Administración de Sistemas Operativos

UD 04. Proyecto Windows Server – Implementación de Directivas de Grupo.

Licencia

Nomenclatura

A lo largo de este tema se utilizarán diferentes símbolos para distinguir elementos importantes dentro del contenido. Estos símbolos son:

Importante

Atención

Interesante

A entregar

UD04. PROYECTO WINDOWS SERVER

1. FECHA DE ENTREGA

Fecha límite de entrega: Indicada en el campus.

La actividad será evaluada cuando haya pasado la fecha límite de la entrega.

! **Atención:** la fecha de entrega no es prorrogable. Si no la entregas en tiempo y forma, la calificación de la actividad será 0.

2. OBJETIVOS:

El alumnado aprenderá a crear y gestionar un dominio dentro de Windows Server 2022. Se trabajará la creación de usuarios, unidades organizativas, la aplicación de directivas de grupo, la configuración de perfiles móviles y fijos, la compartición de impresoras por departamento (Unidad Organizativa) y el acceso a directorios según la OU asignada.

3. LAB STEPS

- Encender la máquina virtual LON-DC01.
- Revisar la existencia de los objetos creados en la práctica anterior.

Item	Nombre	Comentario
Unidad Organizativa	Development	
Unidad Organizativa	Managers	
Unidad Organizativa	Marketing	
Unidad Organizativa	Research	
Unidad Organizativa	Sales	
Unidad Organizativa	IT	
Usuario	Antonio de Triana	Dentro de la UO IT
Usuario	Isco	Dentro de la UO Development
Usuario	Marc Bartra	Dentro de la UO Managers
Usuario	<Nombre del Alumn@>	Dentro de la UO Marketing
Usuario	<Apellido del Alumn@>	Dentro de la UO Research
Usuario	Pablo Fornals	Dentro de la UO Sales
Usuario	Cucho Hernández	Dentro de la UO Sales

Entregable 1: Capture la pantalla donde se muestre las unidades organizativas.

4. ESCENARIO.

En esta práctica, los alumnos asumirán el rol de administradores de sistemas en una entidad deportiva ficticia, el club de fútbol Real Betis Balompié. La entidad quiere centralizar la gestión de sus empleados y departamentos mediante un Dominio Active Directory instalado en Windows Server 2022.

El objetivo es implementar una infraestructura de AD que permita organizar a los jugadores, entrenadores y el personal administrativo en unidades organizativas (OUs) correspondientes,

ofreciendo acceso controlado a recursos internos mediante directivas de grupo, perfiles de usuario y recursos compartidos.

Se creará el dominio "betis.local" en un servidor Windows Server 2022 configurado para servir como controlador de dominio principal. Los usuarios serán los jugadores actuales del Betis, divididos según su posición (delanteros, centrocampistas, defensas, porteros), más un grupo administrativo para el personal no deportivo.

Cada OU tendrá:

- Usuarios con cuentas creadas con nombres reales de jugadores del Betis (p.ej. Rui Silva, Sergio Canales).
- Directivas de grupo para restringir y personalizar el entorno de los usuarios, como deshabilitar el acceso a paneles de control, restringir acceso a unidades USB o establecer fondos de pantalla corporativos.
- Configuración de perfiles móviles y fijos para que los jugadores puedan acceder a su entorno de usuario personalizado desde cualquier terminal del club.
- Compartición de impresoras y carpetas de red específicas para cada área (OUs), permitiendo controlar el acceso según departamento.

Los alumnos practicarán desde la creación del dominio, la estructura del AD, hasta la gestión avanzada de políticas y recursos compartidos, preparando un entorno cercano a un caso real de empresa o institución que gestiona personal y recursos distribuidos.

Deberán documentar todo el proceso con capturas y explicaciones breves de los efectos de cada configuración, fomentando la comprensión del impacto de cada ajuste en la experiencia y seguridad de los usuarios.

5. ACTIVIDAD 01

1. Instalación de Active Directory y creación del dominio

- Instala el rol Servicios de dominio de Active Directory en tu máquina Windows Server 2022.
- Ejecuta el asistente para promocionar el servidor a controlador de dominio. Usa el nombre de dominio: betis.local.
- Confirma que el dominio y el servicio estén activos y accesibles.

2. Creación de Unidades Organizativas (OU)

- Accede a la consola Usuarios y equipos de Active Directory.
- Crea al menos estas OUs:
    - Delanteros
    - Centrocampistas
    - Defensas
    - Porteros
    - Administración
- Inserta una descripción breve en cada OU sobre su función.

3. Creación de usuarios (jugadores del Betis)

- Para cada OU deportiva, crea los siguientes usuarios:
  - OU llamada Porteros:
    - Álvaro Valles, Pau López, Adrián, Fran Vieites, Germán García, Guilherme Fernandes, Manu González
  - OU llamada Defensas:
    - Héctor Bellerín, Diego Llorente, Natan, Marc Bartra, Ricardo Rodríguez, Romain Perraud, Víctor Gómez, Júnior Firpo, Youssouf Sabaly, Nobel Mendy, Félix Garreta, Ángel Ortiz, Pablo Busto, Lucas Alcázar, Rodrigo Kohon, Sergio Arribas (cedido)
  - OU llamada Centrocampistas:
    - Sofyan Amrabat, João Cardoso, Sergi Altimira, Antony, Pablo Fornals, Chimy Ávila, Anass Ezzalzouli, William Carvalho, Iker Losada, Rodrigo Riquelme, Nelson Deossa, Giovani Lo Celso, Marc Roca, Iván Corralejo, Isco, Aitor Ruibal, Mawuli Mensah, Carlos Guirao, Jesús Rodríguez, Dani Pérez, Mateo Flores, Carlos Reina
  - OU llamada Delanteros:
    - Cédric Bakambu, José Morante, Cristian Hernández, Marcos Fernández, Pablo García
  - OU llamada Administración:
    - Manuel Pellegrini, Juan Sevillano.
- Configura una contraseña inicial estándar y obliga al usuario a cambiarla después del primer inicio de sesión.

4. Directivas de grupo (GPO) para restricciones

- Para cada OU, crea y vincula una directiva de grupo.
  - Restricciones para aplicar a todas las OU:
    - Directiva de contraseñas: Define los requisitos de las contraseñas (longitud, complejidad, etc.).
    - Directiva de bloqueo de cuentas: Configura los parámetros para el bloqueo de cuentas de usuario.
  - Restricciones para OU llamada Porteros:
    - Denegar acceso al Panel de Control.
    - Establecer fondo de pantalla específico.
    - Restringir acceso a unidades/USB.
    - Deshabilitar las cuentas de invitado en los ordenadores del dominio.
    - Evitar que los usuarios desactiven Windows Defender.
  - Restricciones para OU llamada Defensas:
    - Denegar acceso al símbolo de sistema.
    - Impedir instalación de Software.
    - Deshabilitar reinicios forzados.
    - Deshabilitar la autenticación NTLM.
    - Deshabilita PowerShell.
  - Restricciones para OU llamada Centrocampistas:
    - Desactivar actualizaciones automáticas de controladores.
    - Restringir acceso a unidades/USB.
    - Ocultar Notificaciones.
    - Eliminar OneDrive.

        - Apagar Windows Defender.
    - Restricciones para OU llamada Delanteros:
        - Ejecutar script en el inicio de sesión.
          REM Muestra un mensaje en la consola
          echo Script de inicio de sesión completado.

          REM Abre una aplicación, por ejemplo, el Bloc de notas
          start notepad.exe
        - Establecer Protector de pantalla/Bloque por inactividad.
        - Mensaje de Inicio de Sesión (Este ordenador es propiedad del Real Betis).
        - Gestión remota de PowerShell.
- Prueba las directivas en los diferentes usuarios de cada OU y documenta los efectos.

5. Configuración de perfiles de usuario

- Configura el perfil móvil para algunos usuarios: guarda su perfil en la ruta \\Servidor\Perf-Movil\[usuario].
- Configura el perfil fijo para otros usuarios: asigna una carpeta en el servidor que no se sincroniza (\\Servidor\Perf-Fijo\[usuario]).
- Verifica el funcionamiento iniciando sesión desde diferentes equipos cliente.

6. Compartición de impresoras por departamento (OU)

- Instala una impresora en el servidor y compártela solo con los usuarios de una OU concreta (ejemplo: solo los de Administración).
- Repite el proceso para los distintos departamentos a modo de simulación, asignando diferentes impresoras por OU.

7. Carga de directorios compartidos según OU

- Crea carpetas compartidas en el servidor para cada OU (ejemplo: \\Servidor\Delanteros, \\Servidor\Porteros).
- Configura los permisos NTFS y de compartición para que solo los miembros de la OU correspondiente tengan acceso.
- Asocia a cada usuario la carpeta de red como unidad de red al iniciar sesión (mediante script de inicio o GPO).

Entregable 1: Capture la pantalla donde se muestre las unidades organizativas.

6. ACTIVIDAD 02

1. Crear una Unidad Organizativa específica para los equipos con control horario

- En el Administrador de Active Directory, crea una OU llamada EquiposHorarios.
- Mueve o crea en ella los objetos de equipo a controlar.

2. Crear una nueva Directiva de Grupo (GPO)

- Abre la Consola de Administración de Directivas de Grupo (GPMC).
- Crea una nueva GPO llamada ControlHorarioEquipos.

- Vincula esta GPO a la OU EquiposHorarios.

3. Configurar restricciones de horario en la GPO

- Edita la GPO y navega a:
  - Configuración del equipo > Directivas > Configuración de Windows > Seguridad > Políticas locales > Restricciones de inicio de sesión.
- Aquí puedes configurar:
  - Horarios permitidos para el inicio de sesión interactivo.
  - Horarios prohibidos para el inicio de sesión.
  - Restringir el inicio de sesión en ciertos horarios para los equipos.

4. Configuración avanzada (mediante scripts o tareas programadas)

- Para restringir cuándo un equipo puede estar encendido (encendido/apagado fuera de horas), puedes crear scripts de apagado o suspensión forzada y asignarlos mediante la GPO a horarios determinados mediante tareas programadas.
- Por ejemplo, un script que apague el equipo a las 22:00 y otro que permita arrancar el equipo a las 7:00 (esto último se puede hacer con Wake-on-LAN si el hardware lo permite).

5. Aplicar la GPO y probar

- En los clientes, ejecuta gpupdate /force para forzar la actualización de directivas.
- Prueba iniciar sesión o usar el equipo fuera del horario permitido y verifica que las restricciones funcionan.

Entregable 2: Capture la pantalla donde se muestre las unidades organizativas.