

	DEPARTAMENTO INFORMÁTICA	
	ADMINISTRACIÓN DE SISTEMAS OPERATIVOS	
	EDITOR ADSI	LDAP 1

Nombre y apellidos:

1. OBJETIVO

Conocer la estructura de la base de datos de Active Directory y operar sobre sus objetos.

Para mejorar la comprensión de las nomenclaturas crearemos una **UNIDAD ORGANIZATIVA** que se denomine **ZASIR** en donde tengamos incluido un equipo cliente y dos usuarios.

DCBRITO [Corriendo] - Oracle VirtualBox



Nombre	Tipo	Descripción
CLIENTE1	Equipo	
Dorian	Usuario	
Raul	Usuario	

2. EDITOR ADSI

A través de esta herramienta podemos consultar las cuatro particiones de AD de forma gráfica.

RECORDEMOS QUE ESTABA SUBDIVIDIDA EN 4 PARTICIONES: DOMINIO – CONFIGURACIÓN – ESQUEMA – APLICACIONES.

Buscar la apariencia de las particiones de Dominio – Configuración – Esquema.

Nombre	Clase	Nombre distintivo	Acciones
OU=2ASIR	organization...	OU=2ASIR,DC=brito,DC=loc	DC=brito,DC=loc
CN=Builtin	builtinDomain	CN=Builtin,DC=brito,DC=loc	
CN=Computers	container	CN=Computers,DC=brito,DC=loc	
OU=Domain Controllers	organization...	OU=Domain Controllers,DC=brito,D...	
CN=ForeignSecurityPrincip...	container	CN=ForeignSecurityPrincipals,DC=b...	
CN=Keys	container	CN=Keys,DC=brito,DC=loc	
CN=LostAndFound	lostAndFound	CN=LostAndFound,DC=brito,DC=loc	
CN=Managed Service Acco...	container	CN=Managed Service Accounts,DC=...	
CN=NTDS Quotas	msDS-Quota...	CN=NTDS Quotas,DC=brito,DC=loc	
CN=Program Data	container	CN=Program Data,DC=brito,DC=loc	
CN=System	container	CN=System,DC=brito,DC=loc	
CN=TPM Devices	msTPM-Info...	CN=TPM Devices,DC=brito,DC=loc	
CN=Users	container	CN=Users,DC=brito,DC=loc	
CN=Infrastructure	infrastructur...	CN=Infrastructure,DC=brito,DC=loc	

2.1 PARTICIÓN DE DOMINIO

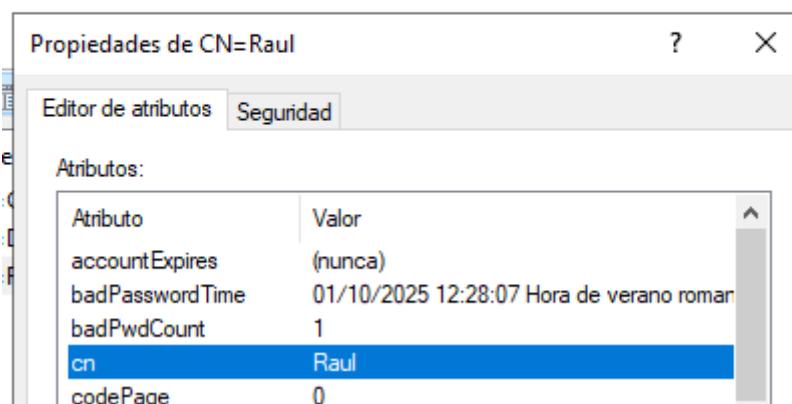
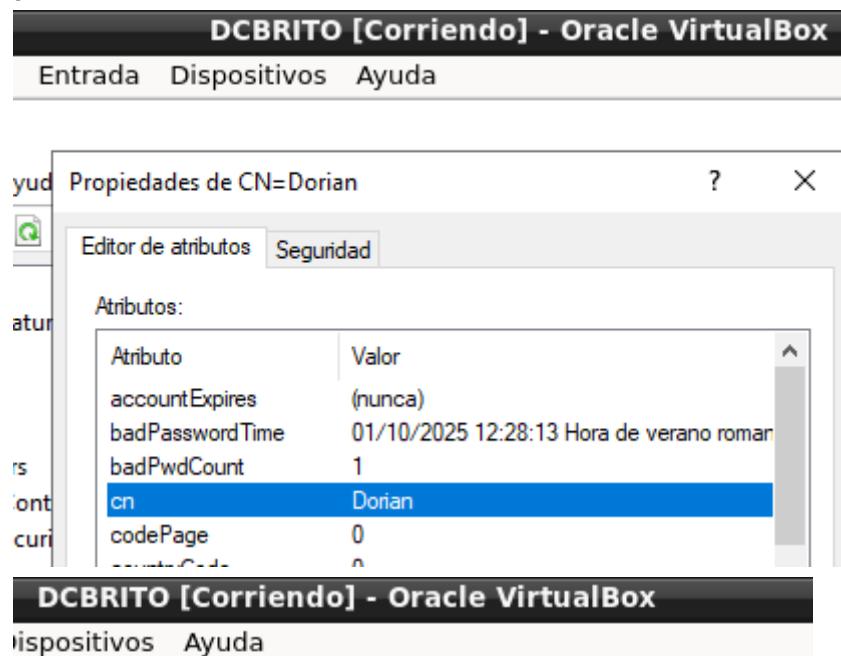
Sobre la partición de Dominio: Buscar e indicar sobre cada **objeto creado** usuario y equipo en el dominio:

EVIDENCIAS:

- CN
- distinguishedName
- sAMAccountName
- lastLogon
- objectSid
- objectGUID
- UPN de un usuario/equipo

Busca el atributo de última conexión de un usuario.

CN



DCBRITO [Corriendo] - Oracle VirtualBox

Dispositivos Ayuda

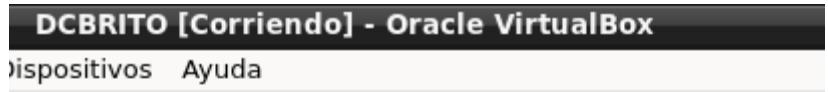
Propiedades de CN=CLIENTE1	
Editor de atributos Seguridad	
Atributos:	
Atributo	Valor
accountExpires	(nunca)
badPasswordTime	(nunca)
badPwdCount	0
cn	CLIENTE1
codePage	0

distinguishedName

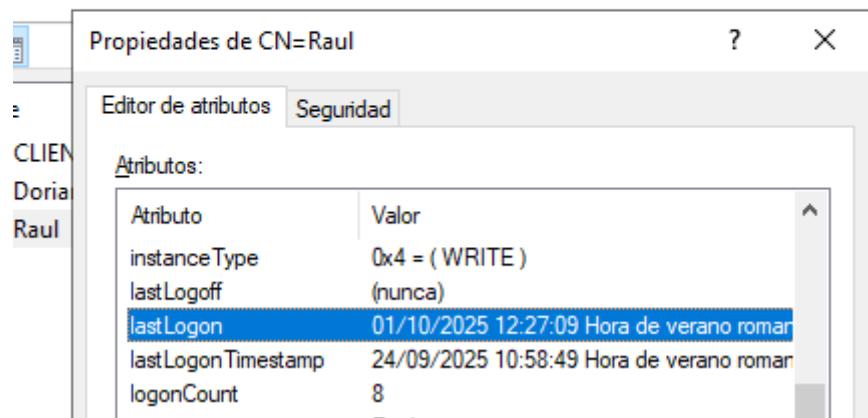
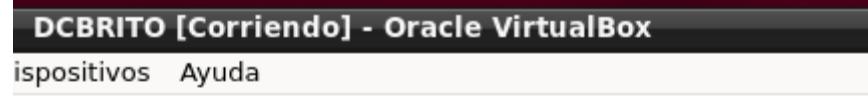
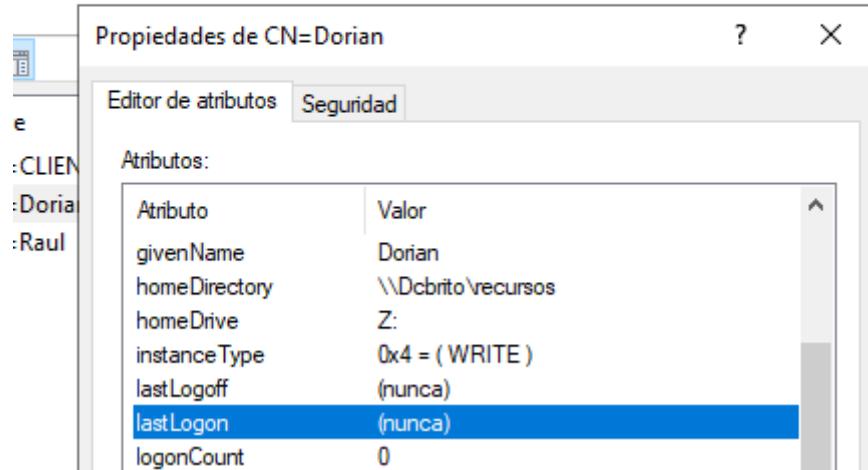
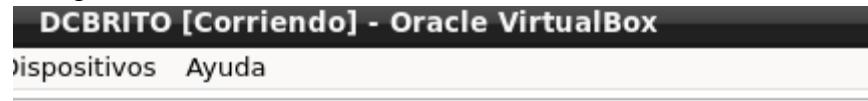
DCBRITO [Corriendo] - Oracle VirtualBox

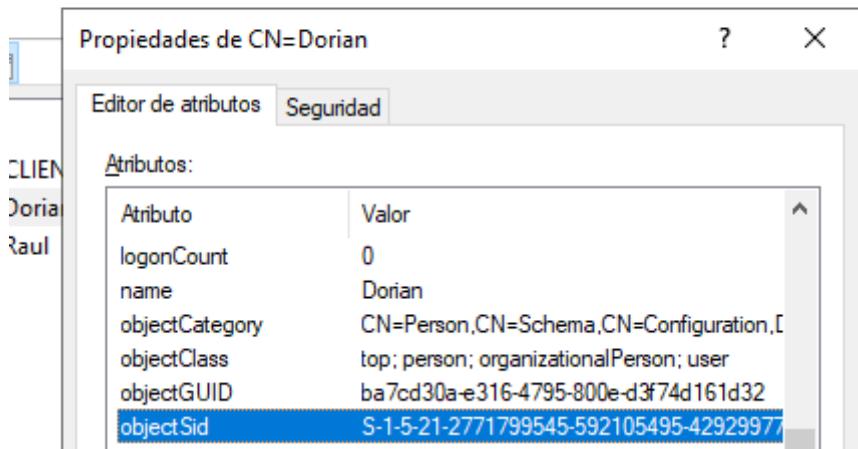
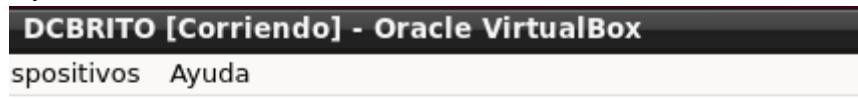
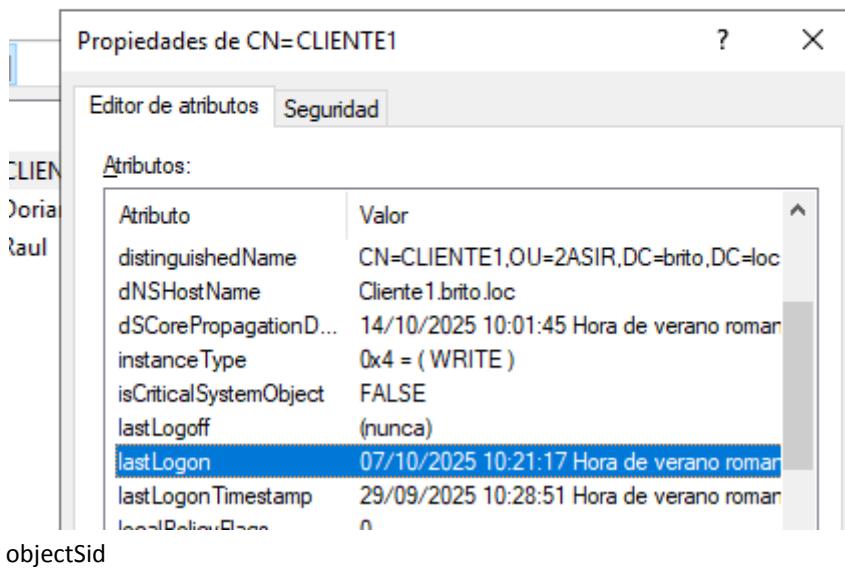
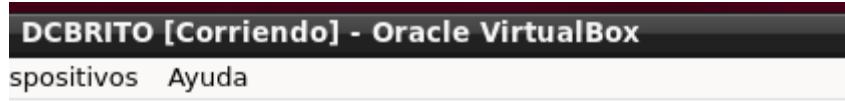
Dispositivos Ayuda

Propiedades de CN=Dorian	
Editor de atributos Seguridad	
Atributos:	
Atributo	Valor
accountExpires	(nunca)
badPasswordTime	01/10/2025 12:28:13 Hora de verano románica
badPwdCount	1
cn	Dorian
codePage	0
countryCode	0
displayName	Dorian
distinguishedName	CN=Dorian,OU=2ASIR,DC=brito,DC=local
dSCorePropagationD...	14/10/2025 10:02:18 Hora de verano románica

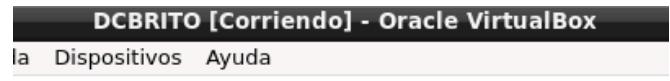


lastLogon

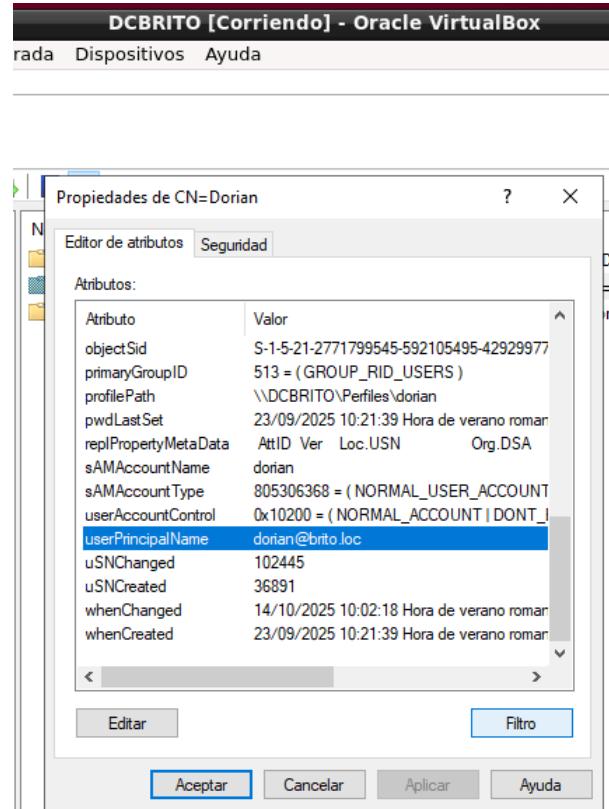




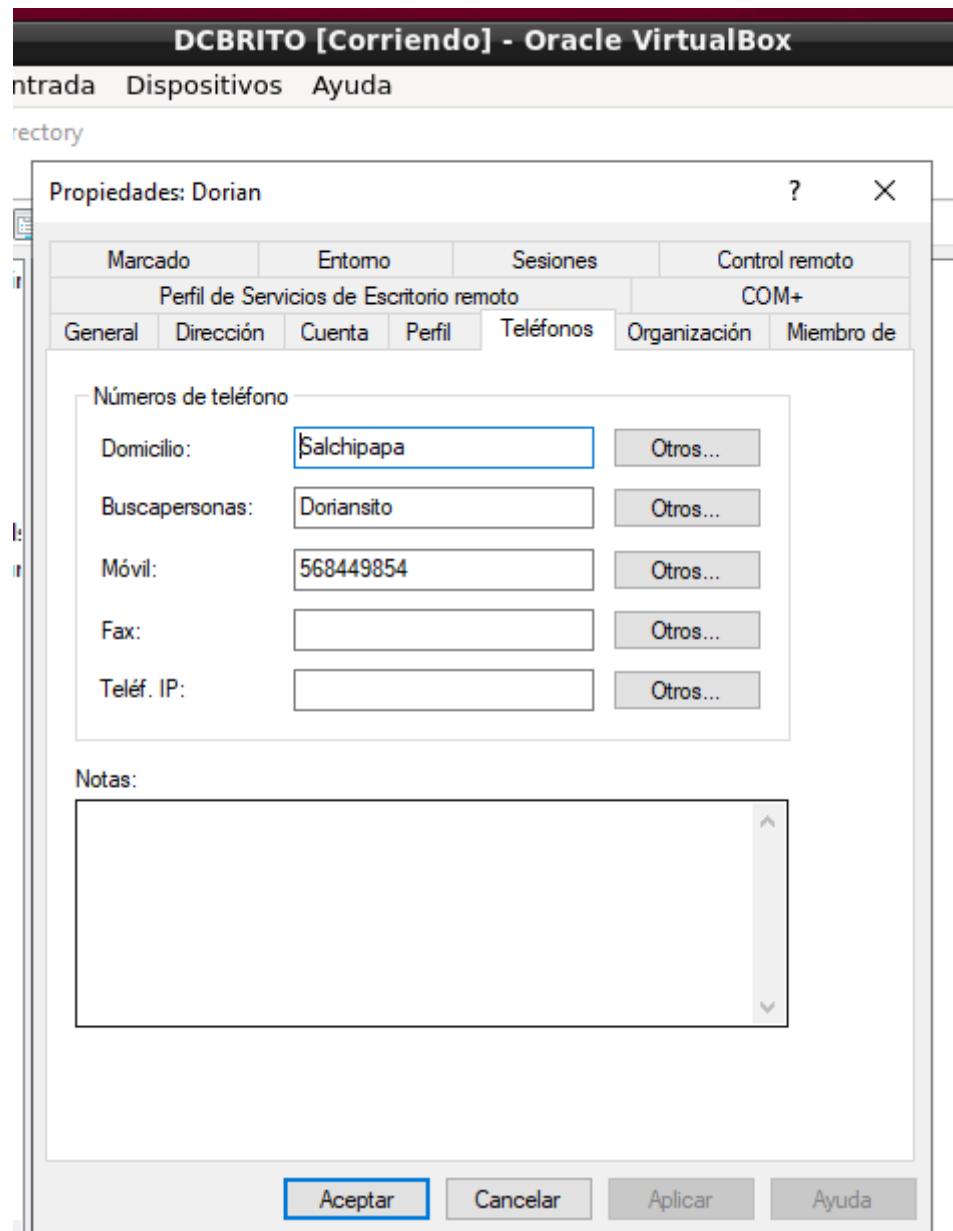
objectGUID

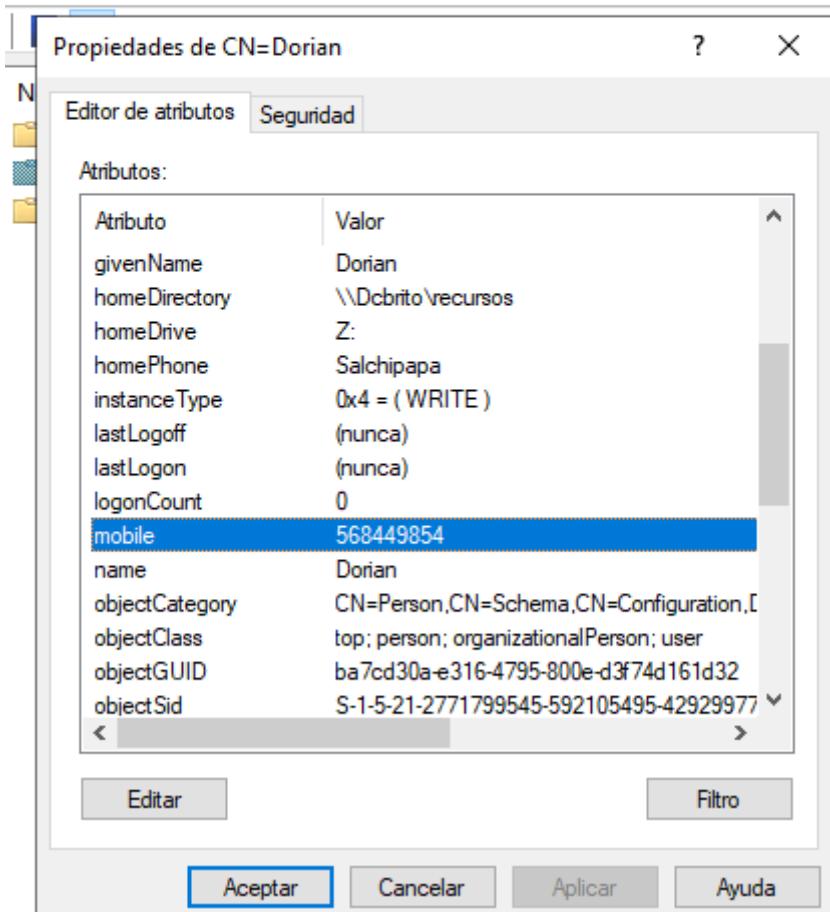
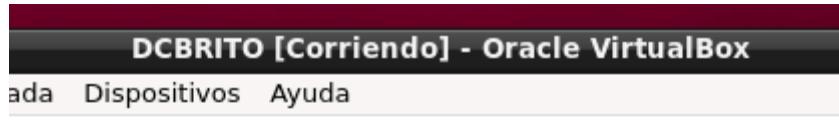


UPN de un usuario/equipo



En ADUC busca e identifica el un atributo de un usuario que sea irrelevante y BUSCALO desde el Editor ADSI desde la partición de dominio para editarla, por ejemplo: teléfono, ciudad. Una vez cambiado vuelve al ADUC para verificarlo.





2.2 PARTICIÓN DEL BOSQUE

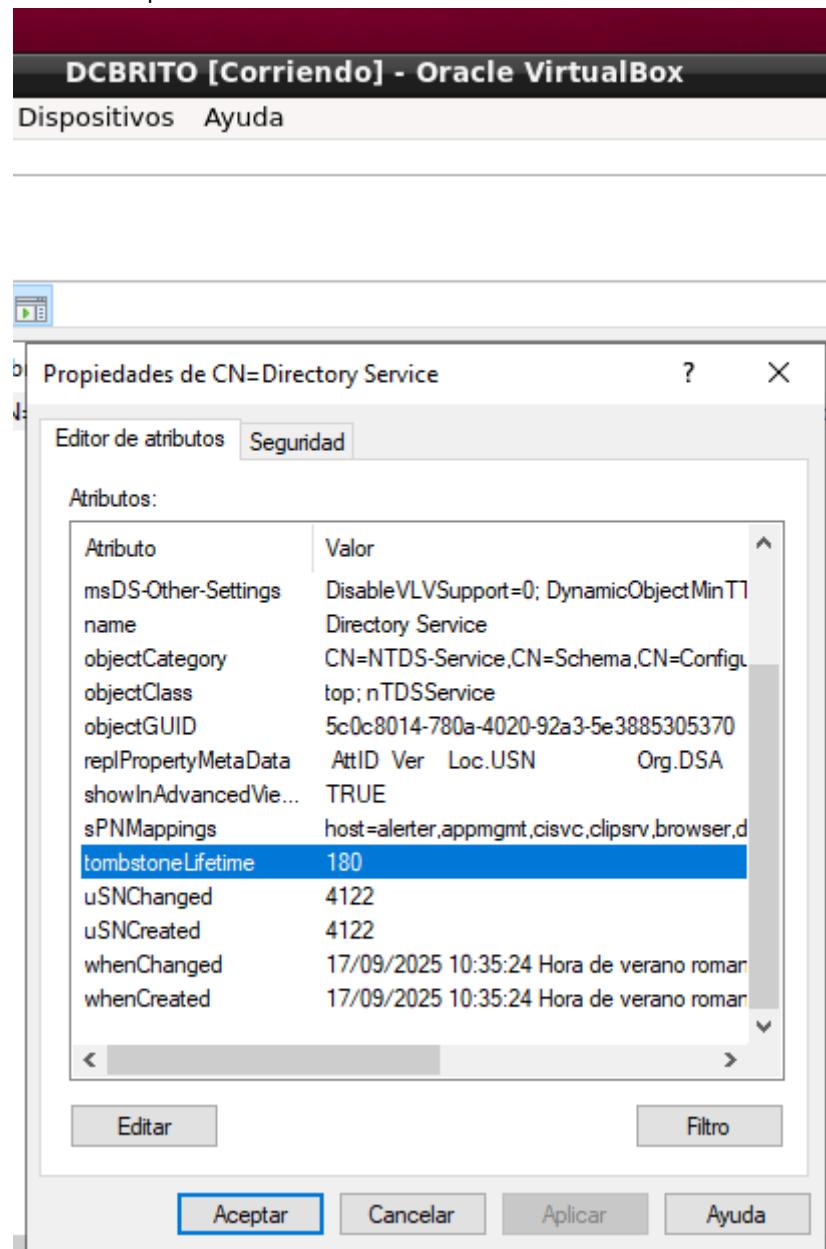
Buscar la ruta identificación y valor del atributo:

- **Nombre distinguido del bosque:** Se encuentra en el contenedor del directorio raíz.
- **Nivel funcional del bosque:** Se encuentra en el contenedor del directorio raíz.
- **Confianzas del bosque:** En el contenedor Trusts.
- **Sitios del bosque:** En el contenedor Sites.
- **Servidores identificados:** Busca en los contenedores de los sitios.
- **Servicios identificados:** En el contenedor Services.

Sobre la partición del BOSQUE (configuración) buscar la ruta para localizar el atributo *Tombstone lifetime*, buscar su ruta, valor y significado. Pegar pantallazo de la ubicación y valor. Si aparece.

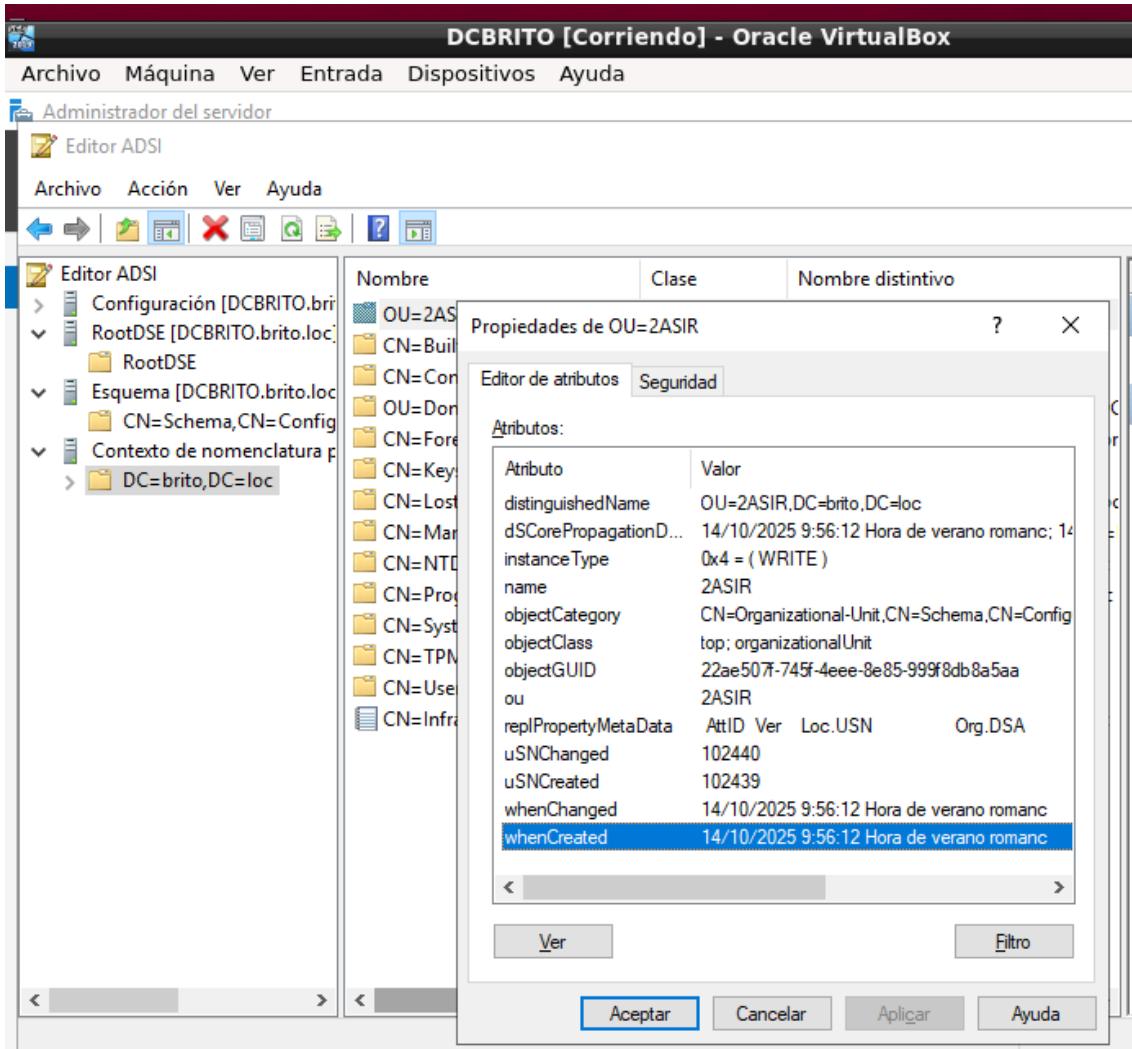
Configuración > CN=Configuration,DC=... > CN=Services > CN=Windows NT > CN=Directory Service.

El atributo tombstoneLifetime define cuánto tiempo se retiene un objeto eliminado de Active Directory antes de ser permanentemente eliminado.



Realizar lo mismo sobre el atributo *whenCreated*.

Este atributo muestra la fecha y hora en que un objeto fue creado.



2.3 PARTICIÓN DE ESQUEMA

Verla y no modificar nada, por favor.

Describe qué funcionalidad tiene esta partición.

La partición de esquema es un mapa de la estructura de Active Directory. Define las clases de objetos (como usuarios, grupos, etc.) y los atributos que pueden tener, así como las relaciones entre ellos. Es fundamental para el funcionamiento del directorio, y por eso el taller recomienda no modificarla.

Nombre	Clase	Nombre distintivo	Acciones
CN=account	classSchema	CN=account,CN=Schema,DC=DCBRITO,DC=brito,DC=loc	
CN=Account-Expires	attributeSchema	CN=Account-Expires,CN=Schema,DC=DCBRITO,DC=brito,DC=loc	
CN=Account-Name-History	attributeSchema	CN=Account-Name-History,CN=Schema,DC=DCBRITO,DC=brito,DC=loc	
CN=ACS-Aggregate-Token	attributeSchema	CN=ACS-Aggregate-Token,CN=Schema,DC=DCBRITO,DC=brito,DC=loc	
CN=ACS-Allocable-RSVP-Binding	attributeSchema	CN=ACS-Allocable-RSVP-Binding,CN=Schema,DC=DCBRITO,DC=brito,DC=loc	
CN=ACS-Cache-Timeout	attributeSchema	CN=ACS-Cache-Timeout,CN=Schema,DC=DCBRITO,DC=brito,DC=loc	
CN=ACS-Direction	attributeSchema	CN=ACS-Direction,CN=Schema,DC=DCBRITO,DC=brito,DC=loc	
CN=ACS-DSBM-DeadTime	attributeSchema	CN=ACS-DSBM-DeadTime,CN=Schema,DC=DCBRITO,DC=brito,DC=loc	
CN=ACS-DSBM-Priority	attributeSchema	CN=ACS-DSBM-Priority,CN=Schema,DC=DCBRITO,DC=brito,DC=loc	
CN=ACS-DSBM-Refresh	attributeSchema	CN=ACS-DSBM-Refresh,CN=Schema,DC=DCBRITO,DC=brito,DC=loc	
CN=ACS-Enable-ACS-Service	attributeSchema	CN=ACS-Enable-ACS-Service,CN=Schema,DC=DCBRITO,DC=brito,DC=loc	
CN=ACS-Enable-RSVP-Access	attributeSchema	CN=ACS-Enable-RSVP-Access,CN=Schema,DC=DCBRITO,DC=brito,DC=loc	
CN=ACS-Enable-RSVP-Messages	attributeSchema	CN=ACS-Enable-RSVP-Messages,CN=Schema,DC=DCBRITO,DC=brito,DC=loc	
CN=ACS-Event-Log-Level	attributeSchema	CN=ACS-Event-Log-Level,CN=Schema,DC=DCBRITO,DC=brito,DC=loc	
CN=ACS-Identity-Name	attributeSchema	CN=ACS-Identity-Name,CN=Schema,DC=DCBRITO,DC=brito,DC=loc	
CN=ACS-Max-Aggregate-Pool	attributeSchema	CN=ACS-Max-Aggregate-Pool,CN=Schema,DC=DCBRITO,DC=brito,DC=loc	
CN=ACS-Max-Duration-Per-Object	attributeSchema	CN=ACS-Max-Duration-Per-Object,CN=Schema,DC=DCBRITO,DC=brito,DC=loc	
CN=ACS-Max-No-Of-Accounts	attributeSchema	CN=ACS-Max-No-Of-Accounts,CN=Schema,DC=DCBRITO,DC=brito,DC=loc	
CN=ACS-Max-No-Of-Logs	attributeSchema	CN=ACS-Max-No-Of-Logs,CN=Schema,DC=DCBRITO,DC=brito,DC=loc	
CN=ACS-Max-Peak-Bandwidth	attributeSchema	CN=ACS-Max-Peak-Bandwidth,CN=Schema,DC=DCBRITO,DC=brito,DC=loc	
CN=ACS-Max-Peak-Bandwidth	attributeSchema	CN=ACS-Max-Peak-Bandwidth,CN=Schema,DC=DCBRITO,DC=brito,DC=loc	
CN=ACS-Max-Size-Of-RSVP-Message	attributeSchema	CN=ACS-Max-Size-Of-RSVP-Message,CN=Schema,DC=DCBRITO,DC=brito,DC=loc	

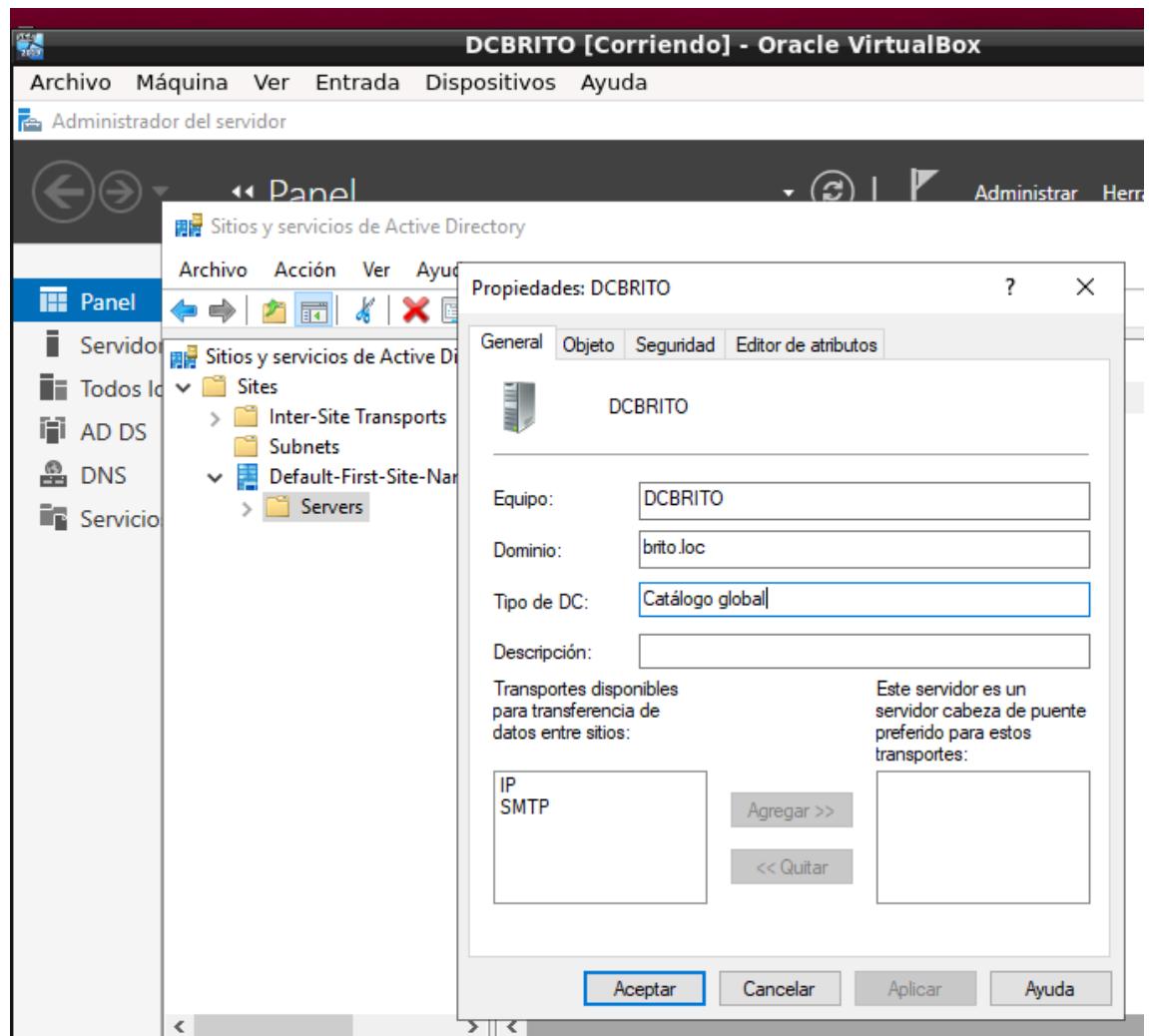
3. CÁTALOGO GLOBAL

Para saber si nuestro controlador es servidor del catálogo global hay varios métodos:

3.1 Active Directory Sites and Services

1. Busca tu servidor de dominio en la lista, haz clic derecho sobre él y selecciona Properties.
2. En la pestaña General, verás una casilla llamada Global Catalog. Si la casilla está marcada, significa que tu servidor es un catálogo global.

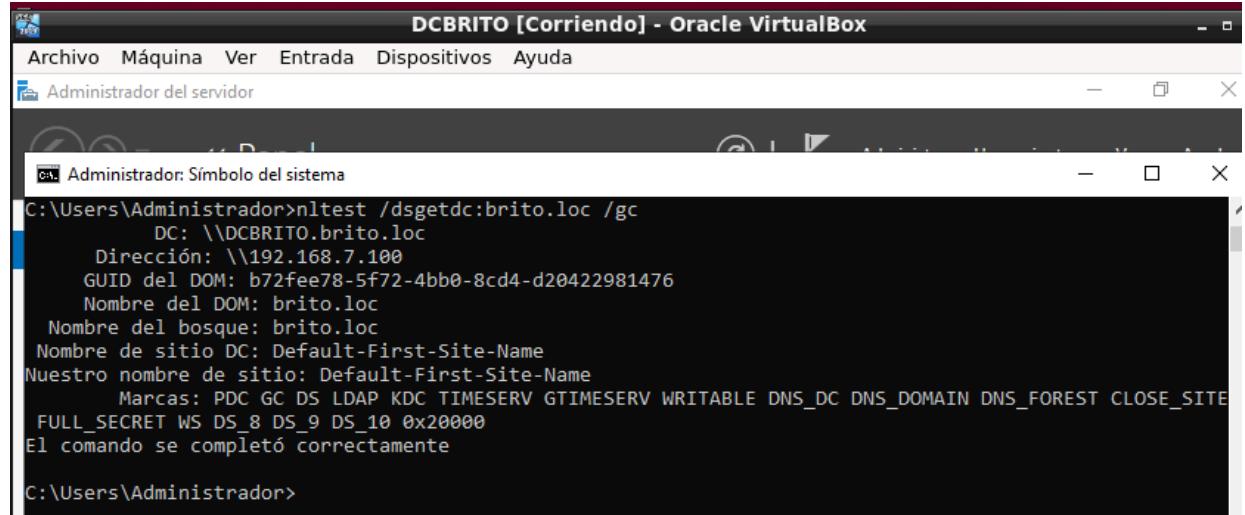
EVIDENCIA



3.2 Símbolo del sistema (línea de comandos)

1. Abre el Símbolo del sistema o PowerShell con privilegios de administrador.
3. Ejecuta el siguiente comando:
4. **nltest /dsgetdc:nombrededominio /gc**
5. Si el servidor es un catálogo global, el resultado mostrará GC en la lista de flags.

EVIDENCIA



```
C:\Users\Administrador>nltest /dsgetdc:brito.loc /gc
DC: \\DCBRITO.brito.loc
Dirección: \\192.168.7.100
GUID del DOM: b72fee78-5f72-4bb0-8cd4-d20422981476
Nombre del DOM: brito.loc
Nombre del bosque: brito.loc
Nombre de sitio DC: Default-First-Site-Name
Nuestro nombre de sitio: Default-First-Site-Name
    Marcas: PDC GC DS LDAP KDC TIMESERV GTIMESERV WRITABLE DNS_DC DNS_DOMAIN DNS_FOREST CLOSE_SITE
    FULL_SECRET WS DS_8 DS_9 DS_10 0x20000
El comando se completó correctamente

C:\Users\Administrador>
```

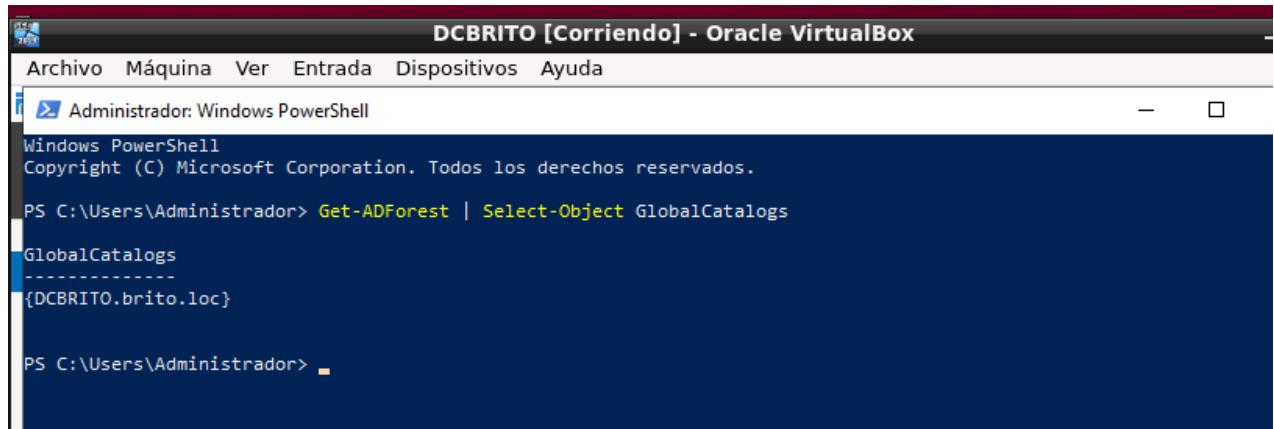
3.3 PowerShell

0. Usa el siguiente comando:

1. **Get-ADForest | Select-Object GlobalCatalogs**

2. Este comando te mostrará una lista de todos los controladores de dominio que actúan como catálogo global en tu bosque. Si tu servidor aparece en la lista, es un GC.

EVIDENCIA



```
DCBRITO [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

PS C:\Users\Administrador> Get-ADForest | Select-Object GlobalCatalogs

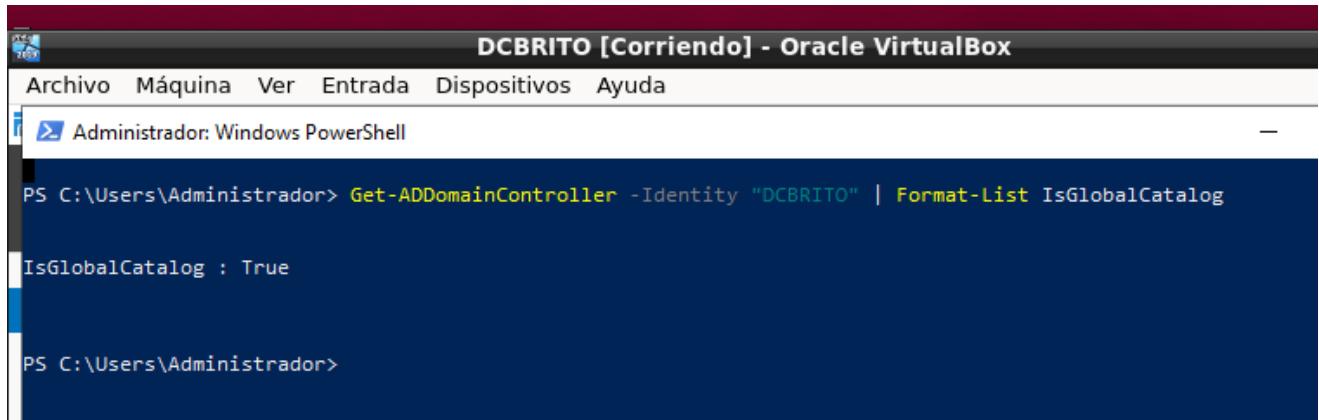
GlobalCatalogs
-----
{DCBRITO.brito.loc}

PS C:\Users\Administrador>
```

3. Otra opción es usar:

4. **Get-ADDomainController -Identity "nombredelservidor" | Format-List IsGlobalCatalog**

EVIDENCIA



```
DCBRITO [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Administrator: Windows PowerShell
PS C:\Users\Administrador> Get-ADDomainController -Identity "DCBRITO" | Format-List IsGlobalCatalog

IsGlobalCatalog : True

PS C:\Users\Administrador>
```