1 Introdución aos Dominios

1.1 Sumario

- 1 Notas previas
  - 1.1 Grupos de Trabajo
  - 1.2 Dominios
- 2 Aspectos relacionados con la administración de dominios
  - 2.1 Estructura
  - 2.2 Disponibilidad
- 3 Labores de administración de dominios
  - 3.1 Infraestructura
  - 3.2 Usuarios y recursos
  - 3.3 Configuración
- 4 Dominios Microsoft. Active Directory

1.2 Notas previas

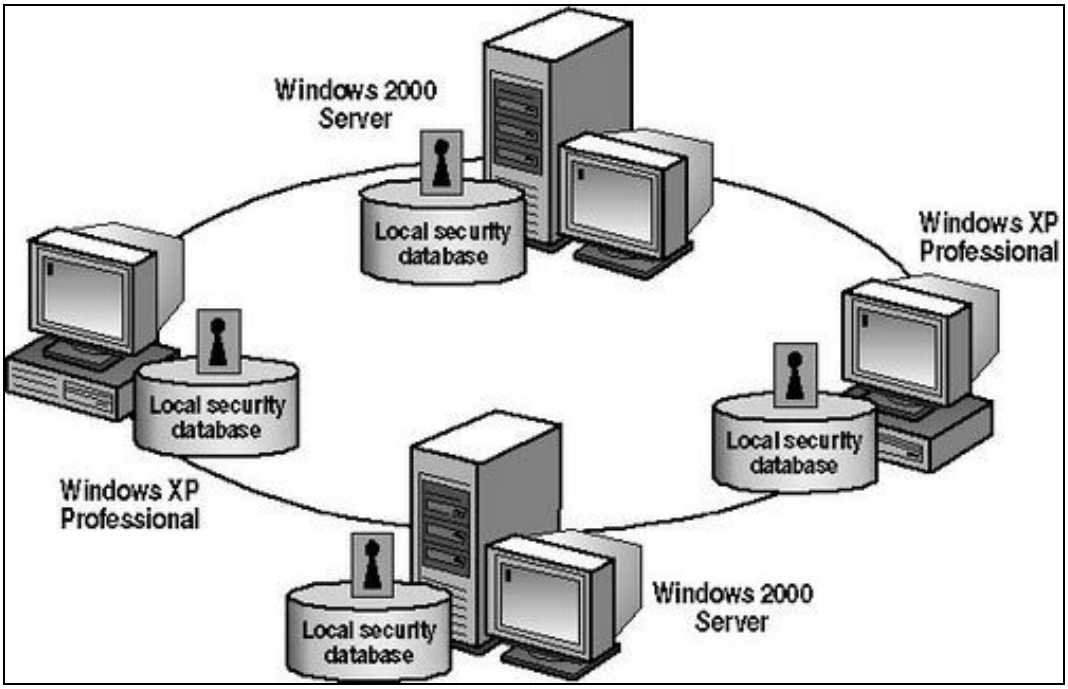
Tradicionalmente los sistemas en entorno de red han ido evolucionando desde un modelo de administración distribuido, basado en el concepto de Grupo de Trabajo, a un modelo de administración centralizado, basado en el concepto de Dominio.

1.2.1 Grupos de Trabajo

Un grupo de trabajo es una organización de los recursos de la red. Por recursos entenderemos todos aquellos elementos que puedan ser compartidos y utilizados en ese entorno. Por ejemplo, una impresora de red, un directorio compartido, un paquete de aplicación, etc.

El modelo de funcionamiento en los entornos de grupo de trabajo está basada en la compartición de recursos por las estaciones o hosts que constituyen la red. De este modo, **cada uno de los equipos o estaciones que comparte un recurso debe controlar el acceso al mismo**, de ahí viene que hablemos de un contexto de administración distribuido asociado a los grupos de trabajo.

Veamos el siguiente gráfico



En él podemos ver que cada estación gestiona las cuentas de usuario que controlan el acceso a los recursos que comparte. De modo que, si un cliente quiere acceder al recurso necesitará aportar una credencial de acceso reconocida localmente por el equipo.

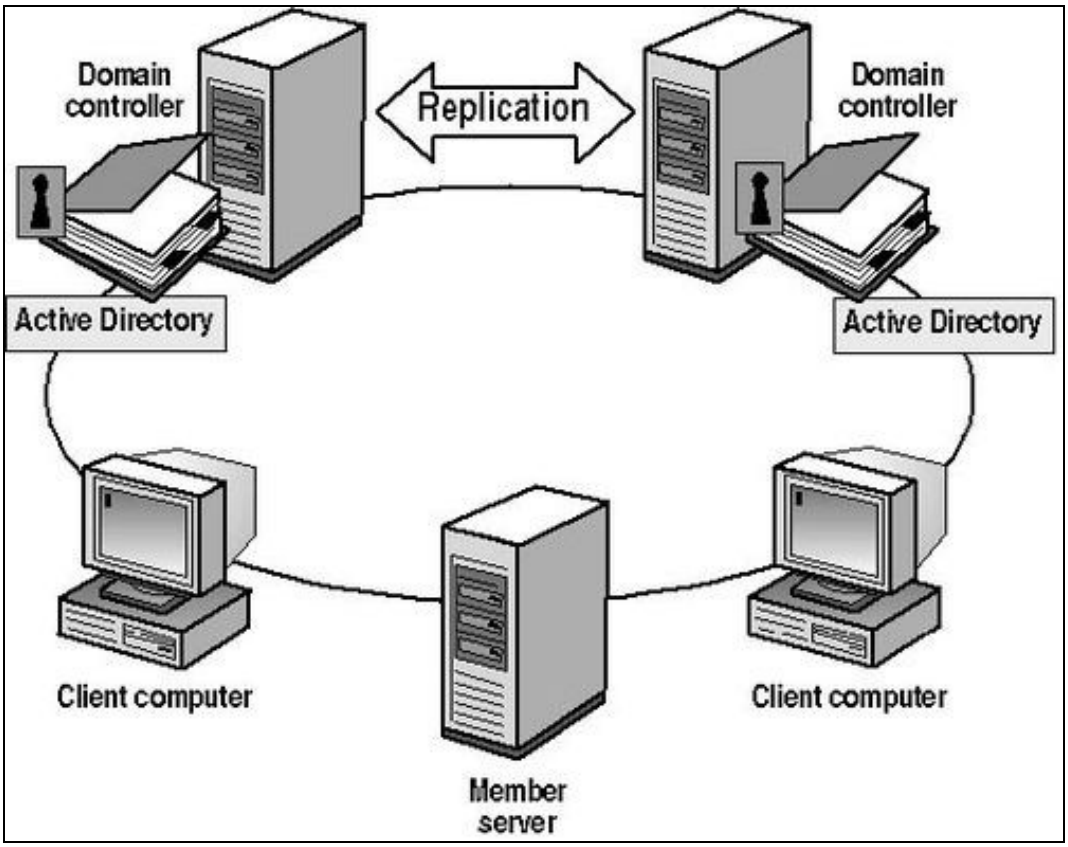
Este modelo dificulta la gestión cuando el número de estaciones crece. Pensad que un administrador de sistemas para poder controlar este entorno necesita conocer y documentar todos los usuarios de todos los equipos que comparten recursos en la red. Según esto, cualquier cliente de un recurso

compartido necesitará conocer todas las credenciales de acceso (usuario y password) de todos los recursos a los que accede en los distintos equipos de la red.

En conclusión, la administración de los recursos de una red basada en grupos de trabajo es poco eficiente y en la actualidad se muestra completamente obsoleta. En los procesos de instalación por defecto de los clientes de una red se presupone una configuración en grupo de trabajo. Por ejemplo, Windows incorpora por defecto las estaciones al grupo de trabajo WORKGROUP. El proceso de adhesión a estructuras de dominio debe de realizarse posteriormente a la instalación, o bien mediante herramientas de personalización de la instalación.

1.2.2 Dominios

La respuesta a las limitaciones de los entornos de red local basadas en grupos de trabajo viene de la mano del concepto de dominio. Un dominio es una estructura de gestión centralizada de recursos distribuidos en la red. Veamos el siguiente gráfico:



En el gráfico podemos ver como hay equipos, Controladores de Dominio (Domain Controllers, DCs), que son los que gestionan el acceso a los recursos compartidos por cualquier equipo de la red. Podemos ver en el gráfico 3 tipos de elementos:

- **Domain Controller** (DC): Controlador de Dominio. Equipo que almacena la base de datos de miembros del dominio, recursos compartidos, permisos de acceso y configuraciones. Al ser un servicio centralizado, que en los grupos de trabajo estaba distribuido entre todos los equipos de la red, suele ser necesario replicarlo para que, en caso de desastre o avería del DC, otro DC adicional pueda seguir realizando el trabajo de gestión de identidades y control de acceso a los recursos. Por ese motivo en el gráfico vemos 2 DCs. También se hace explícito el proceso de replicación de información entre los DCs que hace que ambos dispongan exactamente de la misma información del dominio.
- **Member Server**: Servidor Miembro. Equipos que comparten recursos en la red pero que no son DC. Pueden ser, por ejemplo, servidores de archivos, servidores web, servidores de correo, servidores de aplicaciones, servidores de seguridad, etc.
- **Client Computer**: Cliente. Equipos de los usuarios finales utilizados para trabajar en el entorno de red con los recursos compartidos en la misma

En los dominios se almacena información sobre múltiples aspectos. Las identidades de la red que se gestionan directamente son de 2 tipos, **máquinas** y **usuarios**. Por tanto, para poder trabajar en un entorno de dominio, es necesario que tanto el equipo desde el que se trabaja, como el usuario con el que se inicia sesión, sean identidades reconocidas y acreditadas por el dominio.

Una vez que se registran equipos y usuarios en el dominio, es el momento de realizar la configuración de seguridad en los permisos y acceso a los recursos de la red. Todo este trabajo se lleva a cabo con herramientas de administración dependientes de la tecnología con la que implementemos nuestro dominio.

En este curso veremos la implantación de dominios utilizando la tecnología de Microsoft Active Directory. Existen también implementaciones basadas en software libre de dominios, tanto en modalidad gratuita como comercial. En el ámbito de las libres gratuitas la más utilizada es Samba con soporte de credenciales de usuario gestionado mediante LDAP:

En conclusión, las ventajas que tienen los dominios sobre grupos de trabajo son las siguientes:

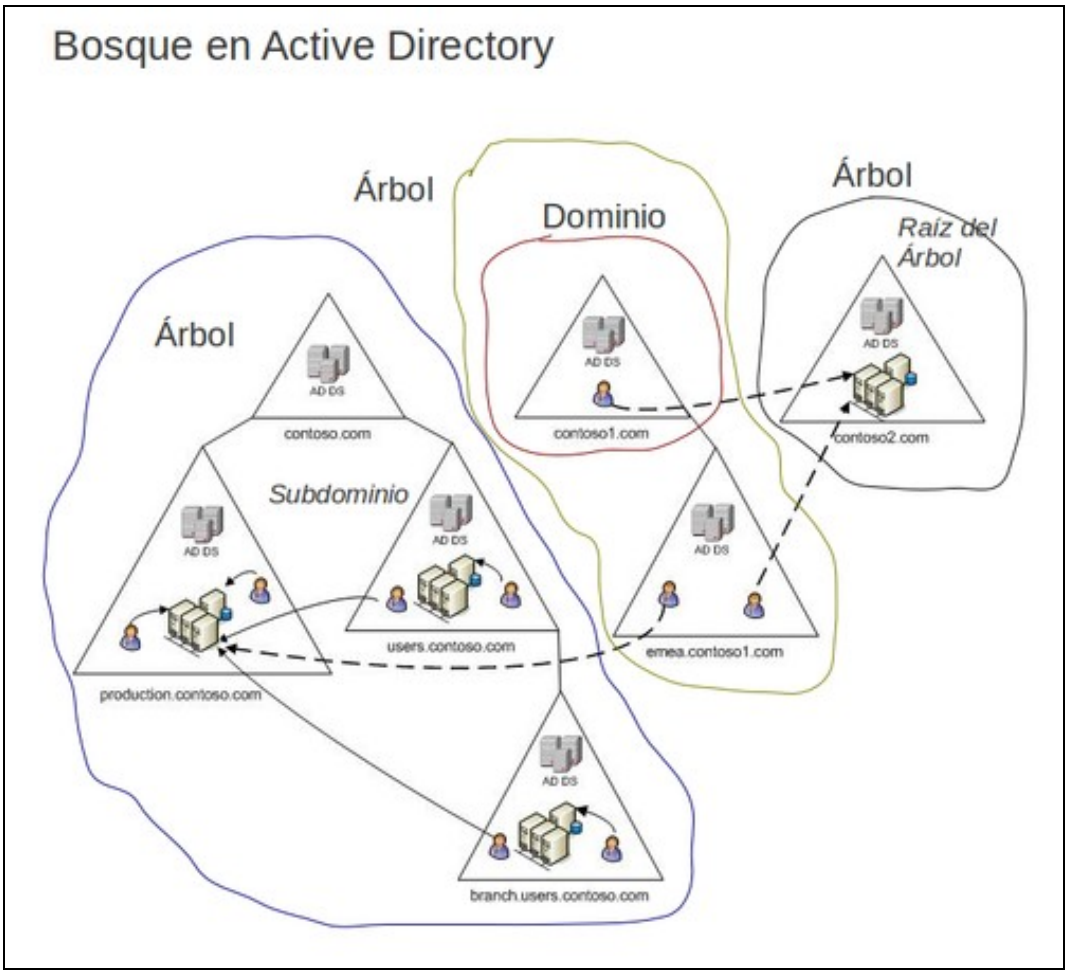
- Facilidad de administración
- Mayor seguridad
- Centralización de recursos
- Facilita las políticas de Copia de Seguridad
- Permite auditar y monitorizar recursos de la red
- Es escalable, es decir, permite aumentar los recursos con impacto limitado
- Soporta un gran número de máquinas y usuarios

1.3 Aspectos relacionados con la administración de dominios

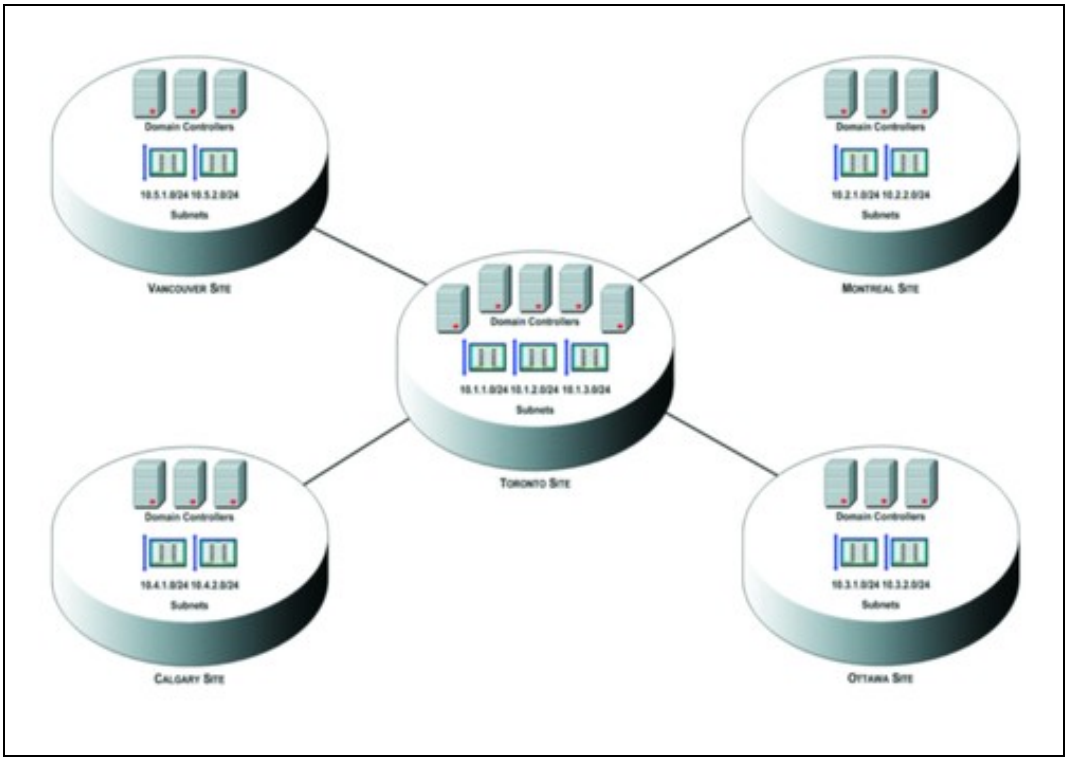
1.3.1 Estructura

A lo largo de esta unidad y de la siguiente veremos herramientas y protocolos relacionados con la gestión de una infraestructura de dominio. El contexto administrativo y tecnológico es amplio, sin embargo desde un punto de vista conceptual podemos identificar los siguientes aspectos relacionados

- **Estructuras lógicas del dominio**
  - Bosque
  - Árbol
  - Dominio
  - Subdominios
  - Unidades Organizativas



- **Estructuras físicas del dominio**
    - ♦ Sitios
    - ♦ Subredes



- **Miembros del dominio**
    - ♦ Equipos
    - ♦ Usuarios
- **Recursos gestionados**
    - ♦ Directorios compartidos
    - ♦ Impresoras
    - ♦ Servicios y aplicaciones
- **Políticas de administración**
    - ♦ Seguridad
    - ♦ Directivas de grupo

A modo de resumen, un dominio es un entorno de administración centralizada que permite gestionar recursos en la red. Esos recursos son distribuidos, es decir, cualquier miembro del dominio puede tenerlos en propiedad y compartirlos. Sin embargo, la gestión en sí de esos recursos se realiza de un modo centralizado y accesible, bajo las correspondientes políticas de acceso y seguridad establecidas.

Para dar soporte a estructuras empresariales complejas y crecientes, se dispone de una estructura organizativa de varios niveles. El elemento de mayor nivel es el **Bosque**, un Bosque es un conjunto de Árboles de dominio. Un **Árbol** es una estructura jerárquica de dominios relacionados entre sí, mediante el uso de un espacio de nombres común. El dominio es la estructura de administración independiente. Cada dominio mantiene su propia base de datos del dominio independiente de las demás. Ahora bien, es posible establecer vínculos, **relaciones de confianza**, entre dominios dentro de arboles o bosques diferentes. De este modo usuarios de un dominio pueden acceder a los recursos de otros dominios. Estas estructuras, Bosques, Árboles y Dominios, son conocidas como estructuras lógicas. Existen también estructuras física, más centradas en la ubicación real de los recursos y en la interconexión de red. Las estructuras físicas son los **Sitios**, es habitual que en una organización extensa un dominio pueda desplegarse en varios sitios, y las **Subredes**, en este caso concepto referido a las redes de infraestructura. Un Sitio abarca, por lo general, una o más Subredes.

Los miembros del dominio son de dos tipos, usuarios y equipos. Para que un miembro pueda trabajar en el dominio deberá tener asociada una identidad válida dentro del mismo. A través de la pertenencia de los miembros a grupos de seguridad se establecen las políticas de acceso y derechos sobre el uso de los recursos. Las labores de administración de la red, en lo relativo al comportamiento y autorizaciones de miembros del dominio (usuarios y máquinas), se establece mediante políticas administrativas denominadas **Directivas de Grupo**, las cuales se asocian a contextos de administración concretos correspondientes a las Estructuras lógicas del dominio.

1.3.2 Disponibilidad

Una característica central, en cualquier sistema en producción de tipo crítico, como aquellos que se encargan de aspectos de seguridad o de proporcionar los recursos básicos de trabajo en un entorno TIC, es la disponibilidad. Un sistema disponible es aquel que resulta accesible en cualquier lugar y momento previstos para su utilización. Al ser un dominio una estructura fundamental en el entorno de red, será un requisito imprescindible, el que se implanten medidas que proporcionen un entorno de trabajo de **Alta Disponibilidad**

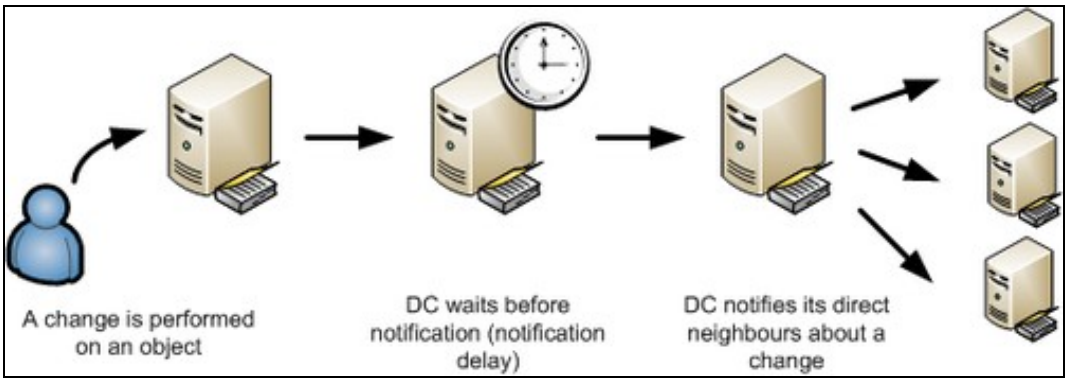
Términos como 24x7, el cual indica 24 horas, 7 días por semana, se refieren precisamente al aspecto de alta disponibilidad de un sistema. En la práctica ningún sistema está protegido contra el fallo técnico o humano, por tanto, para proporcionar este tipo de característica, necesitaremos recurrir a medidas de apoyo basadas en la redundancia de recursos. En general, un servicio en alta disponibilidad es aquel que en, caso de falla, dispone de un respaldo que pueda asumir sus funciones y carga de trabajo. Se utiliza, habitualmente, el término clúster para referirse al aspecto de redundancia, multiplicidad, de recursos del mismo tipo y que persiguen un mismo fin.

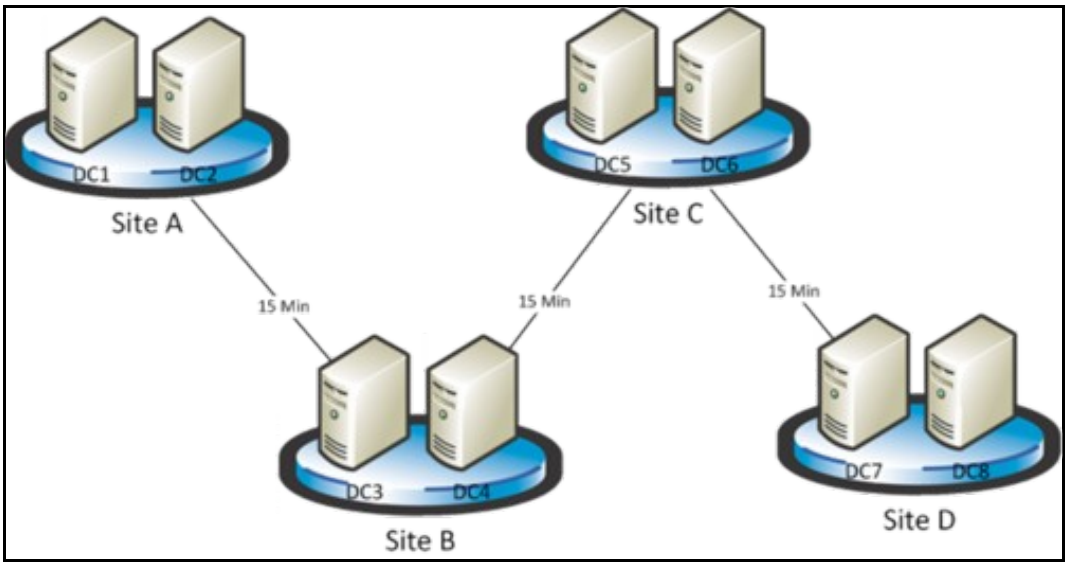
Como veremos, un DC, Controlador de Dominio, es un servidor que alberga la base de datos y datos de configuración y gestión de un dominio. Por tanto, será un candidato ideal para implantar un respaldo sobre él, es decir, en entornos de alta disponibilidad, todo DC estará redundado, para garantizar la prestación del servicio cuando otro DC falle.

En las últimas versiones de Windows Server, desde 2003 en adelante, se dispone de la característica de DC multimaestro, esto es, todos los DCs en la red son iguales, sin que prevalezca uno sobre otros. Anteriormente esto no era así, existiendo 2 roles clásicos, el **PDC (Primary Domain Controller)** y el **BDC (Backup Domain Controller)**. El primero, el PDC, se ocupaba en condiciones normales de autenticar los usuarios y realizar todas las labores relacionadas con las tareas de control de la información almacenada en el dominio. Los BDC estaban ahí como DCs de reserva, ante la posibilidad de un fallo del PDC, o bien para distribuir la carga de operaciones relacionadas con el dominio. Sin embargo, solamente el PDC podía actualizar la base de datos de configuración del directorio, es decir, los BDC operaban, en presencia del PDC, como DCs de solo lectura. Este aspecto suponía una limitación importante, pues cualquier modificación en los datos del directorio debían realizarse en el PDC, en un modelo de funcionamiento denominado de **maestro único**.

Los entornos **multimaestro** solucionan precisamente ese problema, permitiendo que convivan varios DC en la red que puedan modificar la base de datos del directorio, funcionando en modo colaborativo a efectos administrativos. Por tanto, en las últimas versiones de Windows Server desaparece la nomenclatura PDC, BDC, siendo todos los DC equivalentes en cuando a su capacidad y atribuciones. Sin embargo, es necesario hacer notar un aspecto importante. Aún en entornos multimaestro, hay ciertas funciones de control de dominio que solamente puede asumir un DC en la red. Estas funcionalidades se llaman **maestros de operaciones, FSMO, Flexible Single Master Operations** y representan roles únicos, a nivel de dominio o bosque, que solamente uno de los DC puede asumir. En caso de que un DC, que ejecuta un maestro de operaciones se caiga, otro DC de la red deberá asumir la correspondiente función de maestro de operaciones.

Cuando dispongamos de varios DC en la red, éstos deberán estar sincronizados y albergar datos lo más actuales posible, que reflejen el estado más reciente de configuración del dominio. Cuando se realiza alguna actualización de información del dominio, por ejemplo un cambio en una cuenta de un usuario, ésta será registrada en primer lugar por uno de los DCs, siendo propagada a continuación, y según una política preestablecida, a los demás DCs asociados al dominio. Este proceso se conoce como **replicación** y constituye uno de los aspectos de administración más importantes y críticos de un dominio.





En el primer gráfico vemos como se propaga una actualización a lo largo de los DCs del dominio.

En el segundo observamos una configuración multisitio, esto se puede dar, por ejemplo, cuando un domino abarque varias ubicaciones geográficas dispersas. En este caso los DCs se distribuyen asociados a los sitios a los que pertenecen. **Por ejemplo**, DCs del sitio de Madrid, DCs del sitio de Vigo, etc., todos ellos asociados al dominio de una misma empresa. A pesar de que están geográficamente dispersos, son DCs que sirven al mismo dominio y, por tanto, el proceso de replicación los abarca a todos ellos. Ahora bien, la frecuencia de actualización de DCs dentro del mismo sitio es mayor que la de DCs que pertenecen a sitios distintos. Esto es debido a que la conectividad de red en una LAN, dónde conviven los DCs en un sitio, es de un orden de magnitud mucho más elevado que la conectividad a través de una red pública, como Internet o una línea dedicada, que comunicaría a los DCs de sitios diferentes.

1.4 Labores de administración de dominios

A modo de esquema, a continuación, resumimos los aspectos relacionados con la administración de un dominio. En la unidad siguiente se detallarán todos estos aspectos.

1.4.1 Infraestructura

- Definición de estructura lógica
    - ♦ Bosques
- Árboles
- Definición de estructura física
    - ♦ Sitios
- Subredes
- Configuración de la replicación

1.4.2 Usuarios y recursos

- Definición de Usuarios y Grupos de Seguridad
- Definición de Permisos y Privilegios
- Definición de Directorios Compartidos
- Administración de Servicios y Aplicaciones

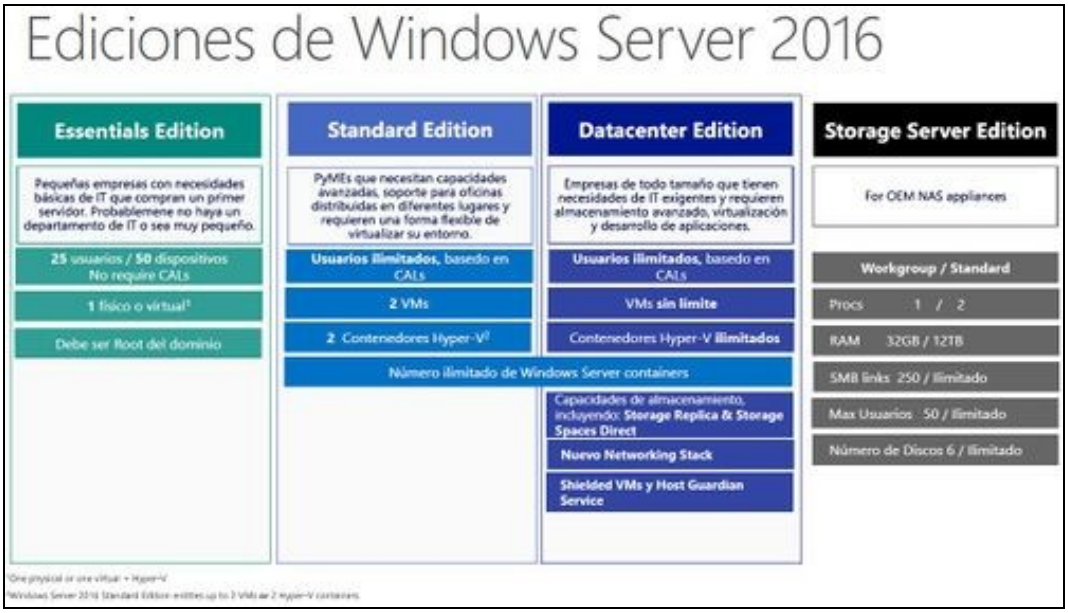
1.4.3 Configuración

- Administración de la Seguridad
- Administración de Directivas de Grupo
- Delegación
- Monitorización y Auditoría

1.5 Dominios Microsoft. Active Directory

Desde hace años Microsoft ha sido líder en el desarrollo de tecnologías para implantación de servicios de dominio en redes de pequeño, mediano y gran tamaño. Desde las primeras versiones de Windows NT Server, hasta las más recientes, Windows 2012, Microsoft ha ido evolucionando el modelo de dominio y sus funcionalidades y soporte de compatibilidad asociado. En la siguiente tabla podemos ver las principales características en función del versión de Windows Server

En las últimas versiones, se incorporan herramientas de gestión integral del dominio y de todos los recursos asociados. Existen varias versiones de Windows Server, las cuales difieren básicamente en el precio y en el uso máximo de recursos que pueden utilizar.



Volver

JavierFP 13:31 18 ene 2019 (CET)