openca - ocspd.conf

Fichier de configuration pour openca-ocspd

Le fichier de configuration est divisé en sections, et est conforme à la syntaxe spécifiée dans openssl-config.

Exemple

```
[ ocspd ]
default_ocspd = OCSPD_default

[ OCSPD_default ]

dir = /usr/local/etc/ocspd
db = $dir/index.txt
md = sha1

ca_certificate = $dir/certs/cacert.pem
ocspd_certificate = $dir/certs/ocspd_cert.pem
ocspd_key = $dir/private/ocspd_key.pem
pidfile = $dir/ocspd.pid

user = ocspd
group = daemon
bind = *
port = 2560
max_childs_num = 5
max_req_size = 8192

request = ocsp_req
response = ocsp_response

dbms = dbms_ldap # Example using the LDAP for CRL retrivial

#dbms = dbms_file # Example using file for CRL

engine = HSM # ENGINE section

####################################################################
[ ocsp_req ]
default_keyfile = key.pem

####################################################################
[ ocsp_response ]
dir = /usr/local/etc/ocspd
ocsp_add_response_certs = $dir/certs/chain_certs.pem
ocsp_add_response_keyid = yes
next_update_days = 0
next_update_mins = 5

####################################################################
```

```
[ dbms_ldap ]

# It is possible to use an URI to identify a CRL and/or the CA certificate, the general format is:
# [protocol]://[user[:pwd]@]server[:port]/[path]
#
# where:
# protocol - specifies the protocol to be used, supported are
# file, ldap, http
# user - is the user for auth (meaningful only if ldap or
# http is used)
# pwd - password used for auth (meaningful only if ldap
# or http is used)
# port - port to connect to (meaningful only if ldap or
# http is used)
# path - complete path to the object (meaningful only if
# http is used)
#
# You can have the CRLs/CA certificates on a simple file
# crl_url = file:///usr/local/etc/ocspd/crl.pem
#
# You can retrieve the CRLs/CA certificates from a web server
# crl_urt = http://server/ca/cacert.der
#
# You can store the CRL into an LDAP server, simply
# store it in certificateRevocationList;binary attribute
#
# There are different way, all legal, to specify the CRL
# URL address:
# crl_url = ldap://user:pwd@ldap.server.org:389
# crl_url = ldap://ldap.server.org:389
crl_url = ldap://localhost

# The CRL entry DN is the DN to look for when retrieving the
# date from the LDAP server. Put here the complete DN (usually
# the DN of the CA's certificate).
crl_entry_dn = "email=email@address, cn=Certification Auth, \
o=Organization, c=IT"

#################################################################
[ dbms_file ]

# You can have the CRL on a simple file in PEM format
crl_url = file:///usr/local/etc/ocspd/crl.pem

[ HSM ]
# Hardware accelerators support via the ENGINE interface
engine_id = MyAccelerator
0.engine_pre = login:1:10:11:myPassword
# 0.engine_post = logout:1:10:11
```

default_ocspd Dans cette section du fichier de configuration sont placés les options utilisées par le répondeur, certains sont disponibles en utilisant les options de la ligne de commande.

db Spécifie la db où tout est concervé. Actuellement, le seul format fichier supporté est celui de openssl.

md Spécifie le hash à utiliser. Défaut : sha1

ca_certificate Chemin vers de certificat de la CA

ocspd_certificate Chemin vers le certificat utilisé par le répondeur

ocspd_key Chemin de la clé privée du certificat utilisé par le répondeur

pidfile fichier du pid du processus

user UID du processus

group GID du processus

bind Adresse d'écoute

port Port d'écoute

threads_num Nombre de threads qui devraient être créés au démarrage. plus le nombre est élevé, plus il peut gérer les fort trafics.

chroot_dir chroot d'application dans le répertoire spécifié

max_req_size Taille maximum de requête reçue. Au delà la requête est détruite. Généralement les requêtes font environ 200/300 octets

request section non utilisé actuellement

response section Ici sont conservés les options pour la construction des réponses

dbms Options pour la crl

ocsp_add_response_certs Chemin d'un fichier contentant les certificats à ajouter à la réponse (généralement toute la chaîne de certification).

ocsp_add_response_keyid Spécifie si l'id de clé est ajouté dans la réponse

next_update_days Nombre de jours jusqu'à la prochaine mise à jours.

next_update_mins idem pour la partie minutes. La réponse est valide pour days+mins

ca_url URI où le certificat de la CA est localisée. (file :// http :// ou ldap ://)

crl_url URI où la crl est localisée (file :// http :// ou ldap ://)

crl_entry_dn avec ldap, spécifie le dn où rechercher l'attribut certificateRevocationList

engine_id Spécifie l'id de l'engine

engine_pre, engine_post Paramètres d'initialisation du périphérique