

Configuration ntopng

Tableau des matières[Cacher]

-  [Introduction](#)
-  [Pré-requis](#)
-  [Matériel](#)
-  [Système](#)
-  [Installation](#)
-  [Système](#)
-  [Installation des dépôts PowerTools & Remi](#)
-  [Désactivation de SELinux & FirewallD](#)
-  [Configuration de l'interface de capture](#)
-  [NtopNG](#)
-  [Configuration du démon](#)
-  [Connexion](#)
-  [Configuration NtopNG finale](#)
-  [Création d'un nouvel utilisateur :](#)
-  [Ajout d'une application](#)
-  [Purge des données](#)

Introduction

Cette page présente l'installation d'Oracle Linux 8 pour permettre le déploiement de la solution NtopNG.

Pré-requis

Matériel

Prérequis conseillés pour une interface de 100 Mbps à 1 Gbps :

- CPU : 4 coeurs
- RAM : 4 Go
- Disque : 100 Go (plus d'informations [<https://www.ntop.org/ntopng/ntopng-disk-requirements-for-timeseries-and-flows/> ici])
- Le serveur doit posséder deux interfaces réseaux :
 - Une pour le management & la connexion à NtopNG
 - L'autre pour la capture des paquets
- Clé USB de 16 Go pour l'installation d'Oracle Linux 8

Système

- Serveur(s) DNS pour permettre l'accès à Internet & la résolution de nom des hôtes qui seront vus au niveau de la capture
- Synchronisation NTP pour "timestamp" correctement les métriques remontées par la solution
- Accès Internet pour l'installation et la mise à jour

Installation

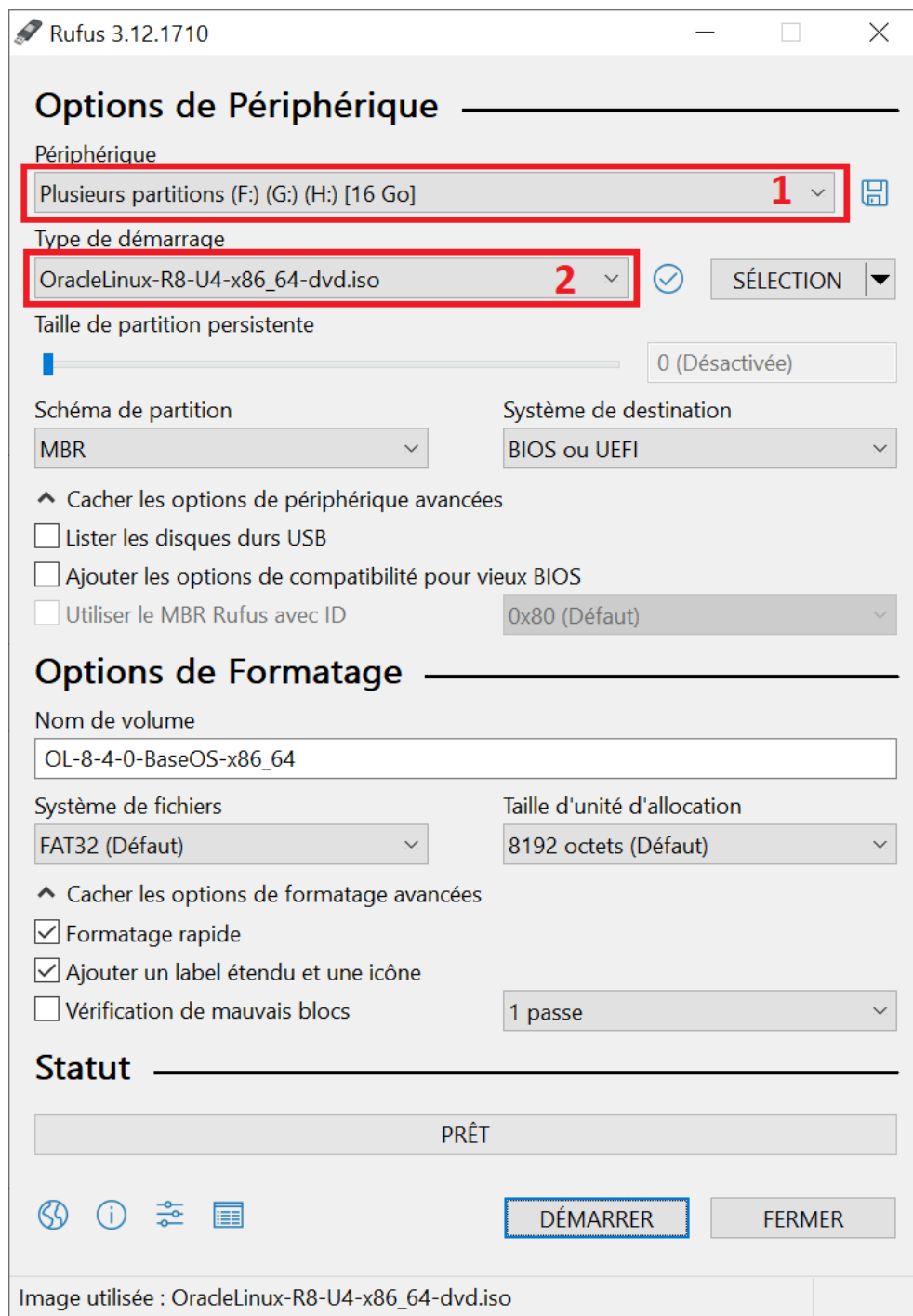
Système

La distribution Oracle Linux actuelle est la version 8.4 et est supportée par NtopNG. Elle peut être téléchargée [https://yum.oracle.com/ISOS/OracleLinux/OL8/u4/x86_64/OracleLinux-R8-U4-x86_64-dvd.iso ici].

Une clé de boot peut être réalisée avec [https://rufus.ie/fr/ Rufus] ([https://github.com/pbatard/rufus/releases/download/v3.15/rufus-3.15.exe Version 3.15 téléchargeable ici]).

On démarre Rufus puis on sélectionne :

1. On sélectionne la clé USB à formater
2. On sélectionne l'ISO Oracle Linux



Rufus 3.12.1710

Options de Périphérique

Périphérique
Plusieurs partitions (F:) (G:) (H:) [16 Go] **1** ▼

Type de démarrage
OracleLinux-R8-U4-x86_64-dvd.iso **2** ▼ ☒ SÉLECTION ▼

Taille de partition persistente
0 (Désactivée)

Schéma de partition
MBR ▼

Système de destination
BIOS ou UEFI ▼

^ Cacher les options de périphérique avancées

☐ Lister les disques durs USB

☐ Ajouter les options de compatibilité pour vieux BIOS

☐ Utiliser le MBR Rufus avec ID 0x80 (Défaut) ▼

Options de Formatage

Nom de volume
OL-8-4-0-BaseOS-x86_64

Système de fichiers
FAT32 (Défaut) ▼

Taille d'unité d'allocation
8192 octets (Défaut) ▼

^ Cacher les options de formatage avancées

☒ Formatage rapide

☒ Ajouter un label étendu et une icône

☐ Vérification de mauvais blocs 1 passe ▼

Statut

PRÊT

☒ ☐ ☐ ☐

DÉMARRER FERMER

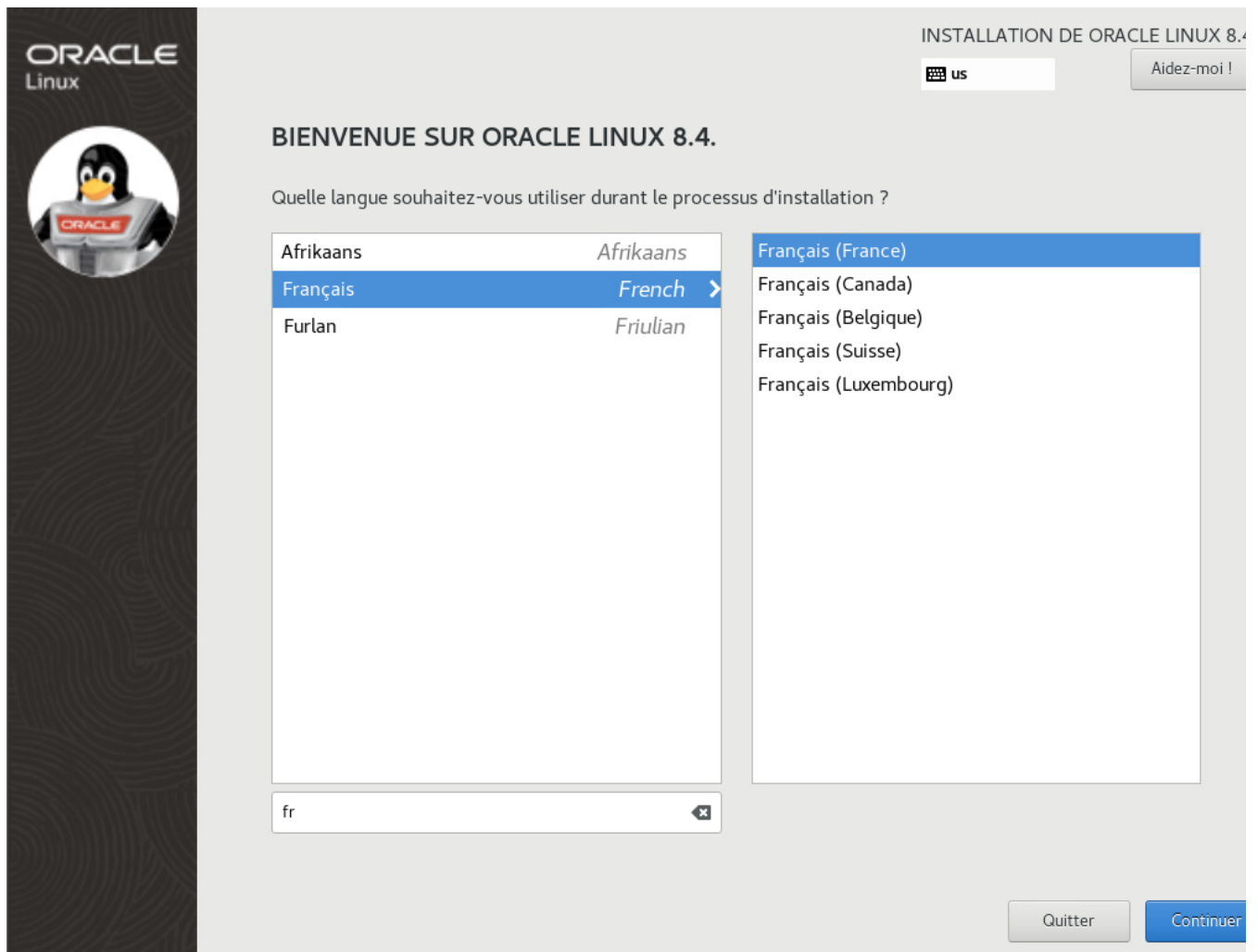
Image utilisée : OracleLinux-R8-U4-x86_64-dvd.iso

Une fois la clé créée, on boot sur celle-ci à l'aide de la touche F12 lors du démarrage, l'écran suivant doit apparaître, on sélectionne "Install Oracle Linux 8.4.0" :

```
Install Oracle Linux 8.4.0
Test this media & install Oracle Linux 8.4.0
Troubleshooting -->
```


```
Use the ▲ and ▼ keys to change the selection.
Press 'e' to edit the selected item, or 'c' for a command prompt.
```

Il faut ensuite attendre quelques minutes avant que l'écran de choix de la langue apparaisse, on peut taper fr pour simplifier la sélection de la langue française :



Le menu principal s'affiche ensuite une fois la langue sélectionnée :

ORACLE
Linux




RÉSUMÉ DE L'INSTALLATION


INSTALLATION DE ORACLE LINUX 8.4


fr (oss)

Aidez-moi !


LOCALISATION


 **Clavier**
Français (variante)

 **Support langue**
Français (France)


 **Heure & Date**
Fuseau horaire Amériques/
New York


LOGICIEL


 **Source d'installation**
Média local


 **Sélection Logiciel**
Serveur avec GUI

SYSTÈME


 **Installation Destination**
Partitionnement automatique
sélectionné


 **KDUMP**
Kdump est activé

 **Nom du réseau & d'hôte**
Non connectée

 **Politique de sécurité**
Aucun profil sélectionné

PARAMÈTRES UTILISATEUR


 **Mot de passe administrateur**
Le compte root est désactivé.

 **Création Utilisateur**
Aucun utilisateur ne sera créé

Quitter

Commencer l'installation

Nous ne modifierons pas vos disques tant que vous n'aurez pas cliqué sur « Commencer l'installation »

 Veuillez compléter les points marqués avec cette icône avant de passer à l'étape suivante.

On commence par cliquer sur "LOGICIEL > Sélection Logiciel" et on sélectionne l'environnement de base "Serveurs" (cela conditionne les paquets installés de base) :

SÉLECTION DE LOGICIELS

Fait

INSTALLATION DE ORACLE LINUX 8.4

fr (oss)

Aidez-moi !

Environnement de base

☐ **Serveur avec GUI**
Un serveur intégré, facile à gérer, avec une interface graphique.
 ☒ **Serveurs**
Un serveur intégré, facile à gérer.
 ☐ **Installation minimale**
Fonctionnalité de base.
 ☐ **Station de travail**
Une station de travail est un système de bureau convivial pour les ordinateurs portables et les PC.
 ☐ **Custom Operating System**
Blocs de base pour personnaliser le système OL.
 ☐ **Hôte de virtualisation**
Hôte de virtualisation minimal.

Logiciel supplémentaire pour l'environnement sélectionné

☐ **Utilitaires de surveillance du matériel**
Ensemble d'outils pour surveiller le matériel du serveur.
 ☐ **Serveur de fichiers Windows**
Ce groupe de packages vous permet de partager des fichiers entre les systèmes Linux et Windows (tm).
 ☐ **Outils de débogage**
Outils pour déboguer les applications ayant un mauvais comportement et diagnostiquer les problèmes de performance.
 ☐ **Serveur de fichiers et de stockage**
Serveur de stockage réseau CIFS, SMB, NFS, iSCSI, iSER et iSNS.
 ☐ **Serveur FTP**
Ces outils vous permettent d'exécuter un serveur FTP sur le système.
 ☐ **GNOME**
GNOME est un environnement de bureau convivial et hautement intuitif.
 ☐ **Agents invités**
Agents utilisés lors d'une exécution sous un hyperviseur.
 ☐ **Prise en charge de l'Infiniband**
Logiciel conçu pour prendre en charge le clustering, la connectivité de grilles à l'aide, une latence faible, un stockage bandwidth avec InfiniBand basé RDMA, et de fabriques iWARP, RoCe et OPA.
 ☐ **Serveur de messagerie**
Ces packages vous permettent de configurer un serveur de messagerie IMAP ou SMTP.
 ☐ **Client NFS**
Permet au système de s'attacher au stockage réseau.
 ☐ **Serveurs de réseau**
Ces packages comprennent des serveurs basés sur le réseau comme DHCP, Kerberos et NIS.
 ☐ **Outils de performance**
Outils pour diagnostiquer le système et les problèmes de performance au niveau des applications.
 ☐ **Gestion distante Linux**

On passe ensuite sur **SYSTEME > Installation Destination**, par défaut le système crée une partition / et une partition /home. Ce n'est pas intéressant pour une appliance.

On passe le partitionnement en manuel puis on clique sur **Fait** :

Fait

fr (oss)

Aidez-moi !

▼ Nouvelle installation de Oracle Linux 8.4

Vous n'avez pas encore créé de point de montage pour votre installation de Oracle Linux 8.4. Vous pouvez :

- [Cliquez ici pour les créer automatiquement.](#)
- Créer de nouveaux points de montage en cliquant sur le bouton « + ».

Les nouveaux points de montage utiliseront le schéma de partitionnement suivant :

LVM

Quand vous aurez créé des points de montage pour l'installation de Oracle Linux 8.4, vous pourrez en voir les détails [ici](#).

+

-

↻

ESPACE DISPONIBLE

100 Gio

ESPACE TOTAL

100 Gio

[1 périphérique de stockage sélectionné](#)

Tout réinitialiser

La page suivante s'affiche ensuite, on clique sur "Cliquez ici pour les créer automatiquement" :

PARTITIONNEMENT MANUEL

Fait

INSTALLATION DE ORACLE LINUX 8

fr (oss)

Aidez-moi !

Nouvelle installation de Oracle Linux 8.4

DONNÉES

/home ol-home	30,98 Gio >
------------------	-------------

SYSTÈME

/ ol-root	63,46 Gio
/boot/efi sda1	600 Mio
/boot sda2	1024 Mio
swap ol-swap	3,96 Gio

+ - ↺

ESPACE DISPONIBLE

1,97 Mio

ESPACE TOTAL

100 Gio

[1 périphérique de stockage sélectionné](#)

ol-home

Point de montage :

Capacité souhaitée :

Type de périphérique :

LVM

☐ Chiffrer

Système de fichiers :

xfs

☒ Reformater

Étiquette :

Périphérique :
VMware Virtual disk (sda)

Modifier...

Groupe De Volumes :
ol (0 O d'espace libre) ▼

Modifier...

Mise à jour des paramètres

Remarque : les paramètres que vous aurez définis dans cet écran ne seront pas appliqués tant que vous n'aurez pas cliqué sur le bouton du menu principal « Commencer l'installation ».

Tout réinitialiser

On supprime le **/home** et on ajoute l'espace disque de celui-ci au point de montage **"/"** pour utiliser tout l'espace disponible :

PARTITIONNEMENT MANUEL

Fait

INSTALLATION DE ORACLE LINUX 8

fr (oss)

Aidez-moi !

▼ Nouvelle installation de Oracle Linux 8.4

SYSTÈME

/	94,44 Gio	>
ol-root		
/boot/efi	600 Mio	
sda1		
/boot	1024 Mio	
sda2		
swap	3,96 Gio	
ol-swap		

+

-

↺

ESPACE DISPONIBLE

1,97 Mio

ESPACE TOTAL

100 Gio

[1 périphérique de stockage sélectionné](#)

ol-root

Point de montage :

/

Périphérique :

VMware Virtual disk (sda)

Modifier...

Capacité souhaitée :

94,44 Gio

Type de périphérique :

LVM

☐ Chiffrer

Système de fichiers :

xfs

☒ Reformater

Groupe De Volumes :

ol (8 Mio d'espace libre)

Modifier...

Étiquette :

Nom :

root

Mise à jour des paramètres

Remarque : les paramètres que vous aurez définis dans cet écran ne seront pas appliqués tant que vous n'aurez pas cliqué sur le bouton du menu principal « Commencer l'installation ».

Tout réinitialiser

On accepte le partitionnement :

PARTITIONNEMENT MANUEL
INSTALLATION DE ORACLE LINUX 8.4

Fait
fr (oss)
Aidez-moi

Nouvelle installation de Oracle Linux 8.4

SYSTÈME

/
94,44 Gio
>

ol-root

Point de montage :
/

Périphérique :
VMware Virtual disk (sda)

RÉSUMÉ DES MODIFICATIONS

Vos personnalisations entraîneront les modifications suivantes qui prendront effet lorsque vous retournerez au menu principal et que vous commencerez l'installation :

Ordre	Action	Type	Périphérique	Point de montage
1	supprimer le format	Unknown	VMware Virtual disk (sda)	
2	créer le format	table de partition (GPT)	VMware Virtual disk (sda)	
3	créer une partition	partition	sda1 sur VMware Virtual disk	
4	créer le format	EFI System Partition	sda1 sur VMware Virtual disk	/boot/efi
5	créer une partition	partition	sda2 sur VMware Virtual disk	
6	créer une partition	partition	sda3 sur VMware Virtual disk	
7	créer le format	physical volume (LVM)	sda3 sur VMware Virtual disk	
8	créer une partition	lvmvg	ol	
9	créer une partition	lvm lv	ol-root	
10	créer le format	xfs	ol-root	/
11	créer une partition	lvm lv	ol-swap	
12	créer le format	swap	ol-swap	

Annuler et retourner au partitionnement personnalisé
Accepter les modifications

+
-
↺

ESPACE DISPONIBLE
1,97 Mio

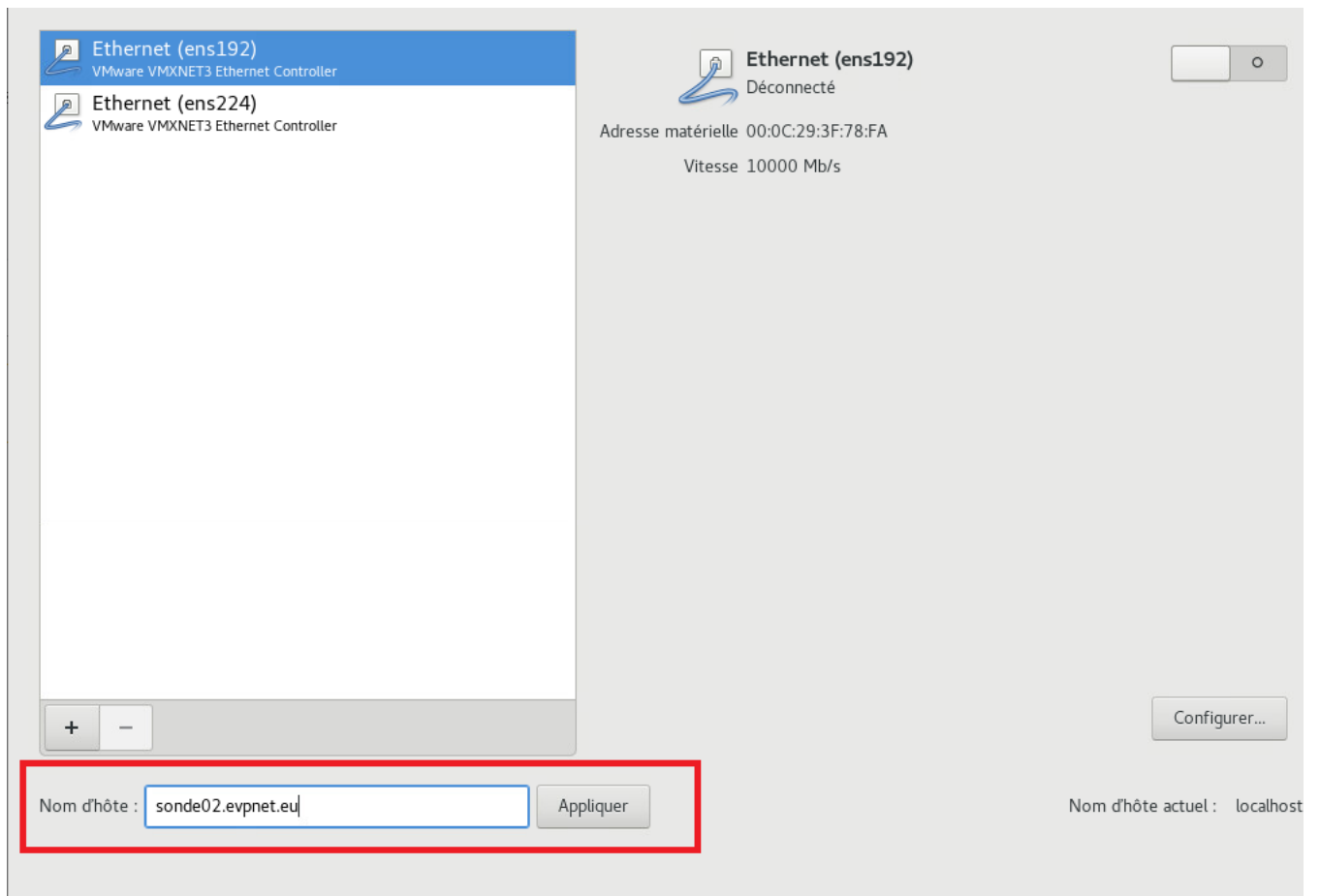
ESPACE TOTAL
100 Gio

[1 périphérique de stockage sélectionné](#)

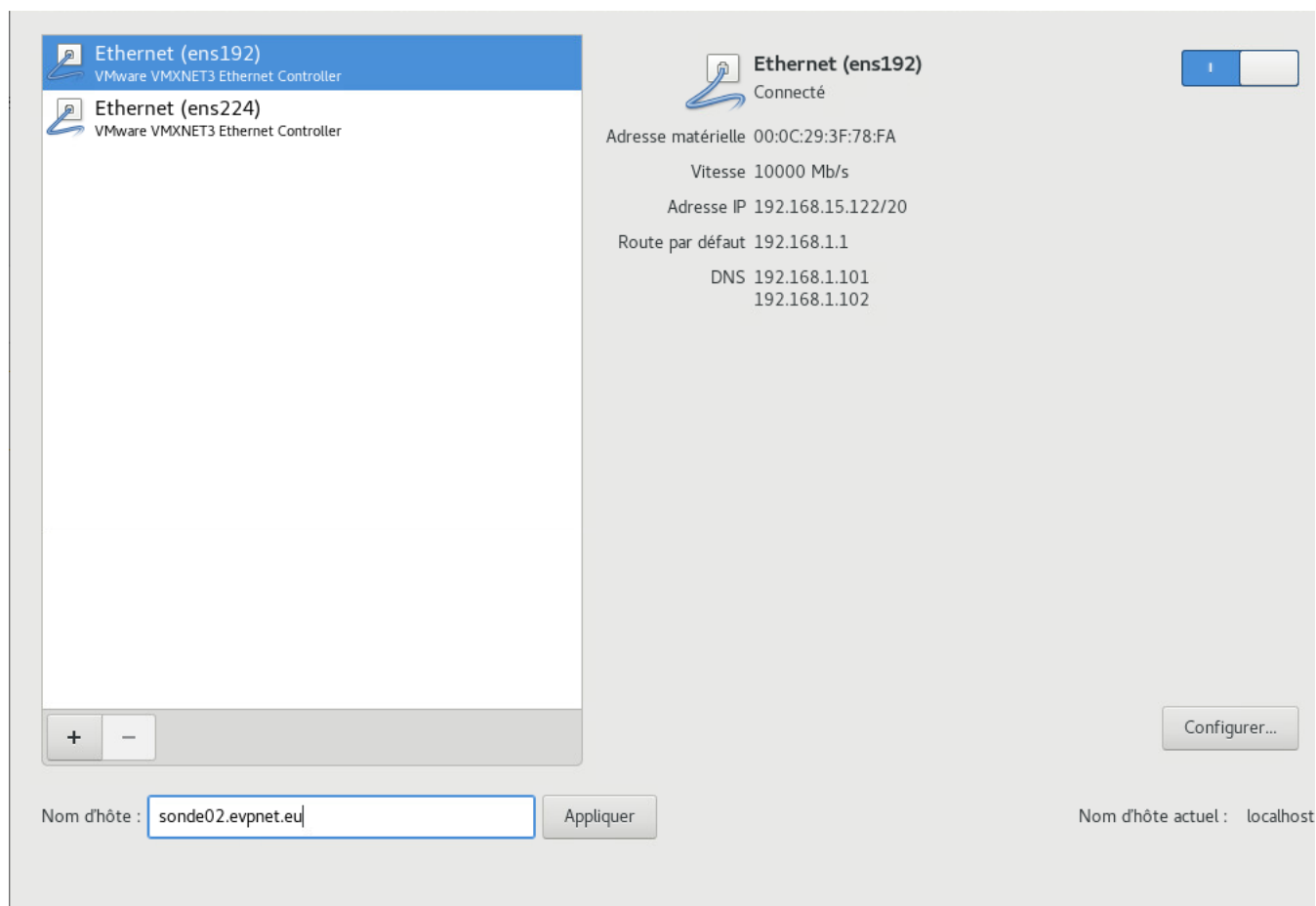
Tout réinitialiser

Remarque : les paramètres que vous aurez définis dans cet écran ne seront pas appliqués tant que vous n'aurez pas cliqué sur le bouton du menu principal « Commencer l'installation ».

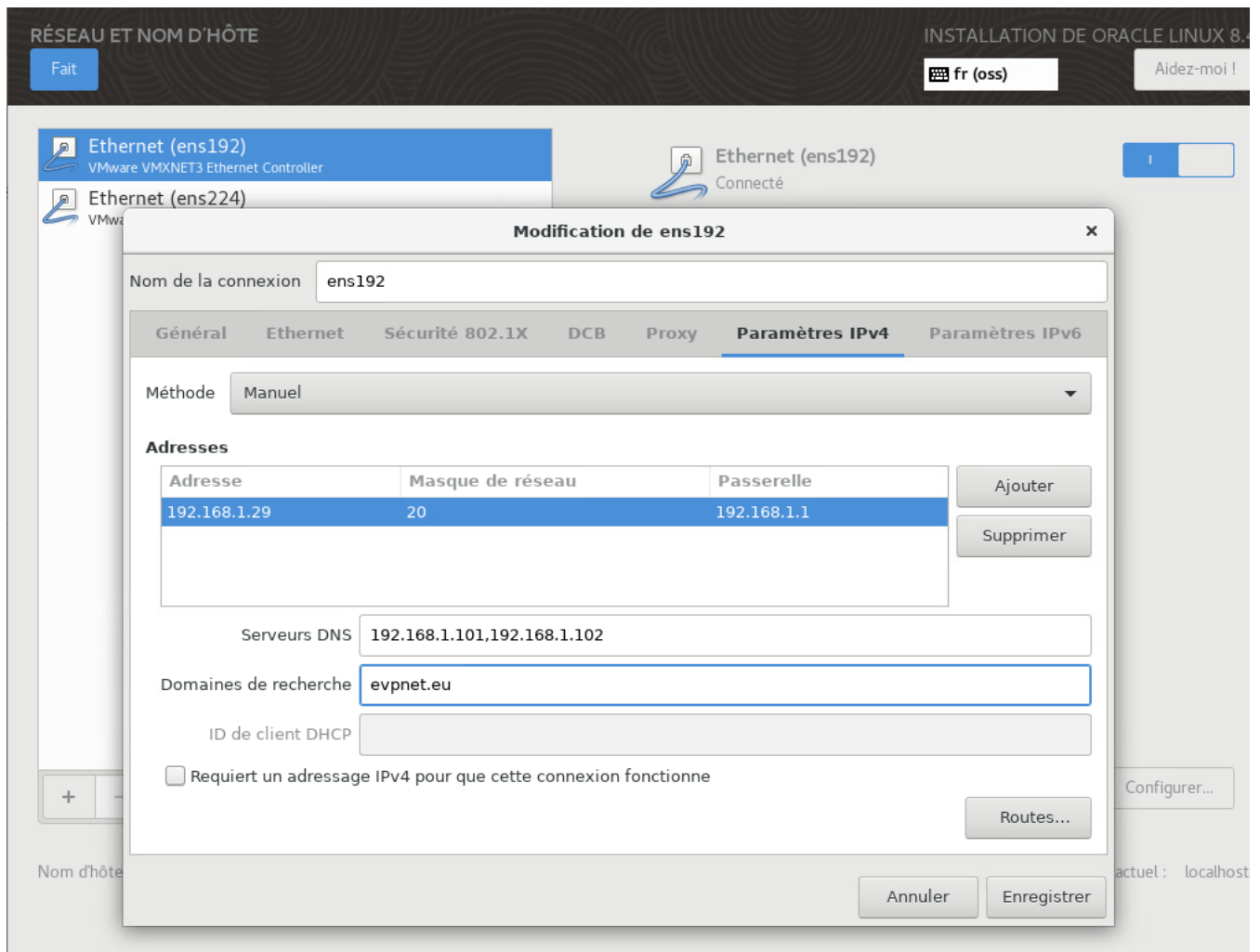
On passe ensuite à la configuration réseau en cliquant sur **SYSTEME > Nom du réseau & d'hôte**, on peut voir les cartes (au moins 2) présentes sur le serveur et on peut configurer le nom d'hôte:



On active ensuite l'interface de management (ens192 dans l'exemple) puis on la configure en cliquant sur **Configurer** et en allant dans l'onglet **Paramètres IPv4**:



Exemple de configuration dans mon environnement, on clique ensuite sur **"Enregistrer"** puis sur **"Fait"** pour retourner au menu principal :



On peut ensuite désactiver la politique de sécurité :

Fait

fr (oss)

Aidez-moi !

Modifier le contenu

Application de la politique de sécurité :



Choisir le profil ci-dessous :

Criminal Justice Information Services (CJIS) Security Policy

This profile is derived from FBI's CJIS v5.4

Security Policy. A copy of this policy can be found at the CJIS Security Policy Resource Center:

<https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center>**Unclassified Information in Non-federal Information Systems and Organizations (NIST 800-171)**

From NIST 800-171, Section 2.2:

Security requirements for protecting the confidentiality of CUI in non-federal information systems and organizations have a well-defined structure that consists of:

- (i) a basic security requirements section;
- (ii) a derived security requirements section.

The basic security requirements are obtained from FIPS Publication 200, which provides the high-level and fundamental security requirements for federal information and information systems. The derived security requirements, which supplement the basic security requirements, are taken from the security controls

Sélectionner le profil

Modifications réalisées ou à faire :



N'applique pas la politique de sécurité

On passe ensuite à la configuration de la timezone via "'LOCALISATION > Heure & Date'", on sélectionne Europe > Paris :

HEURE ET DATE

INSTALLATION DE ORACLE LINUX 8.4

Fait

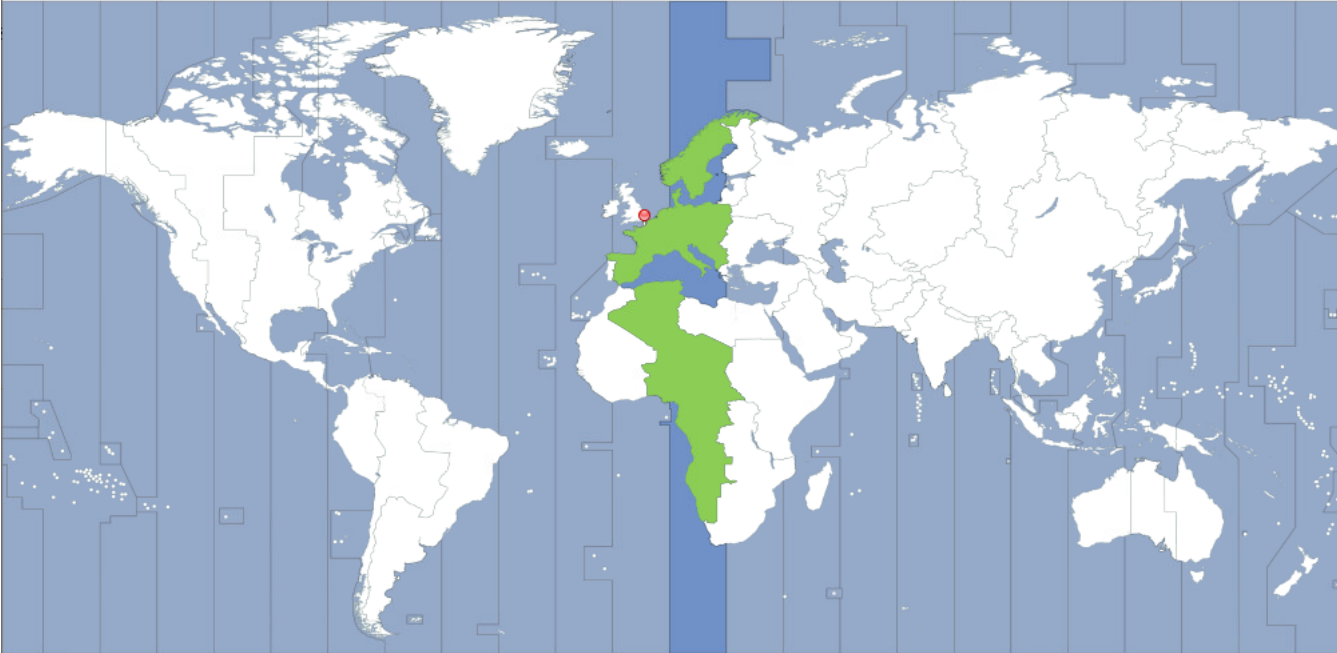
fr (oss)

Aidez-moi !

Région : Europe

Ville : Paris

Heure du réseau




16:23

☒ 24-heures
☐ AM/PM

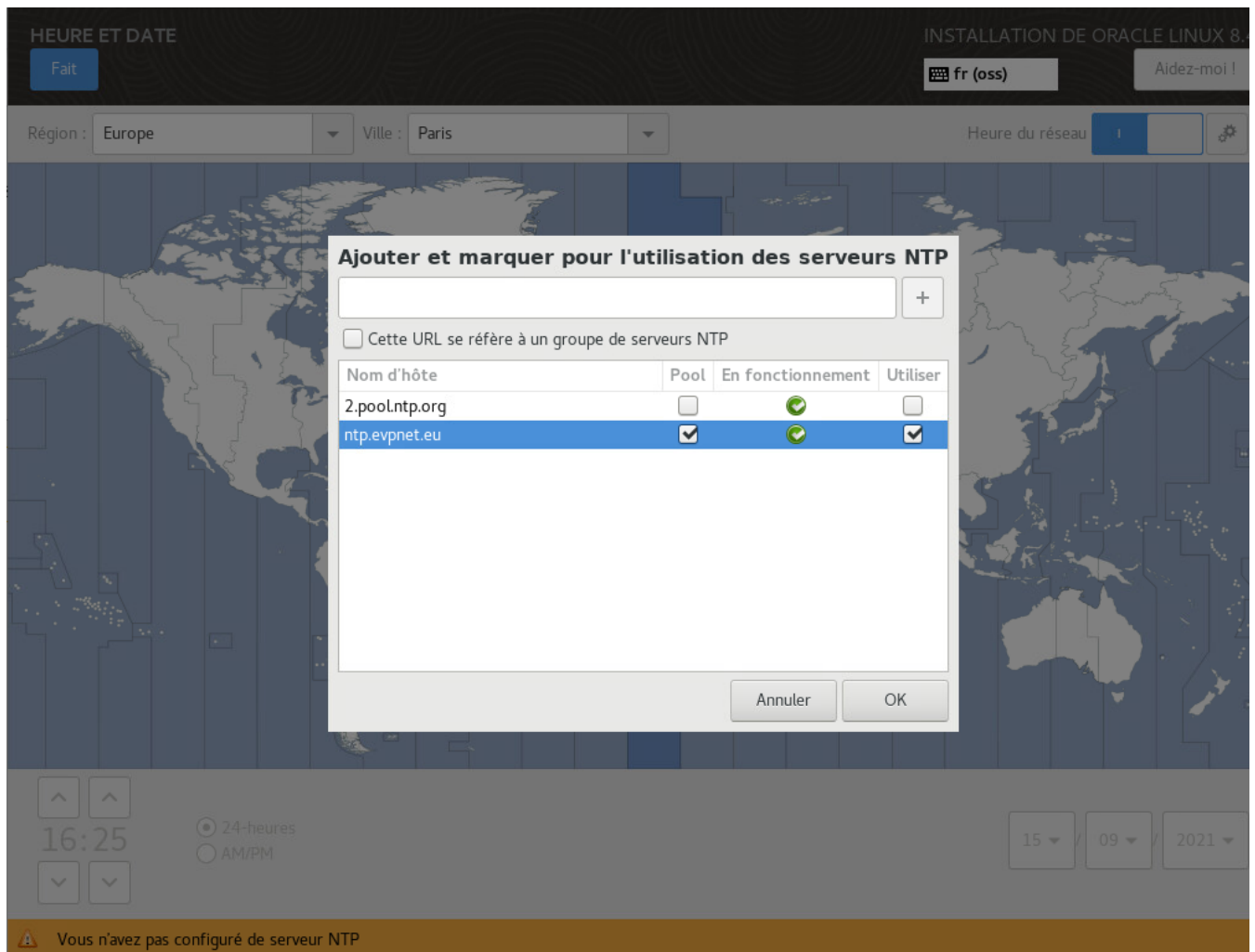
15

09

2021

 Vous n'avez pas configuré de serveur NTP

On peut également saisir un serveur de temps en cliquant sur la roue crantée en haut à droite :



On définit ensuite le mot de passe Administrateur via **"PARAMETRES UTILISATEURS > Mot de passe administrateur"** :

MOT DE PASSE ADMINISTRATEUR

INSTALLATION DE ORACLE LINUX 8

Fait

fr (oss)

Aidez-moi !

Le compte root est utilisé pour administrer le système. Entrez un mot de passe pour l'utilisateur root.

Mot de passe administrateur :

••••••••

Fort

Confirmer :

••••••••

Et on peut ensuite lancer l'installation :



LOCALISATION



Clavier
Français (variante)



Support langue
Français (France)



Heure & Date
Fuseau horaire Europe/Paris

PARAMÈTRES UTILISATEUR



Mot de passe administrateur
Le mot de passe administrateur est défini



Création Utilisateur
Aucun utilisateur ne sera créé

LOGICIEL



Source d'installation
Média local



Sélection Logiciel
Serveurs

SYSTÈME



Installation Destination
Partitionnement personnalisé
sélectionné



KDUMP
Kdump est activé



Nom du réseau & d'hôte
L'interface filaire (ens192) est
connectée



Politique de sécurité
Aucun profil sélectionné

Quitter

Commencer l'installation

Nous ne modifierons pas vos disques tant que vous n'aurez pas cliqué sur « Commencer l'installation »

ORACLE
Linux



Progression de l'installation

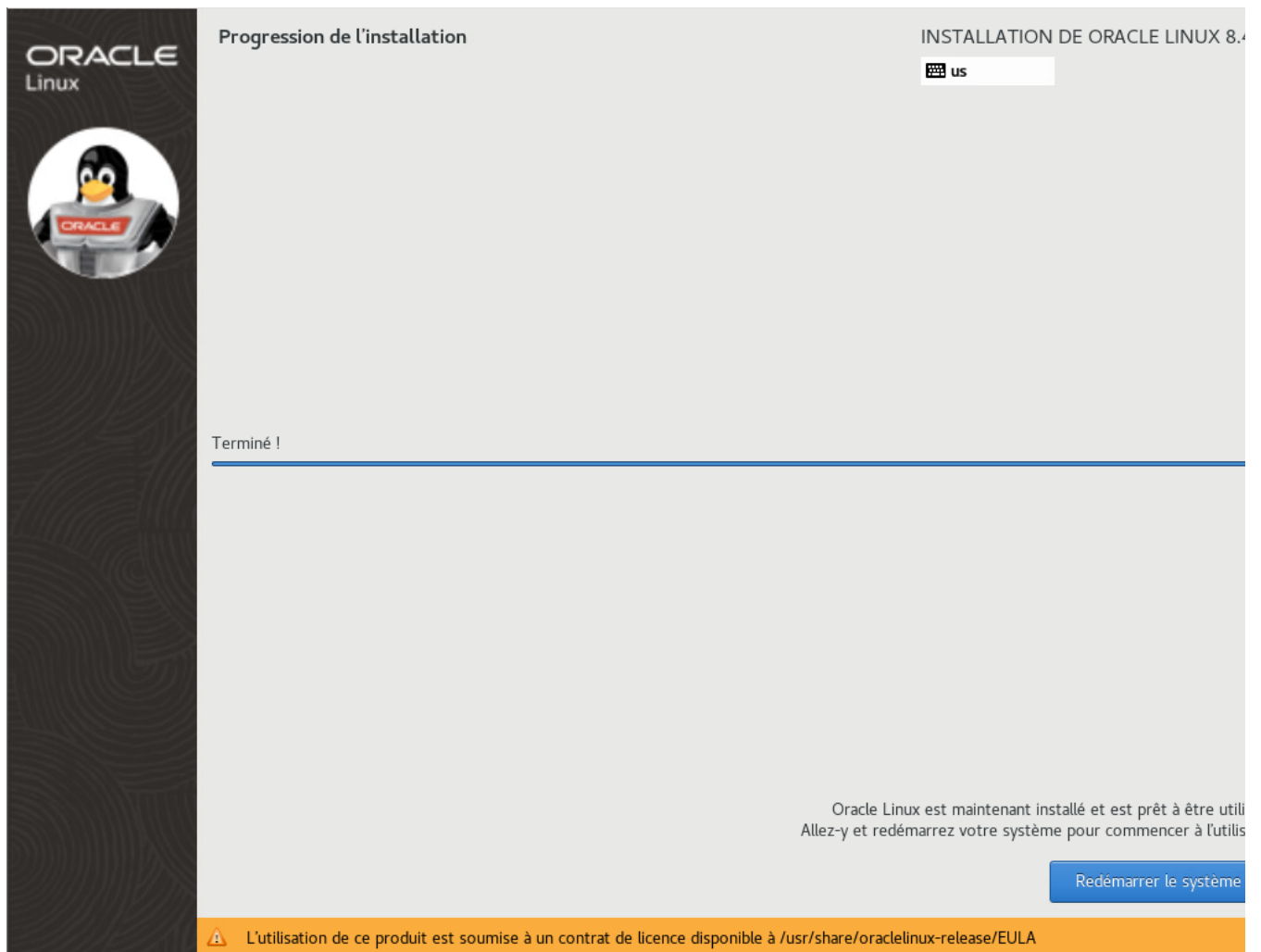
INSTALLATION DE ORACLE LINUX 8.4

fr (oss)

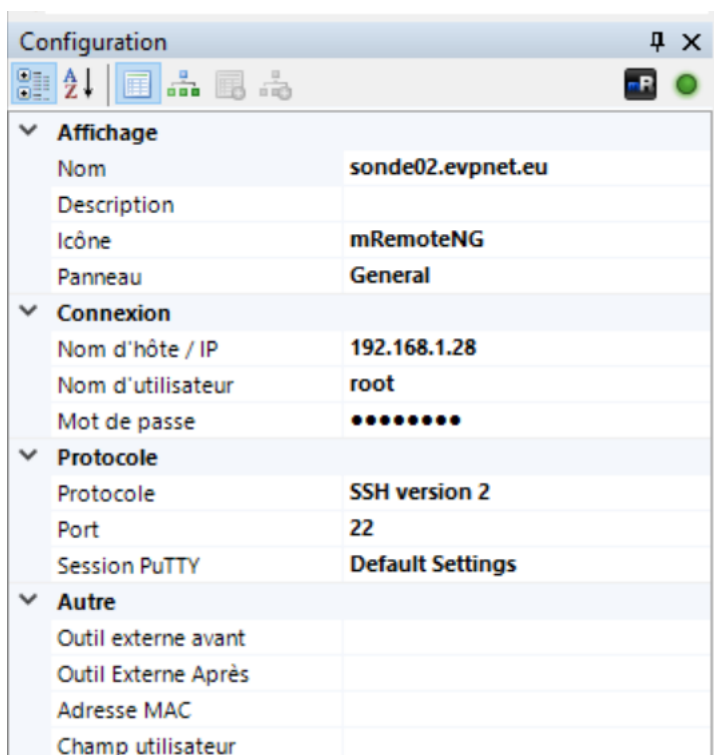
Création de efi sur /dev/sda1

Quitter

Redémarrer le système



Une fois le système installé, on se connecte en SSH et avec le compte **root** sur le serveur avec mRemoteNG par exemple :



On vérifie que tous les packages sont bien à jour avant de passer à l'installation des dépendances et de NtopNG :

```
yum update -y
yum upgrade -y
```

Installation des dépôts PowerTools & Remi

L'installation de NtopNG demande la présence des dépôts Epel / Remi.

Pour epel :

```
dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

```
On peut ensuite procéder à l'installation du repository remi :
rpm -ivh http://rpms.remirepo.net/enterprise/remi-release-8.rpm
yum install dnf-plugins-core
dnf config-manager --set-enabled ol8_codeready_builder
dnf config-manager --set-enabled remi
```

Désactivation de SELinux & Firewalld

Pour SELinux, on édite le fichier /etc/selinux/config :

```
vi /etc/selinux/config
```

Remplacer :

```
SELINUX=enforcing
```

Par :

```
SELINUX=disabled
```

Il faut ensuite redémarrer pour la prise en compte :

```
reboot
```

Puis on désactive le firewall :

```
systemctl disable firewalld
systemctl stop firewalld
```

Configuration de l'interface de capture

Le serveur possède donc plusieurs interfaces, il est nécessaire de déterminer quelle interface sera utilisée pour la capture :

```
# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: enp0s20f0u3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 00:e0:4c:20:d1:15 brd ff:ff:ff:ff:ff:ff
inet 192.168.1.29/20 brd 192.168.15.255 scope global dynamic noprefixroute enp0s20f0u3
valid_lft 613961sec preferred_lft 613961sec
inet6 fe80::4f2f:401a:ec02:7e91/64 scope link noprefixroute
valid_lft forever preferred_lft forever
3: eno1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether f4:4d:30:6f:f7:e8 brd ff:ff:ff:ff:ff:ff
4: wlp58s0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
link/ether 2e:61:d1:70:34:12 brd ff:ff:ff:ff:ff:ff
```

Dans cet exemple, il s'agit d'un NUC avec les interfaces suivantes :

- lo : Loopback
- enp0s20f0u3 : Interface réseau USB, il est déconseillé d'utiliser ces interfaces pour de la capture
- eno1 : Interface physique Intel

- wlp58s0 : Wifi

On peut activer temporairement le mode "promiscuous" via la commande suivante :

```
ip link set ${INTERFACE_CAPTURE} promisc on
```

Soit avec l'interface eno1 :

```
ip link set eno1 promisc on
```

Il faut ensuite ajouter la commande dans /etc/rc.d/rc.local pour qu'elle soit exécutée au démarrage :

```
ip link set eno1 promisc on
```

Il faut par contre autoriser le service à s'exécuter au démarrage, pour cela, il faut recréer le fichier de configuration rc-local :

```
vim /etc/systemd/system/rc-local.service
```

Et y ajouter :

```
[Unit]
Description=/etc/rc.local Compatibility
ConditionPathExists=/etc/rc.local
[Service]
Type=forking
ExecStart=/etc/rc.local start
TimeoutSec=0
StandardOutput=tty
RemainAfterExit=yes
SysVStartPriority=99
[Install]
WantedBy=multi-user.target
```

Ensuite on autorise le fichier /etc/rc.local à être exécuté :

```
chmod +x /etc/rc.local
```

Puis on active le service :

```
systemctl enable rc-local
```

Enfin on redémarre ensuite le serveur pour s'assurer que l'interface est bien en promiscuous.

Elle doit ensuite remonter ainsi avec la commande "'ip addr'" :

```
3: eno1: <BROADCAST,MULTICAST,"PROMISC",UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether f4:4d:30:6f:f7:e8 brd ff:ff:ff:ff:ff:ff
```

NtopNG

L'installation la plus simple se fait par l'ajout des dépôts officiels ([<https://packages.ntop.org/centos-stable/> voici la documentation officielle en anglais]) :

```
cd /etc/yum.repos.d/
wget https://packages.ntop.org/centos-stable/ntop.repo -O ntop.repo
```

On supprime ensuite zeromq3 (qui n'est normalement pas présent) et Apache (pour ne pas avoir de problème lors du démarrage de NtopNG sur le port 80) :

```
yum erase zeromq3
yum erase httpd
yum clean all
```

On installe ensuite les paquets nécessaires au bon fonctionnement de NtopNG :

```
yum install pfring-dkms n2disk nprobe ntopng cento
```

Configuration du démon

Il est nécessaire de renseigner l'interface qui sera utilisée au niveau capture :

```
cd /etc/ntopng/
vim ntopng.conf
```

Et on dé-commente ensuite ces paramètres :

```
# Pour indiquer l'interface de capture :  
-i=eno1  
# On passe le port de connexion à l'interface NtopNG en 80  
#-w=3000  
-w=80
```

Puis on ajoute le paramètre suivant :

```
# On désactive les VLANs si pas de besoin au niveau capture :  
--ignore-vlans
```

Puis on démarre / redémarre NtopNG :


```
systemctl start ntopng  
systemctl enable ntopng
```

Connexion

On vérifie que le port 80 écoute bien et qu'il pointe vers NtopNG :


```
[root@sonde01 ntopng]# netstat -anp | grep 0.0.0.0:80  
tcp 0 0 0.0.0.0:80 0.0.0.0:* LISTEN 2413/ntopng
```

On se connecte ensuite à l'interface avec le compte "admin" et le mot de passe "admin" :




Welcome to ntopng

Login

 [Unable to login?](#)

[User's Guides](#) | [Community](#) | [Support](#) | [FAQ](#) | [Code](#) | [Contact Us](#)



© 1998-21 - ntop.org
ntopng is released under [GPLv3](#).

Un changement de mot de passe sera demandé à la connexion :

Change Password

Default admin password must be changed. Please enter a new password below.

Language



English




Change Password

[Logout](#)

© 1998-21 - ntop.org
ntopng is released under [GPLv3](#).

Configuration NtopNG finale

Il reste ensuite à configurer l'interface pour indiquer que l'interface est de type "Mirroring", pour cela on sélectionne l'interface puis on clique sur la roue crantée et on coche la case devant "Mirrored Traffic" :



Shortcuts

Dashboard

Alerts

Flows

Hosts

Maps


Interface

Settings

Developer

Help

ens224



0 bps

877.20 kbit/s

[Upgrade to Pro/Enterprise version](#)

Interface: ens224

Networks

Packets

DSCP

Apps

ICMP

ARP

Custom Name

Pool

Interface Speed

Ingress Packets Sampling Rate

Local Broadcast Domain Hosts Identifier

Hide from Top Networks

Create Interface Top Talkers

Mirrored Traffic

Dynamic Traffic Disaggregation

Duplicate Disaggregated Traffic

[ntopng Community v.5.0.210915 \(CentOS Linux release 8.3.2011\)](#)

La dernière configuration demande de rajouter le ou les réseaux considérés comme **locaux** dans le fichier de configuration `/etc/ntopng/ntopng.conf`:

```
-m="192.168.1.0/24,192.168.2.0/24"
```

Il faut ensuite redémarrer "ntopng" :

```
systemctl restart ntopng
```

Création d'un nouvel utilisateur :

Création de l'utilisateur :

```
useradd users3I
```

Changer le mot de passe de l'utilisateur :

```
passwdusers3I
```

Créer un répertoire :

```
mkdir /home/users3I
```

Rendre le nouvel utilisateur propriétaire du répertoire :

```
chownusers3I /home/users3I
```

Ajout d'une application

La configuration du dictionnaire applicatif se fait par la modification du fichier `protos.txt` présent dans `/var/lib/ntopng/protos.txt` :

```
vim /var/lib/ntopng/protos.txt
```

Voici un exemple de contenu :

```
tcp:5666@NRPE
tcp:5667@NSCA
tcp:25565@Minecraft
tcp:7777,tcp:7778@Terraria
```

On peut renseigner les applications au niveau :

- * Protocole : "udp" et/ou "tcp" avec un numéro de port associé
- * Nom DNS ou IP via "host"

Les protocoles peuvent être séparés de "," s'ils concernent la même application :

```
tcp:81,tcp:8181@HTTP
udp:5061-5062@SIP
tcp:860,udp:860,tcp:3260,udp:3260@iSCSI
tcp:3000@ntop
host:"*.lvt.dash.us.aiv-cdn.net.c.footprint.net"@AmazonVideo
host:"api-global.netflix.com"@Netflix
```

Le fichier permet également de désactiver les alertes de risque sur des IPs ou noms DNS :

```
ip_risk_mask:192.168.0.0/20=0
host_risk_mask:".evpn.net.eu"]=0
```

Purge des données

La purge des données de la sonde se fait au niveau de l'administration: **Settings>Manage Data>Delete**:

Manage Stored Data

Export

Delete

Delete Host Data

IP or MAC Address

VLAN

NOTES:

- All the persistent data is deleted. Data include stored timeseries, flows, alerts, and Redis caches.