

Présentation et objectifs du cours

Ce cours a pour objectif de vous présenter les annuaires LDAP et son implémentation libre : le projet OpenLDAP.



Vous allez découvrir à travers ce cours les notions liées aux annuaires LDAP. Vous apprendrez également comment mettre en oeuvre, configurer et sécuriser un serveur OpenLDAP. Un dernier chapitre vous proposera la mise en place d'une infrastructure de services réseaux basés sur un annuaire LDAP

Organisation du travail

Le cours est divisé en trois parties majeures :

- une partie théorique qui concerne les annuaires LDAP, qui présente les concepts liés à tous les annuaires LDAP. Il est indispensable de bien assimiler les notions qui y sont présentées car elles constituent la base de ce qui est présenté dans la seconde partie avec OpenLDAP.
- une partie théorique et pratique qui présente le projet OpenLDAP, son implémentation, installation, configuration et sécurisation.
- une partie pratique qui présente différents cas d'implémentation de services réseaux Linux basé sur un référentiel LDAP. (serveur de messagerie, apache, ftp, et samba)

Pré-requis

Il est nécessaire de maîtriser l'administration de système GNU/Linux pour aborder sereinement cette formation, et avoir quelques notions des services réseaux abordés dans la dernière partie.

Table des matières

Avant Propos.....	2
1.Présentation générale des annuaires.....	5
1.1.Définition.....	5
1.1.1.Gestion dynamique de l'annuaire.....	5
1.1.2.Flexibilité.....	6
1.1.3.La recherche.....	6
1.1.4.Gestion de la sécurité.....	7
1.2.Comparaison avec d'autres systèmes.....	8
1.2.1.Les caractéristiques propres d'un annuaire électronique.....	8
1.2.2.Comparaison avec les bases de données.....	9
1.3.Les domaines d'utilisation.....	10
1.3.1.Cas général.....	10
1.3.2.La gestion des identités.....	11
1.3.3.Cas des applications Intranet/Extranet/Internet.....	12
1.3.4.Cas des applications systèmes.....	12
1.4.Historique.....	13
1.4.1.Historique X500.....	14
1.4.2.Historique LDAP.....	15
1.5.La norme LDAP.....	16
1.5.1.Le protocole LDAP.....	17
1.5.2.Modèle d'information.....	19
1.5.3.Modèle de nommage.....	23
1.5.4.Modèle fonctionnel.....	26
1.5.5.Modèle de sécurité.....	31
1.5.6.Modèle de répartition.....	34
1.6.Le format LDIF.....	36
1.6.1.Mode import	37
1.6.2.Mode modification.....	38
1.7.Les URLs LDAP.....	40
1.8.Quelques annuaires LDAP.....	41
2.Implémentation de la suite OpenLDAP.....	42
2.1.Présentation de la suite OpenLDAP.....	42
2.2.Installation d'OpenLDAP.....	45
2.2.1.A partir des sources.....	45
2.2.2.Cas de Debian.....	46
2.2.3.Cas de RedHat.....	46
2.3.Configuration et directives du serveur LDAP.....	47
2.3.1.Configuration du serveur LDAP.....	47
2.3.2.Structure générale.....	48
2.3.3.Directives générales.....	49
2.3.4.Directives sur la sécurité.....	50
2.3.5.Directives sur les schémas.....	50
2.3.6.Gestion des ressources.....	50
2.3.7.Directives des sections backend.....	51
2.3.8.Directives d'une section database.....	52
2.3.9.Directives de réplication.....	53
2.4.Contrôle d'accès aux informations.....	54
3.Administration et exploitation.....	57
3.1.Exploitation.....	57
3.1.1.Démarrage / Arrêt.....	57
3.1.2.Gestion des logs.....	57
3.2.Alimentation de l'annuaire LDAP.....	58
3.2.1.Création de l'annuaire online.....	58
3.2.2.Création de l'annuaire offline.....	59
3.3.Sauvegarde / Restauration de l'annuaire LDAP.....	60
3.3.1.Sauvegarde de l'annuaire.....	60
3.3.2.Restauration de l'annuaire.....	61
3.4.Reconstruction des index.....	61
3.5.Recherches et manipulations dans le DIT.....	62
3.5.1.Recherche dans le DIT : ldapsearch.....	62
3.5.2.Modification d'une entrée : ldapmodify.....	63
3.5.3.Suppression d'une entrée : ldapdelete.....	63
3.6.Outils d'administration graphique.....	64
4.Réplication et referral.....	66
4.1.Réplication : slurpd.....	67
4.1.1.Compte de réplication.....	67
4.1.2.Configuration du maître.....	68
4.1.3.Configuration de l'esclave.....	68
4.1.4.Mise en place.....	69
4.1.5.Fichiers de réplication, explication.....	70

4.2.Réplication : syncrepl.....	71	6.3.2.Choix du suffixe.....	95
4.2.1.Configuration du serveur primaire.....	71	6.3.3.Nommage des entrées : choix du DN.....	96
4.2.2.Configuration du serveur secondaire.....	72	6.4.Topologie du service.....	97
4.2.3.Slurp vs. Syncrepl.....	73	6.4.1.Objectifs.....	97
4.3.Délégation : referral.....	74	6.4.2.Recueil des informations.....	98
4.3.1.Cas d'une délégation inférieure.....	74	6.4.3.Les décisions techniques.....	98
4.3.2.Cas d'une délégation supérieure.....	74	6.5.Sécuriser le service.....	99
5.Sécurisation des serveurs OpenLDAP.....	75	7.Cas pratiques : Intégration LDAP aux services	
5.1.Utiliser un utilisateur non privilégié.....	75	réseaux.....	100
5.2.Choisir un hashage fort pour les mots de passe.....	76	7.1.Authentification système LDAP : pam_ldap et nss_ldap...101	
5.3.Sécurisation réseau	76	7.1.1.Pré-requis LDAP.....	101
5.4.Contrôle d'accès aux informations.....	77	7.1.2.Objectifs.....	104
5.5.Sécurité SSL - TLS	80	7.1.3.pam_ldap et nss_ldap.....	104
5.5.1.Idaps, StartTLS.....	80	7.1.4.Configuration de nss_ldap.....	105
5.5.2.Certificat de l'autorité (CA) auto-signé.....	80	7.1.5.Configuration de pam_ldap.....	107
5.5.3.Création des clés et certificats du serveur.....	82	7.2.Services FTP : Base d'utilisateur LDAP.....111	
5.5.4.Configuration TLS de slapd et clients.....	84	7.3.Apache : Contrôle d'accès et authentification LDAP.....112	
5.5.5.Configuration de la partie client.....	84	7.4.Intégration Messagerie avec LDAP.....114	
5.5.6.Lancement de slapd avec TLS et tests.....	85	7.4.1.Pré-requis LDAP.....	114
6.Déploiement d'une architecture LDAP.....	86	7.4.2.Postfix : Base d'utilisateurs LDAP.....	118
6.1.Identification des besoins en service d'annuaire.....	87	7.4.3.Services IMAP/POP : Base d'utilisateurs LDAP.....	119
6.2.Les données nécessaires.....	87	7.5.Samba / LDAP.....124	
6.3.Conception du modèle de nommage.....	90	7.5.1.Pré-requis.....	124
6.3.1.Design du DIT.....	91	7.5.2.Configuration de Samba.....	128