



Practica Voluntaria

U5 Administración Remota

ASO

Tutor: Enrique Oscar

Alumno: Alejandro Almagro Torregrosa

Licencia CC BY-NC-SA 4.0



Atribución/Reconocimiento-NoComercial-CompartirIgual 4.0
Internacional

<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>

Usted es libre de:

- *Compartir* — copiar y redistribuir el material en cualquier medio o formato
- *Adaptar* — remezclar, transformar y construir a partir del material

La licenciante no puede revocar estas libertades en tanto usted siga los términos de la licencia

Bajo los siguientes términos:

- *Atribución* — Usted debe dar crédito de manera adecuada , brindar un enlace a la licencia, e indicar si se han realizado cambios . Puede hacerlo en cualquier forma razonable, pero no de forma tal que sugiera que usted o su uso tienen el apoyo de la licenciante.
- *NoComercial* — Usted no puede hacer uso del material con propósitos comerciales .
- *CompartirIgual* — Si remezcla, transforma o crea a partir del material, debe distribuir su contribución bajo la misma licencia del original.

No hay restricciones adicionales — No puede aplicar términos legales ni medidas tecnológicas que restrinjan legalmente a otras a hacer cualquier uso permitido por la licencia.



Sumario

1 Securizar ubuntu server por ssh y fail2ban

- 1.1. Preparación de entorno
- 1.2. Configuración de SSH
- 1.3. Verificación SSH
- 1.4. Instalación y configuración fail2ban
- 1.5. Verificación de fail2ban

2 Actualizaciones remotas en Windows Server 2022

2.1. Powershell

- 2.1.1. Configuración del servidor
- 2.1.2. Ejecución en el cliente

2.2. Instalación WSUS

- 2.2.1. Configuración WSUS para utilizar las gpo

2.3. Creación de configuración remota Mediante las GPO para WSUS

1. Securitizar Maquina Virtual Mediante SSH and Fail2ban

1.1. Preparación de entorno

Para esta practica utilizaremos un server ubuntu junto con un cliente en la misma red nat
aso.practica.



- Crearemos en el servidor un usuario nuevo llamado Manuel y pasaremos a configurar el puerto ssh.

```
root@aatsver:/home/aats# adduser manuel
```

1.2. Configuración SSH

- Configuraremos ahora el acceso por ssh para que se produzca por el puerto ssh, en el archivo `/etc/ssh/sshd_conf`:

```
Port 49512
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

```
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```



Ahora guardaremos el archivo y según la documentación de la pagina abra que modificar también el archivo:

GNU nano 7.2

/lib/systemd/system/ssh.socket *

Poniendo lo siguiente:

```
[Socket]
ListenStream=49512
Accept=no
FreeBind=yes
```

Una vez tenemos echo esto le daremos a guardar, y pasaremos a habilitar el servicio ssh.

```
ene 11 15:27:22 aatserver systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
ene 11 15:27:22 aatserver sshd[1002]: Server listening on :: port 49512.
ene 11 15:27:22 aatserver systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
root@aats# systemctl enable ssh.service
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service -> /usr/lib/systemd/system/ssh.service.
root@aats# systemctl status ssh.service
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
   Active: active (running) since Sat 2025-01-11 15:27:22 UTC; 22s ago
   TriggeredBy: ● ssh.socket
     Docs: man:sshd(8)
           man:sshd_config(5)
    Main PID: 1002 (sshd)
      Tasks: 1 (limit: 4556)
     Memory: 2.1M (peak: 2.2M)
        CPU: 14ms
     CGroup: /system.slice/ssh.service
            └─1002 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

ene 11 15:27:22 aatserver systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
ene 11 15:27:22 aatserver sshd[1002]: Server listening on :: port 49512.
ene 11 15:27:22 aatserver systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
```

1.3. Verificación SSH.

Ahora tenemos que verificar por parte del cliente que tenemos acceso desde el puerto 49512, en mi caso **tenia el ufw deshabilitado**, sino tendrías que crear esta regla:

```
root@aatusbuntu:/home/aats# ufw allow 49512/tcp
+Rules updated
Rules updated (v6)
```

Probaremos a conectarnos con un usuario, con el comando **ssh Manuel@ip -p (puerto):**

```
root@aats-VirtualBox:/home/aats# ssh manuel@192.168.1.13 -p 49512
manuel@192.168.1.13's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-51-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of sáb 11 ene 2025 09:13:38 UTC

System load:  0.0               Processes:    238
Usage of /:   83.4% of 11.21GB   Users logged in: 1
Memory usage: 23%              IPv4 address for enp0s3: 192.168.1.13
Swap usage:   0%
```

Vemos la comparación por el puerto 22, poniendo la contraseña correcta (no se ve)

```
root@aatc-VirtualBox:/home/aatc# sshmanuel@192.168.1.13 -p 22
The authenticity of host '192.168.1.13 (192.168.1.13)' can't be established.
ED25519 key fingerprint is SHA256:3edpuVouSZsrKl2pUedjW65id6IPNwt2t4KfcyLQZzE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.1.13' (ED25519) to the list of known hosts.
manuel@192.168.1.13's password:
Permission denied, please try again.
```

1.4. Configuración fail2ban

-Instalación mediante apt por ubuntu:

```
aats.ubuntuuser [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
root@aatserver:/home/aats# apt install fail2ban
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
fail2ban ya está en su versión más reciente (1.0.2-3ubuntu0.1).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 2 no actualizados.
root@aatserver:/home/aats#
```

Ahora procederemos a configurar el archivo jail.conf o si queremos hacer una copia jail.local;

```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
root@aatserver:/home/aats# cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

- Con nano procedemos a editarlo para configurar las opciones que nos muestra el tutorial:

```
[[sshd]
# To use more aggressive sshd modes set filter parameter "mode" in jail.local:
# normal (default), ddos, extra or aggressive (combines all).
# See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and details.
#mode = normal
port = 49152
logpath = %(sshd_log)s
backend = %(sshd_backend)s
filter = sshd
maxretry = 3
findtime = 1m
bantime = 2m
```

Ahora haremos un restart y status para ver que todo cargo correctamente, si es necesaria hacer un enable tambien:

```
root@aatsserver:/home/aats# systemctl restart fail2ban
root@aatsserver:/home/aats# systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
   Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
   Active: active (running) since Sat 2025-01-11 15:38:11 UTC; 4s ago
     Docs: man:fail2ban(1)
  Main PID: 1239 (fail2ban-server)
    Tasks: 5 (limit: 4556)
   Memory: 18.7M (peak: 19.0M)
      CPU: 88ms
   CGroup: /system.slice/fail2ban.service
           └─1239 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

ene 11 15:38:11 aatsserver systemd[1]: Started fail2ban.service - Fail2Ban Service.
ene 11 15:38:11 aatsserver fail2ban-server[1239]: 2025-01-11 15:38:11,746 fail2ban.configreader [1239]: WARNING 'allowipv6' not defined in 'Definition'. Using
ene 11 15:38:11 aatsserver fail2ban-server[1239]: Server ready
lines 1-14/14 (END)
```

Con esto tendríamos configurado ahora el acceso por ssh con las restricciones aplicadas en fail2ban.

1.5. Verificacion fail2ban

Iremos a la maquina cliente y fallaremos aposta el login 3 veces:

```
root@aatac-VirtualBox:/home/aatac# ssh 192.168.1.14 -l manuel -p 49512
manuel@192.168.1.14's password:
Permission denied, please try again.
manuel@192.168.1.14's password:
Permission denied, please try again.
manuel@192.168.1.14's password:
manuel@192.168.1.14: Permission denied (publickey,password).
root@aatac-VirtualBox:/home/aatac#
```

Observaremos que después de 3 veces me ha devuelto a la cli, sin permitirme mas intentos.

Ahora nos conectaremos con el comando anterior:

```
Connection to 192.168.1.14 closed.
root@aatac-VirtualBox:/home/aatac# ssh manuel@192.168.1.14 -p 49512
ssh: connect to host 192.168.1.14 port 49512: Connection refused
root@aatac-VirtualBox:/home/aatac#
```

No nos deja conectar, ni nos pide ninguna password

Comprobación ahora de los logs del servidor.

Haremos un `cat /var/log/fail2ban.log`:

```
2025-01-11 10:02:41,496 fail2ban.filterssystemd [12098]: INFO [sshd] Jail is in operation now (process new journal entries)
2025-01-11 10:02:41,496 fail2ban.jail [12098]: INFO Jail 'sshd' started
2025-01-11 10:03:49,182 fail2ban.filter [12098]: INFO [sshd] Found 192.168.1.11 - 2025-01-11 10:03:48
2025-01-11 10:04:00,174 fail2ban.filter [12098]: INFO [sshd] Found 192.168.1.11 - 2025-01-11 10:03:59
2025-01-11 10:04:03,343 fail2ban.filter [12098]: INFO [sshd] Found 192.168.1.11 - 2025-01-11 10:04:03
2025-01-11 10:04:03,550 fail2ban.actions [12098]: NOTICE [sshd] Ban 192.168.1.11
2025-01-11 10:06:04,631 fail2ban.filter [12098]: INFO [sshd] Found 192.168.1.11 - 2025-01-11 10:06:04
2025-01-11 10:06:37,998 fail2ban.filter [12098]: INFO [sshd] Found 192.168.1.11 - 2025-01-11 10:06:37
2025-01-11 10:07:01,424 fail2ban.filter [12098]: INFO [sshd] Found 192.168.1.11 - 2025-01-11 10:07:00
2025-01-11 10:07:01,800 fail2ban.actions [12098]: WARNING [sshd] 192.168.1.11 already banned
root@aatsserver:/home/aats#
```

Como vemos en los ban al poner un tiempo tan pequeño, **tenemos que ser rápidos al logear otra vez para que nos salte el ultimo log**, que nos indican el warning de un usuario baneado se intenta conectar

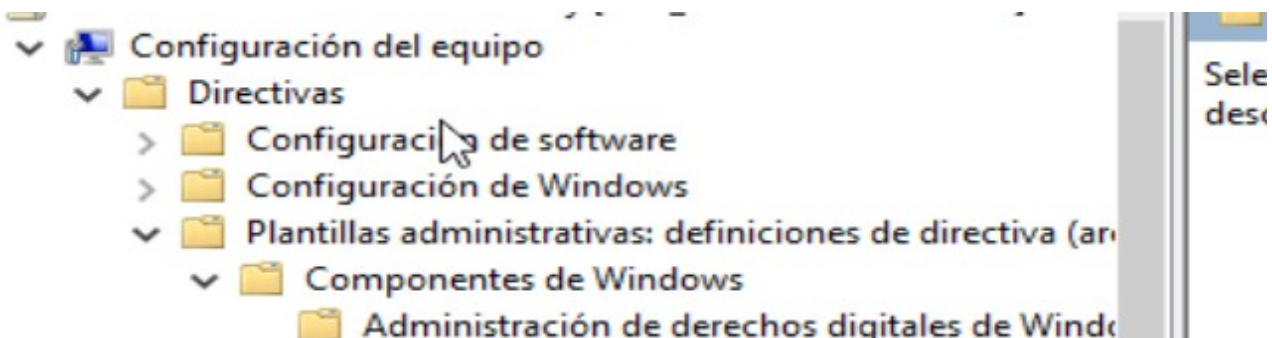
Por lo demás como vemos acepta las conexiones con password erróneas hasta que banea después de los 3 intentos y el inicio del jail.

2. Actualización remota del sistema en Windows Server 2022

2.1. Actualización mediante Powershell

2.1.1. Configuración del Server

Nos aseguramos que en el servidor esta autorizado la ejecución de scripts por gpo:

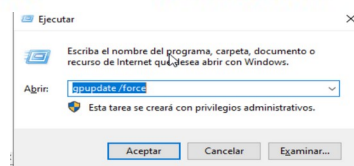


En componentes de windows buscaremos abajo del todo, windows Powershell:

Activar el registro de bloque de script de PowerShell	No configurada	NO
Activar la ejecución de scripts	Habilitada	No
Activar la transcripción de PowerShell	No configurada	No
Establecer la ruta de acceso de origen de Update-Help	No configurada	No

Forzaremos la actualización de directivas:

2.1.2. Ejecución en el cliente





Como configuramos en la practica anterior la Powershell remota ahora nos conectaremos desde el cliente, con el siguiente comando:

```
PS C:\Users\Administrador> Enter-PSSession -ComputerName aat_aso -Credential Administrador  
[aat_aso]: PS C:\Users\Administrador\Documents>
```

Ahora ejecutaremos el comando y instalaremos lo necesario dándole a Si el siguiente modulo:

```
[aat_aso]: PS C:\Users\Administrador\Documents> Install-Module PSWindowsUpdate  
  
Se necesita el proveedor de NuGet para continuar  
PowerShellGet necesita la versión del proveedor de NuGet '2.8.5.201' o posterior para interactuar con repositorios  
basados en NuGet. El proveedor de NuGet debe estar disponible en 'C:\Program  
Files\PackageManagement\ProviderAssemblies' o  
'C:\Users\Administrador\AppData\Local\PackageManagement\ProviderAssemblies'. También puedes instalar el proveedor de  
NuGet ejecutando 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. ¿Quieres que PowerShellGet se  
instale e importe el proveedor de NuGet ahora?  
[S] Sí [N] No [?] Ayuda (el valor predeterminado es "S"): S  
  
Repositorio que no es de confianza  
Estás instalando los módulos desde un repositorio que no es de confianza. Si confías en este repositorio, cambia su  
valor InstallationPolicy ejecutando el cmdlet Set-PSRepository. ¿Estás seguro de que quieres instalar los módulos de  
'PSGallery'?  
[S] Sí [O] Sí a todo [N] No [T] No a todo [?] Ayuda (el valor predeterminado es "N"): S  
[aat_aso]: PS C:\Users\Administrador\Documents>
```

Utilizaremos el comando ahora **Get-WindowsUpdate**:

```
[aat_aso]: PS C:\Users\Administrador\Documents> Get-WindowsUpdate  
  
ComputerName Status KB Size Title  
-----  
AAT_ASO -D----- KB5048654 25GB 2024-12 Actualización acumulativa para Microsoft server operating system ve...  
  
[aat_aso]: PS C:\Users\Administrador\Documents>
```

Lo siguiente, sería **ejecutar un Install**, la actualización me consume el 75% del espacio de la maquina asique no la actualizaré, pero solo faltaría darle a Si enter y se instalara



```
PS C:\Users\Administrador> Enter-PSSession -ComputerName aat_aso -Credential Administrador
[aat_aso]: PS C:\Users\Administrador\Documents> Install-Module PSWindowsUpdate
[aat_aso]: PS C:\Users\Administrador\Documents> Get-WindowsUpdate

ComputerName Status      KB          Size Title
-----
AAT_ASO      -D----- KB5048654    25GB 2024-12 Actualización acumulativa para Microsoft server operating system ve...

[aat_aso]: PS C:\Users\Administrador\Documents> Install-WindowsUpdate

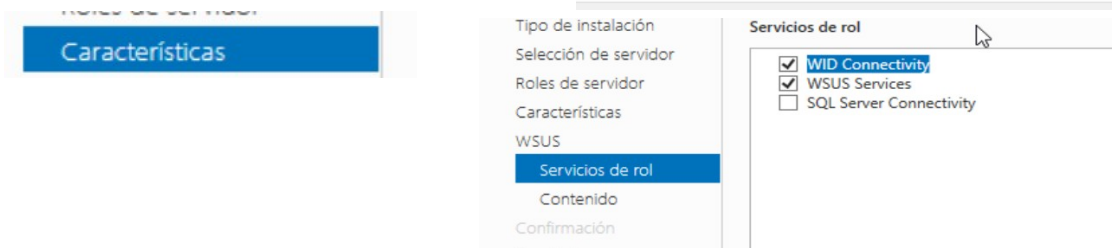
Confirmar
¿Está seguro de que desea realizar esta acción?
Se está realizando la operación "(11/01/2025 13:12:32) 2024-12 Actualización acumulativa para Microsoft server operating system version 21H2 para sistemas basados enx64(KB5048654)[25GB]" en el destino "AAT_ASO".
[S] Sí [O] Sí a todo [N] No [T] No a todo [?] Ayuda (el valor predeterminado es "S"): s
```

2.2. Instalación de WSUS

En el servidor agregaremos una característica y un rol como hicimos previamente con el dominio o dns:



Seguiremos el instalador:



Configuraremos el directorio para el contenido:

Servicios de rol

Contenido

Confirmación

Resultados

para todos los idiomas.

☒ Almacenar actualizaciones en la siguiente ubicación (elegir una ruta de acceso local válida en aat_aso.aso.practica, o una ruta de acceso remota):

CAWSUS

Procederemos a instalar:

Asistente para agregar roles y características

CONFIRMAR SELECCIONES DE INSTALACIÓN

SERVIDOR DE DESTINO
aat_aso.aso.practica

Antes de comenzar

Tipo de instalación

Selección de servidor

Roles de servidor

Características

WSUS

Servicios de rol

Contenido

Confirmación

Resultados

Para instalar los siguientes roles, servicios de rol o características en el servidor seleccionado, haga clic en Instalar.

☐ Reiniciar automáticamente el servidor de destino en caso necesario

En esta página se pueden mostrar características opcionales (como herramientas de administración) porque se seleccionaron automáticamente. Si no desea instalar estas características opcionales, haga clic en Anterior para desactivar las casillas.

.NET Framework 4.8 Features

Servicios WCF

Activación HTTP

Herramientas de administración remota del servidor

Herramientas de administración de roles

Herramientas de Windows Server Update Services

API y cmdlets de PowerShell

Interfaz de usuario de la Consola de administración

Servicio WAS (Windows Process Activation Service)

Exportar opciones de configuración

Especifique una ruta de acceso de origen alternativa

< Anterior

Siguiente >

Instalar

Cancelar

Iniciar tareas posteriores a la instalación:

Configuración posterior a la...

TAREAS

Requiere configuración para Windows Server Update Services en AAT_ASO

Iniciar tareas posteriores a la instalación

Verificamos su instalación:

WSUS 1

Estado

Eventos

Servicios

Rendimiento

Resultados de BPA

En el menú de herramientas, abajo del todo:

Windows Defender Firewall con seguridad avanzada

Windows PowerShell

Windows PowerShell (x86)

Windows Server Update Services

Ahora nos aparecerá un pop-up con un menú:

Asistente para la configuración

Antes de comenzar

Cosas que del

Antes de comenzar

Programa de mejora de Microsoft Update

Elegir servidor que precede en la cadena

Especificar servidor proxy

Elegir idiomas

Elegir productos

Elegir clasificaciones

Configurar programación de sincronización

Finalizado

Siguiente paso

Quitamos el tic de programa de mejora:

☐ Sí, me gustaría participar en el programa de mejora de Microsoft Update

Elegimos de donde viene el servidor:

Puede elegir el servidor que precede en la cadena desde el que su servidor sincroniza las actualizaciones.

☒ Sincronizar desde Microsoft Update

☐ Sincronizar desde otro servidor de Windows Server Update Services

Nombre de servidor:

Número de puerto: 8530

Dejamos el proxy en blanco, ya que no tenemos. Ahora probamos la conectividad:

Haga clic en Iniciar conexión para guardar y descargar la información del servidor que precede en la cadena y del servidor proxy. Este proceso puede durar varios minutos, dependiendo de la velocidad de conexión.

Iniciar conexión

Detener conexión

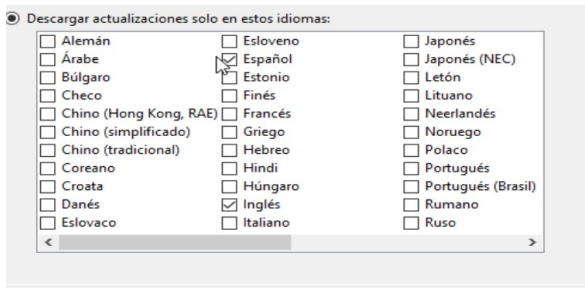
< Atrás

Siguiente >

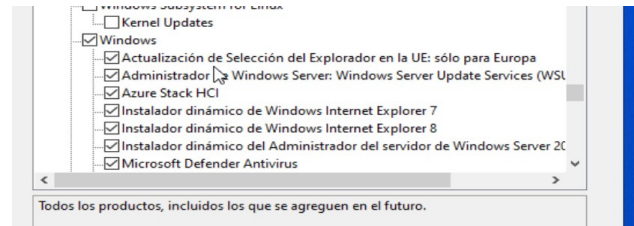
Finalizar

Cancelar

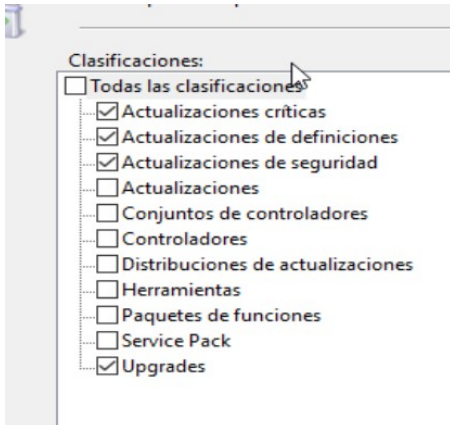
Una vez acabe elegiremos los idiomas:



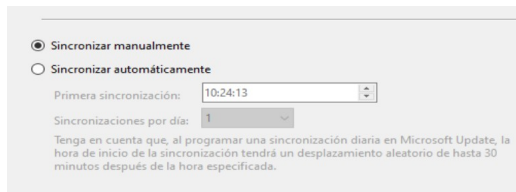
Siguiente paso, que productos queremos, solo los de windows SO en nuestro caso:



Que tipo de actualizaciones queríamos:



Como sincronizamos:

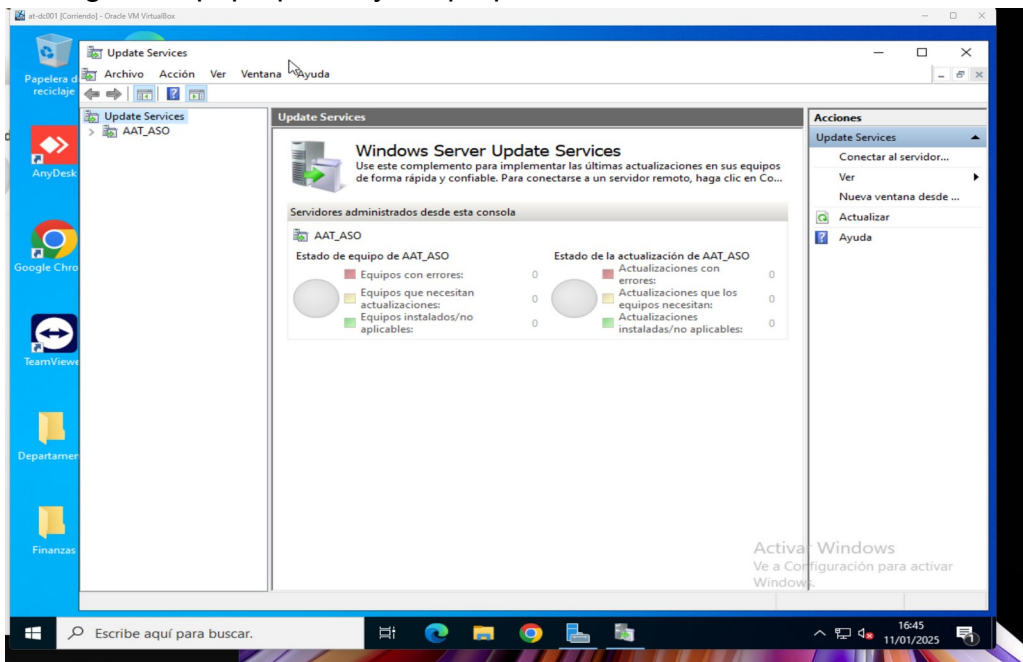


Iniciaremos ahora la sincronización

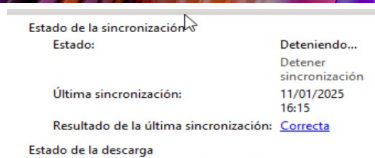


2.2. Configuración de WSUS para utilizar GPO

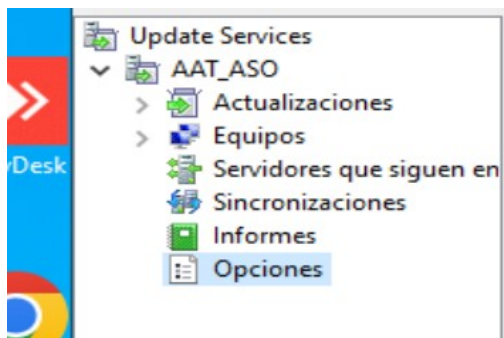
El siguiente pop-up sera ya el propio WSUS:



Detendremos en aat_aso la sincronización para aplicar la gpo:



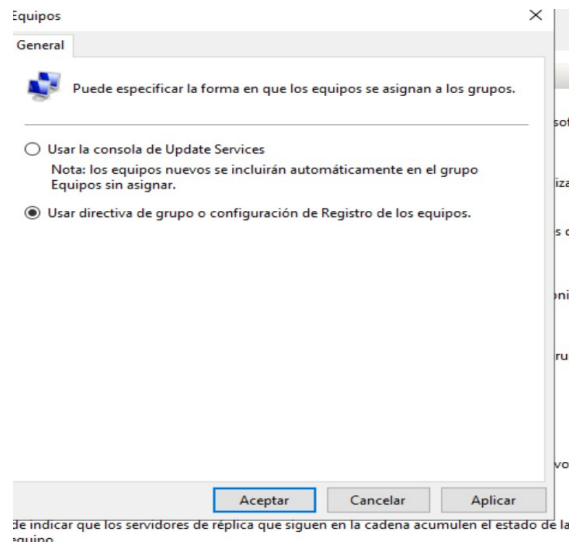
En opciones seleccionaremos:



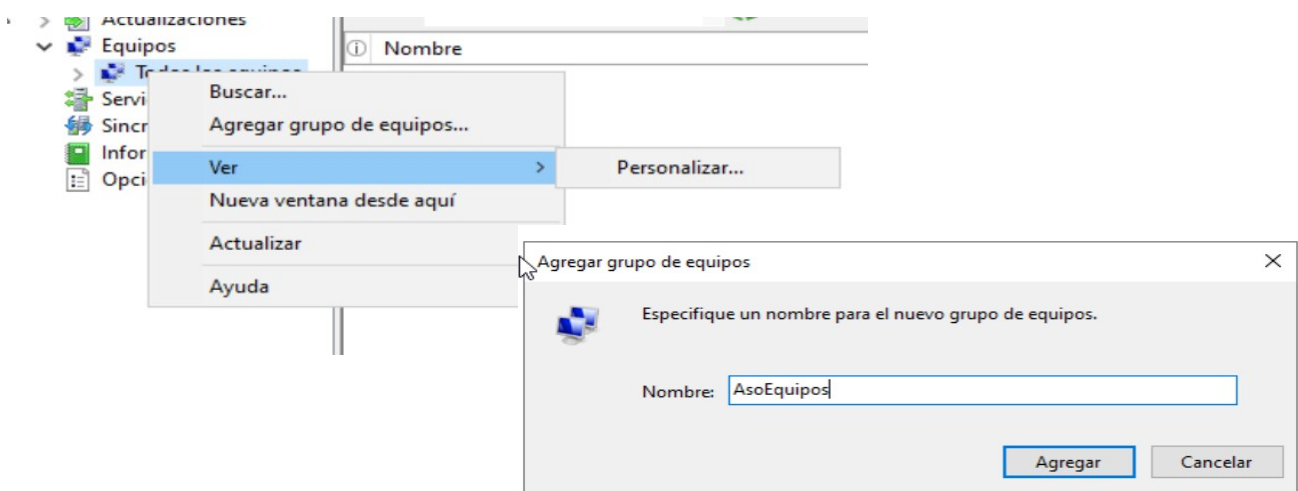
Equipos

Puede especificar la forma en que los equipos se asignan a los grupos.

Pincharemos y aplicaremos la siguiente opción:

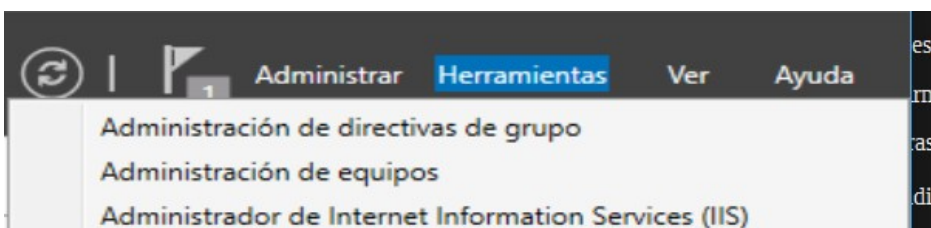


Crearemos el grupo de equipos que utilizaremos para WSUS:

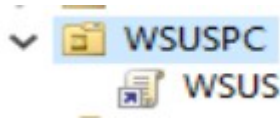


2.3. Configuración de la GPO remota para WSUS

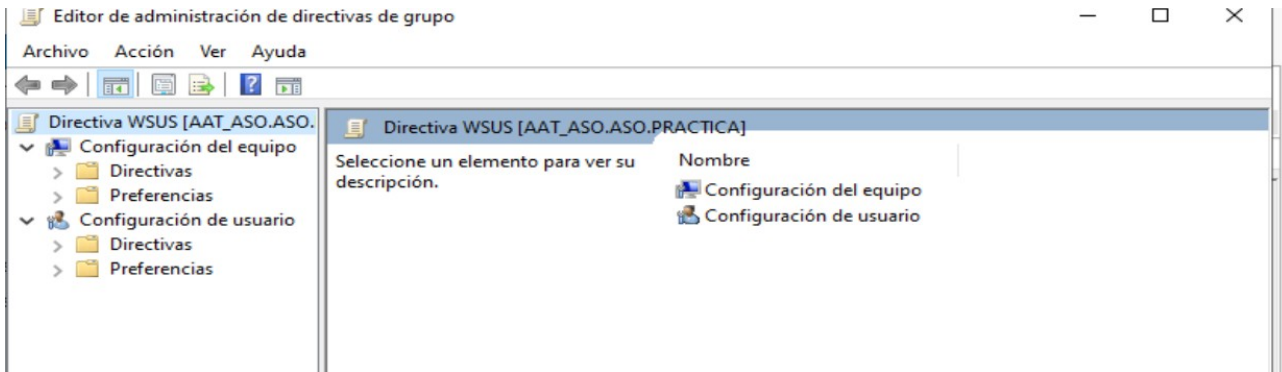
Iremos como siempre a herramientas y administración de GPO:



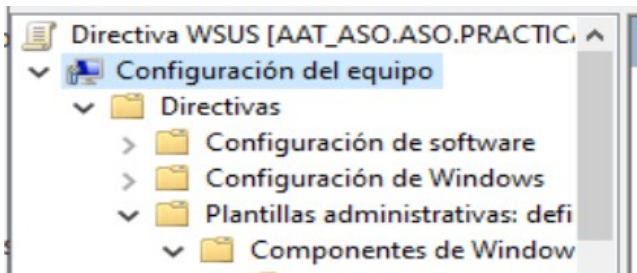
Crearemos una GPO anclada a la ou que contiene los equipos:



Lo siguiente sera editar esta GPO nueva para permitir las windows update:



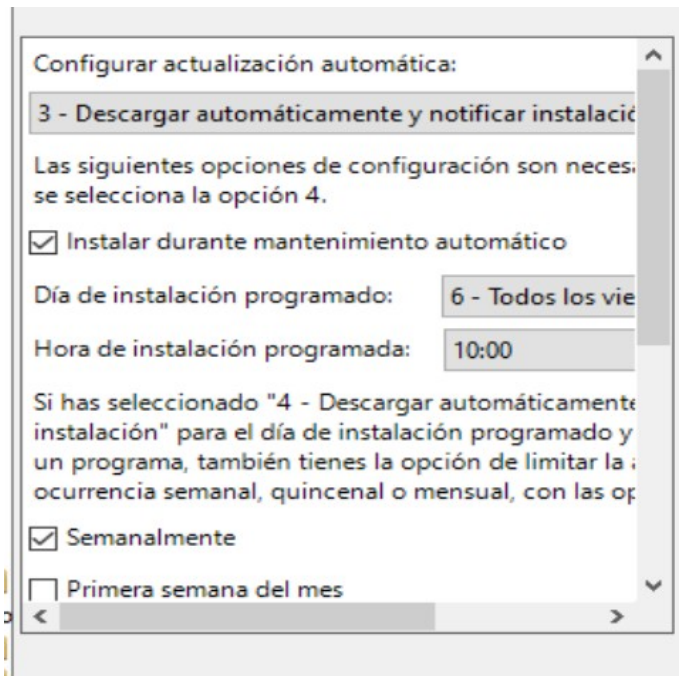
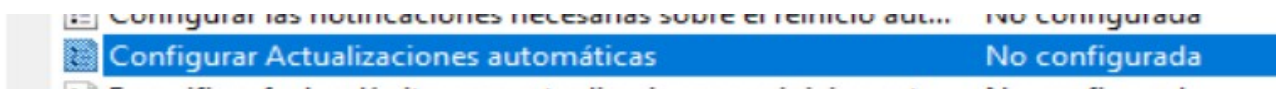
Entraremos en configuración de equipo,
Plantillas administrativas y Componentes de windows:



Abajo del todo estará Windows Update:




Ahora modificaremos las siguientes GPO:



Antes de habilitar:

- 3 Descargar y notificar
- Instalar de modo automático
- Seleccionar Viernes día de almuerzo largo y la hora la cual parten a almorzar.
- Decidir si es semanalmente o primera semana del mes

Segunda GPO:

 Especificar la ubicación del servicio Windows Update en la i... No configurada

☐ No configurada Comentario:

☒ Habilitada

☐ Deshabilitada

Compatible con: Al menos Wind
Pack 3, exclu

Opciones:

Establecer el servicio de actualización de la intranet:

Establecer el servidor de estadísticas de la intranet:

Definir el servidor de descargas alternativo:
(ejemplo: https://IntranetUpd01)

☐ Descarga archivos sin URL en los metadatos si se

☐ No forzar la asignación de certificados TLS para c

Seleccione el comportamiento del proxy para el clie

Usar solo el proxy del sistema para detectar actualiza

Antes de habilitar:

- La ubicación sera el nombre del servidor con el dominio + el puerto por el cual se comunicaran.

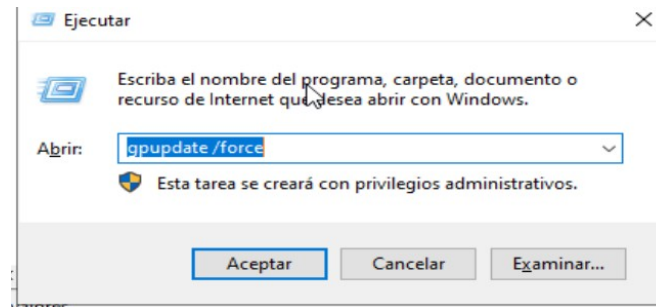
- Establecer el servidor de estadísticas sera la misma dirección

Podremos añadir varias opciones como se muestran nosotros las dejaremos sin marcar.

-3 GPO, Que solo tenemos que dar a habilitar:



Una vez echo esto forzaremos las gpo y ya tendremos configurado el servicio de actualizaciones mediante wsus y gpo:



Vemos como interactúa el WSUS al sincronizar con el servidor:

