Thierry DOSTES (tdostes "@" ibsm.cnrs-mrs.fr)
Maurice LIBES

JT SIARS – 24 & 25 Avril 2008

Les vservers au quotidien

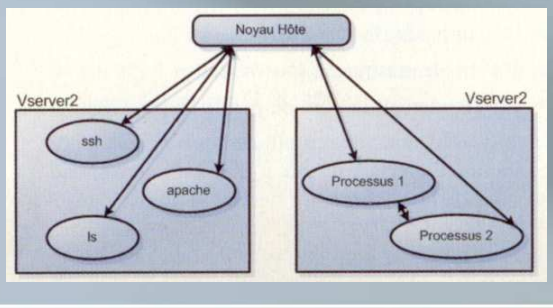
CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Rappels

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Architecture des vservers (1)

- Virtualisation qui intervient au niveau du noyau :
  - Faire croire à plusieurs machines.
  - Séparer les applications/contextes
- Le noyau est « patché » pour rendre cela possible.



Grâce au noyau modifié, la technologie Vserver met en œuvre des contextes séparés qui vont isoler les processus qu'ils hébergent. Ainsi, un processus externe ne pourra interagir avec le processus d'un vserver.

Ces contextes correspondent aux vservers que nous créons sur la machine hôte.

Par défaut, un contexte 0 est créé sur celle-ci. C'est ce contexte qui permet de créer les machines virtuelles et de faire croire à plusieurs machines.

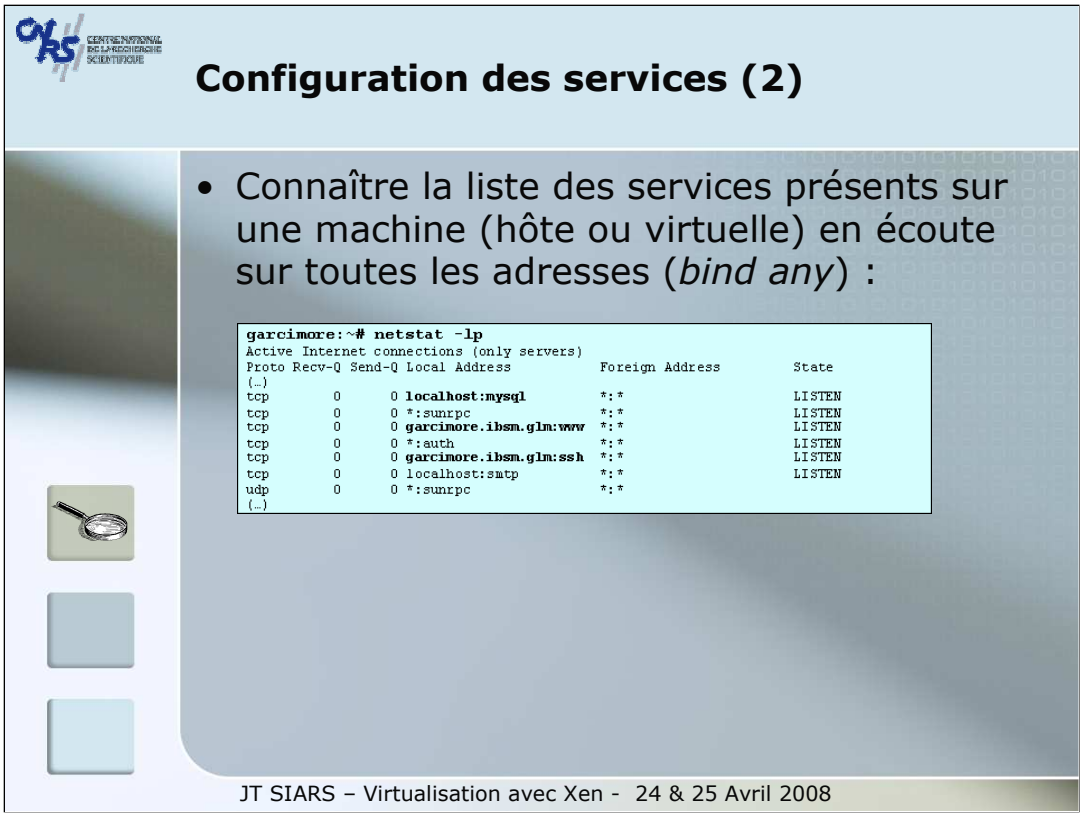
Architecture des vservers (2)

- Chaque contexte dispose d'une adresse IP.
- Le noyau route les informations vers le processus adéquat contenu dans le bon contexte.
- Conséquences :
  - Pas d'interface de boucle locale dans un contexte.
  - Pas de table de routage par vserver.
  - Configuration des services réseaux de l'hôte pour qu'ils écoutent seulement sur l'adresse IP de celui-ci.

Configuration des services (1)

- Bonnes pratiques :
  - Tout service lancé sur la machine hôte ou dans une machine virtuelle doit faire référence à une adresse IP précise « en écoute ».
  - Ainsi, tout trafic destiné à un port déjà utilisé (machine hôte ou virtuelle) sera correctement acheminé.
- Exemple : le service SSH.
  - Par défaut, le démon s'associe à l'adresse 0.0.0.0.
  - Toute requête sur le port SSH sera interceptée par le service en écoute sur cette adresse.

```
galileo:~# netstat -lp
Active Internet connections (only servers)
Proto Recv-Q      Send-Q      Local Address     Foreign Address   State
tcp     0           0           *:ssh             *:*           LISTEN
```



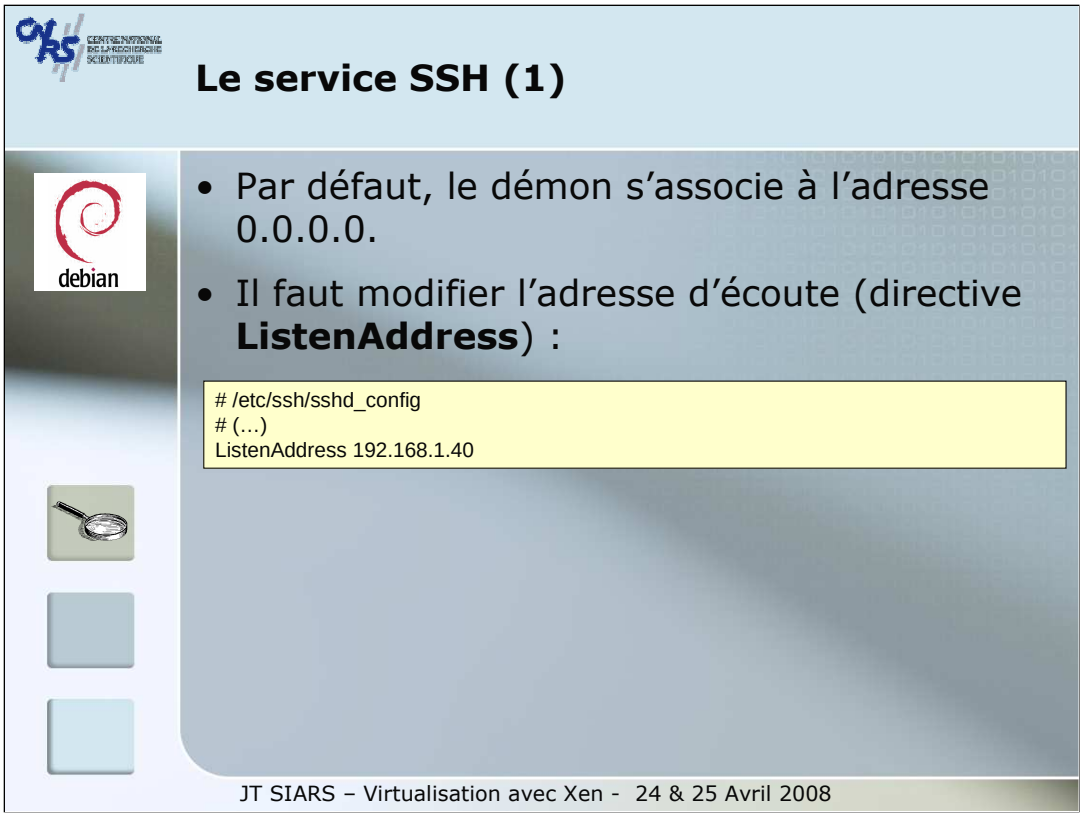
Nous constatons que les services Apache et ssh sont en écoute uniquement sur l'adresse IP propre à la machine physique.

Par défaut, le serveur mysql est en écoute sur **localhost** : nous ne rencontrerons aucun problème pour l'utiliser sur une machine virtuelle.

De même, le service SMTP écoute sur l'interface boucle locale. Cela est possible car nous sommes sur une machine hôte. Il en sera tout autrement dans le cadre vserver, puisque celui ne dispose pas d'une interface de boucle locale.

Exemples de mise en œuvre de services sur vservers.

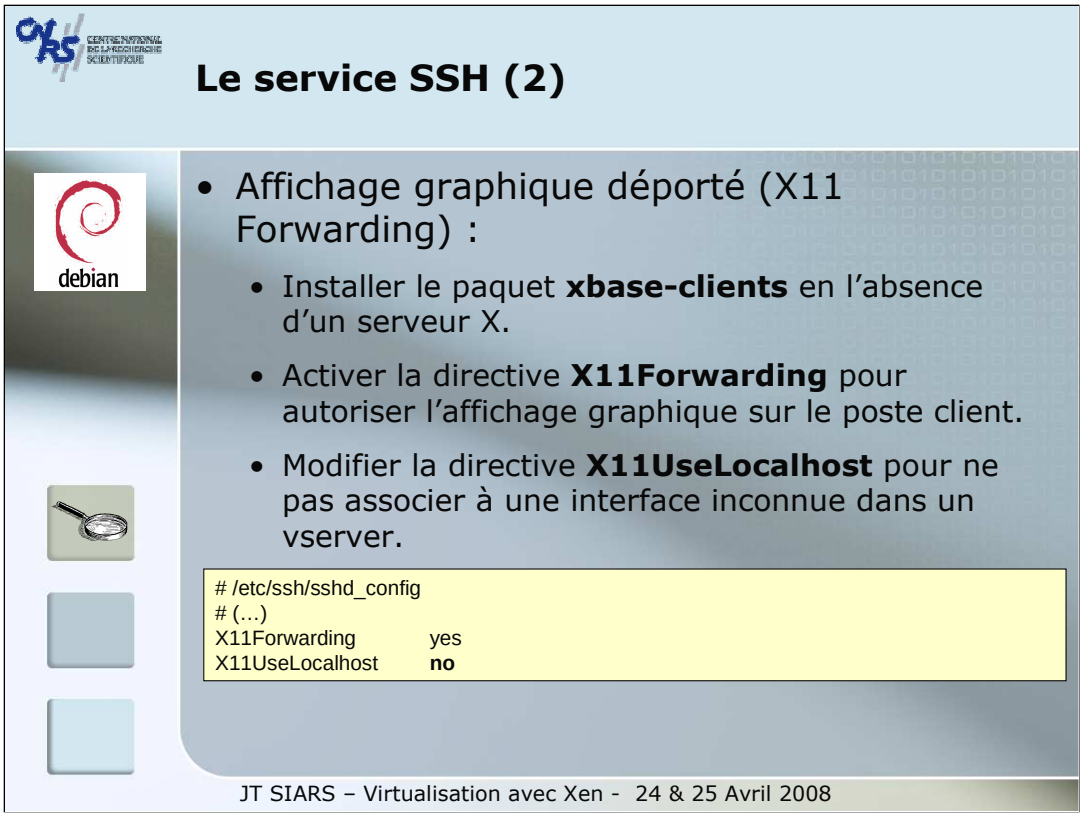
CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE



Par défaut, lors de l'installation du paquet Debian ssh, le démon du service s'associe à l'adresse **0.0.0.0**.

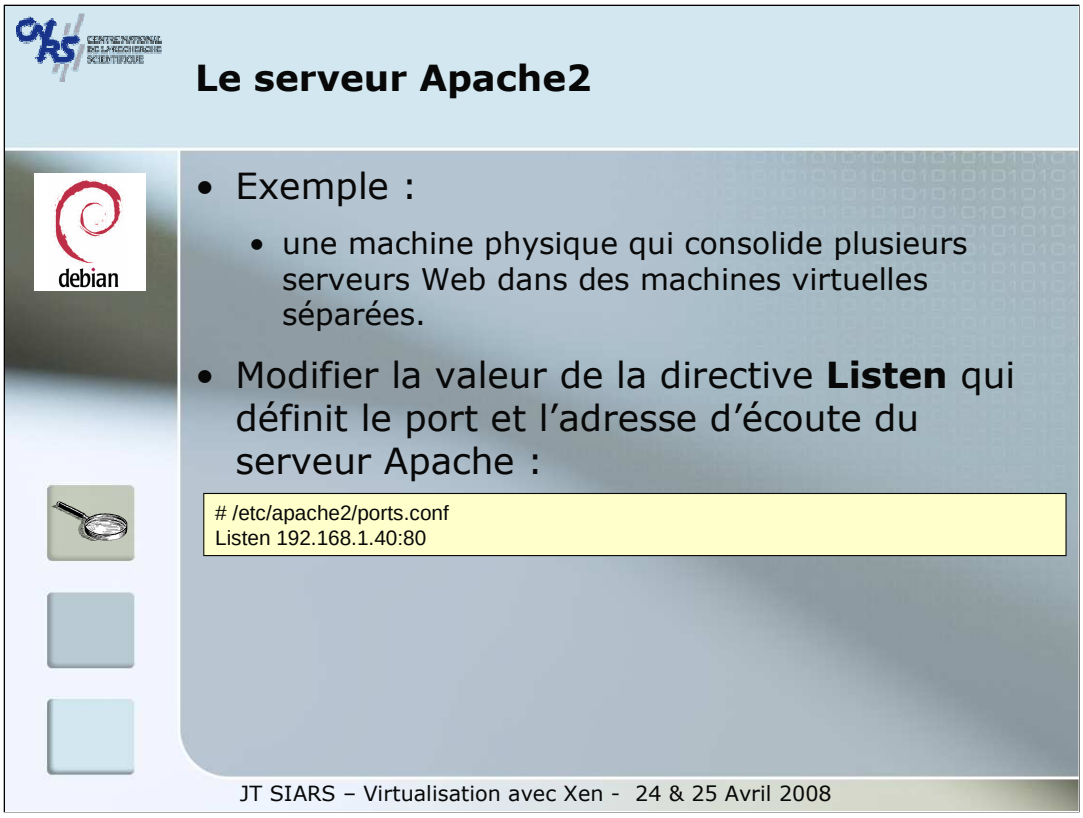
Cette astuce permet de vous dispenser d'installer le serveur ssh sur chacun de vos serveurs virtuels. Chaque connexion vous fera aboutir sur la machine hôte, même si vous spécifiez l'adresse IP d'un vserver.

Aussi, si vous souhaitez installer le démon ssh sur chaque machine virtuelle et si vous voulez pouvoir vous y connecter sans retomber systématiquement sur le service ssh de la machine hôte, alors vous devez modifier l'adresse à laquelle le démon de la machine hôte s'associe en la limitant à la seule adresse IP de cette dernière.



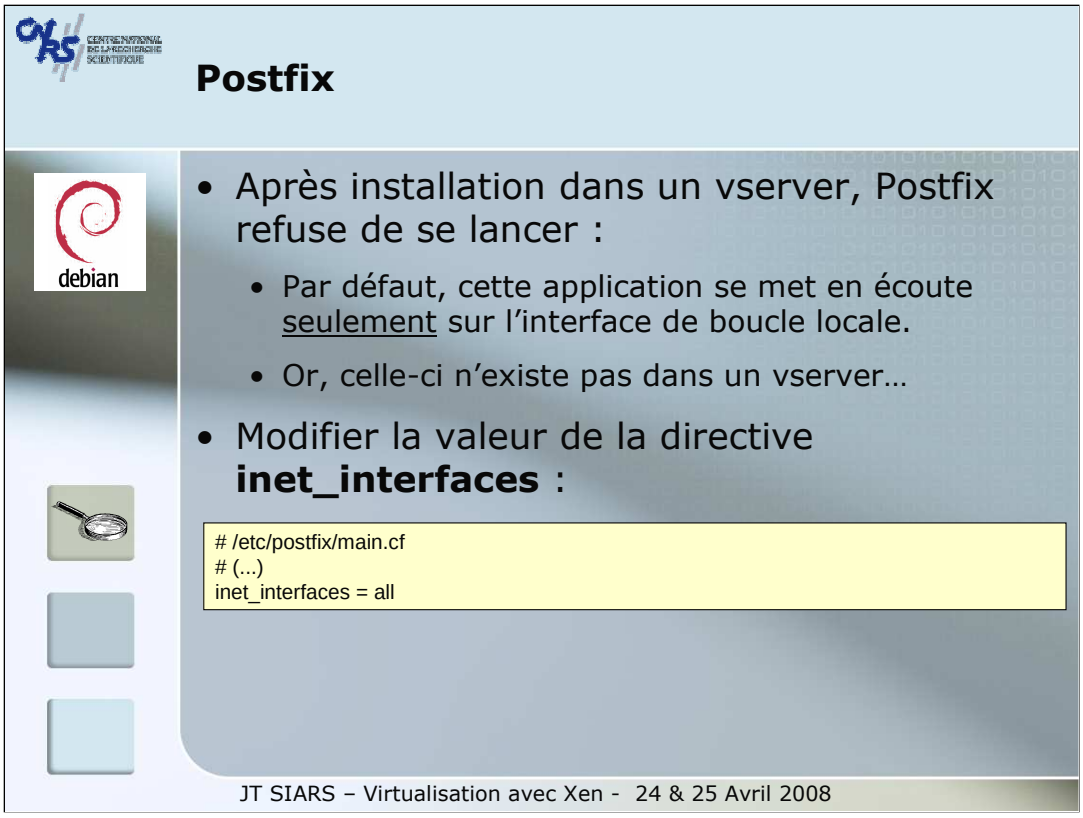
La directive **X11Forwarding** active l'affichage graphique déporté sur l'environnement graphique du client qui se connecte au serveur.

La directive **X11UseLocalhost** indique sur quelle interface réseau la redirection X11 sera couplée. Par défaut, le serveur sshd l'associe à l'adresse de loopback et fixe la variable d'environnement **DISPLAY** à la valeur ***localhost***, valeur qui sera utilisée par les hôtes distants pour se connecter. Dans le cas de notre serveur virtuel, la valeur ***localhost*** ne signifie pas grand-chose puisque toute requête vers ce « nom » sera interceptée par la machine physique hôte. Par conséquent, nous voulons que la valeur de la variable **DISPLAY** soit celle du nom de notre serveur virtuel.



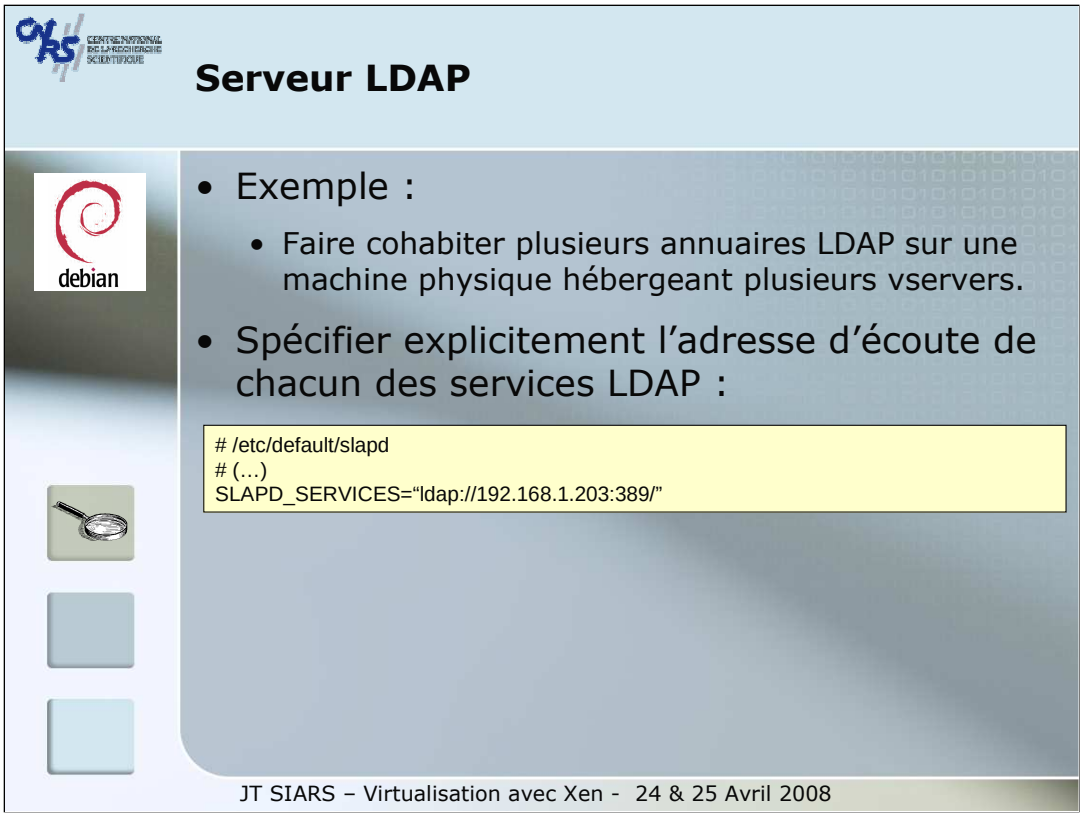
Par exemple, je veux lancer sur ma machine virtuelle un serveur Apache en écoute sur le port 80 alors que ma machine hôte en héberge déjà la même application active sur le même port.

Il faut modifier la configuration du service concerné pour qu'il reste en écoute uniquement sur l'adresse IP de la machine hôte. Nous modifions la valeur de la directive **Listen** présente dans le fichier de configuration **/etc/apache2/ports.conf**. Cette directive permet de spécifier les ports et les adresses pour lesquelles le serveur Apache est en écoute. Nous redémarrons ensuite le service Apache.



Si Postfix refuse de se lancer, éditez le fichier de configuration **/etc/postfix/main.cf** et vérifier la valeur de la directive **inet_interfaces**. Cette option précise les adresses pour lesquelles Postfix est en écoute. Par défaut, la valeur vaut **loopback-only**. Dans le cas des vservers, l'interface locale ne peut être activée. Ainsi, inet_interfaces = loopback-only empêche le démon de démarrer. En conséquence, il faut absolument :

inet_interfaces = all

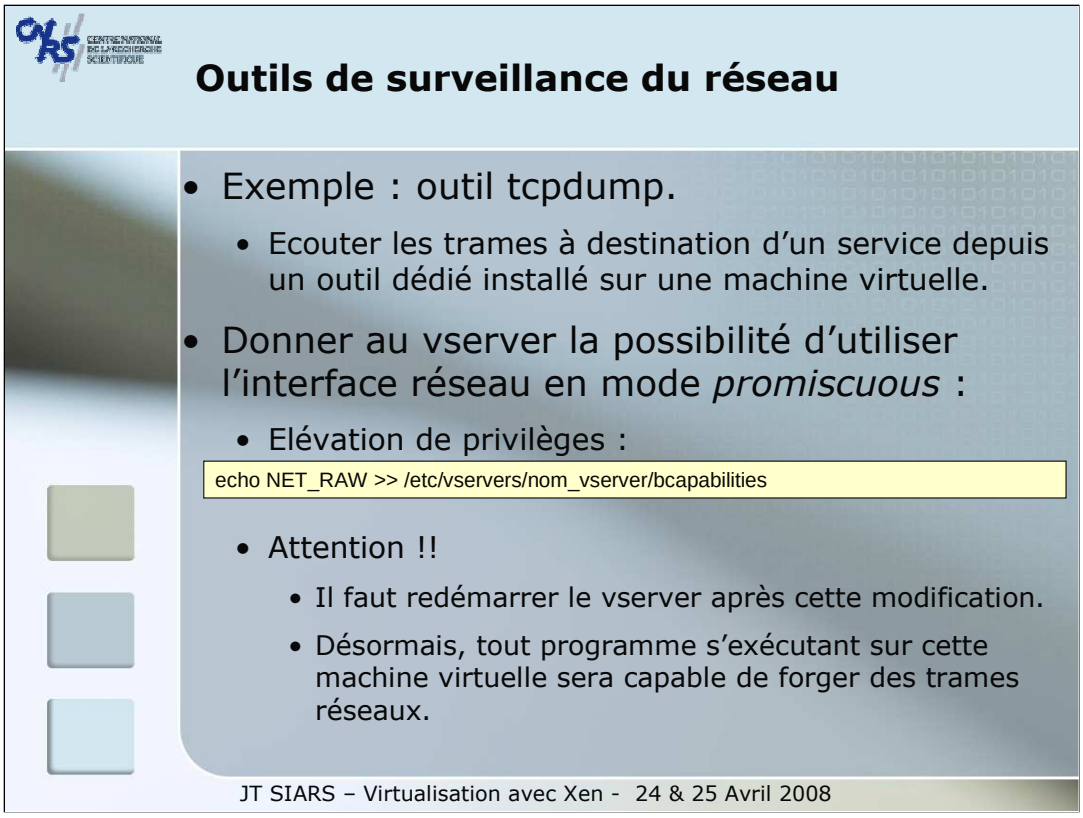


Si plusieurs annuaires LDAP sont amenés à cohabiter sur une machine physique hébergeant plusieurs serveurs virtuels (par exemple pour des tests), il est impératif de spécifier explicitement l'adresse d'écoute du serveur. Pour cela, nous modifions la directive **SLAPD_SERVICES** du fichier de configuration **/etc/default/slapd** :

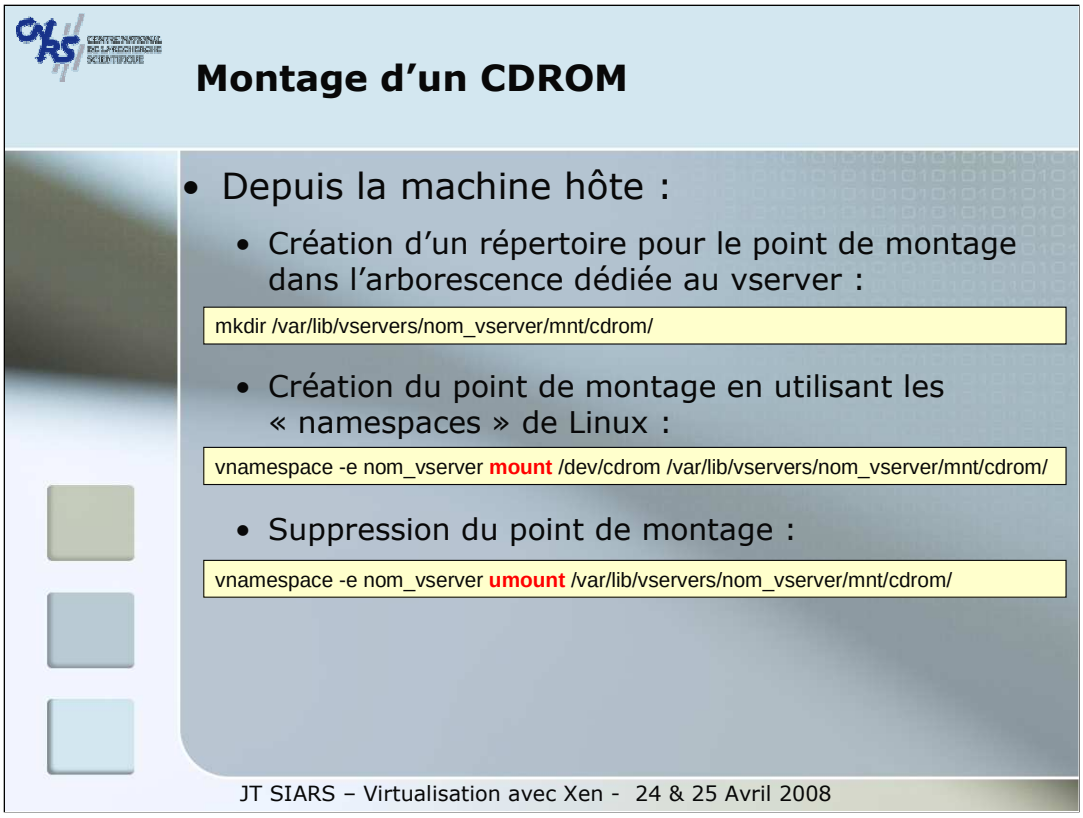
Supervision Nagios : serveur NRPE

- Exemple :
  - Installer l'agent NRPE de supervision sur plusieurs vservers hébergés par une même machine hôte.
- Spécifier explicitement l'adresse d'écoute de l'agent de supervision :

```
# /etc/nagios/nrpe.cfg
# (…)
server_address=192.168.1.32
```



Le mode promiscuous est souvent employé pour diagnostiquer des problèmes de connectivité réseau. Il existe des programmes (sniffeurs ou outils de statistiques) qui utilisent ce mode pour décoder et montrer tout le trafic du réseau à l'administrateur qui les exécute.



Les *namespaces* sont une fonctionnalité du noyau Linux, qui permet à différents processus d'avoir chacun une vue différente sur le système de fichier. En temps normal, nous disposons d'une seule et unique arborescence de fichiers avec des différents montages. Avec les namespaces, il est possible d' avoir différentes partitions montées pour chaque ensemble de processus souhaité.