Info0911

Intro SNMP

Introduction à SNMP

- SNMP
  - Simple Network Management Protocol
    - RFC 1157
  - protocole de supervision de réseau
- Objectifs
  - gestion des équipements du réseau à distance
  - récupération d'informations
  - configuration
  - diagnostique de pannes

Versions de SNMP

- SNMP v1
  - 1988 normalisation IETF (RFC 1157)
  - intégré depuis dans la majorité des entités connectables
  - mécanisme de sécurité limité à une chaîne de caractères
- SNMP v2
  - v2p, v2c, v2u, v2*
  - non issu d'un consensus de normalisation
  - La version 2c s'est imposé comme 'de facto'
- SNMPv3
  - mars 2002
  - intégration des éléments de sécurité :
    - Chiffrage, authentification plus élaborée
    - Droits spécifiques pour les opérations

Que surveiller avec SNMP

- Équipements
  - Équipements réseau (routeurs, etc)
  - Serveurs, machines de bureau
  - Imprimantes
- Quelles informations
  - info de fonctionnement (upTime)
  - Info matériel (processeur, interfaces)
  - Info système (version, installation)
  - Info statistique (charge, interfaces)

Structure d'un système de supervision

- Principe
  - échange d'informations entre des entités
  - collecte d'informations demandées
  - réception d'alertes (trap)
- Eléments
  - équipements gérés (managed devices)
  - Agents
  - systèmes de management réseau (network management systems - NMS)

Équipements Gérés

- Managed Devices
  - éléments de réseau
    - hub, routeur, serveur
- Dotés d'objets de gestion (managed objects)
  - informations sur le matériel
  - éléments de configuration
  - informations statistiques

Agents

- Agents SNMP
  - application de gestion de réseau
  - résidant dans un périphérique
  - assure la transmission des informations
    - collecte des données locales
    - mise en forme des données

Système de Gestion de Réseau

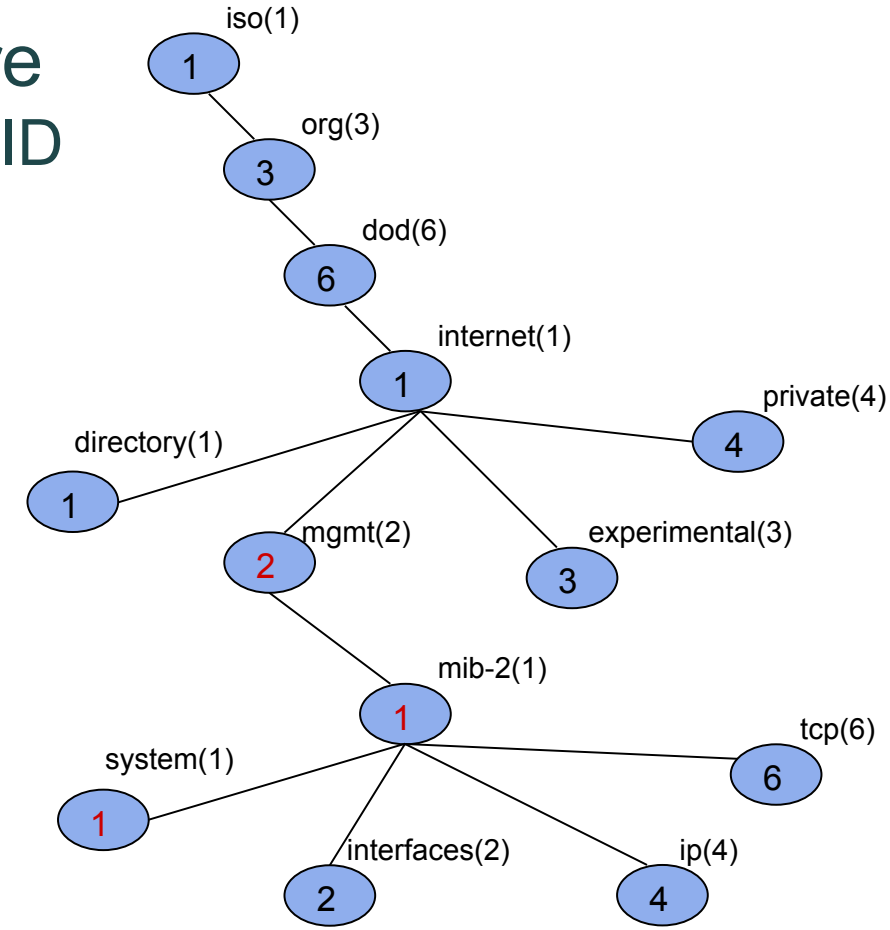
- Network Management Systems (NMS)
  - console de l'administrateur
  - gestion distante des unités du réseau
  - collecte d'informations
    - requêtes / réponses
  - configuration et modification

Représentation des Informations

- MIB (Management Information Base)
  - collection d'objets
  - structuration en base de données virtuelle
  - normalisation de la MIB
  - extensibilité de la base
    - possibilité de charger des "structures spécifiques"
    - adaptation aux spécificités des entités
    - extension offertes par les constructeurs

MIB – Management Information Base

- Base de donnée en arbre
  - Chaque élément a un OID (object ID)
    - Example .1.3.6.1.2.1.1



MIB – Management Information Base

- Format
  - Format ASN-1

- OBJECT-TYPE
  - String qui décrit l'objet MIB
  - Object IDentifier (OID)
- SYNTAX
  - Définie le type d'information stockée
- ACCESS
  - READ-ONLY, READ-WRITE
- STATUS
  - Indique la pertinence de l'information
- DESCRIPTION

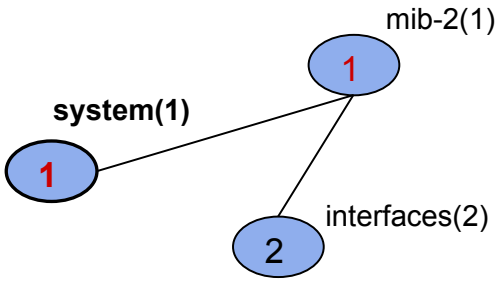
Objet MIB standard :

sysUpTime **OBJECT-TYPE**
SYNTAX INTEGER
ACCESS read-only
STATUS mandatory
DESCRIPTION
"The time (in hundredths of a second) since the
network management portion of the system was last re-initialized."
::= {system 3}

MIB – Management Information Base

system(1) group

- Contains objects that describe some basic information on an entity.
- An entity can be the agent itself or the network object that the agent is on.

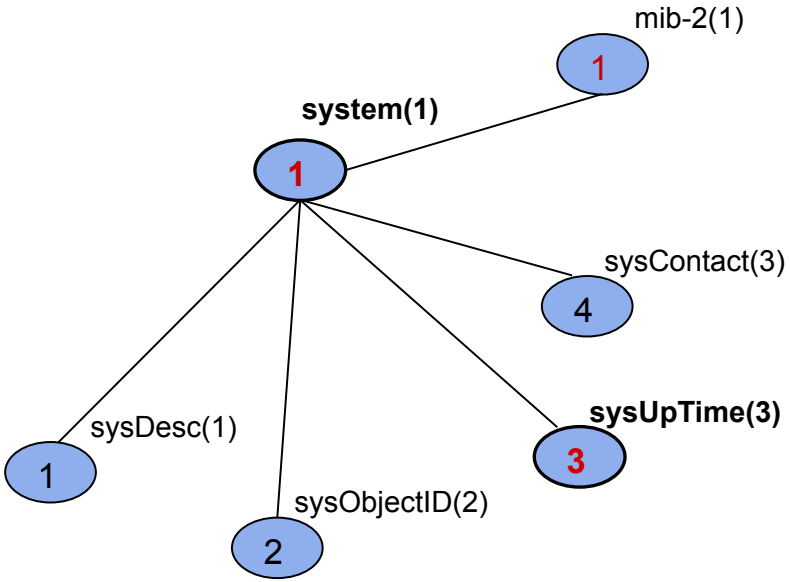


system(1) group objects

- **sysDescr(1)** → Description of the entity.
- **sysObjectID(2)** → Vendor defined OID string.
- **sysUpTime(3)** → Time since net-mgt was last re-initialised.
- **sysContact(4)** → Name of person responsible for the entity.

MIB – Management Information Base

MIB - tree view

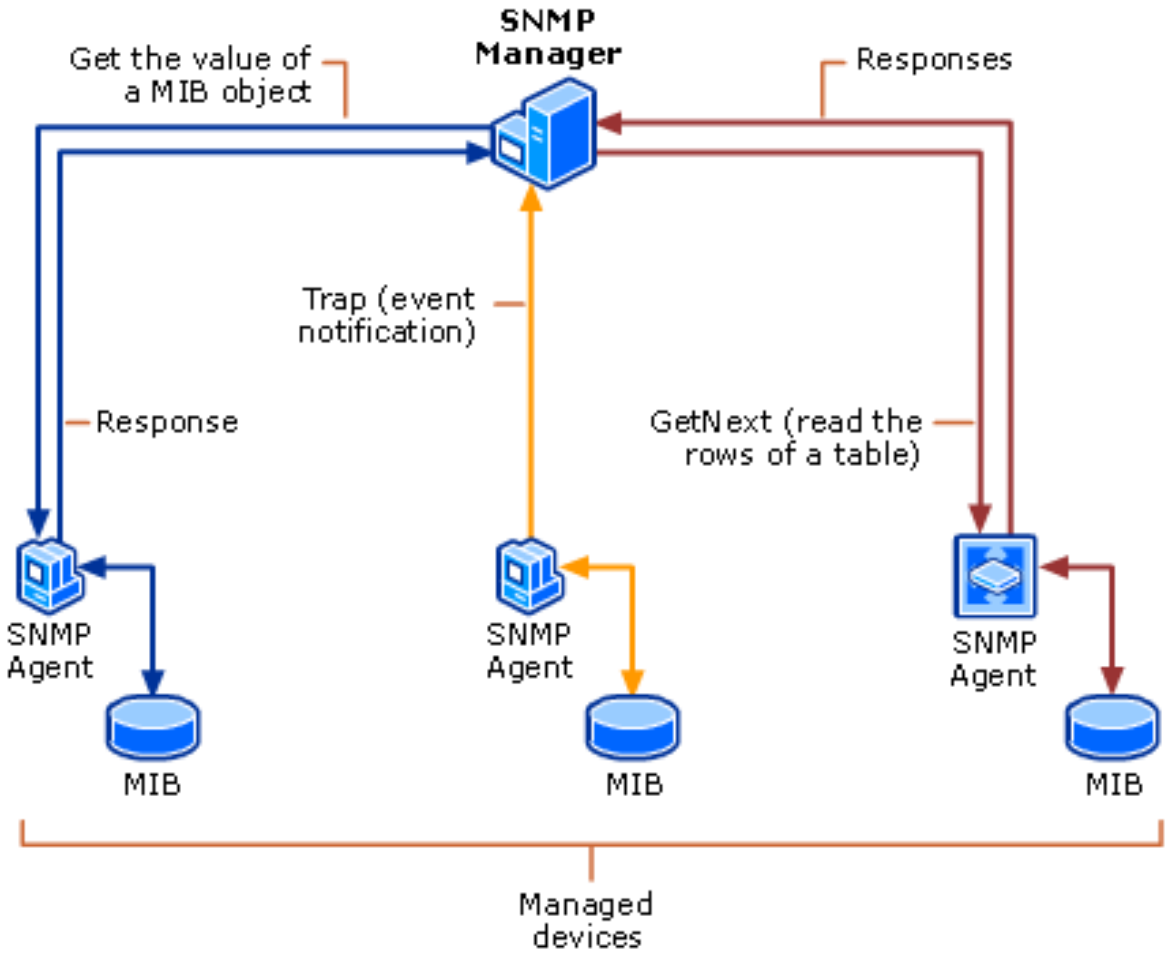


MIB - syntax view

sysUpTime **OBJECT-TYPE**
SYNTAX INTEGER
ACCESS read-only
STATUS mandatory
DESCRIPTION
"The time (in hundredths of a second) since the
network management portion of the system was last re-initialized."
::= {system 3}

Et le protocole SNMP ?

- Protocole qui permet l'interrogation de la base MIB
  - Généralement associé à UDP
- Communication entre les agents et le NMS
  - Requêtes/réponses (port 161)
  - Traps (port 162)


SNMP
Manager
Get the value of
a MIB object
Responses
Trap (event
notification)
Response
GetNext (read the
rows of a table)
SNMP
Agent
SNMP
Agent
SNMP
Agent
MIB
MIB
MIB
Managed
devices

Requêtes

- GetRequest
  - recherche d'une variable sur un agent
- GetNextRequest
  - recherche de la variable suivante
- GetBulk
  - recherche d'une ensemble de variables
- SetRequest
  - modification d'une variable sur un agent

Réponses

- GetResponse
  - structure unique d'une réponse
  - ajout de noSuchObject en cas d'erreur
- Trap
  - message à l'initiative des agents
  - alertes possibles :
    - ColdStart
    - WarmStart
    - LinkDown
    - LinkUp
    - AuthentificationFailure
    - Alertes spécifiques aux fabricants

Commandes SNMP

- SNMP contient 5 différents types de commandes :

1. GetRequest
2. GetNextRequest
3. GetResponse
4. SetRequest
5. Trap

La commande GetRequest

- GetRequest
  - Commande la plus utilisée
  - Utilisée pour intérroger un agent spécifique à propos d'un objet MIB précis
  - Le NMS envoie une requête par type d'objet (OID)
  - Comment savoir combien d'objets (réponses) on aura ?

Commande GetNextRequest

- GetNextRequest
  - Le NMS utilise GetNextRequest pour parcourir (walk) la base MIB
  - Son implémentation doit retourner le OID et la valeur de l'objet que suit celui demandé
  - Une fois que l'agent répond, le NMS peut incrémenter son compteur et faire une autre demande GetNextRequet
  - Ce processus continue jusqu'à ce que l'OID de l'objet change, indiquant la fin de la table

Commande GetResponse

- GetResponse
  - C'est le paquet de réponse aux commandes GetRequet, GetNextRequet ou SetRequet

Commande SetRequest

- SetRequest
  - Envoyé par un NMS qui veut changer une valeur sur la MIB
  - Exemple
    - Un GetRequest sur le serveur Cosy demandant sysLocation.0 peut avoir comme réponse "DptMMI"
    - Si le serveur est déplacé, la commande SetRequest peut être utilisée pour mettre à jour cette valeur ("CRI")
  - Il faut avoir les droits de modification sur la MIB

Commande Trap

- Trap
  - Notification asynchrone
  - Les agents peuvent être programmés pour envoyer des messages Trap lors de certains évenements
  - Exemples :
    - Reboot de la machine
    - Température qui dépasse une limite
    - Lien réseau qui tombe

La sécurité avec SNMP

- SNMPv1/v2 Community
  - 3 types :
    - READ-ONLY : Seulement Get et GetNext
    - READ-WRITE : Get, GetNext et Set
    - TRAP : permet l'envoi d'une Trap
- SNMP v3
  - authentification
  - localisation des mots de passe
  - Cryptage
  - estampillage du temps

Manipulation d'une MIB

- Avec le terminal Unix
- Accès aux OID
  - Commande "snmptranslate"

```
snmptranslate .1.3.6.1.2.1.1.3.0
   SNMPv2-MIB::sysUpTime.0
snmptranslate -On SNMPv2-MIB::system.sysUpTime.0
   .1.3.6.1.2.1.1.3.0
```

Accès aux Données

- Snmpget

```
snmpget -c demopublic -v 2c test.net-snmp.org
system.sysUpTime.0
    sysUpTimeInstance = Timeticks: (428202300) 49 days,
    13:27:03.00Snmpgetnext

snmpgetnext -v 2c -c demopublic test.net-snmp.org
system.sysUpTime.0
    sysContact.0 = STRING: Net-SNMP Coders <net-snmp-
    coders@lists.sourceforge.net>
```

Accès aux Données

- Snmpwalk

```
snmpwalk -c demopublic -v 2c test.net-snmp.org system
    SNMPv2-MIB::sysDescr.0 = STRING: test.net-snmp.org
    SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
    DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (428223981) 49
    days, 13:30:39.81
    SNMPv2-MIB::sysContact.0 = STRING: Net-SNMP Coders <net-snmp-
    coders@lists.sourceforge.net>
    SNMPv2-MIB::sysName.0 = STRING: test.net-snmp.org
    SNMPv2-MIB::sysLocation.0 = STRING: Undisclosed
    SNMPv2-MIB::sysORLastChange.0 = Timeticks: (1) 0:00:00.01
    SNMPv2-MIB::sysORID.1 = OID: SNMPv2-MIB::snmpMIB
    SNMPv2-MIB::sysORID.2 = OID: SNMP-VIEW-BASED-ACM-
    MIB::vacmBasicGroup
    SNMPv2-MIB::sysORID.3 = OID: SNMP-MPD-MIB::snmpMPDMIBObjects.3.1.1
    SNMPv2-MIB::sysORID.4 = OID: SNMP-USER-BASED-SM-
    MIB::usmMIBCompliance
    SNMPv2-MIB::sysORID.5 = OID: SNMP-FRAMEWORK-
    MIB::snmpFrameworkMIBCompliance
    …
```

NIS

Network Information Service

- Protocole client serveur développé par Sun
  - Objectif : centralisation d'informations sur un réseau UNIX
  - Anciennement connu comme "yellow pages"
- NIS a pour objectif la distribution des informations contenues dans des fichiers de configuration
  - noms d'hôte (/etc/hosts)
  - les comptes utilisateurs (/etc/passwd)
  - etc

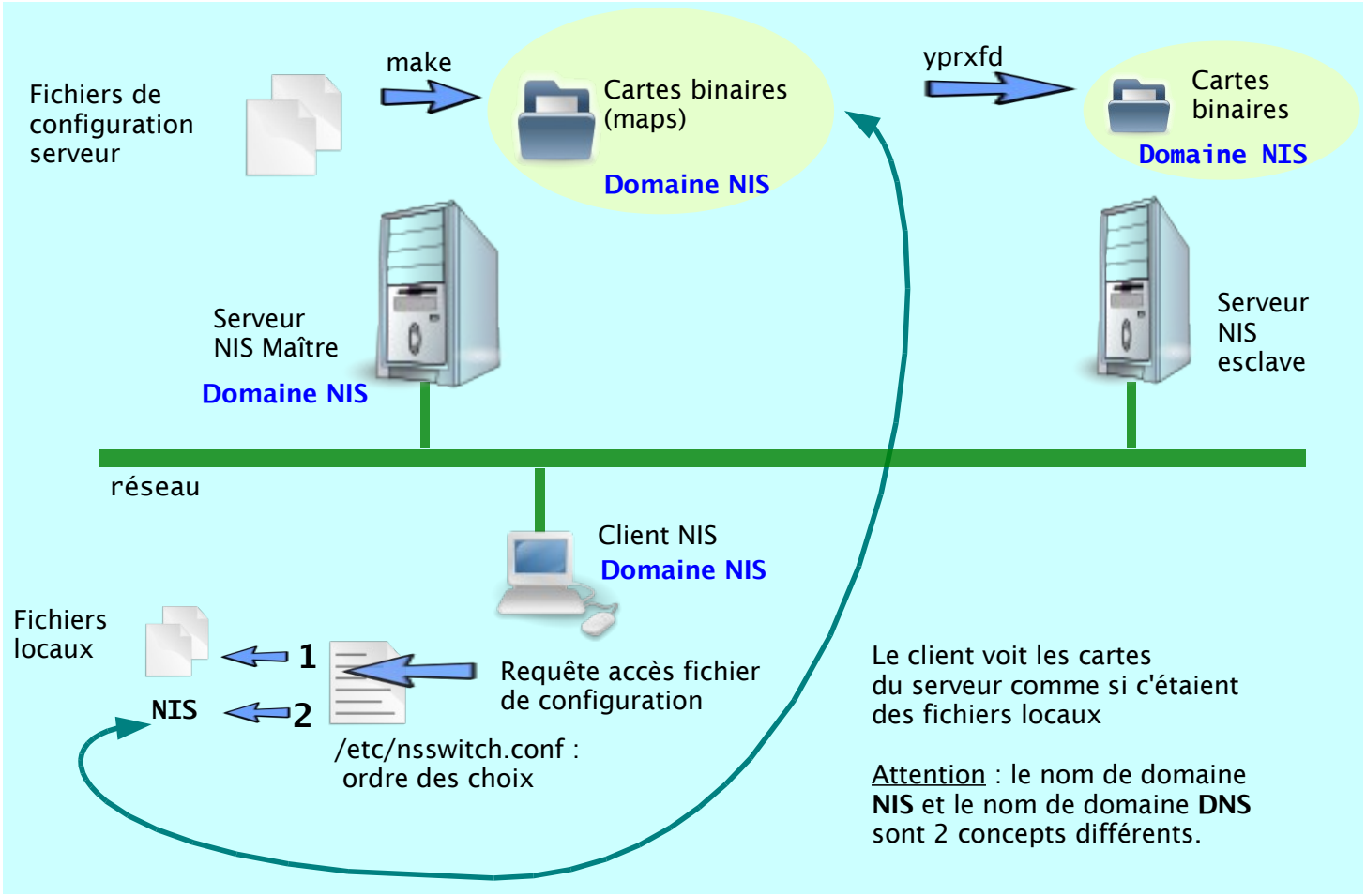
Network Information Service

- Un serveur NIS et tous les clients NIS appartiennent au même domaine NIS
- Aujourd'hui, NIS est de plus en plus abandonné
  - Remplacé par les protocoles LDAP, Kerberos, RADIUS ou autres
    - plus sécurisées et compatibles avec des réseaux hétérogènes

Architecture

- Services/démons utilisés par le service NIS :
- portmap
  - mise en correspondance numéro de ports TCP/IP <-> numéro de processus RPC (voir /etc/rpc pour les numéros réservés)
- Côté serveur :
  - ypserv - implémente le serveur NIS
  - yppasswd - permet de changer un mot de passe sur le serveur NIS depuis un client NIS (démon rpc.yppasswd)
  - Ypxfrd - accélère les transferts entre serveur maître et esclave (démon rpc.ypxfrd)
- Côté client:
  - ypbind - implémente le client NIS

NIS : Principes



Configuration d'un serveur NIS

- Rajoutez la ligne suivante à /etc/hosts.allow :
  - portmap ypserv ypbind : list of IP addresses
- Installez NIS :
  - sudo apt-get install portmap nis
  - Editer /etc/default/portmap et decommenter la ligne ARGS="-i 127.0.0.1"
  - Editer /etc/default/nis et decommenter la ligne NISSERVER = master
  - Editer /etc/yp.conf et rajouter une ligne :
    - domain <domainname> server <servername>
  - Editer /var/yp/Makefile si nécessaire
  - Edit /etc/ypserv.securenets pour limiter l'accès :
    - host 192.168.1.1
    - host 192.168.1.2
  - IMPORTANT!!!: supprimer la ligne 0.0.0.0

NIS Server Configuration

- Générez la base de données NIS

  sudo /usr/lib/yp/ypinit -m
- Réinitialisez le tout :

  sudo /etc/init.d/portmap restart

  sudo /etc/init.d/nis restart
- Si vous changez quelque chose (rajouter un utilisateur) :

  sudo make -C /var/yp

Résolution de problèmes

- Utiliser **ypwhich** pour rechercher un utilisateur et vérifier à quel serveur le client est connecté
- Utiliser ypcat pour vérifier se les données NIS sont correctes.

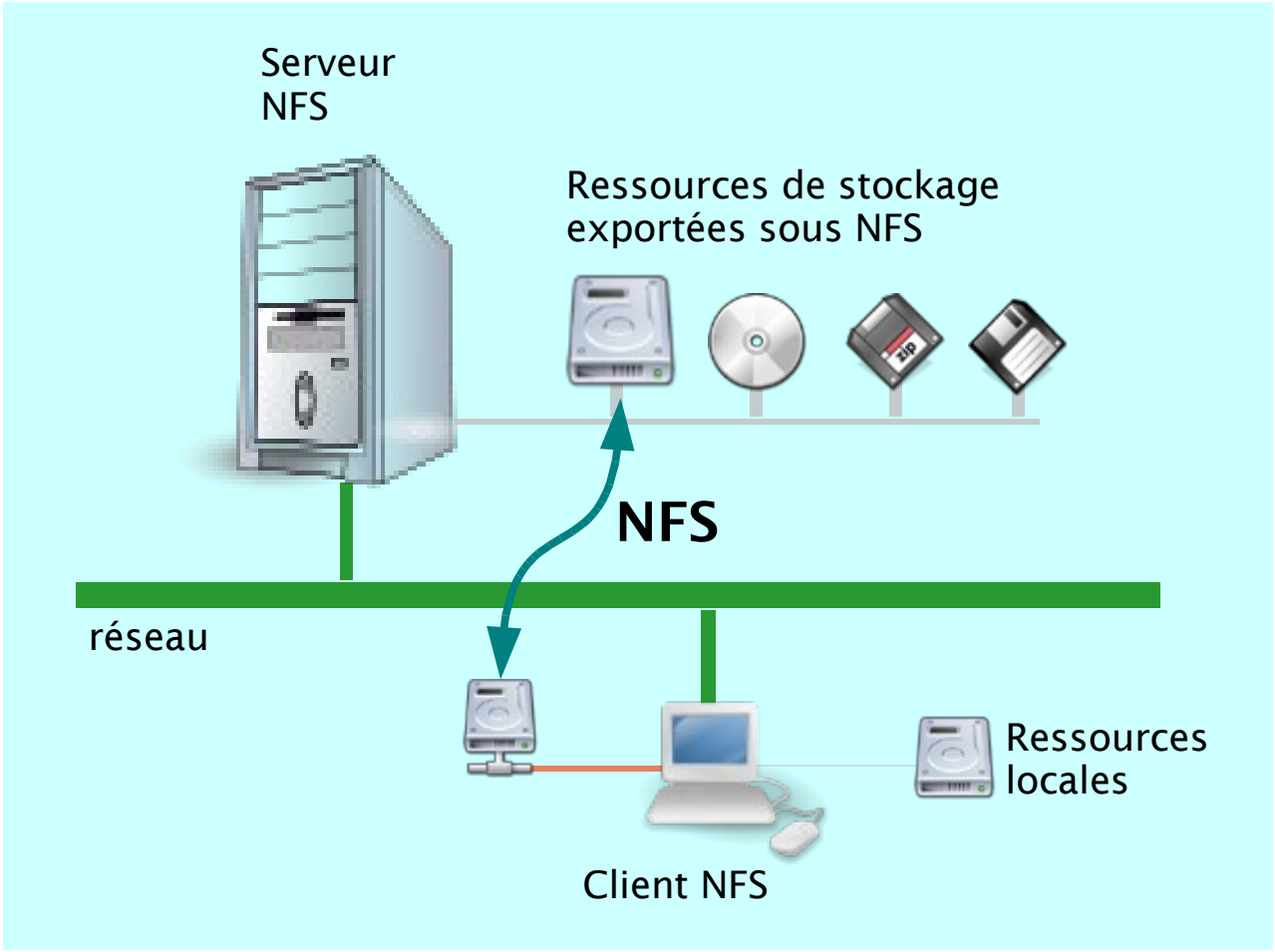
  ypcat passwd | more

Serveur NFS

Network File Service (NFS)

- Le système de fichiers en réseau (Network File System ou NFS) est un protocole qui permet à un ordinateur d'accéder à des fichiers via un réseau
  - Aussi développé par Sun
- Afin d'accéder aux fichiers distants, une authentification (sommaire) est nécessaire
  - Fichier de mot de passe synchronisé manuellement
  - Identification à travers NIS
  - Identification à travers LDAP
- Les versions plus anciennes (1, 2 ou 3) sont peu sécurisées
- La nouvelle version (4) est très différentes (objets distribués)
  - Un RFC pour la version 4.1 est en train de validation
  - Accent sur la performance (on en discute plus tard)

Principe


Serveur
NFS
Ressources de stockage
exportées sous NFS
NFS
réseau
Ressources
locales
Client NFS

Installation et Configuration d'un serveur NFS

- Installation
  - sudo apt-get install portmap nfs-kernel-server
- Configuration des partages
  - Editer le fichier /etc/exports :
    - /home 192.168.0.10(rw,sync,no_subtree_check)
    - /home 192.168.0.0/255.255.255.0(ro,sync,no_subtree_check)
- Maintenant, exportez le partage :
  - sudo exportfs -ra
- Finalement, il faut reinitialiser le service
  - sudo /etc/init.d/portmap restart
  - sudo /etc/init.d/nfs-kernel-server restart

Installation d'un client NFS

- Installation
  - sudo apt-get install portmap nfs-common
- Montage des partages
  - Les partages sont montés comme des dispositifs de stockage
  - sudo mount ServerIP:/chemin/partagé /home/username/point/de/montage
  - **sudo mount 192.168.1.42:/home/music /home/poningru/music**
- Monter un partage au démarrage
  - Possibilité de définir des entrées statiques (avec /etc/fstab) ou dynamiques (avec autofs)

Montage automatique

- Automounter
  - sudo apt-get install autofs
  - Rajouter cette ligne à la fin de /etc/auto.master :
    - /home /etc/auto.home
  - Créer /etc/auto.home et rajouter :
    - * box1.company.com,box2.company.com:/export/home/&
  - sudo /etc/init.d/autofs start
- Montage statique
  - Créer les répertoires d'ancrage (mountpoints).
  - Rajouter les partage sur le fichier /etc/fstab :
    - servername:dir /mntpoint nfs rw,hard,intr 0 0

Serveur SMB

Description du service Samba

- Outil qui permet le partage des fichiers et des imprimantes entre Windows et Linux
  - Utilise un protocole initialement conçu par Microsoft - smb
- C'est LA solution logicielle pour faire d'un serveur GNU/Linux un serveur de fichiers (et d'imprimantes) pour des clients sous Windows
- Dans les dernières versions d'Ubuntu, la configuration est automatique
  - Partage d'un dossier faite comme sous windows (click droit → partager)
- La configuration manuelle reste toutefois possible

Configuration Manuelle de Samba

- Fichier de Configuration : /etc/samba/smb.conf
- Configuration du partage de fichiers et répertoires

```
[nom_partage]
    comment = Fred's Home Directory
path = /home/fred
valid users = fred
public = no
writable = yes
Browseable = yes
printable = no
```

Configuration Manuelle de Samba

- Configuration de partage d'imprimantes

```
[printer_share_name]
comment = Fred's Printer
valid users = fred
path = /var/spool/samba
printer = freds_printer
public = no
writable = no
printable = yes
```

Méthodes d'authentification

- L'authentification utilise des mots de passe spécifiques
  - L'utilisateur doit exister sur la machine
  - Mots de passe stockés dans le fichier /etc/samba/smbpasswd
- Pour donner la permission à des utilisateurs d'accéder un partage :
  - sudo smbpasswd -a username
  - New SMB password:
  - Retype new SMB password:
  - Added user username.
- sudo /etc/init.d/samba reload

LUSTRE, p-NFS, etc…

Systèmes de fichiers “parallèles”

- SMB et NFS sont des systèmes adaptés aux petits réseaux locaux
  - Répertoires partagés
- Dès que la charge s’intensifie, la performance ne suit pas
  - Cas classique : un cluster de calcul avec des lectures/écritures simultanées
- On a vu l’arrivée de solutions dédiées à ces environnements
  - AFS/DFS, CODA, pNFS, LUSTRE
- Caractéristiques principales : serveurs de meta-données et stripping des fichiers
- Le NFS 4.1 s’est largement inspirée de ces systèmes
  - Encore en RFC, mais avec plusieurs implémentations en marche
  - Solution "standardisée" qui remet en cause les concurrents