilidad interna de los empleados.

5. Aplicación de políticas de seguridad mediante GPOs

Para garantizar el cumplimiento de las normas de seguridad de TechNet Solutions, se aplicarán **Directivas de Grupo (GPOs)** a nivel de dominio.

Entre las políticas que deberán implementarse destacan:

- **Restricción del acceso al Panel de Control y Configuración** en usuarios estándar.
- **Redirección de carpetas personales a la unidad del servidor** para centralizar los documentos.
- **Desactivación de dispositivos USB y Bluetooth** para evitar fugas de información.
- **Aplicación de una política de contraseñas robusta**, incluyendo longitud mínima y renovación periódica.
- **Establecimiento de un fondo de pantalla corporativo** y bloqueo de cambios de apariencia.
- **Implementación de un protector de pantalla con bloqueo automático** tras un tiempo de inactividad.
- **Despliegue centralizado de software corporativo** como Office y navegadores web.
- **Desinstalación de aplicaciones no autorizadas** para evitar riesgos de seguridad.

Las **GPOs** son esenciales para **estandarizar la seguridad, personalizar el entorno de trabajo y garantizar la correcta administración de los equipos en la red corporativa**.

6. Creación de carpetas compartidas con permisos diferenciados

TechNet Solutions necesita un sistema de almacenamiento compartido para que los empleados de cada departamento puedan acceder a sus archivos de trabajo de manera segura.

Se deberán crear carpetas compartidas en el servidor con **permisos diferenciados** según los grupos de Active Directory. Por ejemplo:

- \\server\Desarrollo → Accesible solo para el departamento de desarrollo.
- \\server\Soporte → Accesible solo para el equipo de soporte técnico.

- \\server\Administración → Accesible solo para el equipo de administración.

Este apartado garantizará la organización de la información y el acceso seguro a los recursos.

7. Publicación de recursos en el servicio de directorio

Para facilitar la gestión de los recursos en la empresa, se deberán **publicar impresoras, carpetas compartidas y otros recursos en Active Directory**.

El equipo técnico deberá asegurarse de que los usuarios puedan encontrar e instalar estos recursos de manera sencilla a través del servicio de directorio.

Esto permitirá una administración centralizada y simplificará el acceso a los servicios internos.

8. Configuración de un sistema de copias de seguridad

Dado que la información empresarial es un activo crítico, se debe implementar un **sistema de copias de seguridad automatizado** para proteger los datos en caso de fallos o ataques.

El equipo técnico deberá:

- Configurar **Windows Server Backup** para realizar copias programadas de archivos críticos.
- Asegurar que las copias se almacenen en un disco independiente o en una ubicación externa.
- Realizar pruebas de restauración para verificar la efectividad del backup.

Este apartado garantizará la continuidad operativa y la recuperación ante desastres.

9. Unión de equipos cliente (Windows y GNU/Linux) al dominio y verificación de autenticación

Para validar el correcto funcionamiento del dominio, los técnicos deberán unir **equipos Windows y Linux** a Active Directory y comprobar que los usuarios pueden autenticarse correctamente.

Se evaluará la correcta integración de los equipos con el dominio y la aplicación de políticas definidas en GPOs.

Esto permitirá verificar que la infraestructura es funcional y que los usuarios pueden trabajar de manera segura en el entorno corporativo.

10. Configuración de relaciones de confianza entre dominios

TechNet Solutions está en proceso de expansión y ha adquirido una empresa subsidiaria, **InnovaTech**, que cuenta con su propia infraestructura IT y dominio independiente (innovatech.local). Para facilitar la colaboración entre ambas empresas y permitir la administración centralizada de usuarios y recursos, es necesario **establecer una relación de confianza entre dominios**.

El equipo técnico deberá configurar un **Trust Relationship** entre los dominios technet.local y innovatech.local, permitiendo que los usuarios de ambas organizaciones puedan autenticarse y acceder a los recursos compartidos sin necesidad de crear cuentas duplicadas en cada dominio.

Para ello, se deberán definir los siguientes aspectos:

- **Tipo de confianza**: Determinar si la relación será **unidireccional o bidireccional**, dependiendo de los requerimientos de acceso entre ambas empresas.
- **Nivel de confianza**: Especificar si la relación será **de confianza externa, de bosque o de dominio**, dependiendo de la infraestructura existente.
- **Configuración de permisos de acceso**: Definir qué grupos de usuarios podrán autenticarse en el dominio asociado y qué recursos estarán disponibles para ellos.

- **Pruebas de autenticación**: Validar que los usuarios de innovatech.local puedan iniciar sesión en technet.local y viceversa, asegurando que las credenciales se validen correctamente.
- **Seguridad y auditoría**: Implementar registros y políticas de acceso para monitorear las interacciones entre los dominios y garantizar que solo los usuarios autorizados puedan acceder a los recursos compartidos.

Con esta configuración, se facilitará la integración entre ambas organizaciones, permitiendo el uso de aplicaciones comunes, el acceso a archivos compartidos y la colaboración entre equipos de trabajo sin necesidad de administrar cuentas por separado en cada dominio.

Entrega del Proyecto

Los técnicos deberán presentar un **informe detallado**, en formato PDF, con la documentación de cada una de las configuraciones realizadas, capturas de pantalla y pruebas de funcionamiento.

El informe deberá incluir:

- Explicación de la implementación.
- Capturas de configuración y evidencias de funcionamiento.
- Resultados de pruebas de acceso y políticas aplicadas.
- Posibles incidencias encontradas y soluciones aplicadas.

Además, se realizará una **presentación final**, en formato MP4, donde cada técnico expondrá su trabajo.