ACTIVE DIRECTORY

Hecho por:

- Jorge Álvarez Cabado
- Clara Barrios Hermida
- Iván Cillero Seijas

WINDOWS ACTIVE DIRECTORY

¿Qué es?

Es un servicio de directorio de Windows Server. Consiste en una Base de Datos jerárquica y distribuida. Nos sirve para administrar, proteger y organizar los recursos de la red y del equipo como usuarios, archivos, grupos, etc. Por ejemplo, la base de datos puede contener una lista de 100 cuentas de usuario con detalles como el puesto de trabajo, el número de teléfono y la contraseña de cada persona. También registrará sus permisos. Básicamente es como un servidor AAA. En beneficio de otros servidores AAA, Active Directory es mucho más simplificado lo cual agiliza el trabajo para los administradores.

Estructuración

La estructura lógica se centra en la administración de los recursos de la red organizativa, independientemente de su ubicación física, y de la topología de las redes subyacentes.

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. Por tanto, la estructura lógica de Active Directory se compone de elementos intangibles como objetos, clases de objetos, unidades organizativas, dominios, árboles de dominios y bosques.

Objetos

Son los componentes básicos de la estructura lógica. Algunos objetos representan entidades individuales de la red que se denominan hoja y no pueden contener a otros objetos (por ejemplo, un usuario). Sin embargo, para simplificar la organización del directorio, se pueden colocar objetos hoja dentro de otros objetos denominados objetos contenedores. Los objetos contenedor también pueden contener otros contenedores de forma anidada, o jerárquica.

Clases de objetos

Son las plantillas o los modelos para los tipos de objetos que se pueden crear en Active Directory. Cada clase de objeto es definida por un grupo de atributos, los cuales definen los valores posibles que se pueden asociar a un objeto. Cada objeto tiene una combinación única de los valores de atributos.

Unidades organizativas

Es el tipo más común de objeto contenedor y se pueden utilizar para organizar otros objetos con propósitos administrativos, por ejemplo, dividir una empresa en

departamentos. Organizando éstos es más fácil localizar y administrar objetos. También es posible delegar la autoridad para administrar estas unidades organizativas de manera que haya administradores de cada una de ellas.

Dominios

Se usan para agrupar objetos relacionados con el fin de reflejar la red de una organización y comparten en una base de datos común del directorio, políticas de la seguridad y relaciones de confianza con otros dominios. Cada dominio que se crea almacena información acerca de los objetos que contiene. Los dominios proporcionan las tres funciones siguientes:

- Un límite administrativo para los objetos.
- Medios de administrar la seguridad para los recursos compartidos.
- Una unidad de réplica para los objetos.

En cada dominio tiene que haber como mínimo un controlador de dominio que son los encargados de almacenar los datos y de gestionar el dominio en sí. Aunque puede haber varios controladores de dominio dentro de un dominio, y correspondientemente un servicio de replicacion entre todos los controladores para que tengan la misma información actualizada. Pero hay tareas que solo puede realizar un controlador de dominio, que serían:

- Maestro de esquema: si se realiza un cambio en la base de datos solo un controlador se hace cargo y replica a los demas controladores, se hace para evitar que haya modificaciones simultaneas dando lugar a datos diferentes.

- Nomenclatura de dominio: cuando se crea un subdominio se va a hacer contra un dominio en concreto.

- Patrón de RID: genera los identificadores de recursos, por ejemplo para dar de alta un usuario se le va a asignar un ID, esto solo lo puede hacer un controlador ya que se podria generar el mismo ID simultaneamente para otro recurso.

- Emulador PDC: Sirve por ejemplo para la gestion de cambio de contraseñas, solo lo hace un controlador, ya que si se autentifican dos maquinas con el mismo usuario y cambian la contraseña crearia una inconsistencia.

- Maestro de infraestructuras: lleva la cuenta en la que se crean nuevos recursos en el dominio.

Para un administrador esto es transparente pero debe saber que controlador desempeña cada funcion por si alguno de estos cae y hay que hacer que otro desempeñe la funcion.

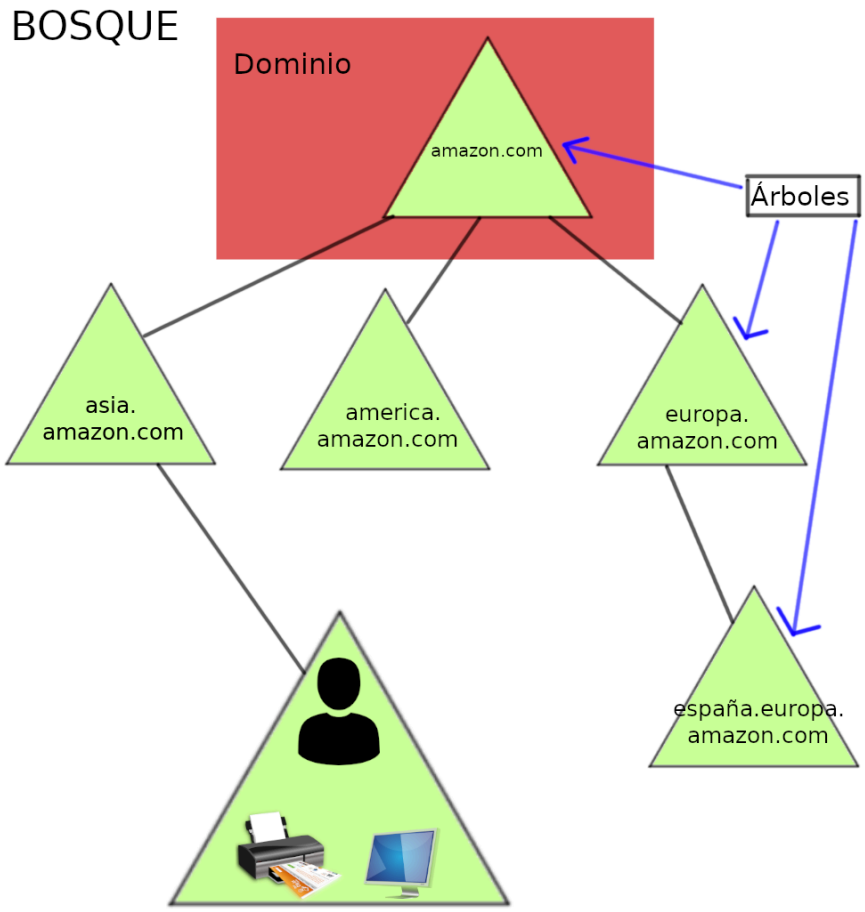
Árbol de dominios

Son dominios agrupados en estructuras jerárquicas que permiten el uso compartido de recursos globales. 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». El dominio hijo a su vez puede tener sus propios hijos, combinándose con el nombre de su padre para formar su propio y único nombre. Por ejemplo «ventas.miempresa.com» «ventas» sería un dominio hijo del principal «miempresa.com»

Bosque

Es una instancia completa del Directorio Activo. En el nivel más alto, pueden agruparse árboles dispares para formar un bosque. Un bosque permite combinar divisiones diferentes en una organización u organizaciones distintas. Éstas no tienen que compartir el mismo esquema de denominación y pueden operar de forma independiente y seguir comunicándose entre sí. Todos los árboles de un bosque comparten el mismo esquema, catálogo global y contenedor de configuración. Por defecto, la información en Active Directory se comparte solamente dentro del bosque. De esta manera, la seguridad del bosque estará contenida en una sola instancia de Active Directory. Así que la mayoría de las veces nuestra organización será de un sólo dominio (miempresa.com) dentro de un solo bosque.

Como conclusión a esta estructura, cabe decir que cuantos más Bosques, Árboles y Dominios se tengan, más complejo será administrarlo llegando a unos niveles de complejidad insoportables así que, se debe diseñar bien la estructura de red.



Funcionamiento

Primero destacar que Active Directory (AD) solo lo pueden usar los dispositivos con entornos de Microsoft. El principal servicio es el Active Directory Domain Services (AD DS). Los equipos que ejecutan AD DS son los controladores de dominio (DC). Lo normal en una empresa es tener varios DC y en todos ellos tener una copia de la BD para todo el dominio. Cualquier cambio, como actualizar una contraseña, se replica por todos los DC. En la BD se guarda una copia completa de sus objetos del dominio y una copia parcial de los objetos de los demas dominios. Esto permite a usuarios y aplicaciones encontrar objetos en cualquier dominio de su bosque.

Administración de objetos y sus propiedades en AD DS

Existen varias herramientas para administrar Active Directory:

- Centro de administración de Active Directory Permite crear y administrar tanto cuentas de usuario, grupo y equipo como unidades organizativas, conecta varios dominios dentro de una sola instancia del Centro de administración y administrarlo y crear y administrar directivas de contraseñas.

- Windows Admin Center Consola basada en Web que se puede utilizar para administrar equipos de servidor y equipos que ejecutan Windows 10

- Herramientas de administración remota del servidor (RSAT) Colección de herramientas que permite administrar roles y características de Windows Server de manera remota.
 - Módulo de Active Directory para Windows PowerShell Permite la administración de AD DS y es uno de los componentes de administración más importantes.

INFRAESTRUCTURA DE RED

Servicios de red

DHCP

DHCP es una norma del Grupo de trabajo en ingeniería de Internet (IETF) diseñada para reducir la carga administrativa y la complejidad de configurar hosts en una red. Al usar el servicio del servidor DHCP, el proceso de configuración de TCP/IP en clientes DHCP es automático.

Además de darle a cada cliente una IP, DHCP puede dar mucha más información, que se pueden ser configurables en cuatro niveles:

- Nivel de servidor: Es el más amplio, y afecta a todos los clientes del Active Directory

- Nivel de ámbito: Afecta a todos los clientes de una subred. Es la más habitual

- Nivel de clase: Afecta a todos los clientes de una clase (p.ej. a todas las impresoras)

- Nivel de cliente: Afecta a un cliente en particular

WINDOWS SERVER nos garantiza la disponibilidad de DHCP mediante:

- Clústeres de servidores: consiste en configurar el rol de DHCP en un clúster en vez de en un único servidor, así si por algún problema un servidor falla otro asume la responsabilidad.
- DHCP Failover: Consiste en dos servidores que se comunican entre ellos de manera coordinada para dar el servicio. Ambos tienen exactamente la misma configuración. Pueden configurarse en “activo-pasivo” -> si el servidor activo no está disponible, es cuando el servidor pasivo empieza a emitir respuestas. La otra forma es “load-balancín” ambos servidores se van alterando para emitir las respuestas.

- Implementación de ámbitos divididos: Dos servidores DHCP activos que se reparten el rango de direcciones. Es la configuración más fácil, pero también la menos eficiente. (doble tráfico broadcast)

DNS

Domain Name System (DNS) es un protocolo para traducir nombres de dominio a direcciones IP. Es un servicio básico para el correcto funcionamiento de cualquier red, domestica o corporativa. En una red de Active Directory, los registros DNS se pueden almacenar en un archivo .zone o en la Base de Datos de Active Directory Domain Services (lo más habitual).

DNS es un rol de servidor que se puede instalar mediante comandos Administrador del servidor o Windows PowerShell. Si va a instalar un nuevo bosque y dominio de Active Directory, DNS se instala automáticamente con Active Directory. Cuando se realiza cualquiera de las operaciones principales de Active Directory, como la autenticación, la actualización o la búsqueda, los equipos usan DNS para buscar controladores de dominio de Active Directory. Además, los controladores de dominio usan DNS para localizarse entre sí.

IPAM

IPAM (IP Address Management) es una característica integrada en Windows Server que permite descubrir, supervisar y auditar un grupo de direcciones IP.

Los servidores IPAM se integran en Active Directory Domain, pueden detectar automáticamente servidores de infraestructura de direcciones IP (DHCP) y servidores de sistema de nombres de dominio (DNS) en su red y le permite administrarlos desde una interfaz central. Después de esto se conecta a los servidores y descarga toda la información de direccionamiento y nos la muestra en un panel de control, desde el cual podemos gestionar la red.

RADIUS

RADIUS (del inglés Remote Access Dial In User Service) Es un protocolo de autenticación y autorización para el acceso a la red. Radius es un mecanismo de autenticación simple y antiguo mientras que active directory ofrece un par de mecanismos de autenticación más complejos.

Radius se suele usar cuando tenemos un dispositivo para configurar que desea realizar una autenticación simple y fácil, y ese dispositivo aún no es miembro del

dominio de Active Directory (Enrutadores en los que los administradores de su red desean iniciar sesión sin configurar la misma cuenta en todos y cada uno de los lugares).

Un combo muy común es la autenticación de dos factores con contraseñas de un solo uso (OTP) sobre RADIUS combinado con AD. Algo así como RSA SecurID , por ejemplo, que principalmente procesa solicitudes a través de RADIUS. Y sí, los dos factores están pensados para aumentar la seguridad

WINDOWS GROUP POLICITY

¿Qué es?

La directiva de grupo es una función de Windows que le permite controlar las operaciones de cuentas, aplicaciones y el propio Windows.

Por sí solo, una configuración en la Política de grupo solo se aplica a una sola computadora. Puede configurar una configuración completa, pero no tiene un montón de uso por sí solo. Así, la directiva de grupo se combina con Active Directory en la configuración empresarial.

¿Qué es GPO?

La política de grupo es un conjunto de políticas, llamadas objeto de política grupal (GPO), que se puede aplicar a todo el domino o a determinadas unidades organizativas múltiples Gpo. Una empresa puede configurar múltiples GPO para diferentes tipos de usuarios. El grupo estándar podría bloquear las cuentas de usuario de Windows para no permitir cuentas por defecto sin políticas de grupo.

Planificación de la implementación de GPO

Se puede controlar qué GPO se aplican a dispositivos de Active Directory en una combinación de tres maneras:

- Jerarquía de unidades organizativas de Active Directory. Esto implica vincular el GPO a una OU específica en la jerarquía de unidad organizativa de Active Directory. Todos los dispositivos de la OU y sus contenedores subordinados reciben y aplican el GPO. El control de la aplicación de GPO mediante la vinculación a las unidades organizativas suele usarse cuando se puede organizar la jerarquía de la unidad organizativa de acuerdo con los requisitos de la zona de aislamiento de dominio. Los GPO pueden aplicar la configuración a los dispositivos en función de su ubicación en Active Directory. Si un dispositivo se mueve de una OU a otra, la directiva

vinculada a la segunda OU finalmente tendrá efecto cuando la directiva de grupo detecte el cambio durante el sondeo.

- Filtrado de grupos de seguridad. Esto implica vincular los GPO al nivel de dominio (u otra OU principal) de la jerarquía de la UNIDAD organizativa y, a continuación, seleccionar qué dispositivos reciben el GPO mediante permisos que solo permiten que los miembros del grupo correctos apliquen el GPO. Los filtros de grupo de seguridad se adjuntan a los propios GPO. Se agrega un grupo al filtro de grupo de seguridad del GPO en Active Directory y, a continuación, se le asignan permisos de lectura y aplicación de directiva de grupo. A otros grupos se les puede denegar explícitamente los permisos leer y aplicar directivas de grupo. Solo aquellos dispositivos cuya pertenencia a grupos se conceden permisos de lectura y aplicación de directiva de grupo sin ningún permiso de denegación explícito pueden aplicar el GPO.
- Filtrado WMI. Un filtro WMI es una consulta que se ejecuta dinámicamente cuando se evalúa el GPO. Si un dispositivo es miembro del conjunto de resultados cuando se ejecuta la consulta de filtro WMI, el GPO se aplica al dispositivo. Un filtro WMI consta de una o más condiciones que se evalúan en el dispositivo local. Puedes comprobar casi cualquier característica del dispositivo, su sistema operativo y sus programas instalados. Si todas las condiciones especificadas son verdaderas para el dispositivo, se aplica el GPO; de lo contrario, se omite el GPO.

Biografia

Documentación de Microsoft – Uso de dominios

Documentación de Microsoft - Grupos de seguridad