Una relación de confianza es un característica de Active Directory que facilita a los usuarios de un dominio tener acceso a los recursos de un dominio diferente. Es decir, que gracias a las confianzas entre dominios, un usuario de un dominio puede autenticarse en otro dominio.

En este contexto, hablamos de un dominio que confía, es decir, que ofrece ciertos recursos y de un dominio de confianza, o dominio en el que se confía, que es donde se autentican los usuarios que utilizarán los recursos.

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

A partir de Windows 2000 server, sigue utilizándose NTLM para autenticar equipos sin soporte para Kerberos V5.

En una relación unidireccional, si la relación se ha establecido entre el dominio A (dominio de confianza) y el dominio B (dominio que confía), los usuarios que se autentiquen en el dominio A podrán tener acceso a los recursos del dominio B, mientras que los usuarios que se autentiquen en el dominio B no podrán acceder a los recursos del dominio A. Si la relación es bidireccional, ambos dominios confían el uno en el otro.

Si una relación es transitiva, podríamos tener un dominio A que confiara en un dominio B a la vez que el dominio B confiara en el dominio C. De esta forma, los usuarios del dominio C podrían tener acceso a los recursos del dominio A (siempre que tengan los permisos adecuados). Hablaremos de este tema de forma más detallada más adelante.

En cualquier caso, al crear una relación de confianza, habrá que configurar ambos lados de la relación (por lo que habrá que disponer de credenciales válidas en ambos dominios).

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

Este trabajo se puede hacer de forma independiente, ejecutando el Asistente para nueva confianza primero en un dominio y luego en el otro, o hacerlo de forma simultánea, con lo que ejecutaremos el Asistente para nueva confianza sólo en uno de los dominios. Si lo hacemos de forma simultánea, se creará automáticamente una contraseña de confianza segura.

Si lo hacemos por separado deberemos asegurarnos de incluir la misma contraseña de confianza en ambos lados de la relación.
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 tanto, cada vez que se crea una nueva relación, se crea un nuevo TDO único con todos sus atributos y se almacena en el contenedor System del dominio.

Como mínimo, los atributos incluidos en un TDO son:

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 diferentes utilizando el Asistente para nueva confianza o la orden Netdom.

Los tipos de relaciones de confianza disponibles son estos:

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 (ver más abajo). Se trata de relaciones no transitivas que pueden ser tanto unidireccionales como bidireccionales.

Confianza de dominio kerberos: Permiten establecer relaciones de confianza entre dominios Windows Server y dominios que utilicen el protocolo kerberos, pero que no sean Windows. 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 tanto unidireccionales como bidireccionales. En el caso de ser bidireccionales, las solicitudes de autenticación pueden llegar desde un bosque a otro.

Confianza directa: Mejoran el tiempo que necesitan los usuarios para iniciar sesión entre dos dominios de árboles distintos en un bosque de Windows Server. Siempre son transitivas y pueden ser tanto unidireccionales como bidireccionales.

¿Con qué dominios podemos establecer relaciones de confianza?

Si disponemos de un dominio con Windows Server 2019, podremos establecer relaciones de confianza con diferentes dominios. Éstos son los siguientes:

Dominios de Windows Server 2019, 2016, 2012 R2, 2012, 2008, 2008 R2 o 2003 del mismo bosque.

Dominios de Windows Server 2019, 2016, 2012 R2, 2012, 2008, 2008 R2 o 2003 de otro bosque.

Dominios de Windows NT 4.0.

Dominios Kerberos V5.

Ruta de acceso de confianza

Antes de que un usuario de un dominio pueda utilizar los recursos de un dominio diferente, el sistema de seguridad debe establecer si el dominio que confía (es decir, el que ofrece el recurso) tiene una relación con el dominio de confianza, que debe ser el dominio donde el usuario se ha autenticado. Esto se consigue calculando 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 imprescindible tener en cuenta la direccionalidad de cada relación de confianza implicada.

Transitividad

Como puede intuirse de lo que dijimos en la introducción, la transitividad establece si una relación de confianza se puede extender más allá de los dos dominios entre los que se estableció inicialmente.

Si establecemos una confianza transitiva, ésta podrá extenderse a otros dominio y si indicamos que sea no transitiva se verá reducida únicamente a los dominios implicados inicialmente en la relación.

Confianzas transitivas

A partir de Windows 2000 Server, cuando creamos un dominio nuevo en un bosque existente, automáticamente se establecerá una relación de confianza bidireccional y transitiva entre el dominio nuevo y su dominio padre. Esta situación se volverá a producir si creamos un nuevo subdominio del dominio anterior. De esta forma, la ruta de acceso de confianza se va ampliando por la jerarquía del árbol de dominios.

Esto significa que un usuario podrá disponer de una cuenta en cualquier dominio del bosque y autentificarse en cualquier otro, pudiendo acceder desde ahí a cualquier recurso sobre el que tenga permisos y que esté compartido en cualquier otro dominio del bosque. En la siguiente imagen podemos ver una confianza de bosque transitiva y bidireccional entre el Dominio A y el Dominio 1 (ambos son dominios raíz de diferentes árboles en bosques distintos). Una vez establecida la relación, cualquier usuario autenticado en cualquiera de los dominios del bosque podrán acceder a todos los recursos ofrecidos en cualquier otro dominio de ese bosque, siempre que los permisos de dichos recursos lo permitan.

Además de las confianzas transitivas automáticas anteriores, también podemos recurrir al Asistente para nueva confianza para crear estas otras:

Confianza directa o Confianza abreviada: Se establece entre dos dominios de un bosque o árbol complejo para abreviar la ruta de acceso de confianza entre ellos. Al crearla, reducimos el tiempo necesario para que un usuario inicie sesión en otro dominio del bosque, algo que resulta particularmente útil si este tipo de autenticaciones se realizan de forma regular. Pueden ser unidireccionales o bidireccionales. Lógicamente, nada impide tener una relación de confianza directa unidireccional que acorte el tiempo de acceso de los usuarios a los recursos en un sentido, pero que al mismo tiempo exista una ruta de acceso de confianza heredada para acceder a los recursos en el sentido inverso.

Confianza de bosque: Se establece entre dos dominios raíz de dos bosques diferentes.

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 de forma automática 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 ésta va creciendo.

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

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

Cuando disponemos de un dominio con Windows 2000 Server o superior y otro con Windows NT.

Cuando disponemos de dos dominios con Windows 2000 Server o superior en bosques diferentes y éstos no están relacionados con una confianza de bosque.

En las versiones más modernas de Windows Server, podemos recurrir al Asistente para nueva confianza para crear las siguientes relaciones de confianza de forma manual:

Confianza externa: Incluye las dos situaciones anteriores, es decir:

Establecer una relación de confianza no transitiva entre un dominio con Windows 2000 Server o superior y otro con Windows NT del mismo bosque o de otro bosque.

Establecer una relación de confianza entre dos dominios con Windows 2000 Server o superior en bosques diferentes.

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 se encuentra fuera del bosque, un usuario del bosque externo podrá acceder a los recursos internos, hasta el punto de que puede convertirse en miembro de los grupos locales del dominio interno