Sécurité du plan de gestion des réseaux IP

Soutenance de thèse

Vincent Cridlig

Université Henri Poincaré, Nancy 1

11 décembre 2006

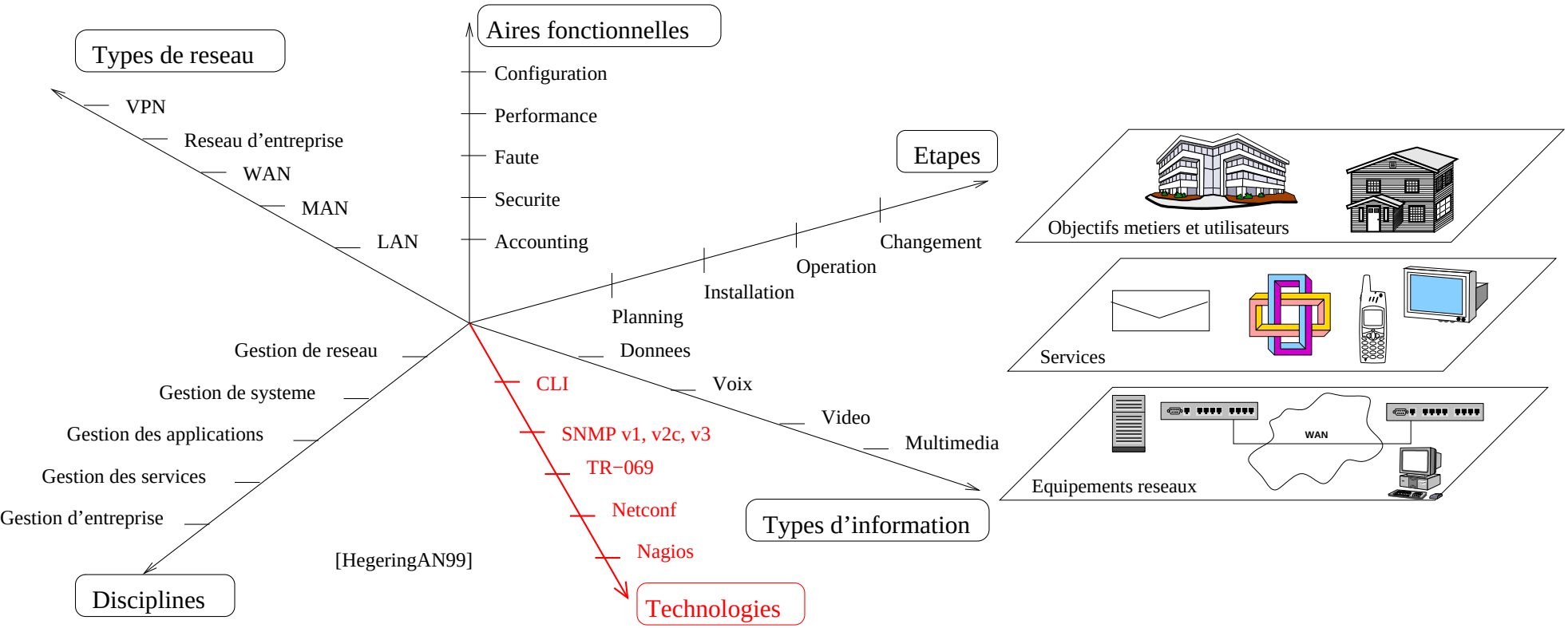
Sommaire

Sommaire

Qu'est-ce que la gestion de réseaux ?

Définition

Acte d'initialiser, de monitorer et de modifier le comportement des fonctions primaires du réseau [Pras95]



Plusieurs niveaux d'hétérogénéité

Protocolaire

- Orienté données (SNMP, TR-069)
- Orienté commandes (CLI)
- Hybride (Netconf par ses extensions)

Modèle de données

- Arborescent (SNMP, TR-069, Netconf)
- Commandes (CLI)

Modèle de sécurité

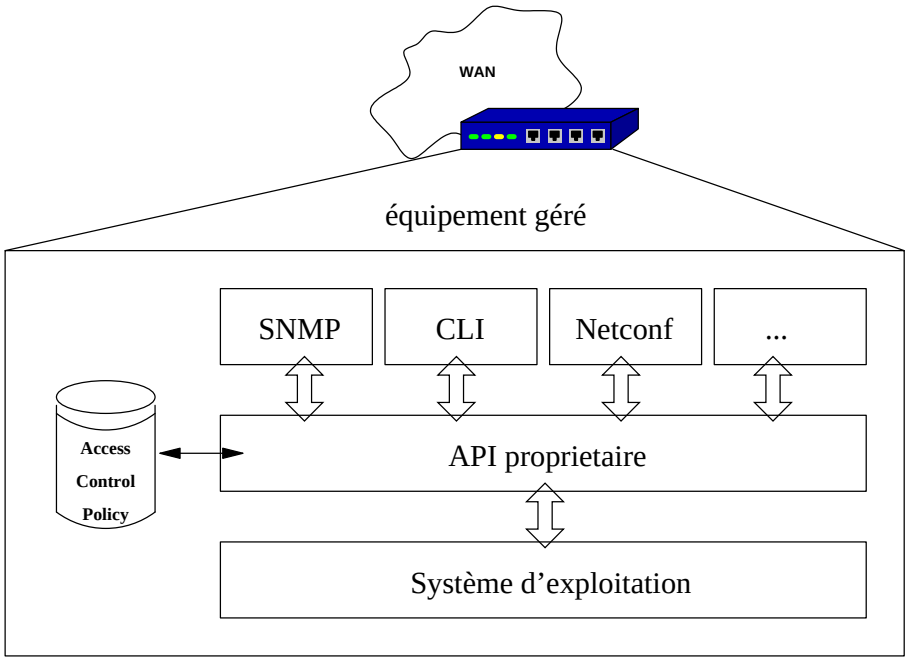
- Intégré (SNMPv3)
- Externe (TR-069, Netconf, CLI, Webmin)

Constat

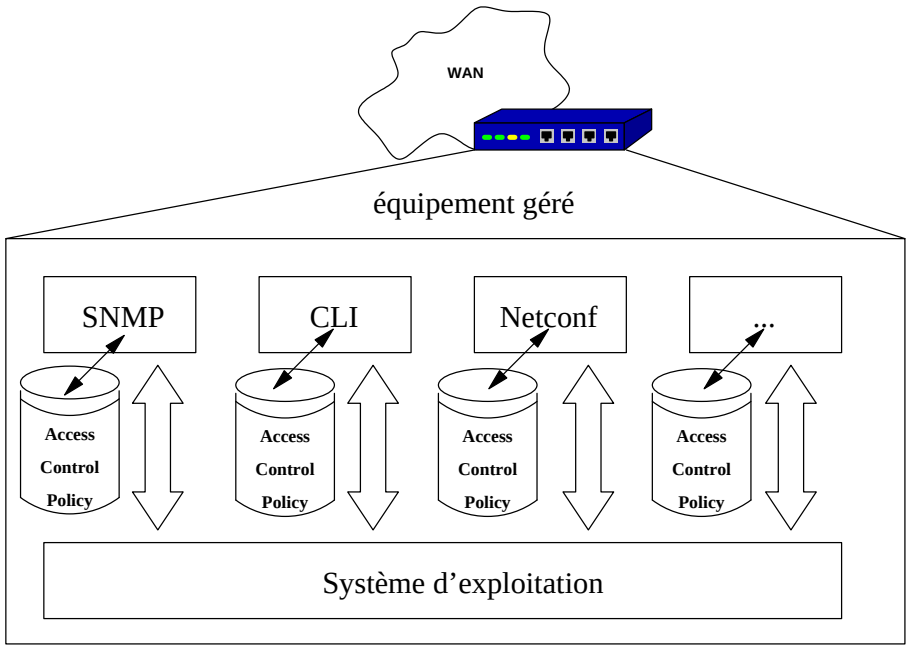
Tous ont un système de contrôle d'accès intégré car très dépendant du modèle de données.

Hétérogénéité des modèles de sécurité

- Illustration du problème
  - Modèle fédéré
  - Modèle non fédéré



modèle fédéré



modèle non fédéré

Coût de maintenance

Il est très coûteux de maintenir une politique de sécurité pour chaque plateforme de supervision :

- Gestion des tokens de sécurité : déploiement et mise à jour (mots de passe, certificats, ...)
- Gestion des identités : une entité peut avoir différentes identités sur différentes plateformes sans lien entre elles
- Gestion des règles d'accès : déploiement et maintenance des privilèges sur des réseaux de grande taille

Note

On parle ici de réseaux constitués de 30 000 à 100 000 équipements. D'où le problème de passage à l'échelle.

Deux niveaux de cohérences

Cohérence locale

Cette propriété est vérifiée si, sur un même équipement, les privilèges d'un gestionnaire sont équivalents quelle que soit l'interface de gestion utilisée.

La cohérence locale pose la question de la **localisation** du processus de contrôle d'accès.

Cohérence globale

Cette propriété est vérifiée si, pour une plateforme de gestion donnée, les privilèges d'un gestionnaire sont équivalents, sur un ensemble d'équipements du réseau.

La cohérence globale est recherchée pour des **classes d'équipements**.

Contributions

- Cohérence locale
  - A model for checking consistency in access control policies for network management IM 2007
  - Role based access control for XML based management gateway DSOM 2004
- Cohérence globale
  - RADIUS-Based SNMP Authorization IM 2005 App
  - An Integrated Security Framework for XML based Management IM 2005
  - Role-Based Access Control for XML Enabled Multi-Protocol Management Gateways eTNSM 2006
- Une plateforme de contrôle d'accès pour Netconf
  - A NetConf Network Management Suite: ENSUITE IPOM 2005
  - XBGP-MAN: A XML management architecture for BGP IJNM 2006
  - Ensuite, une plateforme libre de configuration de réseau Techniques de l'ingénieur
  - Netconf Access Control Framework

    http://www.ietf.org/internet-drafts/draft-cridlig-netconf-rbac-00.txt

Sommaire

Les besoins de sécurité de la supervision

Les services de sécurité nécessaires

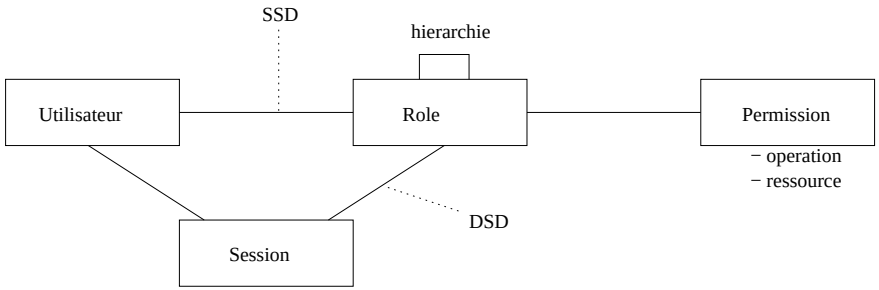
- Confidentialité
- Authentification
- Intégrité
- Anti-rejeu
- Contrôle d'accès

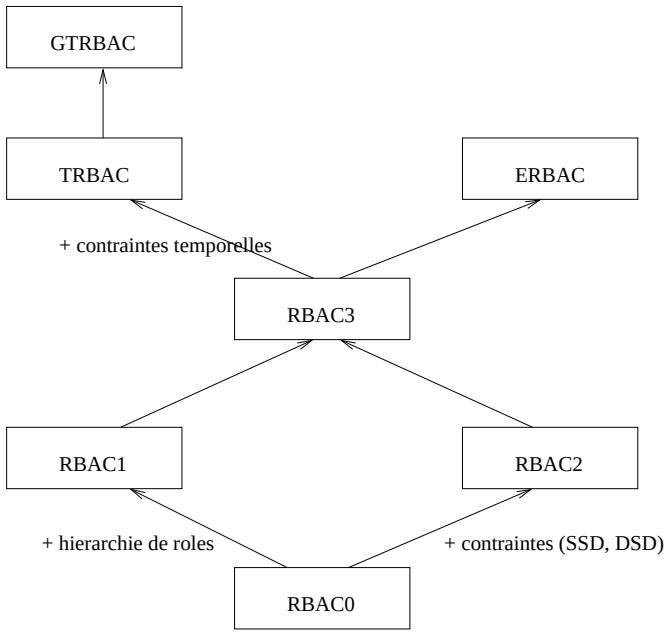
Les contraintes spécifiques

- Grand nombre d'équipements
- Fonctionnement minimal souhaité même en environnement dégradé
- Mécanismes de notifications
- Multiples plateformes et identités

Contrôle d'accès basé sur les rôles (RBAC)

- $RBAC_0$: Rôle et (dé)activation dans une session
- $RBAC_1$: Hiérarchie des rôles
- $RBAC_2$: Contraintes de séparation des pouvoirs
  - statique (SSD)
  - dynamique (DSD)
- $RBAC_3$: $RBAC_1$ ET $RBAC_2$
- *TRBAC*: Contraintes temporelles de mise à disposition d'un rôle
- *GTRBAC*: Généralisation pour l'assignation, l'activation





Sur-modèles avec systèmes cibles

Contrôle d'accès basé sur l'Organisation (OrBAC)

- Multiples politiques ⇒ Contexte
- Obligation, interdiction et recommandation
- Deux niveaux d'abstraction
  - Concret : utilisateurs, objets, action, permission
  - Abstrait : rôles, vues, activités
- Avantage : complet
- Inconvénient : concepts non transposables aux systèmes cibles envisagés

Enterprise RBAC (ERBAC)

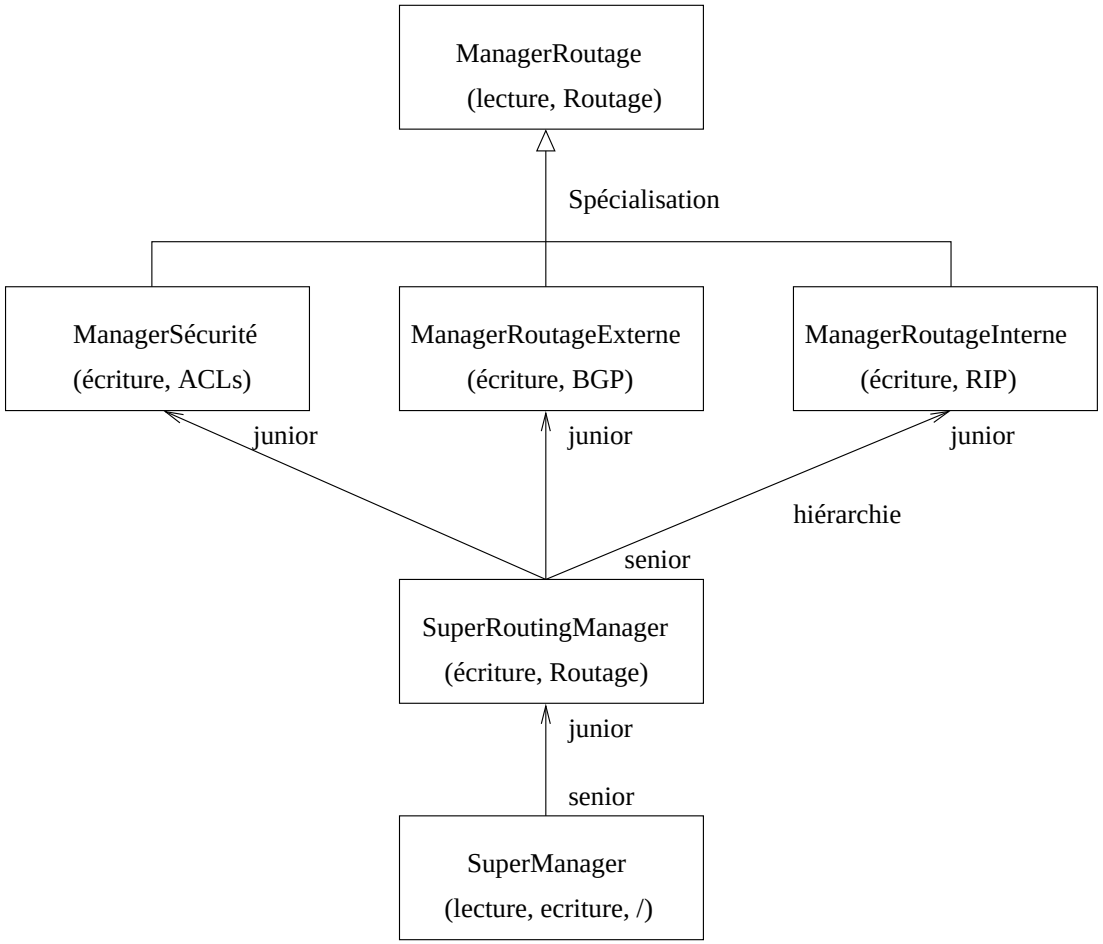
- Vue unifiée de la politique de contrôle d'accès
- Déploiement automatique sur des systèmes cibles
- Inconvénient : pas de modèle de données génériques
- Avantage : évite la traduction du modèle de données

Choix d'un modèle de contrôle d'accès

Pourquoi avoir choisi le modèle RBAC comme dénominateur commun ?

- Adapté à la gestion de grands réseaux
  - Notion de rôle : découplage entre utilisateurs et permissions
  - Réduction des risques d'erreurs de configuration (activation des rôles)
- Passage à l'échelle
  - Le nombre d'utilisateurs est masqué par les rôles
  - Les rôles peuvent être hiérarchiques (spécialisation ou supériorité)
- Maintenabilité
  - lors d'un changement de fonction
  - lors de l'ajout/suppression de permissions

Scénario d'application de RBAC



- Définition des rôles dans un routeur de bordure
- On peut ajouter des rôles pour le monitoring, la sécurité, ...
- 2 types de hiérarchies (cf. OrBAC)
  - supériorité
  - spécialisation

Un exemple de modèle de sécurité intégré : USM/VACM

VACM : View-based Access Control Model

SecurityToGroupTable

Security Model	*Security Name*	*Group Name*
USM	Bob	SysAdmin
USM	Alice	NetAdmin

ViewTreeFamilyTable

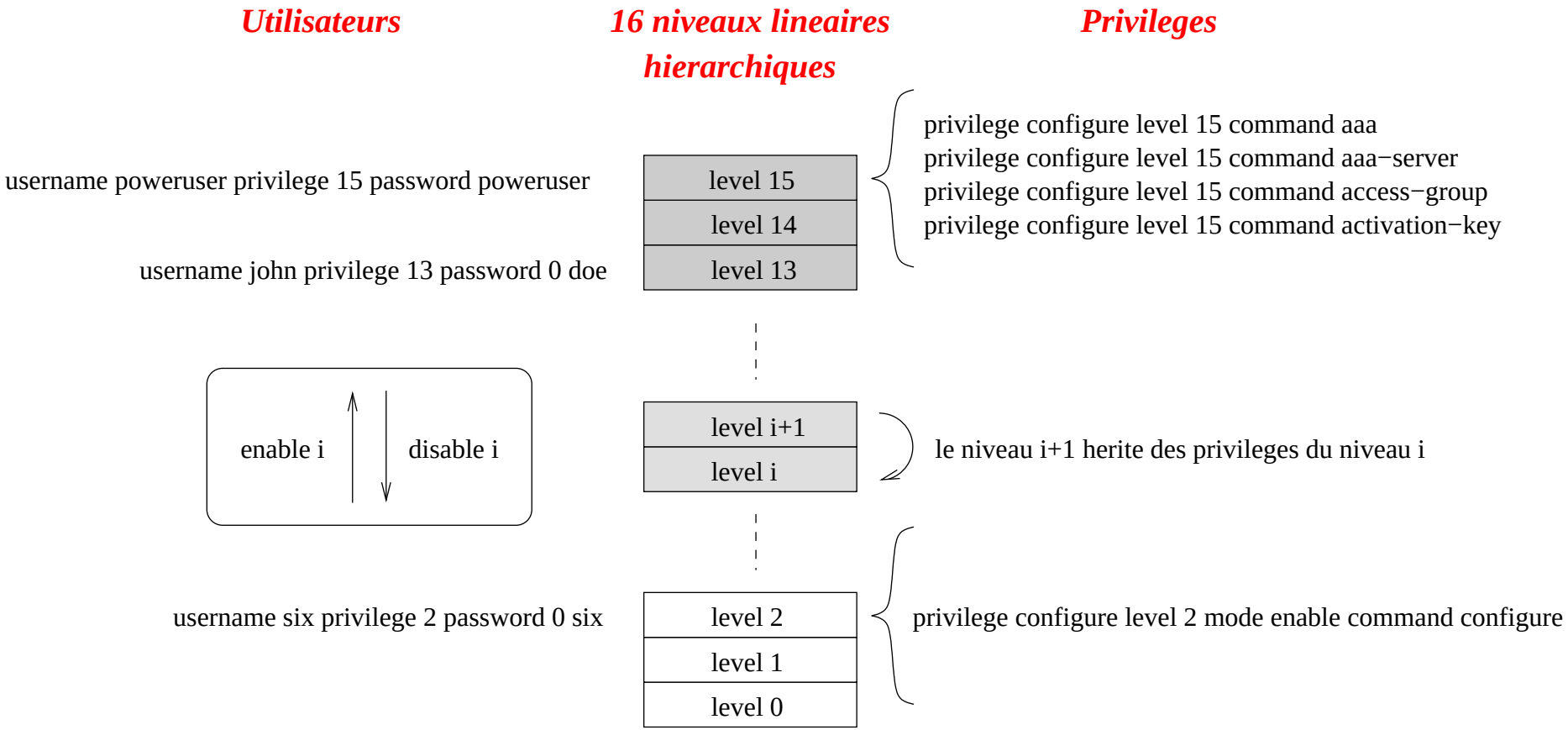
View Name	*Subtree*	*Mask*	*Type*
Mib II	1.3.6.1.2.1	11111111	Included
Network	1.3.6.1.2.1.6	11111111	Included
Network	1.3.6.1.2.1.2	11111111	Included
System	1.3.6.1.2.1.1	11111111	Included

AccessTable

Group Name	*Context Prefix*	*Security Model*	*Security Level*	*Context Match*	*ReadView Name*	*WriteView Name*	*NotifyView Name*
SysAdmin	""	USM	authNoPriv	exact	Mib II	System	None
NetAdmin	""	USM	authPriv	exact	Mib II	Network	None

- Problèmes de conception et de passage à l'échelle :
  - Le modèle de sécurité n'a pas sa place dans AccessTable
  - On ne peut pas construire une vue à partir d'une autre vue
  - Un utilisateur ne peut appartenir qu'à un groupe
  - Les familles de sous-arbres demandent un long temps d'apprentissage

Le modèle de contrôle d'accès de CLI

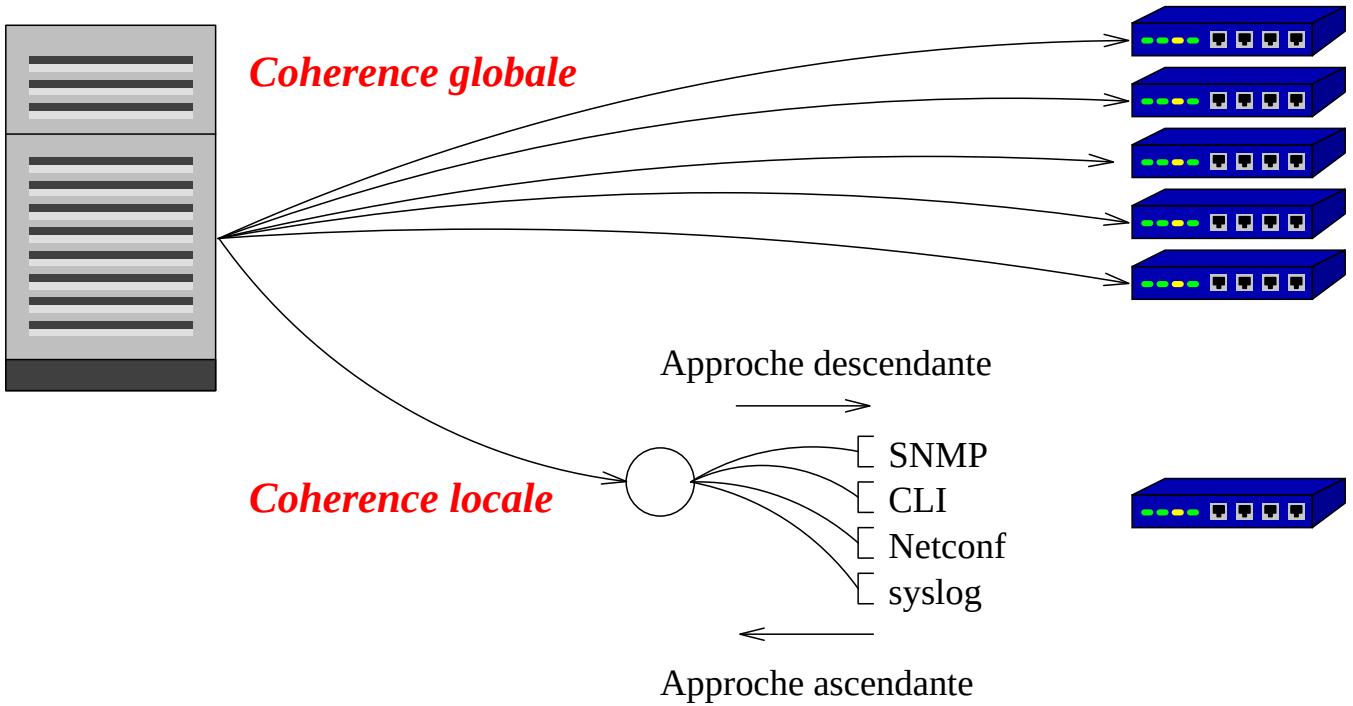


Synthèse

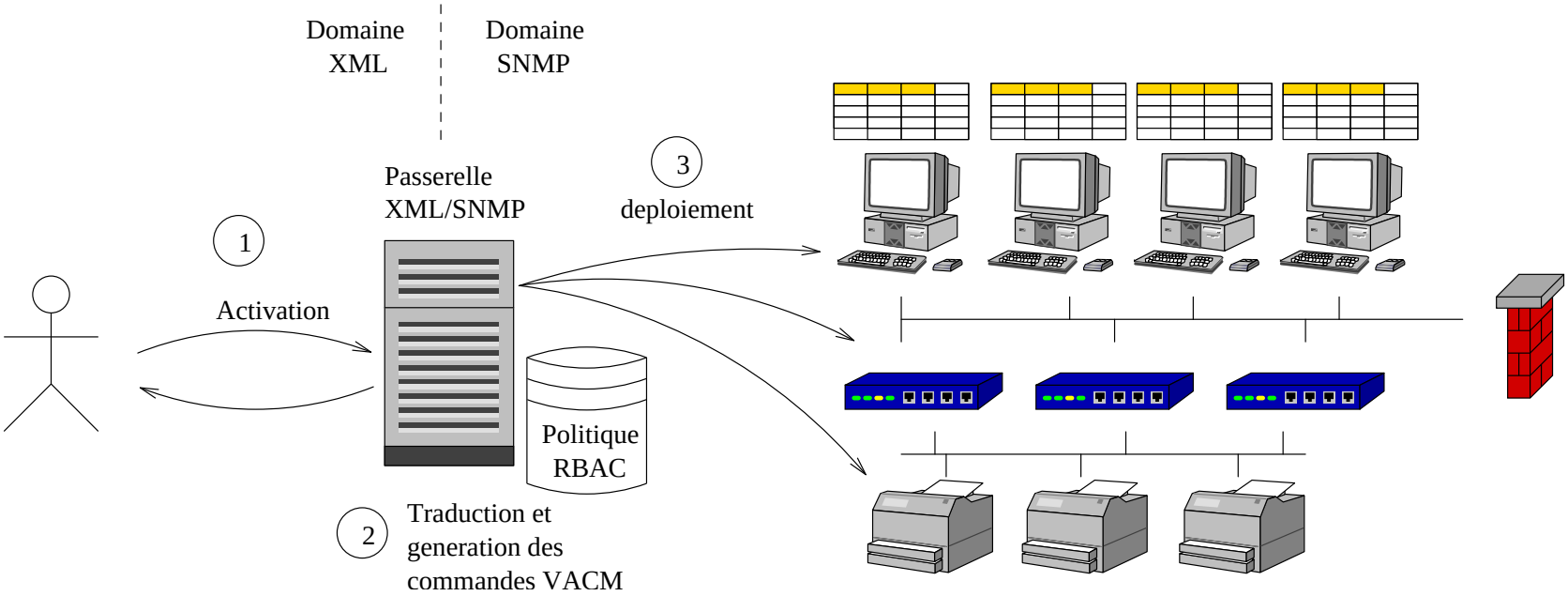
Plateforme de supervision	Authentification du serveur	Confidentialité	Intégrité des données	Authentification du client	Contrôle d'accès
SNMPv1, v2c				mot de passe en clair	
SNMPv3		USM cbc-des	USM hmac-md5-96	mot de passe md5, sha	VACM
CLI/telnet				mot de passe	niveaux
CLI/SSH	ssh-rsa ssh-dss	3des-cbc aes, ...	HMAC hmac-sha1 hmac-md5	SSH Auth. Prot. clé publique mot de passe	niveaux
Netconf/SSH	ssh-rsa ssh-dss	3des-cbc aes, ...	HMAC hmac-sha1 hmac-md5	SSH Auth. Prot. clé publique mot de passe	Pas encore spécifié
Netconf/SOAP /HTTP/SSL	rsa dss	des 3des, rc4	HMAC hmac-sha1 hmac-md5	(optionnel) Certificat client mot de passe	Pas encore spécifié
TR-069/SOAP /HTTP/SSL	rsa dss	des 3des, rc4	HMAC hmac-sha1 hmac-md5	(optionnel) userid/mot de passe Distribution non spécifiée	une ACL par nœud
Webmin /HTTP/SSL	rsa dss	des 3des, rc4	HMAC hmac-sha1 hmac-md5	(optionnel) Certificat client mot de passe	Permissions par module

Sommaire

Différentes approches



Passerelle XML/SNMP



- La passerelle contient la politique RBAC
- L'activation/désactivation d'un rôle sur la passerelle provoque le déploiement des droits

Passerelle XML/SNMP

- (a) Données gérées
- (b) Schéma XML décrivant la structure des données
- (c) Politique de contrôle d'accès de la passerelle (RBAC)
- (d) Politique de contrôle d'accès de l'équipement géré (VACM)

```
<?xml version="1.0" encoding="UTF-8"?>
<snmp-data xmlns:IF-MIB="http://www.ibr.cs.tu-bs.de/
      arbeiten/snmp-xml-gw/xsd/IF-MIB.xsd">
  <context ipaddr="134.169.35.130" hostname=
        "134.169.35.130" port="161" caching="yes"
        community="public" time="2003-03-11T18:50:13">
    <IF-MIB:ifEntry ifIndex="1">
      <IF-MIB:ifDescr>First interface</IF-MIB:ifDescr>
      <IF-MIB:ifPhysAddress enc="hex">00:0C:F1:82:47:5E
            </IF-MIB:ifPhysAddress>
    </IF-MIB:ifEntry>
    [...]
  </context>
</snmp-data>
```

(a)

Passerelle XML/SNMP

- (a) Données gérées
- (b) Schéma XML décrivant la structure des données
- (c) Politique de contrôle d'accès de la passerelle (RBAC)
- (d) Politique de contrôle d'accès de l'équipement géré (VACM)

```
<xsd:element name="ifPhysAddress"
type="SNMPv2−TC:PhysAddress" minOccurs="0">
  <xsd:annotation>
    <xsd:appinfo>
      <maxAccess>read−only</maxAccess>
      <status>current</status>
      <oid>1.3.6.1.2.1.2.2.1.6</oid>
    </xsd:appinfo>
    <xsd:documentation> [...] </xsd:documentation>
  </xsd:annotation>
</xsd:element>
```

(b)

Passerelle XML/SNMP

- (a) Données gérées
- (b) Schéma XML décrivant la structure des données
- (c) Politique de contrôle d'accès de la passerelle (RBAC)
- (d) Politique de contrôle d'accès de l'équipement géré (VACM)

```
<rbac>
<users> <!-- RBAC users -->
<user Id="u1" login="bob" password="bobpassphrase"/>
<user Id="u2" login="alice" password="alicepassphrase"/>
</users>
<roles> <!-- RBAC roles -->
<role Id="r1" name="sysAdmin"/>
<role Id="r2" name="netAdmin"/>
</roles>
<scopes> <!-- RBAC scopes -->
<scope Id="s1" path="/ifEntry" mibns="IF-MIB"/>
<scope Id="s2" path="/ifEntry/ifPhysAddress" mibns="IF-MIB"/>
<scope Id="s3" path="/interfaces/ifNumber" mibns="IF-MIB"/>
</scopes>
<permissions> <!-- RBAC permissions -->
<permission Id="p1" scopeRef="s1" operation="read"/>
<permission Id="p2" scopeRef="s2" operation="write"/>
</permissions>
<UAs> <!-- RBAC user-role association -->
<UA Id="ua1" userRef="u1" roleRef="r1"/>
<UA Id="ua2" userRef="u1" roleRef="r2"/>
<UA Id="ua3" userRef="u2" roleRef="r2"/>
</UAs>
<PAs> <!-- RBAC permission-role association -->
<!-- netAdmin can read <IF-MIB:ifEntry> element -->
<PA Id="pa1" permissionRef="p1" roleRef="r1"/>
<PA Id="pa2" permissionRef="p2" roleRef="r2"/>
</PAs>
</rbac>
```

(c)

Passerelle XML/SNMP

- (a) Données gérées
- (b) Schéma XML décrivant la structure des données
- (c) Politique de contrôle d'accès de la passerelle (RBAC)
- (d) Politique de contrôle d'accès de l'équipement géré (VACM)

Security Model	*User*	*Group*
USM	bob	bobGroup
USM	alice	aliceGroup

vacmSecurityToGroupTable

Group	*Security Model*	*Security Level*	*Read*	*Write*	*Notify*
bobGroup	USM	authPriv	RVbob	WVbob	NVbob
aliceGroup	USM	authPriv	RValice	WValice	NValice

AccessTable

ViewName	*OID*	*Mask*	*Type*
RVbob	1.3.6.1.2.1.2.2.1		Included
WVbob	1.3.6.1.2.1.2.2.1.6		Included
WValice	1.3.6.1.2.1.2.2.1.6		Included

vacmViewTreeFamilyTable

(d)

Passerelle XML/SNMP

- (a) Données gérées
- (b) Schéma XML décrivant la structure des données
- (c) Politique de contrôle d'accès de la passerelle (RBAC)
- (d) Politique de contrôle d'accès de l'équipement géré (VACM)

```
<?xml version="1.0" encoding="UTF-8"?>
<snmp-data xmlns:IF-MIB="http://www.ibr.cs.tu-bs.de/
      arbeiten/snmp-xml-gw/xsd/IF-MIB.xsd">
  <context ipaddr="134.169.35.130" hostname=
        "134.169.35.130" port="161" caching="yes"
        community="public" time="2003-03-11T18:50:13">
    <IF-MIB:ifEntry ifIndex="1">
      <IF-MIB:ifDescr>First interface</IF-MIB:ifDescr>
      <IF-MIB:ifPhysAddress enc="hex">00:0C:F1:82:47:5E
            </IF-MIB:ifPhysAddress>
    </IF-MIB:ifEntry>
    [...]
  </context>
</snmp-data>
```

(a)

```
<xsd:element name="ifPhysAddress"
type="SNMPv2-TC:PhysAddress" minOccurs="0">
  <xsd:annotation>
    <xsd:appinfo>
      <maxAccess>read-only</maxAccess>
      <status>current</status>
      <oid>1.3.6.1.2.1.2.2.1.6</oid>
    </xsd:appinfo>
    <xsd:documentation> [...] </xsd:documentation>
  </xsd:annotation>
</xsd:element>
```

(b)

```
<rbac>
<users> <!-- RBAC users -->
<user Id="u1" login="bob" password="bobpassphrase"/>
<user Id="u2" login="alice" password="alicepassphrase"/>
</users>
<roles> <!-- RBAC roles -->
<role Id="r1" name="sysAdmin"/>
<role Id="r2" name="netAdmin"/>
</roles>
<scopes> <!-- RBAC scopes -->
<scope Id="s1" path="/ifEntry" mibns="IF-MIB"/>
<scope Id="s2" path="/ifEntry/ifPhysAddress" mibns="IF-MIB"/>
<scope Id="s3" path="/interfaces/ifNumber" mibns="IF-MIB"/>
</scopes>
<permissions> <!-- RBAC permissions -->
<permission Id="p1" scopeRef="s1" operation="read"/>
<permission Id="p2" scopeRef="s2" operation="write"/>
</permissions>
<UAs> <!-- RBAC user-role association -->
<UA Id="ua1" userRef="u1" roleRef="r1"/>
<UA Id="ua2" userRef="u1" roleRef="r2"/>
<UA Id="ua3" userRef="u2" roleRef="r2"/>
</UAs>
<PAs> <!-- RBAC permission-role association -->
<!-- netAdmin can read <IF-MIB:ifEntry> element -->
<PA Id="pa1" permissionRef="p1" roleRef="r1"/>
<PA Id="pa2" permissionRef="p2" roleRef="r2"/>
</PAs>
</rbac>
```

(c)

Security Model	*User*	*Group*
USM	bob	bobGroup
USM	alice	aliceGroup

vacmSecurityToGroupTable

Group	*Security Model*	*Security Level*	*Read*	*Write*	*Notify*
bobGroup	USM	authPriv	RVbob	WVbob	NVbob
aliceGroup	USM	authPriv	RValice	WValice	NValice

AccessTable

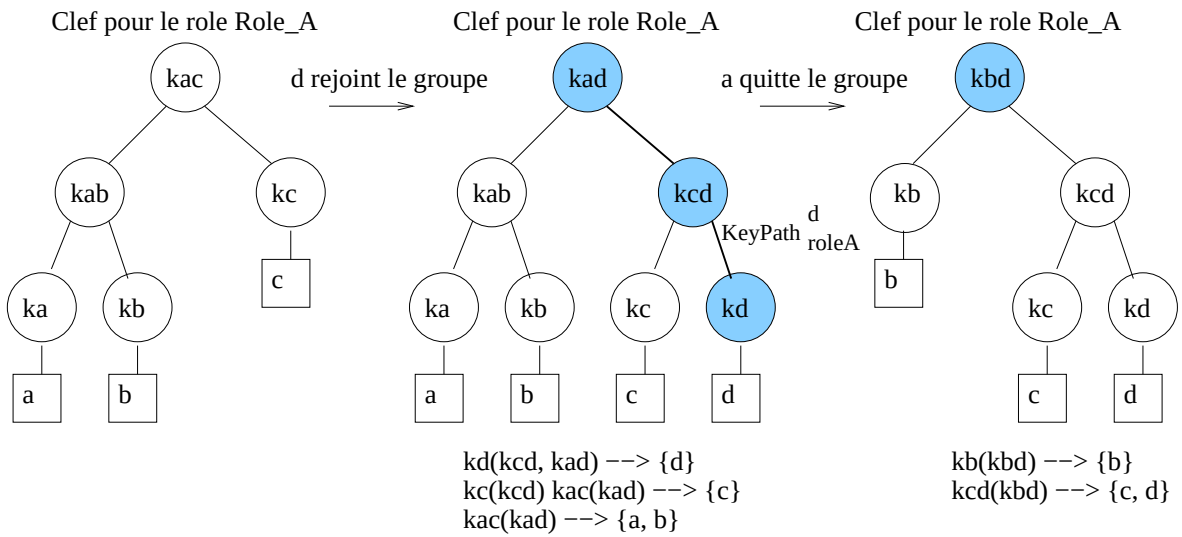
ViewName	*OID*	*Mask*	*Type*
RVbob	1.3.6.1.2.1.2.2.1		Included
WVbob	1.3.6.1.2.1.2.2.1.6		Included
WValice	1.3.6.1.2.1.2.2.1.6		Included

vacmViewTreeFamilyTable

(d)

Parallèle multicast/RBAC dans un contexte Netconf

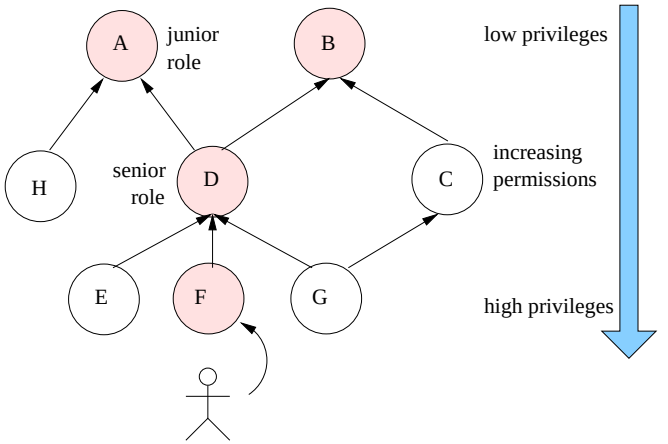
- Fusion groupe multicast/ rôle
  - Chaque rôle correspond à un arbre de clé (algorithme LKH)
  - Rafraîchissement des clés : non plus après un join/leave multicast mais activate/deactivate RBAC
- Entité centralisée pour l'activation des rôles
- Un manager prouve l'activation d'un rôle par la possession de la clé de rôle.



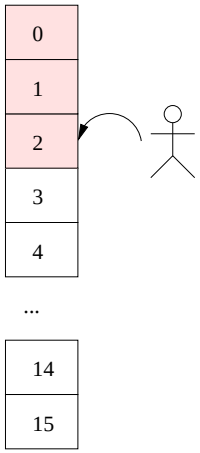
Cohérence locale par translation et déploiement

- Démarche descendante
- Traduction de la politique RBAC vers systèmes cibles:
  - RBAC to VACM [1]
  - RBAC to CLI security level [3]

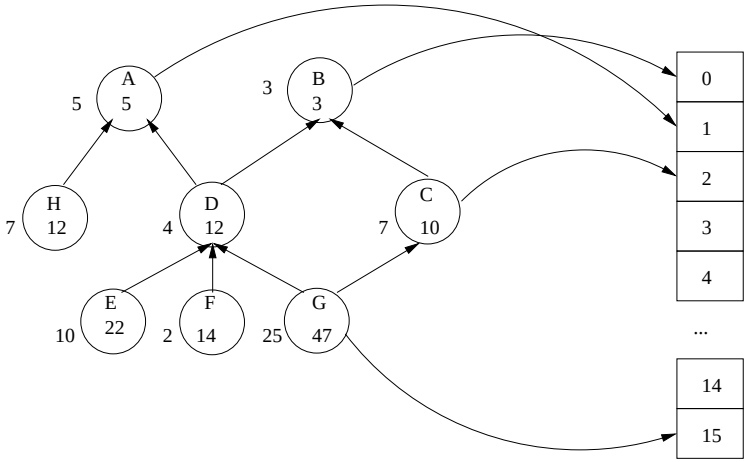
Démarche descendante : RBAC vers CLI



RBAC roles hierarchy



CLI levels hierarchy



RBAC roles hierarchy

CLI levels hierarchy

Roles	b	a	c	d	h	f	e	g
Weights	3	5	10	12	12	14	22	47
CLI Levels	0	0	1	1	1	2	2	2
Weight average	4		11.33			27.66		

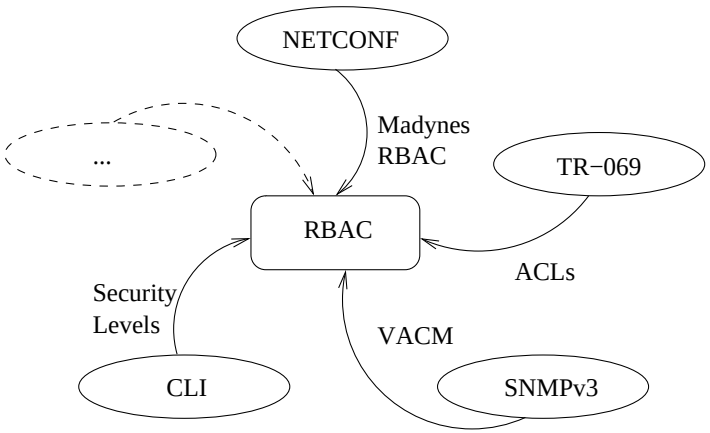
Roles	b	a	c	d	h	f	e	g
Weights	3	5	10	12	12	14	22	47
CLI Levels	0	0	1	1	1	1	2	2
Weight average	4		12				34.5	

Roles	b	a	c	d	h	f	e	g
Weights	3	5	10	12	12	14	22	47
CLI Levels	0	0	1	1	1	1	2	2
Weight average	4		12				34.5	

- Pondération des rôles
- Algorithme de clusterisation K_Means pour regrouper les rôles
- Perte d'information par approximation (RBAC est non-linéaire)

Formalisation et vérification

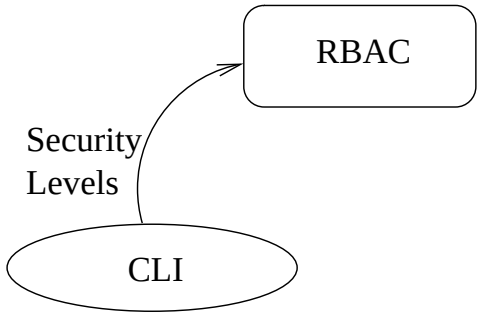
- Vérification post-déploiement (démarche ascendante)
- Formalisation des modèles de contrôle d'accès
- Formalisation des fonctions de conversion
- Réécriture des politiques vers :
  - un modèle commun (RBAC)
  - une notation commune (meta-CLI)
- Algorithme de comparaison des politiques réécrites



Note

⇒ Illustration du cas CLI

Traduction des niveaux de sécurité CLI



- Chaque $niveau_i$ devient un rôle
- La ressource de chaque privilège est décrite en notation meta-CLI compacte
- La politique elle-même est décrite en notation meta-CLI
- Un utilisateur est assigné au rôle correspondant à son niveau de privilège maximum
- Par hiérarchie, un utilisateur peut activer tous les rôles inférieurs

Exemple de traduction avec Meta-CLI

- Représentation arborescente des commandes
- Notation Meta-CLI compacte pour les permissions
- Au-dessous : politique CLI en entrée
- A droite : politique RBAC transformée

```
username john privilege 9 password 0 doe
...
username inout password inout
privilege configure level 8 snmp-server community
privilege configure level 3 command ping
...
privilege configure level 15 command access-group
privilege configure level 15 command activation-key
```

```
- rbac:
    -roles:
        -role: '1'
            -name: 'role9'
    -users:
        -user: '1'
            -name: 'john'
        -user: '2'
            -name: 'six'
    -permissions:
        -permission: '1'
            -scope: '/configure/snmp-server/community'
            -operation: 'w'
        -permission: '2'
            -scope: '/configure/command/ping'
            -operation: 'w'
        -permission: '3'
            -scope:
'/configure/mode/enable/command/configure'
            -operation: 'w'
    -user-role-assignements:
        -user-role-assignement: '2'
            -user: '2'
            -role: '2'
    -permission-role-assignements:
        -permission-role-assignement: '1'
            -permission: '4'
            -role: '3'
```

Comment comparer les politiques RBAC obtenues ?

- On fait l'hypothèse que l'on sait comparer les ressources
- Même si les rôles ne correspondent pas, les permissions peuvent correspondre
- Pour chaque contexte d'activation de rôles dans un politique P_a, trouver un ensemble de rôles dans P_b qui donnent des privilèges au moins équivalents (et réciproquement)
  - en respectant les contraintes SSD et DSD

Note

Pour chaque utilisateur, on peut dégager un différence de privilèges et éventuellement ordonner les politiques de la plus permissive à la moins permissive.

Comment comparer les politiques RBAC obtenues ?

- On fait l'hypothèse que l'on sait comparer les ressources
- Même si les rôles ne correspondent pas, les permissions peuvent correspondre
- Pour chaque contexte d'activation de rôles dans un politique P_a, trouver un ensemble de rôles dans P_b qui donnent des privilèges au moins équivalents (et réciproquement)
  - en respectant les contraintes SSD et DSD

Note

Pour chaque utilisateur, on peut dégager un différence de privilèges et éventuellement ordonner les politiques de la plus permissive à la moins permissive.

Comment comparer les politiques RBAC obtenues ?

- On fait l'hypothèse que l'on sait comparer les ressources
- Même si les rôles ne correspondent pas, les permissions peuvent correspondre
- Pour chaque contexte d'activation de rôles dans un politique P_a, trouver un ensemble de rôles dans P_b qui donnent des privilèges au moins équivalents (et réciproquement)
  - en respectant les contraintes SSD et DSD

Note

Pour chaque utilisateur, on peut dégager un différence de privilèges et éventuellement ordonner les politiques de la plus permissive à la moins permissive.

Comment comparer les politiques RBAC obtenues ?

- On fait l'hypothèse que l'on sait comparer les ressources
- Même si les rôles ne correspondent pas, les permissions peuvent correspondre
- Pour chaque contexte d'activation de rôles dans un politique P_a, trouver un ensemble de rôles dans P_b qui donnent des privilèges au moins équivalents (et réciproquement)
  - en respectant les contraintes SSD et DSD

Note

Pour chaque utilisateur, on peut dégager un différence de privilèges et éventuellement ordonner les politiques de la plus permissive à la moins permissive.

Synthèse

- Cohérence globale
  - + Modèle de déploiement des droits à grande échelle
  - + Gain de temps et coût de configuration réduit
  - - Tenir compte des particularités des équipements
  - - Coûts de déploiement dynamique
- Cohérence locale
  - + Double démarche : descendante et ascendante
  - + Moyen multi-protocole de détecter les incohérences dans les politiques déployées
  - - Les traductions induisent quelques pertes d'information (interdictions, algorithme de clusterisation K_Means)
  - - Traduire la description des ressources protégées est un problème difficile $\Rightarrow$ libsmi

Un framework de contrôle d'accès pour Netconf

Plusieurs étapes de spécification :

- Définition d'une représentation XML du modèle RBAC
- Définition des messages d'activation/désactivation des rôles
- Définition des conséquences sur le traitement des opérations standards

Note

La proposition a été soumise au groupe de travail *netconf* de l'IETF : *draft-cridlig-netconf-rbac-00.txt*

Un framework de contrôle d'accès pour Netconf

Plusieurs étapes de spécification :

- Définition d'une représentation XML du modèle RBAC
- Définition des messages d'activation/désactivation des rôles
- Définition des conséquences sur le traitement des opérations standards

Note

La proposition a été soumise au groupe de travail *netconf* de l'IETF : *draft-cridlig-netconf-rbac-00.txt*

Un framework de contrôle d'accès pour Netconf

Plusieurs étapes de spécification :

- Définition d'une représentation XML du modèle RBAC
- Définition des messages d'activation/désactivation des rôles
- Définition des conséquences sur le traitement des opérations standards

Note

La proposition a été soumise au groupe de travail *netconf* de l'IETF : *draft-cridlig-netconf-rbac-00.txt*

Un framework de contrôle d'accès pour Netconf

Plusieurs étapes de spécification :

- Définition d'une représentation XML du modèle RBAC
- Définition des messages d'activation/désactivation des rôles
- Définition des conséquences sur le traitement des opérations standards

Note

La proposition a été soumise au groupe de travail *netconf* de l'IETF : *draft-cridlig-netconf-rbac-00.txt*

Modèle XML et opération Netconf

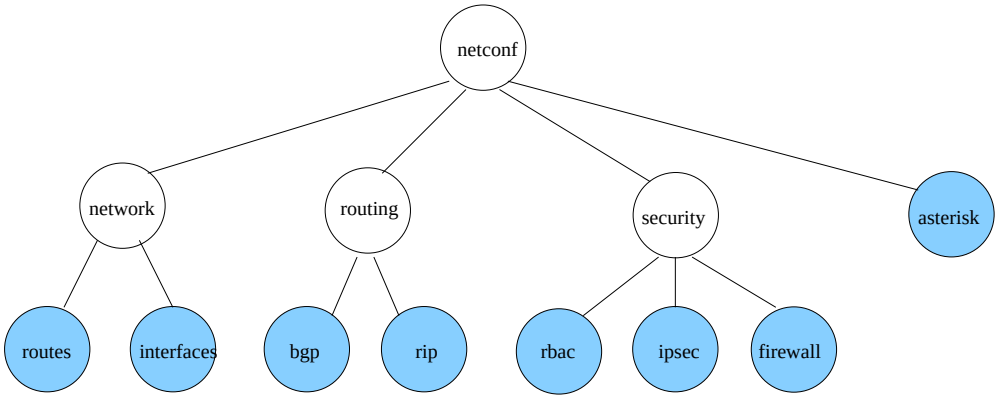
```
<?xml version="1.0" encoding="UTF-8"?>
<rbac xmlns=
"urn:loria:madynes:ensuite:yencap:module:RBAC:1.0">

    <user id="4">
      <login>netconf</login>
      <password>netconf</password>
      <public-key keytype="rsa">AAAAB3NzaC1yc2E...
         ...50RfDJ6M=</public-key>
    </user>

    <role id="1">
      <name>RoutingManager</name>
    </role>
    <role id="2">
      <name>InteriorRoutingManager</name>
      <junior-roles>
        <junior-role roleRef="1"/>
      </junior-roles>
    </role>

    <permission id="3" op="rw">
      <scope>/ycp:netconf/ycp:routing/rip:rip</scope>
    </permission>
</rbac>
```

- RBAC capability annoncée dans le message *hello*
- Méthode de sélection : XPath
- Rôles hiérarchiques
- Opérations d'activation/désactivation

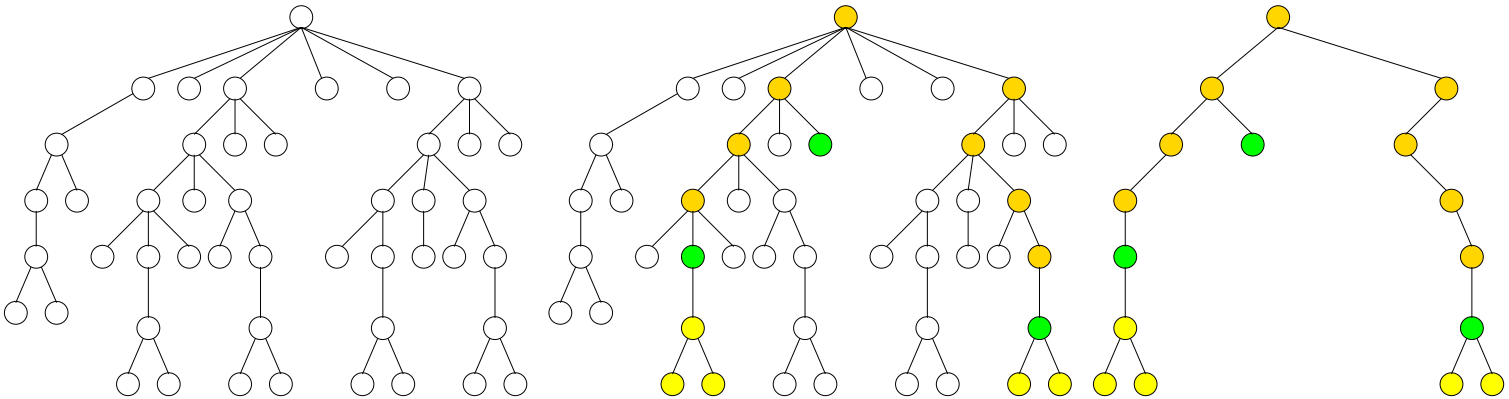
```
<rbac>
  <activate>
    <role>ExteriorRoutingManager</role>
  </activate>
</rbac>
```

```
<rbac>
  <deactivate>
    <role>ExteriorRoutingManager</role>
  </deactivate>
</rbac>
```

Filtrage du modèle de données

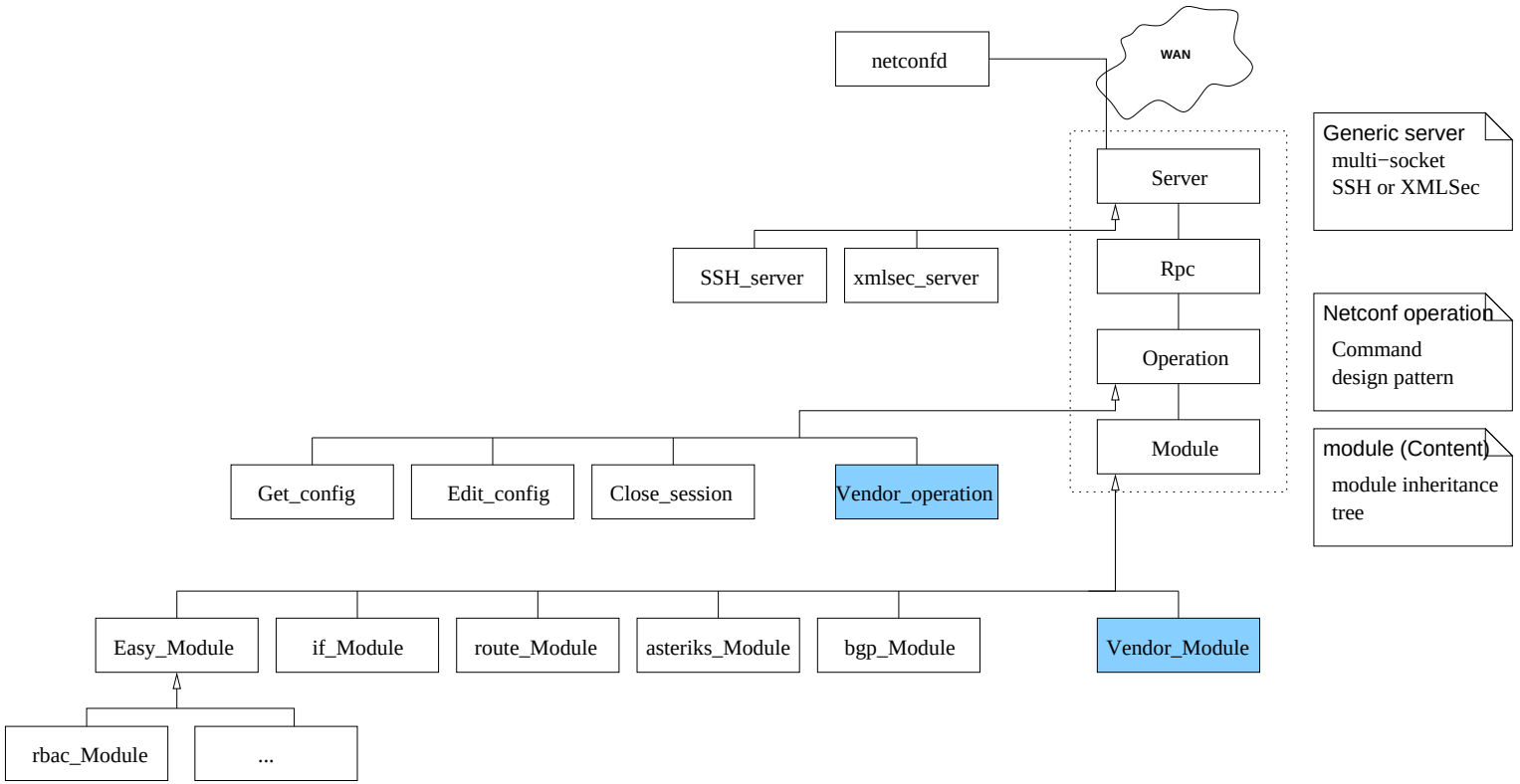


- Modèle de données de EnSuite
- Cas de *get*, *get-config*
- Filtrage par sous-arbre
- Propagation enfants/parents



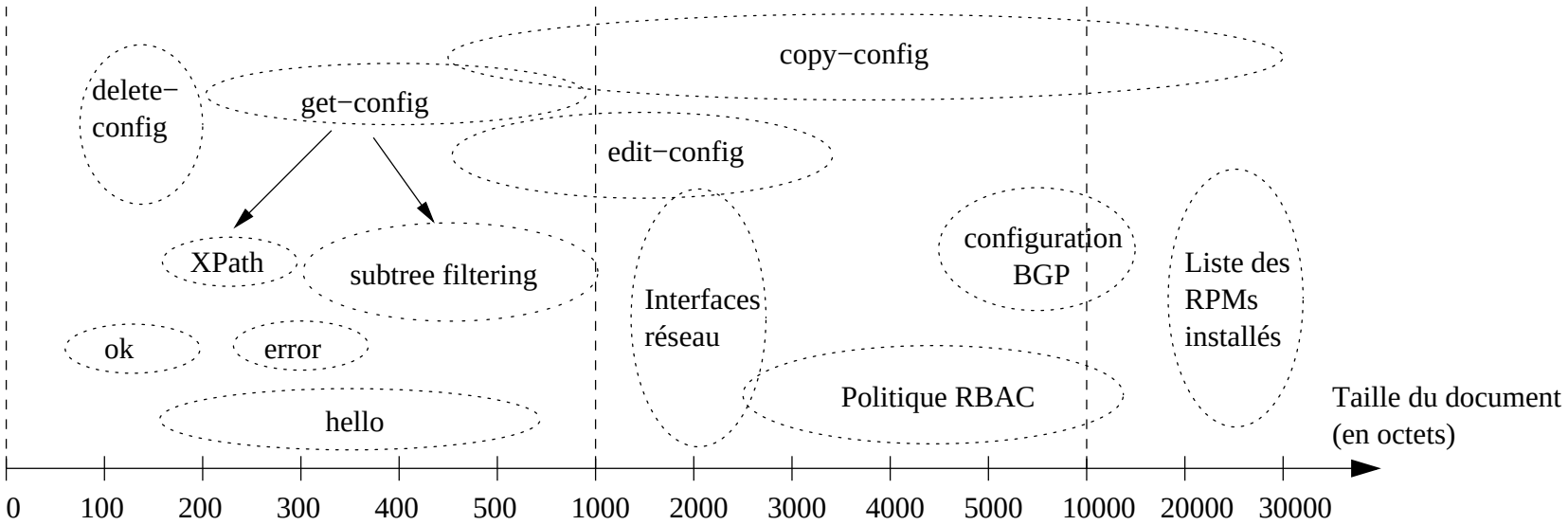
Implantation de Netconf/SSH : plateforme EnSuite

- Python (30 000 lignes de code)
- Agent :
  - Cœur du protocole
  - Extensions
- Manager
  - Filtrage/Classe
  - Extensions

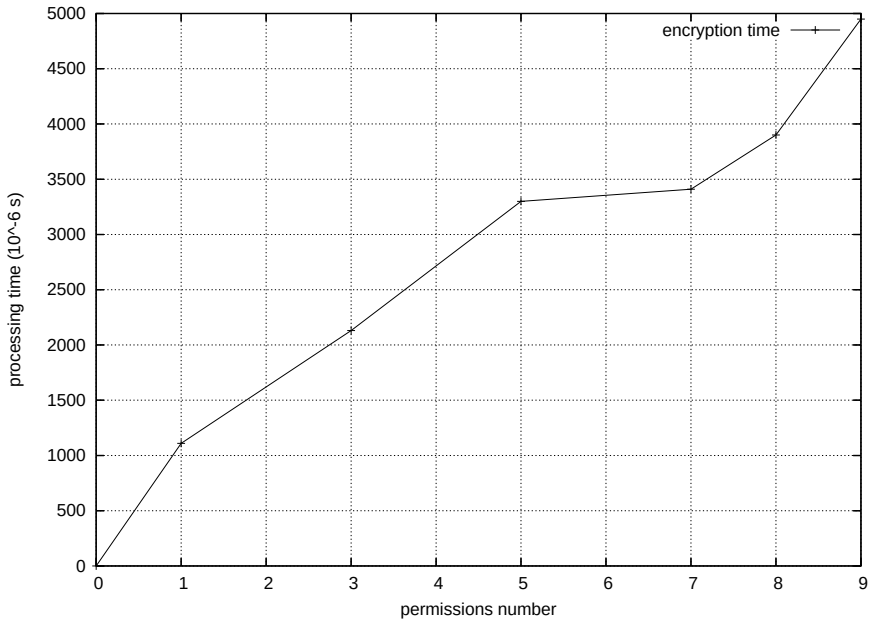


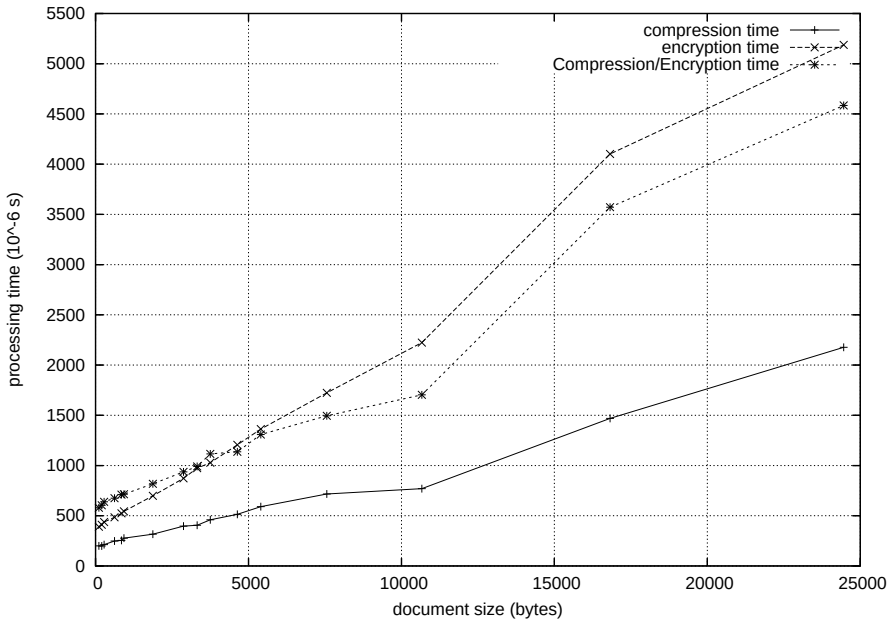
Tests de performances

- Paramètres de tests
  - Chiffrement
  - Authentification
  - Compression
  - Taille de la politique de contrôle d'accès
  - Comparaison XPath/filtrage par sous-arbre



Quelques résultats





- Temps de calcul proportionnel au nombre de permissions actives
- Variable selon la complexité de l'expression XPath
- Seuil d'intérêt pour la compression atteint rapidement

Sommaire

Conclusion

- Problématique : sécurité du plan de gestion IP
  - Les PKI s'imposent partout ⇒ uniformisation naturelle des mécanismes
  - Le contrôle d'accès distribué en environnement hétérogène ⇒ hétérogénéisation progressive
- Contributions
  - Cohérence globale
    - Parallèle groupe multicast/rôle RBAC
    - Utilisation de RADIUS comme référentiel unique des politiques de sécurité
  - Cohérence locale
    - Approche descendante de distribution : modèle central vers modèles cibles
    - Approche ascendante de vérification : modèles cibles vers modèle uniforme

Perspectives

- Utiliser la signature électronique pour lutter contre les reconfigurations silencieuses
- Etendre l'étude de performances focalisée sur les aspects sécurité
  - Netconf - SNMPv3 - SNMP/SSL
  - Netconf RBAC - VACM
- Améliorer l'algorithme de comparaison de politiques RBAC
  - Terminer le problème de la comparaison des ressources
  - Définir plusieurs niveaux d'équivalences (rôles et permissions)
- SAML
  - Propose une approche de coopération entre sites webs pour fédérer les identités des usagers
  - Analyser à quel point SAML se prête à notre contexte
  - Quel est l'impact sur les performances ?

Questions...


V. Cridlig, R. State, and O. Festor.
Role based access control for XML based management gateway.
In *Proceedings of the 15th IFIP/IEEE Distributed Systems: Operations and Management, DSOM 2004*, December 2004.


V. Cridlig, R. State, and O. Festor.
An Integrated Security Framework for XML based Management.
In *Proceedings of the 9th IFIP/IEEE International Symposium on Integrated Network Management, IM 2005*, IFIP Conference Proceedings, May 2005.


V. Cridlig, R. State, and O. Festor.
Role-Based Access Control for XML Enabled Multi-Protocol Management Gateways.
eTransactions on Network and Service Management, 3(1), April 2006.


V. Cridlig, R. State, and O. Festor.
A model for checking consistency in access control policies for network management.

In *Proceedings of the 10th IFIP/IEEE International Symposium on Integrated Management, IM 2007*, IFIP Conference Proceedings, May 2007.