

Active Directory

En el marco de una implementación On-Premise, deben proporcionarse tres cuentas de servicio de Active Directory distintas.

1. Cuenta de solo lectura

Esta cuenta sirve para **consultar el** LDAP con el fin de obtener información sobre los usuarios y grupos.

- **Función: Solo lectura** (Read-Only).
- **Función:** Recupera información sobre el usuario y el grupo a través del protocolo **LDAP** (o LDAPS).
- **Permisos necesarios:** Debe tener los derechos necesarios para realizar búsquedas y leer atributos de usuario en el directorio de Active Directory.
- **Ubicación en la aplicación:** Los datos de identificación de esta cuenta se configurarán en el **archivo de configuración** de Medulla (información solicitada en el formulario de entrega).

2. Cuenta de registro de máquinas (Imaging/Mastering)

Esta cuenta está dedicada a las operaciones de **aprovisionamiento y registro** de nuevas máquinas en el dominio durante el proceso de creación de imágenes (o *masterización*).

- **Función:** Derechos de registro de máquinas en el dominio.
- **Función:** Permitir la adición de ordenadores al dominio de Active Directory.
- **Permisos necesarios:** Debe tener el derecho «**Añadir estaciones de trabajo al dominio**».
- **Integración en el proceso:** Esta cuenta será **integrada y utilizada por** sysprep para ejecutar la operación de unión al dominio durante el mastering del equipo.

3. Cuenta de ejecución de scripts (instalación del agente Medulla)

Esta cuenta es necesaria para las tareas de administración posteriores al despliegue, concretamente para la **instalación remota del agente Medulla** a través de PowerShell, dirigiéndose a una **unidad organizativa (OU)** definida.

- **Función:** Enumerar los equipos del AD y ejecutar scripts de PowerShell de forma remota con derechos delegados.
- **Función:** enumerar los equipos del AD. Instalación y configuración del agente Medulla en los equipos cliente, dirigiéndose a los equipos de una UO específica.
- **Permisos necesarios:**
 - **Derechos delegados sobre la UO de destino:** Debe tener derechos de modificación de los objetos «Computer» y derechos que permitan la ejecución de comandos de forma remota (a través de **WinRM** o una solución equivalente) en los

equipos de la UO especificada.

- **Acceso al recurso compartido de red:** si el script o el instalador del agente Medulla está almacenado en un recurso compartido, la cuenta debe tener derechos de **lectura** sobre dicho recurso compartido.
- **Listar los equipos del AD:** **Debetener** derechos para listar los equipos del AD con el fin de seleccionar aquellos en los que se debe instalar el agente.
- **Uso:** Esta cuenta será utilizada por la aplicación Python para iniciar y validar la ejecución de los scripts de PowerShell en los equipos, garantizando que el agente esté instalado y que el equipo esté correctamente vinculado a la estructura de unidad organizativa adecuada.

Revision #1

Created 2026-04-30 07:39:03 UTC by Adrien Thaisse

Updated 2026-04-30 07:39:03 UTC by Adrien Thaisse