Gestion et Surveillance de Réseau

Création de tickets Cacti, Nagios et Smokeping avec Request Tracker

Notes :

* Les commandes précédées de "$" signifient que vous devez exécuter la commande en tant qu'utilisateur général - et non en tant qu'utilisateur root.
* Les commandes précédées de "#" signifient que vous devez travailler en tant qu'utilisateur root.
* Les commandes comportant des lignes de commande plus spécifiques (par exemple "RTR-GW>" ou "mysql>") signifient que vous exécutez des commandes sur des équipements à distance, ou dans un autre programme.

Exercices

À ce stade de la semaine, Cacti, Nagios et Smokeping devraient être installés sur vos PC. Ces exercices vous montrent comment configurer chacun de ces programmes pour envoyer des alertes au système de tickets RT (Request Tracker) afin de générer des tickets.

Exercices Partie I

0. Ouvrez une session sur votre PC ou ouvrez une fenêtre de terminal en tant qu'utilisateur sysadm.

1. Vérifiez que rt-mailgate a été configuré pour fonctionner avec votre agent MTA

Ouvrez le fichier /etc/aliases :

```
$ sudo editor /etc/aliases
```

Le fichier /etc/aliases devrait comporter les deux lignes suivantes :

```
net-comment: "|/usr/bin/rt-mailgate --queue net --action comment --
url http://localhost/rt/"
net:        "|/usr/bin/rt-mailgate --queue net --action correspond
```

--url http://localhost/rt/"

Si ces lignes ne figurent pas /etc/aliases, veillez à les ajouter. Lorsque vous avez terminé, enregistrez le fichier et quittez. Vous devez ensuite indiquer au MTA (agent de transfert de messagerie) qu'il y a de nouveaux alias à utiliser :

```
$ sudo newaliases
```

2. Configurez Smokeping

Dans le fichier :

```
/etc/smokeping/config.d/Alerts
```

Vous pouvez indiquer à Smokeping où envoyer les alertes. Editez le fichier :

```
$ sudo vi /etc/smokeping/config.d/Alerts
```

Et modifiez le début du fichier comme suit :

```
*** Alerts ***
to = net@localhost
from = smokealert@localhost
```

À la fin du fichier, ajoutez une autre alerte comme ceci :

```
+anydelay
type = rtt
# in milliseconds
pattern = >1
comment = Just for testing
```

Veillez à ce que tout le texte du fichier soit aligné à gauche.

Maintenant sauvegardez le fichier et quittez.

Observez le "pattern" (forme) de cette alerte. Cela signifie qu'une alerte sera déclenchée dès qu'une mesure présentera un retard supérieur à un millième de seconde. Il s'agit juste d'un test. Dans la réalité, vous créerez une alerte en fonction des valeurs de références observées. Par exemple, si le délai de vos serveurs DNS passe subitement de moins de 10 ms à plus de 100 ms.

Vérifiez ensuite que des alertes sont définies pour certains de vos fichiers Targets.
Vous pouvez activer les alertes en les définissant pour une sonde dans le fichier /etc/smokeping/config.d/Probes, ou sous la forme d'entrées Targets individuelles.

Dans le cas présent, nous allons modifier le fichier Targets et activer les alertes pour nos contrôles de latence DNS.

```
$ sudo vi /etc/smokeping/config.d/Targets
```

Recherchez (ou ajoutez si nécessaire) la section suivante dans le fichier :

```
+DNS
probe = DNS
        ...
```

Nous allons maintenant ajouter une entrée pour un serveur DNS global répondant de manière récursive.

```
++GoogleA
menu = 8.8.8.8
title = DNS Latency for google-public-dns-a.google.com
host = google-public-dns-a.google.com
alerts = anydelay
```

Observez la présence d'une ligne "alerts=anydelay".

Pour résumer, la section suivante devrait donc être présente vers la fin de votre fichier Targets :

```
+DNS
probe = DNS
menu = DNS Latency
title = DNS Latency Probes

++GoogleA
menu = 8.8.8.8
title = DNS Latency for google-public-dns-a.google.com
host = google-public-dns-a.google.com
alerts = anydelay
```

(Les éléments doivent être alignés à gauche dans le fichier).

Enregistrez et fermez le fichier, puis redémarrez Smokeping :

```
    $ sudo service smokeping restart
```

Maintenant, vérifiez dans RT si vous avez reçu quelque chose de Smokeping. L'apparition d'un nouveau ticket peut prendre jusqu'à 5 minutes.

REMARQUE : - Si vous n'avez pas déjà configuré les contrôles de latence DNS pour Smokeping vous devrez modifier le fichier /etc/smokeping/config.d/Probes et ajouter l'entrée DNS comme ceci :

```
        $ sudo vi /etc/smokeping/config.d/Probes
```

À la fin du fichier, ajoutez :

```
        + DNS
        binary = /usr/bin/dig
        pings = 5
        step = 180
        lookup = www.nsrc.org
```

Enregistrez et fermez le fichier, puis redémarrez Smokeping :

```
        $ sudo service smokeping restart
```

3. Nagios et création de tickets avec Request Tracker

Pour configurer RT et Nagios afin que les alertes Nagios génèrent automatiquement des tickets vous devez suivre la procédure suivante :

* Créez une entrée de contact appropriée pour Nagios dans /etc/nagios3/conf.d/contacts_nagios2.cfg

* Créez la commande appropriée dans Nagios pour utiliser l'interface rt-mailgate. La commande est définie dans /etc/nagios3/commands.cfg

Les deux étapes suivantes devraient déjà avoir été réalisées dans RT si vous avez terminé les exercices RT.

* Installez le logiciel rt-mailgate et configurez-le correctement dans votre fichier /etc/aliases pour l'agent MTA que vous utilisez.

* Configurez les files d'attente requises dans RT afin de recevoir les e-mails que lui transmet Nagios via rt-mailgate.

5. Configurez un Contact dans Nagios

   - Modifiez le fichier /etc/nagios3/conf.d/contacts_nagios2.cfg

   $ sudo bash
   # vi /etc/nagios3/conf.d/contacts_nagios2.cfg

   - Dans ce fichier, nous allons d'abord ajouter un nouveau nom de contact sous l'entrée de contact root par défaut. Le nouveau contact devrait ressembler à ceci :

```
define contact{
        contact_name                    net
        alias                           RT Alert Queue
        service_notification_period     24x7
        host_notification_period        24x7
        service_notification_options    c
        host_notification_options       d
        service_notification_commands   notify-service-ticket-by-
email
        host_notification_commands      notify-host-ticket-by-email
        email                           net@localhost
        }
```

   - NE SUPPRIMEZ PAS la ligne contact_name "root"!! Cette entrée va en dessous du contact "root".

   - la valeur "c" spécifiée sur la ligne "service_notification_option" signifie d'envoyer une notification uniquement lorsqu'un service est considéré comme "critique" par Nagios (c'est-à-dire arrêté). La valeur "d" en "host_notification_option" signifie arrêt. Le fait de spécifier uniquement "c" et "d" signifie qu'aucune notification ne sera envoyée pour d'autres états.

   - Notez l'adresse e-mail utilisée "net @ localhost" – c'est important car elle a été précédemment définie pour RT.

   - Nous devons maintenant créer un Groupe de contact contenant ce contact.
     Nous appellerons ce groupe "tickets". Tapez ceci à la fin du fichier :

```
define contactgroup{
        contactgroup_name       tickets
```

```
        alias                   email to ticket system for RT
        members                 net,root
        }
```

   - Vous pourriez supprimer le membre "root", mais nous l'avons conservé afin qu'un autre utilisateur reçoive l'e-mail et nous aide à dépanner en cas de problèmes.

   - Maintenant que votre contact est créé, vous devez créer les commandes mentionnées à l'étape initiale de création de contact ci-dessus, à savoir "notify-service-ticket-by-email" et "notify-host-ticket-by-email".

6. Mettez à jour les commandes Nagios

   - Pour créer les commandes "notify-service-ticket-by-email" et "notify-host-ticket-by-email" vous devez modifier le fichier /etc/nagios3/commands.cfg.

   # vi /etc/nagios3/commands.cfg

  - Ce fichier contient déjà deux définitions de commandes que nous utilisons. Il s'agit des commandes "notify-host-by-email" et "notify-service-by-email". Nous allons ajouter deux nouvelles commandes.

  - Nous vous conseillons fortement de COPIER-COLLER le texte ci-dessous. Il est presque impossible de le taper sans erreurs.

  - Placez ces deux nouvelles entrées _SOUS_ les commandes actuelles "notify-host-by-email" et "notify-service-by-email". Ne supprimez pas les anciennes.

  - REMARQUE : Les commandes ci-dessous ne contiennent pas de sauts de lignes. Il s'agit d'une seule ligne. Soyez vigilent car la fonction COPIER-COLLER peut insérer des sauts de ligne en fonction des éditeurs et de l'environnement.

```
################################################################
# Commandes supplémentaires créées pour l'atelier de gestion de
réseau #
################################################################

# 'notifiy-host-ticket-by-email' command definition
define command{
```

```
        command_name    notify-host-ticket-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 -s "** $NOTIFICATIONTYPE$
Host Alert: $HOSTNAME$ is $HOSTSTATE$ **" $CONTACTEMAIL$
        }

# 'notify-service-ticket-by-email' command definition
define command{
        command_name    notify-service-ticket-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$SERVICEOUTPUT$"
| /usr/bin/mail -s "** $NOTIFICATIONTYPE$ Service Alert: $HOSTALIAS
$/$SERVICEDESC$ is $SERVICESTATE$ **" $CONTACTEMAIL$
        }
```

7. Choisissez un service à surveiller avec des tickets RT

- La dernière étape consiste à indiquer à Nagios que vous souhaitez adresser des notifications au contact "tickets" à propos d'un service particulier. Si vous regardez dans le fichier /etc/nagios3/conf.d/generic-service_nagios2.cfg, vous verrez que le groupe de contact (contact_groups) par défaut est "admins". Pour changer ceci pour un service, modifiez le fichier /etc/nagios3/conf.d/services_nagios2.cfg et l'entrée "contact_groups" d'une des définitions de service.

- Pour envoyer un e-mail afin que des tickets soient générés dans RT en cas d'arrêt HTTP dans une boîte, vous devez modifier le contrôle de service SSH de la façon suivante :

```
# check that web services are running
define service {
        hostgroup_name                  http-servers
        service_description             HTTP
        check_command                   check_http
        use                             generic-service
        notification_interval           0 ; spécifiez une valeur > 0
si vous voulez être renotifié
        contact_groups                  tickets
}
```

Notez l'élément supplémentaire que nous avons maintenant,"contact_groups". Vous pouvez procéder de même pour d'autres entrées si vous le souhaitez.

- Lorsque vous avez terminé, enregistrez le fichier et quittez.

- Redémarrez maintenant Nagios pour vérifier que vos modifications sont correctes.

```
# /etc/init.d/nagios3 stop
# /etc/init.d/nagios3 start
```

4.) Générez des tickets RT pour les hôtes

- Pour ce faire, vous devez spécifier "contact_groups tickets" pour les définitions des différents hôtes ou bien modifier le fichier modèle de tous les hôtes et remplacer l'entrée contact_groups par défaut des tickets. Ce fichier est generic-host_nagios2.cfg.

- Si c'est ce que vous souhaitez, allez-y. Des tickets seront générés si un hôte tombe en panne et que vous avez spécifié "tickets" comme "contact_groups" pour cet hôte.

5. Visualisez les tickets Nagios dans RT

Pour vérifier que vos modifications ont été prises en compte, vous pouvez opérer une surveillance HTTP sur l'un de nos serveurs qui n'exécute pas HTTP. Nous allons prendre le second Mac Mini de notre classe ou la boîte désignée "s1.ws.nsrc.org" (voir le schéma du réseau pour plus de détails).

Si vous n'avez pas d'entrée pour cette machine, complétez le fichier dans lequel vos PC sont définis. S'il s'agit d'un fichier nommé pcs.cfg, procédez comme suit :

```
# vi /etc/nagios3/conf.d/pcs.cfg
```

Dans ce fichier, ajoutez (ou vérifiez qu'il y a) une entrée ressemblant à ceci :

```
define host {
    use         generic-host
```

```
    host_name   s1
    alias       s1
    address     10.10.0.241
    parents     sw
}
```

Enregistrez et fermez le fichier.

Maintenant, éditez le fichier nommé /etc/nagios3/conf.d/ hostgroups_nagios2.cfg et ajoutez s2 au groupe d'hôtes pour les contrôles de services http :

```
        # vi /etc/nagios3/conf.d/hostgroups_nagios2.cfg
```

Recherchez l'entrée "hostgroup_name http-servers" et modifiez-la comme suit :

```
# A list of your web servers
define hostgroup {
        hostgroup_name  http-servers
                alias           HTTP servers
                members
localhost,pc1,pc2,pc3,pc4,pc5,pc6,pc7,pc8,pc9,pc10,pc11,pc12,

pc13,pc14,pc15,pc16,pc17,pc18,pc19,pc20,pc21,pc22,pc23,pc24,

pc25,pc26,pc28,pc29,pc30,pc31,pc32,pc35,pc37,pc39,s1
        }
```

N'OUBLIEZ PAS que la ligne listant tous les "membres" ne doit pas comporter de sauts de ligne. Notez que "s1" a été ajouté en fin de ligne.

Maintenant, sauvegardez le fichier, quittez et redémarrez Nagios :

```
        # service nagios3 stop
        # service nagios3 start
```

- Il faudra un certain temps (jusqu'à 10 minutes) à Nagios pour signaler que HTTP est à l'état "critique", mais ensuite un nouveau ticket devrait apparaître dans votre instance RT dans la file d'attente réseau (net) générée par Nagios.

- N'oubliez pas de visiter http://pcX.ws.nsrc.org/rt/ et de vous

connecter en tant qu'utilisateur "sysadmin" avec le mot de passe que vous avez choisi lorsque vous avez créé le compte sysadmin RT. Le nouveau ticket devrait apparaître dans la boîte "10 newest unowned tickets" (10 derniers tickets sans propriétaire) sur la page principale de connexion de RT.

6. Configurez Cacti pour envoyer des e-mails à net@localhost et générer des tickets dans RT

Si vous n'avez pas installé l'architecture de plugins de Cacti, veuillez effectuer cet exercice en dernier.

Vous pouvez voir comment cela fonctionne en vous loguant sur l'instance Cacti exécutée sur la boîte noc où est installée l'architecture de plugins Cacti avec les deux plugins nommés "Settings" (paramètres) et "Threshold" (seuil).

Pour voir comment Cacti peut générer un ticket visitez d'abord :

http://noc.ws.nsrc.org/cacti/

Connectez-vous en tant que "admin" (mot de passe système), puis :

* Cliquez sur l'onglet Console (en haut à gauche)
* Cliquez sur "Settings" (en bas à gauche)
* Cliquez sur l'onglet "Mail / DNS" (en haut à droite)
* Vérifiez que les champs pour les e-mails sont correctement remplis :
    - Test Email (sysadm ou net @ localhost)
    - Mail Services (PHP Mail() Function)
    - From Email Address (cacti@localhost)
    - From Name (Cacti System Monitor)
    - SMTP Hostname (localhost)
    - SMTP Port (25)

Nous devons maintenant créer un seuil (threshold) que nous allons utiliser pour déclencher l'envoi d'un e-mail qui, à son tour, va créer un ticket dans RT :

* Cliquez sur "Thresholds" (au milieu à gauche)

* Cliquez sur le bouton "Add" (ajouter),en haut à droite
* Sélectionnez un hôte (localhost, par exemple)
* Sélectionnez un graphique (Processus)
* Sélectionnez la source de données (proc)
* Cliquez sur le bouton "create" (créer)

Un écran détaillé apparaît alors dans lequel vous pouvez spécifier l'action requise en cas d'atteinte du seuil. Vérifiez ou complétez les éléments suivants :

* Threshold Name (nom du seuil): Un nom descriptif
* Vérifiez que la case "Threshold Enabled" (seuil activé) est cochée
* Threshold Type (type de seuil): valeurs hautes (High) / basses (Low) (pour les processus)
* High Threshold (seuil haut): 50 (valeur occasionnant le déclenchement du seuil)
* Breach Duration (durée de l'interruption): 5 minutes (un ticket sera généré sous 5 à 10 minutes)
* Data Type (type de données) : Exact Value (valeur exacte)
* Re-Alert Cycle (cycle de réémission d'alerte): Never (jamais)
* Extra Alert Emails (adresses e-mail d'alerte supplémentaires) : net@localhost,sysadm@localhost

Ceci aura pour effet d'envoyer un e-mail à net@localhost sous 5 à 10 minutes. Un nouveau ticket sera créé dans RT. En outre, un e-mail sera envoyé à sysadm@localhost. Vous pouvez consulter l'e-mail en tant qu'utilisateur sysadm en tapant :

```
$ mutt -f /var/mail/sysadm
```

Vous pouvez créer tous les types d'états de seuil pouvant être déclenchés et entraînant la génération de tickets. N'hésitez pas à utiliser l'instance cacti sur le Noc pour créer de nouveaux seuils. Vous pouvez voir si ces seuils fonctionnent en vous connectant sur l'instance Noc de Request Tracker (RT):

```
http://noc.ws.nsrc.org/rt/
```

Le nom d'utilisateur est "sysadm" et le mot de passe est celui de la classe.

+-----+

Dernière mise à jour : 2 juin 2011
Hervey Allen