Introducción al concepto de relación de confianza

Una relación de confianza es una característica de Active Directory que facilita a los usuarios de un dominio tener acceso a los recursos de un dominio diferente.

Gracias a las confianzas entre dominios, un usuario de un dominio puede autenticarse en otro dominio.

En Windows NT, las confianzas usaban el protocolo NTLM (NT LAN Manager) para la autenticación de usuarios, implicaban dos dominios, eran unidireccionales y no transitivas. A partir de Windows 2000 Server se utiliza el protocolo Kerberos V5 para autenticar a los usuarios, y las relaciones pueden ser bidireccionales y transitivas.

A partir de Windows 2000 Server, sigue usándose NTLM para autenticar equipos sin soporte para Kerberos V5

En una relación unidireccional, los usuarios autenticados en el dominio de confianza (Dominio A) pueden acceder a los recursos del dominio que confía (Dominio B), mientras que los usuarios del dominio B no podrán acceder a los recursos del dominio A.

Si es una relación bidireccional, ambos dominios confían el uno en el otro.

Si una relación es transitiva, un dominio A que confiara en un dominio B a la vez que el dominio B confiara en el dominio C. Así, los usuarios del dominio C podrían acceder a los recursos del dominio A (si tienen los permisos adecuados).

Al crear una relación de confianza, hay que configurar ambos lados de la relación, por lo que habrá que disponer de credenciales válidas en ambos dominios.

La cuenta de usuarios que usemos para establecer o administrar una relación de confianza debe ser miembro del grupo Administradores del dominio

Objetos del dominio de confianza

Cada relación de confianza de un dominio se representa con un Objeto de Dominio de Confianza (TDO, Trusted Domain Object). Por lo que, cada vez que se crea una relación, se crea un nuevo TDO único con todos sus atributos y se almacena en el contenedor System del dominio.

Los atributos de un TDO son, como mínimo:

- La transitividad
- La direccionalidad de la confianza
- El nombre de los dominios recíprocos

Tipos de confianza

En Windows Server, podemos crear cuatro tipos de relaciones de confianza usando el Asistente para nueva confianza o la orden Netdom.

- **Confianza externa**: Facilita el acceso a recursos pertenecientes a un dominio Windows NT 4.0 o a dominios de bosques diferentes que no estén unidos por una confianza de bosque. Son relaciones no transitivas que pueden ser tanto unidireccionales como bidireccionales
- **Confianza de dominio kerberos**: Permite establecer relaciones de confianza entre dominios Windows Server y dominio que no sean Windows que usen el protocolo kerberos. Pueden ser relaciones transitivas o no transitivas, unidireccionales o bidireccionales.
- **Confianza de bosque**: Permiten compartir recursos entre diferentes bosques. Siempre son transitivas y pueden ser unidireccionales o bidireccionales. En caso de ser bidireccionales, las solicitudes de autenticación pueden llegar de un bosque a otro.
- **Confianza directa**: Mejoran el tiempo necesario para iniciar sesión entre dos dominios de árboles distintos en un bosque de Windows Server. Siempre son transitivas y pueden ser unidireccionales o bidireccionales.

¿Con qué dominios podemos establecer relaciones de confianza?

Teniendo un dominio con Windows Server 2019, podemos establecer relaciones de confianza con los siguientes dominios:

- Dominios de Windows Server 2019, 2016, 2012 R2, 2012, 2008 R2, 2008 o 2003 del mismo bosque
- Dominios de Windows Server 2019, 2016, 2012 R2, 2012, 2008 R2, 2008 o 2003 de otro bosque
- Dominios de Windows NT 4.0
- Dominios de Kerberos V5

Ruta de acceso de confianza

Antes de que un usuario de un dominio pueda usar los recursos de un dominio distinto, el sistema de seguridad debe establecer si el dominio que confía (el que ofrece el recurso) tiene una relación con el dominio de confianza, que debe ser en el que se ha autenticado el usuario.

Esto se consigue gracias a la ruta de acceso de confianza, es decir, la ruta de relaciones de confianza que seguirán las solicitudes de autenticación entre los dominios implicados.

Para establecer la ruta de acceso de confianza, es necesario tener en cuenta la direccionalidad de cada relación de confianza implicada.

Transitividad

La transitividad establece si una relación de confianza se puede extender más allá de dos dominios entre los que se estableció inicialmente.

Si establecemos una confianza transitiva, podrá extenderse a otros dominios. Si indicamos que sea no transitiva, se reducirá únicamente a los dominios implicados inicialmente en la relación.

Confianzas transitivas

Desde Windows 2000 Server, cuando creamos un dominio nuevo en un bosque existente, se establece automáticamente una relación de confianza bidireccional y transitiva entre el nuevo dominio y su dominio padre. Esta situación se replica si creamos un nuevo subdominio del dominio anterior.

Esto significa que un usuario podrá disponer de una cuenta en cualquier dominio del bosque y autenticarse en cualquier otro.

Además de las confianzas transitivas automáticas, podemos crear otras con el Asistente para nueva confianza:

- Confianza directa o Confianza abreviada: Se establece entre dos dominios de un bosque o árbol para abreviar la ruta de acceso de confianza entre ellos y reducir el tiempo necesario para que un usuario inicie sesión en otro dominio del bosque. Pueden ser unidireccionales o bidireccionales.
- Confianza de bosque: Se establece entre dos dominios raíz de dos bosques distintos
- Confianza de dominio kerberos: Se establece entre un dominio Active Directory y un dominio Kerberos V5

Confianzas no transitivas

Las confianzas no transitivas se limitan a los dominios incluidos de forma explícita en la propia relación de confianza, y no se amplían automáticamente cuando se incluya un nuevo dominio en el árbol. Es decir, la ruta de acceso de confianza no se amplía por la jerarquía del árbol de dominios a medida que esta crece.

De forma predeterminada, una relación de confianza no transitiva es unidireccional, pero se puede crear una bidireccional a partir de dos relaciones unidireccionales, una en cada sentido de la relación.

En los siguientes casos, las relaciones de confianza no transitivas son la única forma de establecer una relación:

- Cuando disponemos de de un dominio con Windows 2000 Server o superior y otro con Windows NT
- Cuando tenemos dos dominio con Windows 2000 Server o superior en bosques distintos y éstos no están relacionados con una confianza de bosque

En las versiones más modernas de Windows Server podemos usar el Asistente para nueva confianza para crear manualmente las siguientes relaciones de confianza:

- Confianza externa: Incluye las dos situaciones anteriores
- Confianza de dominio kerberos: Se establece una confianza no transitiva entre un dominio Active Directory y un dominio Kerberos V5

Si creamos una confianza entre un dominio del bosque y otro que está fuera del bosque, un usuario del bosque externo podrá acceder a los recursos internos, hasta poder convertirse en miembro de los grupos locales del dominio interno.

Roles que puede desempeñar un controlador de dominio

Un Controlador de dominio es un ordenador que contiene la base de datos del directorio para un dominio.

Tipos de controladores de dominio

En Active Directory existen los siguientes tipos de controladores de dominio:

- Primer controlador de dominio para un nuevo bosque: Es el equipo donde comenzamos a instalar el dominio. Actúa como Dominio raíz del bosque y se conoce como Maestro de operaciones (FSMO, Flexible Single Master Operations)
- Primer controlador de dominio para nuevo dominio: La instalación de un dominio nuevo en el bosque nos permite reflejar la estructura geográfica o jerárquica de nuestra empresa
- Controladores de dominio adicionales para un dominio: Ofrecen características de tolerancia a fallos y balanceo de carga a la infraestructura.
- Controladores de dominio de solo lectura (RODCs – Read-Only Domain Controllers): Suelen orientarse a entornos con poca seguridad donde no hay personal técnico que se ocupe del mantenimiento
- Controladores de dominio virtualizados: Son controladores de dominio que se ejecutan en máquinas virtuales (normalmente sobre Hyper-V). En las versiones más recientes de Windows Server se incluyen herramientas que ayudan a implementar y administrar estos servidores.

Añadir un nuevo controlador de dominio para un dominio existente

Al añadir un nuevo controlador de dominio a un controlador de dominio existente conseguimos dos cosas: proporcionar a la instalación características de tolerancia a fallos y equilibrar la carga sobre los servicios del directorio.

Configurar el Servidor DNS del controlador de dominio principal

Debemos ir a Herramientas → DNS y, en zonas de búsqueda inversa, hacer clic derecho → Zona nueva.

Debemos crear una zona principal y, además, marcaremos la opción de “Almacenar la zona en Active Directory”

Después, indicamos el ámbito en el que se va a replicar la nueva zona, que será en todos los servidores DNS del dominio para que se incluya el servidor DNS del nuevo controlador cuando lo creemos.

El siguiente paso es indicar si queremos crear la zona para direcciones IPv4 o IPv6. Solo podemos escoger una opción, por lo que debemos hacer dos zonas independientes si usamos ambas versiones de IP.

Después hay que indicar el Id de red (rango de direcciones). Si, por ejemplo, indicamos 192.168.1 se considera el rango desde la 192.268.1.1 hasta la 192.168.1.255

El siguiente paso es indicar el tipo de actualización dinámica que debe permitir la zona DNS. El objetivo de las actualizaciones dinámicas es que los equipos cliente puedan registrarse en la zona y actualizar los registros relativos a sus propios recursos cuando se produzca un cambio.

Cuando acabemos, habremos conseguido que el controlador de dominio resuelva los nombres relativos a la infraestructura. Pero, si en los equipos clientes habíamos configurado la IP del controlador de dominio como servidor DNS único, veremos que la red funciona, pero que los clientes no podrán navegar por Internet.

Esto se debe a que, cuando un cliente aporta un nombre que no pertenece a la red local, el servidor DNS no lo conoce, por lo que no sabe resolverlo. Para evitar esto, configuraremos los reenviadores, que son las IPs que hacen referencia a otros servidores DNS a los que se debe recurrir cuando el nuestro no conozca la dirección que se le está solicitando.

Configurar los reenviadores

Primero, en la ventana de Administrador de DNS, hacemos clic derecho sobre el nombre del controlador de dominio y seleccionamos "Propiedades" en el menú contextual.

En la ventana de propiedades, se accede a la pestaña "Reenviadores", donde ya puede haber una IP definida, como la 1.1.1.1 de Cloudflare y APNIC. Si no hay ninguna dirección, se puede añadir un servidor DNS, como el 8.8.8.8 de Google, repitiendo el proceso si se quieren agregar múltiples servidores. Debemos pulsar “Editar” para añadir un servidor nuevo.

En el caso de tener varios servidores, podemos moverlos con los botones “Subir” y “Bajar”, o eliminarlos con el botón “Eliminar”. También podemos elegir el número de segundos que esperará el sistema antes de enviar la solicitud al siguiente servidor.

Para comprobar que todo está correcto debemos mirar la columna FQDN del servidor. Si está rellena, significa que el servidor ha sido encontrado en Internet e identificado correctamente.

Configurar las características de red del equipo nuevo

Debemos seguir los siguientes pasos:

- Asignar una IP estática que esté libre en la red
- Añadir la máscara de red adecuada
- Incluir la puerta de enlace
- Indicar la IP del servidor principal como DNS preferido

Unir el nuevo equipo como cliente del dominio

La forma más fácil de que la promoción funcione es convertirlo en un nuevo equipo cliente del dominio para asegurarnos de que todas las configuraciones son correctas.

Lo único obligatorio que debemos hacer es, en la ventana de “Cambios en el dominio o el nombre del equipo”, elegir “Dominio” en la parte inferior y escribir el nombre del dominio del que nos vamos a hacer miembros.

Como última comprobación, desde Usuarios y equipos de Active Directory nos dirigimos a la entrada Computers, donde debe aparecer el nombre del equipo nuevo.

Comprobar los servidores DNS

Cuando hayamos configurado el nuevo equipo, debemos acceder a Herramientas → DNS dentro del Administrador del servidor.

Nos desplazamos hasta la entrada con el nombre de nuestro dominio, pasando por “Zonas de búsqueda directa” y podremos ver lo siguiente:

- Los controladores de dominio están registrados como Servidores de nombre (NS)
- El inicio de autoridad (SOA, Start Of Authority) hace referencia a “server-2019-b”
- Ambos controladores de dominio están registrados

Si hacemos la misma comprobación desde el “server-2019-a”, veremos lo mismo, pero el SOA hará referencia al “server-2019-a”

Replicar los controladores de dominio

Durante los próximos minutos, el controlador “server-2019-a” se irá replicando sobre el “server-2019-b”. La creación de los objetos de conexión puede crearse a mano.

Primero iremos a Herramientas → Sitios y servicios de Active Directory.

En el panel izquierdo, desplegamos “Sites, Default-First-Site-Name” y, luego, Servers. En su interior veremos los controladores de dominio que tenemos.

Desplegando cada servidor, tendremos acceso a la configuración de “NT Directory Services (NTDS Settings).

Para crear objetos manualmente, hacemos clic derecho sobre cada entrada NTDS Settings y elegimos Todas las tareas → Comprobar la topología de replicación

Aparecerá un mensaje que informa que la comprobación se ha realizado y que, en este caso, el server a está viniendo al b.

Si ahora actualizamos la información (clic derecho en Sites → Actualizar), podremos ver los objetos de conexión al acceder a cada entrada “NTDS Settings”

Lo siguiente es hacer clic derecho sobre los objetos de conexión de cada servidor y escoger la opción Replicar ahora. Cuando la replicación se complete, aparecerá un mensaje informando de ello.

Comprobar replicación

Para comprobar que desde “server-2019-b” tenemos acceso a todos los datos del dominio, abrimos Herramientas → Usuarios y equipos de Active Directory en el Administrador del servidor.

Cuando accedamos al dominio correspondiente y entremos en Computers, veremos los equipos que actúan como clientes del dominio.

Añadir un subdominio a un dominio existente

Añadiendo un subdominio a un dominio existente, conseguimos crear un subdominio de un dominio existente y comprobar que las relaciones de confianza se crean automáticamente.

—----

Establecer relaciones de confianza con dominios de otros bosques

En el caso de que, en una infraestructura de red, haya un dominio que no pertenezca al mismo bosque que los demás, los usuarios de ambos dominios podrán acceder a los recursos ofrecidos por el dominio contrario, aunque será necesario establecer la relación de confianza de forma explícita.

Si creamos una relación externa, no será una relación transitiva. En estos casos, para que la relación sea bidireccional, habrá que crear dos relaciones unidireccionales.
—---