

RF-232

Micronator

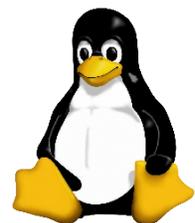
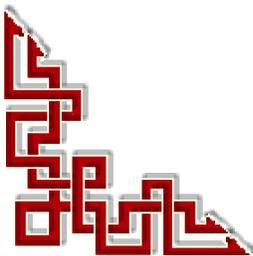
NethServer-201

Cahier-11

NethServer & diaspora*



diaspora*



© 2020 RF-232
6447, avenue Jalobert, Montréal Qc H1M 1L1

Tous droits réservés RF-232

AVIS DE NON-RESPONSABILITÉ

Ce document est uniquement destiné à informer. Les informations, ainsi que les contenus et fonctionnalités de ce document sont fournis sans engagement et peuvent être modifiés à tout moment. **RF-232** n'offre aucune garantie quant à l'actualité, la conformité, l'exhaustivité, la qualité et la durabilité des informations, contenus et fonctionnalités de ce document. L'accès et l'utilisation de ce document se font sous la seule responsabilité du lecteur ou de l'utilisateur.

RF-232 ne peut être tenu pour responsable de dommages de quelque nature que ce soit, y compris des dommages directs ou indirects, ainsi que des dommages consécutifs résultant de l'accès ou de l'utilisation de ce document ou de son contenu.

Chaque internaute doit prendre toutes les mesures appropriées (*mettre à jour régulièrement son logiciel antivirus, ne pas ouvrir des documents suspects de source douteuse ou non connue*) de façon à protéger le contenu de son ordinateur de la contamination d'éventuels virus circulant sur la Toile.

Toute reproduction interdite

Vous reconnaissez et acceptez que tout le contenu de ce document, incluant mais sans s'y limiter, le texte et les images, sont protégés par le droit d'auteur, les marques de commerce, les marques de service, les brevets, les secrets industriels et les autres droits de propriété intellectuelle. Sauf autorisation expresse de **RF-232**, vous acceptez de ne pas vendre, délivrer une licence, louer, modifier, distribuer, copier, reproduire, transmettre, afficher publiquement, exécuter en public, publier, adapter, éditer ou créer d'oeuvres dérivées de ce document et de son contenu.

Avertissement

Bien que nous utilisons ici un vocabulaire issu des techniques informatiques, nous ne prétendons nullement à la précision technique de tous nos propos dans ce domaine.

En un clin-d'oeil

I-	Description générale.....	6
II-	À savoir.....	10
III-	Préparation de l'environnement de travail.....	11
IV-	Réseau LOCAL sans Serveur DNS.....	22
V-	Certificat Let's Encrypt.....	28
VI-	Prérequis.....	34
VII-	Installation.....	51
VIII-	diaspora*.....	59
IX-	Appendices.....	66
X-	Introduction à l'éditeur vi.....	80
XI-	Micronator.org.....	82

Sommaire

I-	Description générale.....	6
	1. Introduction.....	6
	2. diaspora*.....	6
	3. La Fédération.....	7
	4. diaspora*: Le guide du parfait débutant.....	7
	5. But de ce cahier.....	8
	6. Marche à suivre.....	8
	7. Conventions de ce document.....	9
II-	À savoir.....	10
	1. Serveur NethServer.....	10
	2. Poste de travail.....	10
	3. Éditeur de texte.....	10
III-	Préparation de l'environnement de travail.....	11
	1. Configuration du poste de travail.....	11
	2. Fichier hosts du poste de travail.....	11
	3. Installation d'un Serveur NethServer.....	11
	4. Vérification: interface Web NethServer.....	12
	5. Ouverture d'une session PuTTY.....	18
	6. Utilisateurs.....	20
	7. Instantané VirtualBox.....	21
IV-	Réseau LOCAL sans Serveur DNS.....	22
	1. Description.....	22
	2. Difficultés pour un réseau LOCAL sans serveur DNS.....	22
	3. Modification de la passerelle du réseau LOCAL.....	22
	4. Vérification des redirections par la passerelle.....	24
	5. Nom de notre domaine de développement sur la liste blanche.....	24
	6. Sauvegarde des configurations.....	27
	7. Instantané VirtualBox.....	27
V-	Certificat Let's Encrypt.....	28
	1. Description.....	28
	2. Ajout des CNAME pour diaspora*.....	28
	3. Script acme.sh.....	30
	4. Demande d'un certificat de test.....	31
	5. Demande d'un certificat officiel.....	32
	6. Vérification.....	32
	7. Vérification de la connexion sécurisée.....	33
	8. Sauvegarde.....	33
	9. Instantané VirtualBox.....	33
VI-	Prérequis.....	34
	1. Paquets.....	34

2.	Activation de Redis.....	34
3.	PostgreSQL-12.....	35
4.	Redirection par Apache.....	45
5.	Instantané VirtualBox.....	46
6.	Utilitaire sudo.....	46
7.	RVM.....	47
8.	Ruby.....	49
9.	Instantané VirtualBox.....	50
VII-	Installation.....	51
1.	Utilisateur LINUX diaspora.....	51
2.	Téléchargement de la source.....	51
3.	Fichiers de configuration.....	52
4.	Bundler.....	54
5.	Configuration des nouveaux services.....	56
6.	Instantané VirtualBox.....	58
VIII-	diaspora*.....	59
1.	Accès à diaspora*.....	59
2.	Création d'un administrateur.....	59
3.	Réamorçage.....	62
4.	Vérification.....	63
5.	Vérification de la configuration d'Apache.....	64
6.	Désinstallation des compilateurs gcc et cpp.....	65
7.	Instantané VirtualBox.....	65
8.	Serveur de Production.....	65
IX-	Appendices.....	66
1.	Écran conventionnel de démarrage.....	66
2.	Nom du serveur dans l'écran de connexion à Webmail.....	67
3.	Langue à la console du serveur.....	69
4.	Langue de l'interface Web.....	69
5.	Table de mappe de clavier.....	70
6.	Fermeture automatique de session (session timeout).....	71
7.	Fuseau horaire.....	71
8.	Certificat Let's Encrypt.....	72
9.	Changement du mot de passe de root.....	75
10.	ERROR Failed to send host log message.....	79
X-	Introduction à l'éditeur vi.....	80
1.	Référence.....	80
XI-	Micronator.org.....	82
1.	Cours NethServer-101 - NethServer & Commerce en ligne.....	82
2.	Cours NethServer-201 - NethServer & Applications.....	83
3.	Cours NethServer-301 - NethServer & Active Directory.....	83
4.	Cours NethServer-401 - Surveillance Zabbix.....	83
5.	Cours NethServer-501 - Service d'assistance Zammad.....	83
6.	Cours NethServer-601 - Communication d'équipe Mattermost.....	83
7.	Commentaires et suggestions.....	84
8.	Boutique Micronator.....	84
9.	Médias sociaux.....	84
	Crédits.....	85

I- Description générale

1. Introduction

Le **Cahier-201-11: NethServer & diaspora*** du "Cours NethServer-201" décrit l'installation de l'application web de réseau social **diaspora***.

2. diaspora*

Référence: <https://pod.diaspora.software/>.

2.1. Soyez propriétaire de vos données

De nombreux réseaux utilisent vos données pour gagner de l'argent en analysant vos interactions et en utilisant ces informations pour vous proposer des publicités ciblées. Vos données sur **diaspora*** ne servent qu'à vous mettre en relation et à partager avec d'autres personnes.

2.2. Choisissez votre public

Les **Aspects** de **diaspora*** vous permettent de partager seulement avec les personnes que vous choisissez. Vous demeurez aussi ouvert ou aussi restreint que vous le souhaitez. Partagez des photos amusantes avec le monde entier, ou un grand secret avec vos amis les plus proches. C'est vous qui avez le contrôle.

2.3. Soyez celui que vous voulez

De nombreux réseaux vous incitent à utiliser votre véritable identité. Pas **diaspora***. Vous pouvez choisir qui vous voulez être et partager autant ou aussi peu que vous le souhaitez. C'est vraiment vous qui décidez de la façon dont vous interagissez avec les autres.

2.4. Pourquoi dois-je choisir un pod?

Référence: https://wiki.diasporafoundation.org/Choosing_a_pod.

L'une des plus grandes libertés que vous offre **diaspora*** est celle de choisir où vos données personnelles sont stockées, en choisissant un **pod**. Chaque **pod** a un nom de domaine différent et est géré par différentes personnes sur différents serveurs dans différents emplacements physiques. Vous êtes probablement habitué à ne pas avoir le choix de l'emplacement de stockage de vos données lorsque vous vous inscrivez à un nouveau réseau social, il est donc probable que vous n'ayez jamais eu à y penser auparavant. Ne vous inquiétez pas - tous les **pods** se connectent au même réseau **Diaspora**, et une fois inscrit, vous communiquerez et partagerez avec les utilisateurs de tous les **pods**, pas seulement les utilisateurs de votre propre **pod**. Il s'agit simplement de savoir où le contenu que vous partagez sera physiquement hébergé, par souci de sécurité et de confidentialité.

2.5. Qu'est-ce que diaspora*

Référence: https://fr.wikibooks.org/wiki/Diaspora:_Le_guide_du_parfait_d%C3%A9butant.

diaspora* est un réseau social décentralisé. Pour faire simple, et contrairement à **Facebook**, les informations liées aux utilisateurs ne sont pas stockées dans un seul et même endroit. Elles sont dispersées sur différents serveurs également appelés **pods**. L'utilisateur a donc le choix de l'endroit servant au stockage de ses informa-

tions.

L'avantage de ce système est indéniable: personne n'a la capacité de s'approprier les informations de tous les utilisateurs puisque celles-ci sont éparpillées à travers le monde.

Il est également possible d'installer une instance de **diaspora*** sur votre propre serveur. **diaspora*** permet d'avoir un contrôle total sur les informations personnelles qui seront publiées sur le réseau. Par exemple, les images partagées ne seront plus stockées sur un serveur situé dans un endroit inconnu mais sur sa propre machine. L'utilisateur reste donc maître de ses données.

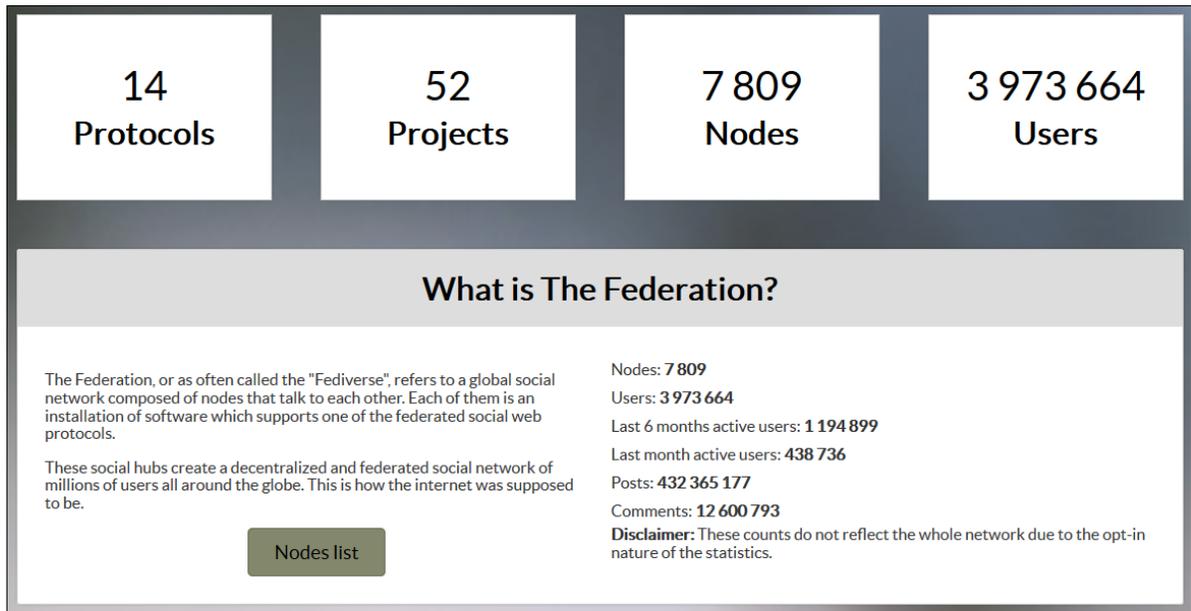
Référence: https://fr.wikipedia.org/wiki/Diaspora*.

2.5.1. Intégration avec les réseaux sociaux

diaspora* vous permet de rester connecté(e) avec vos ami(e)s même si ils/elles ne sont pas encore sur **diaspora***. Il vous suffit de connecter votre compte aux autres services et d'utiliser **diaspora*** comme base: ce que vous posterez sur votre profil sera propagé à ces services automatiquement. **diaspora*** permet la propagation vers les comptes **Facebook**, **Twitter** et **Tumblr** et d'autres sont à venir.

3. La Fédération

Référence: <https://the-federation.info/>.



4. diaspora*: Le guide du parfait débutant



Ce guide est en français.

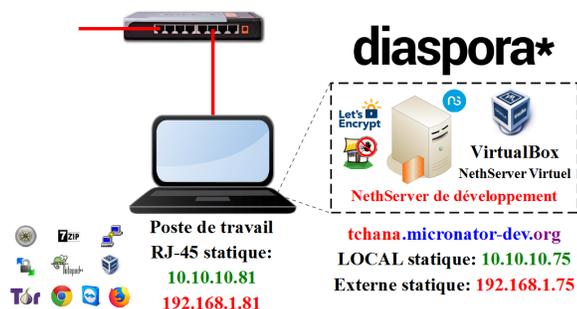
Référence: https://fr.wikibooks.org/wiki/Diaspora_:_Le_guide_du_parfait_d%C3%A9butant.

4.1. Tutoriels diaspora*

Choix de plusieurs langues: <https://diasporafoundation.org/tutorials>.

5. But de ce cahier

Installer l'application web de réseau social **diaspora***.



 Pour cette marche à suivre, nous utiliserons le *Serveur NethServer* du **Cahier-04: Let's Encrypt** du "Cours NethServer-101". <https://www.micronator.org/affaires/produit/nethserver-101cahier-04certificatletsencrypt/>.

6. Marche à suivre

- Préparation de l'environnement de travail
- Réseau LOCAL sans Serveur DNS
- Certificat Let's Encrypt
- Prérequis
 - Paquets & dépendances
 - Activation de Redis
 - PostgreSQL-12
 - Redirection par Apache
 - Instantané VirtualBox
 - Utilitaire sudo
 - RVM
 - Ruby
- Installation
- diaspora*

7. Conventions de ce document

7.1. Notes au lecteur

* Les captures d'écrans ne sont que des références.

** Les informations écrites ont préséance sur celles retrouvées dans les captures d'écrans. Se référer aux différents tableaux lorsque ceux-ci sont présents.

7.2. Conventions

Toutes les commandes à entrer à la console sont en **gras**. Les affichages à surveiller sont en **rouge**, **bleu**, **orange**, **vert** ou **magenta**.

```
# ping 192.168.1.149
192.168.1.149 is alive
#
```

Les liens de référence Internet sont en **bleu** et ceux intra document en **bleu**.



Manipulation, truc ou ruse pour se tirer d'embaras.



Une recommandation ou astuce.



Une note.



Une étape, note ou procédure à surveiller.



Paragraphe non complété ou non vérifié.



Danger pour la sécurité du système.



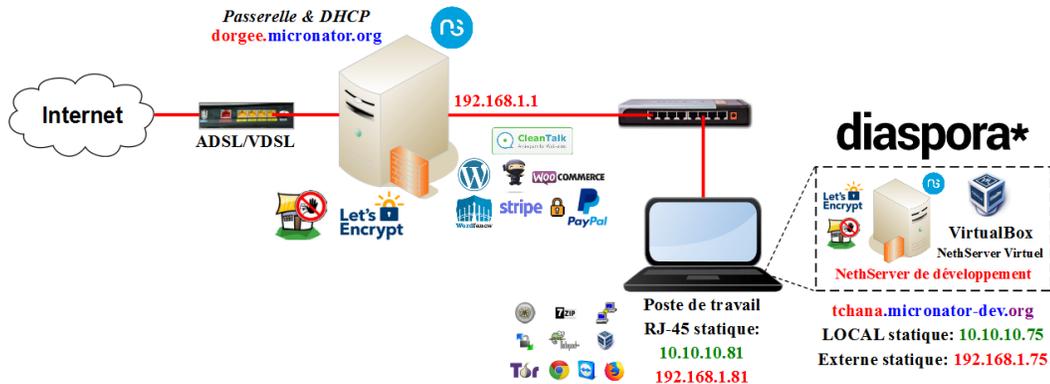
Cette icône indique que la commande est sur une seule ligne. Le **PDF** la mettra sur deux lignes avec un [CR] [LF] entre elles. Il faudra donc copier la commande entière dans un éditeur de texte ASCII et la mettre sur une seule ligne avant de la copier/coller à la console.

Une **chaîne de caractères en magenta** indique qu'il faut remplacer cette chaîne par vos propres paramètres.

```
Commande à exécuter si ce n'est déjà fait.
```

```
Commande indiquée à titre d'information seulement.
```

II- À savoir



1. Serveur NethServer

Le *Serveur NethServer* est un dérivé de la distribution *Linux CentOS* et est équivalent à *CentOS-7.8.2003*.

1.1. dorgee.micronator.org

Serveur physique principal servant de *passerelle* pour les connexions à l'*Internet*.

Serveur *DHCP* pour tout le réseau **LOCAL**.

Domaine principal: micronator.org.

1.2. Serveur NethServer de développement

Serveur virtuel LOCAL sous *VirtualBox Version 6.0.4 r128413 (Qt5.6.2)*.

Nom du serveur: **tchana**.

Domaine de développement: micronator-dev.org.

2. Poste de travail

Windows-8.1 (10.10.10.81), on utilisera ce poste de travail comme station d'administration pour tout ce document.

3. Éditeur de texte

Ne modifiez pas les fichiers avec des éditeurs de documents tels *Notepad*, *TextEdit* ou autres qui ajoutent une *marque d'ordre d'octets (byte order mark)* aux fichiers et qui casse les programmes *PHP*. Utilisez plutôt un éditeur de code tel *vi*, *vim*, *Notepad++*, ou *Atom*; ces éditeurs gèrent l'encodage des fichiers de manière appropriée; ils peuvent aussi être utilisés pour réparer les fichiers précédemment cassés par les autres éditeurs de documents.

Voir le **Cahier-02: Installations & configurations des logiciels prérequis** du "Cours NethServer-101"

<https://www.micronator.org/affaires/produit/nethserver-101-cahier-02installations-configurationsdes-logiciels-prerequis/>

III- Préparation de l'environnement de travail

1. Configuration du poste de travail

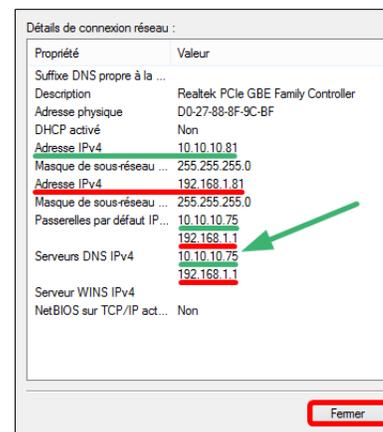
Voir le chapitre *À savoir* du **Cahier-03: NethServer Virtuel** du "Cours NethServer-101" à l'URL:

<https://www.micronator.org/affaires/produit/nethserver-101-cahier-03nethserver-virtuel/>

1.1. Vérification

Clac (*clic droit*) sur le bouton **Démarrer** | **Connexion réseau** | clac sur la carte **Éthernet** | **Statut** | **Détails**.

- Nos deux adresses **IP** et nos deux passerelles son présentes.
- **Fermer** toutes les fenêtres.



2. Fichier hosts du poste de travail

Nous sommes sur un réseau LOCAL et vu que nous n'avons pas de serveur **DNS** pour ce réseau, on ajoute les entrées ci-contre dans le fichier

C:\Windows\System32\drivers\etc\hosts

du poste de travail afin qu'il puisse trouver l'adresse **IP** de notre serveur à l'URL:

<https://www.diaspora.micronator-dev.org/>

```

18
19 # localhost name resolution is handled within DNS itself.
20 # 127.0.0.1    localhost
21 # ::1         localhost
22
23 # Serveur NethServer VirtualBox // POUR diaspora*
24 # Sur station Win-8.1 192.168.1.81
25 10.10.10.75 diaspora.micronator-dev.org
26 10.10.10.75 www.diaspora.micronator-dev.org
27 10.10.10.75 mail.diaspora.micronator-dev.org
28 10.10.10.75 www.mail.diaspora.micronator-dev.org
29 10.10.10.75 smtp.diaspora.micronator-dev.org
30 10.10.10.75 tchana.diaspora.micronator-dev.org
31
    
```



Pour un serveur directement branché à l'Internet, cette procédure de modification du fichier **hosts** du poste de travail n'est pas nécessaire si ces CNAME existent déjà chez le registraire du domaine.



Voir le chapitre **Réseau LOCAL sans Serveur DNS** à la page 22 pour une autre façon de contourner le manque d'un serveur **DNS** pour un réseau LOCAL.

3. Installation d'un Serveur NethServer

Voir le **Cahier-03: NethServer Virtuel** du "Cours NethServer-101":

<https://www.micronator.org/affaires/produit/nethserver-101-cahier-03nethserver-virtuel/>

Pour un serveur virtuel de test, prendre un minimum de **8 GB (25GB recommandé)** dynamiquement alloué pour le disque principal.

3.1. Mise à jour du Serveur NethServer

⚠ Avant de commencer quoi que ce soit, il est toujours préférable de mettre à jour le *Serveur NethServer*.

3.1.1. Ligne de commande

Si vous mettez à jour à la ligne de commande et que vous recevez l'erreur ci-dessous...

```
...
Erreur : Paquet : htmldoc-1.8.28-6.el7.x86_64 (epel)
        Requiert : urw-base35-fonts-legacy
...
```

... lancez la commande suivante:

```
[root@tchana ~]# rpm -Uvh http://mirror.centos.org/centos/7/os/x86_64/Packages/urw-base35-
fonts-legacy-20170801-10.el7.noarch.rpm

Récupération de http://mirror.centos.org/centos/7/os/x86_64/Packages/urw-base35-fonts-
legacy-20170801-10.el7.noarch.rpm
Préparation... ##### [100%]
Mise à jour / installation...
 1:urw-base35-fonts-legacy-20170801-##### [100%]
[root@tchana ~]#
```

4. Vérification: interface Web NethServer

⚠ Il faut activer Javascript et les témoins (*cookies*).

Depuis un poste de travail sur le réseau LOCAL **10.10.10.0/24**, on accède à l'interface Web *Nethserver* <http://10.10.10.75:980>.

4.1. Connexion

Lorsque vous parvenez à l'URL, vous serez invité à entrer un nom d'utilisateur (*qui est **obligatoirement** root avec son mot de passe*). Entrez ce justificatif et cliquez sur **Login** afin d'être amené à l'interface Web *Nethserver*. L'écran du gestionnaire s'affiche.

The screenshot shows the NethServer web interface. On the left is a login form titled 'Bienvenue sur tchana' with fields for 'Nom d'utilisateur' (containing 'root'), 'Mot de passe' (masked with dots), and 'Langue' (set to 'Français (France)'). A 'LOGIN' button is at the bottom. On the right is the dashboard 'Etat du système' with various system metrics: Release (NethServer release 7.8.2003), Mémoire (3664 / 3790 MB used, 126 MB free), Rapports (1 / 2560 MB used), and DNS et DHCP (active). A red box highlights the URL 'https://10.10.10.75:980' in the browser address bar.

⚠ Le cadenas n'est pas vert, car nous utilisons l'adresse IP du *Serveur NethServer*.



Si vous avez de la difficulté à vous connecter, vidangez le cache *DNS* du poste de travail et celui du navigateur Firefox.

- Sur le poste de travail, ouvrir un écran de commandes.

- `ipconfig /flushdns`.

```
Microsoft Windows [version 6.3.9600]
(c) 2013 Microsoft Corporation. Tous droits réservés.

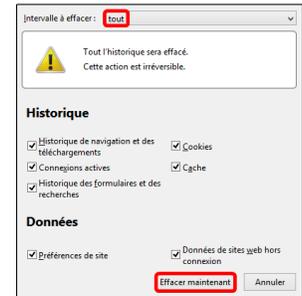
C:\Users\michelandre> ipconfig /flushdns

Configuration IP de Windows

Cache de résolution DNS vidé.

C:\Users\michelandre>
```

Historique | Supprimer l'historique récent... | tout | Effacer maintenant.



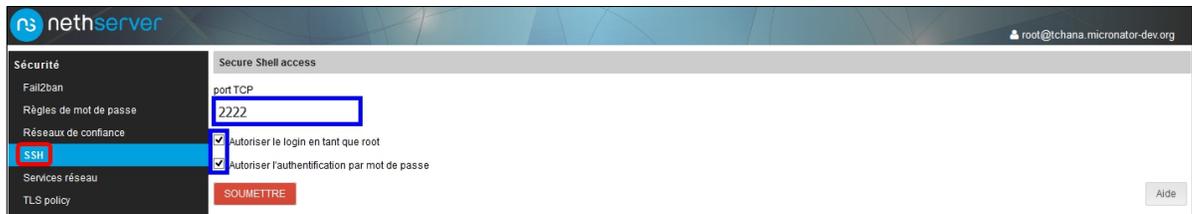
4.2. Fail2ban & ClamAV

Il est fortement recommandé d'installer **Fail2ban** et **ClamAV** pour mieux sécuriser votre *Serveur NethServer*.

Pour l'installation et la configuration de ces modules complémentaires, voir les chapitres *Fail2ban* et *ClamAV* dans le [Cahier-03: NethServer Virtuel](#) du Cours "NethServer-101".

4.3. SSH et paramètres d'accès à distance

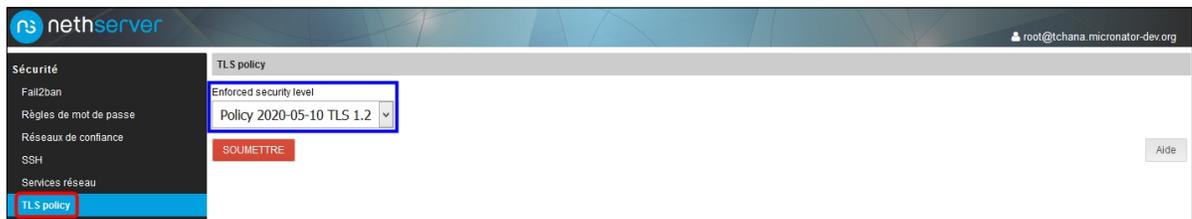
Sécurité | SSH.



4.4. Politique TLS

On s'assure que la **Politique TLS** utilisée est celle en date du *2020-05-10 TLS 1.2*.

Sécurité | TLS policy.



4.5. Certificat du serveur

On vérifie que le certificat émis par le *Serveur NethServer* n'est pas le certificat par défaut, car nous utilisons un certificat **Let's Encrypt**, demandé dans le [Cahier-04: NethServer LOCAL & Certificat Let's Encrypt du "Cours NethServer-101"](#).

Configuration | Certificat du serveur.

The screenshot shows the NethServer configuration interface. The left sidebar has 'Certificat du serveur' highlighted in red. The main content area shows a table of certificates. The 'Défaut' column is highlighted in blue.

Nom	Émetteur	Expire	Défaut	Actions
/etc/pki/lets/certs/NSRV.crt	tchana, O=RF-232, ST=Qc	2029-01-01		Voix

4.6. DNS et Domaines

Configuration | DNS | onglet Hôtes.

On vérifie que le nom **DNS** du domaine **micronator-dev.org** est bien ce qu'il devrait être.

The screenshot shows the NethServer configuration interface. The left sidebar has 'DNS' highlighted in red. The main content area shows the 'Hôtes' tab. A table lists hosts, with the 'micronator-dev.org' row highlighted in blue.

Nom d'hôte	Adresse IP	enregistrement dns joker	Description	Actions
micronator-101.ddns.net	10.10.10.75	Activé	Domaine chez NoIP	Editer
micronator-dev.org	10.10.10.75	Activé	Serveur principal	Editer



L'hôte **micronator-101.ddns.net** provient du [Cahier-04: NethServer LOCAL & Certificat Let's Encrypt du "Cours NethServer-101"](#); on peut supprimer cet hôte.

4.7. Alias

Configuration | DNS | onglet Alias du serveur.

On s'assure que les alias ci-dessous sont présents, sinon on les ajoute.

The screenshot shows the NethServer configuration interface. The left sidebar has 'DNS' highlighted in red. The main content area shows the 'Alias du serveur' tab. A table lists aliases, with the 'mail.micronator-dev.org', 'smtp.micronator-dev.org', and 'www.micronator-dev.org' rows highlighted in blue.

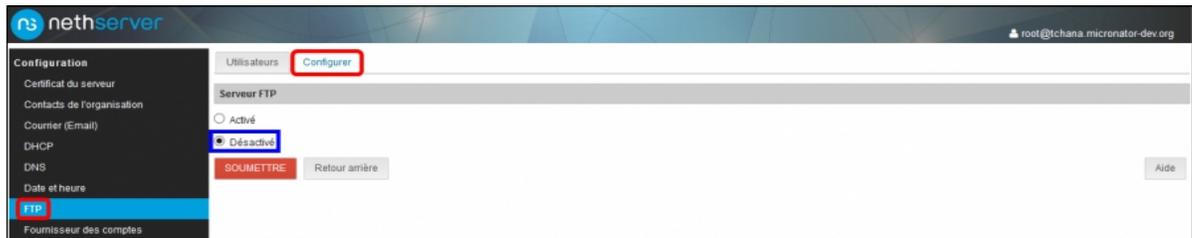
Nom d'hôte	Description	Actions
mail.micronator-dev.org	Serveur principal	Editer
smtp.micronator-dev.org	Serveur principal	Editer
www.micronator-dev.org	Serveur principal	Editer

4.8. Serveur FTP - désactivation recommandée

 **diaspora*** utilise son propre logiciel FTP, il n'est donc pas nécessaire d'activer le service FTP sur le *Serveur NethServer*.

Nous recommandons de ne pas activer ce service, car il n'est pas sécuritaire. Pour le transfert de fichiers, il est préférable d'employer des utilitaires sécurisés tels que **WinSCP** ou **FileZilla**.

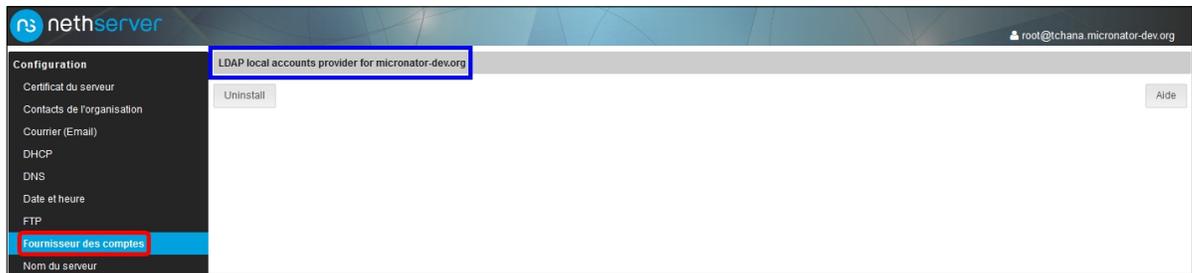
Configuration | FTP | onglet Configurer.



4.9. Fournisseur des comptes

Configuration | Fournisseur des comptes.

LDAP local est notre fournisseur de comptes.



4.9.1. Quelques propriétés de notre fournisseur de comptes

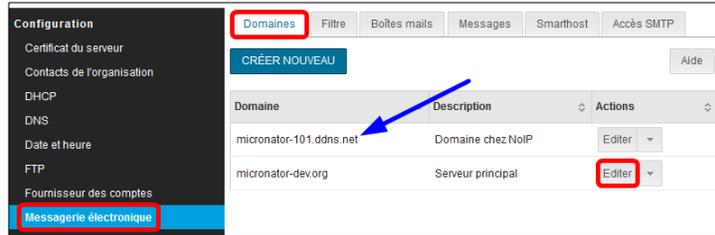
```
[root@tchana ~]# account-provider-test dump

{
  "BindDN" : "cn=ldapservice,dc=directory,dc=nh",
  "LdapURI" : "ldap://127.0.0.1",
  "DiscoverDcType" : "dns",
  "StartTls" : "",
  "port" : 389,
  "host" : "127.0.0.1",
  "isAD" : "",
  "isLdap" : "1",
  "UserDN" : "ou=People,dc=directory,dc=nh",
  "GroupDN" : "ou=Groups,dc=directory,dc=nh",
  "BindPassword" : "OwSvR8Cg_9XbT39w",
  "BaseDN" : "dc=directory,dc=nh",
  "LdapUriDn" : "ldap:///dc%3Dmicronator-dev%2Cdc%3Dorg"
}
[root@tchana ~]#
```

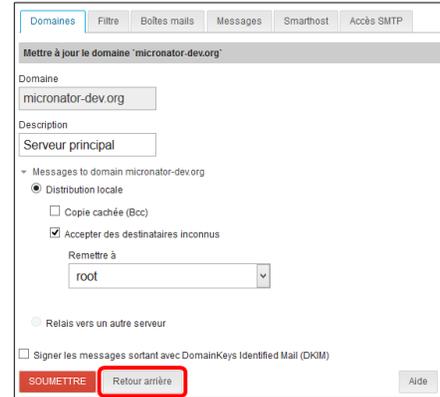
4.10. Messagerie électronique

On vérifie la configuration de la messagerie électronique pour le domaine [micronator-dev.org](#).

Configuration | **Messagerie électronique** | onglet **Domaines** | vis à vis [micronator-dev.org](#) → **Éditer** | on vérifie les entrées | **Retour arrière**.

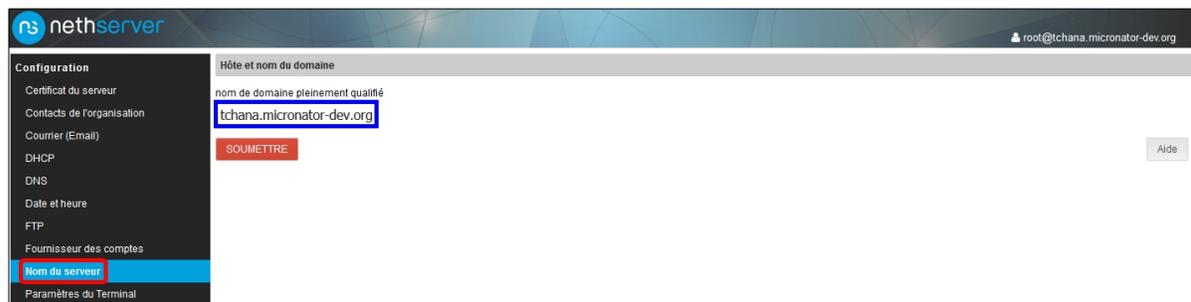


La messagerie pour le domaine [micronator-101.ddns.net](#) provient du **Cahier-04: NethServer LOCAL & Certificat Let's Encrypt** du "Cours NethServer-101", on peut la supprimer.



4.11. Nom du serveur

Configuration | **Nom du serveur**.



4.12. Réseau

Pour le diagramme réseau, voir [À savoir](#) à la page [10](#).

Configuration | **Réseau** | onglet **Nouvelle interface logique** | vis-à-vis la carte ethernet du réseau LOCAL (*LAN vert*) → **Éditer**.

On vérifie la configuration de la carte ethernet du réseau LOCAL.



Configuration | Réseau | onglet Nouvelle interface logique | vis-à-vis la carte ethernet du réseau Externe (LAN rouge) → Éditer.

On vérifie la configuration de la carte ethernet du réseau Externe.

The screenshot shows the configuration page for the 'Internet (rouge)' interface. The left sidebar lists various configuration options, with 'Réseau' highlighted. The main content area is titled 'Editer enp0s8 - pci Intel Corporation 82540EM Gigabit Ethernet Controller (rev 02)'. It displays the link status as 'Actif', speed as '1000 Mbit/s', and MAC address as '08:00:27:99:1a:2e'. The role is set to 'Internet (rouge)'. Under 'Rôle', 'Statique' is selected. The IP address is '192.168.1.75', the subnet mask is '255.255.255.0', and the gateway is '192.168.1.1'. On the right, there are settings for 'Multi WAN' with 'Link name' set to 'red1' and 'Link weight' set to '1'. Below that, there are fields for 'Bande-passante entrante (kbps)' and 'Bande-passante sortante (kbps)'. At the bottom right, there are 'SOUMETTRE' and 'Retour arrière' buttons.

Configuration | Réseau | onglet Serveur DNS:

Primary DSN

→ 192.168.1.1



Pour **Secondary DNS**, on peut utiliser 1.1.1.1 ou 8.8.8.8, mais le premier est plus rapide.

The screenshot shows the 'Configure DNS servers' page in the NethServer interface. The 'Primary DNS' field is set to '192.168.1.1' and the 'Secondary DNS' field is set to '1.1.1.1'. The 'SOUMETTRE' button is visible at the bottom of the configuration area.

4.13. Sauvegardes (données)

Configuration | Sauvegarde (données) | onglet Général et onglet Notification.

The screenshots show the 'Sauvegarde (données)' configuration page. The left sidebar has 'Sauvegarde (données)' highlighted. The main content area is split into two tabs: 'Général' and 'Notification'. The 'Général' tab shows backup settings: 'Type' is set to 'Incrémentiel', 'La sauvegarde complète (full) aura lieu le' is set to 'Dimanche', and 'Politique de rétention' is set to '1 mois'. The 'Notification' tab shows notification settings: 'Envoyer une notification à' is set to 'Toujours', and 'Adresse de l'expéditeur' is empty. A 'SOUMETTRE' button is at the bottom of the notification settings.



Pour en savoir davantage sur la sauvegarde régulière d'un *Serveur NethServer*, consulter le chapitre **Sauvegarde** du [Cahier-03: Création d'un Serveur NethServer virtuel](#) du "Cours NethServer-101". ou celui du [Cahier-05: ADSL/VDSL, DNS dynamique & domaine FQDN](#) du "Cours NethServer-101".

5. Ouverture d'une session PuTTY

Les paramètres sont maintenant définis correctement et on peut utiliser **PuTTY** pour se connecter au *Serveur NethServer*.

Voir le **Cahier-02: Installations & configurations des logiciels prérequis** du "Cours NethServer-101" pour vous familiariser avec ce logiciel de connexion.

<https://www.micronator.org/affaires/produit/nethserver-101-cahier-02installations-configurationsdes-logiciels-prerequis/>

Si nous ne sommes pas déjà logué, nous nous connectons en tant que **root** au *Serveur NethServer tchana* à l'aide de *PuTTY*.

```
login as: root
root@10.10.10.75's password: mot-de-passe-de-root
Last login: Wed Feb 12 15:16:40 2020 from 10.10.10.81

***** Welcome to NethServer *****

This is a NethServer installation.

Before editing configuration files, be aware
of the automatic events and templates system.

      http://docs.nethserver.org

*****
[root@tchana ~]#
```

5.1. Adresse IP

On vérifie les adresses **IP** du serveur.

```
[root@tchana ~]# ifconfig

enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.10.75 netmask 255.255.255.0 broadcast 10.10.10.255
    inet6 fe80::a00:27ff:fea4:9f9f prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:a4:9f:9f txqueuelen 1000 (Ethernet)
    RX packets 102843 bytes 137206748 (130.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 88703 bytes 5977942 (5.7 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.75 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe52:f4bd prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:52:f4:bd txqueuelen 1000 (Ethernet)
    RX packets 2355 bytes 270222 (263.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3874 bytes 3090722 (2.9 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Boucle locale)
    RX packets 2981 bytes 319468 (311.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2981 bytes 319468 (311.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@tchana ~]#
```

5.2. Mise à jour du Serveur NethServer

On s'assure que le *Serveur NethServer* soit bien à jour.

```
[root@tchana ~]# yum update -y

Modules complémentaires chargés : changelog, fastestmirror, nethserver_events
Loading mirror speeds from cached hostfile
* ce-base: mirror.facebook.net
* ce-extras: mirror.facebook.net
* ce-sclo-rh: mirror.facebook.net
* ce-sclo-sclo: mirror.facebook.net
* ce-updates: mirror.facebook.net
* epel: mirror.dst.ca
* nethforge: mirror.nethserver.org
* nethserver-base: mirror.nethserver.org
* nethserver-updates: mirror.nethserver.org
* remi-safe: mirrors.ukfast.co.uk
No packages marked for update
[root@tchana ~]#
```

5.3. Fail2ban

On vérifie que le "pare-feu" **Fail2ban** soit installé.

```
[root@tchana ~]# rpm -qa | grep -i fail2ban

fail2ban-shorewall-0.11.1-9.el7.2.noarch
fail2ban-server-0.11.1-9.el7.2.noarch
nethserver-fail2ban-1.4.2-1.ns7.noarch
fail2ban-sendmail-0.11.1-9.el7.2.noarch
fail2ban-firewalld-0.11.1-9.el7.2.noarch
fail2ban-0.11.1-9.el7.2.noarch
[root@tchana ~]#
```

On vérifie que le service roule sur le serveur.

```
[root@tchana ~]# ps aux | grep -i fail2ban

root      4756  5.4  1.2 1754272 46932 ?        Ssl  15:32   1:51 /usr/bin/python2 -s
/usr/bin/fail2ban-server -xf start
root      18200  0.0  0.0 112840   984 pts/0    S+   16:06   0:00 grep --color=auto -i
fail2ban
[root@tchana ~]#
```

5.4. ClamAV

Par défaut, **ClamAV** est installé, mais partiellement et s'occupe seulement du balayage des courriels.

Dans le [Cahier-03: NethServer Virtuel](#) du "Cours NethServer-101", nous avons installé **ClamAV** qui s'occupe aussi du balayage du système de fichiers.

On vérifie que l'antivirus *ClamAV* soit installé pour le système de fichiers.

```
[root@tchana ~]# rpm -qa | grep -i clamav

clamav-lib-0.102.4-1.el7.x86_64
clamav-0.102.4-1.el7.x86_64
clamav-unofficial-sigs-7.0.1-5.el7.noarch
clamav-update-0.102.4-1.el7.x86_64
clamav-filessystem-0.102.4-1.el7.noarch
[root@tchana ~]#
```

Si nécessaire, on peut mettre à jour la *BD* de *ClamAV*.

```
[root@tchana ~]# freshclam

ClamAV update process started at Tue Sep  8 16:09:02 2020
daily.cld database is up to date (version: 25924, sigs: 4294294, f-level: 63, builder:
raynman)
main.cvd database is up to date (version: 59, sigs: 4564902, f-level: 60, builder: sigmgr)
bytecode.cvd database is up to date (version: 331, sigs: 94, f-level: 63, builder: anvilleg)
[root@tchana ~]#
```

5.5. Scanner Antivirus

Configuration | Scanner Antivirus | onglet Clamscan | on ajuste selon ses choix | SOUMETTRE.

6. Utilisateurs

6.1. Utilisateur michelandre

Si ce n'est déjà fait, on crée l'utilisateur **michelandre** et on l'insère dans le groupe *domain* **admins@micronator-dev.org**.

Gestion | Utilisateurs et groupes | onglet Utilisateurs.

Utilisateur	Nom	Actions
admin@micronator-dev.org	admin	Editer
michelandre@micronator-dev.org	Michel-André	Editer

Onglet Groupes | Éditer.

On s'assure que l'utilisateur [michelandre](#) fasse partie du groupe *domain admins@micronator-dev.org*.

Utilisateurs **Groupe**

Mettre à jour le groupe 'domain admins@micronator-dev.org'

Nom du groupe
domain admins@micror

▼ Membres

Chercher [michelandre@micronator-dev.org] Ajouter

admin@micronator-dev.org	x
michelandre@micronator-dev.org	x

SOUMETTRE Retour arrière Aide

7. Instantané VirtualBox



Il est fortement recommandé d'arrêter le *Serveur NethServer* et d'en prendre un instantané **VirtualBox** afin de pouvoir y revenir si nous exécutons une fausse manipulation qui ruinerait tout notre travail jusqu'ici. Grâce aux **instantanés VirtualBox**, vous pouvez enregistrer l'état particulier d'une machine virtuelle à un moment donné pour pouvoir l'utiliser plus tard. Ainsi, après avoir pris un instantané, vous pourrez à n'importe quel moment revenir à cet état, même si la machine virtuelle a été complètement changée ou endommagée. Voir le chapitre *Instantané d'une machine virtuelle* dans le **Cahier-03: Création d'un Serveur NethServer virtuel** du "Cours NethServer-101".

IV- Réseau LOCAL sans Serveur DNS

1. Description

Ce chapitre est dédié aux environnements qui n'ont pas de serveur DNS sur leur réseau LOCAL.

2. Difficultés pour un réseau LOCAL sans serveur DNS

2.1. Messagerie

- Comme on peut le voir sur le diagramme réseau au début du chapitre [À savoir](#) à la page [10](#), notre *Serveur Nethserver* de développement est sur notre réseau LOCAL.
- S'il n'existe aucun serveur DNS sur le réseau LOCAL, un courriel envoyé à usager-untel@micronator-dev.org ne pourra pas être livré, car le domaine micronator-dev.org est totalement inconnu de tous les hôtes: serveurs, stations, routeurs, etc connectés au réseau LOCAL.
- Tous les courriels vers un hôte inconnu sont alors envoyés à la passerelle dorgee.micronator.org.

2.2. Requête HTML

- S'il n'existe aucun serveur DNS sur le réseau LOCAL, une requête HTML envoyé au domaine micronator-dev.org ne pourra pas être livrée, car le domaine est inconnu sur le réseau LOCAL et elle sera, elle aussi, envoyée à la passerelle dorgee.micronator.org.

La difficulté réside dans le fait que même le serveur dorgee.micronator.org ne connaît pas le domaine micronator-dev.org.

3. Modification de la passerelle du réseau LOCAL

Pour résoudre ces difficultés, nous allons informer le *Serveur Nethserver* dorgee.micronator.org de l'adresse IP du domaine micronator-dev.org.

3.1. Sauvegarde de la configuration NethServer



Avant de modifier le serveur passerelle dorgee du réseau LOCAL, il est fortement recommandé de prendre une sauvegarde de sa configuration NethServer actuelle en cas d'une future erreur de manipulation.

1) **Configuration** | Sauvegarde (Configuration) | **CRÉER UNE SAUVEGARDE.**

2) *Description* → **Config avant dev.org** | **CRÉER UNE SAUVEGARDE.**

3) On vérifie le résultat.



3.2. Messagerie électronique

Nous indiquons à la passerelle micronator.org l'adresse IP de la messagerie électronique du domaine micronator-dev.org

Configuration | Messagerie électronique | onglet Domaines | CRÉER NOUVEAU | on entre les informations demandées | **SOUMETTRE**.



L'adresse IP **192.168.1.75** est celle de la carte réseau du serveur micronator-dev.org sur le réseau LOCAL du serveur passerelle micronator.org.

Lorsque la passerelle recevra un courriel à destination de notre serveur micronator-dev.org, dont elle connaît maintenant l'adresse IP, elle le relaiera vers **192.168.1.75**.

3.3. Entrées DNS

Nous indiquons à la passerelle micronator.org l'adresse IP du domaine micronator-dev.org.

Configuration | DNS | onglet Hôtes | CRÉER NOUVEAU.

On entre les informations demandées | **SOU-METTRE**.

On s'assure du résultat de l'opération.

micronator-dev.org	192.168.1.75	Activé	Pour dev.org
--------------------	--------------	--------	--------------

3.4. Alias

- Nous créons des alias du domaine micronator-dev.org.

Configuration | DNS | onglet Alias du serveur | CRÉER NOUVEAU | on entre les informations demandées | **SOU-METTRE**.

Lorsque la passerelle recevra une requête *HTML* à destination de notre serveur de développement, dont elle connaît maintenant les domaines micronator-dev.org, mail.micronator-dev.org et www.micronator-dev.org, elle les relaiera vers **192.168.1.75**.



Avec ces ajouts au serveur passerelle, n'importe quel hôte du réseau LOCAL pourra communiquer avec notre serveur de développement sans devoir ajouter d'entrées dans leur fichier **hosts**.

4. Vérification des redirections par la passerelle

On peut vérifier si les redirections par la passerelle fonctionnent correctement en supprimant les entrées, spécifiques au *Serveur NethServer* de développement, qu'on avait insérées aux paragraphes [Fichier hosts du poste de travail](#) à la page [11](#).

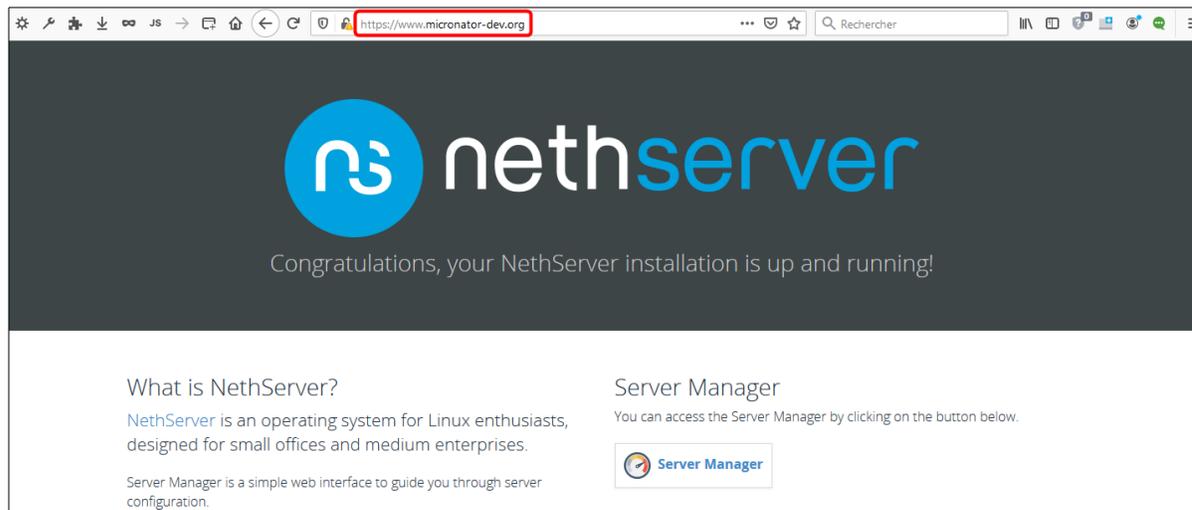
```
19 # localhost name resolution is handled within DNS itself.
20 # 127.0.0.1 localhost
21 # ::1 localhost
22
23
24
```



Il faut vidanger le cache DNS du poste de travail et celui du navigateur **Firefox**.

4.1. Domaine micronator-dev.org

<https://www.micronator-dev.org>



5. Nom de notre domaine de développement sur la liste blanche

5.1. Liste blanche du Serveur NethServer dorgee.micronator.org



Notre serveur de développement est sur le réseau LOCAL (*192.168.1.0/24*) du serveur dorgee.micronator.org. Voir le diagramme au chapitre [À savoir](#) à la page [10](#).

Vu que nous n'utilisons pas d'enregistrement *SPF*¹ et *DKIM*², les courriels en provenance de notre serveur de développement risquent fortement d'être rejetés par le serveur dorgee.micronator.org.



Pour contourner ce rejet, nous allons ajouter notre domaine de développement sur la liste blanche du serveur dorgee.micronator.org en créant un filtre d'autorisation pour ce domaine.



Sur notre *Serveur NethServer* principal (dorgee.micronator.org), dont certains utilisateurs de **diaspora*** sont issus et qui y reçoivent leurs courriels, il nous faut mettre le domaine de notre serveur de développement sur sa liste blanche, sinon dorgee.micronator.org considérera ces courriels comme des pourriels provenant d'un serveur inconnu.

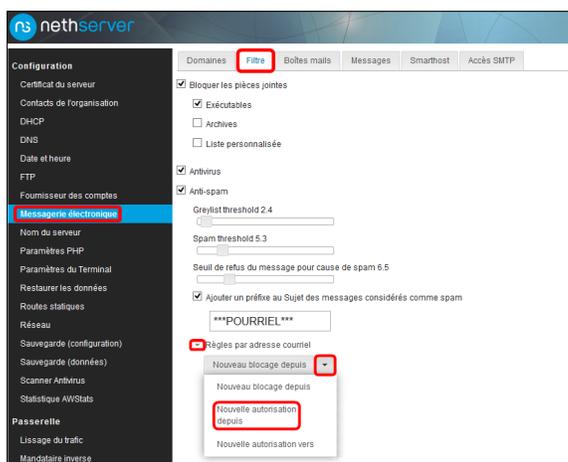
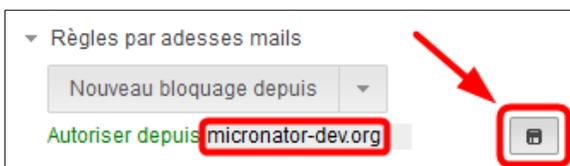
1 **SPF**: Sender Policy Framework https://fr.wikipedia.org/wiki/Sender_Policy_Framework.

2 **DKIM**: DomainKeys Identified Mail https://fr.wikipedia.org/wiki/DomainKeys_Identified_Mail.

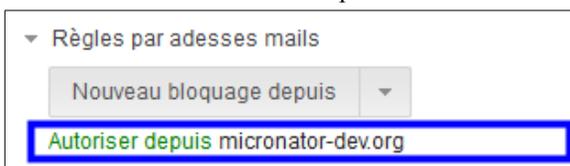
Configuration | Messagerie électronique | onglet Filtre | on clique **Règles par adresses mails** pour afficher les détails.

On déroule le menu **Nouveau blocage depuis** et on clique **Nouvelle autorisation depuis**.

Dans le champ **Autoriser depuis**, on ajoute notre domaine **micronator-dev.org** et on clique l'icône **Fait**.



On vérifie le résultat de cette opération.



SOUMETTRE.



5.2. Liste blanche du Serveur NethServer **tchana.micronator-dev.org**

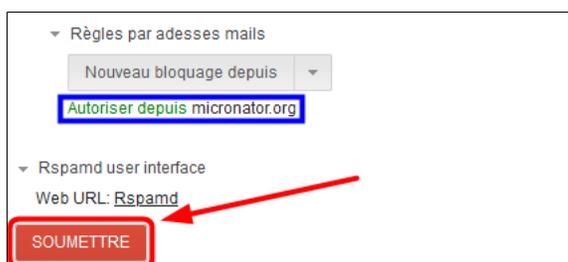
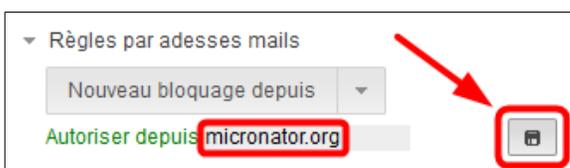
Le *Serveur NethServer* **tchana.micronator-dev.org** pourrait aussi rejeter les courriels provenant du serveur **dorgee.micronator.org** si ce dernier n'utilise pas *SPF* et *DKIM*.

On ajoute donc à **tchana** un filtre d'autorisation en suivant la même procédure que précédemment.

Configuration | Messagerie électronique | onglet FILTRE.

1) On ajoute un filtre **Autoriser depuis** pour le domaine **micronator.org**.

2) On vérifie le résultat | **SOUMETTRE.**



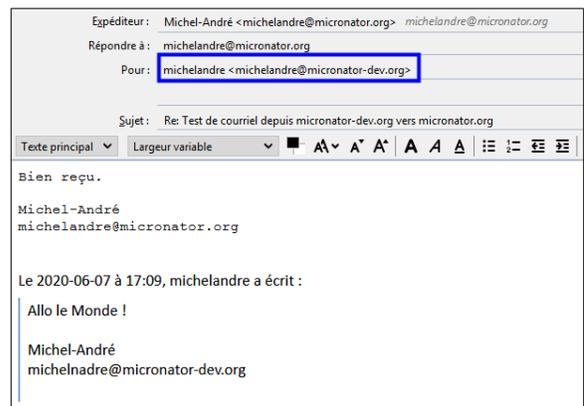
5.3. Vérification

Pour vérifier que le serveur **dorgee.micronator.org** accepte les courriels en provenance de notre domaine de développement, l'utilisateur **michelandre**, qui est un usager du domaine **micronator-dev.org**, écrit un message à l'utilisateur **michelandre** du domaine **micronator.org**.

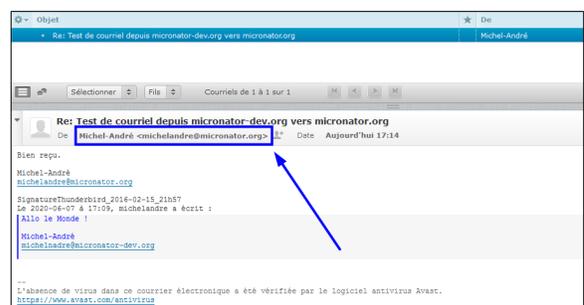
- 1) Connexion à **micronator-dev.org/webmail**.
- 2) L'utilisateur **michelandre** écrit un message et l'envoie.



- 1) L'utilisateur **michelandre** sur **micronator.org** reçoit le message et y répond.
- 2) Une fois la réponse terminée, il l'envoie.



L'utilisateur **michelandre** reçoit le message dans **Webmail** de **micronator-dev.org**.



Les messageries électroniques fonctionnent correctement.

6. Sauvegarde des configurations



On lance des sauvegardes de configuration des serveurs dorgee.micronator.org et tchana.micronator-dev.org.



Configuration | Sauvegarde (Configuration) | **CRÉER UNE SAUVEGARDE** | *Description* → **Config après liste blanche** | **CRÉER UNE SAUVEGARDE** | on vérifie les résultats.

7. Instantané VirtualBox



À ce stade-ci, on peut prendre un instantané de la machine virtuelle afin de pouvoir y revenir en cas d'une future erreur de manipulation.

V- Certificat Let's Encrypt

1. Description

Il faut ajuster le certificat **Let's Encrypt** afin d'y inclure les **CNAME** pour **diaspora***.

Pour l'installation d'un certificat *Let's Encrypt* sur un *Serveur NethServer LOCAL*, voir le **Cahier-04: NethServer LOCAL & Certificat Let's Encrypt** du "Cours NethServer-101":

<https://www.micronator.org/affaires/produit/nethserver-101cahier-04certificatletsencrypt/>.

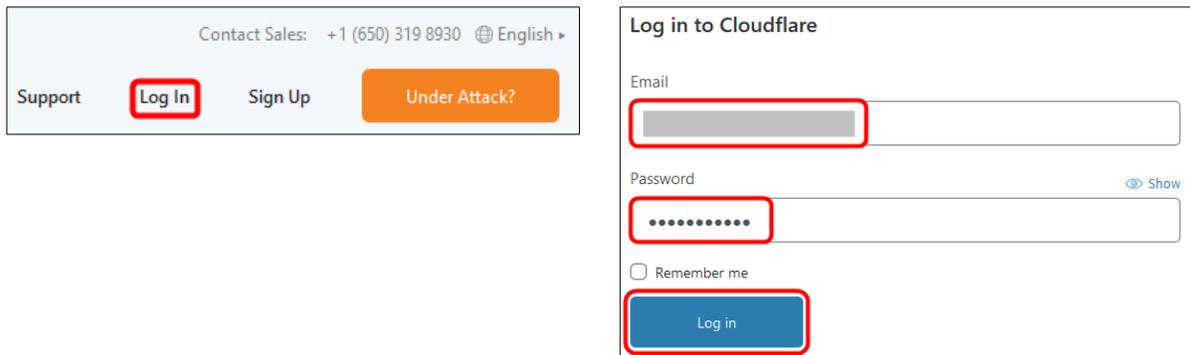
Pour l'installation d'un certificat *Let's Encrypt* sur un *Serveur NethServer* directement branché à l'Internet, voir le **Cahier-05: VDSL, FQDN, Internet et NethServer** du "Cours NethServer-101":

<https://www.micronator.org/affaires/produit/nethserver-101-cahier-05-adsl-vdsl-dns-dynamique-domaine-fqdn/>

2. Ajout des CNAME pour diaspora*

1) On se rend à l'URL <https://dash.cloudflare.com> | **Log In**.

2) On se connecte.

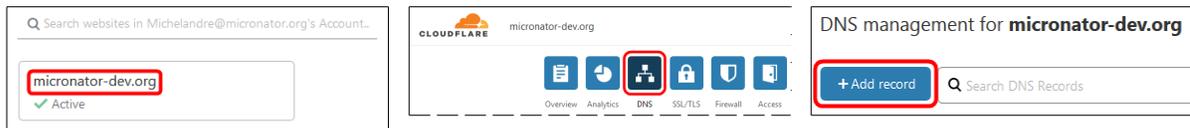


The image shows two screenshots of the Cloudflare dashboard. The first screenshot shows the top navigation bar with 'Log In' highlighted in a red box. The second screenshot shows the 'Log in to Cloudflare' form with the 'Email' and 'Password' input fields highlighted in red boxes, and the 'Log in' button highlighted in a red box.

1) On clique le nom de notre domaine.

2) **DNS**.

3) **Add record**.



The image shows two screenshots of the Cloudflare DNS management interface. The first screenshot shows a search for 'micronator-dev.org' with the result highlighted in a red box. The second screenshot shows the DNS management page for 'micronator-dev.org' with the '+ Add record' button highlighted in a red box.

Certificat Let's Encrypt

On ajoute les *CNAME* suivant:

domaine diaspora: **diaspora**, **www.diaspora**, **mail.diaspora**, **www.mail.diaspora** et **smtp.diaspora**.

Type	Name	Target	TTL	Proxy status
CNAME	diaspora	@	Auto	Proxied
				Cancel Save

Type	Name	Target	TTL	Proxy status
CNAME	www.diaspora	@	Auto	Proxied
				Cancel Save

Type	Name	Target	TTL	Proxy status
CNAME	mail.diaspora	@	Auto	Proxied
				Cancel Save

Type	Name	Target	TTL	Proxy status
CNAME	www.mail.diaspora	@	Auto	Proxied
				Cancel Save

Type	Name	Target	TTL	Proxy status
CNAME	smtp.diaspora	@	Auto	Proxied
				Cancel Save

On vérifie.

Type	Name	Content	TTL	Proxy status	
CNAME	smtp.diaspora	micronator-dev.org	Auto	Proxied	Edit
CNAME	www.mail.diaspora	micronator-dev.org	Auto	Proxied	Edit
CNAME	mail.diaspora	micronator-dev.org	Auto	Proxied	Edit
CNAME	www.diaspora	micronator-dev.org	Auto	Proxied	Edit
CNAME	diaspora	micronator-dev.org	Auto	Proxied	Edit
A	micronator-dev.org		Auto	Proxied	Edit

 Pour un serveur directement branché à l'Internet, si certains de ces *CNAME* ne sont pas déjà présents chez le registraire de votre nom de domaine, il faut les ajouter. Pour plus de détails, voir le chapitre *Régistrare de domaines* dans le [Cahier-05: VDSL, FQDN, Internet et NethServer](#) du "Cours NethServer-101".

3. Script acme.sh

Si ce n'est déjà fait, la commande ci-dessous téléchargera les fichiers accompagnant `acme.sh`, les stockera dans `~/ .acme.sh` et mettra à jour la variable d'environnement `PATH` pour inclure ce chemin.

```
[root@tchana ~]# curl https://get.acme.sh | sh
...
```

On vérifie le chemin du script `acme.sh`.

```
root@tchana ~]# which acme.sh

alias acme.sh='/root/.acme.sh/acme.sh'
      /root/.acme.sh/acme.sh
[root@tchana ~]#
```

On vérifie sa version.

```
[root@tchana ~]# acme.sh -v

https://github.com/acmesh-official/acme.sh
v2.8.6
[root@tchana ~]#
```



Si la version actuelle est antérieure à **v2.8.6**, on réinstalle tout simplement le script `acme.sh` et les fichiers de la nouvelle version écraseront ceux de l'ancienne, sans toutefois affecter les fichiers des requêtes précédentes ou les anciens certificats déjà présents.

```
[root@tchana ~]# curl https://get.acme.sh | sh
...
```



Déconnectez-vous et reconnectez-vous pour activer le chemin du script `acme.sh`.

3.1.1. Vérification de la configuration PKI

```
[root@tchana ~]# config show pki

pki=configuration
CertificateDuration=3650
ChainFile=/etc/pki/tls/certs/chain.pem
CommonName=Micronator
CountryCode=CA
CrtFile=/etc/pki/tls/certs/cert.pem
EmailAddress=VotreAdresseCourriel
KeyFile=/etc/pki/tls/private/privkey.pem
LetsEncrypt=disabled
LetsEncryptDomains=
LetsEncryptMail=
LetsEncryptRenewDays=30
Locality=Montreal
Organization=RF-232
OrganizationalUnitName=Service informatique
State=Qc
SubjectAltName=*.micronator-dev.org
[root@tchana ~]#
```

4. Demande d'un certificat de test

On lance une demande d'un certificat de **TEST** pour notre domaine **diaspora.micronator-dev.org** et ses CNAME.



Le premier paramètre **-d** doit être pour le domaine **diaspora.micronator-dev.org** afin que le certificat soit émis spécifiquement pour celui-ci, car le premier domaine spécifié est celui pour lequel le certificat sera émis et les autres domaines seront des *Noms alternatifs du sujet*.



```
[root@tchana ~]# /root/.acme.sh/acme.sh
--issue
--dns dns_cf
-d diaspora.micronator-dev.org
-d www.diaspora.micronator-dev.org
-d mail.diaspora.micronator-dev.org
-d www.mail.diaspora.micronator-dev.org
-d smtp.diaspora.micronator-dev.org
-d micronator-dev.org
-d www.micronator-dev.org
-d mail.micronator-dev.org
-d wpad.micronator-dev.org
--cert-file /etc/pki/tls/certs/cert.pem
--ca-file /etc/pki/tls/certs/chain.pem
--key-file /etc/pki/tls/private/privkey.pem
--reloadcmd "/sbin/e-smith/signal-event certificate-update"
--test

[dim. sept. 13 13:57:28 EDT 2020] Using stage ACME_DIRECTORY: https://acme-staging-
v02.api.letsencrypt.org/directory
[dim. sept. 13 13:57:29 EDT 2020] Creating domain key
[dim. sept. 13 13:57:29 EDT 2020] The domain key is here:
/root/.acme.sh/diaspora.micronator-dev.org/diaspora.micronator-dev.org.key
[dim. sept. 13 13:57:29 EDT 2020] Multi domain='DNS:diaspora.micronator-
dev.org,DNS:www.diaspora.micronator-dev.org,DNS:mail.diaspora.micronator-
dev.org,DNS:www.mail.diaspora.micronator-dev.org,DNS:smtp.diaspora.micronator-
dev.org,DNS:micronator-dev.org,DNS:www.micronator-dev.org,DNS:mail.micronator-
dev.org,DNS:wpad.micronator-dev.org'
[dim. sept. 13 13:57:29 EDT 2020] Getting domain auth token for each domain
...
[dim. sept. 13 13:59:09 EDT 2020] Your cert is in /root/.acme.sh/diaspora.micronator-
dev.org/diaspora.micronator-dev.org.cer
[dim. sept. 13 13:59:09 EDT 2020] Your cert key is in /root/.acme.sh/diaspora.micronator-
dev.org/diaspora.micronator-dev.org.key
[dim. sept. 13 13:59:09 EDT 2020] The intermediate CA cert is in
/root/.acme.sh/diaspora.micronator-dev.org/ca.cer
[dim. sept. 13 13:59:09 EDT 2020] And the full chain certs is there:
/root/.acme.sh/diaspora.micronator-dev.org/fullchain.cer
[dim. sept. 13 13:59:09 EDT 2020] Installing cert to:/etc/pki/tls/certs/cert.pem
[dim. sept. 13 13:59:09 EDT 2020] Installing CA to:/etc/pki/tls/certs/chain.pem
[dim. sept. 13 13:59:09 EDT 2020] Installing key to:/etc/pki/tls/private/privkey.pem
[dim. sept. 13 13:59:10 EDT 2020] Run reload cmd: /sbin/e-smith/signal-event certificate-
update
[dim. sept. 13 13:59:12 EDT 2020] Reload success
[root@tchana ~]#
```

La demande d'un certificat de **TEST** a été couronné de **succès**.



Si nous rencontrons des difficultés, on peut ajouter le paramètre **--debug** qui nous donnera plus d'informations.

5. Demande d'un certificat officiel

La demande d'un certificat de **TEST** a réussi, on peut alors faire une demande pour un certificat **Officiel**.

On force `--force` le renouvellement pour l'obtention d'un certificat *TLS* officiel.

```
[root@tchana ~]# /root/.acme.sh/acme.sh
--issue
--dns dns_cf
-d diaspora.micronator-dev.org
-d www.diaspora.micronator-dev.org
-d mail.diaspora.micronator-dev.org
-d www.mail.diaspora.micronator-dev.org
-d smtp.diaspora.micronator-dev.org
-d micronator-dev.org
-d www.micronator-dev.org
-d mail.micronator-dev.org
-d wpad.micronator-dev.org
--cert-file /etc/pki/tls/certs/cert.pem
--ca-file /etc/pki/tls/certs/chain.pem
--key-file /etc/pki/tls/private/privkey.pem
--reloadcmd "/sbin/e-smith/signal-event certificate-update"
--force

...
-----BEGIN CERTIFICATE-----
MIIGqjCCBZKgAwIBAgISBDuLN3ITz0jU9nH+ayVoBxnpMA0GCSqGSIb3DQEBCwUA
MEoxCzAJBgNVBAYTA1VTMRYwWFAyDVQKKEw1MZXQncyBFbmnYexB0MSMwIQYDVQ
ExpMZXQncyBFbmnYexB0IEF1dGhvcml0eSBYmzAeFw0yMDAyMjIyMjM1NDlaFw0y
MDA1MjIyMjM1NDlaMCMxITAFBgNVBAMTGzZvcnVtLmlpY3JvbmF0b3ItZGV2Lm9y
...
h8wCiyWzwpocYvJEBb1Idz6KJwPF/6l1bxxmlQw27+kWimKLfiF27htV+MReEJL1
FRrvuUw4nBcjYrs9/764Hr8tVlChMeM/A4SyYM3m3yEQbfTZFtbvH9/emsx7K8Xp
YtBeQSSQDSshQSfepGAU15pcYRiSrU9k07VAXC3uRXb507qffKEh+7wI2DEImLmG
TkxgYd9kLRe3N/tpSyNVGGFfA6RNbPnfCRuWttrX
-----END CERTIFICATE-----
[dim. sept. 13 14:07:00 EDT 2020] Your cert is in /root/.acme.sh/diaspora.micronator-dev.org/diaspora.micronator-dev.org.cer
[dim. sept. 13 14:07:00 EDT 2020] Your cert key is in /root/.acme.sh/diaspora.micronator-dev.org/diaspora.micronator-dev.org.key
[dim. sept. 13 14:07:00 EDT 2020] The intermediate CA cert is in /root/.acme.sh/diaspora.micronator-dev.org/ca.cer
[dim. sept. 13 14:07:00 EDT 2020] And the full chain certs is there: /root/.acme.sh/diaspora.micronator-dev.org/fullchain.cer
[dim. sept. 13 14:07:00 EDT 2020] Installing cert to:/etc/pki/tls/certs/cert.pem
[dim. sept. 13 14:07:00 EDT 2020] Installing CA to:/etc/pki/tls/certs/chain.pem
[dim. sept. 13 14:07:00 EDT 2020] Installing key to:/etc/pki/tls/private/privkey.pem
[dim. sept. 13 14:07:00 EDT 2020] Run reload cmd: /sbin/e-smith/signal-event certificate-update
[dim. sept. 13 14:07:03 EDT 2020] Reload success
[root@tchana ~]#
```

La demande pour un certificat **Officiel** a été couronné de succès.

6. Vérification

6.1. À la console du serveur

Clé publique.

```
[root@tchana ~]# ls -als /etc/pki/tls/certs/cert.pem
4 -rw-r--r-- 1 root root 2269 13 sept. 14:07 /etc/pki/tls/certs/cert.pem
[root@tchana ~]#
```

Chaîne de certification.

```
[root@tchana ~]# ls -als /etc/pki/tls/certs/chain.pem
4 -rw-r--r-- 1 root root 1648 13 sept. 14:07 /etc/pki/tls/certs/chain.pemchain.pem
[root@tchana ~]#
```

Clé privée.

```
[root@tchana ~]# ls -als /etc/pki/tls/private/privkey.pem
4 -rw----- 1 root root 1679 13 sept. 14:07 /etc/pki/tls/private/privkey.pemprivkey.pem
[root@tchana ~]#
```

7. Vérification de la connexion sécurisée

- On se rend à : <https://diaspora.micronator-dev.org>.

La page Web par défaut de *NethServer* s'affiche, car *diaspora** n'est pas encore installé.

Par contre, le cadenas s'affiche correctement, car le certificat a été émis par **Let's Encrypt** qui est une autorité de certification reconnue et la connexion est sécurisée par un chiffrement *TLS/SSL*.



Si vous avez de la difficulté à vous connecter, vidanger le cache *DNS* du poste de travail et celui du navigateur *Firefox*.

8. Sauvegarde

On vérifie si le nom du répertoire `/root/.acme.sh/` est déjà inséré dans le fichier d'inclusion de la sauvegarde régulière des données : `/etc/backup-data.d/custom.include`, sinon on l'y insère.



Prendre tout le contenu de l'encadré pour la commande.

```
NouvelleInclusion="/root/.acme.sh/"
if grep -Fxq "$NouvelleInclusion" /etc/backup-data.d/custom.include
then
    # L'entrée a été trouvée dans custom.include
    echo -e "\nLe fichier custom.include contient déjà l'entrée:\n$NouvelleInclusion \n"
else
    # L'entrée n'a pas été trouvée dans custom.include
    echo -e "$NouvelleInclusion" >> /etc/backup-data.d/custom.include
    echo -e "\nL'entrée: $NouvelleInclusion a été ajoutée\n"
fi
```

On vérifie.

```
[root@tchana ~]# cat /etc/backup-data.d/custom.include | grep acme
/root/.acme.sh/
[root@tchana ~]#
```

Ci-dessus, il n'y a pas de ligne vide avant `/root/.acme.sh/`. Nous en avons inséré une afin de faciliter la copie de la commande.

9. Instantané VirtualBox



À ce stade-ci, on peut prendre un instantané de la machine virtuelle afin de pouvoir y revenir en cas d'une future erreur de manipulation.

VI- Prérequis

Références:

<https://community.nethserver.org/t/howto-install-diaspora-pod-on-nethserver/10581>

<https://community.nethserver.org/t/diaspora-pod-on-nethserver/10558/2>

<https://wiki.diasporafoundation.org/Installation/CentOS/7>

1. Paquets

Installation de certains paquets qui sont prérequis pour l'installation de **diaspora***.

```
[root@tchana ~]# yum install -y tar make automake gcc gcc-c++ git net-tools cmake
libcurl-devel libxml2-devel libffi-devel libxslt-devel
wget redis ImageMagick nodejs

...
Résumé de la transaction
=====
Installation 11 Paquets (+34 Paquets en dépendance)

Taille totale des téléchargements : 76 M
Taille d'installation : 231 M
...
Installé :
ImageMagick.x86_64 0:6.9.10.68-3.e17          automake.noarch 0:1.13.4-3.e17
cmake.x86_64 0:2.8.12.2-2.e17                gcc.x86_64 0:4.8.5-39.e17
gcc-c++.x86_64 0:4.8.5-39.e17               git.x86_64 0:1.8.3.1-23.e17_8
libcurl-devel.x86_64 0:7.29.0-57.e17_8.1    libffi-devel.x86_64 0:3.0.13-19.e17
libxml2-devel.x86_64 0:2.9.1-6.e17.4        libxslt-devel.x86_64 0:1.1.28-5.e17
nodejs.x86_64 1:6.17.1-1.e17

...
Dépendances installées :
OpenEXR-libs.x86_64 0:1.7.1-7.e17
...
zlib-devel.x86_64 0:1.2.7-18.e17

Terminé !
[root@tchana ~]#
```

2. Activation de Redis

CentOS/NethServer n'active et ne démarre pas les services automatiquement, on doit donc le faire manuellement.

Activation de **Redis**.

```
[root@tchana ~]# systemctl enable redis

Created symlink from /etc/systemd/system/multi-user.target.wants/redis.service to
/usr/lib/systemd/system/redis.service.
[root@tchana ~]#
```

Démarrage de Redis.

```
[root@tchana ~]# systemctl start redis
[root@tchana ~]#
```

Vérification.

```
[root@tchana ~]# systemctl status redis

● redis.service - Redis persistent key-value database
   Loaded: loaded (/usr/lib/systemd/system/redis.service; enabled; vendor preset: disabled)
   Drop-In: /etc/systemd/system/redis.service.d
            └─limit.conf
   Active: active (running) since dim. 2020-09-13 15:25:06 EDT; 1min 3s ago
   Main PID: 4046 (redis-server)
   CGroup: /system.slice/redis.service
           └─4046 /usr/bin/redis-server 127.0.0.1:6379

sept. 13 15:25:06 tchana.micronator-dev.org systemd[1]: Starting Redis persistent key-va....
sept. 13 15:25:06 tchana.micronator-dev.org systemd[1]: Started Redis persistent key-val....
Hint: Some lines were ellipsized, use -l to show in full.
[root@tchana ~]#
```

3. PostgreSQL-12

3.1. Installation

3.1.1. Référentiel pgdg12

32 ou 64 bits

Il nous faut connaître le genre de *CPU* utilisé par notre serveur afin de choisir la bonne version de **PostgreSQL**.

```
[root@tchana ~]# uname -p
x86_64
[root@tchana ~]#
```

Version CentOS

Pour connaître la version *CentOS* dont notre serveur est issu.

```
[root@tchana ~]# cat /etc/centos-release
CentOS Linux release 7.8.2003 (Core)
[root@tchana ~]#
```

Lien du référentiel PostgreSQL

Pour connaître le lien **URL** du référentiel **PostgreSQL**, on se rends au site suivant:

<https://yum.postgresql.org/repopackages.php>



Le référentiel **EPEL** (*Extra Packages pour Enterprise Linux*) est présent et **Activé** par défaut sur un *Server NethServer*.

Notre *Serveur NethServer* est un **64 bits** issu de *CentOS-7*. Donc, nous choisissons **CentOS 7 - x86 64**.

AVAILABLE REPO RPMS

As of 15 April 2019, there is only one repository RPM per distro which includes repository information for all available PostgreSQL releases.

- Red Hat Enterprise Linux 8 - x86_64
- CentOS 8 - x86_64
- Oracle Enterprise Linux 8 - x86_64
- Red Hat Enterprise Linux 8 - aarch64(arm64)
- CentOS 8 - aarch64(arm64)
- Red Hat Enterprise Linux 7 - x86_64
- Scientific Linux 7 - x86_64
- **CentOS 7 - x86_64**
- Oracle Enterprise Linux 7 - x86_64

On clique (*clic droit*) sur **CentOS 7 - x86 64** et on copie l'adresse du lien.

Le lien du référentiel **PostgreSQL** pour notre serveur est:

https://download.postgresql.org/pub/repos/yum/repopms/EL-7-x86_64/pgdg-redhat-repo-latest.noarch.rpm



Installation du référentiel

La commande pour installer le référentiel **PostgreSQL** est composée de 2 parties:

- `yum install -y` et
- le lien du référentiel.

On installe le référentiel **PostgreSQL** pour les serveurs *CentOS-7* dont le *Serveur NethServer* est issu.

On entre `yum install -y` (*suivi d'un espace*) et on colle le lien copié précédemment.



Nous avons enlevé l'invite et utilisé une petite police de caractères afin d'entrer la commande sur une seule ligne.

```
yum install -y https://download.postgresql.org/pub/repos/yum/repopms/EL-7-x86_64/pgdg-redhat-repo-latest.noarch.rpm
...
Résumé de la transaction
=====
Installation 1 Paquet
Taille totale : 11 k
Taille d'installation : 11 k
...
Installé :
  pgdg-redhat-repo.noarch 0:42.0-12
Terminé !
[root@tchana ~]#
```

Le référentiel **PostgreSQL** est installé.

3.1.2. Installation de PostgreSQL-12

Maintenant, on peut procéder à l'installation de PostgreSQL-12.



```
[root@tchana ~]# yum install -y --enablerepo=pgdg12
postgreSQL12      postgresql12-libs
postgreSQL12-server postgresql12-contrib
postgreSQL12-devel postgresql12-docs
postgreSQL12-test postgresql12-devel

...
Résumé de la transaction
=====
Installation      8 Paquets (+20 Paquets en dépendance)

Taille totale des téléchargements : 125 M
Taille d'installation : 442 M
...
Installé :
  postgresql-devel.x86_64 0:9.2.24-4.el7_8
  postgresql12.x86_64 0:12.4-1PGDG.rhel7
  postgresql12-contrib.x86_64 0:12.4-1PGDG.rhel7
  postgresql12-devel.x86_64 0:12.4-1PGDG.rhel7
  postgresql12-docs.x86_64 0:12.4-1PGDG.rhel7
  postgresql12-libs.x86_64 0:12.4-1PGDG.rhel7
  postgresql12-server.x86_64 0:12.4-1PGDG.rhel7
  postgresql12-test.x86_64 0:12.4-1PGDG.rhel7

Dépendances installées :
  devtoolset-7-binutils.x86_64 0:2.28-11.el7
  ...
  scl-utils.x86_64 0:20130529-19.el7

Terminé !
[root@tchana ~]#
```

On vérifie l'installation.

```
[root@tchana ~]# rpm -qi postgresql12-server

Name       : postgresql12-server
Version    : 12.4
Release    : 1PGDG.rhel7
Architecture: x86_64
Install Date: dim. 13 sept. 2020 15:44:01 EDT
Group      : Unspecified
Size       : 21296807
License    : PostgreSQL
Signature  : DSA/SHA1, mer. 12 août 2020 07:25:23 EDT, Key ID 1f16d2e1442df0f8
Source RPM : postgresql12-12.4-1PGDG.rhel7.src.rpm
Build Date : mer. 12 août 2020 07:23:55 EDT
Build Host : koji-centos7-x86-64-pgbuild
Relocations : (not relocatable)
Vendor     : PostgreSQL Global Development Group
URL        : https://www.postgresql.org/
Summary    : The programs needed to create and run a PostgreSQL server
Description :
PostgreSQL is an advanced Object-Relational database management system (DBMS).
The postgresql12-server package contains the programs needed to create
and run a PostgreSQL server, which will in turn allow you to create
and maintain PostgreSQL databases.

[root@tchana ~]#
```

3.1.3. Protection du référentiel

Références:

http://lxsoft106.cern.ch/cern/centos/7.6.1810/updates/x86_64/repoview/yum-plugin-protectbase.html

<https://www.cyberciti.biz/faq/rhel-centos-fedora-yum-protect-packages-from-certain-repositories/>.

Nous voulons protéger le référentiel **pgdg12** afin que ses paquets ne soient pas mis à jour par aucun autre référentiel.

On installe le paquet `yum-plugin-protectbase`.

```
[root@tchana ~]# yum install -y yum-plugin-protectbase

...
Résumé de la transaction
=====
Installation      1 Paquet

Taille totale des téléchargements : 27 k
Taille d'installation : 22 k
...
Installé :
  yum-plugin-protectbase.noarch 0:1.1.31-54.e17_8

Terminé !
[root@tchana ~]#
```

On affiche les informations du paquet `yum-plugin-protectbase`.

```
[root@tchana ~]# rpm -qi yum-plugin-protectbase

Name           : yum-plugin-protectbase
Version        : 1.1.31
Release        : 54.e17_8
Architecture   : noarch
Install Date   : dim. 13 sept. 2020 15:47:51 EDT
Group          : System Environment/Base
Size           : 22696
License        : GPLv2+
Signature      : RSA/SHA256, mer. 13 mai 2020 15:54:55 EDT, Key ID 24c6a8a7f4a80eb5
Source RPM     : yum-utils-1.1.31-54.e17_8.src.rpm
Build Date    : mar. 12 mai 2020 12:27:44 EDT
Build Host     : x86-01.bsys.centos.org
Relocations    : (not relocatable)
Packager       : CentOS BuildSystem <http://bugs.centos.org>
Vendor        : CentOS
URL            : http://yum.baseurl.org/download/yum-utils/
Summary       : Yum plugin to protect packages from certain repositories.
Description :
This plugin allows certain repositories to be protected. Packages in the
protected repositories can't be overridden by packages in non-protected
repositories even if the non-protected repo has a later version.
[root@tchana ~]#
```

On s'assure que le paquet est activé c.-à-d. `enabled = 1`.

```
[root@tchana ~]# cat /etc/yum/pluginconf.d/protectbase.conf

[main]
enabled = 1
[root@tchana ~]#
```

Protection de pgdg12

On protège le référentiel **pgdg12** en éditant le fichier: `/etc/yum.repos.d/pgdg-redhat-all.repo` et en ajoutant la ligne `protect = 1` à la fin de la section définissant le référentiel `[pgdg12]`.

```
[root@tchana ~]# vi /etc/yum.repos.d/pgdg-redhat-all.repo
```

```
...
[pgdg12]
name=PostgreSQL 12 for RHEL/CentOS $releasever - $basearch
baseurl=https://download.postgresql.org/pub/repos/yum/12/redhat/rhel-$releasever-$basearch
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-PGDG
protect = 1
...
```



Tous les paquets du référentiel `pgdg12` sont maintenant protégés contre toutes mises à jour provenant de tous les autres référentiels.

On vérifie.

```
[root@tchana ~]# cat /etc/yum.repos.d/pgdg-redhat-all.repo | grep -B7 -A1 protect

[pgdg12]
name=PostgreSQL 12 for RHEL/CentOS $releasever - $basearch
baseurl=https://download.postgresql.org/pub/repos/yum/12/redhat/rhel-$releasever-$basearch
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-PGDG
protect = 1

[root@tchana ~]#
```

3.1.4. Initialisation de la base de données

On initialise la **BD**.



Peut prendre un certain temps.

```
[root@tchana ~]# /usr/pgsql-12/bin/postgresql-12-setup initdb

Initializing database ... OK
[root@tchana ~]#
```

3.1.5. Activation du service PostgreSQL

On active le service **PostgreSQL** pour qu'il démarre avec tous amorçages du *Serveur NethServer*.

```
[root@tchana ~]# systemctl enable postgresql-12.service

Created symlink from /etc/systemd/system/multi-user.target.wants/postgresql-12.service to
/usr/lib/systemd/system/postgresql-12.service.
[root@tchana ~]#
```

On démarre le service **PostgreSQL**.

```
[root@tchana ~]# systemctl start postgresql-12.service

[root@tchana ~]#
```

On examine le statut du service **PostgreSQL**.

```
[root@tchana ~]# systemctl status postgresql-12.service
● postgresql-12.service - PostgreSQL 12 database server
   Loaded: loaded (/usr/lib/systemd/system/postgresql-12.service; enabled; vendor preset:
disabled)
   Active: active (running) since dim. 2020-09-13 15:54:01 EDT; 11s ago
     Docs: https://www.postgresql.org/docs/12/static/
   Process: 5908 ExecStartPre=/usr/pgsql-12/bin/postgresql-12-check-db-dir ${PGDATA}
(code=exited, status=0/SUCCESS)
   Main PID: 5913 (postmaster)
    CGroup: /system.slice/postgresql-12.service
           └─5913 /usr/pgsql-12/bin/postmaster -D /var/lib/pgsql/12/data/
             └─5916 postgres: logger
               └─5918 postgres: checkpointer
                 └─5919 postgres: background writer
                   └─5920 postgres: walwriter
                     └─5921 postgres: autovacuum launcher
                       └─5922 postgres: stats collector
                         └─5923 postgres: logical replication launcher
...
[root@tchana ~]#
```



PostgreSQL-12 est installé et protégé contre les mises à jour par tous les référentiels, sauf `pgdg12`.

3.2. Premiers pas

3.2.1. Référence

Cette section est inspirée de l'article suivant: https://wiki.postgresql.org/wiki/First_steps et sert à démontrer quelques commandes à la console `psql`.

Pour vous familiariser avec **PostgreSQL**, voir le chapitre **PostgreSQL-11** du **Cahier-01: Mattermost - Installation** du cours "NethServer-601": <https://www.micronator.org/affaires/produit/nethserver-601-cahier-01-mattermost-installation/>.

3.3. Configuration finale

3.3.1. MD5

Maintenant, il nous faut configurer **PostgreSQL** pour qu'il accepte les connexions avec mots de passe chiffrés **MD5** pour être ainsi compatible avec les modules **Python**.

On vérifie qu'on est bien **root**.

```
[root@tchana ~]# whoami
root
[root@tchana ~]#
```



En tant qu'utilisateur **root**, on remplace `ident` par `md5` dans le fichier `pg_hba.conf`.

```
[root@tchana ~]# sed -i "/^host/s/ident/md5/g" /var/lib/pgsql/12/data/pg_hba.conf
[root@tchana ~]#
```

On vérifie.

```
[root@tchana ~]# cat /var/lib/pgsql/12/data/pg_hba.conf | grep md5
# METHOD can be "trust", "reject", "md5", "password", "scram-sha-256",
# Note that "password" sends passwords in clear text; "md5" or
host    all             all             127.0.0.1/32      md5
host    all             all             ::1/128           md5
host    replication     all             127.0.0.1/32      md5
host    replication     all             ::1/128           md5
[root@tchana ~]#
```

On redémarre le service **PostgreSQL** pour s'assurer que tout fonctionne encore correctement.

```
[root@tchana ~]# systemctl restart postgresql-12.service
[root@tchana ~]#
```

On vérifie.

```
[root@tchana ~]# systemctl status postgresql-12.service | grep Active
Active: active (running) since dim. 2020-09-13 16:03:27 EDT; 13s ago
[root@tchana ~]#
```

3.3.2. Création de l'utilisateur Linux **diaspora**

On peut choisir le mot de passe qu'on veut, mais l'important est de le mémoriser. De plus, il est préférable qu'il réponde aux normes *NethServer* pour les mots de passe.

Utilisateur Linux

On crée un utilisateur/groupe nommé **diaspora**, qui exécutera l'installation de **diaspora***.

```
[root@tchana ~]# useradd diaspora
[root@tchana ~]#
```

On octroie un mot de passe robuste à l'utilisateur **diaspora** de Linux.

```
[root@tchana ~]# passwd diaspora
Changement de mot de passe pour l'utilisateur mattemost.
Nouveau mot de passe : mot-de-passe-robuste-pour-mattemost
MOT DE PASSE INCORRECT : Le mot de passe comporte moins de 8 caractères
Retapez le nouveau mot de passe : mot-de-passe-robuste-pour-mattemost
passwd : mise à jour réussie de tous les jetons d'authentification.
[root@tchana ~]#
```



Dans notre cas, le mot de passe (*fghtbgh* qui est celui du Grand général Toto) est de 7 caractères seulement; pour un serveur en production, il faut un mot de passe robuste et conforme aux normes *NethServer*. Il ne faut pas utiliser notre exemple.



Le mot de passe doit contenir: au moins 1 chiffre, 1 caractère majuscule, 1 caractère minuscule, 1 caractère non-alphanumérique, 5 caractères différents, ne pas être présent dans les dictionnaires de mots courants et être différent du nom d'utilisateur. De plus, il est impossible de répéter des motifs formés de 3 caractères ou plus (par exemple, le mot de passe *As1.\$AS1.\$* n'est pas valide).

On ajuste les droits du répertoire personnel de l'utilisateur **diaspora** dans lequel on installera **diaspora***.

```
[root@tchana ~]# chmod 755 /home/diaspora/
[root@tchana ~]#
```

On vérifie.

```
[root@tchana ~]# ls -alsd /home/diaspora/
0 drwxr-xr-x 3 diaspora diaspora 95 13 sept. 17:18 /home/diaspora/
[root@tchana ~]#
```

3.3.3. Création d'un usager PostgreSQL pour la BD de diaspora*

On se substitue au super-utilisateur **postgres**.

```
[root@tchana ~]# su - postgres
-bash-4.2$
```

On lance la console **PostgreSQL**.

```
-bash-4.2$ psql
psql (12.4)
Saisissez « help » pour l'aide.
postgres=#
```

On crée l'utilisateur **PostgreSQL usager_diaspora** et on lui donne un mot de passe.

```
postgres=# CREATE USER usager_diaspora WITH CREATEDB PASSWORD 'fghtbgh';
CREATE ROLE
postgres=#
```



Le paramètre **CREATEDB** indique que l'utilisateur **usager_diaspora** peut créer des bases de données.

3.3.4. Création de la BD pour diaspora*

On crée la BD **bddiaspora**.

```
postgres=# CREATE DATABASE bddiaspora;
CREATE DATABASE
postgres=#
```

On vérifie.

```
postgres=# \l

                Liste des bases de données
  Nom          | Propriétaire | Encodage | Collationnement | Type caract. | Droits d'accès
-----+-----+-----+-----+-----+-----
 bddiaspora   | postgres    | UTF8     | fr_FR.utf8      | fr_FR.utf8   |
 postgres    | postgres    | UTF8     | fr_FR.utf8      | fr_FR.utf8   |
 template0    | postgres    | UTF8     | fr_FR.utf8      | fr_FR.utf8   | =c/postgres  +
               |              |          |                  |              | postgres=CTc/postgres
 template1    | postgres    | UTF8     | fr_FR.utf8      | fr_FR.utf8   | =c/postgres  +
               |              |          |                  |              | postgres=CTc/postgres
(4 lignes)
postgres=#
```

Prérequis

On donne tous les droits sur la BD `bddiaspora` à l'utilisateur PostgreSQL `usager_diaspora`.

```
postgres=# GRANT ALL PRIVILEGES ON DATABASE bddiaspora to usager_diaspora;
GRANT
postgres=#
```

On quitte la console PostgreSQL.

```
postgres=# \q
-bash-4.2$
```

On sort de la substitution.

```
-bash-4.2$ exit
déconnexion
[root@tchana ~]#
```

3.3.5. Vérification

On vérifie que tout fonctionne correctement pour l'utilisateur PostgreSQL `usager_diaspora` avec son mot de passe `fghtbgh` et qu'il peut accéder à la BD `bddiaspora`.

```
[root@tchana ~]# psql --host=127.0.0.1 --dbname=bddiaspora --username=usager_diaspora --password
Mot de passe pour l'utilisateur usager_diaspora : fghtbgh
psql (9.2.24, serveur 12.4)
ATTENTION : psql version 9.2, version du serveur 12.0.
          Certaines fonctionnalités de psql pourraient ne pas fonctionner.
Saisissez « help » pour l'aide.
mattermostbd=>
```

Tout fonctionne correctement pour l'utilisateur `usager_diaspora`.

On quitte la console PostgreSQL.

```
mattermostbd=> \q
[root@tchana ~]#
```

3.4. Mot de passe du super-utilisateur postgres

On octroie un mot de passe robuste à l'utilisateur `postgres` de Linux.

```
[root@tchana ~]# passwd postgres
Changement de mot de passe pour l'utilisateur postgres.
Nouveau mot de passe : mot-de-passe-robuste-pour-postgres
MOT DE PASSE INCORRECT : Le mot de passe comporte moins de 8 caractères
Retapez le nouveau mot de passe : mot-de-passe-robuste-pour-postgres
passwd : mise à jour réussie de tous les jetons d'authentification.
[root@tchana ~]#
```



Dans notre cas, le mot de passe (`fghtbgh` qui est celui du Grand général Toto) est de 7 caractères seulement; pour un serveur en production, il faut un mot de passe robuste et conforme aux normes *NethServer*. Il ne faut pas utiliser notre exemple.



Le mot de passe doit contenir: au moins 1 chiffre, 1 caractère majuscule, 1 caractère minuscule, 1 caractère spécial, 5 caractères différents, ne pas être présent dans les dictionnaires de mots courants et être différent du nom d'utilisateur. De plus, il est impossible de répéter des motifs formés de 3 caractères ou plus (*par exemple, le mot de passe `As1.$AS1.$` n'est pas valide*).

3.5. Sauvegarde

3.5.1. Répertoire du fichier `/var/lib/pgsql/`

On vérifie si le nom du répertoire `/var/lib/pgsql/` est déjà inclus dans le fichier d'inclusion de la sauvegarde des données: `/etc/backup-data.d/custom.include`, sinon on l'insère.



Prendre tout le contenu de l'encadré pour la commande.

```
NouvelleInclusion="/var/lib/pgsql/"
if grep -Fxq "$NouvelleInclusion" /etc/backup-data.d/custom.include
then
  # L'entrée a été trouvée dans custom.include
  echo -e "\nLe fichier custom.include contient déjà l'entrée:\n$NouvelleInclusion \n"
else
  # L'entrée n'a pas été trouvée dans custom.include
  echo -e "$NouvelleInclusion" >> /etc/backup-data.d/custom.include
  echo -e "\nL'entrée: $NouvelleInclusion a été ajoutée\n"
fi
```

On vérifie.

```
[root@tchana ~]# cat /etc/backup-data.d/custom.include | grep pgsql

/var/lib/pgsql/
[root@tchana ~]#
```

Ci-dessus, il n'y a pas de ligne vide avant `/var/lib/pgsql/`. Nous en avons inséré une afin de faciliter la copie de la commande.

4. Redirection par Apache

On crée un fichier pour la redirection d'Apache afin qu'il pointe vers le bon répertoire pour **diaspora***.



Prendre tout le contenu de l'encadré pour la commande.

```

cat > /etc/httpd/conf.d/zzz_diaspora.conf << EOL
# Make sure to notice the comments at https://gist.github.com/jhass/719014#gistcomment-19774

<VirtualHost *:80>
  ServerName diaspora.micronator-dev.org

# To make letsencrypt work
  RedirectMatch 301 ^(!?/\.\well-known/acme-challenge/).* https://diaspora.micronator-dev.org
</VirtualHost>
<VirtualHost *:443>
  ServerName diaspora.micronator-dev.org

  DocumentRoot /home/diaspora/diaspora/public

  RewriteEngine On

  RewriteCond %{HTTP_HOST} !^diaspora\.micronator-dev\.org [NC]
  RewriteRule ^/(.*)$ https://diaspora\.micronator-dev\.org/ [L,R,QSA]

# For Camo support
#RewriteRule ^/camo/(.*)$ balancer://camo/ [P,QSA,L]

RewriteCond %{DOCUMENT_ROOT}/%{REQUEST_FILENAME} !-f
RewriteRule ^/(.*)$ balancer://upstream%{REQUEST_URI} [P,QSA,L]

<Proxy balancer://upstream>
# Recommended, using a unix socket (Requires Apache >= 2.4)
# BalancerMember unix:///path/to/diaspora/tmp/diaspora.sock|http://
# Alternatively let diaspora listen on a local port (Use this for Apache < 2.4)
BalancerMember http://localhost:3000
</Proxy>

# For Camo support
#<Proxy balancer://camo>
# BalancerMember http://localhost:8081
#</Proxy>

ProxyRequests Off
ProxyVia On
ProxyPreserveHost On
RequestHeader set X_FORWARDED_PROTO https

<Proxy *>
# Apache < 2.4
#Order allow,deny
#Allow from all
# Apache >= 2.4
Require all granted
</Proxy>

<Directory /home/diaspora/diaspora/public>
Options -MultiViews
# Apache < 2.4
#Allow from all
#AllowOverride all
# Apache >= 2.4
Require all granted
</Directory>

SSLEngine On
SSLCertificateFile /etc/pki/tls/certs/localhost.crt
SSLCertificateKeyFile /etc/pki/tls/private/localhost.key

# Based on https://wiki.mozilla.org/Security/Server_Side_TLS - consider as global configuration
SSLProtocol all -SSLv2 -SSLv3
SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-
AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-
AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-
AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-
DSS-AES256-SHA:DHE-RSA-AES256-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128:AES256:AES:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!
MD5:!PSK
SSLHonorCipherOrder on
SSLCompression off
</VirtualHost>

EOL

```

Redémarrage d'**Apache** pour qu'il relise ses fichiers de configuration et ainsi inclure ce nouveau greffon.

```
[root@tchana ~]# systemctl restart httpd
[root@tchana ~]#
```

Vérification.

```
[root@tchana ~]# systemctl status httpd | grep Active
Active: active (running) since lun. 2020-09-14 14:46:17 EDT; 48s ago
[root@tchana ~]#
```

5. Instantané VirtualBox



À ce stade-ci, on peut prendre un instantané de la machine virtuelle afin de pouvoir y revenir en cas d'une future erreur de manipulation.

6. Utilitaire sudo

Référence: <https://fr.wikipedia.org/wiki/Sudo>.

L'utilitaire **sudo** (abréviation de "*substitute user do*", en français: "*exécuter en se substituant à l'utilisateur*") est une commande informatique utilisée principalement dans les systèmes d'exploitation de type Unix.

Cette commande permet à un administrateur système d'accorder à certains utilisateurs (*ou groupes d'utilisateurs*) la possibilité de lancer une commande en tant que **root**, ou en tant qu'un autre utilisateur, tout en conservant une trace des commandes saisies et des arguments.

L'utilitaire **sudo** s'utilise en ligne de commande, dans un terminal. Il sert par exemple à exécuter, en mode superutilisateur, des commandes ou des applications en console. Il faut faire précéder chacune des commandes à exécuter en mode superutilisateur par la commande **sudo**, de la manière suivante:

```
$ sudo <commande>
```

Le mot de passe demandé est celui de l'utilisateur courant. La commande sera exécutée si le mot de passe entré est correct et que l'utilisateur courant peut effectuer des tâches d'administration. Le mot de passe est mémorisé pour une durée de 15 minutes; au terme de ce laps de temps, il faut entrer de nouveau le mot de passe. La commande pour terminer la session sudo avant la fin des 15 minutes est:

```
$ sudo -k
```

La commande suivante permet d'être connecté en tant que **root** en interface de commande.

```
$ sudo -i
```

6.1. Groupe wheel

Référence: [https://en.wikipedia.org/wiki/Wheel_\(computing\)](https://en.wikipedia.org/wiki/Wheel_(computing)).

Les systèmes Unix modernes utilisent généralement des groupes d'utilisateurs comme protocole de sécurité pour contrôler les privilèges d'accès. Le groupe **wheel** est un groupe d'utilisateurs spécial, utilisé sur certains systèmes Unix, principalement les systèmes **BSD**, pour contrôler l'accès à la commande **su** ou **sudo**, qui permet à un utilisateur de se faire passer pour un autre utilisateur (*généralement le super utilisateur*). Les systèmes d'exploitation de type **Debian** créent un groupe appelé **sudo** avec un objectif similaire à celui de **wheel**.

6.2. Utilisateur LINUX diaspora et le groupe wheel

C'est l'utilisateur LINUX diaspora qui installera diaspora* dans son répertoire personnel. Il installera aussi certains modules qui nécessitent les privilèges de root. Nous allons donc insérer l'utilisateur diaspora dans le groupe wheel et ainsi, si l'utilisateur diaspora précède une commande avec sudo, il disposera des privilèges de root durant l'exécution de celle-ci.

On ajoute l'utilisateur LINUX diaspora dans le groupe wheel.

```
[root@tchana ~]# usermod -aG wheel diaspora
[root@tchana ~]#
```

On vérifie.

```
[root@tchana ~]# cat /etc/group | grep wheel
wheel:x:10:diaspora
[root@tchana ~]#
```

7. RVM

RVM ou *Ruby Version Manager* est un outil de ligne de commande basé sur **Bash** et **Ruby** pour gérer une installation **Ruby**. **RVM** vous permet d'installer et de configurer simultanément plusieurs versions de **Ruby** sur le même serveur pour vous permettre de travailler avec plusieurs environnements **Ruby**.

Nous vous recommandons d'utiliser **Ruby Version Manager** qui garantira que vous roulez la version **Ruby** actuellement recommandée et séparera proprement votre installation diaspora* de toutes les autres applications **Ruby** sur votre machine. Si vous choisissez de ne pas l'utiliser, assurez-vous que votre version de **Ruby** est au moins **2.3.0**, les versions précédentes sont incompatibles. Nous recommandons actuellement d'utiliser la dernière version **Ruby** de la série **2.7**.

Référence: <https://www.howtoforge.com/tutorial/how-to-install-and-use-ruby-on-rails-with-postgresql-on-centos-7/>.

La première étape consiste à installer la dernière version stable de **RVM** (*v-1.29.10*). Nous devons télécharger les clés du référentiel et les importer avec la commande `gpg` avant de commencer à installer **RVM**.



On se substitue à l'utilisateur diaspora.

```
[root@tchana ~]# su - diaspora
Dernière connexion : dimanche 13 septembre 2020 à 17:38:34 EDT sur pts/0
[diaspora@tchana ~]$
```

7.1. Installation

Importation de la première clé `gpg` pour le référentiel.

```
[diaspora@tchana ~]$ curl -sSL https://rvm.io/mpapis.asc | gpg --import -
gpg: répertoire « /home/diaspora/.gnupg » créé
gpg: nouveau fichier de configuration « /home/diaspora/.gnupg/gpg.conf » créé
gpg: Attention : les options de « /home/diaspora/.gnupg/gpg.conf » ne sont pas encore
actives cette fois
gpg: le porte-clefs « /home/diaspora/.gnupg/secring.gpg » a été créé
gpg: le porte-clefs « /home/diaspora/.gnupg/pubring.gpg » a été créé
gpg: /home/diaspora/.gnupg/trustdb.gpg : base de confiance créée
gpg: clef D39DC0E3 : clef publique « Michal Papis (RVM signing) <mpapis@gmail.com> »
importée
gpg: Quantité totale traitée : 1
gpg: importées : 1 (RSA: 1)
gpg: aucune clef de confiance ultime n'a été trouvée
[diaspora@tchana ~]$
```

Importation de la seconde clé pour le référentiel.

```
[diaspora@tchana ~]$ curl -sSL https://rvm.io/pkuczynski.asc | gpg2 --import -
gpg: clef 39499BDB : clef publique « Piotr Kuczynski <piotr.kuczynski@gmail.com> » importée
gpg: Quantité totale traitée : 1
gpg: importées : 1 (RSA: 1)
[diaspora@tchana ~]$
```

La prochaine commande installera téléchargera la dernière version stable de RVM et l'installera.



Peut prendre un certain temps.

```
[diaspora@tchana ~]$ sudo curl -sSL https://get.rvm.io | bash -s stable

Nous espérons que vous avez reçu de votre administrateur système local les consignes
traditionnelles. Généralement, elles se concentrent sur ces trois éléments :

#1) Respectez la vie privée des autres.
#2) Réfléchissez avant d'utiliser le clavier.
#3) De grands pouvoirs confèrent de grandes responsabilités.
```



```
[sudo] Mot de passe de diaspora : mot-de-passe-de-l-utilisateur-diaspora- (fghtbgh)
Downloading https://github.com/rvm/rvm/archive/1.29.10.tar.gz
Downloading https://github.com/rvm/rvm/releases/download/1.29.10/1.29.10.tar.gz.asc
gpg: Signature faite le mer. 25 mars 2020 17:58:42 EDT avec la clef RSA d'identifiant
39499BDB
gpg: Bonne signature de « Piotr Kuczynski <piotr.kuczynski@gmail.com> »
gpg: Attention : cette clef n'est pas certifiée avec une signature de confiance.
gpg: Rien n'indique que la signature appartient à son propriétaire.
Empreinte de clef principale : 7D2B AF1C F37B 13E2 069D 6956 105B D0E7 3949 9BDB
GPG verified '/home/diaspora/.rvm/archives/rvm-1.29.10.tgz'
Installing RVM to /home/diaspora/.rvm/
Adding rvm PATH line to /home/diaspora/.profile /home/diaspora/.mkshrc
/home/diaspora/.bashrc /home/diaspora/.zshrc.
Adding rvm loading line to /home/diaspora/.profile /home/diaspora/.bash_profile
/home/diaspora/.zlogin.
Installation of RVM in /home/diaspora/.rvm/ is almost complete:
```



```
* To start using RVM you need to run `source /home/diaspora/.rvm/scripts/rvm`
in all your open shell windows, in rare cases you need to reopen all shell windows.
Thanks for installing RVM ☐
Please consider donating to our open collective to help us maintain RVM.

☐ Donate: https://opencollective.com/rvm/donate

[diaspora@tchana ~]$
```

Avant de pouvoir commencer à utiliser RVM, il nous faut exécuter la commande ci-dessous.

```
[diaspora@tchana ~]$ source /home/diaspora/.rvm/scripts/rvm

[diaspora@tchana ~]$
```



La commande `source` lit et exécute des commandes à partir de `/home/diaspora/.rvm/scripts/rvm` et modifiera, en outre, le chemin (*PATH*) de l'utilisateur qui l'exécute en y insérant les chemins pour rouler RVM sans devoir spécifier les chemins complets des commandes de ce dernier.

Prérequis

On vérifie si le chemin vers la commande `rvm` a bien été insérée par l'exécution de source ci-dessus.

```
diaspora@tchana ~]$ which rvm
~/.rvm/bin/rvm
[diaspora@tchana ~]$
```

On vérifie la version de **RVM**.

```
[diaspora@tchana ~]$ rvm -v
rvm 1.29.10 (latest) by Michal Papis, Piotr Kuczynski, Wayne E. Seguin [https://rvm.io]
[diaspora@tchana ~]$
```

8. Ruby

La version de **Ruby** demandée par **diaspora*** est la version **Ruby-2.6.5**, malgré que la dernière disponible soit **Ruby-2.7.1** à la page: <https://www.ruby-lang.org/en/downloads/releases/>.



La commande suivante va installer `ruby` et certains **paquets qui sont requis**.

```
[diaspora@tchana ~]$ rvm install ruby-2.6.5

Searching for binary rubies, this might take some time.
Found remote file https://rvm_io.global.ssl.fastly.net/binaries/centos/7/x86_64/ruby-2.6.5.tar.bz2
Checking requirements for centos.
Installing requirements for centos.
Installing required packages: bison, bzip2, libtool, readline-devel, ruby, sqlite-devel, openssl-devel.
diaspora password required for 'yum install -y bison bzip2 libtool readline-devel ruby sqlite-devel openssl-devel': mot-de-passe-de-l-utilisateur-diaspora-(fghtbgh)
.....
Requirements installation successful.
ruby-2.6.5 - #configure
ruby-2.6.5 - #download
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload  Total  Spent    Left  Speed
100 17.9M  100 17.9M    0     0 1789k      0  0:00:10  0:00:10  --:--:-- 1842k
No checksum for downloaded archive, recording checksum in user configuration.
ruby-2.6.5 - #validate archive
ruby-2.6.5 - #extract
ruby-2.6.5 - #validate binary
ruby-2.6.5 - #setup
ruby-2.6.5 - #gemset created /home/diaspora/.rvm/gems/ruby-2.6.5@global
ruby-2.6.5 - #importing gemset
/home/diaspora/.rvm/gemsets/global.gems.....
ruby-2.6.5 - #generating global wrappers.....
ruby-2.6.5 - #gemset created /home/diaspora/.rvm/gems/ruby-2.6.5
ruby-2.6.5 - #importing gemsetfile /home/diaspora/.rvm/gemsets/default.gems evaluated to empty gem list
ruby-2.6.5 - #generating default wrappers.....
[diaspora@tchana ~]$
```

On vérifie le chemin de `ruby`.

```
[diaspora@tchana ~]$ which ruby
~/.rvm/rubies/ruby-2.6.5/bin/ruby
[diaspora@tchana ~]$
```

On fait de la version **2.6.5** la version **Ruby** par défaut du système.

```
[diaspora@tchana ~]$ rvm --default use ruby-2.6.5  
  
Using /home/diaspora/.rvm/gems/ruby-2.6.5  
[diaspora@tchana ~]$
```

On vérifie la version de **Ruby** pour nous assurer que les étapes ci-dessus se sont exécutées correctement:

```
[diaspora@tchana ~]$ ruby -v  
  
ruby 2.6.5p114 (2019-10-01 revision 67812) [x86_64-linux]  
[diaspora@tchana ~]$
```

L'installation des prérequis s'est déroulée correctement.

9. Instantané VirtualBox



À ce stade-ci, on peut prendre un instantané de la machine virtuelle afin de pouvoir y revenir en cas d'une future erreur de manipulation.

VII- Installation

1. Utilisateur LINUX diaspora

 L'installation se fait en tant qu'utilisateur LINUX *diaspora* sous lequel vous souhaitez exécuter **diaspora***, ce qui n'est pas en tant que root.

Si ce n'est déjà fait, on se substitue à l'utilisateur LINUX **diaspora**.

```
[root@tchana ~]# su - diaspora
Dernière connexion : mardi 15 septembre 2020 à 16:54:03 EDT sur pts/0
[diaspora@tchana ~]$
```

On vérifie.

```
[diaspora@tchana ~]$ whoami
diaspora
[diaspora@tchana ~]$
```

Si ce n'est déjà fait, on se rend dans le répertoire personnel de l'utilisateur **diaspora**.

```
[diaspora@tchana ~]$ cd
[diaspora@tchana ~]$
```

On vérifie.

```
[diaspora@tchana ~]$ pwd
/home/diaspora
[diaspora@tchana ~]$
```

2. Téléchargement de la source

On télécharge la source de **diaspora*** à l'aide de l'utilitaire `git`.

```
[diaspora@tchana ~]$ git clone -b master https://github.com/diaspora/diaspora.git
Cloning into 'diaspora'...
remote: Enumerating objects: 181700, done.
remote: Total 181700 (delta 0), reused 0 (delta 0), pack-reused 181700
Receiving objects: 100% (181700/181700), 110.41 MiB | 1.79 MiB/s, done.
Resolving deltas: 100% (139641/139641), done.
[diaspora@tchana ~]$
```

On vérifie.

```
[diaspora@tchana ~]$ ls -als
total 40
0 drwxr-xr-x  6 diaspora diaspora 197 15 sept. 17:28 .
0 drwxr-xr-x  3 root      root      22 15 sept. 15:17 ..
4 -rw-----  1 diaspora diaspora 449 15 sept. 17:24 .bash_history
4 -rw-r--r--  1 diaspora diaspora  18 31 mars  22:17 .bash_logout
4 -rw-r--r--  1 diaspora diaspora 311 15 sept. 16:56 .bash_profile
4 -rw-r--r--  1 diaspora diaspora 349 15 sept. 16:56 .bashrc
4 drwxrwxr-x 16 diaspora diaspora 4096 15 sept. 17:29 diaspora
0 drwx-----  2 diaspora diaspora  99 15 sept. 16:55 .gnupg
4 -rw-rw-r--  1 diaspora diaspora 118 15 sept. 16:56 .mkshrc
0 drwxrw----  3 diaspora diaspora  19 15 sept. 16:54 .pki
4 -rw-rw-r--  1 diaspora diaspora 236 15 sept. 16:56 .profile
4 drwxrwxr-x 25 diaspora diaspora 4096 15 sept. 16:56 .rvm
4 -rw-rw-r--  1 diaspora diaspora 118 15 sept. 16:56 .zlogin
4 -rw-rw-r--  1 diaspora diaspora 118 15 sept. 16:56 .zshrc
[diaspora@tchana ~]$
```

3. Fichiers de configuration

On se rend dans le répertoire diaspora, créé par git.

```
[diaspora@tchana ~]$ cd diaspora/
ruby-2.6.5 - #gemset created /home/diaspora/.rvm/gems/ruby-2.6.5@diaspora
ruby-2.6.5 - #generating diaspora wrappers.....
[diaspora@tchana diaspora]$
```

On copie les fichiers d'exemples vers des fichiers utilisables.

```
[diaspora@tchana diaspora]$ cp config/database.yml.example config/database.yml
[diaspora@tchana diaspora]$
```

```
[diaspora@tchana diaspora]$ cp config/diaspora.yml.example config/diaspora.yml
[diaspora@tchana diaspora]$
```

3.1. Fichier database.yml

On change le nom de l'utilisateur de la base de données pour celui de l'utilisateur LINUX **usager_diaspora**.



Nous avons enlevé l'invite afin d'entrer la commande sur une seule ligne.

```
sed -i '5 s!username: \"postgres\"!username: \"usager_diaspora\"!' config/database.yml
[diaspora@tchana diaspora]$
```

On change le mot de passe par défaut de l'utilisateur de la base de données pour celui de l'utilisateur LINUX **usager_diaspora** (*fghtbgh*) spécifié à la section [Création de la BD pour diaspora*](#) à la page [42](#).



Nous avons enlevé l'invite afin d'entrer la commande sur une seule ligne.

```
sed -i '6 s!password: \"\"!password: \"fghtbgh\"!' config/database.yml
[diaspora@tchana diaspora]$
```

On ajoute une ligne spécifiant un gabarit (*template*) après la ligne spécifiant l'encodage unicode.



Nous avons enlevé l'invite afin d'entrer la commande sur une seule ligne.

```
sed -i 's!encoding: unicode!encoding: unicode\n template: template0!' config/database.yml

[diaspورا@tchana diaspora]$
```

On vérifie.

```
[diaspورا@tchana diaspora]$ cat config/database.yml | grep -B 3 -A 1 "template: template0"

username: "usager_diaspora"
password: "fghtbgh"
encoding: unicode
template: template0

[diaspورا@tchana diaspora]$
```

3.2. Fichier diaspora.yml

3.2.1. URL

On change la ligne spécifiant l'URL par défaut de **diaspora*** pour le **FQDN** de notre **diaspora***.



Nous avons enlevé l'invite afin d'entrer la commande sur une seule ligne.

```
sed -i 's!#url: "https://example.org/"!url: "https://diaspora.micronator-dev.org/"!' config/diaspora.yml

[diaspورا@tchana diaspora]$
```

On vérifie.

```
[diaspورا@tchana diaspora]$ cat config/diaspora.yml | grep -B 1 -A1 "micronator-dev.org"

## will be hardcoded into the database.
url: "https://diaspora.micronator-dev.org/"

[diaspورا@tchana diaspora]$
```

3.2.2. Chemin du certificat

On dé-commente la ligne spécifiant le chemin du certificat de **Let's Encrypt**.



Nous avons enlevé l'invite de la commande, qui s'étant sur 2 lignes.



```
sed -i 's!#certificate_authorities: '\''/etc/pki/tls/certs/ca-bundle.crt'\''!
certificate_authorities: '\''/etc/pki/tls/certs/ca-bundle.crt'\''!' config/diaspora.yml

[diaspورا@tchana diaspora]$
```

On vérifie.



Nous avons enlevé l'invite afin d'entrer la commande, qui s'étant sur 2 lignes.

```
cat config/diaspora.yml | grep -B3 -A 1 "/etc/pki/tls/certs/ca-bundle.crt"

## For Debian, Ubuntu, Archlinux, Gentoo (package ca-certificates):
#certificate_authorities: '/etc/ssl/certs/ca-certificates.crt'
## For CentOS, Fedora:
certificate_authorities: '/etc/pki/tls/certs/ca-bundle.crt'

[diaspورا@tchana diaspora]$
```

3.2.3. Mode de fonctionnement

On change le mode fonctionnement de developement à celui de production.



Nous avons enlevé l'invite de la commande, qui s'étant sur 2 lignes.



```
sed -i 's!#rails_environment: '\''development'\''!rails_environment: '\''production'\''!'
config/diaspora.yml

[diaspora@tchana diaspora]$
```

On vérifie.

```
[diaspora@tchana diaspora]$ cat config/diaspora.yml | grep "rails_environment:"

  rails_environment: 'production'

[diaspora@tchana diaspora]$
```

3.2.4. Port

On dé-commente la ligne spécifiant le port de communication.



Nous avons enlevé l'invite et utilisé une plus petite police afin d'entrer la commande sur une seule ligne.

```
sed -i 's!#listen: '\''127.0.0.1:3000'\''!listen: '\''127.0.0.1:3000'\''!' config/diaspora.yml

[diaspora@tchana diaspora]$
```

On vérifie.

```
[diaspora@tchana diaspora]$ cat config/diaspora.yml | grep "listen:"

#listen: 'unix:tmp/diaspora.sock'
#listen: 'unix:/run/diaspora/diaspora.sock'
listen: '127.0.0.1:3000'

[diaspora@tchana diaspora]$
```

4. Bundler

Bundler fournit un environnement cohérent pour les projets **Ruby** en suivant et en installant les **gemmes** et les versions exactes nécessaires. **Bundler** est une sortie de l'enfer des dépendances et garantit que les **gemmes** dont nous avons besoin sont présentes dans le développement, la mise en scène et la production.

Pour les versions de **Bundler**, voir <https://rubygems.org/gems/bundler/versions>.

On installe le gemme **Bundler-1.17.3** qui est recommandé par **diaspora***.

```
[diaspora@tchana diaspora]$ gem install bundler -v 1.17.3

Fetching bundler-1.17.3.gem
Successfully installed bundler-1.17.3
Parsing documentation for bundler-1.17.3
Installing ri documentation for bundler-1.17.3
Done installing documentation for bundler after 5 seconds
1 gem installed

[diaspora@tchana diaspora]$
```

Installation

On lance le script de configuration de **Bundler**.

```
[diaspora@tchana diaspora]$ ./script/configure_bundler

Configuring Bundler for production environment and postgresql database.
$ bin/bundle config --local jobs 2
You are replacing the current local value of jobs, which is currently nil
$ bin/bundle config --local with postgresql
You are replacing the current local value of with, which is currently nil
$ bin/bundle config --local without test:development
You are replacing the current local value of without, which is currently nil
$ bin/bundle config --local path vendor/bundle
You are replacing the current local value of path, which is currently nil
$ bin/bundle config --local frozen true
You are replacing the current local value of frozen, which is currently nil
$ bin/bundle config --local disable_shared_gems true
You are replacing the current local value of disable_shared_gems, which is currently nil
Bundler configured! Please run 'bin/bundle install' now.
[diaspora@tchana diaspora]$
```

4.1. PG

La gemme **pg** est l'interface **Ruby** vers **PostgreSQL**.

On installe **pg**.

```
[diaspora@tchana diaspora]$ gem install pg -v '1.2.3'

Building native extensions. This could take a while...
Successfully installed pg-1.2.3
Parsing documentation for pg-1.2.3
Installing ri documentation for pg-1.2.3
Done installing documentation for pg after 2 seconds
1 gem installed
[diaspora@tchana diaspora]$
```

4.2. Installation



Peut prendre un certain temps, être patient - surtout pour **sassc**.

```
[diaspora@tchana diaspora]$ bin/bundle install

Fetching gem metadata from https://gems.diasporafoundation.org/..
Fetching gem metadata from https://rubygems.org/.....
Fetching gem metadata from https://gems.diasporafoundation.org/..
Fetching rake 12.3.3
Installing rake 12.3.3
...
Fetching sassc 2.2.1
Installing sassc 2.2.1 with native extensions
...
Using bundler 1.17.3
...
Post-install message from compass:
...
Post-install message from rails-assets-autosize:
...
Post-install message from rails-assets-blueimp-gallery:
...
Post-install message from rails-assets-jquery.ui:
...
Post-install message from rails-assets-utatti-perfect-scrollbar:
...
[diaspora@tchana diaspora]$
```

4.3. Création de la BD

```
[diaspora@tchana diaspora]$ RAILS_ENV=production bundle exec rake db:create db:migrate

Rack::SSL is enabled
Created database 'diaspora_production'
== 0 CreateSchema: migrating =====
-- create_table(:account_deletions, {:id=>:integer})
   -> 0.0110s
....
-- add_index(:aspect_memberships, [:aspect_id, :contact_id],
{:name=>:index_aspect_memberships_on_aspect_id_and_contact_id, :unique=>true})
   -> 0.0227s
....
== 20190511150503 DecryptTwoFactorSecret: migrated (0.0020s) =====
== 20190703231700 FixPendingProfilePhotos: migrating =====
== 20190703231700 FixPendingProfilePhotos: migrated (0.0025s) =====

[diaspora@tchana diaspora]$
```

4.4. Précompilation des actifs



Peut prendre un certain temps, être patient pour quelques minutes.

```
[diaspora@tchana diaspora]$ RAILS_ENV=production bin/rake assets:precompile

Rack::SSL is enabled
I, [2020-09-16T17:19:00.993288 #16133] INFO -- : Writing
/home/diaspora/diaspora/public/assets/manifest-
e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855.js
....
I, [2020-09-16T17:23:27.028142 #16133] INFO -- : Writing
/home/diaspora/diaspora/public/assets/tag_following_tpl.jst-
f2d3dfd635e4ba9212af39c013f9314636fbca0157912e6ba4b2bb6e6778bfd6.hbs.gz
[diaspora@tchana diaspora]$
```

On sort de la substitution pour retourner à l'utilisateur **root**.

```
[diaspora@tchana diaspora]$ exit

déconnexion
[root@tchana ~]#
```

5. Configuration des nouveaux services

5.1. Cibles des services



Prendre tout le contenu de l'encadré pour la commande.

```
cat > /etc/systemd/system/diaspora.target << EOL
[Unit]
Description=Diaspora social network
Wants=postgresql.service
Wants=redis-server.service
After=redis-server.service
After=postgresql.service

[Install]
WantedBy=multi-user.target
EOL
```

5.2. Service Web



Prendre tout le contenu de l'encadré pour la commande.

```
cat > /etc/systemd/system/diaspora-web.service << EOL
[Unit]
Description=Diaspora social network (unicorn)
PartOf=diaspora.target
StopWhenUnneeded=true

[Service]
User=diaspora
Environment=RAILS_ENV=production
WorkingDirectory=/home/diaspora/diaspora
PIDFile=/home/diaspora/diaspora/tmp/pids/web.pid
ExecStart=/bin/bash -lc "bin/bundle exec unicorn -c config/unicorn.rb -E production"
ExecReload=/bin/kill -USR2 $MAINPID
Restart=always

[Install]
WantedBy=diaspora.target
EOL
```

5.3. Service Sidekiq (interface admin)



Prendre tout le contenu de l'encadré pour la commande.

```
cat > /etc/systemd/system/diaspora-sidekiq.service << EOL
[Unit]
Description=Diaspora social network (sidekiq)
PartOf=diaspora.target
StopWhenUnneeded=true

[Service]
User=diaspora
Environment=RAILS_ENV=production
WorkingDirectory=/home/diaspora/diaspora
ExecStart=/bin/bash -lc "bin/bundle exec sidekiq"
Restart=always

[Install]
WantedBy=diaspora.target
EOL
```

5.4. Activation et lancement des services

5.4.1. Activation

```
[root@tchana ~]# systemctl enable diaspora.target diaspora-sidekiq.service diaspora-web.service --now
Created symlink from /etc/systemd/system/multi-user.target.wants/diaspora.target to
/etc/systemd/system/diaspora.target.
Created symlink from /etc/systemd/system/diaspora.target.wants/diaspora-sidekiq.service
to /etc/systemd/system/diaspora-sidekiq.service.
Created symlink from /etc/systemd/system/diaspora.target.wants/diaspora-web.service to
/etc/systemd/system/diaspora-web.service.
[root@tchana ~]#
```

On vérifie.

```
[root@tchana ~]# systemctl status diaspora.target

● diaspora.target - Diaspora social network
   Loaded: loaded (/etc/systemd/system/diaspora.target; enabled; vendor preset: disabled)
   Active: active since mer. 2020-09-16 17:43:57 EDT; 4min 10s ago

sept. 18 10:14:42 tchana.micronator-dev.org systemd[1]: Reached target Diaspora social n...
Hint: Some lines were ellipsized, use -l to show in full.
[root@tchana ~]#
```

```
[root@tchana ~]# systemctl status diaspora-sidekiq.service | grep Active

Active: active (running) since mer. 2020-09-16 17:43:57 EDT; 4min 19s ago
[root@tchana ~]#
```

```
[root@tchana ~]# systemctl status diaspora-web.service | grep Active

Active: active (running) since mer. 2020-09-16 17:43:57 EDT; 4min 29s ago
[root@tchana ~]#
```

Nous sommes prêt à utiliser diaspora*.

6. Instantané VirtualBox

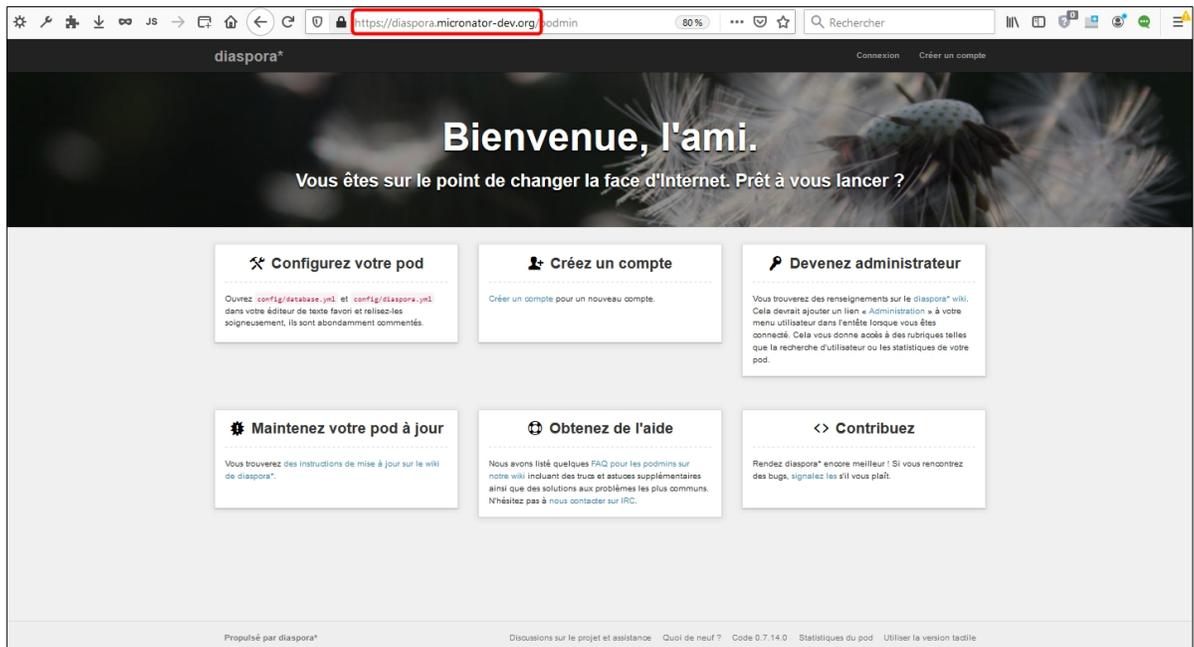


À ce stade-ci, on peut prendre un instantané de la machine virtuelle afin de pouvoir y revenir en cas d'une future erreur de manipulation.

VIII- diaspora*

1. Accès à diaspora*

On se rend à notre page Web diaspora* <https://diaspora.micronator-dev.org/>.

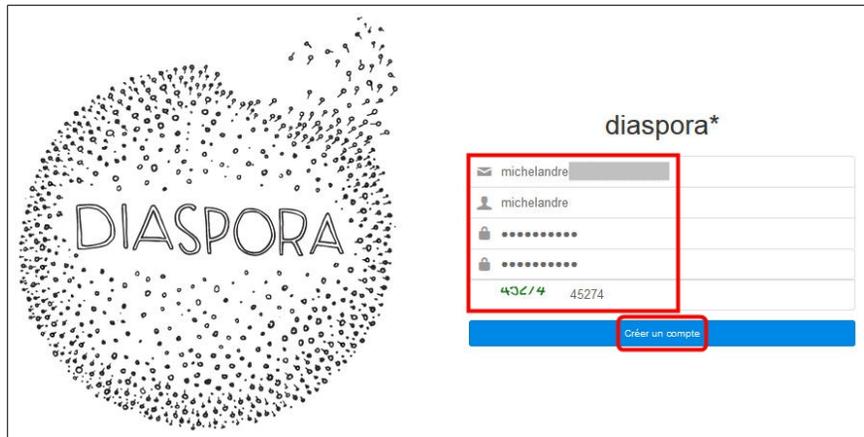


2. Création d'un administrateur

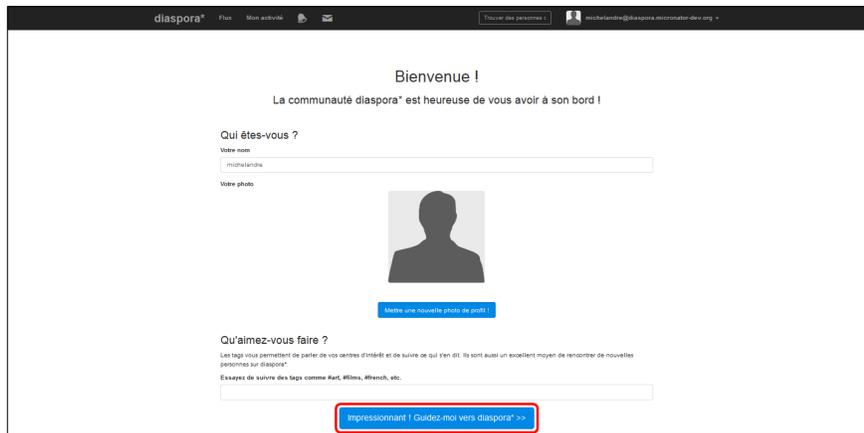
On clique **Créer un compte**.



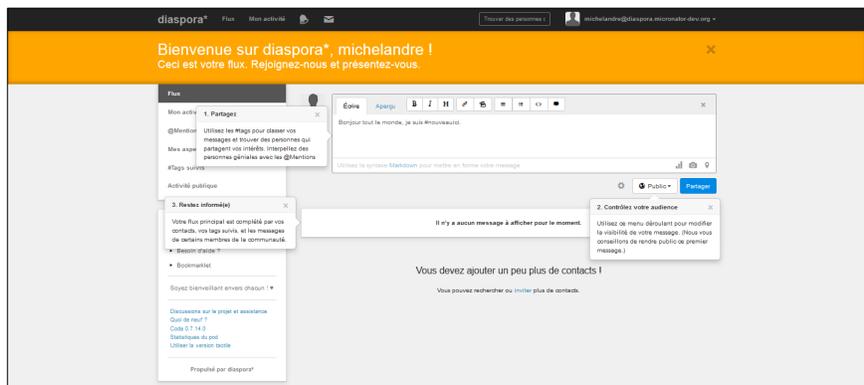
On entre les informations demandées | **Créer un compte.**



Impressionnant ! Guidez-moi vers diaspora*.



La page de bienvenue s'affiche.



! Avec la console rails, on peut définir le rôle d'administrateur.

On se substitue à l'utilisateur LINUX **diaspora**.

```
[root@tchana ~]# su - diaspora
```

```
Dernière connexion : mercredi 16 septembre 2020 à 16:45:53 EDT sur pts/0
[diaspora@tchana ~]$
```

On se rend dans le répertoire diaspora.

```
[diaspora@tchana ~]$ cd diaspora
[diaspora@tchana diaspora]$
```

On vérifie.

```
[diaspora@tchana diaspora]$ pwd
/home/diaspora/diaspora
[diaspora@tchana diaspora]$
```

On lance la console rails. (*Prend quelques secondes.*)

```
[diaspora@tchana diaspora]$ RAILS_ENV=production bundle exec rails console
Rack::SSL is enabled
Loading production environment (Rails 5.2.4.3)
2.6.5 :001 >
```

On définit l'utilisateur **michelandre**, créé précédemment dans l'interface Web de **diaspora***, comme administrateur de notre site **diaspora***.



Remplacez "**michelandre**" par l'utilisateur créé à l'étape précédente:

```
2.6.5 :001 > Role.add_admin User.where(username: "michelandre").first.person
=> #<Role id: 1, person_id: 1, name: "admin", created_at: "2020-09-16 22:16:24",
updated_at: "2020-09-16 22:16:24">
2.6.5 :002 >
```

On sort de la console rails.

```
2.6.5 :002 > exit
[diaspora@tchana diaspora]$
```

On sort de la substitution et on retourne à l'utilisateur **root**.

```
[diaspora@tchana diaspora]$ exit
déconnexion
[root@tchana ~]#
```

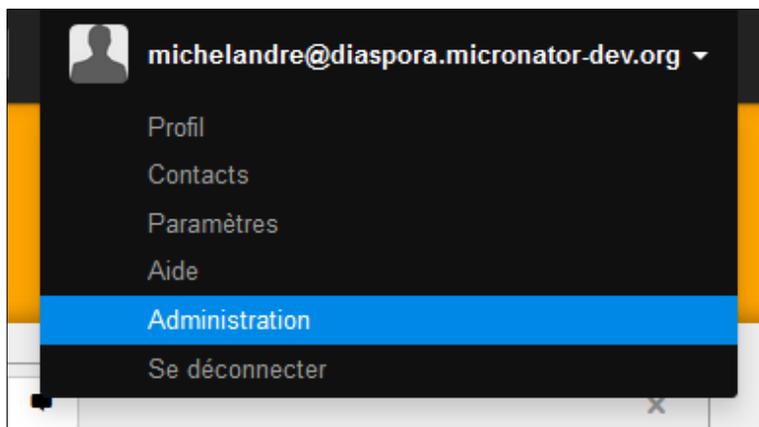
On rafraîchit la page de **diaspora***
| **Quitter la page.**

Cette page demande de confirmer sa fermeture ; des données saisies pourraient ne pas être enregistrées.

Quitter la page

Rester sur la page

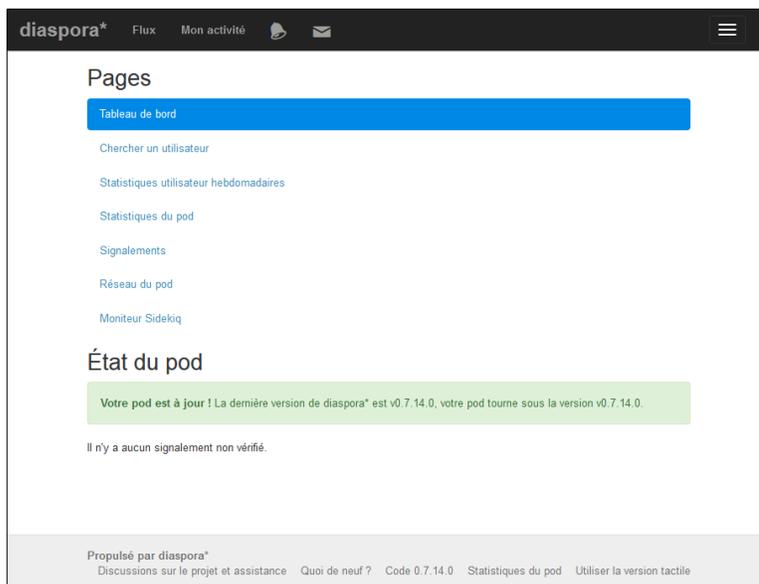
On déroule le menu de [michelandre](#)
| Administration.



Quitter la page.



La page d'administration s'affiche.



3. Réamorçage

On s'assure que tout fonctionne correctement en réamorçant le *Serveur NethServer*.

```
[root@tchana ~]# reboot
```

Après un (ré)amorçage du *Serveur NethServer*, il faut attendre une ou deux minutes avant d'accéder à notre site **diaspora***, afin de laisser le temps à clamd de faire son travail et surtout à **diaspora*** de lancer tous ses logiciels.



On vidange le cache DNS du poste de travail et celui du navigateur **Firefox**.

- Sur le poste de travail, ouvrir un écran de commandes.
- `ipconfig /flushdns`.

```
Microsoft Windows [version 6.3.9600]
(c) 2013 Microsoft Corporation. Tous droits réservés.

C:\Users\michelandre> ipconfig /flushdns

Configuration IP de Windows

Cache de résolution DNS vidé.

C:\Users\michelandre>
```

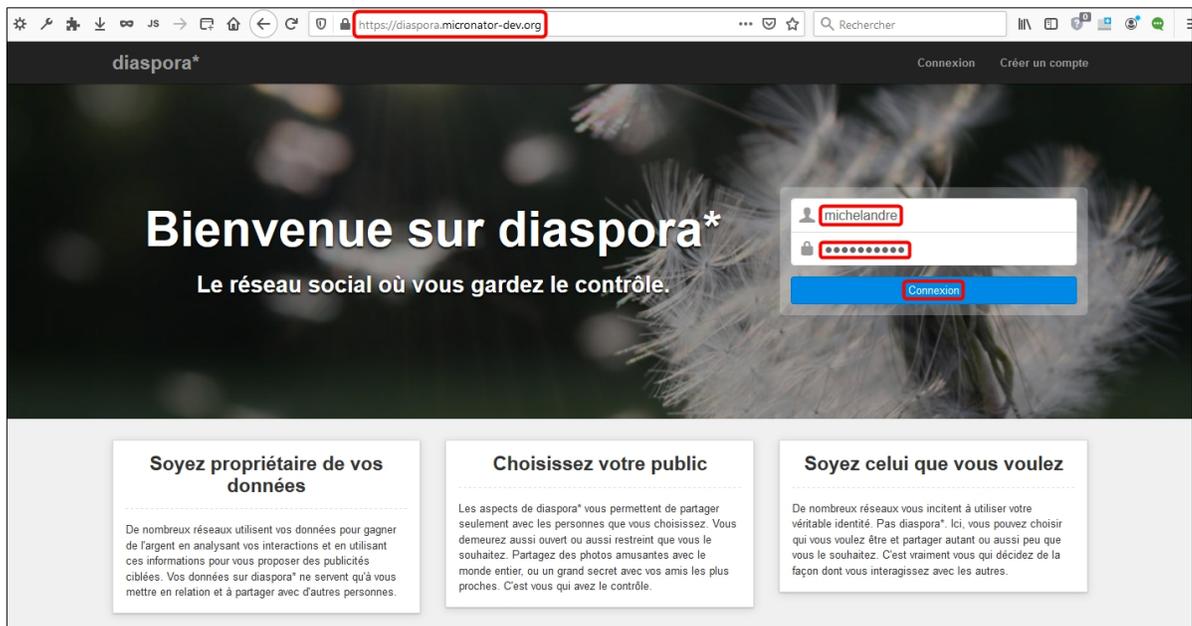
Historique | Supprimer l'histoire récent... | tout | Effacer maintenant.



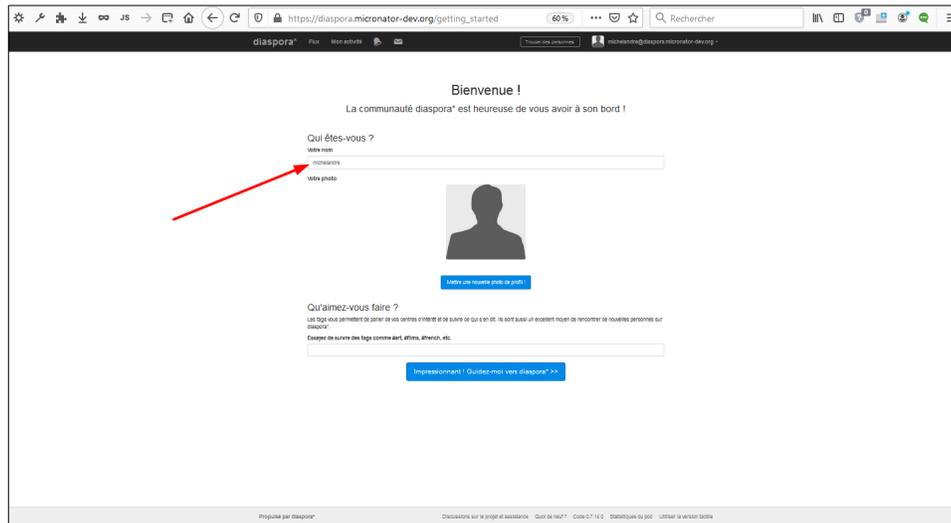
4. Vérification

On se rend à notre site diaspora*: <https://diaspora.micronator-dev.org/>.

La page de bienvenue s'affiche et on se connecte en tant qu'administrateur (*michelandre*).



La page de bienvenue s'affiche et notre nom d'utilisateur/administrateur apparaît.



5. Vérification de la configuration d'Apache



-S Affiche les paramètres tels qu'ils ont été analysés à partir du fichier de configuration (*affiche les paramètres de l'hôte virtuel*).

```
[root@tchana ~]# httpd -S

VirtualHost configuration:
*:80
    is a NameVirtualHost
    default server tchana.micronator-dev.org (/etc/httpd/conf.d/virtualhosts.conf:12)
    port 80 namevhost tchana.micronator-dev.org (/etc/httpd/conf.d/virtualhosts.conf:12)
    port 80 namevhost diaspora.micronator-dev.org (/etc/httpd/conf.d/zzz_diaspora.conf:3)
*:443
    is a NameVirtualHost
    default server tchana.micronator-dev.org (/etc/httpd/conf.d/nethserver.conf:41)
    port 443 namevhost tchana.micronator-dev.org (/etc/httpd/conf.d/nethserver.conf:41)
    port 443 namevhost tchana.micronator-dev.org (/etc/httpd/conf.d/ssl.conf:56)
    port 443 namevhost diaspora.micronator-dev.org (/etc/httpd/conf.d/zzz_diaspora.conf:9)

ServerRoot: "/etc/httpd"
Main DocumentRoot: "/var/www/html"
Main ErrorLog: "/etc/httpd/logs/error_log"
Mutex ssl-stapling: using_defaults
Mutex proxy: using_defaults
Mutex authn-socache: using_defaults
Mutex ssl-cache: using_defaults
Mutex default: dir="/run/httpd/" mechanism=default
Mutex mpm-accept: using_defaults
Mutex authdigest-opaque: using_defaults
Mutex proxy-balancer-shm: using_defaults
Mutex rewrite-map: using_defaults
Mutex authdigest-client: using_defaults
PidFile: "/run/httpd/httpd.pid"
Define: _RH_HAS_HTTPPROCOPTIONS
Define: DUMP_VHOSTS
Define: DUMP_RUN_CFG
User: name="apache" id=48
Group: name="apache" id=48
[root@tchana ~]#
```

diaspora* fonctionne correctement.

6. Désinstallation des compilateurs gcc et cpp

🚫 Le compilateur **gcc** installé sur un serveur est un risque majeur de sécurité, car un pirate pourrait s'en servir pour compiler un logiciel malveillant.

💡 Il est préférable de désinstaller **gcc**, et plus tard, si nous en avons encore besoin, il suffirait de l'installer à nouveau.

Le paquet **gcc** est toujours accompagné de son inséparable collègue **cpp**.

Nous forçons la désinstallation de ces deux **RPM**.

```
[root@tchana ~]# rpm -e --nodeps gcc gcc-c++ cpp
[root@tchana ~]#
```

On vérifie **cpp**.

```
[root@tchana ~]# rpm -qa | grep cpp
[root@tchana ~]#
```

On vérifie **gcc**.

```
[root@tchana ~]# rpm -qa | grep gcc
devtoolset-7-gcc-c++-7.3.1-5.16.el7.x86_64
devtoolset-7-gcc-7.3.1-5.16.el7.x86_64
libgcc-4.8.5-39.el7.x86_64
[root@tchana ~]#
```

Les compilateurs **gcc** et **cpp** ont été supprimés.

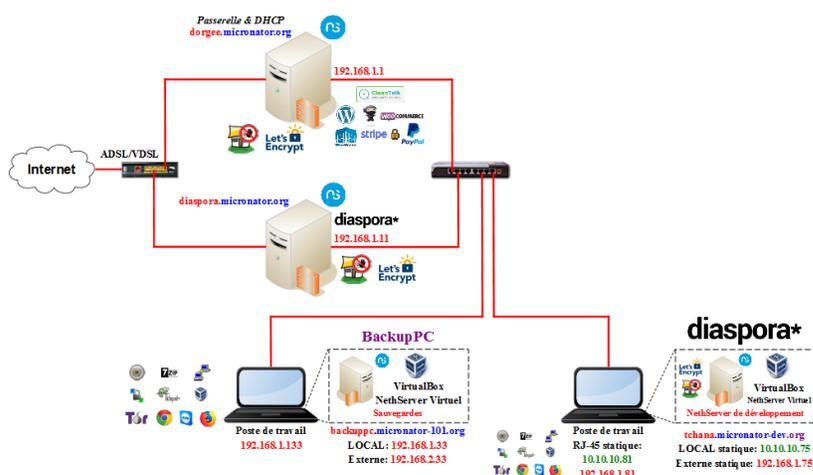
⚠️ La librairie **libgcc** est utilisée par beaucoup de logiciels; il ne faut absolument pas la désinstaller, car un de ses utilisateurs le plus important est le programme de sauvegarde **NethServer**.

7. Instantané VirtualBox

💡 À ce stade-ci, on peut prendre un instantané de la machine virtuelle afin de pouvoir y revenir en cas d'une future erreur de manipulation.

8. Serveur de Production

Une fois que vous maîtrisez tous les aspects de: **NethServer**, **Let's Encrypt**, **WordPress**, **WooCommerce**, **diaspora*** et de **BackupPC**, vous pouvez créer un réseau de *Production* incluant **WordPress**, un site de **Commerce en ligne**, un pod **diaspora***, un serveur de sauvegardes et un serveur de développement; ce qui est le but ultime que nous vous souhaitons.

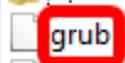
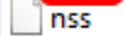


IX- Appendices

1. Écran conventionnel de démarrage

Si nous voulons voir l'écran conventionnel de démarrage, tel que ci-contre, il suffit de supprimer un seul paramètre dans le fichier de configuration de **grub**:

`/etc/default/grub`

/etc/default/	
Nom	Taille
 grub	1 KB
 nss	2 KB

```
[ OK ] Started Reload Configuration from the Real Root.
[ OK ] Reached target Initrd File System.
[ OK ] Reached target Initrd Default Target.
       Starting dracut pre-pivot and cleanup hook...
[ OK ] Started dracut pre-pivot and cleanup hook.
       Starting Cleaning Up and Shutting Down Daemons...
[ OK ] Stopped target Timers.
       Starting Plymouth switch root service...
[ OK ] Stopped Cleaning Up and Shutting Down Daemons.
[ OK ] Stopped dracut pre-pivot and cleanup hook.
[ OK ] Stopped target Initrd Default Target.
[ OK ] Stopped target Basic System.
[ OK ] Stopped target Sockets.
[ OK ] Stopped target System Initialization.
[ OK ] Stopped target Swap.
[ OK ] Stopped target Local File Systems.
[ OK ] Stopped Apply Kernel Variables.
       Stopping udev Kernel Device Manager...
[ OK ] Stopped target Paths.
[ OK ] Stopped target Slices.
[ OK ] Stopped target Remote File Systems.
[ OK ] Stopped target Remote File Systems (Pre).
[ OK ] Stopped dracut initqueue hook.
[ OK ] Stopped udev Coldplug all Devices.
[ OK ] Stopped udev Kernel Device Manager.
[ OK ] Stopped dracut pre-udev hook.
[ OK ] Stopped dracut cmdline hook.
[ OK ] Stopped Create Static Device Nodes in /dev.
[ OK ] Stopped Create list of required static device nodes for the current kernel.
[ OK ] Closed udev Control Socket.
[ OK ] Closed udev Kernel Socket.
       Starting Cleanup udev DB...
[ OK ] Started Cleanup udev DB.
[ OK ] Reached target Switch Root.
[ OK ] Started Plymouth switch root service.
       Starting Switch root...
```

1.1. Suppression du paramètre **rhgb**

Ligne originale dans le fichier `/etc/default/grub`.

```
GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=VolGroup/lv_root rd.lvm.lv=VolGroup/lv_swap
nodmraid rhgb quiet"
```

Après avoir enlevé le paramètre **rhgb**.

```
GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=VolGroup/lv_root rd.lvm.lv=VolGroup/lv_swap
nodmraid quiet"
```

On signale le changement en régénérant le fichier de configuration.

```
[root@tchana ~]# grub2-mkconfig -o /boot/grub2/grub.cfg

Generating grub configuration file ...
Found linux image: /boot/vmlinuz-3.10.0-957.5.1.el7.x86_64
Found initrd image: /boot/initramfs-3.10.0-957.5.1.el7.x86_64.img
Found linux image: /boot/vmlinuz-3.10.0-957.el7.x86_64
Found initrd image: /boot/initramfs-3.10.0-957.el7.x86_64.img
Found linux image: /boot/vmlinuz-0-rescue-8ee070fd1a7a4e8daf17a7dae9f85ac1
Found initrd image: /boot/initramfs-0-rescue-8ee070fd1a7a4e8daf17a7dae9f85ac1.img
done
[root@tchana ~]#
```



Au prochain réamorçage, le nouveau fichier `grub` sera effectif.

2. Nom du serveur dans l'écran de connexion à Webmail

À l'écran de connexion à **Webmail**, dans le champ **Serveur**, le nom du domaine principal du serveur apparaît.

On peut supprimer complètement l'affichage de cette ligne.



Utile surtout si nous avons plusieurs domaines hébergés sur le *Serveur NethServer*, car peu importe le domaine auquel nous nous connectons, c'est toujours le nom du domaine principal qui est affiché.

Pour supprimer l'affichage de cette ligne, il nous faut modifier le fichier de configuration de **PHP**:

```
/etc/roundcubemail/config.inc.php
```

et y ajouter la *ligne de configuration* suivante: `config['default_host'] = '127.0.0.1';`

Par contre, si nous modifions directement ce fichier, le prochain ré-amorçage écrasera la modification lorsque le serveur assemblera les gabarits de configuration du système.



Il nous faut donc créer un *gabarit personnalisé* et y insérer la nouvelle ligne de configuration. Ainsi, lors de l'assemblage des gabarits, le serveur incorporera le *gabarit personnalisé* au gabarit standard de configuration de **PHP**. Les directives du *gabarit personnalisé* ont préséance sur celles du gabarit standard.

Création du répertoire pour le gabarit personnalisé.

```
[root@tchana ~]# mkdir -p /etc/e-smith/templates-custom/etc/roundcubemail/config.inc.php
[root@tchana ~]#
```

On crée le fichier `91CacherNomDuServeur` et on y insère la *ligne de configuration*.



Nous avons utilisé une plus petite police pour la première ligne afin qu'elle ne déborde pas sur la deuxième.



Prendre tout le contenu de l'encadré pour la commande.

```
cat > /etc/e-smith/templates-custom/etc/roundcubemail/config.inc.php/91CacherNomDuServeur <<'EOT'
$config['default_host'] = '127.0.0.1';
EOT
```

On vérifie.



Nous avons enlevé l'invite afin que la commande puisse entrer sur une seule ligne.

```
cat /etc/e-smith/templates-custom/etc/roundcubemail/config.inc.php/91CacherNomDuServeur
$config['default_host'] = '127.0.0.1';
[root@tchana ~]#
```



Il n'y a pas de ligne vide avant `$config...` Nous en avons inséré une pour faciliter la copie de la commande.

On développe le *gabarit personnalisé*.

```
[root@tchana ~]# expand-template /etc/roundcubemail/config.inc.php
[root@tchana ~]#
```



On redémarre le démon `httpd`.

```
[root@tchana ~]# systemctl restart httpd
[root@tchana ~]#
```

On se rend à l'URL de connexion à *Webmail*:

<https://www.micronator-dev.org/webmail/>

Le domaine du serveur ne s'affiche plus.



2.1. Sauvegarde

On vérifie si le nom du répertoire `/etc/e-smith/templates-custom/etc/roundcubemail/` est déjà présent dans le fichier d'inclusion de la sauvegarde des données: `/etc/backup-data.d/custom.include`, sinon on l'insère.



Prendre tout le contenu de l'encadré pour la commande.

```
NouvelleInclusion="/etc/e-smith/templates-custom/etc/roundcubemail/"
if grep -Fxq "$NouvelleInclusion" /etc/backup-data.d/custom.include
then
    # L'entrée a été trouvée dans custom.include
    echo -e "\nLe fichier custom.include contient déjà l'entrée:\n$NouvelleInclusion \n"
else
    # L'entrée n'a pas été trouvée dans custom.include
    echo -e "$NouvelleInclusion" >> /etc/backup-data.d/custom.include
    echo -e "\nL'entrée: $NouvelleInclusion a été ajoutée\n"
fi
```

On vérifie.

```
[root@tchana ~]# cat /etc/backup-data.d/custom.include | grep roundcube
/etc/e-smith/templates-custom/etc/roundcubemail/
[root@tchana ~]#
```

Ci-dessus, il n'y a pas de ligne vide avant `/etc/e-smith/templates-custom/etc/roundcubemail/`. Nous en avons inséré une afin de faciliter la copie de la commande.

3. Langue à la console du serveur

On affiche les langues offertes à la console du serveur.

```
[root@tchana ~]# localectl list-locales | grep fr_
...
fr_CA
fr_CA.iso88591
fr_CA.utf8
...
fr_FR
fr_FR.iso88591
fr_FR.iso885915@euro
fr_FR.utf8
fr_FR@euro
...
[root@tchana ~]#
```

On ajuste la langue désirée pour l'affichage. On choisit **fr_FR.utf8**, car ce choix affectera aussi celui de la traduction pour l'interface Web. Pour l'instant, la traduction **fr_FR** est plus avancé que celle de **fr_CA**.

```
[root@tchana ~]# localectl set-locale LANG=fr_FR.utf8

[root@tchana ~]#
```



Dorénavant, la page de connexion offrira **Français (France)** comme langue par défaut au lieu de **English (United States)** si nous avons installé le module **Langue Française**.

On pourra vérifier la langue d'affichage de la ligne de commande, après le prochain redémarrage, en lançant la commande ci-dessous.

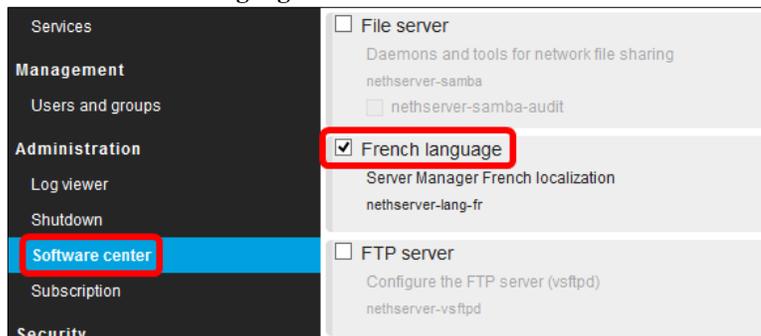
```
[root@tchana ~]# ls -als toto

ls: impossible d'accéder à toto: Aucun fichier ou dossier de ce type
[root@tchana ~]#
```

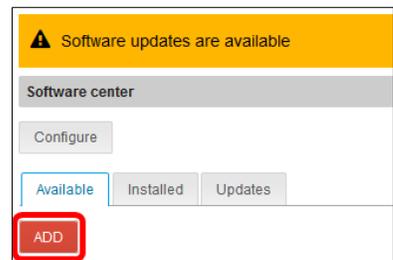
4. Langue de l'interface Web

On change la langue de l'interface.

Administration | **Software center** (peut prendre un certain temps) | on coche **French language**.



ADD.



APPLY CHANGES.

Confirm system changes

Modules to add:

- nethserver-l10n-fr

APPLY CHANGES Back

Le RPM *nethserver-lang-fr* s'installe.

Task is running ✕

52%

RPM transaction
nethserver-lang-fr-1.2.18-1.ns7.noarch Installing

Close

Reload page.

Operation completed successfully
The current page must be reloaded to update the navigation menu

Reload page

On se déconnecte/reconnecte pour activer la traduction française.

root@tchana.micronator-dev.org

Profile

Logout

- Par défaut, *Français (France)* est affiché.

- **LOGIN.**

Bienvenue sur tchana

Nom d'utilisateur
root

Mot de passe
●●●●●●●●

Langue
Français (France)

LOGIN

5. Table de mappe de clavier³

On affiche les claviers disponibles.

```
[root@tchana ~]# localectl list-keymaps | grep ca
ca
ca-eng
ca-fr-dvorak
ca-fr-legacy
ca-multi
ca-multix
dvorak-ca-fr
es-cat
ph-capewell-dvorak
ph-capewell-qwerf2k6
[root@tchana ~]#
```

³ **Table de mappe de clavier:** n.f. Disposition des touches d'un clavier.

Référence: http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=18050861#eng.

On active le clavier **ca-multi**.

```
[root@tchana ~]# localectl set-keymap ca-multi
[root@tchana ~]#
```

On vérifie.

```
[root@tchana ~]# localectl
System Locale: LANG=fr_FR.UTF-8
VC Keymap: ca-multi
X11 Layout: us
[root@tchana ~]#
```

6. Fermeture automatique de session (*session timeout*)

Référence: <http://docs.nethserver.org/en/v7/access.html#session-timeouts>.

Par défaut (à partir de *NethServer 7.5.1804*), une session de gestion du serveur se termine après 60 minutes d'inactivité (*délai d'inactivité*) et expire 8 heures après la connexion (*durée de vie de la session*).

La commande ci-dessous définit 2 heures de *délai d'inactivité* et 16 heures de *durée de vie de la session* maximale. Le temps est exprimé en secondes.

```
[root@tchana ~]# config setprop httpd-admin MaxSessionIdleTime 7200 MaxSessionLifeTime 57600
[root@tchana ~]#
```

Désactivation des délais.

```
[root@tchana ~]# config setprop httpd-admin MaxSessionIdleTime '' MaxSessionLifeTime ''
[root@tchana ~]#
```



Les nouvelles valeurs de délai affecteront les nouvelles sessions. Elles ne changent aucune session active.

7. Fuseau horaire

Pour le fuseau horaire, il existe un fichier pour **Montréal**.

```
[root@tchana ~]# ls -ls /usr/share/zoneinfo/America/ | grep Montreal
4 -rw-r--r-- 3 root root 3477 1 avril 08:27 Montreal
[root@tchana ~]#
```

7.1. Changement du fuseau horaire

On affiche le fuseau horaire actuel.

```
[root@tchana ~]# ls -l /etc/localtime
lrwxrwxrwx 1 root root 37 19 mai 23:48 /etc/localtime -> ../usr/share/zoneinfo/America/Toronto
[root@tchana ~]#
```

On change le fuseau horaire pour celui de **Montréal**.

```
[root@tchana ~]# timedatectl set-timezone America/Montreal
[root@tchana ~]#
```

On vérifie.

```
[root@tchana ~]# ls -l /etc/localtime
lrwxrwxrwx 1 root root 38 22 mai 14:02 /etc/localtime -> ../usr/share/zoneinfo/America/Montreal
[root@tchana ~]#
```

Voilà! Le fuseau horaire **Montréal** est récupéré...

8. Certificat Let's Encrypt

8.1. Description

Un certificat émis par l'autorité de certification *Let's Encrypt* vous permettra de chiffrer les connexions de votre serveur avec une clé *TLS/SSL* reconnue mondialement. Les utilisateurs pourront utiliser **https**.

Référence: https://fr.wikipedia.org/wiki/Let's_Encrypt.

Let's Encrypt est une autorité de certification (CA) lancée le 3 décembre 2015 (*Bêta Version Publique*). Cette autorité fournit des certificats gratuits **X.509** pour le protocole cryptographique **TLS** au moyen d'un mécanisme automatisé destiné à se passer de l'actuel processus complexe impliquant la création manuelle, la validation, la signature, l'installation et le renouvellement des certificats pour la sécurisation des sites Internet.

8.2. Examen du certificat

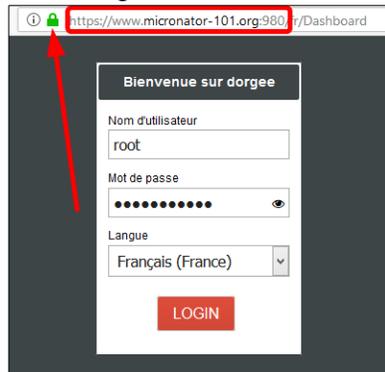


On examine le certificat émis par *Let's Encrypt* pour notre serveur **dorjee.micronator-101.org** qui est **directement branché à l'Internet**.

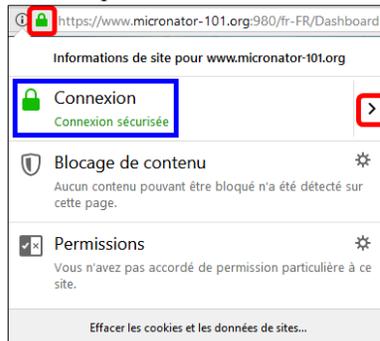
Si la demande de certificat a fonctionné sans erreur, essayez de vous connecter à la page de l'interface Web du *Serveur NethServer*. Le certificat devrait incorporer tous les noms d'hôtes que vous avez inclus et être valide pour les quatre-vingt-dix prochains jours.

On se connecte à l'interface Web: <https://www.micronator-101.org:980>.

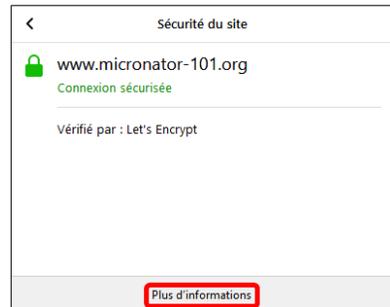
- Le cadenas est **vert**.
- On se logue.



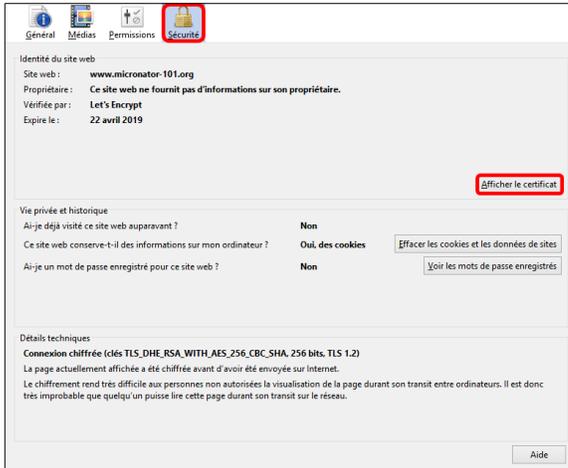
- On clique le cadenas.
- On clique l'icône >.



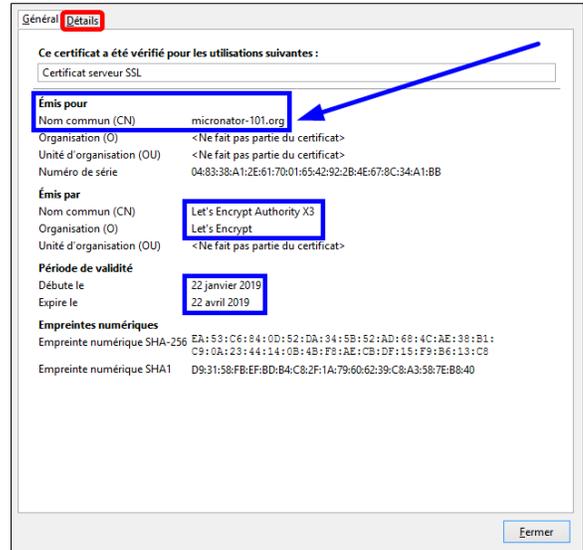
Plus d'informations.



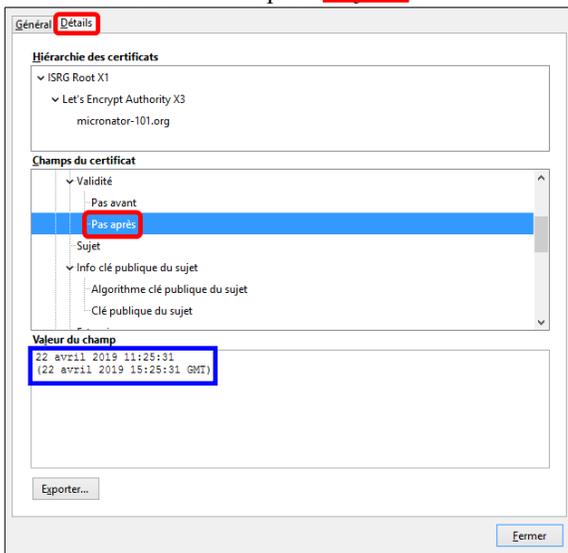
- Onglet Sécurité.
- Afficher le certificat.



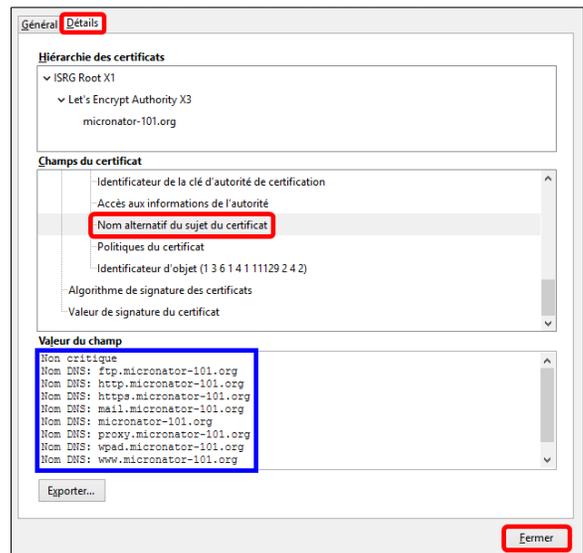
- Onglet Détails.
- Émis pour **micronator-101.org**
- Émis par **Let's Encrypt Authority X3**
- On voit la date de début et de fin.



- Validité | Pas après.
- Le certificat est valide pour 90 jours.



- Nom alternatif du sujet du certificat.
- Tous nos **CNAME** choisis lors de la demande du certificat sont affichés.
- Fermer toutes les fenêtres du certificat.



8.3. Vérification par Qualys SSLabs

Une fois que vous avez obtenu votre certificat, testez-le en vous rendant chez **Qualys SSLabs**, <https://www.ssllabs.com/ssltest/>. Soumettez le nom **FQDN** de votre domaine pour vérifier que le certificat fonctionne correctement.

Hostname: micronator-101.org | **Submit.**



Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: [Home](#) > [About](#) > [SSL Server Test](#)

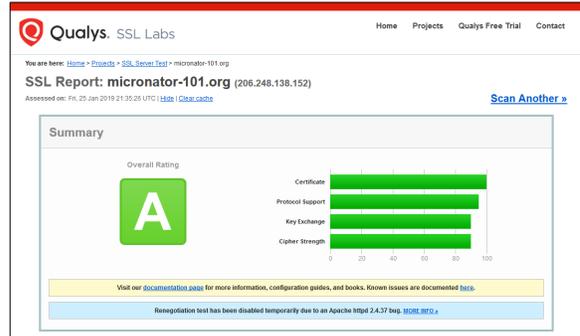
SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.

Hostname:

Do not show the results on the boards

- **Overall Rating** → **A.**
 - **Certificate** → **100%.**



9. Changement du mot de passe de root

Référence: <https://www.rootusers.com/how-to-reset-root-user-password-in-centos-rhel-7/>.

Réinitialiser le mot de passe de **root** est normalement une tâche simple si vous êtes déjà connecté avec les privilèges de **root**. Toutefois, si vous oubliez le mot de passe et devez le changer, les choses deviennent un peu plus difficiles.

Le processus a changé de la version **6** de CentOS/RHEL (*Red Hat Enterprise Linux*) à la version **7**. Auparavant, vous démarriez en **mode mono-utilisateur**, puis changez le mot de passe en tant qu'utilisateur **root**. À partir de la version **7**, les modes équivalents sont: **mode de secours** et **mode d'urgence**. Cependant, ces modes d'opération nécessitent le mot de passe de **root** avant de pouvoir faire quoi que ce soit. Cette section va vous guider dans le nouveau processus pour changer le mot de passe perdu de **root**. Cette procédure doit être exécutée directement à la console du *Serveur NethServer*; assurez-vous donc que vous y avez accès avant de commencer.



Comme pour toutes les tâches de maintenance du système, assurez-vous de disposer d'une sauvegarde/instantané du système avant de poursuivre.

Si votre système Linux est en cours d'exécution, redémarrez-le. S'il ne roule pas, démarrez-le.

Pour *CentOS 7 (NethServer)*, le menu de démarrage vous laissera **5** secondes pour sélectionner le noyau du système d'exploitation à démarrer.

Ces **5** secondes sont importantes, car elles permettent aux administrateurs de sélectionner différents noyaux ou d'éditer les paramètres du noyau existant avant le démarrage.

Dans le menu de démarrage, appuyez sur **e** (*edit*), tel qu'indiqué ci-dessous, pour modifier le noyau existant.

```
CentOS Linux (3.10.0-327.28.3.el7.x86_64) 7 (Core)
CentOS Linux (3.10.0-327.18.2.el7.x86_64) 7 (Core)
CentOS Linux (3.10.0-327.el7.x86_64) 7 (Core)
CentOS Linux (0-rescue-af7f6339749549259f3e0fc2f77d7c0d) 7 (Core)

Use the ↑ and ↓ keys to change the selection.
Press 'e' to edit the selected item, or 'c' for a command prompt.
WWW.ROOTUSERS.COM
```

Dans les options de *grub*, recherchez la ligne débutant par *linux16*, allez à la fin de celle-ci et entrez *rd.break* tel qu'indiqué ci-dessous.

rd.break

```

insmod part_msdos
insmod xfs
set root='hd0,msdos1'
if [ x$feature_platform_search_hint = xy ]; then
  search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1 --hin\
t-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1 --hint='hd0,msdos1' bf9f0973-9\
1d9-470c-828f-9de5f095b37d
else
  search --no-floppy --fs-uuid --set=root bf9f0973-91d9-470c-828f-9de5\
f095b37d
fi
linux16 /vmlinuz-3.10.0-327.28.3.el7.x86_64 root=UUID=37f82268-e090-49\
d4-aae4-e06b172fd86b ro crashkernel=auto rhgb quiet LANG=en_US.UTF-8 rd.break
initrd16 /initramfs-3.10.0-327.28.3.el7.x86_64.img

Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to
discard edits and return to the menu. Pressing Tab lists
possible completions.

```

Appuyez sur [**Ctrl**] + [**x**] pour démarrer avec ces options qui vous amèneront à l'invite *initramfs* avec un shell *root*.

```

insmod part_msdos
insmod xfs
set root='hd0,msdos1'
if [ x$feature_platform_search_hint = xy ]; then
  search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1 --hin\
t-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1 --hint='hd0,msdos1' bf9f0973-9\
1d9-470c-828f-9de5f095b37d
else
  search --no-floppy --fs-uuid --set=root bf9f0973-91d9-470c-828f-9de5\
f095b37d
fi
linux16 /vmlinuz-3.10.0-327.28.3.el7.x86_64 root=UUID=37f82268-e090-49\
d4-aae4-e06b172fd86b ro crashkernel=auto rhgb quiet LANG=en_US.UTF-8 rd.break_
initrd16 /initramfs-3.10.0-327.28.3.el7.x86_64.img

Press Ctrl-x to start. Ctrl-c for a command prompt or Escape to
discard edits and return to the menu. Pressing Tab lists
possible completions.

```

WWW.ROOTUSERS.COM

Appendices

À ce stade, le système racine de fichiers est monté en mode lecture seule (*ro*) dans le répertoire `/sysroot` et doit être remonté avec les autorisations de lecture/écriture (*rw*) pour que nous puissions réellement apporter certaines modifications. Ceci est réalisé avec la commande `mount -o remount,rw /sysroot`.

```
switch_root:/# mount -o remount,rw /sysroot
switch_root:/#
```

```
[ 2.608570] sd 2:0:0:0: [sda] Assuming drive cache: write through
Generating "/run/initramfs/rdsosreport.txt"
[ 3.803779] blk_update_request: I/O error, dev fd0, sector 0
[ 3.900804] blk_update_request: I/O error, dev fd0, sector 0

Entering emergency mode. Exit the shell to continue.
Type "journalctl" to view system logs.
You might want to save "/run/initramfs/rdsosreport.txt" to a USB stick or /boot
after mounting them and attach it to a bug report.

switch_root:/# mount -o remount,rw /sysroot
switch_root:/#
```

WWW.ROOTUSERS.COM

Une fois le système de fichiers remonté, changez-le en une prison **chroot** afin que le répertoire `/sysroot` soit utilisé comme racine du système de fichiers. Ceci est nécessaire pour que toutes les commandes que nous exécuterons se rapportent à `/sysroot`.

La commande à lancer est `chroot /sysroot`.

```
switch_root:/# chroot /sysroot
sh-4.2#
```

```
[ 2.608570] sd 2:0:0:0: [sda] Assuming drive cache: write through
Generating "/run/initramfs/rdsosreport.txt"
[ 3.803779] blk_update_request: I/O error, dev fd0, sector 0
[ 3.900804] blk_update_request: I/O error, dev fd0, sector 0

Entering emergency mode. Exit the shell to continue.
Type "journalctl" to view system logs.
You might want to save "/run/initramfs/rdsosreport.txt" to a USB stick or /boot
after mounting them and attach it to a bug report.

switch_root:/# mount -o remount,rw /sysroot
switch_root:/# chroot /sysroot
sh-4.2#
```

WWW.ROOTUSERS.COM

À partir d'ici, le mot de passe de **root** peut être réinitialisé à l'aide de la commande `passwd`.

```
sh-4.2# passwd
Changing password for user root.
New password: Nouveau-mot-de-passe-de-root
Retype new passwd: Nouveau-mot-de-passe-de-root
passwd: all authentication tokens updated successfully.
sh-4.2#
```

```
sh-4.2# passwd
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
sh-4.2#
```

Si vous n'utilisiez pas **SELinux**, vous pourriez redémarrer à ce stade et tout irait bien. Cependant, par défaut, **CentOS/RHEL-7** active **SELinux**. Nous devons donc corriger le contexte du fichier `/etc/shadow`. En effet, lorsque la commande `passwd` est exécutée, elle crée un nouveau fichier `/etc/shadow`. **SELinux** n'étant pas en cours d'exécution dans ce mode, le fichier est créé sans aucun contexte **SELinux**, ce qui peut entraîner des problèmes lors du redémarrage.

On crée le fichier `/.autorelabel` à l'aide de `touch`.

```
sh-4.2# touch /.autorelabel
sh-4.2#
```



La création de ce fichier effectuera automatiquement un ré-étiquetage de tous les fichiers au prochain démarrage. Notez que ceci peut prendre un certain temps en fonction de la quantité de fichiers que vous avez. Peut prendre environ 2 minutes pour un serveur **CentOS-7** ordinaire.

On quitte l'environnement *chroot*.

```
sh-4.2# exit
exit
sh-4.2#
```

On quitte le *shell* racine *initramfs* (peut prendre un certain temps, être patient...). Le serveur s'amorce.

```
sh-4.2# exit
logout
...
```

9.1. Vérification

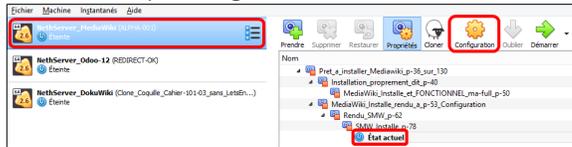
À la console du serveur, vous devriez pouvoir vous connecter avec le nouveau mot de passe que vous avez créé.

10. ERROR Failed to send host log message

Cette erreur s'affiche seulement lors de l'amorçage d'un serveur roulant sous *VirtualBox*.

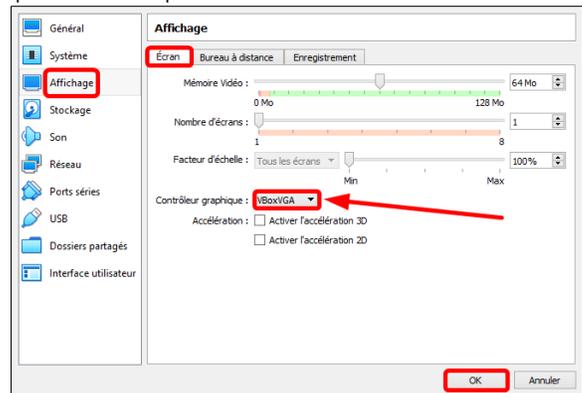
```
[ 22.345495] [drm:umw_host_log [umwgfx]] *ERROR* Failed to send host log messa
ge.
[ 22.434594] [drm:umw_host_log [umwgfx]] *ERROR* Failed to send host log messa
ge.
```

- On arrête le *Serveur NethServer*.
- À l'écran *VirtualBox*, on sélectionne la machine | **État actuel** | **Configuration**.



Au retour, on amorce le **Serveur NethServer** et le message ne s'affichera plus.

Affichage | onglet **Écran** | **Contrôleur graphique** | **VboxVGA** | **OK**.



X- Introduction à l'éditeur vi

1. Référence

<http://www.iro.umontreal.ca/~dift3830/vi.html>. (Dernière consultation, le 30 mai 2016. Novembre 2018, ce lien n'est plus fonctionnel.)

vi est un éditeur de texte très puissant. Sa convivialité par contre lui fait défaut. Ceci dit, il est toujours utile d'en connaître les rudiments, car son omniprésence est presque garantie sur les systèmes modernes.

La documentation de **vi** étant très abondante, on se limitera pour cette démo aux commandes les plus usuelles.

Tout d'abord l'invocation. On peut invoquer **vi** à partir du **shell** de plusieurs façons dont voici quelques-unes:

- **vi**: ouvre **vi** avec un contenu vide.
- **vi nom_de_fichier**: ouvre un fichier et l'affiche à l'écran.
- **vi +nom_de_fichier**: ouvre un fichier et positionne le curseur à la fin de celui-ci.

Dès son invocation, **vi** se met en **mode commande**, dans ce mode il est possible d'entrer les commandes qui seront vues plus bas. Si on tape une commande susceptible de modifier un texte (*insertion d'un caractère par exemple*), **vi** bascule en **mode édition**; dans ce mode tous caractère tapé sera considéré comme faisant partie du texte, tandis que les caractères saisis en **mode commande**, seront eux interprétés comme étant des commandes et ne seront jamais rajoutés au texte.

Afin de basculer du **mode édition** au **mode commande** il suffit de presser la touche [Échap].

Nous allons commencer par invoquer **vi** à partir du **shell** en tapant:

```
vi
```

Ce qui devrait donner l'affichage ci-contre:

```

VIM - Vi IMproved
      version 7.1.12
    by Bram Moolenaar et al.
 Modified by <bugzilla@redhat.com>
 Vim is open source and freely distributable

  Help poor children in Uganda!
type :help iccf<Enter>      for information

type :q<Enter>              to exit
type :help<Enter> or <F1>   for on-line help
type :help version7<Enter> for version info

                                0,0-1      ALL

```

vi est déjà en **mode commande**, pour le faire passer en **mode édition**, on tape la commande **i** (*insert*) qui nous permettra d'insérer du texte.

Après avoir tapé le texte suivant:

```
vi est un éditeur de texte très
utile pour la communauté des
administrateurs.
```

On obtiendra l'affichage ci-contre.

Après cela, on pourrait passer en **mode commande** par simple pression sur la touche [Échap].

```

vi est un editeur de texte tres
utile pour la communaute des
administrateurs.
-- INSERT --

                                4,17      ALL

```

Introduction à l'éditeur vi

Une fois en **mode commande**, on voudrait par exemple, éliminer la ligne blanche qui se trouve juste après la première. Pour cela on positionne le curseur à la hauteur de la 2e ligne et on tape **dd**.

Ceci aura pour effet de supprimer la ligne.

Les commandes abondent dans **vi**, c'est pour cette raison qu'on n'en citera que quelques-unes.

Si on est satisfait, il ne nous reste plus qu'à sauvegarder le document sous le nom **texte1.txt** à l'aide de la commande suivante:

```
:w texte1.txt
```

(Pour les sauvegardes ultérieures, il n'est pas nécessaire d'ajouter le nom de fichier).

Afin de quitter **vi** il suffit de taper la commande:

```
:q texte1.txt
```

Commande	Effets
i (insert)	Insère un texte au curseur
I	Insère au début de la ligne
a (append)	Insère après le curseur
A	Insère à la fin de la ligne
Les flèches	Pour les déplacements
Ctrl-F (forward)	Défiler d'un écran vers le bas
Ctrl-B (backward)	Défiler d'un écran vers le haut
nG (goto)	Va à la nième ligne dans le texte
G	Va à la fin du texte
x	Effacer le caractère courant
dd	Effacer la ligne courante
D	Effacer depuis la position du curseur jusqu'à la fin de la ligne
db (DeleteBegining)	Effacer depuis la position courante jusqu'au début de la ligne
/chaîne	Rechercher la chaîne 'chaîne' dans le texte, on peut taper 'n' (<u>n</u> ext) pour voir l'occurrence suivante
:w fichier	Copie le texte courant sur le disque sous le nom fichier
:wq (write & quit)	Écrit le fichier sur le disque et quitte vi.
:q!	Quitter sans sauvegarder.
:set nu	Affiche le numérotage des lignes.



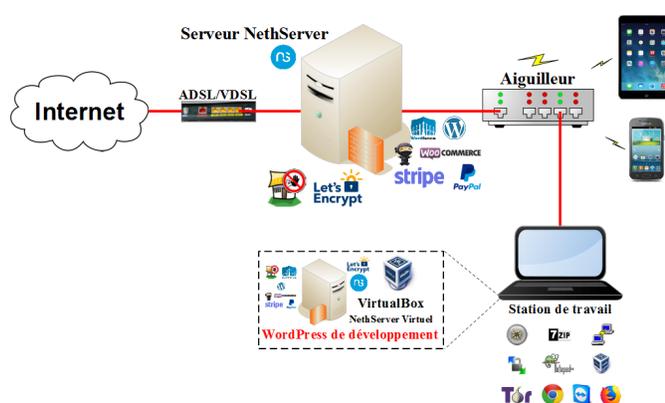
Victoire totale, hissons la bannière de la victoire.

XI- Micronator.org

1. Cours NethServer-101 - NethServer & Commerce en ligne

1.1. But final

Après avoir suivi le "Cours NethServer-101", vous posséderez un site de **Commerce en ligne** fiable et hautement sécuritaire. De plus, vous pourrez utiliser un clone de votre site, sur un *Serveur NethServer* virtuel sur votre poste de travail, pour tester de nouvelles extensions et applications sans compromettre la sécurité ou l'intégrité de votre site en ligne.



1.2. Cahiers

Le Cours **NethServer-101**, se voulant une base solide pour la création d'un site de **Commerce en ligne**, il comprend plusieurs cahiers:

- *Cahier-01*: Les bases de Linux.
- *Cahier-02*: Installation et configuration des logiciels prérequis sur le poste de travail.
- *Cahier-03*: Création d'un *Serveur NethServer* virtuel.
- *Cahier-04*: *Serveur NethServer* LOCAL & Let's Encrypt.
- *Cahier-05*: Abonnement à un *FAI*, installation d'un modem *VDSL*, obtention d'un domaine *FQDN*⁴ et installation d'un *Serveur NethServer* sur une quincaillerie physique.
- *Cahier-06*: Installation de *WordPress*.
- *Cahier-07*: Installation de l'extension de sécurité *Wordfence*.
- *Cahier-08*: Installation de l'extension de vente en ligne *WooCommerce* et création de comptes chez *Stripe* et *PayPal* pour les paiements en ligne.
- *Cahier-09*: Sauvegarde/restauration ou migration d'un site avec l'extension *Duplicator*.
- *Cahier-10*: Serveur mandataire inversé.
- *Cahier-11*: Sauvegarde/restauration avec *BackupPC*.
- *Cahier-12*: *WordPress & CleanTalk*.

⁴ **FQDN**: Dans le *DNS*, un **Fully Qualified Domain Name** (*FQDN*, ou *nom de domaine complètement qualifié*) est un nom de domaine qui révèle la position absolue d'un nœud dans l'arborescence *DNS* en indiquant tous les domaines de niveau supérieur jusqu'à la racine. On parle également de domaine absolu, par opposition aux domaines relatifs. Par convention, le *FQDN* est ponctué par un point final.

Référence: https://fr.wikipedia.org/wiki/Fully_qualified_domain_name.

1.3. Logiciels



Tous les logiciels nécessaires sont du domaine public ou LIBRE sous licence *GPL*; ils ne coûtent pas un sous. Le seul achat nécessaire est l'obtention d'un nom de domaine au prix initial de \$15 CAD et son renouvellement annuel d'environ \$30 CAD.

2. Cours NethServer-201 - NethServer & Applications

Cahier-01: Dolibarr

Cahier-02: Odoo-12

Cahier-03: MediaWiki

Cahier-04: DokuWiki

Cahier-05: Moodle

Cahier-06: Proxmox VE

Cahier-07: Flectra

Cahier-08: Self Service Password

Cahier-09: Forum NodeBB

Cahier-10: Forum Discourse

Cahier-11: diaspora*

3. Cours NethServer-301 - NethServer & Active Directory

Cahier-01: RSAT

Cahier-02: Active Directory

Cahier-03: SSP & Active Directory

Cahier-04: Jonction de stations à AD

4. Cours NethServer-401 - Surveillance Zabbix

Cahier-01: Zabbix - Installation

Cahier-02: Zabbix - Alertes

Cahier-03: Zabbix - Agents

Cahier-04: Zabbix & Émulateur ELM327

Cahier-05: Zabbix & Mise à niveau

5. Cours NethServer-501 - Service d'assistance Zammad

Cahier-01: Zammad - Installation

Cahier-02: Zammad - Création de billets

Cahier-03: Zammad - Sauvegarde & restauration

6. Cours NethServer-601 - Communication d'équipe Mattermost

Cahier-01: Mattermost - Installation

Cahier-02: Mattermost - Mise à niveau

Cahier-03: Mattermost - Récupération après désastre

7. Commentaires et suggestions

RF-232 apprécie grandement échanger avec ses internautes. Vos commentaires et suggestions sont indispensables à l'amélioration de la documentation et du site micronator.org.

N'hésitez pas à nous transmettre vos commentaires et à nous signaler tout problème d'ordre technique que vous avez rencontré ou n'arrivez pas à résoudre. Tous vos commentaires seront pris en considération et nous vous promettons une réponse dans les plus brefs délais.



Brancher les aînés,
encourager l'Informatique LIBRE
et la diffusion du savoir



8. Boutique Micronator

Nous sommes heureux de vous présenter notre boutique en ligne dans laquelle vous trouverez certains de nos produits qui ne sont pas disponibles sur notre site principal. Nous vous laissons le plaisir de la parcourir:

<https://www.micronator.org/affaires/boutique/>.

8.1. Communications sécuritaires chiffrées SSL/TLS

Les communications avec **Stripe** et **PayPal** sont effectuées au moyen d'un **certificat SSL/TLS de 2048 bits** émis par l'Autorité de Certification **Let's Encrypt**.

Faites vos achats en toute confiance, remplissez votre panier et réglez votre commande avec la carte bancaire de votre choix: **MasterCard**, **Visa**, **Discover**, **American Express**, etc.

Stripe

Le montant de votre facture est envoyé directement à **Stripe** qui s'occupe de tout. Les données de votre carte ne sont pas utilisées sur notre site. Les paiements sont sécurisés par le système **Stripe**. [Cliquez ici](#) pour voir les étapes de paiements; celles-ci sont sécurisées par le système **Stripe**.

PayPal

Il n'est pas nécessaire d'ouvrir un compte **PayPal**. Vous pouvez choisir la carte bancaire que vous désirez utiliser. [Cliquez ici](#) pour voir les étapes de paiements; celles-ci sont sécurisées par le système **PayPal**.



9. Médias sociaux



Twitter: <https://twitter.com/TuteurW>.



Facebook: <https://www.facebook.com/micronator>.

Crédits

© 2020 RF-232

Auteur: **Michel-André Robillard CLP**

Remerciement: **Tous les contributeurs GNU/GPL.**

Intégré par: **Michel-André Robillard CLP**

Contact: **michelandre at micronator.org**

Répertoire de ce document: E:\000_DocPourRF232_general\RF-232_NethServer-201-11_Diaspora\RF-232_Cours-201-11_Diaspora_2020-09-18_13h14.odt

Historique des modifications:

<i>Version</i>	<i>Date</i>	<i>Commentaire</i>	<i>Auteur</i>
RC-001	2020-09-13	Début.	M.-A. Robillard

Index

1		
1.1.1.1.....	17	
10.10.10.0/24.....	12	
10.10.10.75.....	18	
10.10.10.81.....	10	
127.0.0.1.....	67	
192.168.1.1.....	17	
192.168.1.75.....	18, 23	
2		
25GB recommandé.....	11	
3		
32 ou 64 bits.....	35	
8		
8 GB.....	11	
8.8.8.8.....	17	
9		
91CacherNomDuServeur.....	67	
A		
a (append).....	81	
À savoir.....	10	
account-provider-test.....	15	
acme.sh -v.....	30	
Active Directory.....	83	
Administration Software center.....	69	
Adresse IP.....	18	
Afficher le certificat.....	73	
Alias.....	14, 23	
alias du domaine.....	23	
Alias du serveur.....	14	
America/Montreal.....	71	
American Express.....	84	
Appendices.....	66	
APPLY CHANGES.....	70	
ASCII.....	9	
astuce.....	9	
Authority X3.....	73	
Autoriser depuis.....	25	
Autorité de Certification Let's Encrypt.....	84	
Avertissement.....	2	
B		
BackupPC.....	65	
BD de ClamAV.....	20	
Bêta Version Publique.....	72	
bleu.....	9	
Boutique Micronator.....	84	
Brancher les aînés.....	84	
But de ce cahier.....	8	
C		
ca-multi.....	71	
cache DNS.....	13, 63	
Cahier-01.....	82	
Cahier-02.....	82	
Cahier-03.....	82	
Cahier-04.....	14, 16, 82	
Cahier-05.....	82	
Cahier-06.....	82	
Cahier-07.....	82	
Cahier-08.....	82	
Cahier-09.....	82	
Cahier-10.....	82	
Cahier-11.....	82	
Cahier-12.....	82	
caractères en magenta.....	9	
CentOS.....	10	
CentOS 7 - x86 64.....	36	
CentOS-7.....	36	
CentOS-7.8.2003.....	10	
cert.pem.....	32	
certificat de TEST.....	31	
Certificat du serveur.....	14	
Certificat Let's Encrypt.....	72	
certificat officiel.....	32	
certificat par défaut.....	14	
certificat SSL/TLS.....	84	
chain.pem.....	33	
Changement du fuseau horaire.....	71	
chroot.....	77	
Clac (clic droit).....	11	
ClamAV.....	13, 19	
Clamscan.....	20	
CNAME.....	11	
Commentaire.....	85	
Commerce en ligne.....	82	
Config avant dev.org.....	22	
configuration PKI.....	30	
Connexion.....	12	
connexion sécurisée.....	33	
console psql.....	40	
Contrôleur graphique.....	79	
Conventions.....	9	
Conventions de ce document.....	9	
cookies.....	12	
Cours NethServer-101.....	82	
Cours NethServer-201.....	83	
Cours NethServer-301.....	83	
Cours NethServer-401.....	83	
Cours NethServer-501.....	83	
Cours NethServer-601.....	83	
CR.....	9	
Crédits.....	85	
Ctrl-B.....	81	
Ctrl-F.....	81	
custom.include.....	33	
D		
db.....	81	
dd.....	81	
Demande d'un certificat de test.....	31	
Description générale.....	6	
Désinstallation des compilateurs.....	65	
DHCP.....	10	
diaspora*.....	83	
Discover.....	84	
DKIM.....	24	
DNS et Domaines.....	14	
DokuWiki.....	83	
Dolibarr.....	83	
domain admins.....	20	
domaine absolu.....	82	
domaine public ou LIBRE.....	83	
dorgee.micronator.org.....	10	
dump.....	15	
E		
Écran conventionnel.....	66	
écran de connexion à Webmail.....	67	
écran du gestionnaire.....	12	
Éditeur de texte.....	10	
éditeur vi.....	80	
EmailAddress.....	30	
Émis par.....	73	
Émis pour.....	73	
Entrées DNS.....	23	
EPEL.....	36	

Index

étape.....	9	instantanés VirtualBox.....	21	mode commande.....	80
Éthernet Statut.....	11	interface Web.....	12	mode d'urgence.....	75
Examen du certificat.....	72	interface Web Nethserver.....	12	mode de secours.....	75
expand-template.....	67	ipconfig /flushdns.....	13, 63	mode édition.....	80
F		J		mode mono-utilisateur.....	75
Facebook.....	84	Javascript.....	12	Modification de la passerelle.....	22
FAI.....	82	Jonction de stations à AD.....	83	Moodle.....	83
Fail2ban.....	13, 19	L		mot de passe de root.....	75
fichier hosts.....	11	LANG=fr_FR.UTF-8.....	71	mount -o.....	77
Fichier hosts.....	11	Langue à la console.....	69	N	
FileZilla.....	15	Langue de l'interface Web.....	69	nethserver-lang-fr.....	70
Filtre.....	25	LDAP local.....	15	nG.....	81
FILTRE.....	25	Let's Encrypt.....	14	Nom alternatif.....	73
filtre d'autorisation.....	25	LF.....	9	Nom du serveur.....	16
Firefox.....	13, 63	Ligne de commande.....	12	non vérifié.....	9
Flectra.....	83	Linux CentOS.....	10	NON-RESPONSABILITÉ.....	2
Forum Discourse.....	83	linux 16.....	76	note.....	9
Forum NodeBB.....	83	list-keymaps.....	70	Notepad++.....	10
fournisseur de comptes.....	15	list-locales.....	69	Notes au lecteur.....	9
Fournisseur des comptes.....	15	liste blanche.....	24	Notification.....	17
FQDN4.....	82	Liste blanche.....	24, 25	Nouvelle autorisation depuis.....	25
fr_CA.....	69	localectl.....	69	Nouvelle interface logique.....	16, 17
fr_FR.utf8.....	69	Locality.....	30	NouvelleInclusion.....	68
Français (France).....	69, 70	localtime.....	72	O	
French language.....	69	Logiciels.....	83	Odoo-12.....	83
freshclam.....	20	LOGIN.....	70	orange.....	9
FTP.....	15	M		Organization.....	30
Fully Qualified Domain Name.....	82	magenta.....	9	OrganizationalUnitName.....	30
Fuseau horaire.....	71	Manipulation.....	9	P	
G		mappe de clavier.....	70	paramètre rhgb.....	66
GPL.....	83	Marche à suivre.....	8	passerelle.....	10
grub.....	76	MasterCard.....	84	passwd.....	78
grub2-mkconfig.....	66	Mattermost - Installation.....	83	PATH.....	30
H		Mattermost - Mise à niveau.....	83	PayPal.....	82, 84
host log message.....	79	Mattermost - Récupération après		PDF.....	9
http://10.10.10.75:980.....	12	désastre.....	83	pg_hba.conf.....	40, 41
I		MaxSessionIdleTime.....	71	pgdg12.....	37
i (insert).....	81	MaxSessionLifeTime.....	71	Plus d'informations.....	72
ifconfig.....	18	MD5.....	40	Politique TLS.....	13
initdb.....	39	Médias sociaux.....	84	poste de travail.....	11
Initialisation.....	39	MediaWiki.....	83	Poste de travail.....	10
initramfs.....	76	Messagerie.....	22	PostgreSQL-11.....	40
insert.....	80	Messagerie électronique.....	16, 23	PostgreSQL-12.....	35, 37
Installation d'un Serveur NethServer		micronator-101.ddns.net.....	14	postgresql-12-setup.....	39
.....	11	micronator.org.....	84	postgresql-12.service.....	39
Instantané VirtualBox.....	21, 27	Micronator.org.....	82	postgresql12.....	37
		Mise à jour du Serveur NethServer		postgresql12-server.....	37
		12	Premiers pas.....	40

Index

Préparation de l'environnement de travail.....	11	Serveur NethServer de développement.....	10	Wordfence.....	82
Primary DSN.....	17	session PuTTY.....	18	WordPress.....	82
privkey.pem.....	33	session timeout.....	71	X	
procédure.....	9	shell.....	80	X.509.....	72
protect = 1.....	39	SPF.....	24	X11 Layout.....	71
Protection de pgdg12.....	39	SSH et paramètres d'accès à distance.....	13	Y	
Protection du référentiel.....	38	SSL/TLS.....	84	yum install -y.....	36
protocole cryptographique TLS.....	72	SSP & Active Directory.....	83	yum-plugin-protectbase.....	38
Proxmox VE.....	83	State.....	30	Z	
PuTTY.....	18	Stripe.....	82, 84	Zabbix - Agents.....	83
Q		SubjectAltName.....	30	Zabbix - Alertes.....	83
Qualys SSL Labs.....	74	sujet du certificat.....	73	Zabbix - Installation.....	83
R		Supprimer l'historique récent.....	13, 63	Zabbix & Émulateur ELM327.....	83
rd.break.....	76	T		Zabbix & Mise à niveau.....	83
recommandation.....	9	témoins.....	12	Zammad - Création de billets.....	83
référence Internet.....	9	TLS policy.....	13	Zammad - Installation.....	83
Référentiel pgdg12.....	35	TLS/SSL.....	33	Zammad - Sauvegarde & restauration.....	83
Régestraire de domaines.....	29	touch.....	78	-	
rejeter les courriels.....	25	Twitter.....	84	--ca-file.....	31, 32
Reload page.....	70	U		--cert-file.....	31, 32
requête HTML.....	23	uname -p.....	35	--debug.....	31
Requête HTML.....	22	Utilisateur Linux.....	41	--dns dns_cf.....	31, 32
Réseau.....	16	Utilisateur michelandre.....	20	--issue.....	31, 32
réseau Externe.....	17	Utilisateurs.....	20	--key-file.....	31, 32
RF-232.....	84	V		--reloadcmd.....	31, 32
rhgb.....	66	Validité Pas après.....	73	--test.....	31
rouge.....	9	VboxVGA.....	79	-d.....	31, 32
roundcubemail.....	68	VC Keymap.....	71	:	
rpm -e --nodeps.....	65	VDSL.....	82	:q!.....	81
rpm -Uvh.....	12	Vérification des redirections.....	24	:set nu.....	81
RSAT.....	83	Version 6.0.4 r128413.....	10	:w fichier.....	81
S		Version CentOS.....	35	:wq.....	81
Sauvegarde.....	33	vi.....	80	[
Sauvegarde des configurations.....	27	vi +nom_de_fichier.....	80	['default_host'].....	67
Sauvegardes (données).....	17	vi nom_de_fichier.....	80	[Ctrl] + [x].....	76
Scanner Antivirus.....	20	Victoire.....	81	[Échap].....	80
script acme.sh.....	30	vim.....	10	[pgdg12].....	39
Secondary DNS.....	17	VirtualBox.....	10	/	
Sécurité SSH.....	13	Visa.....	84	/.autorelabel.....	78
sed.....	40	W		/boot/grub2/grub.cfg.....	66
Self Service Password.....	83	Windows-8.1.....	10		
SELinux.....	78	WinSCP.....	15		
Serveur de Production.....	65	WooCommerce.....	82		
serveur DNS.....	11				
Serveur DNS.....	17, 22				
Serveur FTP.....	15				
Serveur NethServer.....	10				

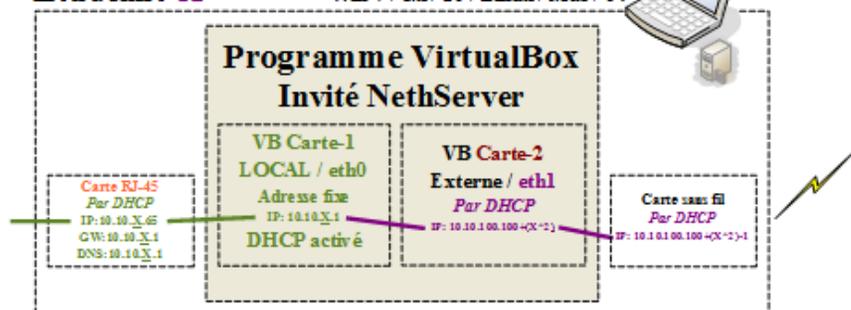
Index

/chaîne.....	81	/etc/shadow.....	78	~	
/etc/centos-release.....	35	/root/.acme.sh/.....	33	~/.acme.sh.....	30
/etc/default/grub.....	66	/sysroot.....	77		
/etc/localtime.....	72	/var/lib/pgsql.....	44		

Cours NethServer-101

Étudiant-X

Win-7 / 8.x / 10 / Linux / Mac / 64



À lire avant l'entrée en classe - lien: [Cours Linux-101](#)

Ce cahier est une adaptation de la page <http://www.linux-france.org/article/ksfcafr/> qui est destinée aux néophytes complets, à ceux qui ne connaissent de l'informatique que l'orthographe du nom et qui désirent utiliser les possibilités offertes par Linux.

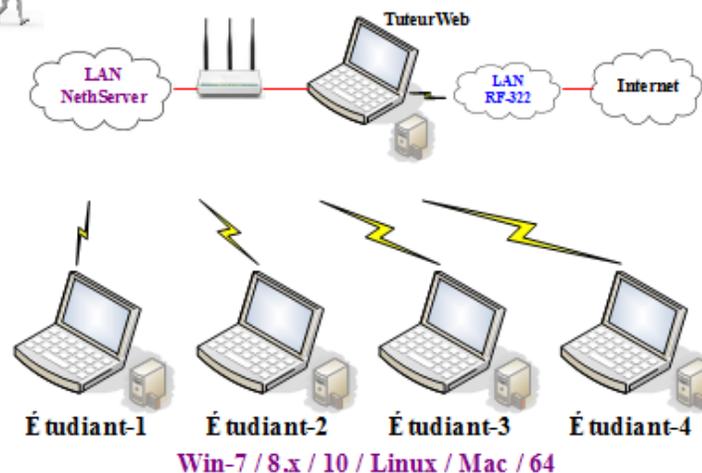
Autre référence:

<http://free-electrons.com/doc/legacy/command-line/unix/linux/introduction/fr.pdf>

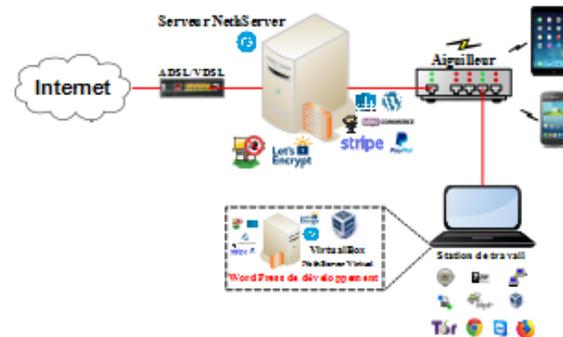
Cahiers de cours

- Cahier-01:** Les bases de Linux.
- Cahier-02:** Installation et configuration des logiciels prérequis sur le poste de travail.
- Cahier-03:** Création d'un **Serveur NethServer** virtuel.
- Cahier-04:** **Serveur NethServer** LOCAL & Let's Encrypt.
- Cahier-05:** Abonnement à un FAI, installation d'un modem VDSL, obtention d'un domaine FQDN et installation d'un **Serveur NethServer** sur une quincaille physique.
- Cahier-06:** Installation de **WordPress**.
- Cahier-07:** Installation de l'extension de sécurité **Word fence**.
- Cahier-08:** Installation de l'extension de vente en ligne **WooCommerce** et création de comptes chez **Stripe** et **PayPal** pour les paiements en ligne.
- Cahier-09:** Sauvegarde/restauration ou migration d'un site avec l'extension **Duplicator**.
- Cahier-10:** Serveur mandataire inversé.
- Cahier-11:** Sauvegarde/restauration avec **Backup PC**.

Salle de classe



But du cours NethServer-101



Cours NethServer-101			
Salle de classe: NethServer			
Salle de classe: Étudiant-X / Cahiers de cours			
Site et code: 2020-09-18	Date de démarrage: 2020-09-18	Par: NethServer	NethServer
Revisions: 3.02	2020-09-18	14:25	Date: Cours-101