

GPO

Aplicable a: Medulla - Agente

Versión: Todas

Entorno: On-Premise / SaaS privado / SaaS compartido

Categoría: Agente Medulla

Implementación del agente Medulla a través de GPO

¿Cuál es el mejor método para implementar el agente Medulla en todos los equipos de un dominio de Active Directory?

El método recomendado es utilizar una **tarea programada a través de las Preferencias de política de grupo (GPP)** con la opción «**Aplicar una vez y no volver a aplicar**».

Este método es:

- Compatible con cualquier archivo EXE (no se necesita MSI)
- Se ejecuta una sola vez por equipo
- Se inicia con derechos de sistema (administrador)
- Es oficialmente compatible con Microsoft
- Fiable y evita reinstalaciones repetidas

¿Cómo se implementa este método?

Paso 1: Preparar el archivo de instalación

1. Copie el instalador en una unidad compartida de red accesible: *(Asegúrese de que la ruta sea accesible para «Todos» o «Equipos del dominio» en modo de lectura).*

```
“ \\SERVIDOR\IMPLANTACIÓN\Medulla-Agent-windows-FULL-latest.exe
```

Cree un script de PowerShell como este:

```
“ $CheminSetup = "\\SERVIDOR\IMPLANTACIÓN\Medulla-Agent-windows-FULL-
latest.exe"
$Arguments = "/S"

$NombreDelServicio = "medullaagent"

$ServiceStatus = Get-Service -Name $NomDuService -ErrorAction
SilentlyContinue

if ($ServiceStatus) {
    Write-Output "El servicio $NombreDelServicio ya existe. Instalación
cancelada."
    Exit 0
}

try {
    Start-Process -FilePath $RutaDeInstalación -ArgumentList $Argumentos -Wait -
NoNewWindow -ErrorAction Stop
}
catch {
    Write-Error "Error de instalación: $_"
    Exit 1
}
```

2. Configure los permisos del recurso compartido:
 - **Lectura** para el grupo **Domain Computers**

Paso 2: Crear el GPO

1. Abra la consola de **administración de directivas de grupo**
2. Cree un nuevo GPO, por ejemplo: `Implementación del agente Medulla`

Paso 3: Configurar la tarea programada

1. Edite el GPO y vaya a:

Configuración del equipo
→ Preferencias
→ Panel de control
→ Tareas programadas

2. Haz clic con el botón derecho → **Nuevo** → **Tarea inmediata (al menos en Windows 7)**

3. En la pestaña **General**:

- Nombre: `Instalación del agente Medulla`
- Cuenta: **SYSTEM**
- Ejecutar con los privilegios más altos

4. En la pestaña **Acciones**:

- **Acción:** Iniciar un programa.
- **Programa/script:** ruta_instalación_powershell/powershell.exe
- **Añadir argumentos:** -ExecutionPolicy Bypass -File "\\Servidor\Recursos compartidos\TuScript.ps1" (Asegúrate de que la ruta sea accesible para «Todos» o «Equipos del dominio» en lectura).

Paso 4: Aplicar la GPO

1. Vincule la GPO a la **Unidad de Organización (OU)** que contiene sus equipos
2. En un equipo de prueba, ejecute:

```
gpupdate /force
```

3. Reinicie el equipo o espere a la próxima actualización de políticas

Atención: siempre es obligatorio reiniciar los equipos tras la instalación del agente; el GPO, por defecto, no reinicia el equipo por sí solo. Por lo tanto, hay que tener en cuenta que cada equipo debe reiniciarse tras la instalación del agente.

¿Por qué no utilizar un script de inicio o de inicio de sesión?

Los scripts tradicionales (Startup Script o Logon Script) presentan varias desventajas:

- Riesgo de ejecución múltiple
- Dificultad para detectar si la instalación ya se ha realizado
- Problemas de permisos según el contexto de ejecución
- Menos fiables que las tareas programadas de GPP

El método mediante tareas programadas GPP resuelve todos estos problemas.

¿Qué hace la opción «Apply once and do not reapply»?

Esta opción garantiza que:

- La tarea se ejecute **una sola vez** en cada equipo
- Aunque el GPO permanezca activo durante años, la instalación no se vuelve a ejecutar
- No se necesita un script de detección complejo
- No se producen reinstalaciones accidentales

Es el equivalente a una implementación «fire and forget» (lanzar y olvidar).

Con la opción «**Apply once and do not reapply**», es imprescindible comprobar que el agente se ha instalado correctamente. Si la instalación ha fallado durante el proceso, no se volverá a ejecutar.

Puede desactivar esta opción («**Apply once and do not reapply**») para evitar problemas de instalación del agente, pero mantener la parte IF en el script de PowerShell que comprueba si el servicio **medullaagent está** presente (por defecto, ya presente en el script anterior):

```
if ($ServiceStatus) {  
    Write-Output "El servicio $NomDuService ya existe. Instalación cancelada."  
    Exit 0  
}
```

¿Cómo comprobar que la implementación ha funcionado?

En un equipo cliente:

1. Comprueba que se ha creado la tarea programada:

Busque la tarea «Instalación del agente Medulla»

2. Compruebe los registros de instalación del agente Medulla
3. Compruebe que el equipo aparece en la consola de Medulla

En el controlador de dominio:

Utilice los informes de GPO para ver qué equipos han aplicado la política.

¿Puedo utilizar este método para actualizar el agente?

Por defecto, el agente se actualiza automáticamente, pero si no es así, sí, aunque con algunas precisiones:

- Si crea un **nuevo GPO** con un nuevo nombre de tarea, se ejecutará una vez en todos los equipos (si «Apply once» está activado)
- Si modifica la ruta del archivo EXE en la tarea existente con «Apply once», **no** se volverá a **ejecutar** (ese es el objetivo de esta opción)

Para las actualizaciones, es preferible:

1. Crear un nuevo GPO con un nuevo nombre de tarea para cada versión principal
2. O utilizar el sistema de actualización integrado de Medulla

¿Cuáles son los requisitos previos?

- Un controlador de dominio de Active Directory (Windows Server 2008 R2 o superior)
- Un recurso compartido de red al que los equipos puedan acceder en modo de lectura
- El instalador del agente de Medulla con la opción de instalación silenciosa (`/S`)
- Permisos para crear y vincular GPO

¿Cuánto tiempo se tarda en implementar todos los equipos?

La implementación se realiza al ritmo de la actualización de las políticas de grupo:

- Por defecto: cada **90 minutos** (con un desfase aleatorio de 0 a 30 minutos)
- Al reiniciar el equipo
- Con ``gpupdate /force`` (inmediato)

Para una implementación rápida en un parque de 100 equipos, calcule entre **2 y 4 horas**, dependiendo de la actividad de la red.

Ejecutar la instalación tras iniciar sesión

La ejecución habitual de un GPO se realiza antes de iniciar sesión con privilegios de SYSTEM.

Esto puede resultar molesto para el usuario, que puede pensar que su ordenador se ha bloqueado.

Solución 1: La tarea programada «Al iniciar la sesión»

El usuario accede a su escritorio y la instalación se inicia de forma silenciosa en segundo plano con derechos de SYSTEM.

1. En su GPO **de equipo** (no de usuario), vaya a: **Preferencias > Configuración del Panel de control > Tareas programadas**.
2. Nuevo > **Tarea programada (al menos en Windows 7)**.
3. **Pestaña General:**
 - **Cuenta de usuario:** `NT AUTHORITY\SYSTEM` (o simplemente escribe `SYSTEM`).
 - Marque la casilla **Ejecutar con los permisos máximos**.
4. **Pestaña Desencadenantes (Triggers):**
 - Nuevo > **Al iniciar sesión** (At log on).
 - Puede elegir «Cualquier usuario».
5. **Pestaña Acciones:**
 - Programa: `ruta_de_instalación_powershell/powershell.exe/powershell.exe`
 - Argumentos: `-ExecutionPolicy Bypass -File "\\Servidor\Compartido\SCRIPT_POWERSHELL.ps1"`

SCRIPT_POWERSHELL.PS1, corresponde al script que aparece al principio de la página y que permite instalar el agente de forma silenciosa.

Solución 2: La opción «Asíncrono»

Si desea conservar su script actual (en «Scripts de inicio») pero simplemente dejar de bloquear la pantalla «Por favor, espere...»:

1. Vaya a la GPO: **Configuración del equipo > Plantillas de administración > Sistema > Scripts**.

2. Busque el parámetro: **Ejecutar scripts de inicio de forma asíncrona**.
3. Póngalo en **Activado**.

Nota: Si crea una tarea con un desencadenador «Al iniciar sesión» y marca «**Aplicar una vez y no volver a aplicar**», el GPO creará la tarea una vez, pero la **tarea permanecerá en el PC y seguirá ejecutándose cada vez que se inicie sesión**. Asegúrate, por tanto, de mantener la condición **IF en** el script que permite verificar la presencia del servicio **medullaagent** (por defecto, ya presente en el script anterior):

```
if ($ServiceStatus) {  
    Write-Output "El servicio $NomDuService ya existe. Instalación cancelada."  
    Exit 0  
}
```

Recursos adicionales

- [Documentación oficial de Microsoft sobre las preferencias de directiva de grupo]([https://docs.microsoft.com/fr-fr/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn581922\(v=ws.11\)](https://docs.microsoft.com/fr-fr/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn581922(v=ws.11)))
- [Documentación de implementación de Medulla](<https://medulla-project.org/>)

Fecha de creación: diciembre de 2024

Autor: Documentación de Medulla

Versión: 1.0

Revision #1

Created 2026-04-30 07:40:34 UTC by Adrien Thaisse

Updated 2026-04-30 07:40:34 UTC by Adrien Thaisse