

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)



Sommaire

- 1 INSTALLATION **Erreur ! Signet non défini.**
 - 1.1 Avec Windows **Erreur ! Signet non défini.**
 - 1.2 Avec Linux (ici CentOS 7) **Erreur ! Signet non défini.**
- 2 CONFIGURATION **Erreur ! Signet non défini.**



1 INSTALLATION

Afin de superviser le serveur VMware nous allons utiliser un script nommé `check_esx3.pl`. Pour se faire, commencez par télécharger 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-vmphere-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-vmphere-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 » :



Eyes Of Network Paramètres Equipements

Rechercher...

Eonweb Configurator

- Tableaux de bord <
- Disponibilités <
- Capacité <
- Production <
- Rapports <
- Administration** >
- Configuration Nagios
- Applications
- Appliquer la configuration

Nagios Daemon Configuration
Modify the general configuration of the Nagios Daemon

Nagios Web Interface Configuration
Modify the configuration of the Web interface for Nagios

Nagios Resources
Modify the collection of resources to use as Nagios Macros

Nagios Commands
Nagios commands are used to check on devices, notifications and pro-active problem recovery.

Contacts
Manage the collection of people who use the monitoring system

Contact Groups
Contact groups are collections of contacts which are responsible for hosts and services in the system

Host Groups
Host Groups are collections of hosts which share similar characteristics

Service Groups
Service groups are collections of services which share similar characteristics

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 protocole 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 redémarrer 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 :

Nom ▲	Description	État	Source	Règles du pare-feu
DCUI	IU de Direct Console	▶ En cours d'exécution	Système de base	Aucun
lbttd	Démon d'association basé sur la charge	▶ En cours d'exécution	Système de base	Aucun
lvsmd	Service Active Directory	■ Arrêté	Système de base	Aucun
ntpd	Processus NTP	▶ En cours d'exécution	Système de base	ntpClient
pcscd	Démon de carte à puce PC/SC	■ Arrêté	Système de base	Aucun
sfcdb-watchdog	Serveur CIM	■ Arrêté	Système de base	CIMHttpServer, CIMHttpsServer
snmpd	Serveur SNMP	▶ En cours d'exécution	Système de base	snmp
TSM	ESXi Shell	■ Arrêté	Système de base	Aucun
TSM-SSH	SSH	▶ En cours d'exécution	Système de base	Aucun
vmsyslogd	serveur Syslog	▶ En cours d'exécution	Système de base	Aucun
vpwa	Agent VMware vCenter	▶ En cours d'exécution	Système de base	vpwHeartbeats
xorg	X.Org Server	■ Arrêté	esx-xserver	Aucun

12 éléments



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.