

## 9. ADMINISTRACIÓN DE ACCESO AL DOMINIO

# **CONTENIDOS**

1. Herramientas de administración
2. Tareas de administración de Active Directory

# 1. HERRAMIENTAS DE ADMINISTRACIÓN

- ▶ Usuarios y equipos de Active Directory
- ▶ Sitios y servicios de Active Directory
- ▶ Dominios y confianzas de Active Directory
- ▶ Microsoft Management Console (MMC)
- ▶ Centro de administración de Active Directory
- ▶ Módulo de Active Directory para PowerShell

# 1. HERRAMIENTAS DE ADMINISTRACIÓN

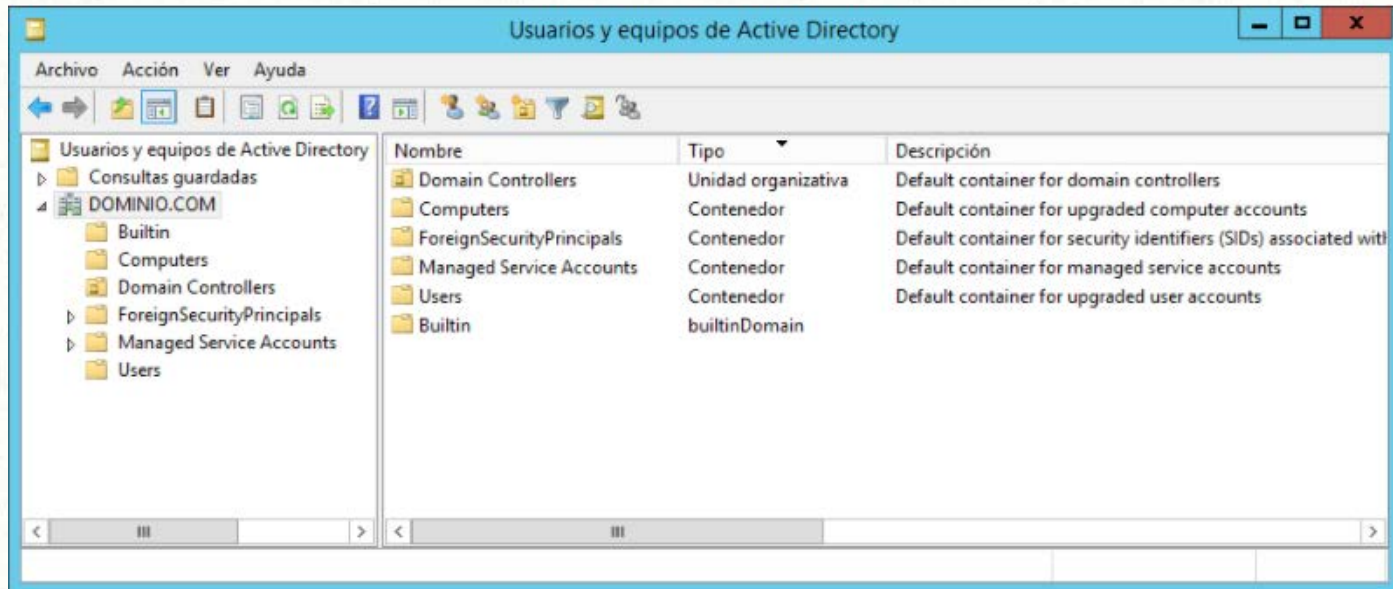
## Usuarios y equipos de Active Directory

- ▶ Crear y administrar equipos, contactos, grupos, unidades organizativas, impresoras, usuarios, ...
- ▶ Crear una cuenta de controlador de dominio de solo lectura (RODC)
- ▶ Delegar el control de tareas comunes sobre objetos Active Directory en usuarios o grupos que se especifiquen
- ▶ Transferir maestros de operaciones a nivel de dominios



# 1. HERRAMIENTAS DE ADMINISTRACIÓN

## Usuarios y equipos de Active Directory



# 1. HERRAMIENTAS DE ADMINISTRACIÓN

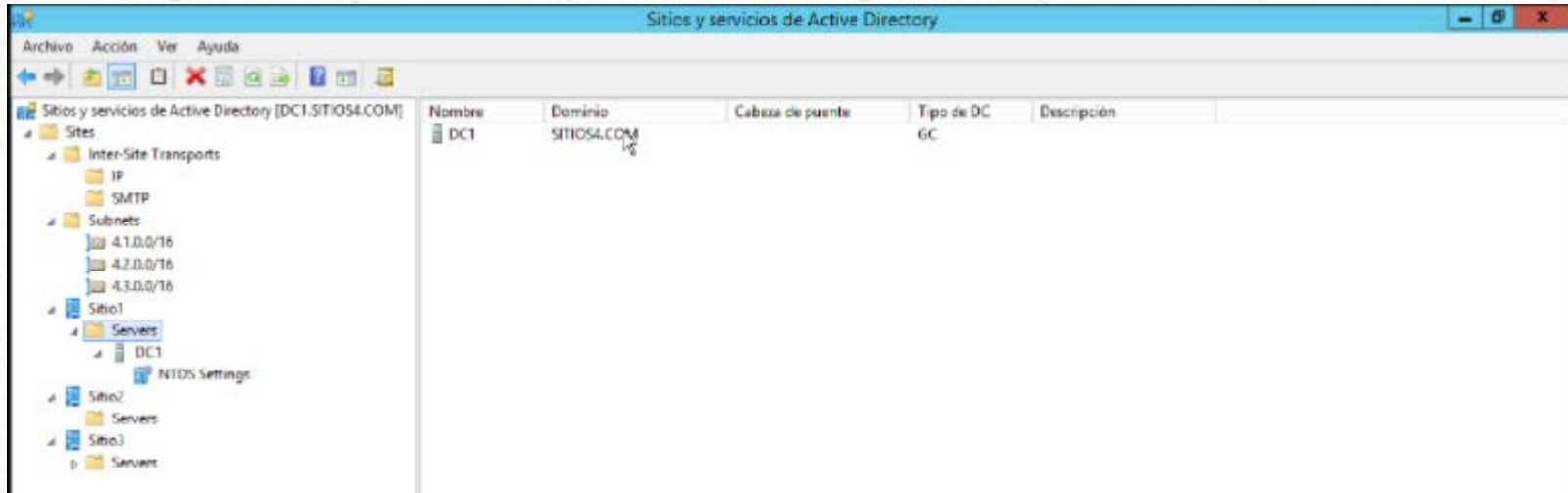
## Sitios y servicios de Active Directory

Se usa para administrar la replicación de los datos del directorio entre todos los sitios de un bosque.

- ▶ Administración de sitios  
Sitios, subredes, servidores, conexiones, vínculos a sitios, ...
- ▶ Publicación de servicios
- ▶ Referencias adicionales

# 1. HERRAMIENTAS DE ADMINISTRACIÓN

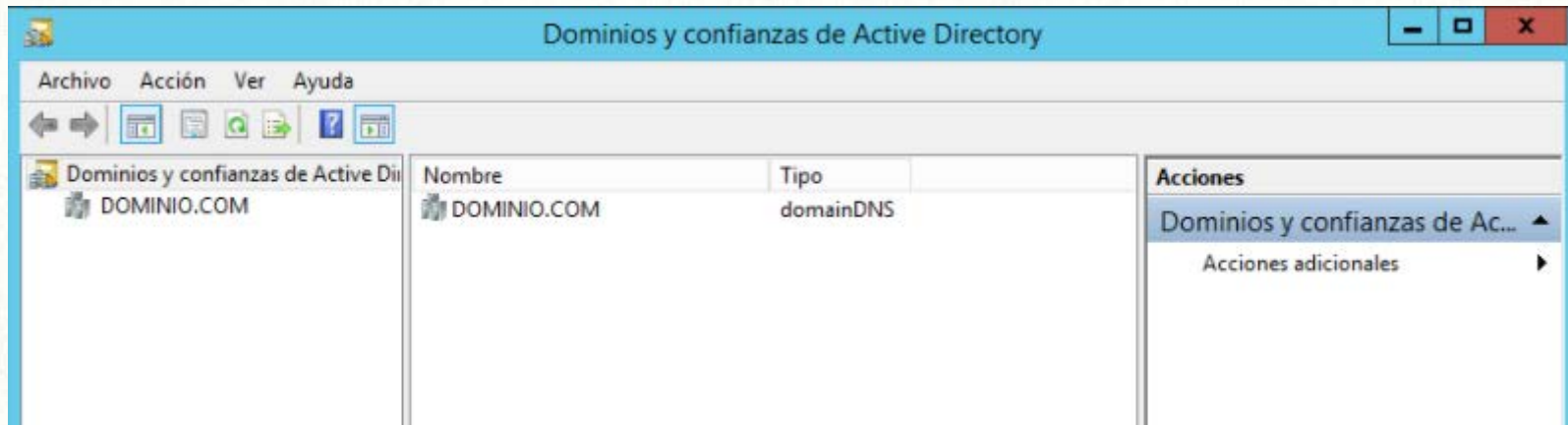
## Sitios y servicios de Active Directory



# 1. HERRAMIENTAS DE ADMINISTRACIÓN

## Dominios y confianzas de Active Directory

Se usa para administrar confianzas de dominio, niveles funcionales del bosque o el dominio y sufijos de nombre principal de usuario





# 1. HERRAMIENTAS DE ADMINISTRACIÓN

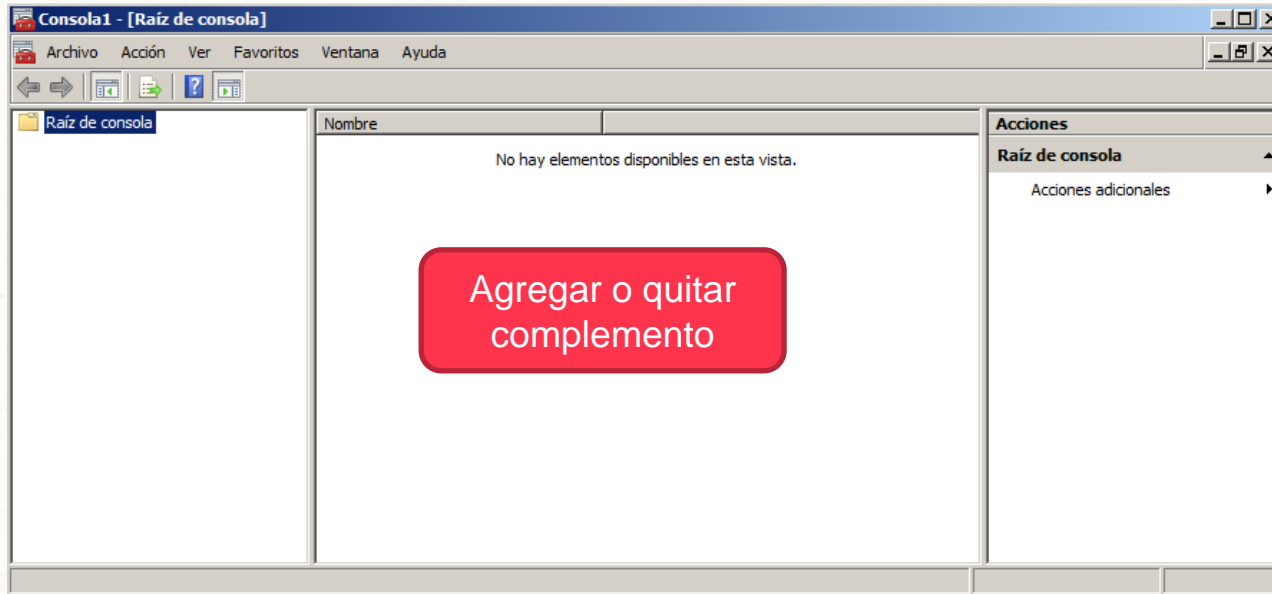
## Microsoft Management Console

Complemento de Microsoft que permite organizar y acceder a varias utilidades de Windows o incluso de otros proveedores

Permite centralizar y configurar las tareas de habituales de administración para hacerlas más accesibles

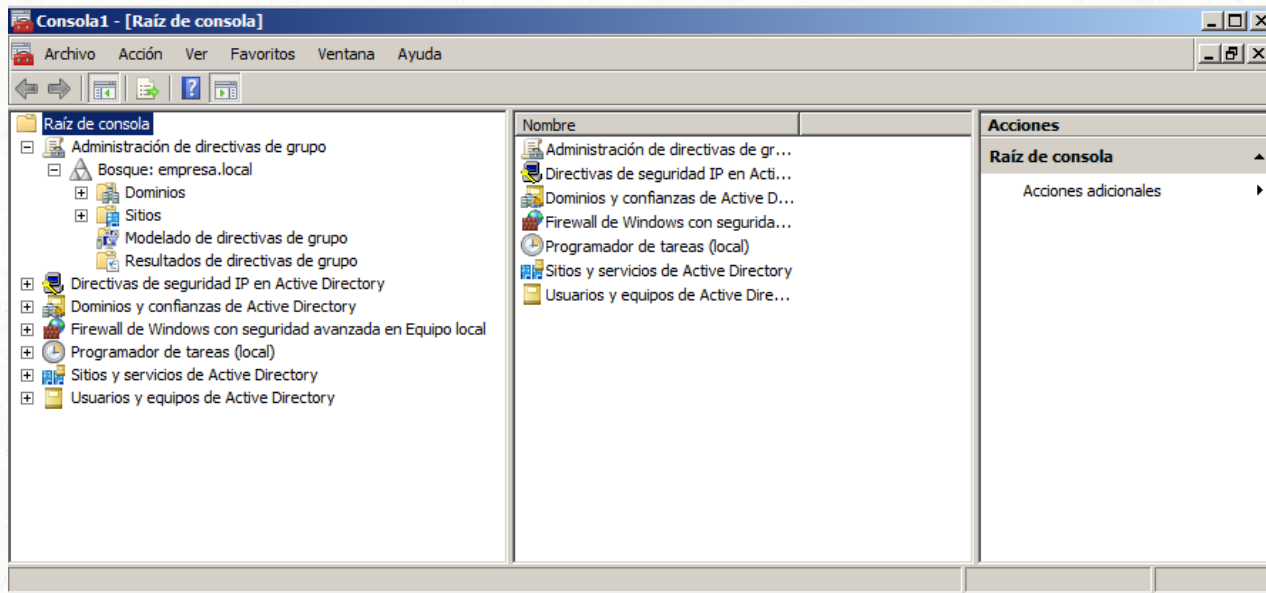
# 1. HERRAMIENTAS DE ADMINISTRACIÓN

## Microsoft Management Console



# 1. HERRAMIENTAS DE ADMINISTRACIÓN

## Microsoft Management Console



# 1. HERRAMIENTAS DE ADMINISTRACIÓN

## Centro de administración de Active Directory

Se incluye a partir de Windows Server 2008 R2.

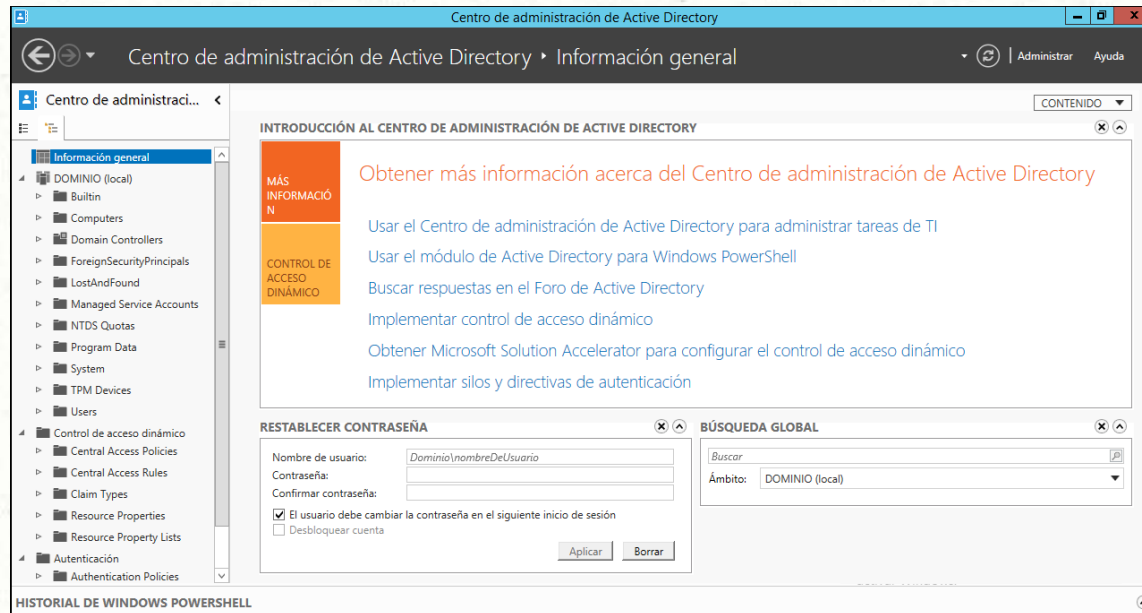
Se puede usar en lugar de mmc para realizar las tareas habituales de administración de objetos de Active Directory mediante la navegación controlada por datos y la navegación orientada por tareas.

Se puede personalizar de modo que se ajuste a los requisitos particulares de administración.



# 1. HERRAMIENTAS DE ADMINISTRACIÓN

## Centro de administración de Active Directory



# 1. HERRAMIENTAS DE ADMINISTRACIÓN

## Centro de administración de Active Directory

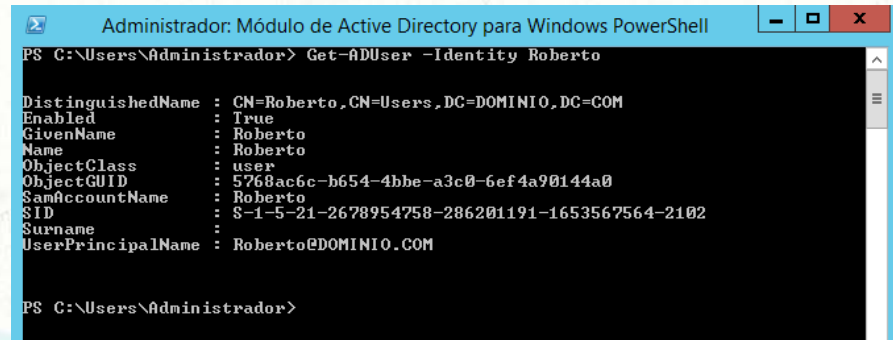
- ☐ Creación y administración de cuentas de usuario
- ☐ Creación y administración de grupos
- ☐ Creación y administración de cuentas de equipo
- ☐ Creación y administración de contenedores y unidades organizativas
- ☐ Conexión de dominios o controladores de
- ☐ Filtros de datos de Active Directory

# 1. HERRAMIENTAS DE ADMINISTRACIÓN

## Módulo de Active Directory para PowerShell

Windows PowerShell es una shell de línea de comandos y lenguaje de scripting.

Incorpora una serie de comandos para la gestión de Active Directory



```
Administrador: Módulo de Active Directory para Windows PowerShell
PS C:\Users\Administrador> Get-ADUser -Identity Roberto

DistinguishedName : CN=Roberto,CN=Users,DC=DOMINIO,DC=COM
Enabled           : True
GivenName        : Roberto
Name             : Roberto
ObjectClass      : user
ObjectGUID       : 5768ac6c-b654-4bbe-a3c0-6ef4a90144a0
SamAccountName   : Roberto
SID              : S-1-5-21-2678954758-286201191-1653567564-2102
Surname          :
UserPrincipalName : Roberto@DOMINIO.COM

PS C:\Users\Administrador>
```

# 1. HERRAMIENTAS DE ADMINISTRACIÓN

## Módulo de Active Directory para PowerShell

Ejemplos:

- Agregar un equipo al dominio:  
`netdom join /d:asir1.local PC1 /OU:Sistemas`
- Listar los usuario del dominio  
`Get-ADUSer`



# 1. HERRAMIENTAS DE ADMINISTRACIÓN

## Tarea 1. Consola de administración

- En una máquina con Windows Server 2008 abrir una consola de administración (mmc)
- Incluir, si aparecen, los siguientes complementos:
  - Usuarios y equipos de AD
  - Dominios y confianzas de AD
  - Sitios y servicios de AD
  - Directivas de seguridad IP en AD
  - Administración de directivas de grupo
  - Carpetas compartidas

## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY



### DELEGAR CONTROL DE UNID. ORGANIZATIVAS

Permite repartir las tareas de administración entre varios usuarios



### AGREGAR UN NUEVO SERVIDOR AL DOMINIO

Facilita la gestión centralizada de los servidores de mi dominio



### AÑADIR DC

Recomendable en dominios grandes para que no todo dependa de un único servidor



### REPLICACIÓN

Intercambio de información entre controladores para que todos tengan la misma información



### SITES

Configuración del dominio en función de la localización física de los elementos de dicho dominio

## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY



### MIGRAR CONTROLADOR DE DOMINIO

Cambiar por ejemplo entre un Server 2008 y un Server 2016



### DEGRADACIÓN DE DC

Cambios para que un controlador de dominio deje de serlo



### RELACIONES DE CONFIANZA

Permite que objetos de distintos dominios puedan comunicarse entre sí



### SUBDOMINIOS

Creación de un subdominio en un dominio ya creado



### CONTROLADOR DE DOMINIO DE SOLO LECTURA (RODC)

Controlador de dominio en el que no se puede modificar la BD del Active Directory

## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

### DELEGAR CONTROL DE UNIDADES ORGANIZATIVAS

- ▶ Con cuenta de Administrador y desde Usuarios y equipos de Active Directory
- ▶ Botón derecho del ratón en la unidad y seleccionar Delegar control
- ▶ Permite delegar tareas administrativas en usuarios que no tienen por qué tener permisos de administración
- ▶ Asistente de delegación



## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

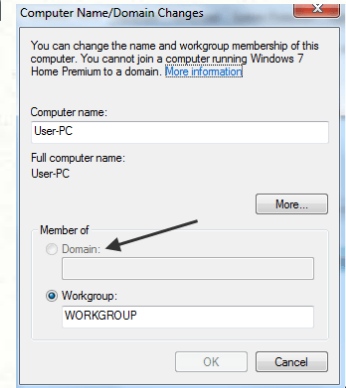
### Tarea 2. Delegar control

- En el dominio creado en la práctica 8.1 crea una nueva unidad organizativa denominada RRHH
- Desde el propio servidor verificar qué puede hacer el usuario gerente con dicha unidad organizativa
- Delegar control total de RRHH al usuario gerente
- Verificar qué puede hacer ahora el gerente en la unidad organizativa RRHH
- En Propiedades, ver los permisos sobre la unidad organizativa

## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

### AGREGAR UN NUEVO SERVIDOR AL DOMINIO

- ▶ El procedimiento es básicamente el mismo que para añadir una estación de trabajo al dominio
- ▶ Indicar el dominio en Sistema/Cambiar configuración
- ▶ Para unirse se solicitarán las credenciales de un usuario con suficientes permisos
- ▶ Reiniciar el servidor



## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

### Tarea 3. Añadir servidor

- Añadir un servidor al dominio creado en la práctica 8.1
- Se recomienda arrancar este servidor desde una máquina diferente a la que tiene el servidor con el controlador de dominio

## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

### AÑADIR CONTROLADOR DE DOMINIO

- ▶ Asignar nombre y dirección estática al controlador secundario
- ▶ Como servidor DNS principal indicar la dirección del servidor principal del dominio y como secundario la dirección del propio servidor
- ▶ Incluirlo en el dominio



## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

### AÑADIR CONTROLADOR DE DOMINIO

- ▶ Aparecerá como un equipo más del dominio
- ▶ Desde el servidor secundario instalar la función de Servicios de dominio de Active Directory
- ▶ Ejecutar el comando dcpromo y seleccionar las opciones adecuada para agregarlo al dominio existente
- ▶ Tras este proceso ya aparecerá como otro controlador de dominio

## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

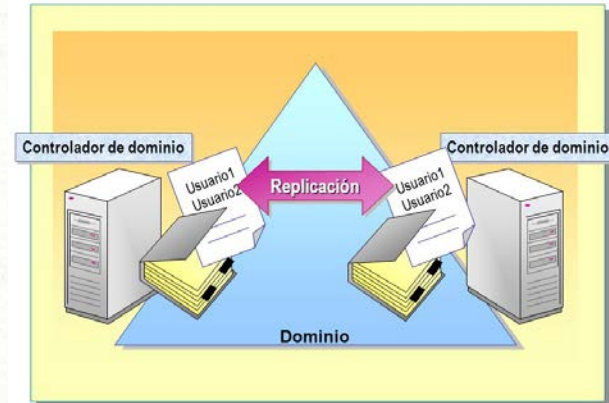
### Tarea 4. Añadir Controlador de dominio

- Realizar las tareas necesarias para que el servidor añadido al dominio en la Tarea 3 se convierta en controlador de dominio
- El dominio tendrá por tanto dos controladores de dominio
- Verificar que aparecen los dos en las herramientas de AD

## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

### REPLICACIÓN ENTRE CONTROLADORES DE DOMINIO

- ▶ Si en un dominio hay varios controladores, es necesario que la información almacenada en ellos sea la misma.
- ▶ La replicación permite que los cambios realizados en un controlador se hagan también en todos los demás controladores del dominio



## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

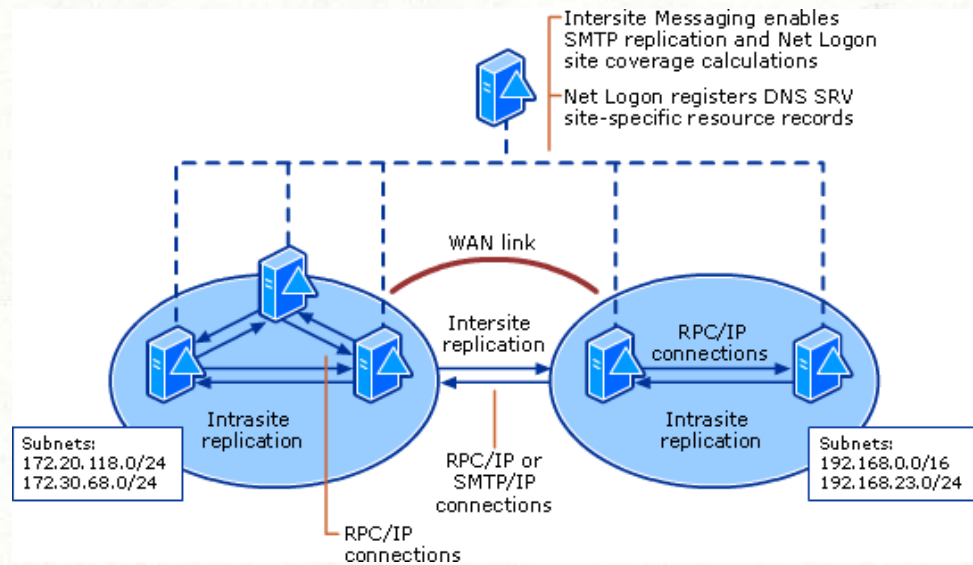
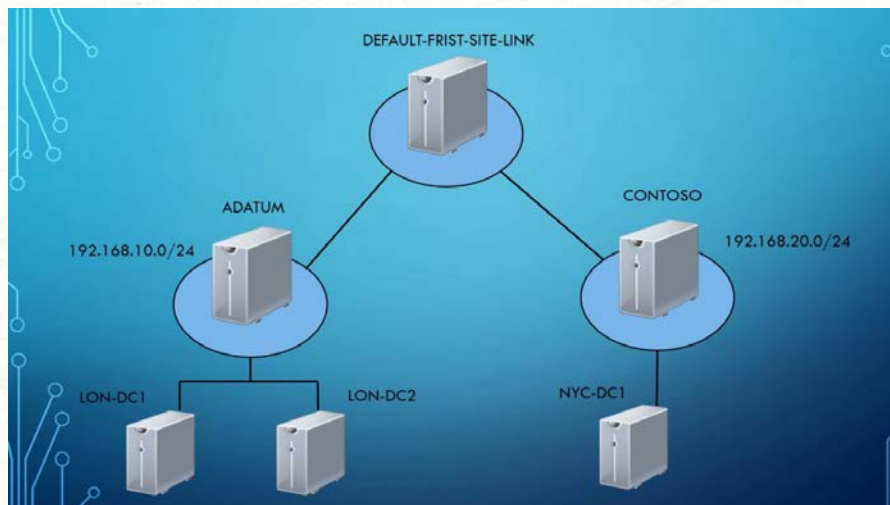
### REPLICACIÓN ENTRE CONTROLADORES DE DOMINIO

- ▶ Dos tipos de replications:
  - Entre servidores que pertenecen al mismo sitio o site (el tiempo medio de actualización es 1 minuto)
  - Entre servidores que pertenecen a sitios distintos
- ▶ Desde WS2008 R2 se puede utilizar la herramienta Replication Status Tool
- ▶ Comandos: repadmin /showrepl



## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

### REPLICACIÓN ENTRE CONTROLADORES DE DOMINIO



## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

### Tarea 5. Replicación entre DC

- Crear en el primer controlador de dominio dos unidades organizativas más, Marketing y Finanzas
- Añadir un nuevo usuario dentro de la unidad organizativa Marketing
- Verificar si estos cambios se han replicado en el segundo controlador

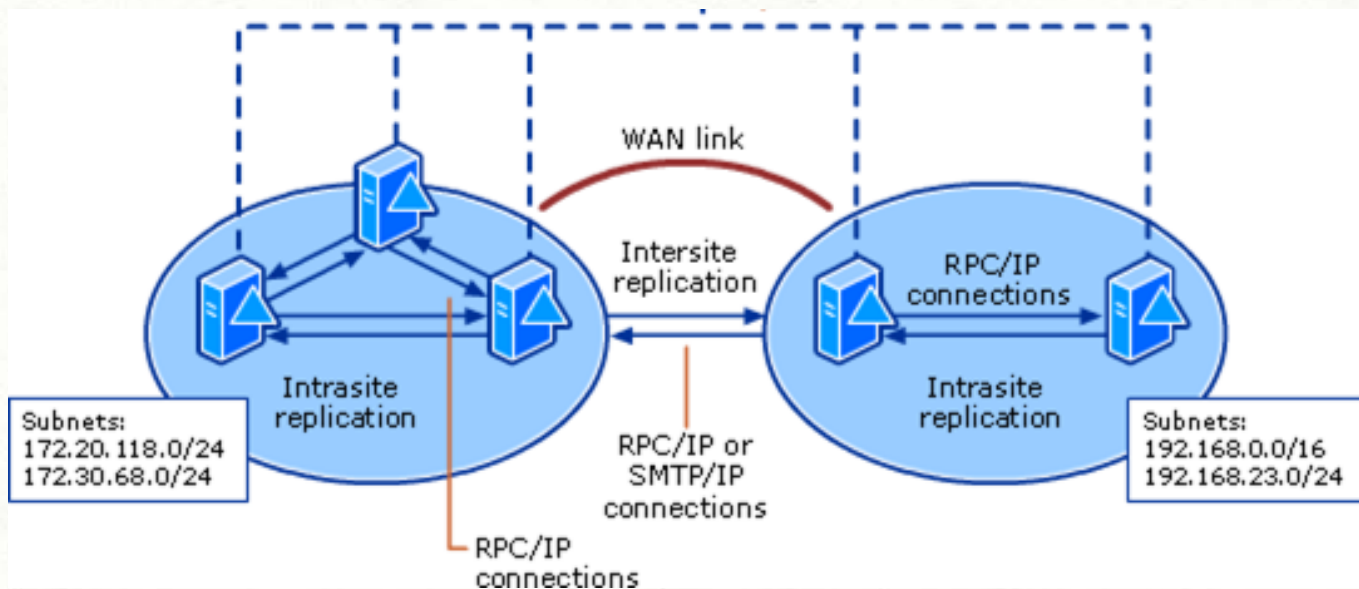
## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

### SITES

- ▶ Muy útil cuando la infraestructura de la organización está geográficamente separada o en redes distintas.
- ▶ Elementos:
  - Sites: generalmente asociados a sitios físicos, como oficinas, sucursales, delegaciones...
  - Subredes: subredes IP que tenemos configurada en cada Site. En un Site podemos tener más de una subred IP
  - Links: conexiones físicas entre los Sites.

## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

### SITES





## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

### SITES

- ▶ Dominio: representa la topología lógica de la organización
- ▶ Sites: representan la topología física de la organización
- ▶ Por defecto un bosque tiene un único site, denominado Default-First-Side-Name
- ▶ El objetivo es aumentar la eficiencia del sistema y evitar retardos en dominios situados en redes distintas

## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

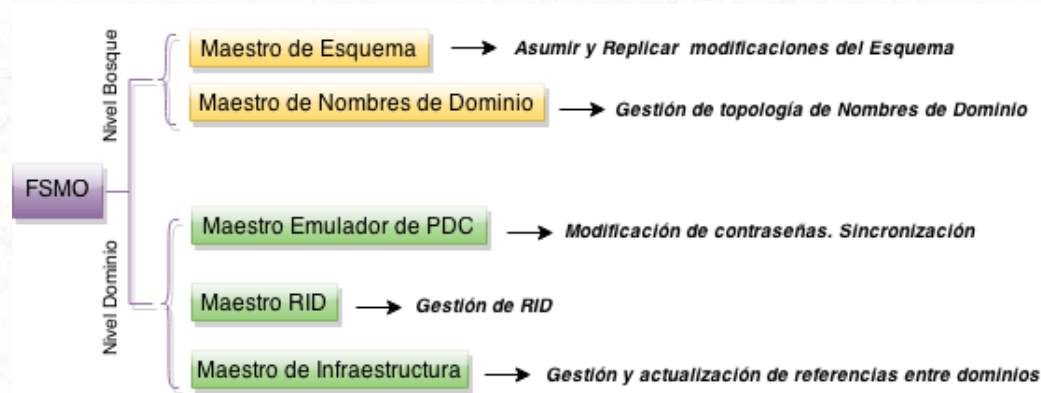
### Tarea 6. Crear diferentes sites en un dominio

- Cambiar el nombre del sitio por defecto, que será Madrid
- Crear un nuevo sitio denominado Roma
- Asignar a Roma la subred 172.15.0.0/24
- Madrid tendrá las subredes 172.15.1.0/24 y 172.15.2.0/24
- La replicación entre Madrid y Roma se hará cada 2 horas con un costo de 80 y solo de lunes a viernes, de 8:00 a 17:00

## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

### MIGRAR CONTROLADOR DE DOMINIO

- ▶ Todos los dominios de Active Directory disponen de 5 roles FSMO (Flexible Single Master Operations), que son funciones específicas realizadas por los DC.



## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

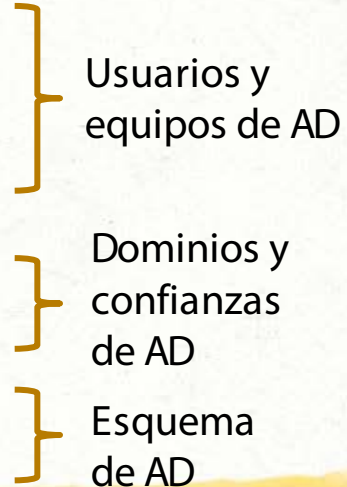
### MIGRAR CONTROLADOR DE DOMINIO

- ▶ Se puede verificar qué controlador lleva a cabo cada función con el comando:  
`netdom query /domain:nombre_dominio fsmo`
- ▶ La transferencia de roles se puede hacer mediante comandos o con la interfaz gráfica



## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

### MIGRAR CONTROLADOR DE DOMINIO

- ▶ Para migrar un controlador de dominio, se deben asignar estos roles al controlador de dominio de destino:
  - Maestro de operaciones, RID Master
  - Controlador principal de dominio, PDC Emulator
  - Infraestructura, Infrastructure Master
  - Maestro de operaciones de nomenclatura de dominios
  - Transferir el Schema Master

## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

### MIGRAR CONTROLADOR DE DOMINIO

1. Añadir el nuevo servidor al dominio
2. Asignarle una dirección IP fija. El servidor DNS será el DC
3. Promoverlo a DC
4. Verificar quién maneja los roles del dominio y cambiarlos para que sea el nuevo DC
5. Elevar el nivel funcional de bosque y dominio, si es necesario
6. Degradar DC antiguo

## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

### Tarea 7. Migrar controlador de dominio

Video migración WS2008 a WS2016

## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

### DEGRADACIÓN DE CONTROLADORES DE DOMINIO

- ▶ Proceso que convierte un controlador de dominio en un simple servidor miembro del dominio
- ▶ Requiere credenciales de administrador del dominio
- ▶ Si es el único DC se borrará también el dominio (siempre que no haya ningún subdominio que dependa de él)
- ▶ Esta operación en principio no elimina las herramientas de AD



## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

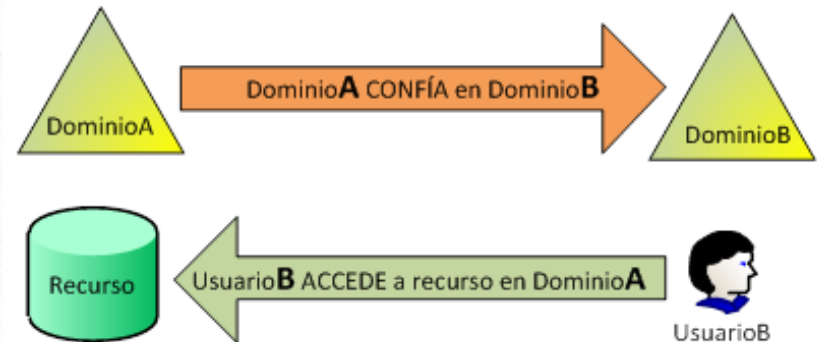
### Tarea 8. Degradar controlador de dominio

- Acceder al último controlador de dominio incluido en la Tarea 4 y degradarlo de manera que deje de funcionar como controlador de dominio
- ¿Sigue perteneciendo al dominio?

## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

### RELACIONES DE CONFIANZA

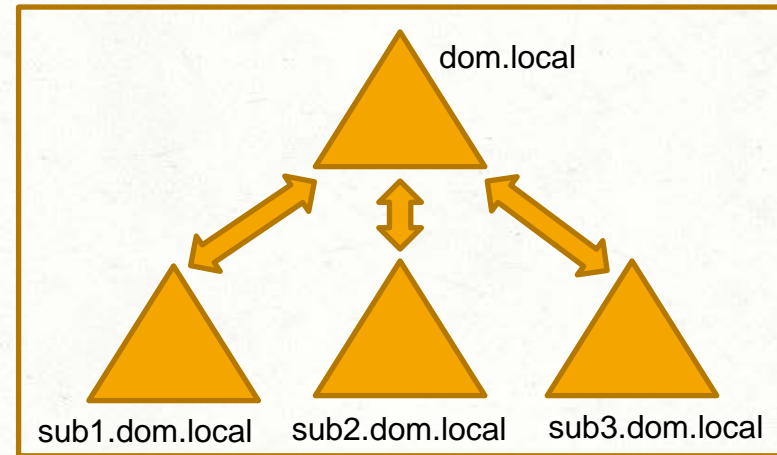
- ▶ Relación entre dominios que permite compartir recursos entre dominios
- ▶ Ambos dominios deben aceptar la relación (A confía en B y B acepta esa confianza)
- ▶ Puede ser bidireccional o no (que A confíe en B y que B confíe en A)



## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

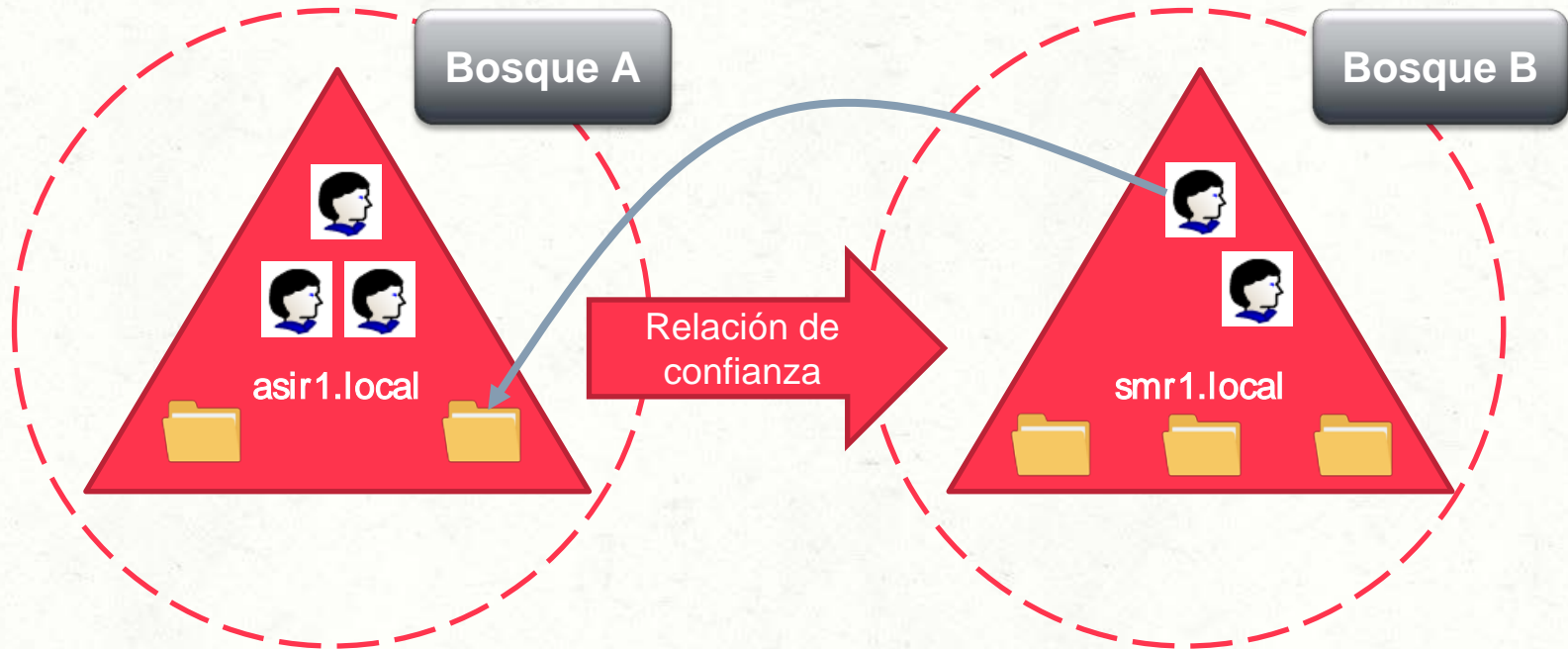
### RELACIONES DE CONFIANZA

- ▶ En el caso de subdominios las relaciones de confianza se establecen automáticamente, no se pueden borrar y son bidireccionales
- ▶ Además son transitivas (si "hijo1" confía en "padre" y "padre" confía en "hijo2" entonces "hijo1" confía en "hijo2")



## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

### RELACIONES DE CONFIANZA





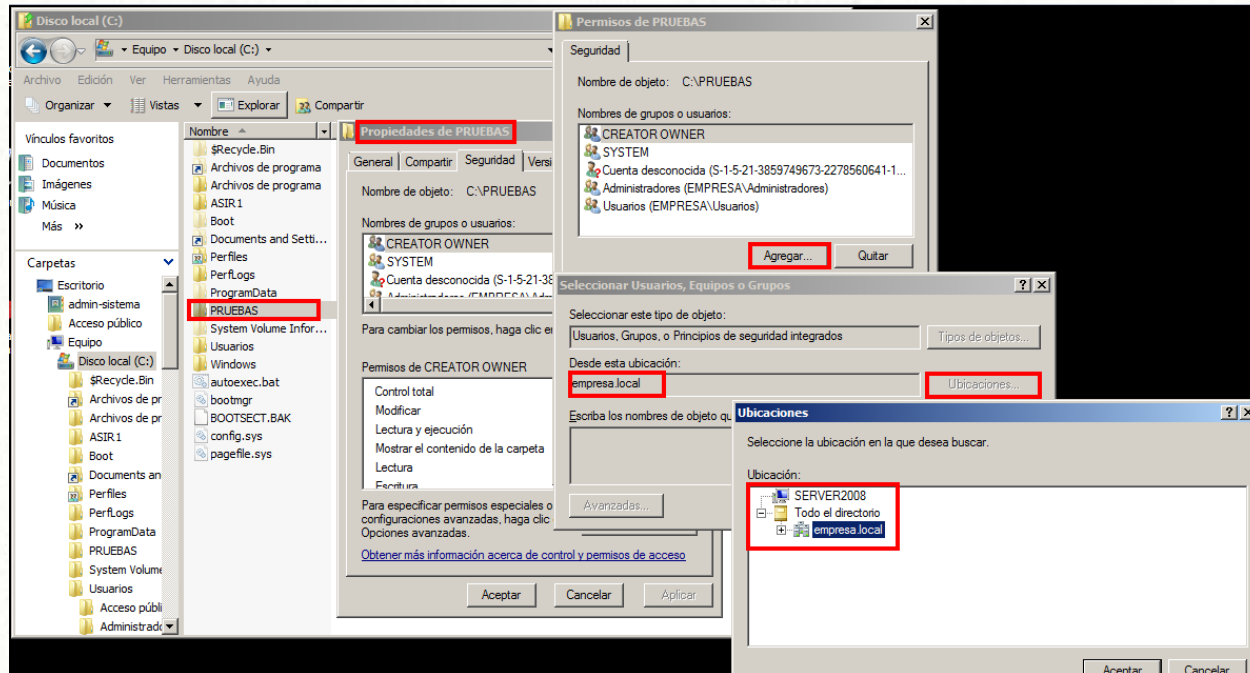
## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

### RELACIONES DE CONFIANZA

1. Modificar el DNS del DC para que pueda resolver los nombres del dominio sobre el que se quiere establecer una relación de confianza (Reenviadores condicionales)
2. Establecer la relación de confianza en la herramienta Dominios y confianzas de Active Directory
3. Esto se hace a través de un asistente que establece el tipo de relación (bidireccional o no, de dominio o de bosque, con todos los usuarios del dominio o no)

## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

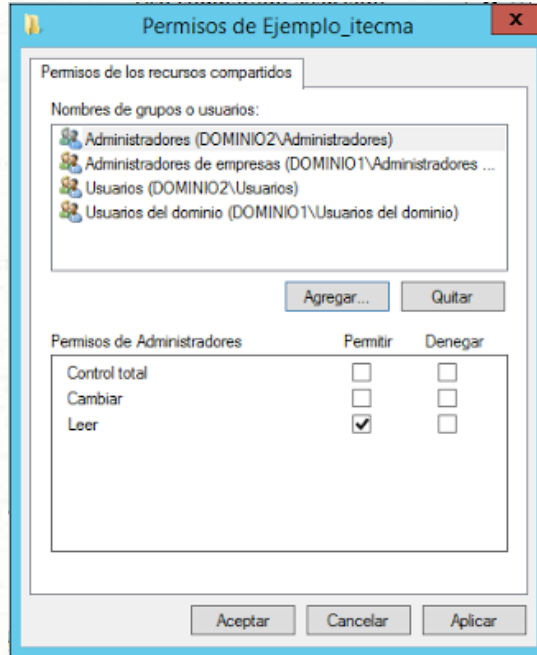
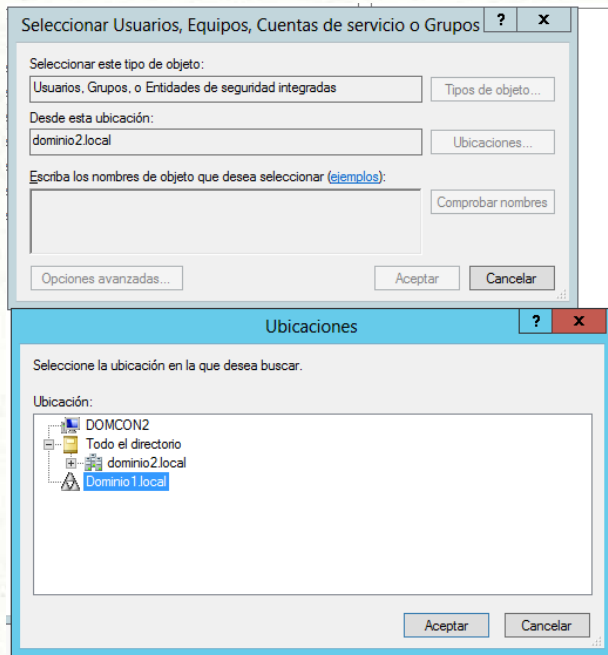
### RELACIONES DE CONFIANZA



Por defecto solo se pueden asignar permisos a usuarios o grupos del dominio local.

## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

### RELACIONES DE CONFIANZA



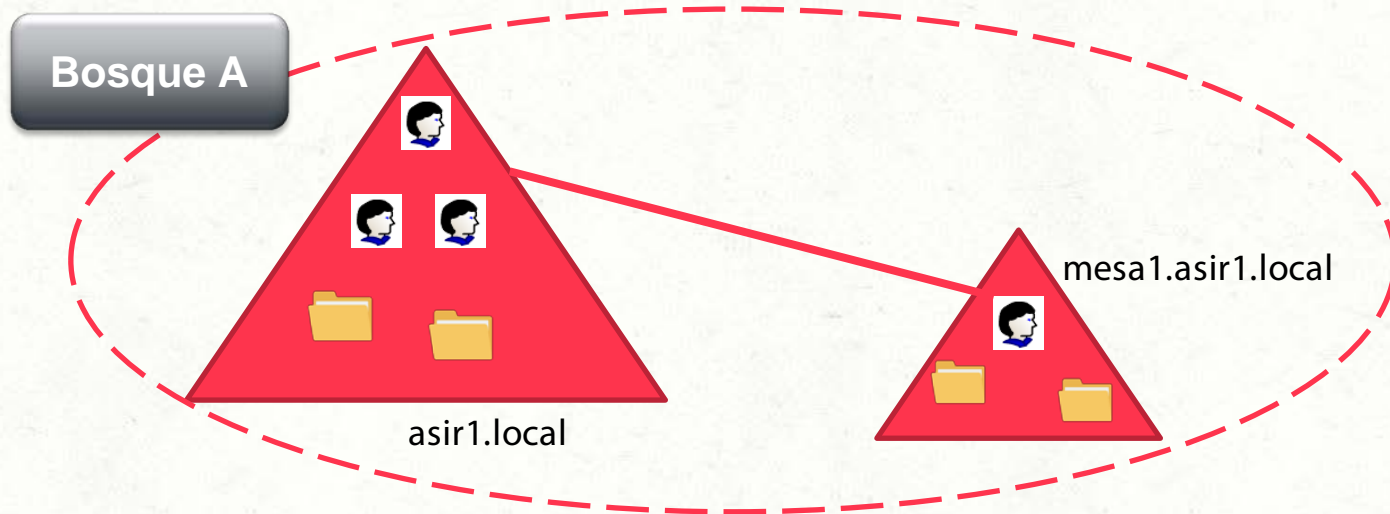
Cuando hay una relación de confianza entre dominios, se puede elegir compartir recursos con usuarios/grupos que están en otro dominio.

En este ejemplo, se va a compartir un recurso de dominio2.local con algún usuario o grupo de dominio1.local

## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

### SUBDOMINIOS

El objetivo es una estructura como la siguiente:





## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

### SUBDOMINIOS

- ▶ De forma implícita se establece una relación de confianza bidireccional entre el dominio y el subdominio
- ▶ En el subdominio tiene que haber un servidor con AD instalado y promocionado a DC
- ▶ Dicho servidor debe apuntar como servidor DNS al DC del dominio principal para poder resolver los nombres
- ▶ En el proceso de promoción, seleccionar la opción de Agregar dominio a un bosque existente

## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

### Tarea 9. Crear un subdominio

- En la Tarea 8 hemos degradado un controlador de dominio. Si estuviera todavía en el dominio, sacarlo de él
- Crear un subdominio en el dominio creado en la práctica 8.1 utilizando el servidor anterior. Verificar que aparece en Dominios y confianzas de Active Directory
- Crear un usuario dentro del subdominio
- En el dominio principal, compartir una carpeta con dicho usuario y comprobar que accede correctamente (otro cliente)

## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

### CONTROLADOR DE DOMINIO DE SOLO LECTURA (RODC)

- ▶ Se trata de un DC que contiene una copia de solo lectura de la base de datos de Active Directory, salvo contraseñas
- ▶ No se pueden cambiar los datos del AD aun teniendo acceso físico al controlador
- ▶ Útil cuando es difícil proporcionar protección física al servidor con rol de DC

## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

### CONTROLADOR DE DOMINIO DE SOLO LECTURA (RODC)

- ▶ No replica datos. Solo recibe las copias de otros DC (replicación unidireccional)
- ▶ Al recibir una solicitud de autenticación la reenvía al DC más cercano (RWDC)
- ▶ Almacena algunas credenciales en caché para trabajar de forma más rápida
- ▶ Se debe poner como servidor DNS el RWDC más cercano



## 2. TAREAS DE ADMINISTRACIÓN DE ACTIVE DIRECTORY

### CONTROLADOR DE DOMINIO DE SOLO LECTURA (RODC)

