

ACTIVE DIRECTORY BAJO ATAQUE COMO PROTEGER TU RED CONTRA PASS-THE-HASH

GUÍA



HENRIQUE ALVES

Tabla de contenido

INTRODUCCIÓN.....3

SECURIZACIÓN DE LAS CUENTAS LOCALES DE EQUIPOS UNIDOS A UN DOMINIO A TRAVÉS DEL USO DE LAPS.4

EDITAMOS LA NUEVA GPO “LAPS”8

EN CASO DE QUE LAPS NO TE GENERE LA CONTRASEÑA9

 Alternativa 9

INTRODUCCIÓN

En entornos empresariales, la seguridad de **Active Directory (AD)** es fundamental para prevenir accesos no autorizados y ataques internos. Uno de los métodos más utilizados por los atacantes para comprometer redes es el **Pass-the-Hash (PtH)**, una técnica que permite moverse lateralmente dentro de la infraestructura utilizando los hashes de contraseñas robadas, sin necesidad de conocer la clave original.

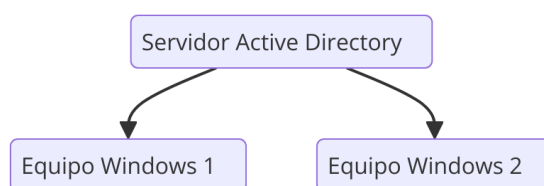
Este tipo de ataque es especialmente peligroso cuando las cuentas de **administrador local** de los equipos dentro del dominio comparten la misma contraseña. Si un atacante compromete una máquina, puede extender su acceso a otros equipos con facilidad, poniendo en riesgo toda la red.

Para mitigar este riesgo, utilizaremos **Microsoft LAPS (Local Administrator Password Solution)**, una herramienta gratuita que permite administrar de manera segura las contraseñas de las cuentas de administrador local en equipos unidos a un dominio. LAPS genera contraseñas aleatorias y únicas para cada máquina, almacenándolas de forma segura en Active Directory y evitando su reutilización.

En esta práctica, implementaremos **LAPS en un servidor Windows con Active Directory**, configurando las políticas necesarias para gestionar automáticamente las credenciales de administrador local en los equipos del dominio. Con esta solución, mejoraremos significativamente la seguridad y reduciremos la exposición de la red ante ataques *Pass-the-Hash*.

En mi caso estoy utilizando una red más grande con varios servidores y equipos.

Como ejemplo para que puedas ponerlo en práctica en VMWare o VirtualBox:



SECURIZACIÓN DE LAS CUENTAS LOCALES DE EQUIPOS UNIDOS A UN DOMINIO A TRAVÉS DEL USO DE LAPS.

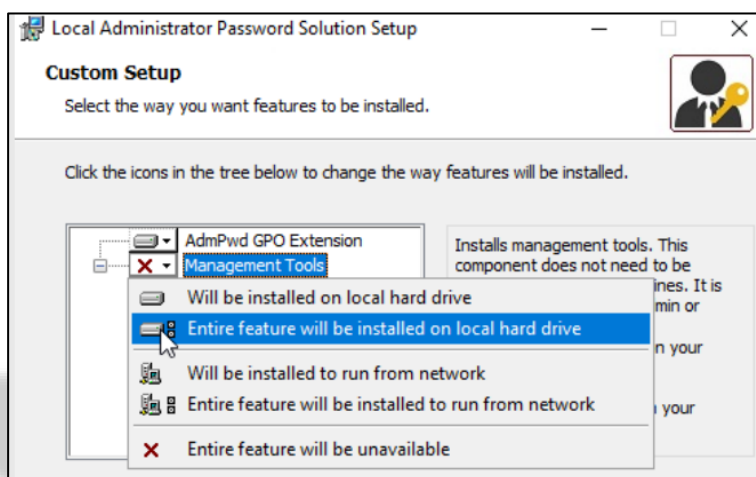
En el controlador de dominio DC01, desde el enlace <https://www.microsoft.com/en-us/download/details.aspx?id=46899> descargamos la utilidad LAPS.x64.msi.

Una vez descargado el fichero “.msi” lo ejecutamos y seguimos el procedimiento estándar de toda instalación Windows con “siguiente-siguiente” has llegar a esta pantalla de la siguiente imagen.

Aquí, en el árbol, desplegamos la opción “Management Tools” y seleccionamos la opción “Entire feature Will be installed on local hard drive” ...

Y pulsamos “Next”.

En la siguiente pantalla simplemente pulsamos el botón “Install” y la aplicación será instalada rápidamente.



A continuación, abrimos una consola de “PowerShell” con permisos de administrador y ejecutamos:

Import-Module AdmPwd.PS

Update-AdmPwdADSchema

Con ello habremos importado el módulo y actualizado el esquema del Directorio Activo.

En el servidor iremos ahora a “Usuarios y Equipos de Active Directory” y colgando de la raíz del dominio cread una nueva unidad organizativa (OU) que se llame “LAPS”. Una vez creada, desplazad a dicha OU la máquina que tengas en la misma red y creamos también un nuevo grupo de seguridad global, colgando de “Users”, con el mismo nombre, es decir “LAPS”

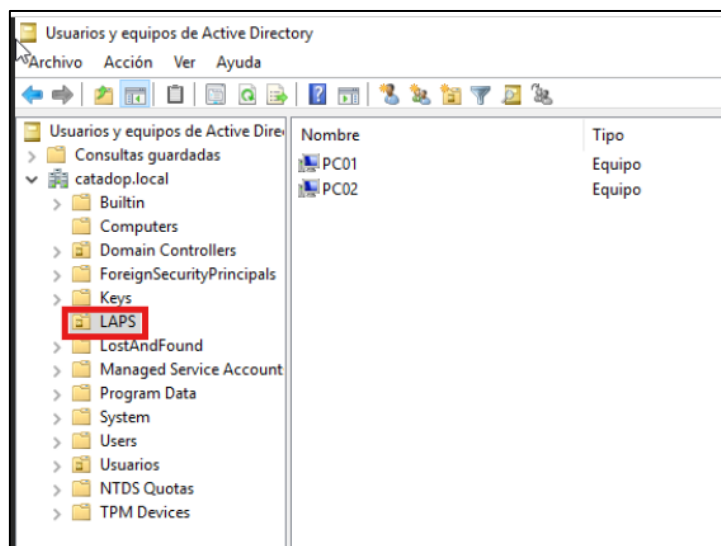
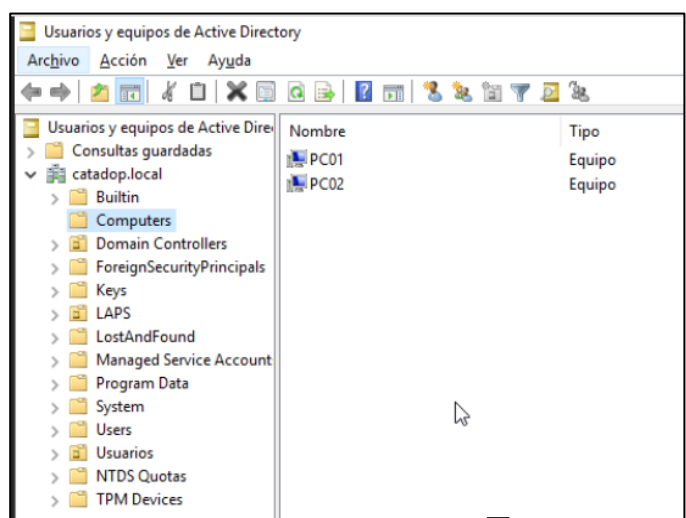
1. **Abrir Usuarios y Equipos de Active Directory:**
 - En el controlador de dominio (AD), abre la consola **Usuarios y Equipos de Active Directory** o (dsa.msc).
2. **Localizar los equipos (Equipo 1):**
 - Ve a la carpeta **Computers** en el panel izquierdo y localiza **EL EQUIPO QUE ESTE EN EL DOMINIO.**

Mover los equipos:

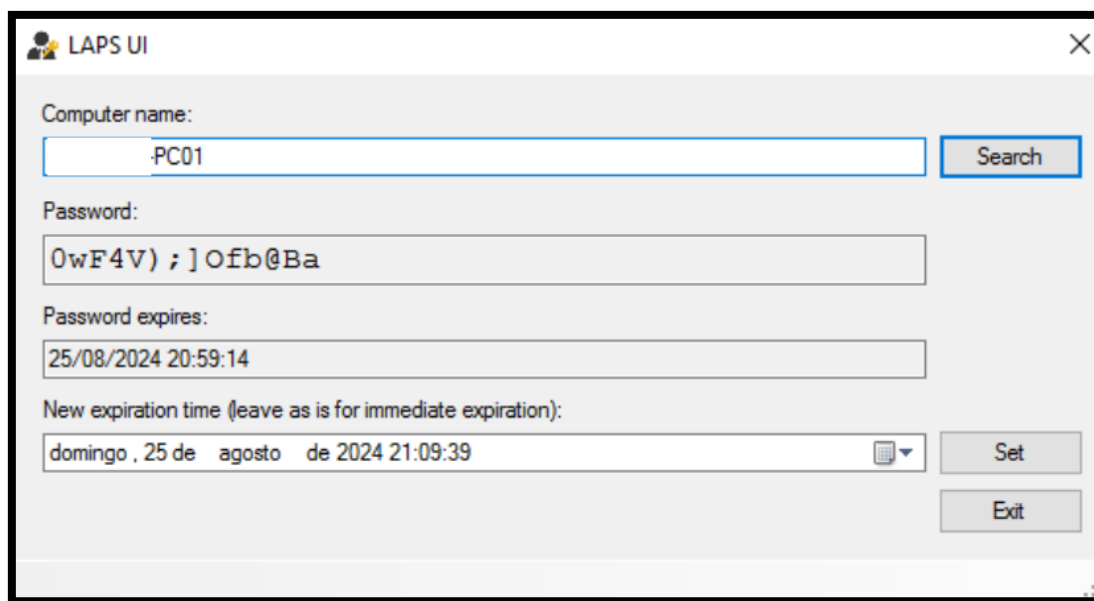
Haz clic derecho en **EQUIPO 1** y selecciona **Mover**.

En la ventana que aparece, selecciona la OU **"LAPS"** y haz clic en **Aceptar**.

Repite el mismo proceso con **otro** equipo que tengas.



En “Computer name” poned el nombre del equipo que este en el dominio, en nuestro ejemplo “PC01”, y acto seguido pulsad el botón “Search”, y entonces os debería cambiar a algo así:



The screenshot shows the LAPS UI window. The 'Computer name' field contains 'PC01' and the 'Search' button is highlighted. The 'Password' field displays '0wF4V) ;] Ofb@Ba'. The 'Password expires' field shows '25/08/2024 20:59:14'. The 'New expiration time (leave as is for immediate expiration):' field shows 'domingo , 25 de agosto de 2024 21:09:39'. The 'Set' and 'Exit' buttons are visible at the bottom right.

Ahora con la contraseña que os aparezca en el campo “Password”, id al equipo PC01 e intentad iniciar sesión con el usuario “Administrador” local (“.\Administrador”) y deberíais poder entrar en la máquina sin problema con la nueva contraseña.

En el servidor que actúa como Active Directory (controlador de dominio)

Recomendado: El módulo **AdmPwd.PS** debería estar instalado en el **controlador de dominio** o en cualquier equipo administrativo desde donde planeas gestionar LAPS.

Razones:

- La gestión de contraseñas, como `Reset-AdmPwdPassword`, se realiza desde el controlador de dominio.
- Puedes usar comandos como `Get-AdmPwdPassword` para consultar contraseñas desde el dominio.
- Es más eficiente administrar **LAPS** desde una ubicación central.

A continuación, una consola de "PowerShell" con derechos administrativos ejecutamos el comando:

```
Set-AdmPwdComputerSelfPermission -OrgUnit "OU=LAPS,DC=catadop,DC=local"
```

Con ello estamos indicando en qué Unidad Organizativa vais a aplicar el uso de LAPS, en este caso una OU también llamada "LAPS".

Seguidamente, en la misma consola "PowerShell", ejecutamos los **siguientes dos comandos**:

```
Set-AdmPwdReadPasswordPermission -OrgUnit "OU=LAPS,DC=catadop,DC=local" -  
AllowedPrincipals "LAPS"
```

```
Set-AdmPwdResetPasswordPermission -OrgUnit "OU=LAPS,DC=catadop,DC=local" -  
AllowedPrincipals "LAPS"
```

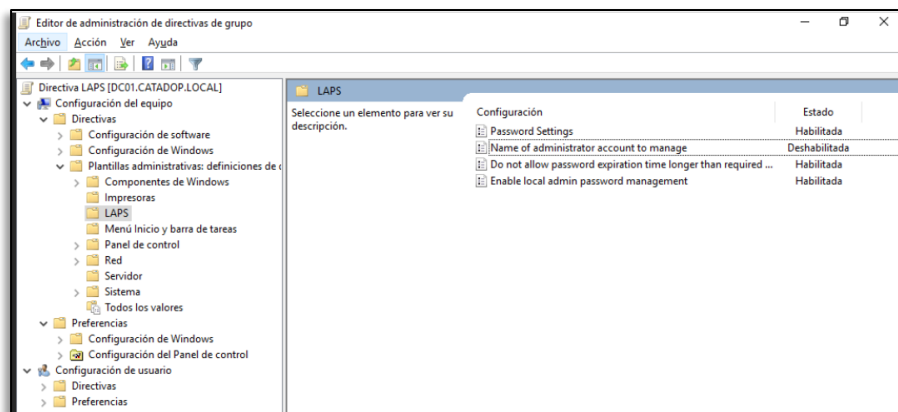
Con esto último habremos asignado permisos de lectura y restablecimiento de las contraseñas al grupo de Directorio Activo llamado "LAPS" creado con anterioridad.

Creación de la GPO específica para LAPS

En el siguiente paso deberemos ir a la consola de "Administración de Directivas de Grupo". Una vez dentro de la consola, vamos a "LAPS", pulsamos el botón derecho, y seleccionamos "Crear una GPO en este dominio y vincularlo aquí ...", asignamos a la nueva GPO el nombre de "LAPS" y pulsamos "Aceptar".

EDITAMOS LA NUEVA GPO “LAPS”

En “**Password Settings**” marcamos la casilla “Habilitada” y en el campo “Password Age (Days)” seleccionamos el valor “1” (periodicidad de renovación de 1 día). La opción “**Name of administrator account to manage**” la dejamos deshabilitada, mientras que las otras dos opciones restantes, es decir, “**Do not allow password expiration time longer than required by policy**” y “**Enable local admin password management**”, las dejamos habilitadas.

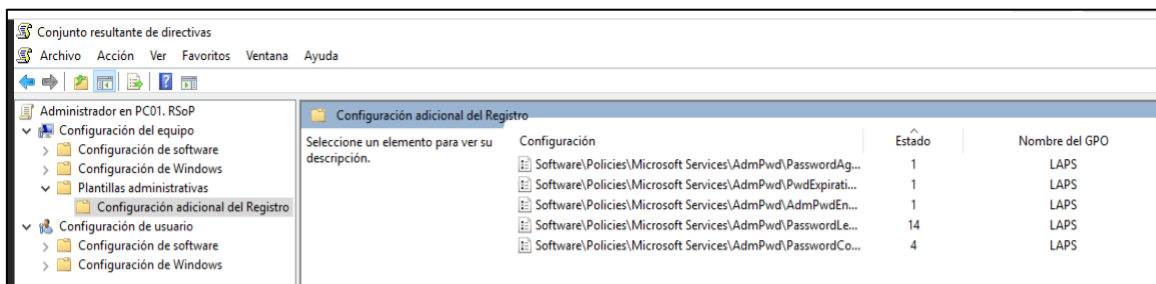


Una vez
realizado
el

despliegue de “LAPS” en el dominio, comprobamos con uno de los equipos clientes, por ejemplo PC01, que se está aplicando “LAPS” correctamente.

Arrancamos pues el equipo PC01, y una vez que esté funcionando entramos primero con el usuario “Administrador” (CATADOP\Administrador) de dominio y ejecutamos en una consola de sistema, primero un “**gpupdate /force**” y a continuación un “**rsop**”.

Esto último debería mostraros una ventana con el siguiente aspecto:



Alternativa

¿Dónde instalar el módulo AdmPwd.PS?

1. En PC01 (equipo cliente)
 - **Propósito:** El módulo **AdmPwd.PS** generalmente **no es necesario** en los equipos gestionados (como PC01), ya que el cliente **AdmPwd GPO Extension** se encarga automáticamente de recibir y aplicar las políticas.
 - **Casos en los que se justifica instalarlo:**
 - Si estás haciendo pruebas en PC01 para verificar su configuración o depurar problemas relacionados con LAPS.
 - Si necesitas comandos avanzados como *Check-AdmPwd* directamente en el cliente.
2. En DC01 (controlador de dominio)
 - **Recomendado:** El módulo **AdmPwd.PS** debería estar instalado en el **controlador de dominio** o en cualquier equipo administrativo desde donde planeas gestionar **LAPS**.
 - **Razones:**
 - La gestión de contraseñas, como *Reset-AdmPwdPassword*, se realiza desde el controlador de dominio.
 - Puedes usar comandos como *Get-AdmPwdPassword* para consultar contraseñas desde el dominio.
 - Es más eficiente administrar **LAPS** desde una ubicación central.

Próximos pasos según lo que hemos hecho

1. Si ya lo instalaste en PC01:

- No es un problema. Puedes usarlo para verificar configuraciones y realizar pruebas con el comando *Check-AdmPwd*.
- Sin embargo, para la administración y generación de contraseñas, deberías instalar también el módulo **AdmPwd.PS** en DC01.

Se realiza lo siguiente tanto en AD como en PC01:

En AD:

1. Habilitar TLS 1.2 en PowerShell

PowerShell puede estar usando una versión obsoleta de TLS para conectarse a los repositorios. Forzaremos el uso de **TLS 1.2**:

Abre PowerShell como administrador.

Ejecuta este comando:

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```

Intenta instalar nuevamente el proveedor de NuGet:
Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force

2. Verificar el estado de NuGet

Después de instalar el proveedor de NuGet, verifica si está disponible:

Ejecuta este comando:

```
Get-PackageProvider -ListAvailable
```

- Esto debería mostrar **NuGet** como uno de los proveedores disponibles.

Si aparece, intenta nuevamente instalar el módulo **AdmPwd.PS**:
Install-Module -Name AdmPwd.PS -Force

Próximo paso: Verificar que el módulo AdmPwd.PS funciona

En la misma sesión de PowerShell, carga el módulo (si no se cargó automáticamente):
Import-Module AdmPwd.PS

Verifica los comandos disponibles en el módulo:
Get-Command -Module AdmPwd.PS

Comandos utilizado:

```
PS C:\Windows\system32> [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
PS C:\Windows\system32> Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force

Name                Version          Source            Summary
-----
nuget                2.8.5.208       https://onege...  NuGet provider for the OneGet meta-package manager

PS C:\Windows\system32> Get-PackageProvider -ListAvailable

Name                Version          DynamicOptions
-----
msi                 3.0.0.0          AdditionalArguments
msu                 3.0.0.0          AdditionalArguments
NuGet               2.8.5.208       Destination, ExcludeVersion, Scope, SkipDependencies, Headers, FilterOnTag, Contains, AllowPrerelease, ...
PowerShellGet       1.0.0.1          PackageManagementProvider, Type, Scope, AllowClobber, SkipPublisherCheck, InstallUpdate, NoPathUpdate, ...
Programs            3.0.0.0          IncludeWindowsInstaller, IncludeSystemComponent

PS C:\Windows\system32> Install-Module -Name AdmPwd.PS -Force
PS C:\Windows\system32> Get-Command -Module AdmPwd.PS

CommandType Name                Version          Source
-----
Cmdlet      Find-AdmPwdExtendedRights 5.0.0.0          AdmPwd.PS
Cmdlet      Get-AdmPwdPassword        5.0.0.0          AdmPwd.PS
Cmdlet      Reset-AdmPwdPassword      5.0.0.0          AdmPwd.PS
Cmdlet      Set-AdmPwdAuditing        5.0.0.0          AdmPwd.PS
Cmdlet      Set-AdmPwdComputerSelfPermission 5.0.0.0          AdmPwd.PS
Cmdlet      Set-AdmPwdReadPasswordPermission 5.0.0.0          AdmPwd.PS
Cmdlet      Set-AdmPwdResetPasswordPermission 5.0.0.0          AdmPwd.PS
Cmdlet      Update-AdmPwdADSchema     5.0.0.0          AdmPwd.PS
```

Verificar permisos con el comando correcto

En **AD**, ejecuta el siguiente comando:

```
Find-AdmPwdExtendedRights -Identity "OU=LAPS,DC=xxxxxx,DC=local"
```

1. Esto buscará los permisos extendidos configurados en la OU **LAPS** y te mostrará los usuarios o grupos que tienen permisos para:
 - **Leer contraseñas** (Read Password).
 - **Restablecer contraseñas** (Reset Password).
2. Revisa la salida para confirmar que los permisos están configurados correctamente para los usuarios/grupos que deberían gestionar LAPS.
 - **NT AUTHORITY\SYSTEM**: El sistema local.
 - **BUILTIN\Administradores**: Los miembros del grupo local de Administradores.
 - **.\Administradores** (o similar): Un grupo administrativo del dominio.

Esto indica que los permisos básicos están correctamente configurados, y estos grupos/usuarios tienen los derechos necesarios para **leer** y **restablecer** contraseñas gestionadas por LAPS.

1. Generar una contraseña para PC01

En **AD**, ejecuta:

```
Reset-AdmPwdPassword -ComputerName "PC01"
```

Esto forzará la generación de una nueva contraseña para el administrador local de **PC01** y la almacenará en Active Directory.

2. Consultar la contraseña de PC01

Después de generar la contraseña, consúltala con este comando:

Get-AdmPwdPassword -ComputerName "PC01"

Este comando devolverá:

- La contraseña generada.
- La fecha de vencimiento.

```
PS C:\Windows\system32> Install-Module -Name AdmPwd.PS -Force
PS C:\Windows\system32> Import-Module AdmPwd.PS
PS C:\Windows\system32> Get-Command -Module AdmPwd.PS
```

CommandType	Name	Version	Source
Cmdlet	Find-AdmPwdExtendedRights	5.0.0.0	AdmPwd.PS
Cmdlet	Get-AdmPwdPassword	5.0.0.0	AdmPwd.PS
Cmdlet	Reset-AdmPwdPassword	5.0.0.0	AdmPwd.PS
Cmdlet	Set-AdmPwdAuditing	5.0.0.0	AdmPwd.PS
Cmdlet	Set-AdmPwdComputerSelfPermission	5.0.0.0	AdmPwd.PS
Cmdlet	Set-AdmPwdReadPasswordPermission	5.0.0.0	AdmPwd.PS
Cmdlet	Set-AdmPwdResetPasswordPermission	5.0.0.0	AdmPwd.PS
Cmdlet	Update-AdmPwdADSchema	5.0.0.0	AdmPwd.PS

```
PS C:\Windows\system32> Find-AdmPwdExtendedRights -Identity "OU=LAPS,DC=catadop,DC=local"
```

ObjectDN	ExtendedRightHolders
OU=LAPS,DC=catadop,DC=local	{NT AUTHORITY\SYSTEM, BUILTIN\Administradores, CATADOP\Ad...

```
PS C:\Windows\system32> Reset-AdmPwdPassword -ComputerName "PC01"
```

DistinguishedName	Status
CN=PC01,OU=LAPS,DC=catadop,DC=local	PasswordReset

```
PS C:\Windows\system32> Get-AdmPwdPassword -ComputerName "PC01"
```

ComputerName	DistinguishedName	Password	ExpirationTimestamp
PC01	CN=PC01,OU=LAPS,DC=catadop,DC=local	5oCzr4. [oq1[\$e	25/01/2025 2:57:29

```
PS C:\Windows\system32>
```

```
PS C:\Windows\system32> Get-AdmPwdPassword -ComputerName "PC01"
```

ComputerName	DistinguishedName	Password	ExpirationTimestamp
PC01	CN=PC01,OU=LAPS,DC=catadop,DC=local	5oCzr4. [oq1[\$e	25/01/2025 2:57:29

```
PS C:\Windows\system32>
```

Ahora ejecutamos los siguientes comandos para tener instalado (AdmPWD.PS) en PC01:

```
PS C:\Windows\system32> [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
PS C:\Windows\system32> Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force

Name            Version      Source      Summary
----            -
nuget            2.8.5.208    https://one... NuGet provider for the OneGet meta-package manager

PS C:\Windows\system32> Get-PackageProvider -ListAvailable

Name            Version      DynamicOptions
----            -
msi              3.0.0.0      AdditionalArguments
msu              3.0.0.0
NuGet            2.8.5.208    Destination, ExcludeVersion, Scope, SkipDependencies, Headers, FilterOnTag, Contains, AllowPrereleaseVersions, Configfile, SkipValidate
PowerShellGet    1.0.0.1      PackageManagementProvider, Type, Scope, AllowClobber, SkipPublisherCheck, InstallUpdate, NoPathUpdate, Filter, Tag, Includes, DscResou...
Programs         3.0.0.0      IncludeWindowsInstaller, IncludeSystemComponent

PS C:\Windows\system32> Install-Module -Name AdmPwd.PS -Force
PS C:\Windows\system32> Import-Module AdmPwd.PS
PS C:\Windows\system32> Get-Command -Module AdmPwd.PS

CommandType      Name                                     Version      Source
-----
Cmdlet            Find-AdmPwdExtendedRights               6.3.1.0      AdmPwd.PS
Cmdlet            Get-AdmPwdPassword                      6.3.1.0      AdmPwd.PS
Cmdlet            Reset-AdmPwdPassword                    6.3.1.0      AdmPwd.PS
Cmdlet            Set-AdmPwdAuditing                      6.3.1.0      AdmPwd.PS
Cmdlet            Set-AdmPwdComputerSelfPermission        6.3.1.0      AdmPwd.PS
Cmdlet            Set-AdmPwdReadPasswordPermission        6.3.1.0      AdmPwd.PS
Cmdlet            Set-AdmPwdResetPasswordPermission       6.3.1.0      AdmPwd.PS
Cmdlet            Update-AdmPwdADSchema                   6.3.1.0      AdmPwd.PS

PS C:\Windows\system32>
```

Iniciar sesión PC01 con usuario Administrador con la contraseña generada:

