



Dynamic DNS sur Debian 8

>>> Debian 8, Bind9, Dhcp3-server

Description :

Le but de ce cours est de mettre en place un serveur DDNS. Ce dernier est un serveur DNS qui ajoute automatiquement dans sa base, les noms de machines qui ont obtenu une adresse IP par le DHCP.

> Article mis à jour le 17/01/2018

Dynamic DNS sur Debian 8

>>> Debian 8, Bind9, Dhcp3-server

Sommaire :

- I) Informations
 - II) Installations et configurations des serveurs
 - 1) Installation et configuration du serveur DHCP
 - 2) Installation et configuration du serveur DNS
 - 3) Tests de fonctionnements
 - III) Mise en place du DDNS
 - 1) Configuration du serveur DNS
 - 2) Configuration du serveur DHCP
 - 3) Tests de fonctionnements
 - 4) Générations des clefs
-

I) Informations

Serveur DNS :

- Nom de machine : dns.toto.com
- Adresse IP : 172.16.1.1

Serveur DHCP :

- Nom de machine : dhcp.toto.com
- Adresse IP : 172.16.1.2

Adresse IP de la passerelle : 172.16.1.254

II) Installations et configurations des serveurs

1) Installation et configuration du serveur DHCP

Un serveur DHCP est un serveur qui attribue une configuration IP (adresse IP, masque, passerelle, serveur de noms) aux ordinateurs configurés en adressage dynamique. Avec un serveur DHCP, l'utilisateur n'a plus besoin d'entrer les informations lui-même, le serveur s'en charge.

- Pour installer un serveur DHCP, suivez cette procédure :

```
aptitude install dhcp3-server
```

Pour le configurer, seul le fichier « dhcpd.conf » doit être modifié :

```
vim /etc/dhcp3/dhcpd.conf
```

Nous commencerons par désactiver les lignes qui doivent l'être (pour désactiver appliquez un # devant la

ligne, c'est ce que l'on appelle commenter une ligne) :

```
# option domain-name "example.org";  
# option domain-name-server ns1.example.org, ns2.example.org;  
  
# default-lease-time 600 ;  
# max-lease-time 7200;
```

Si vous voulez que votre serveur DHCP soit le serveur DHCP principal du réseau dé-commentez la ligne (supprimez le #) :

```
authoritative ;
```

Maintenant nous allons configurer les paramètres de la configuration IP que le serveur fournira au client. Rendez vous à la ligne 50 où vous devriez voir les lignes qui suivent. Dé-commentez les lignes et renseignez les champs pour :

```
Subnet 172.16.1.0 netmask 255.255.255.0 {  
range 172.16.1.100 172.16.1.150;  
option domain-name-server dns.toto.com ;  
option domain-name "toto.com" ;  
option routers 172.16.1.254 ;  
option broadcast-address 172.16.1.255 ;  
default-lease-time 600 ;  
max-lease-time 7200;
```

Pour vous aider à configurer nous allons détailler les différents termes :

- **Subnet** : Correspond au réseau où se trouve votre serveur (Ex : 172.16.1.0).
- **Netmask** : Correspond au masque du réseau où se trouve votre serveur. (Ex : 255.255.255.0).
- **Range** : Correspond aux adresses IP que votre serveur attribuera au client (Ex : 172.16.1.100 à 172.16.1.150).
- **Option domain-name-server** : Ici vous devez donner soit l'adresse IP de votre serveur DNS ou son nom complet.
- **Option domain-name** : Ici vous devez donner le nom de domaine.
- **Option routers** : Correspond à l'adresse IP de votre routeur.
- **Option broadcast-address** : Correspond au broadcast du réseau (Ex : 172.16.1.255).
- **default-lease-time** : correspond à la durée par défaut du bail de la configuration donnée en seconde (ex : 86400).
- **max-lease-time** : correspond à la durée maximale du bail de la configuration donnée en seconde (ex : 172800).

Pour finir on redémarre le serveur DHCP :

```
/etc/init.d/isc-dhcp-server restart
```

2) Installation et configuration du serveur DNS

Il n'est guère facile de faire retenir une adresse du style : 213.251.175.34/ nom_de_mon_site à des visiteurs. Si vous y arrivez, vous êtes un champion. C'est donc le travail de Bind9 de traduire notre nom de domaine. Il vous suffira de définir votre nom de serveur chez votre registrar. (On prendra pour exemple toto.com comme domaine, (DNS comme nom de machine et 172.16.1.1 (masque 255.255.255.0) comme configuration IP)

```
aptitude install bind9
```

Nous commencerons par faire une copie des 2 fichiers que l'on modifiera par la suite pour éviter de les retaper :

```
cp /etc/bind/db.255 /var/cache/bind/db.toto.inv  
cp /etc/bind/db.local /var/cache/bind/db.toto
```

Nous allons maintenant éditer db.toto (**faire très attention à la ponctuation**) :

```
vim /var/cache/bind/db.toto
```

```
; BIND data file for toto.com zone  
@ IN SOA SRV.toto.com. root.toto.com. (  
@ IN NS SRV.toto.com.  
dns IN A 172.16.1.1  
dhcp IN A 172.16.1.2
```

Nous allons maintenant éditer db.toto.inv (faire très attention à la ponctuation) :

```
vim /var/cache/bind/db.toto.inv
```

- Modifiez le fichier :

```
; BIND reverse data file for toto.com zone  
@ IN SOA SRV.toto.com. root.toto.com. (  
@ IN NS SRV.toto.com.  
1 IN PTR dns.toto.com.  
2 IN PTR dhcp.toto.com
```

Dans la ligne :**2 IN PTR SRV**

- Le "2" correspond au 172.16.1.2

Nous allons maintenant modifier le fichier « named.conf.local »

```
vim /etc/bind/named.conf.local
```

- Modifiez le fichier :

```
include "/etc/bind/zones.rfc1918";  
  
zone "toto.com"{  
type master;  
file "/var/cache/bind/db.toto";  
};  
  
zone "1.16.172.in-addr.arpa"{  
type master;  
file "/var/cache/bind/db.toto.inv";  
};
```

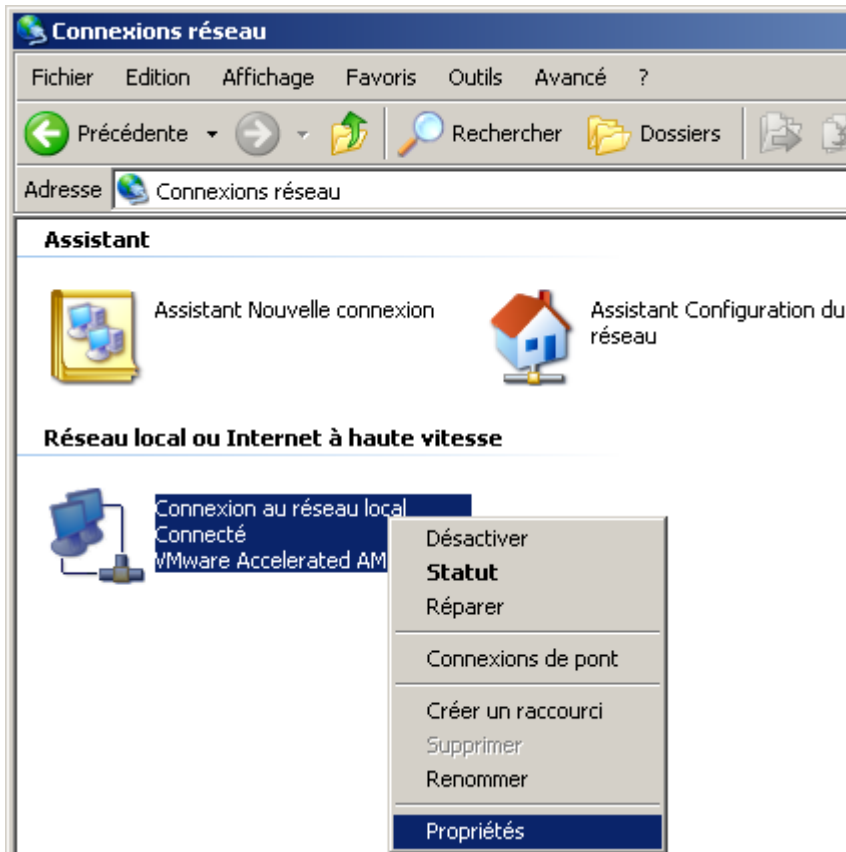
Pour finir on redémarre le serveur DNS :

```
/etc/init.d/bind9 restart
```

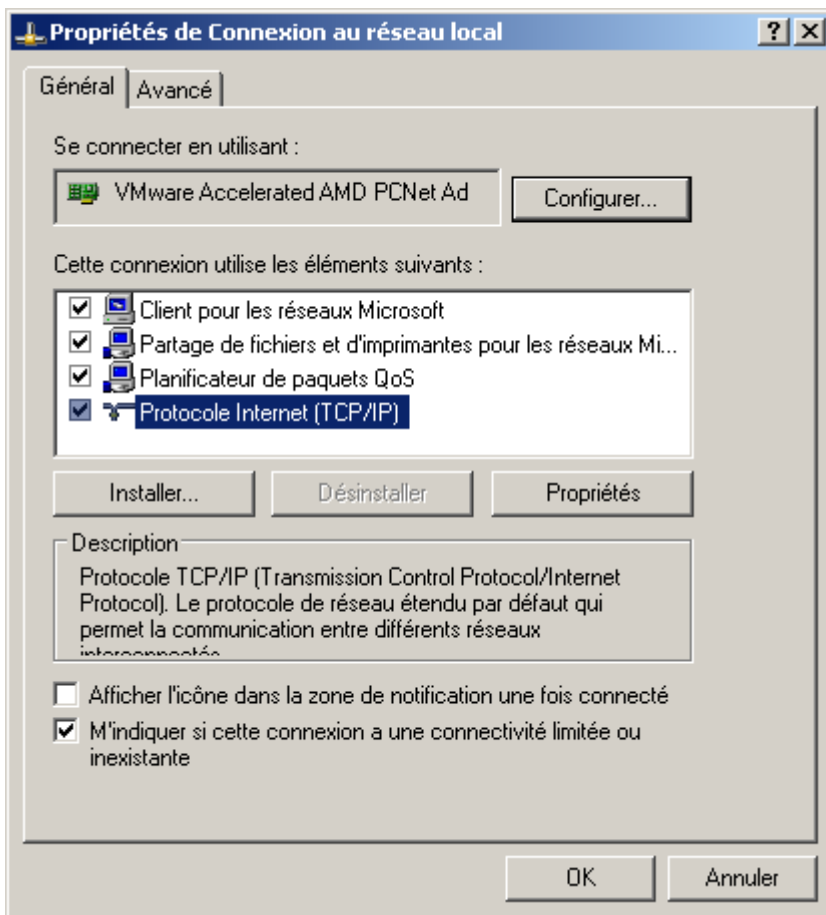
Voilà n'oubliez pas de configurer dans votre configuration réseau, l'adresse de votre serveur en tant que serveur de noms (serveur DNS).

3) Tests de fonctionnements

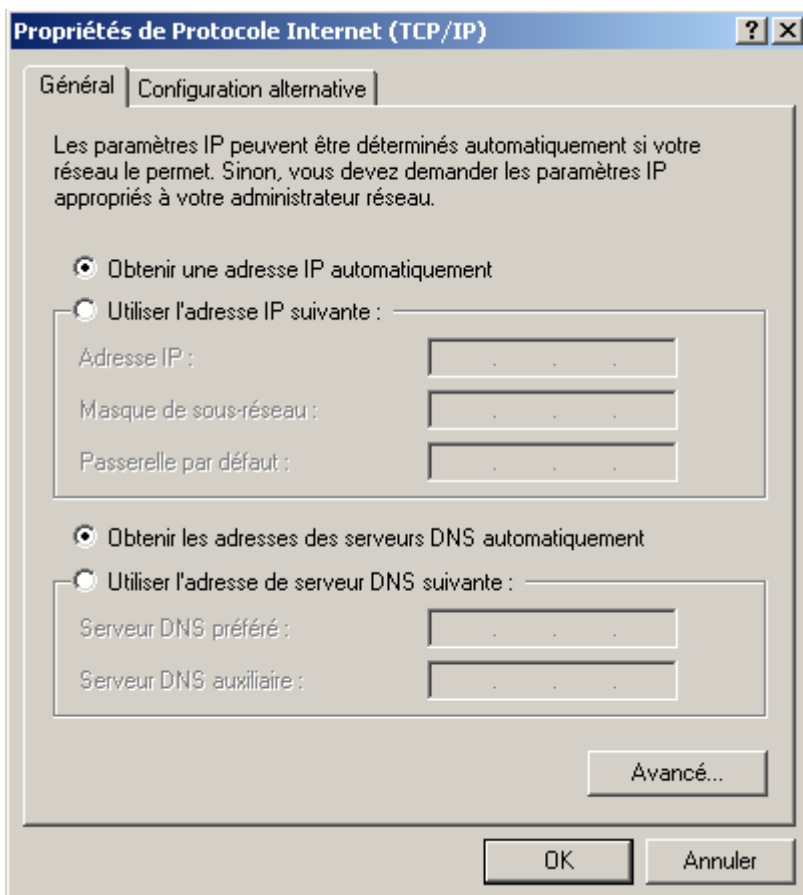
Pour tester le DHCP, nous commençons par ouvrir le "Panneau de configuration", puis "Connexions réseau". On fait un clic droit sur l'interface réseau, "Propriétés" :



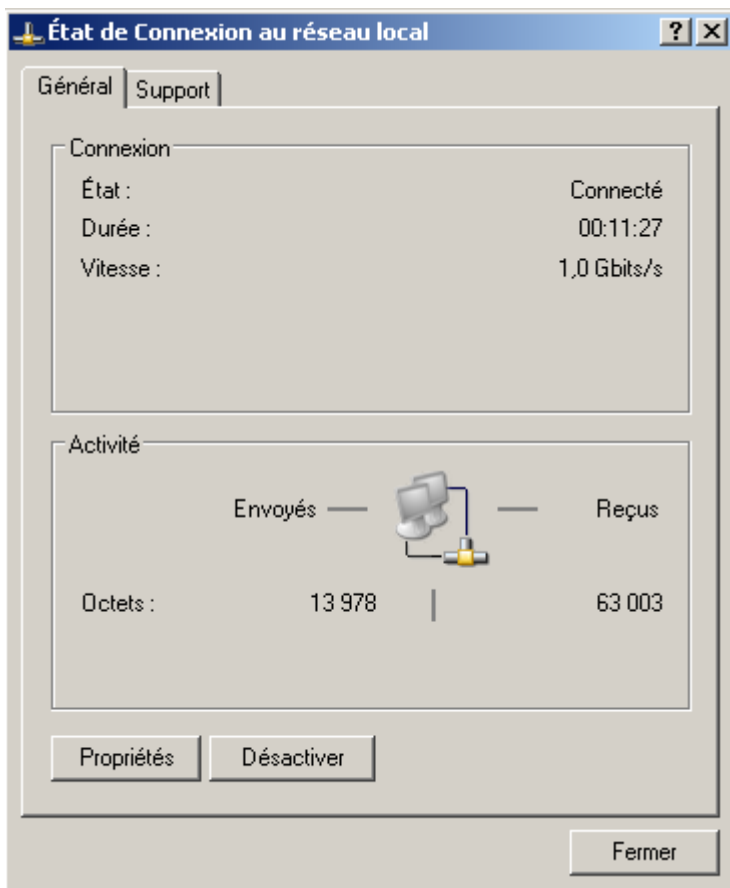
On sélectionne "Protocole Internet (TCP/IP)" et on clique sur "Propriétés" :



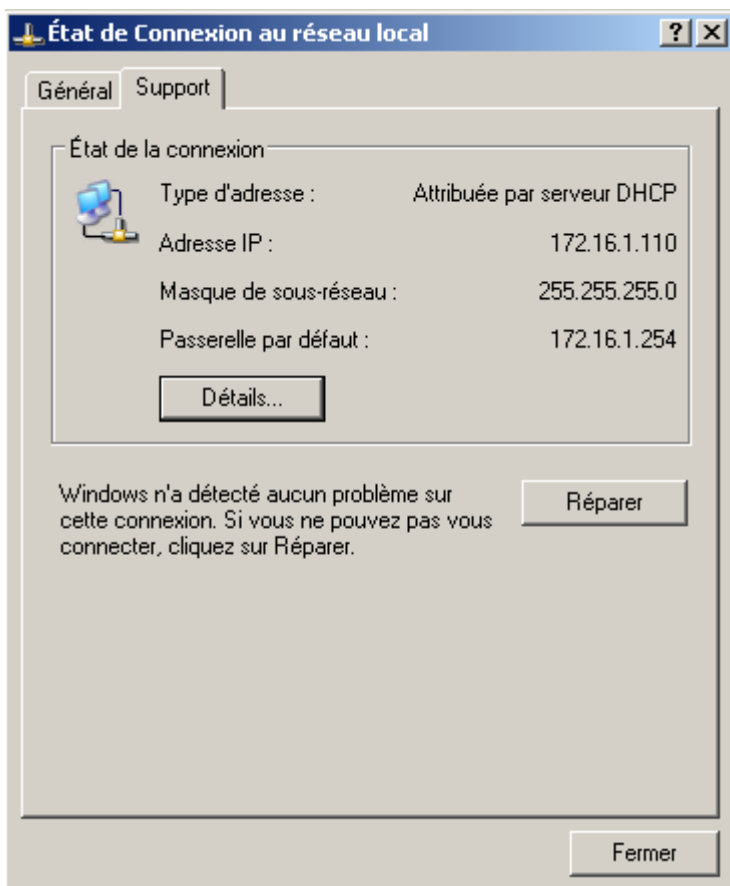
Ensuite nous cochons "Obtenir une adresse IP automatiquement" et "Obtenir les adresses des serveurs DNS automatiquement", puis on clique sur "OK" :



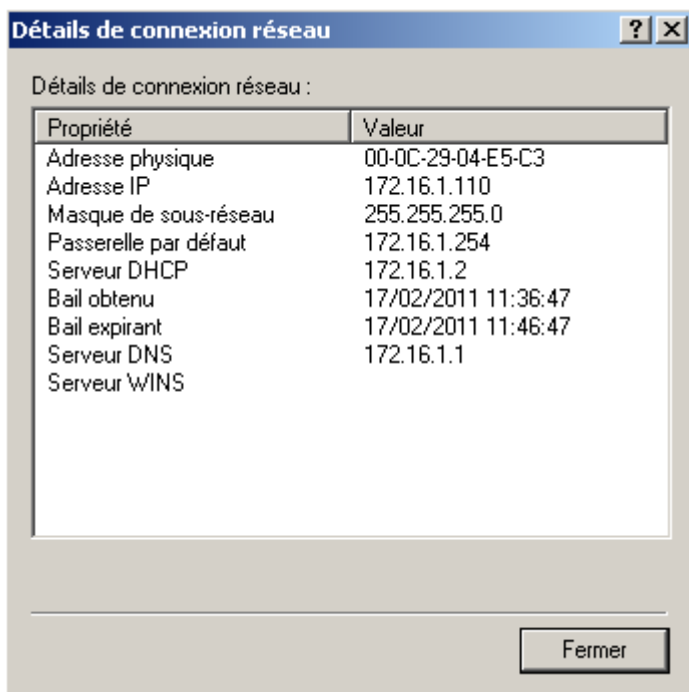
On retourne dans "Connexions réseau" et on double clic sur l'interface réseau.



Cliquez sur l'onglet "Support" :



Puis cliquez sur "Détails" :



Vérifier ensuite que les informations fournies sont bien les informations fournies par votre DHCP.

Testons maintenant le serveur DNS :

Ouvrez l'invite de commande MS-DOS, et tapez "nslookup nom de machine.domaine.TLD"

Regarder le résultat :

```
C:\Documents and Settings\Administrateur>nslookup dns.toto.com
Serveur : dns.toto.com
Address: 172.16.1.1

Nom : dns.toto.com
Address: 172.16.1.1

C:\Documents and Settings\Administrateur>_
```

Nslookup envoie une demande de résolution du nom de machine.domaine.TLD au serveur DNS. Le serveur DNS regarde sa base de correspondance et répond à la requête en renvoyant l'adresse IP associée au nom de machine.domaine.TLD.

III) Mise en place du DDNS

Lors de l'installation de Bind9, celui-ci génère automatiquement une clef rndc-key que l'on peut observer dans le fichier "rndc.key". Nous allons utiliser cette clef pour sécuriser la connexion entre le serveur DNS et le serveur DHCP.

1) Configuration du serveur DNS

Nous commençons par ouvrir le fichier "rndc.key" :

```
vim /etc/bind/rndc.key
```

La clef se présente de cette manière la :

```
key "rndc-key" {
    algorithm hmac-md5;
```



```
secret "yF1eFUcsV7P1M8d+GxGb5g==" ;
};
```

- Copiez la clef dans un fichier texte, elle nous servira dans quelques minutes pour la configuration du serveur DHCP.

- Ouvrez le fichier "named.conf" :

```
vim /etc/bind/named.conf
```

- Et rajoutez la ligne suivante à la fin du fichier :

```
include "/etc/bind/rndc.key";
```

Ensuite nous allons éditez le fichier "named.conf.local" qui déclare les zones gérées par le DNS.

- Ouvrez le fichier "named.conf.local"

```
vim /etc/bind/named.conf.local
```

- Ajoutez la ligne suivante dans la déclaration des zones :

```
allow-update {key "rndc-key";};
```

Vous devriez obtenir quelques choses qui ressemblent à ça :

```
zone "toto.com"{
type master;
file "/var/cache/bind/db.toto";
allow-update {key "rndc-key";};
};

zone "1.168.192.in-addr.arpa"{
type master;
file "/var/cache/bind/db.toto.inv";
allow-update {key "rndc-key";};
};
```

Attention : Respectez l'emplacement des points-virgules "-key";};"

Pour finir, on redémarre le service DNS :

```
/etc/init.d/bind9 restart
```

2) Configuration du serveur DHCP

Nous allons commencer par créer un fichier "rndc.key" dans le dossier "/etc/dhcp" :

```
vim /etc/dhcp/rndc.key
```

- Coller dans ce fichier la clef que vous avez copiée précédemment.

Ensuite éditez le fichier "dhcpd.conf" :

```
vim /etc/dhcp/dhcpd.conf
```

Dans ce fichier nous allons ajouter les deux lignes ci-dessous, qui permettront d'activer le DDNS.

```
#ddns-update-style none;  
ddns-updates on;  
ddns-update-style interim;
```

Nous déclarons maintenant la clef rndc.key dans la zone, pour cela nous allons ajouter les lignes suivantes dans la config du "subnet" :

- Dans l'exemple sci-dessous, "**dns.toto.com**" correspond au nom du serveur et non au nom du fichier.

```
include "/etc/dhcp/rndc.key";  
  
zone toto.com.{  
primary dns.toto.com;  
key rndc-key;  
}  
  
zone 1.16.172.in-addr.arpa. {  
primary dns.toto.com;  
key rndc-key;  
}
```

Pour avoir une vue d'ensemble voici ma configuration présente dans le fichier "dhcpd.conf" :

```
# A slightly different configuration for an internal subnet.  
subnet 172.16.1.0 netmask 255.255.255.0 {  
range 172.16.1.100 172.16.1.150;  
option domain-name-servers dns.toto.com;  
option domain-name "toto.com";  
option routers 172.16.1.254;  
option broadcast-address 172.16.1.255;  
default-lease-time 600;  
max-lease-time 7200;  
  
include "/etc/dhcp/rndc.key";  
  
zone toto.com.{  
primary dns.toto.com;  
key rndc-key;  
}  
  
zone 1.16.172.in-addr.arpa. {  
primary dns.toto.com;  
key rndc-key;  
}  
}
```

Attention à la ponctuation !!

Pour finir on redémarre le service DHCP.

```
services isc-dhcp-server restart
```

3) Tests de fonctionnements

Pour vérifier le bon fonctionnement de notre configuration, Nous allons connecter la station de travail "Client2" sur notre réseau. La station "Client2" est configurée pour obtenir une adresse IP automatique.

Si notre configuration fonctionne, le nom de cette machine "Client2" sera ajouté au serveur DNS.

Nous effectuons un nslookup qui va réaliser une requête auprès du serveur pour que celui-ci nous retourne l'adresse IP de cette station.

4) Générations des clefs

Si vous souhaitez générer une autre clef ou une deuxième clef, tapez cette commande :

```
root@dns:/etc/bind# dnssec-keygen -a HMAC-MD5 -b 128 -n USER rndc2
```

Lorsque la clef sera générée, vous devriez obtenir une ligne équivalente à :

```
Krndc2.+157+48777
```

De plus la commande devrait vous créer deux fichiers :

```
Krndc2.+157+48777.private
```

et

```
Krndc2.+157+48777.key
```

Le fichier ".private" est l'équivalent du fichier "rndc.key" existant. A vous d'adapter ensuite.

5 février 2018 -- N.Salmon -- article_196.pdf



Idum