

Services Web (HTTP/HTTPS)

SAGALEYNI AIDARA ET IBRAHIMA
DIALLO



Introduction aux Services Web

COMPRENDRE HTTP ET HTTPS POUR L'AVENIR

Dans ce module, nous explorerons les services web, notamment le fonctionnement d'**HTTP** et la sécurisation avec **HTTPS**, essentiels dans le paysage numérique moderne et la cybersécurité.



Fonctionnement du protocole HTTP

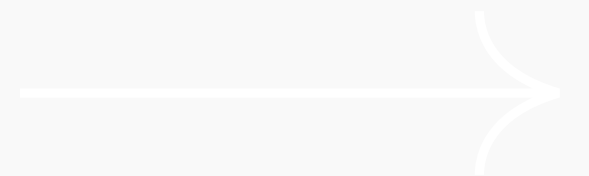
COMPRENDRE LE MODÈLE CLIENT/SERVEUR

HTTP

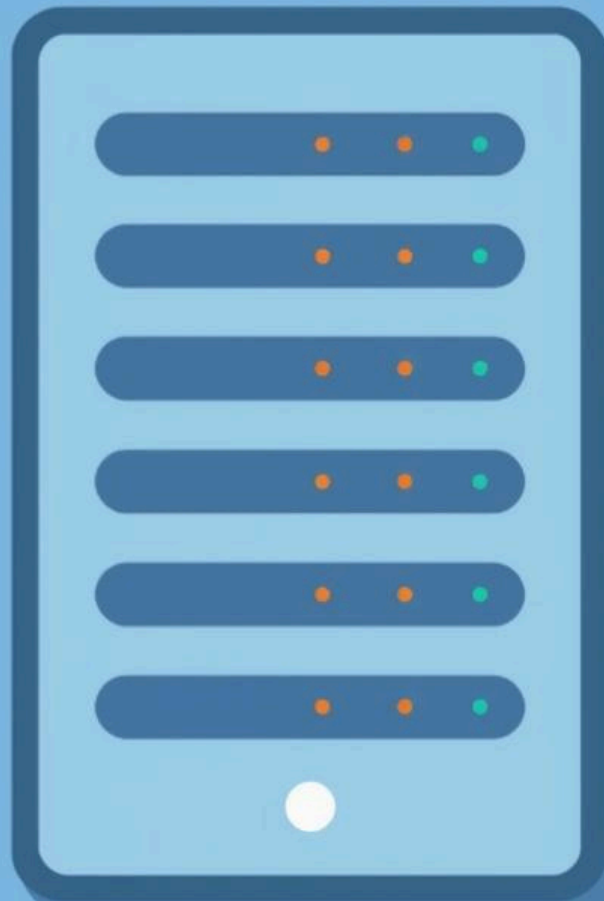
HTTP, ou **HyperText Transfer Protocol**, est le protocole essentiel qui permet la communication entre un navigateur web et un serveur, facilitant ainsi l'accès aux contenus en ligne.

Client/Serveur

Dans le modèle **client/serveur**, le client envoie une requête HTTP, et le serveur répond avec les données demandées, permettant une interaction fluide et efficace sur le web.



Serveurs Web



Les serveurs web, tels qu'**Apache HTTP Server** et **Nginx**, jouent un rôle crucial dans l'hébergement de sites internet. Apache est renommé pour sa simplicité, tandis que Nginx est apprécié pour ses performances. Choisir le bon serveur est essentiel pour une gestion efficace des requêtes.

Les certificats SSL / TLS

CHIFFREMENT ET CONFIDENTIALITÉ DES DONNÉES

Chiffrement des données

Le chiffrement assure que les données transmises entre le client et le serveur sont **protégées**, rendant difficile pour les attaquants d'accéder à des informations sensibles, comme les mots de passe.

Confidentialité

Grâce à SSL/TLS, les échanges deviennent privés et **sécurisés**, garantissant que seules les parties autorisées peuvent accéder aux informations, renforçant ainsi la **confiance** des utilisateurs envers les services en ligne.

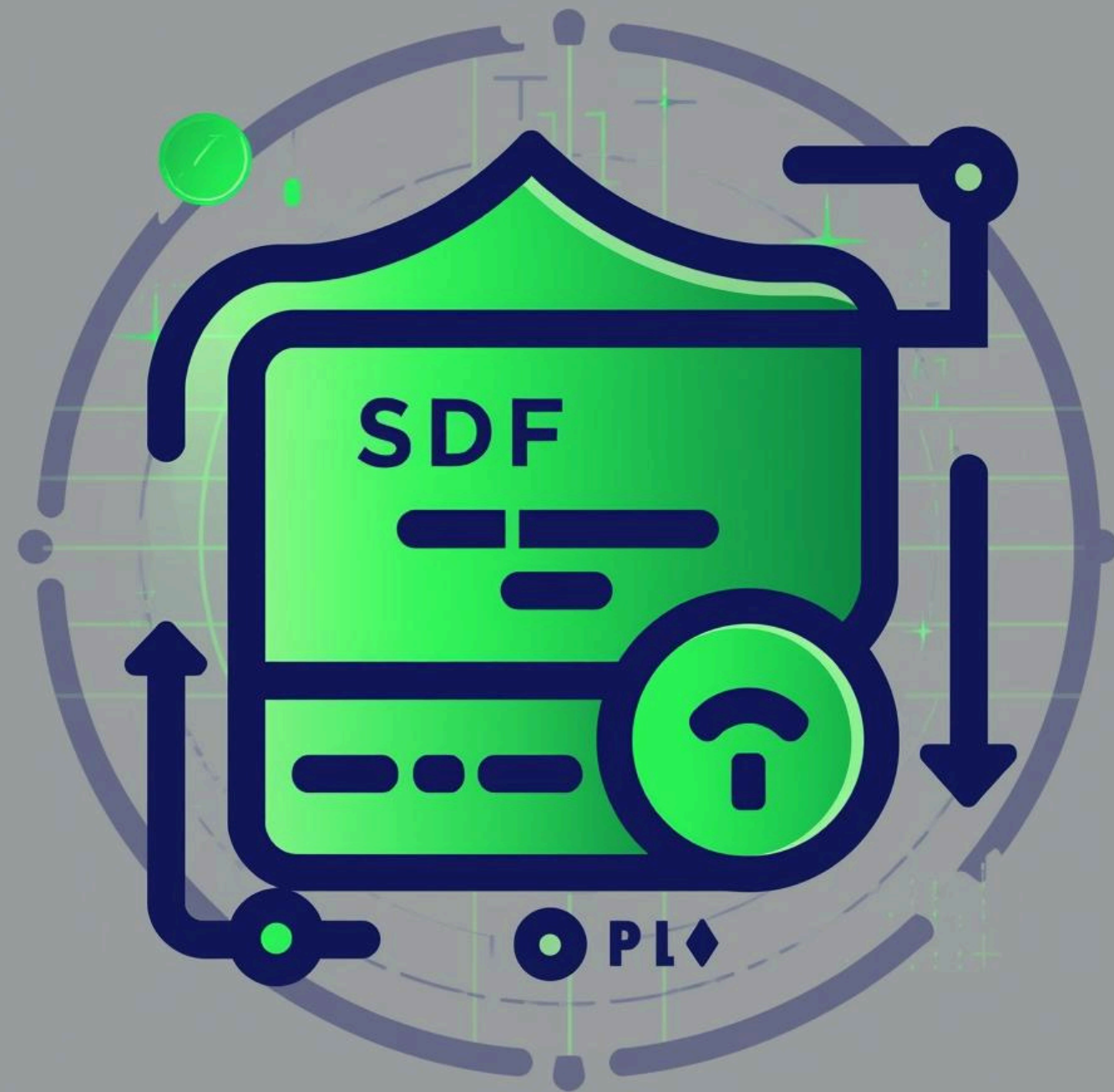


Autorité de certification



Les autorités de certification (CA) jouent un rôle crucial dans la sécurité web. Elles délivrent des certificats SSL/TLS, garantissant la **confiance** entre le client et le serveur. Ces certificats assurent que les échanges de données sont sécurisés et intègres, renforçant ainsi la cybersécurité.

Let's Encrypt



Let's Encrypt est une **autorité de certification gratuite** qui fournit des certificats SSL valables 90 jours. Avec un renouvellement automatique, elle joue un rôle crucial dans la démocratisation de la sécurité HTTPS, permettant aux utilisateurs de sécuriser facilement leurs sites web sans frais.

Certbot

AUTOMATISATION

01 Installation

Pour installer ces certificats, on utilise un outil appelé :
Certbot

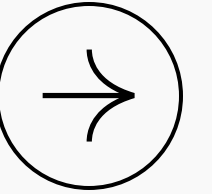
Certbot permet d'automatiser :
la génération du certificat la configuration HTTPS le
renouvellement automatique.

02 Configuration

Certbot facilite la configuration d'HTTPS, rendant le
processus d'obtention et de renouvellement de certificat
rapide et simple.



HTTPS Sécurisé



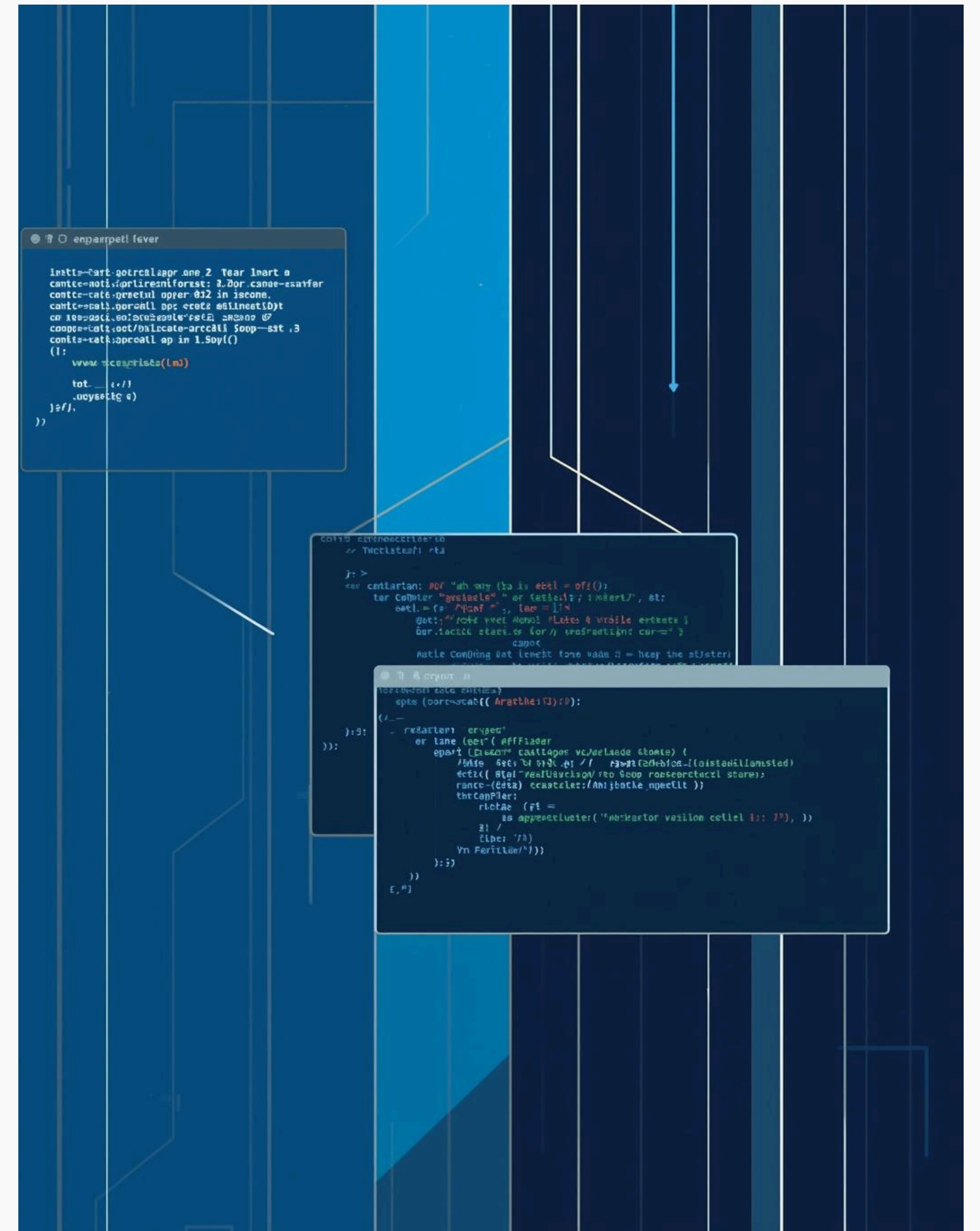
Protection des données avec SSL/TLS



Introduction au déploiement

Installation d'un serveur web sécurisé

L'objectif de cette partie est de **mettre en place** un serveur web sécurisé en utilisant Apache 2 sur un système Ubuntu. Cela garantira la protection des données échangées en ligne.

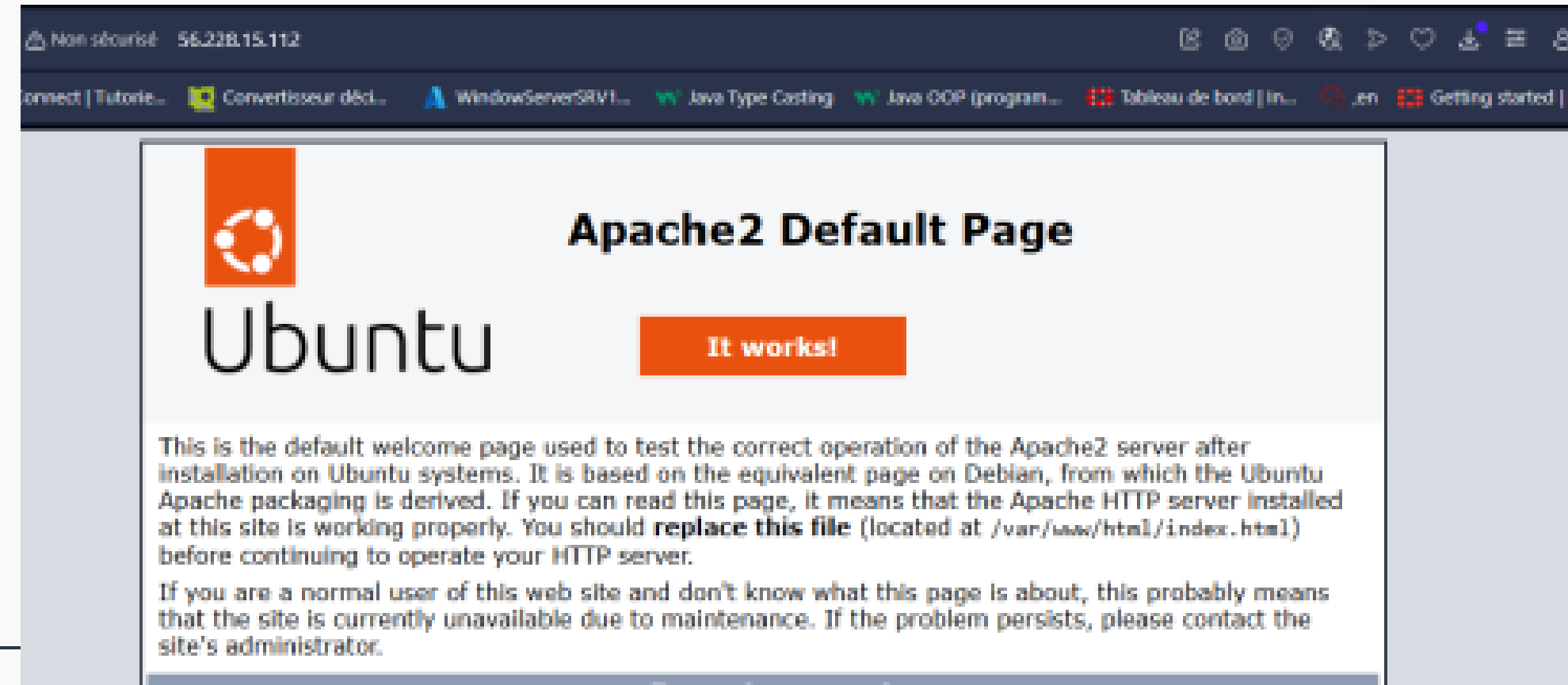


Vérification

TESTER

01 HTTP

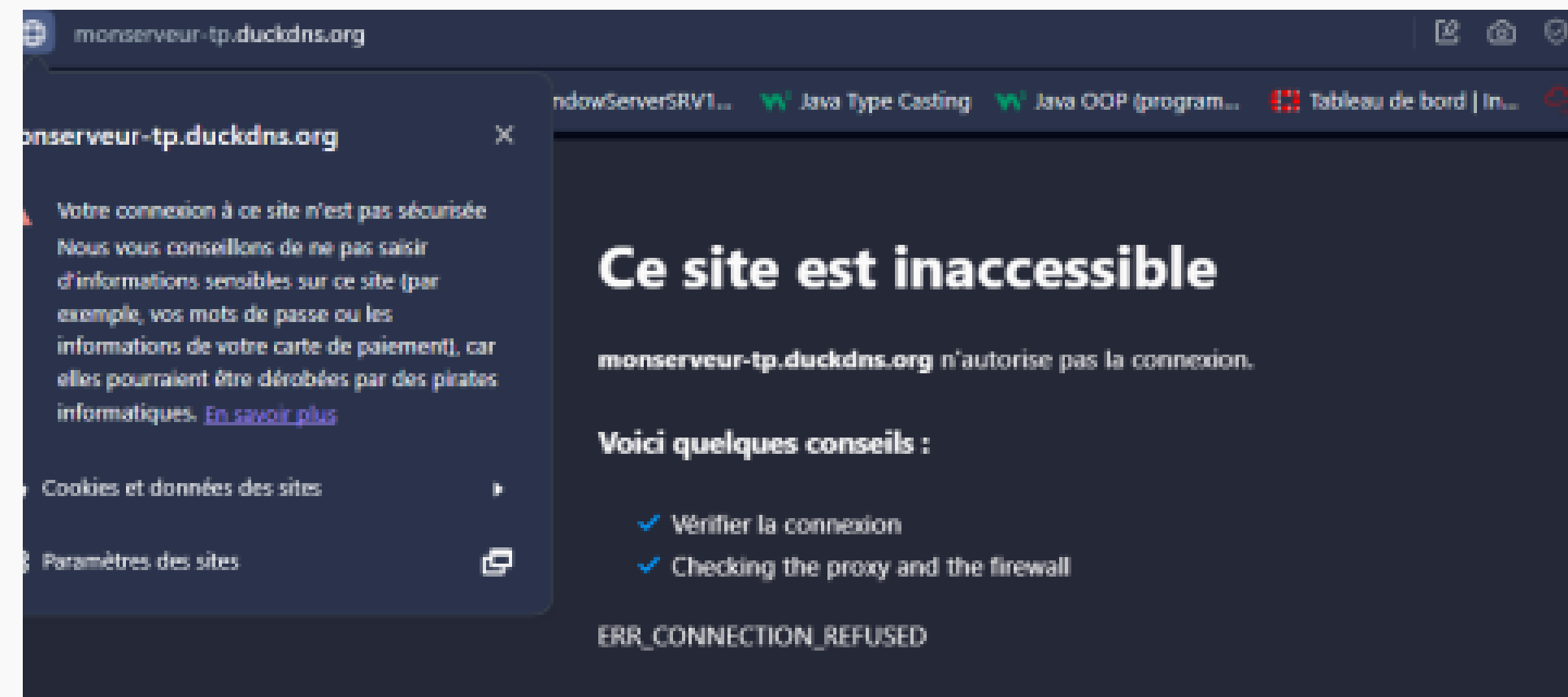
Pour vérifier le site, ouvrez un navigateur et entrez l'**IP publique de la VM** pour accéder à la page.



02 HTTPS

L'URL doit être **https://monserveur-tp.duckdns.org**, mais le certificat doit encore être ajouté pour sécuriser la connexion.

NB: Si on tape https://monserveur-tp.duckdns.org ca ne marche pas puis qu'on a pas encore ajouter le certificat



Configuration

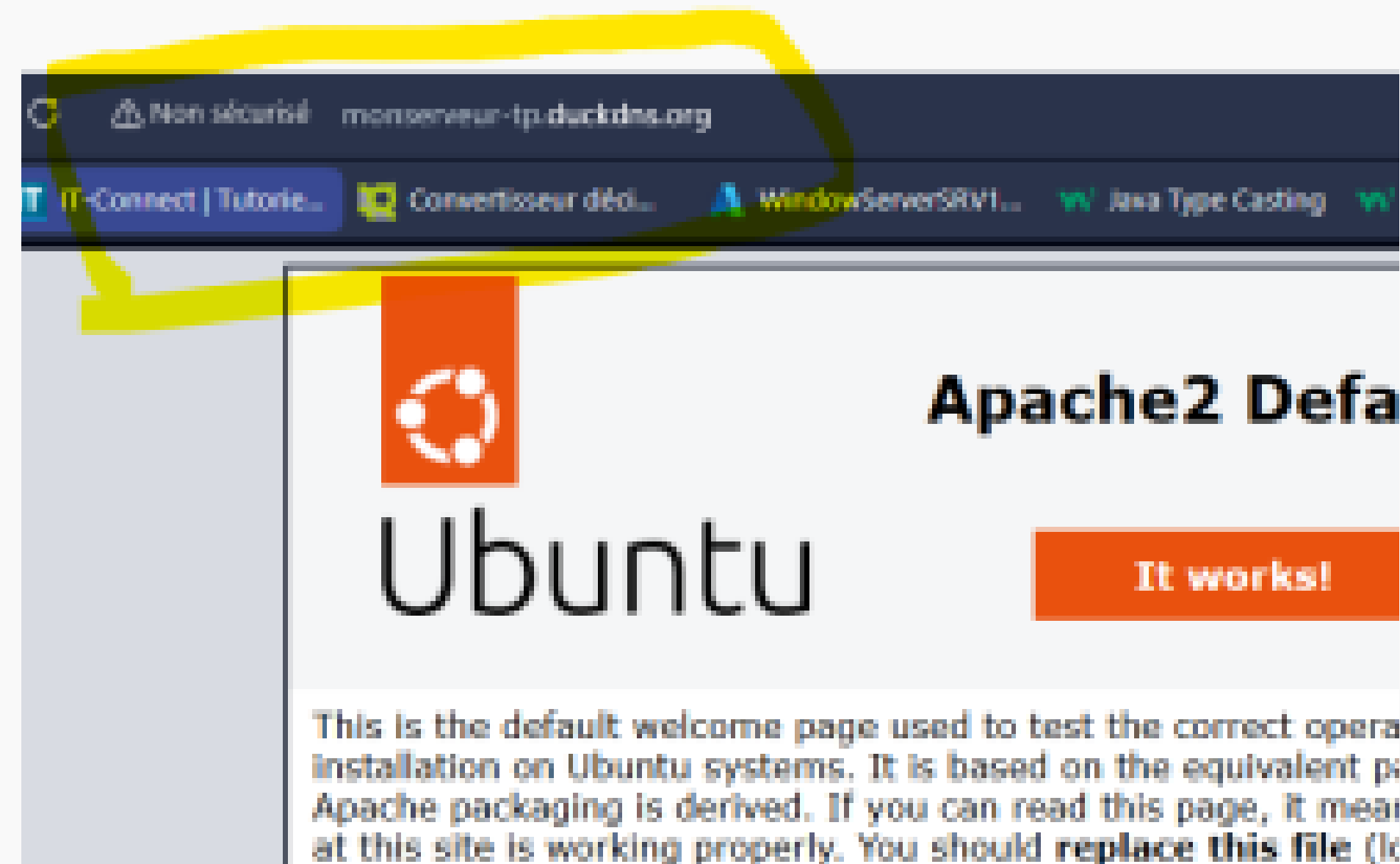
SOUS-DOMAIN

01 Sous-domaine IP

Avoir un sous-domaine gratuit pointant vers la VM AWS qui héberge Apache, pour pouvoir tester HTTP/HTTPS.

Création du sous-domaine :

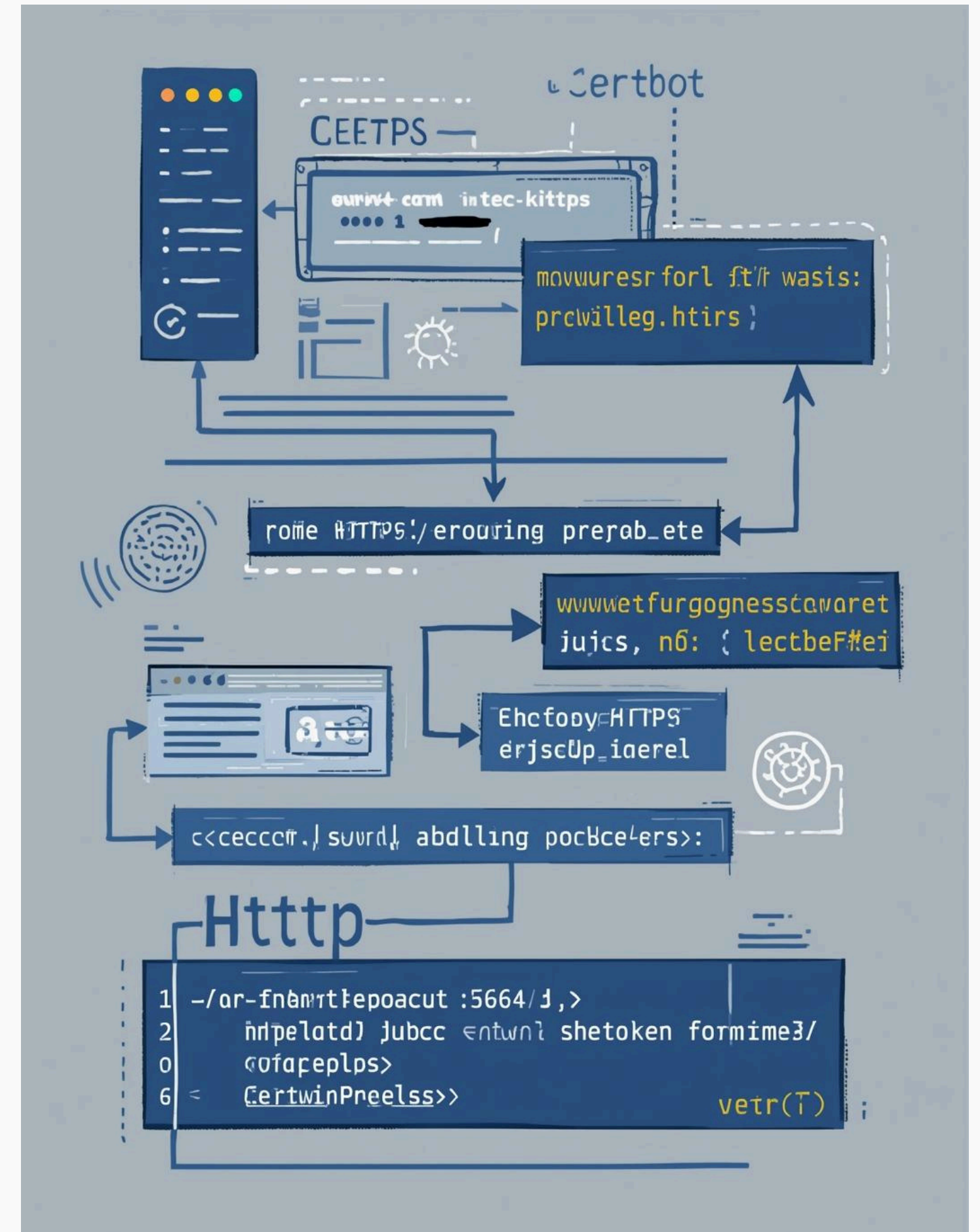
IP: 56.228.15.112 → NomDomain: monserveur-tp.duckdns.org



Configuration HTTPS

Automatisation avec Certbot pour sécurité

La configuration du protocole HTTPS est simplifiée grâce à Certbot, qui permet d'automatiser l'obtention et le déploiement des certificats SSL/TLS pour un serveur sécurisé.



Installer Certbot

Configuration de Certbot sur Apache

Pour sécuriser notre serveur, nous devons **installer Certbot** et le plugin Apache. Certbot nous aidera à automatiser la gestion des certificats SSL/TLS pour HTTPS.

```
amd64-172-31-20-111:~$ sudo apt install certbot python3-certbot-apache -y
amd64-172-31-20-111:~$ sudo apt install certbot python3-certbot-apache -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-lensmod libaugeas0 python3-acme python3-augeas python3-certbot python3-configargparse python3-icu python3-josepy python3-parsedata
  python3-requests-toolbelt python3-rfc3339 python3-rope.component python3-rope.event python3-rope.hookable
Suggested packages:
  apache2-doc python-certbot-doc python3-certbot-nginx apache2-tools python-acme-doc python-certbot-apache-doc
The following NEW packages will be installed:
  apache2-lensmod certbot libaugeas0 python3-acme python3-augeas python3-certbot python3-certbot-apache python3-configargparse python3-icu
  python3-parsedatetimes python3-requests-toolbelt python3-rfc3339 python3-rope.component python3-rope.event python3-rope.hookable
0 upgraded, 16 newly installed, 0 to remove and 0 not upgraded.
Need to get 1552 kB of archives.
After this operation, 7681 kB of additional disk space will be used.
Get:1 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 apache2-lensmod all 1.13.0-1 [321 kB]
Get:2 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 libaugeas0 amd64 1.13.0-1 [100 kB]
Get:3 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 python3-josepy all 1.10.0-1 [22.0 kB]
Get:4 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 python3-requests-toolbelt all 0.9.1-1 [30.0 kB]
Get:5 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 python3-rfc3339 all 1.1-3 [7110 B]
Get:6 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 python3-acme all 1.21.0-1ubuntu0.1 [16.4 kB]
Get:7 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 python3-augeas all 0.5.0-1.1 [9124 B]
Get:8 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 python3-configargparse all 1.5.3-1 [24.9 kB]
Get:9 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 python3-parsedatetimes all 2.4-2 [12.9 kB]
Get:10 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 python3-rope.hookable amd64 0.1.0-1build1 [11.6 kB]
```


Obtention du certificat

Processus d'installation de Let's Encrypt

Pour sécuriser notre site, nous devons obtenir un certificat Let's Encrypt, ce qui garantit le chiffrement des données et l'authentification du serveur, améliorant ainsi la sécurité globale.

```
Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/monserveur-tp.duckdns.org/
Certificate is saved at: /etc/letsencrypt/live/monserveur-tp.duckdns.org/
Certificate expires on 2026-05-25.
The file will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate

Deploying certificate
Successfully deployed certificate for monserveur-tp.duckdns.org to /etc/
Congratulations! You have successfully enabled HTTPS on https://monserveur-tp.duckdns.org

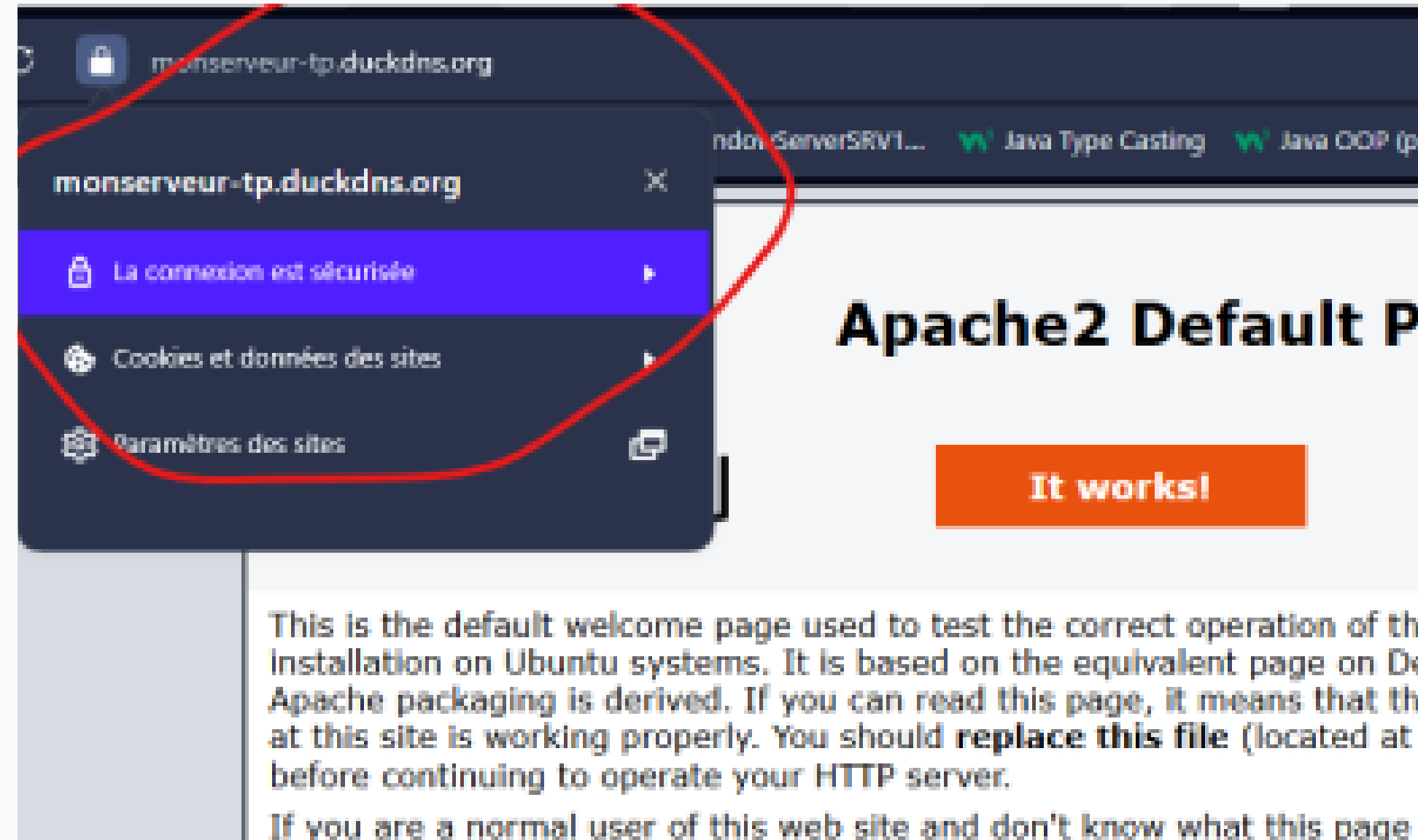
-----
If you like Certbot, please consider supporting our work by:
Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
Donating to EFF: https://eff.org/donate-le

-----
root@kali:~# ssh root@172.31.20.111:~#
```

Test de sécurisation

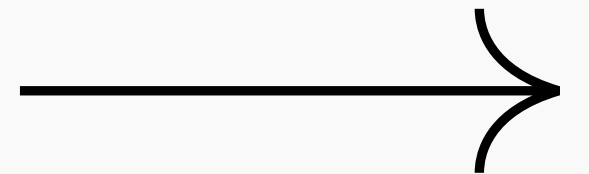
Validation de la connexion HTTPS

Après vérification, nous constatons que le site est maintenant **sécurisé** grâce à la présence d'un cadenas dans la barre d'adresse, garantissant ainsi la **protection des données** échangées.



En conclusion, nous avons vu que :

- HTTP permet la communication web mais n'est pas sécurisé.
- HTTPS ajoute une couche de chiffrement grâce aux certificats SSL/TLS.
- Apache et Nginx permettent d'héberger un site.
- Let's Encrypt facilite la sécurisation gratuitement.



Merci
beaucoup
pour votre
attention

COPIER LE LIEN SUIVANT
POUR LE GUIDE TOTAL DU
PROJET

<https://github.com/Diallo273/Services-Web-HTTP-HTTPS-.git>