Table des matières :

Introduction	
Prérequis	1
Installation	2
Configuration	3
Création d'un certificat ssl	5

### **Introduction**

Un serveur web permet d'héberger et de diffuser des sites internet ou des applications web. En entreprise, il est essentiel pour la communication, le partage d'informations (intranet) et la mise en place de services en ligne.

Apache est l'un des serveurs web les plus utilisés pour sa fiabilité, sa flexibilité et sa compatibilité avec de nombreux systèmes. Il permet d'héberger des sites sécurisés grâce au protocole HTTPS, qui chiffre les échanges pour garantir la confidentialité et l'intégrité des données. L'utilisation d'une autorité de certification (PKI) permet de générer des certificats SSL/TLS et d'assurer une sécurité renforcée pour les utilisateurs et les services web.

### **Prérequis**

Pour installer notre serveur apache nous utilisons ici une machine Debian 12. Il faut préalablement installer un serveur Windows en PKI (autorité de certification) pour certifier et sécuriser notre serveur web.

# **Installation**

Installons apache2 :

apt install apache2

Pour s'assurer qu'apache s'est bien installé, testons à l'adresse ip du serveur sur un client :

http://IP\_SERVEUR\_WEB

Si tout s'est bien passé cette page doit apparaitre :

172.10.10.250 at 〇 一 公
Apache2 Debian Default Page
debian
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should <b>replace this file</b> (located at /var/www/html/index.html) before continuing to operate your HTTP server. If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is <b>fully</b> <b>documented in /usr/share/doc/apache2/README.Debian.gz</b> . Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the <b>manual</b> if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Debian systems is as follows:

## **Configuration**

Déplaçons-nous dans le dossier /etc/apache2/sites-available puis copions le fichier 000default.conf pour créer notre site :

cd /etc/ apache2/sites-available

cp 000-default.conf www.algara.at.conf

root@srv-web:/etc/apache2/sites-available# cp 000-default.conf www.algara.at.conf root@srv-web:/etc/apache2/sites-available# ls 000-default.conf default-ssl.conf www.algara.at.conf

Modifions le fichier de configuration www.algara.at.conf :

nano www.algara.at.conf

GNU nano 7.2

/etc/apache2/sites-available/www.algara.at.conf

ServerName www.algara.at ServerAdmin webmaster@localhost DocumentRoot /var/www/www.algara.at # Available loglevels: trace8, ..., trace1, debug, info, notice, warn, # error, crit, alert, emerg. # It is also possible to configure the loglevel for particular # modules, e.g. #LogLevel info ssl:warn ErrorLog \${APACHE\_LOG\_DIR}/error.log CustomLog \${APACHE\_LOG\_DIR}/access.log combined SSLEngine on SSLCertificateFile /etc/ssl/www.algara.at/www.algara.at.cer SSLCertificateKeyFile /etc/ssl/www.algara.at/www.algara.at.key # For most configuration files from conf-available/, which are # enabled or disabled at a global level, it is possible to # include a line for only one particular virtual host. For example the # following line enables the CGI configuration for this host only # after it has been globally disabled with "a2disconf". #Include conf-available/serve-cgi-bin.conf /VirtualHost>

<b>PROCEDURE : SE</b>	<b>RVEUR WEB HTTPS</b>
-----------------------	------------------------

Créons le dossier /var/www/www.algara.at/ :

mkdir /var/www/www.algara.at

Créons le fichier du code de notre site web :

nano /var/www/www.algara.at/index.html

GNU nano 7.2 <body>

/var/www/www.algara.at/index.html

<h1>Bonjour bienvenu sur mon site</h1>

</body>

# Création d'un certificat ssl

Passons à la création du certificat.

Créons le dossier ou sera stocké notre clé ssl, notre demande de certificat et notre certificat mkdir /etc/ssl/intra.rouliere.eni :

mkdir /etc/ssl/www.algara.at

Déplaçons-nous dans ce dossier et créons notre clé :

cd /etc/ssl/www.algara.at

openssl genrsa -out www.algara.at.key 2048

root@srv-web:/etc/apache2/sites-available# mkdir /etc/ssl/www.algara.at root@srv-web:/etc/apache2/sites-available# cd /etc/ssl/www.algara.at root@srv-web:/etc/ssl/www.algara.at# openssl genrsa -out www.algara.at.key 2048 root@srv-web:/etc/ssl/www.algara.at# ls www.algara.at.key root@srv-web:/etc/ssl/www.algara.at# cat www.algara.at.key -----BEGIN PRIVATE KEY-----MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBKkwggSlAgEAAoIBAQDY4ryMC/BLi/je yko3nQ1zl0DsSrwBs+Y/Cr3XRI/jBHGKvGjFsDLLQWa9qX0GhQiXCNCblqQSGTlv eZ3Cyn8K5eysnEdQ115TIcnQz9o3Rf1KUPZ4p/2/75jAPVPFNSCAk/hkeH7EPjQy

Créons le fichier de configuration permettant de créer la demande de certificat :

nano /etc/ssl/www.algara.at/fic.txt



Page 5 sur 8

Créons notre demande de certificat :

openssl req -new -key www.algara.at.key -out www.algara.at.pem -config fic.txt

root@srv-web:/etc/ssl/www.algara.at# ls
fic.txt www.algara.at.key www.algara.at.pem
root@srv-web:/etc/ssl/www.algara.at# cat www.algara.at.pem
----BEGIN CERTIFICATE REQUEST---MIICzzCCAbcCAQAwRzELMAkGA1UEBhMCRl1xDzANBgNVBAcMBkFuZ2VyczEPMA0G
A1UECgwGYWxnYXJhMRYwFAYDVQQDDA13d3cuYWxnYXJhLmF0MIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA20K8jAvwS4v43spKN50Nc5dA7Eq8AbPmPwq9
10SP4wRxirxoxbAyy0FmvalzhoUIlwjQm5akEhk5b3mdwsp/CuXsrJxHUNdeUyHJ

Il faut maintenant copier notre demande de certificat et la coller dans notre serveur PKI :

Services de certificats Microsoft Active Directory -- algara-SRV-DC1-CA

### Soumettre une demande de certificat ou de renouvellement

Afin de soumettre une demande enregistrée à l'autorité de certifi renouvellement PKCS #7 générée par une source externe (telle

#### Demande enregistrée :

Base-64-encoded Requête de certificat (CMC ou PKCS #10 ou PKCS #7):

BEGIN CERTIFICATE REQUEST
MIICzzCCAbcCAQAwRzELMAkGA1UEBhMCR1IxDzANI
A1UECgwGYWxnYXJhMRYwFAYDVQQDDA13d3cuYWxn
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA20K8jAvwS4v4
10SP4wRxirxoxbAyy0FmvalzhoUIlwjQm5akEhk5l

#### Modèle de certificat :

Serveur Web 🗸

#### Attributs supplémentaires :

Attributs :

Envoyer >

Télécharger le certificat :

Services de certificats *Microsoft* Active Directory -- algara-SRV-DC1-CA

Certificat émis

Le certificat que vous avez demandé a été émis.

○ Codé DER ou 
 ● Codé en base 64

 <u>Télécharger le certificat</u>
 <u>Télécharger la chaîne de certificats</u>

L'envoyer sur le serveur web via scp :

scp .\www.algara.at.cer thomas@srv-web:/tmp

C:\Users\administrateur\Downloads>scp .\www.algara.at.cer thomas@srv-web:/tmp thomas@srv-web's password: www.algara.at.cer 100% 1652 1.6KB/s 00:00

Sur le serveur web, le mettre dans le bon dossier :

mv /tmp/www.algara.at.cer /etc/ssl/www.algara.at/www.algara.at.cer

Activons le module ssl de apache :

a2enmod ssl

Vérifions notre configuration :

apachectl configtest

root@srv-web:/etc/ssl/www.algara.at# apachectl configtest
Syntax OK

Enfin publions notre site :

a2ensite www.algara.at.conf

Sur un client téléchargeons puis installons le certificat :

Services de certificats Active Dire						
C Non sécurisé   srv-dc1/certsrv/certcarc.asp		A	☆	() (	<u>}</u> €	9
ervices de certificats <i>Microsoft</i> Active Directory algara-SRV-DC1-CA		Téléchargement	s	Đ	ς.	
lécharger un certificat d'autorité de certification, une chaîne de c	certificats ou la liste de révocation d	certnew.cer			٢	7
our approuver les certificats approuvés par l'autorité de certification, In	nstaller ce certificat d'autorité de certific	Ouvrir un fichier			-	_
our sélectionner un certificat d'autorité de certification, une chaîne de c	certificats ou une liste de révocation de	Afficher plus				
artificat de l'autorité de certification :						
Actuel [algara-SRV-DC1-CA]						
éthode de codage :						
◎ DER ○ Base 64						
nstaller un certificat d'autorité de certification						
nstaller un certificat d'autorité de certification élécharger un certificat de l'autorité de certification						
staller un certificat d'autorité de certification élécharger un certificat de l'autorité de certification						
staller un certificat d'autorité de certification	Certificat	×				
staller un certificat d'autorité de certification	Certificat     Général Détails Chemin d'accès de certification	×				
Staller un certificat d'autorité de certification élécharger un certificat de l'autorité de certification ichier ouvert - Avertissement de sécurité × Voulez-vous ouvrir ce fichier ?	Certificat Général Détais Chemin d'accès de certification	×				
staller un certificat d'autorité de certification ilécharger un certificat de l'autorité de certification chier ouvert - Avertissement de sécurité × Voulez-vous ouvrir ce fichier ? Nom : C\Users\administrateur\Downloads\certnew.cer	Certificat Général Détais Chemin d'accès de certification	×				
staller un certificat d'autorité de certification         lécharger un certificat de l'autorité de certification         chier ouvert - Avertissement de sécurité         Voulez-vous ouvrir ce fichier ?         Nom: C\Users\administrateur\Downloads\certnew.cer         Éditeur : Éditeur inconnu	Certificat Général Detais Chemin d'accès de certification Informations sur le certificat Ce certificat est conço pour les rôles suivants Totales les atralignes d'insponse. Totales les atralignes d'application	×				
staller un certificat d'autorité de certification         lécharger un certificat de l'autorité de certification         chier ouvert - Avertissement de sécurité         Voulez-vous ouvrir ce fichier ?         Nom: C\Users\administrateur\Downloads\certnew.cer         Éditeur : Éditeur inconnu         Type : Certificat de sécurité	Certificat Général Détais Chemin d'accès de certification Informations sur le certificat Ce certificat est conçu pour les rôles suivants - Toutes les stratégies d'emsoins - Toutes les stratégies d'emsoins	×				
staller un certificat d'autorité de certification         lécharger un certificat de l'autorité de certification         chier ouvert - Avertissement de sécurité       ×         Voulez-vous ouvrir ce fichier ?         Image: Source construction         Éditeur : Éditeur inconnu         Type : Certificat de sécurité         De : C:\Users\administrateur\Downloads\certnew.cer	Certificat Grinfral Detais Chemin d'accès de certification Informations sur le certificat Ce certificat est conçu pour les rôles suivants • Toutes les stratégies d'application	*				
staller un certificat d'autorité de certification slécharger un certificat de l'autorité de certification chier ouvert - Avertissement de sécurité × Voulez-vous ouvrir ce fichier ? Nom : C\Users\administrateur\Downloads\certnew.cer Éditeur : Éditeur inconnu Type : Certificat de sécurité De : C\Users\administrateur\Downloads\certnew.cer	Certificat Grinfral Detais Chemin d'accès de certification Certificat est conçu pour les rôles suivants Toutes les stratégies d'emisions Toutes les stratégies d'emisions Toutes les stratégies d'emisions Délivré à: algare-SRY-OC1-CA	*				
staller un certificat d'autorité de certification sidécharger un certificat de l'autorité de certification x Voulez-vous ouvrir ce fichier ? Nom: C:\Users\administrateur\Downloads\certnew.cer Éditeur : Éditeur inconnu Type: Certificat de sécurité De: C:\Users\administrateur\Downloads\certnew.cer Ouvrir Annuler	Certificat  Grinfral Detais Chemin d'accès de certification  Ce certificat est conçu pour les rôles suivants  Toutes les stratégies d'imasions  Toutes les stratégies d'application  Délivré à: algare-SRV-DC1-CA  Délivré par algare-SRV-DC1-CA	×				
staller un certificat d'autorité de certification blécharger un certificat de l'autorité de certification x Voulez-vous ouvrir ce fichier ? Nom: C\Users\administrateur\Downloads\certnew.cer Éditeur : Éditeur inconnu Type: Certificat de sécurité De: C\Users\administrateur\Downloads\certnew.cer Vourir Annuler vourir Couvrir Center	Certificat  Général Détais Ohemin d'accès de certification  Figure 1 Toutes les stratégies d'application  Toutes les stratégies d'application  Délivré à : algara-SRV-0C1-CA  Délivré par algara-SRV-0C1-CA  Valide du 28/02/2025 au 28/02/2035	×				
staller un certificat d'autorité de certification         élécharger un certificat de l'autorité de certification         richier ouvert - Avertissement de sécurité       ×         Voulez-vous ouvrir ce fichier ?       ×         Image: Staller un certificat de sécurité       ×         Image: Staller un certificat de sécurité       ×         Image: Certificat de s	Certificat Général Detais Chemin d'accès de certification Certificat et conçu pour les rôles suivants Cercertificat et conçu pour les rôles suivants Toutes les stratégies d'application Délivré à : algara-SRV-OC1-CA Délivré par algara-SRV-OC1-CA Valide du 28/02/2025 au 28/02/2035	×				
staller un certificat d'autorité de certification élécharger un certificat de l'autorité de certification Fichier ouvert - Avertissement de sécurité Voulez-vous ouvrir ce fichier ? Nom : C\Users\administrateur\Downloads\certnew.cer Éditeur : Éditeur inconnu Type : Certificat de sécurité De : C\Users\administrateur\Downloads\certnew.cer Cuvrir Annuler Toujours demander avant d'ouvrir ce fichier Les fichiers téléchargés depuis Internet peuvent être utiles, mais ce type de fichier présente un danger potentiel. N'exécutez ou n'enregistrez ce programme que si vous êtes sûr de son origine. Queixes 2	Certificat Général Détais chemin d'accès de certification Certificat est concu pour les rôles suivants Certificat est concu pour les rôles suivants - Toutes les stratégies d'application Délivré à : algara-SRV-OC1-CA Délivré à : algara-SRV-OC1-CA Délivré à : algara-SRV-OC1-CA Valide du 28/02/2025 au 28/02/2035	×				

Une fois les enregistrement DNS effectués, testons notre site :



Notre site est bien certifié, et notre connexion est bien sécurisée.