

PRACTICA 4.bis – INSTALACIÓN DE ACTIVE DIRECTORY e INTEGRACIÓN CON OTROS SERVIDORES.

(Nombre del archivo a subir: XXxx-04-activedirectory.pdf)



A. INSTALACIÓN DE SERVIDOR DE DIRECTORIO LDAP mediante ACTIVE DIRECTORY

1. Montar en un servidor Microsoft Windows Server 2016 un controlador de dominio en la forma XXxx.com.

WSERVER-MORALESESPEJO X

Asistente para configuración de Servicios de dominio de Active Directory

Revisar opciones

SERVIDOR DE DESTINO
MORALES-SERVER

Configuración de implem...
Opciones del controlador...
Opciones de DNS
Opciones adicionales
Rutas de acceso
Revisar opciones
Comprobación de requisi...
Instalación
Resultado

Revisar las selecciones:

Configura este servidor como el primer controlador de dominio de Active Directory en un nuevo bosque.

El nombre del nuevo dominio es "moralesespejo.com". Éste es también el nombre del nuevo bosque.

El nombre NetBIOS del dominio es MORALESESPEJO.

Nivel funcional del bosque: Windows Server 2016
Nivel funcional del dominio: Windows Server 2016

Opciones adicionales:

Catálogo global: Sí

Servidor DNS: Sí

Crear delegación DNS: No

Carpeta de la base de datos: C:\Windows\NTDS

Carpeta del archivo de registro: C:\Windows\NTDS

Carpeta SYSVOL: C:\Windows\SYSVOL

El servicio Servidor DNS se configurará en este equipo.

Este equipo se configurará para usar este servidor DNS como servidor DNS preferido.

La contraseña del nuevo administrador de dominio será la misma que la del administrador local de este equipo.

características de nuestro nuevo dominio

Esta configuración se puede exportar a un script de Windows PowerShell para automatizar instalaciones adicionales

Más información sobre opciones de instalación

< Anterior

Siguiente >

Instalar

Cancelar

Usuarios y equipos de Active Directory

Archivo Acción Ver Ayuda

Usuarios y equipos de Active Dir

- Consultas guardadas
- moralesespejo.com**

ya lo tenemos creado

Nombre	Tipo	Descripción
Builtin	builtinDomain	
Computers	Contenedor	Default container for up...
Domain Con...	Unidad organi...	Default container for do...
ForeignSecu...	Contenedor	Default container for sec...
Managed Se...	Contenedor	Default container for ma...
Users	Contenedor	Default container for up...

2. Añadir usando el **modo gráfico** la siguiente estructura, adaptándolo lo máximo posible a lo que aquí aparece a su introducción en Active Directory.

- Los hosts siguientes de nuestra organización adaptados a nuestro esquema de clase.

dn: cn=equipo1,ou=hosts,dc=XXxx,dc=com

dn: cn=equipo2,ou=hosts,dc=XXxx,dc=com

- Unidades organizativas en la forma:

dn: ou=profesores,ou=usuarios,dc=XXxx,dc=com

dn: ou=alumnos,ou=usuarios,dc=XXxx,dc=com

dn: ou=informaticos,ou=usuarios,dc=XXxx,dc=com

dn: ou=hosts,dc=XXxx,dc=com

- Usuarios en la siguiente forma, cada uno dentro de su unidad organizativa.

dn: uid=Profesor1,ou=profesores,ou=usuarios,dc=XXxx,dc=com

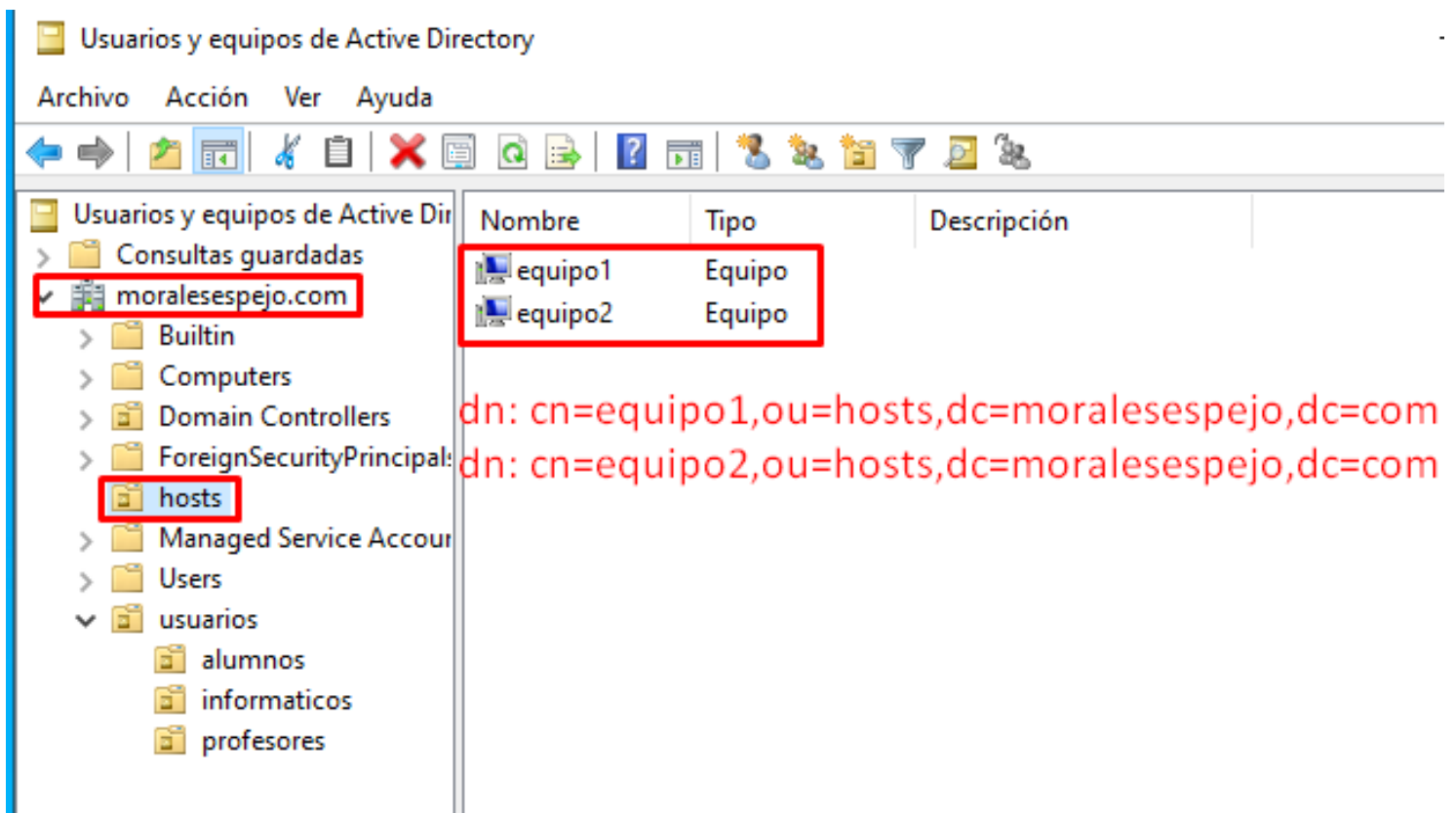
dn: uid=Profesor2,ou=profesores,ou=usuarios,dc=XXxx,dc=com

dn: uid=Alumno1,ou=alumnos,ou=usuarios,dc=XXxx,dc=com

dn: uid=Alumno2,ou=alumnos,ou=usuarios,dc=XXxx,dc=com

dn: uid=Informatico1,ou=informaticos,ou=usuarios,dc=XXxx,dc=com

dn: uid=Informatico2,ou=informaticos,ou=usuarios,dc=XXxx,dc=com



Nombre	Tipo	Descripción
equipo1	Equipo	
equipo2	Equipo	

dn: cn=equipo1,ou=hosts,dc=moralesespejo,dc=com
dn: cn=equipo2,ou=hosts,dc=moralesespejo,dc=com

Usuarios y equipos de Active Directory

Archivo Acción Ver Ayuda

Usuarios y equipos de Active Directory

Consultas guardadas

moralesespejo.com

Builtin

Computers

Domain Controllers

ForeignSecurityPrincipals

hosts

Managed Service Accounts

Users

usuarios

alumnos

informaticos

profesores

Nombre	Tipo	Descripción
Alumno1	Usuario	
Alumno2	Usuario	

dn: uid=Alumno1,ou=alumnos,ou=usuarios,dc=moralesespejo,dc=com
dn: uid=Alumno2,ou=alumnos,ou=usuarios,dc=moralesespejo,dc=com

Usuarios y equipos de Active Directory

Archivo Acción Ver Ayuda

Usuarios y equipos de Active Directory

Consultas guardadas

moralesespejo.com

Builtin

Computers

Domain Controllers

ForeignSecurityPrincipals

hosts

Managed Service Accounts

Users

usuarios

alumnos

informaticos

profesores

Nombre	Tipo	Descripción
Informatico1	Usuario	
Informatico2	Usuario	

dn: uid=Informatico1,ou=informaticos,ou=usuarios,dc=moralesespejo,dc=com
dn: uid=Informatico2,ou=informaticos,ou=usuarios,dc=moralesespejo,dc=com

Usuarios y equipos de Active Directory

Archivo Acción Ver Ayuda



- Usuarios y equipos de Active Directory
 - Consultas guardadas
 - moralesespejo.com
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipal
 - hosts
 - Managed Service Accounts
 - Users
 - usuarios
 - alumnos
 - informaticos
 - profesores

Nombre	Tipo	Descripción
Profesor1	Usuario	
Profesor2	Usuario	

dn: uid=Profesor1,ou=profesores,ou=usuarios,dc=moralesespejo,dc=com
dn: uid=Profesor2,ou=profesores,ou=usuarios,dc=moralesespejo,dc=com

3. Usando el modo gráfico, cree tres grupos de seguridad de ámbito local de dominio (profesores, alumnos e informáticos) e introducir los usuarios correspondientes en los mismos.

Usuarios y equipos de Active Directory

Archivo Acción Ver Ayuda

Usuarios y equipos de Active Dir

Consultas guardadas

moralesespejo.com

Builtin

Computers

Domain Controllers

ForeignSecurityPrincipal:

hosts

Managed Service Account

Users

usuarios

grupos

Nombre	Tipo	Descripción
alumnos	Grupo de seguridad - Dominio local	
informaticos	Grupo de seguridad - Dominio local	
profesores	Grupo de seguridad - Dominio local	

no lo indicaba la tarea pero he creado una UO de grupos para poder guardar los grupos ahí y tenerlos todos de manera más estructurada que tenerlos sueltos colgando del dominio los grupos

Propiedades: informaticos

General Miembros Miembro de Administrado por

Miembros:

Nombre	Carpeta de los Servicios de dominio de Active Dir...
Informatico1	moralesespejo.com/usuarios/informaticos
Informatico2	moralesespejo.com/usuarios/informaticos

miembros del grupo informaticos

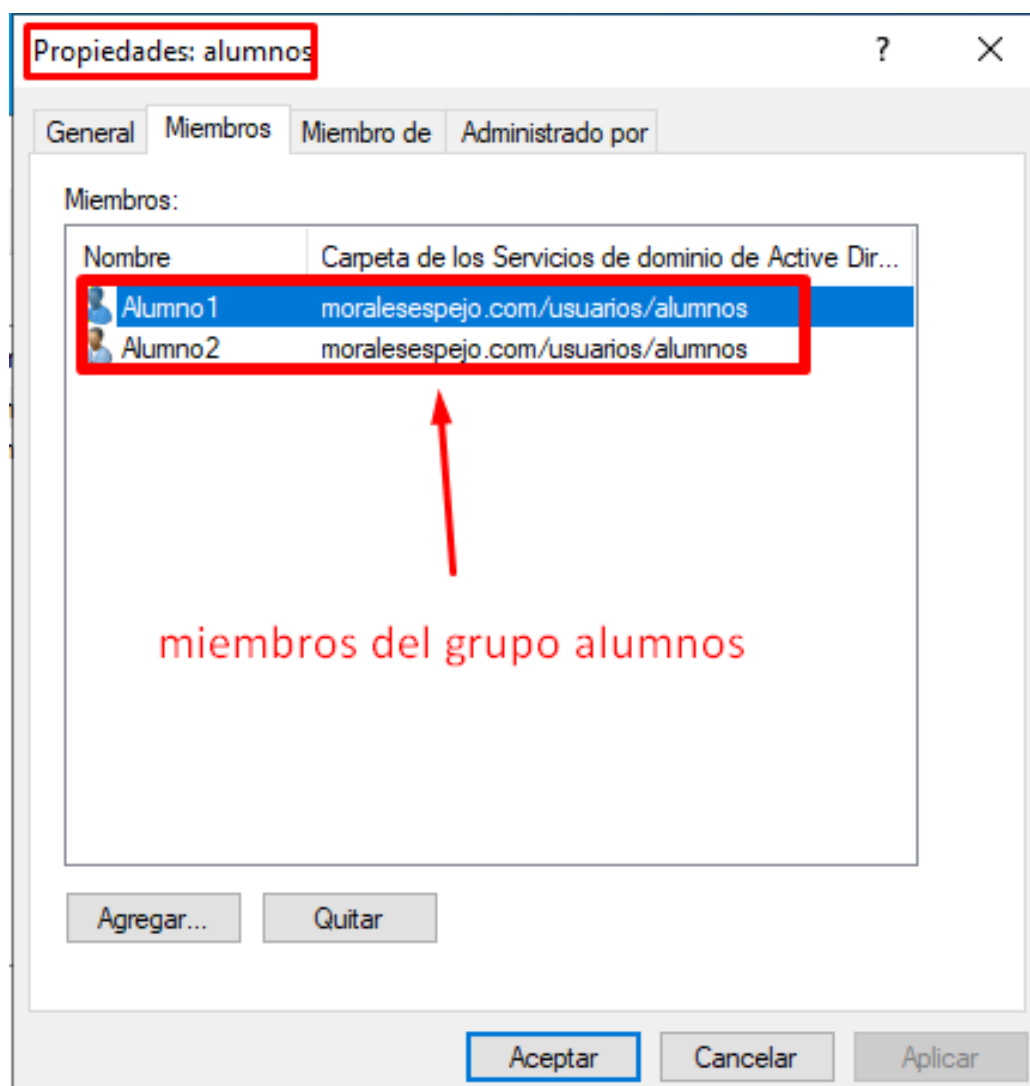
Propiedades: profesores

General Miembros Miembro de Administrado por

Miembros:

Nombre	Carpeta de los Servicios de dominio de Active Dir...
Profesor1	moralesespejo.com/usuarios/profesores
Profesor2	moralesespejo.com/usuarios/profesores

miembros del grupo profesores



4. En relación a los perfiles de usuarios:

- Los usuarios del grupo Alumnos tendrán perfil local. Se asume que estos usuarios usan siempre el mismo ordenador del instituto.

Alumno1 Usuario

Alumno2 Usuario

Propiedades: Alumno1

Marcado Entorno Sesiones Control remoto

Perfil de Servicios de Escritorio remoto COM+

General Dirección Cuenta Perfil Teléfonos Organización Miembro de

Perfil de usuario

Ruta de acceso al perfil:

Script de inicio de sesión:

Carpeta particular

☒ Ruta de acceso local:

☐ Conectar: a:

como los alumnos van a tener un perfil local, por defecto ya tienen el perfil local si dejamos estos campos en blanco en la opción "perfil". Los dejamos en blanco para los dos Alumnos.

Aceptar Cancelar Aplicar Ayuda

- Los usuarios del grupo Profesores tendrán perfil móvil, ya que se mueven por diferentes clases.

creamos la carpeta en disco local C,
por ejemplo

una vez la compartamos, copiamos la ruta

como los usuarios profesores van a tener un perfil móvil, necesitaremos crear una carpeta y compartirla con estos usuario o grupo solamente, para que puedan guardar su perfil.

Le asignamos control total.

Nombre	Fecha de modificación	Tipo	Tamaño
Archivos de programa	29/12/2022 13:57	Carpeta de archivos	
PerfLogs	08/05/2021 10:20	Carpeta de archivos	
Program Files (x86)	08/05/2021 17:06	Carpeta de archivos	
Usuarios	29/12/2022 13:56	Carpeta de archivos	
Windows	29/12/2022 14:06	Carpeta de archivos	
Perfiles	29/12/2022 17:54	Carpeta de archivos	

Propiedades: Perfiles

General Compartir Seguridad Versiones anteriores Personalizar

Uso compartido de carpetas y archivos de red

Perfiles
Compartido

Ruta de acceso de red:
\\MORALES-SERVER\Perfiles

Compartir...

Permisos de Perfiles

Permisos de los recursos compartidos

Nombres de grupos o usuarios:

profesores (MORALESSESPEJO\profesores)

Agregar... Quitar

Permisos de profesores	Permitir	Denegar
Control total	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Cambiar	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Leer	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Nombre	Tipo	Descripción
Profesor1	Usuario	
Profesor2	Usuario	

Propiedades: Profesor1 ? X

Marcado	Entorno	Sesiones	Control remoto			
Perfil de Servicios de Escritorio remoto			COM+			
General	Dirección	Cuenta	Perfil	Teléfonos	Organización	Miembro de

Perfil de usuario

Ruta de acceso al perfil: ORALES-SERVER\Perfiles\%username%

Script de inicio de sesión:

Carpeta particular

☒ Ruta de acceso local:

☐ Conectar: a:

nos vamos al usuario y en su opción perfil, en ruta de acceso al perfil, pegamos la ruta y añadimos al final %username% para que se cree una carpeta con el nombre del usuario

HACEMOS LO MISMO PARA EL OTRO USUARIO PROFESOR

Cuando iniciemos en otro ejercicio más adelante con estos usuarios, observaremos como se le aplica el perfil móvil.

5. Cree tres carpetas que se llame XXXxprofesores, XXXxalumnos y XXXxInformaticos que serán vistas únicamente por los usuarios de cada grupo en cuestión, haciendo uso de los grupos de seguridad y no de las cuentas de usuario directamente.

The screenshot shows a Windows File Explorer window on the left with a list of folders. Three folders are highlighted with a red box: 'moralesespejoALUMNOS', 'moralesespejoINFORMATICOS', and 'moralesespejoPROFESORES'. To the right, two dialog boxes are open. The top one is 'Propiedades: moralesespejoPROFESORES' with the 'Compartir' tab selected. It shows the folder is shared as 'moralesespejoPROFESORES' and the network path is '\\MORALES-SERVER\\moralesespejoPROFESORES'. The bottom dialog is 'Permisos de moralesespejoPROFESORES', showing the 'profesores (MORALESSESPEJO\\profesores)' group selected. Below, a table shows permissions for the 'profesores' group.

Nombre

Fecha de modificación

Tipo

Tamaño

29/12/2022 21:49

Carpeta de archivos

Propiedades: moralesespejoPROFESORES

General Compartir Seguridad Versiones anteriores Personalizar

Uso compartido de carpetas y archivos de red

copiamos la ruta

moralesespejoPROFESORES Compartido

Ruta de acceso de red: \\MORALES-SERVER\\moralesespejoPROFESORES

Compartir...

Permisos de moralesespejoPROFESORES

Permisos de los recursos compartidos

Nombres de grupos o usuarios:

Administrador (Administrador@moralesespejo.com)

profesores (MORALESSESPEJO\\profesores)

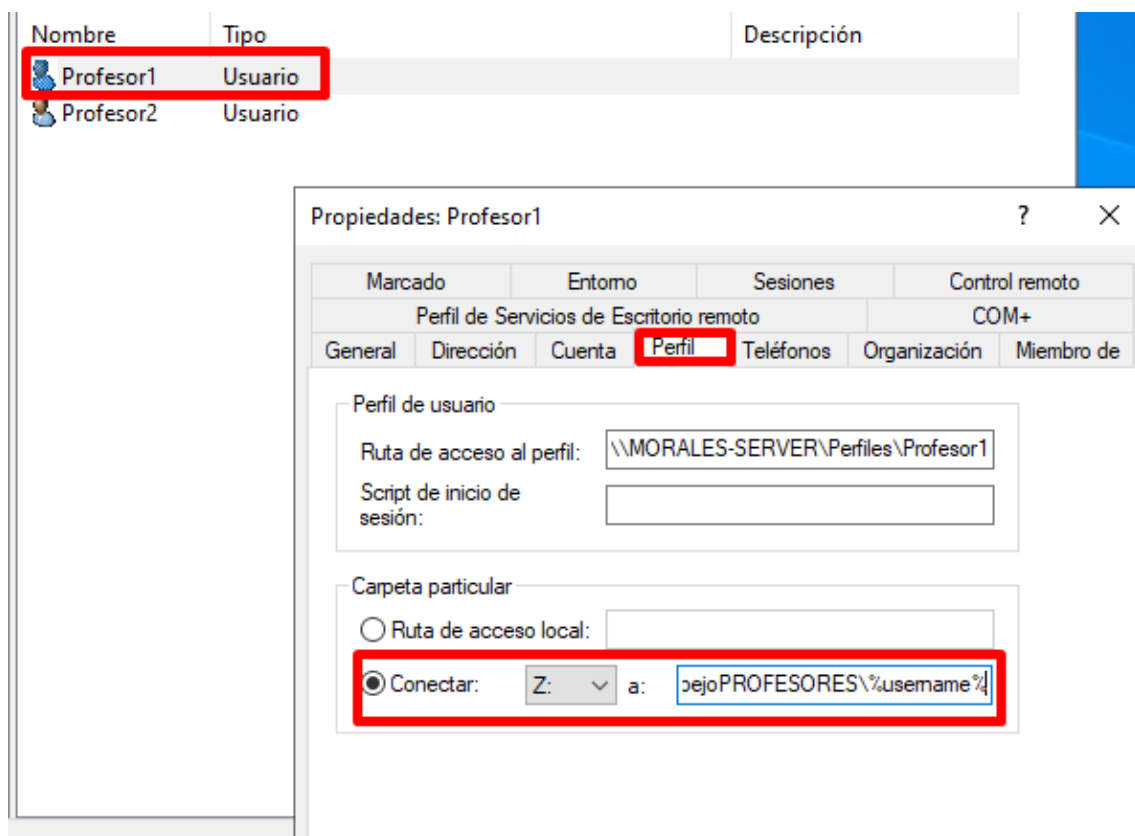
Agregar... Quitar

Permisos de profesores	Permitir	Denegar
Control total	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Cambiar	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Leer	<input checked="" type="checkbox"/>	<input type="checkbox"/>

creamos las carpetas y las compartimos con sus grupos correspondientes.

He añadido el usuario administrador también, lo explico en la siguiente captura

elemento seleccionado



Pegamos la ruta y al final ponemos %username%. Al ser una carpeta particular, cuando peguemos la dirección aquí, cuando le demos a aplicar, %username% se cambiará por el nombre del usuario y por tanto se creará la carpeta del usuario. Como estamos como administradores del dominio, necesitamos que el administrador pueda crear la carpeta y tenga permisos sobre ella, es por ello que tiene que tener ese permiso para crear la carpeta. Una vez se cree dándole a aplicar, podemos quitar el usuario administrador.

Hacemos lo mismo para el resto de usuarios y carpetas.

6. Sacar un backup en formato CSV y en formato LDIF.

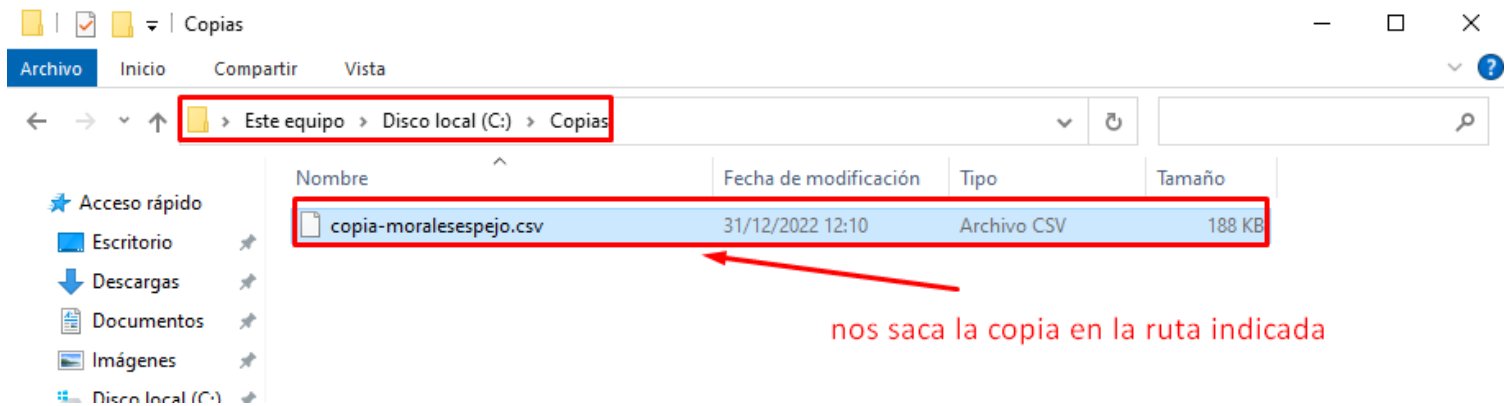
CSV

```
Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.20348.587]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Administrador>csvde -f C:\Copias\copia-moralesespejo.csv -s MORALES-SERVER -d "dc=moralesespejo,dc=com"
Conectándose a "MORALES-SERVER"
Iniciando sesión como usuario actual usando SSPI
Exportando el directorio al archivo C:\Copias\copia-moralesespejo.csv
Buscando entradas...
Escribiendo entradas
.....
Exportación completada. Posprocesamiento en curso...
258 entradas exportadas

El comando se completó correctamente
C:\Users\Administrador>
```

se hace la copia en CSV



nos saca la copia en la ruta indicada

The screenshot shows an Excel spreadsheet with the content of the CSV file. The first row contains column headers, and the subsequent rows contain directory entry data. A red text annotation points to the spreadsheet.

1	DN,objectClass,distinguishedName,instanceType,whenCreated,whenChanged,subRefs,uSNCreated,dSASignature,uSNChanged,name,objectGUID,repUpToDateVector,creationTime,forceLogoff,lockoutDuration,lockOutObservationWindow,lockoutThreshold,maxPwdAge,minPwdLength,modifiedCountAtLastProm,nextRid,pwdProperties,pwdHistoryLength,objectSid,serverState,uASCompat,modifiedCount,auditingPolicy,nTMMixedDomain,rIDManagerReference,fSMORoleOwner,systemFlags,wellKnownObjects,objectCategory,isCriticalSystem	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
1	DC=moralesespejo,DC=Domain	CN=Configur	B:32:F4BE92/B:32:09460C/B:32:22B70C/B:32:18E2EA/B:32:2FBAC1/B:32:AB8153/B:32:AB1D30/B:32:A361B2/B:32:AA3128/B:32:A9D1CA01",16010101 B:32:1EB93889E40C45DF9FC64D238BB6237																			
2	CN=Users,DC=20221229130 16010101000416.0Z,,,	Users,Default container for upgraded user accounts,FALSE,,,																				
3	CN=Computers,DC=20221229130 16010101000416.0Z,,,	Computers,Default container for upgraded computer accounts,FALSE,,,																				
4	OU=Domain Controllers,DC=20221229130 16010101000416.0Z,,,	Default container for domain controllers,FALSE,Domain Controllers,,,																				
5	CN=System,DC=20221229130 16010101000416.0Z,,,	System,Built-in system settings,TRUE,,,																				
6	CN=LostAndFound,DC=20221229130 16010101000416.0Z,,,	LostAndFound,Default container for orphaned objects,TRUE,,,																				
7	CN=Infrastructure,DC=20221229130 16010101000416.0Z,,,	Infrastructure,TRUE,,,																				
8	CN=ForeignSecurityPrincipals,DC=20221229130 16010101000416.0Z,,,	ForeignSecurityPrincipals,"Default container for security identifiers (SIDs) associated with objects from external, trusted domains",FALSE,,,																				
9	CN=Program Data,DC=20221229130 16010101000416.0Z,,,	Program Data,Default location for storage of application data,,TRUE,,,																				
10	CN=Microsoft Windows,DC=20221229130 16010101000001.0Z,,,	Microsoft,Default location for storage of Microsoft application data,,TRUE,,,																				
11	CN=NTDS Quotas,DC=20221229130 16010101000416.0Z,,,	NTDS Quotas,Quota specifications container,TRUE,,100,,,																				
12	CN=Managed Service Accounts,DC=20221229130 16010101000416.0Z,,,	Managed Service Accounts,Default container for managed service accounts,FALSE,,,																				
13	CN=Keys,DC=20221229130 16010101000000.0Z,,,	Keys,Default container for key objects,TRUE,,,																				
14	CN=Winsock,DC=20221229130 16010101000001.0Z,,,	WinsockServices,TRUE,,,																				
15	CN=RpcServices,DC=20221229130 16010101000001.0Z,,,	RpcServices,TRUE,,,																				
16	CN=FileLinks,DC=20221229130 16010101000001.0Z,,,	FileLinks,TRUE,,,																				
17	CN=VolumeTable,DC=20221229130 16010101000000.0Z,,,	VolumeTable,TRUE,,,																				
18	CN=ObjectMoveTable,DC=20221229130 16010101000001.0Z,,,	ObjectMoveTable,TRUE,,,																				
19	CN=Default Domain Policy,DC=20221229130 16010101000001.0Z,,,	Default Domain Policy,TRUE,,,																				
20	CN=AppCategories,DC=20221229130 16010101000001.0Z,,,	AppCategories,TRUE,,,																				
21	CN=Meeting,DC=20221229130 16010101000001.0Z,,,	Meetings,TRUE,,,																				

SI LO ABRIMOS CON EXCEL, VEMOS TODO EL CONTENIDO DEL FICHERO CSV

LDIF

```
Administrador: Símbolo del sistema

C:\Users\Administrador>ldifde -f C:\Copias\copia-moralesespejo.ldif -s MORALES-SERVER -d "dc=moralesespejo,dc=com"
Conectándose a "MORALES-SERVER"
Iniciando sesión como usuario actual usando SSPI
Exportando el directorio al archivo C:\Copias\copia-moralesespejo.ldif
Buscando entradas...
Escribiendo entradas.....
.....
258 entradas exportadas

El comando se completó correctamente
```

se nos genera la copia en formato ldif

Archivos y carpetas

Inicio Compartir Vista

Este equipo > Disco local (C:) > Copias

Nombre	Fecha de modificación	Tipo	Tamaño
copia-moralesespejo.csv	31/12/2022 12:10	Archivo CSV	188 KB
copia-moralesespejo.ldif	31/12/2022 12:17	Archivo LDIF	228 KB

se nos genera en la ruta indicada

copia-moralesespejo.ldif: Bloc de notas

Archivo Edición Formato Ver Ayuda

```
whenCreated: 20221229132727.0Z
whenChanged: 20221229132727.0Z
uSNCreated: 16399
uSNChanged: 16400
name: profesores
objectGUID:: deaR6WAZe0SFd07V+warCQ==
objectCategory:
  CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=moralesespejo,DC=com
dSCorePropagationData: 20221229132727.0Z
dSCorePropagationData: 20221229132727.0Z
dSCorePropagationData: 16010101000000.0Z

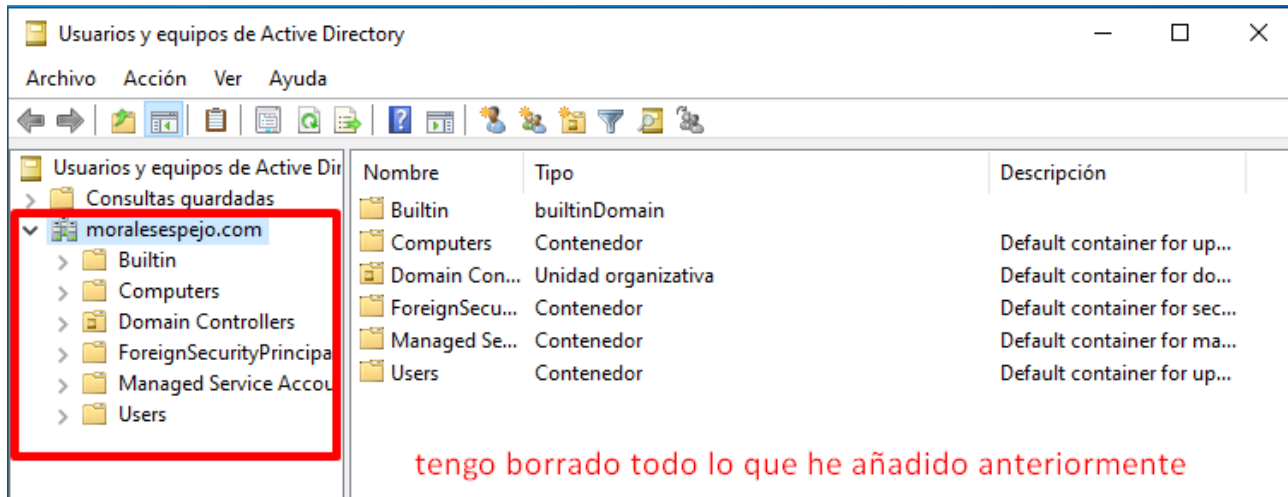
dn: OU=alumnos,OU=usuarios,DC=moralesespejo,DC=com
changetype: add
objectClass: top
objectClass: organizationalUnit
ou: alumnos
distinguishedName: OU=alumnos,OU=usuarios,DC=moralesespejo,DC=com
instanceType: 4
whenCreated: 20221229132742.0Z
whenChanged: 20221229132742.0Z
uSNCreated: 16407
uSNChanged: 16408
```

se nos ha realizado perfectamente en formato ldif

B. POWERSHELL EN MICROSOFT WINDOWS (MODO COMANDO)

Borrar toda la estructura anteriormente (crear un snapshot), ya que vamos a realizar la misma operación que el punto 2 y el punto 3, usando el interfaz de commando de Microsoft Windows Powershell. Para continuar con el ejercicio tiene que estar completamente vacía.

7. Añadir la misma información introducida usando comandos.



tengo borrado todo lo que he añadido anteriormente

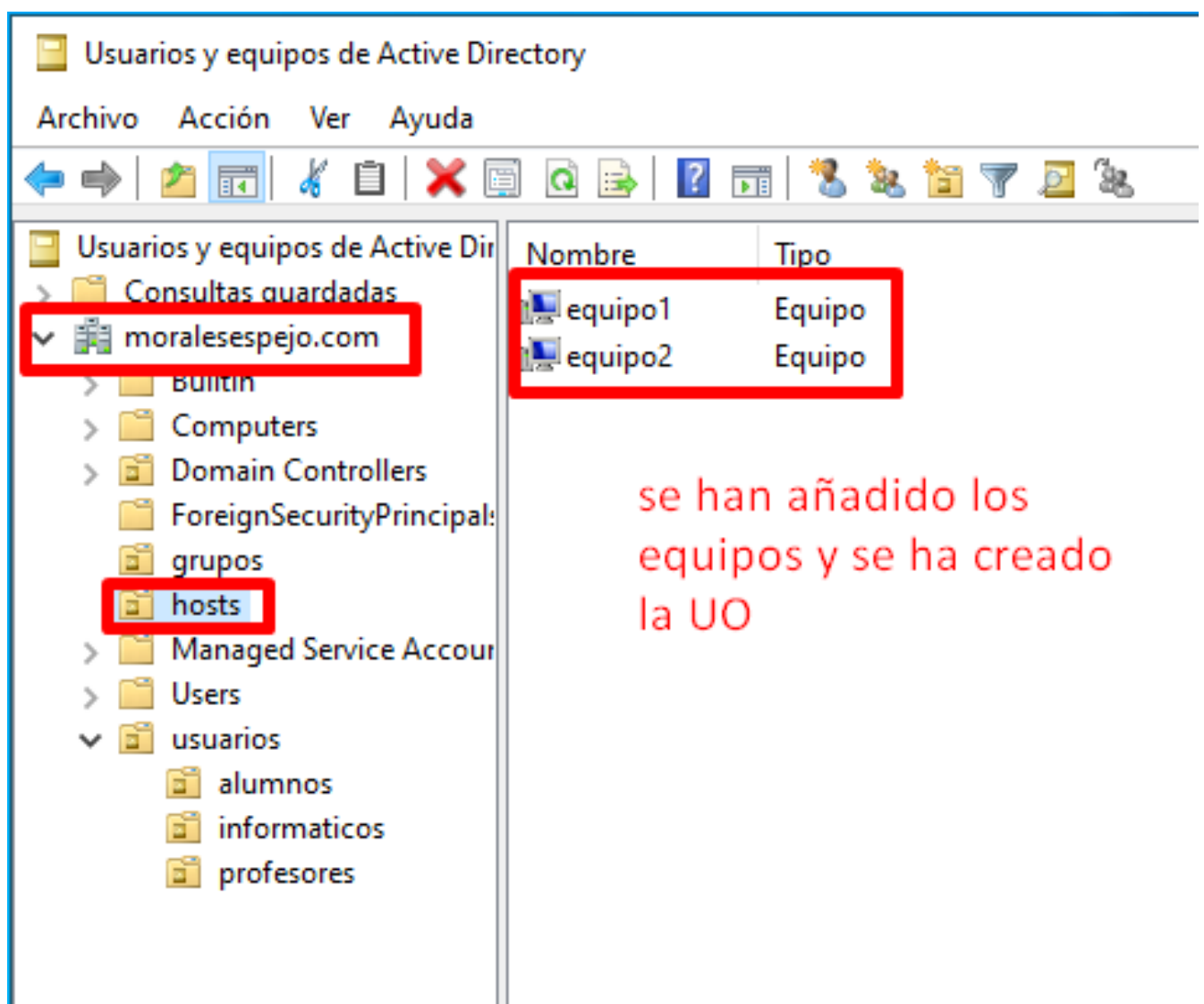
```
Administrador: Windows PowerShell
PS C:\Users\Administrador> echo Raul Morales Espejo
Raul
Morales
Espejo
PS C:\Users\Administrador> new-adorganizationalunit -name hosts
PS C:\Users\Administrador> new-adorganizationalunit -name usuarios
PS C:\Users\Administrador> new-adorganizationalunit -name "alumnos" -path "OU=usuarios,DC=moralesespejo,DC=com"
PS C:\Users\Administrador> new-adorganizationalunit -name "informaticos" -path "OU=usuarios,DC=moralesespejo,DC=com"
PS C:\Users\Administrador> new-adorganizationalunit -name "profesores" -path "OU=usuarios,DC=moralesespejo,DC=com"
PS C:\Users\Administrador> new-adorganizationalunit -name "grupos" -path "DC=moralesespejo,DC=com"
PS C:\Users\Administrador> new-adcomputer -name "equipo1" -path "OU=hosts,DC=moralesespejo,DC=com"
PS C:\Users\Administrador> new-adcomputer -name "equipo2" -path "OU=hosts,DC=moralesespejo,DC=com"
PS C:\Users\Administrador> new-aduser -name "Alumno1" -userprincipalname "Alumno1@moralesespejo.com" -displayname "Alumno1" -givenname "Alu
mo1" -samaccountname "Alumno1" -path "OU=alumnos,OU=usuarios,DC=moralesespejo,DC=com" -accountpassword(read-host -assecurestring "Introduz
ca contraseña") -enabled $true
Introduzca contraseña: *****
PS C:\Users\Administrador> new-aduser -name "Alumno2" -userprincipalname "Alumno2@moralesespejo.com" -displayname "Alumno2" -givenname "Alu
mo2" -samaccountname "Alumno2" -path "OU=alumnos,OU=usuarios,DC=moralesespejo,DC=com" -accountpassword(read-host -assecurestring "Introduz
ca contraseña") -enabled $true
Introduzca contraseña: *****
PS C:\Users\Administrador> new-aduser -name "Informatico1" -userprincipalname "Informatico1@moralesespejo.com" -displayname "Informatico1"
-givenname "Informatico1" -samaccountname "Informatico1" -path "OU=informaticos,OU=usuarios,DC=moralesespejo,DC=com" -accountpassword(read-
host -assecurestring "Introduzca contraseña") -enabled $true
Introduzca contraseña: *****
PS C:\Users\Administrador> new-aduser -name "Informatico2" -userprincipalname "Informatico2@moralesespejo.com" -displayname "Informatico2"
-givenname "Informatico2" -samaccountname "Informatico2" -path "OU=informaticos,OU=usuarios,DC=moralesespejo,DC=com" -accountpassword(read-
host -assecurestring "Introduzca contraseña") -enabled $true
Introduzca contraseña: *****
PS C:\Users\Administrador> new-aduser -name "Profesor1" -userprincipalname "Profesor1@moralesespejo.com" -displayname "Profesor1" -givennam
e "Profesor1" -samaccountname "Profesor1" -path "OU=profesores,OU=usuarios,DC=moralesespejo,DC=com" -accountpassword(read-host -assecurestr
ing "Introduzca contraseña") -enabled $true
Introduzca contraseña: *****
PS C:\Users\Administrador> new-aduser -name "Profesor2" -userprincipalname "Profesor2@moralesespejo.com" -displayname "Profesor2" -givennam
e "Profesor2" -samaccountname "Profesor2" -path "OU=profesores,OU=usuarios,DC=moralesespejo,DC=com" -accountpassword(read-host -assecurestr
ing "Introduzca contraseña") -enabled $true
Introduzca contraseña: *****
PS C:\Users\Administrador>
```

```
Administrador: Windows PowerShell

PS C:\Users\Administrador> new-adgroup -name "informaticos" -samaccountname informaticos -groupcategory security -groupscope DomainLocal -path "OU=grupos,DC=moralesespejo,DC=com"
PS C:\Users\Administrador> new-adgroup -name "profesores" -samaccountname profesores -groupcategory security -groupscope DomainLocal -path "OU=grupos,DC=moralesespejo,DC=com"
PS C:\Users\Administrador> new-adgroup -name "alumnos" -samaccountname alumnos -groupcategory security -groupscope DomainLocal -path "OU=grupos,DC=moralesespejo,DC=com"
PS C:\Users\Administrador>
PS C:\Users\Administrador> add-adgroupmember "informaticos" informatico1,informatico2
PS C:\Users\Administrador> add-adgroupmember "alumnos" alumno1,alumno2
PS C:\Users\Administrador> add-adgroupmember "profesores" profesor1,profesor2
PS C:\Users\Administrador>
```

creamos los grupos

añadimos los usuarios a los grupos



Usuarios y equipos de Active Directory

Archivo Acción Ver Ayuda

Usuarios y equipos de Active Directory

- Consultas guardadas
- moralesespejo.com**
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipal...
 - grupos**
 - hosts

Nombre	Tipo	Descripción
alumnos	Grupo de seguridad - Dominio local	
informaticos	Grupo de seguridad - Dominio local	
profesores	Grupo de seguridad - Dominio local	

se han creado los grupos y cada uno con sus usuarios asignados

Propiedades: alumnos

Propiedades: informaticos

Propiedades: profesores

General Miembros Miembro de Administrado por

Miembros:

Nombre	Carpeta de los Servicios de dominio de Active Dir...
Alumno1	moralesespejo.com/usuarios/alumnos
Alumno2	moralesespejo.com/usuarios/alumnos

Miembros:

Nombre	Carpeta de los Servicios de dominio de Active Dir...
Informatico1	moralesespejo.com/usuarios/informaticos
Informatico2	moralesespejo.com/usuarios/informaticos

Miembros:

Nombre	Carpeta de los Servicios de dominio de Active Dir...
Profesor1	moralesespejo.com/usuarios/profesores
Profesor2	moralesespejo.com/usuarios/profesores

Usuarios y equipos de Active Directory

Archivo Acción Ver Ayuda

Usuarios y equipos de Active Directory

- Consultas guardadas
- moralesespejo.com**
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipal...
 - grupos
 - hosts
 - Managed Service Accour...
 - Users
 - usuarios**
 - alumnos**
 - informaticos
 - profesores

Nombre	Tipo
Alumno1	Usuario
Alumno2	Usuario

alumnos creados y su UO

Usuarios y equipos de Active Directory

Archivo Acción Ver Ayuda

Usuarios y equipos de Active Dir

moralesespejo.com

- Builtin
- Computers
- Domain Controllers
- ForeignSecurityPrincipal:
- grupos
- hosts
- Managed Service Accour
- Users
- usuarios
- alumnos
- informaticos
- profesores

Nombre	Tipo
Informatico1	Usuario
Informatico2	Usuario

informaticos creados con su UO

Usuarios y equipos de Active Directory

Archivo Acción Ver Ayuda

Usuarios y equipos de Active Dir

moralesespejo.com

- Builtin
- Computers
- Domain Controllers
- ForeignSecurityPrincipal:
- grupos
- hosts
- Managed Service Accour
- Users
- usuarios
- alumnos
- informaticos
- profesores

Nombre	Tipo
Profesor1	Usuario
Profesor2	Usuario

profesores creados con su UO

8. Acceder desde un cliente LDAP Windows (Jxplorer y Softerra, etc.) y desde la línea de comando de un sistema operativo GNU/Linux y Microsoft Windows, para comprobar/ver los objetos añadidos.

JXplorer - ldap

File Edit View Bookmark Search LDIF Options Tools Security Help

cn = Quick Search

Explore Results Schema

World

- com
 - moralesespejo
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - grupos
 - alumnos
 - informaticos
 - profesores
 - hosts
 - equipo1
 - equipo2
 - Infrastructure
 - Keys
 - LostAndFound
 - Managed Service Accounts
 - NTDS Quotas
 - Program Data
 - System
 - TPM Devices
 - Users
 - alumnos
 - Alumno1
 - Alumno2
 - informaticos
 - Informatico1
 - Informatico2
 - profesores
 - Profesor1
 - Profesor2

HTML View Table Editor

attribute type	value
cn	Alumno1
instanceType	4
nTSecurityDescriptor	
objectCategory	CN=Person,CN=Schema,CN=Configuration,DC=moralesespejo,DC=com
objectClass	organizationalPerson
objectClass	person
objectClass	top
objectClass	user
accountExpires	9223372036854775807
badPasswordTime	0
badPwdCount	0
codePage	0
countryCode	0
displayName	Alumno1
distinguishedName	CN=Alumno1,OU=alumnos,OU=usuarios,DC=moralesespejo,DC=com
dSCorePropagationData	16010101000000.0Z
givenName	Alumno1
lastLogoff	0
lastLogon	0
logonCount	0
memberOf	CN=alumnos,OU=grupos,DC=moralesespejo,DC=com
name	Alumno1
objectGUID	(non string data)
objectSid	(non string data)
primaryGroupID	513
pwdLastSet	133169599254872234
sAMAccountName	Alumno1
sAMAccountType	805306368
userAccountControl	512
userPrincipalName	Alumno1@moralesespejo.com
uSNCreated	41074
whenChanged	20221231113205.0Z
whenCreated	20221231113205.0Z

Softerra LDAP Administrator 2022

morales > OU=hosts > CN=equipo1

File Edit View Favorites Server Entry Schema Tools Window Help

New (objectClass=*)

Scope Pane

- morales
 - CN=Builtin
 - CN=Computers
 - OU=Domain Controllers
 - CN=ForeignSecurityPrincipals
 - OU=grupos
 - CN=alumnos
 - CN=informaticos
 - CN=profesores
 - OU=hosts
 - CN=equipo1
 - CN=equipo2
 - CN=Infrastructure
 - CN=Keys
 - CN=LostAndFound
 - CN=Managed Service Accounts
 - CN=NTDS Quotas
 - CN=Program Data
 - CN=System
 - CN=Users
 - OU=usuarios
 - OU=alumnos
 - CN=Alumno1
 - CN=Alumno2
 - OU=informaticos
 - CN=Informatico1
 - CN=Informatico2
 - OU=profesores
 - CN=Profesor1
 - CN=Profesor2

Name	Value	Type	Size
objectClass	[5 values]		
cn	equipo1	Directory String	7
distinguishedName	CN=equipo1,OU=hosts,DC=moralesespejo,DC=com	DN	43
instanceType	[Writable]	INTEGER	1
whenCreated	31/12/2022 12:31:26	Generalized Time	17
whenChanged	31/12/2022 12:31:26	Generalized Time	17
uSNCreated	41058	Large integer (a.k.a. INTEGER8)	5
uSNChanged	41062	Large integer (a.k.a. INTEGER8)	5
name	equipo1	Directory String	7
userAccountControl	[WorkstationTrustAccount]	INTEGER	4
badPwdCount	0	INTEGER	1
codePage	0	INTEGER	1
countryCode	0	INTEGER	1
badPasswordTime	unspecified	Large integer (a.k.a. INTEGER8)	1
lastLogoff	unspecified	Large integer (a.k.a. INTEGER8)	1
lastLogon	unspecified	Large integer (a.k.a. INTEGER8)	1
localPolicyFlags	0	INTEGER	1
pwdLastSet	31/12/2022 12:31:26	Large integer (a.k.a. INTEGER8)	18
primaryGroupID	515	INTEGER	3
accountExpires	never	Large integer (a.k.a. INTEGER8)	19

List View HTML View

Output

Show all items View Details

Default schema loaded successfully.
 Schema for 192.168.58.5:389 loaded successfully.
 The host name 'moralesespejo.com' could not be resolved to its address.
 The host name 'DomainDnsZones.moralesespejo.com' could not be resolved to its address.
 The host name 'ForestDnsZones.moralesespejo.com' could not be resolved to its address.

Seleccionar Administrador: Símbolo del sistema

```
C:\Users\Administrador\Desktop>netstat -n | find "389"
TCP    127.0.0.1:389          127.0.0.1:54670      ESTABLISHED
TCP    127.0.0.1:389          127.0.0.1:54672      ESTABLISHED
TCP    127.0.0.1:389          127.0.0.1:57208      ESTABLISHED
TCP    127.0.0.1:54670        127.0.0.1:389        ESTABLISHED
TCP    127.0.0.1:54672        127.0.0.1:389        ESTABLISHED
TCP    127.0.0.1:57208        127.0.0.1:389        ESTABLISHED
TCP    192.168.58.5:389       192.168.58.5:54679    ESTABLISHED
TCP    192.168.58.5:389       192.168.58.5:57224    ESTABLISHED
TCP    192.168.58.5:389       192.168.58.5:57264    ESTABLISHED
TCP    192.168.58.5:389       192.168.58.135:54194  ESTABLISHED
TCP    192.168.58.5:389       192.168.58.137:62140  ESTABLISHED
TCP    192.168.58.5:54679     192.168.58.5:389      ESTABLISHED
TCP    192.168.58.5:57224     192.168.58.5:389      ESTABLISHED
TCP    192.168.58.5:57264     192.168.58.5:389      ESTABLISHED
```

conexiones
realizadas

C:\Users\Administrador\Desktop>

salen dos IP diferentes porque una es jxplorer desde mi máquina real y otra es el softerra desde una máquina virtual porque me caducó la licencia.

9. Cada vez que se arranque el ordenador crear un script que guarde una copia de seguridad de Active Directory.



Administrador: Símbolo del sistema

```
C:\Users\Administrador\Desktop>type morales-script.bat
csvde -f "C:\Copias\scripts\copia-moralesespejo-%date:~-4,4%-%date:~-7,2%-%date:~-10,2%_%time:~0,2%-%time:~3,2%-%time:~6,2%.csv" -s MORALES-SERVER -d "dc=moralesespejo,dc=com"
```

contenido del script. Es el comando que he usado anteriormente, pero le indico con las variables date y time que tenga de nombre la fecha y la hora a la que se realiza la copia.

Programador de tareas

Archivo Acción Ver Ayuda



Programador de tareas (local)
> Biblioteca del Programador de tareas

Nombre	Estado	Desencadenadores	Hora próxima ejecución	Hora última ejecución
Copia AD Raul Morales	Listo	Al iniciar el sistema		30/11/1999 0:00:00
CreateExplorerShellUnelevatedTa...	En ejecu...	Al crear o modificar la t...		02/01/2023 12:15:10
MicrosoftEdgeUpdateTaskMachi...	Listo	Se definieron varios de...	03/01/2023 12:40:03	02/01/2023 12:40:04
MicrosoftEdgeUpdateTaskMachi...	Listo	A las 12:10 todos los dí...	02/01/2023 13:10:03	02/01/2023 12:17:51
npcapwatchdog	Listo	Al iniciar el sistema		02/01/2023 12:14:23

General Desencadenadores Acciones Condiciones Configuración Historial

Al crear una tarea, debe especificar la acción que se producirá cuando se inicie. Para cambiar estas acciones, abra las páginas de propiedades de la tarea con el comando Propiedades.

Acción	Detalles
Iniciar un programa	C:\Users\Administrador\Desktop\morales-script.bat

para que se realice al iniciar el equipo, creamos una tarea en el programador de tareas que se ejecute al iniciar el sistema. Le indicamos que ejecute el script que se encuentra en el escritorio.

General Desencadenadores Acciones Condiciones Configuración Historial

Nombre: Copia AD Raul Morales

Ubicación: \

Autor: MORALESESPEJO\Administrador

Descripción:

marcamos esta opción, si no la marcamos no se ejecuta

Opciones de seguridad

Al ejecutar la tarea, usar esta cuenta de usuario:

Administrador

Cambiar usuario o grupo...

☐ Ejecutar solo cuando el usuario haya iniciado sesión

☒ Ejecutar tanto si el usuario inició sesión como si no

☐ No almacenar contraseña. La tarea solo tendrá acceso a los recursos del equipo local.

☐ Ejecutar con los privilegios más altos

☐ Oculta

Configurar para: Windows Vista™, Windows Server™ 2008



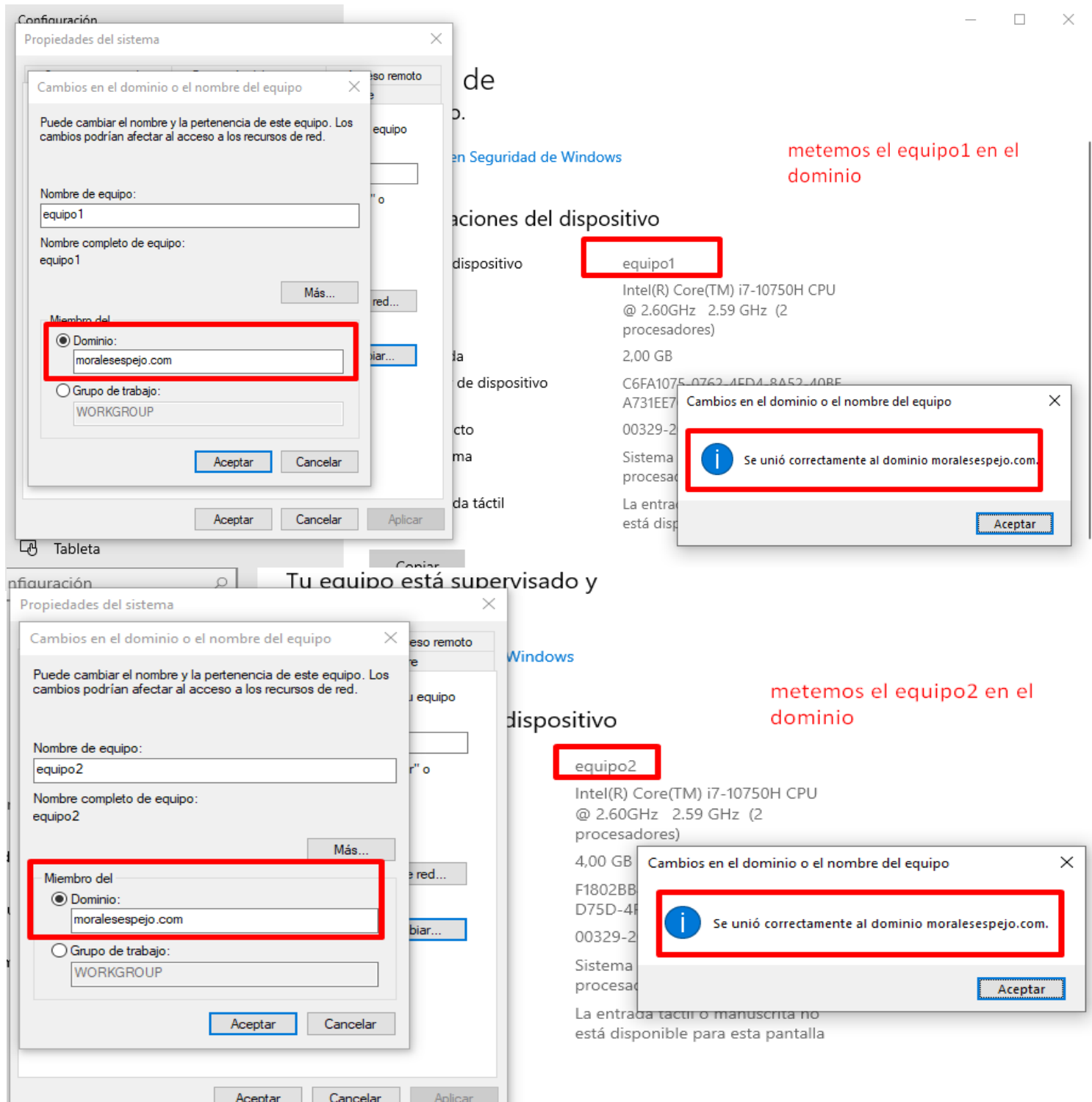
Aceptar

Cancelar

C.- INTEGRACIÓN DE CLIENTES MICROSOFT WINDOWS (WINDOWS 7, 8 Y 10) CON EL SERVIDOR MICROSOFT WINDOWS ACTIVE DIRECTORY.

10. Enlazar tres sistemas operativos diferentes (Windows 7, 8 y 10) con el servidor y probar que:

- Pueden logearse perfectamente los usuarios creados y que se obtiene el perfil adecuado (móvil/local).



Nombre	Tipo	Descripción
equipo1	Equipo	
equipo2	Equipo	

Propiedades: equipo2

Ubicación	Administrado por	Marcado
General	Sistema operativo	Miembro de

Nombre: Windows 10 Enterprise Evaluation

Versión: 10.0 (19044)

Service Pack:

Propiedades: equipo1

Ubicación	Administrado por	Marcado
General	Sistema operativo	Miembro de

Nombre: Windows 10 Enterprise Evaluation

Versión: 10.0 (19044)

Service Pack:

cuando hemos unido los dos, se nos completan los equipos añadidos anteriormente

Home | WSERVER-MORALESPEJO | **MORALES-WINADICIONAL** | W10-moralesespejo

Papelera de reciclaje

prueba de movilidad

creo esta carpeta y nos vamos al otro equipo para ver que allí también se encontrará al ser un perfil de movilidad

Profesor2 (\\MORALES-SERVER\moralesespejoPROFESORES) (Z:)

Nombre	Fecha de modificación	Tipo	Tamaño
he accedido con profesor2 - raul morales	02/01/2023 14:14	Carpeta de archivos	

acceso a la carpeta personal que es solo para este usuario y puedo crear una carpeta

INICIO

Productividad

Office

Microsoft Edge

Microsoft Store

Profesor2

Documentos

Imágenes

Perfiles de usuario

Los perfiles del usuario contienen la configuración de escritorio y otro tipo de información relacionada con su cuenta de usuario. Se puede crear un perfil diferente en cada equipo que use o bien seleccionar un perfil móvil para usarlo en cualquier equipo.

Perfiles almacenados en este equipo:

Nombre	Tamaño	Tipo	Estado	Mod...
EQUIPO1\moralesespejo	401 MB	Local	Local	02/0...
MORALESPEJO\Administr...	1,48 MB	Local	Local	02/0...
MORALESPEJO\Profesor1	2,33 MB	Movilid...	Movilid...	02/0...
MORALESPEJO\Profesor2	2,51 MB	Movilid...	Movilid...	02/0...
Perfil predeterminado	1,52 MB	Local	Local	05/1...

Cambiar tipo...

Eliminar

Copiar a...

Para crear nuevas cuentas de usuario, abra [Cuentas de usuario](#) en Panel de control.

Aceptar

Cancelar

he accedido con el profesor2 y vemos como el tipo de perfil es de movilidad tanto de este usuario como el profesor1.

Home

WSERVER-MORALESPEJO

MORALES-WINADICIONAL

W10-moralesespejo

Papelera de reciclaje

prueba de movilidad

Profesor2 (\\MORALES-SERVER\moralesespejoPROFESORES) (Z:)

ArchivoInicioCompartirVista

Este equipo > Profesor2 (\\MORALES-SERVER\moralesespejoPROFESORES) (Z:)

Acceso rápido

Escritorio

Descargas

Documentos

Nombre	Fecha de modificación	Tipo
he accedido con profesor2 - raul morales	02/01/2023 14:14	Carpeta de archivo
acceso desde equipo 2 con el mismo usuario	02/01/2023 14:35	Carpeta de archivo

INICIO

acceso con el mismo usuario desde el equipo2 y vemos como todo está sincronizado perfectamente, tenemos la misma carpeta y todo en el escritorio.

Profesor2

Documentos

Perfiles de usuario

EQUIPO2

Los perfiles del usuario contienen la configuración de escritorio y otro tipo de información relacionada con su cuenta de usuario. Se puede crear un perfil diferente en cada equipo que use o bien seleccionar un perfil móvil para usarlo en cualquier equipo.

Perfiles almacenados en este equipo:

Nombre	Tamaño	Tipo	Estado	Mod...
EQUIPO2\moralesespejo	1,01 GB	Local	Local	02/0...
MORALESPEJO\administr...	1,37 MB	Local	Local	02/0...
MORALESPEJO\Profesor1	2,06 MB	Movilid...	Movilid...	02/0...
MORALESPEJO\Profesor2	1,95 MB	Movilid...	Movilid...	02/0...
Perfil predeterminado	1,49 MB	Local	Local	22/1...

Cambiar tipo...

Eliminar

Copiar a...

Para crear nuevas cuentas de usuario, abra [Cuentas de usuario](#) en Panel de control.

WSERVER-MORALESESPEJO MORALES-WINADICIONAL W 10-moralesespejo

Perfiles

PERFILES

Disco local (C:) > Perfiles

Nombre	Fecha de modificación	Tipo	Tamaño
Profesor1.V6	02/01/2023 14:32	Carpeta de archivos	
Profesor2.V6	02/01/2023 14:32	Carpeta de archivos	

Profesor2

CARPETA PERSONAL PROFESOR2

<< moralesespejoPROFESORES > Profesor2

Nombre	Fecha de modificación	Tipo	Tamaño
acceso desde equipo 2 con el mismo us...	02/01/2023 14:35	Carpeta de archivos	
he accedido con profesor2 - raul morales	02/01/2023 14:14	Carpeta de archivos	

desde el servidor vemos como se crean los perfiles de cada usuario, como las carpetas que hemos creado en la carpeta profesor2

Home

WSERVER-MORALESPEJO

MORALES-WINADICIONAL

W10-moralesespejo

Papelera de reciclaje

Google Chrome

Alumno2 (\\MORALES-SERVER\moralesespejoALUMNOS) (Z:)

Este equipo > Alumno2 (\\MORALES-SERVER\moralesespejoALUMNOS) (Z:)

Nombre

Fecha de modificación

Tipo

Tamaño

alumno2 creando carpeta - raul morales

02/01/2023 14:52

Carpeta de archivos

Inicio

Productividad

Office

Microsoft Edge

Microsoft Store

Alumno2

Documentos

Imágenes

he accedido con todos los alumnos e informaticos y vemos como los perfiles son locales y por tanto se guarda en el equipo que inicia sesión y no en el servidor

Perfiles de usuario

Los perfiles del usuario contienen la configuración de escritorio y otro tipo de información relacionada con su cuenta de usuario. Se puede crear un perfil diferente en cada equipo que use o bien seleccionar un perfil móvil para usarlo en cualquier equipo.

Perfiles almacenados en este equipo:

Nombre	Tamaño	Tipo	Estado	Mo
EQUIPO2\moralesespejo	1,01 GB	Local	Local	02/1
MORALESPEJO\Administrador	1,39 MB	Local	Local	02/1
MORALESPEJO\Alumno1	89,4 MB	Local	Local	02/1
MORALESPEJO\Alumno2	389 MB	Local	Local	22/
MORALESPEJO\Informatico1	271 MB	Local	Local	02/1
MORALESPEJO\Informatico2	88,5 MB	Local	Local	02/1

Cambiar tipo...

Eliminar

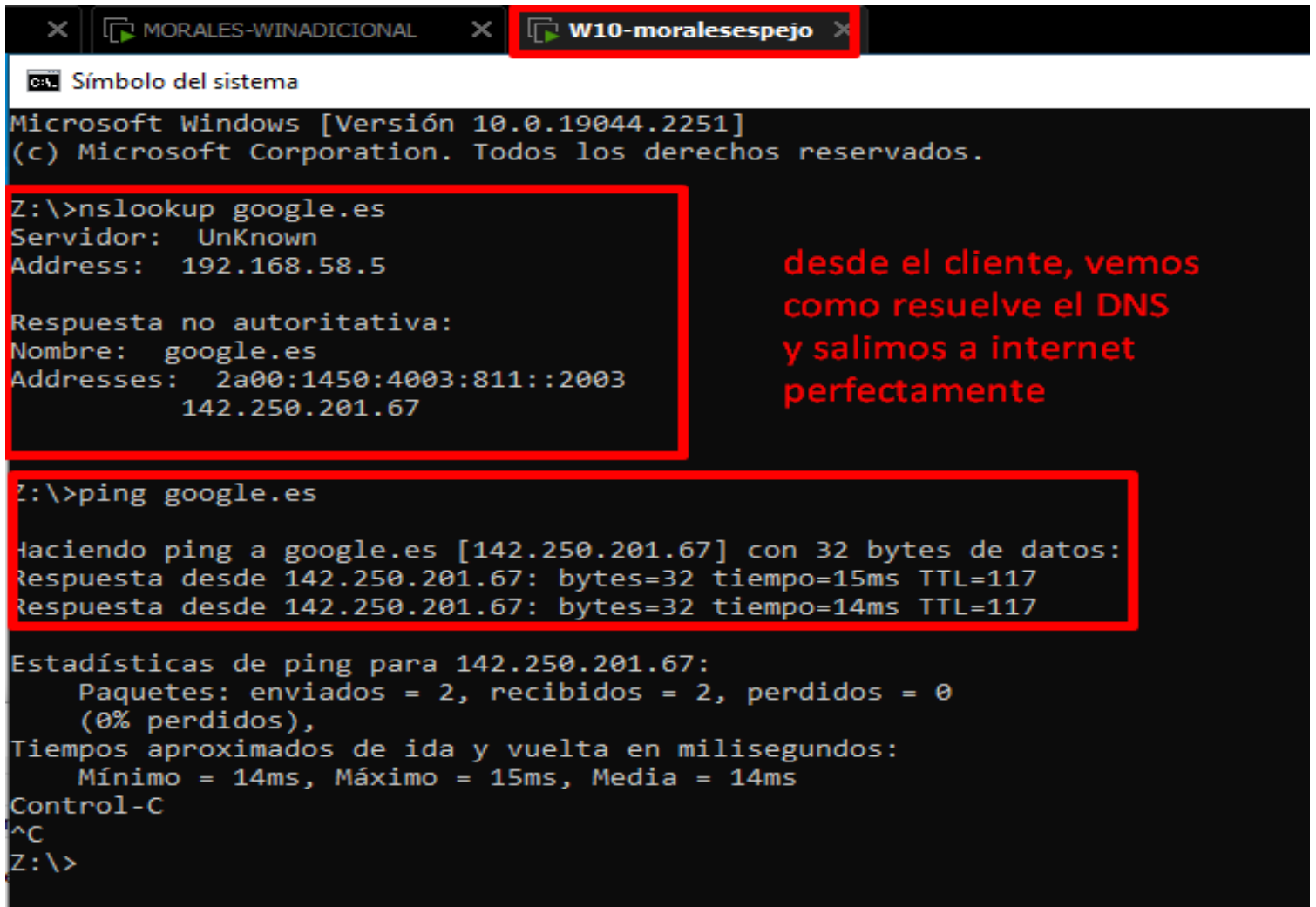
Copiar a...

Para crear nuevas cuentas de usuario, abra [Cuentas de usuario](#) en Panel de control.

Aceptar

Cancelar

- Funciona perfectamente con la integración realizada la resolución de DNS local.



The screenshot shows a Windows command prompt window with two tabs: 'MORALES-WINADICIONAL' and 'W10-moralesespejo'. The active tab is 'W10-moralesespejo'. The command prompt displays the following output:

```
Microsoft Windows [Versión 10.0.19044.2251]
(c) Microsoft Corporation. Todos los derechos reservados.

Z:\>nslookup google.es
Servidor: UnKnown
Address: 192.168.58.5

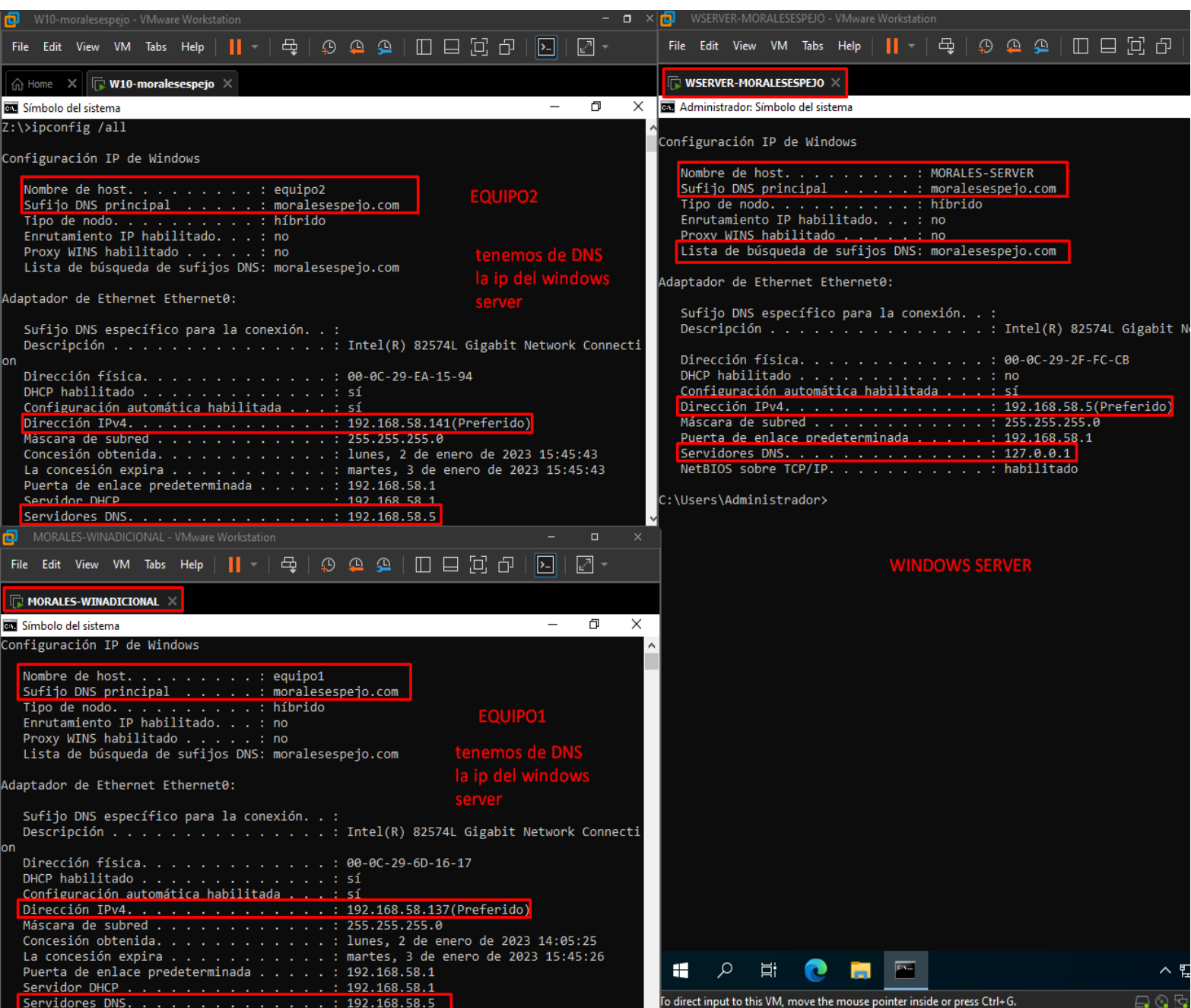
Respuesta no autoritativa:
Nombre: google.es
Addresses: 2a00:1450:4003:811::2003
          142.250.201.67

Z:\>ping google.es

Haciendo ping a google.es [142.250.201.67] con 32 bytes de datos:
Respuesta desde 142.250.201.67: bytes=32 tiempo=15ms TTL=117
Respuesta desde 142.250.201.67: bytes=32 tiempo=14ms TTL=117

Estadísticas de ping para 142.250.201.67:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 14ms, Máximo = 15ms, Media = 14ms
Control-C
^C
Z:\>
```

desde el cliente, vemos como resuelve el DNS y salimos a internet perfectamente



- Funciona perfectamente con la integración realizada la resolución de servicio.

La integración de servicio en Active Directory es un proceso que permite a los servicios informáticos y aplicaciones autenticar a los usuarios utilizando las credenciales almacenadas en el directorio Active Directory. Esto permite a los usuarios acceder a los servicios y aplicaciones con un solo nombre de usuario y contraseña, en lugar de tener que recordar credenciales separadas para cada servicio. Además, la integración del servicio en Active Directory también permite la gestión centralizada de los usuarios y la administración de permisos de acceso a los servicios y aplicaciones.

Por tanto, ya lo hemos comprobado anteriormente accediendo con los usuarios que hemos creado.

C.- INTEGRACIÓN DE MOODLE/JOOMLA CON EL SERVIDOR ACTIVE DIRECTORY.

Se enlazará el servidor Joomla y Moodle con el servidor Active Directory (modo seguro y modo no seguro). Mostrar capturas de cómo pide el usuario/contraseña del servidor LDAP y de la configuración

LDAP server settings

Host URL
auth_ldap | host_url

ldap://192.168.58.5

Default: Empty

Specify LDAP host in URL-form like 'ldap://ldap.myorg.com/' or 'ldaps://ldap.myorg.com/'. Separate multiple servers with ';' to get failover support.

Version

auth_ldap | ldap_version

3

Default: 3

The version of the LDAP protocol your server is using.

Use TLS

auth_ldap | start_tls

No

Default: No

Use regular LDAP service (port 389) with TLS encryption

LDAP encoding

auth_ldap | ldapencoding

utf-8

Default: utf-8

Encoding used by the LDAP server, most likely utf-8. If LDAP v2 is selected, Active Directory uses its configured encoding, such as cp1252 or cp1250.

Bind settings

Prevent password
caching

auth_ldap | preventpassindb

Yes

Default: No

Select yes to prevent passwords from being stored in Moodle's DB.

Distinguished name

auth_ldap | bind_dn

cn=Administrador,cn=Users,dc=moi

Default: Empty

If you want to use bind-user to search users, specify it here. Something like 'cn=ldapuser,ou=public,o=org'

Password

auth_ldap | bind_pw

.....

Password for bind-user.

ponemos contraseña del usuario administrador

User lookup settings

User type
auth_ldap | user_type

MS ActiveDirectory



Default: Default

Select how users are stored in LDAP. This setting also specifies how logins and user creation will work.

Contexts
auth_ldap | contexts

ou=usuarios,dc=moralesespejo,dc=co

Default: Empty

List of contexts where users are located. Separate different contexts with semicolons. Example: 'ou=users,o=org; ou=others,o=org'

Search subcontexts
auth_ldap | search_sub

Yes



Default: No

Search users from subcontexts.

Dereference aliases
auth_ldap | opt_deref

No



Default: No

Determines how aliases are handled during search. Select one of the "No" (LDAP_DEREF_NEVER) or "Yes" (LDAP_DEREF_ALWAYS)

User attribute
auth_ldap | user_attribute

samaccountname

Default: Empty

Force change password

Force change password
auth_ldap | forcechangepassword

Yes



Default: No

Force users to change password on their first login to Moodle.

Use standard page for
changing password
auth_ldap | stdchangepassword

Yes



Default: No

If the external authentication system allows password changes through Moodle, switch this to Yes. This setting overrides 'Change Password URL'. NOTE: It is recommended that you use LDAP over an SSL encrypted tunnel (ldaps://) if the LDAP server is remote.

Password format
auth_ldap | passtype

MD5 hash



Default: Plain text

Specify the format of new or changed passwords in LDAP server.

Password-change URL
auth_ldap | changepasswordurl

Default: Empty

URL of lost password recovery page, which will be sent to users in an email. Note that this setting will have no effect if a forgotten password URL is set in the authentication common settings.

System role mapping

Manager context
auth_ldap | managercontext

Default: Empty

LDAP context used to select for *Manager* mapping. Separate multiple groups with ';'. Usually something like "cn=manager,ou=first-ou-with-role-groups,o=myorg; cn=manager,ou=second-ou-with-role-groups,o=myorg".

Course creator context
auth_ldap |
coursecreatorcontext

Default: Empty

LDAP context used to select for *Course creator* mapping. Separate multiple groups with ';'. Usually something like "cn=coursecreator,ou=first-ou-with-role-groups,o=myorg; cn=coursecreator,ou=second-ou-with-role-groups,o=myorg".

Note: Updating external LDAP data requires that you set binddn and bindpw to a bind-user with e privileges to all the user records. It currently does not preserve multi-valued attributes, and will rer values on update.

Data mapping (First
name)

givenName

Default: Empty

auth_ldap | field_map_firstname

Update local (First
name)

On creation

Default: On creation

auth_ldap |

field_updatelocal_firstname

Update external (First
name)

On update

Default: Never

auth_ldap |

field_updateremote_firstname

Lock value (First name)

Unlocked

Default: Unlocked

auth_ldap | field_lock_firstname

Data mapping
(Surname)

sn

Default: Empty

auth_ldap | field_map_lastname

Update local (Surname)

On creation

Default: On creation

auth_ldap |

field_updatelocal_lastname

Update external
(Surname)

Never

Default: Never

auth_ldap |

field_updateremote_lastname

Lock value (Surname)

Unlocked

Default: Unlocked

auth_ldap | field_lock_lastname

Data mapping (Email
address)

mail

Default: Empty

New Site: Edit profile

No es seguro | 192.168.58.195/user/edit.php

Google (18) YouTube (1) Inicio / Twitter Clases Google Drive How to edit a file u... Registros | DNS | sy... proxmox - Proxmox...

New Site Home Dashboard My courses

P

Profesor1 Message

Profesor1

Expand all

General

First name **Profesor1**

accedemos con el usuario profesor1 perfectamente.

WSERVER-MORALESPEJO - VMware Workstation

File Edit View VM Tabs Help

WSERVER-MORALESPEJO DevOps-MoralesEspejo

Capturando desde Ethernet0

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Vemos como genera paquetes por el puerto 389

tcp.port == 389

No.	Time	Source	Destination	Protocol	Length	Info
74	6.198761	192.168.58.195	192.168.58.5	TCP	74	54850 → 389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS...
75	6.198842	192.168.58.5	192.168.58.195	TCP	74	389 → 54850 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 W...
76	6.199173	192.168.58.195	192.168.58.5	TCP	66	54850 → 389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=268792957...
77	6.199173	192.168.58.195	192.168.58.5	LDAP	140	bindRequest(1) "cn=Administrador,cn=Users,dc=moralesespejo,dc=...
78	6.202436	192.168.58.5	192.168.58.195	LDAP	88	bindResponse(1) success
79	6.202662	192.168.58.195	192.168.58.5	TCP	66	54850 → 389 [ACK] Seq=75 Ack=23 Win=64256 Len=0 TSval=2687929...
80	6.202779	192.168.58.195	192.168.58.5	LDAP	187	searchRequest(2) "ou=usuarios,dc=moralesespejo,dc=com" wholeS...
81	6.202952	192.168.58.5	192.168.58.195	LDAP	212	searchResEntry(2) "CN=Profesor1,OU=profesores,OU=usuarios,DC=...

messageID: 1

protocolOp: bindRequest (0)

bindRequest

version: 3

name: cn=Administrador,cn=Users,dc=moralesespejo,dc=com

authentication: simple (0)

simple: usuario123-

[Response In: 78]

0000 00 0c 29 2f fc cb 00 0c 29 3a 5e a7 08 00 45 00 ..)/....):^...

0010 00 7e 37 84 40 00 3f 06 0d dd c0 a8 3a c3 c0 a8 ~7@?.....:

0020 3a 05 d6 42 01 85 32 c8 cd 50 b9 3c 5b 13 80 18 :..B..2. P<[

0030 01 f6 3d bc 00 00 01 01 08 0a a0 36 8c e8 00 846.

0040 9d c9 30 48 02 01 01 60 43 02 01 03 04 31 63 6e ..0H... C...

0050 3d 41 64 6d 69 6e 69 73 74 72 61 64 6f 72 2c 63 =Adminis tradc

0060 6e 3d 55 73 65 72 73 2c 64 63 3d 6d 6f 72 61 6c n=Users, dc=mc

0070 65 73 65 73 70 65 6a 6f 2c 64 63 3d 63 6f 6d 80 esespejo ,dc=c

0080 0b 75 73 75 61 72 69 6f 31 32 33 2d -usuario 123-

New Site: Edit profile

No es seguro | 192.168.58.195/user/edit.php

Google(18) YouTube(1) Inicio / TwitterClasesGoogle DriveHow to edit a file u...Registros | DNS | sy...proxmox - Proxmox...

New SiteHomeDashboardMy courses

Preferences / Edit profile

Informatico1 Message

Informatico1

Expand all

accedemos con el usuario informatico y también funciona perfectamente.

WSERVER-MORALESPEJO - VMware Workstation

FileEditViewVMTabsHelp

WSERVER-MORALESPEJODevOps-MoralesEspejo

Capturando desde Ethernet0

ArchivoEdiciónVisualizaciónIrCapturaAnalizarEstadísticasTelefoníaWirelessHerramientasAyuda

tcp.port == 389

No.	Time	Source	Destination	Protocol	Length	Info
351	190.782406	192.168.58.195	192.168.58.5	LDAP	190	searchRequest(2) "ou=usuarios,dc=moralesespejo,dc=com" wholeS...
352	190.782554	192.168.58.5	192.168.58.195	LDAP	220	searchResEntry(2) "CN=Informatico1,OU=informaticos,OU=usuario...
353	190.782846	192.168.58.195	192.168.58.5	LDAP	174	searchRequest(3) "CN=Informatico1,OU=informaticos,OU=usuarios...
354	190.782938	192.168.58.5	192.168.58.195	LDAP	178	searchResEntry(3) "CN=Informatico1,OU=informaticos,OU=usuario...
355	190.784492	192.168.58.195	192.168.58.5	LDAP	73	unbindRequest(4)
356	190.784492	192.168.58.195	192.168.58.5	TCP	66	42402 → 389 [FIN, ACK] Seq=314 Ack=289 Win=64128 Len=0 TSval=...
357	190.784543	192.168.58.5	192.168.58.195	TCP	66	389 → 42402 [ACK] Seq=289 Ack=315 Win=2097664 Len=0 TSval=887...
358	190.784576	192.168.58.5	192.168.58.195	TCP	54	389 → 42402 [RST, ACK] Seq=289 Ack=315 Win=0 Len=0

> Internet Protocol Version 4, Src: 192.168.58.5, Dst: 192.168.58.19

> Transmission Control Protocol, Src Port: 389, Dst Port: 42402, Seq

> Lightweight Directory Access Protocol

D.- INTEGRACIÓN DEL SERVIDOR PURE-FTPD CON EL SERVIDOR ACTIVE DIRECTORY.

Se enlazará el servidor Pure-Ftpd con el servidor Active Directory. Mostrar capturas de cómo pide el usuario/contraseña del servidor LDAP y de la configuración, mediante tcpdump/iptraf y de que crea correctamente el directorio de trabajo. Usar un cliente ftp para interactuar con el servidor y probar todas sus propiedades (enabled, número de archivos, ancho de banda, etc.).

He estado investigando en internet sobre este ejercicio y no encuentro nada acerca de pure-ftp con active directory, ni videos ni nada, ya que pure ftp es solo para sistemas Unix. He probado implementarlo con un servidor pure ftpd en una máquina Linux, pero realmente es como si nada porque no le puedo asignar atributos de pure ftpd a los usuarios de Active directory, entonces no lo entiendo. Agradecería que lo pudieras explicar en clase cuando puedas para poder realizarlo bien.

E.- INTEGRACIÓN DEL SISTEMAS OPERATIVO DE VIRTUALIZACIÓN PROXMOX Y ESX.

Enlazar S.O. virtualización PROXMOX y Esxi con el servidor Active Directory.

Edit: LDAP Server añadimos la base del dominio, y el atributo de los usuarios que es sAMAccountName

General Sync Options

Realm: windows-moralesespejo Server: 192.168.58.5

Base Domain Name: ou=usuarios,dc=moralesespejo Fallback Server:

User Attribute Name: sAMAccountName Port: 389

Default: ☒ SSL: ☐

Verify Certificate: ☐ Require TFA: none

Comment:

Help **OK** **Reset**

Edit: LDAP Server añadimos el usuario administrador e indicamos los atributos de los usuarios y grupos

General **Sync Options**

Bind User: cn=Administrador,cn=Users User classes: user, person

Bind Password: Group classes: group

E-Mail attribute: mail User Filter:

Groupname attr.: Group Filter:

Default Sync Options

Scope: Users Enable new users: Yes (Default)

Remove Vanished Options

ACL: ☐ Remove ACLs of vanished users and groups.

Entry: ☐ Remove vanished user and group entries.

Properties: ☐ Remove vanished properties from synced users.

Help **OK** **Reset**

Task viewer: Realm windows/moralesespejo - Sync Preview

Output

Status

Stop

```
(dry test run) starting sync for realm windows-moralesespejo
got data from server, updating users
syncing users
updating user 'Alumno1@windows-moralesespejo'
updating user 'Alumno2@windows-moralesespejo'
updating user 'Informatico1@windows-moralesespejo'
updating user 'Informatico2@windows-moralesespejo'
updating user 'Profesor1@windows-moralesespejo'
updating user 'Profesor2@windows-moralesespejo'
```

NOTE: Dry test run, changes were NOT written to the configuration.
TASK OK

cuando pulsamos
en sincronizar, vemos
como aparecen los usuarios
que hemos creado

Proxmox VE Login

User name: Alumno1

Password:

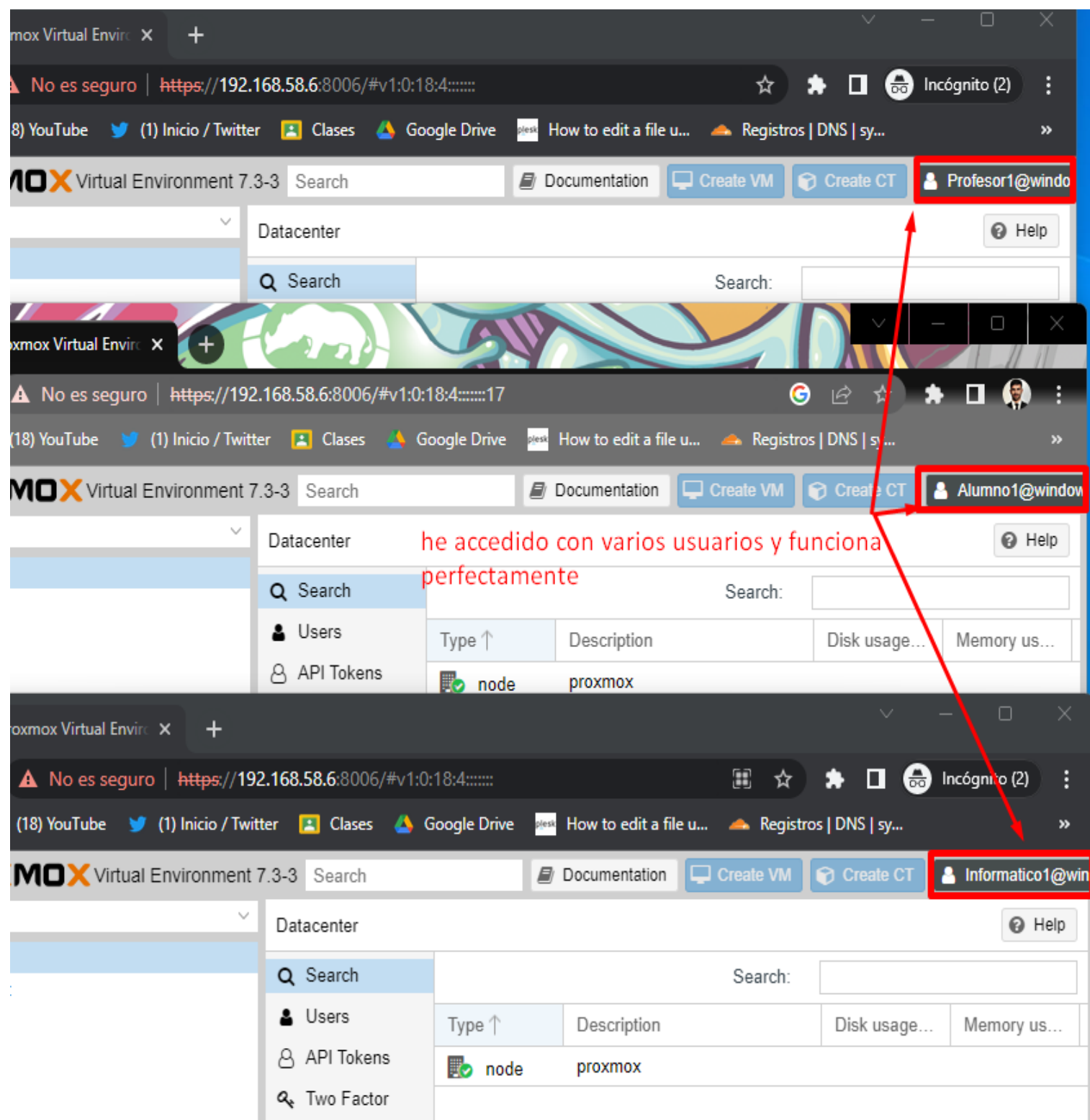
Realm: windows-moralesespejo

Language: English

Save User name: ☐

Login

cuando vayamos a iniciar sesión, seleccionamos
el realm que hemos creado e introducimos el
usuario de nuestro dominio



*Ethernet0

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

tcp.port == 389

No.	Time	Source	Destination	Protocol	Length	Info
3684	83.105023	192.168.58.6	192.168.58.5	TCP	66	48194 → 389 [ACK] Seq=75 Ack=23 Win=64256 Len=0 TSval=278
3685	83.121296	192.168.58.6	192.168.58.5	LDAP	163	searchRequest(2) "ou=usuarios,dc=moralesespejo,dc=com" wh
3686	83.121548	192.168.58.5	192.168.58.6	LDAP	178	searchResEntry(2) "CN=Informatico1,OU=informaticos,OU=usu
3687	83.122201	192.168.58.6	192.168.58.5	LDAP	158	bindRequest(3) "CN=Informatico1,OU=informaticos,OU=usuari
3688	83.124769	192.168.58.5	192.168.58.6	LDAP	88	bindResponse(3) success
3689	83.125330	192.168.58.6	192.168.58.5	LDAP	73	unbindRequest(4)
3690	83.125392	192.168.58.5	192.168.58.6	TCP	54	389 → 48194 [RST, ACK] Seq=157 Ack=271 Win=0 Len=0
3691	83.125454	192.168.58.6	192.168.58.5	TCP	66	48194 → 389 [FIN, ACK] Seq=271 Ack=157 Win=64256 Len=0 TS
4005	96.104570	192.168.58.6	192.168.58.5	TCP	74	40476 → 389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
4006	96.104662	192.168.58.5	192.168.58.6	TCP	74	389 → 40476 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=14
4007	96.104972	192.168.58.6	192.168.58.5	TCP	66	40476 → 389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=27830
4008	96.110176	192.168.58.6	192.168.58.5	LDAP	140	bindRequest(1) "cn=Administrador,cn=Users,dc=moralesespej
4010	96.113050	192.168.58.5	192.168.58.6	LDAP	88	bindResponse(1) success
4011	96.113627	192.168.58.6	192.168.58.5	TCP	66	40476 → 389 [ACK] Seq=75 Ack=23 Win=64256 Len=0 TSval=278
4014	96.128155	192.168.58.6	192.168.58.5	LDAP	158	searchRequest(2) "ou=usuarios,dc=moralesespejo,dc=com" wh
4015	96.128435	192.168.58.5	192.168.58.6	LDAP	168	searchResEntry(2) "CN=Alumno1,OU=alumnos,OU=usuarios,DC=m
4016	96.129176	192.168.58.6	192.168.58.5	LDAP	148	bindRequest(3) "CN=Alumno1,OU=alumnos,OU=usuarios,DC=mora
4017	96.130330	192.168.58.5	192.168.58.6	LDAP	88	bindResponse(3) success
4018	96.131147	192.168.58.6	192.168.58.5	LDAP	73	unbindRequest(4)
4019	96.131221	192.168.58.5	192.168.58.6	TCP	54	389 → 40476 [RST, ACK] Seq=147 Ack=256 Win=0 Len=0

> Frame 4016: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface 0

> Ethernet II, Src: VMware_71:f6:a4 (00:0c:29:71:f6:a4), Dst: VMware_00:0c:29:71:f6:a4 (00:0c:29:71:f6:a4)

> Internet Protocol Version 4, Src: 192.168.58.6, Dst: 192.168.58.5

> Transmission Control Protocol, Src Port: 40476, Dst Port: 389, Seq: 147, Win: 0, Len: 0

> Lightweight Directory Access Protocol

- LDAPMessage bindRequest(3) "CN=Alumno1,OU=alumnos,OU=usuarios,DC=moralesespejo,dc=com"
- messageID: 3
- protocolOp: bindRequest (0)
- bindRequest
 - version: 3
 - name: CN=Alumno1,OU=alumnos,OU=usuarios,DC=moralesespejo,dc=com
 - authentication: simple (0)
 - simple: usuario123-

[Response In: 4017]

0000 00 0c 29 71 f6 a4 00 0c 29 71 f6 a4 08 00 45 00 ...)/.....)d
0010 00 86 60 59 40 00 40 06 e4 bc c0 a8 3a 06 c0 a8 ...Y@. @.
0020 3a 05 9e 1c 01 85 29 93 ea 40 cc 9e 64 ea 80 18). @.
0030 01 f6 d6 08 00 00 01 01 08 0a a5 e1 c4 98 00 05K:
0040 aa bd 30 50 02 01 03 60 4b 02 01 03 04 39 43 4e ..0P....`K:
0050 3d 41 6c 75 6d 6e 6f 31 2c 4f 55 3d 61 6c 75 6d =Alumno1 ,C
0060 6e 6f 73 2c 4f 55 3d 75 73 75 61 72 69 6f 73 2c nos,OU=u su
0070 44 43 3d 6d 6f 72 61 6c 65 73 65 73 70 65 6a 6f DC=moral es
0080 2c 44 43 3d 63 6f 6d 80 0b 75 73 75 61 72 69 6f ,DC=com ·U
0090 31 32 33 2d 123-

filtramos por el puerto 389 en wireshark y vemos los paquetes que se han generado al acceder desde proxmox por lo que está bien integrado.

interceptamos hasta la contraseña del usuario Alumno1 cuando accede a proxmox

Add: Active Directory Server

General Sync Options

Realm: AD-moralesespejo
Domain: moralesespejo.com
Default: ☐

Server: 192.168.58.5
Fallback Server:
Port: 389
SSL: ☐
Verify Certificate: ☐
Require TFA: none

Comment:

Help **Add**

antes hemos añadido la comunicación mediante el realm: LDAP-SERVER. También tenemos la posibilidad de añadir el realm Active Directory, que es parecido solo que hay que indicarle el dominio y especificarle el puerto

Add: Active Directory Server

General **Sync Options**

Bind User: cn=Administrador,cn=Users
Bind Password:
E-Mail attribute: mail
Groupname attr.:

User classes: user,person
Group classes: group
User Filter:
Group Filter:

Default Sync Options
Scope: Users Enable new users: Yes (Default)

Remove Vanished Options
ACL: ☐ Remove ACLs of vanished users and groups.
Entry: ☐ Remove vanished user and group entries.
Properties: ☐ Remove vanished properties from synced users.

Help **Add**

le indicamos el usuario administrador y algunos atributos

Task viewer: Realm AD/moralesespejo - Sync Preview

Output

Status

Stop

(dry test run) starting sync for realm AD-moralesespejo
got data from server, updating users
syncing users

```
adding user 'Administrador@AD-moralesespejo'  
adding user 'Alumno1@AD-moralesespejo'  
adding user 'Alumno2@AD-moralesespejo'  
adding user 'EQUIPO1$@AD-moralesespejo'  
adding user 'EQUIPO2$@AD-moralesespejo'  
adding user 'Informatico1@AD-moralesespejo'  
adding user 'Informatico2@AD-moralesespejo'  
adding user 'Invitado@AD-moralesespejo'  
adding user 'MORALES-SERVER$@AD-moralesespejo'  
adding user 'Profesor1@AD-moralesespejo'  
adding user 'Profesor2@AD-moralesespejo'  
adding user 'krbtgt@AD-moralesespejo'
```

NOTE: Dry test run, changes were NOT written to the configuration.
TASK OK

cuando pulsemos en sincronizar, vemos como se nos sincroniza todos los usuarios que hay en el dominio, ya que no tiene la posibilidad de indicarle un base dn como en LDAP. Podríamos filtrar con filtros.

También si especificamos que sincronice los grupos, sincroniza todos los del dominio, habría que filtrar como he indicado antes.