UD03
Servicio de Directorio

Índice

Introducción

Introducción

- Un **servicio de directorio** es un **conjunto de aplicaciones** utilizada en los **sistemas cliente/servidor**, que sirven **para organizar y centralizar la información** de todos los:
  - Usuarios.
  - Equipos.
  - Grupos (usuarios o equipos).
  - Dominios.
  - Recursos compartidos.
  - Políticas de seguridad.
  - ...
- La gran **ventaja** es que, al centralizar toda esta información, **facilita a los administradores**:
  - La gestión de los **recursos** de la red.
  - El control de acceso de los **usuarios**.

Introducción

- En **Windows Server** vamos a utilizar **Active Directory Domain Services (AD DS)** como Servicio de Directorio.
- Antes de proceder a la instalación y configuración del Servicio de Directorio, debemos tener claro algunos **conceptos relacionados**:
  - **Directorio y Active Directory**.
  - **Active Directory Domain Services (AD DS)**.
  - **Dominio**.
  - **Controlador de dominio**.
  - **Árboles**.
  - **Bosques**.
  - **Unidad organizativa**.
  - **Usuarios, grupos y equipos.**
  - **Esquema.**
  - **Sitio**.

Directorio y Active Directory

Directorio y Active Directory

- Un **Directorio** es un **repositorio único** que contiene la **información** relativa a los **usuarios** y **recursos** de una organización.

Directorio y Active Directory

- **Active Directory es un tipo de Directorio,** que conforma una **base de datos jerárquica de objetos**.
- Los **objetos** de Active Directory **representan las entidades que pueden administrarse en una red de ordenadores**, en nuestro caso en un **Dominio** de Windows Server. **Estos objetos representan**:
  - **Entidades o recursos** existentes en red (usuarios, grupos, equipos,…).
  - **Relaciones entre ellos** (qué miembros tiene cada grupo, qué grupos tienen acceso a cada recurso, directivas de seguridad,…).
- Esta **base de datos** centralizada de objetos de administración puede ser **consultada por todos los ordenadores** miembros del **Dominio** y **modificada** por todos los **Controladores del Dominio**.
- La **gestión de un Dominio** supone **crear y configurar** adecuadamente los **objetos del directorio.**

Directorio y Active Directory

- Una de las **ventajas que ofrece Active Directory** es que puede **utilizar**:
  - **LDAP** (Lightweight Directory Access Protocol - Protocolo Ligero de Acceso a Directorios): es un **protocolo de acceso estándar** que permitirá la consulta de información contenida en el directorio.
  - **ADSI** (Active Directory Services Interface - Interfaces de Servicio de Active Directory): un conjunto de **herramientas ofrecidas por Microsoft**, que tienen una **interfaz orientada a objetos** y que permiten el **acceso a características** de Active Directory Domain Services que **no** están soportadas por **LDAP**.

Active Directory Domain Services (AD DS)

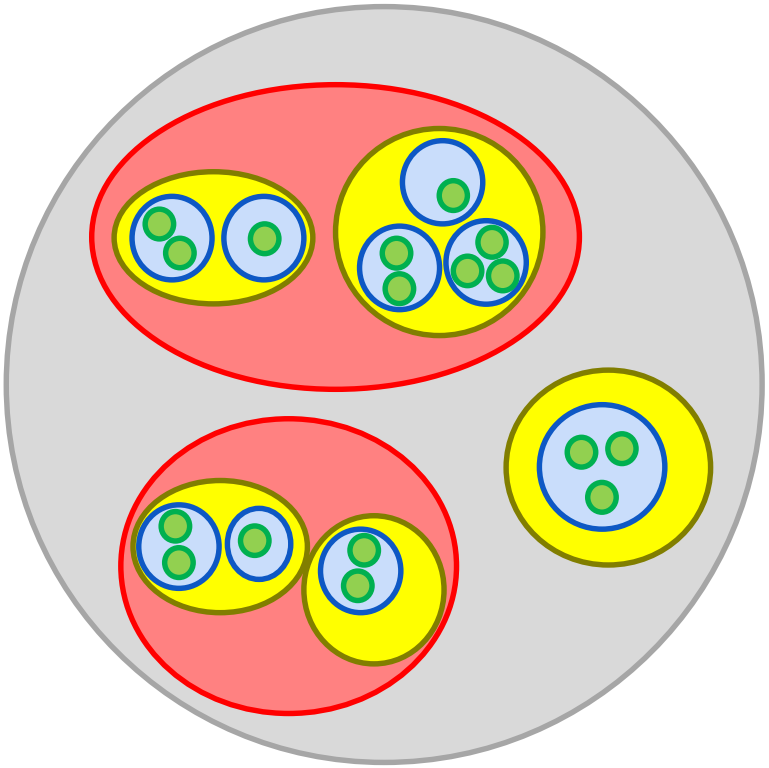
Active Directory Domain Services (AD DS)

- **Windows Server** ofrece la herramienta **Active Directory Domain Services (AD DS)** para llevar a cabo la **gestión de Dominios en Active Directory**.
- **AD DS** proporciona los **métodos para almacenar datos de directorio** y poner dichos datos **a disposición de los usuarios y administradores** de la red.
- Podemos decir, que **AD DS** es el Sistema de Gestión de Base de Datos (**SGBD**) de **Active Directory**.

Active Directory Domain Services (AD DS)

- **Active Directory Domain Services (AD DS)** nos va a permitir:
  - **Almacenar y administrar** toda la **información** relativa a una **organización**. Esto incluirá: sitios, ordenadores, usuarios, objetos compartidos y cualquier otra cosa que pueda formar parte de la infraestructura de red.
  - **Establecer políticas**, sobre los diferentes objetos, que serán válidas en **toda la organización**.
  - **Realizar operaciones**, como la **instalación de programas**, o la aplicación de **actualizaciones críticas**, de forma simultánea y centralizada, en multitud de clientes.

Dominios, Árboles, Bosques, Unidades Organizativas y Esquema



Dominios

- Un **Dominio** es un **conjunto de equipos, usuarios y recursos** en una **misma red** y bajo la **misma base de datos** de Directorio.
- Un **Directorio**, como Active Directory, puede tener **uno o varios Dominios**.
- Cada **Dominio** tiene que tener un **nombre de dominio o Domain Name System (DNS)** que lo identificara dentro del sistema y que se utilizará **además para denominar a los equipos de la red** que pertenezcan a dicho Dominio.
- Para poner **nombre a los Dominios** se utiliza el **protocolo DNS**. Por este motivo, Active Directory necesita **al menos un servidor DNS instalado en la red**.
- Llamamos **Dominio Raíz al primer dominio que se crea** y representa el **sufijo** de la denominación de todos los **equipos de la red**, siguiendo la **nomenclatura** del protocolo **DNS**.

Dominios

- El **uso de Dominios** es de gran **utilidad** porque nos permite:
  - **Definir y delimitar la seguridad entre los distintos Dominios**, ya que las directivas de seguridad y las listas de control de acceso (ACL) serán distintas en cada Dominio de la red.
  - **Delegar permisos administrativos a nivel de unidades organizativas**, que serán subconjuntos dentro del Dominio.
  - **Aplicar políticas de grupo o directivas de grupo**, que serán subconjuntos dentro de las unidades organizativas del Dominio.
  - **Replicar la información**. Cada Dominio almacena datos de sus objetos pero puede **intercambiar información con otros Dominios**, por ejemplo, sobre sus perfiles de usuarios.
- **Cada Dominio** debe tener a su vez un **Controlador de Dominio**.

Dominios

Sistema de nombres de dominio o DNS

- El **sistema de nombres de dominio o DNS** es una **base de datos de nombres** en la que se ubican los nombres de dominio y se **traducen** a **direcciones** de protocolo de internet (**IP**).
- La **estructura** de los nombres de dominio se compone de **varias partes**, llamadas **etiquetas**.
- Estas **etiquetas muestran la jerarquía** dentro del domino.
- La **jerarquía** de dominio se lee **de derecha a izquierda** y cada sección indica una subdivisión.
- El **dominio de nivel superior** es lo que aparece **después del punto** en el nombre de dominio. Por ejemplo: **smr.informatica.es** o **smr.informatica.local**

Dominios
Controlador de Dominio

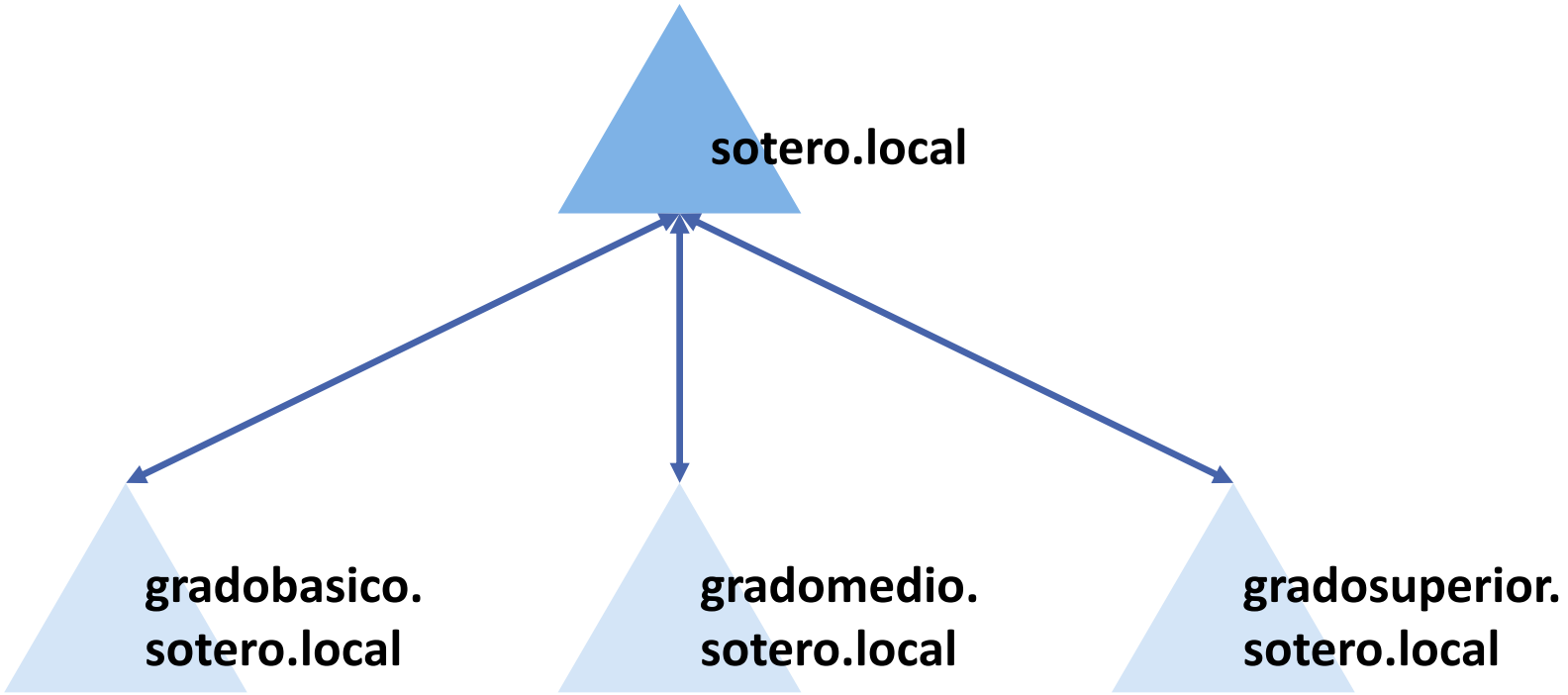
- Un **Controlador de Dominio** (Domain Controller - DC) **contiene la base de datos** de objetos del Directorio **para un determinado Dominio**, **incluida** la información relativa a la **seguridad**.
- El **Controlador de Dominio** será responsable de la **autenticación de objetos** dentro de su **ámbito de control** (facilita la apertura y el cierre de sesión de usuario, las búsquedas en el directorio, etc.).
- En **cada Dominio** existe **al menos un Controlador de Dominio, pero puede haber varios controladores de Dominio asociados**, de modo que cada uno de ellos represente un **rol diferente dentro del Directorio**. Sin embargo, a todos los efectos, **todos** los controladores de dominio, dentro del mismo dominio, **tendrán la misma importancia.**

Árboles

- Un **Árbol de Dominio**, o simplemente árbol, es una **colección de dominios que dependen de una raíz común** y se encuentra organizados como una determinada **jerarquía**.
- Esta **jerarquía** queda **representada** por un **espacio de nombres DNS común**. Es lo que **también** se denomina un **espacio contiguo de nombres**.
- El **espació común de nombres** nos permite saber si dos **Dominios forman parte del mismo árbol**. Por ejemplo:
  - **sotero.es** y **gradomedio.sotero.es** forman parte del **mismo árbol**.
  - **sotero.es** y **gradomedio.camas.es NO** forman parte del **mismo árbol**.
- El **objetivo** de crear este tipo de estructura es **fragmentar los datos del Directorio Activo**, y con ellos:
  - Se **replican** sólo las partes **necesarias**.
  - Por tanto, **ahorramos** ancho de banda en la **red**.

Árboles

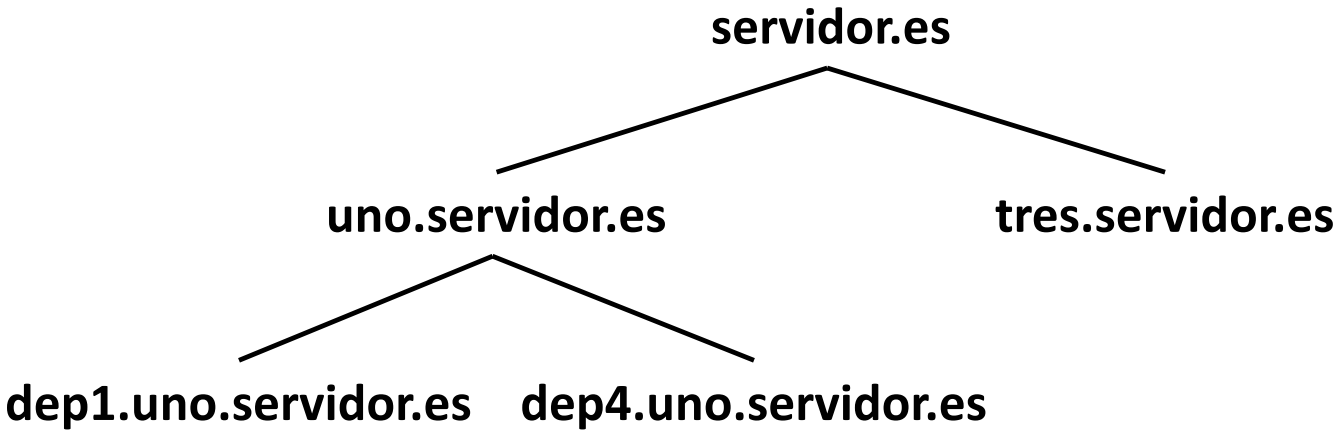
- Si un determinado **usuario** es creado dentro de un **dominio**, este usuario será **reconocido automáticamente** en todos los **dominios** que **dependan jerárquicamente** del dominio al que pertenece.



Árboles

- **Ejemplo**: de los siguientes dominios, ¿Cuáles formarían un Árbol de Dominio si el Dominio Raíz es servidor.es?

tres.servidor.es	servidor2.es	dep4.uno.servidor.es
uno.servidor.es	dep1.uno.servidor.es	tres.servidor2.es



Bosques

- Un **Bosque de Árboles de Dominios**, o simplemente Bosque, está formado por un **conjunto de Árboles de Dominio** que **NO forman un espacio de nombres contiguos**.
- El **Bosque es el mayor contenedor lógico dentro de Active Directory**, abarcando a **todos los dominios** dentro de su ámbito.
- Dentro del Bosque, los **dominios están interconectados por Relaciones de Confianza Transitivas que se construyen automáticamente**. De esta forma:
  - Todos los **dominios** de un bosque **confían** automáticamente **unos en otros.**
  - Los **diferentes árboles** podrán **compartir sus recursos**.

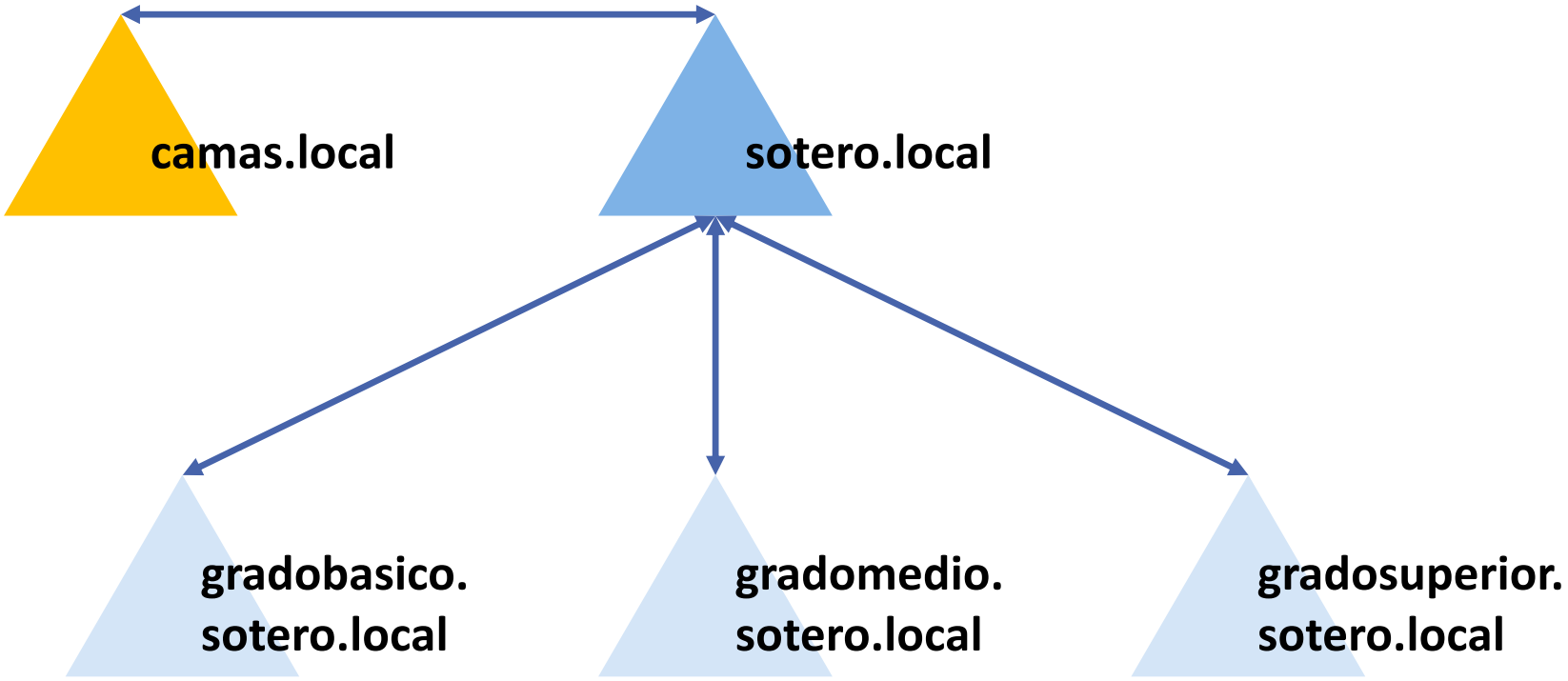
Nota: más adelante definiremos el Concepto de Relación de Confianza.

Bosques

- Un **Bosque contiene** al menos un Dominio, que será el **Dominio Raíz** del Bosque.
- Pero, si no existe una relación jerárquica entre todos los Dominios que forman el Bosque, debido a que pertenecen a distintos Árboles, **¿Cuál es el Dominio Raíz del Bosque?**
- **Respuesta**: Cuando instalamos el **primer Dominio** en un ordenador de nuestra red, que previamente dispone de Windows Server, además del propio Dominio, estamos creando la **raíz de un nuevo Árbol** y también la **raíz de un nuevo Bosque**.
- El **Dominio Raíz del Bosque contiene el Esquema del Bosque**, que se **compartirá con el resto de dominios** que formen parte de dicho bosque

Nota: más adelante definiremos el concepto de Esquema.

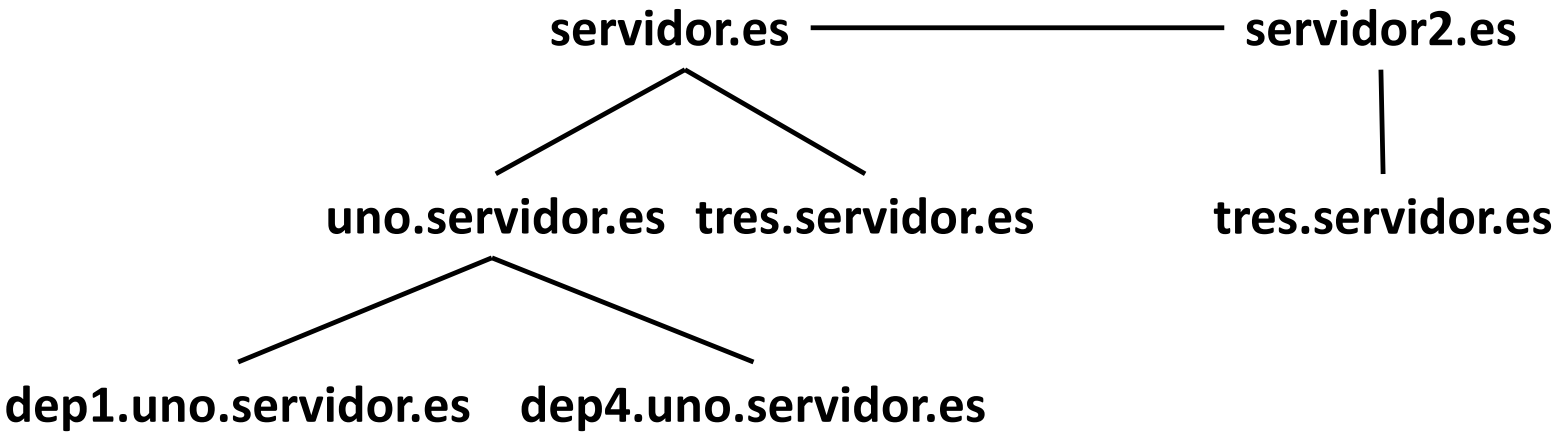
Bosques


camas.local
sotero.local
gradobasico.
sotero.local
gradomedio.
sotero.local
gradosuperior.
sotero.local

Bosques

- **Ejemplo**: con los siguientes dominios, ¿Cuántos Árboles de Dominio hay? ¿Cuál sería la estructura del Bosque si todos los Árboles pertenecen al mismo Bosque?

tres.servidor.es	servidor2.es	dep4.uno.servidor.es
uno.servidor.es	dep1.uno.servidor.es	tres.servidor2.es



Unidades Organizativas

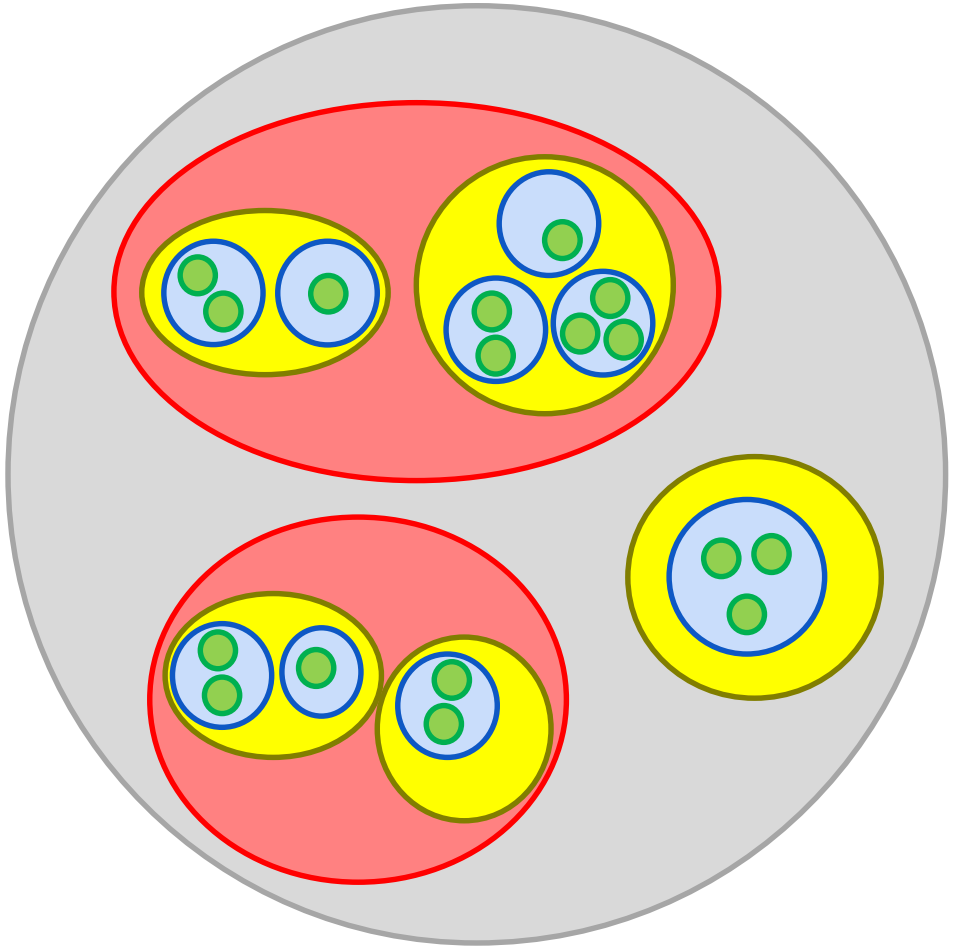
- Las **Unidades Organizativas (UO)** se utilizan dentro de Active Directory para **agrupar objetos dentro de un Dominio**, como usuarios, grupos y equipos, con unos **requisitos comunes para su configuración, administración y mantenimiento**, evitando tener mezclados elementos de diferentes categorías.
- La **Unidad Organizativa se crea sobre un Dominio**, así que, a la hora de crearla, hay que indicar Dominio donde la vamos a crear.
- Las **Unidades Organizativas** forman también una **estructura jerárquica** dentro del Dominio al que pertenecen, pudiéndose **crear una unidad dentro de otra**.
- Las Unidades Organizativas **facilitan la administración en redes de grandes dimensiones**, ya que nos permiten:
  - Establecer una **estructura lógica** que represente de forma adecuada **nuestra organización** y simplifique la administración.
  - **Simplificar la delegación de autoridad** (completa o parcial) sobre los **objetos** que contienen, **a otros usuarios o grupos**.

Esquema

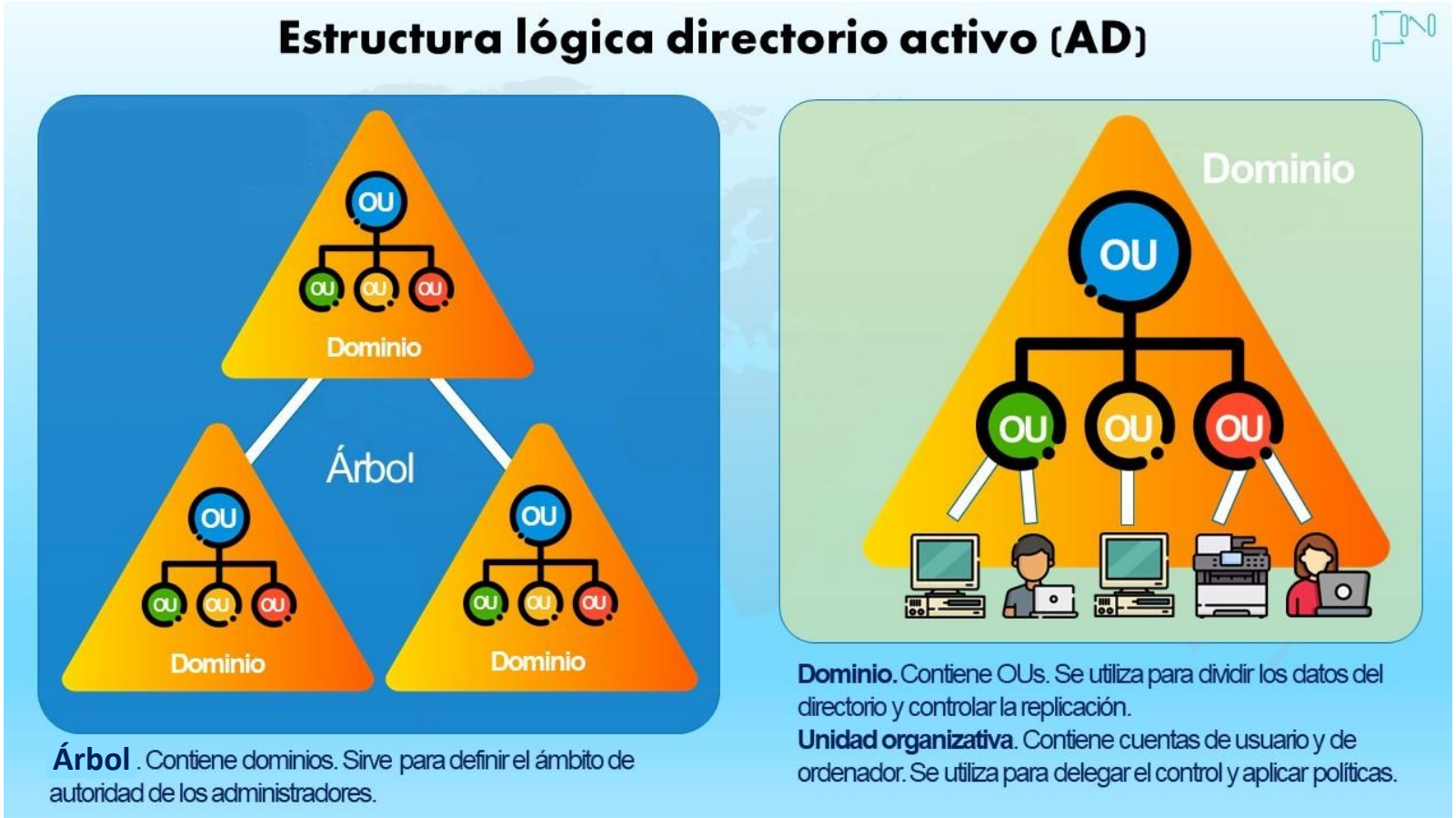
- El **concepto de esquema está relacionado con bases de datos**. El esquema de una base de datos **describe la estructura** de la misma.
- En **Active Directory** se utiliza la palabra **Esquema** para referirse a la **estructura de la base de datos de los objetos del Directorio**. En este sentido, utilizaremos la palabra **atributo** para referirnos a **cada uno de los tipos de información almacenada**.

Resumen

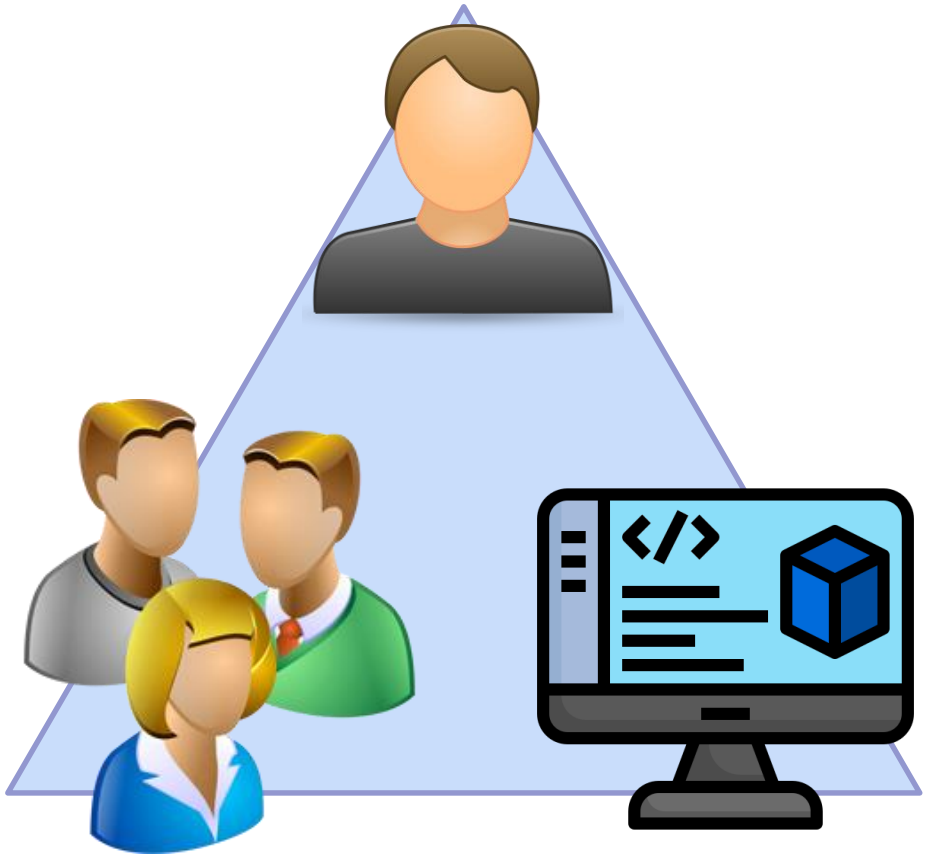
- Bosque
- Árbol
- Dominio
- Unidad Organizativa
- Objeto



Resumen


Estructura lógica directorio activo (AD)
OU
OU
OU
OU
Dominio
Árbol
OU
OU
OU
OU
OU
OU
Dominio
Dominio
Árbol . Contiene dominios. Sirve para definir el ámbito de autoridad de los administradores.
Dominio
OU
OU
OU
OU
Dominio. Contiene OUs. Se utiliza para dividir los datos del directorio y controlar la replicación.
Unidad organizativa. Contiene cuentas de usuario y de ordenador. Se utiliza para delegar el control y aplicar políticas.

Usuarios, Grupos, Equipos y Sitio



Usuarios, grupos, equipos y sitios

- **Usuarios**:
  - No son usuarios locales, son usuarios **globales al Dominio**.
  - Un usuario es **aquel que entra en el sistema utilizando una cuenta** que le dará **acceso** a ciertos **archivos** y **carpetas**, con una **serie de privilegios**, como realizar cambios en el equipo y configurar sus preferencias personales.
- **Grupos**:
  - Los grupos pueden contener **conjuntos de usuarios** y otros **objetos** del Directorio.
  - Se utilizan para **conceder permisos a un conjunto de usuarios** de forma **simultánea**.
  - Los grupos se pueden **crear y eliminar**, además de **añadirles usuarios**.
  - La **eliminación de un grupo no elimina a los usuarios u objetos** que este contenga.

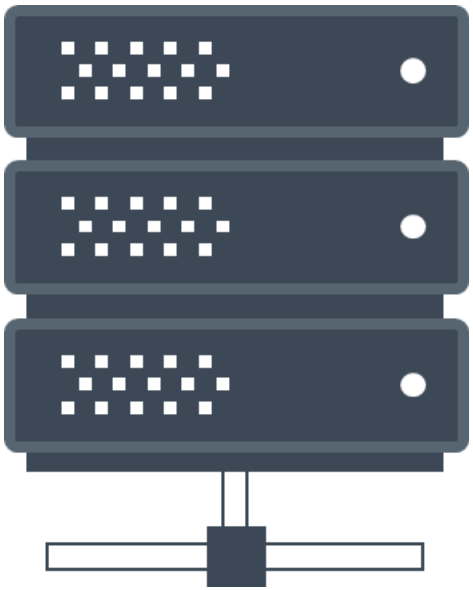
Usuarios, grupos, equipos y sitios

- **Equipos**:
  - Los equipos (**clientes o servidores**) son los **ordenadores que pertenecen al Dominio**.
  - Cada equipo tiene su **Cuenta de Equipo** en el Directorio Activo.
  - Para cada equipo se **guarda la siguiente información** en su Cuenta de Equipo:
    - **Nombre del equipo** (sin el sufijo DNS).
    - **Contraseña**, que utiliza para **acreditarse** en el dominio.
    - **SID**, que es un **identificador de seguridad** se usa para identificar de forma única una entidad de seguridad o un grupo de seguridad.
  - Algunos equipos (**servidores**) pueden contener **Controladores de Dominio**.
  - Las **Cuentas de los Equipos se encuentran** en:
    - **Equipos con Controladores de Dominio** → Unidad Organizativa **DomainControllers**.
    - **Resto** de equipos → Unidad Organizativa **Computers**.

Usuarios, grupos, equipos y sitios

- **Sitios**:
  - Un **Sitio es un grupo de ordenadores (clientes)** que se encuentran **relacionados** de una forma **lógica**.
  - Estos ordenadores pueden encontrarse **físicamente en el mismo lugar o** estar en distintos lugares pero **conectados en red**.
  - **Cada sitio** de Active Directory se **asigna a un Dominio** y un **Dominio** puede tener **varios sitios asignados** a él.
  - De todo lo anterior se deduce que, cada **Dominio tiene al menos un Controlador de Dominio y el Dominio tiene asociados uno o varios sitios**, formados por un grupo de ordenadores clientes que no tienen porque estar en el mismo lugar. Por tanto, el **Controlador de Dominio no tiene porque estar en la misma zona geográfica de los clientes** a los que ofrece sus servicios pero, **todos juntos formarán el mismo sitio**.

Tipos de controladores de dominio



Tipos de controladores de dominio

- En **Active Directory** nos podemos encontrar los **siguientes tipos** de controladores de dominio:
  - **Primer controlador de dominio para nuevo bosque**:
    - Es el **ordenador** donde instalamos el **primer dominio**, que actúa como **dominio raíz del bosque**.
    - Solemos referirnos a él como **Maestro de Operaciones o FSMO** (Flexible Single Master Operations).
  - **Primer controlador de dominio para nuevo dominio**:
    - Es el **ordenador** donde instalamos un **nuevo dominio en** el **bosque**, también llamado **subdominio**.
    - Esta organización en **dominio y subdominios** nos permite crear **árboles con estructura jerárquica** que **reflejan la estructura** geográfica o jerárquica de nuestra **empresa u organización**.

Tipos de controladores de dominio

- **Controladores de dominio adicionales para un dominio**:
  - Es un nuevo ordenador en el instalamos un **controlador de dominio para un dominio que ya cuenta con otro**.
  - Aportan las siguientes **ventajas** sobre la infraestructura:
    - **Tolerancia a fallos**. Si un controlador de dominio falla, el otro sigue dando servicio.
    - **Aumenta el rendimiento** al balancear de carga entre los dos controladores.
- **Controladores de dominio de solo lectura** (RODCs – Read-Only Domain Controllers):
  - Orientado a **entornos con escasa seguridad física** (por ejemplo, una sucursal).
  - **No existe personal** que se pueda **responsabilizar** del mismo, así que una **medida de seguridad** es que no se pueda consultar, pero no modificar.

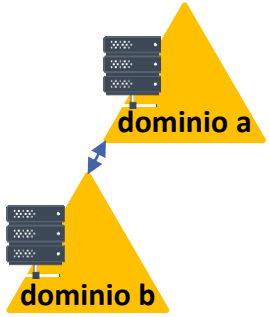
Tipos de controladores de dominio

- **Controladores de dominio virtualizados**:
  - Controladores de dominio que se **ejecutan en máquinas virtuales** (normalmente sobre **Hyper-V**).
  - En las **versiones más recientes de Windows Server** se incluyen **herramientas** que ayudan a la **implantación** y **administración** de este tipo de servidores.

Tipos de controladores de dominio

- En esta **unidad vamos** a configurar los **tres primeros casos**, es decir:
  - Primer controlador de dominio para **nuevo bosque**.

  - Primer controlador de dominio para **nuevo dominio**.



  - Controlador de dominio **adicional** para un dominio.