Version : **2020.01**

Dernière mise-à-jour : 2020/01/30 03:28

SO215 - Gestion des Serveurs de Base

LAB #1 - Installation et Configuration du Serveur DNS bind

Le principe du DNS est basé sur l'équivalence entre un **FQDN** (Fully Qualified Domain Name) et une adresse IP. Les humains retiennent plus facilement des noms tels www.ittraining.center, tandis que les ordinateurs utilisent des chiffres.

Le **DNS** (Domain Name Service) est né peu après l'introduction des FQDN en 1981.

Lorque un ordinateur souhaite communiquer avec un autre par le biais de son nom, par exemple avec www.ittraining.center, il envoie une requête à un server DNS. Si le serveur DNS a connaissance de la correspondance entre le nom demandé et le numéro IP, il répond directement. Si ce n'est pas le cas, il démarre un processus de **Recursive Lookup**.

Ce processus tente d'identifier le serveur de domaine responsable pour le **SLD** (Second Level Domain) afin de lui passer la reqûete. Dans notre exemple, il tenterait d'identifier le serveur de domaine responsable de **ittraining.center**.

Si cette tentative échoue, le serveur DNS cherche le serveur de domaine pour le **TLD** (Top Level Domain) dans son cache afin de lui demander l'adresse du serveur responsable du SLD. Dans notre cas il tenterait trouver l'enregistrement pour le serveur de domaine responsable de **.org**

Si cette recherche échoue, le serveur s'adresse à un **Root Name Server** dont il y en a peu. Si le Root Name Server ne peut pas répondre, le serveur DNS renvoie une erreur à la machine ayant formulé la demande.

Le serveur DNS sert à faire la résolution de noms. Autrement dit de traduire une adresse Internet telle **www.ittraining.center** en **numéro IP**.

Le serveur DNS peut être configuré de trois façons différentes:

- **Serveur DNS Primaire ou Maitre**
  - Ce type de serveur est dit maitre **d'une ou de plusieurs zones** et peut répondre aux requêtes des clients.

- **Serveur DNS Secondaire**
  - Ce type de serveur est une copie d'un serveur DNS primaire et peut répondre aux requêtes des clients.
- **Serveur DNS Cache**
  - Ce type de serveur ne peut pas répondre aux requêtes des clients. Le requêtes sont transférés à un autre serveur DNS. Les réponses sont mises en cache pour une utilisation ultérieure.

Le serveur DNS nécessite à ce que la machine sur laquelle il est installé possède un nom FQDN et une adresse IP fixe. Il est également important à noter que le service de bind ne démarrera **pas** dans le cas où le fichier **/etc/hosts** comporte une anomalie. Deux étapes préparatoires sont donc nécessaires :

- Modification de l'adresse IP de la machine en adresse IP fixe
- Définition d'un nom FQDN (Fully Qualified Domain Name)

Afin d'étudier ce dernier cas, nous prenons en tant qu'exemple la machine suivante :

- **FQDN** - solaris.i2tch.loc
- **Adresse IP** - 10.0.2.15

> **Important** - Il est important de noter que la configuration du serveur DNS dépend du nom de votre machine. Dans le cas où vous changeriez ce nom, vous devez re-configurer votre serveur DNS en éditant les fichiers de configuration directement.

Installation

Les deux paquets nécessaires pour la mise en place d'un serveur DNS sont :

```
# pkginfo | grep -i SUNWbind
system      SUNWbind                        BIND DNS Name server and tools
system      SUNWbindr                       BIND Name server Manifest
```

Par défaut, le service **svc:/network/dns/server:default** est désactivé.

```
# svcs -a | grep dns
disabled        3:56:19 svc:/network/dns/client:default
disabled        3:56:19 svc:/network/dns/server:default
```

Les fichiers de configuration génériques

- /var/run/named.pid
- /var/named/named.ca
- /etc/named.conf
- /etc/rndc.key

/var/run/named.pid

Ce fichier contiendra le numéro du processus de named.

/var/named/named.ca

Ce fichier se trouve dans /var/named. Il est aussi appelé le fichier **root.hints** car il contient les adresses des serveurs DNS root de l'Internet.

Pour créer ce fichier, il convient d'utiliser la commande **dig** :

```
# mkdir /var/named
# cd /var/named
# /usr/sbin/dig @192.36.148.17 . ns > named.ca
# cat named.ca

; <<>> DiG 9.6-ESV-R8 <<>> @192.36.148.17 . ns
; (1 server found)
```

```
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46290
;; flags: qr aa rd; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 13
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       518400  IN      NS      d.root-servers.net.
.                       518400  IN      NS      j.root-servers.net.
.                       518400  IN      NS      l.root-servers.net.
.                       518400  IN      NS      h.root-servers.net.
.                       518400  IN      NS      m.root-servers.net.
.                       518400  IN      NS      a.root-servers.net.
.                       518400  IN      NS      b.root-servers.net.
.                       518400  IN      NS      g.root-servers.net.
.                       518400  IN      NS      i.root-servers.net.
.                       518400  IN      NS      c.root-servers.net.
.                       518400  IN      NS      k.root-servers.net.
.                       518400  IN      NS      e.root-servers.net.
.                       518400  IN      NS      f.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net.     3600000 IN      A       198.41.0.4
a.root-servers.net.     3600000 IN      AAAA    2001:503:ba3e::2:30
b.root-servers.net.     3600000 IN      A       199.9.14.201
b.root-servers.net.     3600000 IN      AAAA    2001:500:200::b
c.root-servers.net.     3600000 IN      A       192.33.4.12
c.root-servers.net.     3600000 IN      AAAA    2001:500:2::c
d.root-servers.net.     3600000 IN      A       199.7.91.13
d.root-servers.net.     3600000 IN      AAAA    2001:500:2d::d
e.root-servers.net.     3600000 IN      A       192.203.230.10
```

```
e.root-servers.net.     3600000 IN      AAAA    2001:500:a8::e
f.root-servers.net.     3600000 IN      A       192.5.5.241
f.root-servers.net.     3600000 IN      AAAA    2001:500:2f::f
g.root-servers.net.     3600000 IN      A       192.112.36.4

;; Query time: 111 msec
;; SERVER: 192.36.148.17#53(192.36.148.17)
;; WHEN: Fri Jan 17 03:58:54 2020
;; MSG SIZE  rcvd: 508
```

/etc/named.conf

Le fichier de configuration principal du serveur DNS Bind est **/etc/named.conf** :

```
# vi /etc/named.conf
# cat /etc/named.conf
options {
    directory "/var/named";
    pid-file "/var/named/named.pid";
    allow-query { any; };
    allow-transfer { any; };
        forwarders { 10.0.2.3; };
};

zone "localhost" {
    type master;
    file "zone/db.localhost";
};

zone "0.0.127.in-addr.arpa" {
    type master;
    file "zone/db.127.0.0.1";
};
```

```
zone "." {
    type hint;
    file "named.ca";
};

zone "2.0.10.in-addr.arpa" {
    type master;
    file "zone/db.2.0.10.hosts";
    forwarders { };
};

zone "i2tch.loc" {
    type master;
    file "zone/db.i2tch.loc.hosts";
    forwarders { };
};
```

Vérifiez le fichier **/etc/named.conf** :

```
# /usr/sbin/named-checkconf
#
```

Dans ce fichier on trouve des sections ayant la forme suivante :

```
section {
   variable1  valeur1;
   variable2  valeur2;
};
```

Il existe différentes sections dont une des plus importantes est **options**. C'est dans cette section que nous définissons les options globales:

```
options {
```

D'abord nous définissons le chemin des fichiers des **zones**:

```
directory "/var/named";
```

Ensuite le fichier pid :

```
pid-file "/var/named/named.pid";
```

Afin de limiter les machines qui peuvent et qui ne peuvent pas utiliser notre DNS, nous utilisons la valeur **allow-query**. Dans notre cas les requêtes sont permises en provenance de tous les clients:

```
allow-query { any; };
```

Dans l'**exemple** qui suit nous autorisons toutes les machines de notre réseau sauf la machine 10.0.2.5, ainsi que la machine locale :

```
     allow-query {
          127/8;
          10.0.2/24;
          !10.0.2.5;
     };
```

La valeur **allow-transfer** autorise les transferts de requête de zones pour tous les clients. La valeur allow-transfer peut également se trouver dans chaque section de zone (voir ci-dessous) :

```
allow-transfer { any;};
```

Dernièrement, nous définissons l'adresse du serveur DNS auquel seront envoyées des requêtes inconnues :

```
  forwarders { 10.0.2.3; };
};
```

La valeur “type” dans une section de zone peut prendre plusieurs valeurs:

- **master**
    - Ce type définit le serveur DNS comme serveur maître ayant **autorité** sur la zone concernée.

- **slave**
  - Ce type définit le serveur DNS comme serveur esclave pour la zone concernée. Ceci implique que la zone est une replication d'une zone maître. Un type de zone esclave contiendra aussi une directive **masters** indiquant les adresses IP des serveurs DNS maîtres.
- **stub**
  - Ce type définit le serveur DNS comme serveur esclave pour la zone concernée mais uniquement pour les **enregistrements** de type **NS**.
- **forward**
  - Ce type définit le serveur DNS comme serveur de transit pour la zone concernée. Ceci implique que toute requête est re-transmise vers un autre serveur.
- **hint**
  - Ce type définit la zone concernée comme une zone racine. Ceci implique que lors du démarrage du serveur, cette zone est utilisée pour récupérer les adresses des serveurs DNS racine.

La valeur “notify” est utilisée pour indiquer si non (no) ou oui (yes) les autres serveurs DNS sont informés de changements dans la zone.

La deuxième directive dans une section de zone comporte la valeur **file**. Il indique l'emplacement du fichier de zone.

Chaque section de zone, à l'exception de la zone “.” est associée avec une section de zone inversée.

```
zone "." {
    type hint;
    file "named.ca";
};
```

La section de zone fait correspondre un nom avec une adresse IP tandis que la section de zone inversée fait l'inverse. La section inversée a un nom d'un syntaxe spécifique :

```
adresse_réseau_inversée.in-addr.arpa.
```

Par exemple, la zone suivante correspond à notre domaine, ici appelée “i2tch.loc”. Une valeur de {!*} interdirait tout transfert de requête de zone. Celui-ci fait correspondre le nom de la machine avec son adresse IP:

```
zone "i2tch.loc" {
    type master;
    file "zone/db.i2tch.loc.hosts";
```

```
    forwarders { };
};
```

La zone suivante est également celle de notre machine mais dans le sens inverse. Le fichier **zone/db.2.0.10.hosts** fait correspondre notre adresse IP avec le nom de la machine.

```
zone "2.0.10.in-addr.arpa" {
    type master;
    file "zone/db.2.0.10.hosts";
    forwarders { };
};
```

Cette zone est la zone créée pour le réseau loopback :

```
zone "localhost" {
    type master;
    file "zone/db.localhost";
};
```

La zone suivante est la zone créée pour le réseau loopback mais dans le sens inverse. Le fichier **zone/db.127.0.0.1** fait correspondre l'adresse IP 127.0.0.1 avec le nom localhost:

```
zone "0.0.127.in-addr.arpa" {
    type master;
    file "zone/db.127.0.0.1";
};
```

Les fichiers de configuration des zones

- /var/named/zone/db.127.0.0.1
- /var/named/zone/db.localhost
- /var/named/zone/db.2.0.10.hosts
- /var/named/zone/db.i2tch.loc.hosts

Important - Chacun de ses fichiers a besoin d'être créé.

Les fichiers de zone sont composées de lignes d'une forme:

nom	TTL	classe	type	donnée

où

- **nom**
  - Le nom DNS.
- **TTL**
  - La durée de vie en cache de cet enregistrement.
- **classe**
  - Le réseau de transport utilisé. Dans notre cas, le réseau est du TCP. La valeur est donc IN.
- **type**
  - Le type d'enregistrement:
    - SOA - Start of Authority - se trouve au début du fichier et contient des informations générales
    - NS - Name Server - le nom du serveur de nom
    - A - Address - indique une résoltuion de nom vers une adresse IP. Ne se trouve que dans les fichiers **.hosts**
    - PTR - PoinTeR - indique une résoltuion d'une adresse IP vers un nom. Ne se trouve que dans les fichiers inversés.
    - MX - Mail eXchange - le nom d'un serveur de mail.
    - CNAME - Canonical Name - un alias d'une machine.
    - HINFO - Hardware Info - fournit des informations sur le matériel de la machine
- **donnée**
  - La donnée de la ressource:
    - Une adresse IP pour un enregistrement de type A
    - Un nom de machine pour un eregistrement de type PTR

Créez le répertoire **/var/named/zone** :

```
# mkdir /var/named/zone
```

db.i2tch.loc.hosts

Ce fichier se trouve dans /var/named/zone. Il est le fichier qui définit la correspondance du nom de la machine **solaris.i2tch.loc** avec son numéro IP, à savoir le **10.0.2.15**. On définit dans ce fichier les machines qui doivent être appelées par leur nom :

```
# vi /var/named/zone/db.i2tch.loc.hosts
# cat /var/named/zone/db.i2tch.loc.hosts
$TTL 3D
@       IN      SOA     solaris.i2tch.loc. root.solaris.i2tch.loc. (
               20200117       ; Serial
               8H   ; Refresh
               2H   ; Retry
               4W  ; Expire
               1D)  ; Minimum TTL
               IN      NS      solaris.i2tch.loc.
localhost                  A       127.0.0.1
dnsmaster                  IN      CNAME   solaris.i2tch.loc.
solaris.i2tch.loc.       IN      A      10.0.2.15

ftp IN CNAME solaris.i2tch.loc.
www IN CNAME solaris.i2tch.loc.
mail IN CNAME solaris.i2tch.loc.
news IN CNAME solaris.i2tch.loc.
```

La première ligne de ce fichier commence par une ligne semblable à celle-ci:

```
$TTL 3D
```

Cette ligne indique aux autres serveurs DNS pendant combien de temps ils doivent garder en cache les enregistrements de cette zone. La durée peut s'exprimer en jours (**D**), en heures (**H**) ou en secondes (**S**).

La deuxième ligne définit une **classe IN**ternet, un **SOA** (Start Of Authority), le nom du serveur primaire et l'adresse de l'administrateur de mail :

```
@       IN      SOA     solaris.i2tch.loc. root.solaris.i2tch.loc. (
```

Le caractère **@** corréspond au nom de la zone et est une abréviation pour le nom de la zone décrit par le fichier de la zone, soit dans ce cas db.**i2tch.loc**.hosts, et présent dans le fichier /etc/named.conf :

```
zone "i2tch.loc" {
      type master;
      file "zone/db.i2tch.loc.hosts";
      forwarders { };
};
```

> **Important** - Notez le point à la fin de chaque nom de domaine. Notez bien le remplacement du caractère @ dans l'adresse email de l'administrateur de mail par le caractère “.”

Le numéro de série doit être modifié chaque fois que le fichier soit changé. Il faut noter que dans le cas de plusieurs changements dans la même journée il est necessaire d'incrémenter les deux derniers chiffres du numéro de série. Par exemple, dans le cas de deux changements en date du 02/12/2019, le premier fichier comportera une ligne Serial avec la valeur 2019120201 tandis que le deuxième changement comportera le numéro de série 2019120202:

```
       20200117       ; Serial
```

La ligne suivante fixe le temps de rafraichissement, soit 8 heures:

```
       8H ; Refresh
```

La ligne suivante fixe le temps entre de nouveaux essaies, soit 2 heures:

```
       2H ; Retry
```

La ligne suivante fixe le temps d'expiration, soit 4 semaines:

```
        4W ; Expire
```

La ligne suivante fix le temps minimum pour la valeur TTL, soit un jour:

```
        1D) ; Minimum TTL
```

Cette ligne identifie notre serveur de noms :

```
IN NS solaris.i2tch.loc.
```

Dans le cas où notre serveur était également un serveur mail. Nous trouverions aussi une entrée du type SMTP (MX) :

```
IN MX 10 mail.i2tch.loc.
```

Ci-dessous on définit avec une entrée du type A, les machines que l'on souhaite appeler par leur nom, à savoir **solaris.i2tch.loc** et **localhost** :

```
localhost                   A           127.0.0.1
solaris.i2tch.loc.      IN A        10.0.2.15
```

Ci-dessous on définit des **Alias** avec des entrées du type CNAME. Les alias servent à identifier une machine.

```
dnsmaster IN CNAME solaris.i2tch.loc.
ftp IN CNAME solaris.i2tch.loc.
www IN CNAME solaris.i2tch.loc.
mail IN CNAME solaris.i2tch.loc.
news IN CNAME solaris.i2tch.loc.
```

Il est possible de vérifier ce fichier grâce à la commande **/usr/sbin/named-checkzone** :

```
# cd /var/named/zone
# /usr/sbin/named-checkzone i2tch.loc db.i2tch.loc.hosts
```

```
zone i2tch.loc/IN: loaded serial 20200117
OK
```

db.2.0.10.hosts

Ce fichier se trouve dans /var/named/zone. Il est le fichier qui définit la correspondance de l'adresse IP de la machine, à savoir le **10.0.2.15** avec le nom **solaris.i2tch.loc.** Le chiffre **15** dans la dernière ligne correspond au 10.0.2.**15**:

```
# vi db.2.0.10.hosts
# cat db.2.0.10.hosts
$TTL 3D
@       IN      SOA     solaris.i2tch.loc.        solaris.i2tch.loc. (
                20200117 ; Serial
                10800   ; Refresh
                3600    ; Retry
                604800  ; Expire
                86400) ; Minimum TTL
                NS      solaris.i2tch.loc.
15       IN      PTR     solaris.i2tch.loc.
```

Il est possible de vérifier ce fichier grâce à la commande **/usr/sbin/named-checkzone** :

```
# /usr/sbin/named-checkzone 2.0.10.in-addr.arpa db.2.0.10.hosts
zone 2.0.10.in-addr.arpa/IN: loaded serial 20200117
OK
```

db.127.0.0.1

Ce fichier se trouve dans /var/named/zone. Il est le fichier qui définit la correspondance entre l'adresse IP **127.0.0.1** et le nom **localhost** :

```
# vi db.127.0.0.1
```

```
# cat db.127.0.0.1
$TTL 3D
@               IN      SOA     i2tch.loc. root.i2tch.loc. (
                20200117 ; Serial
                28800   ; Refresh
                7200    ; Retry
                604800  ; Expire
                86400)  ; Minimum TTL
                NS      solaris.i2tch.loc.
localhost      IN       A     127.0.0.1
```

Vérifier la syntaxe de ce fichier :

```
# /usr/sbin/named-checkzone 0.0.127.in-addr.arpa db.127.0.0.1
zone 0.0.127.in-addr.arpa/IN: loaded serial 20200117
OK
```

db.localhost

Ce fichier se trouve dans /var/named/zone. Il est le fichier qui définit la correspondance du nom **localhost** avec l'adresse IP **127.0.0.1** :

```
# vi db.localhost
# cat db.localhost
$TTL 3D
@       IN      SOA     solaris.i2tch.loc. root.solaris.i2tch.loc. (
         20200117  ; Serial
         8H  ; Refresh
         2H  ; Retry
         4W  ; Expire
         1D) ; Minimum TTL
         NS  solaris.i2tch.loc.
1        IN PTR   localhost.
```

Vérifier la syntaxe de ce fichier :

```
# /usr/sbin/named-checkzone localhost db.localhost
zone localhost/IN: loaded serial 20200117
OK
```

Il est maintenant possible de démarrer le serveur DNS :

<coe> # /usr/sbin/svcadm enable svc:/network/dns/server:default </code>

Avant de pouvoir tester votre serveur DNS, vous avez besoin d'indiquer à votre machine qu'elle doit utiliser elle-même pour la résolution des noms.

Pour le faire, il convient d'éditer le fichier **/etc/resolv.conf** :

```
# vi /etc/resolv.conf
# cat /etc/resolv.conf
nameserver 10.0.2.15
nameserver 10.0.2.3
```

Testez maintenant votre serveur DNS grâce à les commandes **nslookup** et **dig**:

```
# nslookup www.ittraining.center
Server:         10.0.2.15
Address:        10.0.2.15#53

Non-authoritative answer:
Name:   www.ittraining.center
Address: 217.160.0.225

# dig www.ittraining.center

; <<>> DiG 9.6-ESV-R8 <<>> www.ittraining.center
;; global options: +cmd
```

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19555
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 13, ADDITIONAL: 11

;; QUESTION SECTION:
;www.ittraining.center.         IN      A

;; ANSWER SECTION:
www.ittraining.center.  3587    IN      A       217.160.0.225

;; AUTHORITY SECTION:
.                       7153    IN      NS      m.root-servers.net.
.                       7153    IN      NS      a.root-servers.net.
.                       7153    IN      NS      e.root-servers.net.
.                       7153    IN      NS      i.root-servers.net.
.                       7153    IN      NS      j.root-servers.net.
.                       7153    IN      NS      f.root-servers.net.
.                       7153    IN      NS      k.root-servers.net.
.                       7153    IN      NS      b.root-servers.net.
.                       7153    IN      NS      g.root-servers.net.
.                       7153    IN      NS      d.root-servers.net.
.                       7153    IN      NS      h.root-servers.net.
.                       7153    IN      NS      l.root-servers.net.
.                       7153    IN      NS      c.root-servers.net.

;; ADDITIONAL SECTION:
l.root-servers.net.     604754  IN      A       199.7.83.42
l.root-servers.net.     604754  IN      AAAA    2001:500:3::42
m.root-servers.net.     604754  IN      A       202.12.27.33
m.root-servers.net.     604754  IN      AAAA    2001:dc3::35
k.root-servers.net.     604754  IN      A       193.0.14.129
k.root-servers.net.     604754  IN      AAAA    2001:7fd::1
h.root-servers.net.     604754  IN      A       128.63.2.53
h.root-servers.net.     604754  IN      AAAA    2001:500:1::803f:235
```

```
i.root-servers.net.     604754  IN      A       192.36.148.17
i.root-servers.net.     604754  IN      AAAA    2001:7fe::53
j.root-servers.net.     604754  IN      A       192.58.128.30

;; Query time: 0 msec
;; SERVER: 10.0.2.15#53(10.0.2.15)
;; WHEN: Fri Jan 17 11:12:56 2020
;; MSG SIZE  rcvd: 502
```

LAB #2 - Installation et Configuration du Serveur d'Horloge

Introduction

Dans le cas d'un serveur de réseau, il est souvent important de maintenir l'heure de la machine à l'heure exacte pour des raisons de simplification de synchronisation avec des portables ou bien des systèmes de fichiers externes. Pour accomplir cette tâche, nous utilisons les services de serveurs de temps publics disponibles sur Internet sur lesquels nous synchronisons l'horloge de notre serveur. De même, les machines de notre réseau peuvent se synchroniser ensuite avec l'heure de notre serveur.

Le protocole utilisé s'appelle **NTP** (**Network Time Protocol**) qui utilise le port **123**. Celui-ci, permet la synchronisation avec plusieurs serveurs publics. Les serveurs de temps de racine s'appellent des serveurs de **Strate 1**. En dessous se trouvent des serveurs de Strate 2, Strate 3 etc..

Pour connaître le fuseau d'horaire local, utilisez la commande **date** :

```
# date
Fri Jan 17 11:23:14 CET 2020
```

> **Important** - Vous pouvez consulter la liste des codes des zones à l'adresse **http://www.timeanddate.com/library/abbreviations/timezones/**.

Vous pouvez modifier le fuseau d'horaire à l'aide de la commande **tzselect** :

```
# tzselect
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
 1) Africa
 2) Americas
 3) Antarctica
 4) Arctic Ocean
 5) Asia
 6) Atlantic Ocean
 7) Australia
 8) Europe
 9) Indian Ocean
10) Pacific Ocean
11) none - I want to specify the time zone using the POSIX TZ format.
#?
```

Installation

Sous **Solaris**, le serveur ntp est installé par défaut mais désactivé :

```
# svcs -a | grep ntp
disabled        3:56:19 svc:/network/ntp:default
disabled        3:56:20 svc:/network/ntp4:default
```

Activez ensuite le serveur ntp et vérifiez son fonctionnement :

```
# svcadm enable network/ntp
# svcadm enable network/ntp4
# svcs -a | grep ntp
maintenance    11:24:51 svc:/network/ntp:default
```

```
maintenance    11:25:17 svc:/network/ntp4:default
```

Important - Ces services sont respectivement NFSv3 et NFSv4. Les services sont **mutuellement exclusifs**.

A ce stade on peut constater que les services sont en **maintenance**. Consultez donc chaque service pour connaître la raison :

```
# svcs -l network/ntp
fmri         svc:/network/ntp:default
name         Network Time Protocol (NTP)
enabled      true
state        maintenance
next_state   none
state_time   Fri Jan 17 11:24:51 2020
logfile      /var/svc/log/network-ntp:default.log
restarter    svc:/system/svc/restarter:default
contract_id
dependency   require_all/error file://localhost/usr/sbin/ntpq (online) file://localhost/usr/sbin/ntpdate (online)
dependency   require_any/error svc:/network/service (online)
dependency   optional_all/error svc:/milestone/name-services (online)
dependency   require_all/error svc:/system/filesystem/minimal (online)
# svcs -l network/ntp4
fmri         svc:/network/ntp4:default
name         Network Time Protocol (NTP) Version 4
enabled      true
state        maintenance
next_state   none
state_time   Fri Jan 17 11:25:17 2020
logfile      /var/svc/log/network-ntp4:default.log
restarter    svc:/system/svc/restarter:default
contract_id
dependency   require_any/error svc:/network/service (online)
```

```
dependency   exclude_all/none svc:/network/ntp (maintenance)
```

Vous pouvez constater que le problème du service **/network/ntp** ne vient pas des dépendances. Consultez donc les fichiers journaux :

```
# cat /var/svc/log/network-ntp:default.log
[ Nov 29 13:26:33 Disabled. ]
[ Nov 29 13:26:33 Rereading configuration. ]
[ Jan 17 11:24:51 Enabled. ]
[ Jan 17 11:24:51 Executing start method ("/lib/svc/method/xntp") ]
[ Jan 17 11:24:51 Method "start" exited with status 96 ]
# cat /var/svc/log/network-ntp4:default.log
[ Nov 29 13:26:33 Disabled. ]
[ Nov 29 13:26:33 Rereading configuration. ]
[ Jan 17 11:25:17 Enabled. ]
[ Jan 17 11:25:17 Executing start method ("/lib/svc/method/ntp start") ]
Error: Configuration file '/etc/inet/ntp.conf' not found.   See ntpd(1M).
[ Jan 17 11:25:17 Method "start" exited with status 96 ]
```

Important - La sortie nous indique une mauvaise configuration (exited with status 96) du au fait que le fichier **/etc/inet/ntp.conf** n'a pas été trouvé.

Le fichier ntp.conf

Le service **ntp** est configuré par le fichier **/etc/inet/ntp.conf**. Ce fichier n'existe pas sous Solaris. Il est donc necéssaire d'utiliser un fichier modèle fourni :

```
# cp /etc/inet/ntp.server /etc/inet/ntp.conf
```

Ouvrez ce fichier afin de consulter son contenu :

```
# cat /etc/inet/ntp.conf
# ident "@(#)ntp.server 1.7     03/01/17 SMI"
#
# Copyright 1996-2003 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
# /etc/inet/ntp.server
#
# An example file that could be copied over to /etc/inet/ntp.conf and
# edited; it provides a configuration template for a server that
# listens to an external hardware clock, synchronizes the local clock,
# and announces itself on the NTP multicast net.
#

# This is the external clock device.  The following devices are
# recognized by xntpd 3-5.93e:
#
# XType Device    RefID          Description
# -------------------------------------------------------
#  1    local     LCL            Undisciplined Local Clock
#  2    trak      GPS            TRAK 8820 GPS Receiver
#  3    pst       WWV            PSTI/Traconex WWV/WWVH Receiver
#  4    wwvb      WWVB           Spectracom WWVB Receiver
#  5    true      TRUE           TrueTime GPS/GOES Receivers
#  6    irig      IRIG           IRIG Audio Decoder
#  7    chu       CHU            Scratchbuilt CHU Receiver
#  8    parse     ----           Generic Reference Clock Driver
#  9    mx4200    GPS            Magnavox MX4200 GPS Receiver
# 10    as2201    GPS            Austron 2201A GPS Receiver
# 11    arbiter   GPS            Arbiter 1088A/B GPS Receiver
# 12    tpro      IRIG           KSI/Odetics TPRO/S IRIG Interface
# 13    leitch    ATOM           Leitch CSD 5300 Master Clock Controller
# 15    *         *              TrueTime GPS/TM-TMD Receiver
# 17    datum     DATM           Datum Precision Time System
```

```
# 18    acts      ACTS           NIST Automated Computer Time Service
# 19    heath     WWV            Heath WWV/WWVH Receiver
# 20    nmea      GPS            Generic NMEA GPS Receiver
# 22    atom      PPS            PPS Clock Discipline
# 23    ptb       TPTB           PTB Automated Computer Time Service
# 24    usno      USNO           USNO Modem Time Service
# 25    *         *              TrueTime generic receivers
# 26    hpgps     GPS            Hewlett Packard 58503A GPS Receiver
# 27    arc       MSFa           Arcron MSF Receiver
#
# * All TrueTime receivers are now supported by one driver, type 5.
#   Types 15 and 25 will be retained only for a limited time and may
#   be reassigned in future.
#
# Some of the devices benefit from "fudge" factors.  See the xntpd
# documentation.

# Either a peer or server.  Replace "XType" with a value from the
# table above.
server 127.127.XType.0
fudge 127.127.XType.0 stratum 0

broadcast 224.0.1.1 ttl 4

enable auth monitor
driftfile /var/ntp/ntp.drift
statsdir /var/ntp/ntpstats/
filegen peerstats file peerstats type day enable
filegen loopstats file loopstats type day enable
filegen clockstats file clockstats type day enable

keys /etc/inet/ntp.keys
trustedkey 0
requestkey 0
```

```
controlkey 0
```

Les directives actives de ce fichier sont :

```
# egrep -v '^(#|$)'  /etc/inet/ntp.conf > /tmp/ntp.conf
# cat /tmp/ntp.conf
server 127.127.XType.0
fudge 127.127.XType.0 stratum 0
broadcast 224.0.1.1 ttl 4
enable auth monitor
driftfile /var/ntp/ntp.drift
statsdir /var/ntp/ntpstats/
filegen peerstats file peerstats type day enable
filegen loopstats file loopstats type day enable
filegen clockstats file clockstats type day enable
keys /etc/inet/ntp.keys
trustedkey 0
requestkey 0
controlkey 0
```

Les directives suivantes stipulent que votre serveur doit se synchroniser sur l'horloge locale, une horloge fictive, utilisée lors de l'inaccessibilité des serveurs sur Internet :

```
server 127.127.XType.0
fudge 127.127.XType.0 stratum 0
```

La valeur de **XType** doit être prise du tableau fourni dans le fichier lui-même.

La directive suivante permet le broadcast au client :

```
broadcast 224.0.1.1 ttl 4
```

La fonction suivante active le monitoring et fait que le serveur se synchronise avec les clients seulement si ceux-ci se sont bien authentifiés en utilisant une clé d'authenfication valide.

```
enable auth monitor
```

La directive suivante identifie le fichier contenant la déviation moyenne:

```
driftfile /etc/ntp/drift
```

La directive suivante indique le répertoire qui stocke les clefs symétriques lors d'accès sécurisés éventuels :

```
keys /etc/inet/ntp.keys
trustedkey 0
requestkey 0
controlkey 0
```

La directive suivante indique le répertoire de statistiques :

```
statsdir /var/log/ntpstats/
```

La directive suivante indique les statistiques voulues :

```
statistics loopstats peerstats clockstats
```

Les directives suivantes indiquent les statistiques à générer :

```
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable
```

Ce fichier a besoin d'être modifié avant de démarrer le service ntp. Ajoutez donc la section suivante afin de stipuler quel serveur est utilisé pour la synchronisation. La liste peut aussi comporter des FQDN :

```
server 192.43.244.18
server 192.203.230.41
server 128.115.14.97
```

```
server 128.252.19.1
```

Modifiez ensuite les lignes suivantes :

```
server 127.127.XType.1
fudge 127.127.XType.1 stratum 0
```

Vous obtiendrez un fichier similaire à celui-ci :

```
# vi /tmp/ntp.conf
# cat /tmp/ntp.conf
server 192.43.244.18
server 192.203.230.41
server 128.115.14.97
server 128.252.19.1
server 127.127.XType.1
fudge 127.127.XType.1 stratum 0
broadcast 224.0.1.1 ttl 4
enable auth monitor
driftfile /var/ntp/ntp.drift
statsdir /var/ntp/ntpstats/
filegen peerstats file peerstats type day enable
filegen loopstats file loopstats type day enable
filegen clockstats file clockstats type day enable
keys /etc/inet/ntp.keys
trustedkey 0
requestkey 0
controlkey 0
```

Mettez en place le fichier /etc/inet/ntp.conf :

```
# cp /etc/inet/ntp.conf /Documents
# cp /tmp/ntp.conf /etc/inet/
```

Créez ensuite le fichier **/var/ntp/ntp.drift** :

```
# touch /var/ntp/ntp.drift
```

Démarrez ensuite le service network/ntp4 :

```
# svcadm clear svc:/network/ntp4:default
# svcadm enable svc:/network/ntp4:default
```

Constatez l'état du service :

```
# svcs -a | grep ntp
disabled       11:57:03 svc:/network/ntp:default
online         11:57:11 svc:/network/ntp4:default
# svcs -l svc:/network/ntp4:default
fmri         svc:/network/ntp4:default
name         Network Time Protocol (NTP) Version 4
enabled      true
state        online
next_state   none
state_time   Fri Jan 17 11:57:11 2020
logfile      /var/svc/log/network-ntp4:default.log
restarter    svc:/system/svc/restarter:default
contract_id  523
dependency   require_any/error svc:/network/service (online)
dependency   exclude_all/none svc:/network/ntp (disabled)
```

Dernièrement, constatez la présence des statistiques :

```
# cd /var/ntp/ntpstats
# ls
loopstats           loopstats.20200117  peerstats           peerstats.20200117
```

LAB #3 - Installation et Configuration du Serveur FTP

Introduction

Solaris 10 à un serveur FTP pré-installé. Ce serveur est basé sur le serveur **WU-FTPd** de l'Université de Washington.

installation

Vérifiez donc l'état du serveur FTP :

```
# svcs ftp
STATE          STIME    FMRI
online         14:26:56 svc:/network/ftp:default
```

Le serveur FTP est géré par inetd. Consultez donc sa configuration en utilisant la commande **inetadm** :

```
# inetadm -l svc:/network/ftp:default
SCOPE    NAME=VALUE
         name="ftp"
         endpoint_type="stream"
         proto="tcp6"
         isrpc=FALSE
         wait=FALSE
         exec="/usr/sbin/in.ftpd -a"
         user="root"
default  bind_addr=""
default  bind_fail_max=-1
default  bind_fail_interval=-1
default  max_con_rate=-1
default  max_copies=-1
default  con_rate_offline=-1
```

```
default  failrate_cnt=40
default  failrate_interval=60
default  inherit_env=TRUE
default  tcp_trace=FALSE
default  tcp_wrappers=TRUE
default  connection_backlog=10
```

Important - L'option **-a** passé à l'exécutable **in.ftpd** indique l'utilisation du fichier **/etc/ftpd/ftpaccess** pour la configuration du daemon.

Configuration de la Journalisation

Pour rendre la journalisation plus détaillé il faut passé la valeur de la directive **tcp_trace** à **true** :

```
# inetadm -m svc:/network/ftp:default tcp_trace=TRUE
# inetadm -l svc:/network/ftp
SCOPE    NAME=VALUE
         name="ftp"
         endpoint_type="stream"
         proto="tcp6"
         isrpc=FALSE
         wait=FALSE
         exec="/usr/sbin/in.ftpd -a"
         user="root"
default  bind_addr=""
default  bind_fail_max=-1
default  bind_fail_interval=-1
default  max_con_rate=-1
default  max_copies=-1
default  con_rate_offline=-1
```

```
default  failrate_cnt=40
default  failrate_interval=60
default  inherit_env=TRUE
         tcp_trace=TRUE
default  tcp_wrappers=TRUE
default  connection_backlog=10
```

Important - Notez la directive **tcp_trace=TRUE**.

Consulte maintenant le contenu du fichier **/etc/ftpd/ftpaccess** :

```
# cat /etc/ftpd/ftpaccess
# ident "@(#)ftpaccess  1.2     03/05/14 SMI"
#
# FTP server configuration file, see ftpaccess(4).
#

class           realusers       real            *
class           guestusers      guest           *
class           anonusers       anonymous       *

loginfails      3
passwd-check    trivial         warn
private         no
shutdown        /etc/ftpd/shutdown.msg
# email         user@hostname
# guestuser     username
# rhostlookup   no

keepalive       yes
recvbuf         65536           real,guest,anonymous
```

```
sendbuf         65536           real,guest,anonymous
# flush-wait    no              anonymous
# passive       ports           0.0.0.0/0       32768   65535
# timeout       data            600
# timeout       idle            300

banner          /etc/ftpd/banner.msg
greeting        brief
message         /etc/ftpd/welcome.msg   login
message         .message                cwd=*
readme          README*                 login
readme          README*                 cwd=*
# quota-info    *

chmod           no              anonymous
delete          no              anonymous
overwrite       no              anonymous
rename          no              anonymous
umask           no              anonymous

compress        yes             realusers guestusers anonusers
tar             yes             realusers guestusers anonusers

path-filter     guest,anonymous /etc/ftpd/filename.msg  ^[[:alnum:]._-]*$ ^[.-]

noretrieve      relative        class=anonusers         /
allow-retrieve  relative        class=anonusers         /pub

upload          class=anonusers    *    *         no  nodirs
# upload        class=anonusers    *    /incoming yes ftpadm ftpadm 0440 nodirs

# log           commands        real,guest,anonymous
# log           security        real,guest,anonymous
# log           transfers       real,guest,anonymous    inbound,outbound
```

```
# xferlog       format  %T %Xt %R %Xn %XP %Xy %Xf %Xd %Xm %U ftp %Xa %u %Xc %Xs %Xr

# limit-time    anonymous       30
# limit         anonusers       10      Wk0730-1800       /etc/ftpd/toomany.msg
# limit         anonusers       50      SaSu|Any1800-0730 /etc/ftpd/toomany.msg
```

Pour activer la journalisation il convient de décommenter les deux lignes suivantes :

```
# vi /etc/ftpd/ftpaccess
# cat /etc/ftpd/ftpaccess
...
log           transfers       real,guest,anonymous    inbound,outbound
xferlog       format  %T %Xt %R %Xn %XP %Xy %Xf %Xd %Xm %U ftp %Xa %u %Xc %Xs %Xr
...
```

Ajoutez maintenant les options **-l**, **-L**, **-X** et **-w** à la valeur de la directive **inetd_start/exec** :

```
# svccfg
svc:> select ftp
svc:/network/ftp> setprop inetd_start/exec="/usr/sbin/in.ftpd -a -l -L -X -w"
svc:/network/ftp> listprop
general                         framework
general/entity_stability        astring  Unstable
general/restarter               fmri     svc:/network/inetd:default
inetd                           framework
inetd/endpoint_type             astring  stream
inetd/isrpc                     boolean  false
inetd/name                      astring  ftp
inetd/proto                     astring  tcp6
inetd/stability                 astring  Evolving
inetd/wait                      boolean  false
inetd_start                     method
inetd_start/group               astring  root
inetd_start/limit_privileges    astring  :default
```

```
inetd_start/privileges          astring  :default
inetd_start/project             astring  :default
inetd_start/resource_pool       astring  :default
inetd_start/supp_groups         astring  :default
inetd_start/timeout_seconds     count    0
inetd_start/type                astring  method
inetd_start/use_profile         boolean  false
inetd_start/user                astring  root
inetd_start/working_directory   astring  :default
inetd_start/exec                astring  "/usr/sbin/in.ftpd -a -l -L -X -w"
inetd_disable                   method
inetd_disable/exec              astring  :kill
inetd_disable/timeout_seconds   count    0
inetd_disable/type              astring  method
tm_common_name                  template
tm_common_name/C                ustring  "FTP server"
tm_man_in_ftpd                  template
tm_man_in_ftpd/manpath          astring  /usr/share/man
tm_man_in_ftpd/section          astring  1M
tm_man_in_ftpd/title            astring  in.ftpd
tm_man_ftpd                     template
tm_man_ftpd/manpath             astring  /usr/share/man
tm_man_ftpd/section             astring  1M
tm_man_ftpd/title               astring  ftpd
svc:/network/ftp> exit
```

Important - L'option **-l** active la journalisation de chaque session FTP, l'option **-L** active la journalisation des commandes envoyées vers le serveur, l'option **-X** active la journalisation des accès aux fichiers et l'option **-w** active la journalisation des connections au serveur.

Le serveur FTP envoie des traces à syslog en utilisant le Sélecteur **daemon.info**. Modifiez donc le fichier **/etc/syslog** afin que syslog envoie les traces

dans le fichier **/var/adm/ftplog** :

```
# vi /etc/syslog
# cat /etc/syslog
...
*.err;kern.notice;auth.notice           /dev/sysmsg
*.err;kern.debug;daemon.notice;mail.crit    /var/adm/messages
daemon.info                                     /var/adm/ftplog
...
```

Créez le fichier **/var/adm/ftplog** et redémarrer les services **inetd**, **network/ftp** et **system-log** :

```
# touch /var/adm/ftplog
# svcadm restart inetd
# svcadm restart network/ftp
# svcadm restart system-log
```

Connectez-vous maintenant au serveur FTP en tant qu'user1 et tapez quelques commandes :

```
# ftp localhost
Connected to localhost.
220 solaris.i2tch.loc FTP server ready.
Name (localhost:root): user1
331 Password required for user1.
Password:
230 User user1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/export/home/user1" is current directory.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
local.cshrc
```

```
local.login
local.profile
226 Transfer complete.
41 bytes received in 0.0016 seconds (25.43 Kbytes/s)
ftp> quit
221-You have transferred 0 bytes in 0 files.
221-Total traffic for this session was 512 bytes in 1 transfers.
221-Thank you for using the FTP service on solaris.i2tch.loc.
221 Goodbye.
```

Connectez-vous maintenant au serveur FTP en tant qu'anonymous et tapez quelques commandes :

```
# ftp localhost
Connected to localhost.
220 solaris.i2tch.loc FTP server ready.
Name (localhost:root): anonymous
331 Guest login ok, send your complete e-mail address as password.
Password:
230-The response 'dfghj' is not valid
230-Next time please use your e-mail address as your password
230-   for example: joe@localhost.network
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/" is current directory.
ftp> !pwd
/
ftp> !touch test
ftp> !ls
Desktop     core.882    ftp         lost+found  proc        test
Documents   dev         home        mnt         pwd.txt     tmp
bin         devices     inetd.tftp  net         rep         usr
boot        etc         kernel      opt         sbin        var
```

```
core        export      lib         platform    system      vol
ftp> put test
200 PORT command successful.
553 test: Permission denied on server. (Upload)
ftp> quit
221-You have transferred 0 bytes in 1 files.
221-Total traffic for this session was 745 bytes in 1 transfers.
221-Thank you for using the FTP service on solaris.i2tch.loc.
221 Goodbye.
```

Consultez le fichier **/var/adm/ftplog** :

```
# cat /var/adm/ftplog
Jan 18 16:50:16 solaris.i2tch.loc inetd[1421]: [ID 317013 daemon.notice] ftp[1587] from 127.0.0.1 32826
Jan 18 16:59:38 solaris.i2tch.loc in.ftpd[1660]: [ID 927837 daemon.info] connect from localhost
Jan 18 16:59:38 solaris.i2tch.loc inetd[1421]: [ID 317013 daemon.notice] ftp[1660] from 127.0.0.1 32828
Jan 18 16:59:42 solaris.i2tch.loc ftpd[1660]: [ID 165209 daemon.info] USER user1
Jan 18 16:59:47 solaris.i2tch.loc ftpd[1660]: [ID 125383 daemon.info] PASS password
Jan 18 16:59:47 solaris.i2tch.loc ftpd[1660]: [ID 124999 daemon.info] FTP LOGIN FROM localhost [127.0.0.1], user1
Jan 18 16:59:47 solaris.i2tch.loc ftpd[1660]: [ID 470890 daemon.info] SYST
Jan 18 16:59:47 solaris.i2tch.loc ftpd[1660]: [ID 307055 daemon.info] TYPE Image
Jan 18 16:59:50 solaris.i2tch.loc ftpd[1660]: [ID 924372 daemon.info] PWD
Jan 18 16:59:52 solaris.i2tch.loc ftpd[1660]: [ID 313182 daemon.info] PORT
Jan 18 16:59:52 solaris.i2tch.loc ftpd[1660]: [ID 307055 daemon.info] TYPE ASCII
Jan 18 16:59:52 solaris.i2tch.loc ftpd[1660]: [ID 188419 daemon.info] NLST
Jan 18 16:59:52 solaris.i2tch.loc ftpd[1660]: [ID 307055 daemon.info] TYPE Image
Jan 18 16:59:55 solaris.i2tch.loc ftpd[1660]: [ID 225560 daemon.info] QUIT
Jan 18 16:59:55 solaris.i2tch.loc ftpd[1660]: [ID 528697 daemon.info] FTP session closed
Jan 18 17:00:01 solaris.i2tch.loc in.ftpd[1664]: [ID 927837 daemon.info] connect from localhost
Jan 18 17:00:01 solaris.i2tch.loc inetd[1421]: [ID 317013 daemon.notice] ftp[1664] from 127.0.0.1 32830
Jan 18 17:00:04 solaris.i2tch.loc ftpd[1664]: [ID 165209 daemon.info] USER anonymous
Jan 18 17:00:06 solaris.i2tch.loc ftpd[1664]: [ID 351301 daemon.info] PASS dfghj
Jan 18 17:00:06 solaris.i2tch.loc ftpd[1664]: [ID 210975 daemon.info] ANONYMOUS FTP LOGIN FROM localhost
[127.0.0.1], dfghj
```

```
Jan 18 17:00:06 solaris.i2tch.loc ftpd[1664]: [ID 470890 daemon.info] SYST
Jan 18 17:00:06 solaris.i2tch.loc ftpd[1664]: [ID 307055 daemon.info] TYPE Image
Jan 18 17:00:08 solaris.i2tch.loc ftpd[1664]: [ID 924372 daemon.info] PWD
Jan 18 17:00:43 solaris.i2tch.loc ftpd[1664]: [ID 313182 daemon.info] PORT
Jan 18 17:00:43 solaris.i2tch.loc ftpd[1664]: [ID 206289 daemon.info] STOR test
Jan 18 17:00:59 solaris.i2tch.loc ftpd[1664]: [ID 225560 daemon.info] QUIT
Jan 18 17:00:59 solaris.i2tch.loc ftpd[1664]: [ID 528697 daemon.info] FTP session closed
```

Configuration des Connexions Anonymes

Solaris 10 contient un script dénommé **ftpconfig** qui permet de configurer automatiquement un chroot pour les connexions anonymes :

```
# ftpconfig /export/home/ftp_pub
Updating user ftp
Creating directory /export/home/ftp_pub
Updating directory /export/home/ftp_pub
```

Consultez le contenu du répertoire **/export/home/ftp_pub** :

```
# ls -l /export/home/ftp_pub
total 12
lrwxrwxrwx   1 root     bin            9 Jan 18 16:06 bin -> ./usr/bin
d--x--x--x   2 root     sys          512 Jan 18 16:06 dev
d--x--x--x   5 root     sys          512 Jan 18 16:06 etc
d--x--x--x   2 root     bin          512 Jan 18 16:06 lib
drwxr-xr-x   2 root     sys          512 Jan 18 16:06 pub
d--x--x--x   6 root     sys          512 Jan 18 16:06 usr
```

Pour activer le téléversement vers le répertoire **/export/home/ftp_pub/pub**, modifiez le fichier **/etc/ftpd/ftpaccess** :

```
# vi /etc/ftpd/ftpaccess
# cat /etc/ftpd/ftpaccess
```

```
...
upload          class=anonusers    *    /pub    yes
# upload                class=anonusers    *    *         no  nodirs
# upload        class=anonusers    *    /incoming yes ftpadm ftpadm 0440 nodirs
...
```

Modifiez le masque de permissions à 777 sur le répertoire **/export/home/ftp_pub/pub** :

```
# chmod 777 /export/home/ftp_pub/pub
```

Postionnez-vous dans le répertoire **/tmp** et créez le fichier **ftptest** :

```
# cd /tmp
# touch ftptest
# ls
ftptest              hsperfdata_noaccess  hsperfdata_root
```

Connectez-vous au serveur FTP en tant que l'utilisateur **anonymous** et téléversez le fichier **ftptest** :

```
# ftp localhost
Connected to localhost.
220 solaris.i2tch.loc FTP server ready.
Name (localhost:root): anonymous
331 Guest login ok, send your complete e-mail address as password.
Password:
230-The response 'sgsdgdg' is not valid
230-Next time please use your e-mail address as your password
230-   for example: joe@localhost.network
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
```

```
bin
dev
etc
lib
pub
usr
226 Transfer complete.
30 bytes received in 0.00016 seconds (180.11 Kbytes/s)
ftp> cd /pub
250 CWD command successful.
ftp> !ls
ftptest              hsperfdata_noaccess  hsperfdata_root
ftp> put ftptest
200 PORT command successful.
150 Opening BINARY mode data connection for ftptest.
226 Transfer complete.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
ftptest
226 Transfer complete.
9 bytes received in 0.00012 seconds (71.52 Kbytes/s)
```

Sécurisation du Serveur FTP

Afin de sécuriser le serveur FTP, insérez les noms de tous les comptes système dans le fichier **/etc/ftpd/ftpusers**. Tout compte qui figure dans ce fichier ne peut pas se connecter au serveur FTP :

```
# cat /etc/ftpd/ftpusers
# ident "@(#)ftpusers    1.6    11/08/02 SMI"
#
# List of users denied access to the FTP server, see ftpusers(4).
#
```

```
root
daemon
bin
sys
adm
lp
uucp
nuucp
smmsp
listen
gdm
webservd
unknown
nobody
noaccess
nobody4
```

LAB #4 - Installation et Configuration du Serveur DHCP

Introduction

Un serveur DHCP (**Dynamic Host Configuration Protocol**) est un ordinateur exécutant un logiciel serveur DHCP. L’avantage de la présence d’un serveur DHCP sur le réseau local est que celui-ci permet de spécifier à un niveau central les paramètres TCP/IP.

Installation

Sous **Solaris** le serveur DHCP est installé par défaut mais il n'est pas activé :

```
# svcs -a | grep dhcp
disabled       14:26:46 svc:/network/dhcp-server:default
```

Il convient donc de l'activer grâce à la commande **svcadm** :

```
# svcadm enable svc:/network/dhcp-server:default
# svcs -a | grep dhcp
offline        17:10:08 svc:/network/dhcp-server:default
```

Notez que le statut du service passe de ***disabled** à **offline**. Commençons par cannaître la raison de ce statut :

```
# svcs -l svc:/network/dhcp-server:default
fmri         svc:/network/dhcp-server:default
name         DHCP server
enabled      true
state        offline
next_state   none
state_time   Sat Jan 18 17:10:08 2020
restarter    svc:/system/svc/restarter:default
dependency   require_all/refresh svc:/milestone/multi-user (online)
dependency   require_all/restart file:///etc/inet/dhcpsvc.conf (absent)
```

Important - La sortie nous informe que la raison du statut **offline** est l'abscence du fichier de configuration **/etc/inet/dhcpsvc.conf**.

Configuration

Création du Fichier /etc/inet/dhcpsvc.conf

Pour créer le fichier **/etc/inet/dhcpsvc.conf**, utilisez la commande **/usr/sbin/dhcpconfig**. L'ption **-D** indique que l'on configure le serveur en écrasant des valeurs des options utilisées. L'option **-r** spécifie le **back-end store**, dans notre cas des fichiers, et l'option **-p** indique l'emplacement de ces fichiers :

```
# /usr/sbin/dhcpconfig -D -r SUNWfiles -p /var/dhcp
Created DHCP configuration file.
Created dhcptab.
Added "Locale" macro to dhcptab.
Added server macro to dhcptab - solaris.
DHCP server started.
```

Consultez le contenu du fichier **/etc/inet/dhcpsvc.conf** :

```
# cat /etc/inet/dhcpsvc.conf
DAEMON_ENABLED=TRUE
RESOURCE=SUNWfiles
RUN_MODE=server
PATH=/var/dhcp
CONVER=1
```

Il est possible d'ajouter des variables manuellement à ce fichier. Dans notre cas, indiquez l'interface réseau qui sera à l'écoute des reqûetes DHCP :

```
# vi /etc/inet/dhcpsvc.conf
# cat /etc/inet/dhcpsvc.conf
DAEMON_ENABLED=TRUE
RESOURCE=SUNWfiles
RUN_MODE=server
PATH=/var/dhcp
CONVER=1
INTERFACES=e1000g0
```

Création de la Table de Réseau

Configurez maintenant une table réseau pour le serveur DHCP en utilisant l'option **-N** ainsi que le routeur par défaut grâce à l'option **-t** :

```
# /usr/sbin/dhcpconfig -N 10.0.2.0 -t 10.0.2.2
```

```
Added network macro to dhcptab - 10.0.2.0.
Created network table.
```

Listez les tables réseau du serveur DHCP :

```
# pntadm -L
10.0.2.0
```

La table réseau prend la forme d'un fichier nommé **SUNWfiles1_10_0_2_0** dans le répertoire **/var/dhcp** :

```
# ls /var/dhcp | grep 10
SUNWfiles1_10_0_2_0
# cat /var/dhcp/SUNWfiles1_10_0_2_0
# SUNWfiles1_10_0_2_0
#
# Do NOT edit this file by hand -- use pntadm(1M) or dhcpmgr(1M) instead
#
#
```

Important - Notez que la table est actuelleemnt vide.

Consultez les informations concernant la table réseau :

```
# dhtadm -P
Name                    Type        Value
====================================================
10.0.2.0                Macro       :Subnet=255.255.255.0:Router=10.0.2.2:Broadcst=10.0.2.255:
solaris                 Macro
:Include=Locale:Timeserv=10.0.2.15:LeaseTim=86400:LeaseNeg:DNSdmain="i2tch.loc":DNSserv=10.0.2.3:
Locale                  Macro       :UTCoffst=3600:
```

Ajoutez une entrée à la table **10.0.2.0** de la machine **solaris** en utilisant l'option **-A** :

```
# pntadm -A 10.0.2.50 -m solaris 10.0.2.0
# pntadm -P 10.0.2.50
Client ID   Flags    Client IP    Server IP    Lease Expiration             Macro       Comment

00          00      10.0.2.50    10.0.2.15    Zero                         solaris
```

Consultez le contenu du fichier **/var/dhcp/SUNWfiles1_10_0_2_0** :

```
# cat /var/dhcp/SUNWfiles1_10_0_2_0
# SUNWfiles1_10_0_2_0
#
# Do NOT edit this file by hand -- use pntadm(1M) or dhcpmgr(1M) instead
#
10.0.2.50|00|00|10.0.2.15|0|4338936765994762241|solaris|
```

Ajoutez neuf autres entrées :

```
# pntadm -A 10.0.2.51 -m solaris 10.0.2.0
# pntadm -A 10.0.2.52 -m solaris 10.0.2.0
# pntadm -A 10.0.2.53 -m solaris 10.0.2.0
# pntadm -A 10.0.2.54 -m solaris 10.0.2.0
# pntadm -A 10.0.2.55 -m solaris 10.0.2.0
# pntadm -A 10.0.2.56 -m solaris 10.0.2.0
# pntadm -A 10.0.2.57 -m solaris 10.0.2.0
# pntadm -A 10.0.2.58 -m solaris 10.0.2.0
# pntadm -A 10.0.2.59 -m solaris 10.0.2.0
```

Vérifez maintenant le contenu du fichier **/var/dhcp/SUNWfiles1_10_0_2_0** :

```
# cat /var/dhcp/SUNWfiles1_10_0_2_0
# SUNWfiles1_10_0_2_0
#
```

```
# Do NOT edit this file by hand -- use pntadm(1M) or dhcpmgr(1M) instead
#
10.0.2.50|00|00|10.0.2.15|0|2945917106253725697|solaris|
10.0.2.51|00|00|10.0.2.15|0|5726608401178296321|solaris|
10.0.2.52|00|00|10.0.2.15|0|92886742314516481|solaris|
10.0.2.53|00|00|10.0.2.15|0|251075679225905153|solaris|
10.0.2.54|00|00|10.0.2.15|0|14762799578520485889|solaris|
10.0.2.55|00|00|10.0.2.15|0|14206886499516940289|solaris|
10.0.2.56|00|00|10.0.2.15|0|18410996751667298305|solaris|
10.0.2.57|00|00|10.0.2.15|0|6406933419887951873|solaris|
10.0.2.58|00|00|10.0.2.15|0|12357877377504641025|solaris|
10.0.2.59|00|00|10.0.2.15|0|12228117413241028609|solaris|
```

<html> Copyright © 2020 Hugh Norris. </html>