WINDOWS DOMAIN SERVICES

Administración de Sistemas Operativos 2020/21

Grupo CTP

Carlos Torres Paz
Alonso Rodríguez Iglesias
Ignacio Borregán Naya
Ismael Verde Costas
Daniel Feito Pin
José Ángel Álvarez Sánchez

Índice

Active Directory Domain Services

Introducción a AD DS

Definición de AD DS

¿Qué es AD DS?

AD DS es un servicio que ofrece un directorio jerárquico en el que se almacenan usuarios y máquinas Windows, y sobre el que se pueden aplicar ajustes de configuración y seguridad.

Este servicio forma la base de las redes empresariales que ejecutan los sistemas operativos Windows.

Dentro de las configuraciones, podemos encontrar administración de la infraestructura, de seguridad, emisión de certificados digitales o control de acceso remoto.

AD DS incluye componentes físicos y lógicos. Ambos funcionan conjuntamente para administrar la infraestructura de forma eficaz.

Componentes lógicos

Son aquellos no tangibles, entre ellos se encuentran las particiones (partes de la BD que almacenan datos específicos), dominios (contenedor administrativo que almacena usuarios y equipos), los árboles de dominios (colección jerárquica de dominios con un directorio raíz en común) y los bosques (colección de árboles de domino gestionados por la misma organización).

Componentes físicos

Son aquellos objetos físicos que describen objetos del mundo real, entre ellos se encuentran los controladores de dominio (contiene una copia de la BD de AD DS, puede procesar cambios y replicarlos en los demás controladores de dominio en dominio) o los almacenes de datos (existe una copia del almacén de datos en cada dominio)

Objetos: Usuarios, grupos, equipos y Unidades Organizativas

Usuarios

Cada persona que requiera acceso a los recursos de la red precisa de un usuario. Un usuario se resume en un nombre, una contraseña y sus pertenencias a grupos.

Se pueden crear y administrar usuarios desde el Centro de administración de Active Directory, desde el Windows Admin Center o desde Windows Powershell entre otros.

Existen las denominadas cuentas de servicio administradas, que consisten en una cuenta basada en dominio para ejecutar servicios de programas. Windows Server admite un objeto de AD DS, denominado cuenta de servicio administrada, que facilita la administración.

También existen las cuentas de servicio administradas de grupo, que amplían las capacidades de una cuenta de servicio administrada estándar a más de un servidor de dominio.

Grupos

Para hacer más eficiente la organización en las organizaciones, existen los grupos, a los cuales se pueden asignar usuarios para que estos tengan los mismos permisos.

Existen dos tipos de grupo: Seguridad, que como su propio nombre indica, están orientados a administrar la seguridad, y Distribución, aquellos no orientados a la seguridad.

Otro parámetro para tener en cuenta en los grupos es el ámbito de grupo, que determina el alcance de las capacidades o permisos de un grupo.

Hay 4 ámbitos (*scopes*):

Local de máquina: Para estaciones de trabajo o servidores independientes.

Local de dominio: Para administrar el acceso a los recursos o para asignar derechos y responsabilidades de administración. Aplica a todo un dominio.

Global: Para consolidar usuarios que tienen características similares. Aplica a todo un árbol.

Universal: Se usa con más frecuencia en redes multidominio porque combina las características de los grupos locales de dominio y los grupos globales, ya que es aplicable a todo el bosque de una organización.

Equipos (máquinas)

Al igual que los usuarios, las máquinas tienen una cuenta para iniciar sesión, se autentican con el dominio y pueden pertenecer a grupos.

Unidades Organizativas

Una unidad organizativa es un objeto contenedor dentro de un dominio que se usa para contener otros objetos (p.e. Usuarios, Equipos, Grupos y otras Unidades Organizativas).

Puede vincular objetos de directiva de grupo (GPO) directamente a una unidad organizativa para realizar labores de administración. Las GPO son directivas que los administradores crean para desplegar configuraciones en los objetos que pertenecen a la Unidad Organizativa en cuestión.

Se pueden crear nuevas unidades organizativas desde el Centro de administración de Active Directory, el Windows Admin Center o desde el Windows Powershell.

Crear unidades organizativas facilita la administración y permite delegar el control administrativo.

Bosques y dominios de AD DS

¿Qué es un bosque?

Es un contenedor de nivel superior en AD DS. Cada bosque es una colección de uno o varios árboles de dominios que comparten un esquema de directorio común y un catálogo global. Un árbol de dominios es una colección de uno o varios dominios que comparten un espacio de nombres contiguo. El dominio raíz del bosque es el primer dominio que se crea en el bosque.

¿Qué es un dominio?

Un dominio de AD DS es un contenedor lógico que almacena objetos de AD DS. La base de datos de AD DS almacena todos los objetos de dominio, y cada controlador de dominio almacena una copia de la base de datos.

Administración de objetos y sus propiedades en AD DS

Existen varias herramientas para administrar AD DS:

- **Centro de administración de Active Directory**

  Proporciona una GUI para la administración de AD.

  Algunas de las principales tareas que permite son:

  - Crear y administrar cuentas de usuario, equipo y grupo.
  - Crear y administrar unidades organizativas.
  - Conectar varios dominios dentro de una única instancia del Centro de administración y administrarlos.
  - Crear y administrar directivas de contraseña detalladas.

- **Windows Admin Center**

  Consola basada en Web

  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 forma remota.

- **Módulo de Active Directory para Windows PowerShell**

  Permite la administración de AD DS y es uno de los componentes de administración más importantes.

Administración de controladores de dominio de AD DS y roles de FSMO

Implementación de Controladores de Dominio de AD DS

Los controladores de dominio autentican a todos los usuarios y equipos de un dominio. Por lo tanto, es fundamental garantizar el número y ubicación óptimos.

El rol de Controlador de Dominio se puede instalar en cualquier máquina Windows Server.

Mantenimiento de Controladores de Dominio de AD DS

Para asegurar la disponibilidad los controladores de dominio usan un proceso de replicación de arquitectura para copiar datos de un controlador de dominio a otro.

Para mantener la confiabilidad es importante realizar copias de seguridad periódicas.

Para restaurar AD DS, una copia de seguridad debe incluir explícitamente los datos de estado del sistema, que es una colección de archivos críticos de los roles de servidor y sistema operativo que incluyen la base de datos y el registro de AD DS.

Rol de catálogo global de AD DS

El catálogo global es una copia parcial de solo lectura y que admite búsquedas de todos los objetos de un bosque. El catálogo global no contiene todos los atributos de cada objeto. En cambio, mantiene el subconjunto de atributos que es más probable que sean útiles en las búsquedas entre dominios, por ejemplo, givenName, displayName y mail. Es muy útil en bosques de varios dominios.

Maestros de operaciones de AD DS (FSMO)

Los roles de maestro de operaciones de AD DS son responsables de realizar operaciones que no son adecuadas para modelos de arquitectura multimaestro. Un controlador de dominio que tiene uno de estos roles es un maestro de operaciones, también conocido como FSMO. Hay 5 roles de maestro, y todos son asignados al primer controlador de dominio instalado en un bosque, pudiendo transferirse posteriormente. Solo uno de todos los controladores de dominio de un bosque puede asumir cada rol, es decir no puede haber redundancia en los roles.

Tipos de roles de maestro:

- **Maestro de esquema**: Realiza todos los cambios de esquema.
- **Maestro de nomenclatura de dominios**: Agrega o quita un dominio o hace cambios en el nombre de dominio.
- **Maestro de infraestructura**: Mantiene las referencias a objetos entre dominios y su integridad.
- **Maestro de RID**: Enfocado a que no se repitan IDs de seguridad.
- **Maestro emulador de PDC**: Actúa como origen de hora del dominio.

Esquemas de AD DS

Un esquema de AD DS es el componente que define todos los atributos y clases de objeto que AD DS utiliza para almacenar los datos.

Todos los controladores de dominio de un bosque contienen una copia del esquema que se aplica a ese bosque. Cualquier cambio en el esquema se replica en todos los controladores de dominio del bosque,

por ello, se recomienda hacer cambios solo cuando sea necesario. Además, el esquema no permite eliminaciones.

Implementación de objetos de directiva de grupo

Definición de objetos de directiva de grupo (GPO)

Directiva de grupo es un marco de los sistemas operativos Windows con componentes que residen en AD DS, en controladores de dominio y en cada una de las instancias de servidor y cliente de Windows. Normalmente son usadas para configurar valores que no se quiere que configuren los usuarios, pero también se usan para aumentar la seguridad o aplicar configuraciones avanzadas del sistema.

Un objeto de directiva de grupo (GPO) es un objeto que contiene una o más configuraciones de directiva, que aplican a una o varias opciones de configuración a distintos niveles. Los GPO se aplican siempre sobre una Unidad Organizativa, y aplica a todos los objetos bajo esa Unidad Organizativa. Las GPOs no afectan al grupo al que pertenecen los usuarios o equipos a los que aplican.

Administración de características avanzadas de AD DS

Relaciones de confianza.

Un bosque representa un límite de seguridad. Proporciona autenticación y autorización seguras para sus Usuarios, Equipos y Aplicaciones.

Las confianzas de AD DS permiten el acceso a los recursos de otros dominios en un entorno de AD DS complejo. Cuando se implementa un dominio es fácil de gestionar, pero cuando se implementan bosques de varios árboles de dominios, se vuelven más complejas. Las relaciones de confianza pueden ser unidireccionales o bidireccionales, son transitivas, y hay varios tipos diferentes.

Implementación de bosques de ESAE (entorno administrativo de seguridad mejorada).

Están compuestos por tres elementos: un bosque de Active Directory administrativo dedicado, un bosque de producción y una relación de confianza unidireccional del bosque de producción al bosque ESAE.

El bosque administrativo tiene controles de seguridad mejorados y hospeda cuentas, grupos y estaciones de trabajo con privilegios de acceso.

En el bosque de producción, los administradores realizan las actividades cotidianas de una organización. Se configura el bosque de producción para que las tareas administrativas solo puedan realizarse utilizando las cuentas que hospeda el bosque de ESAE. Las cuentas de usuario estándar se hospedan en él.

Ventajas:

- Cuentas bloqueadas: son cuentas de usuario estándar sin privilegios del bosque de ESAE que se configuran con privilegios elevados en el bosque de producción. Así si una cuenta se ve

comprometida mientras se usa en el bosque de producción, no se puede usar para realizar tareas administrativas en el bosque de ESAE.
- Autenticación selectiva.
- Manera sencilla de mejorar la seguridad: El diseño del bosque de ESAE proporciona una mejora de la seguridad de los bosques de producción.

Supervisión del estado operativo de AD DS

La insuficiencia de recursos del sistema puede provocar un bajo rendimiento del sistema del controlador de dominio.

Los cuatro recursos clave del sistema son:

- La unidad central de procesamiento (CPU).
- El subsistema de disco.
- La memoria.
- La red.

Se puede usar varias herramientas de Windows Server para diversos tipos de supervisión, tanto supervisión histórica como supervisión en tiempo real.

Herramientas más frecuentes:

- Administrador de tareas.
- Monitor de recursos.
- Visor de eventos.
- Monitor de rendimiento.

Implementación, configuración y administración

Administración segura de Windows Server

Privilegios mínimos y delegación de privilegios

En cualquier tipo de entorno, es una buena política asignar los privilegios mínimos y necesarios a cada usuario para que pueda desempeñar su actividad de forma correcta. Para esto existen los privilegios delegados. Estos se le pueden asignar a una OU, grupo o usuario y se aplican sobre otra OU, grupo o usuario en concreto dentro del árbol del dominio. Se pueden asignar múltiples tipos de privilegios delegados, entre los más habituales se encuentran:

- Crear, borrar y administrar cuentas
- Resetear la contraseña de usuarios
- Crear, borrar y administrar grupos
- Modificar los miembros que pertenecen a un grupo

PAW

Otra distinción importante es el uso de PAWs (Privileged Access Workstation). Para garantizar la seguridad, los administradores usarán este equipo exclusivamente para tareas de gestión de la infraestructura. Este equipo debe estar protegido de internet y se bloqueará para poder realizar únicamente las tareas administrativas necesarias.

Es recomendable usar Windows 10 Enterprise debido a las características de seguridad que este incluye como Credential Guard, que permite proteger los hashes NTLM.

A mayores, es posible que el administrador tenga que hacer al mismo tiempo de usuario y para ello existen dos aproximaciones recomendables:

- Disponer dos estaciones de trabajo.
- Disponer dentro del PAW de una VM para realizar tareas de usuario.

Servidores de salto

Un servidor de salto nos permite obtener acceso a dispositivos y administrarlos en una zona de seguridad diferente, como una red interna y una red perimetral. Es recomendable que se combinen con el uso de equipos PAW.

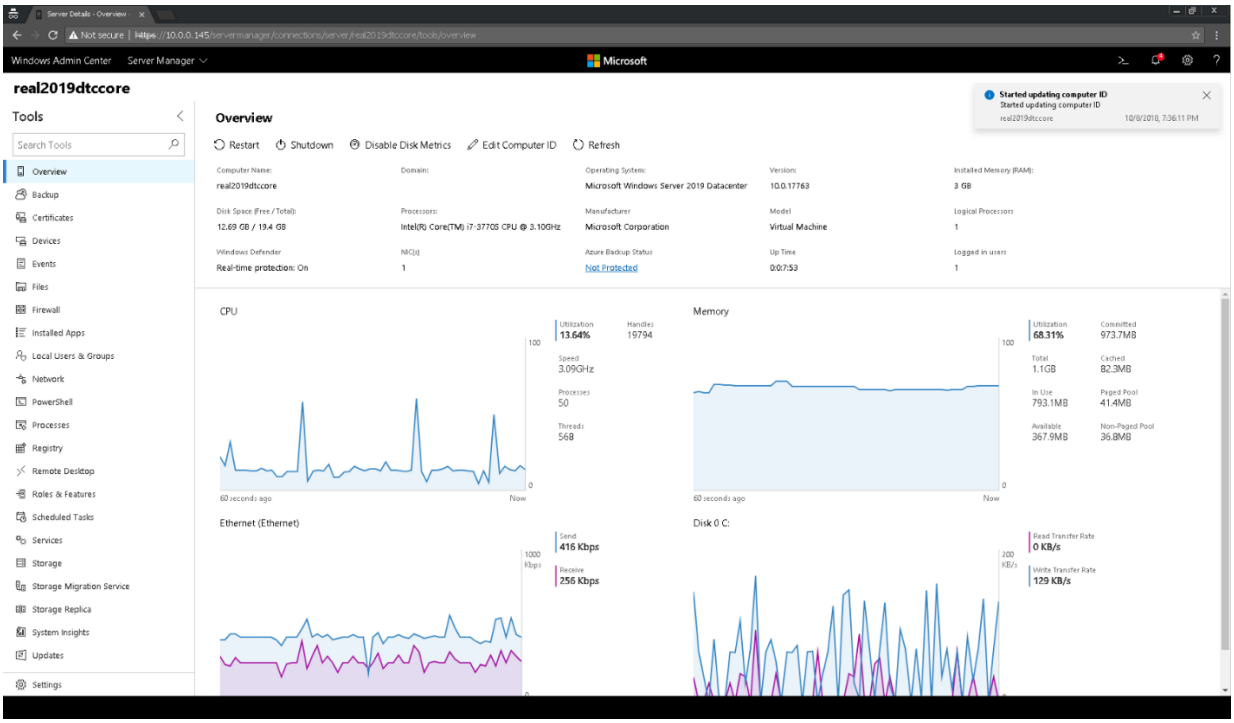
Administración de Windows Server

Para administrar Active Directory, desde Windows Server 2019 tenemos Windows Admin Center, una aplicación web que nos permite gestionar los siguientes módulos:

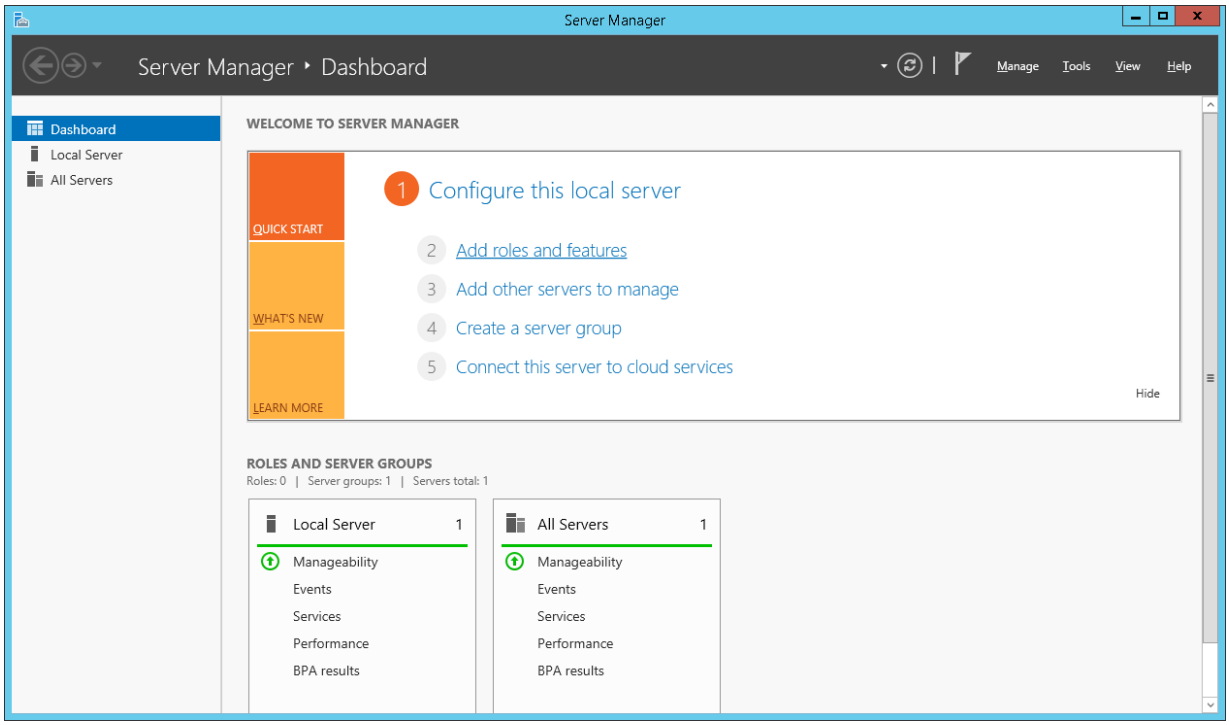
- Administración del servidor
- Clústeres de conmutación por error
- Clústeres hiperconvergidos
- Clientes de Windows 10

Adicionalmente, las máquinas Windows Server disponen de una interfaz gráfica nativa al estilo de Windows 10, para administrar el servidor llamada Administrador del Servidor (Server Manager). Podemos conectar con escritorio remoto (RDP) para configurarlos mediante el mismo, o añadirlos al

Administrador central. También existe la posibilidad de habilitar WinRM (Windows Remote Shell) que también nos permite realizar una administración de forma remota, entre otros.



WebApp: Windows Admin Center



GUI Tradicional de Escritorio: Windows Server Manager

Infraestructura de Red

Servicios de Red gestionados por Windows Server:

DHCP

DHCP (Dynamic Host Configuration Protocol) es un protocolo de autoconfiguración de dispositivos en red, de forma que cuando un nuevo dispositivo cliente se conecta a la red, el servidor DHCP le asigna una configuración IP, compuesta por:

- Dirección IP
- Máscara de subred
- Puerta de enlace
- Configuración DNS (servidores y sufijo)

DHCP utiliza paquetes IP de broadcast (a la dirección 255.255.255.255). Estos paquetes no se enrutan entre subredes, por tanto, debemos tener un servidor DHCP para cada subred, o un mecanismo para centralizarlos en uno solo. Cualquier servidor Windows Server puede tener el rol de servidor DHCP. Además, ese servicio DHCP se debe autorizar en el dominio de Active Directory, para evitar que otras máquinas no autorizadas hagan concesiones DHCP en nuestra red.

Además de darle a cada cliente una IP, DHCP puede dar mucha más información. Ésta es configurable en cuatro niveles:

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

Si un parámetro de configuración (p.ej. servidores DNS) está configurado en varios niveles, se usa siempre el más bajo. De esta forma se pueden configurar unas opciones globales y luego para algunos casos concretos, configurar excepciones.

Configuración de ámbitos:

> Cada ámbito DHCP hace referencia a una subred. Debemos definir el rango de IPs asignables (no tiene por qué ser toda la subred, ni un fragmento múltiplo de 2), la máscara de la subred y el tiempo de concesión. Además, es habitual definir puerta de enlace predeterminada y servidores DNS (si no están definidos ya en el nivel de servidor). Además, podemos realizar reservas DHCP, de forma que una dirección concreta del rango va a estar siempre reservada para el mismo cliente.

Alta disponibilidad de DHCP:

DHCP puede llegar a ser un servicio crítico, especialmente en redes con muchos clientes móviles, y una caída del servicio puede suponer que muchos clientes se queden sin conectividad.

Windows Server nos proporciona varios mecanismos para garantizar la disponibilidad de DHCP:

- Clústeres de servidores:

    - Podemos configurar el rol DHCP en un clúster en lugar de en un servidor individual, de forma que, si un servidor del clúster se cae, otro asume la responsabilidad.

- Implementación de ámbitos divididos:
    - Consiste en tener dos servidores DHCP activos en la red, que se reparten el rango de direcciones disponibles. De esta forma, nunca se solapan las direcciones asignadas por uno y por otro. Esta configuración es la más sencilla, aunque también la más ineficiente, ya que, si están funcionando los dos servidores, va a haber el doble de tráfico de broadcast.

- DHCP Failover
    - Es la forma más eficiente de HA para DHCP, y la que permite una mayor granularidad en las opciones de configuración. Consiste en configurar dos servidores para que se comuniquen entre ellos y se coordinen para dar el servicio. Ambos servidores comparten la misma configuración, el mismo rango de direcciones asignables, y los dos llevan la cuenta de todos los clientes que hay conectados a la red. Pueden configurarse en modo “load balancing”, de forma que se van alternando para dar las respuestas (a diferencia de los ámbitos divididos, aquí nunca ocurre que los dos servidores emitan una respuesta a la vez), o en modo “activo-pasivo”, de forma que el pasivo solo emite una respuesta si el activo no está disponible.

DNS

Domain Name Service (DNS) es un protocolo para traducir nombres de dominio a direcciones IP. Es un servicio básico para el correcto funcionamiento de cualquier red, doméstica 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 se organiza en zonas. Una zona es el conjunto de nombres que comparten un sufijo. Por ejemplo, la zona "udc.es" contiene todos los nombres de la forma "*.udc.es", y puede tener otras zonas (p.e "fic.udc.es" es una "subzona" dentro de udc.es). En AD, el equivalente a una "zona" sería un árbol de dominios.

Si configuramos una zona para que se almacene en la Base de Datos de AD DS, ésta se replica automáticamente en los demás servidores del Dominio que tienen instalado el rol de DNS. Puede configurarse para que se replique en todos los servidores de ese bosque (conjunto de dominios), lo cual es útil en la gestión de redes que tienen varios nombres de dominio.

También existe la posibilidad de que un servidor DNS secundario que no sea una máquina Windows Server pueda pedir una transferencia de zona. La transferencia de zona es una petición a la que el servidor responde con una lista de todos los registros que tiene para esa zona. Es una herramienta muy útil para la gestión de servidores secundarios, pero es importante configurar el servidor principal para que sólo responda a las peticiones de transferencia de zona que provienen de servidores secundarios autorizados.

Los registros se pueden crear a mano, añadiendo uno por uno los nombres con sus IPs, y se pueden crear dinámicamente. Cuando una máquina del Dominio se conecta a la red y obtiene una configuración IP del servidor DHCP del Dominio, ésta se registra en la zona DNS correspondiente, y se añade un registro A y uno PTR (resolución inversa).

Resolución de nombres externos a la organización:

Por defecto, un servidor DNS de Windows Server, al recibir una petición para una zona que no conoce, seguirá la jerarquía DNS desde el principio (servidores raíz, luego servidores del TLD, luego servidores del dominio…). Se puede configurar para que en lugar de eso reenvíe las peticiones DNS a otro servidor (p.ej. un servidor que nos proporcione nuestro ISP). Además, se pueden configurar redirecciones condicionales, para que las consultas a determinados dominios se reenvíen a determinados servidores.

DNS de Horizonte Dividido

Además de para resolver nombres de dominio a direcciones IP, en una red Windows el servicio DNS se usa para las comunicaciones con los servidores del dominio y para la autenticación en Active Directory. En los dominios que tienen asociado un Active Directory, existen entradas tipo SRV que dan soporte a los diferentes servicios de Active Directory. Sin embargo, desde Internet sólo se debe acceder a los registros DNS públicos. Para mejorar la seguridad en este aspecto, la responsabilidad del servicio DNS de un dominio se puede dividir en dos: uno o varios servidores que atiendan las peticiones DNS públicas de Internet, y otros que atiendan las peticiones desde la red privada, incluyendo las peticiones de registros SRV de Active Directory.

Además, los servidores DNS Windows Server permiten la implantación de Directivas DNS, que consisten en devolver una respuesta u otra a la misma consulta, según la red donde esté el cliente que hizo la consulta.

IP Address Management (IPAM)

IPAM es una suite de herramientas incluidas en Windows Server para facilitar el diseño y administración del direccionamiento IP de redes muy grandes. En una organización puede haber uno o varios servidores IPAM (puede haber uno para toda la organización, o uno en cada zona (p.ej en cada sede de la compañía), repartiéndose la carga). Los servidores IPAM se integran en Active Directory Domain Services, y gracias a AD DS averiguan cuales son los servidores que hay en el Dominio y cuáles son los roles que desempeña cada uno. Después se conecta a esos servidores y se descarga toda la información de direccionamiento IPv4 e IPv6, y nos la muestra en un panel de control centralizado. Desde este panel podemos gestionar el direccionamiento de la organización, las zonas y los registros DNS, los ámbitos DHCP, intervalos, reservas… todo lo que tenga que ver con direccionamiento IP. Además, IPAM puede mostrarnos sugerencias si hay una red que estamos dejando sin usar, o una red que se está quedando demasiado pequeña.

Implementación de Acceso Remoto

Es habitual que una organización quiera proporcionar a sus trabajadores una forma de poder conectarse a las aplicaciones empresariales desde fuera de las oficinas. Windows Server ofrece varias opciones para implementar esta funcionalidad.

VPN

Windows Server implementa varios protocolos de VPN:

- PPTP (Protocolo antiguo e inseguro, no se recomienda su uso)
- L2TP/IPsec
- SSTP
- IKEv2/IPsec

Aunque existe la posibilidad, no es habitual usar Windows Server como servidor de VPN. Existen dispositivos hardware específicos para este tipo de funcionalidades, con mayores capacidades y protocolos más avanzados, seguros y eficientes.

RADIUS

RADIUS (Remote Access Dial In User Service) es un protocolo de autenticación y autorización en red. NPS es la implementación de Windows Server del protocolo RADIUS. Podemos instalar el rol de servidor NPS en una máquina Windows Server que sea miembro del Directorio Activo, y ésta usará la base de datos de usuarios de AD DS para comprobar las solicitudes de conexión. El uso de RADIUS permite que el control de usuarios esté centralizado, y las demás aplicaciones o servicios solo tengan que delegar en el servidor RADIUS las solicitudes de autenticación de los usuarios.

Web Application Proxy

Windows Server, más concretamente, el rol de Microsoft Internet Information Services, puede funcionar como un proxy inverso para las aplicaciones web que estén almacenadas en los servidores de la organización. Esto permite que los usuarios se autentiquen con el servidor proxy, y sus peticiones no pasan a dentro de la red hasta que están autenticados y la conexión es segura. El servidor WAP de Windows Server usa la base de datos de usuarios de Active Directory para autenticar las conexiones entrantes, y permite habilitar medidas de seguridad adicionales como la autenticación de doble factor.

Bibliografía:

En la documentación oficial de Microsoft, realizamos los siguientes "learning paths"

- https://docs.microsoft.com/es-es/learn/paths/active-directory-domain-services/
- https://docs.microsoft.com/es-es/learn/paths/windows-server-deployment-configuration-administration/
- https://docs.microsoft.com/es-es/learn/paths/windows-server-network-infrastructure/

Fecha de última revisión de todos los enlaces previos

02/05/2021