−Table des matières

Exemples de services monitorés

Mise en place d'un contrôle du RAID logiciel sous Linux (mdadm)

Prérequis

Sur la machine à monitorer

- Nous avons mis à disposition l'ensemble des scripts utilisées dans une archive nommé "monitoring".

Télécharger et décompresser notre archive "monitoring" dans ”/usr/local/bin/monitoring” de la machine à monitorer.

Remarques: contenu de notre archive ”monitoring”
- Nous avons créé le script “monitoring_returncode” afin d'obtenir un code de retour valide traité par le script “check_snmp_extend” lors de son exécution par Nagios.
- Le plugin “check_openvz” a été récupéré sur le site gforge.opensource-sw.net et nous l'avons légèrement modifié pour adapter le format de sortie du script. Ce plugin ne sera pas utilisé dans le cas présent
- Le plugin “nagios-linux-swraid.pl” a été téléchargé depuis site www.logix.cz.
- Le plugin “check_snmp_extend” a été téléchargé depuis le site www.logix.cz.
- Le plugin “check_hparray” a été téléchargé depuis le site de Exchange Nagios. Nous l'avons ensuite légèrement modifié pour adapter le format de sortie du script et activer ou non l'alerte “Warning” pour l'upgrade du firmware HP.

- Installer La librairie Yaml pour Perl (libyaml-perl) sinon gare à l'erreur de dépendance pour le plugin Nagios de Perl:

```
...
Could not read '/root/.cpan/build/Params-Validate-1.07-IrrpPl/META.yml'. Falling back to other methods to determine prerequisites
```

```
apt-get install libyaml-perl
```

- Installer les modules PERL “Nagios::Plugin” et “Net:SNMP”

```
cpan -i Nagios::Plugin Net::SNMP
```

Vous pouvez utiliser l'outil CPANM pour installer vos modules PERL. Cet outil permet d'installer automatiquement les dépendances de chaque module, sans confirmation par l'utilisateur (facilement scriptable donc 😉).

```
wget -O - http://cpanmin.us | perl - --self-upgrade
```

puis

```
cpanm -i Nagios::Plugin Net::SNMP
```

- Installer le paquet “sudo”

Afin de permettre à l'utilisateur qui exécute le daemon SNMP (de la machine à monitorer) d'exécuter les différents plugins de contrôle.

Sur le serveur de monitoring

- Assurez-vous que le paquet “snmp” soit installé. La commande “check_snmp_extend” utilise la commande “snmpget” issue du paquet snmp !

```
apt-get install snmp
```

- Télécharger et décompresser notre archive "monitoring". Copier le plugin nommé “check_snmp_extend” dans votre dossier de plugins Nagios (/usr/local/nagios/libexec/) et attribuer à “check_snmp_extend” les bons droits.

Configuration

Sur la machine à monitorer

- Editer le fichier de configuration de l'outil “sudo” (/etc/sudoers) selon l'exemple ci-dessous:

Adapter les paramètres réseaux à votre infrastructure !

```
# /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the man page for details on how to write a sudoers file.
#

Defaults        env_reset

# Host alias specification
```

```
# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL) ALL

# Host alias specification
Host_Alias NET_AUTH = localhost.localdomain, 192.168.7.0/24, 192.168.12.0/24
#User alias specification
User_Alias MY_USERS = snmp
#Cmnd alias specification
Cmnd_Alias MY_CMD = /usr/local/bin/monitoring/monitoring_returncode

MY_USERS NET_AUTH=(root)NOPASSWD: MY_CMD

# Allow members of group sudo to execute any command
# (Note that later entries override this, so you might need to move
# it further down)
%sudo ALL=(ALL) ALL
#
#includedir /etc/sudoers.d
```

N'oubliez pas de relancer “sudo” après chaque modification de son fichier de conf !

```
/etc/init.d/sudo restart
```

- Editer le fichier de configuration du daemon “snmpd” (/etc/snmp/snmpd.conf) comme dans l'exemple ci-dessous:

```
com2sec readonly  default         public
group MyROSystem v1         paranoid
group MyROSystem v2c        paranoid
group MyROSystem usm        paranoid
group MyROGroup  v1         readonly
group MyROGroup  v2c        readonly
group MyROGroup  usm        readonly
group MyRWGroup  v1         readwrite
group MyRWGroup  v2c        readwrite
group MyRWGroup  usm        readwrite
view all    included  .1                             80
view system included  .iso.org.dod.internet.mgmt.mib-2.system
access MyROSystem ""      any       noauth    exact  system none   none
access MyROGroup  ""      any       noauth    exact  all    none   none
access MyRWGroup  ""      any       noauth    exact  all    all    none
syslocation MON ENTREPRISE, notre rue et numero, mon pays
syscontact MOI <moi@monentreprise>
extend echotest /bin/echo hello world
#
# Pour le contrôle du RAID
# ========================
extend raid-md1 /usr/bin/sudo /usr/local/bin/monitoring/monitoring_returncode "/usr/local/bin/monitoring/nagios-linux-swraid.pl --device=md1"
extend raid-md2 /usr/bin/sudo /usr/local/bin/monitoring/monitoring_returncode "/usr/local/bin/monitoring/nagios-linux-swraid.pl --device=md2"
extend raid-md3 /usr/bin/sudo /usr/local/bin/monitoring/monitoring_returncode "/usr/local/bin/monitoring/nagios-linux-swraid.pl --device=md3"
```

N'oubliez pas de relancer le daemon snmpd après toute modification de son fichier de configuration !

```
/etc/init.d/snmpd restart
```

Test

Sur le serveur de monitoring

- Connectez-vous en tant qu'utilisateur “nagios” sur votre serveur de monitoring
- Exécutez la commande ci dessous:

```
nagios@monserveur:~$ /usr/local/nagios/libexec/check_snmp_extend adresse_ip_machine_a_monitorer raid-md3
Execute "/usr/local/bin/monitoring/nagios-linux-swraid.pl --device=md3"; return code was:0 OK - md3 [UU] has 2 of 2 devices active (active=sda3,sdb3 failed=none spare=none)
nagios@monserveur:~$
```

Si vous utilisez Centreon pour gérer Nagios, veuillez suivre la procédure décrite dans notre tutoriel sur Centreon (CENTREON) pour ajouter une nouvelle commande dans Centreon.

Mise en place d'un contrôle de serveur OpenVZ

Prérequis

Sur la machine à monitorer (le serveur OpenVZ)

- Nous avons mis à disposition l'ensemble des scripts utilisées dans une archive nommé "monitoring".

Télécharger et décompresser notre archive "monitoring" dans ”/usr/local/bin/monitoring” de la machine à monitorer.

Remarques: contenu de notre archive “monitoring”
- Nous avons créé le script “monitoring_returncode” afin d'obtenir un code de retour valide traité par le script “check_snmp_extend” lors de son execution par nagios.
- Le plugin “check_openvz” a été récupéré sur le site gforge.opensource-sw.net et nous l'avons légèrement modifié pour adapter le format de sortie du script.
- Le plugin “nagios-linux-swraid.pl” a été téléchargé depuis site www.logix.cz. Ce plugin ne sera pas utilisé dans le cas présent
- Le plugin “check_snmp_extend” a été téléchargé depuis le site www.logix.cz.
- Le plugin “check_hparray” a été téléchargé depuis le site de Exchange Nagios. Nous l'avons ensuite légèrement modifié pour adapter le format de sortie du script et activer ou non l'alerte “Warning” pour l'upgrade du firmware HP.

- Installer La librairie Yaml pour Perl (libyaml-perl) sinon gare à l'erreur de dependance pour le plugin Nagios de Perl:

```
...
Could not read '/root/.cpan/build/Params-Validate-1.07-IrrpPl/META.yml'. Falling back to other methods to determine prerequisites
```

```
apt-get install libyaml-perl
```

- Installer les modules PERL “Nagios::Plugin” et “Net:SNMP”

```
cpan -i Nagios::Plugin Net::SNMP
```

Vous pouvez utiliser l'outil CPANM pour installer vos modules PERL. Cet outil permet d'installer automatiquement les dépendances de chaque module, sans confirmation par l'utilisateur (facilement scriptable donc 😉).

```
wget -O - http://cpanmin.us | perl - --self-upgrade
```

puis

```
cpanm -i Nagios::Plugin Net::SNMP
```

- Installer le paquet “sudo”

Afin de permettre à l'utilisateur qui exécute le daemon SNMP (de la machine à monitorer) d'exécuter les différents plugins de contrôle.

Sur le serveur de monitoring

- Assurez-vous que le paquet “snmp” soit installé. La commande “check_snmp_extend” utilise la commande “snmpget” issue du paquet snmp !

```
apt-get install snmp
```

- Télécharger et décompresser notre archive "monitoring". Copier le plugin nommé “check_snmp_extend” dans votre dossier de plugins Nagios (/usr/local/nagios/libexec/) et attribuer à “check_snmp_extend” les bons droits.

Configuration

Sur la machine à monitorer

- Editer le fichier de configuration de l'outil “sudo” (/etc/sudoers) comme l'exemple ci-dessous:

Adapter les paramètres réseaux à votre infrastructure !

```
# /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the man page for details on how to write a sudoers file.
#

Defaults        env_reset

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL) ALL

# Host alias specification
Host_Alias NET_AUTH = localhost.localdomain, 192.168.7.0/24, 192.168.12.0/24
#User alias specification
User_Alias MY_USERS = snmp
#Cmnd alias specification
Cmnd_Alias MY_CMD = /usr/local/bin/monitoring/monitoring_returncode

MY_USERS NET_AUTH=(root)NOPASSWD: MY_CMD

# Allow members of group sudo to execute any command
# (Note that later entries override this, so you might need to move
# it further down)
%sudo ALL=(ALL) ALL
#
#includedir /etc/sudoers.d
```

N'oubliez pas de relancer “sudo” après chaque modification de son fichier de conf !

```
/etc/init.d/sudo restart
```

- Editer le fichier de configuration du daemon “snmpd” (/etc/snmp/snmpd.conf) comme dans l'exemple ci-dessous:

```
com2sec readonly  default         public
group MyROSystem v1         paranoid
group MyROSystem v2c        paranoid
group MyROSystem usm        paranoid
group MyROGroup  v1         readonly
group MyROGroup  v2c        readonly
group MyROGroup  usm        readonly
group MyRWGroup  v1         readwrite
group MyRWGroup  v2c        readwrite
group MyRWGroup  usm        readwrite
view all    included  .1                               80
view system included  .iso.org.dod.internet.mgmt.mib-2.system
access MyROSystem ""      any       noauth    exact  system none   none
access MyROGroup  ""      any       noauth    exact  all    none   none
access MyRWGroup  ""      any       noauth    exact  all    all    none
syslocation MON ENTREPRISE, notre rue et numero, mon pays
syscontact MOI <moi@monentreprise>
extend echotest /bin/echo hello world
#
# Pour OpenVZ
# ===========
extend .1.3.6.1.4.1.31039.1.1.2 vzquota /bin/sed -e 's/ \+/ /g' /proc/vz/vzquota
extend .1.3.6.1.4.1.31039.1.1.1 beancounters /bin/sed -e 's/ \+/ /g' /proc/bc/resources
extend openvz-status /usr/bin/sudo /usr/local/bin/monitoring/monitoring_returncode "/usr/local/bin/monitoring/check_openvz -l"
```

N'oubliez pas de relancer le daemon snmpd après toutes modifications de son fichier de configuration !

```
/etc/init.d/snmpd restart
```

Remarque:
Pour connaître les options du plugin “check_openvz”, vous pouvez exécuter:
[code]
/usr/local/bin/monitoring/check_openvz -h

[code]

Test

Sur le serveur de monitoring

- Connectez vous en tant qu'utilisateur “nagios” sur votre serveur de monitoring
- Exécutez la commande ci-dessous:

```
nagios@monserveur:~$ /usr/local/nagios/libexec/check_snmp_extend adresse_ip_machine_a_monitorer openvz-status
Execute "/usr/local/bin/monitoring/check_openvz -l"; return code was:0 Ok - OPENVZ OK
nagios@monserveur:~$
```

En cas d'erreur voici un exemple de ce que l'on peut avoir:

```
nagios@monserveur:~$ /usr/local/nagios/libexec/check_snmp_extend adresse_ip_machine_a_monitorer openvz-status
Execute "/usr/local/bin/monitoring/check_openvz -l"; return code was:2 Critical: 2 from 2 VE(s) - OPENVZ CRITICAL
CRITICAL - 246: othersockbuf Failures increased from 0 to 867 (held=48552, maxheld=4269912, barrier=6720443, limit=23104443)
CRITICAL - 250: shmpages     Failures increased from 0 to 4 (held=272, maxheld=1568, barrier=60270, limit=60270)
nagios@monserveur:~$
```

Si vous utilisez Centreon pour gérer Nagios, veuillez suivre la procédure décrite dans notre tutoriel sur Centreon (CENTREON) pour ajouter une nouvelle commande dans Centreon.

Liens supplémentaires