Cheq-AD 15: Tu Auditoría Rápida de Active Directory

Este documento presenta una guía concisa para realizar una auditoría rápida de Active Directory utilizando comandos de PowerShell y CMD. La auditoría se centra en diez áreas clave que son fundamentales para garantizar la salud y seguridad de un entorno Active Directory. Cada sección incluye comandos específicos y criterios de evaluación que permiten identificar el estado de los componentes críticos.

¿Qué área de Active Directory debe auditarse?

Contraseñas de Servicio

Asegura que las contraseñas de servicio sean seguras y gestionadas correctamente.

Cuentas Privilegiadas

Revisa y gestiona cuentas con altos permisos para prevenir el acceso no autorizado.

GPO Huérfanas

Identifica y elimina objetos de política de grupo no utilizados para mantener la organización.

Catálogo Global

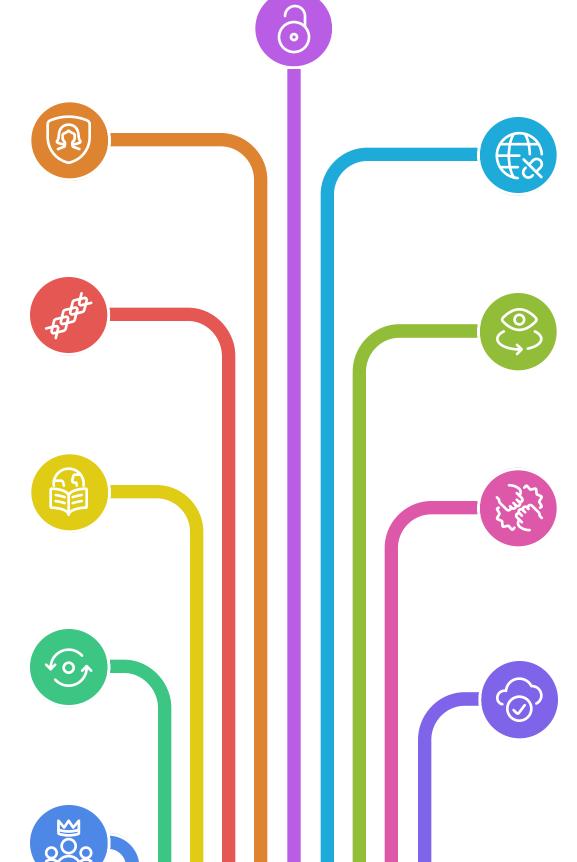
Confirma la disponibilidad de información completa del directorio para consultas.

Replicación

Verifica la sincronización de datos entre controladores de dominio para la consistencia.

Roles FSMO

Asegura la distribución adecuada de roles críticos para la funcionalidad del dominio.



Errores DNS

Diagnostica y corrige problemas de resolución de nombres para garantizar la conectividad de la red.

Auditoría Activada

Verifica que el registro de eventos esté habilitado para el seguimiento y análisis.

Delegaciones en OUs

Revisa y gestiona los permisos delegados en unidades organizativas para el control de acceso.

Backups Verificados

Confirma la integridad y disponibilidad de los datos de respaldo para la recuperación ante desastres.

1. FSMO roles

(Get-ADForest).SchemaMaster (Get-ADForest).DomainNamingMaster

ambos en DC redundante $\rightarrow X$ si caen en un mismo DC viejo

2. Replicación

repadmin /replsummary

Fails = $0 \rightarrow \checkmark$

3. Catálogo global

Get-ADForest | select GlobalCatalogs

 \geq 2 GC por site \rightarrow \checkmark

4. GPO huérfanas

Get-GPO -All | ?{ -not \$_.GpoStatus }

Resultado vacío = 🗸

5. Cuentas privilegiadas

Get-ADGroupMember "Administrators"

Solo grupos/SDDL esperados → ✓

6. Contraseñas de servicio

Get-ADUser -Filter * -Properties PasswordLastSet | ?{ \$_.ServicePrincipalName }

Get-ADOrganizationalUnit -LDAPFilter "(gPLink=*)" -Properties ManagedBy

≥ 2 años sin cambio = X

7. DNS errores

dnscmd /statistics /errors

 $0 \text{ errores} \rightarrow \checkmark$

8. Auditoría activada

auditpol /get /category:* Subcategorías críticas en Success+Failure → ✓

9. Delegaciones en OUs

Lista vacía = revisar → △!!

10. Backups verificados

wbadmin get versions

Restore test < 90 días → ✓