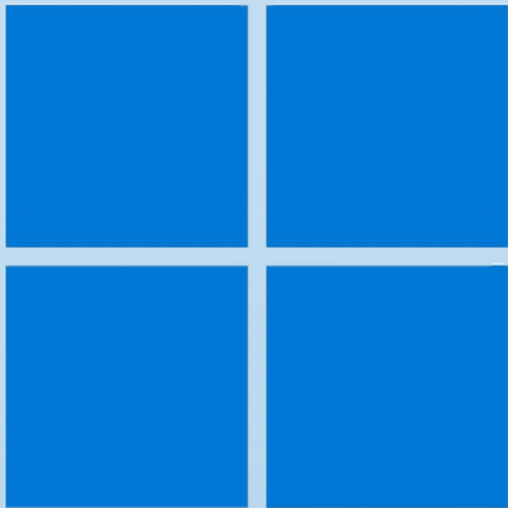


SERVIDOR DE DOMINIO: ACTIVE DIRECTORY



Microsoft

Active Directory

SISTEMAS OPERATIVOS EN RED
JUAN CARLOS NAVIDAD GARCÍA

1. ¿Qué es un servicio de directorio? Funciones y Ejemplo para sistemas Windows y otro para sistemas Linux

Un servicio de directorio es una aplicación o conjunto de aplicaciones que sirven para, en una red informática, almacenar, organizar y centralizar la información de los usuarios, equipos, grupos, dominios, recursos compartidos, políticas de seguridad, etc, con el fin de facilitar su localización y administración.

- En Linux se utiliza LDAP Lightweight Directory Access Protocol, o Protocolo ligero de acceso a directorios.
- En Windows se utiliza Active Directory Domain Services, ADDS.

2. Define los principales elementos jerárquicos de la Base de datos de ADDS

- Objetos: es el elemento básico de la red. Un usuarios o equipo son ejemplos de objetos, que se suelen denominar hoja, dentro de la estructura jerárquica.
- Dominio de Active Directory: es un contenedor lógico utilizado para administrar unidades organizativas, usuarios, grupos, equipos y políticas de seguridad, entre otros objetos.
- Árbol: dominio o agrupación de dominios para permitir el uso compartido de recursos globales.
- Bosque: árbol o agrupación de árboles, por tanto, agrupación de dominios que comparten una misma estructura y configuración.

3. Cual es la herramienta utilizada para gestionar los recursos en el dominio del active directory. (usuarios, grupos, OU, equipos, etc)

Se utiliza el Administrador del servidor, para poder acceder a los diferentes apartados de Active Directory.

4. Que es una plantilla de creación de usuarios. Como se utiliza

Básicamente es una hoja de cálculo con formato .csv con toda la información de los usuarios a crear. Este fichero posteriormente tendríamos que importarlo desde terminal para que se nos creen los usuarios en el sistema. El comando es:

```
- csvde -r "(objectclass=user)" -f c:\fichero.csv
```

5. Diferencia entre grupos

- a. Locales: A los miembros de estos grupos solo se les puede asignar permiso dentro de un dominio.
- b. Globales: A los miembros de estos grupos se les pueden asignar permisos en cualquier dominio del bosque. Se suelen utilizar para administrar cuentas de usuario y de equipos que requieren un mantenimiento diario.
- c. Universales: A los miembros de estos grupos se les pueden asignar permisos en cualquier dominio del bosque. Conviene utilizar estos grupos para aquellos que abarquen varios dominios.

6. Como se puede agregar un equipo a un dominio

Panel de control → Sistema y seguridad → Sistema

En el apartado Nombre de equipo, le damos a Cambiar y desde ahí podremos agregar o modificar un dominio.

Una vez introducido, hay añadir la dirección DNS a nuestra interfaz de red. Panel de control → Redes e Internet → Conexiones de red.

Hacemos click derecho sobre nuestra interfaz y le damos a propiedades.

En la ventana que se nos abre, clicamos sobre Protocolo de Internet TCP / IPv4 Y Pulsaremos en el botón Propiedades.

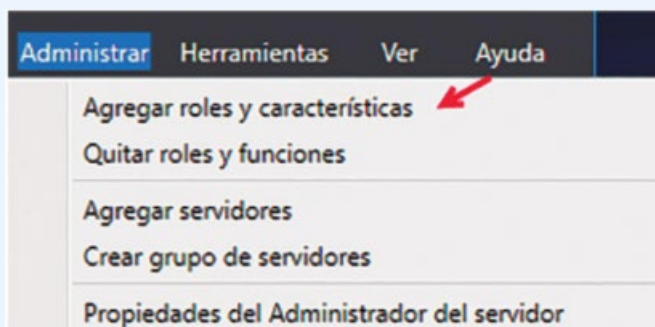
Desde la nueva ventana fijaremos la dirección IP del servidor DNS para que así localice el dominio.

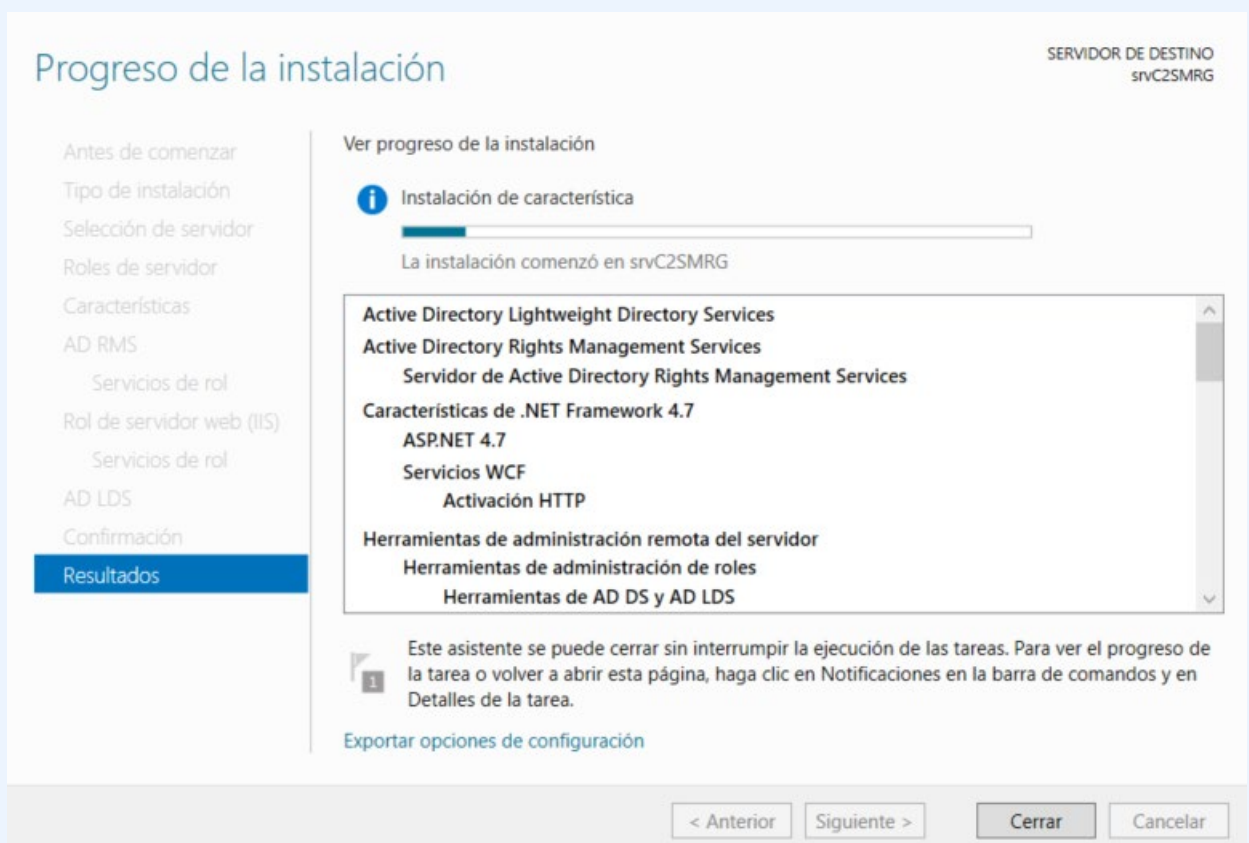
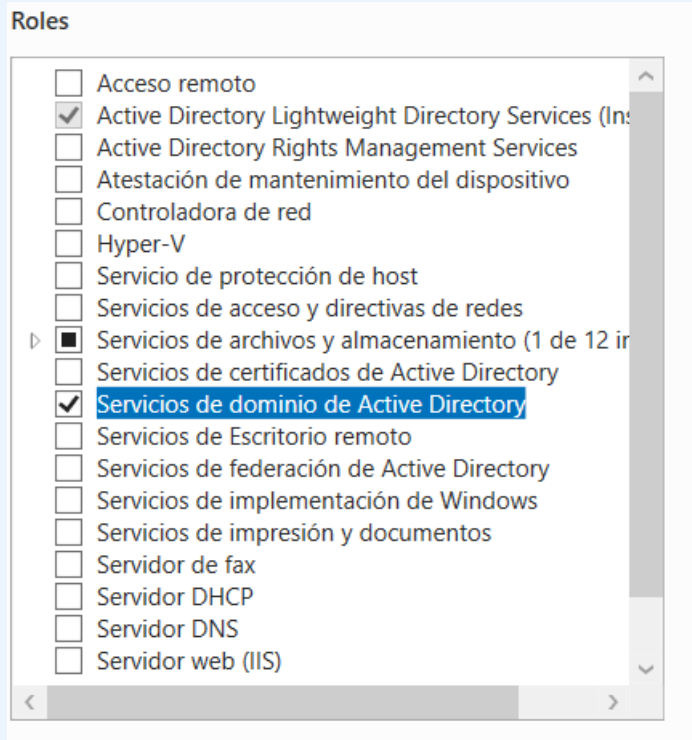
7. Define perfil de usuario. Tipos de perfiles

Un perfil de usuario de Windows es un conjunto de carpetas, archivos y parámetros de Registro y de configuración que definen el entorno de un usuario que inicia una sesión con una cuenta de usuario específica.

- Perfiles locales: Perfiles creados en un equipo cuando un usuario inicia sesión. El perfil es específico de un usuario, local al equipo y se almacena en el disco duro del equipo local.
- Perfiles móviles: Perfiles creados por un administrador y almacenados en un servidor.

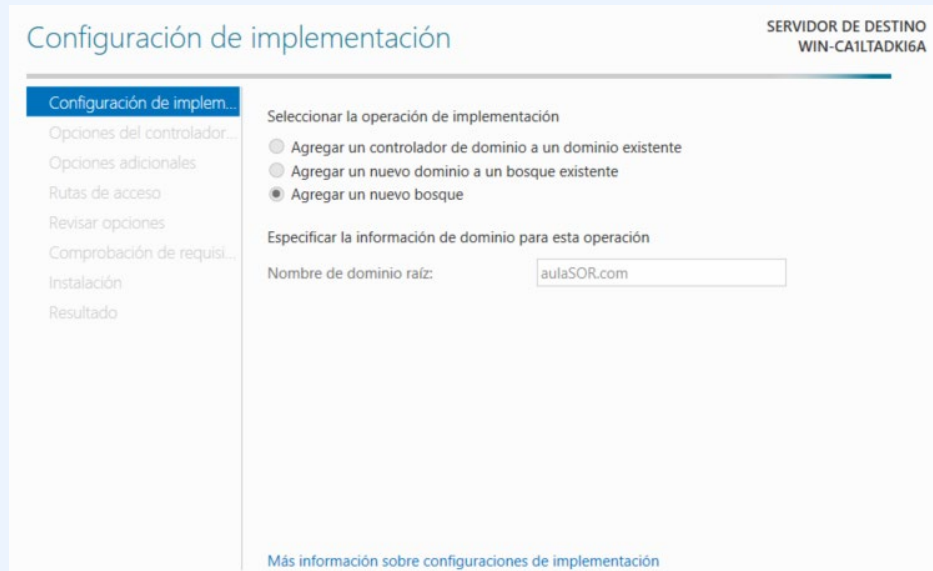
1. Instala el rol servicios de dominio de Active Directory y las características relacionadas



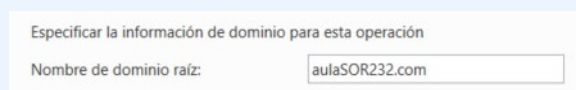


2. Configura el AD promocionando el servidor como controlador de dominio de forma que:

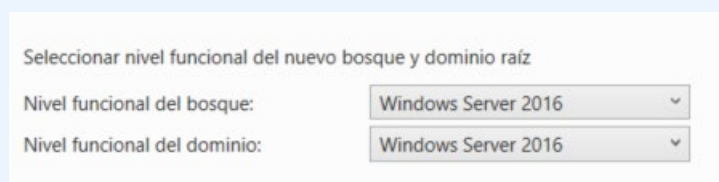
- a. El equipo actuará como primer controlador de dominio de un nuevo bosque



- b. El nombre del dominio estará formado por tus iniciales seguidas del SMRn°puesto.local



- c. El nivel de funcionalidad del bosque será el equivalente a tu versión de windows server (2016)



- d. El nombre NetBios del dominio y la ubicación de los datos del directorio serán los que predetermine el asistente

Asistente para configuración de Servicios de dominio de Active Directory

Opciones adicionales

SERVIDOR DE DESTINO
WIN-CA1LTADKI6A

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

Verifique el nombre NetBIOS asignado al dominio y cámbielo si es necesario

Nombre de dominio NetBIOS:

Rutas de acceso

SERVIDOR DE DESTINO
WIN-CA1LTADKI6A

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

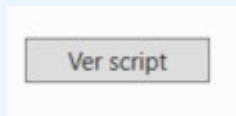
Especificar la ubicación de la base de datos de AD DS, archivos de registro y SYSVOL

Carpeta de la base de datos: ...

Carpeta de archivos de registro: ...

Carpeta SYSVOL: ...

- e. Exportar el script de PowerShell para automatizar futuras instalaciones

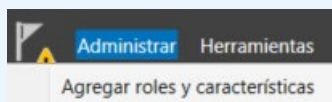


```
#
# Script de Windows PowerShell para implementación de AD DS
#

Import-Module ADDSDeployment
Install-ADDSForest `
-CreateDnsDelegation:$false `
-DatabasePath "C:\Windows\NTDS" `
-DomainMode "WinThreshold" `
-DomainName "aulaSOR232.com" `
-DomainNetbiosName "AULASOR232" `
-ForestMode "WinThreshold" `
-InstallDns:$true `
-LogPath "C:\Windows\NTDS" `
-NoRebootOnCompletion:$false `
-SysvolPath "C:\Windows\SYSVOL" `
-Force:$true
```

1. Herramienta administrador del servidor/panel/agregar roles y características

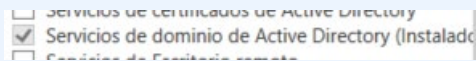
- a. Instalación de roles



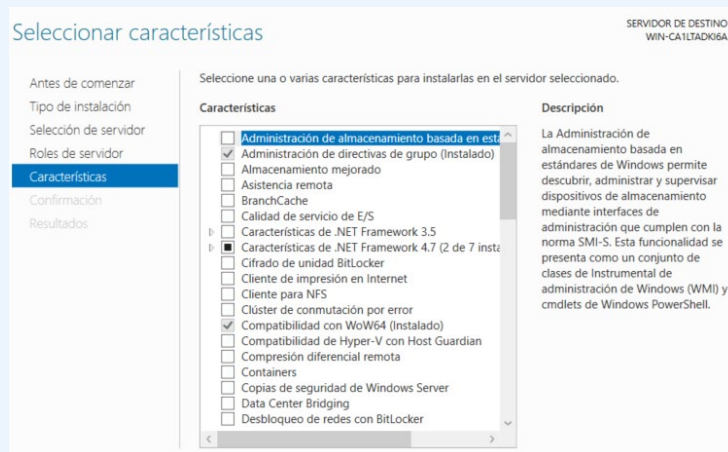
- b. Seleccionamos el servidor



c. Servicio de dominio de active directory



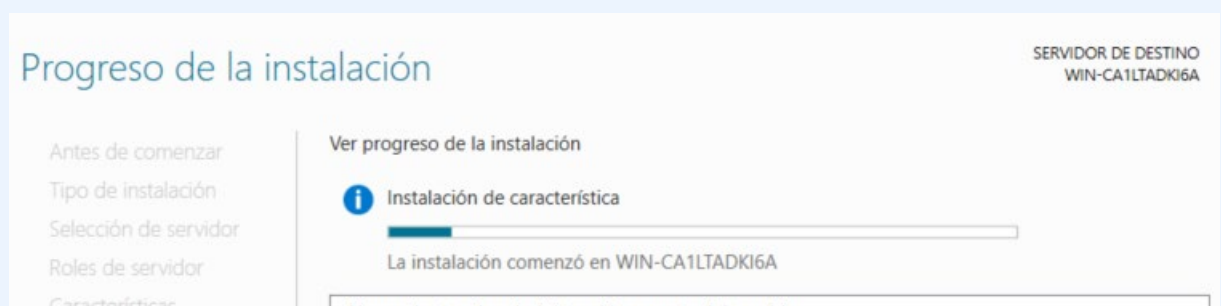
d. Agregar características



e. Activar casilla de reinicio

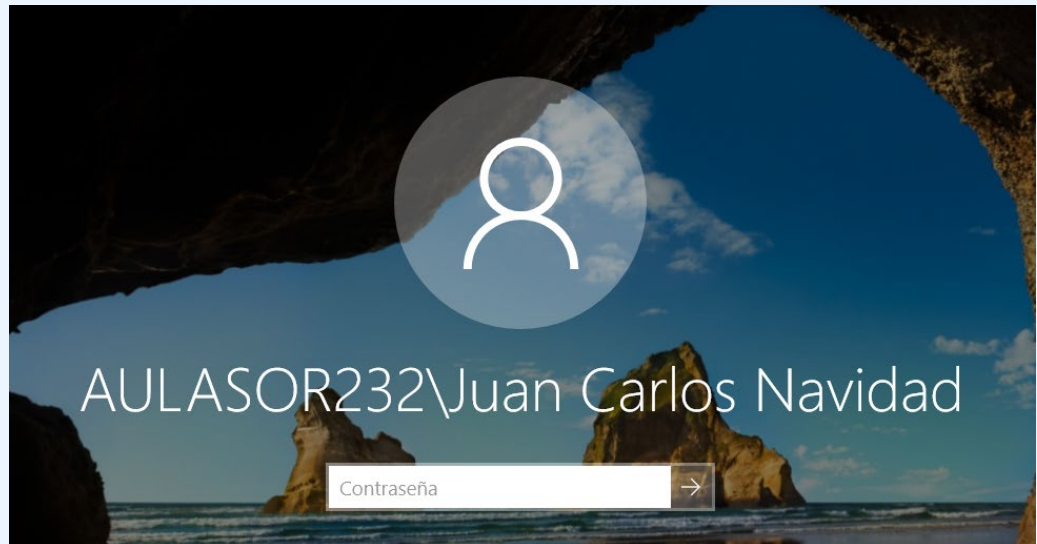


f. Confirmamos e instalamos.



2. Promover este servidor a controlador de dominio. (el controlador de dominio es el equipo principal en una red de windows que administra inicios de sesión de usuario y permisos. Además aloja un active directory y controla los recursos de red:

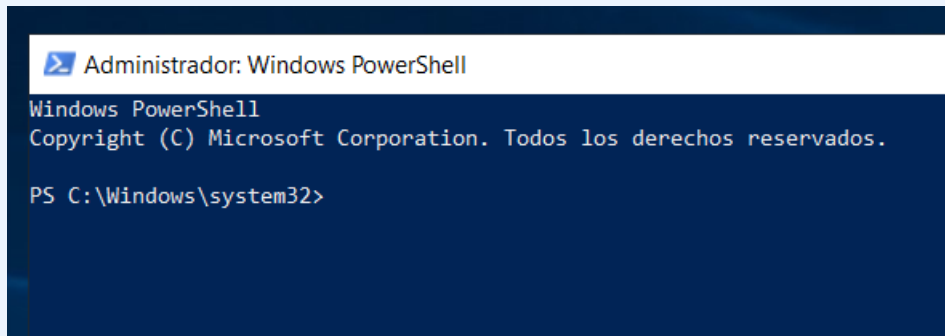
- a. Iniciamos sesión para verificar que nos aparece
 - i. Dominio\Administrador



- b. Una vez dentro verificamos que el proceso se ha realizado correctamente accediendo a las propiedades del equipo y verificando que se ha creado el dominio.

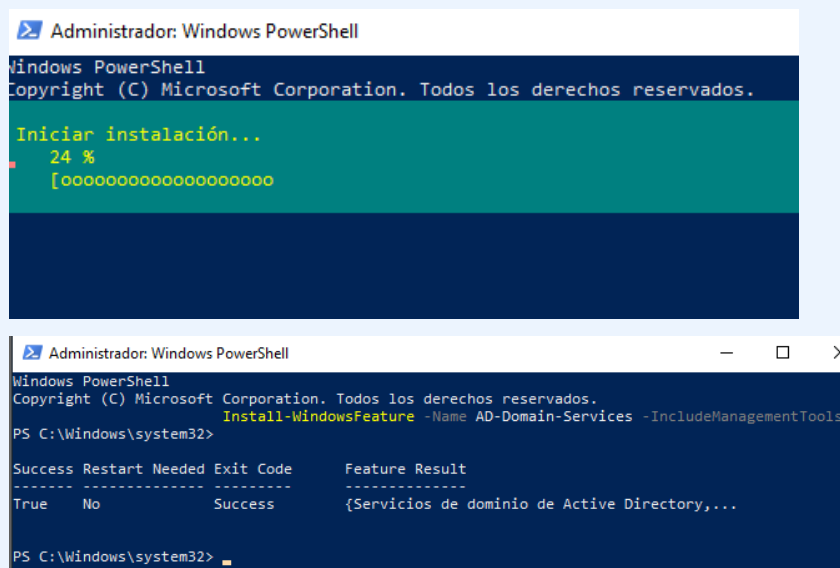
Configuración de nombre, dominio y grupo de trabajo del equipo	
Nombre de equipo:	WIN-CA1LTADKI6A
Nombre completo de equipo:	WIN-CA1LTADKI6A.aulaSOR232.com
Descripción del equipo:	WSSOR
Dominio:	aulaSOR232.com

1. Powershell

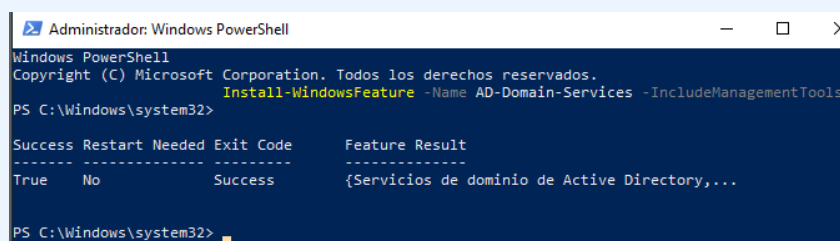


2. Utilizar el comando install-windowsFeature para instalar roles o características

```
Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools
```



a. Nos aparecerá el resumen indicando success en caso de instalación correcta



3. Promocionar el servidor como controlador de dominio

- a. Necesitamos los cmdlets del modulo ADDSDeployment, por lo que tendremos que importarlo

Import-Module ADDSDeployment

```
PS C:\Windows\system32> Import-Module ADDSDeployment
PS C:\Windows\system32>
```

- i. Instalamos un bosque nuevo

Install-ADDSForest

- ii. Nos pedirá nombre de dominio y contraseña

```
PS C:\Windows\system32> Install-ADDSForest

cmdlet Install-ADDSForest en la posición 1 de la canalización de comandos
Proporcione valores para los parámetros siguientes:
DomainName: aulaSOR232.com
SafeModeAdministratorPassword: *****
Confirmar SafeModeAdministratorPassword: *****

El servidor de destino se configurará como un controlador de dominio y se reiniciará cuando se
complete esta operación.
¿Desea continuar con esta operación?
[S] Sí [O] Sí a todo [N] No [T] No a todo [U] Suspender [?] Ayuda
(el valor predeterminado es "S"):S
ADVERTENCIA: Los controladores de dominio de Windows Server 2019 tienen un valor
predeterminado para la configuración de seguridad denominada "Permitir algoritmos de
criptografía compatibles con Windows NT 4.0" que evita el uso de algoritmos de criptografía
débiles al establecer sesiones de canal de seguridad.

Para obtener más información acerca de esta opción de configuración, consulta el artículo
942564 de Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=104751).
```

4. Inicia el sistema y comprueba con sconfig que el sistema dispone de un dominio.

```
=====
                        Configuración del servidor
=====

Dominio o grupo de trabajo:      Dominio: aulaSOR232.com
Nombre de equipo:                WIN-ARE9EIEBN1A
Agregar administrador local
Configurar administración remota  Habilitado
Configuración de Windows Update: Solo descarga
Descargar e instalar actualizaciones
Escritorio remoto:              Deshabilitado
```

5. Comprobaremos la estructura AD

- Importaremos el modulo que nos va a permitir trabajar con directorios activos (cmdlets)

Import-Module ActiveDirectory

```
Administrador: Windows PowerShell
PS C:\Windows\system32> Import-Module ActiveDirectory
PS C:\Windows\system32>
```

- Comprobar los roles y características que tenemos instalados en el sistema
<https://technet.microsoft.com/en-us/library/jj205469.aspx>

Get-WindowsFeature -ComputerName server-2019-b

```
PS C:\Windows\system32> Get-WindowsFeature -ComputerName MIN-ARE9E1BN1A

Display Name      Name      Install State
-----
[ ] Acceso remoto RemoteAccess Available
[ ] DirectAccess y VPN (RAS) DirectAccess-VPN Available
[ ] Enrutamiento Routing Available
[ ] Proxy de aplicación web Web-Application-Proxy Available
[ ] Active Directory Lightweight Directory Services ADLDS Available
[ ] Active Directory Rights Management Services AD RMS Available
[ ] Servidor de Active Directory Rights Management Services AD RMS-Server Available
[ ] Compatibilidad con la federación de identidades AD FS-Identity Available
[ ] Atestación de mantenimiento del dispositivo DeviceHealthAttestation Available
[ ] Controladora de red NetworkController Available
[ ] Hyper-V Hyper-V Available
[ ] Servicio de protección de host HostGuardianServiceRole Available
[ ] Servicios de acceso y directivas de redes NPAS Available
[X] Servicios de archivos y almacenamiento FileAndStorage-Services Installed
[X] Servicios de almacenamiento Storage-Services Installed
[X] Servicios de iSCSI y archivo File-Services Installed
[X] Servidor de archivos FS-FileServer Installed
[ ] Administrador de recursos del servidor d... FS-Resource-Manager Available
[ ] BranchCache para archivos de red FS-BranchCache Available
[ ] Carpetas de trabajo FS-SyncShareService Available
[ ] Desduplicación de datos FS-Data-Deduplication Available
[ ] Espacios de nombres DFS FS-DFS-Namespace Available
[ ] Proveedor de almacenamiento del destino ... iSCSITarget-VSS-VDS Available
[ ] Replicación DFS FS-DFS-Replication Available
[ ] Servicio del agente VSS del servidor de ... FS-VSS-Agent Available
[ ] Servidor del destino iSCSI FS-iSCSITarget-Server Available
[ ] Servidor para NFS FS-NFS-Service Available
[ ] Servicios de certificados de Active Directory AD-Certificate Available
[ ] Entidad de certificación AD-Cert-Authority Available
[ ] Inscripción web de entidad de certificación AD-Cert-Web-Enrollment Available
[ ] Respondedor en línea AD-Cert-Online-Cert Available
[ ] Servicio de inscripción de dispositivos de red AD-Cert-Device-Enrollment Available
[ ] Servicio web de directiva de inscripción de ... AD-Cert-Enroll-Web-Pol Available
[ ] Servicio web de inscripción de certificados AD-Cert-Enroll-Web-Svc Available
[X] Servicios de dominio de Active Directory AD-Domain-Services Installed
[ ] Servicios de Escritorio remoto Remote-Desktop-Services Available
```

c. Comprobar la estructura del directorio

Get-ADForest

```
PS C:\Windows\system32> Get-ADForest

ApplicationPartitions : {DC=DomainDnsZones,DC=aulaSOR232,DC=com, DC=ForestDnsZones,DC=aulaSOR232,DC=com}
CrossForestReferences : {}
DomainNamingMaster    : WIN-ARE9EIEBN1A.aulaSOR232.com
Domains               : {aulaSOR232.com}
ForestMode            : Windows2016Forest
GlobalCatalogs       : {WIN-ARE9EIEBN1A.aulaSOR232.com}
Name                  : aulaSOR232.com
PartitionsContainer    : CN=Partitions,CN=Configuration,DC=aulaSOR232,DC=com
RootDomain            : aulaSOR232.com
SchemaMaster          : WIN-ARE9EIEBN1A.aulaSOR232.com
Sites                 : {Default-First-Site-Name}
SPNSuffixes           : {}
UPNSuffixes           : {}
```