

Authentification Distribuée sur Grille de Grappes basée sur LDAP

S. Varrette, S. Georget, J-L. Roch, F. Leprevost

Université du Luxembourg, LIASIT & FNRL, Luxembourg
INRIA Sophia Antipolis, Service DREAM, Sophia Antipolis, France
Projet MOAIS (CNRS/INPG/INRIA/UJF), Laboratoire ID-IMAG, Grenoble, France



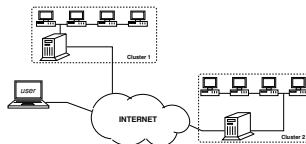
Conférence RenPAR'16, 6 avril 2005, Le Croisic, FRANCE

Sommaire

- 1 Contexte & Motivations
- 2 Notion de service de nommage et d'annuaire
- 3 Expérimentations
- 4 Conclusion & Perspectives

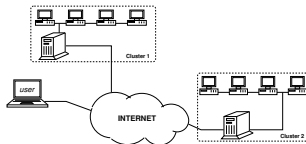
Contexte & Motivations

Environnement de type grille (pour le calcul)

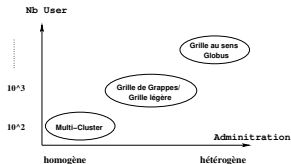


- "*Desktop Grid*" [1] : exploitation de ressources inexploitées

Environnement de type grille (pour le calcul)



- *"Desktop Grid"* [1] : exploitation de ressources inexploitées
- *"Grilles de Calcul"*



- agglomération de clusters
- accès limité à un certain nombre d'utilisateurs
- Sous-classification (nbre d'utilisateurs+homogénéité administrat^o)

Motivations



- Projet Grid5000 (<http://www.grid5000.org>)
 - 8 sites en France/Topologie : grille de grappe
 - "5000 noeuds"
 - capacité à rebooter dans un env. donné.
 - batch scheduler : OAR (<http://oar.imag.fr/>)
 - Besoin d'un système d'auth. robuste/scalable.
- Contraintes :
 - Disponibilité
 - Sécurité
 - Délégation
- Etude d'une alternative scalable à NIS



Authentification d'utilisateurs en environnement Linux

Repose sur 2 composants :

- ❶ Le système *PAM* (Pluggable Authentication Module)
 - intégration transparente de diverses techno. d'authentification
 - standard UNIX basé sur crypt, RSA, LDAP...
 - Base des services du système (login, passwd, su, ssh...)
 - API standard
 - mapping des requêtes d'auth. sur des actions spécifiques.
 - "modules PAM" (Ex : `pam_unix.so`, `pam_ldap.so`...).

Authentification d'utilisateurs en environnement Linux

Repose sur 2 composants :

- ❶ Le système *PAM* (Pluggable Authentication Module)
- ❷ Le système *NSS* (Name Service Switch) :
 - Utilisé par les appli. pour accéder aux informations utilisateur.
 - Informations traditionnellement contenues dans des tables
 - soit locales (/etc/passwd, /etc/shadow...)
 - soit sur un (des) serveur(s) distant(s) → 'Naming Service'
 - NSS = API interface entre application / naming service
 - spécifie la liste ordonnée des méthodes d'accès
 - fichier de configuration /etc/nsswith.conf

Notion de service de nommage et d'annuaire

Services de nommages

- Authentification hors réseau
 - tables locales passwd, shadow...
 - fichiers textes stockés dans le répertoire /etc

¹Network Information Service

²Domain Name Service

Services de nommages

- Authentification hors réseau
 - tables locales passwd, shadow...
 - fichiers textes stockés dans le répertoire /etc
- Sur un cluster : *service de nommage*
 - centralisation des informations sur un ou plusieurs serveurs
 - évite maintenance de la cohérence des copies locales
 - Pb du passage à l'échelle dans le cadre des grilles de grappes
 - Quelques exemples :
 - NIS¹(1985) : maps centralisées accessibles par appels RPC, modèle Maître/Esclave difficilement hiérarchique.
 - NIS+ : sécurité/arbre hiérarchique pour les données
 - DNS² : gestion hiérarchique des résolutions de noms.

¹Network Information Service

²Domain Name Service

Les annuaires électroniques

Definition (Annuaire électronique)

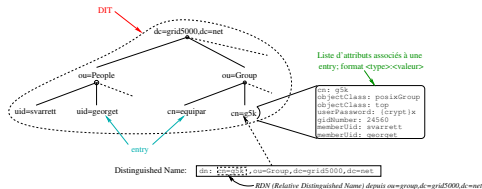
Un annuaire électronique est une base de données spécialisée qui permet de partager une base d'informations sur un réseau.

- Tout type d'informations : coordonnées → données systèmes.
- Partage de bases d'informations à travers un réseau
- normalisation ISO dédiée aux annuaires électroniques
 - norme X.500
- Version allégée de X.500, adaptée aux réseaux TCP/IP
 - LDAP³ [3]
 - Implémentation Open Source : OpenLDAP
<http://www.openldap.org>

³Lightweight Directory Access Protocol

LDAP

- LDAP = annuaire électronique sur le modèle de DNS, similaire à une BD.
- Nombreuses garanties en terme de sécurité
 - mécanismes de chiffrement (SSL/TLS)
 - mécanismes d'authentification (SASL⁴)
 - mécanismes de règles d'accès (ACL⁵)
- Organisation de contenu hiérarchique



⁴Simple Authentication and Security Layer

⁵Access Control List

Avantages/inconvénients LDAP vs BD

Critère	LDAP	Base de Données
Rapport R/W	optimisé en lecture	lecture/écriture
Extensibilité	facile	difficile
Distribution des tables	inhérente	rare [1]
Réplication	possible	possible
Modèle transactionnel	simple	avancé
Standard	oui	non (SGBD)

[1] Stonebraker, M & all, "Mariposa : A New Architecture for Distributed Data." In ICDE, 1994

Avantages/Inconvénients LDAP/NIS

Critère	LDAP	NIS
Port	spécifique (389/636)	arbitraire (RPC)
Chiffrement	possible	impossible
Contrôle d'accès	oui	non
Distribution des tables	oui	non
Réplication	oui (partielle possible)	oui (totale)
Sémantique recherches	avancée	simple

Expérimentations

Modèle local

- Difficulté d'administration
 - Nécessite intervention sur chaque noeud
- Solution *inefficace* : recherche linéaire dans les fichiers :

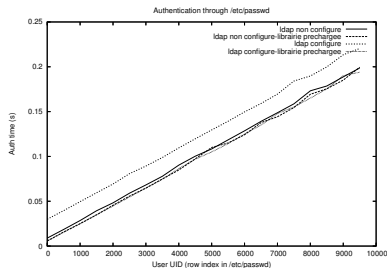
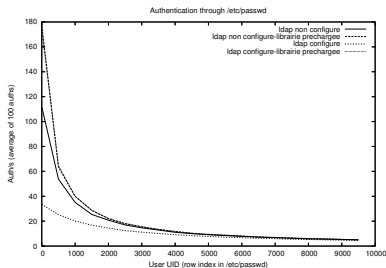


FIG.: Modèle par tables locales : impact du positionnement dans la table sur le temps d'authentification.

Comparaison NIS/Gestion locale

- Comparaison sur le temps d'authentification
 - Modèle local : dépend du nbre d'utilisateurs
 - Pour NIS : constant par rapport au nbre d'utilisateurs :

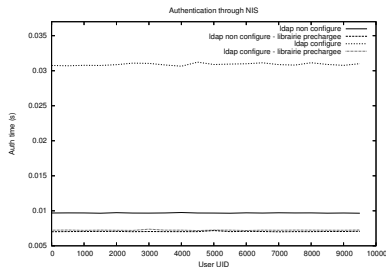
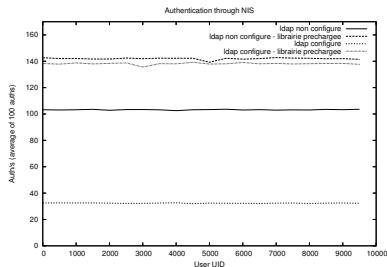
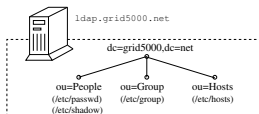


FIG.: Cas de NIS : indépendance de l'uid authentifié et de la taille de la base sur le temps d'authentification.

Modèle LDAP centralisé client/serveur

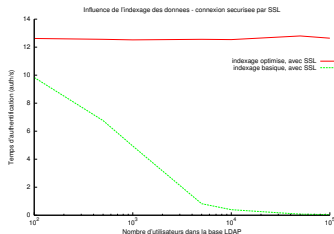
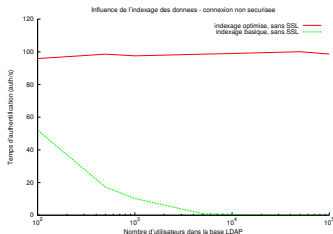


• Premier modèle pour Grid5000

- Serveur centralisé à Sophia
- Etude de ce modèle exhibe :

- Ses limites
- L'impact de la conf. du serveur LDAP :

• Influence de l'indexage des données dans LDAP :



Modèle LDAP centralisé client/serveur (2)

● Impact du niveau de logs d'un serveur LDAP

Niv.	Description	Impact
-1	enable all debugging	++++
0	no debugging	-
1	trace function calls	+++
2	debug packet handling	0
4	heavy trace debugging	+
8	connection management	++
16	print out packets sent/received	0
32	search filter processing	+
64	configuration file processing	0
128	access control list processing	+++
256	stats log connections/op/results	+
512	stats log entries sent	≈0
1024	print coms with shell backends	0
2048	print entry parsing debugging	0

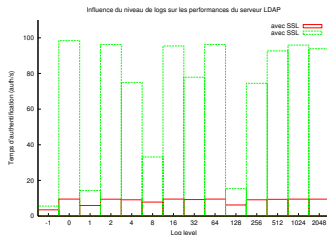


FIG.: Les niveaux de log dans OpenLDAP

Modèle LDAP centralisé client/serveur (3)

- Impact du backend utilisé
 - backend = manière dont sont stockées les données d'un serveur OpenLDAP.
 - Ex : ldbm (défaut), bdb...
 - Influence : quasi nulle ?
- Influence du chiff. symétrique + protocole d'échange de clé dans SSL
 - Comparaison des niveaux de sécurité HIGH et MEDIUM⁶
 - Influence nulle mais expérience inadaptée ?

⁶terminologie OpenSSL

Modèle LDAP centralisé client/serveur (4)

- Impact de SSL sur LDAP :

PAM		NSS		#authentications/s		
ldap	ldaps	ldap	ldaps	intervalle	moyenne	avec preload
X		X		entre 94 et 97	95.99	145.9
X			X	entre 92 et 95	94.15	144.4
	X	X		entre 12 et 13	12.46	14.28
	X		X	entre 12 et 13	12.51	14.27

Note : résultats obtenus pour client/serveur sur le même cluster

- Explication : nbre de mess. échangés par authentification
 - ldap : 45 messages LDAP + 35 messages TCP
 - ldaps : 70 messages TLS (LDAPS)+ 47 messages TCP
- Bilan : divise les performances par 9 mais indispensable.

Modèle LDAP centralisé client/serveur (5)

- Influence de la latence entre client/serveur LDAP
 - Client et serveur sur des clusters différents

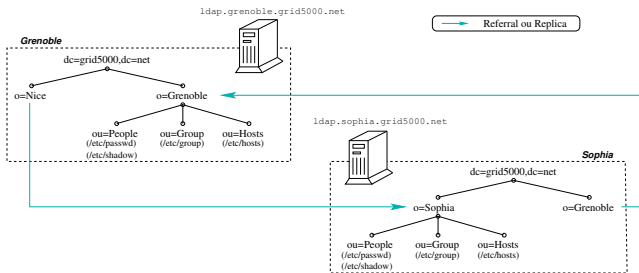
PAM		NSS		#authentications/s	
ldap	ldaps	ldap	ldaps	intervalle	moyenne
X		X		entre 15 et 22	20.1
X			X	entre 7 et 23	17.6
	X	X		entre 6 et 7	6.89
	X		X	entre 5 et 7	6.79

- Pour comparaison : influence de la latence entre C/S NIS

Type latence	#authentications/s			
	intervalle	moyenne	intervalle avec preload	moy. avec preload
Intra-Cluster	entre 230 et 310	263.0	entre 266 et 338	290
Inter-Cluster	entre 32 et 37	35.1	entre 31 et 38	35.3

Modèle distribué plat

- LDAP permet la distribution des tables (modèle DNS)
 - Soit par *referral* $\simeq$ pointeur sur un serveur
 - Pb : efficacité + disponibilité (solution : proxy cache ?)
 - Soit par réplication partielle de certaines branches



Modèle distribué plat (2)

- Chaque site est maître de sa branche et esclave pour les autres
- Intégration du contenu de chaque branche dans la hiérarchie LDAP via le backend meta

Mode	backend meta		#auth./s (ldap)			#auth./s (ldaps)			Commentaires
	Grenoble	Sophia	min.	moy.	max.	min.	moy.	max.	
central.	désact.	désact.	84.9	89.0	107.3	16.7	17.4	17.9	mode centralisé (rappel)
réplica	désact.	désact.	82.9	96.6	108.9	17.2	17.4	17.8	Impact conf. des réplicas
réplica	local	local	82.0	87.9	97.1	16.9	17.1	17.5	User géré à Grenoble
réplica	local	local	81.3	88.9	97.6	16.8	17.2	17.5	User géré à Sophia
réplica	local	distant	35.8	36.8	38.3	13.3	13.4	13.7	User géré à Grenoble impact backend distant
réplica	local	distant	16.1	16.5	17.0	9.2	9.2	9.4	User géré à Sophia impact backend distant

- Avantages de l'approche par réplica :
 - Performances garanties par rapport au modèle centralisé
 - Pas de pbs de blocage lorsqu'un serveur "tombe"
- Inconvénient : mise en place + lourde

Conclusion & Perspectives

- NIS reste une solution rapide et performante.
- Pbs de sécurité de NIS pallié par notre approche
 - basée sur LDAP
 - alternative "plus simple" que Globus
 - mode distribué "plat" par réplica adapté à Grid5000
- Plateforme actuelle de Grid5000
- Perspectives :
 - Ajout d'informations complémentaires (pour autres applis)
 - gestion des ressources via LDAP (syst. d'infos)
 - Tests de performances pour le modèle referral+proxy cache
 - Comparaison avec Globus.

Bibliographie



Fedak (G.), Germain (C.), N'eri (V.) et Cappello (F.). –

Xtremweb : A generic global computing system. *In : In IEEE Int. Symp. on Cluster Computing and the Grid.* –
2001.



Foster (I.), Kesselman (C.), Tsudik (G.) et Tuecke (S.). –

A Security Architecture for Computational Grids. *In : Fifth ACM Conference on Computer and Communications Security Conference*, pp. 83–92. –
San Francisco, California, 3–5 Novembre 1998.



Wahl (M.), Howes (T.) et Kille (S.). –

RFC 2251 - *Lightweight Directory Access Protocol (v3)*. –
Rapport technique, IETF, Dec. 1997. [http ://www.ietf.org/rfc/rfc2251.txt](http://www.ietf.org/rfc/rfc2251.txt)



Varrette (S.), Roch (J.-L.), Denneulin (Y.) et Leprevost (F.). –

Secure Architecture for Clusters and Grids. *In : Proceedings of the 2ème Conférence Internationale sur les Infrastructures Critiques CRIS 2004*), éd. par IEEE. –
Grenoble, France, October 2004.



Varrette (S.), Georget (S.), Roch (J.-L.), et Leprevost (F.). –

Authentification Distribuée sur Grille de Grappes basée sur LDAP. *In : Proceedings des 16èmes rencontres francophones du parallélisme (RenPar'16)* –
Le Croisic, France, April 6-8 2005.

Merci pour votre attention...

Questions ?

