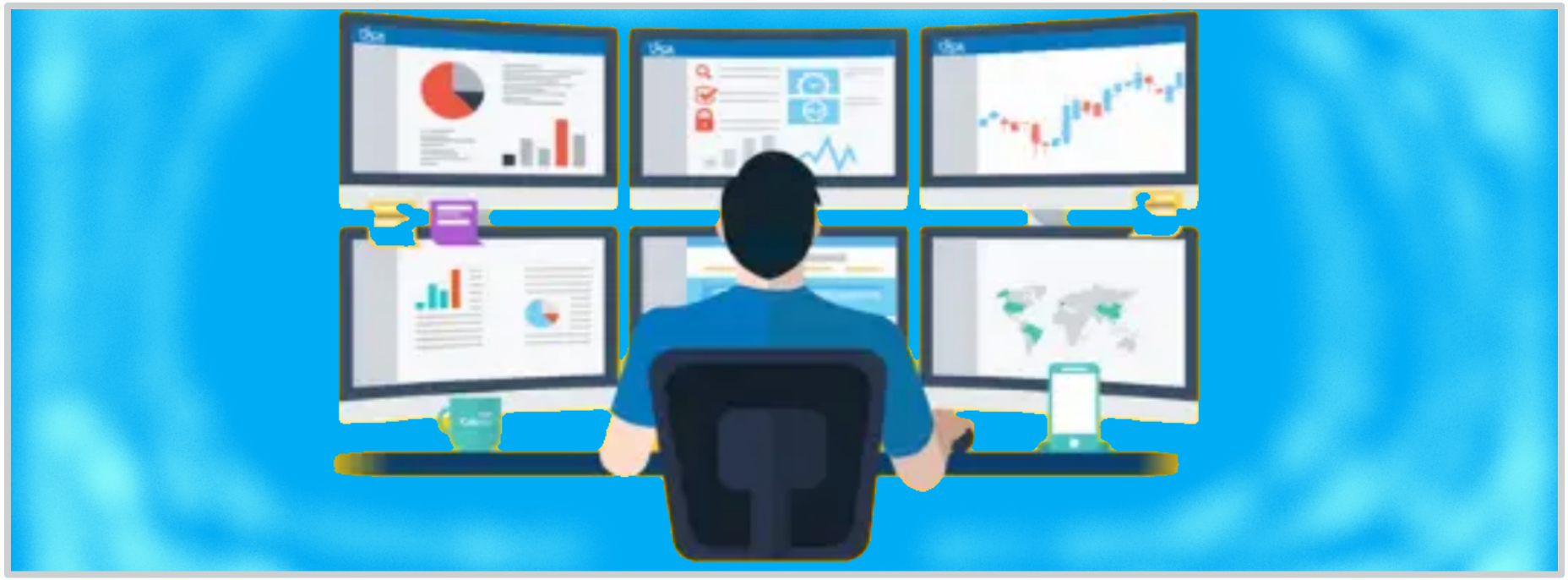


SNMP

Rappel et approfondissement

SNMP & MIB

- SNMP
  - Protocole spécifique à la supervision
  - Simple Network Management Protocol
  - Simple, car il embarque seulement 6 opérations
    - "get" : permet au superviseur de récupérer une information de la MIB
    - "getnext" : permet au superviseur de récupérer l'information suivante de la MIB
    - "set" : permet d'écrire une information dans la MIB
    - "getbulk" : permet de récupérer en masse des informations de la MIB
    - "inform" : permet de transfert de trap vers un autre superviseur
    - "trap" : permet la transmission d'alerte à partir de l'agent SNMP

- MIB
  - Base de données des informations de l'agent
  - Management Information Base
  - 2 niveaux
    - Arborescence commune à tout équipement
      - ✓ MIB-II, HOST-RESOURCES, …
    - Arborescence éditeurs
      - ✓ Juniper, Cisco, …
  - Complexité forte
    - Des milliers d'informations
    - Parfois beaucoup de traps

SNMP

- S'appuie sur les datagrammes UDP (User Datagram Protocol)
  - Pas d'acquittement. Une trame perdue ne sera pas connue ni par son récepteur ni par son émetteur.
- 3 versions
  - V1 : en dépréciation
  - V2c : encore présent, mais ne permet pas le chiffrement
  - V3 : permet le chiffrement
- Met en jeu :
  - Un "manager" SNMP, appelé en anglais NMS pour Network Management System (NMS)
  - Un "agent" SNMP

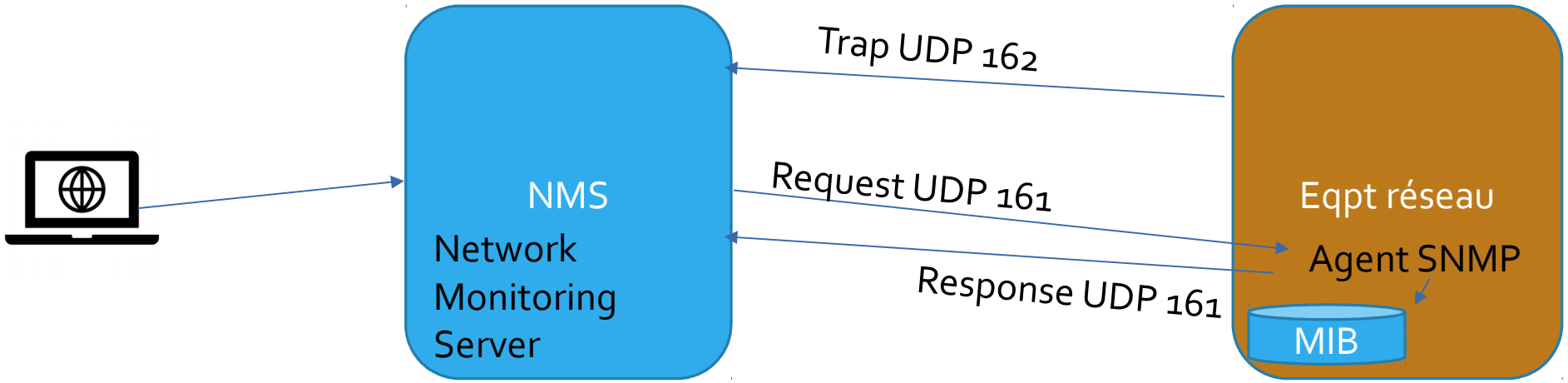
Utilitaires

- Distribution "net-snmp" avec les commandes les plus courantes
  - "snmpget" : récupération d'une information de la MIB
  - "snmpset" : écrit une information dans la MIB
  - "snmpwalk" : récupération d'une branche de la MIB
  - "snmptrap" : envoi d'un trap
  - ...

Configuration de l'agent SNMP

- L'agent doit autoriser le gestionnaire SNMP (NMS) à l'interroger
  - Via une configuration de type ACL (ACcess List) et une communauté en V2
  - Via une configuration de type ACL, une identité et des méthodes de chiffrement des phases :
    1. d'authentification
    2. d'échanges de données

SNMP Compléments



MIB & ACL – SNMP v1 et v2c

ACL : Access ControL

Défaut pour les versions 1 et 2c du protocole

com2sec notConfigUser default public

group notConfigGroup v1 notConfigUser

group notConfigGroup v2c notConfigUser

Visibilité :

view systemview included .1.3.6.1.2.1.1

view systemview included .1.3.6.1.2.1.25.1.1

access notConfigGroup "" any noauth exact systemview none none

Get SNMP

- Requête SNMP de la description du système dans la MIB

$ snmpget -v 2c -On -c public 127.0.0.1 .1.3.6.1.2.1.1.1.0

.1.3.6.1.2.1.1.1.0 = STRING: Linux zce.utak.fr 4.18.0-348.12.2.el8_5.x86_64 #1 SMP Wed Jan 19 17:53:40 UTC 2022 x86_64

$ snmpget -v 2c -c public 127.0.0.1 .1.3.6.1.2.1.1.1.0

SNMPv2-MIB::sysDescr.0 = STRING: Linux zce.utak.fr 4.18.0-348.12.2.el8_5.x86_64 #1 SMP Wed Jan 19 17:53:40 UTC 2022 x86_64

$ snmpwalk -v 2c -c public 127.0.0.1 .1.3.6.1.2.1.1.1

SNMPv2-MIB::sysDescr.0 = STRING: Linux zce.utak.fr 4.18.0-348.12.2.el8_5.x86_64 #1 SMP Wed Jan 19 17:53:40 UTC 2022 x86_64

MIB & ACL

On restreint l'accès à notre "NMS"

ACL : Access ControL

com2sec mynms 128.78.148.17 P@ss-2-Lecture

group notConfigGroup v2c mynms

Visibilité :

view systemview included .1.3.6.1.2.1.1

view systemview included .1.3.6.1.2.1.25.1.1

access notConfigGroup "" any noauth exact systemview none none

Get SNMP

- Requête SNMP de la description du système dans la MIB

$ snmpget -v 2c -On -c P@ss-2-Lecture zce.utak.fr .1.3.6.1.2.1.1.1.0

.1.3.6.1.2.1.1.1.0 = STRING: Linux zce.utak.fr 4.18.0-348.12.2.el8_5.x86_64 #1 SMP Wed Jan 19 17:53:40 UTC 2022 x86_64

$ snmpget -v 2c -c public zce.utak.fr .1.3.6.1.2.1.1.1.0

SNMPv2-MIB::sysDescr.0 = STRING: Linux zce.utak.fr 4.18.0-348.12.2.el8_5.x86_64 #1 SMP Wed Jan 19 17:53:40 UTC 2022 x86_64

$ snmpwalk -v 2c -c public zce.utak.fr .1.3.6.1.2.1.1.1

SNMPv2-MIB::sysDescr.0 = STRING: Linux zce.utak.fr 4.18.0-348.12.2.el8_5.x86_64 #1 SMP Wed Jan 19 17:53:40 UTC 2022 x86_64

MIB & ACL – SNMP v3

Création de l'utilisateur par commande en ligne :

```
$ sudo net-snmp-create-v3-user -ro -A pwdPass01 -a SHA -X keyPass01 -x AES totor
```

On obtient l'entrée suivante dans le fichier /etc/snmp/snmpd.conf

```
rouser totor
```

On restreint l'accès à une vue limitée de la MIB en modifiant la directive

```
rouser totor priv -V systemview
view    systemview    included   .1.3.6.1.2.1.1
```

On vérifie l'accès

```
$ snmpwalk -u totor -A pwdPass01 -a SHA -X keyPass01 -x AES -l authPriv zce.utak.fr -v3 .1
```

SNMP

Rappel et approfondissement

1

Ce document rappelle et approfondie les éléments sur le protocole ICMP et ses déclinaisons dans les outils de base.

SNMP & MIB

- SNMP
  - Protocole spécifique à la supervision
  - Simple Network Management Protocol
  - Simple, car il embarque seulement 6 opérations
    - "get" : permet au superviseur de récupérer une information de la MIB
    - "getnext" : permet au superviseur de récupérer l'information suivante de la MIB
    - "set" : permet d'écrire une information dans la MIB
    - "getbulk" : permet de récupérer en masse des informations de la MIB
    - "inform" : permet de transfert de trap vers un autre superviseur
    - "trap" : permet la transmission d'alerte à partir de l'agent SNMP

- MIB
  - Base de données des informations de l'agent
  - Management Information Base
  - 2 niveaux
    - Arborescence commune à tout équipement
      - ✓ MIB-II, HOST-RESOURCES, ...
    - Arborescence éditeurs
      - ✓ Juniper, Cisco, ...
  - Complexité forte
    - Des milliers d'informations
    - Parfois beaucoup de traps

UTAK

SNMP

- S'appuie sur les datagrammes UDP (User Datagram Protocol)
  - Pas d'acquittement. Une trame perdue ne sera pas connue ni par son récepteur ni par son émetteur.
- 3 versions
  - V1 : en dépréciation
  - V2c : encore présent, mais ne permet pas le chiffrement
  - V3 : permet le chiffrement
- Met en jeu :
  - Un "manager" SNMP, appelé en anglais NMS pour Network Management System (NMS)
  - Un "agent" SNMP

3

UTAK

Malgré le titre de l'article, celui-ci est complet et source d'informations :

Le ping pour les débutants | IT-Connect


Utilitaires

- Distribution "net-snmp" avec les commandes les plus courantes
  - "snmpget" : récupération d'une information de la MIB
  - "snmpset" : écrit une information dans la MIB
  - "snmpwalk" : récupération d'une branche de la MIB
  - "snmptrap" : envoi d'un trap
  - ...

UTAK

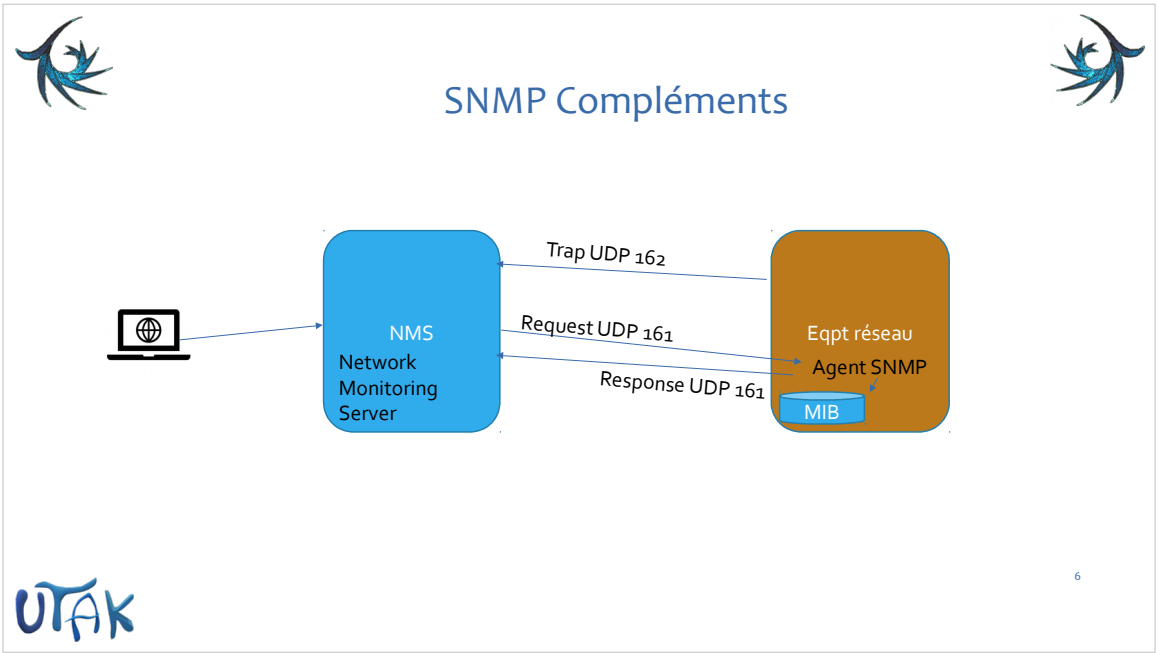
4

Liste exhaustive des commandes :
snmpget(1), snmpgetnext(1), snmpset(1), snmpbulkget(1), snmpbulkwalk(1), snmpwalk(1), snmptable(1), snmpnetstat(1), snmpdelta(1), snmptrap(1), snmpinform(1), snmpusm(1), snmpstatus(1), snmptest(1), snmp.conf(5).

Configuration de l'agent SNMP

- L'agent doit autoriser le gestionnaire SNMP (NMS) à l'interroger
  - Via une configuration de type ACL (ACcess List) et une communauté en V2
  - Via une configuration de type ACL, une identité et des méthodes de chiffrement des phases :
    1. d'authentification
    2. d'échanges de données

UTAK



NMS : Network Management Server

MIB & ACL – SNMP v1 et v2c

ACL : Access ControL

Défaut pour les versions 1 et 2c du protocole

com2sec notConfigUser default public

group notConfigGroup v1 notConfigUser

group notConfigGroup v2c notConfigUser

Visibilité :

view systemview included .1.3.6.1.2.1.1

view systemview included .1.3.6.1.2.1.25.1.1

access notConfigGroup "" any noauth exact systemview none none

UTAK

Get SNMP

- Requête SNMP de la description du système dans la MIB

$ snmpget -v 2c -On -c public 127.0.0.1 .1.3.6.1.2.1.1.1.0

.1.3.6.1.2.1.1.1.0 = STRING: Linux zce.utak.fr 4.18.0-348.12.2.el8_5.x86_64 #1 SMP Wed Jan 19 17:53:40 UTC 2022 x86_64

$ snmpget -v 2c -c public 127.0.0.1 .1.3.6.1.2.1.1.1.0

SNMPv2-MIB::sysDescr.0 = STRING: Linux zce.utak.fr 4.18.0-348.12.2.el8_5.x86_64 #1 SMP Wed Jan 19 17:53:40 UTC 2022 x86_64

$ snmpwalk -v 2c -c public 127.0.0.1 .1.3.6.1.2.1.1.1

SNMPv2-MIB::sysDescr.0 = STRING: Linux zce.utak.fr 4.18.0-348.12.2.el8_5.x86_64 #1 SMP Wed Jan 19 17:53:40 UTC 2022 x86_64

8

Option O (grand O et pas zéro)

MIB & ACL

On restreint l'accès à notre "NMS"

ACL : Access ControL

com2sec mynms 128.78.148.17 P@ss-2-Lecture

group notConfigGroup v2c mynms

Visibilité :

view systemview included .1.3.6.1.2.1.1

view systemview included .1.3.6.1.2.1.25.1.1

access notConfigGroup "" any noauth exact systemview none none

UTAK

Get SNMP

- Requête SNMP de la description du système dans la MIB

$ snmpget -v 2c -On -c P@ss-2-Lecture zce.utak.fr .1.3.6.1.2.1.1.1.0

.1.3.6.1.2.1.1.1.0 = STRING: Linux zce.utak.fr 4.18.0-348.12.2.el8_5.x86_64 #1 SMP Wed Jan 19 17:53:40 UTC 2022 x86_64

$ snmpget -v 2c -c public zce.utak.fr .1.3.6.1.2.1.1.1.0

SNMPv2-MIB::sysDescr.0 = STRING: Linux zce.utak.fr 4.18.0-348.12.2.el8_5.x86_64 #1 SMP Wed Jan 19 17:53:40 UTC 2022 x86_64

$ snmpwalk -v 2c -c public zce.utak.fr .1.3.6.1.2.1.1.1

SNMPv2-MIB::sysDescr.0 = STRING: Linux zce.utak.fr 4.18.0-348.12.2.el8_5.x86_64 #1 SMP Wed Jan 19 17:53:40 UTC 2022 x86_64

10

Option O (grand O et pas zéro)

MIB & ACL – SNMP v3

Création de l'utilisateur par commande en ligne :

```
$ sudo net-snmp-create-v3-user -ro -A pwdPass01 -a SHA -X keyPass01 -x AES totor
```

On obtient l'entrée suivante dans le fichier /etc/snmp/snmpd.conf

```
rouser totor
```

On restreint l'accès à une vue limitée de la MIB en modifiant la directive

```
rouser totor priv -V systemview
view   systemview   included   .1.3.6.1.2.1.1
```

On vérifie l'accès

```
$ snmpwalk -u totor -A pwdPass01 -a SHA -X keyPass01 -x AES -l authPriv zce.utak.fr -v3 .1
```


UTAK