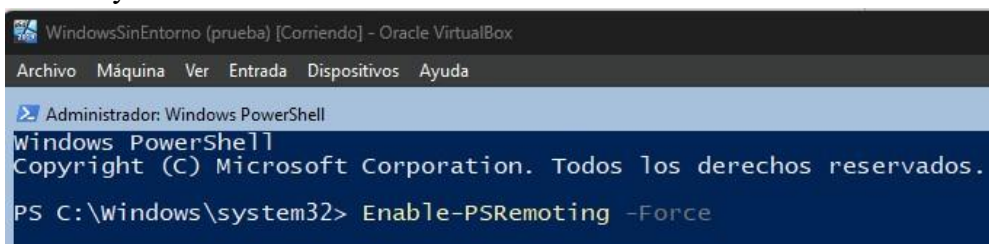


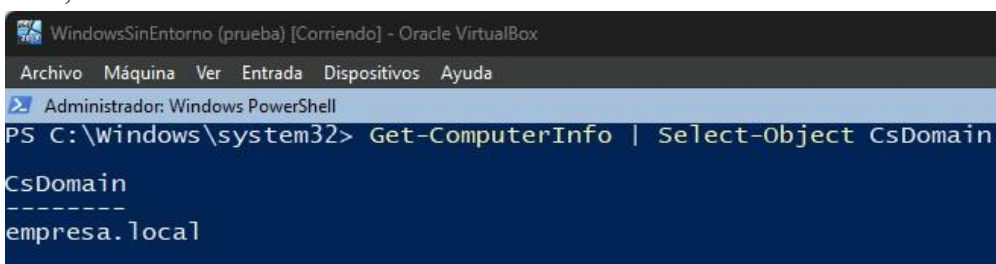
Seguridad y administración remota en Windows Server

1. Configuración de PowerShell Remoting seguro.

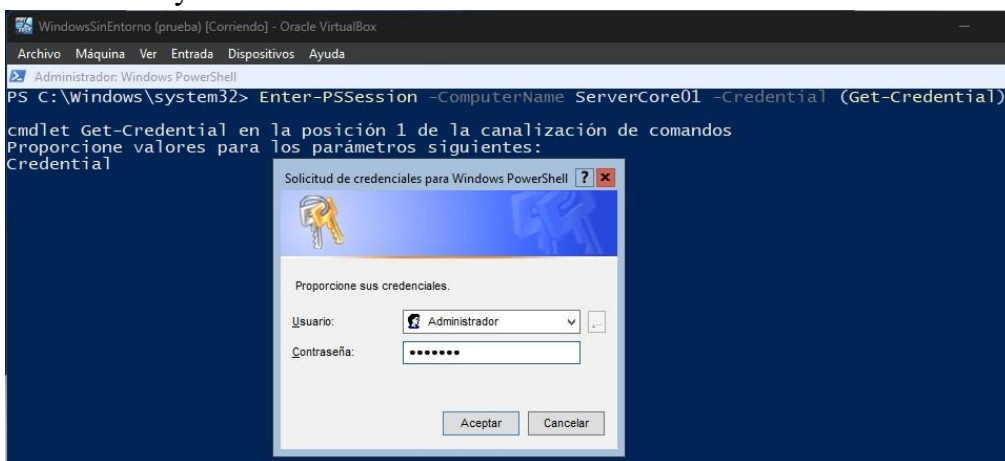
- Configurar PowerShell Remoting en un servidor Windows Server asegurando la autenticación mediante Kerberos o certificados.
- Primero debemos habilitar el Powershell Remoting con el siguiente comando y no nos debe dar error.



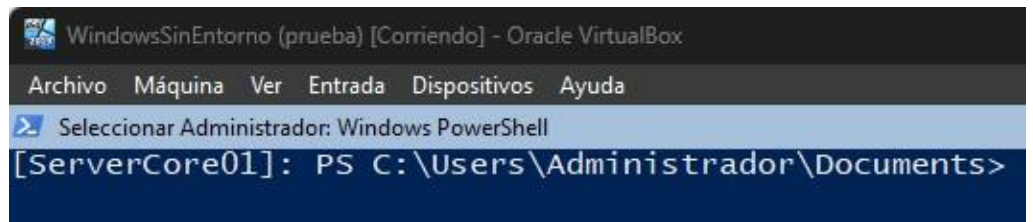
- Verificamos si el equipo está unido al dominio con el siguiente comando que está en la imagen, es caso de no estar unido debemos unirlo, en este caso está unido al dominio.



- Luego debemos asegurar la autenticación con kerberos con el siguiente comando que aparece en la imagen, de esta manera nos pedirá ingresar con el usuario y contraseña.



- y ahora debería salir la siguiente ruta después de autenticar con kerberos y probar la conexión remota.



- Restringir el acceso a usuarios específicos mediante políticas de seguridad.
- Para restringir acceso a usuarios específicos debemos crear un grupo de administración remota con los siguientes comandos
New-LocalGroup "RemotePowerShellUsers",
Add-LocalGroupMember -Group "RemotePowerShellUsers" -Member "empresa.local\empleado1".

```
PS C:\Windows\system32> New-LocalGroup "RemotePowerShellUsers"

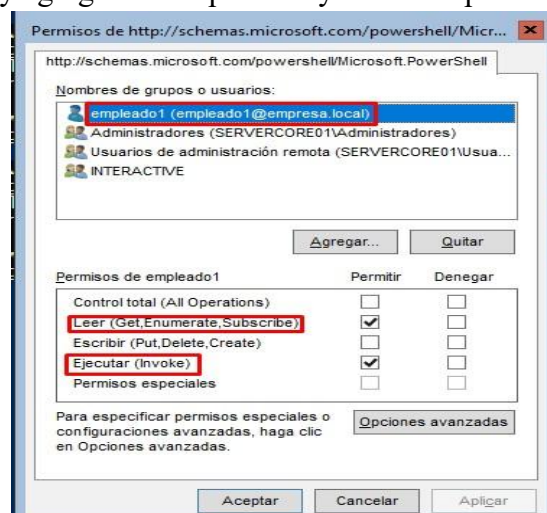
Name                Description
----                -
RemotePowerShellUsers
```

```
PS C:\> Add-LocalGroupMember -Group "RemotePowerShellUsers" -Member empresa.local\empleado1
```

- Ahora configuramos la sesión remota con el siguiente comando.

```
PS C:\> Set-PSSessionConfiguration -Name Microsoft.PowerShell -ShowSecurityDescriptorUI
ADVERTENCIA: Set-PSSessionConfiguration puede tener que reiniciar el servicio WinRM si se ha
registrado recientemente una configuración que use su nombre, aunque algunas estructuras de datos
del sistema pueden seguir almacenándose en caché. En ese caso, puede ser necesario reiniciar
WinRM.
Se desconectarán todas las sesiones de WinRM conectadas a configuraciones de sesión de Windows
PowerShell, como Microsoft.PowerShell y configuraciones de sesión creadas con el cmdlet
Register-PSSessionConfiguration.
```

- y agregamos empleado1 y le damos permiso de escritura y lectura



- Generar un script en PowerShell (.ps1) con los comandos utilizados y capturas de pantalla del resultado.
- el script estará en un archivo .ps1 dentro de un .zip

2. Implementación de seguridad en Server Core y Firewall.

- Configurar los servicios críticos (DHCP y DNS) en Server Core, asegurando su correcto funcionamiento y minimizando la superficie de ataque.
- instalamos los roles DHCP Y DNS en nuestro servidor core.

DHCP:

```
PS C:\> Install-WindowsFeature DHCP -IncludeManagementTools
```

Success	Restart Needed	Exit Code	Feature Result
True	No	NoChangeNeeded	{}

DNS:

```
PS C:\> Install-WindowsFeature DNS -IncludeManagementTools
```

Success	Restart Needed	Exit Code	Feature Result
True	No	Success	{Servidor DNS}

- Verificamos que estén instalados los dos roles.

```
PS C:\> Get-WindowsFeature DHCP,DNS
```

Display Name	Name	Install State
[X] Servidor DHCP	DHCP	Installed
[X] Servidor DNS	DNS	Installed

- Ahora configuramos el DHCP Scope básico con el siguiente comando de la imagen.

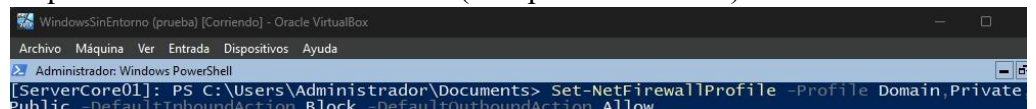
```
PS C:\> Add-DhcpServerv4Scope -Name "Scope_Empresa_Local" -StartRange 192.168.4.100 -EndRange 192.168.4.150 -SubnetMask 255.255.255.0
```

- Luego configuramos la zona DNS principal.

```
PS C:\> Add-DnsServerPrimaryZone -Name "empresa.local" -ZoneFile "empresa.local.dns"
```

- Implementar reglas de firewall para restringir accesos no autorizados mediante Windows Defender Firewall con políticas avanzadas.

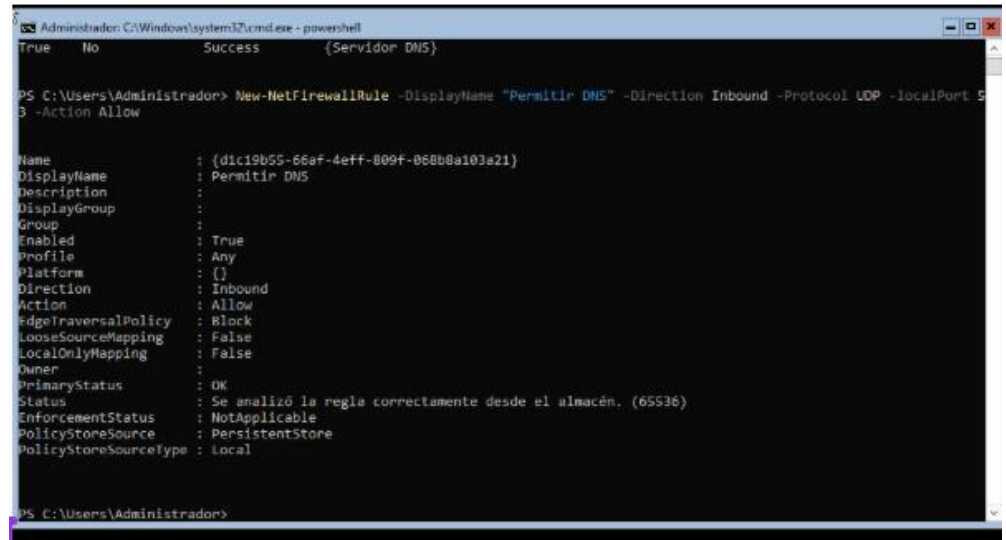
- Bloqueamos todo el tráfico entrante (excepto lo necesario).



```
WindowsSinEntorno (prueba) [Corriendo] - Oracle VirtualBox
Administrador: Windows PowerShell
[ServerCore01]: PS C:\Users\Administrador\Documents> Set-NetFirewallProfile -Profile Domain,Private
Public -DefaultInboundAction Block -DefaultOutboundAction Allow
```

- Permitimos DHCP Y DNS juntos con los siguientes comandos.

DNS UDP:



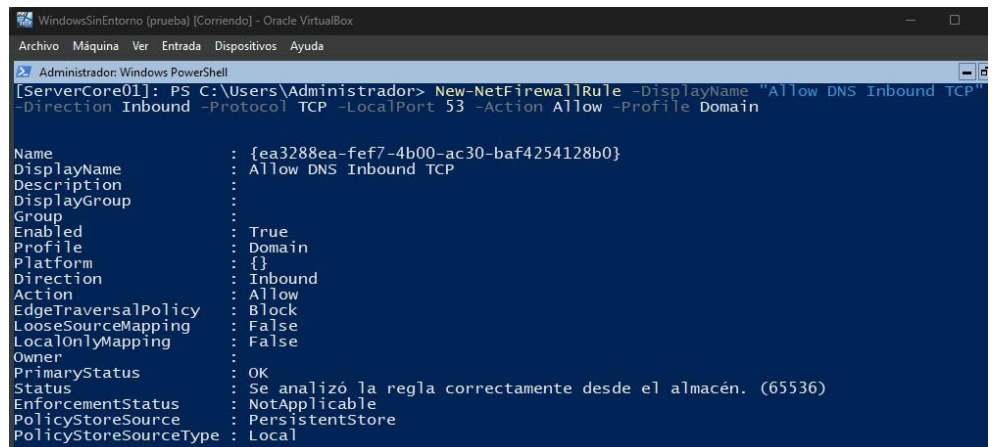
```
Administrator: C:\Windows\system32\cmd.exe - powershell
True No Success (Servidor DNS)

PS C:\Users\Administrador> New-NetFirewallRule -DisplayName "Permitir DNS" -Direction Inbound -Protocol UDP -localPort 53 -Action Allow

Name : {d1c19b55-66af-4eff-809f-068b8a103a21}
DisplayName : Permitir DNS
Description :
DisplayGroup :
Group :
Enabled : True
Profile : Any
Platform : {}
Direction : Inbound
Action : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping : False
Owner :
PrimaryStatus : OK
Status : Se analizó la regla correctamente desde el almacén. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local

PS C:\Users\Administrador>
```

DNS TCP:



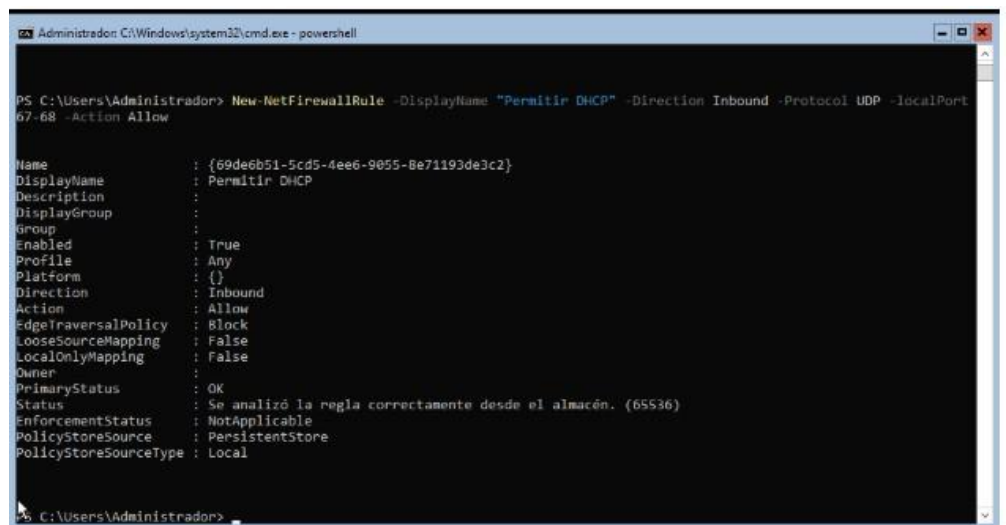
```
WindowsSinEntorno (prueba) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

Administrador: Windows PowerShell

[ServerCore01]: PS C:\Users\Administrador> New-NetFirewallRule -DisplayName "Allow DNS Inbound TCP" -Direction Inbound -Protocol TCP -LocalPort 53 -Action Allow -Profile Domain

Name : {ea3288ea-fef7-4b00-ac30-baf4254128b0}
DisplayName : Allow DNS Inbound TCP
Description :
DisplayGroup :
Group :
Enabled : True
Profile : Domain
Platform : {}
Direction : Inbound
Action : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping : False
Owner :
PrimaryStatus : OK
Status : Se analizó la regla correctamente desde el almacén. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local
```

DHCP:



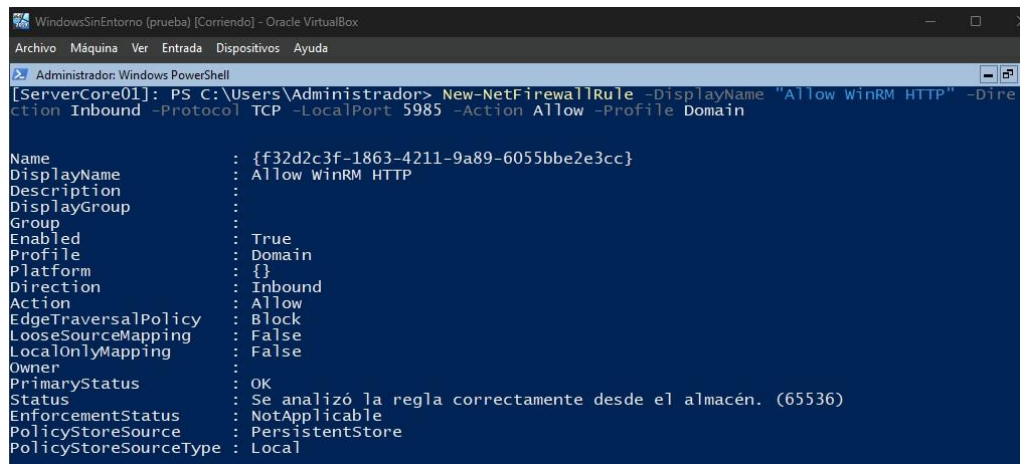
```
Administrator: C:\Windows\system32\cmd.exe - powershell

PS C:\Users\Administrador> New-NetFirewallRule -DisplayName "Permitir DHCP" -Direction Inbound -Protocol UDP -localPort 67-68 -Action Allow

Name : {69de6b51-5cd5-4ee6-9055-8e71193de3c2}
DisplayName : Permitir DHCP
Description :
DisplayGroup :
Group :
Enabled : True
Profile : Any
Platform : {}
Direction : Inbound
Action : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping : False
Owner :
PrimaryStatus : OK
Status : Se analizó la regla correctamente desde el almacén. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local

PS C:\Users\Administrador>
```

- Ahora Habilitamos sólo lo necesario para administración

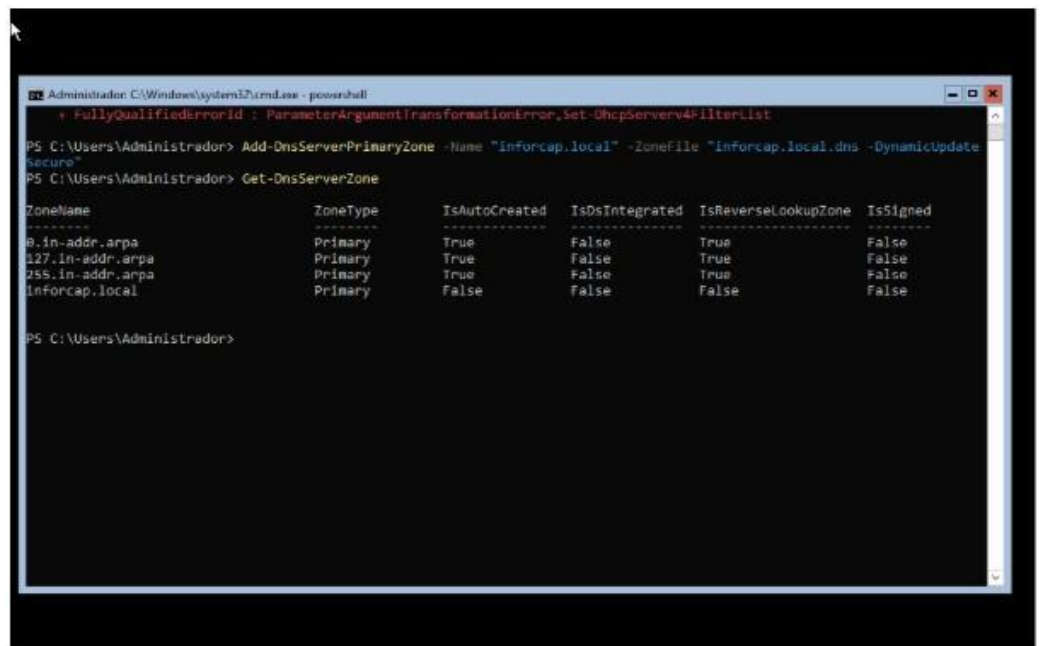


```
WindowsSinEntorno (prueba) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Administrador: Windows PowerShell
[ServerCore01]: PS C:\Users\Administrador> New-NetFirewallRule -DisplayName "Allow WinRM HTTP" -Direction Inbound -Protocol TCP -LocalPort 5985 -Action Allow -Profile Domain

Name                : {f32d2c3f-1863-4211-9a89-6055bbe2e3cc}
DisplayName          : Allow WinRM HTTP
Description          :
DisplayGroup         :
Group                :
Enabled              : True
Profile              : Domain
Platform             : {}
Direction            : Inbound
Action               : Allow
EdgeTraversalPolicy  : Block
LooseSourceMapping   : False
LocalOnlyMapping     : False
Owner                :
PrimaryStatus        : OK
Status               : Se analizó la regla correctamente desde el almacén. (65536)
EnforcementStatus    : NotApplicable
PolicyStoreSource    : PersistentStore
PolicyStoreSourceType : Local
```

3. Gestión segura de zonas DNS y asignación de IPs.

- Configurar y asegurar una zona DNS en Windows Server, limitando el acceso a la administración mediante permisos adecuados.
- Ahora debemos restringir la administración DNS dando permisos de zona de la siguiente manera.



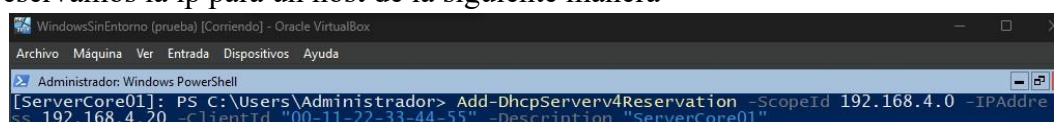
```
Administrator: C:\Windows\system32\cmd.exe - powershell
+ FullyQualifiedErrorId : ParameterArgumentTransformationError,Set-DhcpServerV4FilterList

PS C:\Users\Administrador> Add-DnsServerPrimaryZone -Name "inforcap.local" -ZoneFile "inforcap.local.dns" -DynamicUpdate "Secure"
PS C:\Users\Administrador> Get-DnsServerZone

ZoneName                ZoneType      IsAutoCreated  IsDnsIntegrated  IsReverseLookupZone  IsSigned
-----
0.in-addr.arpa          Primary       True           False            True                 False
127.in-addr.arpa        Primary       True           False            True                 False
255.in-addr.arpa        Primary       True           False            True                 False
inforcap.local           Primary       False          False            False                False

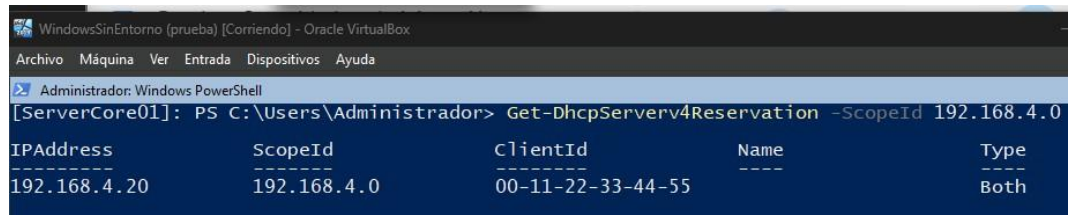
PS C:\Users\Administrador>
```

- Implementar una política de asignación de IPs estáticas y dinámicas utilizando DHCP de manera segura.
- reservamos la ip para un host de la siguiente manera



```
WindowsSinEntorno (prueba) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Administrador: Windows PowerShell
[ServerCore01]: PS C:\Users\Administrador> Add-DhcpServerV4Reservation -ScopeId 192.168.4.0 -IPAddress 192.168.4.20 -ClientId "00-11-22-33-44-55" -Description "ServerCore01"
```

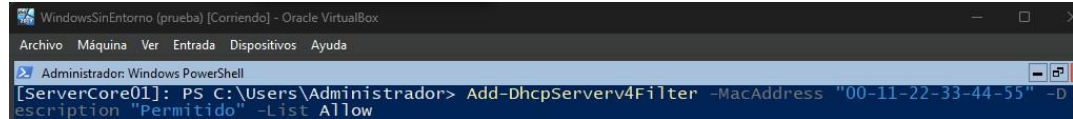
- verificamos con el siguiente comando si está reservado



```
WindowsSinEntorno (prueba) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Administrador: Windows PowerShell
[ServerCore01]: PS C:\Users\Administrador> Get-DhcpServerv4Reservation -ScopeId 192.168.4.0

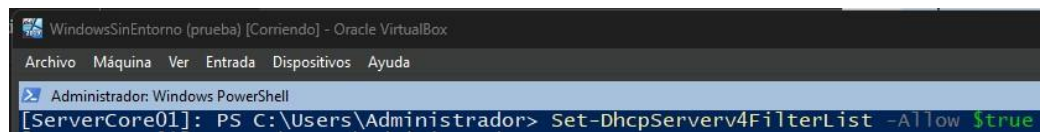
IPAddress          ScopeId            ClientId           Name              Type
-----
192.168.4.20       192.168.4.0       00-11-22-33-44-55 -----
Both
```

- Por último activamos el filtrado por mac con el siguiente comando



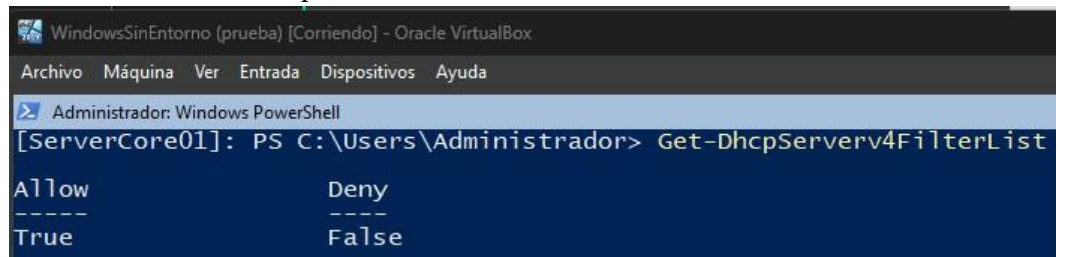
```
WindowsSinEntorno (prueba) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Administrador: Windows PowerShell
[ServerCore01]: PS C:\Users\Administrador> Add-DhcpServerv4Filter -MacAddress "00-11-22-33-44-55" -Description "Permitido" -List Allow
```

- activamos en true el -Allow



```
WindowsSinEntorno (prueba) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Administrador: Windows PowerShell
[ServerCore01]: PS C:\Users\Administrador> Set-DhcpServerv4FilterList -Allow $true
```

- por último verificamos que esté true



```
WindowsSinEntorno (prueba) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Administrador: Windows PowerShell
[ServerCore01]: PS C:\Users\Administrador> Get-DhcpServerv4FilterList

Allow          Deny
-----
True           False
```

Script

```
Enable-PSRemoting -Force

New-LocalGroup "RemotePowerShellUsers"
Add-LocalGroupMember -Group "RemotePowerShellUsers" -Member "empresa.local\empleado1"

Set-PSSessionConfiguration -Name Microsoft.PowerShell -ShowSecurityDescriptorUI
```