Table des matières :

Table des matières :	1
Objectif :	2
1.Le fichier openssl.cnf	2
2.Création des certificats :	3
3.Création d'un certificat SSL pour un serveur web :	4
4.Installation du certificat SSL	5

Avant-Propos

Compétences :

- A1.1.1 Analyse du cahier des charges d'un service à produire
- A1.2.4 Déterminer des tests nécessaires à la validation d'un service (3)
- A4.1.9 Rédaction d'une documentation technique

User : arthur et root

Objectif :

Dans cette procédure, nous allons montrer comment installer et configurer un serveur équilibrage de charges au moyen du service Keepalived sous Debian.

OS	Distribution	Version
Debian	Linux	8.5

1. Le fichier openssl.cnf

On commence par crée l'arborescence :

arthur@debian8:~\$ mkdir tpssl_

arthur@debian8:~\$ mkdir certs/_

arthur@debian8:~\$ mkdir private∕.

arthur@debian8:~\$ mkdir crl/_

arthur@debian8:~\$ mkdir newcerts____

On crée le fichier index vide

arthur@debian8:~\$ touch index.txt_

On crée le fichier serial avec la valeur 01



On copie le fichier openssl.cnf dans le répertoire tpssl.

arthur@debian8:~\$ cp /etc/ssl/openssl.cnf /home/arthur/tpssl/

On modifie ensuite le fichier copier pour modifie la valeur dir

arthur@debian8:~/tpssl\$ nano openssl.cnf

- 2. Création des certificats :
- 1. Création du certificat de l'autorité de certification

Cette étape consiste à crée la paire de clés privée/publique puis un certificat racine autosigné.

On aura donc une clé privée protégée par un mot de passe et une demande de certificat numérique valable 3650 jours.

arthur@debian8:~/tpssl\$ openssl req -new -x509 -extensions v3_ca -keyout private /cakey.pem -out cacert.pem -days 3650 -config ./openssl.cnf Generating a 2048 bit RSA private key ...+++ ...+++ writing new private key to 'private/cakey.pem' Enter PEM pass phrase: Verifying - Enter PEM pass phrase: -----You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. -----Country Name (2 letter code) [AU]:FR State or Province Name (full name) [Some-State]:14 Locality Name (eg, city) []:caen Organization Name (eg, company) [Internet Widgits Pty Ltd]: Organizational Unit Name (eg, section) []: Email Address []:

Les deux fichiers de certificats sont maintenant apparus :

arthur@debian8:~/tpssl\$ ls cacert.pem certs crl index.txt newcerts openssl.cnf private serial

2. Extraction du certificat racine :

L'extraction consiste à afficher une sortie écran d'un certificat. On peut alors vérifier que le certificat est conforme aux attentes.

arthur@debian8:~/tpssl\$ openssl x509 –text –in cacert.pem

Pour sauvegarder vos fichiers, procédez à leur archivage :

arthur@debia	an8:∼∕tpssl\$	s tar –czf roc	otca.tar.gz pr:	ivate∕cakey.pem	cacert.pem
arthur@debia	an8:∼∕tpssl\$	S ls			
cacert.pem	crl	newcerts	private	serial	
certs	index.txt	openssl.cnf	rootca.tar.gz		
	~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~				

- 3. Création d'un certificat SSL pour un serveur web :
- 3. Création de la paire de clé et de la demande de certificat :



On vérifie la présence des 2 fichiers webkey.pem et newreg.pem



4. Signature de la demande de certificat par l'autorité :

arthur@debian8:~/tpssl\$ openssl ca –config ./openssl.cnf –policy policy_anything _out certs/webcert.pem _infiles certs/newreq.pem_

Il faudra répondre yes aux deux questions.

5. Vérification du chemin de certification

L'objectif est de vérifier que la signature du certificat a bien été effectuée par notre autorité de certification. Cela prouve que le chemin de certification est correct. Pour cela on utilise la commande verify d'openssl :

arthur@debian8:~/tpssl\$	openssl verify –Cafile cacert.pem certs/webcert.pem
usage: verify [–verbose]	[-CApath path] [-CAfile file] [-purpose purpose] [-crl_
check] [–no_alt_chains]	[–attime timestamp] [–engine e] cert1 cert2
recognized usages:	
sslclient	SSL client
sslserver	SSL server
nssslserver	Netscape SSL server
smimesign	S/MIME signing
smimeencrypt	S/MIME encryption
crlsign	CRL signing
any	Any Purpose
ocsphelper	OCSP helper
timestampsign	Time Stamp signing

4. Installation du certificat SSL

6. Export des certificats et de la clé privée

Décryptage de la clé privée du serveur web

La commande suivante permet de générer un nouveau fichier contenant la clé privée non cryptée (webkey-clair.pem)

arthur@debian8:~/tpssl\$ openssl rsa −in private/webkey.pem –out private/webkey–c lair.pem Enter pass phrase for private/webkey.pem: writing RSA key

Copier ensuite les fichiers webcert.pem, webkey-clair.pem dans le répertoire SSL d'Apache. (À faire en root)

root@debian8:~# cp /home/arthur/tpssl/private/webkey–clair.pem /etc/apache2/ssl/

root@debian8:~# cp /home/arthur/tpssl/certs/webcert.pem /etc/apache2/ssl/

7. Configuration d'Apache :

root@debian8:/etc/apache2/ssl# a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create s
elf–signed certificates.
To activate the new configuration, you need to run:
service apache2 restart
root@debian8:/etc/apache2/ssl# service apache2 restart

Nous devons crée un hôte virtuel (virtual host) pour qu'Apache soit capable de répondre aux requêtes SSL (https).

root@debian8:/etc/apache2/sites-available# nano default-ssl.conf

MARIETTE ARTHUR 14/11/2016 VERSION: 1

[OpenSSL HTTPS]

SSLCertificateFile /etc/apache2/ssl/webcert.pem_ SSLCertificateKeyFile /etc/apache2/ssl/webkey-clair.pem

root@debian8:/etc/apache2/sites-available# a2ensite default-ssl.conf

On lance le navigateur firefox avec l'url

L

root@debian8:∕et	c/apache2/sites-available# service apache	2 reload
On test sur le navigateur	r firefox : en https	
• The second s	マ C 🔍 Rechercher 👌 自 🔸 1	
	Cette connexion n'est pas certifiée	
	Vous avez demandé à Firefox de se connecter de manière sécurisée à 192.168.1.16 , mais nous ne pouvons pas confirmer que votre connexion est sécurisée.	
	Normalement, lorsque vous essayez de vous connecter de manière sécurisée, les sites présentent une identification certifiée pour prouver que vous vous trouvez à la bonne adresse. Cependant, l'identité de ce site ne peut pas être vérifiée.	
	Que dois-je faire ?	
	Si vous vous connectez habituellement à ce site sans problème, cette erreur peut signifier que quelqu'un essaie d'usurper l'identité de ce site et vous ne devriez pas continuer.	
	Sortir d'ici !	
• •	Détails techniques	
• •	Je comprends les risques	

On doit choisir « sortir d'ici » car le certificat n'a pas été vérifié par une autorité de certification de confiance.

8. Ajout de notre autorité de certification dans le navigateur FIREFOX

Afin d'éviter le message d'acceptation du certificat, il est possible de configurer le navigateur pour qu'il accepte tous les certificats venant de notre autorité de certification. Pour cela, il faut absolument copier le certificat racine (cacert.pem) sur le poste du client et l'importer dans la configuration du navigateur.

/options/avancé [chiffrement] – afficher les certificats -importer

On utilise FTP pour copier le fichier de la VM vers notre le pc client, on se connecte avec notre session de vm arthur.

I 192.168.1.16 💕 Nouvelle session						
📔 Mes docun 👻 🚰 🕎	 ← - →	- 🗈 🗈 🎜 🎜	2.	🌗 tp 👻 🚰 🔽 🛛 🖛 🕶	-> - 主	🔁 🏠 🔁 🗖
Envoyer 🕞 📝 Edite	er 🗙 🛃 🛯	Propriétés 🏾 🎽 📑	»	📲 Télécharger 🙀 📝	Editer 🗙 🚽	» 🕂 »
C:\Users\amariette\Docume	ents			/home/arthur/tpssl		
Nom	Taille	Туре	Da	Nom	Taille	Date de modification
₽		Répertoire parent	04,	₽		15/11/2016 09:02:02
퉬 copie USB		Dossier de fichiers	18,	퉬 certs		15/11/2016 06:45:23
🌗 GNS3		Dossier de fichiers	12,	\rm 📕 crl		15/11/2016 05:33:09
🐌 ISO		Dossier de fichiers	03,	newcerts		15/11/2016 06:54:37
MARIETTE		Dossier de fichiers	12/	private		15/11/2016 07:29:13
🛗 Mes formes		Dossier de fichiers	18,	Cacert.pem	2 KB	15/11/2016 06:19:57
퉬 Modèles Office perso		Dossier de fichiers	17,	index.txt	1 KB	15/11/2016 06:54:37
퉬 openElement		Dossier de fichiers	02,	index.txt.attr	1 KB	15/11/2016 06:54:37
퉬 SQL		Dossier de fichiers	04,	index.txt.old	0 KB	15/11/2016 05:33:31
퉬 Visual Studio 2010		Dossier de fichiers	29,	openssl.cnf	11 KB	15/11/2016 06:09:48
퉬 Visual Studio 2013	/	Dossier de fichiers	30,	🔚 rootca.tar.gz	3 KB	15/11/2016 06:28:11
💗 debian8.5.machine 1	5 13 323 KB	Open Virtualizatio	19,	serial	1 KB	15/11/2016 06:54:37
PRO FTP.odt	613 KB	OpenDocument T	30,	serial.old	1 KB	15/11/2016 05:33:52
オ	>					

On retourne sur firefox pour importer le certificat :

/options/avancé [chiffrement] – afficher les certificats -importer

D Général	Avancé
Q Recherche	Général Données collectées Réseau Mises à jour Certificats
Contenu	Requêtes Lorsqu'un serveur demande mon certificat personnel : gn sélectionner un automatiquement Image: me demander à chaque fois
 Sync Avancé 	✓ Interroger le répondeur OCSP pour confirmer la validité de Afficher les certificats Sélectionner un fichier contenant un (ou des) certificat ▲fficher les certificats Périphériques de sécurité Organiser ▼ Nouveau dossier
	Gestionnaire de certificats Favoris Bibliothèque Vous certificats Bureau Emplacements Vous possèdez des certificaties enregistrés identifiant ces autorités de certification Emplacements Nom Mom du certificat Périphérique de sécurité Bibliothèque Scientertificaties 4 (c) 2005 TÜRKTRUST Bilgi Betigim Güve TÜRKTRUST Elektronik Setfrika Hizmet Saglayu Builtin Object Token A-Trust Ges. f. Sicherheitssysteme im elektr. Date A-Trust-Qual-03 Builtin Object Token AC Camefrima S.A. Chambers of Commerce Root - 2008 Builtin Object Token Global Chambersign Root - 2008 Builtin Object Token AC Camefrima S.A. Chambers of Commerce Root - 2008 Builtin Object Token AC Camefrima S.A. Chambers of Commerce Root - 2008 Builtin Object Token AC Camefrima S.A. Chambers of Commerce Root - 2008 Builtin Object Token AC Camefrima S.A. Chambers of Commerce Root - 2008 Builtin Object Token AC Camefritime S.A. Exporter Supprimer ou ne plus faire confiance Yoir Modifier la confiance Exporter Supprimer ou ne plus faire confiance
	ОК

Une boite de dialogue apparait, on coche les 3 cases.

Il reste un problème de résolution de noms DNS. En effet, la valeur du champ « Common Name » du certificat crée précédemment est « techrom.fr ». Si vous n'accédez pas au serveur web avec URL basée sur le même nom, la plupart des navigateurs affichent un message d'avertissement. Ce problème pourra être résolu lorsque le nom de domaine du serveur

1. Résolution du problème DNS

Afin de résoudre ce problème dans pour autant modifier le système de résolution DNS, nous allons installer une résolution statique DNS par l'intermédiaire du fichier /etc/hosts. Ajouter la ligne suivante :

GNU nano 2.2.0	6	Fichier : /etc/host	s
127.0.0.1 127.0.1.1 192.168.1.16	localhost debian8.5 techrom.fr_	debian8	

On va enregistrer aussi sur notre pc client ds une session avec les droits admin

🕨 📗 🕨 Ordinateu	ur 🕨 Windows 7 SIO (C:) 🕨 Windows 🔸 System32 🕨 drivers 🔸 etc	
r 🔻 📄 Ouvri	ir Graver Nouveau dossi o	
ris reau Iplacements récer	Nom Image: C:\Windows\System32\drivers\etc\hosts - Notepad++ [Adminis Fichier Édition Recherche Affichage Encodage Langage Image: Display the same series of the same	Para
léchargements othèques	miniodatamini networks protocol 1 # Copyright (c) 1993-2009 Microsoft Cor 2 # services 3 # This is a sample HOSTS file used by M	p. icr
cuments ages Jsique Jéos	<pre>4 # 5 # This file contains the mappings of IP 6 # entry should be kept on an individual 7 # be placed in the first column followe 8 # The IP address and the host name shou 9 # contact</pre>	ad li d b ld
ipe résidentiel	<pre>9 # space. 10 # 11 # Additionally, comments (such as these</pre>) m
nateur	12 # lines or following the machine name d	eno
ndows 7 SIO (C:)	13 #	
ndows 7 PEDAGO	14 # For example:	
ARIETTE (G:)	15 # 16 # 102.54.94.97 rhino.acme.com	
au	17 # 38.25.63.10 x.acme.com 18 # localhost name resolution is handled 20 # 127.0.0.1 localhost 21 # ::1 localhost 22 23 127.0.0.1 localhost 24 192.168.1.144 sisr.local 25 192.168.1.144 slam.local 26 192.168.1.16 techrom.fr	wit

On test dans notre navigateur avec https://techrom.fr

Apache2 Debian Default Page: I >	· [+
https://techrom.fr	⊽ C ^e Q, Rechercher
debian	Apache2 Debian Default Page
ucbidit	It works!

MARIETTE ARTHUR 14/11/2016 VERSION: 1