Prácticas de Infraestructura Informática

Bloque 2: Gestión de equipos mediante Directorio Activo

Sesión 1 - Gestión centralizada de identidad y autorización

Objetivos

Uno de los aspectos básicos de la gestión de los sistemas informáticos de una organización es el control de acceso a los servicios que proporcionan y a la información que almacenan. Los SO multitarea modernos (Windows y Linux) proporcionan mecanismos de control de acceso a nivel de equipo. Para ello, utilizan cuentas de usuario locales y listas de control de acceso para el manejo de recursos. Si bien estos mecanismos de control, locales a cada equipo, son imprescindibles, aspectos tales como la movilidad de los usuarios (que pueden requerir utilizar múltiples equipos en la organización), así como el acceso a través de red a recursos y servicios distribuidos por toda la organización, requieren mecanismos de control de acceso que sean o bien globales a toda la organización, o bien que afecten a partes sustanciales de la misma. El control de acceso tiene dos aspectos diferenciados que son la gestión de la identidad y la gestión de la autorización.

Para gestionar la identidad y la autorización a nivel de organización, la plataforma Windows proporciona la tecnología conocida como Servicios de Dominio de Directorio Activo *(Active Directory Domain Services)*, o simplemente, Directorio Activo, que es el objeto de esta práctica. El Directorio Activo, además de permitir una gestión centralizada de identidad y autorización, también es la base de un conjunto de tecnologías orientadas a la administración centralizada de los equipos de la organización, mejorando ostensiblemente la eficiencia de los técnicos de mantenimiento. Este otro aspecto del directorio activo será tratado en las sesiones 2 y 3 de este bloque de prácticas.

Teoría del Directorio Activo

- **Infraestructura informática NO estructurada**

  La figura 1 representa un caso de infraestructura informática NO estructurada. Los diferentes equipos de la organización se conectan a la red y pueden intercomunicarse entre ellos y acceder a Internet. Sin embargo, no existe un mecanismo de ámbito global que permita a los usuarios de la organización iniciar sesión en múltiples equipos o acceder a un determinado recurso. En este caso, por ejemplo, para proporcionar acceso a un servidor de ficheros habría que configurar una lista de control de acceso en dicho servidor, especificando cada usuario de la organización que requiera tener acceso. Esta forma de administrar los sistemas es muy ineficiente.

  De igual forma, si se desea aplicar una determinada política administrativa a un conjunto de equipos, la única forma de hacerlo sería equipo por equipo. Esta forma de operar requiere un gran esfuerzo por parte de los técnicos de mantenimiento.

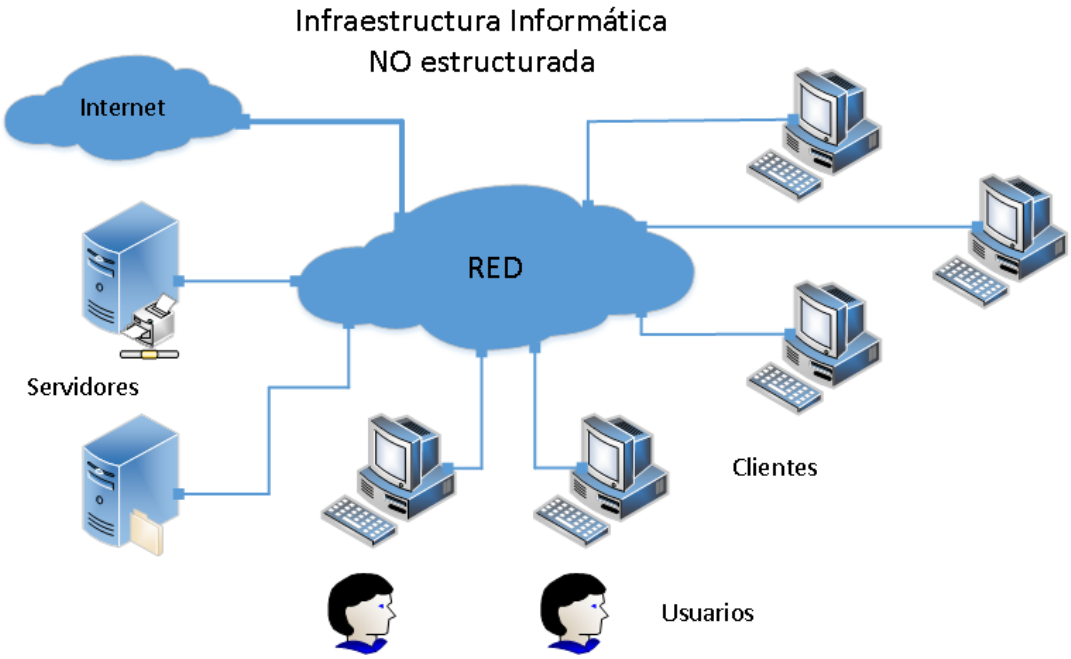


Figura 1. Infraestructura informática NO estructurada

- **Perspectiva general del Directorio Activo**

  Con objeto de resolver los problemas de gestión planteados por la infraestructura informática no estructurada, Microsoft desarrolla la tecnología conocida como Directorio Activo o *Active Directory* (AD). Se trata de una base de datos distribuida (ya que puede estar repartida entre varios servidores), cuyo objetivo es mantener una estructura organizativa de los usuarios y equipos de una organización. En base a dicha estructura, AD proporciona un esquema de autenticación centralizada de usuarios, soporte a la autorización centralizada y soporte a la administración centralizada de equipos.

  Arquitectura física simplificada

  La figura 2 muestra una arquitectura física simplificada de un directorio activo, implementada a través de un servidor único. El directorio activo permite establecer ámbitos de gestión de equipos, que reciben el nombre de *dominios*. Asimismo, el servidor que gestiona un domino recibe el nombre de servidor de dominio. Los equipos del dominio se comunican con el servidor de dominio a través de la red. En cada equipo del dominio, se pone en marcha un servicio, denominado NetLogon (NL en la figura) que mantiene las comunicaciones con el servidor de dominio. En el servidor de dominio se ejecuta, entre otros, el Servicio de Dominio de Active Directory (SDAD en la figura). Este servicio es el que convierte un servidor en un servidor de dominio.

  El servidor de dominio cuanta con una base de datos centralizada de usuarios. De esta forma, un usuario con cuenta en el dominio puede iniciar sesión en cualquier ordenador integrado en el dominio. El servicio NetLogon se encarga de gestionar las comunicaciones necesarias con el servidor de dominio para llevar a cabo el inicio de sesión.

  El dominio también juega un papel muy importante en la autorización de acceso a recursos. El servidor de archivos mostrado en la figura 2 se encuentra integrado en el dominio. Gracias a ello se pueden utilizar los usuarios y grupos de usuarios del servidor de dominio para gestionar el acceso a los recursos del servidor de archivos. Si un usuario inicia sesión en un equipo con una cuenta del dominio que tenga derechos de acceso al servidor de archivos, el usuario tendrá automáticamente acceso a los recursos de dicho servidor.

  NOTA: El Directorio Activo NO debe entenderse como una arquitectura de red. Ésta se encuentra por debajo de los servicios del Directorio Activo. El directorio activo es una infraestructura de

servicios que permiten cohesionar un conjunto de equipos conectados a la red, de manera que se genere para ellos un ámbito centralizado de identificación, autorización y administración.

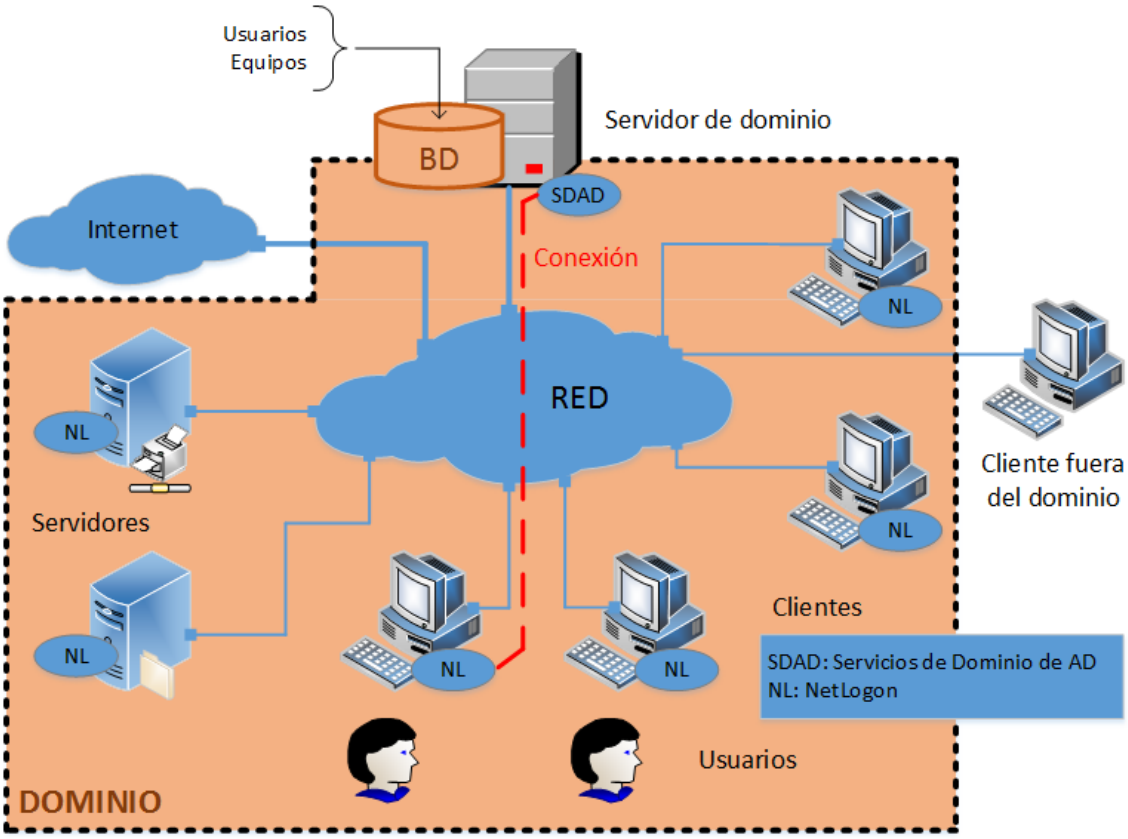


Figura 2. Arquitectura física simplificada de un directorio activo

La arquitectura física simplificada del Directorio Activo, presentada en la figura 2, ha servido para comprender el concepto de Directorio Activo y su funcionamiento básico. Esta arquitectura es perfectamente utilizable en entornos de trabajo de dimensiones no excesivamente grandes, entendiendo por dimensión el número de clientes y servidores gestionados. Sin embargo, esta arquitectura del directorio activo basada en un único dominio es la más simple de las posibles. El Directorio Activo ha sido diseñado para que escale a grandes organizaciones mediante el concepto de dominios jerarquizados. A continuación, se presenta cómo se organiza un directorio activo en base a este concepto.

Arquitectura lógica

Define los niveles jerárquicos utilizados para organizar los usuarios y equipos. Estos niveles, que se ejemplifican en la figura 3, son los siguientes:

Bosque (Forest): Conjunto total de todos los elementos a gestionar por una infraestructura de Directorio Activo. Estos elementos son básicamente usuarios y equipos. Representa una frontera lógica de lo que va a ser gestionado por el Directorio.

Dominios (Domains): Son particiones jerarquizadas del bosque. En el bosque siempre hay un dominio raíz, bajo el cual se pueden ir creando otros dominios siguiendo una jerarquía arborescente. Los dominios son los que contienen los datos del directorio, como las cuentas de usuarios y las de equipos.

Unidades organizativas (OUs): Representan agrupaciones de objetos dentro de un dominio y su objetivo es generar particiones administrativas dentro de los dominios. Así, por ejemplo, se pueden asignar diferentes administradores a diferentes unidades organizativas dentro de un dominio.

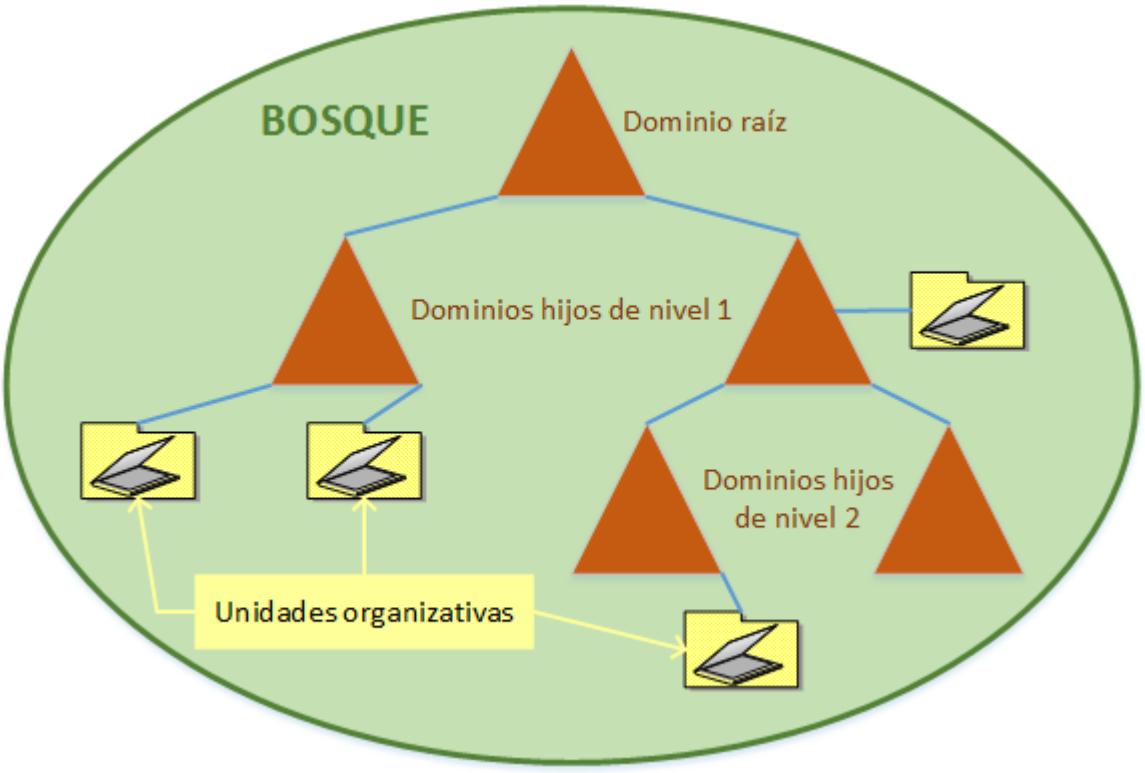


Figura 3. Arquitectura lógica de un directorio activo

Implementación física

Cada dominio se implementa, al menos, mediante un servidor, en el que se instala y configura el rol de *servicios de dominio de directorio activo*. Dicho servidor contiene la base de datos con todos los usuarios y equipos del dominio. Cada servidor de dominio puede replicarse para obtener la redundancia necesaria, o bien para mejorar las prestaciones cuando se trata de dominios con muchos usuarios y equipos.

Modelos de organización de dominios

- *Modelo de dominio único*. Se trata de un bosque que contiene un dominio raíz, el cual contiene todas las cuentas de usuarios y equipos del bosque. Es el modelo más simple de administrar y diseñar. Este modelo, dada su simplicidad, será el adecuado para la gestión de la organización de ejemplo, utilizada en estas prácticas.
- *Modelo regional*. Se trata de organizar los dominios en base a una distribución geográfica. Típicamente, una organización con sedes en varias ciudades diferentes encajaría en este modelo.

Ejemplo de diseño: gestión de las aulas de informática de la Universidad de Oviedo

El bosque estaría formado por todos los equipos de las aulas (2500) y todos los usuarios de las mismas, o sea, los colectivos de profesores y alumnos. Fuera de este bosque quedarían el resto de equipos de la organización, como, por ejemplo, los ordenadores de los despachos de los profesores o los ordenadores utilizados por el personal de administración y servicios. Los usuarios pertenecientes al colectivo de personal de administración y servicios también quedarían fuera de este bosque. Así se observa cómo el bosque representa una frontera lógica de lo que va a ser gestionado por el directorio activo.

La organización de los dominios encajaría bien en un modelo regional, como el que se representa en la figura 4. Habría un servidor de dominio en cada ciudad, que gestionaría los equipos ubicados en su ciudad. El dominio raíz se gestionaría mediante un servidor que razonablemente podría estar en el CPD corporativo, en Oviedo. El dominio raíz podría no contener equipos, pero podría contener a todos los usuarios, profesores y alumnos. De esta forma, debido a la jerarquía, todos los usuarios podrían iniciar sesión en cualquier equipo de la universidad.

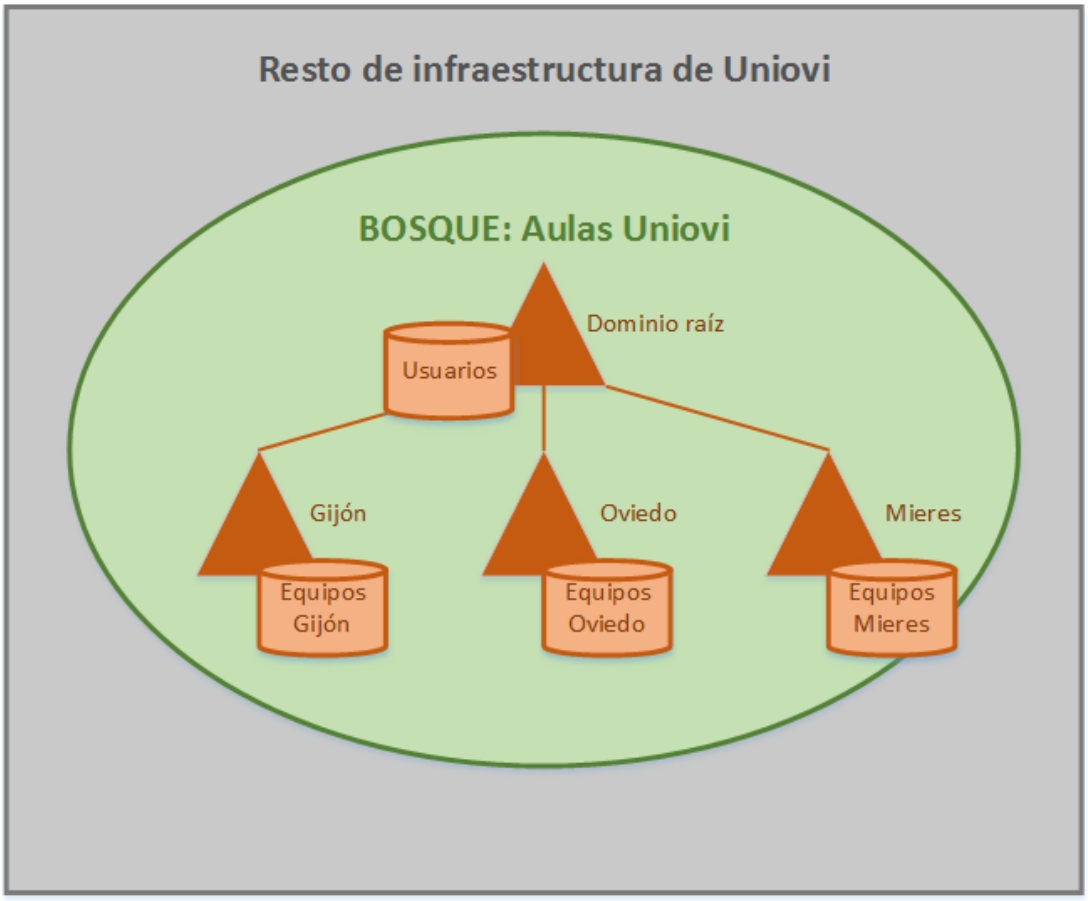


Figura 4. Ejemplo de diseño de directorio activo: Aulas de Uniovi

NOTA: El modelo real que se utiliza en la Universidad para la gestión de aulas no se ajusta al ejemplo representado. En realidad, el modelo se basa en un dominico único (aulasuo.uniovi.es), con servidores replicados en Oviedo y Gijón. No obstante, el modelo de Directorio Activo regional también encajaría perfectamente en la gestión de las aulas de Uniovi.

Diseño de la jerarquía de nombres de los dominios

Los dominios se nombran utilizando nombres DNS, idénticos a los que se utilizan en Internet. Los nombres DNS están formados por un prefijo y un sufijo, como por ejemplo ibm.com.

A la hora de establecer los nombres para los dominios, lo primero que debe hacerse es establecer el nombre DNS del dominio raíz del bosque. Esto tiene dos partes, la elección del sufijo y la del prefijo.

Con relación al sufijo, Microsoft recomienda utilizar un sufijo registrado en la red de la organización. En el caso de la Universidad de Oviedo, dicho sufijo sería *uniovi.es*, tal y como se muestra en la figura 5. De esta forma, los nombres de los dominios encajarían con la jerarquía de nombres DNS de la organización.

Con relación al prefijo, debería ser un nombre no utilizado en la red. En el ejemplo de las aulas de Uniovi, podría ser, por ejemplo, *aulas*.

Combinando prefijo y sufijo se obtiene el nombre del dominio raíz del bosque. Éste sería *aulas.uniovi.es*.

Los dominios de nivel inferior se nombran siguiendo la jerarquía de nombres DNS. En el ejemplo de las aulas de Uniovi, los nombres de estos dominios podrían ser los siguientes: *gijon.aulas.uniovi.es*, *oviedo.aulas.uniovi.es* y *mieres.aulas.uniovi.es*.

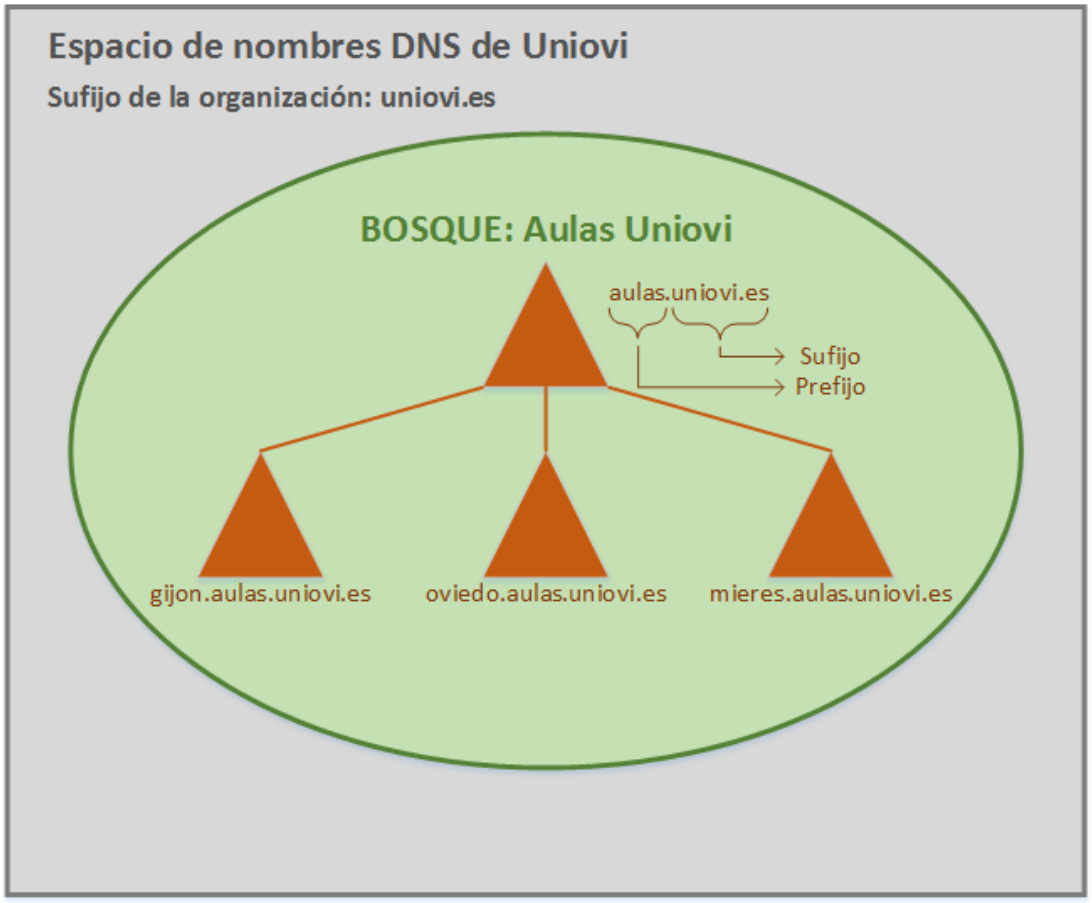


Figura 5. Ejemplo de jerarquía de nombres para el DA de la aulas de Uniovi

En el caso de que una infraestructura de directorio activo se aplique el ámbito de una red privada (no visible en Internet), Microsoft recomienda utilizar el sufijo *local*. Éste es precisamente el caso que se aplicará en las prácticas de esta asignatura.

Infraestructura DNS

Los servicios de *Active Directory* requieren una infraestructura DNS para resolver todas las necesidades de localización de los equipos que forman parte del bosque.

Dicha infraestructura DNS puede ser proporcionada por servidores DNS de la organización, o puede montarse de manera integrada en los servidores de dominio. Esta es la opción más cómoda y la que utilizaremos.

Evaluación de conceptos

- Una vez leídos los apartados de Objetivos y Teoría del Directorio Activo, contesta las siguientes preguntas. Si en alguna de ellas tienes dudas, pregúntale a tu profesor.

  (1) PREGUNTA. En el apartado Objetivos, se hace referencia a los tres grandes ámbitos de gestión de equipos, en los que el Directorio Activo aporta soluciones. Indica cuáles son dichos ámbitos de gestión.

  1)
  2)
  3)

  (2) PREGUNTA. Indica el problema que se plantea en una infraestructura informática no estructura cuando se requiere proporcionar autorización de acceso a un determinado recurso.

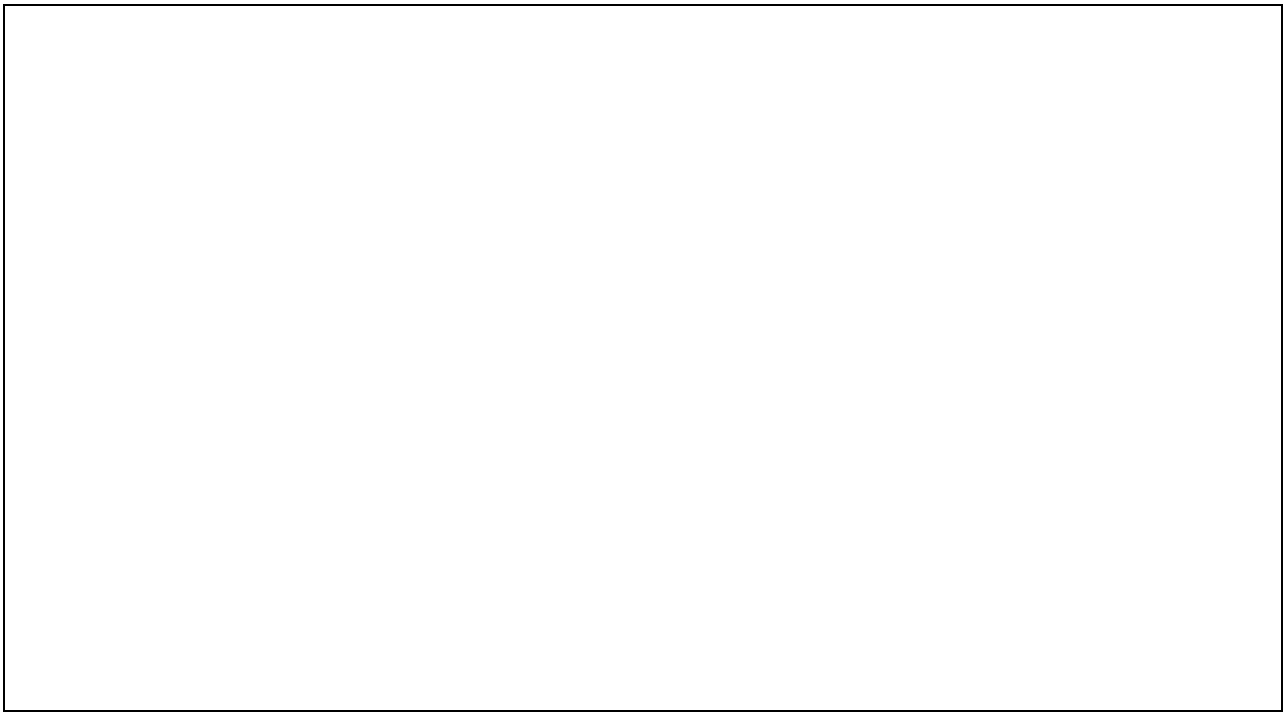
  (3) PREGUNTA. El Directorio Activo es una base de datos distribuida. ¿Qué se mantiene en dicha base de datos?

  (4) PREGUNTA. Imagina que pretendiéramos gestionar los equipos impares del laboratorio 1S31 (o sea, los que están instalados solo con Windows 11), con un Directorio Activo simple, siguiendo el esquema representado en la Figura 2. Para ello, podríamos decidir, por ejemplo, instalar el servidor de dominio en el ordenador ubicado en la mesa del profesor. La arquitectura de red del laboratorio es simple. Se trata de un único *switch* que interconecta todos los equipos del laboratorio. Para llevar a cabo el despliegue del Directorio Activo indicado, ¿sería necesario realizar alguna modificación en la arquitectura de red del laboratorio? Justifica tu respuesta indicando la condición esencial que debe cumplir la configuración de red de los equipos impares para que puedan integrarse en el dominio desplegado en el ordenador del profesor. Si tienes dudas, pregúntale a tu profesor.

  ¿sería necesario realizar alguna modificación en la arquitectura de red del laboratorio?

  Condición que debe cumplir la configuración de red de los equipos impares

(5) PREGUNTA. Imagina que se pretende gestionar los equipos de los laboratorios del Departamento de Informática mediante un directorio activo jerarquizado. El Departamento dispone de tres laboratorios: el 1S31 y el 1S29, en Gijón, y el SoftwareLab, en Mieres. Se desea disponer de un domino raíz para la gestión global de los laboratorios y un subdominio para cada laboratorio en particular. Se conoce que el nombre DNS asignado al Departamento de Informática de la Universidad es `di.uniovi.es`. Asimismo, se desea que la jerarquía de nombres usada para nombrar los dominios del directorio activo para laboratorios se integre en la jerarquía de nombre DNS de la Universidad. Teniendo en cuenta la información indicada, y utilizando el programa Paint, dibuja una representación del directorio activo solicitado, indicando el nombre asignado a cada uno de los dominios que lo integran.



Desarrollo

- **Instalación de los servicios de *Active Directory***
  - Para instalar los Servicios de *Active Directory* se utiliza la máquina PLX-S-DC.
  - Arranca PLX-S-DC e inicia sesión con el *Administrador*.

Configuración de red

  - En PLX-S-DC, configura el protocolo TCP/IP de la interfaz de red con los siguientes valores:
    - Dirección IP: 192.168.0.25
    - Máscara de subred: 255.255.255.0
    - Puerta de enlace: 192.168.0.100
  - En *Windows Defender Firewall con seguridad avanzada*, genera la regla de entrada *Permitir ICMPv4*.
  - En el *Administrador de Hyper-V*, conecta la interfaz de red de PLX-S-DC a *Red virtual interna*.
  - Comprueba que puedes hacer ping desde PLX-S-DC al sistema anfitrión.
  - Comprueba que puedes hacer ping desde PLX-S-DC al DNS de Uniovi (156.35.14.2).
  - Comprueba que puedes hacer ping desde el anfitrión a PLX-S-DC.

Procedimiento de instalación

La instalación se llevará a cabo a través de dos asistentes, el de *Agregar roles* y el utilizado para *Promocionar un servidor a servidor de dominio*. El primero instala todo el software necesario y el segundo lleva a cabo las configuraciones requeridas.

Instalación del rol Servicios de dominio de Active Directory

  - **ATENCIÓN: en este punto estás en PLX-S-DC, NO estás en el anfitrión**.
  - *Administrador del Servidor* --> *Servidor local* -> menú *Administrar* -> opción *Agregar roles y características*. Entonces se abre el *Asistente para agregar roles y características*.
  - Avanza utilizando las opciones por defecto hasta *Roles de servidor*.
  - En *Roles de servidor*, selecciona *Servicios de dominio de Active Directory*. Aparece una ventana indicando que hay que agregar un conjunto de características (herramientas). Es habitual que ciertos roles o características dependan a su vez de otros roles o características. Mantén seleccionada la casilla de verificación *Incluir herramientas de administración (si es aplicable)*. Entonces, pulsa en *Agregar características*.
  - En este punto, *Servicios de dominio de Active Directory* queda seleccionado. Pulsa *Siguiente* para continuar.
  - El asistente pasa al apartado *Características*. Pulsa en *Siguiente*.
  - Se llega a la ventana informativa *Servicios de dominio de Active Directory*. Esta ventana proporciona información importante a tener en cuenta sobre el funcionamiento de este servicio. Lee la información proporcionada en la ventana. Entonces, contesta las siguientes preguntas:

    (6) PREGUNTA. Los servicios de dominio de Active Directory almacenan información acerca de diversas categorías de elementos. ¿Cuáles?

    (7) PREGUNTA. ¿Qué recomienda Microsoft para garantizar que los usuarios puedan iniciar sesión en la red, en el supuesto de que falle un servidor controlador de dominio?

    NOTA: la contestación a la pregunta 2 es lo que se debe hacer en instalaciones en producción, como es el caso de los servidores de dominio que se utilizan para autenticar en las aulas de Uniovi.

Sin embargo, debido a la complejidad de la replicación de servidores, en estas prácticas se utilizará un único servidor controlador de dominio para dar servicio al dominio de prácticas.

- Pulsa en *Siguiente* para continuar con la instalación del rol.
- En este punto, el asistente proporciona un resumen de lo que se va instalar. Marca la casilla de verificación *Reiniciar automáticamente el servidor de destino en caso necesario*. Entonces pulsa en *Instalar*.
- Una vez que se ha completa la instalación, cierra el asistente.

Promoción del servidor a controlador de dominio

- En el icono de notificaciones del *Administrador del servidor* (es un banderín, justo a la izquierda del menú *Administrar*), se muestra un símbolo de admiración en amarillo, lo que indica que hay notificaciones para el usuario. Abre las notificaciones.
- La notificación indica *Requiere configuración para Servicios de dominio de Active Directory en PLX-S-DC*. Esto se debe a que aún falta llevar a cabo una etapa de configuración adicional, para que el servidor pueda comenzar a trabajar como servidor de dominio. Para pasar a dicha etapa, pulsa en el enlace *Promover este servidor a controlador de dominio*.
- Se abre el *Asistente para configuración de Servicios de dominio de Active Directory*.
- En *Seleccionar la operación de implementación*, debes tener en cuenta que lo que vas a hacer ahora es poner en marcha una infraestructura de directorio activo desde cero. Esto comienza siempre por la creación de un nuevo bosque. Por consiguiente, selecciona *Agregar un nuevo bosque*. En el campo *Nombre de dominio raíz*, introduce el nombre *practicas.local* (recuerda que según se ha indicado anteriormente, Microsoft recomienda utilizar el sufijo *local* para el caso de los directorios activos que funcionan en una red privada, no visible en Internet, como es el caso de estas prácticas).
- En *Opciones del controlador de dominio*, se establecen las siguientes opciones:
  - En *Seleccionar nivel funcional del nuevo bosque y dominio raíz*, mantén el valor por defecto, *Windows Server 2016*.

    NOTA: Las capacidades de los Servicios de *Active Directory* se han ido incrementando con las sucesivas evoluciones del sistema operativo Windows. Cuando en un mismo bosque o en un mismo dominio se van a mezclar controladores de dominio implementados con sistemas operativos diferentes (Windows 2008, 2008 R2, 2012, 2012 R2, 2016) hay que establecer el nivel funcional del bosque y del dominio para que coincidan con el correspondiente al sistema operativo más antiguo. Entonces todos los servidores de dominio se comportarán según el nivel especificado. En el caso de estas prácticas solo va a haber un servidor de dominio con *Windows Server 2019*, por consiguiente, se mantiene el nivel funcional más alto posible que es el *Windows Server 2016*.
  - En *Especificar capacidades del controlador de dominio*, mantén seleccionado *Servidor de Sistema de nombre de dominio (DNS)*. Esto instalará también un *Servidor DNS* en el controlador de dominio, que actuará como *Servidor DNS* para todas las máquinas del dominio.
  - En *Escribir contraseña de modo de recuperación de servicios de directorio (DRMS)*, escribe la contraseña *ADclave00*. Siempre se usará esta contraseña para todas las cuentas relacionadas con el dominio (esta contraseña es la que se utiliza para restaurar los servicios de directorio cuando éstos no se inician, ya que en este caso los usuarios del dominio no estarán disponibles).
- En *Opciones de DNS*, ignora el mensaje *"No se puede crear una delegación para este servidor DNS…"*, pulsa *Siguiente* para continuar.
- En *Opciones adicionales*, acepta el nombre NetBIOS asignado por defecto (PRACTICAS).
- En *Rutas de acceso*, se especifica la ubicación de la base de datos de AD DS, los archivos de registro y SYSVOL. Mantén los valores por defecto (se trata de las ubicaciones donde se guarda toda la información del directorio activo).

- Finalmente, se muestra un resumen de la configuración seleccionada para la instalación. Pulsa en *Siguiente* para comenzar la configuración de los servicios de *Active Directory*.
- El asistente ejecuta una *Comprobación de requisitos previos*. La comprobación es satisfactoria. Pulsa en *Instalar*.
- Cuando se completa el proceso de configuración, el sistema se reinicia de forma automática.
- Inicia sesión con el usuario *Administrador*.
- En este punto, los servicios de Active Directory ya están plenamente operativos en PLX-S-DC, y la máquina actúa como servidor del dominio *practicas.local*.

Configuración de la infraestructura DNS

Mediante la instalación de un Directorio Activo con DNS integrado, el sistema ha configurado automáticamente un *Servidor DNS*. Dicho servidor proporciona la infraestructura DNS para la organización de ejemplo.

Antes de continuar con el Directorio Activo, se revisará brevemente el funcionamiento del servicio DNS, y se completará la configuración de red de los equipos de la organización de ejemplo, añadiendo la configuración DNS.

Rol DNS

- *Administrador del Servidor --> Servidor local*, entonces, en la parte inferior del panel informativo, ubícate en la sección *Roles y características*. Ordena la tabla informativa por *Tipo*, y observa que se ha agregado el rol *Servidor DNS*. Entonces, cierra el *Administrador del servidor*.

Herramienta para la administración del DNS

- Al instalar el rol DNS, se instala una herramienta para la administración del DNS.
- *Herramientas administrativas -> DNS*. Al abrir esta herramienta, observa que PLX-S-DC actúa como servidor DNS.

Zonas de búsqueda directa

- Despliega PLX-S-DC. Se puede observar las zonas de búsqueda, siendo las más importantes las de búsqueda directa. Estas zonas almacenan los registros que trasforman las direcciones DNS en direcciones IP.
- Abre *Zonas de búsqueda directa*. Se observan dos zonas: *practicas.local* y *_msdcs.practicas.local*.
- *practicas.local* es la responsable de la traducción de los nombres DNS del dominio. Cada nodo que se agregue al dominio tendrá un registro en esta zona que traducirá el nombre DNS del nodo a su dirección IP (estos registros se conocen como de tipo A). En este momento solo hay un nodo agregado al dominio que es PLX-S-DC. Abre el registro de tipo A correspondiente a este nodo.

  (8) PREGUNTA. Indica los datos almacenados en este registro de tipo A.

```
Nombre de dominio completo (FQDN):
Dirección IP:
```

- Asimismo, se crea un registro para el nombre del propio dominio, al que se le asigna también la dirección IP del servidor. Abre este segundo registro, comprobando que el nombre DNS del dominio (*practicas.local*) se encuentra registrado.
- La zona *_msdcs.practicas.local* se utilizaría para gestionar otros dominios del bosque, lo que no se aplica en el caso de estas prácticas.
- Cierra la herramienta de administración del DNS.

Configuración IP del Servidor de dominio

- Abre la configuración IPv4 del Servidor de dominio.

(9) PREGUNTA. ¿Con qué dirección IP se ha configurado el campo *Servidor DNS preferido*?

(10) PREGUNTA. ¿Por qué se ha establecido dicha configuración? Si tienes dudas, pregúntale a tu profesor

Primera prueba de funcionamiento del DNS

- De momento, el DNS solo tiene dos direcciones configuradas, *PLX-S-DC.practicas.local y practicas.local*. Utilizando el propio Servidor de dominio, prueba que *ping* responde a estos dos nombres.

Configuración del DNS en otras máquinas de la organización

- Para realizar este apartado, es necesario que las máquinas virtuales desplegadas en la plataforma Hyper-V tengan conexión con la red externa. Debido a ello, es necesario activar el servicio NAT en el anfitrión. En el sistema anfitrión, *Herramientas administrativas -> Enrutamiento y acceso remoto -> botón derecho sobre 1S31-XXX (local) -> Todas las tareas -> Iniciar*.
- De momento, vas a configurar el DNS en PLX-C-51 y en PLX-C-52.
- Arranca las máquinas PLX-C-51 y PLX-C-52.
- En PLX-C-51, configura el DNS en el protocolo IPv4. Para ello, en el campo *Servidor DNS preferido* debes poner la dirección IP de PLX-S-DC, que es 192.168.0.25.
- En PLX-C-51, *ping* a *PLX-S-DC.practicas.local* y *practicas.local* para comprobar que el DNS funciona.

  NOTA: cuando se le pasa un nombre a *ping*, éste tendrá que consultar al DNS para obtener la IP. Así se comprueba el correcto funcionamiento del DNS.
- En PLX-C-52, configura el DNS en el protocolo IPv4.
- En PLX-C-52, *ping* a *PLX-S-DC.practicas.local* y *practicas.local* para comprobar que el DNS funciona.
- En PLX-S-DC, Abre la herramienta DNS.
- En este punto, es recomendable ajustar un aspecto de la configuración del servidor DNS. Se trata de los *Reenviadores*, que se explican en detalle un poco más adelante. Por defecto, el servidor DNS configura 3 reenviadores, utilizando la dirección IPv6 de los mismos. Sin embargo, el router NAT de la plataforma de prácticas no ha sido configurado para gestionar direcciones IPv6. Debido a ello, el servidor DNS no puede establecer contacto con dichos reenviadores, lo que genera algunas deficiencias en el funcionamiento del DNS. Para evitar estas deficiencias, lo mejor es eliminar dichos reenviadores.
- En la herramienta DNS, selecciona PLX-S-DC. Entonces, abre *Reenviadores*. Puedes observar que hay tres reenviadores configurados mediante una dirección IPv6. En la columna *FQDN de servidor*, se indica <No se puede resolver>. Esto significa que el servidor DNS no puede contactar con el reenviador, debido a la razón explicada anteriormente. Selecciona el primer reenviador (fec0:0:0:0:ffff::1). Pulsa *Editar*. De nuevo, selecciona el primer reenviador y pulsa *Eliminar*. En este punto, elimina también el segundo reenviador (fec0:0:0:0:ffff::2) y el tercero (fec0:0:0:0:ffff::3). *Acepta* para completar la eliminación de los reenviadores.
- Ahora puedes continuar con las pruebas de funcionamiento del DNS.
- ¿Resolverá el Servidor DNS del controlador de dominio nombres externos a la red virtual de la plataforma de prácticas? Vas a realizar unas pruebas para analizar este asunto.
  - En PLX-C-51, ping a www.uniovi.es. Se observa que el DNS resuelve el nombre
  - En PLX-C-52, ping a www.google.es. Se observa que el DNS resuelve el nombre

- ¿Por qué resuelve el servidor DNS, ubicado en la red interna, nombres externos? La explicación se encuentra en un mecanismo utilizado por los servidores DNS conocido como *Sugerencias de raíz (root hints)*. Para ver esto, en PLX-S-DC, abre la herramienta *DNS* y selecciona PLX-S-DC. En la ventana derecha se observa el elemento *Sugerencias de raíz*. Abre este elemento. Se trata de servidores DNS de Internet que pueden servir de base para resolver cualquier consulta DNS.

  (11) PREGUNTA. Indica la dirección IP del servidor DNS denominado A.ROOT-SERVERS.NET.

- Comprueba que puedes hacer ping a dicho servidor.
- El uso de los servidores que integran las sugerencias de raíz es costoso en términos de tiempo de respuesta. Debido a ello, es mejor utilizar reenviadores.
- Abre de nuevo *Sugerencias de raíz* y lee el párrafo explicativo en la parte superior de la ficha. En dicho párrafo se indica que las sugerencias de raíz solo se usan en el caso de que no haya reenviadores disponibles.
- Cierra la ventana en la que se muestran las *Sugerencias de raíz*.

Configuración de los reenviadores

Un reenviador es un enlace que se pone en un servidor DNS primario hacia otro DNS secundario, de modo que las consultas que no puedan ser resueltas por el primario son enviadas al secundario para su resolución. En el caso de estas prácticas, lo lógico es utilizar como DNS secundario el DNS principal de la Universidad (156.35.14.2), para que él resuelva todas las direcciones externas a la red virtual de la plataforma de prácticas.

- En el administrador del *DNS* abre *Reenviadores*. Observa que, de momento, no hay ningún reenviador configurado. Observa que se encuentra marcado obligatoriamente *Usar sugerencias de raíz si no hay reenviadores disponibles*. Pulsa *Editar*. En el registro que se abre escribe la dirección IP del servidor DNS principal de la Universidad (156.35.14.2). Pulsar *Aceptar*. El sistema se conecta con dicha IP, valida que se trate de un SERVIDOR DNS y, si es así, el reenviador queda establecido.

  (12) PREGUNTA. ¿Cuál es el nombre DNS del servidor DNS primario de la Universidad?

- Finalmente, *Aplicar* para completar la configuración de los reenviadores, y *Aceptar* para cerrar las fichas de propiedades del DNS.
- En PLX-C-51, abre el navegador. Escribe la dirección *www.ibm.com*. Comprueba que accedes a la página correctamente, lo que significa que el DNS resuelve el nombre.
- En PLX-C-52, abre el navegador. Escribe la dirección *www.uniovi.es*. Igualmente, comprueba que accedes a la página especificada.
- En PLX-S-DC, cierra la herramienta de configuración del DNS.
- Apaga las máquinas PLX-C-51 y PLX-C-52.
- A partir de este momento, no se necesita acceder a la red externa en esta sesión. Debido a ello, se detiene el acceso a la red para evitar actualizaciones. En el sistema anfitrión, *Herramientas administrativas -> Enrutamiento y acceso remoto ->* botón derecho sobre *1S31-XXX (local) -> Todas las tareas -> Detener*.

- **Planteamiento de directorio activo para la organización de ejemplo**

  Supongamos que la organización de ejemplo es una institución educativa, ámbito que te resultará muy cercano. Se va a diseñar un ejemplo de directorio activo para gestionar una organización de este tipo, en la que hay dos ámbitos bien diferenciados, el relativo a la docencia y el correspondiente a la gestión de la organización.

  Los elementos fundamentales a gestionar son los ordenadores y los usuarios. A continuación, se plantean un conjunto de elementos de ejemplo.

  Elementos de la organización

  ORDENADORES

Servidores (2)	Orientados a soportar los servicios requeridos por los ordenadores clientes.
Clientes (4)	Se diferencian dos ámbitos de clientes: 1) aulas de informática, en las que se desarrollan tareas docentes, y 2) ámbito de gestión, al que corresponden los equipos del personal de administración, y los equipos personales de los profesores. Se incluirán dos clientes en cada ámbito.

  USUARIOS

Profesores (2)	*Prof1 y Prof2*
Alumnos (2)	*Alu1 y Alu2*
PAS (2)	*PAS1 y PAS2* (NOTA: PAS significa Personal de Administración y Servicios)

  Arquitectura lógica del directorio activo propuesto

  Se propone un bosque con un único dominio raíz. En una pequeña organización esto es lo normal.

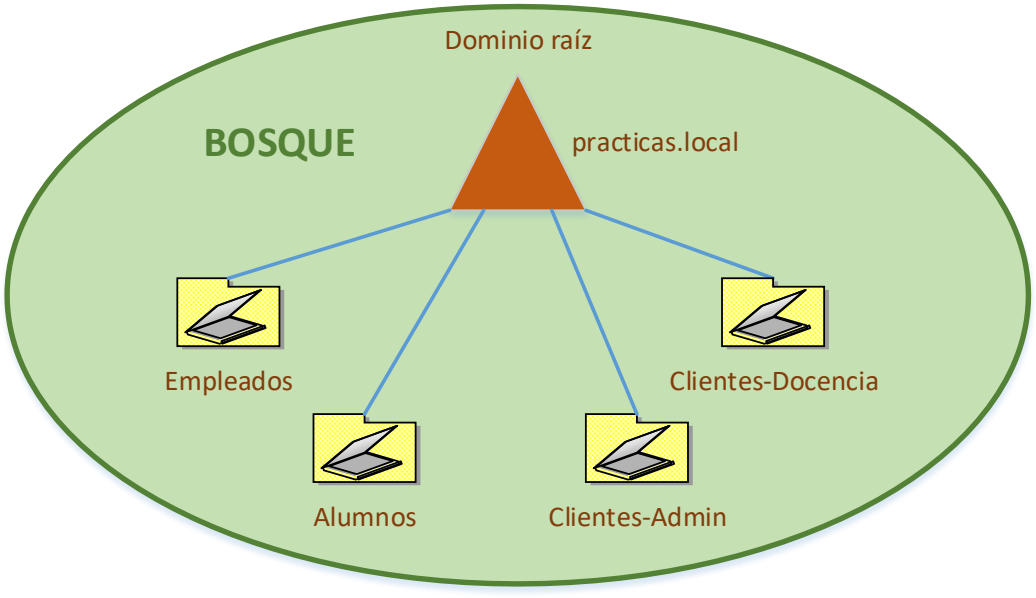


Figura 6. Arquitectura lógica del DA de la organización de ejemplo

  Nombre del dominio raíz

  Si el dominio fuese a contener una agrupación de máquinas con direcciones públicas en Internet, se debería elegir un nombre que encajase perfectamente en la jerarquía de nombres DNS de la organización. Por ejemplo, según se comentó anteriormente, un dominio para gestionar aulas en la Universidad de Oviedo podría llamarse *aulas.uniovi.es*, que encajaría con el sufijo DNS registrado para dicha organización *(uniovi.es)*. En el caso de estas prácticas, los sistemas se conectan a una red privada, por lo que no es necesario encajar el nombre DNS del dominio con una jerarquía DNS preestablecida. En instalaciones de laboratorio privadas se suele utilizar el sufijo *.local*. Visto esto,

un buen nombre para el dominio raíz puede ser *practicas.local* (el sufijo .local es no visible en Internet, por lo que solo puede utilizarse en redes privadas).

Unidades organizativas

Las políticas administrativas se aplican habitualmente en el ámbito de las unidades organizativas, por eso hay que pensar detenidamente la organización de las mismas. Una primera regla habitual es no mezclar objetos de diferentes tipos, separando así las unidades organizativas que contienen usuarios de las que contienen equipos. Se definen las unidades organizativas *Empleados* y *Alumnos* para contener a los usuarios correspondientes. Asimismo, se establece una unidad organizativa para los equipos clientes usados en la administración (Clientes-Admin), y otra destinada a los equipos clientes utilizados en la docencia (Clientes-Docencia).

NOTA: crearás todos los elementos del directorio activo planteado en este apartado en lo puntos siguientes.

- **Herramientas para la gestión del directorio activo**
  - Pon tu atención en la máquina PLX-S-DC.
  - Despliega *Herramientas administrativas*. Entonces observa las herramientas que se han instalado en el sistema para gestionar el directorio activo al instalar el rol *Servicios de Dominio de Active Directory*. Estas herramientas son las siguientes:
    - *Usuarios y equipos de Active Directory*. Ésta es la única herramienta que se va a utilizar en estas prácticas. Se verá enseguida.
    - *Sitios y servicios de Active Directory*. Esta herramienta se usa para gestionar grandes despliegues siguiendo el modelo regional. Solo en este caso los *Sitios* adquieren sentido.
    - *Dominios y confianzas de Active Directory*. Esta herramienta se utiliza, fundamentalmente, para gestionar relaciones entre dominios ubicados en bosques diferentes, que es lo que se conoce habitualmente como relaciones de confianza. Nada de esto es aplicable en estas prácticas.
    - *Centro de administración de Active Directory* es una versión enriquecida de *Usuarios y equipos de Active Directory*, pero con más opciones y un poco más complicada. Pensando en las operaciones simples a realizar en estas prácticas, es mejor utilizar *Usuarios y equipos de Active Directory*.
  - A continuación, se va a analizar, someramente, la herramienta *Usuarios y equipos de Active Directory*, ya que es la única necesaria para gestionar la organización de ejemplo.

Herramienta *Usuarios y equipos de Active Directory*

  - Abre la herramienta. Los elementos raíz mostrados por esta herramienta son los dominios, en el caso de estas prácticas, *practicas.local*.
  - Cuando se crea un dominio, se generan en él, por defecto, unos objetos conocidos como contenedores, cuyo objetivo es almacenar otros objetos del dominio. Algunos son bastante obvios, otros, no tanto. Para ver los contenedores creados en el dominio, despliega el nodo *practicas.local*.
  - Pondrás tu atención en tres de estos contenedores, que son los que serán aplicables a las prácticas a realizar. Dos de estos contenedores contienen cuentas de equipos y el otro, cuentas de usuario y grupos de seguridad. Los contenedores a manejar son los siguientes:
    - *Computers*. En él se crean por defecto los objetos correspondientes a los equipos que se agregan al dominio. Ábrelo y comprueba que, de momento, está vacío.
    - *Domain controllers*. Almacena los objetos correspondientes a los controladores de dominio. Ábrelo y observa que en él se encuentra PLX-S-DC. Pulsa en este objeto para ver sus propiedades. En las propiedades, se puede agregar información sobre el controlador, como por ejemplo su ubicación (piensa, por ejemplo, en grandes organizaciones).
    - *Users*. Contiene grupos de seguridad creados por defecto en el dominio como por ejemplo *Admins. del dominio* y *Usuarios del dominio*. El objetivo de estos grupos es proporcionar

derechos a los usuarios que contenga, así como proporcionar acceso a recursos del dominio. Estos grupos creados por defecto en el dominio se denominan grupos integrados.

(13) PREGUNTA. ¿Qué grupo será utilizado para contener a los usuarios con derechos de administración del DNS? Si tienes dudas, pregúntale a tu profesor.

• Configuración del directorio activo para la organización de ejemplo

Cuentas de usuario iniciales

- Hasta ahora, se ha hablado de grupos de seguridad, pero ¿hay alguna cuenta de usuario disponible cuando se crea el dominio? Alguna tiene que haber, ya que, si no, no se podría iniciar sesión en el dominio.
- Observa que en *Users* hay tres cuentas de usuario. Se reconocen fácilmente porque el nombre del usuario va precedido por un icono formado por una sola persona, a diferencia de los grupos, que van precedidos por un icono con dos personas.

  (14) PREGUNTA. Indica, a continuación, los tres usuarios presentes en *Users*.

- Vas a analizar el origen de estas cuentas.
- Arranca PLX-S-01.
- Entra en sesión con el usuario *Administrador*.
- En ambos servidores (PLX-S-DC y PLX-S-01), abre *Herramientas administrativas -> Administración de equipos*. ¿Qué ha cambiado entre ambos? Debes observar que en el servidor de dominio ha desaparecido *Usuarios y grupos locales*. Esto se debe a que el servidor de dominio se ha convertido en la base de datos de usuarios del dominio. Por razones de seguridad, los usuarios locales se eliminan, de modo que solo se puede abrir sesión en él con los usuarios del dominio. Debido a esto, desaparece la utilidad administrativa *Usuarios y grupos locales*.
- En PLX-S-01, ¿qué usuarios locales hay registrados?

  (15) PREGUNTA. Indica los usuarios locales registrados en PLX-S-01. No tengas en cuenta *DefaultAccount* y *WDAGUtilityAccount*, que son cuentas especiales utilizadas por el sistema para determinadas tareas administrativas.

- ¿Coinciden tus contestaciones a las preguntas 14 y 15? La respuesta debe ser sí. Los usuarios que observas ahora en PLX-S-01 son los mismos que había en PLX-S-DC antes de promocionarlo a controlador de dominio.

  Las cuentas de usuario locales existentes en un servidor se trasforman a cuentas del domino cuando éste se promociona a controlador de dominio. Como las cuentas locales *Administrador* e *Invitado* son integradas (y por tanto no eliminables), se garantiza, como mínimo, la disponibilidad de estas cuentas en el domino tras su creación.

  En caso de estas prácticas, antes de la promoción de PLX-S-DC a controlador de dominio, también se encontraba disponible la cuenta *Alumno* (no integrada). Para que dicha cuenta no se pierda, es pasada automáticamente a la base de datos de usuarios del dominio.
- Apaga PLX-S-01.

Pertenencia a grupos

- Para ver a qué grupos pertenece un usuario, en la herramienta *Usuarios y equipos de Active Directory* se pincha sobre él y en la ficha *Miembro de* se ve la pertenencia a grupos.

- Abre *Usuarios y equipos de Active Directory*. Selecciona el contendor *Users*. Observa que el usuario *Administrador* pertenece, entre otros, a los grupos *Admins del dominio* y *Usuarios del dominio*.

  (16) PREGUNTA. Observa el usuario *Alumno*. ¿A qué grupos integrados pertenece?

- En general, los usuarios pueden pertenecer a varios grupos integrados, con objeto de asignarles diferentes "derechos de acceso a recursos", así como "roles administrativos".
- Elimina el usuario *Alumno*, ya que no forma parte de los usuarios de la organización educativa de ejemplo. *Botón derecho -> Eliminar*.

Actualización de contraseñas

- Con objeto de mantener el orden indispensable para la realización de las prácticas, se utilizará la misma clave para todos los usuarios del dominio. Esta clave será *ADclave00*. Como ahora el usuario *Administrador* de la máquina PLX-S-DC es un usuario del dominio, es recomendable asignarle esta clave.
- En la herramienta *Usuarios y equipos de Active Directory*, botón derecho sobre *Administrador*. Entonces *Restablecer contraseña*. Introduce la contraseña *ADclave00*. Cierra sesión. Inicia de nuevo sesión con el usuario *Administrador*. De esta forma comprobarás que el cambio de contraseña ha sido satisfactorio.

Creación de unidades organizativas

- En este punto, se crearán las OU definidas anteriormente: *Empleados*, *Alumnos*, *Clientes-Admin* y *Clientes-Docencia*.
- Para crear una OU, en *Usuarios y equipos de Active Directory* se selecciona el dominio *(practical.local)*. Entonces *Botón derecho -> Nuevo -> Unidad organizativa*.
- Crea las 4 OU.

Creación de los usuarios de la organización

- En este punto, se crearán los usuarios definidos anteriormente: Prof1, Prof2, PAS1 y PAS2 en la OU *Empleados*, y Alu1 y Alu2 en la OU *Alumnos*.
- Para crear un usuario, se selecciona la OU. Entonces *Botón derecho -> Nuevo -> Usuario*. Se abre la ventana *Nuevo objeto: Usuario*. El nombre del usuario se debe introducir en el campo *Nombre de inicio de sesión de usuario*. No obstante, para que se pueda completar su creación, hay que escribir algo en los datos personales del usuario. De forma estándar, puedes volver a escribir el nombre de inicio de sesión en el campo *Nombre completo*. Como contraseña se utiliza *ADclave00* para todos los usuarios, y como opciones de contraseña, *El usuario no puede cambiar la contraseña* y *La contraseña nunca expira*.
- Siguiendo las indicaciones anteriores, crea los 6 usuarios de la organización.

Creación de grupos de seguridad

- En este punto, se crearán los grupos *Profesores*, *Alumnos* y *PAS* en los que se incluirán los usuarios correspondientes. *Profesores* y *PAS* se crearán en la OU *Empleados*, y *Alumnos* en la OU *Alumnos*.
- Para crear un grupo, se selecciona la OU. Entonces *Botón derecho -> Nuevo -> Grupo*. En el ámbito, se puede dejar el valor por defecto (Global), aunque daría igual el ámbito elegido ya que la infraestructura de DA creada en esta práctica es de dominio único. El *Tipo de grupo* sería *Seguridad*. (NOTA: los grupos de *Distribución* están orientados a la gestión de correo electrónico).
- Siguiendo las indicaciones anteriores, crea los tres grupos.

- A continuación, hay que agregar a cada grupo los usuarios correspondientes. Se ejemplifica cómo llevar a cabo esta operación mediante el grupo *Alumnos*. Para ello, abre el grupo *Alumnos*, elige la ficha *Miembros* y se pulsa en *Agregar*. Se abre la ventana de selección de objetos. Para no tener que elegir entre todos los objetos del directorio, en el campo *Desde esta ubicación* (que por defecto tiene como valor el dominio) se introduce la OU *Alumnos*. Para esto, tienes que pulsar en *Ubicaciones* y seleccionar la OU *Alumnos*. Después, pulsa en *Opciones avanzadas* y después en *Buscar ahora*. Entonces se muestran todos los elementos existentes en la ubicación seleccionada (*Alumnos*, en este caso). Selecciona *Alu1* y *Alu2* y *Acepta*. Tendrás que volver a *Aceptar* un par de veces para completar la operación.
- Siguiendo las indicaciones anteriores, agrega los usuarios *Prof1* y *Prof2* al grupo *Profesores*, y los usuarios *PAS1* y *PAS2* al grupo *PAS*.

Sobre las cuentas de equipo

Aunque las cuentas de equipo pueden crearse manualmente, después no resulta sencillo asignarlas a los equipos que se unen al dominio. Es mejor dejar que el directorio activo haga el trabajo automáticamente, ya que cuando se agrega un equipo al dominio, se crea pare él una cuenta en el contenedor *Computers*. En este momento, *Computers* está vacía, ya que aún no se han agregado equipos al dominio.

Agregación de equipos al dominio

De momento, se agregarán al dominio los equipos clientes PLX-C-51 y PLX-C-52.

- Arranca las máquinas PLX-C-51 y PLX-C-52. Ambas ya deben tener el DNS correctamente configurado.

Agregación de PLX-C-51 al dominio

- Antes de agregar este equipo al dominio, vas a fijarte en el estado de un servicio del sistema operativo. Se trata del servicio *Net Logon*, que ha sido introducido en la figura 2.
- En PLX-C-51, abre la herramienta *Servicios*, a la que se accede a través de *Herramientas de Windows*. Busca el servicio *Net Logon*. Lee la descripción del servicio.

  (17) PREGUNTA. ¿Cuál es el cometido del servicio *Net Logon*?

- Observa que el servicio se encuentra en el estado *detenido* y que su *Tipo de inicio* está en el estado *Manual*. O sea, como el equipo aún no ha sido agregado a ningún dominio, el servicio *Net Logon* no se encuentra operativo.
- Minimiza la consola *Servicios*.
- *Panel de control -> Sistemas y seguridad -> Sistema*. Entonces, debajo de las *Especificaciones del dispositivo*, observa el área de *Vínculos relacionados*. Pulsa sobre el vínculo *Dominio o grupo de trabajo*. Se abre la venta *Propiedades del sistema*. En la ficha *Nombre de equipo*, pulsa en *Cambiar*. En el apartado *Miembro del*, selecciona *Dominio* y escribe el nombre del dominio al que se desea unir el equipo (*practicas.local*). Pulsa en *Aceptar*. Entonces el equipo se conecta al servidor de dominio. Éste solicita introducir las credenciales de un usuario (del dominio) que tenga el derecho de agregar equipos. Utiliza el usuario *Administrador*. Debes observar un mensaje indicando que el equipo se unió correctamente al dominio (NOTA: es posible que este mensaje quede oculto por la ventana del sistema). Pulsa en *Aceptar*.
- Reinicia el equipo para que los cambios sean efectivos.
- En *Panel de control -> Sistemas y seguridad -> Sistema*, comprueba que el equipo se ha agregado al dominio. Esto puede verse fácilmente, ya que cuando un equipo se agrega a un dominio, debajo del campo *Nombre del dispositivo* (PLX-C-51, en este caso), se agrega otro

campo llamado *Nombre completo del dispositivo*, en el que se incluye el dominio. El contenido de este campo debe ser *PLX-C-51.practicas.local*.

- En PLX-C-51, Abre la herramienta *Servicios*. Busca el servicio *Net Logon*. Observa que el servicio está *En ejecución* y que su tipo de inicio ha sido modificado a *Automático*, lo que significa que el servicio se inicia automáticamente en el arranque del sistema.

  (18) PREGUNTA. ¿Por qué es necesario que el tipo de arranque de *Net Logon* se haya configurado en *Automático*? Si tienes dudas, pregúntale a tu profesor.

DNS

- Al agregar el equipo al dominio, se ha registrado automáticamente en el DNS. En PLX-C-52 (el otro cliente arrancado), haz un *ping* al nombre DNS de PLX-C-51, o sea, a *PLX-C-51.practicas.local*, comprobando que responde.
- En PLX-S-DC, abre la herramienta DNS y comprueba que aparece un registro de tipo A para PLX-C-51.

  (19) PREGUNTA. ¿En qué zona de búsqueda has comprobado la existencia de dicho registro?

Cuenta de ordenador

- Cuando un equipo se agrega al dominio, se crea para él automáticamente una cuenta de ordenador. Estas cuentas se crean por defecto en el contenedor *Computers*.
- En PLX-S-DC, abre *Usuarios y equipos de Active Directory*. Observa que en el contenedor *Computers* se ha creado una cuenta (Objeto) para el ordenador que se acaba de agregar al dominio. Ábrela y observa la información que contiene.

  (20) PREGUNTA. Indica el grupo de seguridad al que pertenece la cuenta de equipo que se acaba de crear.

Agregación de PLX-C-52 al dominio

- Con objeto de observar un aspecto de uso del DNS, antes de agregar este equipo al dominio, en su configuración IP, borra el DNS, dejándolo en blanco.
- Trata de agregar el equipo al dominio.
- Se produce un fallo, ¿por qué? La razón es que el servidor DNS está sin configurar. Por consiguiente, el equipo no tiene forma de saber quién es "practicas.local". Esto debe hacerte reflexionar sobre la importancia esencial que tiene el DNS en la localización de los diferentes servicios de red.
- Vuelve a configurar correctamente el DNS.
- Agrega el equipo al dominio. Ahora la agregación debe llevarse a cabo satisfactoriamente.
- Reinicia.
- Inicia sesión con el usuario *Alumno*.
- Comprueba la pertenencia al dominio en *Panel de control -> Sistemas y seguridad -> Sistema*.
- Comprueba que el equipo se ha registrado en el DNS. Para ello, haz *ping* al nombre DNS del equipo (*PLX-C-52.practicas.local*) desde PLX-C-51.
- En PLX-S-DC, comprueba la creación del registro DNS.
- En PLX-S-DC, en el contenedor *Computers*, comprueba la creación de la cuenta del equipo en el dominio.
- A partir de este momento, PLX-C-52 ya no se necesita en esta sesión. Apaga la máquina.

- **Inicio de sesión en el dominio frente a inicio de sesión local**

  Una vez que un equipo ha sido integrado en un dominio, hay dos formas de iniciar sesión en él, o bien utilizando un usuario local, o bien utilizando un usuario del dominio. Los ordenadores del dominio pueden ser utilizados por cualquier usuario del dominio de forma segura. Esto es muy útil en ordenadores de uso libre, como los ubicados en aulas de informática, bibliotecas, etc.

  A continuación, se van a analizar las diferentes formas de inicio de sesión en los ordenadores del dominio.

  Repaso de perfiles de usuario

  Es un espacio para almacenar datos e información de configuración relativos a cada usuario. Cada usuario que inicia sesión en una máquina debe tener un perfil, y si no lo tiene, se le crea.

  Los perfiles de usuario se almacenan en la carpeta *C:\Usuarios*.

  - En PLX-C-51, entra en esta carpeta y observa que en ella se encuentra únicamente el perfil del usuario *Alumno*. Adicionalmente, hay una carpeta llamada *Acceso público*, cuyo objetivo es contener información pública para todos los usuarios del sistema.

  La idea es que cuando se inicia sesión con un usuario del dominio, se crea un perfil para dicho usuario en la carpeta C:*Usuarios*.

  Inicio de sesión con usuarios del dominio

  - En PLX-C-51, cierra la sesión abierta con el usuario local.
  - En la pantalla de inicio de sesión, el sistema presenta el último usuario que inició sesión, que en este caso es el usuario local *Alumno*.
  - Para iniciar sesión con un usuario diferente, pulsa sobre *Otro usuario*. Como el equipo está integrado en el dominio PRACTICAS, el inicio de sesión por defecto se realizará en este dominio, tal y como se indica debajo del campo *Contraseña*. Para iniciar sesión en PRACTICAS, utiliza, por ejemplo, el usuario *Alu1*. Entonces el sistema contacta con el servidor de dominio para iniciar sesión con este usuario.
  - Al iniciar sesión por primera vez con *Alu1*, se crea un perfil para este usuario en la carpeta *Usuarios*. Por defecto, el nombre de esta carpeta es igual que el nombre del usuario. Comprueba la creación de la carpeta indicada.
  - Usando el botón de *Inicio*, comprueba que el usuario que tiene sesión abierta es *Alu1*.

  Inicio de sesión con usuarios locales

  - Cierra la sesión abierta con *Alu1*.
  - Cuando trates de iniciar sesión de nuevo, el sistema presenta el último usuario utilizado, que es *Alu1*.
  - En este punto, vas a volver a iniciar sesión con el usuario local *Alumno*. Para ello, pulsa sobre *Otro usuario*.
  - Por defecto, el sistema trata de iniciar sesión en el dominio. Para indicar al sistema que el usuario que se va a introducir es local, debe precederse el usuario con los caracteres ".\" (sin las comillas), que significan "ordenador local". Observa que en el momento que escribes ".\" en el campo *Nombre de usuario*, debajo del campo *Contraseña*, se indica "Iniciar sesión en PLX-C-51", que es el ordenador local. Entonces, escribe *Alumno* y la contraseña e inicia sesión.
  - Usando el botón de *Inicio*, comprueba que el usuario que tiene sesión abierta es *Alumno*.

- **Gestión de acceso a un recurso compartido mediante Directorio Activo**

  Se dispone de un servidor de ficheros que proporciona un recurso compartido de archivos a la red. Se desea controlar la autorización de acceso a dicho recurso mediante la integración del servidor de ficheros en el directorio activo. Dicha integración proporcionará la posibilidad de utilizar los grupos de seguridad del directorio para controlar el acceso.

Preparación del servidor de ficheros

- Se utiliza PLX-S-01 como servidor de ficheros.

Actualización de la nomenclatura del servidor

- En el *Administrador de Hyper-V*, cambia el nombre de la máquina virtual. El nombre elegido para este servidor es PLX-S-FS *(File Server)*.
- Desconecta el disco duro (PLX-S-01.vhdx) de la máquina virtual y después cambia el nombre del fichero correspondiente a este disco. Utiliza el nombre PLX-S-FS.vhdx.
- Conectar el disco PLX-S-FS.vhdx a la máquina PLX-S-FS.
- Arranca la máquina. Cambia el nombre del sistema por PLX-S-FS. Reinicia para que el cambio sea efectivo.
- Comprueba que el cambio de nombre se ha realizado satisfactoriamente.

Actualización de los usuarios del servidor

Eliminación del usuario Alumno

Es necesario eliminar este usuario para que no se produzca autenticación silenciosa al establecer conexiones desde los clientes a este servidor, ya que en los clientes existe este mismo usuario con la misma clave.

- Elimina el usuario *Alumno* utilizando la herramienta *Administración de equipos*.
- Elimina el perfil del usuario *Alumno*, de la carpeta *C:\Usuarios*.

Creación del usuario Pruebas

- Este será el usuario utilizado para acceder al recurso compartido proporcionado por PLX-S-FS.
- Usuario: *Pruebas*; Clave: *MVclave00*. Selecciona las opciones *El usuario no puede cambiar la contraseña* y *La contraseña nunca expira*.
- Cierra sesión y entrar con el usuario *Pruebas*, con objeto de comprobar que este usuario se ha creado correctamente.
- Ten en cuenta que, a diferencia del usuario *Administrador* para el que se ha cambiado el fondo del escritorio a tono de color verde, el escritorio del usuario *Pruebas* se configura con el tono de color por defecto, que es el azul, y que es el que se utiliza también en el sistema anfitrión. Ten esto en cuenta para no confundir si te encuentras en la MV o en el anfitrión.
- Intenta apagar PLX-S-FS. ¿Puedes? Investiga cómo apagar el equipo. Si tienes dudas, pregúntale a tu profesor.

  (21) PREGUNTA. Indica lo que has hecho para poder apagar el equipo.

- En este punto, PLX-S-FS debe quedar apagada.

Agregación de un disco de datos

En un servidor de ficheros, resulta razonable separar los espacios de almacenamiento utilizados para el sistema operativo y para los datos. Así resulta habitual utilizar, por ejemplo, un disco duro separado para cada uno de ellos. De esta forma, si el sistema resulta dañado (debido a un virus, por ejemplo), los datos no se verán afectados y serán recuperables.

En un entorno de virtualización, la separación resulta todavía más efectiva, ya que un disco de datos conectado a una máquina virtual puede moverse a otra máquina secundaria sin ninguna dificultad, si ocurriese un problema en la máquina primaria. De esta forma se mejora la disponibilidad de los datos almacenados.

- PLX-S-FS está apagada.
- Crea un nuevo disco duro virtual, con formato *vhdx*, de tipo *dinámico*, llamado PLX-S-FS-DATA.vhdx y de 40GB. Éste es el disco de datos.
- Conecta este disco como segundo disco a la controladora ISCSI de la máquina virtual.
- Arranca la máquina. Inicia sesión con el *Administrador*.

Creación de un volumen en el disco de datos

- Abre el *Administrador de discos*, que se encuentra ubicado en *Administración de equipos*.
- Observa el nuevo disco que acabas de agregar al sistema, de 40GB. Cuando se agrega un nuevo disco, por defecto, está desactivado. Hasta que un administrador no lo active, el disco no será utilizable.
- Botón derecho sobre el disco, en el área donde se indica *Desactivado*. Entonces elige la opción *En línea*. El disco pasa el estado *Sin inicializar*. Esto significa que aún no ha sido particionado.
- De nuevo, botón derecho sobre el disco, en el área donde se indica *Sin inicializar*. Entonces elige la opción *Inicializar disco*. Como *estilo de partición*, elige GPT, que es el estilo moderno de particionado, y *Aceptar*. En este punto, el disco ya está listo para ser utilizado.
- Se procede ahora a crear un volumen en el disco. Botón derecho sobre el área que representa el espacio de almacenamiento del disco -> *Nuevo volumen simple*. En *Especificar el tamaño del volumen*, asigna todo el tamaño disponible al volumen.
- En *Asignar letra de unidad o ruta de acceso*, asigna la letra D.
- *En Formatear la partición*, elige *Formatear este volumen con la configuración siguiente*.
  - Sistema de archivos: *NTFS*
  - Tamaño de la unidad de asignación: *Predeterminado*
  - Etiqueta de volumen: *en blanco*
  - Dar formato rápido: *Sí*
- Cuanto termine el asistente, estará disponible en el sistema el volumen *D*.
- Abre el explorador de archivos y comprueba que el nuevo volumen está disponible.

Creación del recurso compartido de archivos

- En el directorio raíz de la unidad D, crear una carpeta llamada *Compartida*.
- Se procede ahora a compartir *Compartida*. Para ello, *Botón derecho -> Propiedades ->* ficha *compartir -> botón Compartir*. Entonces se muestra la lista de usuarios y grupos que tendrán acceso al recurso a través de la red. De momento, solo se muestra el usuario *Administrador* y el grupo *Administradores*, lo que es demasiado restrictivo. Aquí es donde hay que establecer qué usuarios estarán autorizados a acceder al recurso (Autorización).
- Agrega también el usuario *Pruebas*, proporcionándole permisos de lectura y escritura. Pulsa *Compartir* para completar la operación.
- Se muestra la ventana *Detección de redes y uso compartido de archivos*. Elegir la opción *No, convertir la red a la que estoy conectado en una red privada*. Entonces se pulsa en *Listo* para completar la operación.
- Para comprobar que el recurso ha sido compartido, abre *Administración de equipos*, despliega *Carpetas compartidas* y selecciona *Recursos compartidos*. Entonces puedes ver todos los recursos compartidos por el sistema. Varios de ellos terminan con el carácter $, lo que significa que son recursos compartidos ocultos. Entre los recursos disponibles, debes observar *Compartida*.

Acceso al recurso compartido cuando *FS está fuera del dominio*

- En PLX-S-FS, iniciar sesión con el usuario Pruebas.
- En PLX-S-FS (usuario *Pruebas*), crea un fichero de texto cualquiera en *D:\Compartida*.
- En este punto, se plantea la necesidad de acceder a *Compartida* (recurso de red) desde el equipo PLX-C-51.
- El primer aspecto clave a tratar es la nomenclatura del recurso compartido. Para identificar a estos recursos se utilizan nombres UNC. Lee el Anexo A, al final de este guion, donde se explican los nombres UNC. Entonces contesta las siguientes preguntas:

  (22) PREGUNTA. ¿Qué significa UNC?

  (23) PREGUNTA. ¿Qué elementos pueden utilizarse en un nombre UNC para identificar al servidor del recurso de red?

- En PLX-C-51, se procede a acceder al recurso compartido. Para ello, abre la herramienta *Buscar*, y en el campo de búsqueda introduce el nombre UNC del servidor que proporciona el recurso compartido. En este caso, el nombre es el siguiente: \\192.168.0.1.
- En este punto, PLX-S-FS solicita unas credenciales para proporcionar acceso a sus recursos compartidos. Utiliza las credenciales correspondientes al usuario *Pruebas* recientemente creado. Entonces se abre una ventana de exploración mostrando los recursos compartidos por el servidor. En dicha ventana debes observar el recurso *Compartida*.
- La autorización de acceso se establece en cada recurso. Como el usuario *Pruebas* ha sido autorizado en el recurso *Compartida*, el usuario podrá acceder al recurso (lectura y escritura) sin problemas.
- Comprueba que tienes acceso al fichero que creaste anteriormente, tanto en lectura como en escritura.
- En PLX-C-51, cierra sesión.

PROBLEMA: Para acceder al recurso compartido has tenido que proporcionar unas credenciales de un usuario local de FS. ¿Cómo puede gestionarse la autorización de acceso al recurso para todos los usuarios de la organización? Está claro que añadir al servidor todos los usuarios de la organización no sería eficiente. En este ejemplo, solo hay 6 usuarios, pero podrían ser miles.

SOLUCIÓN: Agregar PLX-S-FS al dominio para poder usar los mecanismos de autorización del dominio, basados en los grupos de seguridad que integran a los usuarios del dominio.

Acceso al recurso compartido cuando *PLX-S-FS está integrado en el dominio*

Agregación de PLX-S-FS al dominio

- Cierra la sesión abierta con el usuario *Pruebas* e inicia sesión como *Administrador*.
- Comprueba la configuración IP de PLX-S-FS. Falta la configuración del DNS. Configúralo con la dirección apropiada.
- Agrega el servidor al dominio. Habrá que reiniciarlo para que la agregación se complete con éxito.

Pruebas de acceso desde PLX-C-51

- Inicia sesión con el usuario local *Alumno*.
- A continuación, se va a proceder a establecer una conexión a los recursos compartidos de PLX-S-FS. Anteriormente, te conectaste a PLX-S-FS utilizando el nombre UNC *\\192.168.0.1*. ¿Se podrá utilizar ahora un nombre UNC alternativo? La respuesta es SÍ. Al integrar PLX-S-FS en el dominio, se ha registrado en el DNS y, por lo tanto, se podrá acceder a sus recursos compartidos con su nombre DNS, es decir, *\\PLX-S-FS.practicas.local*.

- En PLX-C-51, utilizando la herramienta *Buscar*, abre los recursos compartidos en PLX-S-FS, usando el UNC *\\PLX-S-FS.practicas.local*. Cuando el sistema pida credenciales de acceso, utiliza un usuario del dominio, por ejemplo *Prof1*. Comprueba que se proporciona acceso al servidor. Sin embargo, comprueba también que este usuario no puede acceder al recurso *Compartida*. Esto es debido a que el usuario *Prof1* no está autorizado para acceder a este recurso. En este momento ningún usuario del dominio lo está.
- En PLX-C-51, cierra la sesión abierta con el usuario *Alumno*.

Autorización a nivel de dominio

Supongamos que se desea proporcionar acceso al recurso *Compartida* a todos los profesores de la organización.

- En PLX-S-FS, *Compartida -> Botón derecho -> Propiedades* -> ficha *Compartir* -> botón *Compartir*. En la lista de usuarios autorizados para acceder al recurso, eliminar el usuario local *Pruebas*. Entonces seleccionar *Buscar personas*. Se abre la ventana *Seleccionar usuarios o grupos*. En el campo *Desde esta ubicación* debes elegir *practicas.local*. Pulsa en *Opciones avanzadas*. Autentícate en el dominio con el *Administrador*. Pulsar en *Buscar ahora* y elige el grupo *Profesores*. Proporciona acceso de *Lectura y escritura* para este grupo. Entonces *Compartir*.
- En PLX-C-51, inicia sesión con el usuario local. Conéctate a los recursos compartidos de PLX-S-FS autenticándote como *Prof1*. Comprueba que tienes acceso total a *Compartida*.
- En PLX-C-51, cierra sesión.
- En PLX-C-51, inicia sesión con el usuario local. Conéctate a los recursos compartidos de PLX-S-FS autenticándote como *Alu1*. Se establece la conexión. Sin embargo, observa que no puedes acceder a *Compartida*. Esto es debido a que los alumnos no están autorizados para acceder a esta carpeta.
- Apaga todas las máquinas virtuales.

Conclusión

El dominio proporciona un esquema de autenticación y autorización global para todos los recursos proporcionados por los servidores integrados en el dominio.

Anexo A: Nombre de recursos de red

Al igual que hay unos convenios para especificar las ubicaciones que ocupan los archivos en el sistema de ficheros de un ordenador, es necesario también establecer convenios para especificar estas ubicaciones cuando los ficheros se encuentran en un recurso de red, como una carpeta compartida.

En las plataformas Windows, la especificación de las ubicaciones de red se realiza mediante nombres UNC, que es el acrónimo de *Universal Naming Convention*.

Los nombres UNC constan de 3 partes: un nombre de servidor, un nombre de un recurso compartido y, opcionalmente, una ruta hacia una carpeta o fichero.

La estructura de un nombre UNC es la siguiente:

\\servidor\recurso_compartido\ruta_fichero

El servidor se indica mediante un nombre DNS o utilizando una dirección IP.