Telecommunications

RE221

Rapport

Administration d'un service WEB

Etudiants :
Baudry Alexandre
(abaudry10@gmail.com)
Bousquet Nicolas
(nbousquet001@bordeaux-inp.fr)

Professeurs :
Baptiste Lagardère
Gaylord Saint-James

13 mai 2022

Table des matières

1 Introduction

Pour s'assurer que les services réseau fonctionnent bien, il est important de surveiller les systèmes qui le composent. Il est possible d'obtenir des alertes dès qu'un dysfonctionnement apparait, ou alors de pouvoir regarder un élément du système d'information sur la durée à l'aide de graphiques. La surveillance du système se fait avec des outils de supervision (monitoring) qui sont des processus automatiques définis par l'administrateur système afin de l'alerter dès qu'un processus est dysfonctionnel.

2 Définitions

2.1 HTTP

Le service **HTTP** ou Hypertext Transfer Protocol, est un protocole de transmission permettant à l'utilisateur d'accéder à des pages web par l'intermédiaire d'un na- vigateur.

Une définition simple de service pour superviser un service HTTP sur la machine remotehost pourrait ressembler à ceci :

```
define service {
    use                 generic-service ; Inherit default values from a template
    host_name           remotehost
    service_description HTTP
    check_command       check_http
}
```

FIGURE 1 – Définition de service pour superviser un service HTTP

2.2 SMTP

Le service **SMTP** ou Simple Mail Transfer Protocol, désigne un protocole standardisé de communication. Il est principalement employé pour le transfert du courrier électronique d'un serveur à un autre.

Une définition simple de service pour superviser un serveur SMTP sur remotehost devrait ressembler à ceci :

```
define service {
    use                 generic-service ; Inherit default values from a template
    host_name           remotehost
    service_description SMTP
    check_command       check_smtp
}
```

FIGURE 2 – Définition de service pour superviser un service SMTP

2.3 IMAP

Le service **IMAP** ou Internet Message Access Protocol, désigne un protocole permet- tant l'accès direct à ses courriers électronique sur un serveur de messagerie.

Les parties des fichiers de configurations donnant les définitions sont les suivants :

Une définition simple de service pour superviser un serveur IMAP4 sur remotehost devrait ressembler à ceci :

```
define service {
    use                 generic-service ; Inherit default values from a template
    host_name           remotehost
    service_description IMAP
    check_command       check_imap
}
```

Supervision IMAP

FIGURE 3 – Définition de service pour superviser un service IMAP

Les test de ces services sont effectués ci-dessous :

```
define service{
        use                             generic-service
        host_name                       localhost
        service_description             HTTP
                check_command                   check_http
        }

define service{
        use                             generic-service
        host_name                       localhost
        service_description             SMTP
                check_command                   check_smtp
        }

define service{
        use                             generic-service
        host_name                       localhost
        service_description             IMAP
                check_command                   check_imap
        }
```

FIGURE 4 – Test des services

Host	Service	Status	Last Check	Duration	Attempt	Status Information
localhost	Current Load	OK	2022-05-04 09:35:11	0d 0h 34m 30s	1/4	OK - load average: 0.00, 0.05, 0.31
	Current Users	OK	2022-05-04 09:35:49	0d 0h 33m 52s	1/4	USERS OK - 3 users currently logged in
	Disk Space	OK	2022-05-04 09:36:26	0d 0h 33m 15s	1/4	DISK OK
	HTTP	OK	2022-05-04 09:37:04	0d 0h 32m 37s	1/4	HTTP OK: HTTP/1.1 200 OK - 10975 bytes in 0.000 second response time
	IMAP	CRITICAL	2022-05-04 09:37:41	0d 0h 32m 0s	1/4	connect to address 127.0.0.1 and port 143: Connection refused
	SMTP	CRITICAL	2022-05-04 09:38:19	0d 0h 31m 22s	1/4	connect to address 127.0.0.1 and port 25: Connection refused
	SSH	OK	2022-05-04 09:38:56	0d 0h 30m 45s	1/4	SSH OK - OpenSSH_6.7p1 Debian-5+deb8u8 (protocol 2.0)
	Total Processes	OK	2022-05-04 09:39:34	0d 0h 30m 7s	1/4	PROCS OK: 186 processes

FIGURE 5 – Interface web de Nagios

3 Logiciel Nmap

Le logiciel Nmap est disponible depuis les dépôts logiciels de Debian en version 7.40 avec le paquet nmap. apt install nmap Le logiciel Nmap consiste en un binaire d'exploration réseau, qui permet de réaliser des audits de sécurité. Il a été conçu pour analyser rapidement de très grands réseaux. Il est également possible de l'utiliser sur une seule cible.

Le logiciel Nmap est capable d'effectuer de nombreux tests en interrogeant une ou plusieurs cibles. Le rapport de sortie du logiciel se résume en une liste des cibles analysées avec une liste correspondant au numéro de port, au protocole utilisé et au nom du service avec son état. Le logiciel suit toujours la syntaxe suivante : **nmap -options adresse_ip_des_cibles**

3.1 Résultat de la commande Nmap

La commande avec nmap permettant de récupérer le maximum d'informations sur notre poste (Logiciels et ports) est : **nmap -sS -sU -sV 172.18.1.111**

Le résultat de la commande est le suivant :

```
root@exp1-11:/# nmap -sS -sU -sV 172.18.1.111

Starting Nmap 6.47 ( http://nmap.org ) at 2022-05-13 09:21 CEST
Nmap scan report for exp1-11.retel.enseirb (172.18.1.111)
Host is up (0.000064s latency).
Not shown: 1995 closed ports
PORT    STATE         SERVICE VERSION
22/tcp  open          ssh     OpenSSH 6.7p1 Debian 5 (protocol 2.0)
80/tcp  open          http    Apache httpd 2.4.10 ((Debian))
111/tcp open          rpcbind 2-4 (RPC #100000)
68/udp  open|filtered dhcpc
111/udp open          rpcbind 2-4 (RPC #100000)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at http://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 384.86 seconds
root@exp1-11:/#
```

FIGURE 6 – Résultat de la commande Nmap

4 Configuration de notre connexion à distance

4.1 Modifiez le port d'écoute de SSH

On modifie le port d'écoute SSH en accedant au fichier de configuration **/etc/ssh/sshd_config**

```
  GNU nano 2.2.6               File: sshd_config

# Package generated configuration file
# See the sshd(8) manpage for defails

# What ports, IPs and protocols we listen for
#Port 22
Port 23
```

FIGURE 7 – Résultat de la commande Nmap

4.2 Conexion en SSH avec un compte innexistant

Lorsque l'on tente de se connecter en ssh à l'aide d'un compte innexistant on obtient le resultat suivant :

FIGURE 8 – Test de connexion SSH avec un compte innexistant

La liste des ces logs se trouve dans le fichier **/var/log/auth.log**

5 Contrôle des accès réseaux : le pare-feu

5.1 Commandes iptables pour les services suivants

5.1.1 SSH

```
1 #SSH
2 iptables -A INPUT -i eth2 --protocol tcp --source-port 22 -m state --state ...
      ESTABLISHED -j ACCEPT
3 iptables -A OUTPUT -o eth2 --protocol tcp --destination-port 22 -m state ...
      --state NEW,ESTABLISHED -j ACCEPT
```

5.1.2 Port 25 pour SMTP

```
1 #SMTP
2 iptables -A INPUT -i eth2 --protocol tcp --source-port 25 -m state --state ...
      ESTABLISHED -j ACCEPT
3 iptables -A OUTPUT -o eth2 --protocol tcp --destination-port 25 -m state ...
      --state NEW,ESTABLISHED -j ACCEPT
```

5.1.3 Ports 110 et 143 pour pop et imap

```
1 #POP / IMAP
2 iptables -A INPUT -i eth2 --protocol tcp --source-port 110 -m state --state ...
      ESTABLISHED -j ACCEPT
3 iptables -A OUTPUT -o eth2 --protocol tcp --destination-port 110 -m state ...
      --state NEW,ESTABLISHED -j ACCEPT
4 iptables -A INPUT -i eth2 --protocol tcp --source-port 143 -m state --state ...
      ESTABLISHED -j ACCEPT
5 iptables -A OUTPUT -o eth2 --protocol tcp --destination-port 143 -m state ...
      --state NEW,ESTABLISHED -j ACCEPT
```

5.1.4 Port 443 pour HTTPS

```
1 #HTTPS
2 iptables -A INPUT -i eth2 --protocol tcp --source-port 443 -m state --state ...
      ESTABLISHED -j ACCEPT
3 iptables -A OUTPUT -o eth2 --protocol tcp --destination-port 443 -m state ...
      --state NEW,ESTABLISHED -j ACCEPT
```

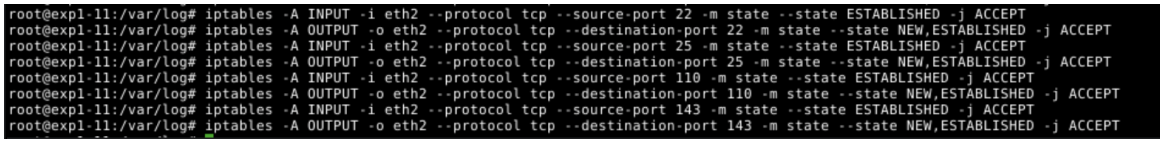

FIGURE 9 – Commandes iptables

Pour vérifier les règles en cours sur la machine locale, on utilise l'option -L de la commande iptables :

iptable -L

```
root@exp1-11:/var/log# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere            tcp spt:ssh state ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere            tcp spt:ssh state ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere            tcp spt:smtp state ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere            tcp spt:pop3 state ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere            tcp spt:imap2 state ESTABLISHED

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:ssh state NEW,ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:ssh state NEW,ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:smtp state NEW,ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:pop3 state NEW,ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:imap2 state NEW,ESTABLISHED
```

FIGURE 10 – Règles en cours sur la machine locale