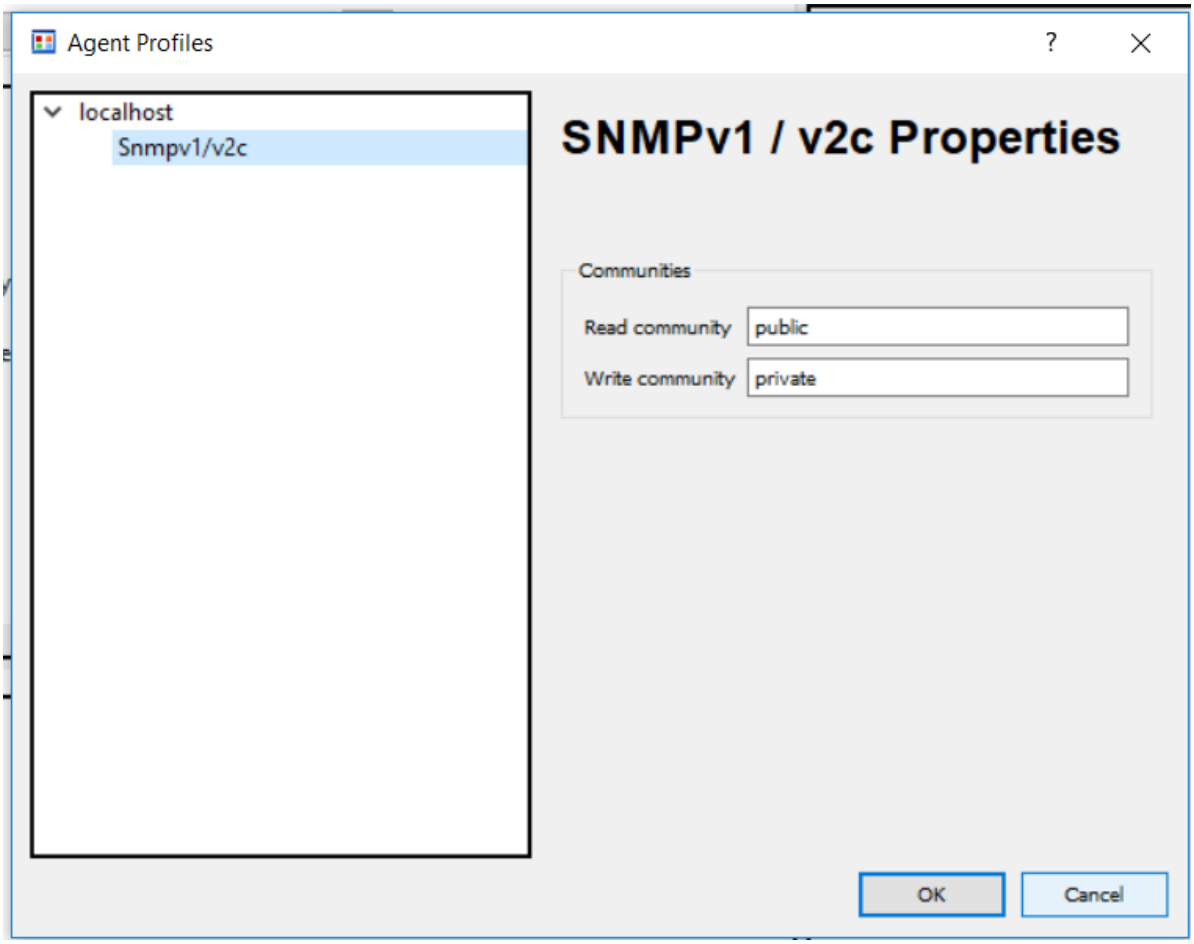
GRX - SNMP

> Auteurs : Jérôme Arn & Doran Kayoumi

Objectif 2 - Configurer un «SNMP Manager»

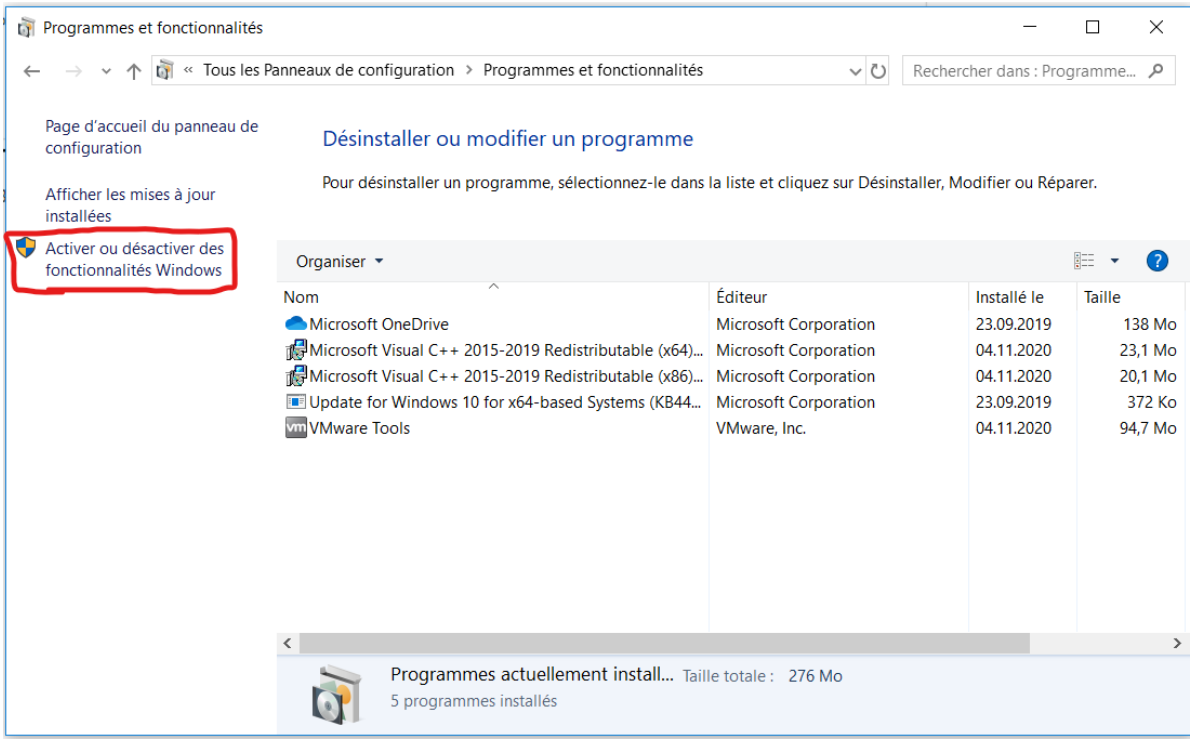
Après avoir installé `SNMPb`, on voit bien que le profile host `localhost` existe déjà.

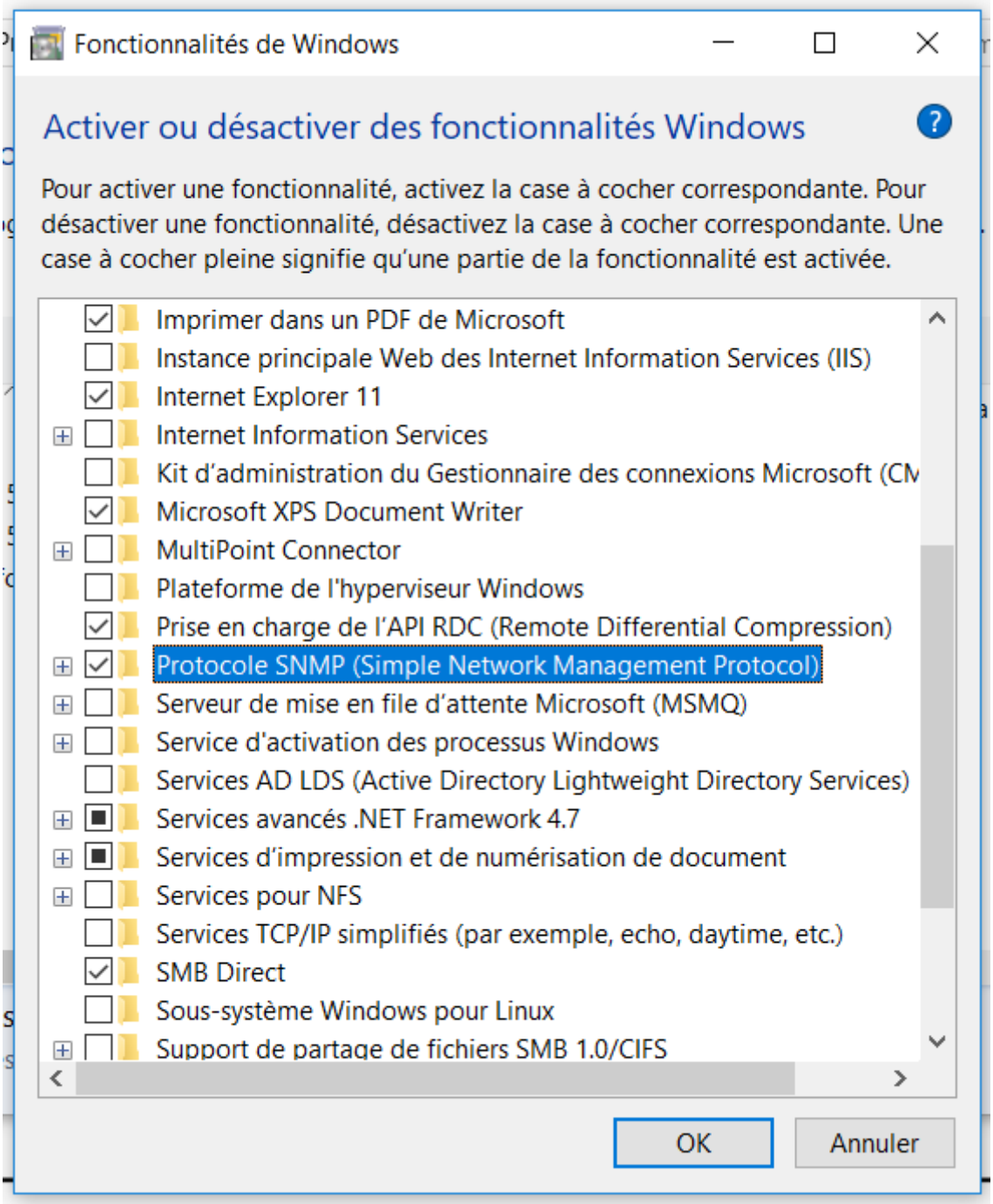


Objectif 3 - Configurer les agents SNMP en mode v2

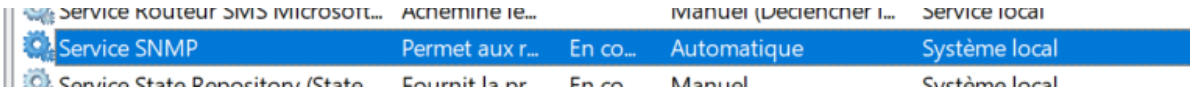
Activer SNMP sur Win A

Affin d'activer l'agent SNMP, Il suffit d'ouvrir le `panneau de configuration`, ouvrir la section `Programmes et fonctionnalités` où l'on peut activer ou désactiver les fonctionnalités de Windows. Ensuite depuis la fenêtre `Fonctionnalités de Windows`, il suffit de cocher `Protocole SNMP (Simple Network Management Protocol)`.

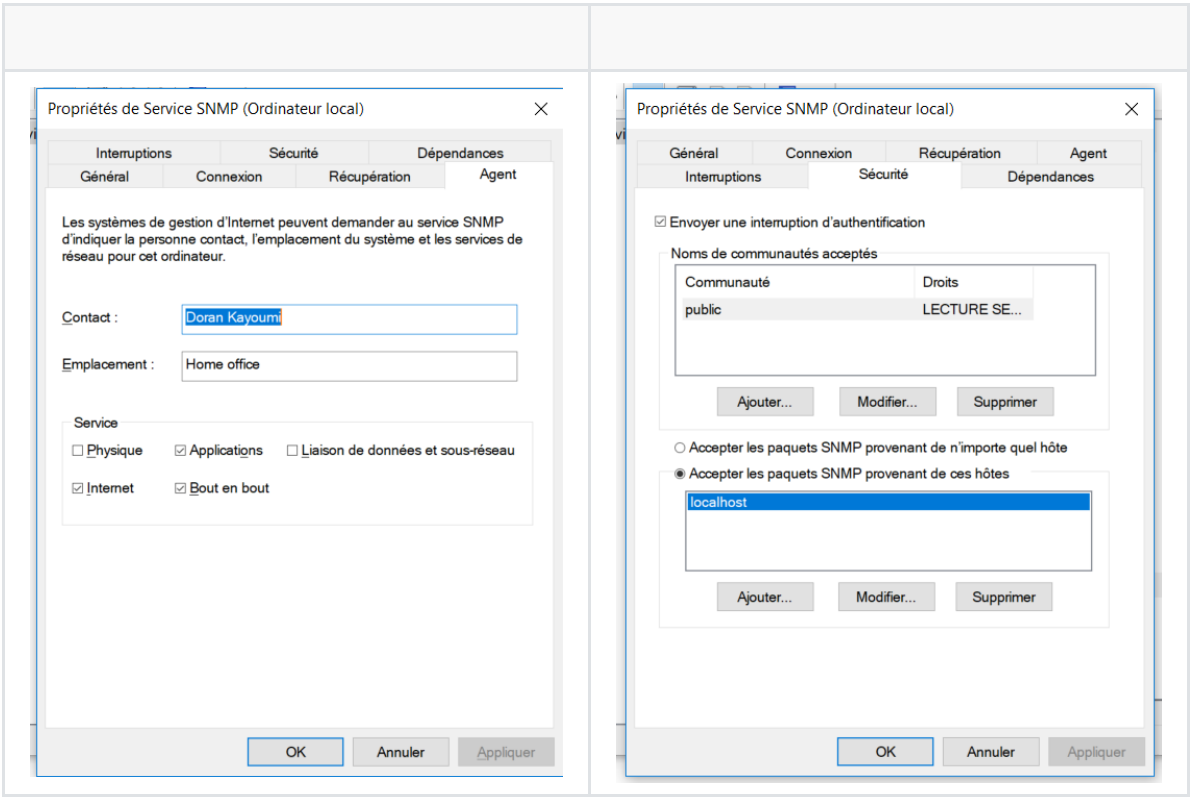

Programmes et fonctionnalités
Tous les Panneaux de configuration › Programmes et fonctionnalités
Rechercher dans : Programme...
Page d'accueil du panneau de configuration
Afficher les mises à jour installées
Activer ou désactiver des fonctionnalités Windows
Désinstaller ou modifier un programme
Pour désinstaller un programme, sélectionnez-le dans la liste et cliquez sur Désinstaller, Modifier ou Réparer.
Organiser
Nom
Éditeur
Installé le
Taille
Microsoft OneDrive
Microsoft Corporation
23.09.2019
138 Mo
Microsoft Visual C++ 2015-2019 Redistributable (x64)...
Microsoft Corporation
04.11.2020
23,1 Mo
Microsoft Visual C++ 2015-2019 Redistributable (x86)...
Microsoft Corporation
04.11.2020
20,1 Mo
Update for Windows 10 for x64-based Systems (KB44...
Microsoft Corporation
23.09.2019
372 Ko
VMware Tools
VMware, Inc.
04.11.2020
94,7 Mo
Programmes actuellement install... Taille totale : 276 Mo
5 programmes installés



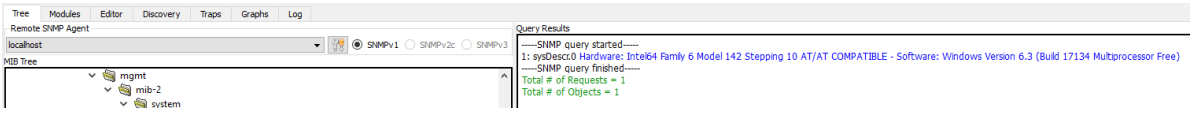
Pour configurer le service, il faut ouvrir `services.msc` (en administrateur). Afin de s'assurer que le service tourne en permanence, il faut définir un `type de démarrage` **automatique**.



Ensuite, on peut configurer le service (clic droit `Propriété`).



Ensuite depuis `SNMPb`, on peut "découvrir" le nouvel agent.



5 objets SNMP

Name:	**ifIndex**
Oid:	1.3.6.1.2.1.2.2.1.1
Composed Type:	InterfaceIndex
Base Type:	INTEGER
Status:	current
Access:	read-only
Kind:	Column
SMI Type:	OBJECT-TYPE
Size	1 .. 2147483647
Module:	IF-MIB
Description:	A unique value, greater than zero, for each interface. It is recommended that values are assigned contiguously starting from 1. The value for each interface sub-layer must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization.

Name:	**ifDescr**
Oid:	1.3.6.1.2.1.2.2.1.2
Composed Type:	DisplayString
Base Type:	OCTET STRING
Status:	current
Access:	read-only
Kind:	Column
SMI Type:	OBJECT-TYPE
Size	0 .. 255
Module:	IF-MIB
Description:	A textual string containing information about the interface. This string should include the name of the manufacturer, the product name and the version of the interface hardware/software.

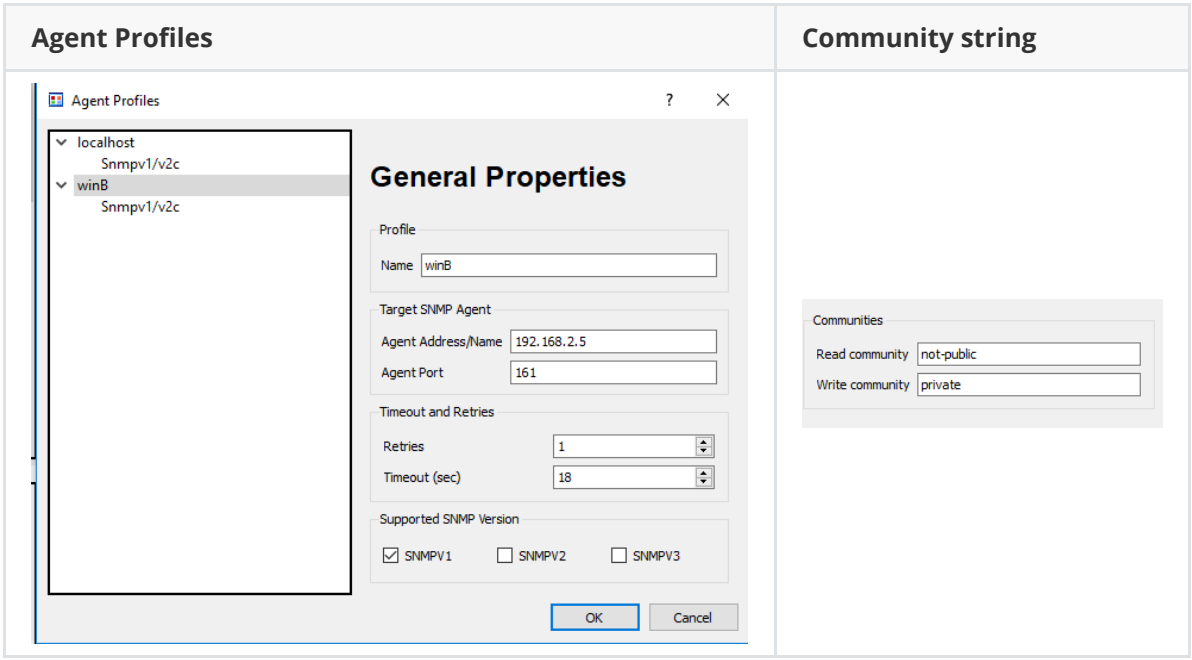
Name:	ifType
Oid:	1.3.6.1.2.1.2.2.1.3
Composed Type:	
Base Type:	
Status:	current
Access:	read-only
Kind:	Column
SMI Type:	OBJECT-TYPE
Module:	IF-MIB
Description:	The type of interface. Additional values for ifType are assigned by the Internet Assigned Numbers Authority (IANA), through updating the syntax of the IANAifType textual convention.

Name:	ifSpeed
Oid:	1.3.6.1.2.1.2.2.1.5
Composed Type:	Gauge32
Base Type:	UNSIGNED32
Status:	current
Access:	read-only
Kind:	Column
SMI Type:	OBJECT-TYPE
Size	0 .. 4294967295
Module:	IF-MIB
Description:	An estimate of the interface's current bandwidth in bits per second. For interfaces which do not vary in bandwidth or for those where no accurate estimation can be made, this object should contain the nominal bandwidth. If the bandwidth of the interface is greater than the maximum value reportable by this object then this object should report its maximum value (4,294,967,295) and ifHighSpeed must be used to report the interace's speed. For a sub-layer which has no concept of bandwidth, this object should be zero.

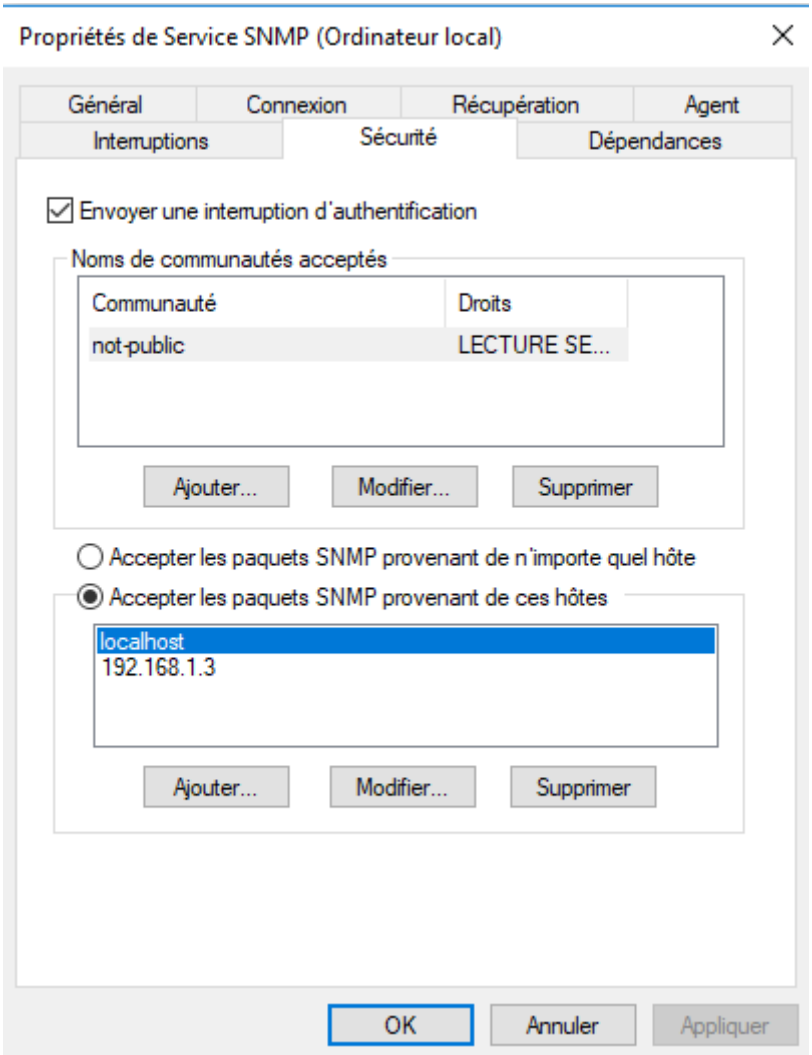
Name:	ifAdminStatus
Oid:	1.3.6.1.2.1.2.2.1.7
Composed Type:	Enumeration
Base Type:	ENUM
Status:	current
Access:	read-write
Kind:	Column
SMI Type:	OBJECT-TYPE
Value List	up (1) down (2) testing (3)
Module:	IF-MIB
Description:	The desired state of the interface. The testing(3) state indicates that no operational packets can be passed. When a managed system initializes, all interfaces start with ifAdminStatus in the down(2) state. As a result of either explicit management action or per configuration information retained by the managed system, ifAdminStatus is then changed to either the up(1) or testing(3) states (or remains in the down(2) state).

Modification de Win A pour interroger Win B

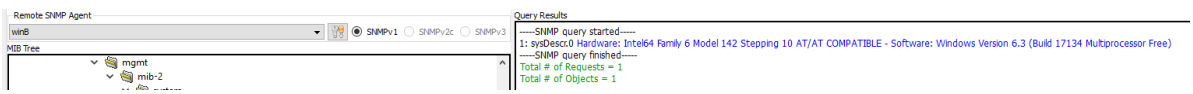
Pour permettre la machine Win A d'interroger la machine Win B, il suffit d'ajouter un nouveau `Agent Profiles` en lui spécifiant l'adresse IP de Win B. Et finalement, il faut changer la valeur de la `community string RO` à **not-public**.



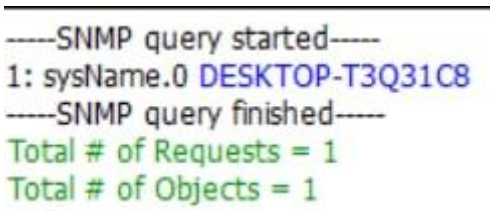
Ensuite, lors de la configuration de Win B, il a fallut ajouter Win A (192.168.1.3) dans la liste des hôtes pouvant envoyer des paquets SNMP.



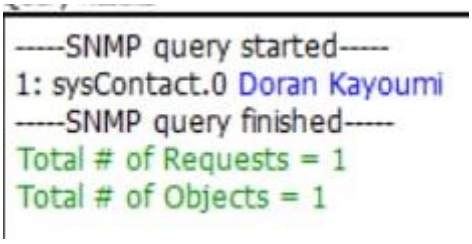
Et maintenant, si l'on interroge l'agent Win B afin d'obtenir la `description système`, on vois que l'on reçoit bien une réponse.



Interrogation de Win B

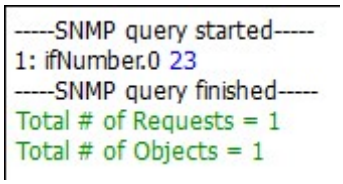


> Nom de l'équipement



> Nom du responsable de l'équipement

> Modèle de l'équipement



> Nombre d’interfaces de l'équipement

N°	Octets rentrant	Octets sortant
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	0	0
12	0	0
13	0	0
14	0	0
15	143228093	6094462
16	143228093	6167312
17	144602155	6224228
18	0	0
19	0	0
20	0	0
21	0	0
22	0	0
23	0	0

> Trafic sur chaque interfaces
> Note: Pour simplifier la récupération du trafic sur chaque interfaces, nous avons créé un petit script Powershell

```
for($i=1; $i -lt 24; ++$i) {
    echo("OutOctets");
    Get-SNMP 192.168.2.3 ifOutOctets.$i -Community not-public
    echo("InOctets");
    Get-SNMP 192.168.2.3 ifInOctets.$i -Community not-public
}
```

> A l'aide de Wireshark, capturez et présentez de manière lisible les trames lorsque la machine Windows 10 A interroge la machine Windows 10 B pour obtenir le nom de l'équipement (les champs concernant SNMP doivent être visibles et commentés).

```
data: get-request (0)
  get-request
      request-id: 1188
      error-status: noError (0)
      error-index: 0
    variable-bindings: 1 item
      1.3.6.1.2.1.1.5.0: Value (Null)
          Object Name: 1.3.6.1.2.1.1.5.0 (iso.3.6.1.2.1.1.5.0)
          Value (Null)
```

On peut voir que dans la requête, on retrouve l'Oid de sysName **1.3.6.1.2.1.1.5**.

```
get-response
    request-id: 1188
    error-status: noError (0)
    error-index: 0
  variable-bindings: 1 item
    1.3.6.1.2.1.1.5.0: 4445534b544f502d54335133314338
        Object Name: 1.3.6.1.2.1.1.5.0 (iso.3.6.1.2.1.1.5.0)
      Value (OctetString): 4445534b544f502d54335133314338
          Variable-binding-string: DESKTOP-T3Q31C8
```

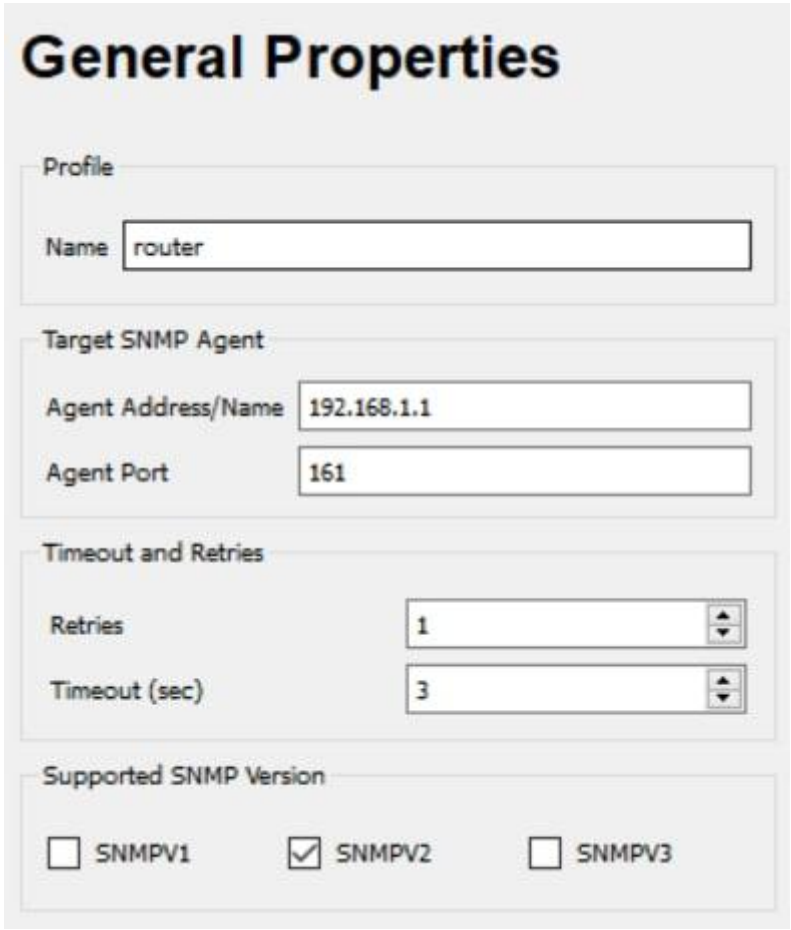
Et dans la réponse, on a le nom de la machine dans le champ **variable-binding-string**.

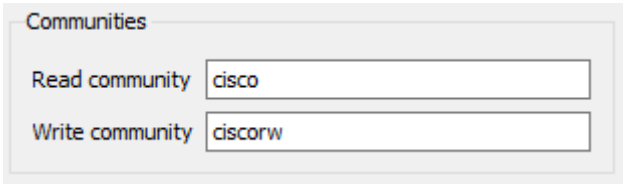
Activer et configurez l'agent SNMP sur le routeur Cisco

> Configurez le routeur cisco de manière à pouvoir le gérer via SNMPv2 (choisissez « cisco » pour community string RO et « ciscor » pour community string RW). Configurez également le routeur pour qu'il envoie ses traps snmp au manager.

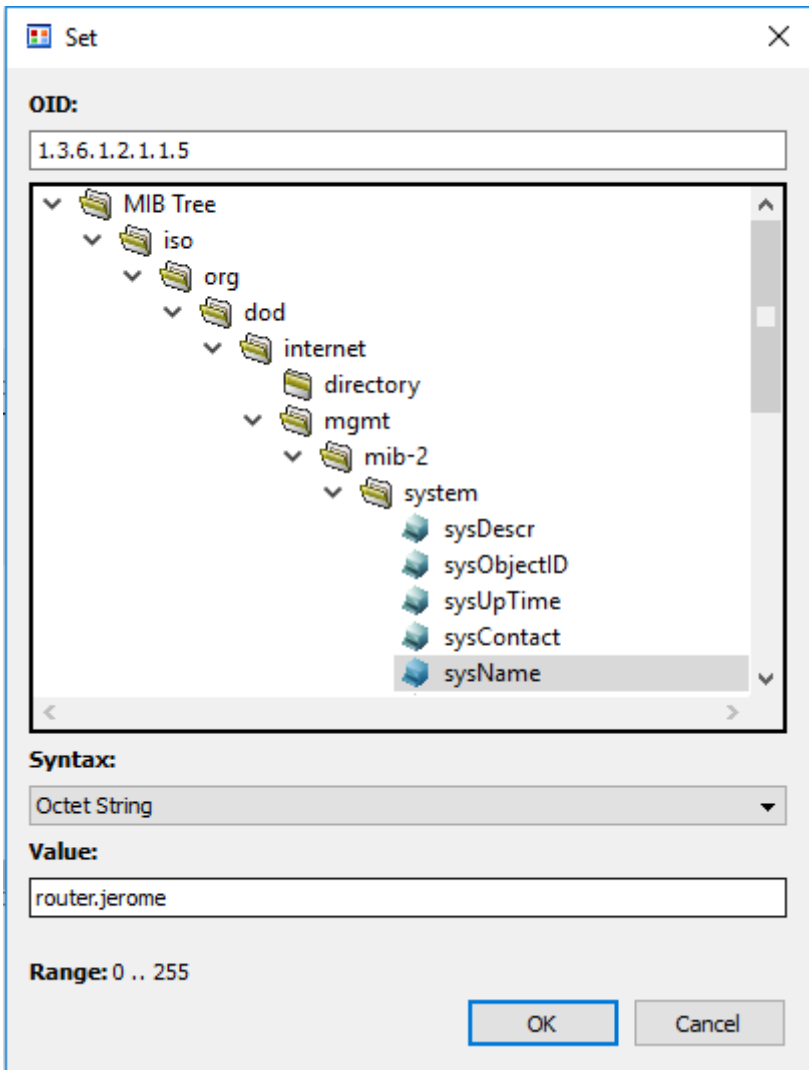
```
Router(config)#snmp-server community cisco ro
Router(config)#snmp-server community ciscorw rw
Router(config)#snmp-server con
Router(config)#snmp-server contact jerome.arn@heig-vd.ch
```

> Créez un nouveau profil dans l'application SNMPb pour pouvoir gérer votre routeur.





> Changez le nom du routeur à l'aide de l'application SNMPb (nouveau nom : router) tout en capturant/analysant les messages échangés à l'aide de Wireshark



On voit sur la capture suivante que si l'on fait une requête sur le nom du routeur. On peut confirmer le changement.

```
▼ set-request
    request-id: 1192
    error-status: noError (0)
    error-index: 0
  ▼ variable-bindings: 1 item
    ▼ 1.3.6.1.2.1.1.5.0: 726f757465722e6a65726f6d65
        Object Name: 1.3.6.1.2.1.1.5.0 (iso.3.6.1.2.1.1.5.0)
      ▼ Value (OctetString): 726f757465722e6a65726f6d65
          Variable-binding-string: router.jerome
```

> Que pouvez-vous dire sur la sécurité du protocole SNMPv2 ? Citez deux moyens d'améliorer la sécurité de notre infrastructure.

Ce n'est pas sécurisé car les messages ne sont pas authentifié. et les messages sont transmis en clair sur le réseau.

- Chiffrer les données transmissent sur le réseau
- authentification des messages

Passer à la version 3 de SNMP si l'équipement le supporte car il y a de l'authentification et du chiffrement.

> Générez une trap SNMP en déclenchant un événement sur votre routeur (un peu d'imagination...) et vérifiez que vous récupérez bien la « SNMP trap » sur l'application SNMPb.

```
router(config)#snmp-server host 192.168.1.3 version 2c cisco config
router(config)#snmp-server enable traps config
```

No	Date	Time	Timestamp	Notification Type	Message Type	Version	Agent Address	Agent port
0001	2020-11-15	17:32:03	0:18:46.46	enterprises.9.9.4...	Trap(v2)	SNMPv2c	192.168.1.1	63392

> Analysez les trames de la capture précédente et décodez la signification des différents messages SNMP en recherchant la signification du « OID code » à l'aide du SNMP Object Navigator Cisco https://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index (compte Cisco à créer si nécessaire)

```
data: snmpV2-trap (7)
  snmpV2-trap
      request-id: 11
      error-status: noError (0)
      error-index: 0
    variable-bindings: 5 items
      1.3.6.1.2.1.1.3.0: 135945
      1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.4.1.9.9.43.2.0.1 (iso.3.6.1.4.1.9.9.43.2.0.1)
          Object Name: 1.3.6.1.6.3.1.1.4.1.0 (iso.3.6.1.6.3.1.1.4.1.0)
          Value (OID): 1.3.6.1.4.1.9.9.43.2.0.1 (iso.3.6.1.4.1.9.9.43.2.0.1)
      1.3.6.1.4.1.9.9.43.1.1.6.1.3.17: 1
          Object Name: 1.3.6.1.4.1.9.9.43.1.1.6.1.3.17 (iso.3.6.1.4.1.9.9.43.1.1.6.1.3.17)
          Value (Integer32): 1
      1.3.6.1.4.1.9.9.43.1.1.6.1.4.17: 2
          Object Name: 1.3.6.1.4.1.9.9.43.1.1.6.1.4.17 (iso.3.6.1.4.1.9.9.43.1.1.6.1.4.17)
          Value (Integer32): 2
      1.3.6.1.4.1.9.9.43.1.1.6.1.5.17: 3
          Object Name: 1.3.6.1.4.1.9.9.43.1.1.6.1.5.17 (iso.3.6.1.4.1.9.9.43.1.1.6.1.5.17)
          Value (Integer32): 3
```

1.3.6.1.4.1.9.9.43.2.0.1	ciscoConfigManEvent	0	0	Notification of a configuration management event as recorded in ccmHistoryEventTable.

Windows Powershell permet de créer des scripts, utiles pour récupérer des informations de manière régulière et automatisée par exemple.

> Récupérez le nom de votre routeur à l'aide de la cmdlet adéquate.

```
PS> Get-SNMP 192.168.1.1 sysName.0 -Community cisco
```

> Configurez le routeur de manière à ce qu'il n'accepte des requêtes SNMP que de la part de votre machine Windows 10 A uniquement. Validez votre configuration en vérifiant que votre machine Windows 10 B n'y a plus accès.

```
# à l'aide d'une access list on définit la machine winA comme étant la seule à
pouvoir faire des requêtes
access-list 99 permit 192.168.1.3
access-list 99 deny any
snmp-server community cisco ro 99
snmp-server community ciscorw rw 99
```

On peut constater que les requêtes sur la machine WinB aboutissent à un timeout. Ce qui veut dire qu'elle n'a plus l'accès au routeur

Objectif 4 - MIBs privées

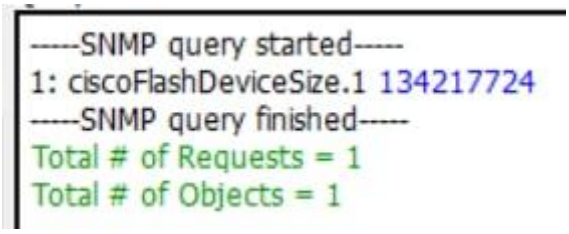
Afin d'interroger des objets spécifiques à votre équipement, vous avez besoin d'intégrer à votre manager SNMP (l'application SNMPb) les MIB privées nécessaires. Vous désirez obtenir des informations sur la mémoire flash embarquée sur votre routeur: chargez les MIBs privées nécessaires

> donnez la liste des MIBs que vous avez chargé.

- CISCO-FLASH-
- CISCO-SMI

> Note: Nous avons du ajouter `CISCO-SMI` car c'est une dépendance de `CISCO-FLASH-MIB`

> montrez le résultat obtenu en effectuant un requête depuis l'application SNMPb



> Taille de la mémoire flash embarquée sur le routeur

Objectif 5 - Configurer les agents SNMP en mode v3

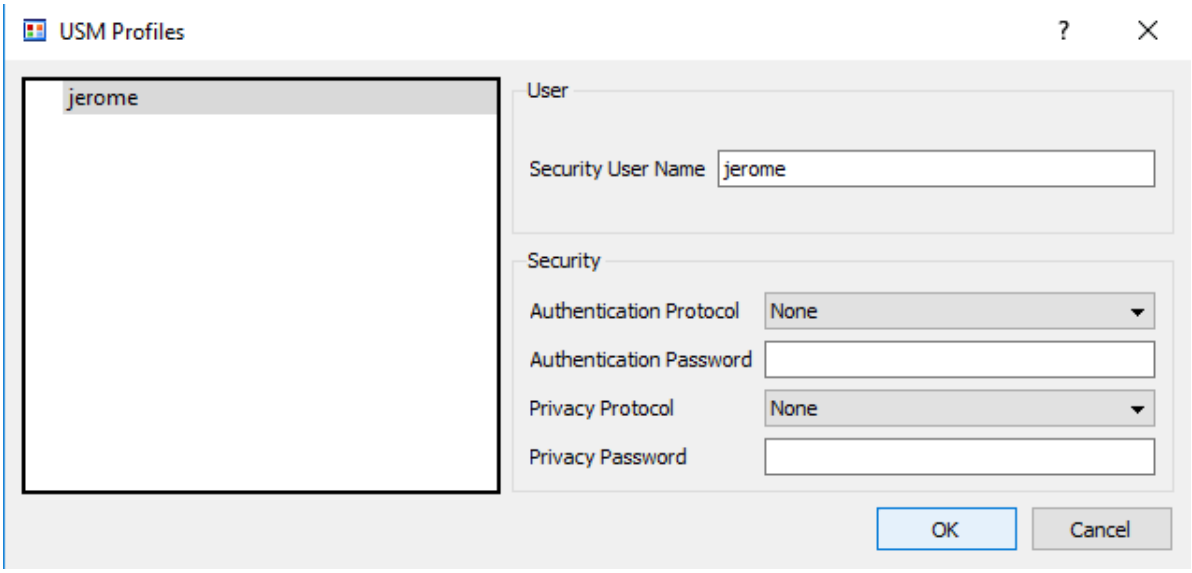
> Modifiez la configuration de votre router afin qu'il n'accepte plus que des requête SNMPv3.

```
access-list 1 permit 192.168.1.3
snmp-server group GRX v3 noauth access 1
snmp-server user jerome GRX v3
# pour supprimer l'usage de la version 1 et 2
no snmp-server community cisco
no snmp-server community ciscorw
```

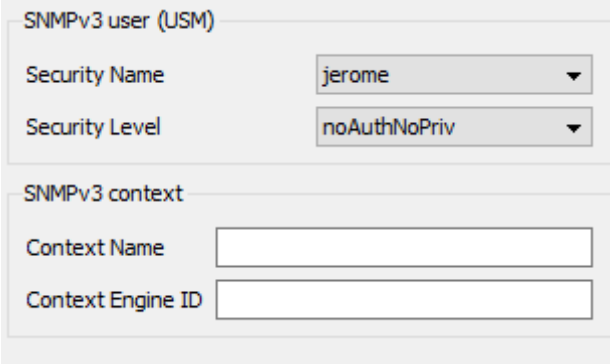
On constate que si on fait des requêtes sur le router en version 1 et 2, il y a désormais un timeout qui apparaît.

> Configurez votre application SNMPb en conséquence et montrer le résultat d'une requête sur la valeur SysUpTime (MIB-2)

Il faut d'abord créer un profil user SNMPV3. Puis dans le profil du router, cochez la case **SNMPV3**.



Dans l'onglet SnmpV3 du profil du router, sélectionner le security name qui a été paramétré auparavant ainsi que le type authentification.

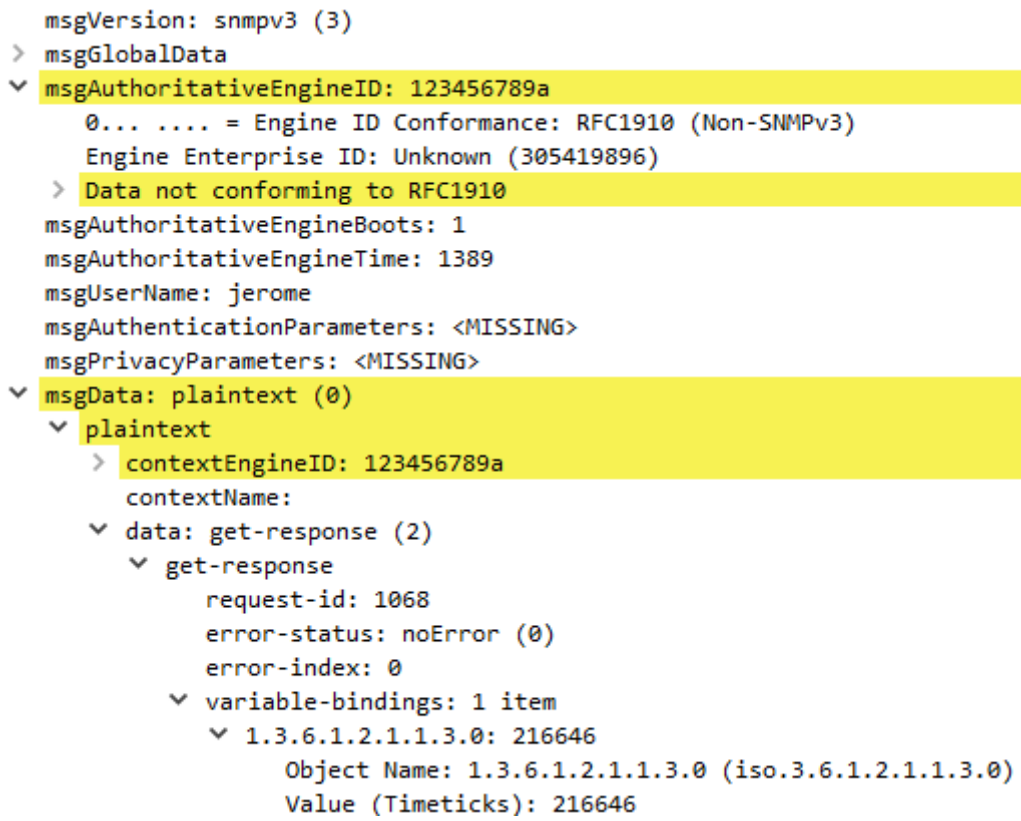


> Capturez/analysez les messages lors d'une requête SNMPv3

On peut aussi voir que dans la requête, les données du messages sont transmissent en clair.

```
msgData: plaintext (0)
  plaintext
    contextEngineID: 123456789a
        0... .... = Engine ID Conformance: RFC1910 (Non-SNMPv3)
        Engine Enterprise ID: Unknown (305419896)
      > Data not conforming to RFC1910
    contextName:
    data: get-request (0)
      get-request
          request-id: 1068
          error-status: noError (0)
          error-index: 0
        variable-bindings: 1 item
          1.3.6.1.2.1.1.3.0: Value (Null)
              Object Name: 1.3.6.1.2.1.1.3.0 (iso.3.6.1.2.1.1.3.0)
              Value (Null)
    [Response In: 3]
```

On constate que la version snmpV3 est notifié dans l'entête. Puis on voit que le nom d'utilisateur est en clair et on voit la valeur de réponse pour la requête **sysUpTime** dans l'entête data: get-response > variable-bindings.


msgVersion: snmpv3 (3)
msgGlobalData
msgAuthoritativeEngineID: 123456789a
0... .... = Engine ID Conformance: RFC1910 (Non-SNMPv3)
Engine Enterprise ID: Unknown (305419896)
Data not conforming to RFC1910
msgAuthoritativeEngineBoots: 1
msgAuthoritativeEngineTime: 1389
msgUserName: jerome
msgAuthenticationParameters: <MISSING>
msgPrivacyParameters: <MISSING>
msgData: plaintext (0)
plaintext
contextEngineID: 123456789a
contextName:
data: get-response (2)
get-response
request-id: 1068
error-status: noError (0)
error-index: 0
variable-bindings: 1 item
1.3.6.1.2.1.1.3.0: 216646
Object Name: 1.3.6.1.2.1.1.3.0 (iso.3.6.1.2.1.1.3.0)
Value (Timeticks): 216646