

Copyright (c) Cedric TEMPLE

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

Table des matières

1	Présentation	2
1.1	Introduction	2
1.2	Philosophie de Zabbix	2
1.3	Sécurisation du flux	4
2	Installation de Zabbix	6
2.1	Installation côté machine agent	6
2.2	Installation côté machine centrale	8
3	Interface web	9
3.1	Configuration avancée	10
3.1.1	Ajout d'une machine	10
3.1.2	Ajout d'un graph	11
3.1.3	Paramètres des machines	11
3.1.4	Ajout d'alarme	11
4	Annexes	13
4.1	Difficultés possibles	13
4.2	Création d'un certificat	14

Chapitre 1

Présentation

1.1 Introduction

Ce document présente tout d'abord le fonctionnement de Zabbix puis son installation, l'interface utilisateur pour la configuration des machines et enfin un moyen de sécurisation des communications.

Zabbix est un logiciel permettant de monitorer les éléments physiques (mémoire, CPU, disques, ...) ou les services réseaux (SMTP, HTTP, ...) d'un ou plusieurs serveurs. Il peut monitorer de trois manières : soit par un processus lancé sur chaque machine et qui collecte les données locales, soit par un check externe (seuls les services réseaux pourront être testés), soit par SNMP (il peut aussi monitorer un équipement tel qu'un switch ou un routeur qui supporte SNMP).

Il peut générer des graphes de chaque paramètre (numérique) monitoré (voir figure 1.1), lever des alertes (voir figure 1.2), envoyer des mails lors d'une alerte, gérer plusieurs utilisateurs avec une vue pour chacun, ... La configuration est centralisée sur une même interface graphique et les données sont stockées dans une base MySQL.

1.2 Philosophie de Zabbix

Zabbix est constitué de deux parties : le frontend en PHP et les outils en C. Le frontend permet de configurer aisément tous les tests pour toutes les machines,

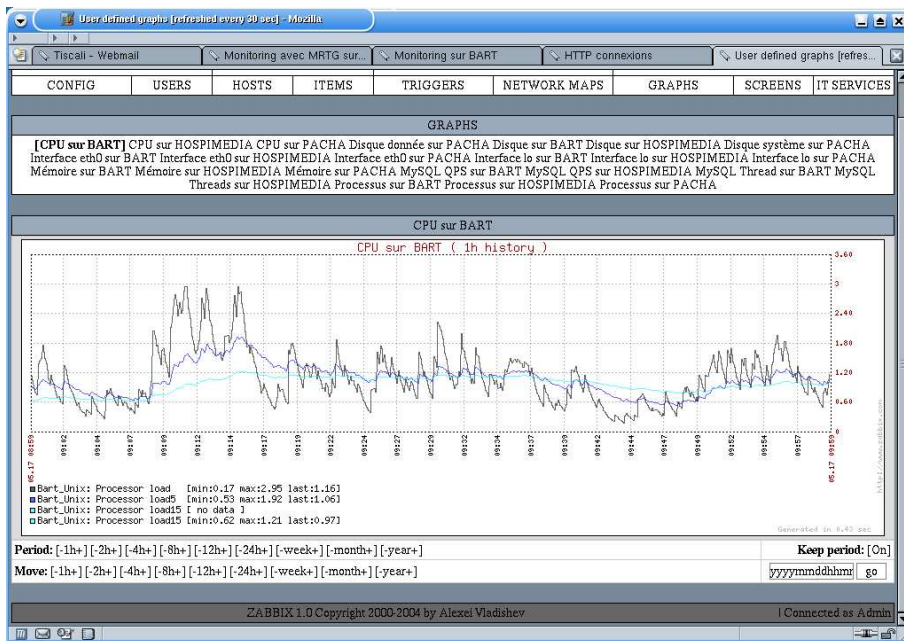


FIG. 1.1 – Génération de graph

Time	Description	Status	Severity
2004.May.14 14:12:22	Sshd is not running on Hospimedia_Unix	OFF	Average
2004.May.14 14:12:22	Syslogd is not running on Hospimedia_Unix	OFF	Average
2004.May.14 14:12:18	Low number of free inodes on Hospimedia_Unix' volume /home	OFF	High
2004.May.14 14:12:18	Low number of free inodes on Hospimedia_Unix's volume /	OFF	High
2004.May.14 14:12:18	Mysql is not running on Hospimedia_Unix	OFF	Average
2004.May.14 14:12:17	SSH server is down on Hospimedia_Unix	OFF	Average
2004.May.14 14:12:17	Processor load is too high on Hospimedia_Unix	OFF	Average
2004.May.14 14:12:07	IMAP server is down on Hospimedia_Unix	OFF	Average
2004.May.14 14:12:07	POP3 server is down on Hospimedia_Unix	OFF	Average
2004.May.14 14:12:07	Email (SMTP) server is down on Hospimedia_Unix	OFF	Average
2004.May.14 14:12:06	WEB (HTTP) server is down on Hospimedia_Unix	OFF	Average
2004.May.14 14:12:06	Too many processes on Hospimedia_Unix	OFF	High
2004.May.14 14:11:56	Apache is not running on Hospimedia_Unix	OFF	Average
2004.May.14 14:11:55	Lack of free memory on server Hospimedia_Unix	OFF	Average
2004.May.14 14:11:54	Lack of free swap space on Hospimedia_Unix	OFF	High
2004.May.14 14:11:53	Server Hospimedia_Unix is unreachable	OFF	High
2004.May.14 14:11:08	Email (SMTP) server is down on Hospimedia_Standalone	ON	Average
2004.May.14 14:10:58	Server Hospimedia_Unix is unreachable	ON	High
2004.May.14 14:10:53	Lack of free memory on server Hospimedia_Unix	UNKNOWN	Average
2004.May.14 14:10:53	Low free disk space on Hospimedia_Unix's volume /	UNKNOWN	High
2004.May.14 14:10:53	Low number of free inodes on Hospimedia_Unix's volume /	UNKNOWN	High
2004.May.14 14:10:53	Too many processes on Hospimedia_Unix	UNKNOWN	High
2004.May.14 14:10:53	Processor load is too high on Hospimedia_Unix	UNKNOWN	Average
2004.May.14 14:10:53	Too many processes running on Hospimedia_Unix	UNKNOWN	Average
2004.May.14 14:10:53	Lack of free swap space on Hospimedia_Unix	UNKNOWN	High
2004.May.14 14:10:53	Too may users connected on server Hospimedia_Unix	UNKNOWN	Average
2004.May.14 14:10:53	/passwd has been changed on server Hospimedia_Unix	UNKNOWN	Average
2004.May.14 14:10:53	Low free disk space on Hospimedia_Unix's volume /home	UNKNOWN	High

FIG. 1.2 – Les alertes

ce qui en fait une centralisation de la configuration. Il est ainsi plus facile de monitorer les services depuis une seule interface. Les outils font le monitoring des services (zabbix_agentd) et la centralisation des données (zabbix_suckerd et zabbix_trapperd). Zabbix définit donc deux types de machines : une machine qui centralise les données (qui sera appelée “machine centrale” et sur laquelle sera lancée un serveur de données et un serveur avec PHP) et une ou plusieurs machines qui seront monitorées (“machine agent”).

Remarque :

- la machine centrale peut être machine agent mais ce n’est pas obligatoire (on peut décider d’installer une machine à part qui ne fera rien d’autre que centraliser les données)
- la base de données peut être installée sur une machine et le frontend sur une autre machine
- zabbix_suckerd se connecte à chaque zabbix_agentd
- zabbix_trapperd attend les informations lorsqu’un utilisateur utilise zabbix_sender en ligne de commande

Dans notre cas nous avons : une machine centrale (appelée BART) et plusieurs machines agents (appelées Pacha, Dédié **et Bart**). Donc le frontend, la base de données, zabbix_suckerd et zabbix_trapperd sont situées sur Bart ; zabbix_agentd est situé sur Pacha, Dédié et Bart.

1.3 Sécurisation du flux

Les informations circulant entre les zabbix_agentd et le zabbix_suckerd ne sont pas cryptées et n’ont pas d’encodage particulier. Exemple avec telnet :

```
[root@bart root]# telnet localhost 10000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
proc_cnt[httpd]
20.000000Connection closed by foreign host.
[root@bart root]#
```

En faisant un telnet sur la machine locale sur le port d’écoute de zabbix_agentd (10000) et en lui envoyant une commande qui demande le nombre de processus httpd en exécution (proc_cnt[httpd]) nous arrivons à obtenir le nombre exacte

(20). Il est donc très facile d'avoir toutes les informations lorsqu' on connaît le protocole.

Certes, zabbix permet de filtrer selon l'adresse du serveur (voir fichier de configuration) mais il est tout à fait possible de spoofer cette adresse. Les informations qui circulent sont sensibles. En effet, si une personne mal intentionnée souhaite faire une deni de service cela lui est très simple. Il lui suffit de s'inscrire plusieurs fois au site de recrutement et d'envoyer le plus gros fichier possible comme CV. Il en en plus possible de faire cela de manière automatisée avec Perl :LWP. Il faut donc trouver un moyen de sécuriser mais surtout d'authentifier les personnes se connectant sur le port. Ce mécanisme est possible avec stunnel : un outil utilisant les Secure Socket Layer avec possibilité de gestion des certificats. Il suffit alors de générer un certificat d'une CA (Certificat Authority) puis un certificat signé par le certificat de la CA pour chaque côté de la liaison. Enfin à l'établissant la connexion et de chque côté, stunnel va vérifier le certificat de l'autre côté et établir la connexion que si et seulement si il peut attester de l'identité du détenteur du certificat. En résumé, pour "pirater" la liaison il faut obtenir le certificat de la CA, qui est sur notre réseau local (Bart). Cependant, la personne qui aura réussi à obtenir ce certificat n'aura pas besoin de le pirater car elle aura déjà la main mise sur notre réseau.

Chapitre 2

Installation de Zabbix

L'installation est bien documentée et se trouve dans le répertoire doc de l'archive. Il y a deux installation types : une côté machine centrale et une côté machine agent.

2.1 Installation côté machine agent

Il faut tout d'abord détarrer/dézipper l'archive. Puis aller ensuite dans le répertoire zabbix-VERSION et faire “./configure”. Il faut bien vérifier que toutes les bibliothèques sont trouvées (aucune bibliothèque autre qu'un système avec GCC et GNU/make n'est nécessaire). La suite est aisée : make. Voilà pour la compilation. (Remarque : le make install habituel ne fonctionne pas).

Maintenant il créer un répertoire de configuration :

```
make /etc/zabbix
```

et y copier le fichier de configuration

```
cp misc/conf/zabbix_agentd.conf /etc/zabbix/
```

Attention : on utilise les démons pas les outils inetd donc il faut faire attention : copier zabbix_agentd.conf et non zabbix_agent.conf. Il faut modifier les paramètres intéressants :

```
# l'adresse du serveur  
# attention à bien mettre 127.0.0.1 si on est en local  
Server=192.168.0.202
```

```

# le port d'écoute
ListenPort=10000

# les parametres pour la BD ne sont pas utiles donc
# on les commente
# DBHost=localhost
# DBName=zabbix
# DBPassword=zabbixpass
# DBSocket=/var/run/mysqld/mysqld.sock

# si il y a un serveur MySQL que l'on souhaite monitorer
# il faut decommenter les lignes suivantes
UserParameter=mysql[ping],mysqladmin -uroot -ppassword ping|
 \ grep alive|wc -l
UserParameter=mysql[uptime],mysqladmin -uroot -ppassword
 \ status | cut -f2 -d":"|cut -f1 -d"T"
UserParameter=mysql[threads],mysqladmin -uroot -ppassword
 \ status| cut -f3 -d":"|cut -f1 -d"Q"
UserParameter=mysql[questions],mysqladmin -uroot -ppassword
 \ status| cut -f4 -d":"|cut -f1 -d"S"
UserParameter=mysql[slowqueries],mysqladmin -uroot -ppassword
 \ status|cut -f5 -d":"|cut -f1 -d"O"
UserParameter=mysql[qps],mysqladmin -uroot -ppassword status|
 \ cut -f9 -d":"
UserParameter=version[mysql],mysql -V

```

Ensuite il faut copier le fichier de démarrage zabbix_agentd... qui se trouve dans l'arborescence misc/init.d/... Il faut prendre celui qui correspond le mieux. De même il faut modifier quelques paramètres :

```

# l'endroit où l'archive a été décompressée
BASEDIR=/opt/zabbix
# le pid file si désire le changer d'endroit
PIDFILE=/var/tmp/zabbix_agentd.pid

```

Voilà il ne reste plus qu'à lancer zabbix_agentd :
/etc/init.d/zabbix_agentd

2.2 Installation côté machine centrale

De même il faut lancer dans l'ordre :

```
./configure --with-mysql [--with-snmp]
make
mkdir /etc/zabbix
cp misc/conf/zabbix_{agentd,suckerd,trapperd}.conf /etc/zabbix/
cp misc/init.d/./zabbix_{agent,sucker,trapper} /etc/init.d/
```

Remarque : selon le répertoire où ils se trouvent les fichiers de démarrage ont des noms différents. Ensuite il faut s'occuper de MySQL :

```
mysqladmin -uroot -p create zabbix
mysql -uroot -p < create/mysql/schema.sql
mysql -uroot -p < create/data/data.sql
[on peut créer un utilisateur zabbix avec un mot de passe
et des droits limités à la seule base zabbix]
```

Là encore il faut modifier les fichiers de configuration et de démarrage pour qu'ils correspondent à l'installation. Puis il suffit de lancer les démons :

```
/etc/init.d/zabbix_agentd start
/etc/init.d/zabbix_suckerd start
/etc/init.d/zabbix_trapperd start
```

Enfin, il faut s'occuper de l'interface PHP qui se trouve dans le répertoire frontend/php/ en modifiant le fichier frontend/php/include/db.inc.php : les paramètres pour la base de données (nom de la base, nom de l'utilisateur et son mot de passe). Ne pas oublier de créer un VirtualHost pour Apache, ou un autre moyen d'y accéder. Remarque : le répertoire frontend/php/ peut être déplacé dans un autre répertoire sans que cela pose problème.

Chapitre 3

Interface web

L'interface graphique est assez complexe à aborder au début mais après un temps d'adaptation de quelques heures on s'y retrouve très vite et on arrive à faire tout ce que l'on souhaite. La première chose à faire est de bien lire le tutorial écrit dans la documentation officielle pour suivre les étapes une par une et bien les comprendre. Nous allons voir un cas d'utilisation.

Tout d'abord la page est constituée de deux parties : le bandeau supérieur (permettant de naviguer entre chaque catégorie) et l'affichage de la catégorie. Le bandeau possède deux parties lorsque l'on est un utilisateur avec des droits limités (droit en lecture seulement) et trois parties lorsqu'on est authentifié comme "admin". La première chose à faire est donc de s'authentifier en administrateur (en cas de première utilisation, login : admin et mot de passe vide). Nous allons maintenant naviguer entre chaque catégorie.

- latests values : voir les dernières valeurs pour chaque machine
- triggers : vérifier la validité ou non des alarmes (sont elles actives ou non ?)
- queue : afficher les paramètres en attente de réponse de la part des agents
- alarms : donner l'historique de toutes les dernières alarmes avec leur changement d'état
- alerts : recenser tous les envoies (ou non) des emails en cas d'alarmes
- network maps : le plan du réseau avec l'affichage des états
- graphs : les graphiques enregistrés
- screens : regrouper logique de graphs (pour faire un bilan sur une machine par exemple)
- IT services : représenter les serveurs sous forme hiérarchique
- home : se connecter/se déconnecter
- about : suivre les liens vers le site de zabbix

- status of zabbix : obtenir des informations comme le nombre de valeur stockées, le nombres d’alertes levées, ...
- availability report : voir la fiabilité des levées d’alertes
- config : configurer le temps d’enregistrement des laertes, ajouter différents médias (email, SMS) d’alertes
- users : ajouter/supprimer/modifier des groupes, des utilisateurs
- hosts : ajouter/supprimer/modifier des machines
- items : éditer les paramètres pour chaque machine
- triggers : éditer les envoies d’alertes pour chaque paramètre de chaque machine

3.1 Configuration avancée

Nous allons voir les possibilités de configuration de Zabbix. Il ne sera pas vu les choses les plus simples comme l’ajout d’un utilisateur, ni les screens, ni le dessin de réseau, ...

3.1.1 Ajout d’une machine

On peut si on le souhaite ajouter une machine et l’affecter directement dans un groupe. Pour cela il faut aller dans le menu Hosts puis dans la partie ‘Host’ en bas. On donne le nom de la machine (par exemple Dédié), son groupe (ou on rentre une valeur dans ‘New Group’), on clique sur ‘Use ip Adress’ et on rentre l’adresse IP (et non le nom de machine) et le port d’écoute du service. Pour avoir un template (ET IL VAUT MIEUX sinon il faudra rentré les paramètres avec leur syntaxe correcte UN PAR UN!!!) on utilise ‘Use the host as template’ et on sélectionne celui que l’on souhaite. Remarque : il existe des templates déjà fait

- Host.Unix : une machine Unix avec les partitions, le CPU, les interfaces, les services, ...
- Host.SNMP : un équipement capable de répondre aux requêtes SNMP
- Host.Standalone : une machine dont les services sont monitorés de l’extérieur (ne nécessite pas d’agent installé dessus)
- Application.MySQL : une machine exécutant un serveur MySQL (QpS, requêtes lentes, threads, ...)
- Host.Win32 : une machine windows.

3.1.2 Ajout d'un graph

Les graphs pour chaque paramètre ne sont pas générés automatiquement mais seulement à la consultation de la page. On peut avoir les graphs pour chaque paramètre en allant dans la partie 'Latests values', en sélectionnant la machine et en cliquant sur 'Graph' pour le paramètre souhaité. Cependant, ceci n'est pas pratique et on ne peut pas obtenir un graph avec plusieurs courbes. Il faut alors les construire soi-même. Pour cela il faut sélectionner 'Graphs' (sur la troisième ligne, la première ne permettant que de consulter), choisir un nom et une taille dans la partie 'Graph' en bas et cliquer sur 'add'. Voilà, le graph est alors créé mais ne contient aucune valeur. Pour lui ajouter des valeurs, il faut cliquer sur ce graph, puis on peut sélectionner un paramètre ("bart : Number of running processes apache" par exemple), choisir sa couleur et si il doit être en pointillé, ... et cliquer sur 'add'. Pour ajouter une autre courbe ("bart : Number of running processes sshd") on fait de même. Ce qui permet en un seul coup d'oeil d'avoir plusieurs paramètres.

3.1.3 Paramètres des machines

Tout d'abord il faut sélectionner 'Items' et choisir sa machine dans la partie 'Configuration of Items'. La première chose à faire est de désactiver tous les items qui ne seront pas utilisés (par exemple si la machine n'a qu'une seule partition, il n'est pas nécessaire de monitorer la partition /home). Pour cela il faut sélectionner chaque paramètre (case à cocher sur la gauche), descendre tout en bas de la fenêtre et cliquer sur 'Disable selected'. Ensuite il faut modifier certains paramètres comme par exemple si on souhaite comptabiliser le nombre de processus nommés 'machin' il faut sélectionner un exemple faisant cela ('Change' et non le paramètre) puis modifier le nom du programme en 'machin' (—> proc_cnt[machin]) et modifier les autres champs (description, ...) selon la convenance et cliquer sur 'add' (et non sur 'update' qui mettra à jour le paramètre courant). Conseil : pour ajouter un test il vaut mieux prendre en exemple un autre, c'est beaucoup plus simple que de retaper la syntaxe particulière.

3.1.4 Ajout d'alarme

Pour cela il faut qu'il y existe un utilisateur et que cet utilisateur est un média pour le prévenir (vérifier dans 'Config' puis dans 'Users'). Ensuite il faut aller dans la partie 'triggers' puis sélectionner la machine. On peut changer les caractéristiques de l'alarme.

téristiques (degré, valeur de dépassement à partir de laquelle envoyée l'alarme, ...) de l'alarme en cliquant sur 'change' pour chaque alarme. On peut modifier le moyen d'envoyer l'alarme en cliquant sur 'Action'. Dans cette partie on peut choisir d'envoyer à une seule personne ou un groupe de personne, d'envoyer l'alarme seulement si elle devient 'On' ou 'Off' ou les deux, le délai entre deux messages et le texte qui sera envoyé. Remarque : zabbix permet de remplacer certains patterns par leur valeur (exemple : le pattern HOSTNAME sera remplacé par la valeur du nom de la machine, Dédié_Standalone :smtp_perf.last(0) permet d'avoir la dernière (last(0) valeur du paramètre smtp_perf de la machine Dédié_Standalone).

Chapitre 4

Annexes

4.1 Difficultés possibles

Voici un petit florilège des problèmes que l'on peut rencontrer et une manière de les résoudre. Cette partie peut(ou doit ?) subir des modifications.

- les images ne s'affichent pas pour les graphes : soit PHP n'est pas compilé avec GD2 et libpng soit la table history est bloquée sur le serveur MySQL (peut arriver si le disque dur est rempli ; il faut alors réparer la table : "repair table history ;" avec un client mysql)
- pas de réponses des autres hosts pourtant leur agent est lancé : peut venir du fait que c'est zabbix_trapperd qui n'est pas lancé sur la machine centrale
- plus aucunes données reçues, malgré le fait que tout marche sur toutes les machines : lorsque le tunnel réalisé avec stunnel entre le serveur Dédié et bart ne fonctionne pas, stunnel bloque zabbix dans un état d'attente. Si la connexion tunnelée est indisponible (en cas de panne du réseau par exemple) il vaut mieux arrêter le tunnel avec un killall stunnel sur bart puis le redémarrer AU RETOUR (et uniquement là) de la connexion entre Dédié et bart
- zabbix_??? ne veut ne veut pas se lancer ou s'arrêter (ou les deux) : tout d'abord tuer tous les processus : killall zabbix_??? mais aussi le tunnel : killall stunnel ; puis effacer les fichiers de pid pour chaque processus (voir dans les fichiers de configuration où ils se trouvent) et relancer chaque processus
- tous les processus sont lancés sur toutes les machines et pourtant il n'y a aucune donnée dans les graphiques : peut être que 1 : la mauvaise adresse

- IP ou le mauvais port est entré ; 2 : les hosts ou les paramètres sont “Not Monitored” ou “Not supported” : il suffit de changer leur état.
- tous les hôtes répondent sauf Dédié : le host Dédié doit être configuré dans l’interface graphique avec l’adresse IP : 127.0.0.1 et le port 10003 pour être utilisé au travers du tunnel ; il peut arriver aussi que stunnel ne soit pas lancé (voire planté mais là c’est beaucoup moins courant)
- lors d’ajout d’une courbe à un graph il n’y a pas le paramètre souhaité : le host n’est pas monitoré ou le paramètre n’est pas monitoré ; il faut activer le host ou le paramètre.

4.2 Création d’un certificat

```
mkdir stunnel
cd stunnel
```

```
export SSLEAY_CONFIG='pwd'/openssl.cnf
```

faire le fichier de config donner en annexe

```
Creation d’un certificat pour la CA (Certificate Authority)
(NOTE: il faut entrer une phrase vide à la première question
"file ...")
/usr/lib/ssl/misc/CA.pl -newca
```

```
Creation d’un certificat AGENT:
openssl req -new -nodes -keyout certagentzabbix.pem
-out certagentzabbix_req.pem
REMARQUE: pour la question: "Organizational Unit Name (eg,
section) []:" il faut entrer un truc du style
"zabbix_agent".
```

```
Et on le signe avec la CA:
openssl ca -notext -infiles certagentzabbix_req.pem
>> certagentzabbix.pem
```

```
Creation d’un certificat SERVEUR:
openssl req -new -nodes -keyout certserveurzabbix.pem
```

```
-out certserveurzabbix_req.pem
REMARQUE: pour la question: "Organizational Unit Name (eg,
          section) []:"
il faut entrer un truc du style "zabbix_serveur".
```

```
Et on le signe avec la CA:
openssl ca -notext -infiles certserveurzabbix_req.pem
>> certserveurzabbix.pem
```

Installation des certificats:

```
certificat de la CA (côté serveur ET agent):
cp demoCA/cacert.pem /etc/ssl/certs/
```

```
certificat des agents (côté agent):
cp certagentzabbix.pem /etc/ssl/certs/
cp demoCA/private/cakey.pem /etc/ssl/certs/zabbixCA.pem
c_rehash
```

```
certificat du serveur (côté serveur):
cp certserveurzabbix.pem /etc/ssl/certs/
c_rehash
```

tunnels:

```
côté machine central et pour chaque agent crypté:
stunnel -c -d 127.0.0.1:PORT[i] -r IP[i]:10002
        -p /etc/ssl/certs/certserveurzabbix.pem
        -v 2 -D 3 -A /etc/ssl/certs/cacert.pem
```

dans notre exemple sur la machine bart:

```
stunnel -c -d 127.0.0.1:10003 -r 213.186.36.143:10002
        -p /etc/ssl/certs/certserveurzabbix.pem
        -v 2 -D 3 -A /etc/ssl/certs/cacert.pem
```

Ici nous n'avons qu'un agent à crypter: la machine Dédié
les autres n'ont pas besoin d'un tel tunnel.

côté agent (sur Dédié):

```
stunnel -d 10002 -r 127.0.0.1:10000 -p
        /etc/ssl/certs/certagentzabbix.pem
        -v 2 -A /etc/ssl/certs/cacert.pem
```

```

ANNEXE: fichier openssl.cnf
#####
#####

#
# OpenSSL example configuration file.
# This is mostly being used for generation of
# certificate requests.
#

# This definition stops the following lines choking
# if HOME isn't defined.
HOME                = .
RANDFILE            = $ENV::HOME/.rnd

# Extra OBJECT IDENTIFIER info:
# oid_file           = $ENV::HOME/.oid
oid_section         = new_oids

# To use this configuration file with the "-extfile"
# option of the "openssl x509" utility, name here
# the section containing the X.509v3 extensions
# to use:
# extensions         =
# (Alternatively, use a configuration file that has only
# X.509v3 extensions in its main [= default] section.)

[ new_oids ]

# We can add new OIDs in here for use by 'ca' and 'req'.
# Add a simple OID like this:
# testoid1=1.2.3.4
# Or use config file substitution like this:
# testoid2=${testoid1}.5.6

```

```

#####
[ ca ]
default_ca = CA_default

#####
[ CA_default ]

dir                = ./demoCA
certs              = $dir/private/certs
crl_dir            = $dir/crl
database           = $dir/index.txt
new_certs_dir      = $dir/newcerts

certificate        = $dir/cacert.pem
serial             = $dir/serial
#crlnumber         = $dir/crlnumber

crl                = $dir/crl.pem
private_key        = $dir/private/cakey.pem
RANDFILE           = $dir/private/.rand

x509_extensions   = usr_cert

name_opt           = ca_default
cert_opt           = ca_default

default_days       = 365
default_crl_days  = 30
default_md         = md5
preserve           = no

policy             = policy_match

# For the CA policy
[ policy_match ]
countryName        = match
stateOrProvinceName = match
organizationName   = match

```

```
organizationalUnitName = optional
commonName             = supplied
emailAddress           = optional
```

```
[ policy_anything ]
countryName            = optional
stateOrProvinceName   = optional
localityName           = optional
organizationName       = optional
organizationalUnitName = optional
commonName             = supplied
emailAddress           = optional
```

```
#####
```

```
[ req ]
default_bits           = 1024
default_keyfile         = privkey.pem
distinguished_name     = req_distinguished_name
attributes              = req_attributes
x509_extensions        = v3_ca
```

```
string_mask = nombstr
```

```
[ req_distinguished_name ]
countryName                = Country Name (2 letter code)
countryName_default        = FR
countryName_min            = 2
countryName_max            = 2
```

```
stateOrProvinceName       = State or Province Name (full name)
stateOrProvinceName_default = Nord
```

```
localityName              = Locality Name (eg, city)
localityName_default       = Loos
```

```
0.organizationName        = Organization Name (eg, company)
0.organizationName_default = Dédié
```

```

organizationalUnitName      = Organizational Unit Name (eg, sect

commonName                  = Common Name (eg, YOUR name)
commonName_max              = 64
commonName_default         = TEMPLE Cedric

emailAddress                = Email Address
emailAddress_max           = 64
emailAddress_default       = cedric.temple@Dédié

[ req_attributes ]
challengePassword          = A challenge password
challengePassword_min     = 4
challengePassword_max     = 20

unstructuredName           = An optional company name

[ usr_cert ]

basicConstraints=CA:FALSE

nsComment                  = "OpenSSL Generated Certificate"

subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer:always

[ v3_req ]

basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment

[ v3_ca ]

subjectKeyIdentifier=hash

authorityKeyIdentifier=keyid:always,issuer:always

```

```
basicConstraints = CA:true
```

```
[ crl_ext ]
```

```
authorityKeyIdentifier=keyid:always,issuer:always
```

GNU Free Documentation License

Version 1.2, November 2002

Copyright (C) 2000,2001,2002 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats

include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.
- I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
- N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of

Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may

distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <http://www.gnu.org/copyleft/>.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.