C05-net-std-supp - COURS LINUX - MTN

Guillaume ASTIER

26/02/16

Table des matières

Les interfaces réseaux

Introduction

Sous Linux, ces interfaces sont nommées eth0, eth1, … pour des interfaces filaires, et wlan0, wlan1, … pour des interfaces sans fil (wifi).

Il existe également une interface spéciale, nommée lo (pour loopback) qui désigne toujours votre propre ordinateur.

Pour intégrer une machine/serveur Linux à un réseau, il faut au minimum configurer les éléments suivants :

- un nom d'hôte
- une adresse IP
- un masque de sous-réseau
- une passerelle par défaut
- un mécanisme pour résoudre les noms (DNS, hosts, NIS, etc.)

Le nom d'hôte

Le nom d'hôte peut être affecté dynamiquement avec la commande hostname

```
1 # hostname wopr
2 # hostname
3 wopr
```

Ou de façon permanente grâce au fichier /etc/hostname

Configuration manuelle d'une interface réseau

Dynamic Host Configuration Protocol : Si un serveur DHCP est disponible sur votre réseau, vous pouvez demander une configuration par DHCP

```
1 # dhclient eth0
```

Adresse IP et masque de sous-réseau : La commande ifconfig permet de configurer l'adresse IP et le masque de sous-réseau d'une interface donnée :

```
# ifconfig eth0 192.168.0.42 netmask 255.255.255.0
# ifconfig eth0 192.168.0.42/24
```

Affichage IP

La commande ifconfig sans option permet de vérifier le résultat.

```
# ifconfig
eth0      Link encap:Ethernet  HWaddr 06:62:7f:77:4a:77
          inet addr:172.16.0.236  Bcast:172.16.0.255  Mask
             :255.255.255.0
          inet6 addr: fe80::462:7fff:fe77:4a77/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:9001  Metric:1
          RX packets:1212774297 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1119018757 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1108922947604 (1.1 TB)  TX bytes:634187321271 (634.1
              GB)
```

Route

Passerelle par défaut : La commande route permet de configurer les routes réseaux :

```
# route add default gw 192.168.0.1 dev eth0
```

La commande route -n permet d'afficher les routes positionnées.

Autre commandes

ip : Les commandes de configuration réseau tendent à être remplacées par la commande ip, couteau suisse de la configuration réseau.

```
# ip addr add 192.168.0.42/24 dev eth0
# ip route add default via 192.168.0.1 dev eth0
```

Configuration statique d'une interface réseau

Pour que la configuration soit effective à chaque redémarrage de la machine, il faut renseigner les paramètres dans le fichier /etc/network/interfaces :

```
auto lo eth1
allow-hotplug eth0
iface lo inet loopback
iface eth0 inet dhcp
iface eth1 inet static
    address 192.168.0.42
    netmask 255.255.255.0
    gateway 192.195.0.1
```

Résolution de noms

DNS

DNS : Le système utilise les serveurs de nom (DNS) dont les adresses IP sont notées dans le fichier /etc/resolv.conf :

```
# cat /etc/resolv.conf
nameserver 192.0.2.71
nameserver 192.0.2.72
```

Les commandes host ou dig permettent de vérifier le bon fonctionnement du serveur DNS.

"fake" DNS Linux

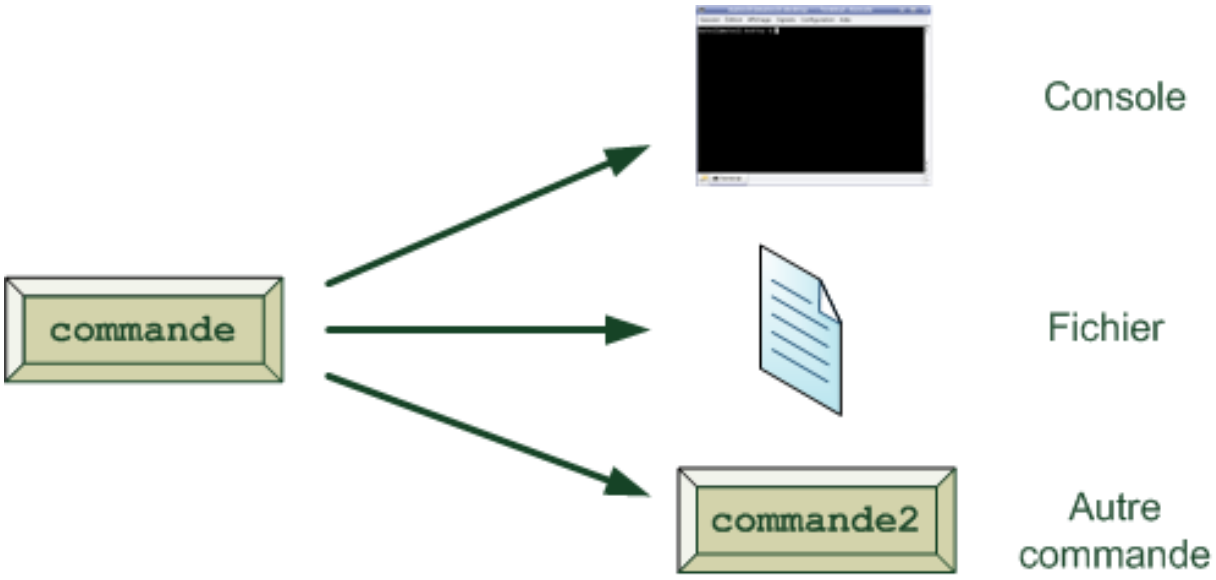
Le fichier /etc/hosts permet une résolution locale de noms d'hôte en adresses IP.

```
# cat /etc/hosts
127.0.0.1 localhost localhost.localdomain
192.0.0.1 albator
192.0.0.2 harlock
```

Les flux de redirection

Principe

Le principe de des flux de redirection permet de rediriger la sortie standard du terminal (le résultat d'une commande) dans un fichier ou dans une autre commande.



La redirection dans un fichier

Pour ce faire vous allez utiliser les caractères suppérieur et inferieur

'>' : redirige dans un fichier et l'écrase s'il existe déjà ;

'»' : redirige à la fin d'un fichier et le crée s'il n'existe pas.

ex :

```
# Créer une liste de tous mes fichiers présent dans ma home
find . > /tmp/all_my_local_file
# Ajouter en fin de liste ceux d'un autre utilisateur
find /home/mario >> /tmp/all_my_local_file
```

2>, 2» et 2>&1 : redirection erreurs

Sous linux il existe 2 type de sortie :

- la sortie standard : pour tous les messages (sauf les erreurs)
- la sortie d'erreurs : pour toutes les erreurs.

Prenons par exemple le cas suivant : Un fichier liste.txt n'existe pas sur la machine

```
cat liste.txt | grep ma_chaine > liste_filtre.txt
cat: liste.txt: Aucun fichier ou dossier de ce type
```

Dans ce cas présent un message va apparaître sur votre sortie standard : votre terminal.

Mais acunne donnée ne va populer le fichier liste_filtre.txt

STDERR

L'id du flux d'erreur sous linux et le 2

Pour pouvoire l'utiliser avec les redirection la bonne syntaxe est :

- 2>

```
grep ma_chaine liste.txt > liste_filtre.txt 2> liste_err.txt
```

Dans ce cas le fichier 'liste_filtre.txt' sera créé vide mais le fichier 'liste_err.txt' sera populer par l'erreur.

L'erreur *'grep: liste.txt: Aucun fichier ou dossier de ce type'* ne sera d'ailleur pas affiché dans le terminal.

Supervision

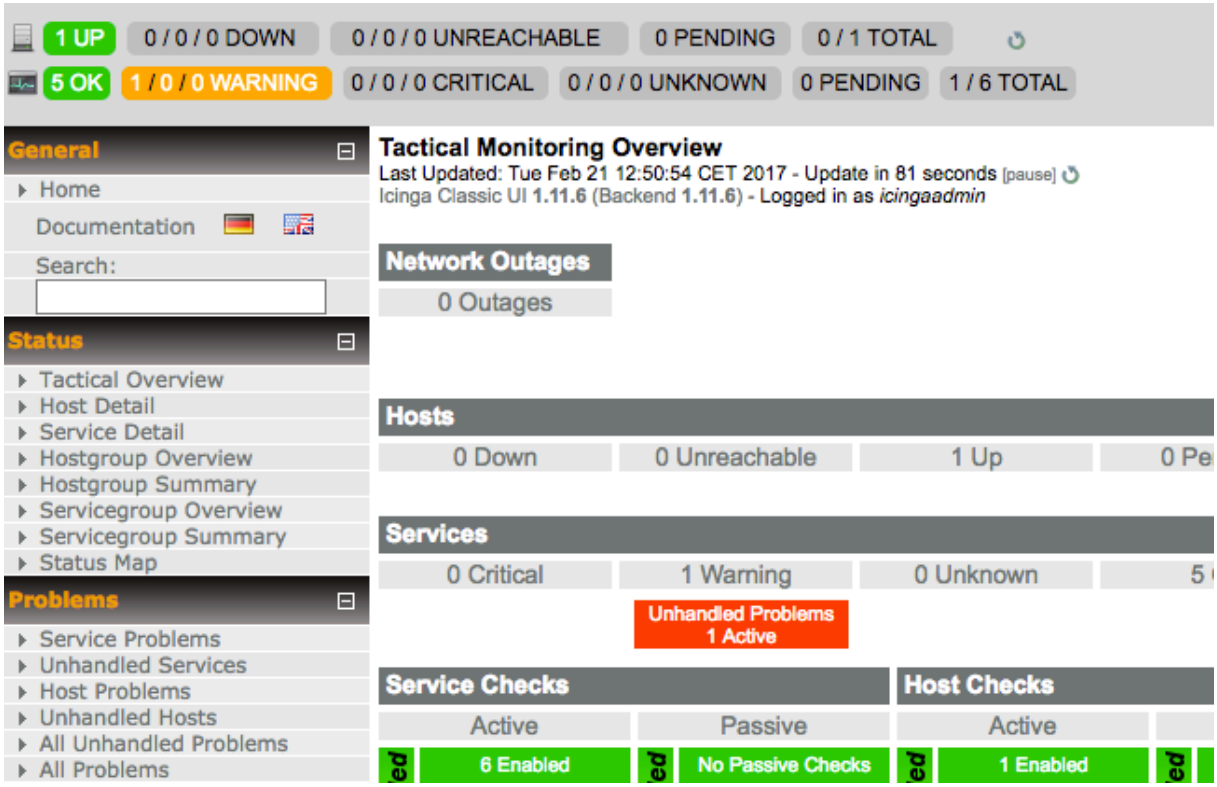
Définition

Définition : La supervision consiste à l'analyse et l'acquisition de données provenant d'outils physique ou numérique auquels il est possible de passer des paramètres ajustant la criticité du retour de ces derniers que l'on peut appeler sonde.

Dans le monde de l'informatique il existe énormément d'outils qui permetent de faire de la supervision. les plus connus sont :

- NAGIOS / ICINGA
- CENTREON
- CACTI

Nous allons ici voire les services et les processus d'une machine sous linux qu'un outils de supervision peut surveiller.



Surveiller quoi ?

Linux comme vous l'avez vu depuis le début est un outils puissant mais qui nécessite un minimum de connaissance.

Cependant il est important de s'équiper afin d'être outiler pour comprendre l'état de son Système d'Information.

L'outils de superision est installé sur une machine en local mais les sondes ne sont pas forcement local et peuvent être sur d'autre machines.

Nous allons prendre l'exemple de Nagios/Icinga/Nrpe . Il s'agit d'un ensemble d'outils et de pluggin permétant la suprevision sous linux. Nagios étant surtout le plus répendu.

Sonde en local

Périmètre

Les sondes qui vérifie l'état local de la machine :

Une sonde est sensiblement constituée de 2 manières :

- Bolleen
- Range

Les Sondes dites "locals" sont executées sur l'instance avec un retour sur la même instances

Sonde Booleen

* Une sonde de type boolen (Oui/Non)

```
1  #!/bin/bash
2  [[ -f $1 ]] && (echo "OK "; exit 0) || (echo "CRIT "; exit 2)
```

- $1 récupère l'arguement envoyé à la sonde
- && Si la condition précédente est vrai
- || Si la condition précédente est fausse

Sonde Range

Range dans le sens "sonde bornée" par des métrique spécifique à la sonde

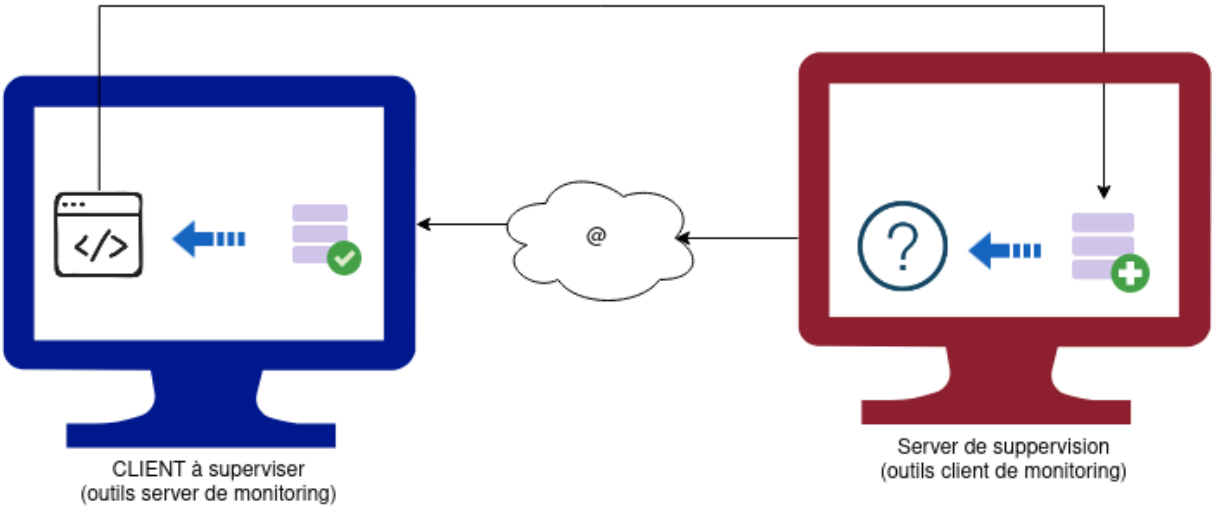
```
1  #!/bin/bash
2
3  Min=$1
4  Max=$2
5  Get=$(who | wc -l)
6
7  [[ ${Get} -lt $Min ]] && (Txt="OK"; Val=0)
8  [[ ${Get} -ge $Min ]] && (Txt="WARN"; Val=1)
9  [[ ${Get} -ge $Max ]] && (Txt="CRIT"; Val=2)
10 echo "${Txt} : We are $Get"
11 exit $Val
```

Sonde “réseau”

Périmètre

Une sonde de type réseau est la plus part du temps un appel à une sonde locals et ceux par le réseau

Un Server de suppervision va communiquer à un client d’executer une sonde et va attendre son retour pour enregistrer le status de la sonde.



Exemple de sonde d’analyse de service

Généralitée

La plus GRANDE majoritée des service de monitoring fonctionne de cette manière :

- Le client execute un script simple que seul le client peut éxecuté
- Le client peut recevoir des demandes des instances de suppervisions
- L’instance de suppervision ne peut pas demander directement à executé un script mais une sonde sur le client distant

Postula

- La machine central-log doit avoir le service de réception des logs de tous le réseau actif (syslog-ng)
- Le monitoring est suppreviser par la machine supp-admin

Le scirpt sur central-log

```
#!/bin/bash
SerivceUp=$(ps axf| grep -w $1 | grep -v grep)
[[ -z ${SerivceUp} ]] && (Txt=CRIT;Out=2) || (Txt=OK;Out=0)
echo "Service $1 is $Txt"
exit $Out
```

Conf sur supp-admin

supp-admin va demander à central-log de lancer la sonde *IsServiceUp* avec comme arguement syslog-ng

supp-admin ne connait pas le code qui va être executé sur central-log

Conf sur central-log

Ici nous devons configurer notre client pour qu'il accepte les requêtes de supp-admin + les arguments des sondes demandées