Active Directory. Servicios de Acceso Remoto

El servicio de Directorio Activo proporciona la estructura y las funciones para organizar, administrar y controlar el acceso a los recursos de red.

Un servicio de directorio almacena información sobre los recursos de la red y permite que los mismos resulten accesibles a los usuarios y a las aplicaciones.

Un Active Directory (o Directorio Activo, como prefirais) sirve para unir y identificar máquinas y usuarios dentro de la red, a los que se les proporciona ciertos parámetros de configuración y privilegios de manera centralizada desde un servidor. Se puede llegar a decir que, en parte, es una base de datos central con los equipos, usuarios y configuraciones. Y una herramienta muy útil para los Administradores de Sistemas.

Pongamos el caso que disponemos de 5 equipos basados en Microsoft Windows y a la vez, 5 usuarios que tienen que operar en estos equipos. Una solución es poner los 5 equipos en red con el mismo usuario de Administrador y la misma contraseña, a ser posible en blanco (no será la primera vez que lo vea) y que los usuarios cambien de un equipo a otro según las necesidades. Cuando se tiene que instalar o parametrizar una aplicación (las plantillas del Office, por ejemplo), hay que ir a cada equipo y aplicar la configuración correspondiente.

¿Que pasa cuando en lugar de 5 equipos tengo 25, o 50, 100, 250, 500, 1000, 5000… con sus correspondientes usuarios, o hasta incluso más usuarios que equipos (en el caso de lugares de trabajo a turnos)? ¿Y los parámetros que tengo que modificar no son 1 sino 200, 300, 500… para cada equipo y cada usuario?
O me vuelvo loco aplicando configuraciones y adelgazo 50 Kgs de golpe de tanto andar o busco una alternativa, el Active Directory.

Por otra parte, hay la seguridad y privacidad de la información. Es posible que en una red pequeña todos puedan tener acceso a todas partes, pero ¿estáis seguros? Sólo hay que pensar un poco la pregunta, a consciencia, para adivinar que no todo es o puede ser público. Y el cumplimiento de las leyes a las que estamos sujetos (el desconocimiento de la ley no implica su incumplimiento).

¿Os suena la LOPD y la LSSI? Por no decir otras normativas de seguridad específicas de cada sector. Esto, hace necesario aplicar ciertos niveles de seguridad a la información y identificar los usuarios del sistema para, además, poderlos desvincular de los equipos.

¿Desvincular el usuario del equipo? Un pequeño paréntesis para explicar de forma breve este concepto que trataré en una entrada posterior.
Para los que hace tiempo que estáis en informática, os sonará que antes era muy habitual que cada usuario tuviese SU equipo. Este se personalizaba con lo que necesitaba el usuario: aplicaciones, documentos, fondos de pantalla, configuraciones, etc… Si se estropeaba el equipo, el usuario asignado ya no podía trabajar porque todo estaba en aquel equipo. Pues bien, desvincular el usuario del equipo significa coger todo lo que es el usuario en el mundo digital (sus documentos y configuraciones) y ponerlo en un sitio central (servidor), haciendo que sea accesible desde cualquier equipo de la red, siempre y cuando pertenezca al mismo Active Directory. De esta manera, si al usuario se le estropea el equipo, sólo hay que sustituirlo por otro o desplazarse a un sitio de trabajo libre, identificarse como usuario y de manera transparente aparece su entorno de trabajo (documentos, fondos de pantalla, configuraciones, etc…; incluso se pueden hacer aparecer las aplicaciones que utiliza); pudiendo continuar su tarea. ¿Quien permite hacer esto? Pues el Active

Directory, desde la versión 2000 (Microsoft Windows Server 2000).

Funcionalidad

El Directorio Activo nos permite organizar, administrar y controlar el acceso a los recursos de red.

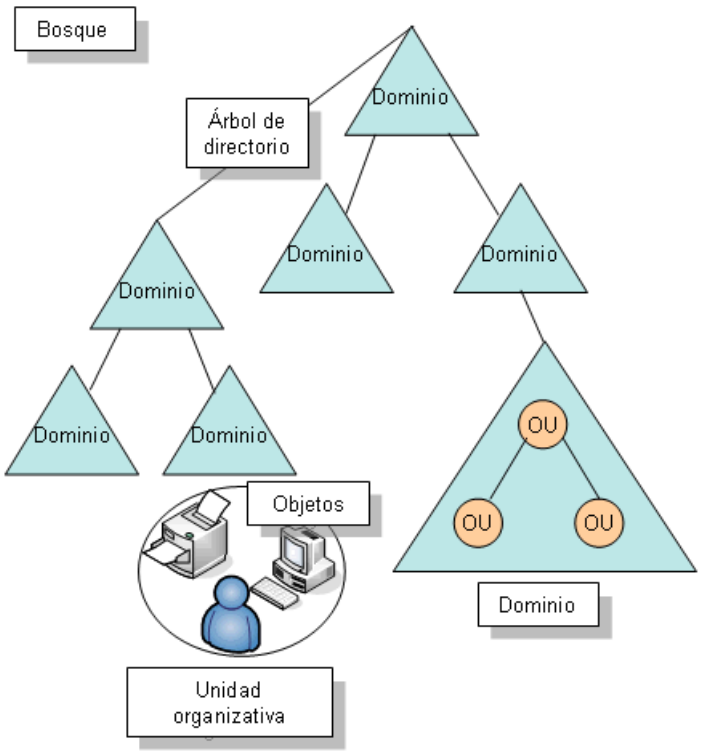
Por otro lado también hace que la topología física de red y los protocolos pasen desapercibidos por el usuario.

El Directorio Activo permite a los administradores controlar escritorios distribuidos, servicios de red y aplicaciones desde una ubicación central, al tiempo que utiliza una interfaz de administración coherente.

Podríamos decir que Active Directory es una tecnología, no un producto ni una aplicación concreta, sino que se utilizan diferentes aplicaciones para configurarlo según el apartado en que se quiere actuar. La implementación de un Active Directory requiere de un estudio y diseño previo según el ámbito donde se despliega. No es lo mismo desplegar un Active Directory en una red de 5 equipos situados en un único emplazamiento físico, que en una red de 50 equipos distribuidos en 5 sitios físicos o una red de 3000 equipos con diferentes departamentos y sitios físicos; por poner algún ejemplo. Ahora bien, a grosso modo, la configuración será la misma para la red de 5 equipos que para la de los 3000.

Estructura Lógica del Directorio Activo.

Los objetos de Active Directory representan usuarios y recursos, como por ejemplo, los ordenadores y las impresoras. A su vez algunos objetos pueden ser contenedores de otros objetos.



La estructura lógica de Active Directory incluye los siguientes componentes:

- Objetos: Son los componentes básicos de la estructura lógica.

- Clases de objetos: Son las plantillas para los tipos de objetos que se pueden crear en Active Directory.

- Unidades Organizativas:

  Emplearemos estos objetos para organizar otros objetos con propósitos administrativos. También podemos delegar el control para tener administradores de cada una de ellas.

  Se ubican dentro de cada dominio y son contenedores, carpetas, que contienen los equipos, usuarios, grupos de seguridad, distribución, etc… y donde se aplican políticas de configuración, delegaciones administrativas, etc… Por lo tanto, sirven para organizarnos como Administradores. Un buen diseño de las mismas permitirá una administración más ágil.

- Dominios:

  Están compuestos por colecciones de objetos administrativos que comparten base de datos común, políticas de seguridad y relaciones de confianza con otros dominios.

  Es un límite de replicación, forma parte del árbol y contiene las unidades organizativas, los equipos, usuarios, grupos de seguridad, grupos de distribución, etc… Es una parte más tangible, con la que más se trabaja. Como mínimo hay un dominio.

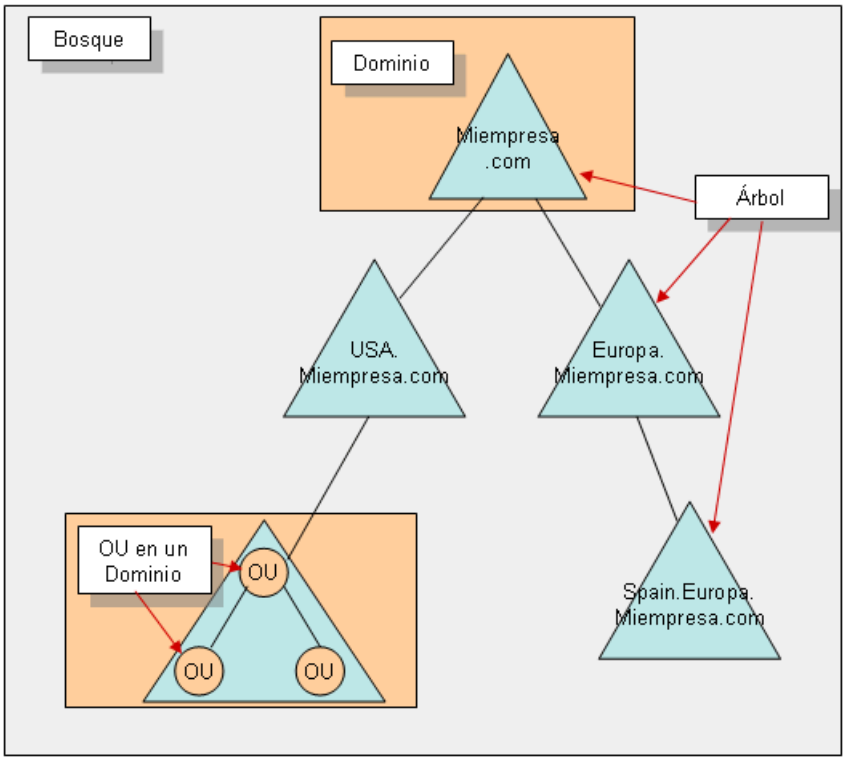
- Árbol de dominios:

  Son dominios agrupados en estructuras jerárquicas. Cuando se agrega un segundo dominio a un árbol, se convierte en hijo del dominio raíz. El dominio al cual un “dominio hijo” se une se llama”Dominio Padre”.

  Al igual que el bosque, es un concepto más que otra cosa. Un árbol contiene los dominios y se considera un árbol diferente cuando un dominio contiene dos subdominios por debajo. Como mínimo habrá un árbol, el principal, aunque quizás no se vea como tal.

- Bosque:
  Es una instancia completa del Directorio Activo y consta en uno o más árboles.

  Es un primer nivel del Active Directory y se considera el límite de seguridad. Equivaldría a una cosa parecida a la jurisdicción de la policía en una ciudad. Todo lo que contiene el bosque se puede administrar de manera centralizada y, por lo tanto, asignar permisos de seguridad de una manera o otra. Lo que queda fuera del bosque, es eso, está fuera del alcance de ser administrado.



Estructura física de Active Directory

- Controladores de dominio (DC): Son servidores ejecutando Windows Server y el software del Directorio Activo. Es el servidor que contiene y ofrece el servicio de Active Directory. Como mínimo hay uno por Active Directory y dominio.

- Servidor DNS: El Active Directory se sustenta en la resolución de nombres DNS, por lo tanto, es necesario disponer de este servicio en la red. Todos los equipos que pertenezcan al Active Directory deben tener configurado, como servidor DNS (en las propiedades TCP/IP de cada equipo), un servidor de la red que ofrezca esta resolución, normalmente se monta en el mismo servidor DC.

- Sitios del Directorio Activo: Agrupa recursos dentro de un bosque de acuerdo a su ubicación física o subred.

- Catálogo Global:

  Es un servidor DC que almacena una copìa de todos los objetos del Active Directory a nivel de bosque. En el catálogo global, se guarda una copia completa de todos los objetos del Active Directory para el dominio al que pertenece el servidor, y una copia parcial de todos los objetos, los atributos más buscados, del resto de dominios del bosque. Hace las funciones de buscar objetos, proporciona autenticación del nombre principal del usuario, pertenencia a grupos de seguridad universales en entornos de múltiples dominios y valida referencias a objetos dentro de un bosque.

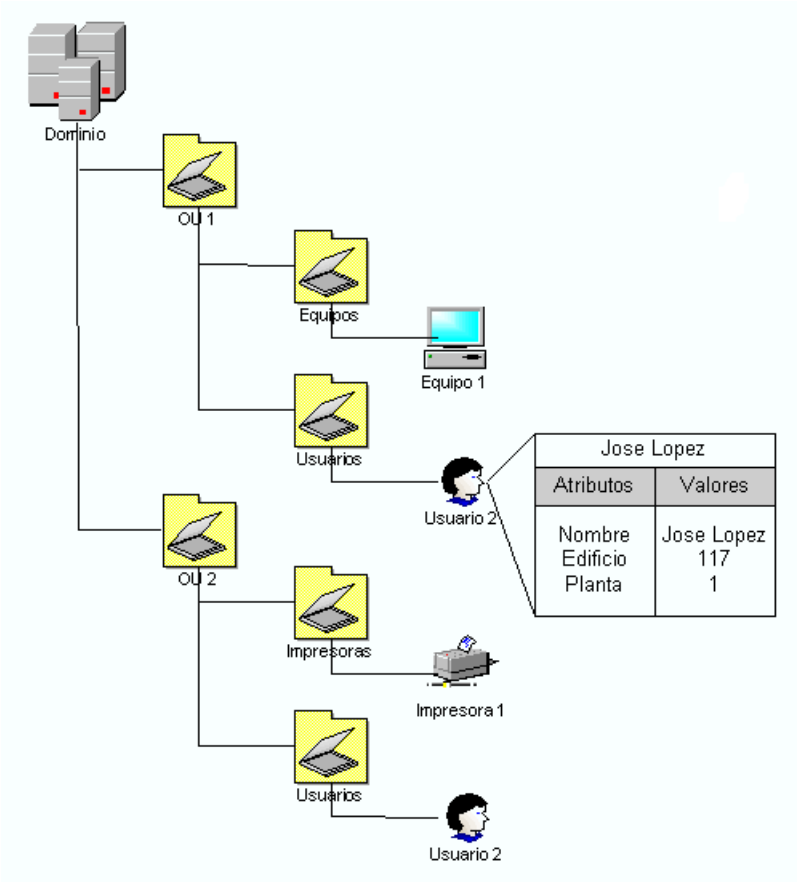
  Habilita a controladores de dominio de otros dominios del mismo bosque a localizar recursos de cualquier dominio. Por ejemplo, los usuarios que estén buscando recursos como ficheros, carpetas o impresoras de otro dominio lo harán en el catálogo global para así buscar no solo en su dominio sino en la base de datos completa.

- Particiones del Directorio Activo: Cada Controlador de dominio contiene las siguientes particiones:

    - Partición del dominio: Contiene la réplica de todos los objetos en ese dominio.
    - Partición de configuración: Contiene la topología del bosque.
    - Partición del esquema: Contiene el esquema del bosque.
    - Particiones de aplicaciones: contienen los objetos relacionados a la seguridad y se utilizan en las aplicaciones.

Servicios de directorio

Un servicio de directorio es un depósito estructurado de información sobre personas y recursos en una organización.



- Permite a usuarios y aplicaciones tener acceso a la información sobre objetos.
- Hace transparentes la topología y los protocolos físicos de la red.

Escritorio Remoto de sesión

Hoy en día, en muchos lugares de trabajo, el poder acceder a la información desde cualquier lugar y dispositivo, ha pasado de ser una anécdota a una necesidad. Cada vez más, los directivos de las empresas, la fuerza comercial, los técnicos, etc… piden poder acceder a la información estén donde estén. Sobre todo en entornos de pequeñas y medianas empresas (PYMES). Ya no se quiere, o se puede, estar atado a un lugar de trabajo fijo, que me obliga a esperar o desplazar para acceder a la

información que se necesita ya. El teletrabajo es una realidad en nuestras vidas.

Ahora bien, tenemos ciertas limitaciones. Las líneas de comunicación no tienen suficiente ancho de banda para ejecutar ciertas aplicaciones, que requieran de movimientos de datos. El cumplimiento de normativas internas o leyes sobre la protección de datos son suficientemente importantes para no permitir que los datos se distribuyan por cualquier lugar.

¿Como solucionamos la conexión remota a la información? En parte, desplazando el lugar de trabajo donde están los datos, básicamente donde están los servidores, en los centros de proceso de datos. Y en parte, haciendo que el usuario pueda visualizar y interactuar con estos datos de manera remota como si estuviera desplazado donde está el servidor.

El objetivo de Microsoft Remote Desktop, anteriormente conocido como Terminal Server, es disponer de un servidor, o varios según el número de usuarios y alta disponibilidad del entorno, con las aplicaciones que deben utilizar los usuarios. Éstos, mediante una aplicación cliente o navegador, se conectarán al servidor. Este le proporciona a cada usuario un escritorio entero (el entorno de toda la vida), o bien la aplicación concreta a la que tiene permiso para acceder.

Un concepto importante es que el usuario trabaja directamente en el servidor, los datos no viajan nunca directamente al equipo del usuario. El ancho de banda que se requiere para trabajar es mínimo al pasar sólo información sobre la posición del cursor, las teclas que se pulsan y el contenido gráfico de la pantalla (que sería lo que más pudiera consumir de ancho de banda).

Al separar el usuario de las aplicaciones implica otras limitaciones: reproducción multimedia, conexión de dispositivos varios, tarjetas de firma electrónica, escáneres, etc… que se deben tener en cuenta en estos despliegues.

Portal Web de Escritorio Remoto (RemoteApp)

Una de las características de este entorno es poder publicar directamente las aplicaciones mediante un portal web. Son las conocidas RemoteApp. Una manera más sencilla para los usuarios de poder acceder a las aplicaciones, sin realizar complicadas configuraciones en sus equipos.

Basta acceder a una dirección URL y seleccionar la aplicación que se quiere ejecutar o bien configurar el cliente de Windows para que actualice directamente estas aplicaciones en su menú de inicio. Pero detrás de este portal hay una configuración específica que hay que realizar.