



Protocolos de Internet

1° CUATRIMESTRE DE 2024

Trabajo Práctico N° 1C

Grupo: 4

Profesor/a: Javier Adolfo Ouret

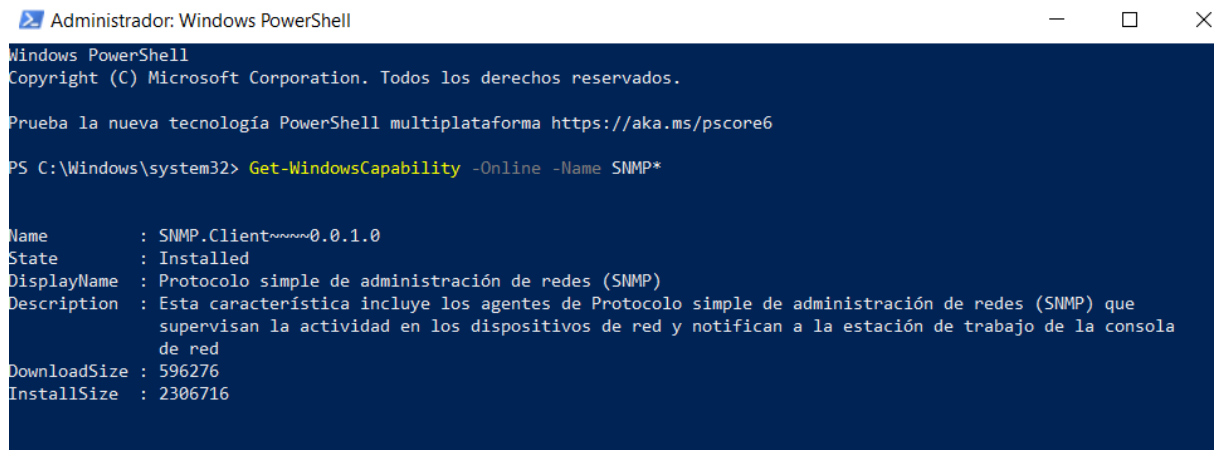
Integrantes:

N o	Apellido y Nombre	Legajo	Email
1	Marina Mercadal	152150976	marinamercadal@uca.edu.ar
2	Martina Naiquen Ruiz	29181	martinaruiz@uca.edu.ar
3	Carolina Suarez	152000738	suarezmacaro@gmail.com

TP2

Primero instalamos SNMP con PowerShell como administrador en Windows. Para eso utilizamos los siguientes comandos:

Get-WindowsCapability -Online -Name SNMP*: se utiliza en PowerShell para buscar capacidades relacionadas con SNMP disponibles en línea en un sistema Windows.



```
Administrador: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

PS C:\Windows\system32> Get-WindowsCapability -Online -Name SNMP*

Name       : SNMP.Client~~~~0.0.1.0
State      : Installed
DisplayName : Protocolo simple de administración de redes (SNMP)
Description : Esta característica incluye los agentes de Protocolo simple de administración de redes (SNMP) que supervisan la actividad en los dispositivos de red y notifican a la estación de trabajo de la consola de red
DownloadSize : 596276
InstallSize  : 2306716
```

En este caso podemos ver que en State (Estado) SNMP ya está instalado; si no fuera así el State estaría vacío y tendríamos que instalarlo. Para ello usamos el comando:

Get-WindowsCapability -name SNMP* -online | Add-WindowsCapability

-Online: este comando busca y agrega cualquier capacidad relacionada con SNMP que esté disponible en línea en el sistema Windows en el que se ejecuta.

Una vez instalado, ejecutamos los siguientes comandos:

Set-ItemProperty-Path "HKLM:\SYSTEM\CurrentControlSet\services\SNMP\Parameters\RFC1156Agent" -Name "sysContact" -Value "Nombre" -type String:

este comando establece el nombre del contacto de administración del agente SNMP en el valor "Nombre" en el registro de Windows. Es útil para modificar la configuración del sistema, cambiar la configuración de aplicaciones y realizar otras tareas de administración del sistema que requieran cambios en el registro.

Desglosamos el comando anterior en sus partes:

Set-ItemProperty: Este cmdlet (comando de PowerShell) se utiliza para establecer una propiedad de un elemento en el registro de Windows.

-Path "HKLM:\SYSTEM\CurrentControlSet\services\SNMP\Parameters\RFC1156Agent": Este parámetro especifica la ruta del registro donde se encuentra la clave que contiene la propiedad que se quiere modificar. En este caso, se está apuntando a la clave que contiene la configuración del agente SNMP.

-Name "sysContact": Este parámetro especifica el nombre de la propiedad que se quiere establecer o modificar. En este caso, se está trabajando con la propiedad

"sysContact" que generalmente almacena el nombre del contacto de administración para el agente SNMP.

-Value "Nombre": Este parámetro especifica el valor que quieres asignar a la propiedad. En este caso, se está estableciendo el valor "Nombre" para la propiedad "sysContact".

-type String: Se está indicando que la propiedad es de tipo "String" (cadena de texto).

Set-ItemProperty -Path

"HKLM:\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\RFC1156Agent" -Name "sysLocation" -Value "UCA" -type String: este comando a diferencia del anterior, establece la ubicación física del sistema o dispositivo SNMP en "UCA" en el registro de Windows. En este caso, se está estableciendo el valor "UCA" para la propiedad "sysLocation".

Set-ItemProperty-Path"HKLM:\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities" -Name "COMUNIDAD_PDI" -Value 8 -type DWord:

En este caso la ruta de registro está apuntando a la clave que contiene las comunidades SNMP válidas. Además se está estableciendo una comunidad SNMP llamada "COMUNIDAD_PDI", con el valor 8 (valor de datos binarios (DWORD) que representa los permisos que se asignan a esta comunidad) y de tipo DWord (tipo de datos binario de 32 bits.)

Set-ItemProperty-Path"HKLM:\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\PermittedManagers" -Name "1" -Value "localhost" -type String :

La ruta está apuntando a la clave que contiene la lista de administradores permitidos para SNMP. El nombre de la propiedad está establecido con el valor 1 ,se utiliza comúnmente como un identificador para el primer administrador en la lista. El valor asignado es : localhost, esto significa que la administración SNMP está permitida desde el propio dispositivo ("localhost"). Y el tipo de datos es de String.

Set-ItemProperty-Path"HKLM:\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\PermittedManagers" -Name "2" -Value "192.168.1.78" -type String:

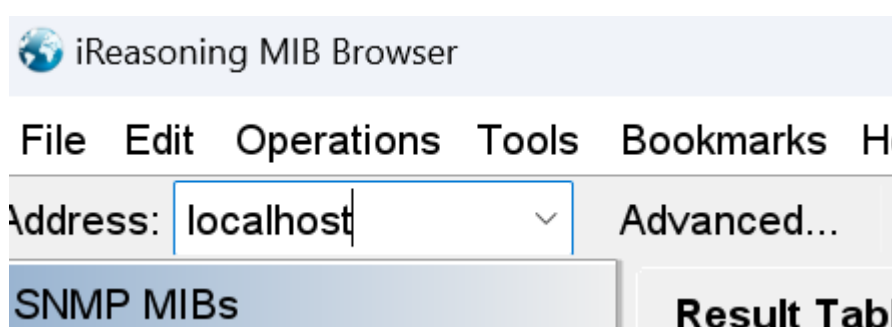
en este caso, a diferencia del anterior,se está estableciendo un nombre numérico para representar al segundo administrador permitido. El valor de la propiedad es: 192.168.1.78 y se establece como la dirección IP del segundo administrador permitido. Esto significa que la administración SNMP desde la dirección IP especificada está permitida.

```

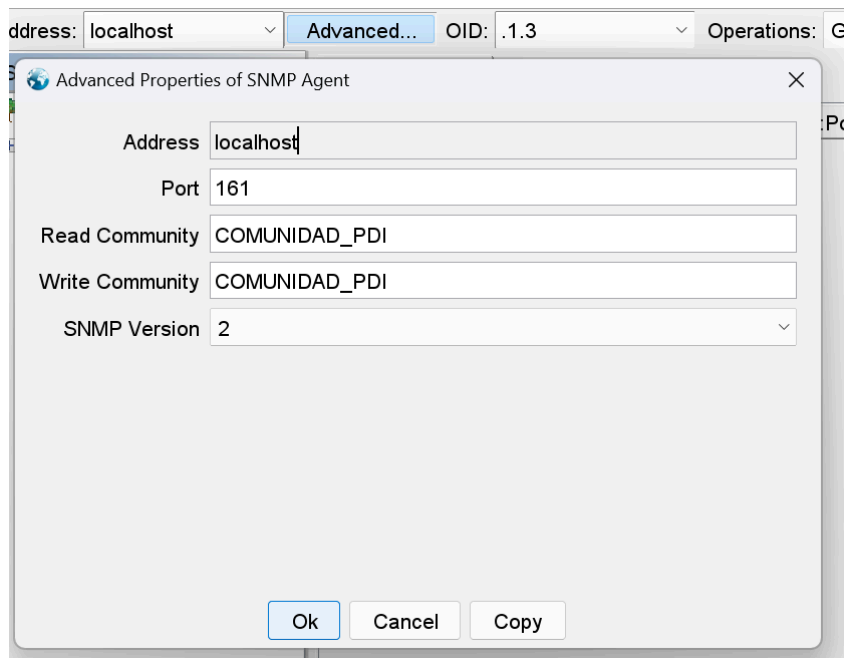
PS C:\Windows\system32> Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\services\SNMP\Parameters\RFC1156Agent" -Name "sysContact" -Value "Nombre" -type String
PS C:\Windows\system32> Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\services\SNMP\Parameters\RFC1156Agent" -Name "sysLocation" -Value "UCA" -type String
PS C:\Windows\system32> Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\services\SNMP\Parameters\ValidCommunities" -Name "COMUNIDAD_PDI" -Value 8 -type DWord
PS C:\Windows\system32> Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\services\SNMP\Parameters\PermittedManagers" -Name "1" -Value "localhost" -type String
PS C:\Windows\system32> Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\services\SNMP\Parameters\PermittedManagers" -Name "2" -Value "192.168.1.78" -type String
PS C:\Windows\system32>

```

Luego de instalar el Mib Browser:



Luego seleccione Advanced:



Lo que estamos
haciendo en MIB
Browser son

configuraciones específicas para establecer la comunicación SNMP con un agente
SNMP en mi dispositivo local.

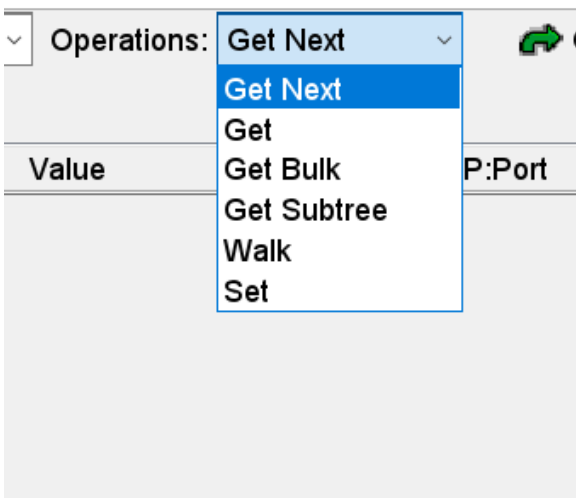
Al agregar "localhost" en la dirección, estoy indicando que quiero comunicarme con un agente SNMP que se ejecuta en mi propio dispositivo local.

Las comunidades SNMP actúan como contraseñas para acceder a un dispositivo SNMP (Read Community y Write Community). En este caso estoy especificando que las solicitudes SNMP enviadas al agente SNMP deben incluir COMUNIDAD_PDI como parte de la solicitud.

Y por último le estoy asignado la versión 2 de SNMP.

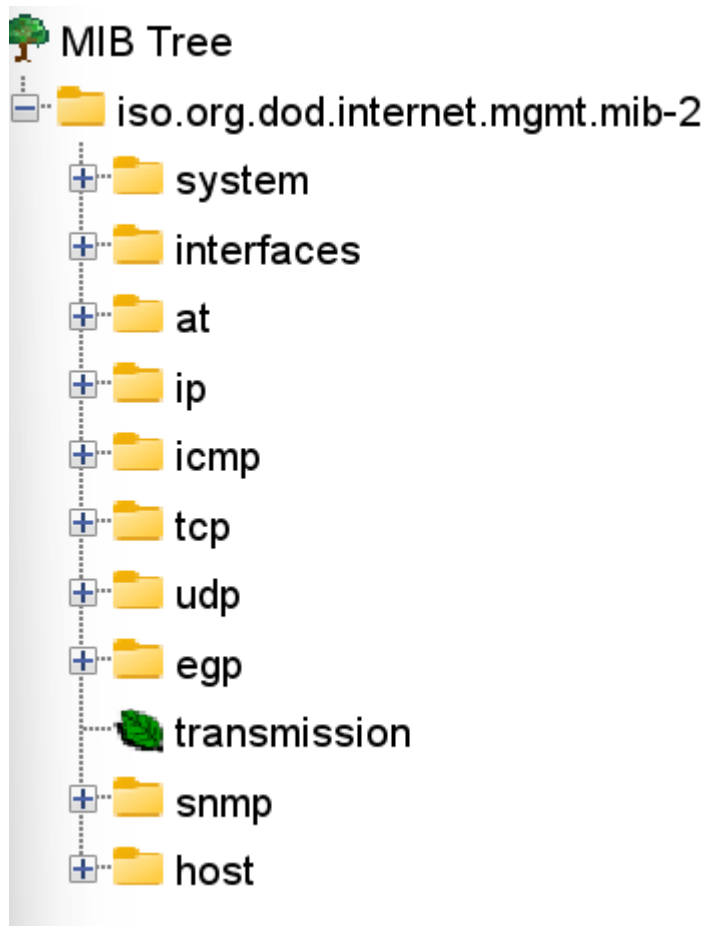
En resumen, al realizar estas configuraciones en el MIB Browser, estoy preparando el entorno para comunicarse con un agente SNMP que se ejecuta en mi dispositivo local y configurando las credenciales (comunidad SNMP) necesarias para acceder a él. Esto permite realizar consultas SNMP y obtener información del dispositivo local utilizando el MIB Browser.

Para ello usamos los comandos básicos :



name/OID	value	type	IP:Port
sysDescr.0	Hardware: Intel64 Family 6 Model 140 Stepping 1 AT/AT COMP...	OctetString	127.0.0.1..
sysDescr.0	Hardware: Intel64 Family 6 Model 140 Stepping 1 AT/AT COMP...	OctetString	127.0.0.1..
sysObjectID.0	.1.3.6.1.4.1.311.1.1.3.1.1	OID	127.0.0.1..
sysUpTime.0	24 hours 16 minutes 15.87 seconds (8737587)	TimeTicks	127.0.0.1..
sysContact.0	Nombre	OctetString	127.0.0.1..
sysName.0	LAPTOP-2O4JRJF2	OctetString	127.0.0.1..
sysLocation.0	UCA	OctetString	127.0.0.1..
sysServices.0	76	Integer	127.0.0.1..
ifNumber.0	44	Integer	127.0.0.1..
ifIndex.1	1	Integer	127.0.0.1..
ifIndex.2	2	Integer	127.0.0.1..

En el lateral izquierdo podemos encontrar el árbol de la MIB:



Donde debajo del mismo tenemos la tabla de datos, en donde seleccionamos por ejemplo sysObjectID:

Name	sysObjectID
OID	.1.3.6.1.2.1.1.2
MIB	RFC1213-MIB
Syntax	OBJECT IDENTIFIER
Access	read-only

Y nuestra tabla de resultados en donde se observa el nombre, valor tipo e ip:puerto, es decir socket

Name/OID	Value	Type	IP:Port
sysObjectID.0	.1.3.6.1.4.1.311.1.1.3.1.1	OID	127.0.0.1..