Compte rendu livre Nagios - Au coeur de la supervision Open Source Edition ENI Lien vers le livre :
http://www.eyrolles.com/Informatique/Livre/nagios-au-coeur-de-la-supervision-open-source-9782746046030

Conseils et outils intéressants

Utiliser les champs host_name, display_name et alias pour avoir réciproquement le nom de la machine affiché dans l'interface (srv-name), son nom DNS FQDN (srv-name.domaine.local) et sa description (serveur contrôleur de domaine).

Séparer les scripts de plugins officiels de ceux qui sont ajoutés manuellement. Créer un dossier contrib et laisser le dossier par défaut aux plugins officiels.

check_tcp possède de nombreux alias présent par défaut : check_clamd, check_ftp, check_, check_imap, check_jabber, check_nntp, check_nntps, check_pop, check_simap, check_spop, check_ssmtp, check_udp.

check_tcp est aussi utilisé pour l'udp.

check_dns et check_dig permet de tester la résolution directe et inverse en passant par un serveur.

Contrôle de l'ensemble de la chaîne des services de messagerie avec NagiosCheckEmailDelivery.
http://apricoti.pbwiki.com

Pipe ou tube qui permet de faire passer des requêtes au serveur Nagios. /var/nagios/rw/nagios.cmd

Vu du serveur Nagios, liste des commandes possibles à soumettre au serveur.
http://www.nagios.org/developerinfo/externalcommands/commandlist.php

NSCA, en 5667 en daemon ou xinetd, permet de réceptionner des informations remontées de manière passive par des éléments.

Pour grapher, c'est un système basé sur RRDtool qui est utilisé. Il en existe de nombreux. RRDtool est maintenu par la même personne qui a créé MRTG. Explication sur RRDtool :
http://ed.zehome.com/?page=rrdtool

Outils de génération de graphique basé sur RRDtool.

- PNP
- N2RRD
- NagiosGrapher
- NagiosGraph

- Drraw ou Cacti pour la présentation des données.

- Nagiostats couplé à MRTG pour grapher l'utilisation du serveur de supervision Nagios.

Snmpd est l'agent SNMP actif (écoute sur le port UDP 161). Snmptrapd est le programme qui réceptionne les traps SNMP (écoute sur le port UDP 162).

snmptt : convertit les OID des interruptions reçus en messages explicites. Il s'intercale entre

snmptrapd et Nagios. Il permet de ce fait de stocker les interruptions dans une base de données MySQL ou PostgreSQL.

Journaux (logs)

Système de gestion de logs sur la machine Nagios peut être intéressant. Metalog, Syslog-NG ou Rsyslog. Syslog-NG et Rsyslog peuvent stocker les messages dans une base de données MySQL ou PostgreSQL avec un module. C'est Rsyslog qui est le plus simple à configurer.

Comparatif entre syslog-ng et rsyslog http://www.rsyslog.com/doc-rsyslog_ng_comparison.html

SEC (Simple Event Correlator) est un logiciel open source de corrélation d'évènements écrit en Perl.

Splunk est un moteur de traitements des fichiers journaux, un moyen de recherche et une interface de navigation. L'interface est très aboutie. Un partenariat à été réalisé avec Nagios, il est donc intégré à Nagios. Un lien s'intègre dans l'interface web standard de Nagios. La version gratuite permet de traiter 500 Mega de journaux quotidiennement.

8pussy http://www.8pussy.org est une application dédié au traitement des journaux capable d'analyser, d'alerter et de rendre des statistiques sur les évènements qui y sont contenus. 8Pussy est capable d'analyser les logs des services suivants : Bind, Cisco Switch, Cisco Router, Ironport Mailserver, Linux Kernel/System, Monit, MySQL, Nagios, NetApp, Postfix, PostgreSQL, Squid, Syslog-ng, Windows Snare Agent, Xen... Il peut alerter par mail, par messagerie jabber, et par send_nsca. Avec send_nsca, il est donc possible d'intercaler 8pussy entre le daemon du protocole syslog et Nagios.

Moyens d'alertes

nagios checker, SMS avec carte GSM ou autre + site d'SMS distant, ou messagerie instantané jabber. L'avantage de jabber est qu'on ne conserve pas les messages et que c'est hyper rapide de recevoir l'information.

Changer l'interface Nagios (thèmes) Thème Nuvola

NDOutils

Ndoutils est un logiciel de courtage d'évènements. Module officiel pour stocker la configuration de nagios et les résultats de contrôle de Nagios dans une base de données MySQL ou PostgreSQL. Oracle est prévu. Nagios ne sait pas lire les données dans cette base. C'est une interface supplémentaire qui peut-être intégrée à Nagios qu'il faut employer. Cette interface est Nagvis. Il permet en plus de gérer des cartes précises. On positionne des éléments en fonction de leurs coordonnées x et y. Des cartes plus personnelles sont présentes dans GroundWorks Monitor.

NDOUtils fournit quatre outils : ndomod, log2ndo, file2sock, et le démon ndo2db.

Nagios Business Process Addons

http://nagiosbp.sourceforge.net Nagios Business Process View est une possiblité supplémentaire de pouvoir organiser la supervision et surtout les vues de celles-ci, à l'instar de Nagvis. Il permet de s'affranchir des limites des groupes de services de Nagios et permet de définir des relations entre services et ressources qui vont bien au delà de ce qu'il est possible de faire avec de simple dépendances.

NagTrap

http://nagtrap.org module qui permet d'intérroger la base de données renseignée par SNMPTT pour le stockage des interruptions SNMP. C'est une interface PHP. Il fournit également un plug-in Nagios nommé check_snmp_trap.

Conseils et outils intéressants

Interface pour Nagios : GroundWorks Monarch, Fruity, NagiosAdmin, NagiosQl. Vérifier qu'elles fonctionnent en Nagios version 3.

Vérification de l'utilisation des processus Nagios ne prennent pas plus de 50% de l'utilisation processeur de la machine et 100% en critique. Utiliser check_procs. check_procs -u nagios -m CPU -w 50 -c 100

Contrôler l'heure système du serveur Nagios et alerter lorsqu'il y a une différence par rapport à une ou plusieurs références sur le net. Utiliser check_ntp_time check_ntp_time -H fr.pool.ntp.org -w 30 -c 60

chek_lm_sensors permet de superviser les ressources (températures, voltage, ...) des composants du serveurs. Il faut cependant avoir un agent pour que cela fonctionne. La version SNMP demande l'ajout de MIB et elles ne sont pas prevues par défaut.

Contrôle de la température de la pièce et de l'humidité de la pièce avec une sonde à 132 € qui fonctionne en USB et qui dispose d'un pilote OpenSource et d'un plug-in prévu pour Nagios! http://messpc.de/sensor_alphanumerisch.php

Il est possible de réaliser des checks CPU par exemple encapsulé dans une commande check_by_ssh afin de crypter le flux. Il faut pour cela paramétrer les clés publiques/privées sur chaque hôte afin de ne pas entrer de mot passe.

La mib2 contient 11 sous-ensembles :

- system

- interfaces
- at
- ip
- icmp
- tcp
- udp
- egp
- transmission
- snmp

snmpget permet d'obtenir une valeur d'OID et snmpwalk les valeurs d'un sous-ensemble.

Utiliser un logiciel de parcour de MIB pour avoir une visualisation de ce qu'on veut obtenir comme valeur. Utiliser **MIB Browser** par exemple. Il est multiplateforme.

Contrôle des équipements réseaux : état, trafic par ports et réception de la journalisation sont possible dans la plupart des routeurs et switchs via SNMP.

Etat des ports avec check_ifoperstatus et check_ifstatus. Mesure du trafic sur les interfaces avec check_snmp_netint.pl http://william.leibzon.org/nagios/

snmpconf : outil pour configurer le fichier snmpd.conf sans connaissance particulière de la syntaxe du fichier.

Monit est plus précis que les check_procs, check_load et check_file.

Collectd pour effectuer des statistiques sur pleind'éléments et les stocker dans un fichier rrd ou csv. Fonction avec des éléments en mode passif.

Agent nsclient++ intérrogeable via check_nt (en clair) ou via check_nrpe qui peut être sécurisé.

Logs

Snare (System iNtrusion Analysis & Reporting Environnement) est un agent fonctionnant sous Linux et Windows qui permet de convertir et d'envoyer les logs à un serveurs syslog.

Evtwin : convertisseur d'évènement en intérruption SNMP.

Solutions de redondance et de performance

Pour des performances, on peut faire un serveur proxy nagios. On peut utiliser DNX (Distributed Nagios eXecutor). L'intérêt est de maintenir une latence basse. Il ne faut pas que le temps des requêtes émises dépasse le temps disponible et les limites de la carte réseau.

Autre possibilité pour les grosses infrastructures : les serveurs distribués.

Logiciels qui étendent Nagios

Utiliser Cacti est intéressant pour grapher les données de Nagios. Par contre ne fonctionne qu'avec MySQL. Cacti disposent de plugins qui sont disponiblent sur http://cactiusers.org/index.php

NPC (Nagios Plugin for Cacti) est un plugin qui permet de complètement intégrer Nagios à Cacti.

Centreon (http://centreon.com) se base complètement sur Nagios et ajoute une interface graphique. Il est tout à fait possible d'utiliser les 2 interfaces en même temps.

Nagios Enterprise en 2008 pour fédérer les besoins entreprises.

GroundWork Monitor Community

Nagios et la sécurité

OSSIM

Hyperic HQ : Nagios en Java. OpenNMS est aussi en Java. Il est conçu pour gérer d'abord le SNMP. Zenoss : logiciel de supervision en Python basé sur Zope.

Plugins utilitaires Urlize : permet d'encapsuler le message de sortie d'un plug-in pour en créer une balise HTML avec un lien cliquable. check_multi permet de créer un service qui regroupe un ensemble de fonctionnalités. Ex : un service network qui contient 5 commande check_snmp_int.pl pour chaque interface réseau d'un élément.

Autres logiciels Open Source

Zabbix. Munin. Gagnlia. Hobbit Monitor.

From:
https://wiki.ouieuhtoutca.eu/ - **kilsufi de noter**

Permanent link:
https://wiki.ouieuhtoutca.eu/nagios_au_coeur_de_la_supervision_open_source

Last update: **2021/01/21 21:42**