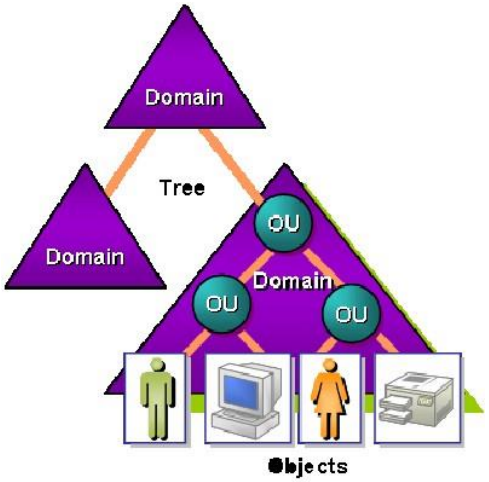
GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO

Servicios de directorio

José Pablo Hernández

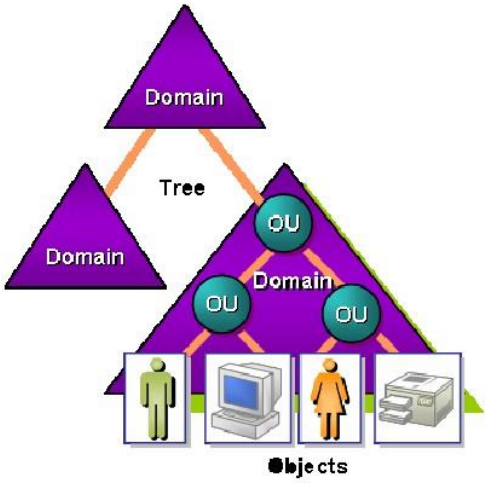
Servicios de directorio.



Un servicio de directorio (SD) es una aplicación o un conjunto de aplicaciones que almacena y organiza la información sobre los usuarios de una red de ordenadores, sobre recursos de red, y permite a los administradores gestionar el acceso de usuarios a los recursos sobre dicha red.

Además, los servicios de directorio actúan como una capa de abstracción entre los usuarios y los recursos compartidos.

Servicios de directorio.

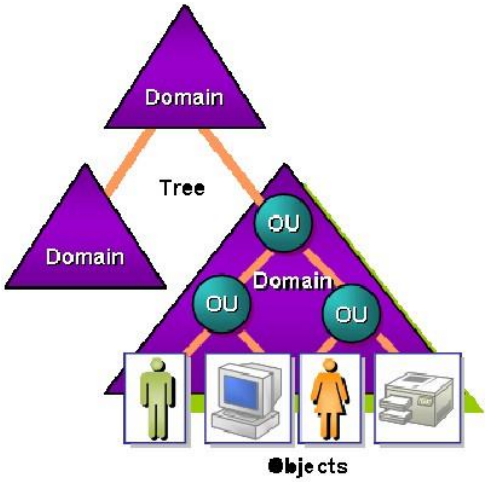


Como base de datos, un servicio del directorio está altamente optimizado para lecturas y proporciona alternativas avanzadas de búsqueda en los diferentes atributos que se puedan asociar a los objetos de un directorio.

Los datos que se almacenan en el directorio son definidos por un esquema extensible y modificable.

Los servicios de directorio utilizan un modelo distribuido para almacenar su información y esa información generalmente está replicada entre los servidores que forman el directorio.

Servicios de directorio.



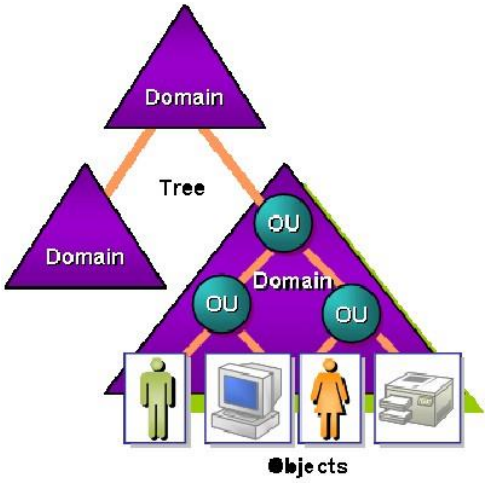
Un servicio de directorio sencillo es, por ejemplo, un servicio de nombres para corresponder los nombres de los recursos de la red con sus respectivas direcciones de red.

Con este tipo de servicio de directorio, un usuario no tiene que recordar la dirección física de los diferentes recursos de la red, pues con saber simplemente su nombre estará accediendo a tal recurso demandado.

Cada recurso de la red se considera como un objeto en el servidor de directorio, donde la información de un recurso en particular se almacena como atributos de ese objeto.

La información que representa un objeto se establece de forma segura, accediendo a tales objetos usuarios con los permisos adecuados para poder manipular dicha información.

Servicios de directorio.

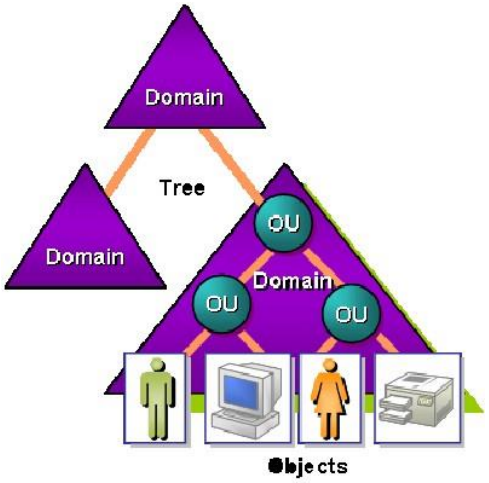


El proceso del diseño del directorio tiene normalmente un conjunto de las reglas que determinan cómo se nombran y se identifican los recursos de la red.

Las reglas especifican que los nombres sean únicos e inequívocos.

En X.500 (los estándares de servicio de directorio) y en LDAP el nombre se denomina distinguished name (DN) y se utiliza para referirse al nombre único de una entrada.

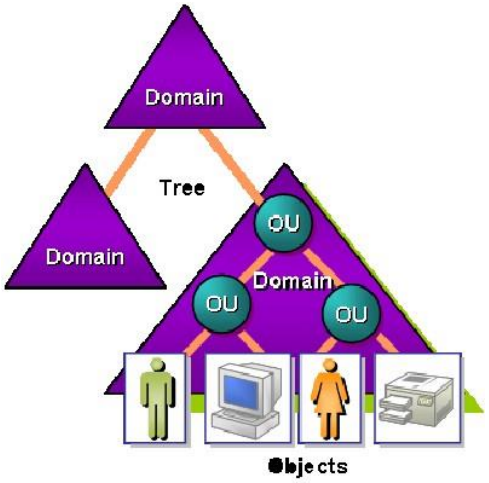
Servicios de directorio.



Un servicio del directorio es una infraestructura compartida de la información para localizar, manejar, administrar, y organizar los componentes y recursos comunes de una red, que pueden incluir:

Volúmenes
Carpetas
Archivos
Impresoras
Usuarios
Grupos
Dispositivos
Números de teléfono
Otros objetos.

Servicios de directorio. Protocolo X.500.

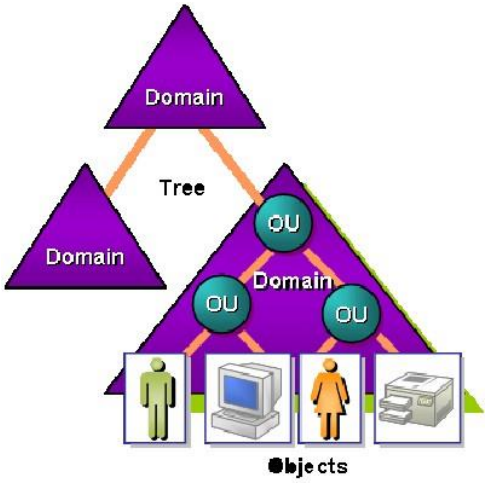


X.500 es un conjunto de estándares de redes de ordenadores de la ITU-T sobre servicios de directorio, entendidos estos como bases de datos de direcciones electrónicas (o de otros tipos).

El estándar se desarrolló conjuntamente con la ISO como parte del Modelo de interconexión de sistemas abiertos, para usarlo como soporte del correo electrónico X.400.

Los protocolos definidos por X.500 incluyen, protocolo de acceso al directorio (DAP), el protocolo de sistema de directorio, el protocolo de ocultación de información de directorio, y el protocolo de gestión de enlaces operativos de directorio.

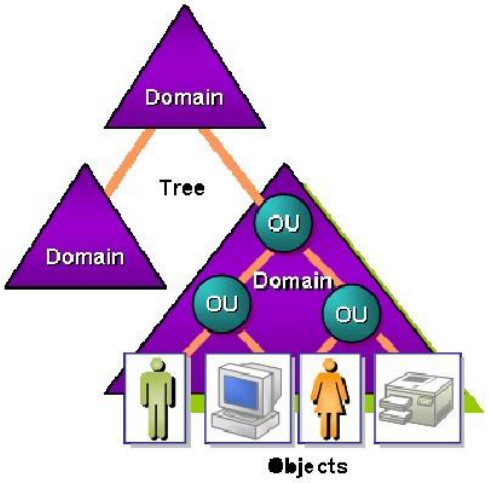
Servicios de directorio. Protocolo LDAP.



LDAP son las siglas de Lightweight Directory Access Protocol (en español Protocolo Ligero de Acceso a Directorios) que hacen referencia a un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.

LDAP también se considera una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas.

Servicios de directorio. Protocolo LDAP.

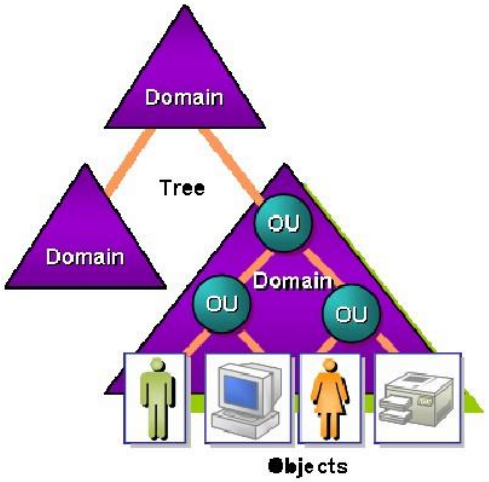


Habitualmente, almacena la información de autenticación (usuario y contraseña) y es utilizado para autenticarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc).

A manera de síntesis, LDAP es un protocolo de acceso unificado a un conjunto de información sobre una red.

La versión actual es LDAPv3, que está especificada en una serie de Internet Engineering Task Force (IETF) Standard Track Request for Comments (RFCs) como se detalla en el documento RFC 4510.

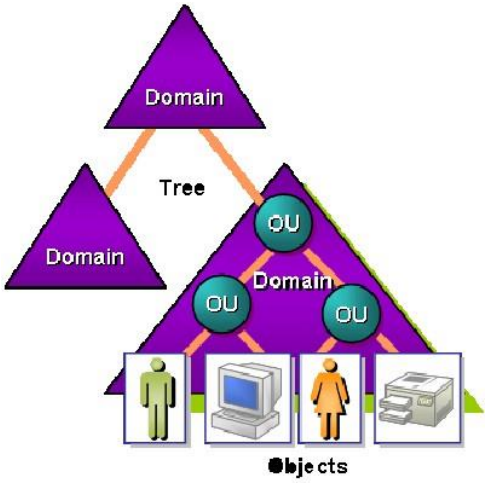
Servicios de directorio. Protocolo LDAP.



La comprensión de los requerimientos de directorios por parte de las compañías de telecomunicaciones estaba bien desarrollada después de 70 años de producir y manejar directorios de teléfonos.

Estas compañías introdujeron el concepto de servicios de directorio a Tecnologías de Información y Redes de Computadoras, que culminó en la especificación X.500 en la década de 1980.

Servicios de directorio. Protocolo LDAP.



Los servicios de directorio X.500 se accedían tradicionalmente vía DAP (Directory Access Protocol), que requería la pila de protocolos OSI (Open Systems Interconnection).

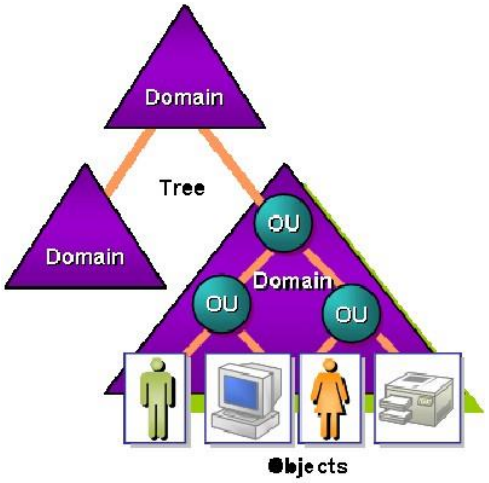
LDAP fue originalmente dirigido a ser un protocolo alternativo y ligero para acceder a servicios de directorio X.500 a través de la pila de protocolos más simple (y ahora más difundida) TCP/IP.

Pronto se implementaron servidores de directorio LDAP independientes, así como los servidores de directorio que soportaban DAP y LDAP.

El último se hizo popular en empresas debido a que eliminaba cualquier necesidad de desplegar una red OSI.

Ahora, los protocolos de directorio X.500 incluyendo DAP pueden ser usados directamente sobre TCP/IP.

Servicios de directorio. Protocolo LDAP.

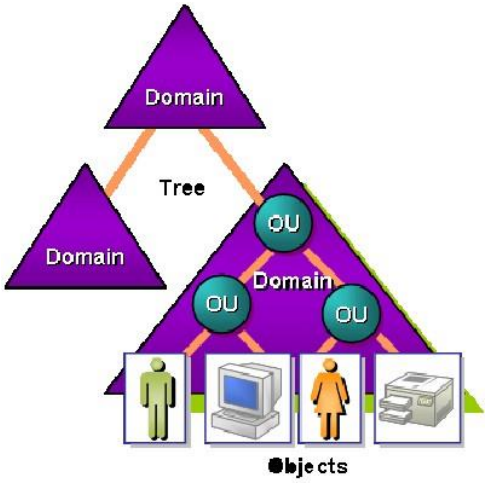


Un cliente inicia una sesión de LDAP conectándose a un servidor LDAP, por defecto en el puerto TCP 389.

El cliente luego envía una petición de operación al servidor, y el servidor envía respuestas.

Con algunas excepciones, el cliente no necesita esperar una respuesta antes de enviar la siguiente petición, y el servidor puede responder en cualquier orden.

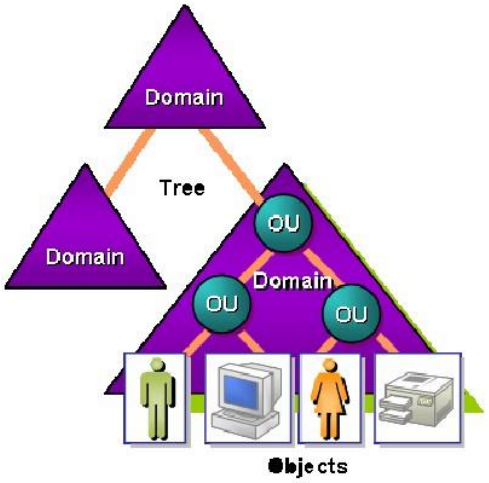
Servicios de directorio. Protocolo LDAP.



El cliente puede requerir las siguientes operaciones:

- Start TLS — usar la extensión Transport Layer Security (TLS) LDAPv3 para una conexión segura
- Bind — autenticarse y especificar una versión del protocolo LDAP
- Search — buscar y obtener entradas de directorio
- Compare — probar si una entrada nombrada contiene un valor de atributo dado
- Add — Añadir una nueva entrada
- Delete — Borrar una entrada
- Modify — Modificar una entrada
- Modify Distinguished Name (DN) — Modificar o renombrar una entrada
- Abandon — abortar una petición previa
- Extended Operation — operación genérica usada para definir otras operaciones
- Unbind — cerrar la conexión (no es el inverso de Bind)

Servicios de directorio. Protocolo LDAP.

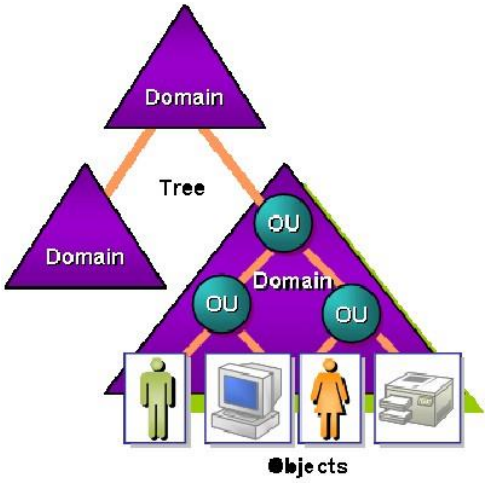


Estructura de directorio

Una entrada puede tener este aspecto cuando es representada en el formato LDAP Data Interchange Format (LDIF) (LDAP por sí mismo es un protocolo binario):

```
dn: cn=John Doe,dc=example,dc=com
cn: John Doe
givenName: John
sn: Doe
telephoneNumber: +1 888 555 6789
telephoneNumber: +1 888 555 1232
mail: john@example.com
manager: cn=Barbara Doe,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

Servicios de directorio. Active Directory.

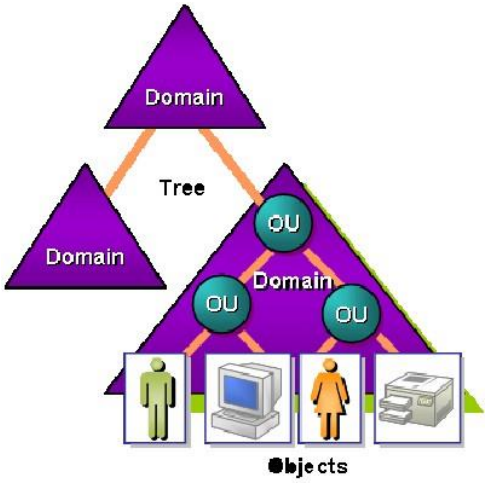


Active Directory (AD) es el término que usa Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores.

Utiliza distintos protocolos (principalmente LDAP, DNS, DHCP, Kerberos...).

Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso.

Servicios de directorio. Active Directory.

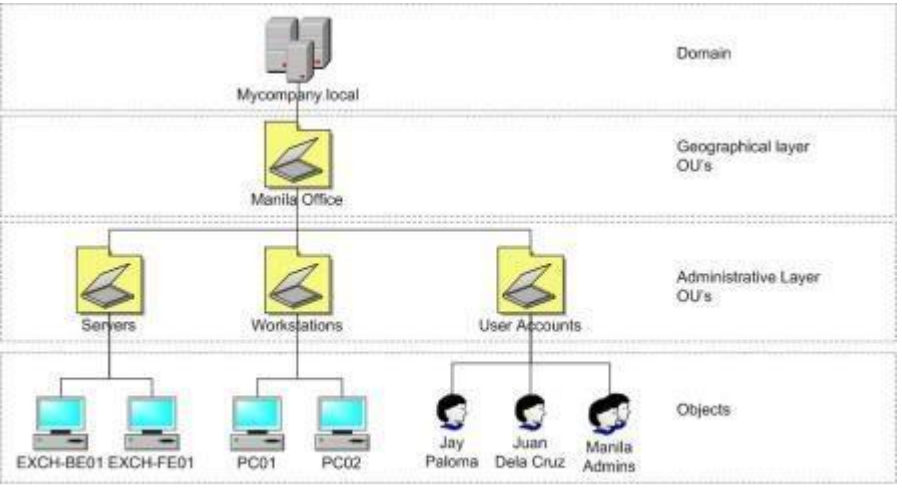


Active Directory permite a los administradores establecer políticas a nivel de empresa, desplegar programas en muchos ordenadores y aplicar actualizaciones críticas a una organización entera.

Un Active Directory almacena información de una organización en una base de datos central, organizada y accesible.

Pueden encontrarse desde directorios con cientos de objetos para una red pequeña hasta directorios con millones de objetos.

Servicios de directorio. Active Directory.

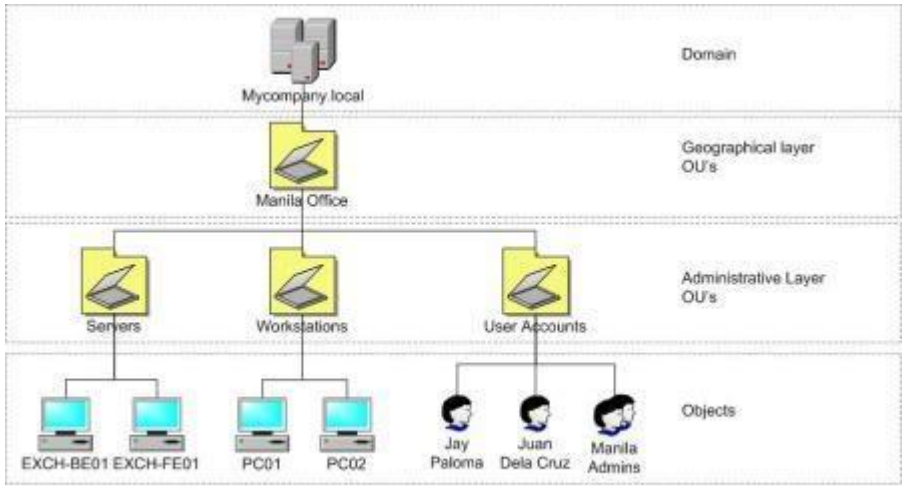


Organizational Units (OU's) are containers that provide the hierarchical mechanism for organizing objects within the domain. OU's can contain user, group and computer objects as well as other OU's

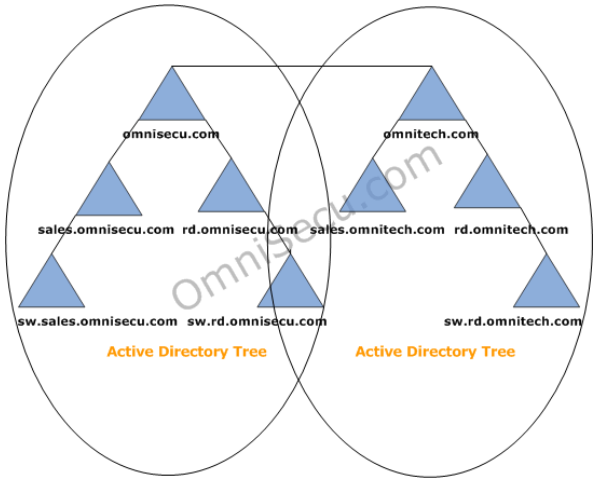
Active Directory está basado en una serie de estándares llamados X.500, aquí se encuentra una definición lógica a modo jerárquico.

Dominios y subdominios se identifican utilizando la misma notación de las zonas DNS, razón por la cual Active Directory requiere uno o más servidores DNS que permitan el direccionamiento de los elementos pertenecientes a la red, como por ejemplo el listado de equipos conectados; y los componentes lógicos de la red, como el listado de usuarios.

Servicios de directorio. Active Directory.



Organizational Units (OU's) are containers that provide the hierarchical mechanism for organizing objects within the domain. OU's can contain user, group and computer objects as well as other OU's

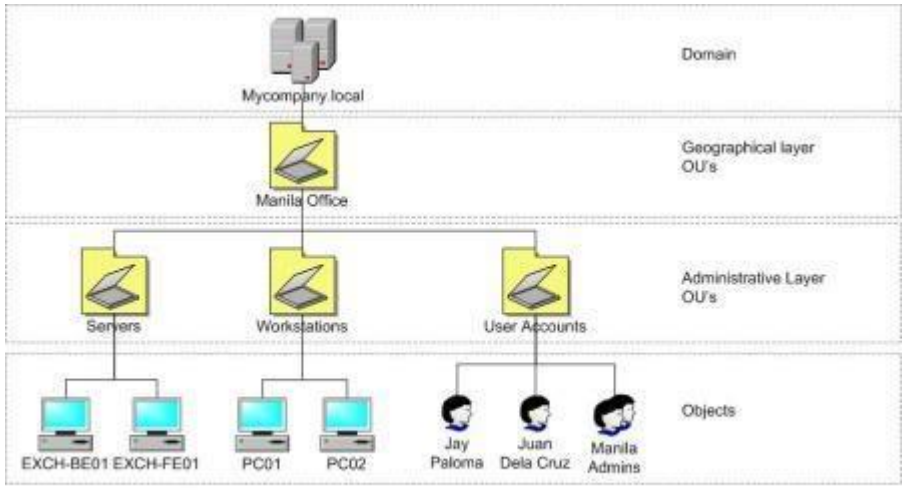


Un ejemplo de la estructura descendente (o herencia), es que si un usuario pertenece a un dominio, será reconocido en todo el árbol generado a partir de ese dominio, sin necesidad de pertenecer a cada uno de los subdominios.

A su vez, los árboles pueden integrarse en un espacio común denominado bosque (que por lo tanto no comparten el mismo nombre de zona DNS entre ellos) y establecer una relación de «trust» o confianza entre ellos.

De este modo los usuarios y recursos de los distintos árboles serán visibles entre ellos, manteniendo cada estructura de árbol el propio Active Directory.

Servicios de directorio. Active Directory.

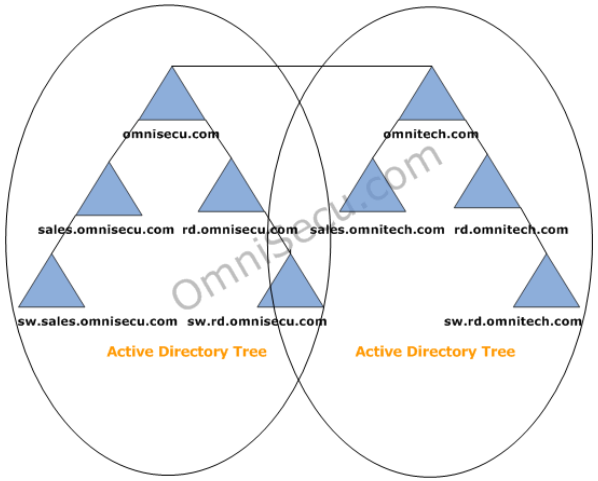


Organizational Units (OU's) are containers that provide the hierarchical mechanism for organizing objects within the domain. OU's can contain user, group and computer objects as well as other OU's

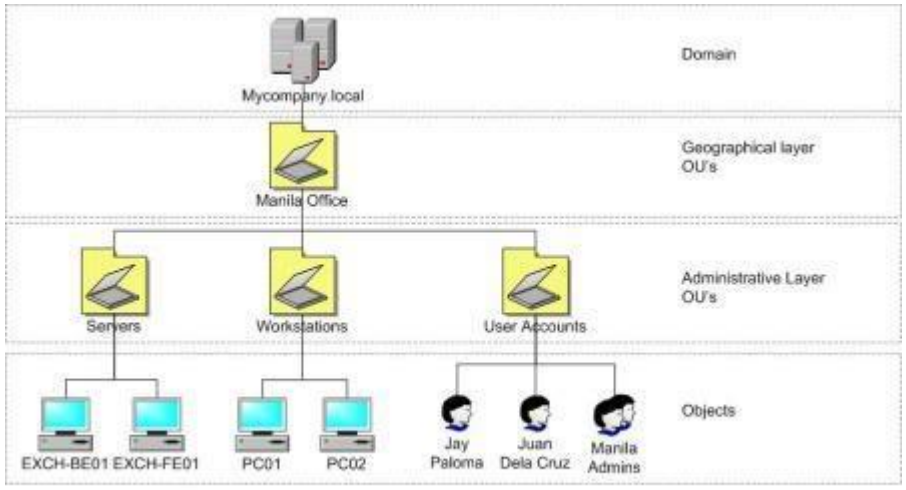
Active Directory se basa en una estructura jerárquica de objetos.

Los objetos se enmarcan en tres grandes categorías. — recursos (p.ej. impresoras), servicios (p.ej. correo electrónico), y usuarios (cuentas, o usuarios y grupos).

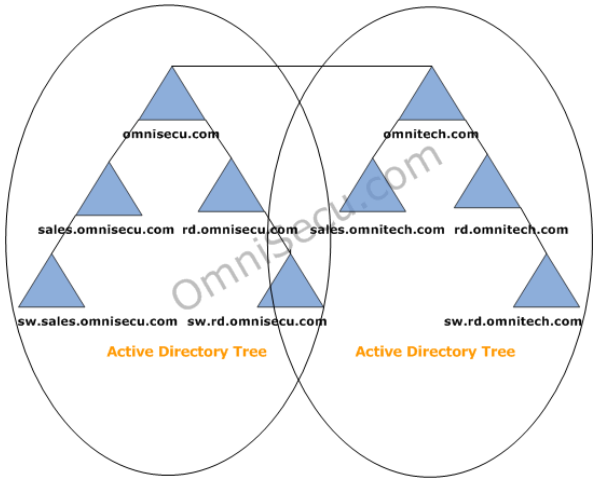
El AD proporciona información sobre los objetos, los organiza, controla el acceso y establece la seguridad.



Servicios de directorio. Active Directory.



Organizational Units (OU's) are containers that provide the hierarchical mechanism for organizing objects within the domain. OU's can contain user, group and computer objects as well as other OU's



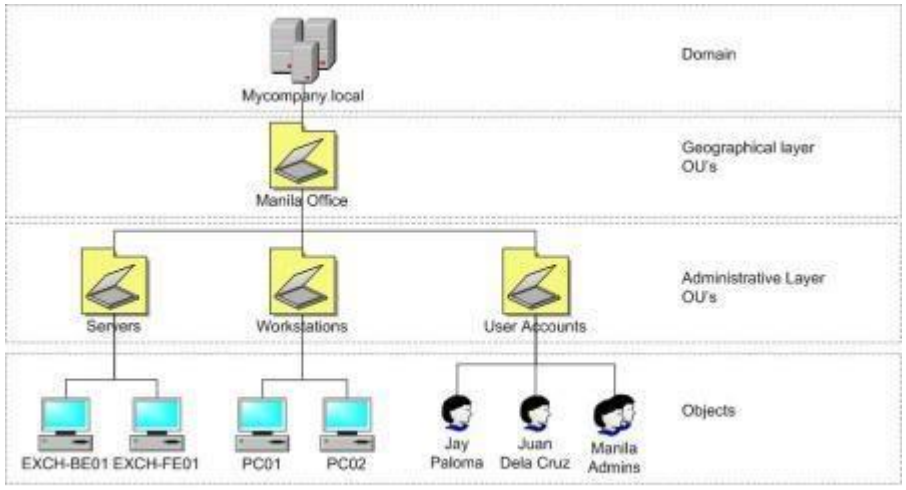
Cada objeto representa una entidad individual —ya sea un usuario, un equipo, una impresora, una aplicación o una fuente compartida de datos— y sus atributos.

Los objetos pueden contener otros objetos.

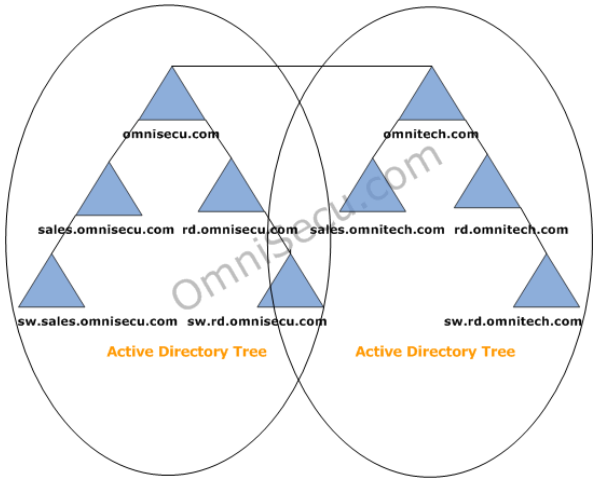
Un objeto está unívocamente identificado por su nombre y tiene un conjunto de atributos—las características e información que el objeto puede contener—definidos por y dependientes del tipo.

Los atributos, la estructura básica del objeto, se definen por un esquema, que también determina la clase de objetos que se pueden almacenar en el AD.

Servicios de directorio. Active Directory.



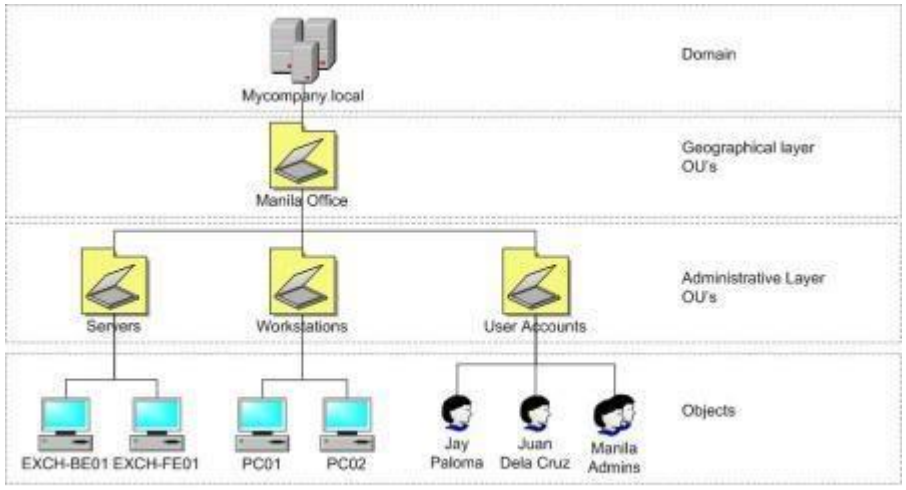
Organizational Units (OU's) are containers that provide the hierarchical mechanism for organizing objects within the domain. OU's can contain user, group and computer objects as well as other OU's



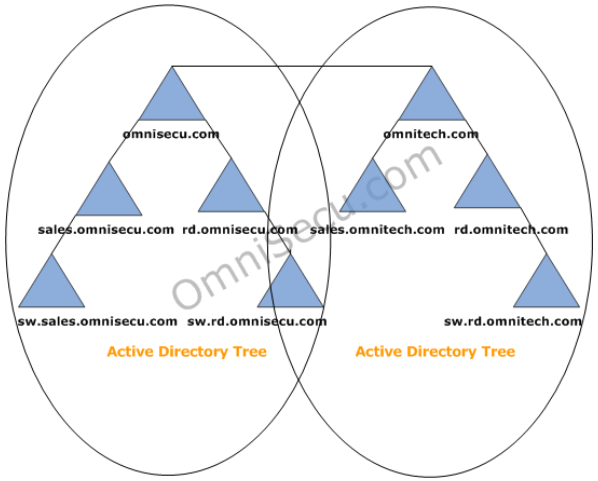
Su funcionamiento es similar a otras estructuras de LDAP (Lightweight Directory Access Protocol), ya que este protocolo viene implementado de forma similar a una base de datos, la cual almacena en forma centralizada toda la información relativa a un dominio de autenticación.

Una de sus ventajas es la sincronización presente entre los distintos servidores de autenticación de todo el dominio.

Servicios de directorio. Active Directory.



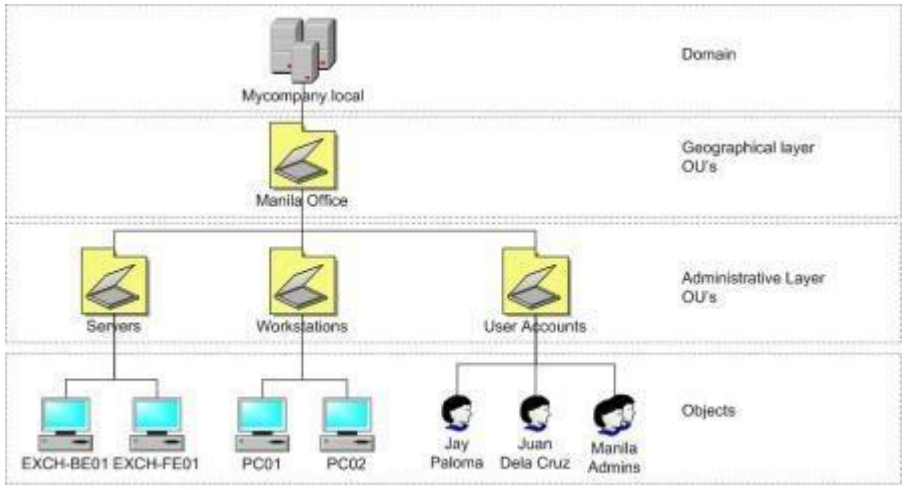
Organizational Units (OU's) are containers that provide the hierarchical mechanism for organizing objects within the domain. OU's can contain user, group and computer objects as well as other OU's



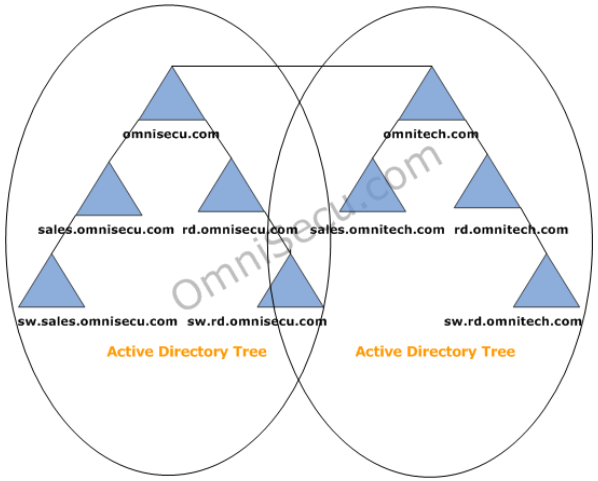
Cada uno de los objetos tendrá atributos que permiten identificarlos en modo unívoco (por ejemplo, los usuarios tendrán campo «nombre», campo «email», etcétera, las impresoras de red tendrán campo «nombre», campo «fabricante», campo «modelo», campo "usuarios que pueden acceder", etc).

Toda esta información queda almacenada en Active Directory replicándose de forma automática entre todos los servidores que controlan el acceso al dominio..

Servicios de directorio. Active Directory.



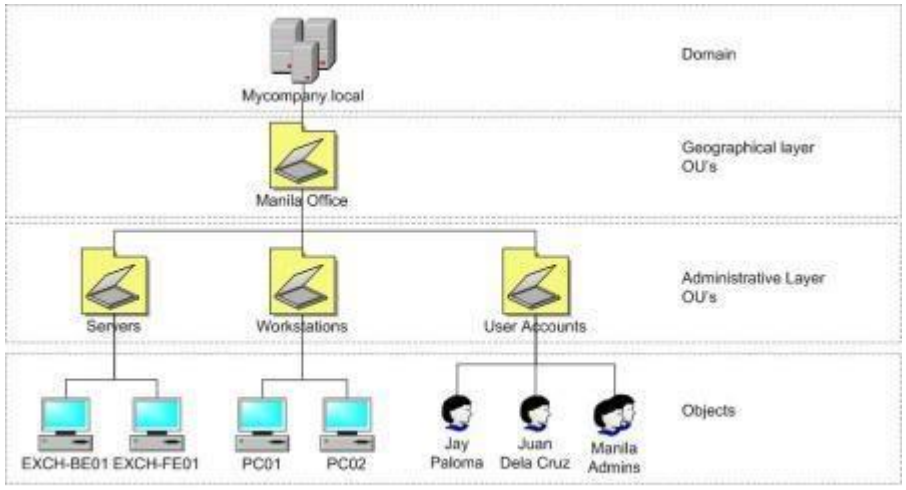
Organizational Units (OU's) are containers that provide the hierarchical mechanism for organizing objects within the domain. OU's can contain user, group and computer objects as well as other OU's



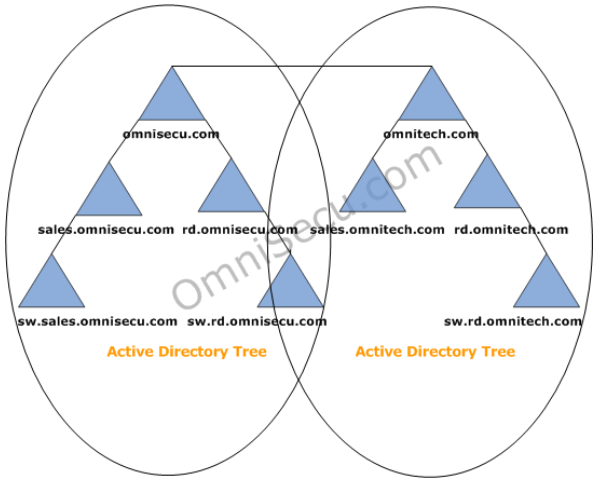
Es posible crear recursos (como carpetas compartidas, impresoras de red, etc) y conceder acceso a estos recursos a usuarios, con la ventaja que estando todos estos objetos memorizados en Active Directory, y siendo esta lista de objetos replicada a todo el dominio de administración, los eventuales cambios serán visibles en todo el ámbito.

Para decirlo en otras palabras, Active Directory es una implementación de servicio de directorio centralizado en una red distribuida que facilita el control, la administración y la consulta de todos los elementos lógicos de una red (como pueden ser usuarios, equipos y recursos).

Servicios de directorio. Active Directory.



Organizational Units (OU's) are containers that provide the hierarchical mechanism for organizing objects within the domain. OU's can contain user, group and computer objects as well as other OU's

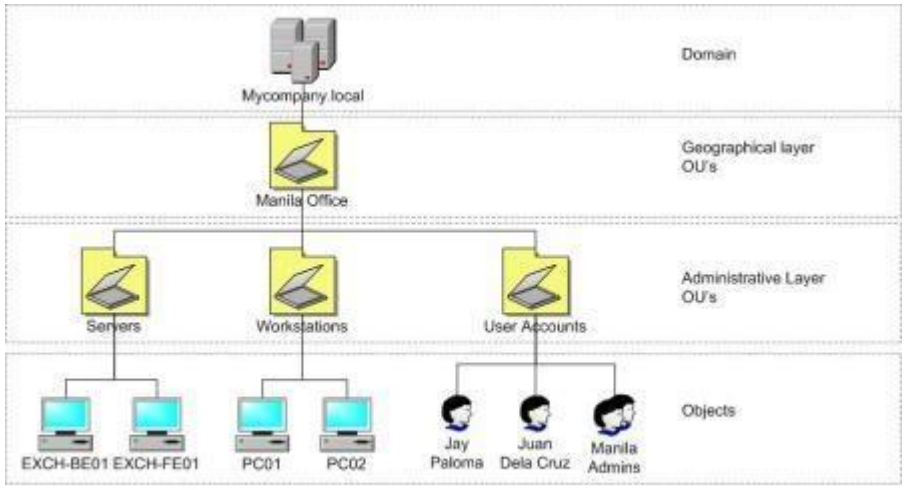


Para permitir que los usuarios de un dominio accedan a recursos de otro dominio, Active Directory usa una relación de confianza (en inglés, trust).

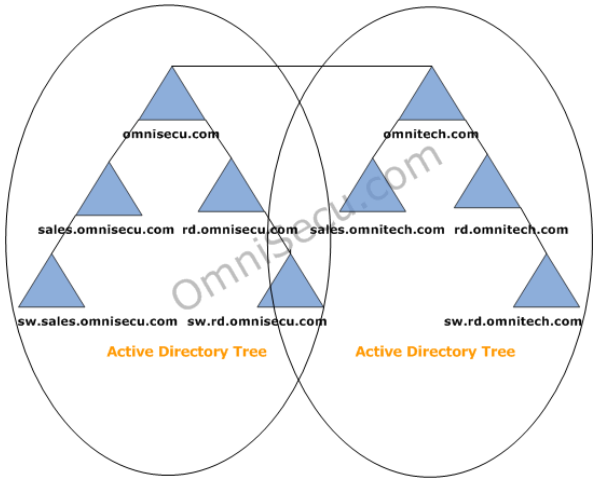
La relación de confianza es creada automáticamente cuando se crean nuevos dominios.

Active Directory usa el protocolo V5 de Kerberos, aunque también soporta NTLM y usuarios webs mediante autentificación SSL/TLS.

Servicios de directorio. Active Directory.



Organizational Units (OU's) are containers that provide the hierarchical mechanism for organizing objects within the domain. OU's can contain user, group and computer objects as well as other OU's



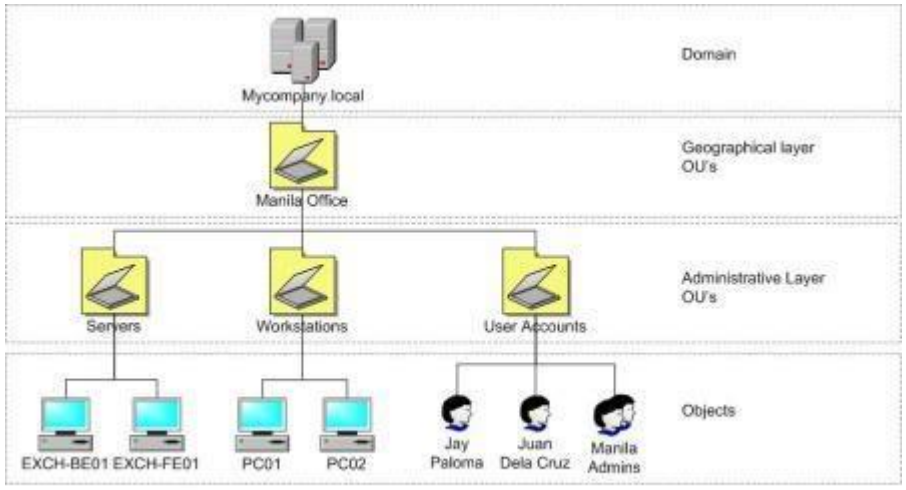
Los direccionamientos a recursos de Active Directory son estándares con la Convención Universal de Nombrado (UNC), Localizador Uniforme de Recursos (URL) y nombrado de LDAP.

Un Nombre Distinguido (DN) es una secuencia de nombres completos relativos (RDN) conectados por comas.

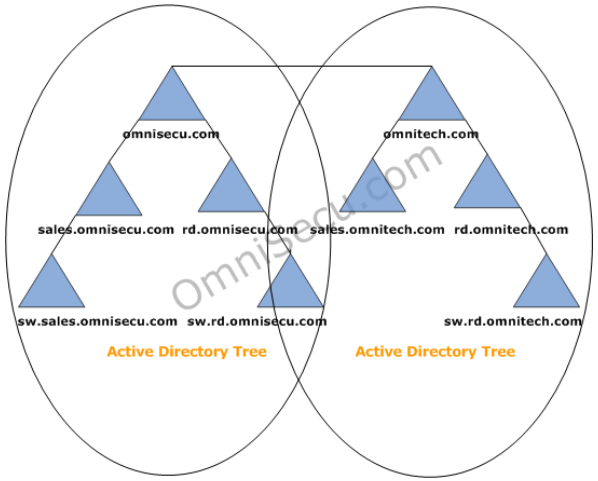
El RDN es un atributo con un valor asociado en la forma atributo = valor, normalmente expresada en un formato de cadena UTF-8.

CN = Jeff Smith, OU = Ventas, DC = Fabrikam, DC = COM

Servicios de directorio. Active Directory.

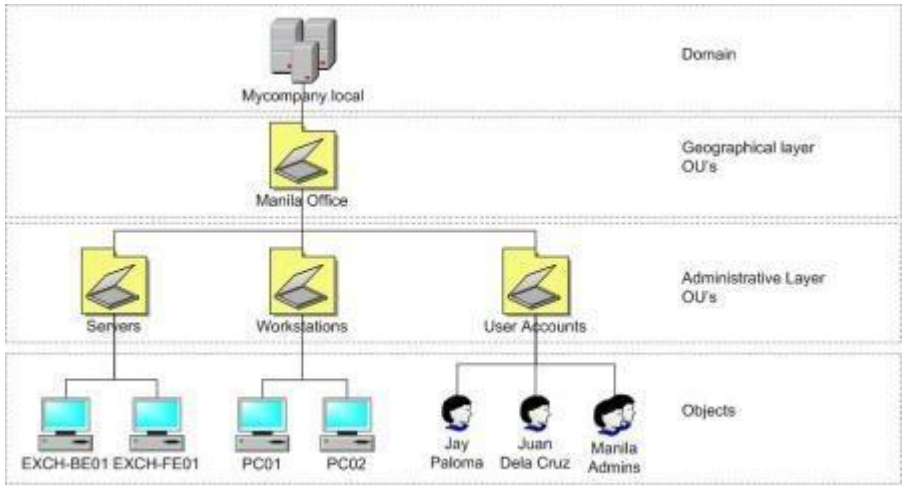


Organizational Units (OU's) are containers that provide the hierarchical mechanism for organizing objects within the domain. OU's can contain user, group and computer objects as well as other OU's

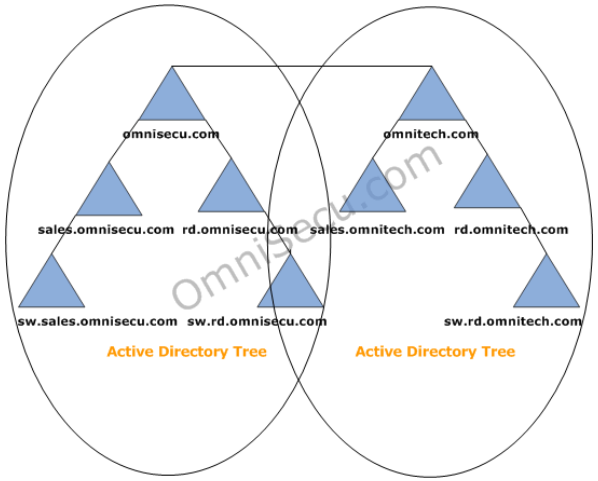


- DC domainComponent
- CN commonName
- OU organizationalUnitName
- O organizationName
- STREET streetAddress
- L localityName
- ST stateOrProvinceName
- C countryName
- UID userid

Servicios de directorio. Active Directory.



Organizational Units (OU's) are containers that provide the hierarchical mechanism for organizing objects within the domain. OU's can contain user, group and computer objects as well as other OU's



Una impresora llamada Imprime en una Unidad Organizativa (en inglés, Organizational Units, OU) llamada Ventas y un dominio foo.org, puede escribirse de las siguientes formas para ser direccionado:

En DN sería

CN=Imprime,OU=Ventas,DC=foo,DC=org, donde CN es el nombre común (en inglés, Common Name)

DC es clase de objeto de dominio (en inglés, Domain object Class).

En forma canónica sería foo.org/Ventas/Imprime