	DEPARTAMENTO INFORMÁTICA	
	2º ASIR - ASO	
	CONSULTAS LDAP en Power Shell	

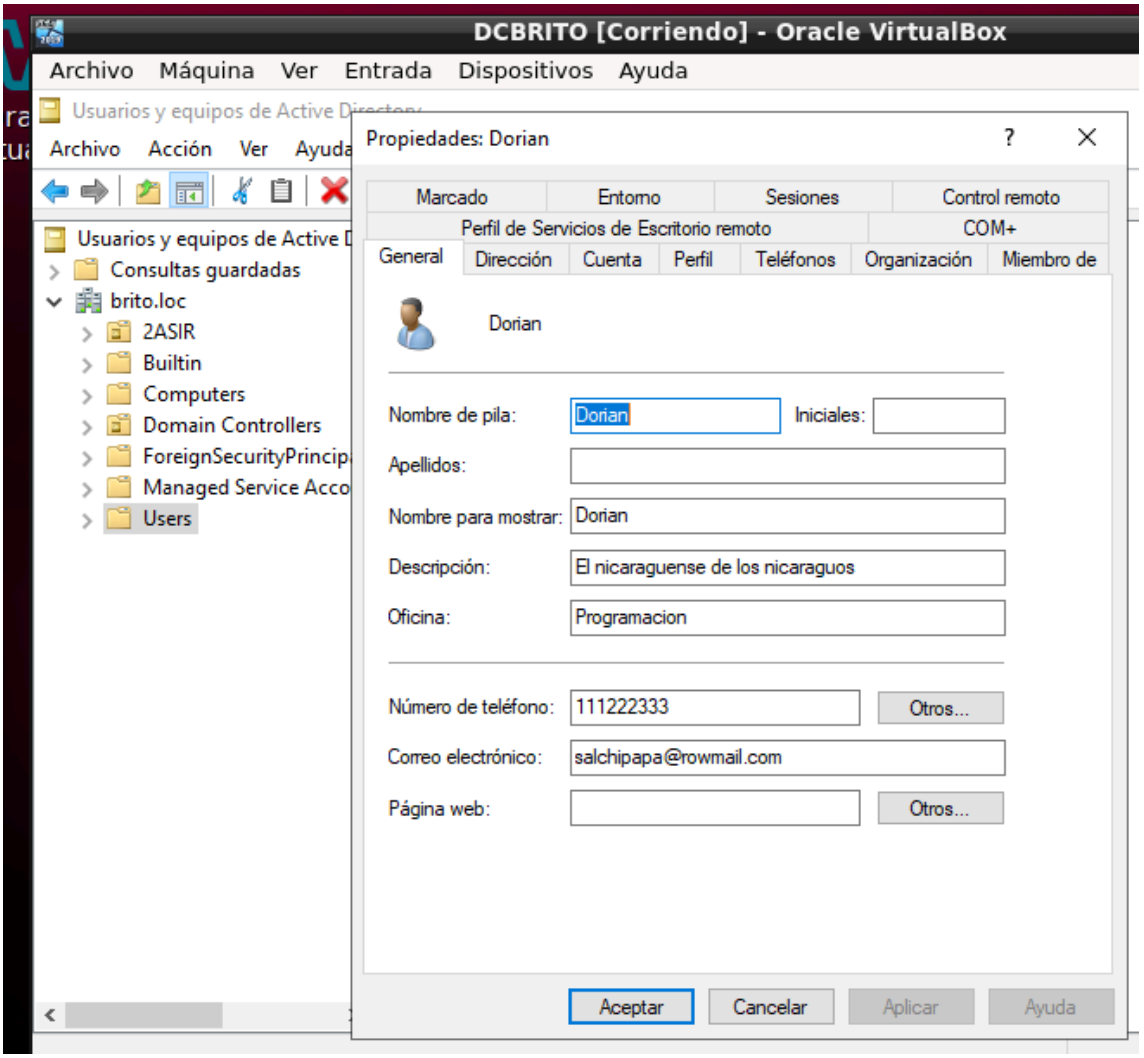
0. OBJETIVOS

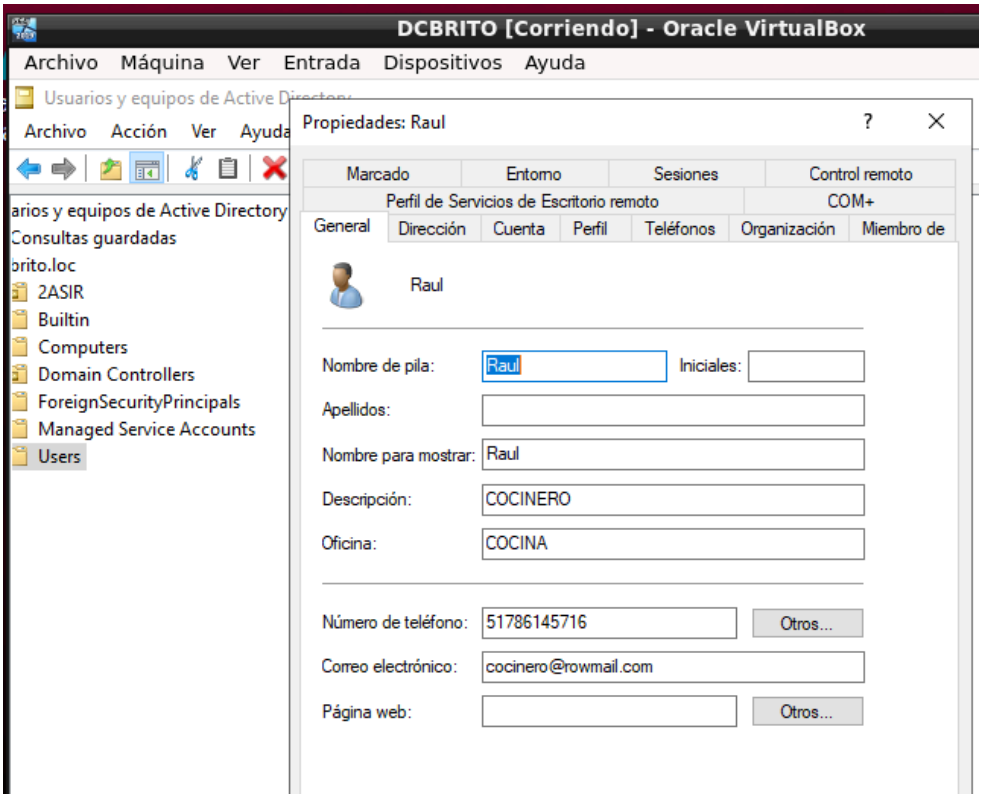
- Realizar consultas LDAP mediante POWER SHELL

1. INICIO

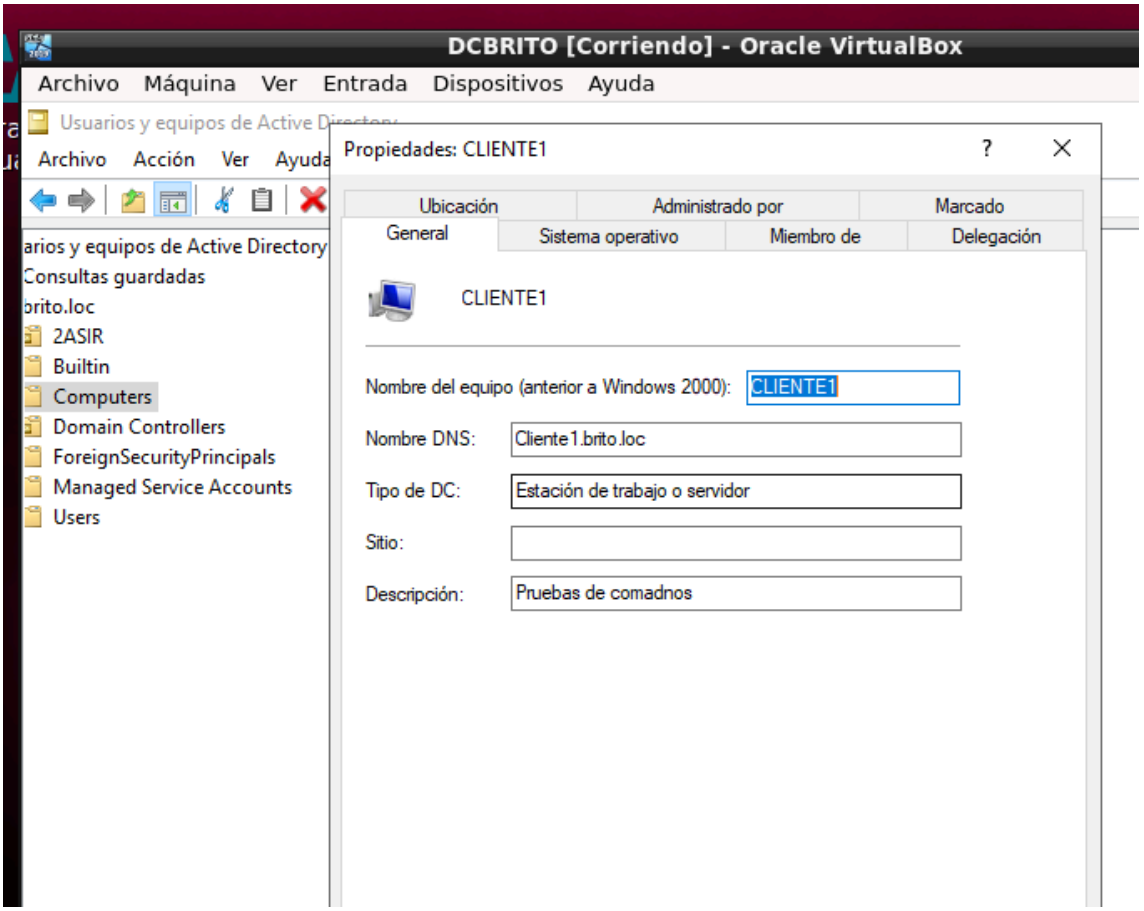
Con el objeto de obtener los máximos atributos debemos de completar mediante la herramienta de USUARIOS Y EQUIPOS DE ACTIVE DIRECTORY toda información posible sobre **dos usuarios ya creados y sobre un equipo cliente**.

USUARIO: Sobre las fichas General – dirección y organización.





EQUIPO: solamente nos permite la descripción – rellenar.



2. Get-ADUser

Para poder utilizar los comandos relacionados con AD es necesario instalar el módulo de código para el entorno de active directory. Normalmente en un DC viene cargado.

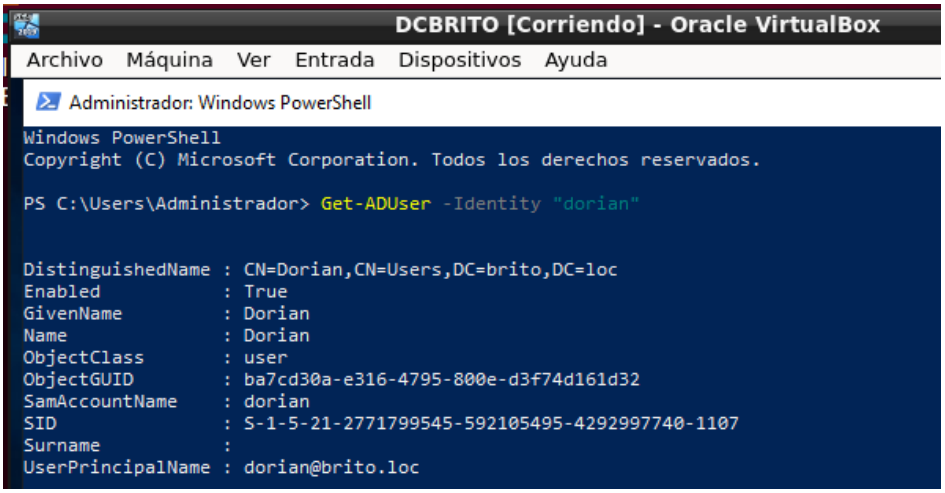
Buscar la instrucción para cargarlo en caso de un equipo cliente.

En un equipo cliente (como Windows 10 pro), el módulo no viene instalado. Habría que instalar las RSAT (Remote Server Administration Tools). Con en comando Get-WindowsCapability -Name RSAT.ActiveDirectory* -Online | Add-WindowsCapability -Online.

USUARIO 1

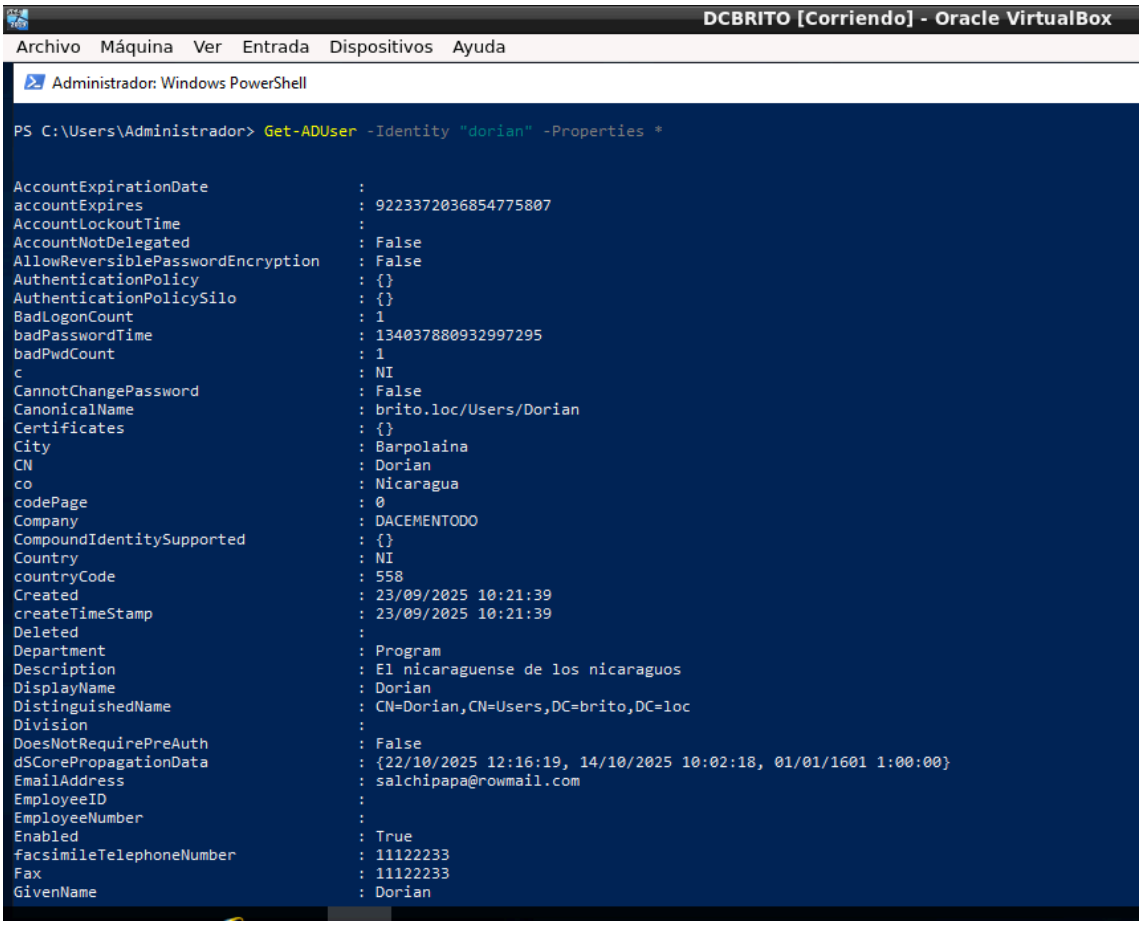
Utilizar el cmlet Get-ADUser para obtener los atributos principales de un usuario, nombre, nombre distinguido, nombre de cuenta sam, nombre usuario principal UPN, SID,

Atributos Principales:



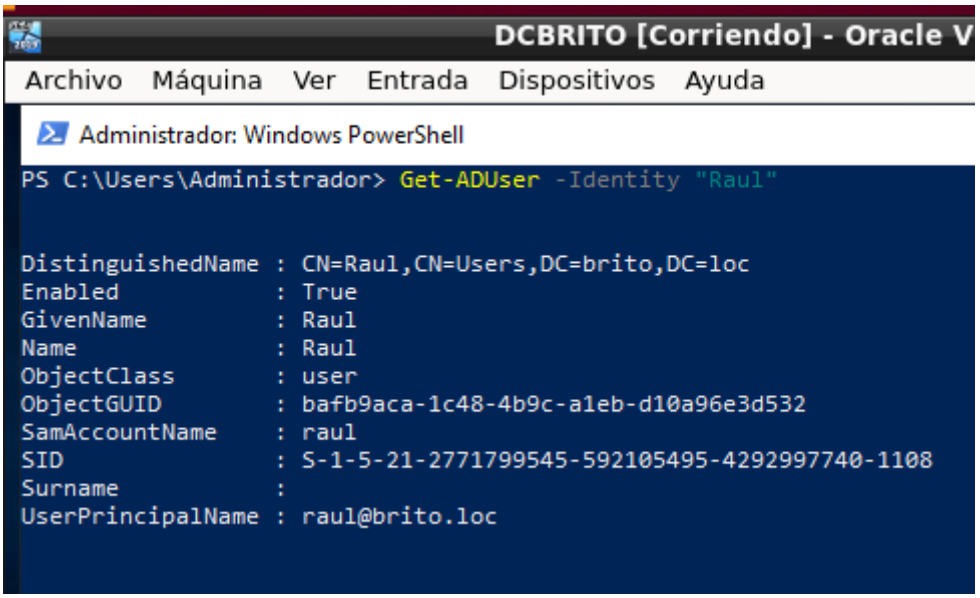
Utilizar el mismo cmlet para conseguir todos los atributos del usuario.

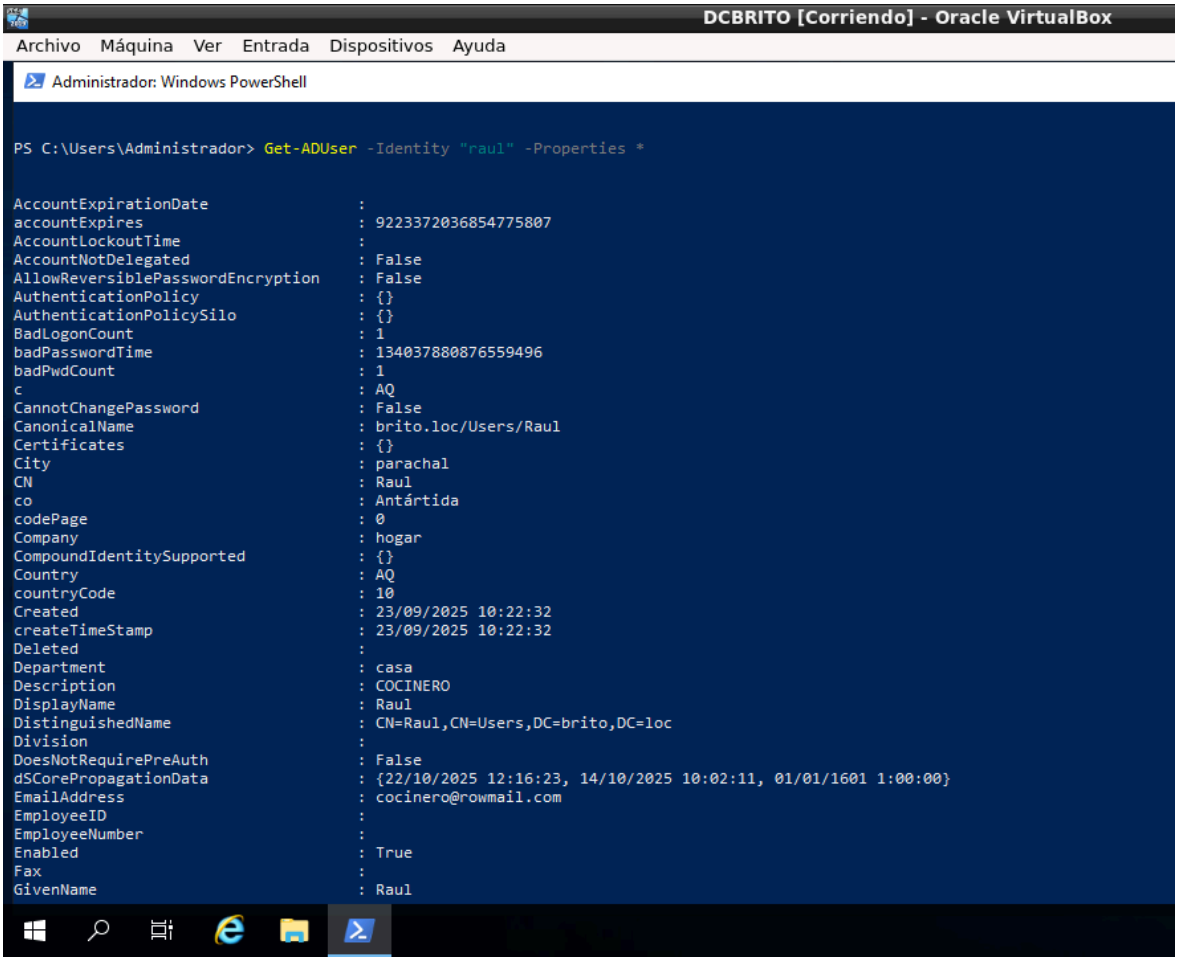
Todos los Atributos:



USUARIO 2

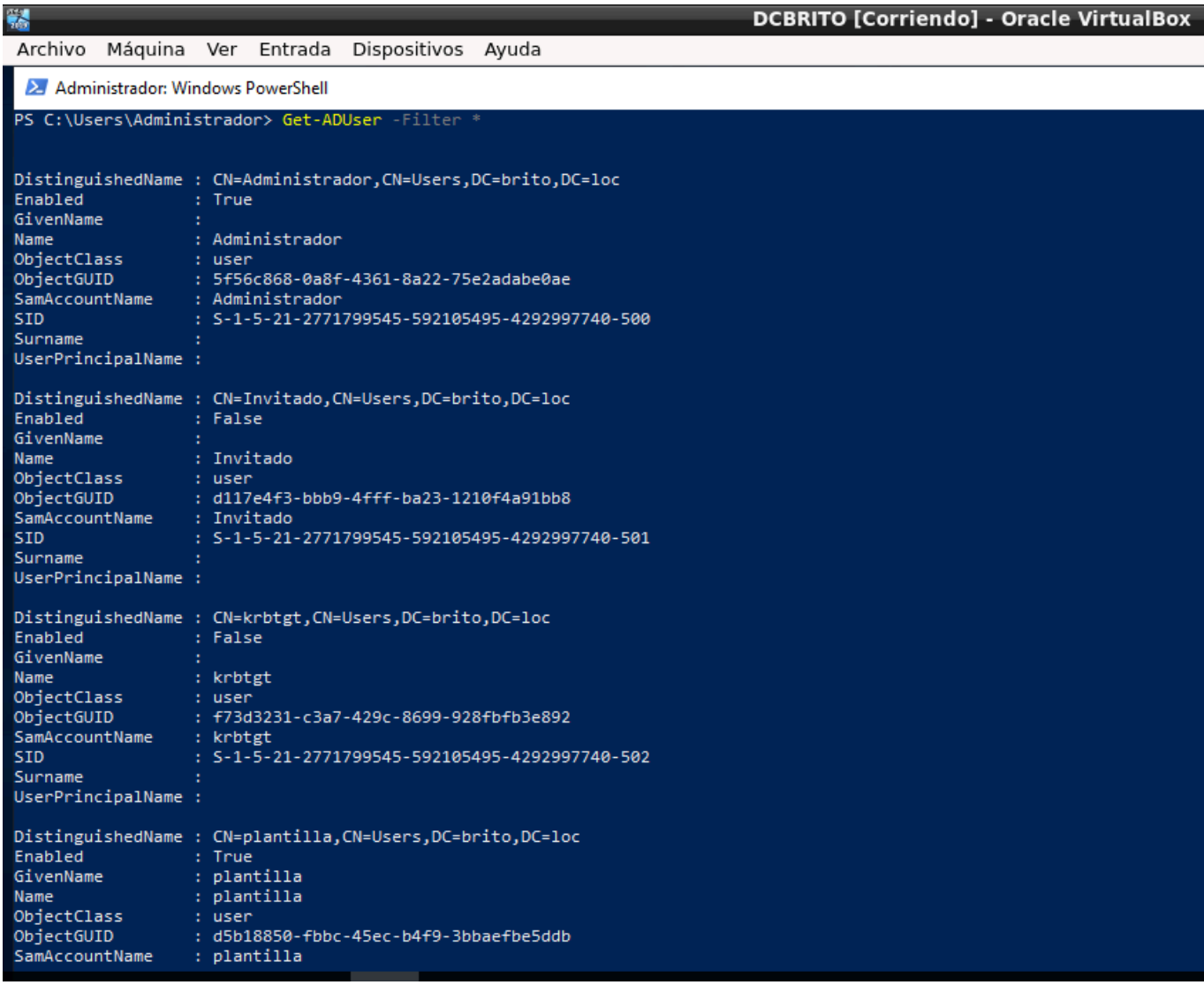
Lo mismo



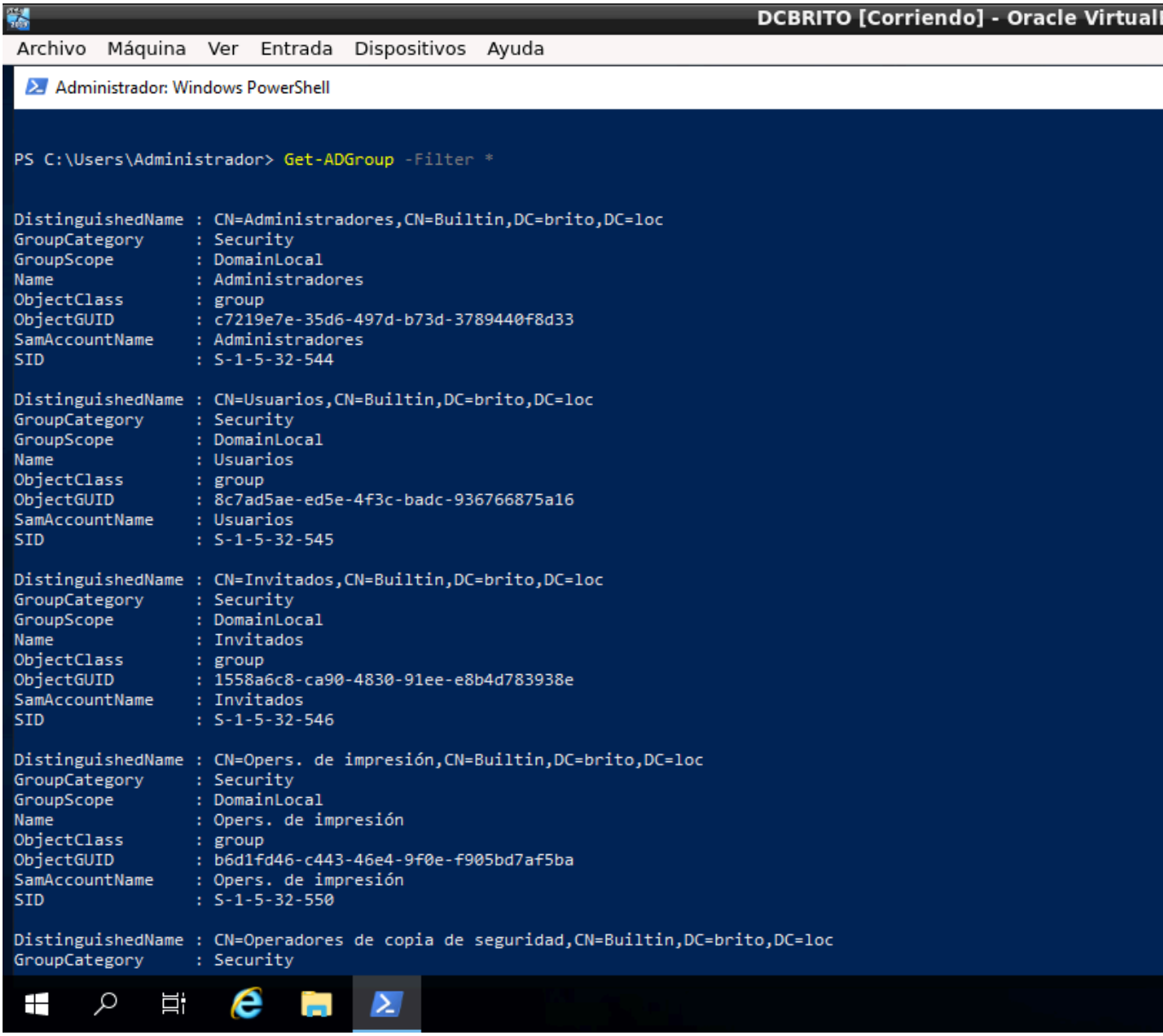


3. OTROS

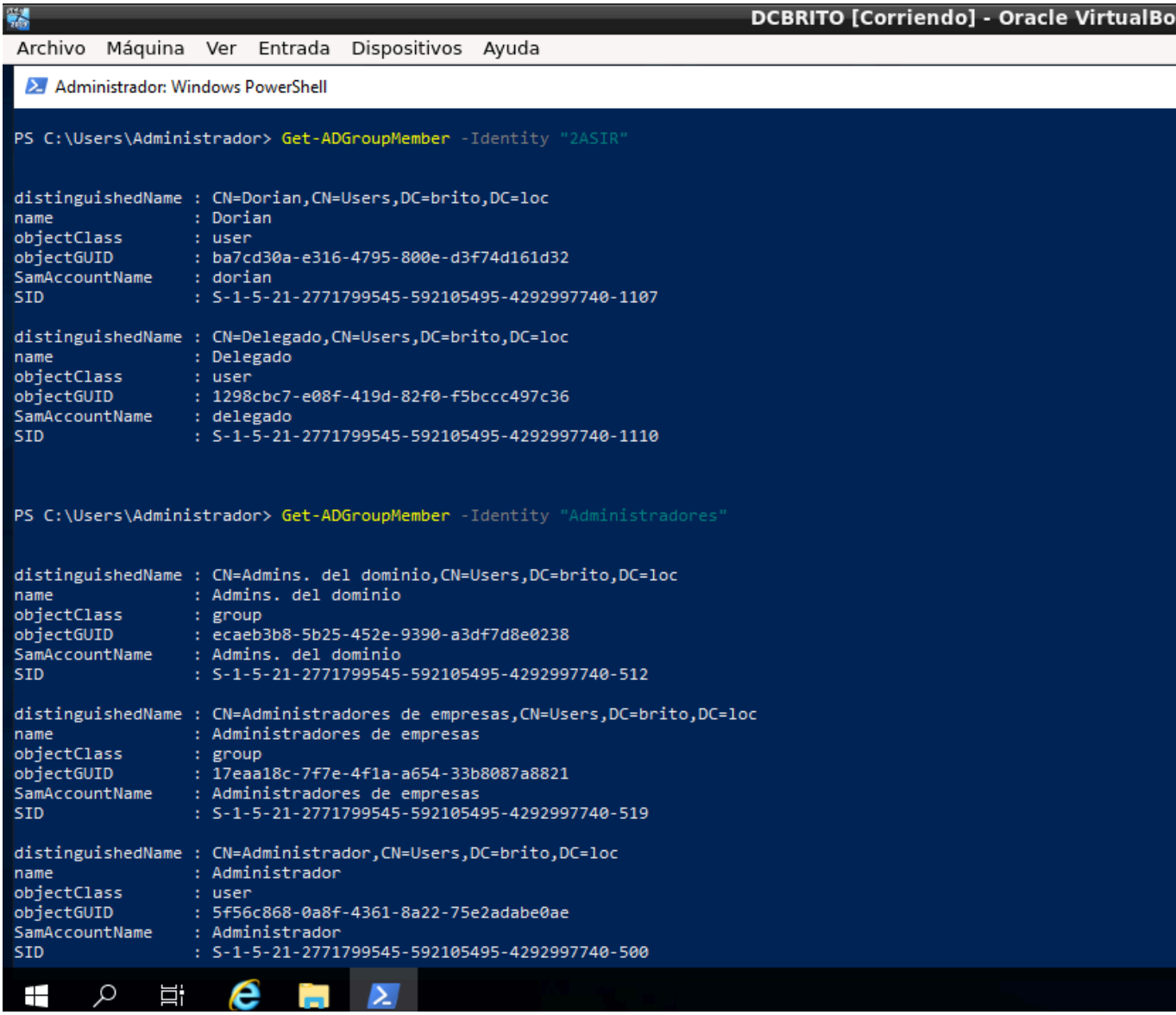
Obtener la lista de usuarios del dominio.



Obtener la lista de grupos del dominio.

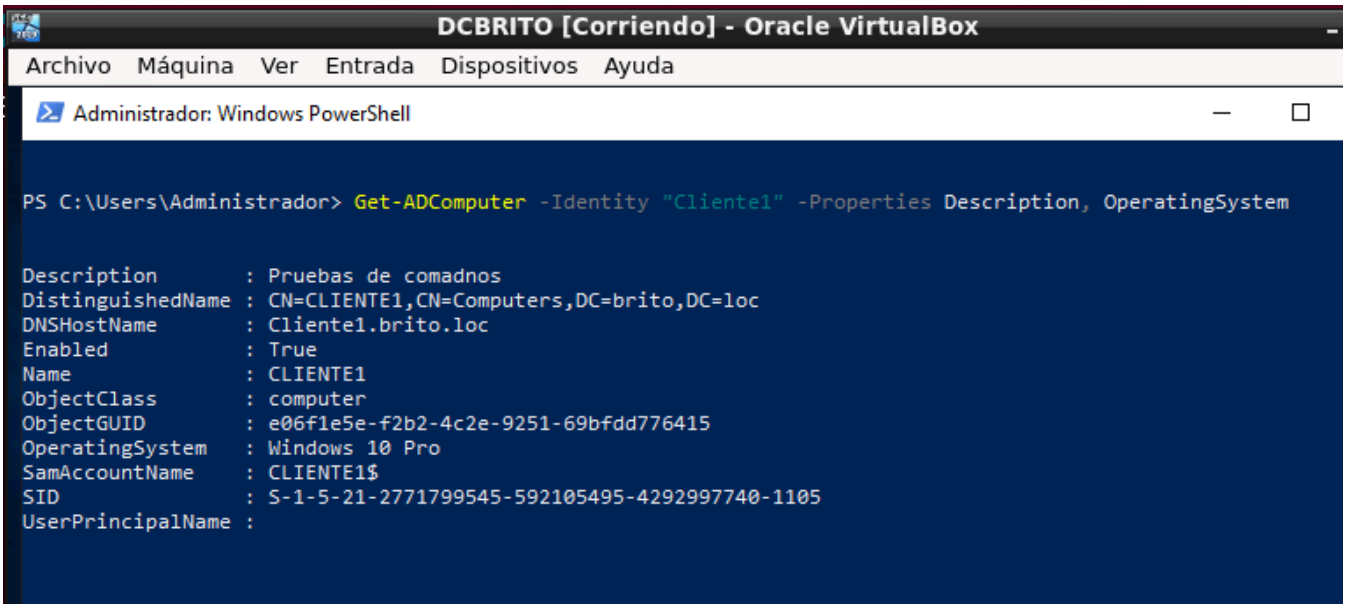


Obtener de un grupo de seguridad sus usuarios.



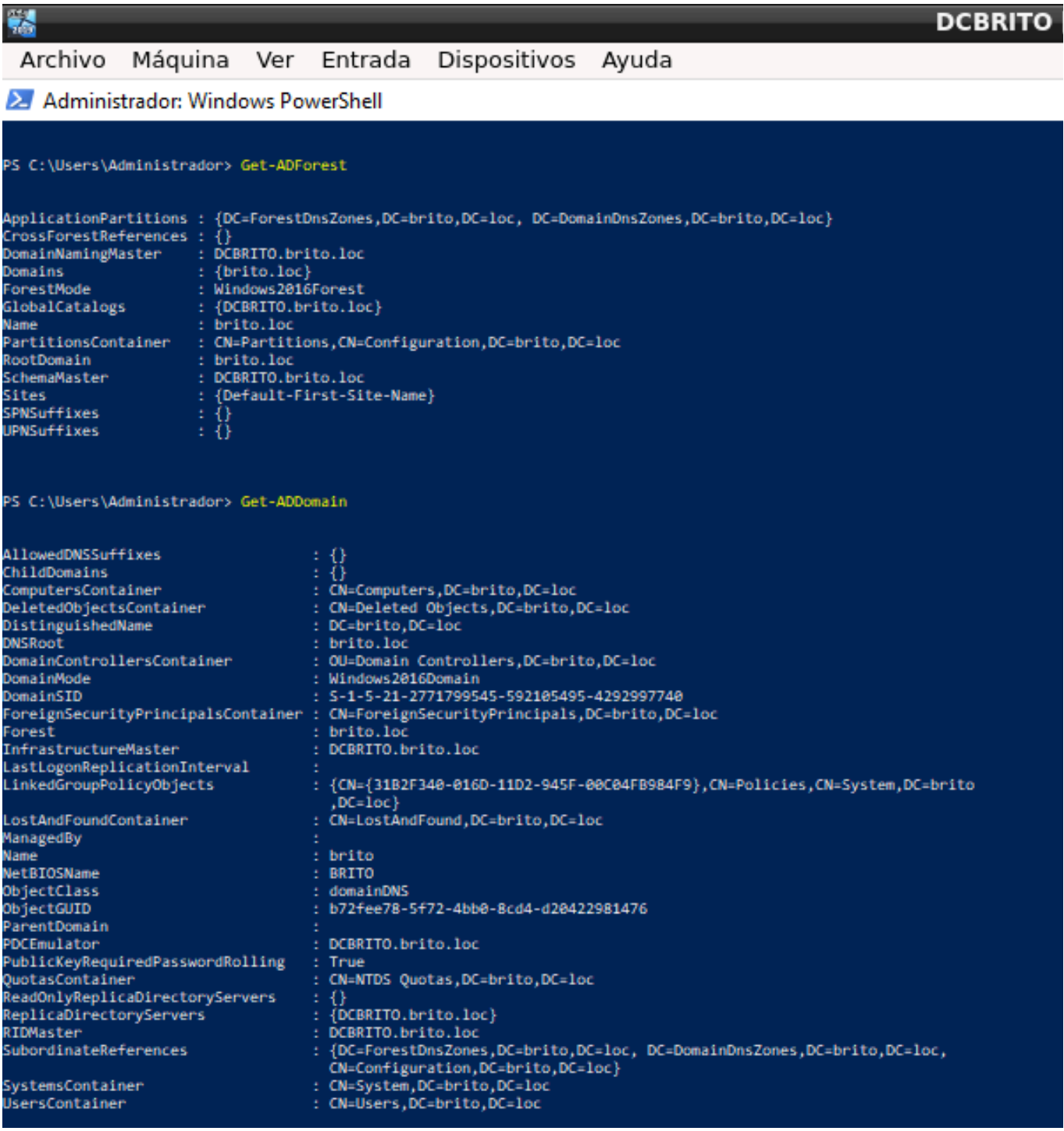
4. Get-ADComputer

Obtener la información esencial de un equipo cliente.



5. Get-ADForest y Get-ADDomain

Para obtener la información sobre el bosque y/o sobre un dominio en concreto.



Ejecuta e investiga cada objeto /atributo que se obtiene.

ANÁLISIS DE GET-ADFOREST

Este comando te da información sobre toda la estructura de Active Directory, que en mi caso se llama brito.loc.

-. Name / RootDomain: brito.loc

Este es el nombre DNS completo del bosque. Es el primer dominio que se creó y es la raíz de todo.

-. ForestMode: Windows2016Forest

Este es el Nivel Funcional del Bosque. Determina las características de AD disponibles en todo el bosque. Un nivel de 2016 significa que todos los Controladores de Dominio (DC) en todos los dominios de tu bosque deben ser, como mínimo, Windows Server 2016.

-. DomainNamingMaster: DCBRITO.brito.loc

Este rol es único en todo el bosque. El servidor DCBRITO es el único que tiene la autoridad para agregar o quitar nuevos dominios al bosque.

-. SchemaMaster: DCBRITO.brito.loc

Este es el segundo Rol FSMO único en el bosque. El DCBRITO es el único servidor que puede realizar cambios en el "esquema" (la plantilla o "blueprint" de Active Directory). Por ejemplo, si instalas un programa como Microsoft Exchange, este necesita añadir nuevos atributos a los usuarios (como "buzón de correo"), y solo puede hacerlo contactando con el Schema Master.

-. GlobalCatalogs: DCBRITO.brito.loc

Esto indica qué servidores son Catálogos Globales (GC). Un GC almacena una copia completa de su propio dominio y una copia parcial de todos los demás dominios del bosque. Es esencial para búsquedas rápidas y para los inicios de sesión de usuarios en dominios diferentes.

ANÁLISIS DE GET-ADDOMAIN

Este comando te da información específica sobre tu dominio (que también es brito.loc, ya que solo tienes uno).

-. NetBIOSName: BRITO

Este es el nombre "corto" o "pre-Windows 2000" de tu dominio. Es el que se usa para iniciar sesión con el formato DOMINIO\usuario (ej. BRITO\Administrator).

-. DomainMode: Windows2016Domain

Este es el Nivel Funcional del Dominio. A diferencia del nivel de bosque, este controla las características dentro de este dominio específico. Debe ser igual o superior al nivel del bosque.

-. DomainSID: S-1-5-21-27...

Este es el Security Identifier (SID) único para tu dominio. Cada objeto (usuario, grupo, equipo) en tu dominio tendrá un SID que comienza con este número, seguido de su propio ID único (RID).

-. PDCEmulator: DCBRITO.brito.loc

Este es el tercer Rol FSMO (único por dominio). Es uno de los más importantes. Se encarga de:

– Sincronizar la hora de todos los equipos del dominio.

– Gestionar los cambios de contraseña (se replican a él primero).

– Ser el servidor al que se conecta la herramienta de Administración de GPOs.

-. RIDMaster: DCBRITO.brito.loc

Este es el cuarto Rol FSMO (único por dominio). El "Maestro RID" es el responsable de dar "paquetes" de RIDs (Relative IDs) a cada DC. Cuando creas un usuario, el DC local le asigna un RID de su paquete para formar el SID completo. Si un DC se queda sin RIDs, le pide más a este maestro.

-. InfrastructureMaster: DCBRITO.brito.loc

Este es el quinto y último Rol FSMO (único por dominio). Se encarga de actualizar las referencias de objetos entre dominios (por ejemplo, si un usuario del Dominio A está en un grupo del Dominio B).

-. ComputersContainer / UsersContainer: CN=Computers... / CN=Users...

Estos son los contenedores por defecto donde se crean los nuevos equipos y usuarios. Es importante notar que son "Contenedores" (CN) y no "Unidades Organizativas" (OU), lo que significa que no puedes aplicarles GPOs directamente. Por eso es una buena práctica redirigirlos a OUs personalizadas.