Tema

4

Administración de Sistemas

Servicio de Directorios

Universidad Francisco de Vitoria
UFV Madrid

Grado en Ingeniería Informática
Escuela Politécnica Superior

Objetivos y resultados de aprendizaje

- Conocer las propiedades principales de los diversos sistemas y su diversa capacidades y adecuación. Realizando un análisis comparativo de sus características distintivas y similitudes. Haciendo hincapié en la gestión de archivos y administración de usuarios.

- Los objetivos específicos consisten en:

  - ✓ Conocer las características de Active Directory, una de las arquitecturas de sistemas más habituales.

  - ✓ Implementar un entorno empresarial basado en Microsoft Windows Server.

Evaluación del tema

- Los resultados de aprendizaje correspondiente a este tema se evaluarán con los siguientes tipos de pruebas:

  - ✓ Pruebas escritas de carácter teórico
  - ✓ Participación en clase
  - ✓ Practica: Implementar un Entorno de AD y probar las características de autenticación centralizada.

Bibliografía

- Para obtener más información puedes consultar:

  ✓ Bibliografía incluida en la guía didáctica.

  ✓ Lectura Obligatorias (Epígrafes DNS y DCHP)

  a) https://docs.microsoft.com/es-es/windows-server/networking/dns/dns-top
  b) https://docs.microsoft.com/es-es/windows-server/networking/technologies/dhcp/dhcp-top
  c) https://learn.microsoft.com/es-es/windows-server/storage/dfs-namespaces/dfs-overview

  ✓ Lectura Recomendada:

  a) https://docs.microsoft.com/es-es/azure/active-directory/fundamentals/auth-ldap
  b) https://forsenergy.com/es-es/dssite/html/842d13a6-aab7-4811-96b8-40ee9aa40dfa.htm

Índice de contenidos

- ✓ Administración de Usuarios y Equipos (Active Directory)
- ✓ GPO: Directivas de Grupo
- ✓ DNS: Sistema de Nombre de Dominios
- ✓ DHCP: Protocolo de Configuración Dinámica de Host

Active Directory (Qué es)

Universidad Francisco de Vitoria UFV Madrid

- AD almacena información acerca de los usuarios, equipos y recursos de red y permite el acceso a los recursos por parte de usuarios y aplicaciones.

- Asimismo, proporciona una forma coherente de asignar nombres, describir, localizar, obtener acceso, administrar y proteger la información de estos recursos.

- En AD se usa LDAP (Lightweight Directory Access Protocol). Es un protocolo de aplicación para trabajar con varios servicios de directorio. Los servicios de directorio, como Active Directory, almacenan información de usuarios y cuentas, e información de seguridad, como contraseñas. Luego, el servicio permite que la información se comparta con otros dispositivos de la red

Active Directory (Funciones)

Universidad Francisco de Vitoria UFV Madrid

- Centralizar el control de los recursos de red.
  - ✓ Al centralizar el control de recursos como servidores, archivos compartidos e impresoras, sólo los usuarios autorizados pueden obtener acceso a los recursos de Active Directory.

- Centralizar y descentralizar la administración de recursos.
  - ✓ Los administradores pueden administrar equipos cliente distribuidos, servicios de red y aplicaciones desde una ubicación central mediante una interfaz de administración coherente o pueden distribuir tareas administrativas mediante la delegación del control de los recursos a otros administradores.

Active Directory (Funciones)

Universidad Francisco de Vitoria UFV Madrid

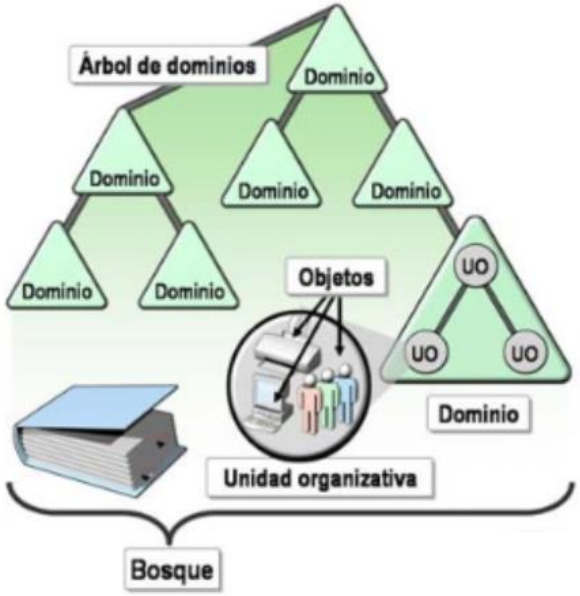
- Almacenar objetos de forma segura en una estructura lógica.
  - ✓ Active Directory almacena todos los recursos como objetos en una estructura lógica, jerárquica y segura.

- Optimizar el tráfico de red.
  - ✓ La estructura física de Active Directory permite utilizar el ancho de banda de red de forma más efectiva.
  - ✓ Por ejemplo, garantiza que, cuando un usuario inicie una sesión en la red, la autoridad de autenticación más cercana a él lo autentique, reduciendo así la cantidad de tráfico de red.

Active Directory (Estructura Lógica)

Universidad Francisco de Vitoria UFV Madrid

- Active Directory proporciona un almacenamiento seguro de información acerca de los objetos en su estructura lógica jerárquica.
- Los objetos de Active Directory representan a los usuarios y los recursos, como equipos e impresoras.
- Algunos objetos son contenedores de otros objetos.
- Conocer el propósito y la función de estos objetos, permite realizar diversas tareas, entre las que se incluyen la instalación, configuración, administración y solución de problemas de Active Directory.
- Componentes de la Estructura Lógica:
  - ✓ Objetos
  - ✓ Unidades Organizativas
  - ✓ Dominios / Árboles de Dominios / Bosques



Active Directory (Estructura Lógica)

Universidad Francisco de Vitoria UFV Madrid

- Objetos.
  - ✓ Son los componentes más básicos de la estructura lógica. Las clases de objetos son plantillas o planos técnicos para los tipos de objetos que se pueden crear en Active Directory.
  - ✓ Cada clase de objetos se define mediante un grupo de atributos, que definen los posibles valores que se pueden asociar a un objeto. Cada objeto posee una única combinación de valores de atributos.
- Unidades organizativas.
  - ✓ Se pueden utilizar estos objetos contenedores para estructurar otros objetos de modo que admitan los propósitos administrativos. Mediante la estructuración de los objetos por unidades organizativas, se facilita su localización y administración.
  - ✓ También se puede delegar la autoridad para administrar una unidad organizativa. Las unidades organizativas pueden estar anidadas en otras unidades organizativas, lo que simplifica la administración de objetos.

Active Directory (Estructura Lógica)

Universidad Francisco de Vitoria UFV Madrid

- Dominios.
  - ✓ Se trata de las unidades funcionales centrales en la estructura lógica de Active Directory que son un conjunto de objetos definidos de forma administrativa y que comparten una base de datos, directivas de seguridad y relaciones de confianza comunes con otros dominios.
  - ✓ Los dominios proporcionan las siguientes tres funciones:
    - ➢ Un límite administrativo para objetos
    - ➢ Un medio de administración de la seguridad para recursos compartidos
    - ➢ Una unidad de replicación para objetos

Active Directory (Estructura Lógica)

Universidad Francisco de Vitoria UFV Madrid

- Árboles de dominios.
  - ✓ Los dominios que están agrupados en estructuras jerárquicas se denominan árboles de dominios. Al agregar un segundo dominio a un árbol, se convierte en secundario del dominio raíz del árbol.
  - ✓ El dominio al que está adjunto un dominio secundario se denomina dominio primario. Un dominio secundario puede tener a su vez su propio dominio secundario.
  - ✓ El nombre de un dominio secundario se combina con el nombre de su dominio primario para formar su propio nombre único de Sistema de nombres de dominio (DNS, Domain Name System), como EPS.UFV.ES De esta forma, el árbol dispone de un a espacio de nombres contiguo.

Active Directory (Estructura Lógica)

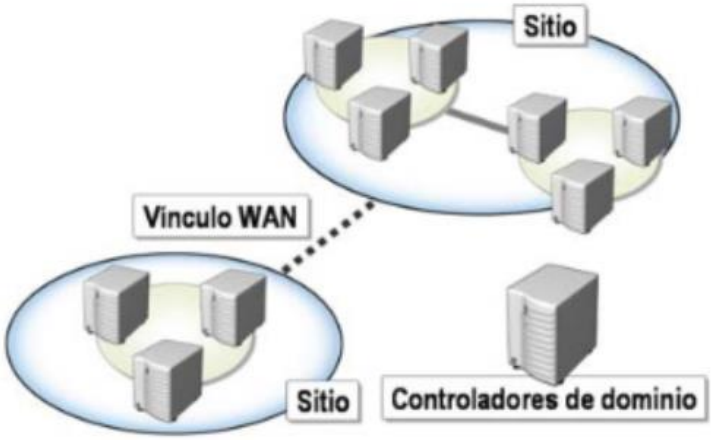
Universidad Francisco de Vitoria UFV Madrid

- Bosques.
  - ✓ Un bosque es una instancia completa de Active Directory. Consta de uno o varios árboles.
  - ✓ En un árbol de sólo dos niveles, que se recomienda para la mayoría de las organizaciones, todos los dominios secundarios se convierten en secundarios del dominio raíz de bosque para formar un árbol contiguo.
  - ✓ El primer dominio del bosque se denomina dominio raíz de bosque. El nombre de ese dominio se refiere al bosque, como por ejemplo UFV.ES
  - ✓ De forma predeterminada, la información de Active Directory se comparte sólo dentro del bosque. De este modo, el bosque es un límite de seguridad para la información contenida en la instancia de Active Directory.

Active Directory (Estructura Física)

Universidad Francisco de Vitoria UFV Madrid

- A diferencia de la estructura lógica, que se basa en requisitos administrativos, la estructura física de Active Directory optimiza el tráfico de red mediante la determinación del lugar y el momento en que se produce la replicación y el tráfico de conexión.
- Para optimizar el uso del ancho de banda de red de Active Directory, se debe comprender la estructura física.
- Los elementos de la estructura física de Active Directory son los siguientes:
  - ✓ Controladores de Dominios
  - ✓ Sitios
  - ✓ Vínculos WAN



Active Directory (Estructura Física)

Universidad Francisco de Vitoria UFV Madrid

- Controladores de dominio (CD).
  - ✓ En estos equipos se ejecuta Microsoft Windows Server y Active Directory.
  - ✓ Cada controlador de dominio realiza funciones de almacenamiento y replicación.
  - ✓ Un controlador de dominio sólo puede admitir un dominio.
  - ✓ Para asegurarse de la disponibilidad continua de Active Directory, cada dominio debe disponer de más de un controlador de dominio.
  - ✓ Cada controlador de dominio contiene las siguientes particiones de Active Directory:
    - ➢ La *partición del dominio:* contiene una replica de todos los objetos de ese dominio.
    - ➢ La *partición de configuración:* contiene la topología del bosque.
    - ➢ La *partición del esquema*: Cada bosque tiene un esquema para que la definición de las clases de objetos sea coherente.
    - ➢ Las particiones de configuración y del esquema pueden replicarse en los CD del bosque. La partición de dominio se replica en los CD del dominio.

Active Directory (Estructura Física)

Universidad Francisco de Vitoria UFV Madrid

- Sitios de Active Directory.
  - ✓ Estos sitios son grupos de equipos conectados correctamente.
  - ✓ Al establecer sitios, los controladores de dominio de un único sitio se comunican con frecuencia. Esta comunicación minimiza la latencia dentro del sitio, es decir, el tiempo necesario para que un cambio realizado en un controlador de dominio pueda replicarse en otros controladores de dominio.
  - ✓ Se pueden crear sitios para optimizar el uso del ancho de banda entre los controladores de dominio que están en ubicaciones diferentes.

Active Directory (Estructura Física)

Universidad Francisco de Vitoria UFV Madrid

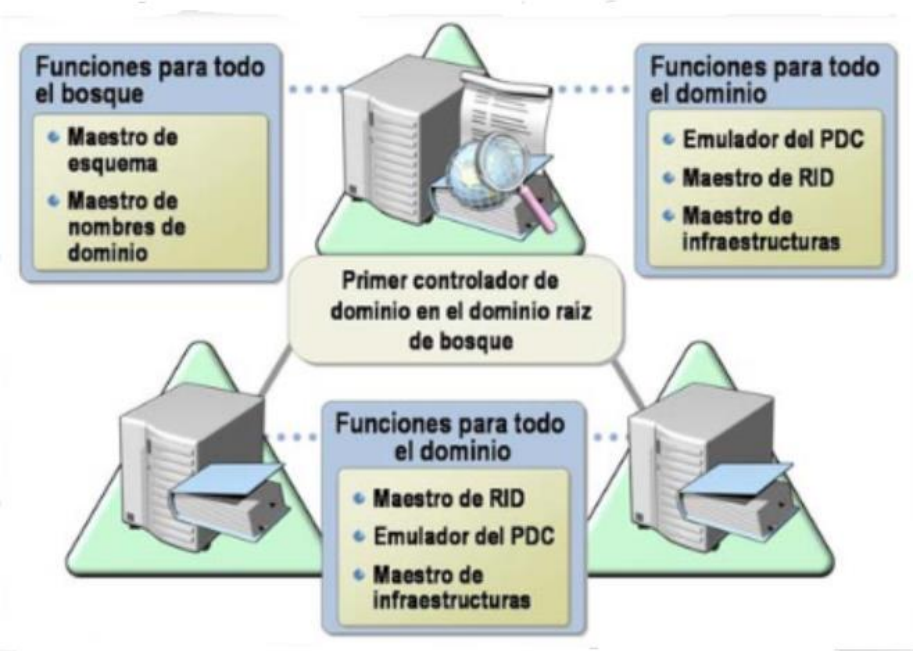
- Vínculos WAN
  - ✓ Los sitios y el establecimiento de vínculos WAN entre ellos, facilitan varias actividades, entre las que se incluyen:
    - ➢ *Replicación*: AD DS (Active Directory Domain Services) equilibra la necesidad de información de directorio actualizada con la de optimización de banda ancha al replicar la información de un sitio cuando los datos están actualizados y entre sitios de acuerdo con un programa configurable.
    - ➢ *Autenticación*: La información del sitio ayuda a que la autenticación sea más rápida y eficaz. Cuando un cliente inicia sesión en un dominio, primero solicita la autenticación a un controlador de dominio del sitio local. Al establecer sitios, se puede garantizar que los clientes usan los controladores de dominio más cercanos a ellos para la autenticación, lo cual reduce la latencia de la autenticación y el tráfico en conexiones de red de área extensa (WAN).

Active Directory (Maestros de Operaciones)

Universidad Francisco de Vitoria UFV Madrid

- Cuando se realiza un cambio en un dominio, el cambio puede replicarse a través de todos los controladores del dominio. Algunos cambios, como los que se realizan en el esquema, pueden replicarse en todos los dominios del bosque. Esta replicación se denomina replicación de varios maestros.

- Active Directory define cinco funciones de maestro de operaciones, con una ubicación predeterminada para cada una. Las funciones de maestro de operaciones abarcan todo el bosque o todo el dominio.



Active Directory (Maestros de Operaciones)

Universidad Francisco de Vitoria UFV Madrid

- Funciones para todo el bosque. (Únicas para un bosque) :
  - ✓ *Maestro de esquema:* Controla todas las actualizaciones del esquema. El esquema contiene una lista general de clases de objetos y atributos utilizados para crear todos los objetos de Active Directory como, por ejemplo, usuarios, equipos e impresoras.
  - ✓ *Maestro de nombres de dominio:* Controla la adición o la eliminación de dominios del bosque. Sólo el controlador de dominio que posee la función de maestro de nombres de dominio puede agregar un nuevo dominio al bosque.
  - ✓ Sólo existe un maestro de esquema y un maestro de nombres de dominio en todo el bosque.

Active Directory (Maestros de Operaciones)

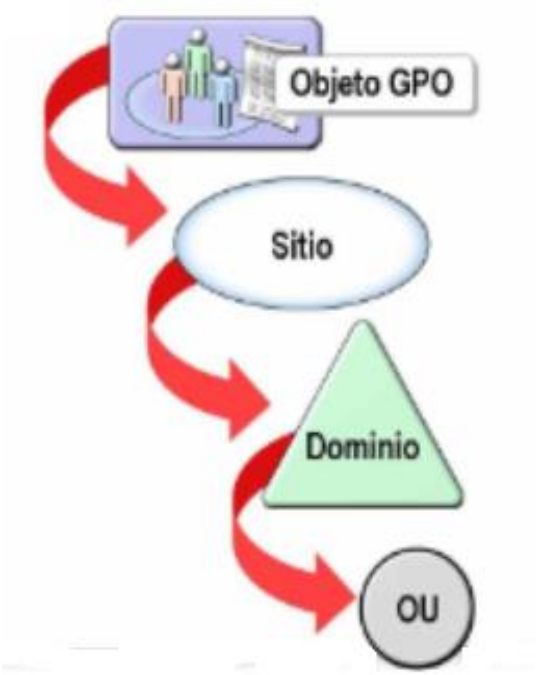
Universidad Francisco de Vitoria UFV Madrid

- Funciones para todo el dominio. (Únicas para cada dominio de un bosque) :
  - ✓ *Emulador del controlador de dominio principal:* (PDC, Primary domain controller). Admite controladores de reserva (BDC, Backup domain controller).El emulador del PDC es el primer controlador de dominio que se crea en un dominio nuevo.
  - ✓ *Maestro de identificadores relativos*: Este maestro asigna bloques de identificadores relativos (RID, relative identifier) a cada controlador del dominio. A continuación, el controlador de dominio asigna un RID a los objetos creados a partir de su bloque asignado de identificadores relativos.
  - ✓ *Maestro de infraestructuras:* Al desplazar objetos de un dominio a otro, este maestro actualiza las referencias a objetos de su dominio que apuntan al objeto en el otro dominio. La referencia al objeto contiene el identificador único global (GUID, globally unique identifier) del objeto
  - ✓ Cada dominio de un bosque dispone de su propio emulador del PDC, maestro de RID y maestro de infraestructuras.

GPO (Objeto de Directiva de Grupo)

Universidad Francisco de Vitoria UFV Madrid

- El servicio de directorios Active Directory utiliza la Directiva de grupo para administrar los usuarios y equipos de la red.
- Mediante la Directiva de grupo se puede definir el estado del entorno de trabajo de un usuario una sola vez y, a continuación, dejar que la familia Windows Server aplique de manera continua la configuración de Directiva de grupo definida.
- Se puede aplicar la configuración de Directiva de grupo en toda la organización, o bien sólo a grupos específicos de usuarios y equipos.



GPO (Objeto de Directiva de Grupo)

Universidad Francisco de Vitoria UFV Madrid

- Directiva de grupo para usuarios
  - ✓ La configuración de Directiva de grupo para usuarios incluye el comportamiento específico del sistema operativo, la configuración de escritorio, la configuración de seguridad y las opciones de aplicaciones asignadas y publicadas, la configuración de aplicaciones, las opciones de redirección de carpetas y las secuencias de comandos de inicio y cierre de sesión de los usuarios.
  - ✓ La configuración de Directiva de grupo relativa al usuario se aplica cuando éste inicia sesión en el equipo y durante el ciclo de actualización periódico.
  - ✓ La configuración de Directiva de grupo que personaliza el entorno de escritorio del usuario, o aplica directivas de bloqueo a los usuarios, se encuentra en Configuración de usuario, en el Editor de objetos de directiva de grupo.

GPO (Objeto de Directiva de Grupo)

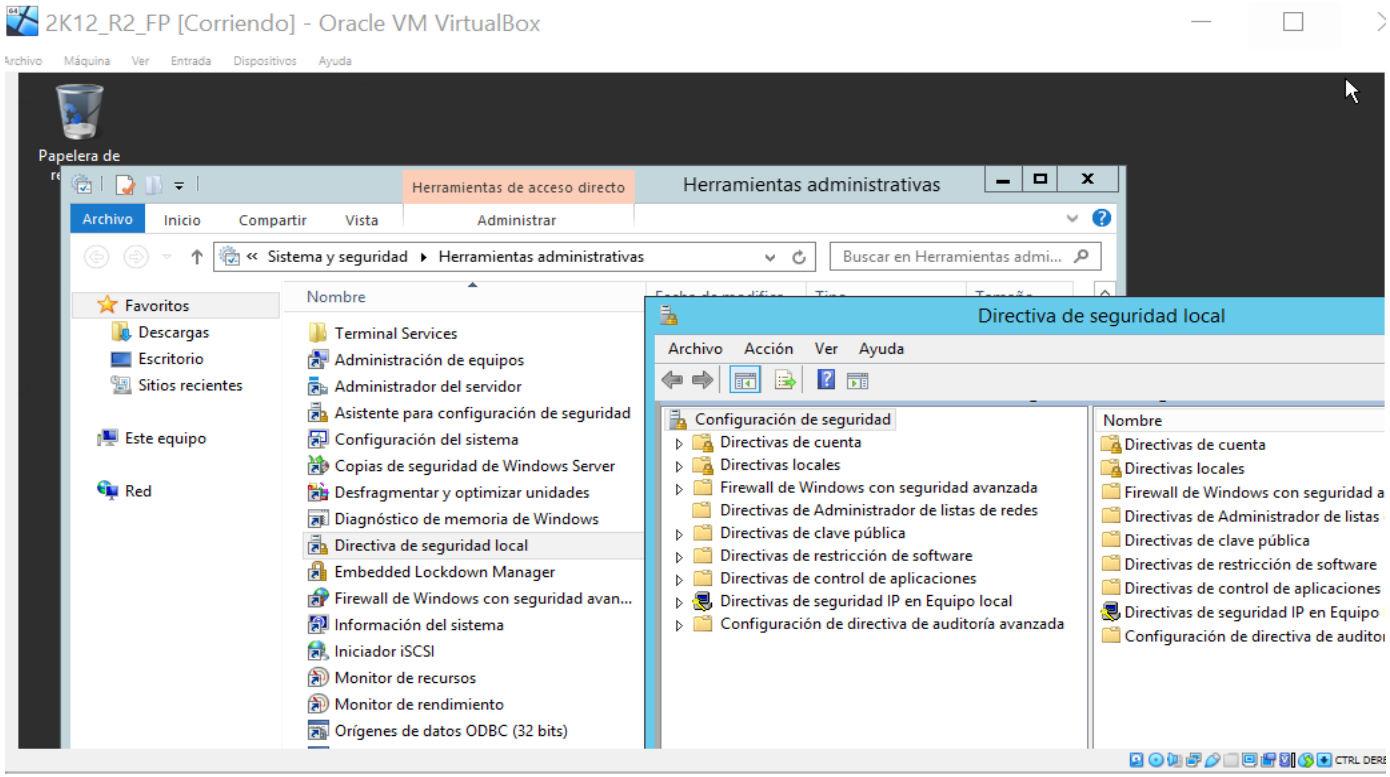
Universidad Francisco de Vitoria UFV Madrid

- Directiva de grupo del Equipo
  - ✓ La configuración de Directiva de grupo incluye el comportamiento del sistema operativo, el comportamiento del escritorio, la configuración de seguridad, las secuencias de comandos de inicio y cierre del equipo, las opciones de aplicación asignadas por el equipo y la configuración de aplicaciones.
  - ✓ La configuración de Directiva de grupo relativa al equipo se aplica cuando el sistema operativo se inicializa y durante el ciclo de actualización periódico. En general, la configuración de Directiva de grupo relativa al equipo tiene prioridad sobre cualquier otra configuración de Directiva de grupo relativa al usuario con la que pueda estar en conflicto.
  - ✓ La configuración de Directiva de grupo que personaliza el entorno de escritorio de todos los usuarios de un equipo, o que aplica directivas de seguridad a los equipos de una red, se encuentra en Configuración del equipo, en el Editor de objetos de Directiva de grupo.

GPO (Objeto de Directiva de Grupo)

Universidad Francisco de Vitoria UFV Madrid

- Para modificar un objeto de Directiva de grupo local es necesario haber iniciado sesión como miembro del grupo Administradores del dominio, Administradores de organización o Propietarios del creador de Directiva de grupo.
- Configurar una directiva de equipo local:



GPO (Objeto de Directiva de Grupo)

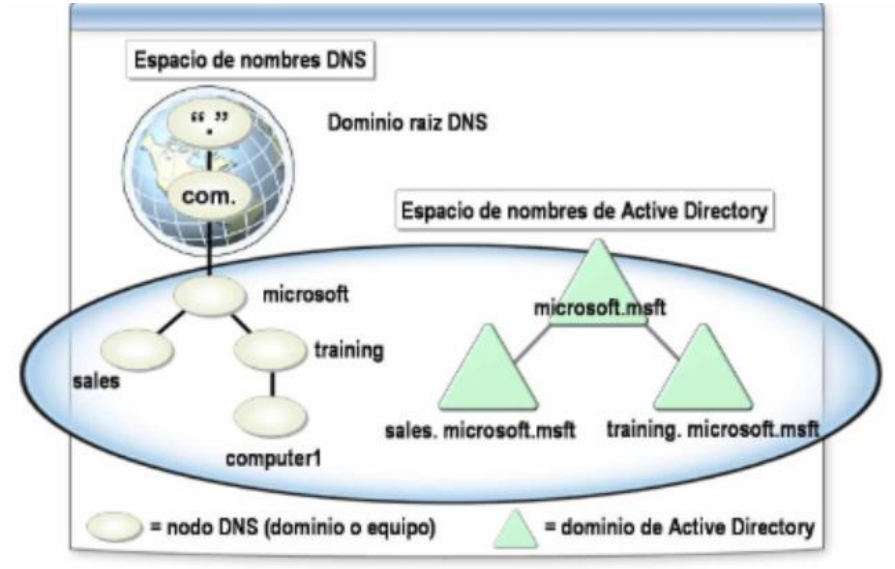
Universidad Francisco de Vitoria UFV Madrid

- Herencias y Prioridad
  - ✓ El orden en que se aplican los GPO depende del contenedor de Active Directory al que se vinculen los objetos. Se aplican primero al sitio, luego a los dominios y, finalmente, a las unidades organizativas de los dominios.
  - ✓ Los objetos de Directiva de grupo se acumulan, es decir, se pueden heredar Un contendor secundario hereda los objetos de Directiva de grupo del contenedor primario.
  - ✓ La herencia de Directiva de grupo es el orden en que Windows Server aplica los objetos de Directiva de grupo. El orden en que se aplican y cómo se heredan finalmente determina qué valores de configuración afectan a los usuarios y equipos.
  - ✓ Si hay varios objetos de Directiva de grupo establecidos en el mismo valor, de forma predeterminada, el último que se aplica tiene prioridad.

DNS (Domain Name System)

Universidad Francisco de Vitoria UFV Madrid

- Integración de DNS y Active Directory
  - ✓ La integración de DNS y Active Directory resulta esencial, puesto que un equipo cliente de una red con Windows Server 2003 debe poder localizar un controlador de dominio para que los usuarios puedan iniciar la sesión en un dominio o utilicen los servicios proporcionados por Active Directory.
  - ✓ Los clientes localizan controladores de dominio y servicios utilizando registros de recurso A y registros SRV.

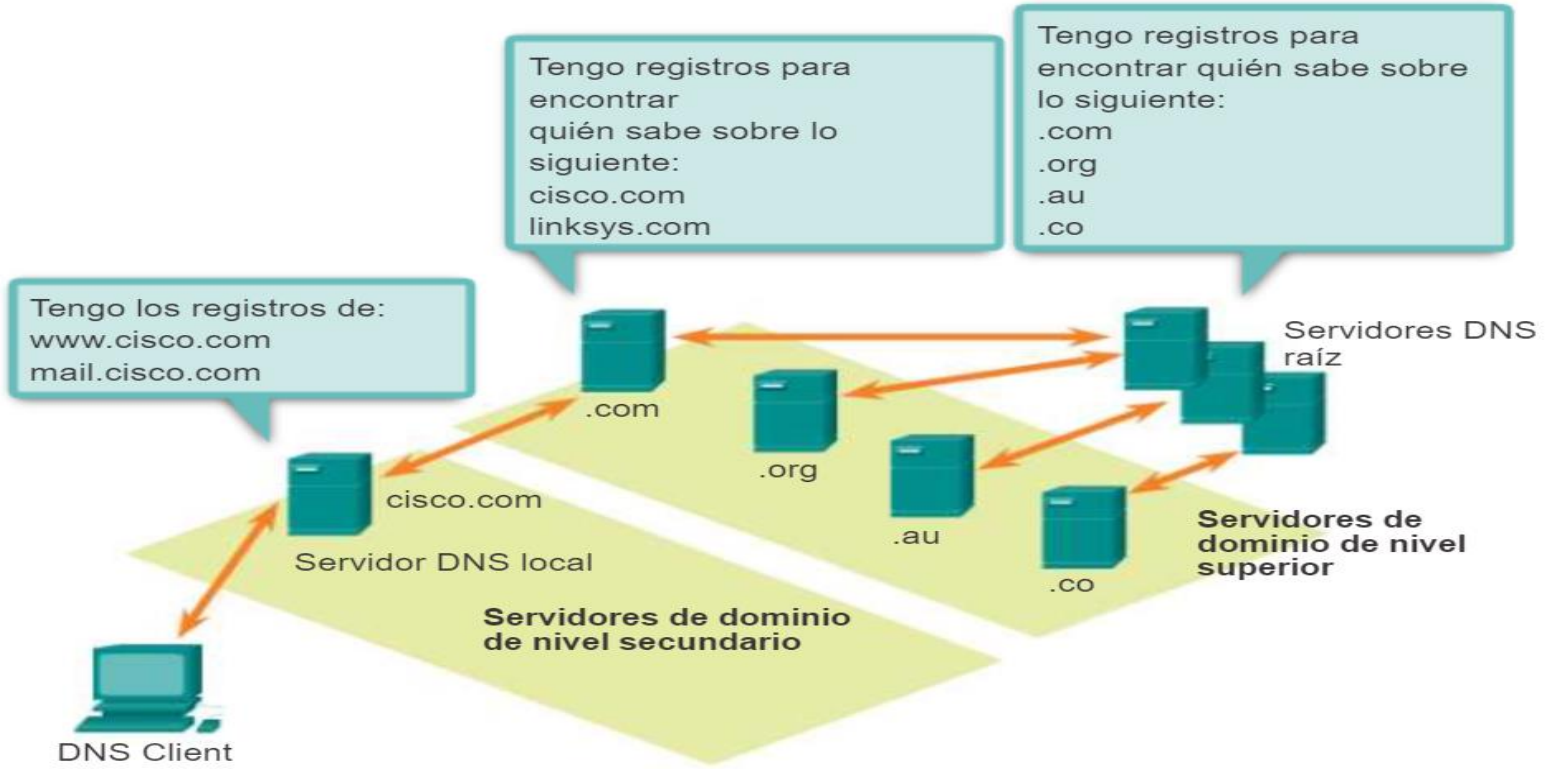


- ➢ El registro de recurso A contiene el FQDN y la dirección IP del controlador de dominio.
- ➢ El registro SRV contiene el FQDN del controlador de dominio y el nombre del servicio que proporciona dicho controlador de dominio.

DNS (Domain Name System)

Universidad Francisco de Vitoria UFV Madrid

- Niveles Servidores DNS(*)



Una jerarquía de servidores DNS contiene los registros de recursos que relacionan los nombres con las direcciones.

(*) http://itroque.edu.mx/cisco/cisco1/course/module10/10.2.2.3/10.2.2.3.html

DHCP

Universidad Francisco de Vitoria UFV Madrid

- Dynamic Host Configuration Protocol
  - ✓ Todos los dispositivos de una red basada en TCP/IP deben tener una dirección IP de unidifusión única para tener acceso a la red y sus recursos. Sin DHCP, las direcciones IP de los equipos nuevos o los equipos que se mueven de una subred a otra deben configurarse manualmente. Las direcciones IP de los equipos que se quitan de la red se deben reclamar manualmente.
  - ✓ Con DHCP, todo este proceso se automatiza y administra de forma centralizada. El servidor DHCP mantiene un grupo de direcciones IP y concede una dirección a cualquier cliente habilitado para DHCP cuando se inicia en la red. Dado que las direcciones IP son dinámicas (alquiladas) en lugar de estáticas (asignadas de forma permanente), las direcciones que ya no se usan se devuelven automáticamente al grupo para su reasignación.

DFS

Universidad Francisco de Vitoria UFV Madrid

- Distributed File Systems
  - ✓ Un sistema de archivos distribuido, o DFS, es un esquema de almacenamiento y gestión de datos que permite a los usuarios o a las aplicaciones acceder a archivos desde un almacenamiento compartido en cualquiera de los múltiples servidores en red. Sus datos compartidos y almacenados en un clúster de servidores permiten a muchos usuarios compartir recursos de almacenamiento y archivos de datos en múltiples equipos.
  - ✓ Razones para su Uso
    - Para almacenar datos de forma permanente en soportes de almacenamiento secundario.
    - Para compartir información de forma fácil, eficiente y segura entre usuarios y aplicaciones.

DFS

Universidad Francisco de Vitoria UFV Madrid

- Características
  - ✓ **Transparencia de acceso**: los usuarios acceden a los archivos como si estuvieran almacenados localmente en sus propios terminales
  - ✓ **Transparencia de la ubicación**: las máquinas host no necesitan saber dónde se encuentran los datos del archivo porque el DFS lo gestiona
  - ✓ **Bloqueo de archivos:** el sistema bloquea los archivos en uso en todas las ubicaciones para evitar que dos usuarios de diferentes ubicaciones hagan cambios en el mismo archivo al mismo tiempo.
  - ✓ **Cifrado de datos en tránsito:** DFS protege los datos cifrándolos a medida que se mueven por el sistema

DFS

Universidad Francisco de Vitoria UFV Madrid

- Funcionamiento
  - ✓ Los datos en sí pueden residir en diversos dispositivos o sistemas de almacenamiento, desde unidades de disco duro (HDD) hasta unidades de estado sólido (SSD) y la cloud pública.
  - ✓ Cuando un usuario hace clic en un nombre de archivo para acceder a esos datos, el DFS comprueba varios servidores, dependiendo de dónde se encuentre el usuario, y luego sirve la primera copia disponible del archivo en ese grupo de servidores. Esto evita que cualquiera de los servidores se atasque demasiado cuando muchos usuarios acceden a los archivos y también mantiene los datos disponibles a pesar de que el servidor funcione mal o falle.
  - ✓ A través de la función de replicación de archivos DFS, cualquier cambio realizado en un archivo se copia en todas las instancias de ese archivo en los nodos del servidor.