axians

Supervision des hôtes VMware®

OBJECTIF :

Pouvoir réaliser (et donc superviser) des ‘checks’ sur les services actifs sur tous les OS (Windows, Linux et même MacOS).

Il sera donc possible de vérifier en temps réel si tous nos services sont bien actifs.

REDACTION : mars 2020

VERSION : 1.0

PAR : GUENAT Lilian (Stagiaire)

VINCI ENERGIES

Sommaire

1 INSTALLATION

Afin de superviser le serveur VMware nous allons utiliser un script nommé check_esx3.pl. Pour se faire, commencez par téléchargez VMware vSphere SDK pour Perl sur le serveur Linux qui héberge Nagios, et décompressez-le à l'aide de la commande :

- cd /tmp
- tar zxvf VMware-vSphere-Perl-SDK-6.5.tar.gz

Cela a pour effet de créer le sous-répertoire vmware-vsphere-cli-distrib, dans lequel se trouve le script d'installation vmware-install.pl.

Avant d'exécuter ce script, exécutez la commande :

- yum install perl-Pod-Perldoc perl-CPAN openssl-devel

Elle permet de s'assurer que le serveur est conforme aux conditions logicielles requises.

Après avoir installé les logiciels indispensables, exécutez les commandes :

- cd vmware-vsphere-cli-distrib
- ./vmware-install.pl

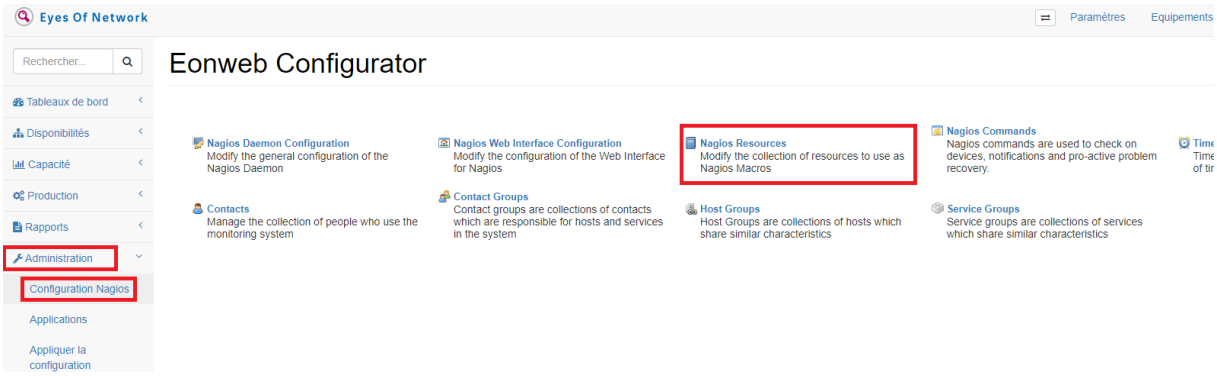
Puis, suivez les indications du script. A présent, il faut télécharger le script check_esx3.pl grâce aux commandes suivantes :

- git clone git://git.op5.org/nagios/op5plugins.git
- cd op5plugins
- cp check_esx3.pl /srv/eyesofnetwork/nagios/plugins/
- chown nagios:eyesofnetwork /srv/eyesofnetwork/nagios/plugins/check_esx3.pl
- chmod 755 /srv/eyesofnetwork/nagios/plugins/check_esx3.pl

Si la 1ère commande ne fonctionne pas, faites la commande yum install git puis réessayez.

Ce plugin nécessite un compte d'utilisateur sur le serveur ESX et vCenter pour qu'il puisse se connecter et récupérer les informations de supervision.

Il est d'ailleurs fortement conseillé d'ajouter les identifiants dans les « Nagios Resources » dans « Administrations » > « Configuration Nagios » > « Nagios Resources » :



Utilisez deux $USER$ au choix afin d'inclure les identifiants facilement dans les commandes par la suite.

2 INSTALLATION V2

Afin de pouvoir superviser notre hôte ESXi nous allons utiliser le protocol SNMP. Pour se faire connectez-vous en SSH sur votre serveur avec vos identifiants ‘root’.

A présent, entrez la commande suivante pour définir votre communauté, en remplaçant EyesOfNetwork par la vôtre.

- esxcli system snmp set --communities EyesOfNetwork

Pour nous, ici, ce sera EyesOfNetwork puisque c’est celle qu’on utilise depuis le début.

Maintenant, nous pouvons activer le service SNMP sur notre hôte avec la commande suivante :

- esxcli system snmp set --enable true

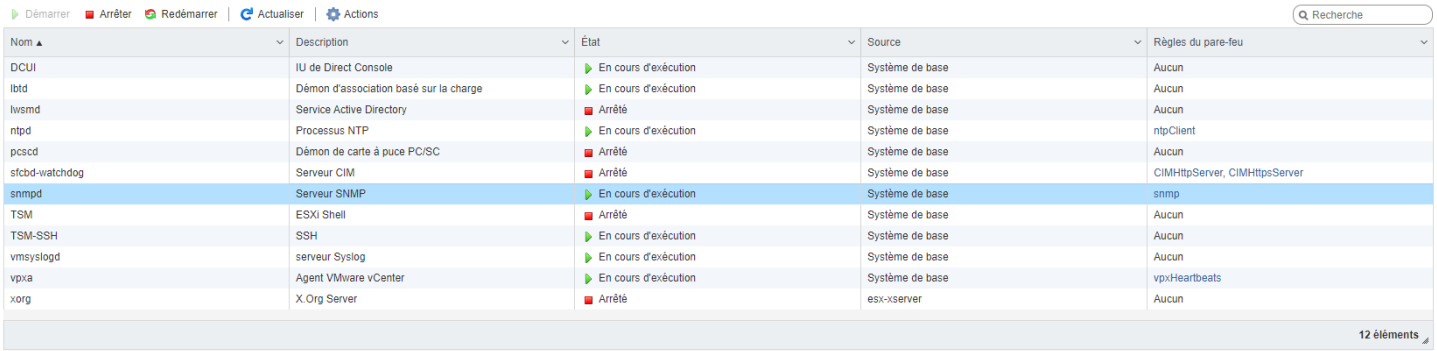
Nous devons à present ajuster le pare-feu de l’hôte même s’il y a de fortes chances qu’il autorise déjà ce trafic, mais au cas où, autorisez les connexions de n'importe où :

- esxcli network firewall ruleset set --ruleset-id snmp --allowed-all true
- esxcli network firewall ruleset set --ruleset-id snmp --enabled true

Maintenant les règles modifiées, vous pouvez rédemmarer le service SNMP avec la commande suivante :

- /etc/init.d/snmpd restart

Patience, il a fallu dans notre cas 30 à 45 secondes pour que le service redémarre sur l’hôte. Une fois cela fait, vous pouvez confirmer que le service fonctionne via l'interface graphique :



Il est toutefois possible de sécuriser un peu plus ce que l'on vient de faire faisant une restriction sur une certaines plages d'adresses IP comme cet exemple :

- esxcli network firewall ruleset set --ruleset-id snmp --allowed-all false
- esxcli network firewall ruleset allowedip add --ruleset-id snmp --ip-address 192.168.0.0/24
- esxcli network firewall ruleset set --ruleset-id snmp --enabled true

Dans ce cas, nous autorisons uniquement les adresses IP 192.168.0.0 à 192.168.0.254 à faire des interrogations SNMP sur l'hôte.