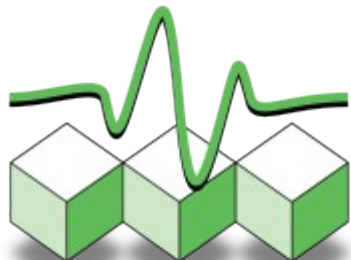


LINAGORA

Formation



Administration et sécurité



Optimisation OpenLDAP

Auteurs :

- Clément OUDOT, Raphaël OUAZANA et Sébastien BAHLOUL
- LINAGORA *Formation* : formation@linagora.com




Licence

Paternité - Pas d'Utilisation Commerciale - Partage des Conditions Initiales à l'Identique 2.0 France

Vous êtes libres :

- de reproduire, distribuer et communiquer cette création au public,
- de modifier cette création.

Selon les conditions suivantes :

-  Paternité. Vous devez citer le nom de l'auteur original.
-  Pas d'Utilisation Commerciale. Vous n'avez pas le droit d'utiliser cette création à des fins commerciales.
-  Partage des Conditions Initiales à l'Identique. Si vous modifiez, transformez ou adaptez cette création, vous n'avez le droit de distribuer la création qui en résulte que sous un contrat identique à celui-ci.

À chaque réutilisation ou distribution, vous devez faire apparaître clairement aux autres les conditions contractuelles de mise à disposition de cette création.

Chacune de ces conditions peut être levée si vous obtenez l'autorisation du titulaire des droits.

Ce qui précède n'affecte en rien vos droits en tant qu'utilisateur (exceptions au droit d'auteur : copies réservées à l'usage privé du copiste, courtes citations, parodie...)

Pourquoi LINAGORA met ce support sous licence Creative Commons

- Volonté de contribuer activement à l'essor du logiciel libre
- Promouvoir l'échange et favoriser l'émulation communautaire
- Assurer la pérennité de l'industrie logiciel libre et ne comptabiliser que la Valeur Ajoutée (le formateur)
- Partager le savoir et la connaissance à une vaste échelle

LINAGORA croit au Libre !

Présentation du formateur

- Parcours du formateur

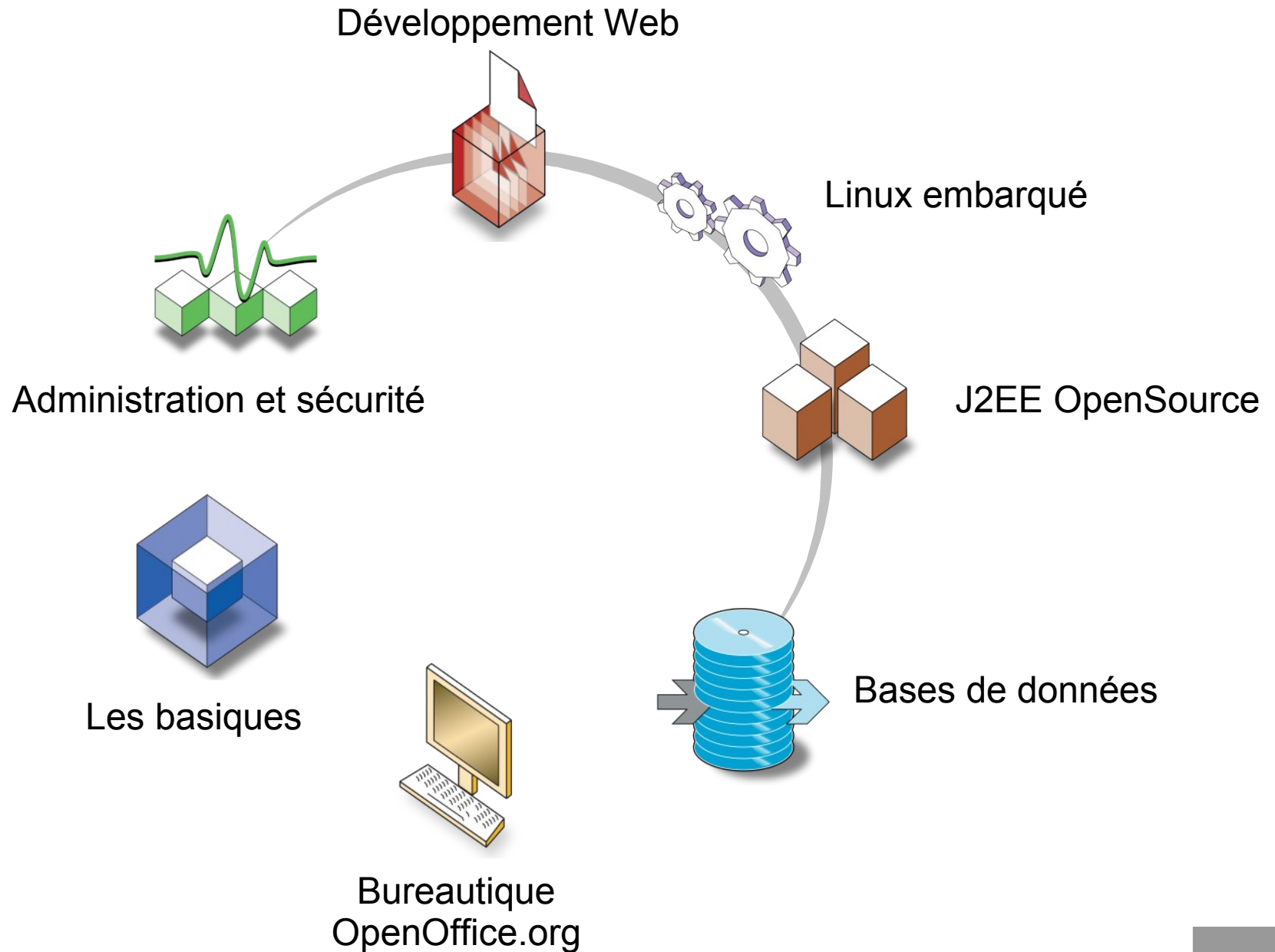
LINAGORA, premier EOS

- Créateur des concepts SS2L (Société de Services en Logiciels Libres) et TM2L (Tierce Maintenance Logiciel Libre), LINAGORA se définit désormais comme un Éditeur Orienté Service (EOS).
- LINAGORA propose une **Open Source Software Assurance** (OSSA) sur 150 logiciels libres :
 - Prêts à l'industrialisation, sur une plate-forme unique : le 08000LINUX.com.
 - Avec garantie de service contractuelle : en cas de bug, LINAGORA s'engage au résultat sur des délais de résolution.
 - Gestion de la feuille de route du logiciel pour le compte du client et s'engage au reversement des développements.
- LINAGORA apporte également son expertise sur toute une gamme de **services professionnels** et de **formations** au travers de **LINAGORA Formation**.

LINAGORA Formation

- **7 années d'expérience**, au service des technologies libres et Open Source
- **40 modules** de formation répartis au travers de **7 filières**
- Un cadre agréable, au cœur de Paris
- Deux salles de formation climatisées pouvant accueillir jusqu'à 10 stagiaires.
- **2006 : Plus de 150 stages** effectués
- **2006 : Plus de 900 stagiaires**
- **Une satisfaction** moyenne client de **18/20**
- **Une note moyenne formateur** de **16,27/20**

Filières de formations



Organisation générale et planning

09h30 : début des cours

10h30 : pause du matin

10h45 : reprise des cours

12h00 : pause déjeuner

13h00 : reprise des cours

15h00 : pause de l'après-midi

15h15 : reprise des cours

17h30 : fin de journée

17h30 : libre discussion avec le formateur

Jour 1 :

- Introduction
- Optimisation
- Sauvegarde
- Script d'initialisation

Jour 2 :

- Traces applicatives
- Mandataire LDAP
- Équilibrage de charge avec LVS
- Supervision Nagios et Cacti

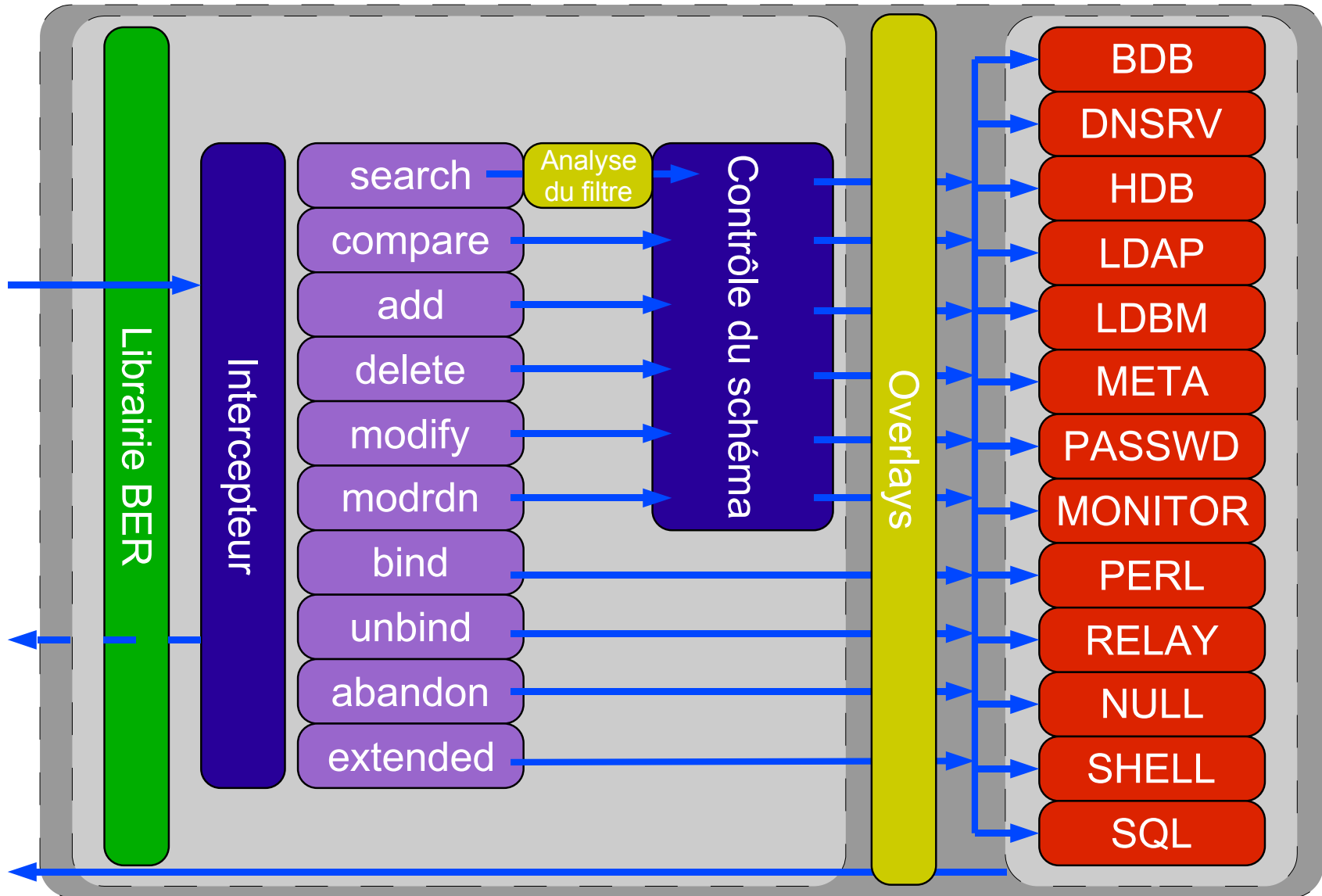
Plan de cours

- Introduction
- Optimisation
- Sauvegardes
- Script d'initialisation
- Traces applicatives
- Mandataire LDAP
- Équilibrage de charge avec LVS
- Supervision Nagios et Cacti

Le choix d'OpenLDAP

- OpenLDAP de qualité industrielle :
 - Support des modes de réplication et de l'initialisation de réplicat
- OpenLDAP moteur dans les standards LDAP :
 - SyncRepl
 - Internationalisation
 - Gestion des identifiants indépendants entryUUID
- Performances & architecture permettant d'obtenir des charges extrêmes :
 - DGCP : infrastructure d'annuaire pour des accès en lecture et écriture à plus de 5000 requêtes par seconde
 - Carrefour : 9 annuaires en haute-disponibilité répartis sur sites distants
- Utilisé dans les projets InterLDAP et FederID

Rappel du fonctionnement d'OpenLDAP



Plan de cours

- Introduction
- Optimisation
- Sauvegardes
- Script d'initialisation
- Traces applicatives
- Mandataire LDAP
- Équilibrage de charge avec LVS
- Supervision Nagios et Cacti

Optimisation du système

- Fichiers de contrôles des limitations :
 - `/proc/sys/kernel/threads-max` : nombre maximal de fils d'exécution par processus
 - `/proc/sys/fs/file-max` : nombre maximal de descripteurs de fichiers ouverts par processus
 - `/proc/sys/net/ipv4/ip_local_port_range` : portée des ports ouvrable sur le serveur
- Utilisation des TCP-wrappers à banir : 3 fichiers ouverts par connexion !
- Utilisation d'un noyau 2.6 préemptif (Algorithme en $O(1)$ au lieu de $O(n)$ pour un noyau 2.4)
- Serveur DNS cache local (extrêmement important !) et adresses locales (serveurs proches, routeurs, ...) dans `/etc/hosts`, intégration de `nscd`

Optimisation de l'architecture

- Équilibrage de charge sur des annuaires en lecture
- Utilisation de mandataires avec rôle de cache
- Utilisation de backends différents suivant la section de l'arborescence (DIT) visé : utilisation de backends sous-jacents (directive subordinate)
- Délégation au travers des referrals (default et smart referral)
- Architecture répartie avec minimisation des flux réseaux de lecture

Optimisation LDBM

- Uniquement dans slapd.conf :
 - cachesize <n> : nombre d'entrées maintenues en mémoire par slapd
 - dbcachesize <n> : taille en octet maintenue en mémoire pour chaque fichier d'index ouvert
 - dbnolocking : évite le verrouillage des bases à chaque modification (peut générer des corruptions en cas d'utilisation des outils slap*)
 - dbnosync : évite la synchronisation instantanée à chaque modification de la mémoire sur le disque
 - dbsync <freq> <maxdelays> <delay> : (implique dbnosync) synchronise la base en attente en mémoire tous les <freq> secondes. Le serveur évite la synchronisation en période d'utilisation en attendant <delay> secondes, et ceci de façon répétée <maxdelays> fois
- Attention, LDBM n'est plus maintenu et sera supprimé dans la prochaine version d'OpenLDAP !

Optimisation BDB

- Dans slapd.conf :
 - cachesize <n> : nombre d'entrées maintenues en mémoire par slapd (1000 par défaut)
 - cachefree <n> : nombre d'entrées à supprimer du cache quand celui-ci est complet (1 par défaut)
 - checkpoint <size> <time> : la base de données synchronise les historiques sur le disque tous les <size> kilo octets ou toutes les <time> secondes
 - dbnosync : évite la synchronisation instantanée à chaque modification de la mémoire sur le disque
 - dirtyread : permet la lecture de données non synchronisées avec le disque (peut engendrer des retours d'entrées non valables si une des opérations en cours est annulée). Par défaut, les entrées sont verrouillées lors de leur modification donc inaccessibles.

Optimisation BDB

- Dans slapd.conf :
 - idlccachesize <n> : spécifie le nombre en espaces indexés d'entrées fréquemment recherchées
 - lockdetect {...} : mode de détection des verrous multiples et abandon des opérations en cours :
 - oldest
 - youngest
 - fewest
 - random
 - default
 - searchstack <depth> : profondeur des piles par défaut stockant les filtres de recherches (16 * 512 ko soit 8 Mo). L'allocation supplémentaire est très pénalisante, mais l'augmenter nécessite plus de mémoire
 - shm_key : identifiant de la clé de mémoire partagée
 - index_substr_if_minlen : longueur minimale d'un index de sous-chaîne

Optimisation BDB

- Dans DB_CONFIG :
 - set_cachesize <gbytes> <bytes> <ncache> : taille du cache :
 - gbytes : nombre de giga octets
 - bytes : nombre d'octets
 - ncache : nombre de zones mémoire à créer (une seule zone si 0 ou 1)
 - set_flags <flag> : positionne des drapeaux :
 - DB_TXN_WRITE_NOSYNC : évite la synchronisation automatique des données en mémoire avec le disque. Attention : risque d'endommager les données
 - DB_LOG_AUTOREMOVE : supprime automatiquement les fichiers d'historique non utilisés. Attention : cela empêche un recouvrement critique des données
 - set_lg_max <n> : taille en octets des fichiers d'historique
 - set_lg_bsize <n> : taille en octets de la zone tampon
 - set_lg_regionmax <n> : taille en octets du cache des noms des fichiers d'historique
 - set_lg_dir <n> : répertoire de stockage des fichiers d'historique

Calcul des caches BDB

- Taille idéale :
 - Taille totale des fichiers DB (`du -hs *.bdb -c`)
 - Ajouter l'évolution prévue de la taille de l'annuaire
- Taille optimale : taille des données les plus utilisées :
 - Utilisation des outils BerkeleyDB : `db_stat -c fichier.bdb` :
 - Underlying database page size : taille d'une page
 - Number of tree internal pages : nombre de pages internes
 - Calcul du cache minimal : $\sum (\text{nb pages internes} + 1) * \text{taille d'une page}$
 - Vérification : `db_stat -m`
- Cache des historiques :
 - `set_lg_max > 4 * set_lg_bsize`

Nombre de clients simultanés

- C'est un des critères majeurs de performance d'un annuaire LDAP
- Augmentation par le matériel :
 - Plus de mémoire : l'utilisation de support physique constitue la principale source de ralentissement des serveurs LDAP
 - Plus de serveurs « simples » plutôt que des machines quadri ou octo-processeur
 - Cartes réseaux gigabit
- Augmentation par le logiciel :
 - concurrency <n> : Nombres de connexions simultanées
 - threads <n> : Nombre de fils d'exécution pour la file initiale :
 - Nombre optimal : 16 fois le nombre de processeurs

Limitation des types de recherches

- La limitation des types de recherches peut se faire au travers des syntaxes de chaque attribut et ainsi permettre d'éviter de tomber hors du champ des indexes
- Validation en fonction de la syntaxe :
 - attributetype (0.9.2342.19200300.100.1.20
 - DESC 'RFC1274: home telephone number'
 - NAME ('homePhone' 'homeTelephoneNumber')
 - EQUALITY telephoneNumberMatch
 - SUBSTR telephoneNumberSubstringsMatch
 - SYNTAX 1.3.6.1.4.1.1466.115.121.1.50)
- Syntaxe et normalisation associées :
 - ldapSyntax (1.3.6.1.4.1.1466.115.121.1.50 DESC 'Telephone Number')

Autres limitations

- Contrairement à d'autres serveurs, OpenLDAP permet de spécifier des limites en temps de réponses et en nombre d'entrées retournées qui dépendent de l'utilisateur connecté (authentifié ou non) :
 - `limits <who> <limit>+`
- `conn_max_pending <n>` : nombre de requêtes simultanées en attente pour une connexion anonyme
- `conn_max_pending_auth <n>` : nombre de requêtes simultanées en attente pour une connexion authentifiée
- `maxderefdepth <n>` : nombre maximal de dérèférencement au travers d'alias

Optimisation des applications

- Ne pas ouvrir de multiples connexions dans un script :
 - Risque d'incohérence des résultats à l'affichage
- Travailler à l'intérieur d'une connexion :
 - le protocole LDAP sait effectuer plusieurs opérations à l'intérieur de la même connexion
 - Attention, l'opération unbind ne fait pas que déconnecter l'utilisateur, elle ferme aussi la connexion
- Ne pas vérifier les mises-à-jour par des lectures :
 - Si le code retour est égal à 0, l'opération s'est bien déroulée
- Ne pas stocker les fichiers binaires dans l'annuaire :
 - Ils ralentissent fortement les temps de réponse
 - Utiliser le DN ou un autre identifiant pour nommer les fichiers sur le disque

Optimiser la sécurité

- Limiter le nombre de résultats retournés en anonyme ainsi que le temps maximum
- Limiter les opérations étendues, les recherches en suivant les alias et les referrals
- Limiter les règles d'égalité partielle, notamment sur les attributs longs
- Positionner les quelques paramètres réseaux ci-dessous :
 - `sockbuf_max_incoming <n>` : taille maximale du buffer recevant les informations sur une connexion anonyme
 - `sockbuf_max_incoming_auth <n>` : taille maximale du buffer recevant les informations sur une connexion authentifiée
 - `idletimeout <n>` : temps maximum d'une connexion inactive
- Pas de protection interne contre les attaques DDOS

Bien indexer son annuaire

- À partir d'un annuaire vide, établir les recherches effectuées couramment par les différents clients de l'annuaire
- À partir d'un annuaire existant, mettre en œuvre des dispositifs de captures de trames, ou analyser les traces logicielles, afin de mettre en évidence l'usage des annuaires :
 - Portée des recherches
 - Composition du filtre et attributs associés
 - attribut = * : index de type présence (pres)
 - attribut = valeur : index de type égalité (eq)
 - attribut = a* : index de type égalité partielle finale (subfinal)
 - attribut = *a : index de type égalité partielle initiale (subinitial)
 - attribut = a*b : index de type égalité partielle quelconque (subany)
 - Index de type égalité partielle sub = subinitial + subany + subfinal
- Penser à réindexer après tout modification
- Penser à l'utilisation de l'option -q pour une réindexation plus rapide, voire la suppression temporaire des autres index

Plan de cours

- Introduction
- Optimisation
- Sauvegardes
- Script d'initialisation
- Traces applicatives
- Mandataire LDAP
- Équilibrage de charge avec LVS
- Supervision Nagios et Cacti

Types de sauvegardes

- Données seules : export LDIF
- Données et informations opérationnelles : export LDIF
- Configuration : copie de fichiers
- Fichiers de base de données : copie de fichiers
- Fichiers d'historique de la base de données : copie de fichiers
- Fichiers des traces applicatives : copie de fichiers ou réseau
- Fichiers de la réplication : copie de fichiers

Export LDIF

- Export à chaud (annuaire allumé):
 - Utilisation de ldapsearch :
 - Permet de sauvegarder à travers le réseau
 - Nécessite des droits sur la base
 - Choix des attributs opérationnels
 - Utilisation de slapcat
 - Sauvegarde en local
 - Très rapide
 - Entrées non triées
 - Attributs opérationnels fournis obligatoirement
- Export annuaire éteint :
 - Uniquement avec slapcat
 - Peut être fait sur un réplicat, pour maintenir l'annuaire principal allumé

Import LDIF

- Import à chaud :
 - Utilisation de ldapadd :
 - Choix des données à importer
 - Gestion des erreurs
 - Import à distance
 - Pas de récupération des attributs opérationnels
 - Pas possible avec un fichier issu de slapcat
 - Utilisation de slapadd : vivement déconseillé
- Import annuaire éteint :
 - Utilisation de slapadd :
 - Import local uniquement
 - Utilisé pour un import total
 - Conserve les attributs opérationnels
 - Très rapide avec l'option -q (moins de tests d'intégrité)
 - Possibilité de paramétrer la directive tool-threads de slapd.conf pour accélérer encore l'import

Copie des fichiers

- Avantages :
 - Compatible avec des logiciels de sauvegarde
 - Possibilité de sauvegarder données et configuration
 - Les exports LDIF peuvent faire partie des fichiers copiés
- Inconvénients :
 - La sauvegarde des fichiers de base de données implique celle des historiques (sous peine de corruption de la base au prochain redémarrage)
 - Difficile de rechercher des données dans les fichiers binaires
 - Procédures de recouvrement des données plus complexes
 - Peut être incompatible avec différentes architectures

Plan de cours

- Introduction
- Optimisation
- Sauvegardes
- Script d'initialisation
- Traces applicatives
- Mandataire LDAP
- Équilibrage de charge avec LVS
- Supervision Nagios et Cacti

Script d'initialisation

- Aucun script n'est fourni par défaut dans OpenLDAP
- Chaque distribution fournit ses propres scripts
- Rôle du script :
 - Lancer le démon :
 - Vérifier qu'il n'est pas en activité
 - S'assurer que les droits sont suffisants
 - Vérifier la configuration avant le lancement
 - Stopper le démon :
 - Envoyer un signal d'arrêt
 - Forcer l'arrêt si nécessaire
 - Autres :
 - Sauvegarde
 - Outils BerkeleyDB

Créer son script

- Script shell ou bash
- Exécutable
- Installé dans `/etc/init.d`
- Liens symboliques dans `/etc/rc.d` pour démarrage et arrêt automatiques
- Paramètres minimaux :
 - start
 - stop
 - restart
- Lancement des exécutables `slapd` et `slurpd`
- Arrêt des processus, identifiés par PID ou nom de processus

Script générique LINAGORA

- Téléchargement sur <http://www.linagora.org/article122.html>
- Il requiert les outils suivants :
 - logger : pour transmettre les messages à syslog
 - BerkeleyDB : pour les outils de recouvrement et d'archivage
 - OpenLDAP : pour les utilitaires de réindexation, de sauvegarde et de test
- Configuration :
 - Interne au script (déconseillé)
 - Externe, dans /etc/default
- Compatible OpenLDAP 2.2 et 2.3

Actions du script

- start :
 - Effectue un test de la configuration
 - Démarre slurpd si des réplicats sont configurés
 - Démarre slapd en recouvrant les données si demandé
- stop :
 - Arrête slapd et sauvegarde les données si demandé
 - Arrête slurpd s'il est démarré
- forcestop :
 - Si les PID sont récupérés, un kill -KILL est effectué sur ceux-ci
 - Sinon un killall -KILL sur le nom des binaires est effectué
- restart :
 - Lance les commandes de l'action stop
 - Lance les commandes de l'action start

Autres actions

- configtest :
 - la configuration est testée (utilitaire slaptest)
- db_recover :
 - les données sont réparées (utilitaire db_recover)
- reindex :
 - les données sont réindexées (utilitaire slapindex)
- removelogs :
 - les anciens historiques de la base de données sont supprimés (utilitaire db_archive)
- backup :
 - les données sont sauvegardées sous format LDIF (utilitaire slapcat)

Configuration du script - obligatoire

- IP : adresse (interface) d'écoute d'OpenLDAP. Le caractère * peut être utilisé pour désigner toutes les interfaces
- PORT : port d'écoute d'OpenLDAP. Si plusieurs ports sont concernés, utiliser le paramètre SLAPD_SERVICES
- SLAPD_PATH : répertoire d'installation d'OpenLDAP. Il permet de renseigner facilement les paramètres suivants
- DATA_PATH : répertoire de stockage des données, comme indiqué dans le paramètre directory de slapd.conf
- SLAPD_PID_FILE : fichier de stockage du PID de slapd, comme indiqué dans le paramètre pidfile de slapd.conf
- SLAPD_CONF : fichier de configuration principal
- SLAPD_SERVICES : liste d'URI LDAP, séparées par un espace, sur lesquelles écoute OpenLDAP

Configuration du script - obligatoire

- SLAPD_BIN : chemin du binaire slapd
- SLAPCAT_BIN : chemin de l'utilitaire slapcat
- SLAPINDEX_BIN : chemin de l'utilitaire slapindex
- SLAPTEST_BIN : chemin de l'utilitaire slaptest
- SLURPD_PID_FILE : fichier de stockage du PID de slurpd, comme indiqué dans le paramètre replica-pidfile de slapd.conf
- SLURPD_BIN : chemin du binaire slurpd.
- BDB_PATH : répertoire d'installation de BerkeleyDB. Il permet de renseigner facilement les paramètres suivants
- DB_ARCHIVE_BIN : chemin de l'utilitaire db_archive
- DB_RECOVER_BIN : chemin de l'utilitaire db_recover

Configuration du script - obligatoire

- **RECOVER_AT_STARTUP** : activer la réparation de la base de données avant de démarrer slapd. Ceci est inutile et déconseillé pour OpenLDAP 2.3.x, mais fortement recommandé pour OpenLDAP 2.2.x
- **BACKUP_AT_SHUTDOWN** : sauvegarder les données après l'arrêt de slapd
- **BACKUP_PATH** : répertoire où sont stockés les fichiers LDIF
- **BACKUP_FILE** : chemin du fichier de sauvegarde. Si le nom du fichier est fixe, il sera écrasé à chaque nouvelle sauvegarde. Il est possible de le rendre variable en y incluant la date
- **TIMEOUT** : temps maximum d'attente de la fin d'un processus. Après ce temps, un message invite à utiliser l'action forcestop
- **FD_LIMIT** : nombre limite de descripteurs de fichiers ouverts

Configuration du script - facultative

- **SLAPD_PARAMS** : options supplémentaires à passer à slapd. Les options -h, -f, -u et -g sont déjà inscrites
- **SLAPD_USER** : utilisateur propriétaire des processus slapd et slurpd
- **SLAPD_GROUP** : groupe propriétaire des processus slapd et slurpd
- **SLURPD_PARAMS** : options supplémentaires à passer à slurpd. L'option -f est déjà inscrite

Niveaux des traces applicatives

- 1 (0x1 trace) : appels des fonctions
- 2 (0x2 packet) : gestion des paquets
- 4 (0x4 args) : arguments des fonctions (très verbeux)
- 8 (0x8 conns) : gestion des connexions
- 16 (0x10 BER) : affichage des paquets envoyés et reçus
- 32 (0x20 filter) : exécution des filtres de recherche
- 64 (0x40 config) : analyse du fichier de configuration
- 128 (0x80 ACL) : analyse des ACLs
- 256 (0x100 stats) : statistiques sur les opérations
- 512 (0x200 stats2) : statistiques sur les entrées envoyées

Niveaux des traces applicatives

- 1024 (0x400 shell) : communication avec le shell
- 2048 (0x800 parse) : analyse d'une entrée
- 4096 (0x1000 cache) : cache (inutilisé)
- 8192 (0x2000 index) : indexation (inutilisé)
- 16384 (0x4000 sync) : réplication SyncRepl
- 32768 (0x8000 none) : seuls les messages ne dépendant pas du niveau de traces applicatives
- -1 : tous les niveaux réunis

Syslog

- Fichier de configuration : `/etc/syslog.conf`
- Relance du démon : `/etc/init.d/syslog restart`
- Optimisation en rendant les traces asynchrones :
 - `local4.*` `-/var/log/slaped.log`
- Centralisation des traces sur un serveur distant :
 - `local4.*` `-@SERVEUR`
 - penser à activer l'option `-r` sur le serveur syslog distant
- **Plus généralement, le programme netcat permet d'envoyer des informations sur un serveur distant**

Captures de flux

- La capture de flux permet de se positionner entre le client et le processus OpenLDAP
- Les traces applicatives ne permettent d'analyser que les informations parvenues correctement à OpenLDAP
- Le logiciel le plus répandu est Wireshark (anciennement Ethereal) :
 - Analyse les échanges SSL/TLS
 - Décode les flux LDAP
 - Logiciel libre
 - <http://www.wireshark.org/>
- Un processus collecte les informations dans un fichier sur le serveur
- Ce fichier peut être ensuite analysé graphiquement sur un poste de travail

Exemple de capture Wireshark (Ethereal)

(Untitled) - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: + Expression... Clear Apply

No. .	Time	Source	Destination	Protocol	Info
65	4.920019	127.0.0.1	127.0.0.1	TCP	57875 > 1389 [ACK] Seq=1121 Ack=71962 Win=49460 Len=0 TSV=8309959 T
66	4.920074	127.0.0.1	127.0.0.1	TCP	57875 > 1389 [ACK] Seq=1121 Ack=71976 Win=49460 Len=0 TSV=8309960 T
67	5.690528	127.0.0.1	127.0.0.1	LDAP	MsgId=13 Search Request, Base DN=ou=personnes,dc=lapeyre,dc=com
68	5.693399	127.0.0.1	127.0.0.1	LDAP	MsgId=13 Search Entry
69	5.693460	127.0.0.1	127.0.0.1	TCP	57875 > 1389 [ACK] Seq=1219 Ack=72252 Win=49460 Len=0 TSV=8310153 T

Frame 74 (173 bytes on wire, 173 bytes captured)

- Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
- Internet Protocol, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
- Transmission Control Protocol, Src Port: 57875 (57875), Dst Port: 1389 (1389), Seq: 1219, Ack: 72558, Len: 107
- Lightweight Directory Access Protocol
 - LDAP Message, Search Request
 - Message Id: 14
 - Message Type: Search Request (0x03)
 - Message Length: 71
 - Response In: 75
 - Base DN: uid=1234,ou=personnes,dc=lapeyre,dc=com
 - Scope: Base (0x00)
 - Dereference: Base Object (0x02)
 - Size Limit: 0
 - Time Limit: 0
 - Attributes Only: False
 - Filter: (objectClass=*)
 - LDAP Controls

```

0000  00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00  .....E.
0010  00 9f af 1c 40 00 40 06 8d 3a 7f 00 00 01 7f 00  ....@.@. ....
0020  00 01 e2 13 05 6d d4 31 6b 91 d3 f8 f2 2f 80 18  ....m.l k.../..
0030  30 4d fe 93 00 00 01 01 08 0a 00 7e ce 33 00 7e  0M..... ~.3.~
    
```

File: "/tmp/etherXXXXkv2XRV" 78 KB 00:00:06 P: 78 D: 78 M: 0 Drops: 0

Plan de cours

- Introduction
- Optimisation
- Sauvegardes
- Script d'initialisation
- Traces applicatives
- Mandataire LDAP
- Équilibrage de charge avec LVS
- Supervision Nagios et Cacti

Utilité d'un mandataire

- Virtualiser différents annuaires en un seul point d'entrée (rôle de méta annuaire virtuel) ou pour répartir la charge
- Présenter l'information sous différentes formes
- Diriger la même connexion sur deux serveurs d'annuaires différents en fonction de la nature de l'action (consultation / mise à jour)
- Filtrer le contenu en fonction du point d'accès et de règles spécifiques
- Adapter des traitements sur le mandataire sans toucher au serveur principal

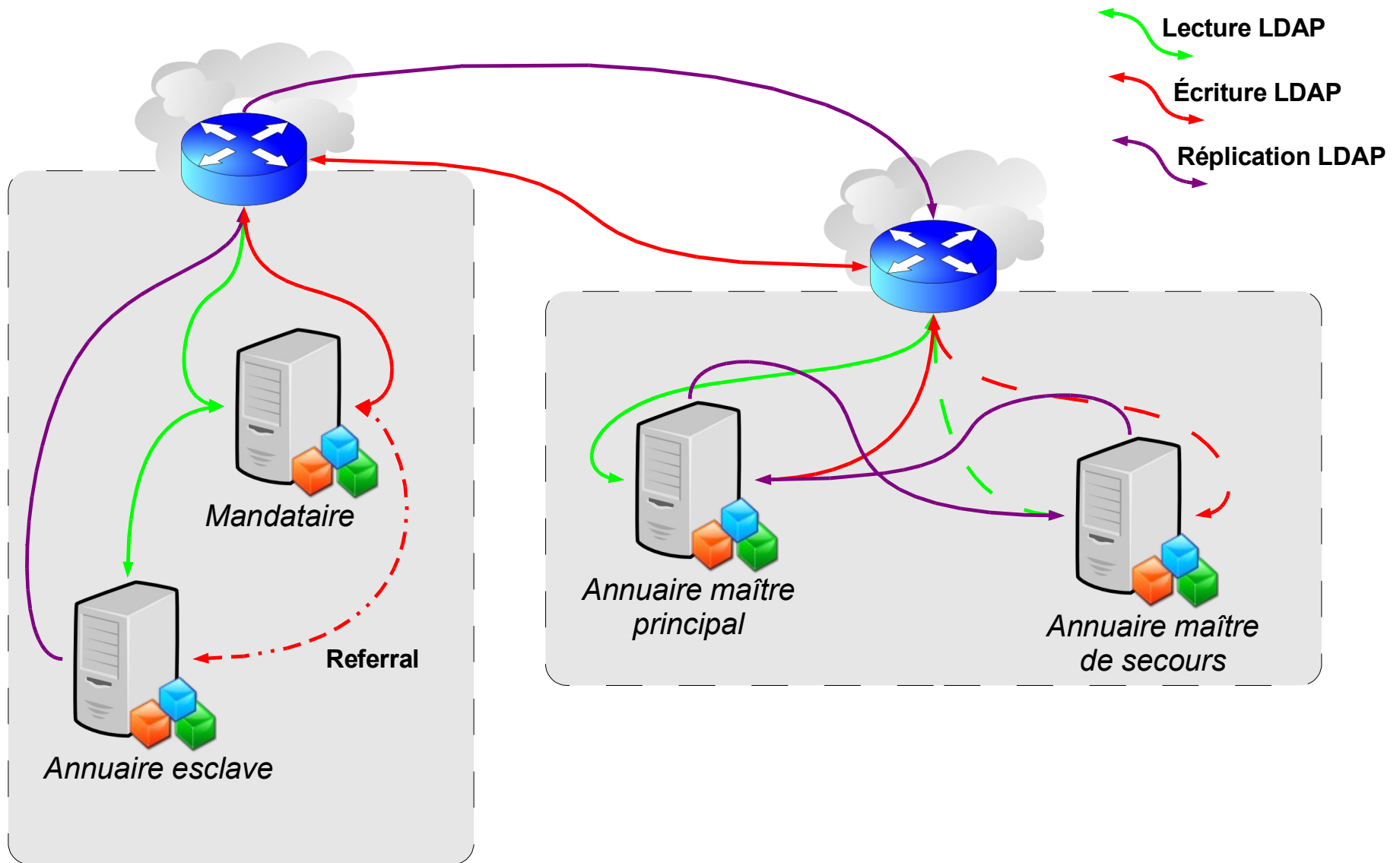
Les types de mandataires

- Mandataire « ldap » :
 - Réécriture et mapping de contexte de nommage
 - Interception des referrals
- Mandataire « meta » :
 - Virtualisation de différents contexte de nommage sur un seul point d'accès
 - Interception des referrals
- Mandataire « acls » :
 - Projet InterLDAP, non inclus dans OpenLDAP
 - Basé sur un mandataire « ldap »
 - Spécifie des règles d'accès complexes

Mise en œuvre d'un mandataire « Idap »

- Compilation d'OpenLDAP avec activation du backend Idap :
 - `./configure --enable-ldap=yes`
- Configuration du backend dans `slapd.conf` :
 - `database ldap`
 - `suffix dc=linagora,dc=com`
 - `uri "ldap://maitre:389 ldap://doublure:1389"`
 - `rebind-as-user`
- Liste des options :
 - `man -M $prefix/man slapd-ldap`

Exemple d'infrastructure avec mandataire



Plan de cours

- Introduction
- Optimisation
- Sauvegardes
- Script d'initialisation
- Traces applicatives
- Mandataire LDAP
- Équilibrage de charge avec LVS
- Supervision Nagios et Cacti

La haute-disponibilité

- Assurer un service continu 7j/7, 24h/24 :
 - Impératifs des utilisateurs et des applications
 - Contraintes internationales : les fuseaux horaires
 - Contraintes techniques : traitements de nuit
- Sécuriser les données :
 - Redondance
 - Répartition géographique
- La reprise sur échec (fail over service, ou FOS) :
 - Partage d'une adresse virtuelle entre 2 machines
 - Si une machine tombe, l'autre prend le relais
- L'équilibrage de charge (load balancing, ou LB) :
 - Les machines sont reliées à un équipement qui possède l'adresse virtuelle

La haute-disponibilité des annuaires LDAP

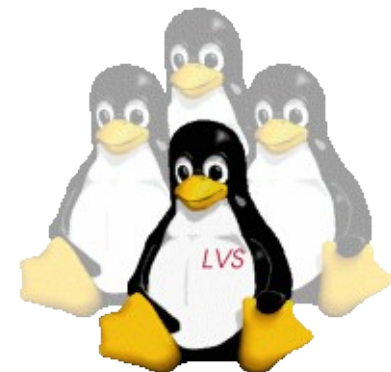
- Traitement des flux de lecture et d'écriture :
 - Lecture : équilibrage de charge et reprise sur échec
 - Écriture : reprise sur échec uniquement
 - Mécanisme Referral (LDAPv3)
- Réplication des données :
 - Un point d'écriture unique
 - De 1 à n esclaves à gérer
 - Temps de latence à intégrer
- Le mécanisme multi-maîtres :
 - Plusieurs points d'écriture → facilité de bascule (reprise sur échec)
 - Charge d'écriture supplémentaire
 - Intégrité des données non garantie

Activation du mode multimaîtres

- Dans les sources d'OpenLDAP, modifier le configure.in :
 - supprimer « dnl » au début de la ligne ENABLE_MULTIMASTER
- Régénérer le script configure :
 - autoconf
- Vérifier :
 - ./configure --help | grep multimaster
- Recompiler OpenLDAP :
 - ./configure --enable-multimaster=yes
- Configurer les annuaires en ambivalence maître/esclave, sans paramètre « updateref »
- Remarque : cette fonctionnalité est prévue par défaut dans OpenLDAP 2.4, tout en conservant l'intégrité des données

Présentation de LVS

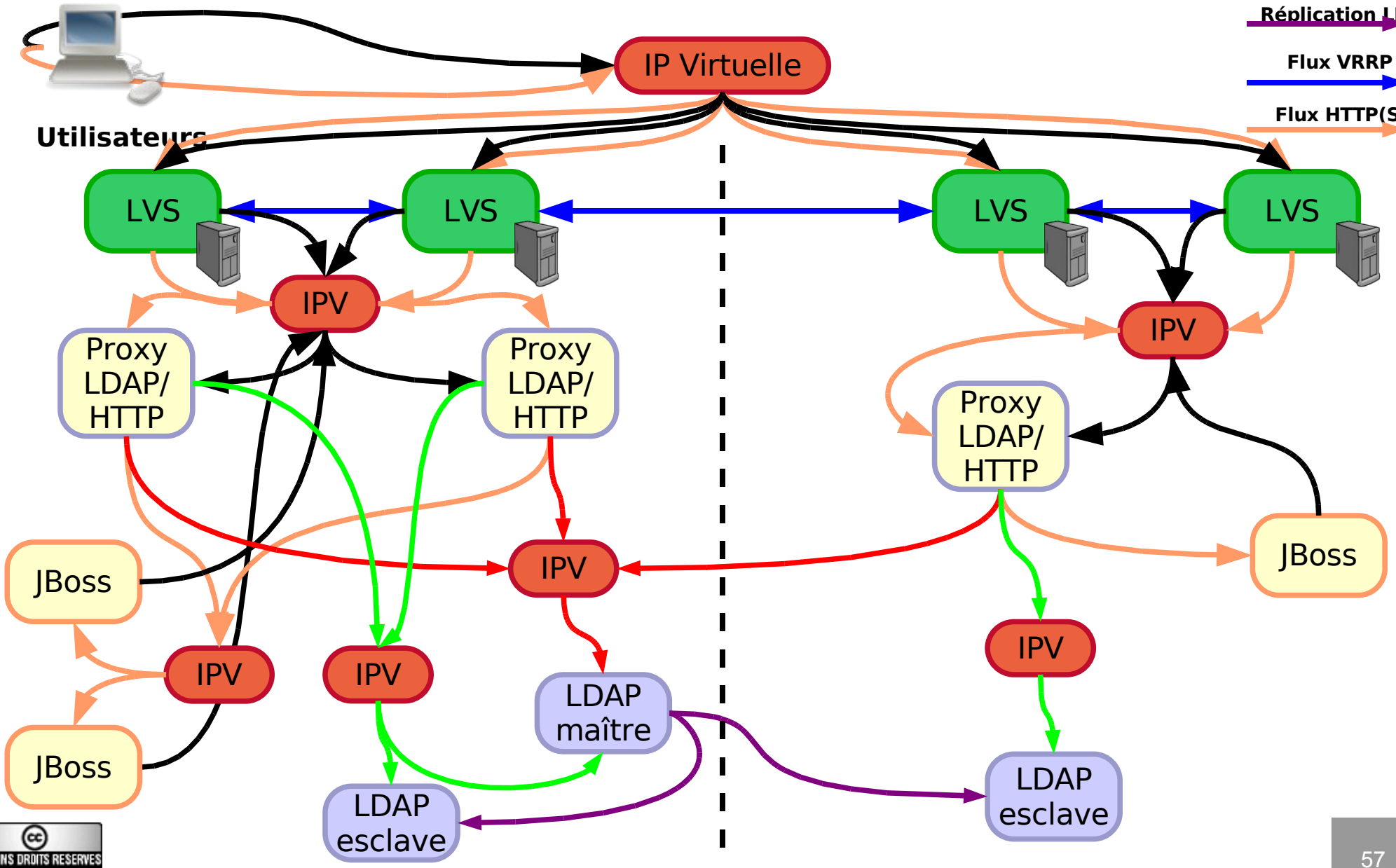
- Linux Virtual Server
- Projet initié en 1998
- Patch pour les noyaux 2.2 et 2.4
- Inclus par défaut depuis la version 2.4.28
- Équivalent à du routage haut-niveau incluant de l'équilibrage de charge
- Pas de VRRP (Virtual Router Redundancy Protocol)
- Pas de détection des serveurs éteints



Activation de LVS

- Installer le client ipvsadm
- Configurer sur l'équilibreur et les annuaires une adresse IP primaire
- Configurer sur l'équilibreur une adresse IP virtuelle
- Définir l'équilibreur comme passerelle des annuaires
- Utiliser ipvsadm pour créer les règles d'équilibrage :
 - ipvsadm -A -t **IPV**:389 -s rr
 - ipvsadm -A -t **IPV**:389 -r **IPLDAP**:389 -m
- Activer le routage interne du noyau
- Activer le NAT :
 - iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to-source=**IPV**

Exemple d'architecture



Plan de cours

- Introduction
- Optimisation
- Sauvegardes
- Script d'initialisation
- Traces applicatives
- Mandataire LDAP
- Équilibrage de charge avec LVS
- Supervision Nagios et Cacti

Nagios

- Historique :
 - 1999 : Création de NetSaint par Ethan Galstad
 - 2002 : NetSaint devient Nagios
 - 2004 : Sortie de Nagios 1.2
 - 2006 : sortie de la version 2.0
- Supervision matérielle :
 - Raid, ventilateurs, CPU, DIMM, ...
 - Agent SNMP matériel
- Supervision système :
 - Processus, Partitions
 - Services
 - RAM, CPU, charge machine, ...

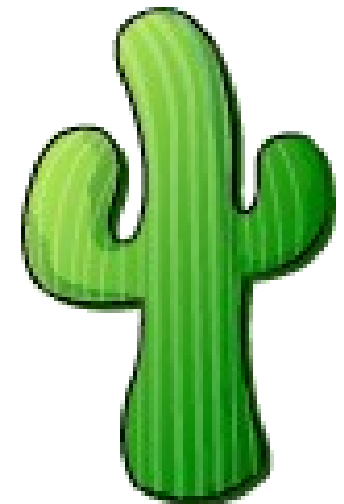
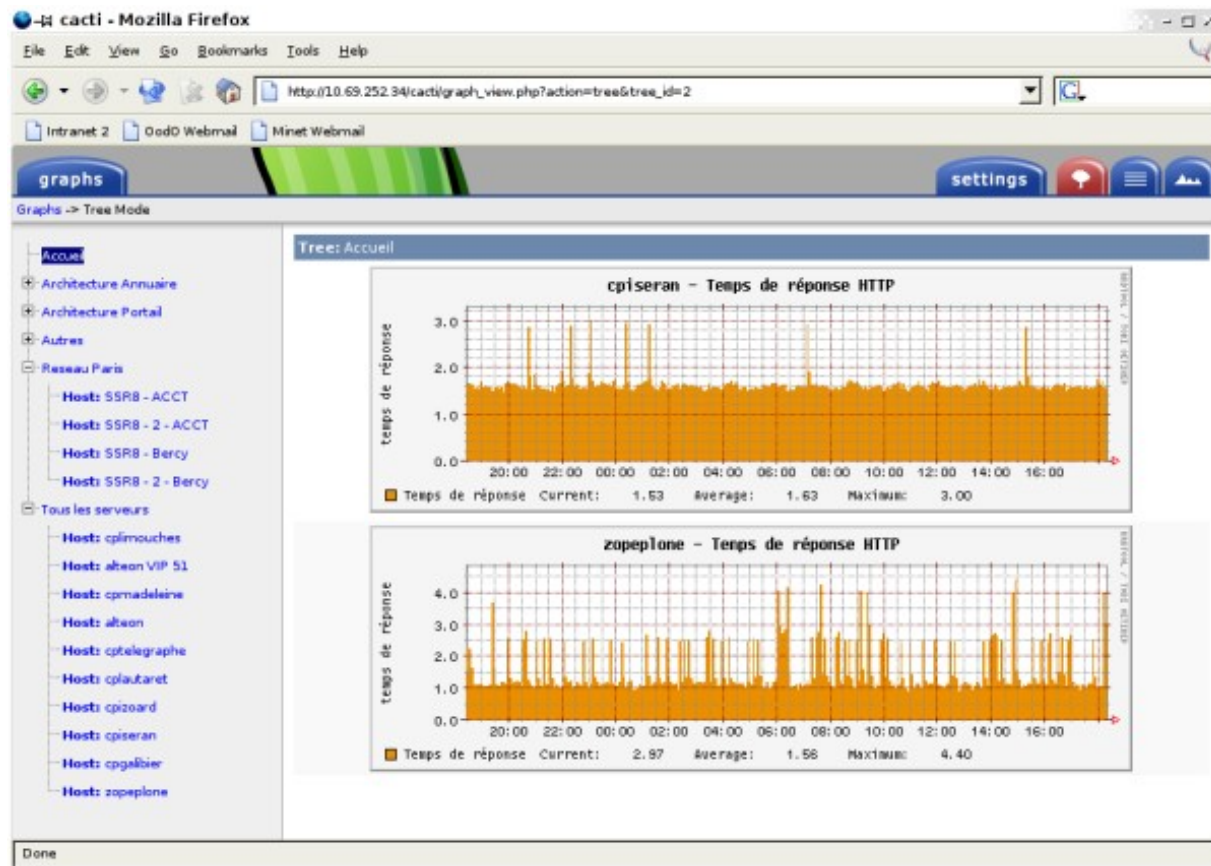
Nagios®

Greffons Nagios LDAP

- Présence d'une entrée dans un annuaire LDAP :
<http://www.linagora.org/article71.html>
- Calcul du temps de réponse d'un annuaire LDAP :
<http://www.linagora.org/article75.html>
- Vérification du statut de la réplication OpenLDAP :
<http://www.linagora.org/article91.html>
- Les deux premiers s'exécutent à distance (recherches LDAP)
- Le dernier est local, est doit passer par NCSA ou NRPE

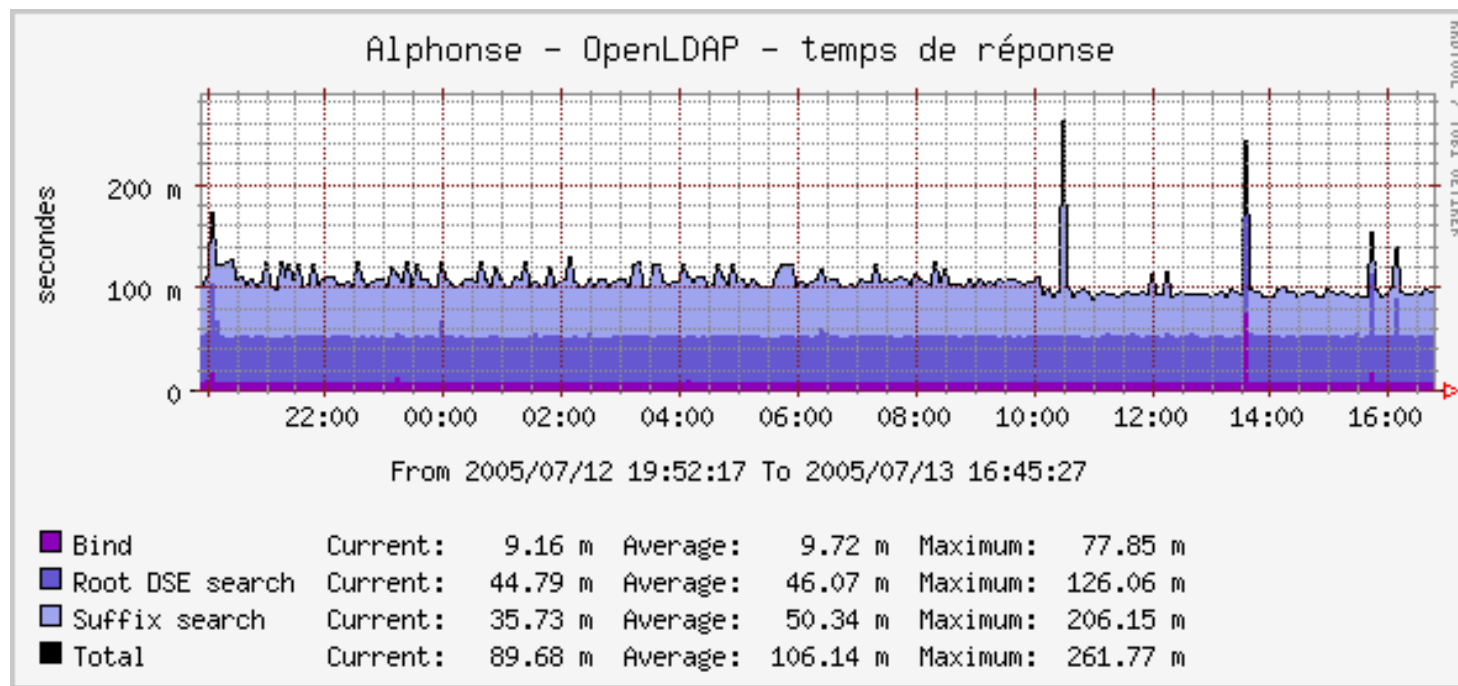
Cacti

- Cacti recueille des données dans des Round Robin Database et génère des graphiques publiés dans une interface Web



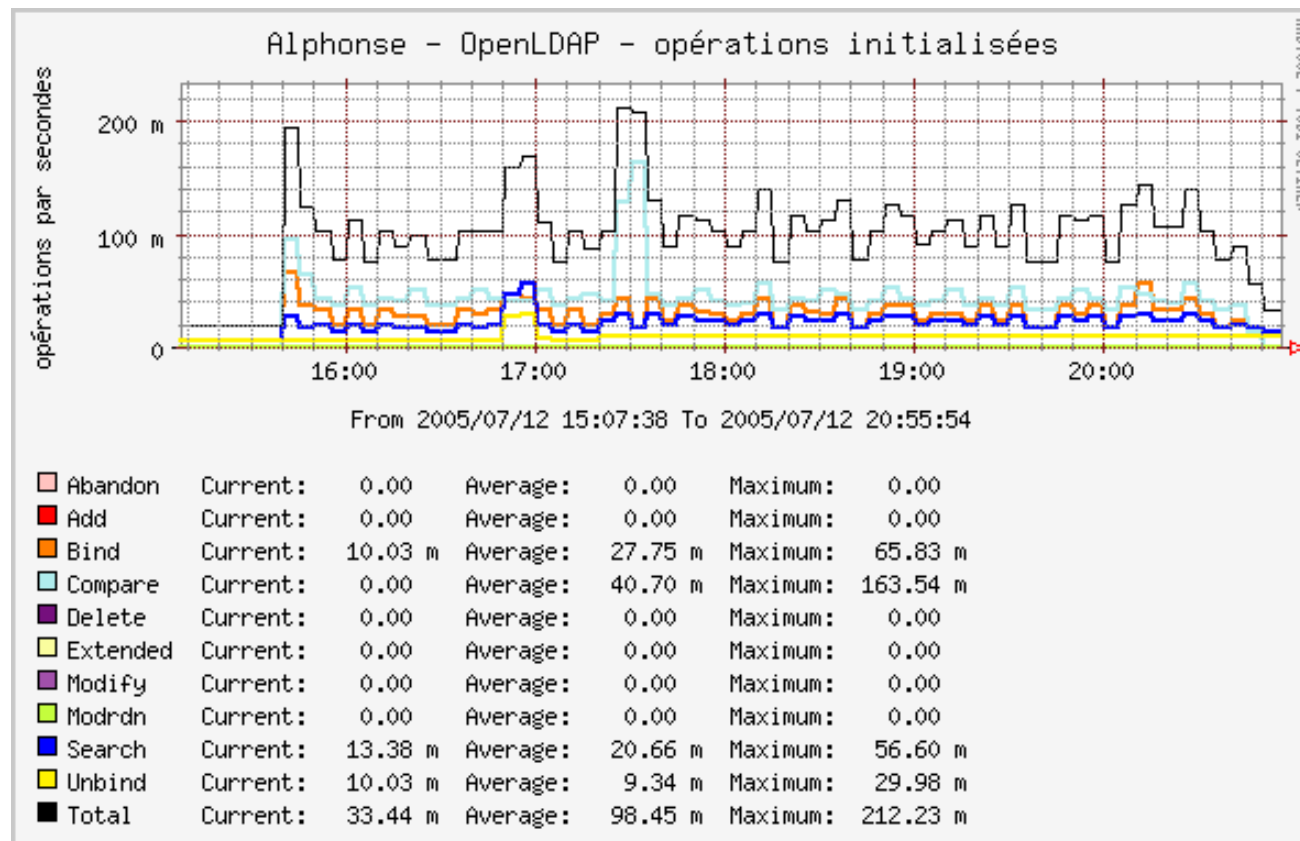
Greffons Cacti LDAP

- Calcul du temps de réponse :
<http://www.linagora.org/article121.html>
- Calcule le temps nécessaire pour effectuer une authentification (anonyme ou non), une recherche en base sur le RootDSE et une recherche en sub de 20 entrées (maximum) sous la racine



Greffons Cacti LDAP

- Statistiques sur les opérations OpenLDAP : <http://www.linagora.org/article120.html>
- Basé sur les données du backend monitor



Pour aller plus loin...

- Sites :
 - <http://www.openldap.org>
 - <http://www.linuxvirtualserver.org/>
 - <http://www.nagios.org>
 - <http://www.cacti.net>
 - <http://www.linagora.org>
- Listes de diffusion :
 - ldap-fr@cru.fr (LDAP et OpenLDAP, en français)
 - openldap-software@openldap.org (en anglais)
 - openldap-devel@openldap.org (en anglais)

Et si vous souhaitez continuer votre apprentissage...

Détachez ce coupon et adressez-le au pôle *Formation* :

Yves MIEZAN EZO
 Email : formation@linagora.com
 Tél : 01 58 18 68 28
 Fax : 01 58 18 68 29



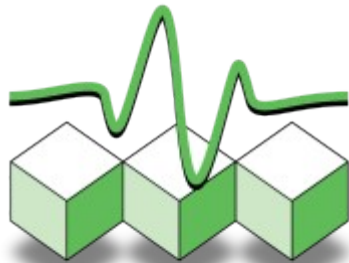
**Bénéficiez de
 100 €
 de réduction
 sur votre prochaine
 formation !**

Nom :
Prénom :
Société :
Mail :
Tél :
Stage :Date :
Tarif catalogue :€.....Réduction : - 100 €.....Tarif final :.....€

Code Opération « **LNGFetdevientfortenlibre** »

LINAGORA

Formation



Administration et sécurité

Merci de votre attention

LINAGORA *Formation*
formation@linagora.com