**GUÍA COMPLETA DE CONMUTACIÓN Y RECUPERACIÓN DE CONTROLADOR DE DOMINIO (FSMO)**

**Proyecto IPVCSI – Sedes Castellón y Madrid**

**Infraestructura del Dominio**

| **Rol** | **Nombre de equipo** | **IP** | **Ubicación** | **Estado inicial** |
| --- | --- | --- | --- | --- |
| Controlador de dominio principal (FSMO) | srv-ad1 | 10.20.10.11 | Castellón | Activo |
| Controlador de dominio de respaldo | srv-ad2 | 10.30.10.11 | Madrid | Replicado |

**Objetivo del Procedimiento**

Simular la caída del controlador de dominio principal (srv-ad1) y garantizar que srv-ad2 asuma la autenticación de usuarios.  
Además, si srv-ad1 no va a volver en corto plazo, srv-ad2 deberá **asumir los roles FSMO** temporalmente.  
Cuando srv-ad1 se recupere, deberá **recuperar los roles FSMO** y continuar como principal.

**Escenario 1 – Caída temporal sin transferir FSMO**

Este escenario **no requiere tomar los roles FSMO**, ya que la caída es breve. Sirve para verificar que srv-ad2 puede mantener el servicio:

**1 Apagar srv-ad1**

* Desde VirtualBox, apaga srv-ad1 (o desconecta su tarjeta de red).

**2 Comprobaciones desde srv-ad2**

En srv-ad2, abrir PowerShell y ejecutar:

nltest /dclist:ipvcsilocal.lan

echo %logonserver%

whoami /all

🔹 Esto verifica que srv-ad2 está autenticando usuarios correctamente.

**3 Encender srv-ad1 y verificar replicación**

* Inicia srv-ad1 nuevamente.
* Ejecuta en PowerShell:

repadmin /replsummary

repadmin /syncall /APeD

* Verifica conectividad DNS con:

nslookup srv-ad2

ping srv-ad2

* Confirma que los roles FSMO siguen en srv-ad1 con:

netdom query fsmo

**Escenario 2 – Caída prolongada: Toma forzada de roles FSMO**

⚠ Este procedimiento **solo debe realizarse si srv-ad1 no va a recuperarse a corto plazo**. Se forzará a srv-ad2 a asumir los roles FSMO de forma definitiva.

**FASE 1: Transferencia forzada de roles FSMO a srv-ad2**

En srv-ad2, abre CMD como administrador:

ntdsutil

roles

connections

connect to server srv-ad2

quit

seize naming master

seize schema master

seize rid master

seize pdc

seize infrastructure master

quit

quit

Esto fuerza a srv-ad2 a asumir **todos los roles FSMO**.  
Puedes confirmar con:

netdom query fsmo

**Escenario 3 – srv-ad1 vuelve y debe recuperar los FSMO**

⚠ Asegúrate de que srv-ad1 está sincronizado y replicando correctamente antes de devolverle los roles.

Para ello ejecutamos desde srv-ad1 en PowerShell repadmin /syncall /AdeP

**FASE 2: Restaurar FSMO a srv-ad1**

En srv-ad1, abre PowerShell como administrador:

ntdsutil

roles

connections

connect to server srv-ad2

quit

seize naming master

seize schema master

seize rid master

seize pdc

seize infrastructure master

quit

quit

🔹 Con esto, srv-ad1 vuelve a ser el titular de los roles FSMO.

🔹 Verifica el resultado con:

netdom query fsmo

**📌 Recomendaciones Finales**

* Verifica siempre que los **relojes están sincronizados** con NTP (w32tm /query /status) en ambos DCs.
* Asegúrate de que **DNS** funciona correctamente entre ambos DCs.
* Usa repadmin /showrepl y dcdiag para diagnósticos adicionales.

## ****Resumen de Comandos Útiles****

| **Comando** | **Descripción** |
| --- | --- |
| nltest /dclist:dominio | Ver controladores de dominio disponibles |
| echo %logonserver% | Ver DC que atiende a un cliente |
| repadmin /replsummary | Ver estado de replicación global |
| repadmin /syncall /APeD | Forzar replicación |
| netdom query fsmo | Ver roles FSMO actuales |
| w32tm /query /status | Ver estado del servicio horario |
| whoami /all | Ver tokens de autenticación |