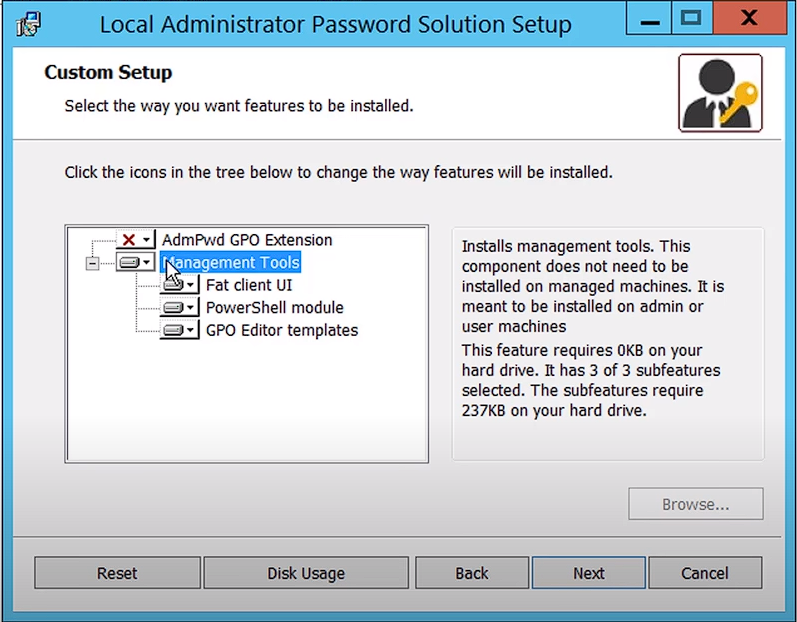
1. Inicialmente descargamos LAPS(x86/x64).msi, según la arquitectura de nuestro sistema
2. Ejecutamos el instalador y procedemos a instalar las extensiones necesarias para nuestro Servidor



1. Finalizamos la instalación
2. Ahora vamos a crear 2 grupos de seguridad en nuestro AD, estos van a diferenciarse de quienes tienen acceso de lectura y quienes de reseteo en la GUI de LAPS. Ej. “LAPS-RO” y “LAPS-RW”. Podríamos crear más como por ej. “LAPS-SERVERS-RO” o “LAPS-SERVERS-RW”, cuales servirían para poder determinar lo mismo pero no para equipos cliente sino para otros servidores. Y así podríamos crear la cantidad necesaria según nuestro requerimiento.
3. Agregamos a los usuarios en cada grupo pertinente o grupos que ya tengamos definidos con anterioridad
4. En este punto pasaremos a realizar la extensión de atributos o de esquema. Para esto abriremos una terminal de PowerShell como administrador, y comenzaremos a ejecutar:

#extendemos el Schema

Update-AdmPwdADSchema

#si tendríamos algún tipo de error sobre el paquete, lo que deberíamos realizar es la importación pertinente

Import-module AdmPwd.PS

#le damos permisos, a los equipos que queramos impactar con esta implementación, a que escriban en el AD en los atributos. Se debe repetir con todas la OU necesarias. Si tengo solo una OU con ese nombre basta con ponerlo que será identificada, de lo contrario deberemos colocar la ruta completa

Set-AdmPwdComputerSelfPermission -OrgUnit <nombre de la OU a delegar permisos>

#ahora le damos permiso de lectura a los usuarios

Set-AdmPwdReadPasswordPermission -OrgUnit <nombre de la OU a delegar permiso>

-AllowedPrincipals <usuario or grupo>

#para darle permiso de reseteo de contraseña

Set-AdmPwdResetPasswordPermission -OrgUnit <name of the OU to delegate

permissions> -AllowedPrincipals <users or groups>

#entendamos que ambos permisos son independientes, es decir, que tenga permiso de #reseteo no significa que podrá verla

1. En este paso vamos a crear la GPO que nos va a permitir llegar a los equipos que requerimos administrar.

Abrimos nuestro administrador de GPO en nuestro DC, creamos la política y editamos.

Primero debemos configurar la instalación del Soft en los equipos, para ellos nos posicionamos en “Computer Configuration > Policies > Software Settings”, realizamos click derecho en 'Software Installation' > 'New' > 'Package' y seleccionamos el instalador de LAPS en una ubicación compartida.

Segundo debemos configurar la plantilla administrativa, para esto cerramos la edición y la volvemos a abrir. Nos posicionamos en “Computer Configuration > Policies > Administrative Templates\LAPS” y configuramos de la siguiente forma:

* “Enable Local admin Password management”= 'Enabled'
* “Password Settings”='Enabled (Aquí podemos configurar Complejidad, largo y edad)'
* “Do not allow Password expiration time longer than required by policy” = 'Enabled'
* “Name of Administrator account to manage”=Configuraremos el nombre de la cuenta administrador a administrar, si no se configura la política buscara la cuenta administrador que Windows instala por default

Guardamos y a probar la GPO.

Nota: Si tuviésemos varios DC debemos copiar la plantilla “AdmPwd.admx”, ubicada en “%Windows\PolicyDefinitions” a “%Windows\SYSVOL\sysvol\<DomainName>\Policies\PolicyDefinitions” y el “AdmPwd.adml”, ubicado en “%Windows\PolicyDefinitions\en-US” a “%Windows\SYSVOL\sysvol\<DomainName>\Policies\PolicyDefinitions”

Nota 2: Podemos agregar los dos instaladores (x86 y x64) en la misma política, pero debemos configurar lo siguiente en el instalador de 32 Bits.

Dentro de la configuración de la política, realizamos doble click en 'LAPSx86.msi', dentro de la pestaña 'Deployment' ingresamos a las opciones avanzadas y des tildamos la siguiente opción 'Make this 32-bit X86 application available to Win64 machines'. No es obligatorio hacerlos pero de esta forma nos aseguramos que el instalador x86 no se ejecute en sistemas de 64 bits.

Nota 3: LAPS solo va a afectar a una cuenta local admin por equipo, la cual va a ser la especificada en la GPO

1. Una vez creada la política y asignada a la OU deseada, forzamos con un “gpupdate /force”, y nos va a pedir reiniciar el equipo. O directamente reiniciamos el equipo.

Consultar quien tiene permisos vía powershell

(Find-AdmPwdExtendedrights -orgunit <OU name>).ExtendedRightHolders

Atributos para consultar via AD

ms-Mcs-AdmPwd (Almacena la contraseña)

ms-Mcs-AdmPwdExpirationTime (Almacena la fecha de expiración de la contraseña)

Importante: Luego del primer reinicio y LAPS haya sido instalado en el equipo cliente mediante la GPO configurada, es muy probable que haya que volver a realizar un nuevo reinicio o un “gpupdate /force” para que aplique ahora si los permisos de LAPS en el equipo y escriba dentro de los atributos anteriormente mencionados.

Dentro del atributo ms-Mcs-AdmPwdExpirationTime se va a guardar un valor numérico que no nos va a aportar ningún dato concreto pero para transformarlo en una fecha y hora legible deberemos utilizar el siguiente comando en una consola 'cmd'

w32tm /ntte <numero a convertir>

Consultar pass y fecha de expiración vía powershell

Get-AdmPwdPassword -ComputerName <computername>

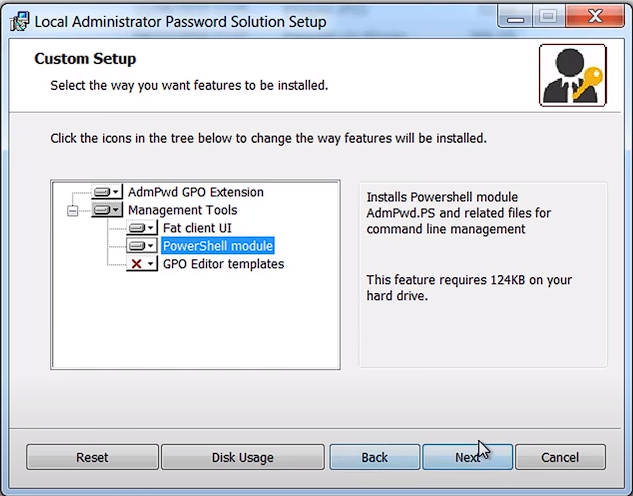
También podríamos realizar una consulta directamente al AD mediante powershell y un ejemplo podría ser:

Get-ADComputer -filter {Name -Like “<palabra clave>\*”} -Properties ms-Mcs-AdmPwd | Select Name, ms-Mcs-AdmPwd

En este ejemplo la consulta nos traería todos los equipos que coincidan en su nombre inicialmente con la palabra clave que utilicemos y que terminen de cualquier forma y que nos muestre en una lista el nombre del equipo y su contraseña administrador local.

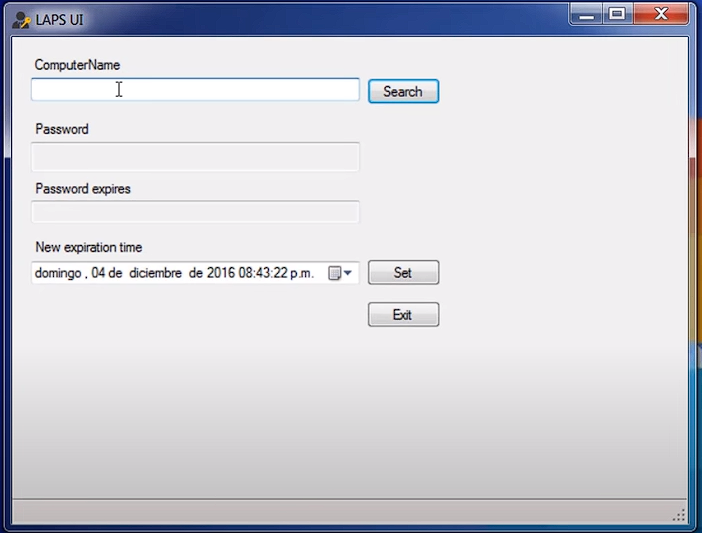
Consulta mediante GUI de LAPS

Instalamos la aplicación en la PC donde debemos consultar (Administradores o Help Desk o Soporte). Solo instalaremos la GUI y las extensiones de powershell.

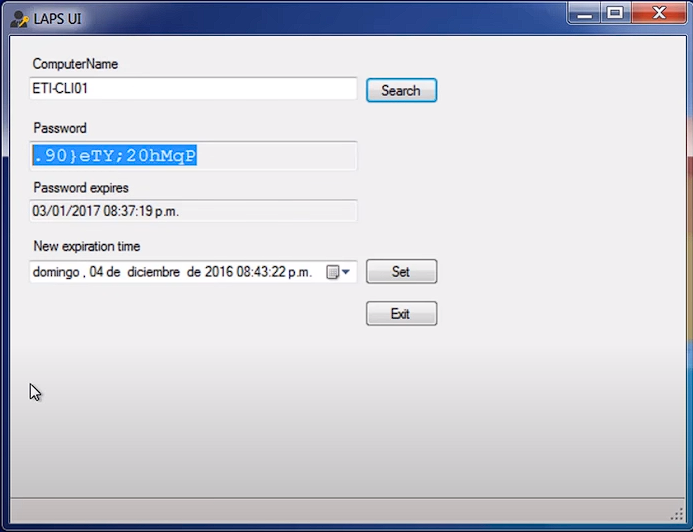


Los permisos para leer o no o para resetear o no se ajustan a las credenciales con las que iniciemos sesión de Windows.

Así veremos la interfaz:



Colocamos el nombre del equipo y clickeamos en “Search”.



Nos mostrara la pass determinada para la cuenta administrador local de ese equipo y la fecha de expiración. Si tuviésemos permiso de reseteo, lo que nos permite no es directamente resetear la pass pero si cambiar la fecha de expiración.

Si se inicia sesión con un usuario sin permiso de lectura en la consulta vería la fecha de expiración pero no la pass como en la siguiente imagen.

