Administration système en réseau : Network File System

Philippe Latu
philippe.latu(at)linux-france.org

http://www.linux-france.org/prj/inetdoc/

Historique des versions		
$Revision: 1321 $	$Date: 2008-09-24 10:21:50 +0200 (mer 24 sep 2008) $	$Author: latu $
Année universitaire 2006-2007		

Résumé

Après la phase de découverte du «voisinage réseau», l'objectif de ces travaux pratiques est l'étude du fonctionnement du système de fichiers réseau phare du monde Unix/Linux : NFS.

Table des matières

1. Copyright et Licence

1.1. Méta-information

Cet article est écrit avec *DocBook*[1] XML sur un système *Debian GNU/Linux*[2]. Il est disponible en version imprimable aux formats PDF et Postscript : `admin.reseau.nfs.pdf`[3]| `admin.reseau.nfs.ps.gz`[4].

2. Adressage IP des postes de travail

Tableau 1. Affectation des adresses IP pour les travaux pratiques NFS

Poste 1	Poste 2	Passerelle par défaut
asterix	obelix	`172.19.116.1/26`
tintin2	haddock	`10.0.119.65/27`
dupond	tif	`10.0.121.129/27`
hochet	blake	`172.19.114.129/26`
jourdan	mortimer	`192.168.108.129/25`
dupont	danny	`10.5.6.1/23`

Pour ces travaux pratiques, de nombreuses questions peuvent être traitées à l'aide du document de référence : *Linux NFS-HOWTO*. Il faut cependant faire correspondre les configurations décrites dans ce document avec les configurations proposées avec les paquets de la distribution *Debian GNU/Linux*.

Pour chaque paire de postes de travaux pratiques, il faut attribuer les rôles serveur et client. Le serveur doit exporter une partie de son arborescence locale de système de fichiers et le client doit pouvoir y accéder de façon transparente via un montage du système de fichiers distant. Voir le support : *Systèmes de fichiers réseau : NFS & CIFS*.

3. Configuration commune au client et au serveur NFS version < 4

Plusieurs services communs doivent être actifs pour que les accès au système de fichiers réseau NFS soient utilisables.

3.1. Gestion des appels RPC

1. Quel est le service chargé de la gestion des appels RPC ?

Rechercher dans le support *Linux NFS-HOWTO* le service utilisé par NFS pour le multiplexage des appels de procédures distants.

2. Quel est le paquet correspondant à ce service ? Vérifier que ce paquet est bien installé.

Rechercher dans les supports *Systèmes de fichiers réseau : NFS & CIFS* ou *Linux NFS-HOWTO*.

3. Quel est le numéro de port utilisé par le service ? Quel est le principe de fonctionnement du service pour le traitement des appels de procédures distants ?

Utiliser les commandes systèmes d'identification des services réseau en écoute sur les interfaces, rechercher dans les pages de manuels de l'application et utiliser le support *Systèmes de fichiers réseau : NFS & CIFS*.

4. Quelle est a commande qui permet de lister les services accessibles via un appel RPC ? À quel paquet appartient cette commande ?

Rechercher dans dans le support *Linux NFS-HOWTO*.

[1] http://www.docbook.org
[2] http://www.debian.org
[3] http://www.linux-france.org/prj/inetdoc/telechargement/admin.reseau.nfs.pdf
[4] http://www.linux-france.org/prj/inetdoc/telechargement/admin.reseau.nfs.ps.gz

5. Comment modifier la configuration du paquet de gestion des appels RPC pour que le service soit accessible depuis le réseau local en plus de l'hôte sur lequel il est installé ?

   Reprendre la liste des commande de gestion des paquets *Debian* pour retrouver l'opération de «reconfiguration» d'un paquet. Autre possibilité, éditer le fichier des options par défaut du service. Ce fichier doit se trouver dans le répertoire `/etc/default/`.

6. Donner deux exemples d'exécution : un en local et un sur le poste de travaux pratiques voisin.

7. Réaliser une capture à l'aide de l'analyseur réseau lors de l'exécution de la commande et relever : le protocole de transport utilisé, les numéros de ports caractéristiques de cette transaction ainsi que le nom de la procédure RPC utilisée.

```
 Poste 1                                        Poste 2
-------------------------------------------------------------
 <commande>       --- requête --->            <processus>

                  <-- réponse ----
```

3.2. Gestion des paquets NFS

1. Quel est le paquet commun au client et au serveur ? Identifier le jeu de commandes fournies.

   Rechercher le dans la base de données des paquets.

2. Une fois le paquet installé, quels sont les différents moyens qui permettent d'identifier l'ouverture du nouveau service ?

   Passer en revue les commandes qui listent les processus, les sockets unix|inet ouverts en écoute et les appels RPC.

3. Réaliser une capture réseau lors de l'exécution des commandes et relever les protocoles et les numéros de ports caractéristiques de ces transactions. Relativement aux questions sur Section 3.1, « Gestion des appels RPC », est-ce que de nouveaux ports tcp|udp en écoute sont apparus ? Pourquoi ?

```
 Poste 1                                        Poste 2
-------------------------------------------------------------
 <commande>       --- requête --->            <processus>

                  <-- réponse ----
```

4. Configuration du client NFS version < 4

Le rôle du client est d'intégrer un accès au système de fichiers d'un hôte distant dans son arborescence locale. On parle de «montage NFS». Dans un premier temps, on teste les opérations de montage manuel. Bien sûr, ces tests ne peuvent aboutir que si une arborescence à été exportée par un serveur.

Ensuite, on teste les opérations de montage automatisées ou «automontage». Si le serveur NFS n'est pas encore disponible au moment des tests de montage manuel, il faut préparer les fichiers de configuration du service d'automontage.

4.1. Opérations manuelles de (montage|démontage) NFS

1. Quelle est la commande qui permet de tester la disponibilité du service de montage NFS sur un hôte distant ?

   Utiliser les pages de manuels de la commande identifiée dans la section précédente.

2. Quelle est la commande qui permet d'identifier l'arborescence disponible à l'exportation sur le serveur NFS ?

   Rechercher dans la liste des fichiers du paquet de service commun NFS.

3. Réaliser une capture lors de l'exécution des commandes et relever les numéros de ports caractéristiques de ces transactions.

4. Créer le répertoire `/mnt/nfs`. Quelle est la syntaxe de la commande permettant de «monter» le répertoire exporté par le serveur NFS sur ce nouveau répertoire ?

   Rechercher dans le support *Linux NFS-HOWTO*.

5. A quel paquet appartient cette commande ? Cette commande est-elle exclusivement liée au protocole NFS ?

   Interroger la base de données des paquets de la distribution.

6. Quelles sont les options de montage disponibles avec le protocole NFS ? Relever la signification des options principales ?

   Rechercher dans le support *Linux NFS-HOWTO*. Les options caractéristiques sont : choix du protocole de transport, taille des blocs de données et version NFS. On peut aussi consulter les pages de manuels de la catégorie 5 concernant les formats de fichiers à l'aide de la commande **`man 5 nfs`**.

7. Une fois la commande de montage exécutée, tester la validité du montage avec les commandes **mount** et **df**.

8. Réaliser une capture lors de l'exécution des commandes et relever les numéros de ports caractéristiques de ces transactions. Est-il possible de retrouver les informations échangées dans les données de capture ?

```
Client                                                          Serveur
-----------------------------------------------------------------------
mount                    --- requête RPC --->                  portmapper

mount                    <--- numéro port ---                  portmapper

mount                    --- requête RPC --->                  mountd

mount                    <-- réponse --------                  mountd

lecture/écriture         ---- I/O ------------>                nfsd

lecture/écriture         <- ACK fin opération -                nfsd
```

9. Quelles seraient les opérations à effectuer pour rendre un montage NFS statique permanent ?

   Il est inutile de modifier les fichiers de configuration du système sachant que l'on change de méthode de montage dans la section suivante.

4.2. Opérations automatisées de (montage|démontage) NFS

Note

Il existe plusieurs implémentations libres pour le service d'automontage. On se limite ici au logiciel lié au noyau Linux.

Dans cette section, on reprend le processus de montage précédent en utilisant le service d'automontage. L'objectif étant de rendre les opérations d'accès au système de fichiers réseau totalement transparentes pour l'utilisateur, le recours au montage manuel doit être évité le plus possible.

1. Quel est le paquet qui contient les outils nécessaires au fonctionnement de l'automontage ?

   Interroger les métadonnées dans le cache du gestionnaire de paquet APT en cherchant le mot clé **automount**.

2. Comment réaliser un automontage du répertoire `/mnt/nfs` ? Quels sont les fichiers de configuration à éditer ou à créer ?

Utiliser les fichiers exemples fournis avec le paquet en créant un fichier de configuration spécifique pour la question.

3. Une fois la configuration en place, tester la validité du montage avec les commandes **mount** et **df**.

4. Réaliser une capture lors de l'exécution des commandes et relever les numéros de ports caractéristiques de ces transactions. Est-il possible de retrouver les informations échangées dans les données de capture ?

5. Configuration du serveur NFS version < 4

Le rôle du serveur est de mettre à disposition sur le réseau une partie de son arborescence locale de système de fichiers. On parle d'«exportation».

Note

Il existe plusieurs implémentations libres de serveur NFS. On se limite ici à l'utilisation du logiciel lié au noyau Linux.

1. Quel est le paquet qui contient les outils nécessaires au fonctionnement du serveur NFS ?

   Interroger les méta-données dans le cache du gestionnaire de paquet avec la commande **apt-cache** en cherchant les mots clés `nfs` et `server`.

2. Quel est le fichiers de configuration principal de gestion des exportations NFS ?

   Rechercher dans le support *Linux NFS-HOWTO*.

3. Créer le répertoire `/var/exports`. Quelle est la syntaxe à utiliser dans le fichier de configuration pour «exporter» le répertoire ?

   Rechercher dans le support *Linux NFS-HOWTO* ou utiliser les pages de manuels fournies avec le paquet du serveur NFS.

4. Quelles sont les principales options disponibles pour l'exportation d'une arborescence ? Relever la signification des paramètres.

   Rechercher dans le support *Linux NFS-HOWTO*. On doit s'intéresser plus particulièrement aux options : `ro|rw`, `sync|async` et `*squash`

5. Effectuer plusieurs séries de tests en modifiant les paramètres d'exportation et relever les différence à l'aide de captures avec l'analyseur réseau.

6. Réaliser une capture et relever les numéros de ports caractéristiques de des transactions de montage. Est-il possible de retrouver les informations échangées dans les données de capture ?

6. Gestion des droits sur le système de fichiers NFS

Le contrôle les droits sur les objets de l'arborescence exportée par le serveur NFS est limité au masque de permissions de ces objets. Il est donc important de faire correspondre les identifiants `uid` et `gid` entre le client et le serveur.

Les manipulations suivantes sont à réaliser en «concertation» entre les administrateurs des postes client et serveur.

1. Sur le serveur, créer un nouveau compte utilisateur fictif en lui affectant la valeur `1111` pour les identifiants `uid` et `gid`. Quelles sont les options de la commande **adduser** qui permettent de réaliser ces opérations ?

   Utiliser les pages de manuels de la commande **adduser**.

2. Toujours sur le serveur, créer plusieurs objets (fichiers et répertoires) avec des masques de permissions différents ayant pour propriétaire le nouveau compte utilisateur fictif. Quels sont les options des commandes **chmod** et **chown** à utiliser pour réaliser ces opérations ?

Utiliser les pages de manuels des commandes.

3. Sur le poste client, effectuer différents tests d'accès et de modification sur les nouveaux objets mis à disposition par le serveur NFS. Quelles sont les commandes qui permettent de modifier les droits sur les objets existants ?

   Utiliser les pages de manuels des commandes.

4. Sur le client, créer aussi un nouveau compte utilisateur fictif en lui affectant la valeur `1111` pour les identifiants `uid` et `gid`. Quelles sont les options de la commande **adduser** qui permettent de réaliser cesopérations ?

   Utiliser les pages de manuels de la commande **adduser**.

5. Une fois connecté avec ce nouveau compte utilisateur, reprendre les mêmes tests d'accès aux objets de l'arborescence exportée par le serveur NFS. Quelles sont les évolutions constatées ?

7. Système de fichiers NFS & sécurité

Il y a une vingtaine d'années que le mécanismes RPC et NFS ont été conçus. À cette époque la sécurité n'était pas une préoccupation aussi présente dans le système d'information. Il a donc fallu appliquer des fonctions de sécurité sur des protocoles qui n'étaient pas prévus pour.

On distingue 2 catégories dans les traitements de sécurisation :

Les appels RPC
: Le service `portmap` ne dispose d'aucun mécanisme interne de sécurité. C'est la raison pour laquelle on lui associe les utilitaires *TCP wrapper* qui «encadrent» les accès aux appels RPC.

  Il faut ajouter que l'affectation dynamique de numéro de port pour les montages NFS ne facilite pas la configuration des pare-feux. C'est encore une raison pour encadrer le fonctionnement de `portmap`. Jusqu'à la version 3 du protocole NFS on essaie de fixer à l'avance le numéro de port utilisé par le service `mountd`. À partir de la version 4, l'affectation dynamique est abandonnée au profit d'un numéro de port unique : tcp/2049.

Les échanges NFS
: Dans un premier temps, le serveur NFS définit la liste des clients autorisés à accéder à son système de fichiers. Ensuite, une fois l'opération de montage effectuée, les échanges NFS bénéficient «naturellement» du masque de permissions de tous les objets du système de fichiers.

  Jusqu'à la version 3 du protocole NFS aucun contrôle de confidentialité ou d'intégrité n'est effectué sur les échanges réseau. À partir de la version 4, des services de chiffrement ont été ajoutés pour chiffrer les flux et garantir l'intégrité des informations échangées.

1. Quel est le paquet qui contient les outils *TCP wrapper* ?

   Interroger les méta-données dans le cache du gestionnaire de paquet avec la commande **apt-cache** en cherchant les mots clés `tcp` et `wrapper`.

2. Quels sont les fichiers de configuration qui fixent les conditions d'accès aux services contrôlés par les *TCP wrappers* ?

   Consulter les pages de manuels des outils *TCP wrapper*.

3. Quel est l'outil qui permet de valider la syntaxe des fichiers de configuration en affichant l'état courant des contrôles d'accès ?

   Consulter la liste des fichiers du paquet.

4. Quel est le fichier de configuration à éditer pour limiter l'accès aux appels RPC au réseau local utilisé ?

   Utiliser les pages de manuels et les exemples du support *Linux NFS-HOWTO*.

5. Au niveau serveur, quelles sont les options d'exportation à utiliser pour s'assurer que le client ne pourra pas effectuer d'opération d'administration sur les objets de l'arborescence exportée ?

Utiliser les recommandations du support *Linux NFS-HOWTO*.

8. Documents de référence

Systèmes de fichiers réseau : NFS & CIFS

Systèmes de fichiers réseau : NFS & CIFS[5] : présentation des modes de fonctionnement des systèmes de fichiers réseau NFS & CIFS.

Linux NFS-HOWTO

Linux NFS-HOWTO[6] : documentation complète sur la configuration d'un serveur et d'un client NFS.

[5] http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.fs/
[6] http://nfs.sourceforge.net/nfs-howto/