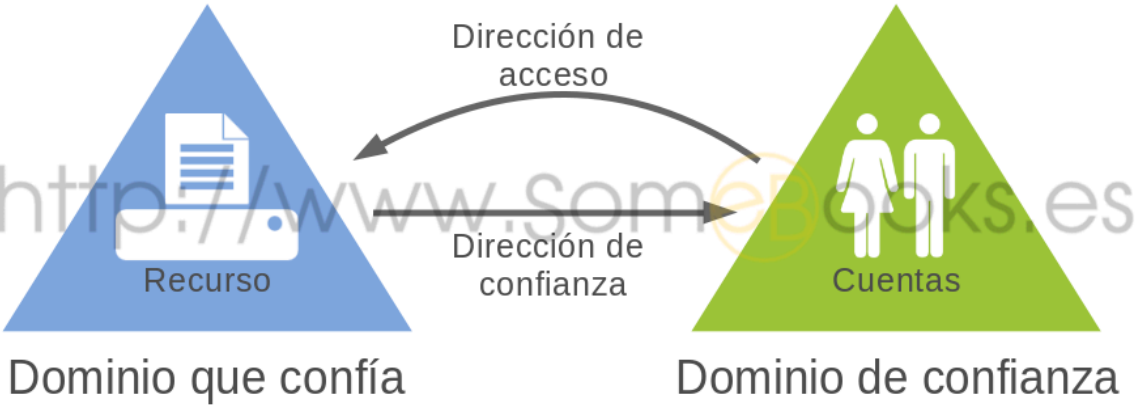
Resumen TEMA 10

10.1. Concepto de la relación de confianza.

Una relación de confianza es una característica de Active Directory que permite a usuarios de un dominio, acceder a recursos de un dominio diferente.



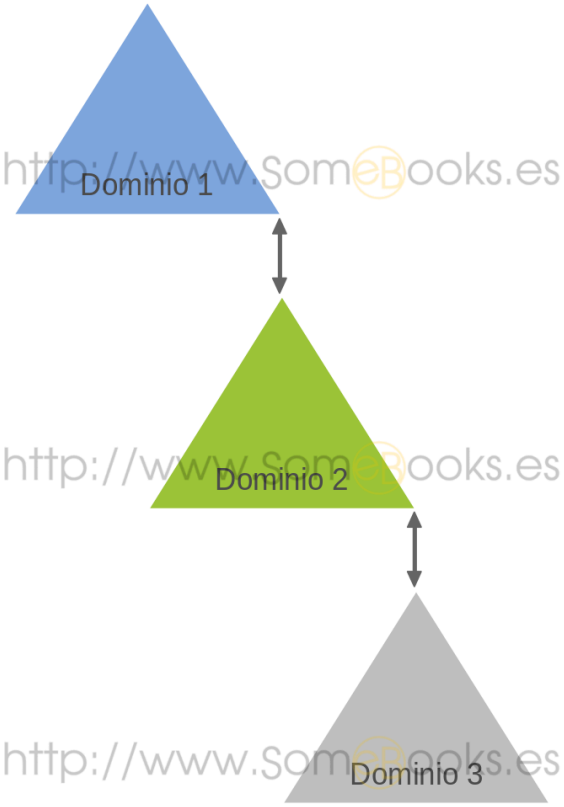
En Windows NT las confianzas utilizaban el protocolo NTLM *(NT LAN Manager)* para la autenticación de los usuarios. Eran solo de dos dominios, unidireccionales y no transitivas.

A partir de Windows 2000 Server, se utiliza el protocolo Kerberos V5 para autenticar a los usuarios.

> ⚠️ A partir de Windows 2000 server, se sigue usando NTLM (NT LAN Manager) pero para autenticar equipos que no tengan soporte de Kerberos V5.

- **Relación Unidireccional**: La empresa A confía en el B, por lo tanto, los usuario que accedan a la Empresa A, pueden ver los recursos del B.
- **Relación Bidireccional:** La empresa A confía en la empresa B, y al revés también.
- **Relación Transitiva:** Si la empresa A confía en el B y la empresa B confía en la empresa C, los usuarios de la empresa C, podrán acceder a la empresa A.

(Si queremos hacer una relación, tendremos que configurar ambos lados. Deberemos tener las credenciales válidas en ambos dominios.)



⚠️ Una cuenta que establezca o administre las relaciones de confianza debe ser miembro del grupo **Administradores del dominio. (**Se puede hacer de forma independiente ejecutando el *Asistente para nueva confianza* primero en un dominio y luego en otro, o hacerlo a la vez, y se creará una contraseña de confianza segura automáticamente**.)**

Objetos del dominio de confianza.

Cada relación se representa con un *Objeto de Dominio de Confianza TDO (Trusted Domain Object)* que se almacena en *System*.

Los TDO son como un contrato y deben tener mínimo estos atributos:

- La transitividad (Transitiva o No Transitiva)
- La direccionalidad (Unidireccional o Bidireccional)
- El nombre de los dominios. (Empresa A y Empresa B)

Tipos de Confianza.

Podemos crear 4 tipos de relaciones de confianza usando tanto el *Asistente para nueva confianza* o la orden *Netdom:*

- **Confianza externa:** Transitivas, pueden ser unidireccionales o bidireccionales. Acceso a un dominio Windows NT o a un dominio de otro bosque.
- **Confianza de kerberos:** Confianza entre dominios de WS y dominios que usen el kerberos que no sean windows. Transitivas, no transitivas, unidireccional y bidireccional.
- **Confianza de bosque:** Compartir recursos con bosques distintos. Transitivas, unidireccionales, y bidireccionales.
- **Confianza directa:** Mejor tiempo al conectarse a dominios de árboles distintos. Transitivas, unidireccionales, y bidireccionales.

Tipos de Confianza	Descipción	Transitiva	No Transitiva	Unidireccional	Bidireccional
Confianza externa	Fácil acceso a recursos de un Windows NT 4.0.	❌	✅	✅	✅
Confianza de kerberos	Confianza usando kerberos en WS y una máquina sin windows. con kerberos.	✅	✅	✅	✅
Confianza de bosque	Compartir en diferentes bosques.	✅	❌	✅	✅
Confianza directa	Conexión a dominios de bosques distintos.	✅	❌	✅	✅

¿Con que dominios podemos establecer una relación de confianza?

- 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

Rutas de acceso a confianza.

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

Transitividad

Cuando hablamos de transitividad, significa que la relación puede extenderse más allá de los dominios que tenemos al inicio.

Confianzas Transitivas

En Windows 2000 Server, cuando creamos un dominio en un bosque existente, se crea automáticamente una relación bidireccional y transitiva entre el dominio nuevo y su padre.

Confianzas No Transitivas

Por defecto, una relación *no transitiva* es *unidireccional.*

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

RODCs: significa en inglés Read-Only Domain Controllers

⚠️ Al añadir un nuevo *Controlador de Dominio* a un *Dominio Existente*, matamos dos pájaros de un tiro. Proporcionar la tolerancia a fallos y equilibrar la carga de los servicios utilizados.

FSMO
: significa en inglés Flexible Single Master Operation