

Création d'une image générique EyesOfNetwork

Table des matières

Prérequis.....	1
Installation de la solution	2
Paramétrage du système	3
Modification de la configuration réseau.....	3
Mise à jour du système	4
Configuration du service SNMP	4
Configuration du service Postfix.....	4
Configuration du fichier main.cf	5
Configuration du service SSH	5
Restauration de la configuration.....	6
Restauration de la sauvegarde Backup Manager	6
Sauvegarde et restauration des templates de supervision.....	7
Configuration de la supervision	8
Ajout des hôtes à Nagios	8
Les NAS	9
Windows Server	9
Installation de NSClient++	9
Supervision d'un service précis.....	9
Modification du modèle d'hôte Windows	10
Ajout d'une commande.....	10
Modification du template Windows	10
Les commutateurs.....	10
Les serveurs VMware.....	11

Prérequis

Le logiciel `vim` (Vi IMproved) est un éditeur de texte puissant. Nous allons donc l'utiliser tout au long de la procédure. Il est également possible d'effectuer les modifications avec `nano`.

Pour effectuer une recherche dans un fichier, il faut utiliser la touche `/`

Pour entrer en mode «**Insertion**», il faut appuyer sur `i`

Pour enregistrer les modifications, il faut faire la combinaison `[Echap] :x!`
ou `[Echap] :wq!`

Pour quitter un fichier sans enregistrer les modifications, il faut faire `[Echap] :q!`

Toutes les modifications seront effectuées avec les privilèges `root`.

Installation de la solution

Pour la création d'une image générique d'EyesOfNetwork, nous allons définir une configuration générique que nous pourrons ensuite déployer chez les différents clients.

Une fois que l'on a démarré sur l'ISO, on choisit l'option «**Install or upgrade an existing system**» ce qui va lancer la procédure d'installation. Le programme d'installation va ensuite demander à vérifier l'ISO. Il est recommandé d'accepter afin d'éviter les erreurs pendant l'installation. Une fois la vérification faite, on peut commencer l'installation.

Le programme d'installation texte lance donc une interface graphique, on clique sur «**Next**».

On choisit ensuite la langue «**français**» et «**français (latin9)**» comme disposition de clavier (clavier français standard avec le symbole €).

L'installation de faisant sur des périphériques locaux, on sélectionne ensuite l'option «**Périphériques de stockage basiques**».

On donne ensuite à la machine le nom d'hôte générique «**eon**». On modifiera l'adresse FQDN (Fully Qualified Domain Name) de la machine après l'installation. Sur cet écran, il est aussi possible de modifier la configuration réseau. Nous allons laisser le DHCP attribuer automatiquement une adresse à la machine pour éviter les conflits sur le réseau. Nous changerons cette adresse au moment du déploiement (x.x.x.250 en général).

Il faut ensuite choisir le fuseau horaire, ici «**Europe/Paris**».

Nous devons ensuite définir le mot de passe pour l'utilisateur «**root**» (administrateur). C'est avec ce compte que se feront les tâches d'administration sur le serveur.

Pour le partitionnement, on choisit l'option «**Créer un partitionnement personnalisé**» pour pouvoir définir l'espace disque alloué à EyesOfNetwork.

Nous allons créer la partition `/boot` (partition d'amorçage). Pour le reste, nous allons utiliser des volumes logiques, beaucoup plus souples et évolutifs.

On choisit donc créer, puis partition standard. Dans le champ «**point de montage**», on définit `/boot` de 200 Mo avec **ext4** comme système de fichiers.

On crée ensuite un PV pour LVM (volume physique) d'une taille de 55300 Mo.

Dans ce volume physique, on va créer un VG (groupe de volumes) ou seront répartis les LV (volumes logiques). On clique donc sur «**Créer**» puis «**Groupe de volumes LVM**». Dans la même fenêtre, on clique ensuite sur «**Ajouter**».

Pour le premier LV, nous définissons `/` (racine) comme point de montage, **ext4** comme système de fichiers journalisés, **lv_root** comme nom et nous lui attribuons une taille de 51200 Mo.

Pour le second LV, nous définissons SWAP comme système de fichiers, dans le champ «**nom**» on remplit avec **lv_swap** avec une taille de 4096 Mo.

On peut ensuite valider la configuration de l'espace de stockage sur le disque en validant avec le bouton «**Écrire les modifications sur le disque**».

Sur l'écran suivant, l'assistant d'installation propose une personnalisation des dépôts et des paquets à installer. Nous allons donc cocher la case «Personnaliser maintenant» afin de sélectionner les paquets qui nous intéressent.

Dans la partie **EyesOfNetwork Supervision**, on sélectionne «Base» et «Options».

Les paquets présents dans «Options» sont les suivants :

- **cntlm** : proxy d'authentification HTTP(S)
- **ndo2fs** : Écrit les données de `ndomod` dans des fichiers plats
- **ndoutils** : Addon pour Nagios. Compte 4 éléments (`ndomod`, `file2sock`, `log2ndo`, `ndo2db`)
- **nsca** : Addon pour l'envoi de commandes externes à Nagios
- **nsca-send** : module de `nsca`
- **ntop** : Outil de supervision du trafic réseau

Dans la partie **EyesOfNetwork Production**, on sélectionne «Gestion des incidents» et «Inventaire» pour installer les logiciels **GLPI** et **OCS-NG**.

Nous pouvons ensuite cliquer sur suivant et lancer l'installation des composants sur la machine. Une fois l'installation terminée, on peut redémarrer la machine.

Paramétrage du système

Modification de la configuration réseau

Pour modifier les fichiers de configuration de la machine, il faut se connecter avec l'utilisateur `root`. On peut aussi effectuer ces modifications avec un accès `SSH`. Si l'interface n'est pas activée, lancer la commande

```
#ifup eth0
```

Pour modifier l'adresse IP de la machine, il faut éditer le fichier de configuration de l'interface désirée (ici `eth0`) avec la commande

```
#vim /etc/sysconfig/network-scripts/ifcfg-eth0
```

(on peut aussi utiliser la commande `nano`, moins compliquée que `vim`) où **IPADDR** est l'adresse IP de la machine, **NETMASK** son masque réseau et **GATEWAY** l'adresse de la passerelle.

```
DEVICE=eth0
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=yes
BOOTPROTO=none
IPADDR=X.X.X.X
NETMASK=X.X.X.X
GATEWAY=X.X.X.X
```

On modifie ensuite le fichier du service réseau avec `vim /etc/sysconfig/network`

```
NETWORKING=yes  
NETWORKING_IPV6=no  
HOSTNAME=eon.domaineFQDN  
GATEWAY=X.X.X.X
```

On édite ensuite le fichier de configuration DNS avec la commande `vim /etc/resolv.conf` où «**nameserver**» est l'adresse du serveur DNS

```
search adresseFQDN  
nameserver X.X.X.X
```

On peut ensuite redémarrer le service réseau avec

```
#service networking restart
```

ou

```
#/etc/init.d/networking restart
```

Mise à jour du système

Pour mettre à jour CentOS et les outils système, il suffit de lancer la commande

```
#yum update
```

Si le prompt renvoie une erreur **404**, c'est que les fichiers de configuration des repositories sont obsolètes dans le fichier `/etc/yum.repos.d/CentOS-Base.repo` (`$releasever`)

On relance donc la commande en précisant cette fois la version de la release de CentOS

```
#yum update --releasever 6.5
```

[EDIT 05/2014]

Suite à la faille `HeartBleed` dans le paquet `openssl`, il est nécessaire de le mettre à jour vers la version 1.0.1g (car la version EON 4 n'est pas patchée)

Configuration du service SNMP

La configuration du service SNMP est un point très important. Il faut donc commencer par définir la communauté SNMP. En général, la communauté SNMP par défaut est «**public**». Ici, la communauté est «**EyesOfNetwork**».

Configuration du service Postfix

Pour l'envoi de notifications par mail, Nagios a besoin du service d'un serveur de messagerie. Par défaut, EyesOfNetwork intègre le serveur Postfix. Il est possible de paramétrer Postfix pour qu'il serve de relai à un serveur de messagerie principal.

Configuration du fichier main.cf

La configuration de Postfix est simple car elle repose sur un unique fichier de configuration : `/etc/postfix/main.cf`

Afin d'obtenir un système de notifications par mail opérationnel, il n'y a que quelques paramètres à changer dans le fichier main.cf.

L'édition d'une ligne précise avec vim se fait en ajoutant `%nbligne` à la fin de la ligne de commande ; par exemple `vim /etc/main.cf %75`

ligne 75: myhostname = hôte.domaine.tld

`-> On remplit ici le nom fqdn de la machine

ligne 83: mydomain = domaine.tld

`-> On remplit ici le domaine parent de la machine

ligne 98: myorigin = \$myhostname

`-> Envoie le courrier comme "user@\$myhostname"

ligne 296: relay_domains = mail.b2bouygtel.com

`-> Définition du domaine auquel les mails seront relayés

ligne 297: default_transport = smtp

`-> Définition du mode de transport par défaut

ligne 298: relayhost = smtp.b2bouygtel.com

`-> Permet de préciser un serveur SMTP comme relai. C'est vers cette machine que tout le courrier est routé.

Configuration du service SSH

Il est recommandé de désactiver l'accès SSH pour l'utilisateur `root`. Il faudra donc se connecter avec un utilisateur aux droits restreints et ensuite accéder au compte `root` pour les tâches d'administration.

Pour désactiver l'accès `root` en SSH, il faut éditer le fichier `/etc/ssh/sshd_config` et modifier la ligne `#PermitRootLogin yes` par `PermitRootLogin no` (il faut enlever le `#` au début de la ligne, cela permet au démon `sshd` de prendre en compte le paramètre au prochain rechargement des fichiers).

On peut ensuite créer un utilisateur avec des droits restreints avec la commande

```
#useradd maintenance -g wheel
```

On définit un mot de passe pour cet utilisateur avec

```
#passwd maintenance
```

Il faut définir le mot de passe et le confirmer.

On redémarre ensuite le service `sshd` avec la commande

```
#service sshd restart
```

ou

```
#/etc/init.d/sshd restart
```

Pour vérifier que la configuration de ssh s'est bien passée, on se connecte avec le nouvel utilisateur avec

```
#ssh maintenance@X.X.X.X
```

Le prompt doit maintenant afficher

```
[maintenance@eon ~]$
```

à la place de

```
[root@eon ~]#
```

Pour passer à l'utilisateur `root`, on utilisera `su -` (le `-` permet de charger les variables d'environnement et les préférences de l'utilisateur) après la connexion avec l'utilisateur `maintenance`

Restauration de la configuration

Restauration de la sauvegarde Backup Manager

La distribution EyesOfNetwork fournit par défaut l'utilitaire `backup-manager` qui permet de sauvegarder la configuration de la machine. Par défaut, ces sauvegarde sont placées dans le répertoire `/var/archives/`

La restauration de ces configurations se fait de manière simple : pour les fichiers de la base de données, il suffit d'un pipe (tube, redirection) et pour les sauvegardes des répertoires `/etc`, `/home` et `/srv` il suffit d'un simple `tar` (copie).

La procédure de restauration est donc la suivante : Pour les fichiers de la base de données, on se rend dans le dossier contenant les sauvegardes avec la commande `cd /var/archives`. On peut lister l'ensemble des fichiers présents dans le répertoire avec la commande `ls -al`.

Il est aussi possible de faire un dump (sauvegarde de base de données à un instant donné) de la base de données manuellement avec la commande

```
mysql> mysqldump -h localhost -pSaturne2 -u root --all-databases > $REP
```

où `$REP` est le répertoire de sauvegarde.

Les archives étant au format `bzip2`, il faut d'abord les extraire avec

```
#bunzip2 *.bz2
```

On peut ensuite restaurer un à un les fichiers sauvegardés avec la commande suivante :

```
#mysql -uroot -p00t66 -hlocalhost -P3306 $table < $host.imag.fr-cacti.$date.sql
```

où `$table` est le nom de la table à restaurer (`cacti`, `eonweb`, `glpi`..), `$host` est le hostname de la machine et `$date` la date de sauvegarde du fichier au format `AAAAMMJJ`. On répète l'action avec chacun des fichiers à restaurer.

Selon le format de compression utilisé par backup-manager, on lancera une des commandes suivantes pour la restauration

- tar : `#tar -xvcf fichier.tar -C chemin_de_décompactage`
- tar.gz : `#tar -xvzf fichier.tar -C chemin_de_décompactage`
- tar.bz2 : `#tar -xvjf fichier.tar -C chemin_de_décompactage`

Par exemple, pour restaurer le répertoire `/etc`, on utilisera

```
#tar -xvzf $host-etc.$date.master.tar.gz -C /
```

Une fois la restauration des fichiers effectuée, il se peut que GLPI affiche le message suivant :



The screenshot shows the GLPI interface with a table titled "Tests effectués" (Tests performed) and a "Résultats" (Results) column. All tests passed, indicated by green circles. Below the table, a red warning message states: "Votre version de la base de données n'est pas compatible avec la version des fichiers installés. Une mise à jour est nécessaire." (Your database version is not compatible with the version of the installed files. An update is necessary.) A "Mise à jour" (Update) button is located below the message.

Tests effectués	Résultats
Test du Parseur PHP	●
Test de l'extension MySQL.	●
Test des Sessions	●
Test de l'utilisation de Session_use_trans_sid	●
Test sur l'extension magic_quotes_sybase	●
Test sur l'extension ctype	●
Test sur les fonctions Json	●
Test sur l'extension mbstring	●
Test de la mémoire allouée	●
Test d'écriture du fichier de configuration	●
Test d'écriture de fichiers documents	●
Test d'écriture de fichiers dump	●
Test d'écriture des fichiers de sessions	●
Test d'écriture des fichiers des actions automatiques	●
Test d'écriture des fichiers de cache	●
Test d'écriture des fichiers de graphiques	●
Test d'écriture des fichiers de log	●
SELinux en mode Disabled	●

Votre version de la base de données n'est pas compatible avec la version des fichiers installés. Une mise à jour est nécessaire.

Mise à jour

Il suffit de cliquer sur le bouton mise à jour, GLPI va ensuite faire une optimisation de ses tables dans la base de données.

Sauvegarde et restauration des templates de supervision

Il est possible au sein de EyesOfNetwork d'effectuer une sauvegarde mais aussi une restauration des modèles créés. Il suffit pour cela de se rendre dans le menu de gestion des modèles, de sélectionner les modèles que l'on souhaite exporter, mettre l'action sur **Export** et cliquer sur **Submit**.

HOST TEMPLATES

Add A New Host Template

Actions : Export Submit

Host Template Name	Description	ALL
AIX4	Template Aix 4	<input checked="" type="checkbox"/>
AIX5	Template Aix 5	<input checked="" type="checkbox"/>
BROCADE	Template Brocade	<input checked="" type="checkbox"/>
CISCO	Template Cisco	<input checked="" type="checkbox"/>
DELL	Template Dell	<input checked="" type="checkbox"/>
EMC	Template Emc	<input checked="" type="checkbox"/>
ESX	Template Esx	<input checked="" type="checkbox"/>
FOUNDRY	Template Foundry	<input checked="" type="checkbox"/>
GENERIC_HOST	Template Generic	<input checked="" type="checkbox"/>

Pour restaurer le fichier XML créé, il faut se rendre dans la partie **Nagios** → **configuration** du menu latéral puis de se rendre dans la catégorie **Imports**, de sélectionner le fichier à restaurer. Il est ainsi possible de restaurer chacun des fichiers XML précédemment sauvegardés.

General Templates Network Imports Tools About

EONWEB CONFIG IMPORTER

Import your XML File.

Parcourir Aucun fichier sélectionné. Submit

Configuration de la supervision

Ajout des hôtes à Nagios

Afin de pouvoir commencer la supervision du parc de machines, il faut commencer par ajouter des hôtes à Nagios en spécifiant le type de machine à superviser.

Il faut donc se rendre sur l'interface d'administration d'EyesOfNetwork (eonweb) puis dans l'onglet **Administration** puis dans la partie **Équipement** dans le volet de gauche

EONWEB CONFIGURATOR Search:

General Templates Network Imports Tools About

TOP LEVEL NETWORK HOSTS

Add A New Child Host

Object to Add : HostGroup Do It! Actions : Delete Submit

Il suffit ensuite de cliquer sur **Add A New Child Host**, puis ajouter un nom à la machine dans le champ **Host Name**, une brève description dans le champ **Host Description**. On renseigne ensuite l'adresse IP de la machine dans le champ **Address**, puis un nom d'affichage que l'on pourra facilement reconnaître dans le champ **Display Name**.

La liste déroulante en dessous est très importante puisqu'elle permet d'affecter un template à la machine que l'on ajoute. Cela permet d'avoir une série d'actions et de contrôles prédéfinis en fonction du type d'hôte. Ces **Templates** permettent une configuration simplifiée des hôtes à superviser. En effet, il suffit de créer les modèles en fonction du type de machine et de service à superviser puis de les appliquer. Il paraît donc nécessaire de déterminer les services que l'on souhaite surveiller ainsi que le type de machine afin de créer les templates les plus génériques possibles.

ADD A TOP-LEVEL HOST

Host Name:

This directive is used to define a short name used to identify the host. It is used in host group and service definitions to reference this particular host. Hosts can have multiple services (which are monitored) associated with them. When used properly, the \$HOSTNAME\$ macro will contain this short name.

Host Description:

This directive is used to define a longer name or description used to identify the host. It is provided in order to allow you to more easily identify a particular host. When used properly, the \$HOSTALIAS\$ macro will contain this alias/description.

Address:

This directive is used to define the address of the host. Normally, this is an IP address, although it could really be anything you want (so long as it can be used to check the status of the host). You can use a FQDN to identify the host instead of an IP address, but if DNS services are not available this could cause problems. When used properly, the \$HOSTADDRESS\$ macro will contain this address. Note: If you do not specify an address directive in a host definition, the name of the host will be used as its address. A word of caution about doing this, however - if DNS fails, most of your service checks will fail because the plugins will be unable to resolve the host name.

Display Name (Optional):

Host Templates To Inherit From (Top to Bottom):

Add Template To Inherit From:

AIX4

Add Template

Add Host

[Cancel]

Nous allons donc commencer par lister les équipements rencontrés le plus souvent. Nous avons donc recensé des commutateurs, serveurs (Windows 2003, 2008, 2012, ESXi) et leurs services, les NAS ainsi que routeurs et pare-feu.

Les NAS

Pour ajouter un NAS dans Nagios pour le superviser, il suffit de [l'ajouter comme un hôte classique](#) et de spécifier **Linux** dans la liste déroulante **Add Template To Inherit From**. On est alors en mesure de superviser les interfaces réseau de l'équipement, la mémoire disponible, l'espace disque disponible, la charge processeur utilisée, l'heure du système ainsi que son uptime.

Pour ce type d'équipement, il est inutile d'éditer le template, toutes les informations nécessaires sont déjà fournies, même le l'agrégation de cartes réseaux. (**bond0**)

Windows Server

Installation de NSClient++

Nous allons ensuite ajouter un hôte Windows Server. Les services à superviser étant plus spécifiques sur ces équipements, nous allons devoir installer un agent NSClient++ puis modifier le fichier `C:\Programmes\NSClient++\nsclient.ini` afin de le faire communiquer correctement avec le serveur EON.

Il faut donc commencer par télécharger l'exécutable sur le site officiel de l'éditeur puis de l'installer. On peut l'installer en cliquant sur **Suivant**, la configuration sera effacée avec un fichier `nsclient.ini` préparé au préalable.

Dans le fichier `nsclient.ini`, il est impératif de modifier un certain nombre de paramètres pour s'assurer du bon fonctionnement de NSClient++.

Il faut donc ajouter dans la partie `[/settings/default]` la ligne **allowed hosts = X.X.X.X** et **password = mot_de_passe**

On peut ensuite modifier la ligne suivante afin d'exclure de la supervision les services qui ne nous intéressent pas

```
; alias_service_ex - Alias for alias_service_ex. To configure this item add a section called: /settings/external scripts/alias/alias_service_ex
alias_service_ex = checkServiceState CheckAll "exclude=Net Driver HPZ12" "exclude=Pnl Driver HPZ12" exclude=stisvc exclude="XXXX"
```

Supervision d'un service précis

Modification du modèle d'hôte Windows

Ajout d'une commande

Il faut d'abord ajouter une commande personnalisée au sein de Nagios pour pouvoir ensuite l'intégrer à un template. Il faut donc se rendre dans l'onglet **Administration**, dans le volet **configuration** la partie **Nagios Commands**. On clique ensuite sur **Add A New Command**. Pour surveiller l'ensemble des services, on remplit les champs comme suit.

ADD A COMMAND

Command Name:
check_all_services
This directive is the short name used to identify the command. It is referenced in contact, host, and service definitions, among other places.

Command Line:
\$USER1\$/check_nrpe -H \$HOSTADDRESS\$ -c alias_service
This directive is used to define what is actually executed by Nagios when the command is used for service or host checks, notifications, or event handlers. Before the command line is executed, all valid macros are replaced with their respective values. See the documentation on macros for determining when you can use different macros. Note that the command line is not surrounded in quotes. Also, if you want to pass a dollar sign (\$) on the command line, you have to escape it with another dollar sign.

Command Description:
Check all services
This is a description of the command.

Create Command Cancel

- **Command Name** : check_all_services
- **Command Line** : \$USER1\$/check_nrpe -H \$HOSTADDRESS\$ -c alias_service
- **Command Description** : check all services

Une fois la commande ajoutée, le bandeau suivant devrait s'afficher

Command added.

Modification du template Windows

On peut maintenant passer à la modification du template en lui-même. On se rend dans l'onglet **Administration**, puis dans le volet **modèles**. On sélectionne ensuite le modèle à modifier (il est possible de dupliquer le modèle afin de ne pas modifier ceux existant par défaut)

On se rend dans la partie **Services** et on remplit comme suit. Il n'est pas nécessaire ici de donner une valeur à \$ARG1\$ car la commande ne contient pas de variable.

ADD SERVICE FOR HOST TEMPLATE WINDOWS-SERVER

Service Description:
check_all_services
This directive is used to define the description of the service, which may contain spaces, dashes, and colons (semicolons, apostrophes, and quotation marks should be avoided). No two services associated with the same host can have the same description. Services are uniquely identified with their host_name and service_description directives.

Display Name: (Optional)
Check all services

Service Templates To Inherit From (Top to Bottom):

Add Service To Inherit From: EMC Add Template

Check Command: check_all_services Provide Value
The full path and arguments to the command to run for this service's checks. If you leave this as empty, you will be able to select a pre-defined command with arguments later.

Check Command Parameters:

Value for \$ARG1\$: Add Parameter

Add Service Cancel

Pour appliquer les changements effectués, il faut se rendre dans la partie **appliquer la configuration** dans le volet de gauche puis cliquer sur **Restart Job**

Les commutateurs

La supervision de commutateurs est simple. En effet, il suffit de vérifier que l'hôte joignable sur le réseau, donc une simple requête ICMP suffit. On ajoute donc le commutateur comme n'importe quel autre équipement réseau en lui appliquant le template **Generic Host**.

Les serveurs VMware

La supervision des serveurs VMware est elle aussi plutôt simple. Il faut en effet appliquer à la machine le template **ESX** déjà présent dans la solution EyesOfNetwork.