

Résumé

Ce support reprend les deux précédents sur NFSv4 et LDAP en associant les services. Le système de fichiers réseau NFSv4 sert au partage des répertoires utilisateur tandis que l'annuaire LDAP sert au partage des attributs des comptes utilisateur et de la configuration du service d'automontage. Une fois que les deux services associés sont en place, les comptes utilisateurs peuvent être utilisés de façon transparente depuis n'importe quel poste client faisant appel à ces services.

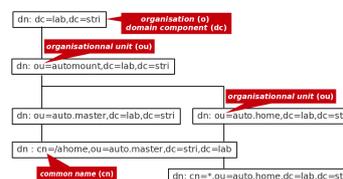


Table des matières

1. Copyright et Licence	2
1.1. Méta-information	2
2. Adressage IP des postes de travail	2
3. Mise en œuvre de l'annuaire LDAP	2
4. Mise en œuvre de l'exportation NFS	3
5. Configuration de l'automontage avec le service LDAP	4
6. Accès aux ressources LDAP & NFS depuis le client	5
6.1. Configuration LDAP	5
6.2. Configuration NFS avec automontage	6
7. Documents de référence	6

1. Copyright et Licence

Copyright (c) 2000,2015 Philippe Latu.
Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

Copyright (c) 2000,2015 Philippe Latu.
Permission est accordée de copier, distribuer et/ou modifier ce document selon les termes de la Licence de Documentation Libre GNU (GNU Free Documentation License), version 1.3 ou toute version ultérieure publiée par la Free Software Foundation ; sans Sections Invariables ; sans Texte de Première de Couverture, et sans Texte de Quatrième de Couverture. Une copie de la présente Licence est incluse dans la section intitulée « Licence de Documentation Libre GNU ».

1.1. Méta-information

Ce document est écrit avec [DocBook](http://www.docbook.org)¹ XML sur un système [Debian GNU/Linux](http://www.debian.org)². Il est disponible en version imprimable au format PDF : [sysadm-net.autofs-ldap-nfs.q.pdf](http://www.inetdoc.net/pdf/sysadm-net.autofs-ldap-nfs.q.pdf)³.

2. Adressage IP des postes de travail

Tableau 1. Affectation des adresses IP des postes de travaux pratiques

Poste 1	Poste 2	Passerelle par défaut	Organisation
alderaan	bespin	172.24.132.17/28	o: zone1.lan-213.stri
centares	coruscant	172.20.129.17/29	o: zone2.lan-213.stri
dagobah	endor	192.168.123.17/28	o: zone3.lan-213.stri
felucia	geonosis	192.168.125.49/28	o: zone4.lan-213.stri
hoth	mustafar	10.5.6.1/23	o: zone5.lan-213.stri
naboo	tatooine	172.20.136.81/28	o: zone6.lan-213.stri

Pour chaque paire de postes de travaux pratiques, il faut attribuer les rôles de serveur et de client. Le serveur doit mettre en œuvre le service d'annuaire LDAP comprenant les propriétés des comptes utilisateurs et exporter l'arborescence du système de fichiers de ces mêmes comptes utilisateurs avec NFS. Le client doit accéder à ces ressources. Il doit permettre l'authentification auprès du serveur LDAP pour les comptes utilisateurs concernés et pouvoir monter dynamiquement à la demande le système de fichiers de ces comptes utilisateurs.

L'objectif en fin de séance de travaux pratiques est de pouvoir se connecter sur un poste client avec ses identifiants `login/password` et d'accéder à son répertoire utilisateur stocké sur le serveur de façon totalement transparente.

3. Mise en œuvre de l'annuaire LDAP

Cette partie reprend les étapes décrites dans le support [Introduction aux annuaires LDAP avec OpenLDAP](#)⁴. Il s'agit d'installer les paquets correspondants au logiciel OpenLDAP, d'initialiser une base avec le bon contexte de nommage puis d'implanter les deux unités organisationnelles et les entrées des comptes utilisateurs.

Q1. Comment installer le service d'annuaire LDAP sur le poste serveur ?

¹ <http://www.docbook.org>

² <http://www.debian.org>

³ <http://www.inetdoc.net/pdf/sysadm-net.autofs-ldap-nfs.q.pdf>

⁴ http://www.inetdoc.net/travaux_pratiques/index.html#sysadm-net.ldap

Choisir les paquets à installer et valider le bon fonctionnement du service en contrôlant la liste des processus et des numéros de ports ouverts.

- Q2.** Comment initialiser une nouvelle base et un nouveau contexte de nommage pour ce service d'annuaire ?

Réinitialiser la configuration du démon `slapd` avec le contexte de nommage défini dans la [Section 2, « Adressage IP des postes de travail »](#).

- Q3.** Comment activer la journalisation des transactions sur le service d'annuaire ?

Créer un fichier LDIF qui remplace la valeur par défaut de l'attribut `olcLogLevel` par `stats`.

- Q4.** Comment implanter les deux unités organisationnelles `people` et `groups` dans le nouvel annuaire ?

Créer un fichier LDIF qui décrit la création des deux unités organisationnelles dans le bon contexte. Ajouter ces deux unités organisationnelles dans l'annuaire.

- Q5.** Comment implanter les quatre comptes utilisateurs dans cet annuaire ?

Créer un fichier LDIF qui décrit la création des quatre comptes utilisateurs dans le bon contexte avec un jeu d'attributs complet pour l'authentification et le système de fichiers. Ajouter ces comptes dans l'annuaire.

4. Mise en œuvre de l'exportation NFS

Cette partie reprend les étapes décrites dans le support [Introduction au système de fichiers réseau NFSv4](#)⁵. Après avoir traité la partie commune de la configuration NFS, il s'agit d'installer le paquet correspondant au serveur NFS et de créer l'arborescence des comptes utilisateurs à exporter avec le bon contexte de nommage.

- Q6.** Comment installer et valider les services commun au client et au serveur NFS ?

Rechercher et installer le paquet puis contrôler la liste des processus et des numéros de port ouverts.

- Q7.** Quelles modifications faut il apporter au fichier de configuration des services NFS communs pour privilégier l'utilisation de la version 4 du protocole ?

Identifier le fichier de configuration et les paramètres (in)utiles pour NFSv4

- Q8.** Comment installer et configurer le paquet relatif à l'exportation d'une arborescence avec le protocole NFS ?

- Q9.** Comment valider la configuration de l'exportation réalisée par le serveur NFS ?

- Q10.** Quel est le montage local à mettre en place pour garantir la cohérence du schéma de nommage entre les postes serveur et client ?

- Q11.** Comment créer automatiquement l'arborescence d'un utilisateur qui n'existe que dans l'annuaire LDAP ?

Rechercher les fonctions de création automatique de répertoire utilisateur dans la liste des modules PAM.



Avertissement

Cette opération se déroule en plusieurs étapes dans la mesure où il est impossible de créer un répertoire utilisateur directement depuis le client.

1. Activer l'appel au module PAM de création de répertoire utilisateur sur le serveur NFSv4.

⁵ http://www.inetdoc.net/travaux_pratiques/index.html#sysadm-net.nfs

2. Effectuer une première connexion directe sur le serveur, via SSH par exemple, permet de réaliser l'opération de création de l'arborescence initiale.
3. Toute nouvelle connexion sur un client NFSv4 utilise l'arborescence utilisateur créée lors de l'étape précédente.

5. Configuration de l'automontage avec le service LDAP

Le principe de l'automontage veut que le montage d'une arborescence de système de fichiers réseau se fasse automatiquement et uniquement à l'utilisation. En effet, il n'est pas nécessaire de mobiliser les ressources du protocole NFS tant qu'une arborescence n'est pas effectivement parcourue. Dans le contexte de ce support, il n'est pas nécessaire de monter l'arborescence d'un répertoire utilisateur si celui-ci n'est pas connecté sur le poste client. On optimise ainsi les ressources du système et du réseau.

Du point de vue administration système, il est essentiel que la configuration des postes clients ne soit pas remise en question à chaque évolution du serveur ou à chaque ajout de nouveau compte utilisateur. C'est ici que le service LDAP intervient. Ce service sert à publier la configuration de l'automontage en direction des clients.

Pour appliquer ces principes, cette section doit couvrir les étapes suivantes.

- Pour compléter les informations publiées par le service LDAP, il faut ajouter un schéma spécifique à la fonction d'automontage et ensuite importer le contenu d'un fichier de description LDIF contenant les paramètres de configuration à diffuser vers les clients.
- Pour que le montage des arborescences soit automatique, il faut ajouter un paquet spécifique sur les systèmes clients et désigner le service LDAP comme fournisseur de la configuration. Cette désignation se fait à l'aide du Name Service Switch.

La principale difficulté dans le traitement des questions suivantes vient du fait qu'il est nécessaire d'échanger des informations entre le client et le serveur.

Dans le contexte de ce support, le service LDAP et le serveur NFS sont implantés sur le même système.

Q12. Quel est le paquet de la distribution Debian GNU/Linux qui fournit le service d'automontage via LDAP ?

Rechercher le mot clé automount dans le champ description du catalogue des paquets disponibles.

Q13. Sur quel type de poste ce paquet doit il être installé ?

Le service d'automontage est à exécuter sur le poste qui ne détient pas le système de fichiers dans lequel se trouvent les répertoires utilisateur.

Q14. Quelles sont les informations relatives au service LDAP à transférer entre client et serveur ?

Pour publier la configuration de l'automontage via le service LDAP, il est nécessaire de disposer du schéma de définition des attributs dans l'annuaire. Ce schéma est fourni avec le paquet `autofs-ldap` et doit être transféré vers le serveur LDAP pour compléter le catalogue des objets qu'il peut contenir.

Q15. Dans quel répertoire les informations transférées doivent elles être placées ?

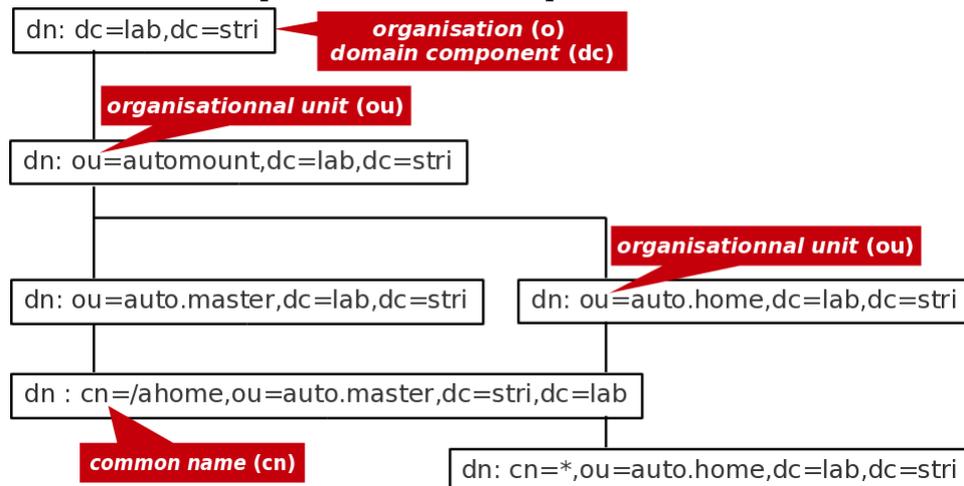
Rechercher le répertoire de stockage des fichiers de schémas dans l'arborescence du serveur LDAP.

Q16. Comment intégrer ces nouvelles informations d'automontage dans la configuration du service LDAP ?

L'intégration du nouveau schéma dans la configuration du serveur se fait en plusieurs étapes. Le fichier délivré avec le paquet `autofs-ldap` doit être converti en fichier LDIF avant d'être ajouté au DIT de configuration du démon `slapd`.

- Q17.** Quelle est la syntaxe du fichier de description LDIF contenant la configuration de l'automontage ?

Le fichier de description ci-dessus correspond à l'arborescence suivante.



Arborescence LDAP de l'automontage - vue complète⁶

- Q18.** Comment intégrer ces définitions dans l'annuaire LDAP ?

Retrouver la syntaxe de la commande **ldapadd** qui permet d'insérer de nouvelles entrées dans l'annuaire.

6. Accès aux ressources LDAP & NFS depuis le client

Dans cette section, on suppose que l'annuaire LDAP du poste serveur est disponible et accessible. Dans un premier temps, on configure le poste client pour qu'il obtienne de façon transparente les informations sur les comptes utilisateurs desservis par l'annuaire. Dans un second temps, on complète sa configuration pour qu'il obtienne, toujours de façon transparente les informations sur le système de fichiers réseau.

Cette partie reprend les étapes décrites dans la section [Configuration Name Service Switch](#)⁷ du support [Introduction aux annuaires LDAP avec OpenLDAP](#)⁸.

6.1. Configuration LDAP

- Q19.** Quels sont les paquets de bibliothèques LDAP relatifs au mécanisme Name Service Switch et au gestionnaire d'authentification PAM ?

Rechercher la liste des paquets dont le nom débute par `libnss`.

- Q20.** Quelles sont les étapes de la configuration des paquets de bibliothèques NSS et PAM ?

Lors de l'installation des deux paquets, on passe par une série de menus `debconf`.

- Q21.** Quelles sont les modifications à apporter au fichier de configuration `/etc/nsswitch.conf` pour activer l'accès aux ressources de l'annuaire LDAP ?

Rechercher la syntaxe permettant de lancer des recherches dans l'annuaire en plus des fichiers locaux au système.

- Q22.** Comment valider la configuration de l'accès à l'annuaire LDAP ?

Rechercher une commande permettant d'effectuer un appel système au bibliothèques standard `libc`.

⁶ http://www.inetdoc.net/travaux_pratiques/sysadm-net.autofs-ldap-nfs/images/ldap-automount.png

⁷ http://www.inetdoc.net/travaux_pratiques/sysadm-net.ldap.q/sysadm-net.ldap.clnt.html#sysadm-net.ldap.clnt.nss

⁸ http://www.inetdoc.net/travaux_pratiques/index.html#sysadm-net.ldap

6.2. Configuration NFS avec automontage

On considère que le paquet `autofs-ldap` a déjà été installé pour fournir le schéma de la partie automontage au serveur LDAP. Voir [Section 5, « Configuration de l'automontage avec le service LDAP »](#).

Q23. Quelle est la modification à apporter au fichier de configuration `/etc/nsswitch.conf` pour que le démon `automount` accède aux ressources de l'annuaire LDAP ?

Il faut ajouter une directive supplémentaire qui spécifie l'ordre de recherche des informations pour le démon `automount`.

Q24. Quel est le fichier de configuration du service d'automontage dans lequel sont définis ses paramètres globaux ?

Rechercher le répertoire dans lequel sont placés les fichiers de paramétrage de tous les services.

Q25. Quelles sont les modifications à apporter à ce fichier pour que le démon accède à l'annuaire LDAP et que la journalisation soit active ?

Il faut éditer le fichier avec les éléments suivants.

- Désigner l'unité organisationnelle qui contient les entrées de configuration de l'automontage
- Faire apparaître les évènements du service d'automontage dans les journaux système
- Désigner le serveur LDAP à contacter
- Spécifier le point d'entrée pour les recherches dans l'annuaire

Q26. Quelles sont les méthodes qui permettent de valider le fonctionnement du service d'automontage ?

Donner deux moyens d'acquérir l'identité d'un utilisateur ou d'une utilisatrice défini(e) dans l'annuaire LDAP uniquement.

ne pas oublier de consulter les journaux système pour observer les étapes de ces connexions utilisateur.

7. Documents de référence

OpenLDAP Software 2.4 Administrator's Guide

Le guide [OpenLDAP Software 2.4 Administrator's Guide](#)⁹ est la référence essentielle sur le service LDAP.

Systèmes de fichiers réseau : NFS & CIFS

[Systèmes de fichiers réseau](#)¹⁰ : présentation des modes de fonctionnement des systèmes de fichiers réseau NFS & CIFS.

Linux NFS-HOWTO

[Linux NFS-HOWTO](#)¹¹ : documentation historique complète sur la configuration d'un serveur et d'un client NFS jusqu'à la version 3 incluse.

Nfsv4 configuration

[Nfsv4 configuration](#)¹² : traduction française extraite des pages du projet CITI de l'université du Michigan.

⁹ <http://www.openldap.org/doc/admin24/>

¹⁰ <http://www.inetdoc.net/presentations/network-file-systems/>

¹¹ <http://nfs.sourceforge.net/nfs-howto/>

¹² https://wiki.linux-nfs.org/wiki/index.php/Nfsv4_configuration_fr