

## Nagios et création de tickets 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 "rtrX" ou "mysql>") signifient que vous exécutez des commandes sur des équipements à distance, ou dans un autre programme.

### Exercices

-----

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 opérées 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.

### Exercices

-----

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

#### 1.) Configurez un Contact dans Nagios

-----

- Modifiez le fichier /etc/nagios3/conf.d/contacts\_nagios2.cfg

```
# 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
}

```

- 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. 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".

## 2.) 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. Elles constituent une seule ligne. Soyez vigilant 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 "** $NOTIFICATIONTYPE$\n  
Host Alert: $HOSTNAME$ is $HOSTSTATE$ **" $CONTACTEMAIL$\n  
    }  
  
# '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$SERVICEOUTPUT$\n  
| /usr/bin/mail -s "** $NOTIFICATIONTYPE$ Service Alert: $HOSTALIAS  
$/$SERVICEDESC$ is $SERVICESTATE$ **" $CONTACTEMAIL$\n  
    }  
}
```

### 3.) 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 de coupure SSH dans une boîte, vous devez modifier le contrôle de service SSH de la façon suivante :

```
define service {
    hostgroup_name          ssh-servers
    service_description     SSH
    check_command           check_ssh
    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 vérifiez 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" dans les définitions des différents hôtes ou bien modifier le fichier modèle de tous les hôtes et remplacer l'entrée contact\_groups par défaut par 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 devrez arrêter le service ssh sur votre machine ou une autre machine.

```
# /etc/init.d/ssh stop
```

- Il faudra un certain temps (jusqu'à 10 minutes) à Nagios pour signaler que SSH 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://MyMachine/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.