

Systemd for fun & profits en BUT 1

Jean-Marc Pouchoulon

Mai 2022

1 Compétences à acquérir lors du TP.

Compétence principale :

- Utiliser systemd afin de gérer un serveur Linux.

Niveaux dans la compétence :

- Niveau 1 utilisateur :
 - Concepts et utilisation basique de Systemd (exemple d'un service "ping").
 - Gestion d'une unité de service (ssh, systemd-networkd, systemd-resolved).
 - Manipulations avec systemd-runtime.
 - Gestion de systemd.

Savoirs liés :

- Processus.
- Cgroups.
- Capabilities.
- Services & units.

Savoir-faire :

- Créer, lancer, auditer un service avec systemd.
- Utiliser systemd en tant qu'administrateur systèmes.
- Surcharger un service.
- Analyser le comportement d'un système au travers de systemd.
- Analyser le boot d'un ordinateur.
- Utiliser un DropIn pour réveiller un service.
- Utiliser un template systemd pour démarrer des applications versionnées.
- Limiter les ressources consommées par un service.
- Sécuriser une unité de service systemd.

2 Pré-requis, recommandations et notation du TP.

Vous travaillerez individuellement. Il vous explicitement demandé de faire valider votre travail par l'enseignant. Ces "checks" permettront de vous noter. Un compte rendu succinct (fichiers de configuration , copie d'écran montrant la réussite de votre construction ...) est demandé et à rendre sur Moodle.

2.1 Obtenir de l'aide sur systemd.

2.1.1 Changements à réaliser sur votre VM

Vous travaillerez avec une VM en utilisant l'OVA Ubuntu sur <http://store.iutbeziers.fr>

3 Configurez la version deux des cgroups

Systemd utilise par défaut la version 1 des cgroups¹.

Afin de bénéficier de la pleine puissance de systemd modifiez le fichier `/etc/default/grub` en rajoutant à `GRUB_CMDLINE_LINUX_DEFAULT` l'item `"systemd.unified_cgroup_hierarchy=1"`.

Après un `"update-grub"` rebootez votre système.

3.1 Aide sur systemd.

```
man systemd.unit
man systemd.service
man systemd.socket
man systemd.resource-control
man systemd.timer
...
```

La complétion avec la touche `tab` fonctionne aussi.

```
apt install bash-completion
```

Pour recharger une unité modifiée.

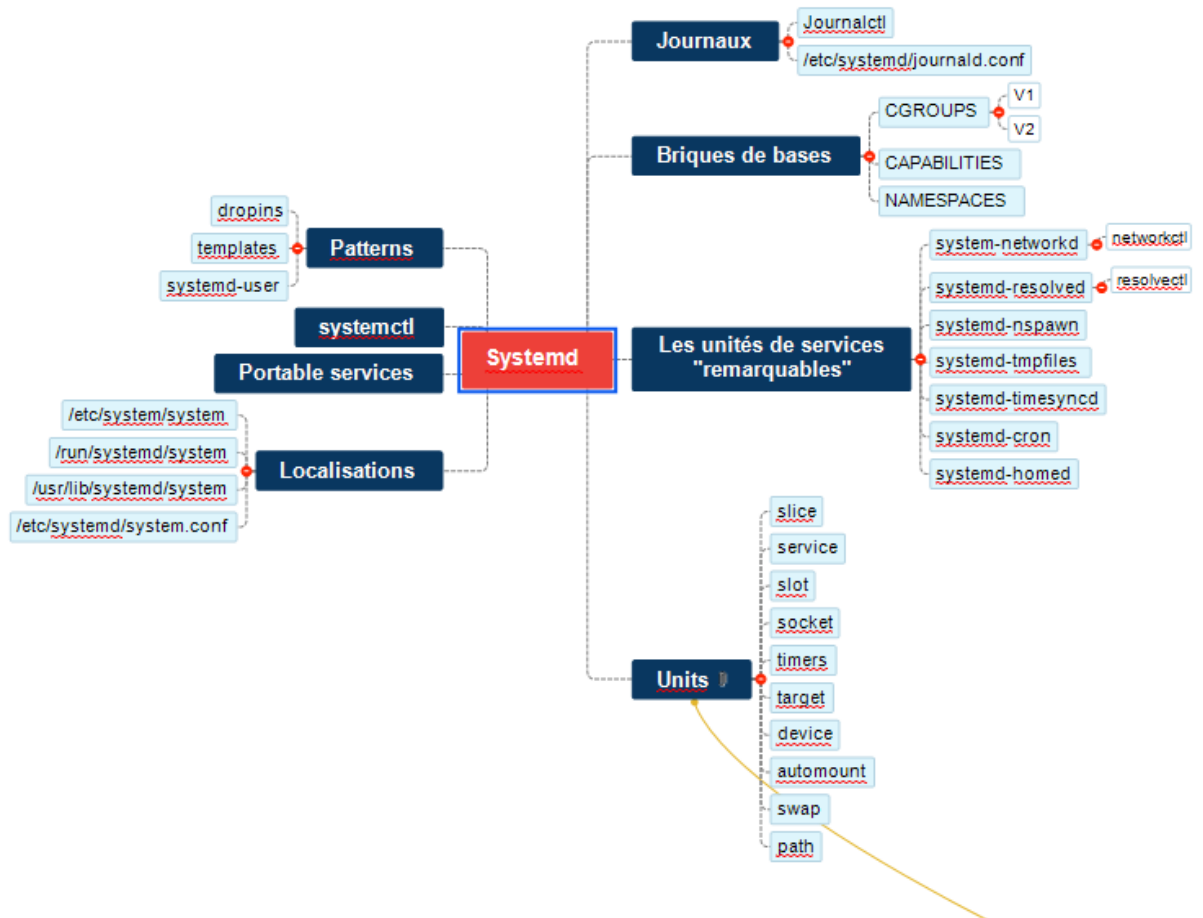
```
systemctl daemon-reload
```

Pour éditer avec vim :

```
export SYSTEMD_EDITOR=/usr/bin/vim
```

1. <https://wiki.archlinux.org/index.php/cgroups>

FIGURE 1 – Vue d'ensemble de systemd :



4 Niveau 1 : concepts et utilisation basique de systemd

4.1 Quelques éléments sur systemd

Systemd distingue plusieurs types de "units" (voir schéma ci-dessus). Chaque "units" est une abstraction d'une ressource de l'O.S.. Le type service est bien entendu essentiel.

Le type Socket permet un fonctionnement de type xinetd. // Un exemple de "unit file" de cups (daemon d'impression) :

```
# /lib/systemd/system/cups.service
[Unit]
Description=CUPS Scheduler
Documentation=man:cupsd(8)
After=network.target nss-user-lookup.target nslcd.service
Requires=cups.socket

[Service]
ExecStart=/usr/sbin/cupsd -l
Type=notify
Restart=on-failure
```

Le fichier permet de faire le lien avec le binaire à démarrer mais aussi d'explicitier les relations avec les autres units. Il indique aussi que la "unit" cups.socket doit être actif, que le service sera redémarré en cas de "fail" et que entre autre le réseau doit être fonctionnel.

La commande maître afin d'interagir avec systemd est **systemctl**. Le fichier maître qui définit le comportement général de systemd est `/etc/systemd/system.conf` accompagné de `/etc/systemd/journald.conf` pour paramétrer la journalisation des logs.

Les concepteurs de systemd ont astucieusement prévu les interactions des gestionnaires de paquets et des administrateurs systèmes avec systemd : les concepteurs de package installent les configurations systemd dans `/lib/systemd`, les administrateurs systèmes locaux dans `/etc/systemd`. Une configuration pour la durée de la session peut être faite `/run/systemd`. Attention `/etc` a la précedence sur `/run` qui a la précedence sur `/lib`. Il ne sert donc à rien de modifier pour la session si une configuration du service existe déjà dans `/etc`.

Par exemple pour empêcher une connexion ssh sur votre machine pour la durée de la session il suffit d'arrêter le service ssh :

```
systemctl stop ssh
```

On va utiliser `ssh.socket` qui a pour particularité de démarrer un process ssh quand il y a une connexion. On surcharge le service `ssh.socket` pour le *runtime de la machine* :

```
sudo systemctl edit --runtime ssh.socket
```

avec la configuration suivante :

```
[Socket]
IPAddressDeny=any
IPAddressAllow=127.0.0.1,IP_Du_COPAIN
```

et de démarrer le service `ssh.socket` en runtime :

```
sudo systemctl start --runtime ssh.socket
```

Il suffit de redémarrer la machine ou le service ssh pour que la modifications ne soient plus prise en compte (précédence de /etc sur /run) Vous pouvez lister les chemins des configurations des unit-files au travers de cette commande :

```
systemd-analyze unit-paths
/etc/systemd/system.control
/run/systemd/system.control
/run/systemd/transient
/run/systemd/generator.early
/etc/systemd/system
/etc/systemd/system.attached
/run/systemd/system
/run/systemd/system.attached
/run/systemd/generator
/usr/local/lib/systemd/system
/lib/systemd/system
/usr/lib/systemd/system
/run/systemd/generator.late
```

Cette façon de préserver les modifications des fichiers de configuration de systemd lors des mises à jour s'appelle un "DropIn". permet de travailler en surchargeant une configuration existante.

Les fichiers suivants intéresseront particulièrement les administrateurs réseaux :

- /etc/systemd/networkd.conf (configuration du réseau)
- /etc/systemd/resolved.conf (configuration de la résolution de nom).

Les commandes *hostnamectl* , *networkctl*, *resolvectl* sont aussi des commandes usitées.

4.2 Quelques options de bases de systemctl

1. Listez les "units".
2. Listez les "unit-files".
3. Listez les "units" de type service.
4. Listez les propriétés du daemon cups.
5. Affichez la configuration du service ssh. Quel est le service qui doit précéder son démarrage?
6. Comment empêcher le re-démarrage de ce service? testez la solution.
7. Vérifiez que le service ssh est redémarré automatiquement si vous "killez" son processus. Visualisez le journal du service pour le confirmer.
8. Listez les dépendances du service ssh.
9. Quel est la cible par défaut du démarrage de la machine virtuelle?
10. Donnez la localisation du service ssh dans l'arborescence de la machine.
11. Est-ce que ce service est démarré? activé? en échec?
12. Listez les dépendances du service ssh.
13. En une seule commande listez toutes les unités liées à ssh? est ce que l'unité ssh.socket est activée?

4.3 Création et gestion d'un service de "ping"

1. Créez le service ip-accounting-test.service² en utilisant la commande :

```
systemctl edit --full --force ip-accounting-test.service
```

L'option `--force` n'est utile qu'à la création de l'unité de service. L'option `--full` permet d'éditer directement un service de niveau "OS".

Renseignez un simple ping :

2. <http://0pointer.net/blog/ip-accounting-and-access-lists-with-systemd.html>

[Service]

```
ExecStart=/usr/bin/ping 8.8.8.8  
IPAccounting=yes
```

2. Démarrez le service.
3. Quel est le status du service ?
4. A l'aide de journalctl listez les messages relatifs au service créé. Listez le dernier évènement avec journalctl l'option -n 1 ? rajoutez l'option "-o verbose" afin d'afficher les variables d'environnements.
5. A l'aide de "systemctl status" déduire ce que fait l'option IPAccounting.
6. Utilisez la commande :

```
systemctl show ip-accounting-test -p IPIngressBytes -p IPIngressPackets -p IPEgressBytes -p IPEgressPackets
```

7. Surchargez afin de modifier indirectement (via systemctl edit sans l'option -full) le service ip-accounting-test pour pinguer l'IP 1.1.1.1 en lieu et place de l'IP 8.8.8.8 ?
8. Comment fonctionne la "surcharge" d'un service ? quel est l'intérêt de ce mode de fonctionnement ?
9. Bloquez les accès réseaux à votre VM en utilisant la commande suivante :

```
systemctl set-property system.slice IPAddressDeny=any IPAddressAllow=localhost
```

10. Autorisez uniquement l'IP de votre hôte à se connecter.(Systemctl se base sur l'"IP NAT").