SysArmorTech

Hardening y Mantenimiento de Active Directory

Caso real de migraciòn crítica y modernizaciòn en menos de 2 horas

Caso real de migración crítica de Active Directory

Cómo reemplazar un controlador de dominio defectuoso y modernizar la infraestructura minimizando la indisponibilidad

Guía técnica para administradores e ingenieros de infraestructura

Alfredo Arévalo
Infrastructure & Systems Engineer

Edición 2026 · Versión 1.0

Nota de Descargo: Los scripts presentados en esta guía han sido **probados previamente en entornos de producción reales** y posteriormente **ajustados y personalizados** de acuerdo con las necesidades específicas de la infraestructura en la que se aplicaron. Se recomienda ejecutar siempre las **pruebas de diagnóstico en un entorno de homologación** antes de su despliegue definitivo, con el fin de validar compatibilidad y minimizar riesgos.

Contenido

Introducción

Bienvenido a la Guía de Campo

Administrar la plataforma de identidad corporativa en entornos modernos requiere más que seguir asistentes de instalación con interfaz gráfica. En arquitecturas híbridas donde conviven controladores de dominio tradicionales con infraestructura en la nube (como Microsoft Azure), los ingenieros de sistemas nos enfrentamos a desafíos reales: inconsistencias en la replicación DFSR, bloqueos de herencia innecesarios en Directivas de Grupo (GPO), conflictos de capa física/enlace en el direccionamiento IP y la exigencia de cifrar el tráfico de autenticación mediante LDAPS sin comprometer la operación.

Este documento no es un manual teórico sobre las definiciones de Active Directory. Es una **memoria técnica y un compendio de procedimientos ejecutados con éxito**, orientados a eliminar la deuda técnica acumulada en la infraestructura, optimizar el rendimiento de autenticación en controladores **Windows Server 2025** y automatizar las tareas repetitivas mediante PowerShell bajo principios de *Clean Code* y *Clean Infrastructure*.

Al finalizar esta guía, contarás con una suite de scripts y una metodología clara para auditar, asegurar y validar la salud integral de tu dominio con estándares de nivel *Enterprise*.

Objetivo General

Proporcionar a los administradores e ingenieros de TI una guía metodológica y una batería de automatizaciones en PowerShell para ejecutar migraciones, auditorías de GPOs y aseguramiento de Active Directory sobre Windows Server 2025, **minimizando el riesgo de interrupción y reduciendo la ventana de indisponibilidad**.

Objetivos Específicos

1. **Automatizar el Despliegue:** Implementar la instalación y promoción desatendida de nuevos Controladores de Dominio utilizando PowerShell para estandarizar la infraestructura.
2. **Eliminar Deuda Técnica en GPOs:** Identificar y sanear políticas vacías, bloqueos de herencia incorrectos y desalineaciones en la replicación SYSVOL/DFSR para optimizar el tiempo de inicio de sesión (*Fast Link*).
3. **Asegurar la Capa de Autenticación:** Desplegar el protocolo LDAP sobre SSL/TLS (LDAPS) exportando la cadena de confianza correcta mediante la Entidad Certificadora (CA) institucional.
4. **Validación de Salud Operativa:** Diagnosticar la estabilidad del dominio mediante pruebas de conectividad en puertos críticos, registros SRV en DNS y la interpretación de eventos clave de seguridad.

Capítulo 1: El Nuevo Estándar: Windows Server 2025 en la Infraestructura Enterprise

Novedades Claves para el Administrador de Sistemas en Windows server 2025

- **Actualización local desde Windows Server 2012 R2**: Se puede actualizar directamente a Windows Server 2025 desde Windows Server 2012 R2 y/o versiones posteriores, esto parece simple pero que significa realmente que puede actualizar hasta cuatro versiones a la vez.

- **Mejoras en el Motor de Active Directory:** El tamaño de página de la base de datos pasó de 8KB a 32KB (OPTIONAL feature/Database Page Size), permitiendo un rendimiento superior en consultas complejas, en resumen, el directorio activo en Windows Server 2025 ahora es como una agenda más grande, con un buscador más rápido y con candados más seguros para proteger la información, donde las organizaciones pueden trabajar con más datos, encontrarlos enseguida y mantenerlos protegidos automáticamente.

- **Fortalecimiento Criptográfico y Cierre de Puertos Inseguros:** Bloqueo de protocolos obsoletos por defecto, refuerzo en el canal Kerberos y soporte extendido de cifrado para LDAP/LDAPS, para entenderlo más fácilmente Windows Server 2025 refuerza sus candados digitales y cierra las puertas débiles que nadie usa. Así, la información está más protegida y los atacantes tienen menos formas de entrar.

- **Integración Nativa Híbrida con Azure:** Capacidades mejoradas para sincronización de identidades, gestión de parches en caliente (***Hotpatching***) y conectividad segura con VNETs. Esto en que nos ayuda realmente Windows Server 2025 nos da la ventaja que se conecta con la nube de Azure: para que las actualizaciones se instalan sin apagar el sistema y los datos viajan de forma privadas y seguras, buscando que el trabajar sea más fácil, rápido y protegido.
- **Sustituto de la Replicación Antigua:** Consolidación definitiva de **DFSR** para la carpeta SYSVOL, eliminando completamente rastros del viejo motor FRS, simplificando mucho podemos decir antes, Active Directory usaba un mensajero viejo y lento para mantener sincronizados los manuales internos. Ahora,

Windows Server 2025 usa un servicio moderno que asegura que todas las copias estén actualizadas y elimina por completo el sistema antiguo. Es más rápido, seguro y confiable."

- **Cuenta de servicios gestionados delegada (dMSA):** Las cuentas de servicio gestionadas delegadas (dMSA) en Windows Server 2025 son una evolución de las cuentas de servicio tradicionales: eliminan la necesidad de manejar contraseñas manualmente, las rotan automáticamente y vinculan la autenticación a la identidad del dispositivo, ofreciendo mayor seguridad y control, estas cuentas podemos decir que son como llaves digitales inteligentes que solo funcionan en la máquina correcta. No necesitan que alguien cambie la contraseña porque se actualizan solas, y además dejan un registro claro de todo lo que hacen. Esto hace que los servicios críticos funcionen de manera más segura y confiable.

- **Solución de contraseña de administrador local de Windows:** LAPS (Local Administrator Password Solution) es una herramienta de Microsoft que ayuda a proteger las cuentas de administrador locales en los equipos de una organización. Para explicarlo mejor LAPS es como tener un candado diferente, pero muy fuerte en cada computadora de la empresa. El sistema cambia esas llaves automáticamente y las guarda en una caja fuerte digital a la que solo los administradores tienen acceso. Así, si alguien roba una llave, no puede entrar a los otros equipos.

Nota de Ingeniero: Al analizar las **novedades en seguridad** y las **mejoras que ofrece Windows Server 2025**, identifiqué una oportunidad para optimizar la infraestructura de controladores de dominio existente. El objetivo fue encontrar la forma más **sencilla, eficiente y segura** de realizar la migración hacia esta nueva versión, altamente recomendable por sus **avances críticos en rendimiento, protección y administración de Active Directory**. Windows Server 2025 elimina tecnologías obsoletas y refuerza la defensa frente a **amenazas modernas**, permitiendo a los administradores implementar un entorno más **robusto, confiable y preparado para el futuro**.

Capítulo 2: Escenario Real y Diagnóstico de la Problemática

En este caso real, un controlador de dominio con fallos graves de replicación fue reemplazado por una instalación limpia de Windows Server 2025. Gracias a una planificación detallada, logramos mantener el mismo nombre e IP y reducir la indisponibilidad a menos de 2 horas o menos. La migración eliminó errores críticos y modernizó la infraestructura, garantizando estabilidad y seguridad.

En la infraestructura original, uno de los controladores de dominio (**DCRepa3**) presentaba **fallos graves de replicación**, afectando la sincronización de objetos y políticas entre los sitios. Esto generaba:

- Retrasos en la autenticación de usuarios remotos.
- Errores de replicación en el sitio de respaldo (**IDC Respaldo**).
- Riesgo de pérdida de coherencia en el catálogo global.

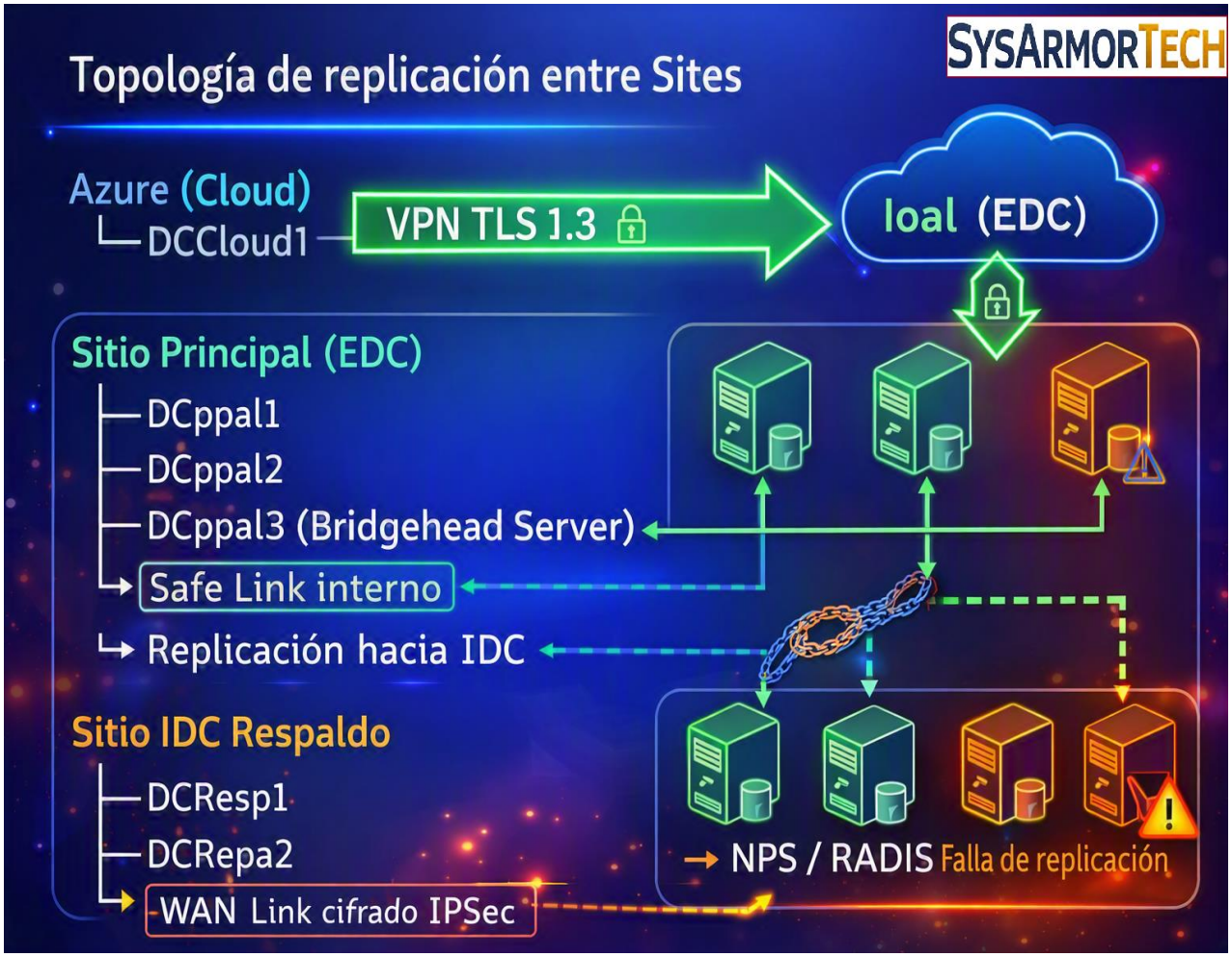
La causa raíz se relacionó con una instalación antigua de Windows Server 2016 que acumulaba inconsistencias en el **SYSVOL** y el **NTDS**, además de conflictos de FSMO.

2.1. Descripción de la Topología Híbrida

Nota de privacidad: Los nombres de servidores, sitios y controladores han sido modificados para proteger la identidad de la organización.

La arquitectura estaba distribuida de la siguiente manera, tres sitios:

- **Azure (Cloud):** 1 DC (**DCCloud1**) conectado por **VPN segura**.
- **Sitio Principal (EDC):** 3 DCs (**DCppal1**, **DCppal2**, **DCppal3**) enlazados por **Safe Link** interno.
- **Sitio IDC Respaldo:** 3 DCs (**DCResp1**, **DCRepa2**, **DCRepa3**) conectados por **WAN Link cifrado (IPSec)**.



El controlador afectado (**DCRepa3**) cumplía funciones críticas de **NPS/RADIUS**, por lo que su indisponibilidad impactaba la autenticación de red.

2.2. Deudas Técnicas Identificadas

- **Acumulación de GPOs Ineficientes:** Políticas vacías, configuraciones redundantes y el uso desmedido de *Enforced* para omitir bloqueos de herencia mal diseñados.
- **Inconsistencias de Red (ACD / DHCP):** El fenómeno de las direcciones IP marcadas como *(Duplicado)* y las reservaciones *Inactivas* tras la creación de adaptadores virtuales o cambios de direccionamiento.
- **Necesidad de Cifrado LDAPS:** El requerimiento operativo de asegurar la autenticación sobre el puerto 636 sin exponer credenciales ni claves privadas en la red.

2.3. Levantamiento de información

Problemática:

Durante las revisiones al controlador de dominio DCRepa3, se detectó un problema adicional: este servidor tenía asignados tres roles FSMO (probablemente PDC Emulator, RID Master e Infrastructure Master). Como ocurre en muchas organizaciones, algunas aplicaciones están configuradas para depender directamente del nombre o la dirección IP del servidor. En caso de reemplazarlo, es fundamental identificar qué aplicaciones lo referencian, ya que muchas de ellas ya no cuentan con soporte para realizar ajustes o redirecciones hacia otro controlador de dominio. Esta fue la razón principal por la que se decidió mantener el mismo nombre y la misma IP durante la reinstalación.

Tras ejecutar varios comandos de diagnóstico, se evidenció que las actualizaciones anteriores del sistema operativo en los controladores de dominio no se habían realizado de forma limpia, sino directamente sobre la versión existente. Esto generó acumulación de errores previos, lo que hizo crítica la limpieza completa antes del reemplazo.

Riesgos Principales:

- Conflictos de SPN (Service Principal Name): Si el nombre del servidor se duplica en la red antes de eliminar correctamente el anterior, el protocolo Kerberos fallará.
- USN Rollback: Una replicación mal gestionada puede provocar una base de datos de Active Directory inconsistente.
- Errores heredados: Si el error está a nivel de base de datos de AD, promover un nuevo controlador sin una limpieza adecuada replicará el problema al nuevo equipo.

2.4. Hoja de Ruta Sugerida

El objetivo fue ejecutar este procedimiento paso a paso, asegurando que la transición se realizara de forma exitosa y que las aplicaciones no percibieran cambios.

- **Saneamiento previo**
  - Ejecutar dcdiag /v en el servidor antiguo.
  - Si se detectan errores graves de replicación, corregirlos antes de promover el nuevo controlador; de lo contrario, se trasladarán problemas heredados a la nueva instalación.

Que se busca corregir con esta hoja de ruta

- Migraciones a Windows Server 2025.
- Errores de replicación DFSR y registros duplicados.
- Implementación rápida de LDAPS sin romper producción.
- Limpieza de deudas técnicas y auditoría con PowerShell.

- **Preparación del nuevo servidor**
  - Instalar **Windows Server 2025** con un nombre y dirección IP temporales.
  - Ejecutar adprep /domainprep / adprep /domainprep /gpprep
  - Promoverlo como **Controlador de Dominio** dentro del sitio existente.
  - Permitir que replique completamente durante al menos **24–48 horas** para garantizar consistencia.

- **Transferencia de roles FSMO**

Con este script de powershell se validó como estaba distribuidos los roles FSMO en los controladores

```
# Definimos los roles FSMO para comparar
$DomainRoles = Get-ADDomain | Select-Object PDCEmulator, RIDMaster, InfrastructureMaster
$ForestRoles = Get-ADForest | Select-Object SchemaMaster, DomainNamingMaster

Get-ADDomainController -Filter * | Select-Object `
    Name,
    IPv4Address,
    OperatingSystem,
    Site,
    @{Name="Roles_FSMO"; Expression={
        $roles = @()
        if ($_.Name -eq ($DomainRoles.PDCEmulator -split '\.')[0]) { $roles += "PDC" }
        if ($_.Name -eq ($DomainRoles.RIDMaster -split '\.')[0]) { $roles += "RID" }
        if ($_.Name -eq ($DomainRoles.InfrastructureMaster -split '\.')[0]) { $roles += "Instructure" }
        if ($_.Name -eq ($ForestRoles.SchemaMaster -split '\.')[0]) { $roles += "Schema" }
        if ($_.Name -eq ($ForestRoles.DomainNamingMaster -split '\.')[0]) { $roles += "Naming" }
        $roles -join ", "
    }} | Format-Table -AutoSize
```

Migrar los tres roles críticos al nuevo servidor mientras ambos están activos, se recomienda usar el cmdlet, Por PowerShell para mayor seguridad y control

Move-ADDirectoryServerOperationMasterRole

- **El "Gran Cambio" (ventana de mantenimiento)**

Apagar el servidor antiguo (sin despromoverlo aún, para tener opción de revertir si es necesario).

En el servidor nuevo:

- Cambiar la **IP** por la del servidor anterior.
- Renombrar el **host** con el nombre del servidor anterior (requiere reinicio).
- Verificar los registros **DNS** y confirmar que el **GUID del objeto NTDS** coincida correctamente.

Tabla de Verificación Crítica

Elemento	Acción
DNS	Asegúrate de que el nuevo servidor apunte a otro DC para DNS mientras se configura.
Catálogo Global	Asegúrate de que el nuevo sea Catálogo Global (GC) antes de apagar el viejo.
Metadata Cleanup	Si el viejo no vuelve, deberás hacer un ntdsutil para borrar los restos del viejo del AD.

Capítulo 3: Automatización del Despliegue con PowerShell (Clean Infrastructure)

3.1. Instalación Desatendida de AD DS

Fue necesario instalar un nuevo servidor con un nombre e IP temporales, garantizando que estuviera en la misma VLAN para evitar problemas de comunicación durante el cambio. En lugar de depender de la interfaz gráfica, se optó por PowerShell, lo que permitió:

Ventajas de este enfoque respecto a la interfaz gráfica (GUI)

1. Repetibilidad: Elimina el error humano en la selección de OUs o configuraciones de DNS.
2. Estandarización: Garantiza que las rutas de base de datos (NTDS) y logs se mantengan estandarizadas en toda la granja de servidores.
3. Eficiencia de tiempo: Reduce el tiempo de aprovisionamiento de un DC a menos de 5 minutos.

Ejemplo:

Código PowerShell: Install-WindowsFeature AD-Domain-Services -IncludeManagementTools

3.2. Promoción del Controlador de Dominio 2025

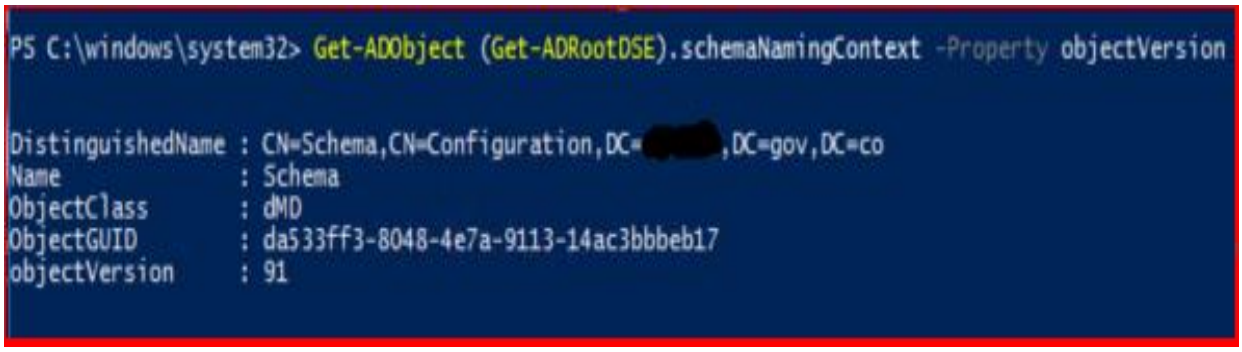
Antes de aprovechar la migración hacia un controlador de dominio con Windows Server 2025, fue necesario ejecutar una serie de comandos de preparación en el bosque y en el dominio:

- adprep /forestprep Actualiza el esquema de Active Directory en todo el bosque. Este paso prepara el entorno para aceptar un controlador de dominio con una versión más reciente de Windows Server.
- adprep /domainprep Actualiza los permisos y objetos dentro del dominio de Active Directory, garantizando compatibilidad antes de incorporar un controlador de dominio más moderno.

Nota: Desde Windows Server 2012, el ejecutable adprep.exe se integra automáticamente durante la ejecución del cmdlet Install-ADDSDomainController si se cuenta con los privilegios de Schema Admin y Enterprise Admin, aunque ejecutarlo manualmente de forma previa sigue siendo una excelente práctica de auditoría previa.

- Verificación de versión de esquema (opcional pero recomendada) Para Windows Server 2025, el atributo objectVersion, en Windows Server 2025 el objectVersion oficial del esquema de Active Directory es 91 (Windows Server 2022 era 90, Server 2019 era 88, Server 2016 era 87). Esto evitará confusión en tus lectores técnicos.

Código PowerShell: Get-ADObject (Get-ADRootDSE).schemaNamingContext -Property objectVersion



Instalación del controlador temporal DCRepa3-NUEVO

Para realizar la instalación del rol de AD DS (Active Directory Domain Services) y la posterior promoción del servidor de manera 100% automatizada por PowerShell (ideal para despliegues limpios en Windows Server 2025), el procedimiento consta de dos etapas: la instalación de las características del sistema y la promoción del Dominio/Controlador.

Paso 1: Instalación del Rol de AD DS y Herramientas de Administración

Abre PowerShell como Administrador en el nuevo servidor y ejecuta:

1. Instalar el rol de Active Directory Domain Services y herramientas RSAT

Install-WindowsFeature -Name AD-Domain-Services –IncludeManagementTools

Paso 2: Promoción a Controlador de Dominio

Elige el comando que corresponda al tipo de despliegue que estás realizando:

Este es el comando para agregar **DCRepa3-NUEVO** como un controlador secundario o de réplica a tu dominio existente:

```
# Promocionar el servidor como un nuevo DC dentro de un dominio existente
Install-ADDSDomainController `
    -DomainName "dominio.gov.co" `
    -InstallDns:$true `
    -CreateDnsDelegation:$false `
    -SiteName "Default-First-Site-Name" `   # Cambiar por el nombre de tu sitio si aplica (ej. Azure/Bogota)
    -DatabasePath "C:\Windows\NTDS" `
    -LogPath "C:\Windows\NTDS" `
    -SysvolPath "C:\Windows\SYSVOL" `
    -Force:$true
```

(Durante la ejecución, la consola te pedirá las credenciales de un administrador del dominio y la contraseña del modo de restauración de servicios de directorio - DSRM).

Paso 3: Transferencia de Roles FSMO (antes de apagar el viejo)

Código PowerShell: Move-ADDirectoryServerOperationMasterRole -Identity "DCRepa3" -OperationMasterRole PDCEmulator,RIDMaster,InfrastructureMaster

3.3. El proceso de "Suplantación"

Este fue el punto crítico para garantizar que las aplicaciones con **IP y nombre "quemados"** no fallaran. El orden estricto fue:

- **Apagar el servidor viejo (DC)**

Mantenerlo apagado, adicional se deshabilito la tarjeta de red por seguridad, sin des promoverlo permite revertir en caso de problemas.

- Apágalo físicamente, des habilitar la tarjeta o desconéctalo de la red
- No lo des promuevas aún

- **Limpieza de DNS**

Eliminar registros antiguos evita conflictos de resolución.

Abrir consola DNS en otro DC

- Borrar registros A que apunten a la IP vieja
- Confirmar que el sistema no los regeneró automáticamente

- **Renombrar el nuevo servidor (DC)**

El nuevo servidor debe asumir el nombre del antiguo o anterior para que las aplicaciones lo reconozcan.

- Cambiar nombre de **DCRepa3-NUEVO** a **DCRepa3**
- Reiniciar el servidor tras el cambio

- **Asignar la IP antigua**

La IP estática debe coincidir con la del servidor DC previo.

- Configurar la IP del nuevo servidor igual a la del viejo

- **Forzar registro en DNS y AD**

Garantiza que el nuevo servidor sea reconocido como legítimo.

- Ejecutar ipconfig /registerdns
- Ejecutar dcdiag /fix para validar registros y replicación

- **El "Metadata Cleanup" (Paso Final)**

Como el servidor viejo **DCRepa3** técnicamente nunca fue des promovido (porque lo apagamos para mantenerlo de respaldo), el Active Directory todavía piensa que ese objeto servidor existe pero está "offline".

Si decides que el nuevo servidor funciona bien y no vas a volver atrás, debes borrar el objeto del servidor viejo del AD usando Users and Computers (clic derecho -> Delete sobre el objeto viejo, si es que aparecen duplicados) o mediante ntdsutil. Esto evitará errores de replicación constantes.

Capítulo 4: Pruebas Finales y Validación de Salud (Nivel 3)

4.1. Diagnóstico del Servicio de Directorio y Réplica

Así se validó que los cambios hayan replicado a todos los DCs actuales, Asegurándonos que ninguna columna muestre fallos (fails) en las últimas horas después de la suplantación.

- **Código PowerShell: repadmin /replsummary**
- **Código PowerShell:** Scripts con repadmin, Get-ADReplicationPartnerMetadata y validación de SYSVOL.

Este script verificará la salud del nuevo DC y que el dominio reconozca al nuevo DCRepa3 como el dueño legítimo de los roles y que los servicios críticos estén respondiendo normalmente.

```
Write-Host "--- Iniciando Validación de Salud del DC (DCRepa3) ---" -ForegroundColor Cyan

# 1. Verificar roles FSMO
Write-Host "`n[1] Verificando Roles FSMO:" -Yellow
Get-ADDomain | Select-Object PDCEmulator, RIDMaster, InfrastructureMaster | Format-List

# 2. Verificar conectividad y registros DNS
Write-Host "[2] Verificando registros DNS y conectividad:" -Yellow
Test-Connection -ComputerName "DCRepa3.dominio.gov.co" -Count 2
ipconfig /displaydns | Select-String "DCRepa3" | Select-Object -First 5

# 3. Diagnóstico de Directorio (DCDIAG)
Write-Host "[3] Ejecutando DCDIAG rápido (Connectivity y Advertising):" -Yellow
dcdiag /test:Connectivity /test:Advertising

# 4. Verificar servicios críticos
Write-Host "[4] Estado de servicios base (ADWS, DNS, Netlogon):" -Yellow
Get-Service ADWS, DNS, Netlogon, KDC | Select-Object Name, Status

Write-Host "`n--- Validación Finalizada ---" -ForegroundColor Cyan
```

4.2. Resumen de las pruebas posteriores, validación de Salud y Réplica de Active Directory

Verifica la topología de replicación, latencias y sincronización entre el servidor de Azure y el de la sede local.

Validación de Salud y Réplica de Active Directory

Verifica la topología de replicación, latencias y sincronización entre el servidor de Azure y el de la sede local.

Pruebas Diagnósticas de DNS y Servicios Esenciales (SRV Records)

Valida que el servicio DNS del nuevo DC haya registrado correctamente sus registros SRV (esenciales para que los clientes encuentren el controlador de dominio).

Verificación de Carpetas SYSVOL y NETLOGON (DFSR)

Confirmación del estado de las carpetas compartidas donde residen las GPOs y scripts de inicio de sesión

Batería de Pruebas DCDIAG en Un Solo Comando

La herramienta estándar por excelencia para validar un controlador de dominio antes de pasarlo a producción real.

Script de Diagnóstico "All-in-One" (Reporte Rápido)

Se ejecutó este script para que valide todo y nos entregue un resumen consolidado en pantalla:

```
Write-Host "============================================" -ForegroundColor Cyan
Write-Host " AUDITORÍA RÁPIDA DE SALUD - nuevo_DCRepa3  " -ForegroundColor Cyan
Write-Host "============================================" -ForegroundColor Cyan

# Test 1: Roles FSMO que conoce
Write-Host "`n[1/4] Roles FSMO Detectados:" -ForegroundColor Yellow
(Get-ADDomain).InfrastructureMaster
(Get-ADDomain).PDCEmulator

# Test 2: Estado del Canal Seguro
Write-Host "`n[2/4] Verificando Canal Seguro:" -ForegroundColor Yellow
Test-ComputerSecureChannel -Verbose

# Test 3: Eventos Recientes de Error en Directory Services (Últimas 24 horas)
Write-Host "`n[3/4] Revisando Errores en 'Directory Service Log':" -ForegroundColor Yellow
```

```
$errors = Get-WinEvent -LogName "Directory Service" -FilterXPath "*[System[(Level=1 or Level=2) and TimeCreated[timediff(@SystemTime) <= 86400000]]]" -ErrorAction SilentlyContinue
if ($errors) {
    $errors | Select-Object TimeCreated, Id, Message | Format-Table -Wrap
} else {
    Write-Host "Sin errores críticos registrados en las últimas 24 horas." -ForegroundColor Green
}

# Test 4: Conectividad LDAPS Cifrada (Puerto 636)
Write-Host "`n[4/4] Probando Puerto LDAPS (636):" -ForegroundColor Yellow
$ldaps = Test-NetConnection -ComputerName "DCRepa3" -Port 636
if ($ldaps.TcpTestSucceeded) {
    Write-Host "LDAPS Operativo y Escuchando." -ForegroundColor Green
} else {
    Write-Host "ALERTA: Puerto 636 no responde. Revisa el certificado de empresa-CA." -ForegroundColor Red
}
```

4.3. Detalles Finales a Tener en Cuenta

1. Para que la "suplantación" sea perfecta, se tuvieron en cuenta estos dos detalles manuales que a veces causan fallos en las aplicaciones:
2. Limpieza de la Caché ARP: En los switches core o routers que conectan a los clientes con el servidor, puede quedar la dirección MAC del servidor viejo asociada a la IP. Si ves que el servidor no responde tras el cambio, es posible que el switch necesite un clear arp-cache o simplemente esperar unos minutos.
3. El Objeto "Computadora" en AD: * Al renombrar el nuevo servidor a DCRepa3, Windows intentará actualizar el objeto en la unidad organizativa (OU) de Domain Controllers.
    - Si el objeto antiguo de DCRepa3 todavía existe, podrías recibir un error de "nombre duplicado".
    - Truco: Antes de renombrar el nuevo, entra en Active Directory Users and Computers, busca el DCRepa3 viejo y cámbiale el nombre ahí mismo a algo como DCRepa3 -OLD (o bórralo si ya tienes backup). Esto liberará el nombre para el nuevo

4.4. Resultados y Beneficios

La migración del controlador de dominio defectuoso (**DCRepa3**) se realizó en una instalación limpia a **Windows Server 2025** se ejecutó con éxito, manteniendo el mismo **nombre e IP** para garantizar la continuidad de las aplicaciones dependientes.

Resultados técnicos

- **Replicación estable:** Se eliminaron los errores críticos de sincronización entre sitios.
- **Modernización:** El entorno pasó de versiones heredadas a **Windows Server 2025**, con mejoras en seguridad y rendimiento.
- **Roles FSMO asegurados:** Los tres roles críticos (PDC Emulator, RID Master, Infrastructure Master) fueron transferidos sin incidentes.
- **Infraestructura limpia:** La reinstalación evitó la propagación de errores heredados en la base de datos de Active Directory.

Beneficios ejecutivos

- **Reducción de indisponibilidad:** El impacto en los usuarios fue mínimo, con una ventana de mantenimiento inferior a **2 horas**.
- **Continuidad de negocio:** Las aplicaciones críticas siguieron funcionando sin necesidad de ajustes adicionales.
- **Mayor seguridad:** Se reforzó la autenticación y la confiabilidad del servicio NPS/RADIUS.
- **Base sólida para el futuro:** La infraestructura quedó preparada para integraciones híbridas con Microsoft Entra ID y escenarios de nube.

Capítulo 5: Conclusiones y Lecciones Aprendidas

- No quemar IP o nombre: Evitar que aplicaciones dependan rígidamente de un identificador estático. Esto limita la flexibilidad y complica futuras migraciones.
- Planificación previa: La preparación del bosque y dominio con adprep y la verificación del esquema fueron pasos críticos para garantizar compatibilidad y evitar errores posteriores.
- Automatización con PowerShell: Usar scripts parametrizados permitió estandarizar procesos, reducir errores humanos y asegurar trazabilidad.
- Transferencia controlada de roles FSMO: Migrar roles mientras ambos servidores estaban activos evitó riesgos de pérdida de autoridad en el dominio.

- Ventana de mantenimiento mínima: Diseñar un plan que redujo la indisponibilidad a menos de 2 horas fue clave para mantener la continuidad del negocio.
- Limpieza antes de migrar: No basta con instalar encima de versiones antiguas; una reinstalación limpia evita replicar errores heredados en la base de datos de AD.
- Validación post-cambio: Verificar DNS, GUID de NTDS y registros de replicación aseguró que el nuevo controlador fuera reconocido correctamente como legítimo.

Nota: ¿Por qué no es una buena práctica quemar la IP o un nombre de un Controlador de Dominio?

- Rigidez Ante Migraciones: Como estás viendo con la migración a Windows Server 2025, si mañana decides cambiar el direccionamiento de Azure o mover el DC a otra subred, tendrías que recompilar o modificar la configuración de N aplicaciones.
- Falla de Alta Disponibilidad: Un Domain Controller puede entrar en mantenimiento o fallar. Si la app apunta a la IP 10.X.Y.Z y ese servidor cae, la app muere, aunque el DC de on-premises (DCRepa3) esté funcional.
- Problemas con SSL/TLS (LDAPS): El certificado que acabamos de instalar está emitido para el FQDN DCRepa3.dominio.gov.co. Si la app intenta conectar por IP, el handshake TLS fallará porque el nombre solicitado (la IP) no coincide con el nombre del certificado (Hostname Mismatch).
- Carga Desbalanceada: Estarías sobrecargando un solo DC mientras los demás están ociosos.

¿Tu organización enfrenta una migración compleja, problemas de replicación o necesita soporte especializado de Nivel 3 en Active Directory?

*En **SysArmor Tech** ayudamos a organizaciones a modernizar, estabilizar y automatizar su infraestructura Microsoft.*

Conoce nuestros servicios:
sysarmortech.com

¿Necesitas evaluar un entorno específico? Contáctanos para conversar sobre tu escenario