

Capítulo 1

Roles y características

1. Organización del libro

El libro se compone de 18 capítulos, que presentan las distintas características del sistema operativo Windows Server 2016.

Con el objetivo de poder practicar en buenas condiciones, el capítulo Instalación del entorno de pruebas detalla la creación de una maqueta, equipada con 5 máquinas virtuales:

- **AD1, AD2, SV1 y SRVCore**, con Windows Server 2016.
- Una máquina cliente **CL10-01** con Windows 10.

Los capítulos, cada uno dedicado a un tema diferente, pueden recorrerse de manera independiente. Cada capítulo está construido para que pueda conocer la teoría y también su puesta en práctica sobre una o varias VM (o máquina virtual). El sistema operativo instalado en la máquina host es Windows Server 2012 R2, las máquinas virtuales funcionan con Windows Server 2016 en el caso de máquinas servidoras y con Windows 10 en la máquina cliente. AD1, AD2 y SV1 ejecutan su sistema operativo con una interfaz gráfica, SRVCore lo hace únicamente por línea de comandos.

Es posible descargar varios scripts y modelos de administración con formato ADM desde la página del libro en el sitio web de Ediciones ENI.

2. Roles

Los siguientes roles y características son una pequeña lista de aquellos presentes en Windows Server 2016.

Desde Windows Server 2008 R2, es posible instalar los distintos roles desde la consola **Administración del servidor**. Estos últimos aportan características suplementarias a los servidores. De este modo, el equipo IT puede ofrecer servicios suplementarios (direccionamiento IP automático de los puestos de trabajo y otro equipamiento conectado a la red, servidores de impresión...) a sus usuarios. La mayor parte de ellos contienen servicios de rol, que permiten habilitar ciertas funcionalidades. Se instalan bien generalmente durante la instalación de algún otro rol o funcionalidad. También pueden agregarse tras la instalación.

2.1 Acceso remoto

El rol **Acceso remoto** permite proveer un **servicio** VPN. La parte de enrutamiento está, también, presente y ofrece la funcionalidad que permite el enrutamiento de paquetes.

Los servicios de rol disponibles son:

- **Direct Access y VPN**: Direct Access permite establecer una conexión a la red de la empresa sin intervención alguna del usuario. La conexión se establece únicamente cuando el usuario se conecta desde el exterior de la red local.
- **Enrutamiento**: este servicio de rol permite instalar varios tipos de routers, entre ellos los que ejecutan RIP y los proxys IGMP.

2.2 Hyper-V

Desde Windows Server 2008, es posible instalar el hipervisor de Microsoft, **Hyper-V**. Permite implementar una plataforma de virtualización. Se ha enriquecido con Windows Server 2012 y 2012 R2. Se han integrado nuevas características a Windows Server 2016. Ahora es posible agregar en caliente para una VM una tarjeta de red virtual, así como la memoria. Esta funcionalidad resulta muy interesante y permite reducir el tiempo de indisponibilidad del servicio ofrecido por la máquina virtual correspondiente. Se han agregado otras funcionalidades, como la distribución del servicio de integración, a Hyper-V en Windows Server 2016.

2.3 DHCP (Dynamic Host Configuration Protocol)

El rol permite distribuir contratos DHCP a los distintos equipos que realizan la demanda. Puede instalarse sobre un servidor en modo instalación completa o en modo Core (instalación sin interfaz gráfica).

2.4 DNS (Domain Name System)

Obligatorio en un dominio Active Directory, permite resolver nombres en direcciones IP y a la inversa. Este servicio permite a su vez a los puestos cliente encontrar sus controladores de dominio. Puede instalarse sobre un servidor que no posea interfaz gráfica.

2.5 IIS (Internet Information Services)

Servidor web, permite mostrar y almacenar sitios y aplicaciones web. En la actualidad, cada vez es más frecuente que una aplicación posea una interfaz web.

Este rol es el que más servicios de rol posee.

- **Características HTTP comunes:** instala y administra las características HTTP básicas. Este servicio de rol permite crear mensajes de error personalizados con el objetivo de gestionar las respuestas generadas por el servidor.
- **Estado y diagnóstico:** aporta herramientas necesarias para la supervisión y el diagnóstico de la integridad de los servidores.
- **Rendimiento:** permite realizar compresión de contenido.
- **Seguridad:** implementa herramientas que permiten asegurar la seguridad del servidor frente a usuarios malintencionados y las consultas IIS.
- **Herramientas de administración:** provee herramientas de administración para las versiones anteriores de IIS.
- **Servidor FTP:** permite instalar y administrar un servidor FTP.

2.6 AD DS (Active Directory Domain Services)

Permite almacenar información de identificación de usuarios y equipos del dominio. Este rol se ejecuta en un servidor con el nombre del controlador de dominio, que tiene como función autenticar a los usuarios y los equipos presentes en el dominio AD.

Este rol puede instalarse en un servidor que no posea interfaz gráfica.

2.7 AD FS (Active Directory Federation Services)

El rol provee un servicio federado de gestión de identidades. Identifica y autentifica un usuario que quiera acceder a una extranet.

De este modo, dos empresas pueden compartir de forma segura información de identidad de Active Directory sobre un usuario Office 365 solo.

El rol está compuesto por varios servicios:

- **Servicio de federación:** instala la infraestructura necesaria para proveer acceso a los recursos.
- **Agente Web AD FS:** permite validar los testigos de seguridad entregados y autorizar un acceso autenticado a un recurso web.
- **Proxy FSP - (Federation Service Proxy):** permite recoger información de autenticación desde un navegador o una página web.

2.8 AD RMS (Active Directory Rights Management Services)

Protege un recurso contra un uso no autorizado. Los usuarios se identifican y se les concede permisos para acceder a la información protegida.

Es, así, más sencillo prohibir a un usuario copiar un documento en una memoria USB o imprimir un archivo confidencial.

Durante la instalación del rol, es posible instalar dos servicios:

- **Active Directory Rights Management Server:** permite proteger un recurso frente a un uso no autorizado.
- **Compatibilidad con la federación de identidades:** aprovecha las relaciones de federación entre dos organizaciones para establecer la identidad del usuario y permitirle el acceso a un recurso compartido.

2.9 AD CS (Active Directory Certificate Service)

Instala una autoridad de certificación con el objetivo de realizar operaciones de emisión y de administración de certificados.

Es posible agregar seis servicios de rol durante la instalación:

- **Autoridades de certificación:** provee una infraestructura de clave pública.
- **Inscripción en web de entidades de certificación:** se instala una interfaz web que permite, a un usuario, realizar solicitudes y renovaciones de certificados. Es, también, posible recuperar listas de revocación de certificados o realizar una inscripción de certificados de tarjetas.

- **Respondedor en línea:** permite gestionar y administrar la información del estado de la revocación.
- **Servicio de inscripción de dispositivos de red:** emite y gestiona los certificados de los routers y demás periféricos de red.
- **Servicio web de inscripción de certificados:** este servicio de rol ofrece la posibilidad a los usuarios y equipos de realizar la inscripción y renovación de certificados.
- **Servicio web de directiva de inscripción de certificados:** ofrece a los usuarios y equipos información sobre la directiva de inscripción de certificados.

2.10 Servicios de implementación de Windows (Windows Deployment Services - WDS)

Este rol provee un servicio de despliegue de sistemas operativos a través de la red. El servidor posee dos tipos de imágenes: **imágenes de arranque**, que permiten acceder a la instalación de Windows o a una carpeta compartida (MDT), e **imágenes de instalación**, que contienen los metadatos necesarios para la instalación del sistema operativo.

Con la instalación de este servicio es posible instalar dos servicios de rol:

- **Servidor de despliegue:** provee las funcionalidades necesarias para el despliegue de un sistema operativo. Este servicio también tiene en cuenta funcionalidades de captura.
- **Servidor de transporte:** se utiliza para transmitir datos en modo multidifusión.

2.11 Servicio de acceso y directivas de redes

Este rol permite gestionar accesos a la red mediante acceso inalámbrico, servidores VPN, así como conmutadores de autenticación 802.1x. La instalación de NPS (*Network Policy Server*) permite implementar la protección de acceso a la red (NAP).

Los servicios de rol disponibles son:

- **Servidor NPS:** permite implementar directivas de acceso a la red para las solicitudes de conexión.
- **Autoridad HRA:** emisión de certificados de integridad para los puestos de trabajo conforme a las exigencias de integridad.
- **HCAP** (*Host Credential Authorization Protocol*): la solución NAP está integrada con la solución de control de acceso Cisco.

2.12 WSUS

Permite aprobar las actualizaciones antes de su instalación en un puesto cliente, estando este último en un rango dentro de un grupo de ordenadores. Esta solución permite realizar una aprobación para un grupo en particular (por ejemplo: grupo "pruebas" en primer lugar y, a continuación, si el correctivo no provoca ningún problema, se aprueba para el resto).

Existen tres servicios de rol disponibles:

- **WID Database:** instala la base de datos que utiliza WSUS en WID (*Windows Internal Database*). Este tipo de base de datos pueden utilizarla otros roles (AD RMS, etc.).
- **WSUS Services:** instala el servicio WSUS, así como el resto de los componentes necesarios.
- **Base de datos:** instala la base de datos para los servicios WSUS (se necesita un servidor SQL, a diferencia de WID Database).

2.13 Servicios de archivos e iSCSI

El servicio de archivos permite implementar cuotas en el sistema de archivos, así como un sistema de filtrado por extensión, con el objetivo de prohibir que se almacenen ciertos archivos. Es posible instalar un espacio de nombres DFS mediante un servicio de rol.

Los siguientes servicios ofrecen la posibilidad de instalarse como servicio de rol:

- **Servidor de archivos:** gestión de carpetas compartidas.
- **BranchCache para archivos de red:** incluye BranchCache en el servidor. Este servicio permite implementar la caché de documentos con el objetivo de reducir el uso de la línea existente entre dos sitios remotos. El usuario solo tiene, por ejemplo, que buscar los documentos en su puesto local, de modo que se actualizan en caché en un servidor o un puesto local.
- **Desduplicación de datos:** permite liberar el espacio de disco suprimiendo datos duplicados; en el volumen se almacena una copia única de los datos idénticos.
- **Espacio de nombres DFS:** instala las herramientas necesarias para la creación y la gestión del espacio de nombres.
- **Administrador de recursos del servidor de archivos:** herramienta que permite administrar un sistema de archivos mediante la creación de cuotas y el filtrado de archivos.
- **Replicación DFS:** sincroniza carpetas sobre varios servidores locales o un sitio remoto.