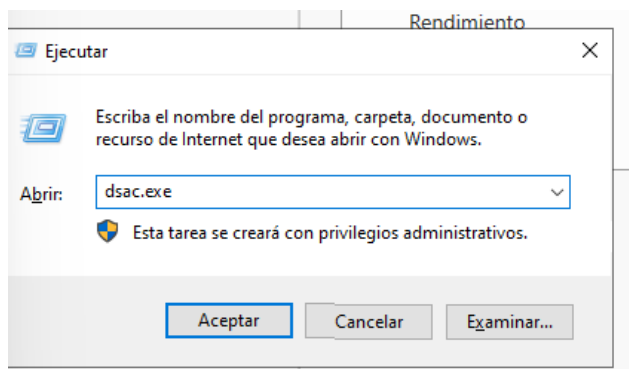


UD1-P01-ANEXO Ampliación (actividad opcional 1/4 punto)

Alejandro Almagro Torregrosa

1) Primera opcion, Active Directory Administration Center (ADAC):

Le daremos inicio + r y escribiremos lo siguiente:

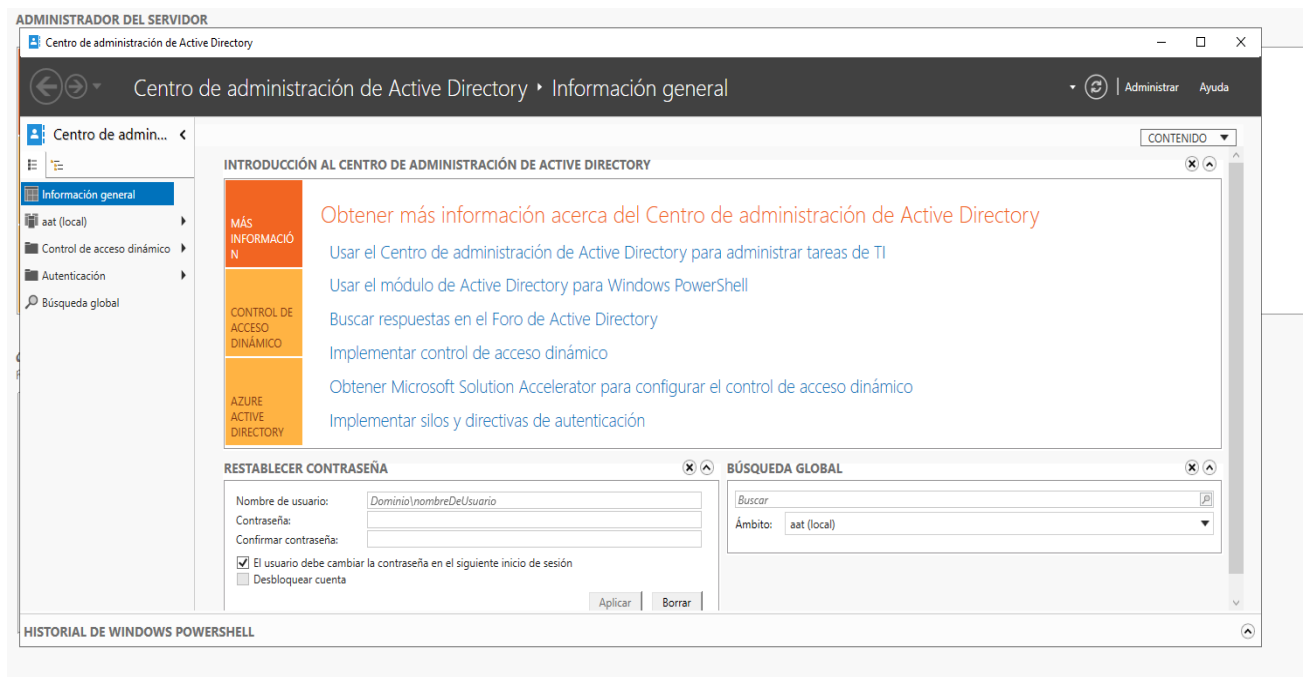


ores

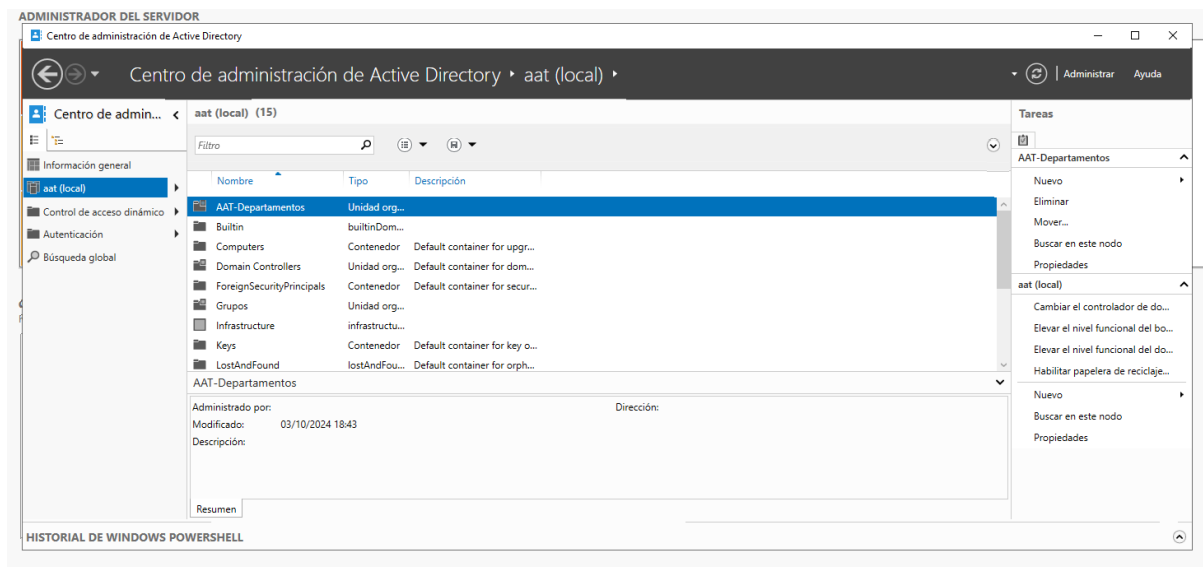
servic



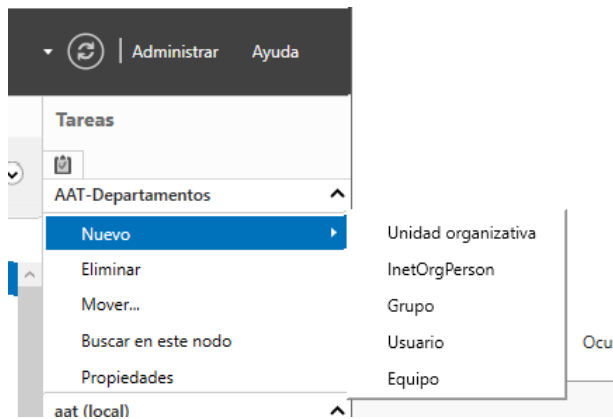
Se abra el siguiente pop-up:



Dandole al dominio se nos abre otro pop up, a la derecha veremos el menu entero para poder hacer cosas mucho mas comodas:



Al darle a nuevo veremos lo siguiente:



Todo mas sencillo y rapido que haciendolo de la manera tradicional, veamos el menu de todas las opciones:

Crear InetOrgPerson:

TAREAS SECCIONES

*** Cuenta**

Organización

Miembro de

Configuración de contraseña

Perfil

Directiva

Silo

Cuenta

Nombre:

Iniciales del s...

Apellidos:

Nombre co...

Inicio de sesi... @

Inicio de sesi... aat *

Contraseña:

Confirmar co...

Crear en: OU=AAT-Departamentos,DC=aat,DC=local [Cambiar...](#)

☐ Proteger contra eliminación accidental

[Horas de inicio de sesión...](#) [Iniciar sesión en...](#)

La cuenta exp ☒ Nunca ☐ Fin de

Opciones de contraseña:

☒ El usuario debe cambiar la contra...

☐ Otras opciones de contraseña

☐ Microsoft Passport o la tarjeta...

☐ La contraseña nunca expira

☐ El usuario no puede cambi...

Opciones de cifrado:

Otras opciones:

Organización

Nb para mostr...

Oficina:

Correo electr.:

Página web:

Puesto:

Departamento:

Compañía:

Administrador: [Editar...](#) [Borrar](#)

[Más información](#)

[Aceptar](#) [Cancelar](#)

Crear Grupo:

TAREAS SECCIONES

*** Grupo**

Administrado por

Miembro de

Miembros

Configuración de contraseña

Grupo

Nombre gru... *

Nomb. grup... *

Tipo de grupo: ☒ Seguridad ☐ Distribución

Ámbito de grupo: ☐ Dominio local ☒ Global ☐ Universal

☐ Proteger contra eliminación accidental

Correo electr.:

Crear en: OU=AAT-Departamentos,DC=aat,DC=local [Cambiar...](#)

Descripción:

Notas:

Administrado por

Administ. por: [Editar...](#) [Borrar](#)

☐ El administ. puede actualizar lista sus...

Números teléf.:

Principal:

Móvil:

Fax:

Oficina:

Dirección:

Ciudad Estado o p... Código po...

País o región:

Miembro de

[Más información](#)

[Aceptar](#) [Cancelar](#)

Crear Usuario: TAREAS SECCIONES

*** Cuenta**

Organización

Miembro de

Configuración de contraseña

Perfil

Directiva

Silo

Cuenta

Nombre:

Iniciales del s...

Apellidos:

Nombre co*

Inicio de sesi... @

Inicio de sesi... aat *

Contraseña:

Confirmar co...

Crear en: OU=AAT-Departamentos,DC=aat,DC=local [Cambiar...](#)

☐ Proteger contra eliminación accidental

La cuenta exp ☒ Nunca ☐ Fin de

Opciones de contraseña:

☒ El usuario debe cambiar la contra...

☐ Otras opciones de contraseña

☐ Microsoft Passport o la tarjeta...

☐ La contraseña nunca expira

☐ El usuario no puede cambi...

Opciones de cifrado:

Otras opciones:

Horas de inicio de sesión... Iniciar sesión en...

Organización

Nb para mostr...

Puesto:

Oficina:

Departamento:

Correo electr.:

Compañía:

Página web:

Administrador: [Editar...](#) [Borrar](#)

[Más información](#) [Aceptar](#) [Cancelar](#)

Crear Equipo: TAREAS SECCIONES

*** Equipo**

Administrado por

Miembro de

Directiva

Silo

Equipo

Nombre de equipo: *

Nombre (NetBIOS) de equ... *

Crear en: OU=AAT-Departamentos,DC=aat,DC=local [Cambiar...](#)

Usuario o grupo: Predeterminado: Admins. del dominio [Cambiar...](#)

El anterior usuario o grupo puede unir este equipo a un dominio

☐ Asignar la cuenta de este equipo como un equipo anterior a Windows 2000

☐ Proteger contra eliminación accidental

Administrado por

Administr. por: [Editar...](#) [Borrar](#) Oficina:

Números teléf.:

Principal:

Móvil:

Fax:

Dirección:

Calle

Ciudad Estado o pro... Código postal

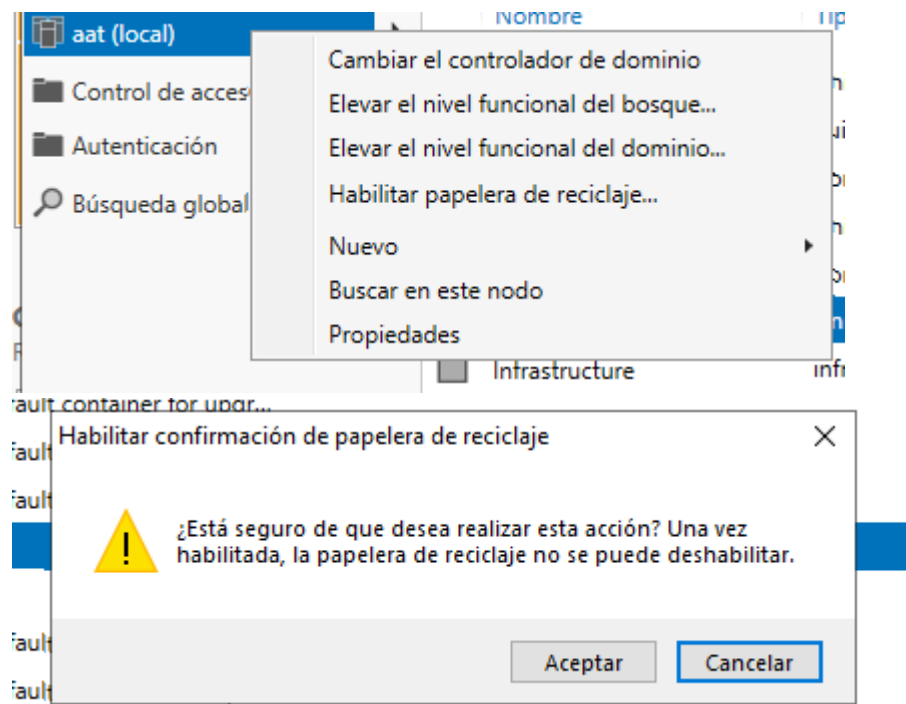
País o región:

Miembro de

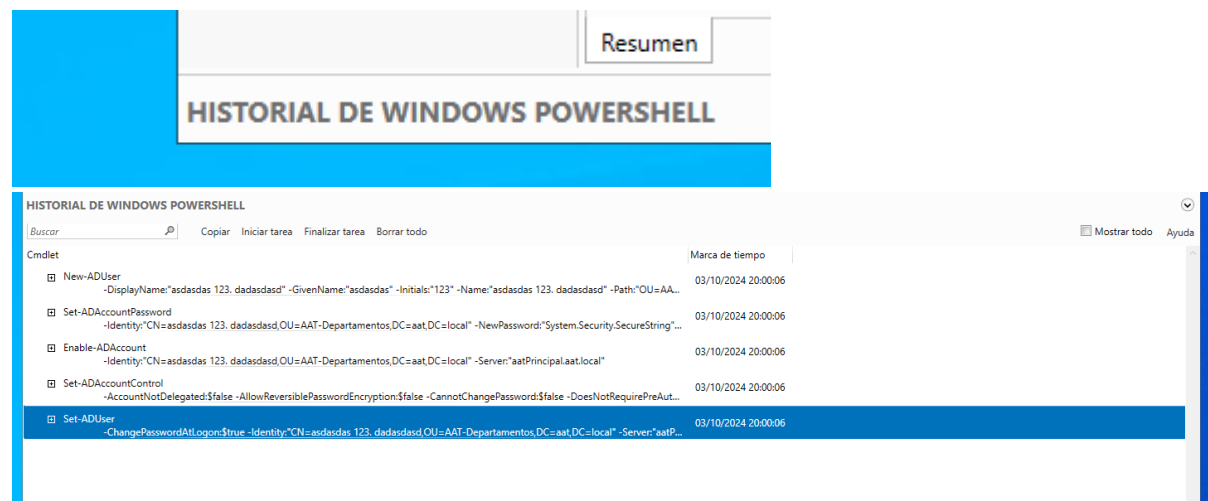
[Más información](#) [Aceptar](#) [Cancelar](#)

Como podemos observar todas las opciones son mas completas, intuitivas y comodas de completar en comparación al metodo tradicional.

-Habilitación de la papelera de reciclaje, lo cual nos permitira recuperar objetos que eliminemos del active directory(Click derecho en el dominio):

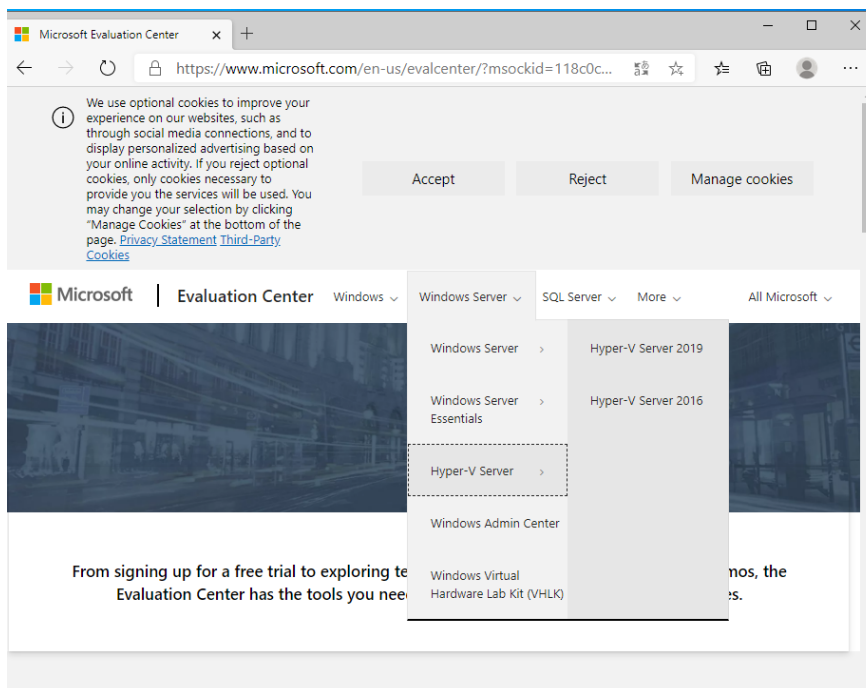
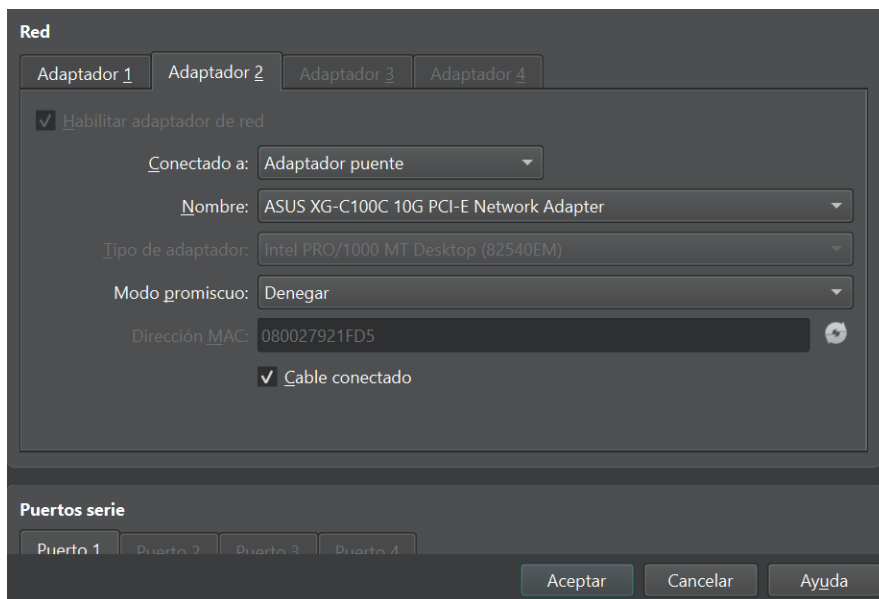


Ver el historial de la powershell(Hace falta crear usuarios o cosas para ver este historial):



2) Windows Admin Center:

Descargaremos esta herramienta desde el windows evaluation center, para esta opcion hemos puesto un adaptador puente a la maquina, para poder acceder a internet:



Windows Admin Center

[Get started for free](#) ▾

Aqui hay dos opciones para poder instalarlo:

1. Si quieres instalarlo en un controlador de dominio nos saltara un error, ya que supone estos problemas:
 - a. El instalador puede modificar nuestras opciones de seguridad (WinRM, Registros, etc.)
 - b. Deja un puerto abierto para conexión, en este caso el TCP 443 se comunica y en w10 utiliza el puerto 6516 por defecto
 - c. WAC siempre permite que se instale la primera conexión en la máquina. En este caso, es tu DC. Una vez que alguien puede acceder al portal, el atacante puede entrar fácilmente todo el sitio de Active Directory.

La solución al menos en la v1 es modificar el .msi que utilizamos para instalarlo con un programa externo.

Installed OR (MsiNTProductType <> 2) OR (INSTALLATION_TYPE ~= "AzureVmExtension")

Donde 2 significa que la condición de inicio es que no debe ejecutarse en un Windows NT tipo 2.

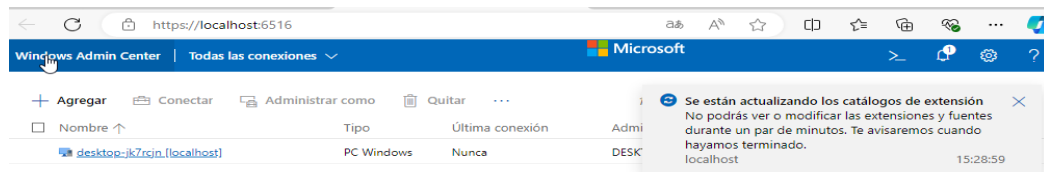
Siguiendo estas instrucciones modificamos la condición a :

Installed OR (MsiNTProductType >= 1) OR (INSTALLATION_TYPE ~= "AzureVmExtension")

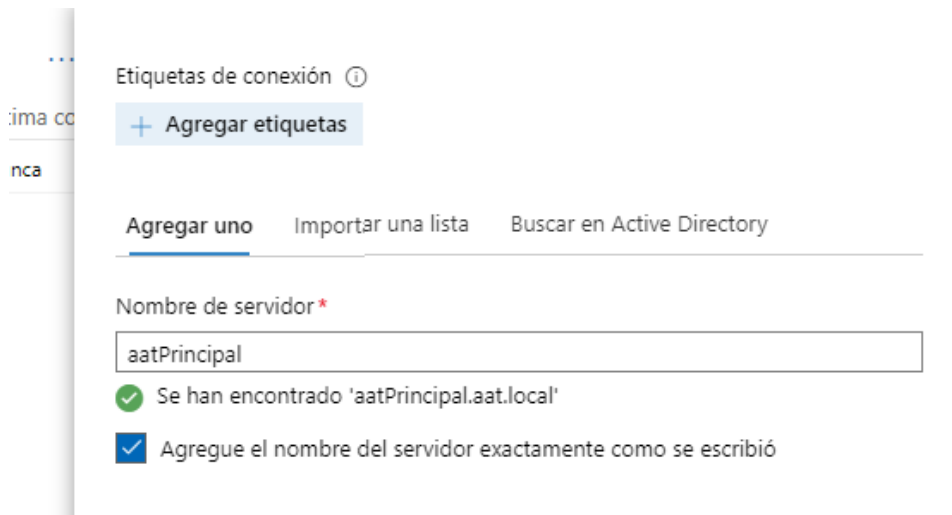
Se guarda el msi y se instala, hay otra manera con la Gateway actualizada pero por no hacer más largo este sistema que no he gastado dejo aquí el [enlace](#).

2. La otra opción es instalarlo en una máquina cliente nuestro caso el Windows 10 utilizado para la práctica siguiendo las mismas capturas de arriba.;

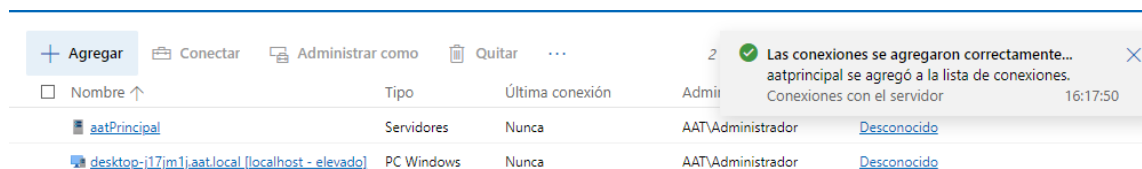
Cuando instalemos se abra una pestaña en el navegador



Ahora le daremos a agregar un servidor



Ahora una vez agregado, pincharemos en el dominio y se nos abra un nuevo menu con multiples opciones como muestro en la imagen:



Este menu apreciamos una cantidad de opciones y personalizaciones

Reiniciar

Apagar

Habilitar las métricas de disco

Editar el id. de equipo

Actualizar

Esenciales

Nombre del equipo	Dominio	Sistema operativo	Versión
aatprincipal	aatlocal	Microsoft Windows Server 2022 Standard	10.0.20348
Memoria instalada (RAM)	Espacio en disco (Libre/Total)	Procesadores	Fabricante
5.91 GB	36.38 GB / 49.34 GB	13th Gen Intel(R) Core(TM) i9-13900KF	innotek GmbH
Procesadores lógicos	NIC(s)	Periodo de uso	Usuarios conectados
4	2	00:00:49:21	1
Antivirus de Microsoft Defender	Modelo	Modo de lenguaje de PowerShell	Estado de Azure Backup
Protección en tiempo real: Activado	VirtualBox	Idioma completo Learn more c/	Sin protección
Estado de Azure Arc			
No instalado			

Supervisión

Alertas

CPU

Utilización 0.84%

Identificadores 50266

Velocidad 3GHz

Procesos 110

Memoria

Utilización 38.11%

Comprometido 2.3GB

Total 5.9GB

En uso 2.3GB

En caché 3.5GB

Bloque paginado 206.4MB

aatPrincipal

Buscar herramientas

Información general

Configuración

Herramientas

Actualizaciones

Almacenamiento

Aplicaciones instaladas

Archivos y uso compartido de archivos

Azure Backup

Azure File Sync

Azure Kubernetes Service

Azure Monitor

Centro híbrido de Azure

Certificados

Conmutadores virtuales

Dispositivos

Escritorio remoto

Eventos

Firewall

Grupos y usuarios locales

Información del sistema

Para poder acceder a crear usuarios y grupos necesitaremos agregar el rol de escritorio remoto a nuestro servidor y conectarnos desde el centro de administracion:

Ver progreso

SERVIDOR DE DESTINO
Implementación estándar seleccionada

Antes de comenzar

Tipo de instalación

Tipo de implementación

Escenario de implementa...

Servicios de rol

Agente de conexión a Esc...

Acceso web de RD

Host de virtualización de...

Confirmación

Finalización

Los servicios de rol Servicios de Escritorio remoto seleccionados se están instalando.

Servidor	Progreso	Estado
Servicio de rol Agente de conexión a Escritorio remoto		
aatPrincipal.aat.local	<div></div>	Pendiente
Servicio de rol Acceso web de RD		
aatPrincipal.aat.local	<div></div>	Pendiente
Servicio de rol Host de virtualización de Escritorio remoto		
aatPrincipal.aat.local	<div></div>	Pendiente

Configuración | Escritorio remoto

Configuración de búsquedas

- General
- Recursos compartidos de archivos (servidor de SMB)

Variables de entorno

Configuración de inicio/apagado

Diagnóstico y comentarios

Escritorio remoto

Azure Arc para servidores

Control de acceso basado en roles

Escritorio remoto

- Elige una opción y después indica quién se puede conectar.
- No permitir conexiones remotas a este equipo

Permitir conexiones remotas a este equipo

Permitir conexiones únicamente de equipos que ejecuten el escritorio remoto con Autenticación a nivel de red (recomendado)

Podemos utilizar la powersell en remoto y ver procesos tambien:

PowerShell - Administrador del s

https://localhost:6516/servermanager/connections/server/aatprincipal/tools/powershell

Windows Admin Center | Administrador del servidor

Microsoft

aatPrincipal

Buscar herramientas

Escritorio remoto

Eventos

Firewall

Grupos y usuarios locales

Información del sistema

Máquinas virtuales

Microsoft Defender for Cloud

Monitor de rendimiento

PowerShell

Procesos

Red extendida de Azure

Redes

Registro

Réplica de almacenamiento

Roles y características

Seguridad

Servicio de migración de almacenamiento

Servicios

Supervisión de paquetes

Tareas programadas

PowerShell

Desconectar

Conectando con aatprincipal, Usuario de inicio de sesión AAT\Administrador.

Iniciar proceso

Finalizar proceso

Crear volcado del proceso

Buscar identificadores

...

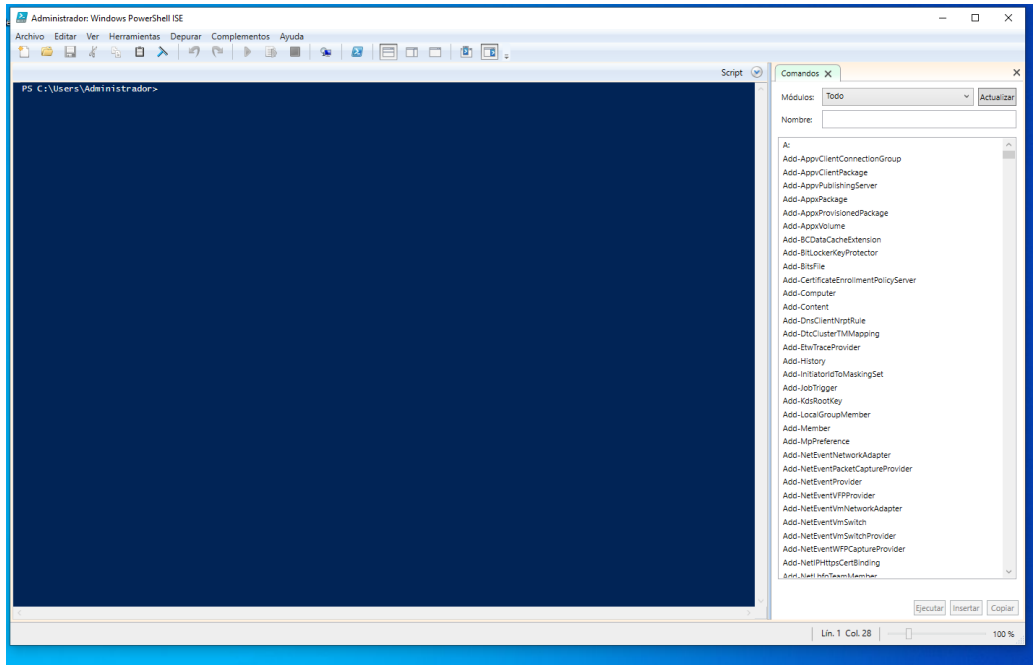
118 elementos

Buscar

Nombre	PID	Descripción	Estado	CPU	Nombre de usuario	Espacio de trabajo (memo...
Proceso inactivo del sistema	0	Porcentaje de tiempo de inactivi	En ejecución	41.2 %	SYSTEM	8 KB
Interrupciones del sistema	1	Llamadas a procedimiento diferit	En ejecución	0 %	SYSTEM	0 B
Sistema	4	Kernel y sistema NT	En ejecución	0 %	SYSTEM	148 KB
Registry	124	-	En ejecución	0 %	SYSTEM	70.65 MB
smss.exe	372	Administrador de sesión de Winc	En ejecución	0 %	SYSTEM	1.24 MB
svchost.exe	396	Proceso host para los servicios d	En ejecución	0 %	SERVICIO LOCAL	7.17 MB
svchost.exe	408	Proceso host para los servicios d	En ejecución	0 %	SYSTEM	10.51 MB
csrss.exe	476	Proceso en tiempo de ejecución	En ejecución	0 %	SYSTEM	6.21 MB
wininit.exe	564	Aplicación de inicio de Windows	En ejecución	0 %	SYSTEM	7.11 MB
csrss.exe	572	Proceso en tiempo de ejecución	En ejecución	0 %	SYSTEM	5.91 MB
winlogon.exe	636	Aplicación de inicio de sesión de	En ejecución	0 %	SYSTEM	11.09 MB
sqlservr.exe	680	SQL Server Windows NT - 64 Bit	En ejecución	0 %	MSSQLSMICROSOFT##WID	201.3 MB
services.exe	708	Aplicación de servicios y control	En ejecución	0 %	SYSTEM	15.2 MB
lsass.exe	728	Local Security Authority Process	En ejecución	0 %	SYSTEM	62.56 MB
svchost.exe	872	Proceso host para los servicios d	En ejecución	0 %	Servicio de red	15.04 MB
svchost.exe	936	Proceso host para los servicios d	En ejecución	0 %	SYSTEM	22.25 MB
svchost.exe	988	Proceso host para los servicios d	En ejecución	0 %	Servicio de red	11.24 MB
dwm.exe	1000	Administrador de ventanas del e	En ejecución	0 %	DWM-1	71.06 MB
StartMenuExperienceHost.exe	1032	-	En ejecución	0 %	Administrador	54.11 MB
svchost.exe	1036	Proceso host para los servicios d	En ejecución	0 %	SYSTEM	9.79 MB
svchost.exe	1108	Proceso host para los servicios d	En ejecución	0 %	SERVICIO LOCAL	7.11 MB
svchost.exe	1116	Proceso host para los servicios d	En ejecución	0 %	SERVICIO LOCAL	7.17 MB

3. PowerShell :

Aqui tenemos la opcion de windows powershell ise, lo cual nos abre una ventana que tiene un menu a la derecha, siempre iniciarlo como administrador:



Aqui podremos hacer uso de scripts para crear usuarios, grupos o unidades organizativas :

Script Usuario nuevo:

Import-Module ActiveDirectory

\$nombre = "Juan"

\$apellido = "Pérez"

\$nombreUsuario = "jperez"

\$contraseña = "P@ssword123!" # Asegúrate de cumplir los requisitos de contraseña

\$unidadOrganizativa = "OU=Usuarios,DC=midominio,DC=com" # Cambia por tu OU y dominio

New-ADUser `

-Name "\$nombre \$apellido" `

-GivenName \$nombre `

-Surname \$apellido `

-SamAccountName \$nombreUsuario `

-UserPrincipalName "\$nombreUsuario@midominio.com" `

```
-Path $UnidadOrganizativa `
-AccountPassword (ConvertTo-SecureString $contraseña -AsPlainText -Force)
`
-Enabled $true `
-ChangePasswordAtLogon $false
Write-Host "Usuario $nombreUsuario creado con éxito."
```

Script grupo:

```
Import-Module ActiveDirectory
$nombreGrupo = "GrupoMarketing" $descripcionGrupo = "Grupo de usuarios
del departamento de Marketing" $unidadOrganizativa =
"OU=Grupos,DC=midominio,DC=com"
New-ADGroup ` -Name $nombreGrupo ` -GroupScope Global ` -
GroupCategory Security ` -Path $unidadOrganizativa ` -Description
$descripcionGrupo
Write-Host "Grupo $nombreGrupo creado con éxito."
```

Crear una OU:

```
Import-Module ActiveDirectory
$nombreOU = "Marketing" $dominio = "DC=midominio,DC=com"
New-ADOrganizationalUnit ` -Name $nombreOU ` -Path $dominio
Write-Host "Unidad organizativa $nombreOU creada con éxito."
```

Todos estos scripts hay que guardarlos con un nombre en .ps1 y identificados como Unuevo.ps1, Gnuevo.ps1, OUnueva.ps1

Comandos basicos de powershell:

Otras opciones serian el monitoreo de recursos del servidor o status

Obtener uso de la CPU en tiempo real:

```
Get-WmiObject Win32_Processor | Select-Object -Property LoadPercentage
```

Ver los procesos que más consumen CPU:

```
Get-Process | Sort-Object CPU -Descending | Select-Object -First 10
```

Para ver cuánta memoria RAM está en uso y disponible:

```
Get-WmiObject Win32_OperatingSystem | Select-Object
TotalVisibleMemorySize,FreePhysicalMemory
```

Espacio en disco por volumen:

```
Get-PSDrive -PSProvider FileSystem | Select-Object Name, @{Name="Used  
(GB)";Expression="{0:N2}" -f ($_.Used/1GB)}}, @{Name="Free  
(GB)";Expression="{0:N2}" -f ($_.Free/1GB)}
```

Ver el uso de disco por archivo o carpeta:

```
Get-ChildItem "C:\RUTA\DE\LA\CARPETA" -Recurse | Measure-Object -Property  
Length -Sum
```

Puedes monitorear el uso de red utilizando el siguiente comando para ver los adaptadores de red y su información:

```
Get-NetAdapterStatistics
```

Para verificar si un servicio en específico está corriendo:

```
Get-Service -Name "NombreDelServicio"
```

Y para listar todos los servicios:

```
Get-Service
```

Puedes filtrar por procesos específicos, por ejemplo, para ver solo procesos de SQL Server:

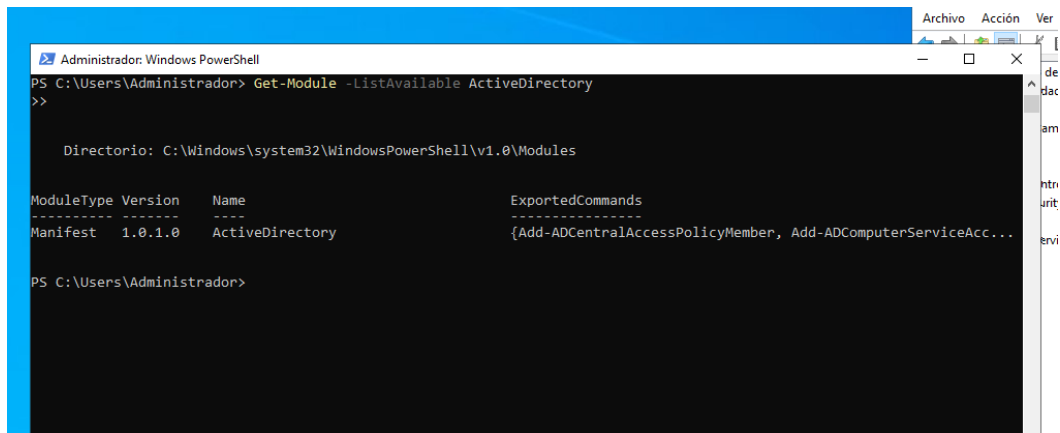
```
Get-Process -Name "*sql*"
```

4. Command-line tools (dsadd)

Habiendo instalado los roles y características deberíamos poder utilizarla desde la powershell con permisos de administrador sin problemas, pero sino seguiremos estos pasos:

```
Get-Module -ListAvailable ActiveDirectory
```

Si ves el módulo ActiveDirectory listado, significa que ya puedes utilizar los comandos relacionados con AD, incluyendo dsadd, sino instalamos:



```
Administrador: Windows PowerShell
PS C:\Users\Administrador> Get-Module -ListAvailable ActiveDirectory
>>

Directorio: C:\Windows\system32\WindowsPowerShell\v1.0\Modules

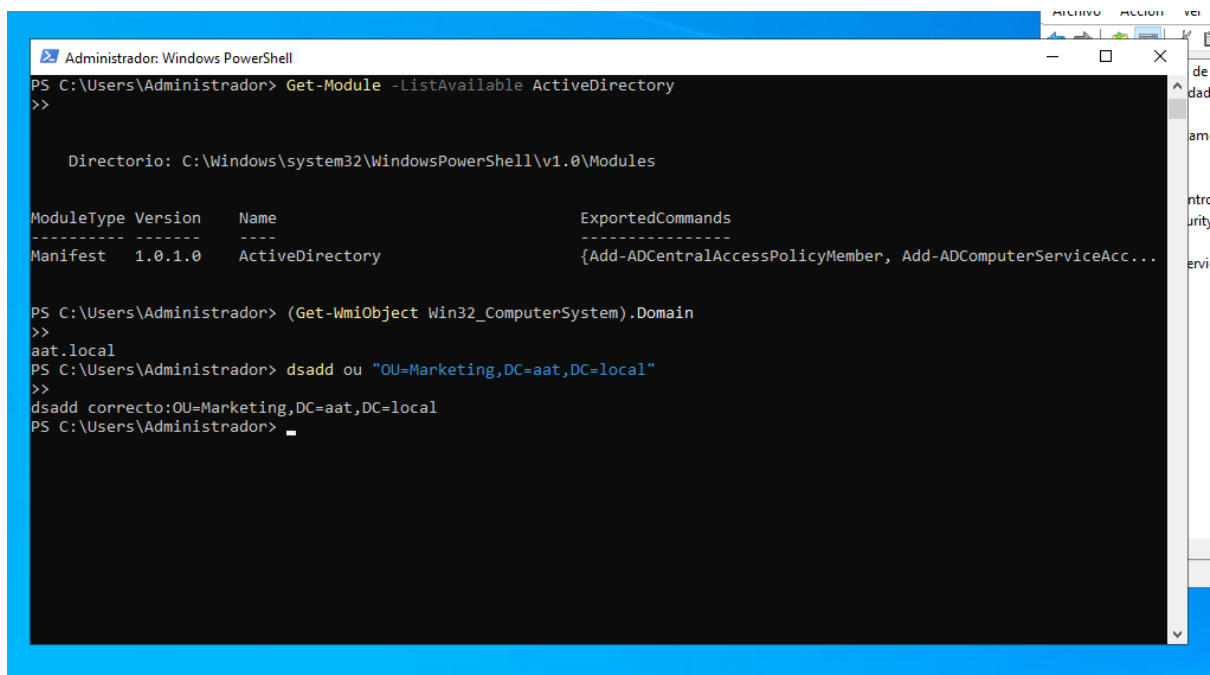
ModuleType Version      Name                               ExportedCommands
-----
Manifest 1.0.1.0 ActiveDirectory {Add-ADCentralAccessPolicyMember, Add-ADComputerServiceAcc...
```

Install-WindowsFeature -Name "RSAT-AD-Tools" -IncludeAllSubFeature

En nuestro caso lo tenemos instalado.

Para poner una OU:

dsadd ou "OU=Marketing,DC=aat,DC=local"



```
Administrador: Windows PowerShell
PS C:\Users\Administrador> Get-Module -ListAvailable ActiveDirectory
>>

Directorio: C:\Windows\system32\WindowsPowerShell\v1.0\Modules

ModuleType Version      Name                               ExportedCommands
-----
Manifest 1.0.1.0 ActiveDirectory {Add-ADCentralAccessPolicyMember, Add-ADComputerServiceAcc...

PS C:\Users\Administrador> (Get-WmiObject Win32_ComputerSystem).Domain
>>
aat.local
PS C:\Users\Administrador> dsadd ou "OU=Marketing,DC=aat,DC=local"
>>
dsadd correcto:OU=Marketing,DC=aat,DC=local
PS C:\Users\Administrador> _
```

Para agregar un grupo a esa ou:

dsadd group "CN=Técnicos,OU=Marketing,DC=aat,DC=local" -secgrp yes -scope g -desc "Grupo de técnicos de la OU Marketing"


```
dsadd correcto:OU=Marketing,DC=aat,DC=local
PS C:\Users\Administrador> dsadd group "CN=Técnicos,OU=Marketing,DC=aat,DC=local" -secgrp yes -scope g -desc "Grupo de t
écnicos de la OU Marketing"
>>
dsadd correcto:CN=Técnicos,OU=Marketing,DC=aat,DC=local
PS C:\Users\Administrador>
```

Crear un usuario:

dsadd user "CN=Juan Pérez,OU=Marketing,DC=aat,DC=local" -pwd P@ssword123

```
PS C:\Users\Administrador> dsadd user "CN=Juan Pérez,OU=Marketing,DC=aat,DC=local" -pwd P@ssword123
>>
dsadd correcto:CN=Juan Pérez,OU=Marketing,DC=aat,DC=local
PS C:\Users\Administrador>
```

Para agregar a Juan Pérez al grupo de técnico podemos recurrir al comando:

dsmod group "CN=Técnicos,OU=Marketing,DC=aat,DC=local" -addmbr "CN=Juan Pérez,OU=Usuarios,DC=aat,DC=local"

Pero no me funcionaba:

```
PS C:\Users\Administrador> dsmod group "CN=Técnicos,DC=aat,DC=local" -addmbr "CN=Juan Pérez,OU=Usuarios,DC=aat,DC=local"
dsmod incorrecto:CN=Técnicos,DC=aat,DC=local:No se encuentra el objeto de directorio.
Escriba dsmod /? para obtener ayuda.
PS C:\Users\Administrador>
```

En su defecto utilice:

Add-ADGroupMember -Identity "Técnicos" -Members "Juan Pérez"

Además podremos crear equipos, grupos de distribución o contactos:

dsadd computer "CN=Equipo1,OU=Marketing,DC=aat,DC=local"

```
PS C:\Users\Administrador> dsadd computer "CN=Equipo1,OU=Marketing,DC=aat,DC=local"
dsadd correcto:CN=Equipo1,OU=Marketing,DC=aat,DC=local
PS C:\Users\Administrador>
```

dsadd group "CN=GrupoDistribucion,OU=Marketing,DC=aat,DC=local" -secgrp no

```
PS C:\Users\Administrador> dsadd group "CN=GrupoDistribucion,OU=Marketing,DC=aat,DC=local" -secgrp no
dsadd correcto:CN=GrupoDistribucion,OU=Marketing,DC=aat,DC=local
PS C:\Users\Administrador>
```

dsadd contact "CN=Contacto1,OU=Marketing,DC=aat,DC=local" -email contacto@ejemplo.com

```
PS C:\Users\Administrador> dsadd contact "CN=Contacto1,OU=Marketing,DC=aat,DC=local" -email contacto@ejemplo.com
dsadd correcto:CN=Contacto1,OU=Marketing,DC=aat,DC=local
PS C:\Users\Administrador>
```

