Active Directory

Transcribed on August 6, 2025 at 9:51 AM by Minutes AI

Speaker 1 (00:09)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar el tema del directorio activo.

Hablaremos de Active Directory Domain Service, hablaremos de los controladores de dominio, catálogo global del proceso de autenticación y hablaremos de las consolas de administración y los servicios que tenemos disponibles para administrar el directorio activo.

Un dominio requiere de uno o más controladores de dominio que van a ser los servidores encargados de almacenar una copia de la base de datos del directorio activo que va a estar permanentemente sincronizada entre todos aquellos controladores de dominio que pertenezcan al mismo dominio.

Normalmente al ser un servicio crítico, yo voy a querer tener más de un controlador de dominio porque si en un momento determinado ese controlador de dominio deja de funcionar, todos los procesos de autorización y autenticación se verían comprometidos.

Entonces, al menos la recomendación de Microsoft es que tengamos dos servidores por cada uno de los dominios.

Entonces cada uno de esos servidores va a conservar una base de datos con toda la estructura y los elementos del directorio activo y va a estar permanentemente sincronizándola con el resto de controladores de ese mismo dominio.

Los dominios nos van a permitir crear usuarios, crear grupos y crear cuentas de equipo.

También vamos a poder crear unidades organizativas que son un contenedor especial del directorio activo al que luego vamos a poder hacer diferentes operaciones como delegaciones o asignar configuraciones a través de objetos de directiva de grupo a través de GPOS.

Un dominio nos va a ofrecer un recurso de administración central en un entorno de confianza donde los controladores de dominio se van a encargar del proceso de autenticación y autorización.

Vamos a ver cómo instalar un controlador de dominio, vamos a poder hacerlo a través de Windows PowerShell, vamos a poder hacerlo a través del entorno gráfico y vamos a ver la importancia que tiene los servicios de DNS de resolución de nombres de dominio en lo que se refiere a la parte de resolver recursos de un dominio y que debemos tener en cuenta cuando nosotros queremos desplegar un controlador de dominio.

Para crear nuestro primer dominio estamos en Server Manager y desde Server Manager nos vamos a la parte de Administrar, añadir roles y características, nos vamos a Siguiente, seleccionamos el equipo, damos a siguiente y en la parte de roles vamos a tener Active Directory Domain Service, damos añadir, este es el rol principal, si os fijáis tenemos más roles que están relacionados con el directorio activo.

Tenemos Active Directory Certificate Service, Active Directory Federation Service, Railway Directory Service o Rail Management Service.

Estos otros roles son servicios relacionados con el directorio activo, pero el controlador del directorio activo es Active Directory Domain Service.

Daríamos a Siguiente, Siguiente y daríamos a Instalar.

Como os había comentado en ocasiones anteriores, el proceso de instalación es siempre el mismo.

Una vez que nosotros sabemos el rol, la característica o el servicio que queremos instalar, pues prácticamente el proceso de instalarlo es siguiente, siguiente, siguiene.

Luego lo difícil o lo complejo es saber configurar esos roles o saber configurar esas estructuras que vamos a desplegar.

Vamos a esperar a que termine el proceso de instalación.

Una vez que se instalan las características, nos aparecería la opción para promover este servidor a controlador de dominio.

El asistente nos va a guiar durante todo el paso de instalación.

Lo que tenemos que tener claro es en la primera opción qué es lo que nosotros queremos desplegar.

Si nosotros lo que queremos es desplegar un controlador de dominio adicional en un dominio que ya existe, es decir, que no vamos a crear una estructura nueva, sino que ya tenemos un dominio, tenemos uno o varios controladores de dominio y vamos a añadir un servidor adicional, la recomendación de Microsoft es que el dominio es un entorno crítico, por lo tanto, se recomienda que al menos haya dos controladores de dominio, de tal forma que si uno de los controladores de dominio tiene algún inconveniente, vamos a tener otro que va a estar respaldando el servicio de autenticación y autorización dentro de la organización.

Esta sería la primera opción.

En la segunda opción, nosotros lo que haríamos sería desplegar un nuevo dominio, que puede ser un dominio hijo, es decir, si yo tengo el dominio EMPRESA.

COM, pues sería un dominio hijo MAIL EMPRESA.

COM o un dominio nuevo, es decir, con un nombre diferente.

Yo tengo el dominio ZARA.

COM y voy a desplegar el dominio, pero los dos dominios van a estar dentro del mismo bosque.

Veremos posteriormente que esto tiene implicaciones a nivel de seguridad, es decir, que yo voy a tener dos dominios con nombres diferentes, pero si están dentro del mismo bosque van a tener una relación de confianza, van a tener una relación a nivel de seguridad.

Esto sería un nuevo árbol de dominio que estaría integrado dentro del mismo bosque.

Si yo lo que quiero es tener un dominio totalmente independiente, o cuando yo creo mi primer dominio, lo que tengo que crear es un dominio que a su vez tiene que crear un bosque, es decir, el bosque es una estructura que contiene dominios.

Entonces cuando yo creo mi primer dominio, a la vez que estoy creando ese dominio, estoy creando un contenedor de ámbito superior que es el bosque, que generalmente va a tener el mismo nombre que tiene el dominio.

En este caso, si yo creo el dominio ANGEL.

COM doy a siguiente.

Bueno, en esta pantalla lo que me va a preguntar es por el nivel funcional, tanto a nivel de bosque como a nivel de dominio vemos que tenemos diferentes niveles funcionales desde 2008 hasta 2016, tanto en la parte de nivel de bosque como lo que sería la parte de nivel funcional del dominio.

El nivel funcional nos va a permitir disfrutar de las últimas características que tenemos en el sistema operativo en relación a Active Directory.

Es decir, que yo para una determinada característica tendré que tener un nivel funcional de bosque de 2016 o de 2012 o un nivel funcional de dominio de 2016.

Si yo tengo un nivel funcional de server 2016, no puedo tener controladores de dominio que tengan una versión inferior a 2016.

Puedo tener servidores, yo puedo tener un servidor de archivos, un servidor DNS, servidor web que sea 2012, que sea 2008, pero no puedo tener un servidor que esté utilizando el rol de controlador de DOM.

Es decir que el nivel funcional me va a marcar el mínimo de versión que tengo que tener desplegada para los controladores de dominio.

¿Por qué voy a elevar el nivel funcional?

Porque para que funcionen algunas características es obligatorio que el nivel funcional esté en un determinado rango.

Entonces hay características que para poder desplegarlas sólo voy a poder hacerlo si el nivel funcional del bosque es 2016.

¿Why Star?

Otro elemento que vamos a tener para poder configurar aquí es si queremos que el servidor sea servidor de DNS, si queremos que sea catálogo global o si queremos que sea un controlador de dominio de solo lectura.

Un controlador de dominio de solo lectura no va a poder hacer cambios en el directorio activo.

Es un rol, es un servicio que está muy bien para estar en una organización dentro de una sucursal donde no hay departamento IT o donde esa máquina tiene que resolver las peticiones de dominio, pero no nos fiamos de que esa máquina no pueda ser sustraída o que esa máquina no pueda ser configurada de mala forma por alguien que no tenga suficiente experiencia.

Entonces en ese tipo de entornos el controlador de dominio lo que va a hacer es que nos va a permitir tener un controlador de dominio que resuelve las peticiones, pero ese controlador de dominio no va a poder generar cambios en la estructura de Active Directory.

Como podemos ver viene apagada la característica y eso es porque este es el primer controlador de dominio.

Es decir, un controlador de dominio de solo lectura es una copia secundaria.

Por lo tanto es necesario que copie los datos de un controlador de dominio que sea de lectura y escritura.

El primer controlador de dominio de un dominio nunca puede ser RODG.

El catálogo global también es obligatorio.

El catálogo global lo veremos posteriormente y vamos a ver que tiene que haber un catálogo global obligatoriamente por cada dominio.

Entonces cuando nosotros desplegamos el primer controlador de dominio obligatoriamente tiene que ser catálogo global.

La recomendación es que todos los controladores de dominio sean servidores de DNS para que sean ellos los que resuelvan las peticiones de DNS.

Además, el sistema de replicación del servicio de DNS se va a hacer entre controladores de dominio de una forma mucho más segura que el protocolo que se utiliza por defecto en DNS para replicar los registros y las tomas.

Finalmente tenemos aquí otro elemento que es interesante que es la clave, el password que vamos a tener que poner para cuando queramos poner el controlador de dominio en modo restauración.

Hemos dicho que el controlador de dominio mantiene la base de datos del directorio activo.

En un momento determinado puede ser que nosotros queramos recuperar esa base de datos a un estado anterior, es decir, hacer como una especie de restauración de un backup de la base de datos con los objetos de Active Directory.

Para poder hacer esa operación necesitamos poner el controlador de dominio en modo restauración y en ese momento nos va a pedir esta clave.

Es importante que no confundamos eso con la clave que nosotros ponemos con la clave que nosotros tenemos para el administrador del dominio, porque esa clave realmente lo que hace es que esa clave se toma desde el administrador que crea el dominio.

El administrador que crea el dominio le va a dar esa clave, va a poner ese password al administrador de dominio.

Bueno, aquí en la parte de delegación es importante dejarlo en blanco.

Después lo que va a hacer es que va a verificar la parte de la contraseña de netbios, pero a diferencia de lo que piensa la mayor parte de la gente, casi todas las resoluciones que se hacen dentro del directorio activo se hacen a través de servicios de DNS, de hecho prácticamente no se utiliza netbios, hay un montón de resoluciones anteriores que se van a utilizar previamente antes de utilizar netamente.

Lo siguiente que tenemos que configurar es donde se va a almacenar la base de datos del directorio activo.

Fijaros que por defecto nos lo crea en el volumen de sistema, tanto el archivo, la base de datos NTDS como la carpeta SYSBO.

En un entorno de producción esto nunca puede estar en el volumen de sistema, siempre tiene que estar en un volumen diferente, que además puede llegar a coger un tamaño considerable y vamos a evitar que se bloquee el sistema.

Para proyectos o para configuraciones de backup o configuraciones de seguridad también va a ser ventajoso que la base de datos de Active Directory y la carpeta SYSVOL estén un volumen separado.

Luego tendríamos aquí finalmente la revisión.

Podríamos ver un script del despliegue exacto que estamos haciendo, que podríamos copiar para después llevarlo a otras máquinas, hacer exactamente el mismo despliegue.

Con este script en Windows PowerShell daríamos a siguiente.

Se van a verificar los prerrequisitos antes del proceso de instalación, aunque nos van a aparecer varios warnings.

Por ejemplo, nos va a aparecer generalmente un warning relacionado con el servicio de resolución de nombres, con el servicio de DNS, porque nosotros no instalamos el rol de DNS, nosotros instalamos Active Directory Domain Service y Active Directory Domain Service a su vez, si no quitamos el check, que es lo que debemos hacer, debemos mantener ese check marcado, nos va a instalar Active Directory Domain Service y nos va a instalar el servicio de DNS.

Entonces generalmente en la parte de prerrequisitos nos va a marcar eso como un warning, porque necesitamos resolver los registros del dominio con un servidor DNS que no existe, aunque nosotros vamos a crearlo en ese momento.

Simplemente damos a instalar y esperamos a que termine la instalación.

Una vez que termina la instalación, lo siguiente que nos va a pedir es un reinicio.

Siempre que nosotros convertimos un servidor en controlador de dominio o siempre que nosotros unimos una máquina al dominio, va a ser obligatorio un proceso de reinicio.

Una vez reiniciada la máquina, si nos vamos a la parte de Local Server, vamos a poder observar que donde antes teníamos la opción de Workgroup, nos va a figurar que pertenecemos a un determinado dominio.

Entonces en este caso vemos que estaríamos aquí dentro del dominio de Ángel.

COM y si nos vamos a la parte de Tools.

Dentro de la parte de Tools, automáticamente nos van a aparecer una serie de herramientas administrativas.

Active Directory, Administrative Center, Dominios y Confianzas, un módulo para Power Excel, Sitios y Servicios, Usuarios y Equipos y además vamos a tener la consola de administración del servicio de DNS.

Cuando nosotros abrimos la consola del servicio de DNS, nos vamos a encontrar con que vamos a tener una zona de búsqueda directa y una zona de búsqueda inversa relacionadas con el directorio activo.

Si nos vamos a la zona de búsqueda directa del dominio, vamos a ver que aquí de forma dinámica nos van a ir apareciendo las máquinas que están en el dominio.

En este caso está solo el controlador de dominio, una máquina que se llama Dc, está solo el controlador de dominio, una máquina que se llama Dc, con su correspondiente dirección IP.

Pero si nos vamos también a la parte de TCP IP, vemos que tenemos una serie de registros que no son registros tipo A, sino que son registros tipo servicio, que son para el catálogo global, para el sistema de distribución de claves, para la parte de Kerberos y para la localización y los servicios del propio árbol de hereda.

Es decir, que la resolución de los recursos del directorio activo se hace a través de resoluciones de DNS.

Esto quiere decir que normalmente nosotros en la parte de configuración de IP, en este caso en la máquina virtual, si yo me voy a la configuración de la máquina virtual, pues voy a tener aquí una dirección IPV que está asignada automáticamente.

Entonces esto estaría incorrecto.

Yo tendría que asignar la dirección IP de forma manual, por ejemplo poner 192.

168.1.192.1 1.

2.

54 y el DNS tiene que apuntar a sí mismo, es decir, 192.168.1.11 o 127.001, que realmente 127.001 es una IP que apunta a sí misma, es decir, apunta a localhost automáticamente.

Yo ahora voy a refrescar Server Manager para que me aparezca aquí la configuración.

Esto puede pasar en muchas configuraciones, que nosotros hacemos una configuración en Server Manager y si luego no damos aquí a la parte de actualizar, no la vemos reflejada en la pantalla.

Entonces, cuando yo tengo esta dirección IP, tengo que cumplir dos condiciones.

Todos los equipos cliente, es decir, todos los equipos del dominio tienen que poder contactar con el controlador de dominio.

Entonces tiene que poder o alcanzar esa red o estar dentro de la misma red, entonces tendría que ser 192.1681 lo que sea y todos los equipos tienen que tener configurado en su adaptador de red en la parte de DNS al controlador de Domi, en este caso 192.168.1 para que el servicio de DNS del controlador de dominio pueda resolver esos recursos a todos los equipos client.

Si estamos en una máquina virtual, en este caso estamos en virtualbox, si yo me voy a la parte de la configuración y me voy a la parte del adaptador de red, en la parte del adaptador de red yo no puedo tener nada porque habría un filtrado de direcciones y no habría comunicación entre el equipo cliente y el controlador de dominio.

Entonces o bien tiene que estar todas las adaptadoras de red como adaptador puente o tiene que estar como red interna para que puedan comunicarse los adaptadores de red de las máquinas que se quieren unir al dominio o que quieran participar del dominio con las máquinas que sean controladores de dominio.

La unidad principal de Active Directory es el controlador de dominio, es el cerebro de Active Directory.

Cada controlador de dominio va a almacenar una copia de la base de datos que es este archivo NTDS DIV y de la carpeta SYSVOL.

Cualquier controlador de dominio puede hacer cambios en Active Directory, excepto aquellos controladores que sean de solo lectura.

Para hacer los cambios utilizan un protocolo de replicación que es DFS, aunque en versiones anteriores utilizaba FRS, hoy en día no sería habitual que nos encontráramos con replicaciones mediante FRS que correspondían con servidores de la versión de 2003.

Los controladores de dominio van a incluir el servicio de Kerberos para la autenticación y también un sistema de distribución de claves y van emitir los famosos tickets CGT para que después los usuarios puedan recibir las autorizaciones cuando quieren acceder a un recurso.

La mayor parte de los recursos se van a resolver a través de peticiones del servicio de DNS mediante servicios como los que hemos visto.

El catálogo global es una base de datos parcial de algunos objetos de Active Directory para localizar recursos que están dentro de dominios que pertenecen al mismo bosque.

¿Cómo funciona el proceso de autenticación?

Los usuarios van a autenticarse contra el controlador de dominio, es decir, los usuarios van a demostrar que dicen que son quienes dicen ser y para ello se les va a proponer un desafío, puede ser una contraseña puede ser una autenticación multifactor, etc.

Una vez que sobrepasan ese proceso de autenticación, que superan ese proceso de autenticación, se les va a emitir un ticket TGT, que es lo que se va a utilizar para poder después acceder a los recursos.

Dentro de la administración del Directorio Activo, nosotros vamos a tener una serie de herramientas que son el Centro Administrativo de Active Directory, Usuarios, Equipos del Directorio Activo, Sitios y Servicios, Dominios y Confianzas, el Esquema del Directorio Activo y un módulo para duendos PowerShell.

Si nosotros queremos administrar el Directorio Activo, nos vamos a la parte de Tools, nos vamos, por ejemplo, al Centro Administrativo de Active Directory y dentro de la parte del Dominio vamos a tener un contenedor para los equipos.

Si nos vamos al contenedor de Computers, vemos que no tenemos en este caso ningún dispositivo, no tenemos ningún equipo.

Tenemos una unidad organizativa que es para los Controladores de Dominio.

En este caso sí que vemos que tenemos un equipo, que es este, que es de C, que es el controlador de Dominio que está en esa unidad organizativa.

Y luego tendríamos los usuarios y los grupos que están creados dentro de un contenedor que se llama Usuarios.

Vemos que aquí tendríamos los diferentes usuarios.

Si yo quiero crear un usuario, voy a Nuevo, selecciono Usuario y para crear el usuario voy introduciendo los datos.

Es importante introducir el UPN y la contraseña.

Damos a OK y ya crearíamos el usuario.

Si yo vuelvo a entrar dentro de lo que sería la parte del uso del Usuario, nos vamos a la parte de Extensiones, nos vamos a la parte de Atributos y dentro de la parte de Atributos hay una serie de elementos que es importante conocer.

El Esquema del Directorio Activo, el Esquema del Bosque.

Esquema del Directorio Activo El esquema del Bosque nos va a marcar todos los atributos que tiene un determinado objeto, en este caso el objeto Usuario.

Entre ellos es muy habitual el distinguishname.

Distinguishname tiene siempre este formato, en este caso CN Angel, CN Users desde Angel, desde CO, y va a ser un identificador que va a servir para que Active Directory reconozca el objeto.

Aparte de este elemento, tenemos otro elemento que es el distinguishName.

Este identificador de seguridad es un objeto único que se crea cuando nosotros creamos un determinado objeto.

Cuando creamos un usuario se le asigna desde un pool de identificadores que tiene el Controlador de Dominio.

Este identificador, que tiene que ser único, como hemos visto los dominios y los bosques nos permiten una administración centralizada de los recursos de una organización, donde el controlador de dominio va a ser un elemento fundamental para que funcione correctamente toda esta estructura.

El límite por defecto para la parte de administración es el dominio, pero el límite para la parte de seguridad, la frontera para la parte de seguridad es a nivel de bosque, es decir, que todos los dominios que pertenecen al mismo bosque tienen una relación implícita de confianza.

Si yo quiero que dos dominios no tengan esa relación, tengo que crear cada uno de esos dominios en un bosque diferente, de esta manera no habría una relación de confianza a nivel de seguridad.

Tenemos una proposición de ejercicio que es que instaléis el directorio activo, el rol de Active Directory Domain Service, crear un nuevo dominio en un nuevo bosque, configurar el adaptador de red y después con otro equipo Windows 11 u otro servidor podéis configurar una dirección IP en la misma red y después unir ese equipo al dominio que acabáis de crear.

Llegamos al final de la sesión, os esperamos en el siguiente vídeo.

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar el tema del ejercicio anterior, se pedía instalar el rol de controlador de dominio, es decir, Active Directory Domain Service, crear un nuevo dominio en un nuevo bosque y después unir otro equipo al dominio.

El primer aspecto que debemos tener en cuenta es la parte de la conectividad entre las máquinas virtuales.

Entonces para eso en la parte de configuración tenemos que ir a la parte de red y asegurarnos que las máquinas virtuales que queramos conectar estén en la misma red virtual.

En mi caso voy a ponerlas dentro de la red interna, que será la red que voy a utilizar.

Una vez que estamos en la máquina virtual, estamos en un servidor en este caso que se llama DC, este servidor tiene configurada la dirección IP, si nos vamos a la parte de Ethernet, nos vamos a las propiedades del adaptador, nos vamos a las propiedades de IPV y veis que tenemos configurado en este caso una dirección ip que es 192.168.1.11 y el servidor DNS que es la misma máquina.

También es aconsejable en la parte del nombre que nosotros entremos en la parte de configuración, esto sería la descripción, no la forma de cambiar el nombre.

Para cambiar el nombre es aquí, seleccionamos ahí y aquí es donde podemos unir un equipo a un dominio que ya exista y es donde podemos cambiar el nombre.

Cuando nosotros vamos a desplegar un controlador de dominio es fundamental cambiar el nombre del equipo, asignar ese nombre previamente antes de hacer cualquier configuración.

Una vez cumplidos todos los prerrequisitos nos vamos a la parte de Administrar, Añadir roles y características y dentro de la parte de Añadir roles y características seleccionamos el servidor y seleccionamos Active Directory Domains.

Decimos que sí, que queremos añadir las características, damos a siguiente, damos a siguiente, damos a siguiente y damos a Instalar.

Vamos a esperar que termine el proceso de instalación.

Finalizado el proceso de instalación de características, vamos a hacer las tareas de configuración posteriores.

Para ello promovemos el servidor a Controlador de dominio.

En esta opción vamos a seleccionar un nuevo bosque y tenemos que poner el nombre del dominio, que tiene que ser un nombre de dominio que tenga un formato válido, es decir, un nombre com Org Academy, damos así Cliente, seleccionamos la password para el modo de restauración de la base de datos de Active Directory, aquí seleccionamos la ubicación de la base de datos y de la carpeta SYSVOL.

Recordar que en un entorno de producción no debe estar nunca en el volumen de sistema, tiene que estar en un volumen diferente.

Vamos a Siguiente, damos a Siguiente y damos a Instalar.

Una vez finalizada la instalación el equipo nos va a solicitar reinicio.

Una vez reiniciado el equipo podemos observar que estamos dentro del dominio Hackers Academy y si nos vamos a la parte de Tools tendremos las consolas de administración de Active Directory, el centro administrativo, Dominios y confianzas, el PowerShell, sitios y servicios y Usuarios y equipos de Active Director.

Si nos vamos a Usuarios y equipos del directorio activo, desplegamos la información del dominio y vemos que en la parte de Computers no hay ningún equipo y en la parte de Controladores de dominio vamos a tener en este caso el equipo Dc, que es el equipo desde que hemos instalado Active Directory Domain Services, el controlador de dominio.

Estamos en el equipo cliente, en este caso Windows 11, donde inicia, nos vamos a la parte de Configuración y en la parte de configuración nos vamos a ir a la parte de configuración del adaptador de red, vamos a Redes, Internet, nos vamos a la parte de configuración avanzada y vamos a editar la configuración de Excel, Vamos a editar opciones del adaptador, nos vamos a TCP IPV y tenemos que configurar el equipo dentro de la misma red que el controlador de dominio, en este caso 192.

168.1.

Lo que sea.

Además es importante que nuestro servidor DNS sea la dirección IP del controlador de dominio, en este ejemplo es 192.168.1.1.

Vamos a la parte de System.

En la parte de System nos vamos a la parte de abajo del todo y vamos a seleccionar About.

Aquí es donde nosotros podemos unir un equipo al dominio.

Para ello nos vamos aquí a la parte de Cambiar, seleccionamos Dominio y ponemos el nombre del dominio.

Academy nos solicita un usuario y contraseña y nos da la bienvenida al dominio.

También es necesario el proceso de reinicio cuando vamos a unir un equipo al dominio.

Daríamos aquí a cerrar y podríamos reiniciar el equipo y de esta manera el equipo se uniría al dominio.

Si nosotros vamos al servidor el controlador de dominio, nos vamos a la parte de Tools y nos vamos nuevamente a Usuarios y equipos de Active Directory.

Desplegamos en la parte del dominio, nos vamos a la parte de Computers y vemos que nos aparece ya la cuenta de equipo de este equipo que se ha unido al dominio.

Si nos vamos a la parte de Tools y nos vamos a la consola de DNS, dentro de las zonas de búsqueda directa en la zona del dominio, vemos que nos aparece aquí la dirección IP de la cuenta de equipo que hemos agregado al dominio.

Hemos visto cómo instalar el rol de Active Directory, cómo crear un nuevo dominio y cómo unir equipos a este dominio.

Llegamos al final de la sesión, os esperamos en el siguiente vídeo.