



Active Directory Overview



▼ Diagrams AD

⚠ All activities were performed in a controlled lab environment for educational and defensive security purposes.

Lab Overview - MARVEL-SHIELD.local

This lab simulates a common internal Active Directory attack scenario where an attacker located in the same network segment abuses name resolution protocols (LLMNR/NBT-NS) to capture credentials.

Once valid credentials are obtained, post-compromise enumeration is performed to map the domain and identify privilege escalation paths using LDAP and BloodHound.

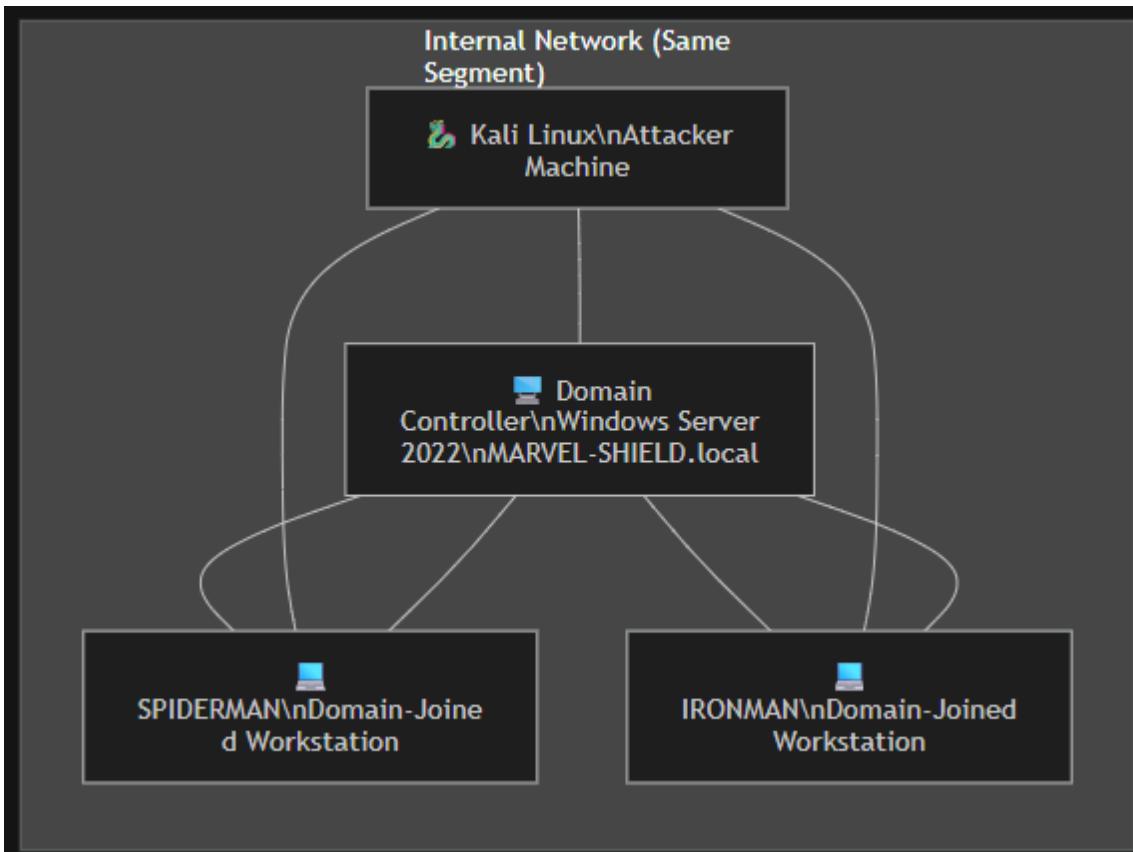


Diagrama del flujo de ataque - Active Directory Pentesting

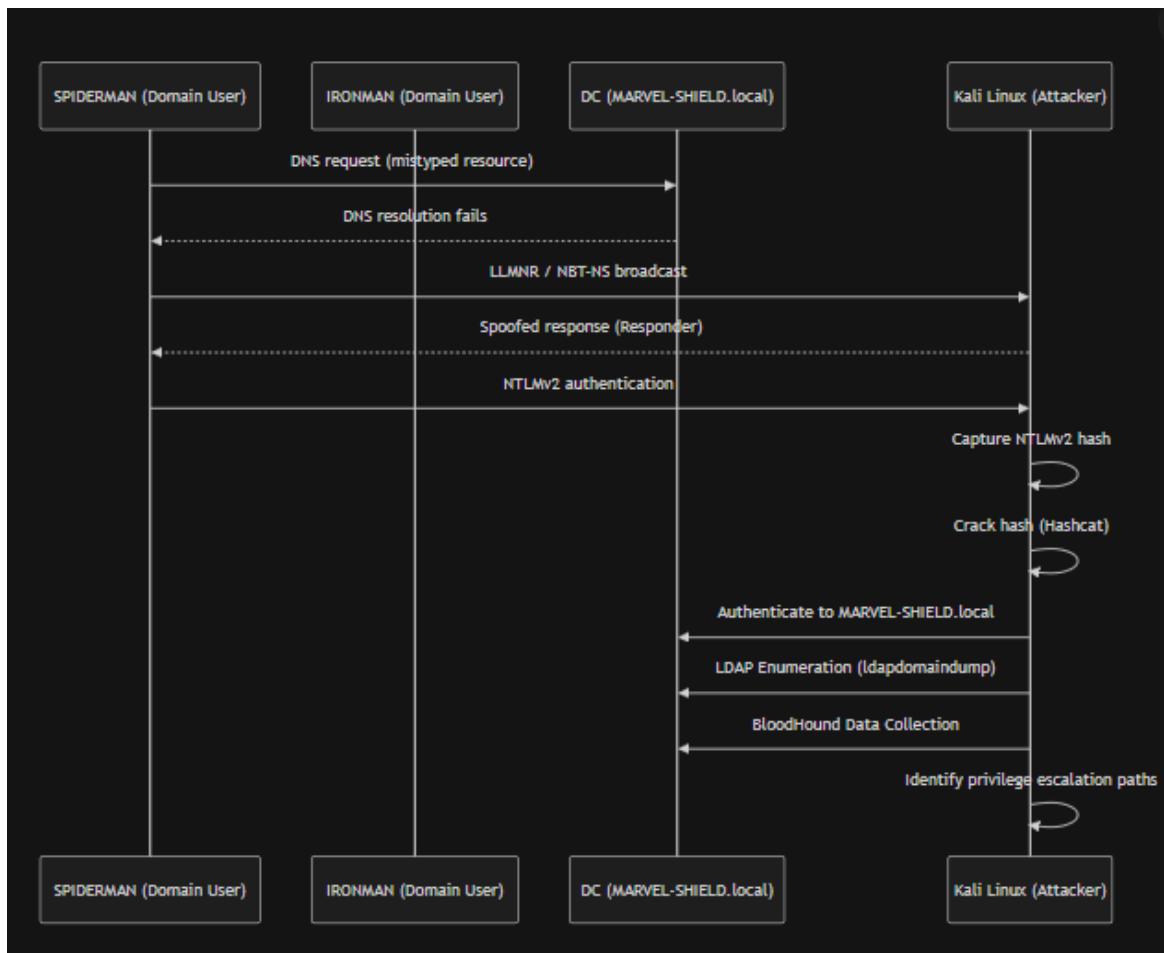
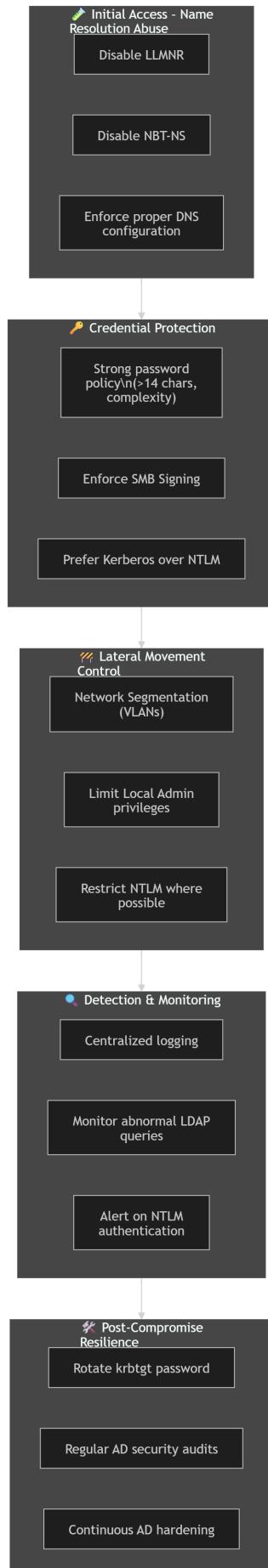


Diagrama de mitigaciones - Active Directory (MARVEL-SHIELD)



Defense-in-Depth for MARVEL-SHIELD.local

This diagram maps defensive controls directly to each stage of a typical Active Directory attack.

The goal is not to rely on a single control, but to layer mitigations across prevention, detection, and response to reduce both the likelihood and impact of compromise.

▼ **Chapter 6.1. Active Directory**

Directory service developed by Microsoft to manage Windows domain networks

Stores information related to objects, such as Computers, Users, Printers, etc.

Autenticates using Kerberos tickets, esto se usa para dispositivos no windows para autentificarse en AD via RADIUS o LDAP

Why Active Directory? (English)

- Active Directory is the **most commonly used identity management service in the world**
 - **93% of Fortune 1,000 companies implement the service in their networks**
(<https://techcommunity.microsoft.com/t5/enterprise-mobility-security/success-with-enterprise-mobility-identity/ba-p/248613>)
- Can be exploited **without ever attacking patchable exploits**
 - Instead, we abuse **features, trusts, components, and more**



¿Por qué Active Directory? (Español)

- Active Directory es el **servicio de gestión de identidades más utilizado en el mundo**

- El 93% de las empresas Fortune 1,000 implementan este servicio en sus redes
(<https://techcommunity.microsoft.com/t5/enterprise-mobility-security/success-with-enterprise-mobility-identity/ba-p/248613>)
 - Puede ser explotado sin necesidad de atacar vulnerabilidades parcheables
 - En su lugar, se abusan características, relaciones de confianza, componentes y más
 - AD no se “rompe” por CVEs
 - Se compromete por mal diseño, malas configuraciones y excesiva confianza
-

Active Directory Components (English)

Active Directory is composed of both physical and logical components.

PHYSICAL

- Data store
- Domain controllers
- Global catalog server
- Read-Only Domain Controller (RODC)

LOGICAL

- Partitions
- Schema
- Domains
- Domain trees
- Forests
- Sites

- Organization units (OUs)
-

Componentes de Active Directory (Español)

Active Directory está compuesto por componentes tanto físicos como lógicos.

FÍSICOS

- Almacén de datos
- Controladores de dominio
- Servidor de catálogo global
- Controlador de dominio de solo lectura (RODC)

LÓGICOS

- Particiones
- Esquema
- Dominios
- Árboles de dominio
- Bosques
- Sitios
- Unidades organizativas (OU)

AD DS Data Store (English)

The AD DS data store contains the database files and processes that store and manage directory information for users, services, and applications.

The AD DS data store:

- Consists of the **Ntds.dit** file
- Is stored by default in the **%SystemRoot%\NTDS** folder on all domain controllers

- Is accessible only through the domain controller processes and protocols
-



Almacén de Datos AD DS (Español)

El almacén de datos de AD DS contiene los archivos de base de datos y los procesos que almacenan y administran la información del directorio para usuarios, servicios y aplicaciones.

El almacén de datos de AD DS:

- Consiste en el archivo Ntds.dit
- Se almacena de forma predeterminada en la carpeta %SystemRoot%\NTDS en todos los controladores de dominio
- Solo es accesible a través de los procesos y protocolos del controlador de dominio

Logical AD components



AD DS Schema (English)

The AD DS Schema:

- Defines every type of object that can be stored in the directory
- Enforces rules regarding object creation and configuration

Object Types

Object Type	Function	Examples
Class Object	What objects can be created in the directory	User, Computer
Attribute Object	Information that can be attached to an object	Display name

Esquema de AD DS (Español)

El Esquema de AD DS:

- Define cada tipo de objeto que puede almacenarse en el directorio
- Aplica reglas relacionadas con la creación y configuración de objetos

Tipos de Objetos

Tipo de Objeto	Función	Ejemplos
Objeto de Clase	Qué objetos pueden crearse en el directorio	Usuario, Equipo
Objeto de Atributo	Información que puede asociarse a un objeto	Nombre visible

Nota rápida (útil para AD Security / Pentesting)

- Modificar el esquema es una acción crítica (casi irreversible)
- Muchas soluciones (Exchange, SCCM, etc.) extienden el esquema
- Un abuso del esquema puede impactar todo el bosque

¿Qué es el Schema de Active Directory?

El Schema es el “manual de reglas” de Active Directory.

Define qué cosas existen en el directorio y qué información puede tener cada cosa.



Analogía sencilla

Piensa en Active Directory como una base de datos gigante.

El Schema sería:

-  El diseño de la base de datos

- Las tablas permitidas
- Las columnas que puede tener cada tabla

Sin schema:

AD no sabría qué es un usuario, qué es una computadora, ni qué datos guardar.

◆ ¿Qué define exactamente el Schema?

1 Clases (Class Objects)

Definen qué tipos de objetos pueden existir.

Ejemplos:

- Usuario
- Computadora
- Grupo
- Impresora

👉 “Puedes crear usuarios y computadoras, pero no cualquier cosa inventada”.

2 Atributos (Attribute Objects)

Definen qué información puede tener cada objeto.

Ejemplos en un usuario:

- Nombre
- Apellido
- Correo
- DisplayName
- Password (de forma cifrada)

👉 “Un usuario puede tener nombre y correo, pero no atributos que no estén definidos”.

⚠ Por qué es TAN importante

- El schema es **global para todo el bosque**
 - **Modificarlo es crítico y casi irreversible**
 - Productos como **Exchange o SCCM** lo extienden
 - Un error aquí afecta **toda la organización**
-

En una sola frase

 **El Schema es el plano que define qué puede existir en Active Directory y cómo debe verse cada objeto.**

Si quieres, puedo:

- Explicártelo desde **seguridad / ataques**
- Compararlo con **LDAP**
- O bajarlo a nivel **principiante absoluto** para capacitación

Domains (English)

Domains are used to group and manage objects in an organization.

Domains:

- An administrative boundary for applying policies to groups of objects
 - A replication boundary for replicating data between domain controllers
 - An authentication and authorization boundary that provides a way to limit the scope of access to resources
-

Dominios (Español)

Los dominios se utilizan para agrupar y administrar objetos dentro de una organización.

Dominios:

- Un límite administrativo para aplicar políticas a grupos de objetos

- Un límite de replicación para la replicación de datos entre controladores de dominio
- Un límite de autenticación y autorización que proporciona una forma de limitar el alcance de acceso a los recursos

Un **dominio** en Active Directory es **una frontera**.

Sirve para decir **hasta dónde aplican reglas, datos y permisos**.

◆ 1 Límite administrativo

Significa:

- Las **políticas (GPOs)** se aplican dentro del dominio
- Los administradores gestionan usuarios, PCs y permisos **de ese dominio**

📌 Ejemplo:

- Dominio: `empresa.local`
- Todos los usuarios de ese dominio reciben:
 - Políticas de contraseña
 - Políticas de bloqueo
 - Configuraciones de Windows

◆ 2 Límite de replicación

Significa:

- Los **controladores de dominio (DCs)** solo replican información **dentro del mismo dominio**
- No replican todo con otros dominios automáticamente

📌 Ejemplo:

- `ventas.empresa.local`
- `finanzas.empresa.local`

Cada uno replica sus propios usuarios y objetos.

♦ 3 Límite de autenticación y autorización

Significa:

- Un dominio controla quién puede autenticarse
- Define a qué recursos puedes acceder

📌 Ejemplo:

- Un usuario de `ventas.empresalocal`
 - ✗ No entra automáticamente a recursos de `finanzas.empresalocal`
 - ✓ Solo si hay confianza (trust)

📘 Analogía sencilla

Piensa en un dominio como:

- 🏢 Un edificio
- Con sus:
 - Reglas
 - Guardias
 - Llaves
 - Oficinas

Otro edificio puede estar conectado, pero no es lo mismo.

✳️ En una frase clara

👉 Un dominio es el límite principal donde Active Directory aplica reglas, replica información y controla accesos.

📌 Trees (English)

A domain tree is a hierarchy of domains in AD DS.

All domains in the tree:

- Share a contiguous namespace with the parent domain

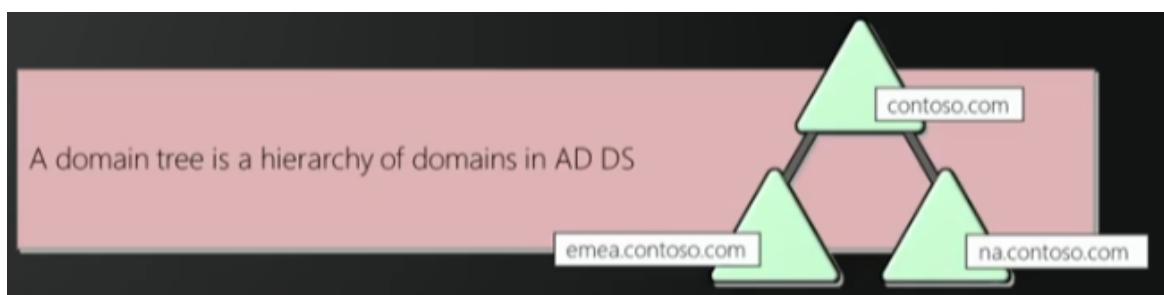
- Can have additional child domains
 - By default create a two-way transitive trust with other domains
-

📌 Árboles de Dominio (Español)

Un árbol de dominio es una jerarquía de dominios en AD DS.

Todos los dominios del árbol:

- Comparten un espacio de nombres contiguo con el dominio padre
- Pueden tener dominios hijos adicionales
- Por defecto crean una relación de confianza bidireccional y transitiva con otros dominios



🧠 Explicación clara y aterrizada

Un Domain Tree (árbol de dominios) es un conjunto de dominios relacionados jerárquicamente que comparten el mismo nombre base.

◆ ¿Qué significa “namespace contiguo”?

Que todos los dominios usan el mismo nombre principal, solo agregando niveles.

📌 Ejemplo:

- Dominio raíz: `contoso.com`

- Dominios hijos:
 - `emea.contoso.com`
 - `na.contoso.com`

👉 Todos terminan en `contoso.com`

◆ **Jerarquía (padre → hijos)**

- `contoso.com` → dominio **padre**
- `emea.contoso.com` → dominio **hijo**
- `na.contoso.com` → dominio **hijo**

Cada dominio:

- Tiene sus propios usuarios
- Sus propios DCs
- Sus propias políticas

◆ **Confianza bidireccional y transitiva (clave 🔒)**

Por defecto:

- Si `emea.contoso.com` confía en `contoso.com`
- Y `contoso.com` confía en `na.contoso.com`
- Entonces `emea` y `na` también confían entre sí

👉 Eso es **transitividad**

📌 Ejemplo práctico:

- Usuario en `emea.contoso.com`
- Puede acceder a recursos en `na.contoso.com`
- Si los permisos lo permiten

📘 Analogía sencilla

Piensa en:

-  Árbol = Empresa
-  Ramas = Regiones
-  Hojas = Oficinas

Todo pertenece a la **misma marca (contoso.com)**.

En una frase clara

 Un domain tree es una estructura jerárquica de dominios que comparten el mismo nombre base y confían entre sí automáticamente.

Forests (English)

A forest is a collection of one or more domain trees.

Forests:

- Share a common schema
 - Share a common configuration partition
 - Share a common global catalog to enable searching
 - Enable trusts between all domains in the forest
 - Share the Enterprise Admins and Schema Admins groups
-

Bosques (Español)

Un bosque es una colección de uno o más árboles de dominio.

Bosques:

- Comparten un esquema común
 - Comparten una partición de configuración común
 - Comparten un catálogo global común para habilitar búsquedas
 - Habilitan relaciones de confianza entre todos los dominios del bosque
 - Comparten los grupos Enterprise Admins y Schema Admins
-

Explicación clara (nivel conceptual)

Un Forest (Bosque) es el límite de seguridad MÁS grande en Active Directory.

👉 Todo lo que esté dentro del bosque **confía entre sí** y **comparte reglas críticas**.

◆ ¿Qué significa cada punto?

1 Comparten el Schema

- Todos los dominios usan **las mismas definiciones de objetos**
 - Si cambias el schema → impactas **todo el bosque**
- 📌 Por eso modificar el schema es **crítico**.
-

2 Comparten la partición de configuración

- Define cómo funciona AD a nivel global
 - Servicios, sitios, replicación, etc.
- 👉 Es como el **archivo de configuración central**.
-

3 Comparten el Global Catalog

- Permite buscar usuarios y objetos **en todo el bosque**
 - Sin importar el dominio
- 📌 Ejemplo:

Buscar a “Juan Pérez” sin saber si está en ventas.contoso.com o na.contoso.com

4 Confianza entre todos los dominios

- La confianza es:
 - Automática

- Bidireccional
- Transitiva

👉 Esto facilita el acceso... y también los ataques 😊

5 Grupos ultra-privilegiados compartidos

- Enterprise Admins
- Schema Admins

📌 Miembro de estos grupos = poder sobre TODO el bosque.

📘 Analogía sencilla

- 🌲 Bosque → Corporación completa
- 🌳 Árboles → Empresas / marcas
- 🏢 Dominios → Regiones o áreas

Todo bajo un mismo gobierno central.

🧩 En una frase clara

👉 Un forest es el límite máximo de confianza y configuración en Active Directory. Si caes el forest, cae todo.

📌 Organizational Units (OUs) - English

OUs are Active Directory containers that can contain users, groups, computers, and other OUs.

OUs are used to:

- Represent your organization hierarchically and logically
- Manage a collection of objects in a consistent way
- Delegate permissions to administer groups of objects
- Apply policies

Unidades Organizativas (OU) - Español

Las OU son contenedores de Active Directory que pueden contener usuarios, grupos, computadoras y otras OU.

Las OU se utilizan para:

- Representar a la organización de forma jerárquica y lógica
 - Administrar un conjunto de objetos de manera consistente
 - Delegar permisos para administrar grupos de objetos
 - Aplicar políticas
-

Explicación clara y aterrizada

Una OU (Organizational Unit) es básicamente una **carpeta dentro de un dominio**.

Sirve para **organizar, administrar y aplicar reglas** a usuarios y computadoras.

◆ ¿Qué puede haber dentro de una OU?

-  Usuarios
-  Computadoras
-  Grupos
-  Otras OU (sub-OUs)

 **Ojo:** las OU NO son límites de seguridad como dominios o forests.

◆ ¿Para qué se usan realmente?

1 Representar la estructura de la empresa

Puedes organizar AD como tu empresa funciona:

📌 Ejemplo:

```
empresa.local
└── OU Ventas
└── OU Finanzas
└── OU TI
    └── OU Servidores
    └── OU Usuarios
```

2 Administrar objetos de forma consistente

Todo lo que esté en la misma OU:

- Se administra igual
- Tiene las mismas políticas

📌 Ejemplo:

- Todas las PCs de **Ventas**
- Todas las PCs tienen la misma configuración

3 Delegar permisos (MUY importante)

Puedes dar permisos sin hacer admin del dominio.

📌 Ejemplo:

- El jefe de TI puede:
 - Crear usuarios solo en **OU Ventas**
 - Resetear contraseñas ahí
- ❌ No toca Finanzas ni servidores

4 Aplicar políticas (GPOs)

Las **Group Policy Objects** se aplican:

- A sitios
- A dominios
- **Principalmente a OUs**

📌 Ejemplo:

- Bloquear USB
 - Configurar firewall
 - Forzar fondos de pantalla
 - Políticas de contraseña (según diseño)
-

📘 Analogía sencilla

- 📁 Dominio → Archivador
- 📁 OU → Carpetas
- 📄 Usuarios / PCs → Documentos

📌 Trusts (English)

Trusts provide a mechanism for users to gain access to resources in another domain.

Types of Trusts

Type	Description
Directional	The trust direction flows from the trusting domain to the trusted domain
Transitive	The trust relationship is extended beyond a two-domain trust to include other trusted domains

Notes

- All domains in a forest trust all other domains in the forest
 - Trusts can extend outside the forest
-

📌 Confianzas (Trusts) - Español

Las confianzas proporcionan un mecanismo para que los usuarios obtengan acceso a recursos en otro dominio.

Tipos de Confianza

Tipo	Descripción
Direccional	La dirección de la confianza fluye del dominio que confía hacia el dominio confiado
Transitiva	La relación de confianza se extiende más allá de dos dominios para incluir otros dominios confiables

Notas

- Todos los dominios dentro de un bosque confían en los demás dominios del bosque
 - Las confianzas pueden extenderse fuera del bosque
-

Explicación clara (esto es CLAVE en AD)

Una **trust (confianza)** es un acuerdo entre dominios que dice:

“Acepto usuarios del otro dominio para que accedan a mis recursos”.

◆ Confianza direccional (Directional)

La confianza **NO siempre es mutua**.

 Ejemplo:

- Dominio A **confía en** Dominio B
- Usuarios de B pueden acceder a recursos en A
- Usuarios de A  NO acceden a B

 Es como decir:

“Acepto visitas, pero no puedo entrar yo”.

◆ Confianza transitiva (Transitive)

La confianza **se hereda**.

📌 Ejemplo:

- A confía en B
- B confía en C
- Entonces A confía en C

👉 Esto pasa **automáticamente dentro de un forest.**

◆ Trusts dentro del Forest

Por defecto:

- Todos los dominios del forest:
 - Confían entre sí
 - La confianza es:
 - Bidireccional
 - Transitiva

📌 Por eso el forest es el **límite máximo de seguridad.**

◆ Trusts fuera del Forest

Se pueden crear trusts con:

- Otro forest
- Otro dominio externo
- Otra empresa

📌 Ejemplo:

- Empresa A
- Empresa B (proveedor)

👉 Se hace un **External Trust o Forest Trust.**

📘 Analogía sencilla

- 🏢 Dominio → Oficina
- 💬 Trust → Pase de visitante

Algunas oficinas:

- Te dejan entrar
- Otras no
- Algunas solo a ciertas áreas

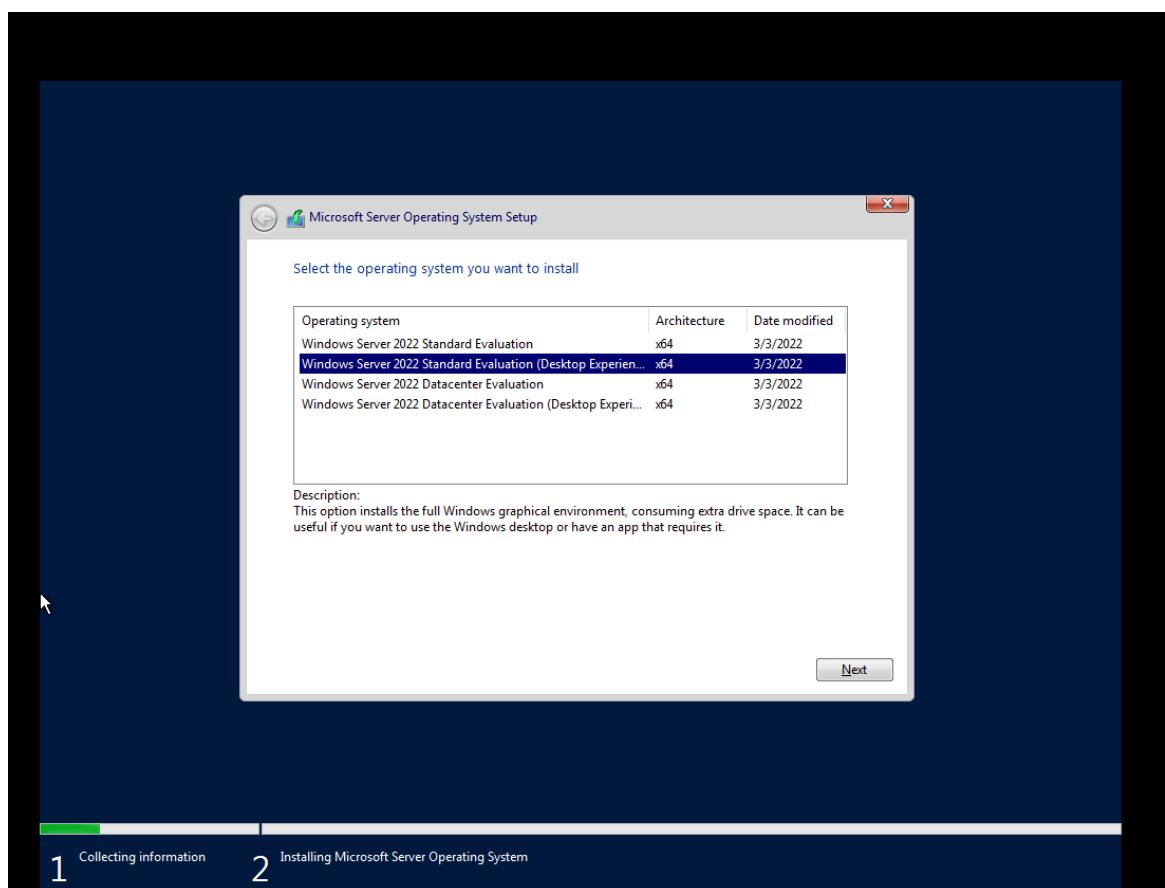
En una frase clara

👉 Una trust es la regla que define quién puede acceder a recursos en otro dominio y hasta dónde llega esa confianza.

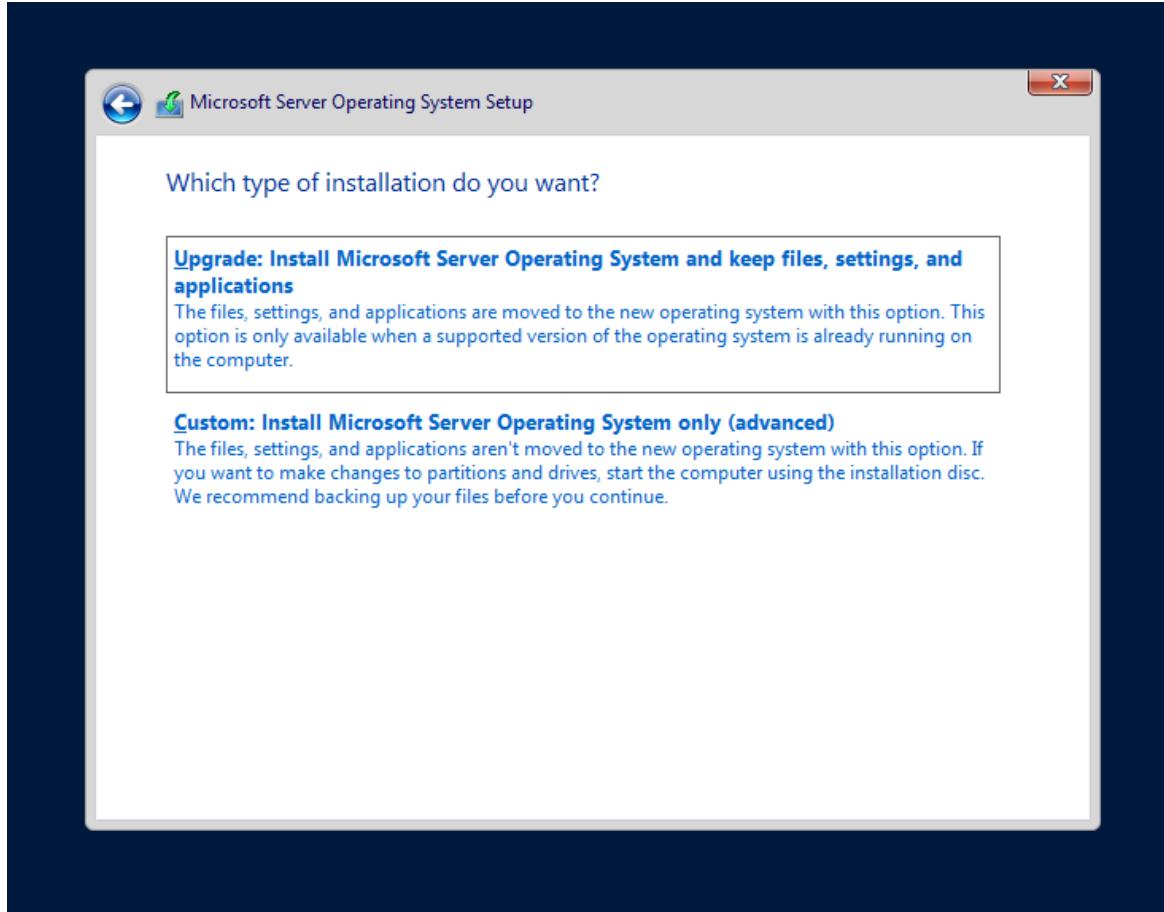
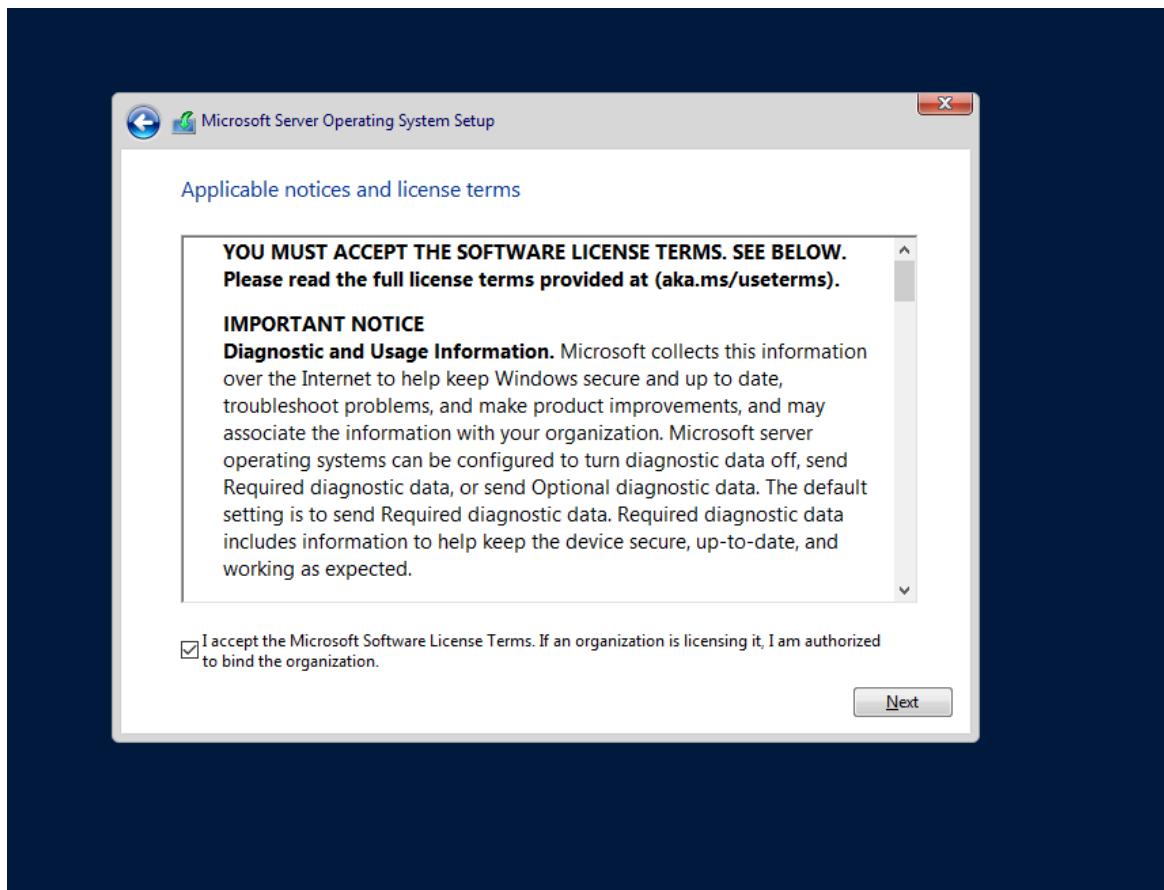
▼ Chapter 6.2. Armar active

directory casero

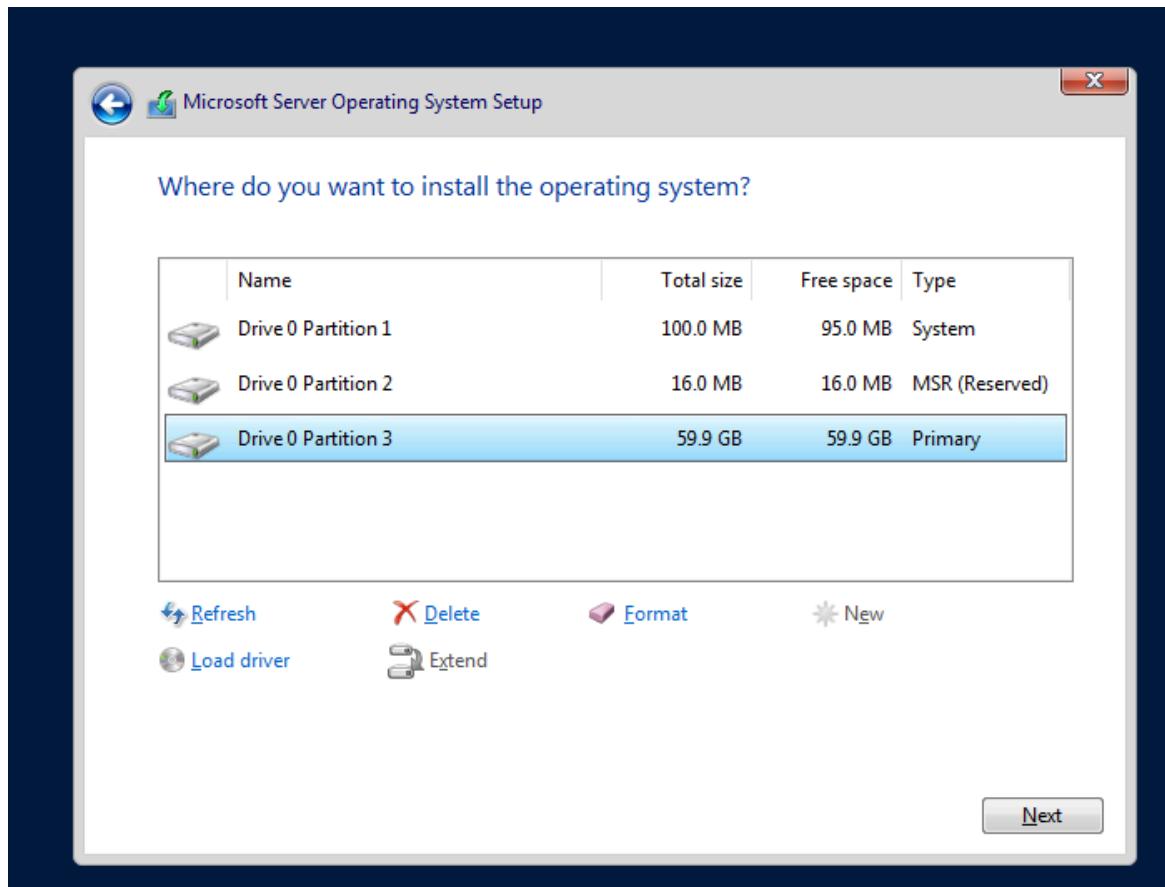
Primero necesitamos los .iso de en este caso Windoes server 2022 y 2 windows 11 Enterprise edition



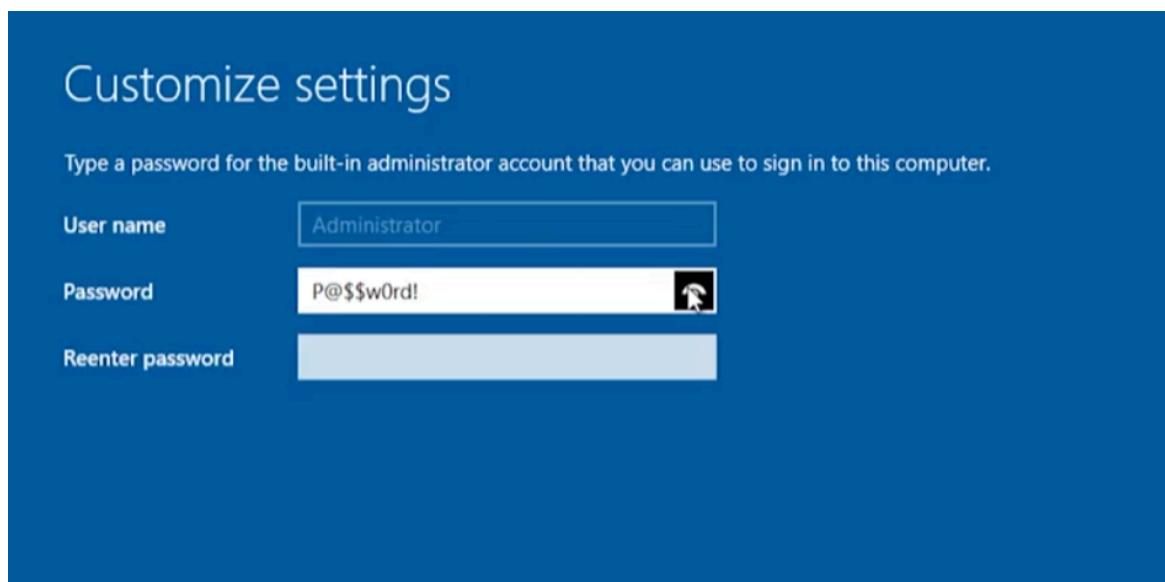
Ahora seguimos los pasos en pantalla,



Despues en custom.

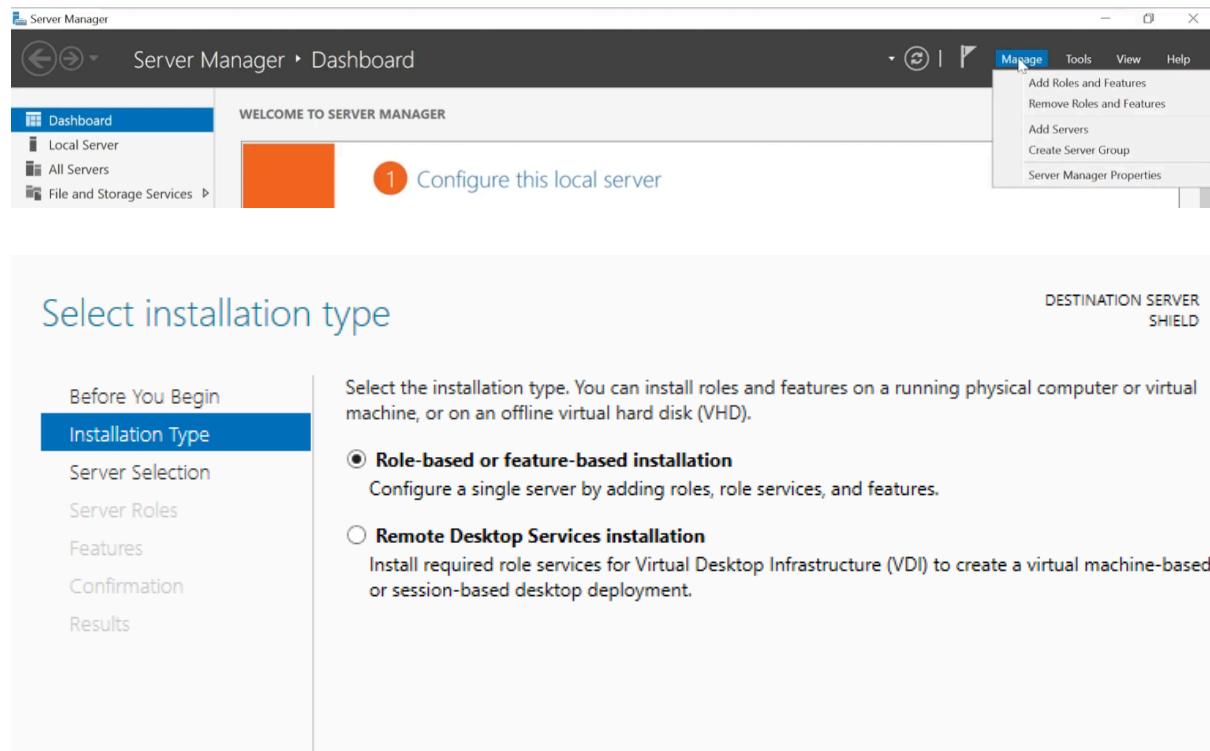


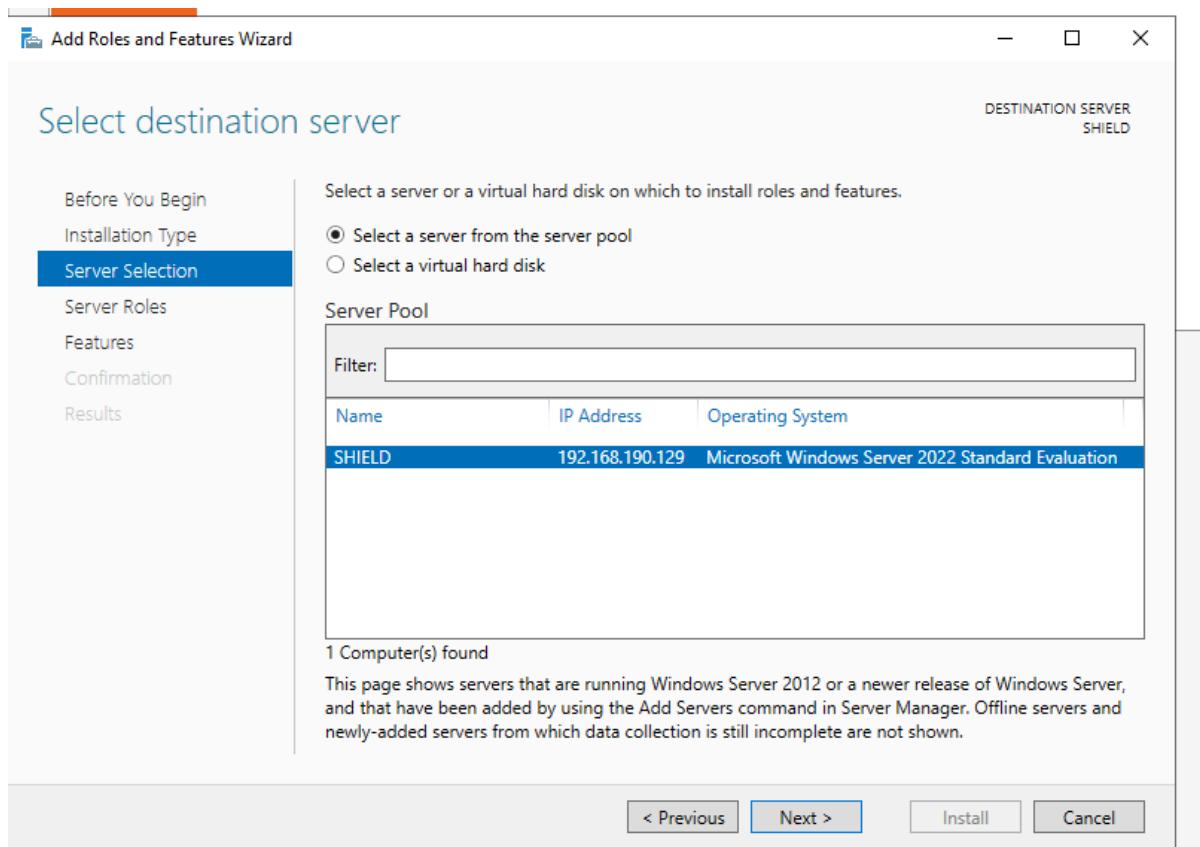
new --> apply---> Primary Drive -> next



P@\$\$w0rd!

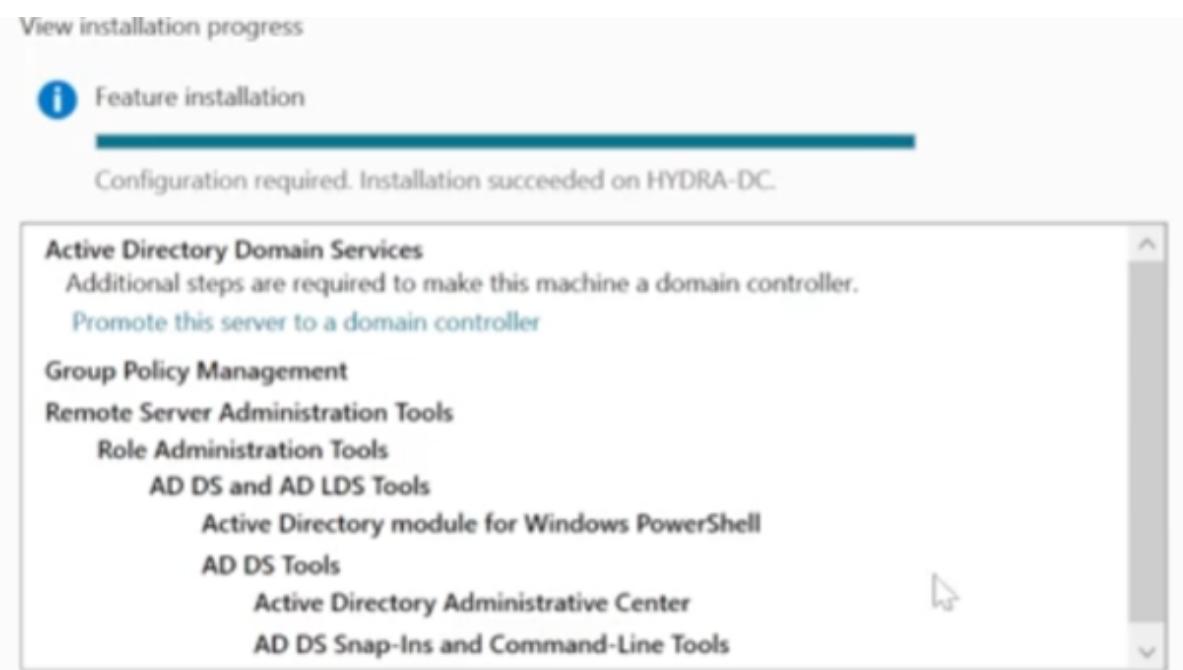
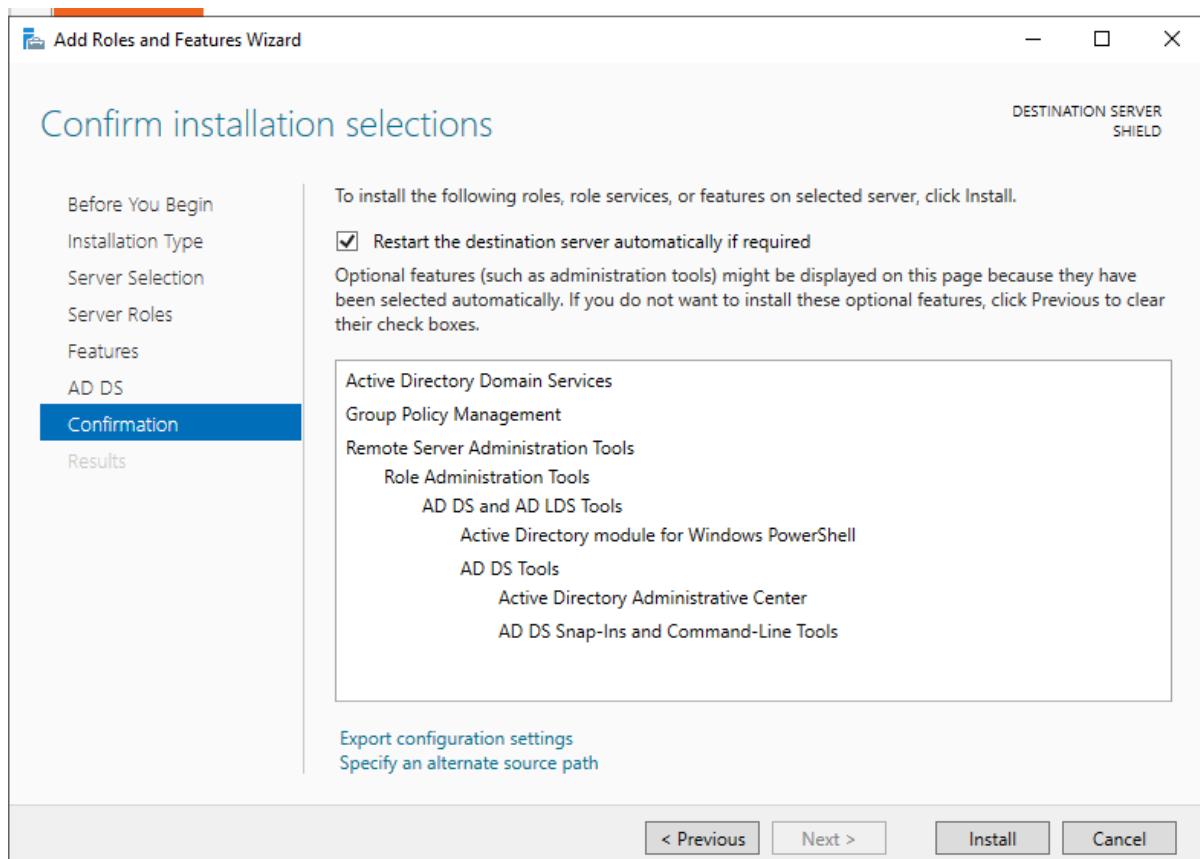
ahora en el Server Manager vamos a esa parte



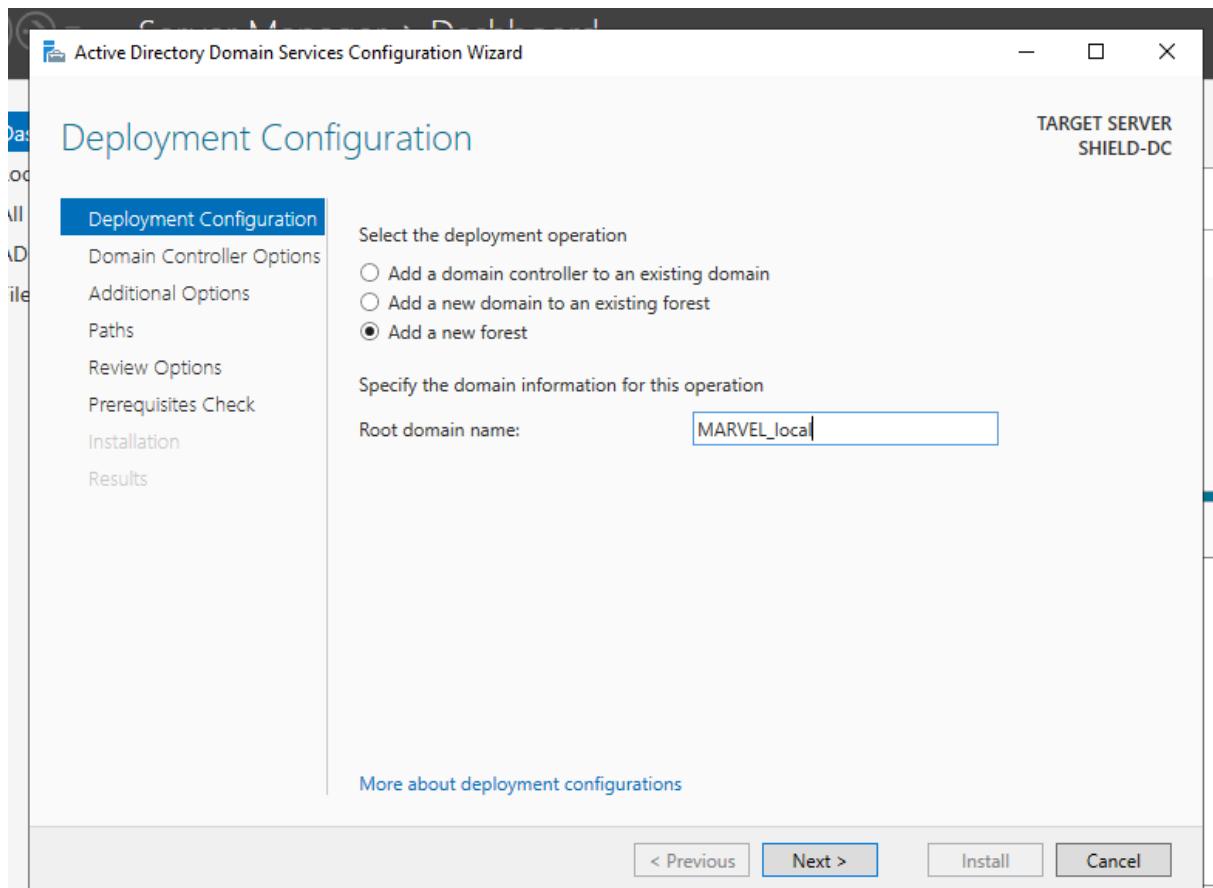


damos a esos 2 next despues agregamos esto lo cual nos permitira tener los servicios de AD

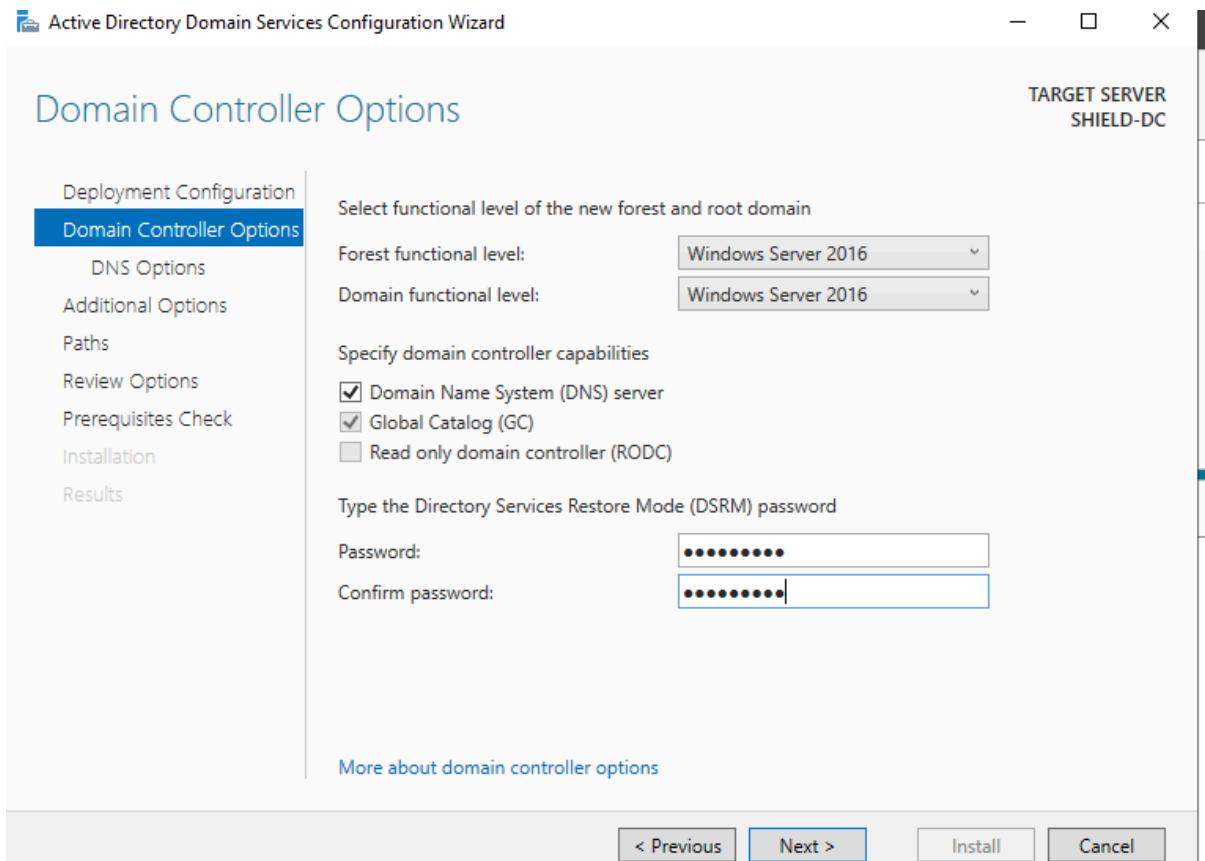
- Active Directory Certificate Services
- Active Directory Domain Services
- Active Directory Federation Services



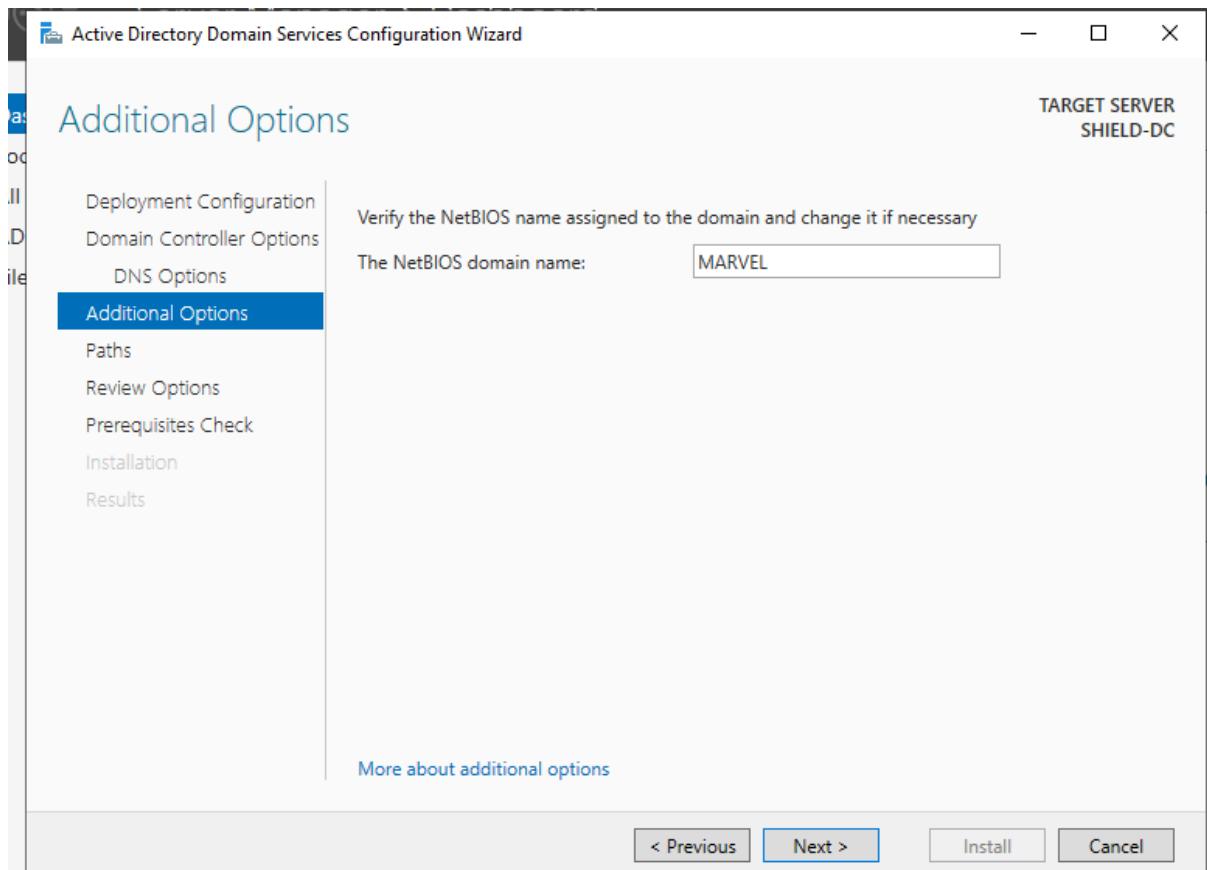
y install



damos next y despues



damos la misma contraseña que el server y next



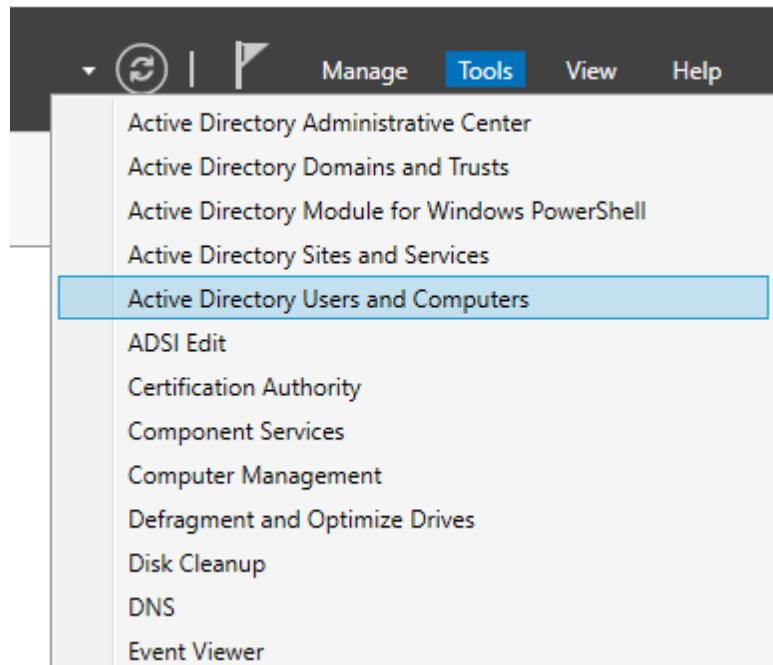
Specify the location of the AD DS database, log files, and SYSVOL

Database folder:	C:\Windows\NTDS	...
Log files folder:	C:\Windows\NTDS	...
SYSVOL folder:	C:\Windows\SYSVOL	...

despues visualizamos las rutas y le damos next

una vez cargada damos next

Vamos a setear Users, Grupos y politicas



Primero vamos a esta parte para ajustar las políticas usuarios etc.

A screenshot of the Active Directory Users and Computers console window. The title bar says "Active Directory Users and Computers". The menu bar includes File, Action, View, and Help. The toolbar has various icons for navigation and management. The left pane shows a tree view of the directory structure under "MARVFI.local", with "Saved Queries" expanded. The right pane displays a table of objects with columns for Name, Type, and Description. A context menu is open over the "Organizational Units" container, listing options like New, All Tasks, View, Refresh, Export List..., Properties, and Help. A sub-menu for "New" is open, showing options: Computer, Contact, Group, InetOrgPerson, msDS-ShadowPrincipalContainer, msImaging-PSPs, MSMQ Queue Alias, Organizational Unit (which is selected and highlighted with a blue selection bar), Printer, User, and Shared Folder. At the bottom of the window, there is a message "Create a new object...".

vamos a esta parte con click derecho para crear una OU movemos todos a nuevo OU groups solo dejamos al administrador y al invitado

Name	Type	Description
Administrator	User	Built-in account for ad...
Guest	User	Built-in account for gue...

Creamos 2 nuevos admin dandole a copy

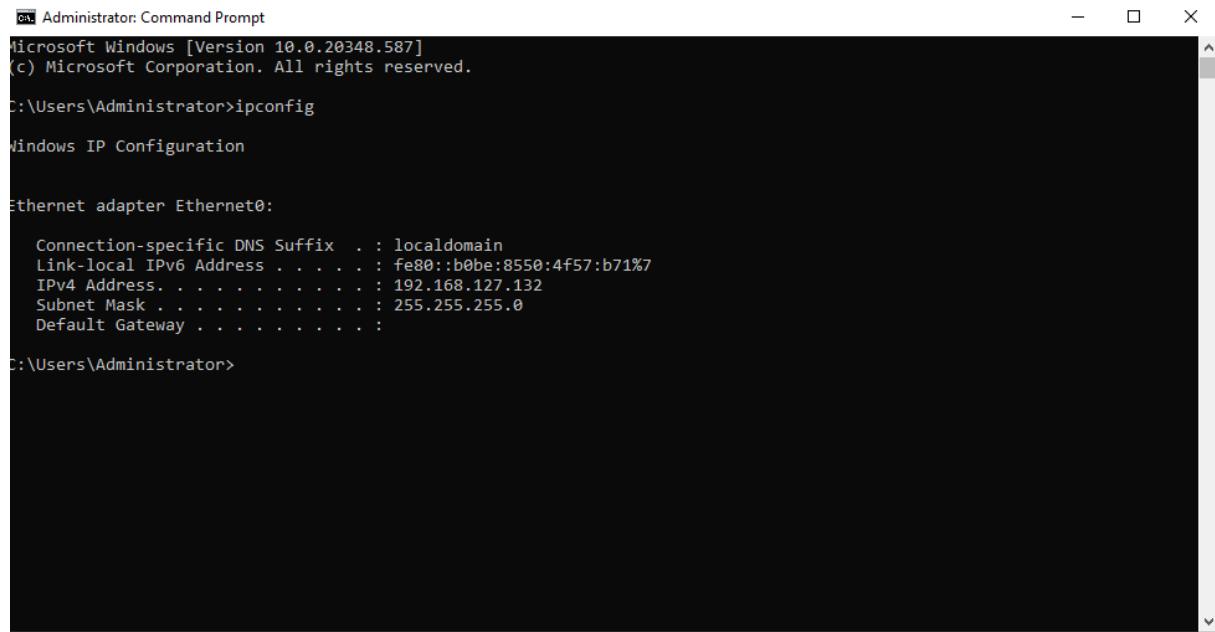
```
tony stark / password123!
SQL MYpassword123#
Frank Castel / Password1
Peter Parker / Password2
```

Ahora creamos una carpeta de archivos compartidos,

The screenshot shows the Windows Server Manager interface under File and Storage Services > Shares. The left navigation pane has 'Shares' selected. The main area lists 'SHARES' with 2 total shares: 'HYDRA-DC (2)'. The 'NETLOGON' share is highlighted. The 'VOLUME' panel on the right shows 'NETLOGON on HYDRA-DC' with a 20% used status.

Share	Local Path	Protocol	Availability Type
NETLOGON	C:\Windows\SYSVOL\sysvol\MAR...	SMB	Not Clustered
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Not Clustered

Share	Local Path	Protocol	Availability Type
▲ SHIELD-DC (3)			
NETLOGON	C:\Windows\SYSVOL\sysvol\MAR...	SMB	Not Clustered
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Not Clustered
hackme	C:\Shares\hackme	SMB	Not Clustered



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

  Connection-specific DNS Suffix  . : localdomain
  Link-local IPv6 Address . . . . . : fe80::b0be:8550:4f57:b71%7
  IPv4 Address . . . . . : 192.168.127.132
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

C:\Users\Administrator>
```

tambien ponemos la ip estatica y listo.

Diagrama del laboratorio - Active Directory (MARVEL-SHIELD)