TP 4 : Supervision avec Nagios

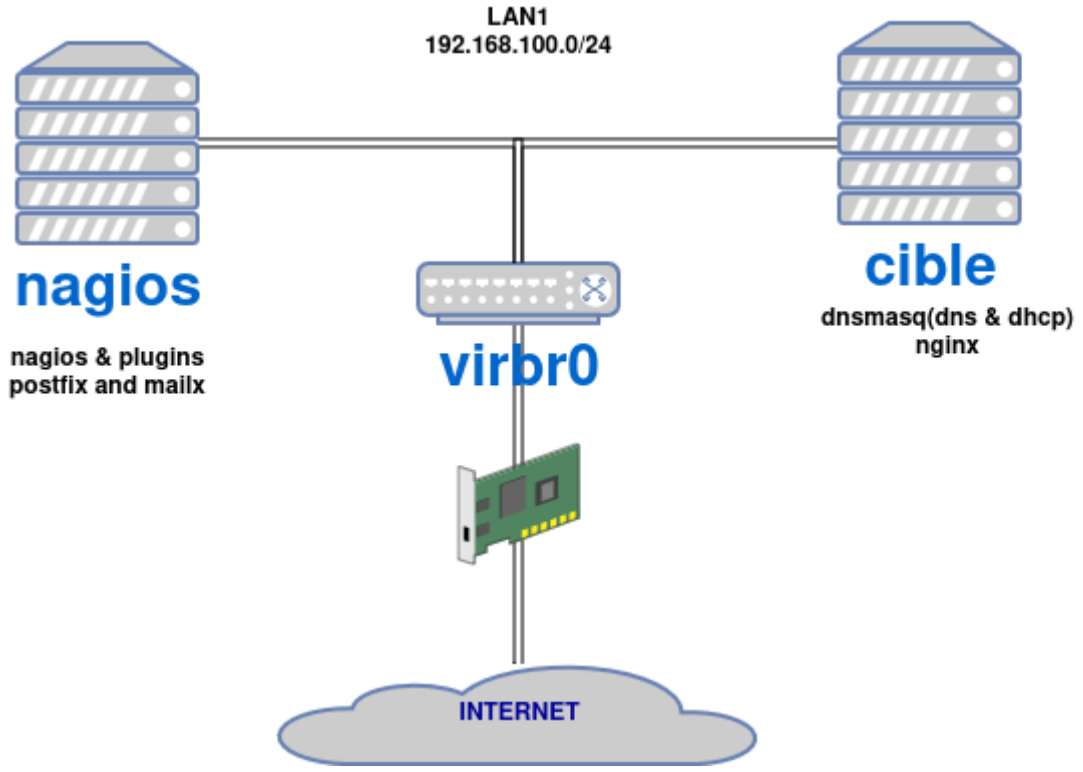
Objectif

Mettre en place une solution de supervision réseau basique avec Nagios pour surveiller les services critiques du réseau, notamment DNS, DHCP, ainsi que les hôtes dans le réseau.

Outils

- **Nagios** : Outil de supervision réseau.
- **Libvirt, KVM, cloud-init** : Outils de virtualisation.
- **Linux (Alpine)** : Système d'exploitation pour installer et configurer Nagios et la machine cible.

Plan du TP



0. Configuration de base

```
.
├── cible.cfg                  # Contient la config de base cloud-init de la
machine cible
├── cible.sh                   # Permet de créer la VM cible
├── clean_net.sh               # Permet de supprimer tous les réseaux sauf
"default"
├── clean_vm.sh                # Permet de supprimer les VM Nagios et cible
├── lan1.xml                   # Permet de créer le réseau lan1
├── nagios.cfg                 # Contient la config de base cloud-init de la VM
Nagios
└── nagios.sh                  # Permet de créer la VM Nagios
```

1. Installation de Nagios

1. **Pré-requis : Création du réseau lan1**
   - Lancer le script :

     ```
     ./create_net.sh
     ```

   - Vérifier que lan1 est bien créé :

     ```
     zprojet@ares18:~/tps/tp4/TP4$ virsh net-list
     Name      State    Autostart   Persistent
     --------------------------------------------
     default   active   yes         yes
     lan1      active   yes         yes
     ```

   - Le fichier `./create_net.sh` permet de créer le réseau lan1 à partir du fichier `lan1.xml` comme dans les TP précédents.
2. **Pré-requis : Création de la VM Nagios**
   - Lancer le script :

     ```
     ./nagios.sh
     ```

   - Le fichier `nagios.sh` permet d'automatiser la création de la VM Nagios avec cloud-init. N'hésitez pas à lire le contenu du fichier pour comprendre les commandes exécutées.
3. **Accès à l'interface web**
   - Vous pouvez maintenant accéder à l'interface web de Nagios via l'URL suivante : `http://<adresse_IP_VM>/nagios`. Utilisez les identifiants `nagiosadmin` pour le nom d'utilisateur et `nagiosadmin` pour le mot de passe.
4. **Pré-requis : Création de la VM Cible**
   - Lancer le script :

     ```
     ./cible.sh
     ```

   - Le fichier `cible.sh` permet d'automatiser la création de la VM cible avec cloud-init. N'hésitez pas à lire le contenu du fichier pour comprendre les commandes exécutées.

2. Supervision des services DNS et DHCP

1. **Surveillance du service DNS**
   - Dans le fichier de configuration des hôtes et services de Nagios, ajouter un bloc pour l'hôte cible :

     ```
     define host {
         use                     linux-server
         host_name               cible
         alias                   cible
         address                 <address_ip_cible>
     }
     ```

Attention : vous devez récupérer l'adresse IP de la machine cible. Pour cela, utilisez `virsh console cible` pour vous connecter à la VM cible.

- Ajouter l'hôte cible au groupe `linux-servers` :

```
define hostgroup {
    hostgroup_name          linux-servers
    alias                   linux-servers
    members                 localhost,cible
}
```

- Ajouter un bloc pour surveiller le service DNS dans `/etc/objects/localhost.cfg` :

```
define service {
    use                     generic-service
    host_name               cible
    service_description     DNS Service
    check_command           check_dns!google.com!$HOSTADDRESS$
}
```

- Ajouter une commande `check_dns` dans `/etc/objects/commands.cfg` si elle n'existe pas :

```
define command {
    command_name    check_dns
    command_line    $USER1$/check_dns -H $ARG1$
}
```

- Relancer le service Nagios pour appliquer la configuration :

```
sudo systemctl restart nagios
```

- Vérifier dans l'interface web de Nagios que le service DNS est au vert. /!\ Attention : il faut attendre environ 5 minutes pour voir la mise à jour. Ce temps peut être changé dans le fichier `template.cfg`, bloc `local-service`, variable `check_interval`.

2. **Surveillance du service DHCP**

- Ajouter une vérification pour le service DHCP dans `/etc/objects/localhost.cfg` :

```
define service {
    use                     generic-service
    host_name               cible
    service_description     DHCP Service
    check_command           check_dhcp!$HOSTADDRESS$
}
```

- Ajouter une commande pour le service DHCP dans `/etc/objects/commands.cfg` si elle n'existe pas :

```
define command {
    command_name    check_dhcp
    command_line    $USER1$/check_dhcp -s $ARG1$ -i $ARG2$
}
```

- Relancer le service Nagios :

```
sudo systemctl restart nagios
```

- Vérifier dans l'interface web de Nagios que le service DHCP est au vert. /!\ Attention : il faut attendre environ 5 minutes pour voir la mise à jour.

3. Supervision des hôtes

1. **Ajout d'un nouveau service à surveiller (le serveur NGINX déployé sur la cible)**
   - Pour surveiller le service NGINX, ajouter un service dans `/etc/objects/localhost.cfg` :

```
define service {
    use                     generic-service
    host_name               cible
    service_description     CHECK NGINX
    check_command           check_http!$HOSTADDRESS$!5!10
}
```

2. **Redémarrer Nagios pour appliquer la nouvelle configuration** :

```
sudo systemctl restart nagios
```

Vérifier dans l'interface web de Nagios que le service NGINX répond et est au vert. /!\ Attention : il faut attendre environ 5 minutes pour voir la mise à jour.

4. Configuration d'alertes et tableau de bord

1. **Configurer les alertes par e-mail**
   - L'envoi d'e-mails est optionnel. Vous pouvez laisser cette partie. Pour les courageux, dans le fichier `nagios.cfg`, des commandes de configuration de Postfix sont présentes pour l'envoi des mails. Il faudra remplacer les paramètres par les vôtres.
   - Configurer la commande pour l'envoie de mails dans les fichier `/etc/objects/commands.cfg` , vous pouvez remplacer nagios@ares.fr par votre @gmail:

```
define command {
command_name    notify-host-by-email
command_line    /usr/bin/printf "%b" "***** Nagios *****\n\nNotification
Type: $NOTIFICATIONTYPE$\nHost: $HOSTNAME$\nState: $HOSTSTATE$\nAddress:
$HOSTADDRESS$\nInfo: $HOSTOUTPUT$\n\nDate/Time: $LONGDATETIME$\n" |
/usr/bin/mail  -r nagios@ares.fr -s "** $NOTIFICATIONTYPE$ Host Alert:
$HOSTNAME$ is $HOSTSTATE$ **" $CONTACTEMAIL$
}

define command {
command_name    notify-service-by-email
command_line    /usr/bin/printf "%b" "***** Nagios *****\n\nNotification
Type: $NOTIFICATIONTYPE$\n\nService: $SERVICEDESC$\nHost:
$HOSTALIAS$\nAddress: $HOSTADDRESS$\nState: $SERVICESTATE$\n\nDate/Time:
$LONGDATETIME$\n\nAdditional Info:\n\n$SERVICEOUTPUT$\n" |  /usr/bin/mail
-r nagios@ares.fr -s "** $NOTIFICATIONTYPE$ Service Alert:
$HOSTALIAS$/$SERVICEDESC$ is $SERVICESTATE$ **" $CONTACTEMAIL$
}
```

- Configurer l'envoi d'e-mails pour les alertes dans `/etc/objects/contacts.cfg` :

```
define contact {
    contact_name                    nagiosadmin
    use                             generic-contact
    alias                           Nagios Admin
    email                           admin@gmail.com
}
```

  Remplacez `admin@gmail.com` par l'adresse e-mail à laquelle vous souhaitez recevoir les alertes.

- La notification d'un hôte ou d'un service s'obtient en modifiant la période et en activant la notification sur l'hôte ou le service concerné.

```
define host {
    use                     linux-server
    host_name               cible
    alias                   cible
    address                 192.168.100.154
    notifications_enabled   1                # activer la notification
    max_check_attempts      10
    check_period            24x7
    notification_interval   2                # interval d'envoie
    notification_period     24x7
}
```

- **Redémarrer Nagios pour appliquer la nouvelle configuration** :

```
sudo systemctl restart nagios
```

Vérifier dans l'interface web de Nagios que les notificatio sont émises

```
Dans le panneau latéral gauche, cliquez sur Hosts, puis sélectionnez l'hôte
concerné et observez la ligne :
Last Notification:  10-10-2024 07:14:59 (notification ...)
```

2. **Tableau de bord**
    - Vous pouvez accéder au tableau de bord Nagios via le navigateur web à l'adresse `http://<IP_VM>/nagios` pour visualiser en temps réel l'état des hôtes et services supervisés ainsi que les alertes générées.

Suivi post-TP

vous devez fournir :

- La configuration des hôtes et services supervisés dans Nagios.
- Une capture d'écran du tableau de bord Nagios montrant l'état des services et des hôtes.
- Un exemple d'alerte reçue par e-mail (optionnelle).