REPUBLIQUE DU SENEGAL

Un people – Un but – Une foi

UNIVERSITE ALIOUNE DIOP DE BAMBEY

UFR : Sciences Appliquées et Technologie de L'Information et de la Communication (SATIC)

DEPARTEMENT : Technologie de l'Information et de la Communication (TIC)

FILIERE : Systèmes Réseaux et Télécommunications (SRT)

NIVEAU : Licence 3

TP3 SECURITE: CRYPTOGRAPHIE ET CHIFFREMENT

2023 - 2024

Presente par:

Mamadou Thiam

Encadre par:

Mr. Diouf

Table des matières

PRESENTATIOTN D'OPENSSL

Introduction :

OpenSSL est une boite à outils cryptographiques (la plus répandue). Elle est open source avec licence GPL et téléchargeable sur http://www.openssl.org. Elle implémente les protocoles SSL (Secure Socket Layer) et TLS (Transport Layer Security) pour permettre aux applications client/serveur de communiquer de façon sécurisée.

Une session SSL se déroule en deux temps : • une phase de poignée de mains (handshake) durant laquelle le client et le serveur s'identifient, conviennent du système de chiffrement et d'une clé qu'ils utiliseront par la suite ; la phase de communication proprement dite durant laquelle les données échangées sont compressées, chiffrées et signées. Pour connaître toutes les fonctionnalités de openSSL utiliser : man openssl.

La syntaxe générale de la commande openssl est :

```
> openssl commande options
```

PREMIERE PARTIE :

1. CHIFFFREMENT SYMETRIQUE

Dans cette partie nous allons demontrer comment chiffrer et dechiffrer des informations grace au chiffrement Symetrique.Tout dabord c'est quoi le terme symetrique ? En quoi consiste t_il ?

Le prinicipe c'est d'avoir une cle, qui, simulatement va nous servir de chiffrer ou de dechiffrer le contenu d'un message.

Avant tout on va dabord créer un fichier message, qui va contenir les informations que l'on souhaite proteger.

[CAPTURE]

Ensuite, on utilisera l'algorithme de chiffrement AES de taille 128 bits et de type cbc :

Synthaxe pour chiffrement symetrique

```
┌──(mamadou㉿kali)-[~/TPCrypto]
└─$ openssl enc -aes-128-cbc -e -in message -out messageChiffre
enter AES-128-CBC encryption password:
Verifying - enter AES-128-CBC encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
```

Synthaxe pour dechiffrement symetrique

```
┌──(mamadou㉿kali)-[~/TPCrypto]
└─$ openssl enc -aes-128-cbc -d -in messageChiffre -out messageDechiffre
enter AES-128-CBC decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
```

2. CHIFFREMENT ASYMETRIQUE: exemple RSA

Le principe du chiffrement asymetrique c'est d'avoir une paire de cles(privee/publique), liees mathematiquement.

La cle publique sera utilise pour chiffrer le message , la cle privee va elle nous servir a dechiffrer ce message.

Exemple : Voici les etapes illustrant le chiffrement asymetrique.

Generation d'une paire de cles RSA

```
┌──(mamadou㉿kali)-[~/TPCrypto]
└─$ openssl genrsa -out maCle.pem 2048

┌──(mamadou㉿kali)-[~/TPCrypto]
└─$ ls
maCle.pem  message  messageChiffre  messageDechiffre
```

Exploration de la partie publique

```
┌──(mamadou㉿kali)-[~/TPCrypto]
└─$ openssl rsa -in maCle.pem -out maClePublique.pem -pubout
writing RSA key

┌──(mamadou㉿kali)-[~/TPCrypto]
└─$ ls
maCle.pem          message         messageDechiffre
maClePublique.pem  messageChiffre  personel
```

Visualisation des cles RSA

contenue de la cle privee :

```
┌──(mamadou㉿kali)-[~/TPCrypto]
└─$ openssl rsa -in maCle.pem -text -noout
Private-Key: (2048 bit, 2 primes)
modulus:
    00:a2:e3:e4:e0:98:43:84:7b:87:cc:4b:a7:98:b7:
    1c:00:35:a3:67:25:8e:e5:e3:16:ca:43:d1:e3:bd:
    12:93:7e:ff:69:8f:7e:13:bf:da:de:2a:5f:6b:26:
    32:aa:3b:bf:c8:5a:ac:7e:1f:b0:a5:74:d1:ed:fe:
    ed:11:8e:e6:6f:59:6c:d8:01:c3:90:95:a7:33:f0:
    de:77:32:ba:c2:d6:f6:03:55:db:01:0f:20:c6:3a:
    99:63:2a:72:2c:b4:14:29:92:c0:69:db:54:c5:a2:
    f5:f1:82:85:cb:46:31:95:1b:9f:13:f6:6d:ec:3b:
    f3:ce:84:62:5d:e6:84:43:8e:2f:20:04:23:56:bb:
    a7:fa:04:43:7a:be:68:55:12:76:f3:2c:71:d9:ec:
    7c:c4:60:f9:78:12:b2:f2:69:30:2a:e8:a3:7b:47:
    3e:45:cd:d6:d2:d1:5a:72:3f:32:ff:83:43:71:65:
    39:f6:35:1d:54:37:50:2b:92:f2:6c:fb:be:a2:43:
```

Contenue de la cle publique :

```
┌──(mamadou㉿kali)-[~/TPCrypto]
└─$ openssl rsa -in maClePublique.pem -text -noout -pubin
Public-Key: (2048 bit)
Modulus:
    00:a2:e3:e4:e0:98:43:84:7b:87:cc:4b:a7:98:b7:
    1c:00:35:a3:67:25:8e:e5:e3:16:ca:43:d1:e3:bd:
    12:93:7e:ff:69:8f:7e:13:bf:da:de:2a:5f:6b:26:
    32:aa:3b:bf:c8:5a:ac:7e:1f:b0:a5:74:d1:ed:fe:
    ed:11:8e:e6:6f:59:6c:d8:01:c3:90:95:a7:33:f0:
    de:77:32:ba:c2:d6:f6:03:55:db:01:0f:20:c6:3a:
    99:63:2a:72:2c:b4:14:29:92:c0:69:db:54:c5:a2:
    f5:f1:82:85:cb:46:31:95:1b:9f:13:f6:6d:ec:3b:
    f3:ce:84:62:5d:e6:84:43:8e:2f:20:04:23:56:bb:
    a7:fa:04:43:7a:be:68:55:12:76:f3:2c:71:d9:ec:
    7c:c4:60:f9:78:12:b2:f2:69:30:2a:e8:a3:7b:47:
    3e:45:cd:d6:d2:d1:5a:72:3f:32:ff:83:43:71:65:
    39:f6:35:1d:54:37:50:2b:92:f2:6c:fb:be:a2:43:
    69:33:66:3b:6c:bd:6e:34:3f:40:2c:9c:43:bb:b0:
    a0:f1:69:0a:a7:ee:dd:6d:ad:c0:22:cb:19:37:88:
    43:3f:1c:26:c8:42:af:17:2e:78:67:e0:f2:12:ac:
    2f:13:25:b4:ac:d8:29:3c:78:a6:a0:69:28:c0:d4:
    b9:a5
Exponent: 65537 (0x10001)
```

Chiffrement/Dechiffrement de donnees par RSA :

Chiffrement :

```
┌──(mamadou㉿kali)-[~/TPCrypto]
└─$ openssl pkeyutl -encrypt -in message -inkey maClePublique.pem -out messag
eChiffre_rsa -pubin

┌──(mamadou㉿kali)-[~/TPCrypto]
```

Dechiffrement :

```
┌──(mamadou㉿kali)-[~/TPCrypto]
└─$ openssl pkeyutl -decrypt -in messageChiffre_rsa -inkey maCle.pem -out mes
sageDechiffre_rsa

┌──(mamadou㉿kali)-[~/TPCrypto]
```

3. HACHAGE ET SIGNATURE NUMERIQUE DE FICHIERS

Dans un premier temps on va faire le hachage, la signature et la verification de manière separee :

Hachage : creation d'empreinte pour notre message « «secret »

```
┌──(mamadou㉿kali)-[~/TPCrypto]
└─$ openssl dgst -md5 -out secret_md5 secret

┌──(mamadou㉿kali)-[~/TPCrypto]
```

Signature : on va maintenant signer l'empreinte avec notre cle privee

```
┌──(mamadou㉿kali)-[~/TPCrypto]
└─$ openssl pkeyutl -sign -in secret_md5 -inkey maCle.pem -out secret_signed_
md5

┌──(mamadou㉿kali)-[~/TPCrypto]
```

Enfin on fait une verfication,

```
┌──(mamadou㉿kali)-[~/TPCrypto]
└─$ openssl pkeyutl -verify -in secret_md5 -inkey maClePublique.pem -sigfile
secret_signed_md5 -pubin
Signature Verified Successfully
```

la verfication semble reussi.

Dans cette etape : le hachage et la signature vont etre combinees

```
┌──(mamadou㉿kali)-[~/TPCrypto]
└─$ openssl dgst -md5 -sign maCle.pem -out signed1_md5 secret

┌──(mamadou㉿kali)-[~/TPCrypto]
└─$
```

Apres cela on procede a une verification

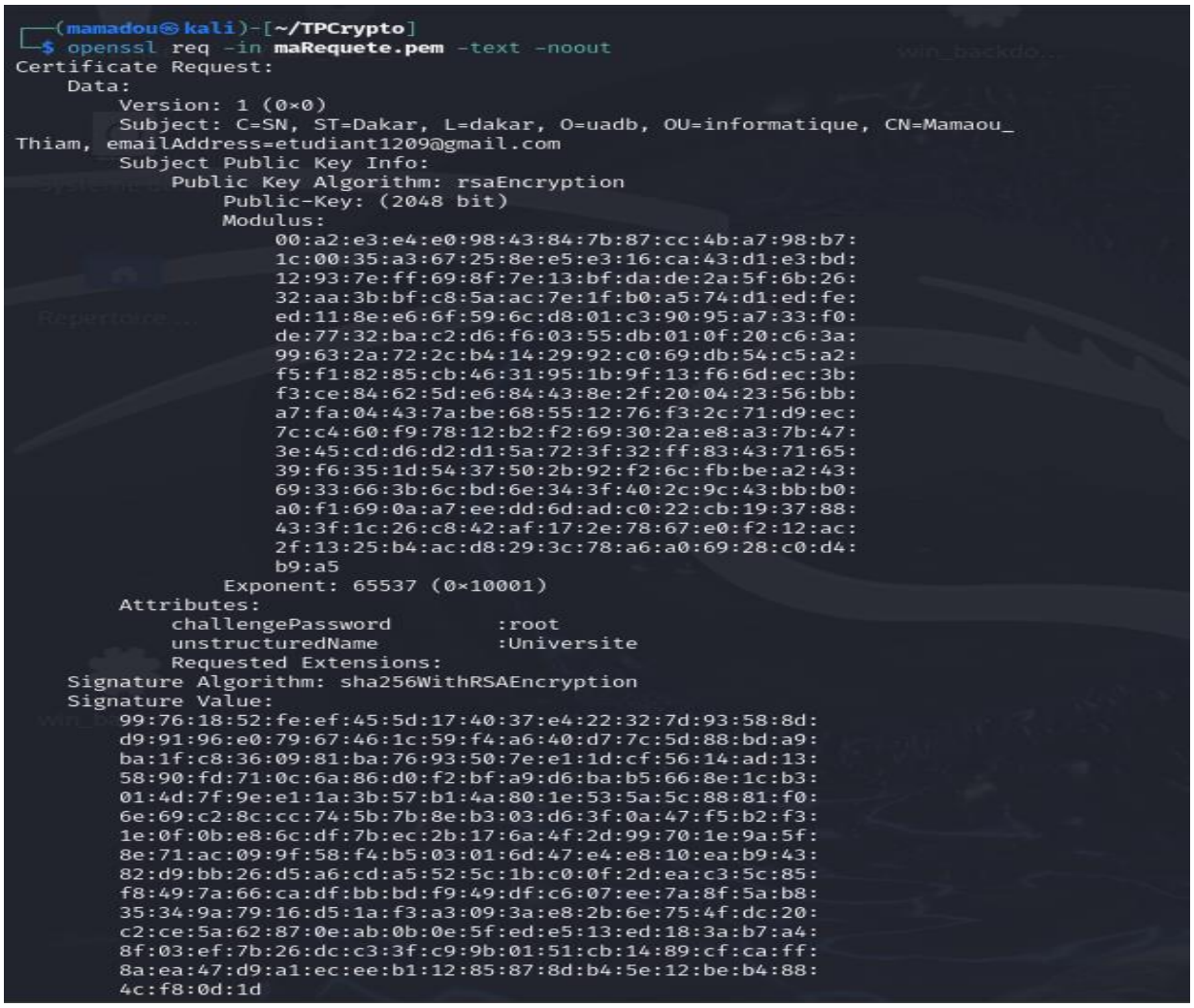
```
┌──(mamadou㉿kali)-[~/TPCrypto]
└─$ openssl dgst -md5 -verify maClePublique.pem -signature signed1_md5 secret

Verified OK

┌──(mamadou㉿kali)-[~/TPCrypto]
└─$
```

« OK » : la verification a reussi.

- CERTIFICATS NUMERIQUES :

Generation de la paire de cles RSA

Création d'une requête de certificats auprès de l'autorité d'enregistrement (RA) :



Auto-signer une requête (le demandeur devient CA) Demande de signature de certificat auprès de la CA

DEUXIEME PARTIE :

TRAVAIL A RENDRE :

- Sécurisation d'un serveur web Apache avec SSL (passer de http à https) :

Demaarons les configurations

```
mamadou@mamadou-VirtualBox:~$ 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:
Module socache_shmcb already enabled
Module ssl already enabled
mamadou@mamadou-VirtualBox:~$ a2ensite default-ssl
Site default-ssl already enabled
mamadou@mamadou-VirtualBox:~$ service apache2 reload
mamadou@mamadou-VirtualBox:~$
```

Nous allons créer notre premier certificat qui sera en http

```
mamadou@mamadou-VirtualBox:~$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048
 -sha256 -out /etc/apache2/server.crt -keyout /etc/apache2/server.key
Generating a RSA private key
.............+++++
............+++++
writing new private key to '/etc/apache2/server.key'
-----
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]:SN
State or Province Name (full name) [Some-State]:Dakar
Locality Name (eg, city) []:Hann_bel_aire
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UADB
Organizational Unit Name (eg, section) []:TIC
Common Name (e.g. server FQDN or YOUR name) []:Mamadou_Thiam
Email Address []:m38730081@gmail.com
```

Allons dans notre fichier de configuration https « default-ssl.conf »

```
mamadou@mamadou-VirtualBox:/etc/apache2/sites-available$ sudo nano /etc/apache2/sites-
available/default-ssl.conf
```

Mettons les bons chemins des fichiers certificats et cle privee

```
SSLCertificateFile    /etc/apache2/server.crt
SSLCertificateKeyFile /etc/apache2/server.key

#   Server Certificate Chain:
#   Point SSLCertificateChainFile at a file containing the
#   concatenation of PEM encoded CA certificates which form
#   certificate chain for the server certificate. Alternativ
#   the referenced file can be the same as SSLCertificateFil
#   when the CA certificates are directly appended to the se
#   certificate for convinience.
#SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt
```

Dans le fichier de configuration default-ssl.conf, ajoutons ce bout de text

```
                # BrowserMatch "MSIE [2-6]" \
                #               nokeepalive ssl-unclean-shutdown \
                #               downgrade-1.0 force-response-1.0

        </VirtualHost>
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet

SSLProtocol -ALL +TLSv1 +TLSv1.1 +TLSv1.2
SSLHonorCipherOrder On
SSLCipherSuite ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
SSLCompression off
```

```
mamadou@mamadou-VirtualBox:/etc/apache2/sites-available$ 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:
Module socache_shmcb already enabled
Module ssl already enabled
mamadou@mamadou-VirtualBox:/etc/apache2/sites-available$ a2ensite default-ssl
Site default-ssl already enabled
mamadou@mamadou-VirtualBox:/etc/apache2/sites-available$ service apache2 reload
```

```
mamadou@mamadou-VirtualBox:/etc/apache2/sites-available$ service apache2 reloada2dissi
te default
Usage: apache2 {start|stop|graceful-stop|restart|reload|force-reload}
mamadou@mamadou-VirtualBox:/etc/apache2/sites-available$
```

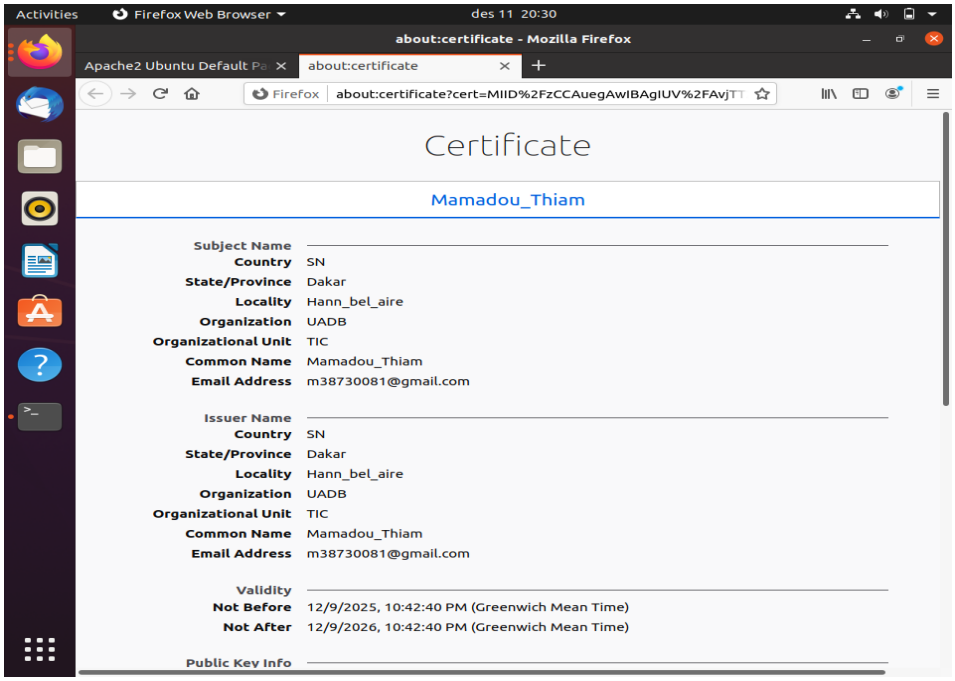
Ajouter ce bout de text dans le fichier de configuration dt https(mamadou-ssl.conf)

```
                #               downgrade-1.0 force-response-1.0

Redirect permanent / https://mamadou-hitech.duckdns.org

        </VirtualHost>
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

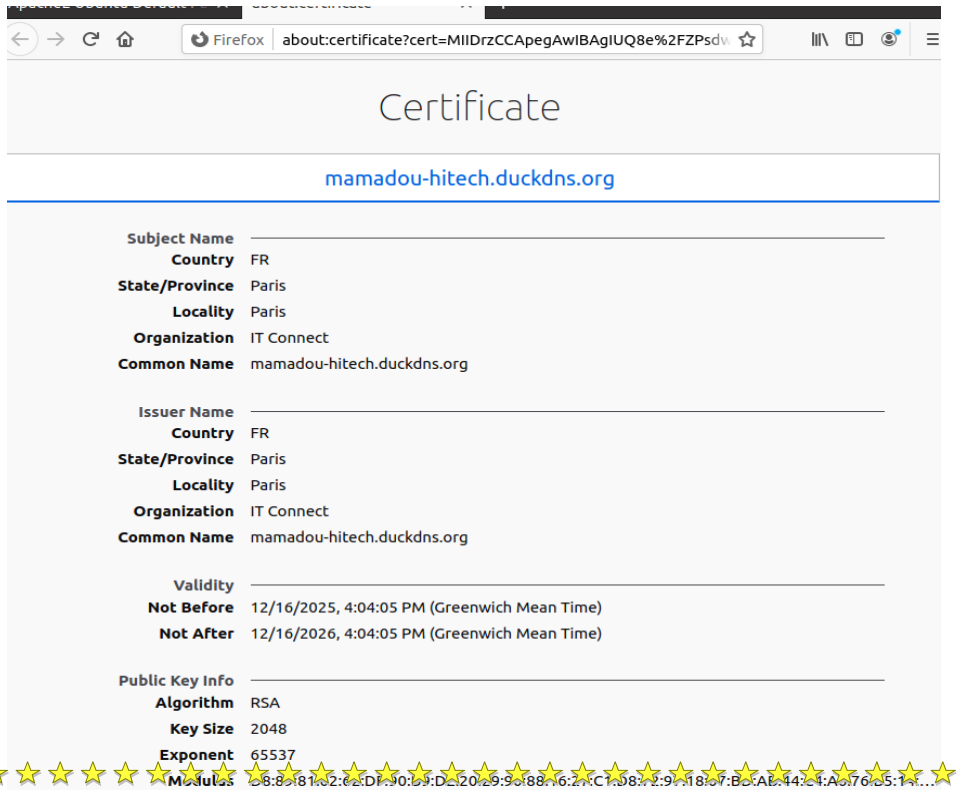
Enregistrer les modifications en redemarrant le serveur web apache

```
mamadou@mamadou-VirtualBox:/etc/apache2/sites-available$ service apache2 reload
mamadou@mamadou-VirtualBox:/etc/apache2/sites-available$
```

Voici le certificat genere pour le http



Voici le certificat genere pour le https



- Utilisation de HTTPS avec Apache2 avec des certificats Let's encrypt :

```
mamadou@mamadou-VirtualBox:~$ sudo a2enmod ssl
[sudo] password for mamadou:
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Module ssl already enabled
mamadou@mamadou-VirtualBox:~$
```

Activation d'apache :

```
mamadou@mamadou-VirtualBox:~$ sudo systemctl reload apache2
mamadou@mamadou-VirtualBox:~$
```

```
mamadou@mamadou-VirtualBox:~$ a2query -m ssl
ssl (enabled by site administrator)
mamadou@mamadou-VirtualBox:~$
```

- *Problème rencontré lors de l'utilisation de Certbot avec Let's Encrypt*

Lors de la configuration HTTPS avec des certificats Let's Encrypt, la commande suivante a été exécutée :

```
sudo certbot certonly --webroot -w /var/www/html -d manadou-hitech.duckdns.org
```

Voici le resultat de la commande

```
mamadou@mamadou-VirtualBox:/etc/apache2/sites-available$ sudo certbot certonly --webro
ot \
>   -w /var/www/html \
>   -d mamadou-hitech.duckdns.org
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Requesting a certificate for mamadou-hitech.duckdns.org

Certbot failed to authenticate some domains (authenticator: webroot). The Certificate
Authority reported these problems:
  Domain: mamadou-hitech.duckdns.org
  Type:   connection
  Detail: 41.82.212.193: Fetching http://mamadou-hitech.duckdns.org/.well-known/acme-c
hallenge/KO68p3J3_2lZrqg2GY4A5WDS0tvM-5dS11M-HXRG_xI: Timeout during connect (likely f
irewall problem)

Hint: The Certificate Authority failed to download the temporary challenge files creat
ed by Certbot. Ensure that the listed domains serve their content from the provided --
webroot-path/-w and that files created there can be downloaded from the internet.

Some challenges have failed.
Ask for help or search for solutions at https://community.letsencrypt.org. See the log
file /var/log/letsencrypt/letsencrypt.log or re-run Certbot with -v for more details.
mamadou@mamadou-VirtualBox:/etc/apache2/sites-available$
```

Cependant, cette commande a échoué avec l'erreur suivante :

Certbot failed to authenticate some domains (authenticator: webroot)

Domain: manadou-hitech.duckdns.org

Type: connection

Detail: 41.82.212.193: Fetching http://manadou-hitech.duckdns.org/.well-known/acme-challenge/K068p333_21Zrqg2GY4ASMD5otvM-5d511M-HXRG_x1: Timeout during connect (likely firewall problem)

Voici les contenues des fichiers de configurations de http et https

```
 GNU nano 4.8                          mamadou.conf
<VirtualHost *:80>
    ServerName mamadou-hitech.duckdns.org
    Redirect permanent / https://mamadou-hitech.duckdns.org/
</VirtualHost>
```

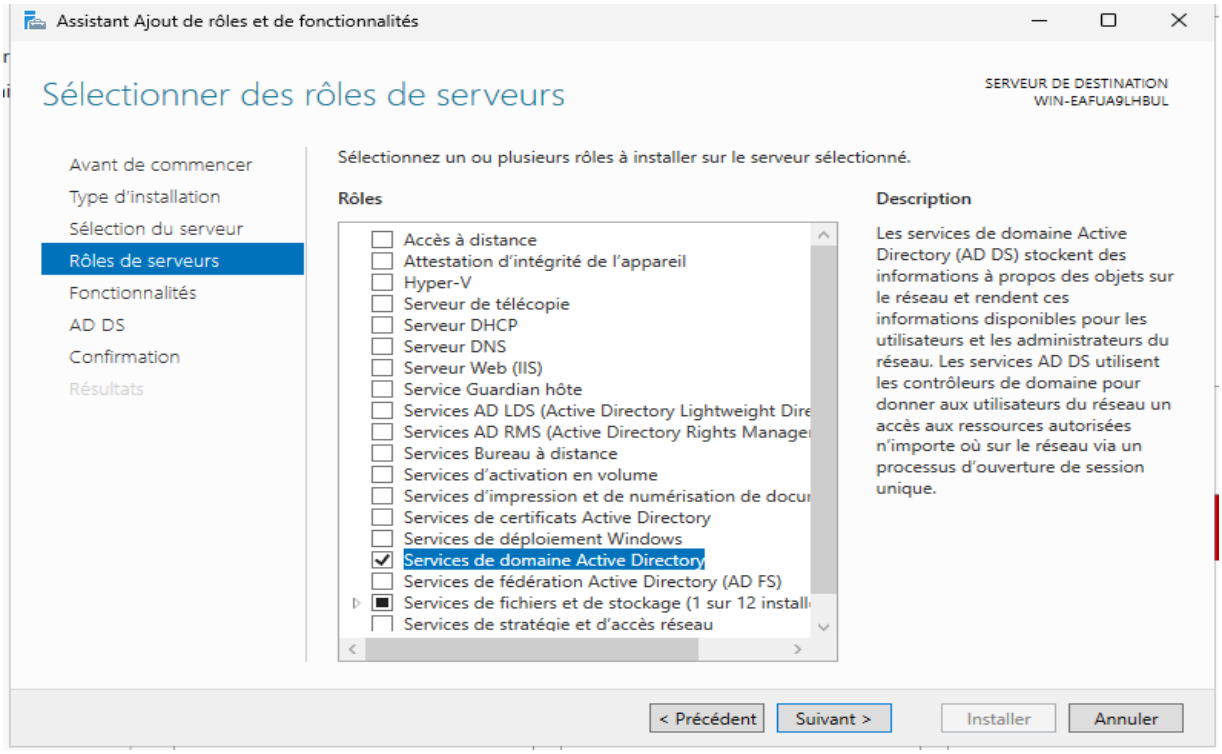
```
 GNU nano 4.8                          mamadou-ssl.conf
<VirtualHost *:443>
    ServerName mamadou-hitech.duckdns.org
    ServerAdmin webmaster@mamadou-hitech.duckdns.org

    DocumentRoot /var/www/html

    SSLEngine on
    SSLCertificateFile /etc/apache2/server.crt
    SSLCertificateKeyFile /etc/apache2/server.key

    <Directory /var/www/html>
        Options -Indexes +FollowSymLinks
        AllowOverride none
        Require all granted
    </Directory>

    Header always set Strict-Transport-Security "max-age=15768000"

    ErrorLog ${APACHE_LOG_DIR}/mamadou-ssl-error.log
    CustomLog ${APACHE_LOG_DIR}/mamadou-ssl-access.log combined
</VirtualHost>
```

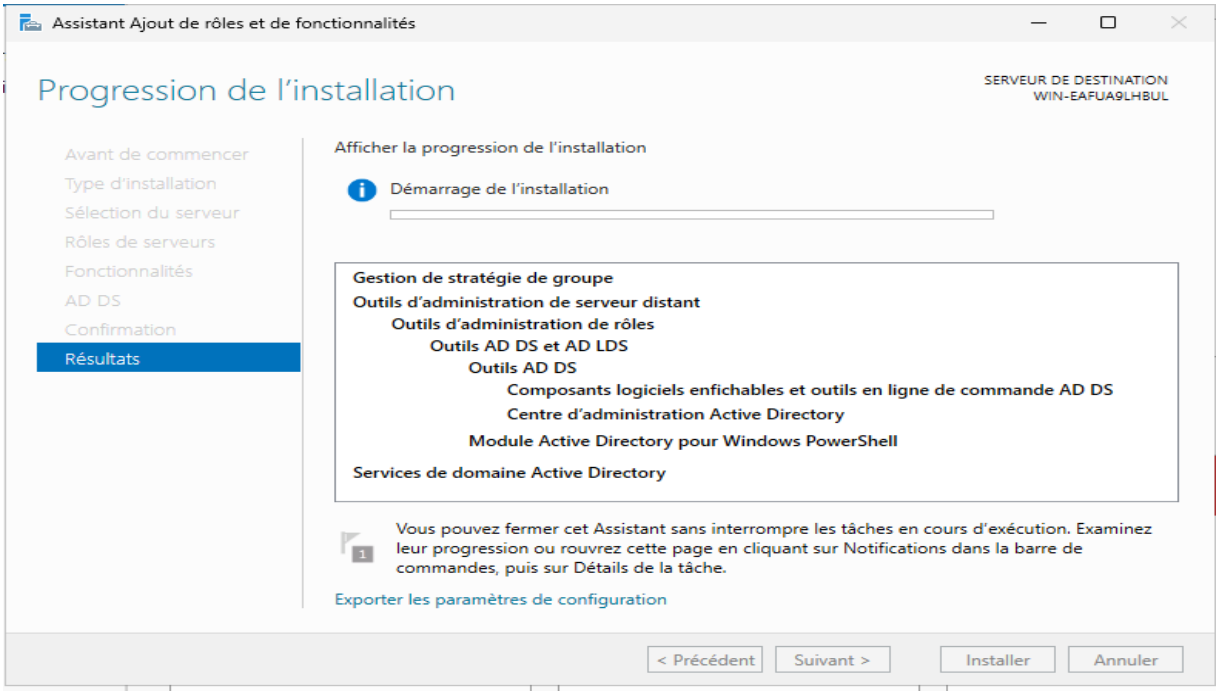
Voici le domaine que j’ai crée dans le site DUCKDNS.ORG

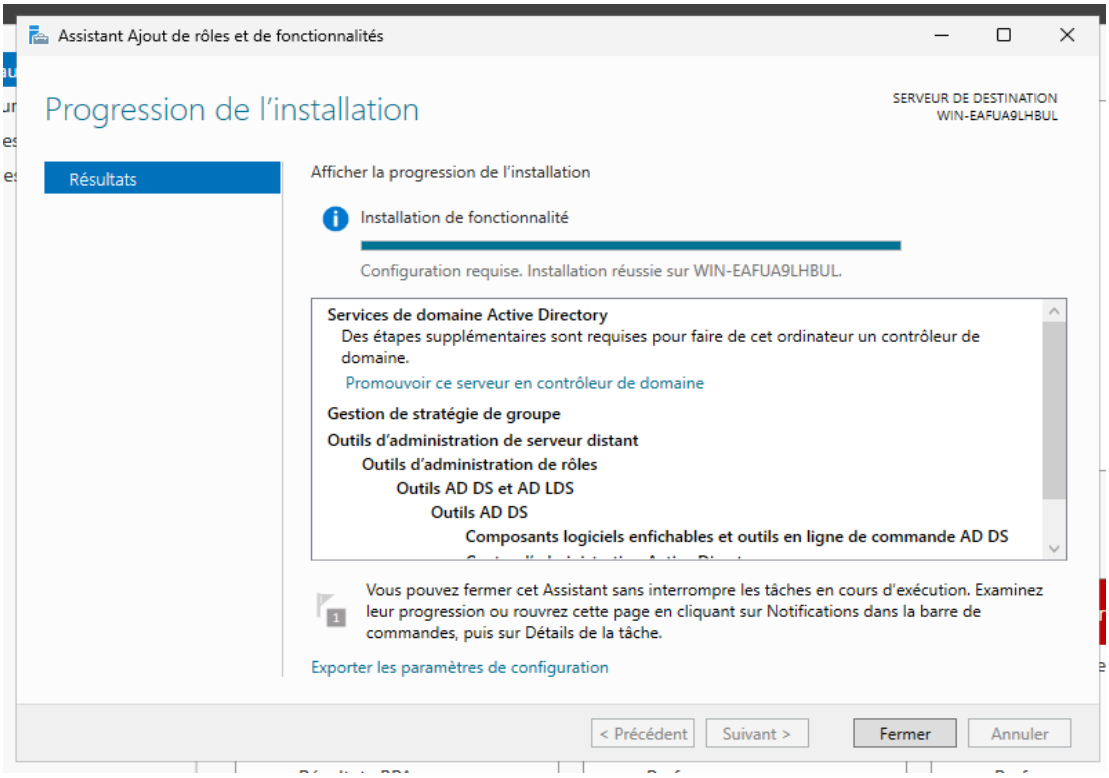
- Créer une autorité de certification racine d'entreprise sous Windows Server :

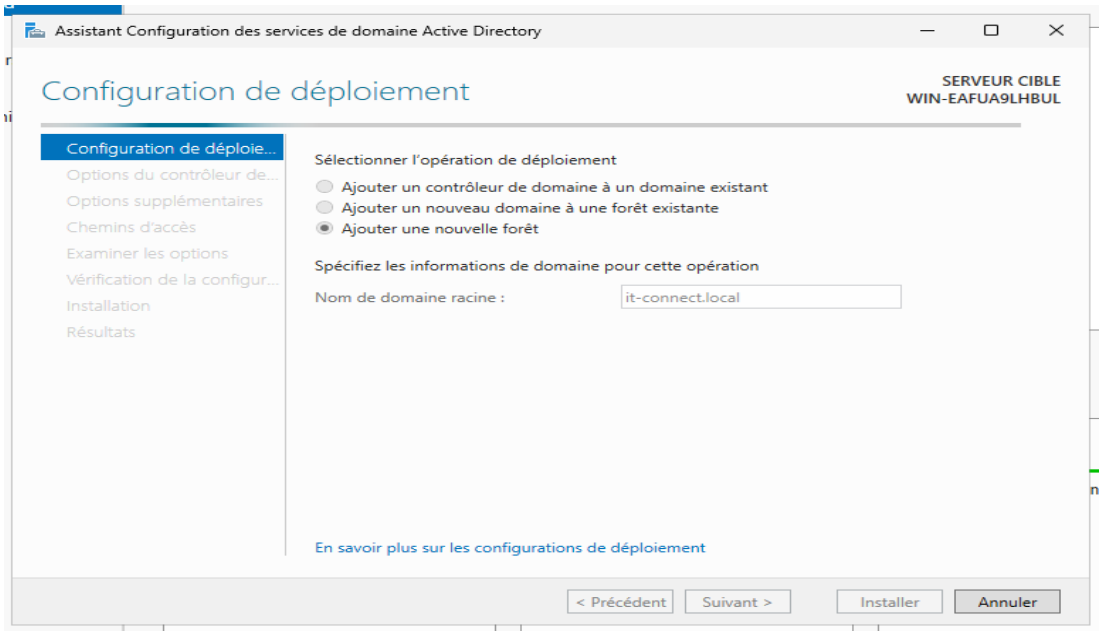
Configurons dabord le service d'active directory

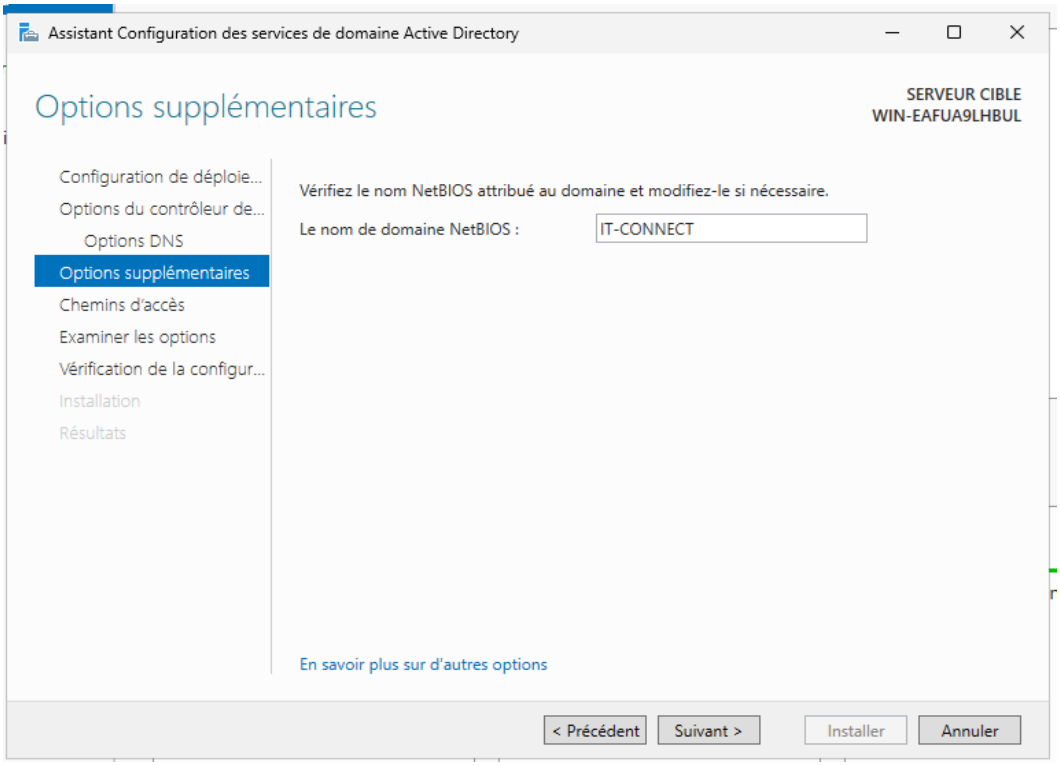
Voici l'enesemble des etapes :

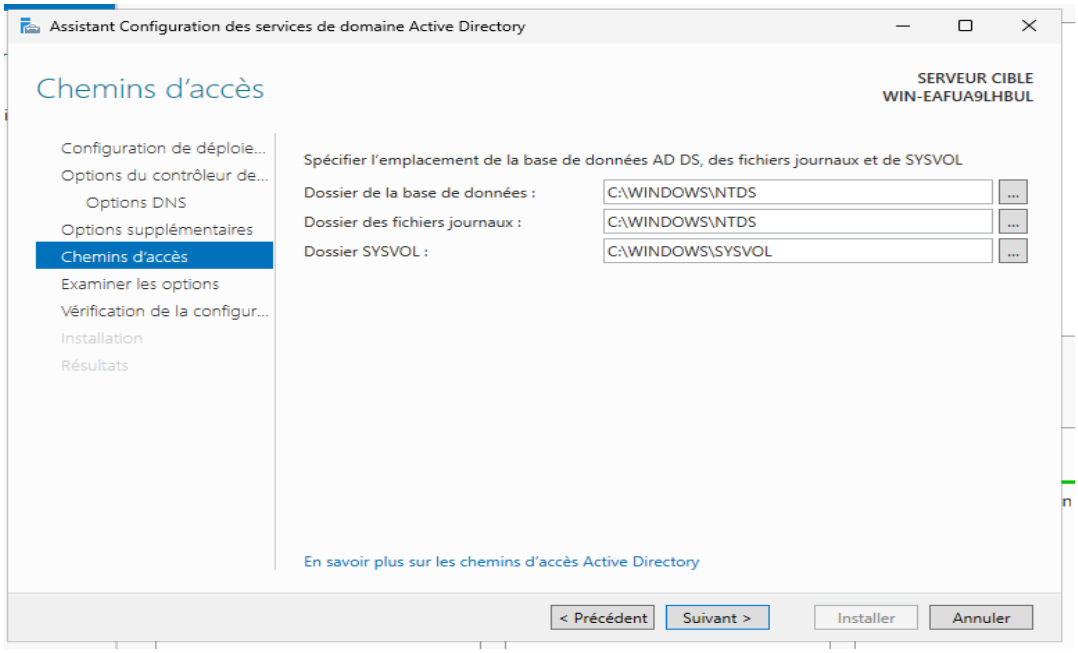


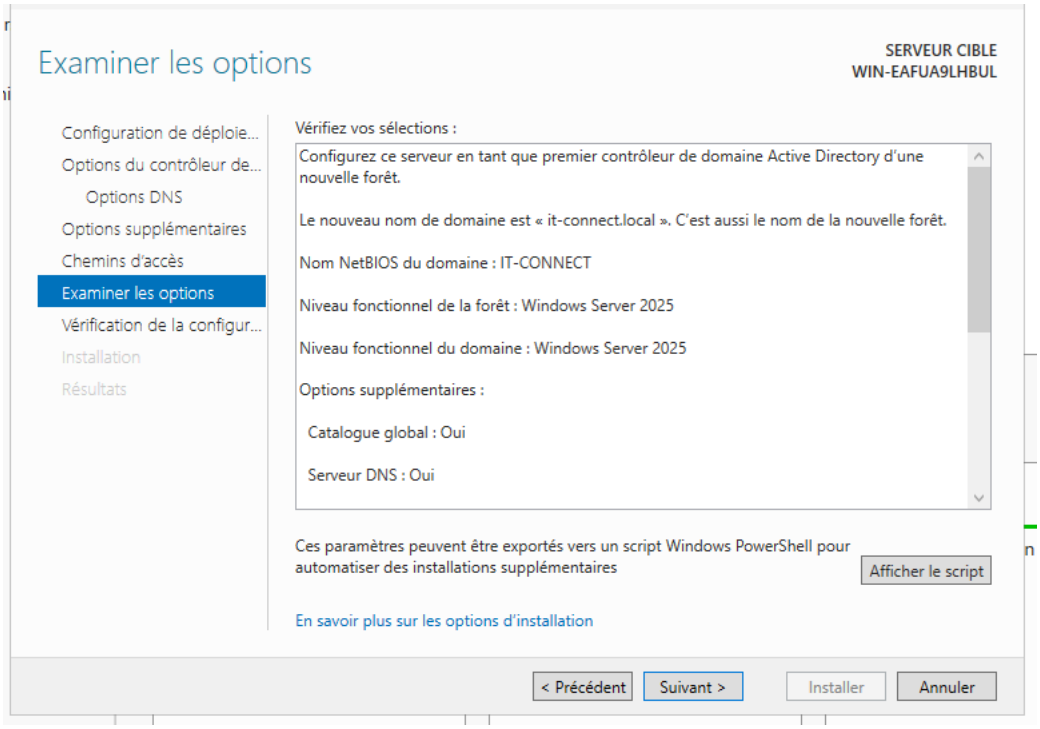


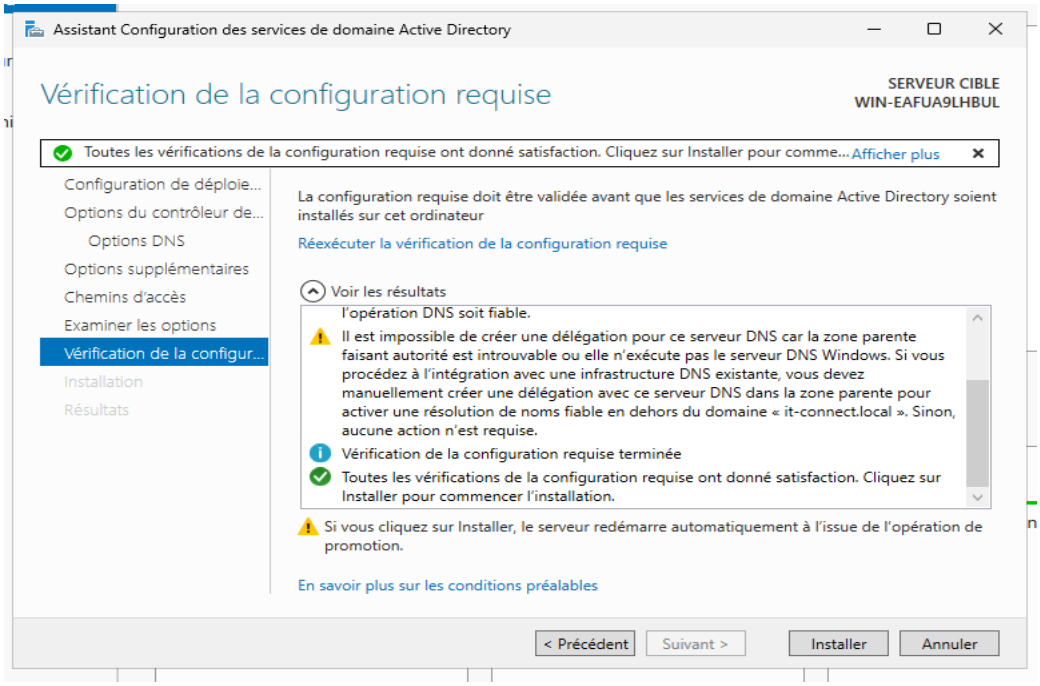

Assistant Ajout de rôles et de fonctionnalités
Progression de l'installation
SERVEUR DE DESTINATION
WIN-EAFUA9LHBUL
Résultats
Afficher la progression de l'installation
Installation de fonctionnalité
Configuration requise. Installation réussie sur WIN-EAFUA9LHBUL.
Services de domaine Active Directory
Des étapes supplémentaires sont requises pour faire de cet ordinateur un contrôleur de domaine.
Promouvoir ce serveur en contrôleur de domaine
Gestion de stratégie de groupe
Outils d'administration de serveur distant
Outils d'administration de rôles
Outils AD DS et AD LDS
Outils AD DS
Composants logiciels enfichables et outils en ligne de commande AD DS
Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche.
Exporter les paramètres de configuration
< Précédent
Suivant >
Fermer
Annuler

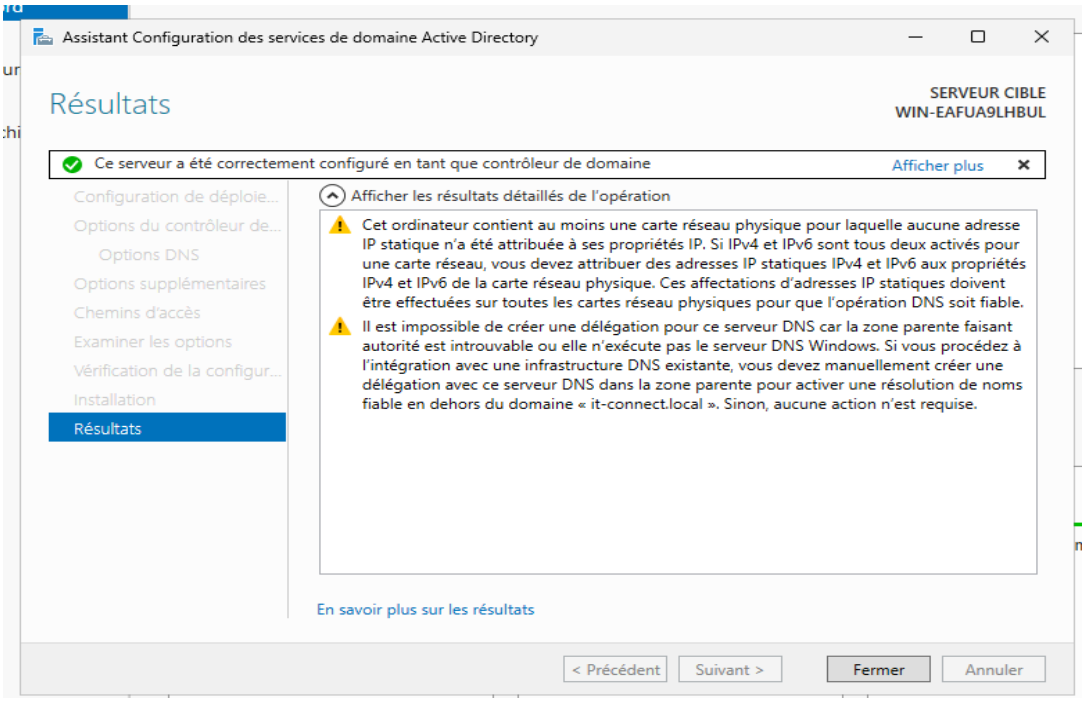

Assistant Configuration des services de domaine Active Directory
Configuration de déploiement
SERVEUR CIBLE
WIN-EAFUA9LHBUL
Configuration de déploie...
Options du contrôleur de...
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
Sélectionner l'opération de déploiement
Ajouter un contrôleur de domaine à un domaine existant
Ajouter un nouveau domaine à une forêt existante
Ajouter une nouvelle forêt
Spécifiez les informations de domaine pour cette opération
Nom de domaine racine :
it-connect.local
En savoir plus sur les configurations de déploiement
< Précédent
Suivant >
Installer
Annuler


Assistant Configuration des services de domaine Active Directory
Options supplémentaires
SERVEUR CIBLE
WIN-EAFUA9LHBUL
Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
Vérifiez le nom NetBIOS attribué au domaine et modifiez-le si nécessaire.
Le nom de domaine NetBIOS :
IT-CONNECT
En savoir plus sur d'autres options
< Précédent
Suivant >
Installer
Annuler


Assistant Configuration des services de domaine Active Directory
Chemins d'accès
SERVEUR CIBLE
WIN-EAFUA9LHBUL
Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
Spécifier l'emplacement de la base de données AD DS, des fichiers journaux et de SYSVOL
Dossier de la base de données :
C:\WINDOWS\NTDS
Dossier des fichiers journaux :
C:\WINDOWS\NTDS
Dossier SYSVOL :
C:\WINDOWS\SYSVOL
En savoir plus sur les chemins d'accès Active Directory
< Précédent
Suivant >
Installer
Annuler


Examiner les options
SERVEUR CIBLE
WIN-EAFUA9LHBUL
Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
Vérifiez vos sélections :
Configurez ce serveur en tant que premier contrôleur de domaine Active Directory d'une nouvelle forêt.
Le nouveau nom de domaine est « it-connect.local ». C'est aussi le nom de la nouvelle forêt.
Nom NetBIOS du domaine : IT-CONNECT
Niveau fonctionnel de la forêt : Windows Server 2025
Niveau fonctionnel du domaine : Windows Server 2025
Options supplémentaires :
Catalogue global : Oui
Serveur DNS : Oui
Ces paramètres peuvent être exportés vers un script Windows PowerShell pour automatiser des installations supplémentaires
Afficher le script
En savoir plus sur les options d'installation
< Précédent
Suivant >
Installer
Annuler

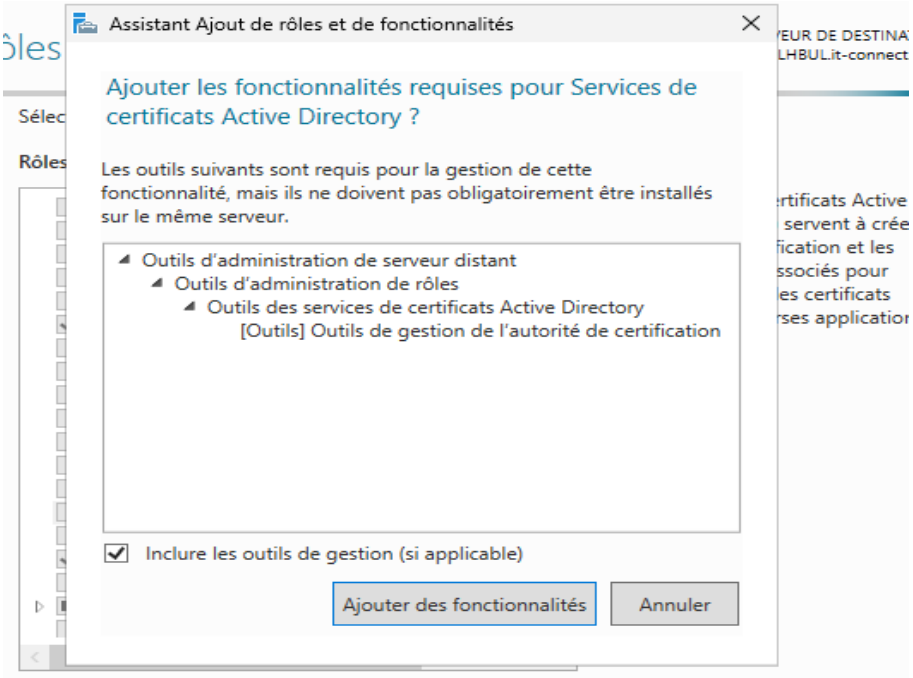

Assistant Configuration des services de domaine Active Directory
Vérification de la configuration requise
SERVEUR CIBLE
WIN-EAFUA9LHBUL
Toutes les vérifications de la configuration requise ont donné satisfaction. Cliquez sur Installer pour comme...
Afficher plus
Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
La configuration requise doit être validée avant que les services de domaine Active Directory soient installés sur cet ordinateur
Réexécuter la vérification de la configuration requise
Voir les résultats
l'opération DNS soit fiable.
Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est introuvable ou elle n'exécute pas le serveur DNS Windows. Si vous procédez à l'intégration avec une infrastructure DNS existante, vous devez manuellement créer une délégation avec ce serveur DNS dans la zone parente pour activer une résolution de noms fiable en dehors du domaine « it-connect.local ». Sinon, aucune action n'est requise.
Vérification de la configuration requise terminée
Toutes les vérifications de la configuration requise ont donné satisfaction. Cliquez sur Installer pour commencer l'installation.
Si vous cliquez sur Installer, le serveur redémarre automatiquement à l'issue de l'opération de promotion.
En savoir plus sur les conditions préalables
< Précédent
Suivant >
Installer
Annuler



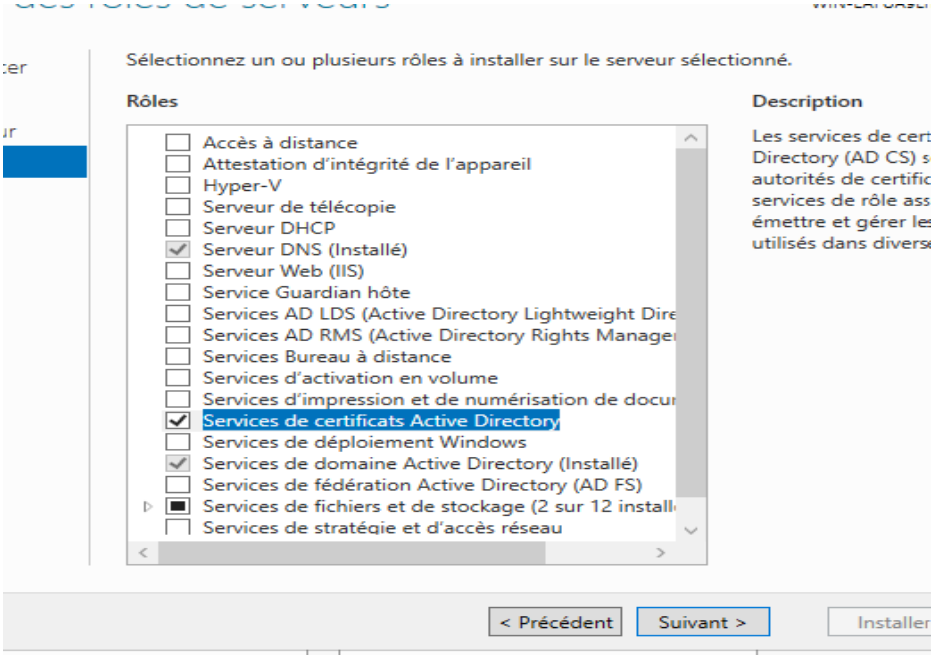
Fin de la configuration de l'active directory !

Maintenant on demarre la configuration de l'ADCS

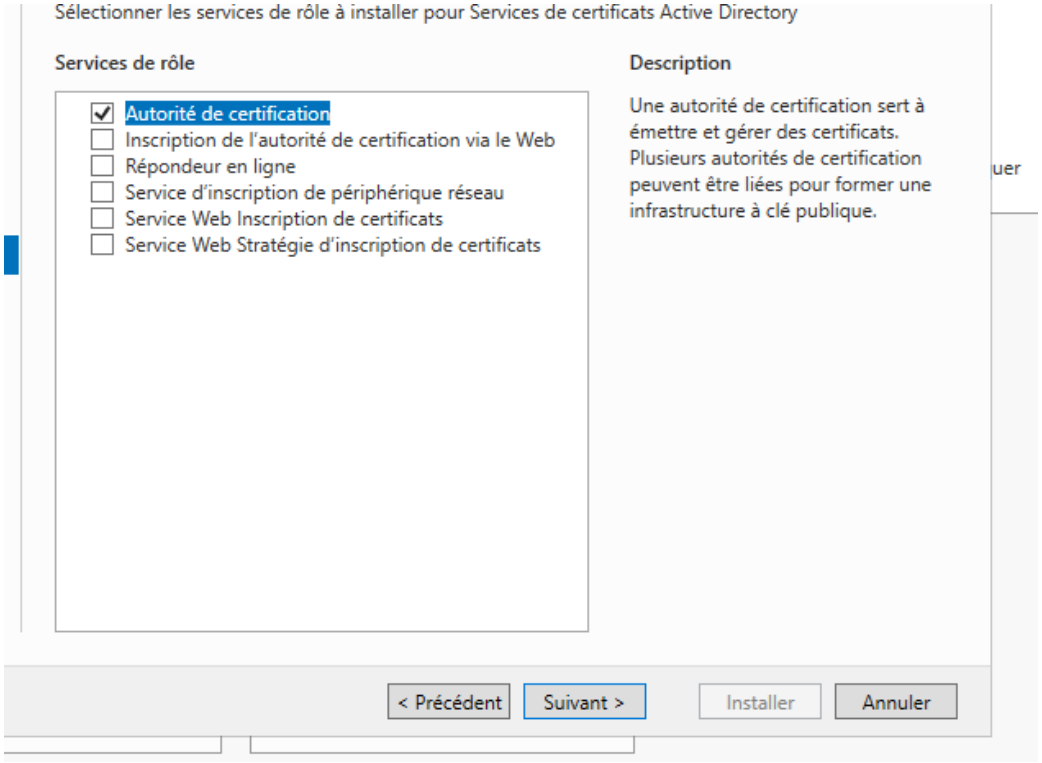
1 : Demarrage de la configuration Services de certificat d'active directo

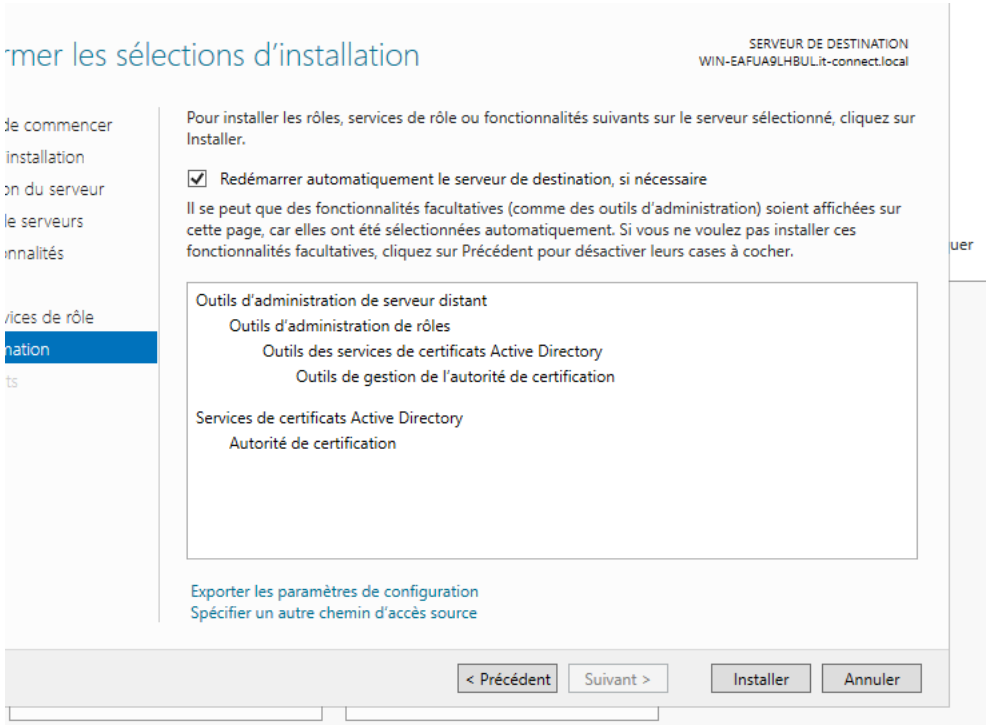


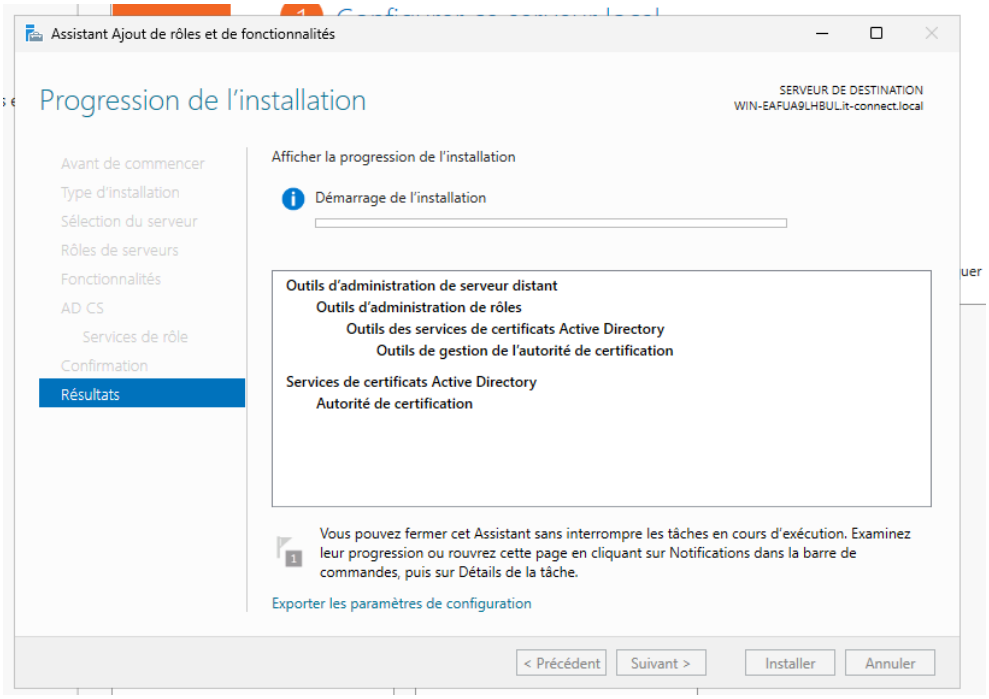
2



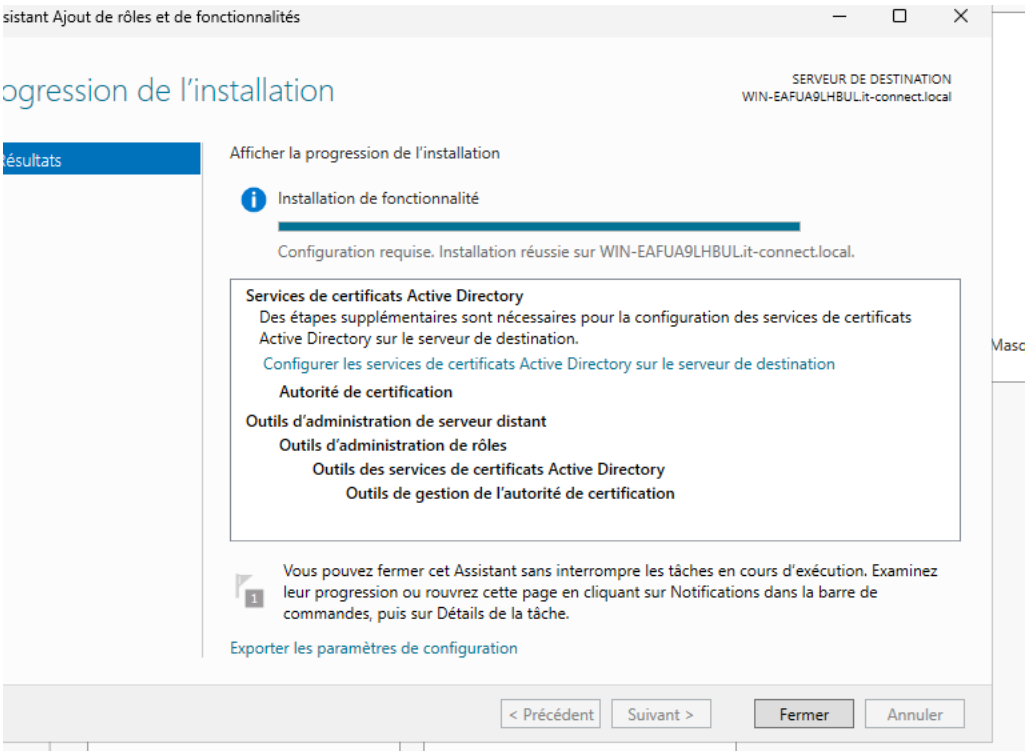
3 : Puis, avancez jusqu'à l'étape " Services de rôle" où vous n'aurez qu'à cocher " Autorité de certi cation".

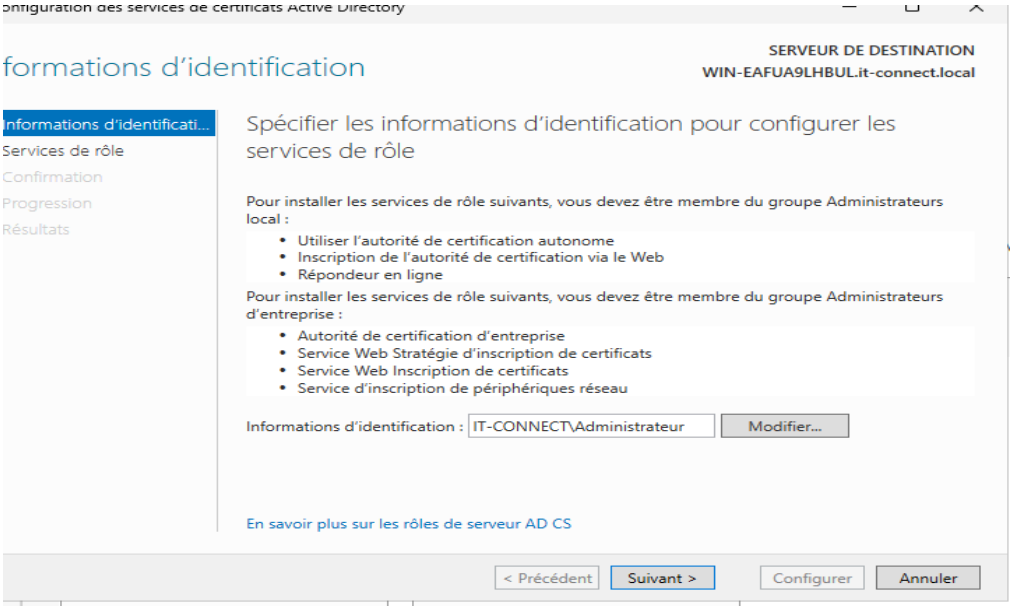



rmer les sélections d'installation
SERVEUR DE DESTINATION
WIN-EAFUA9LHBUL.it-connect.local
de commencer
installation
on du serveur
le serveurs
nnalités
vices de rôle
nation
ts
Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.
Redémarrer automatiquement le serveur de destination, si nécessaire
Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.
Outils d'administration de serveur distant
Outils d'administration de rôles
Outils des services de certificats Active Directory
Outils de gestion de l'autorité de certification
Services de certificats Active Directory
Autorité de certification
Exporter les paramètres de configuration
Spécifier un autre chemin d'accès source
< Précédent
Suivant >
Installer
Annuler

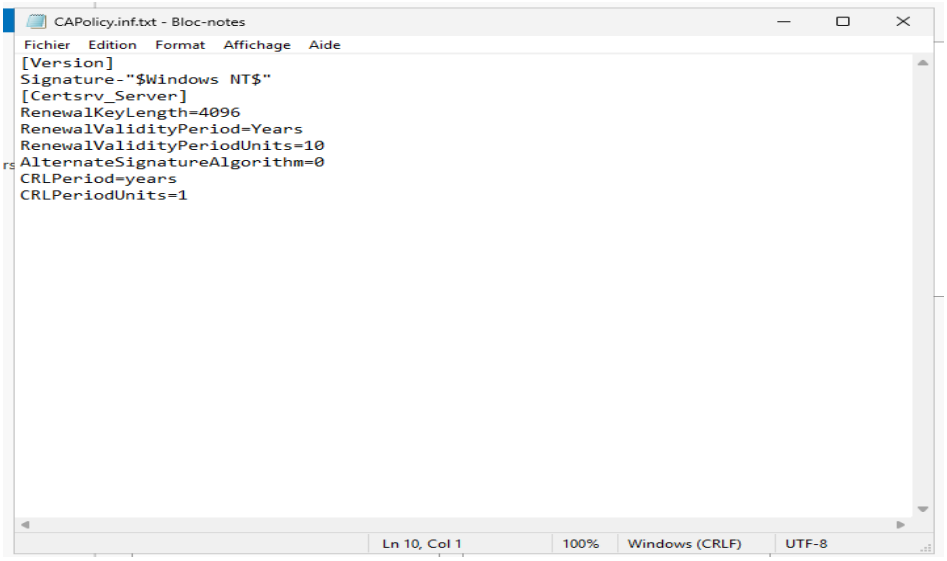

Assistant Ajout de rôles et de fonctionnalités
Progression de l'installation
SERVEUR DE DESTINATION
WIN-EAFUA9LHBUL.it-connect.local
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
AD CS
Services de rôle
Confirmation
Résultats
Afficher la progression de l'installation
Démarrage de l'installation
Outils d'administration de serveur distant
Outils d'administration de rôles
Outils des services de certificats Active Directory
Outils de gestion de l'autorité de certification
Services de certificats Active Directory
Autorité de certification
Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche.
Exporter les paramètres de configuration
< Précédent
Suivant >
Installer
Annuler

Avancez jusqu'à la n et lancez l'installation. Quand c'est terminé, cliquez sur le bouton " Fermer".





Sachez qu'à ce moment précis, vous pouvez créer un chier nommé " C:\Windows") sur votre serveur ADCS. Vous pouvez éditer le chier avec le Bloc-notes. Ce chier sert à CAPolicy.inf" (dans " précongurer certaines options de l'autorité de certi cation que nous allons créer. Voici un exemple, à titre purement indicatif

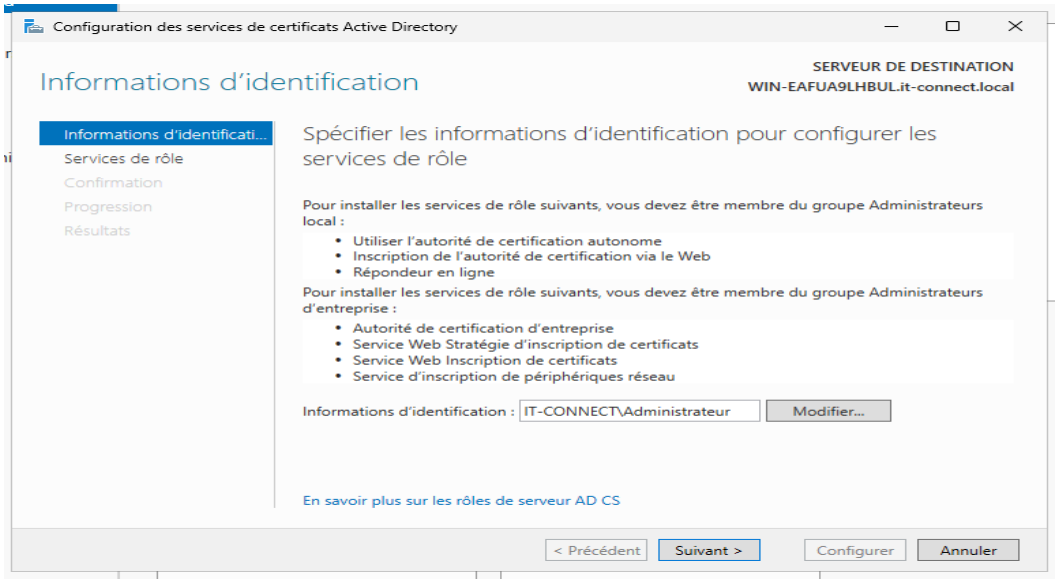


Poursuivez la conguration via le lien " Congurer les services de certi cats Active Directory" visible dans le Gestionnaire de serveur.

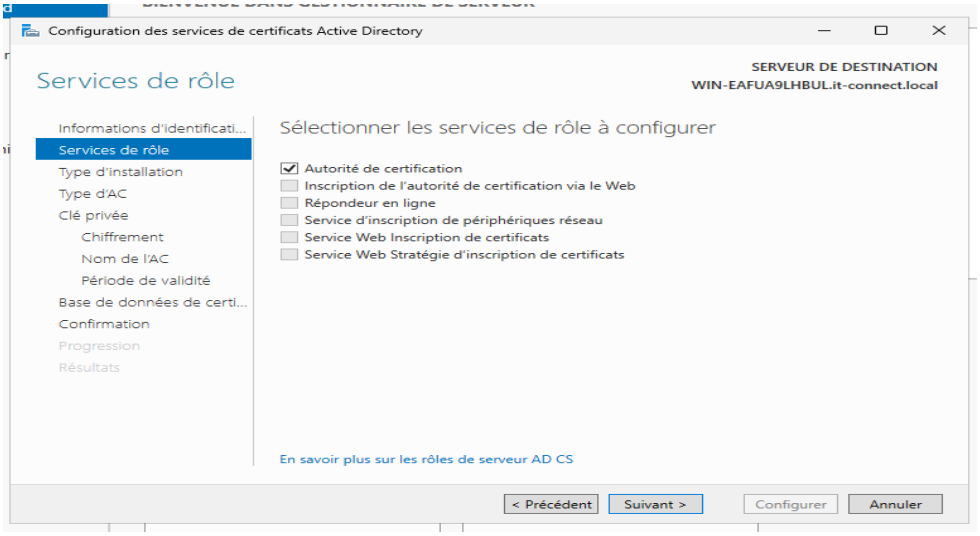
La partie installation du rôle s'arrête ici, ensuite, nous allons créer l'autorité de certification racine.

- Créer l'autorité de certification racine :

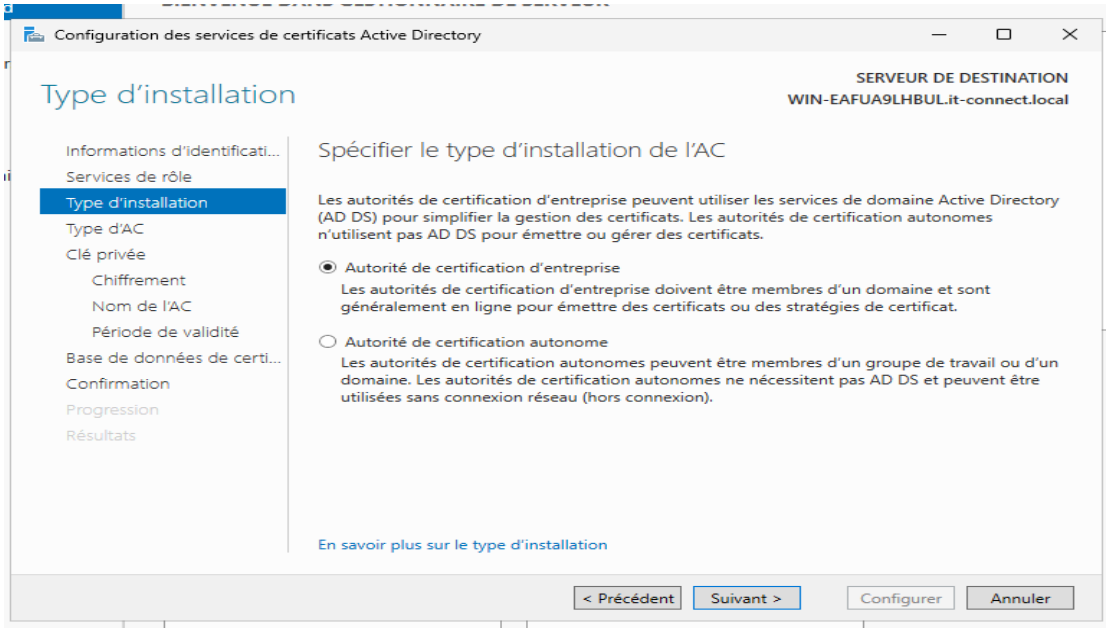
Cliquez directement sur le bouton " Suivant" si vous êtes connecté avec un compte administrateur. Sinon, cliquez sur le bouton " Modi er" pour sélectionner un compte



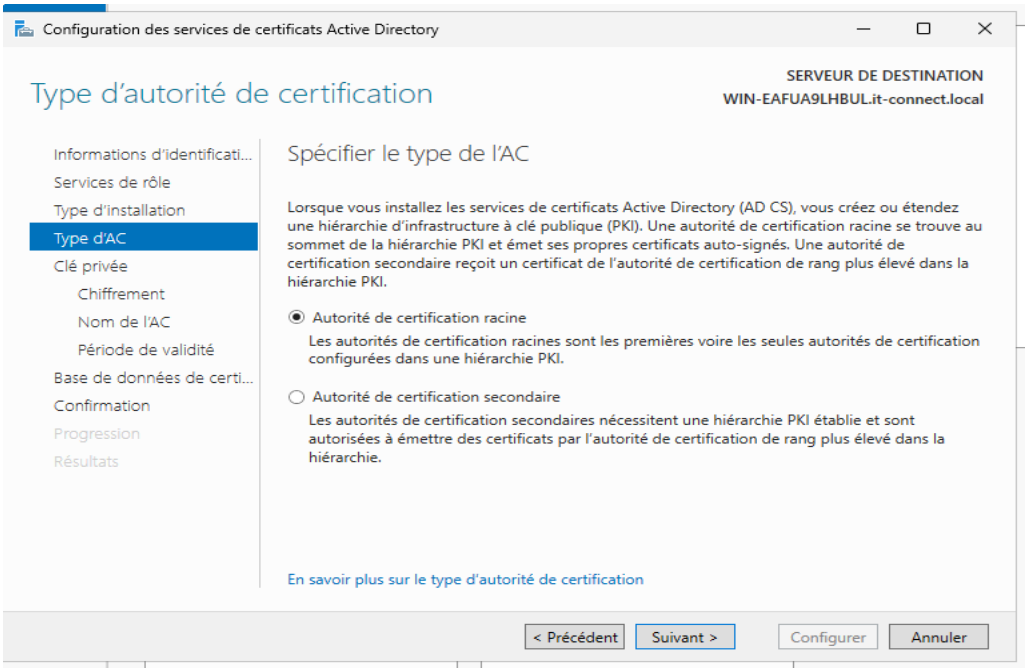
Plusieurs rôles sont proposés, sélectionnez uniquement " Autorité de certification".



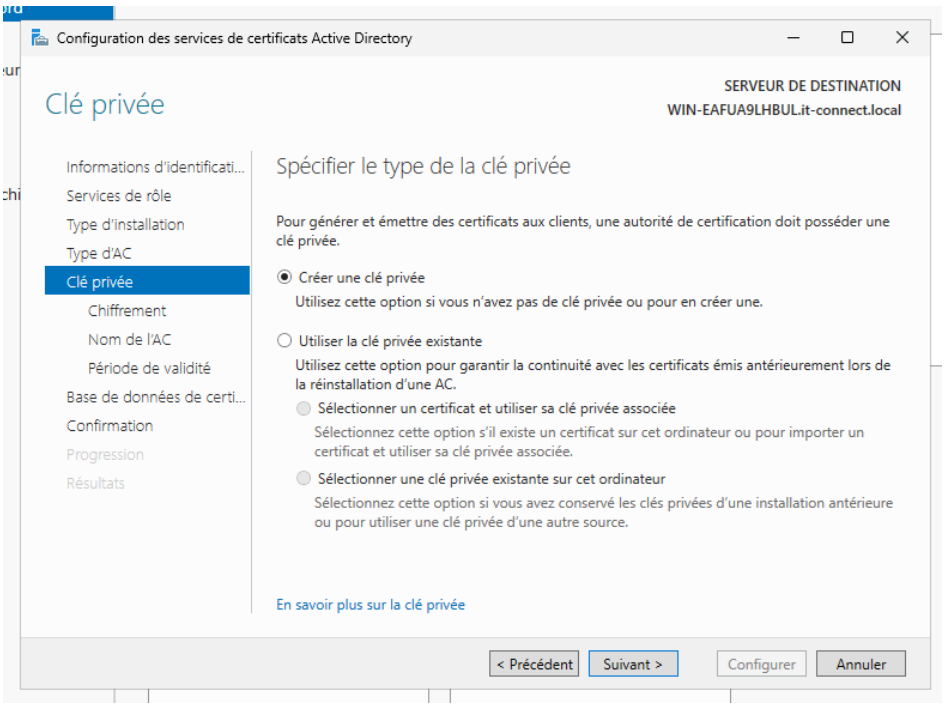
Sélectionnez ensuite " Autorité de certi cation d'entreprise" et poursuivez. Ce choix est fait, car nous sommes en environnement Active Directory et que nous utilisons qu'un seul serveur. Dans le cas où une hiérarchie de CA est mise en place, cette première autorité de certi cation sera congurée en tant que CA autonome, puis la CA intermédiaire déployée sur un second serveur, serait une autorité de certification d'entreprise.



Comme il s'agit de la première Autorité de certification de notre infrastructure, sélectionnez l'option “Autorité de certi cation racine”.

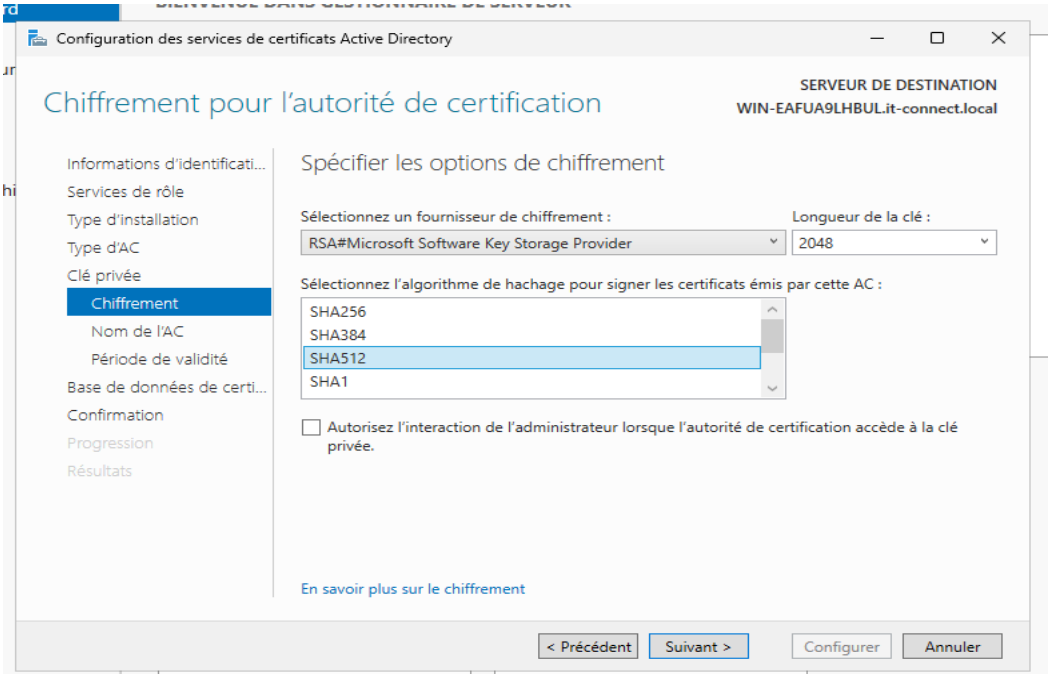


Nous allons créer une nouvelle clé privée, car nous partons de zéro.

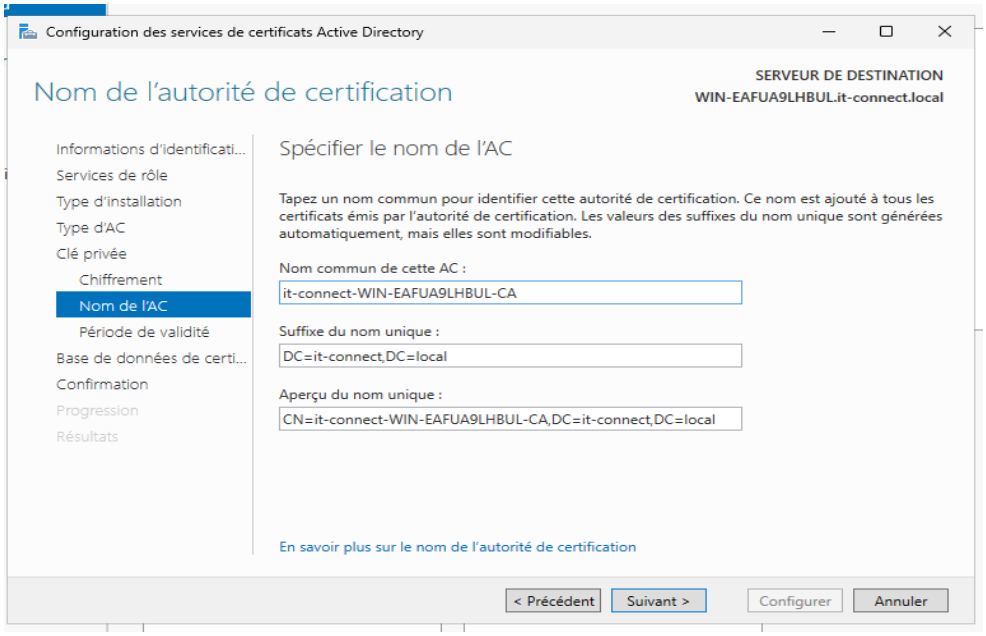


Pour sécuriser notre clé privée avec un algorithme de hachage suf samment robuste, sélectionnez SHA512" et utilisez "

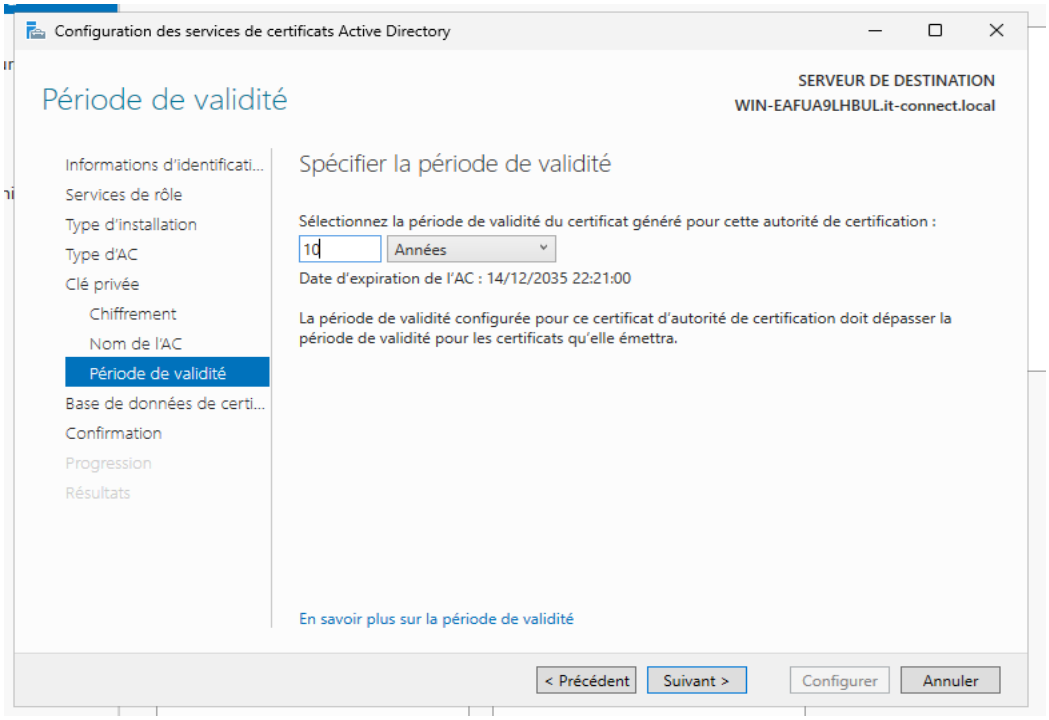
4096" comme longueur de clé. Ce sont des valeurs adéquates pour l'autorité de certi cation racine. Dans tous les cas, sachez que le SHA1 est déprécié par Microsoft depuis janvier 2017, il convient donc de l'éviter.



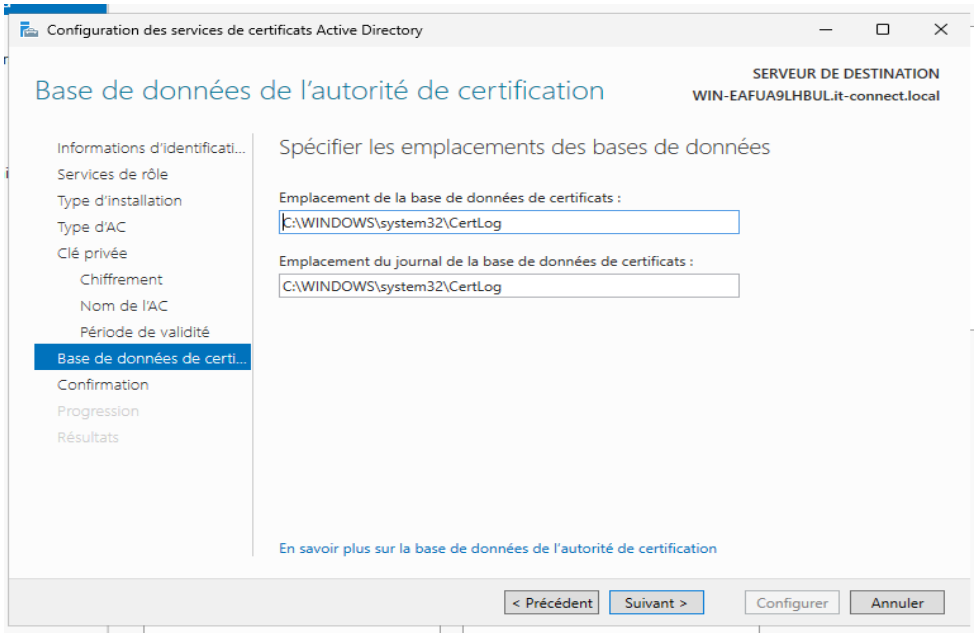
Indiquez un nom pour votre autorité de certi cation, il s'agit d'un nom qui sera indiqué dans les différents certi cats que vous allez émettre avec votre CA. Prenez le temps de remplir correctement ces informations.



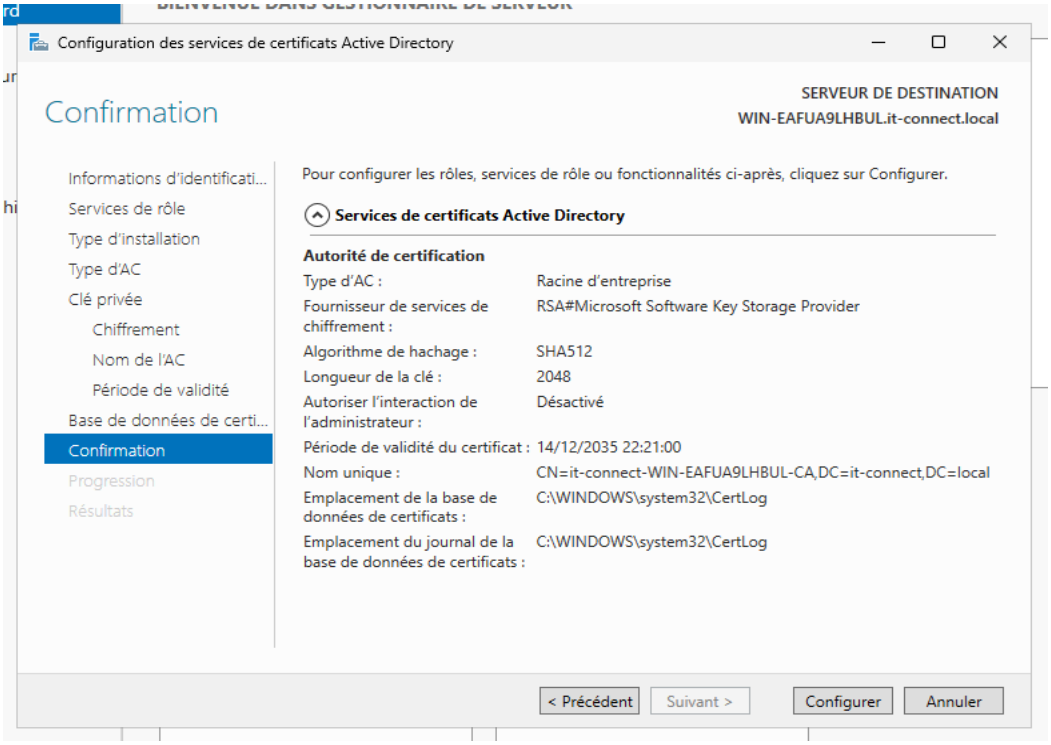
Spécifiez la durée de validité du certificat généré pour votre CA, par défaut la valeur est de 5 années. Vous pouvez indiquer " 10" au lieu de "5".

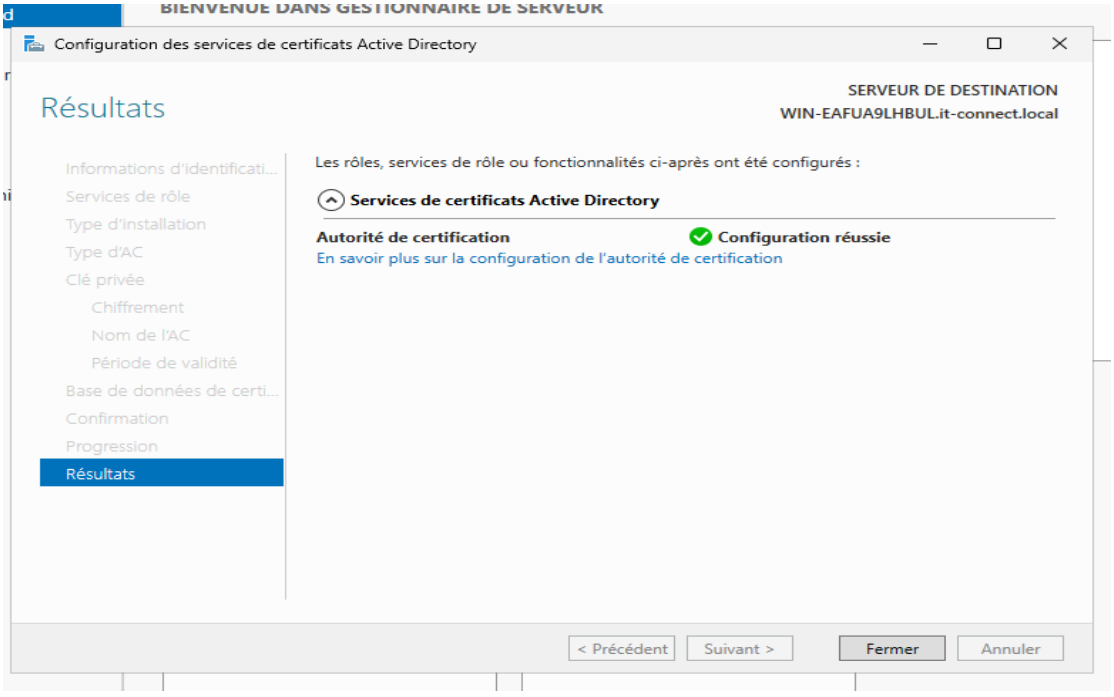


Laissez par défaut les chemins indiqués pour stocker la Poursuivez directement. base de données des certi cats et les logs associés.

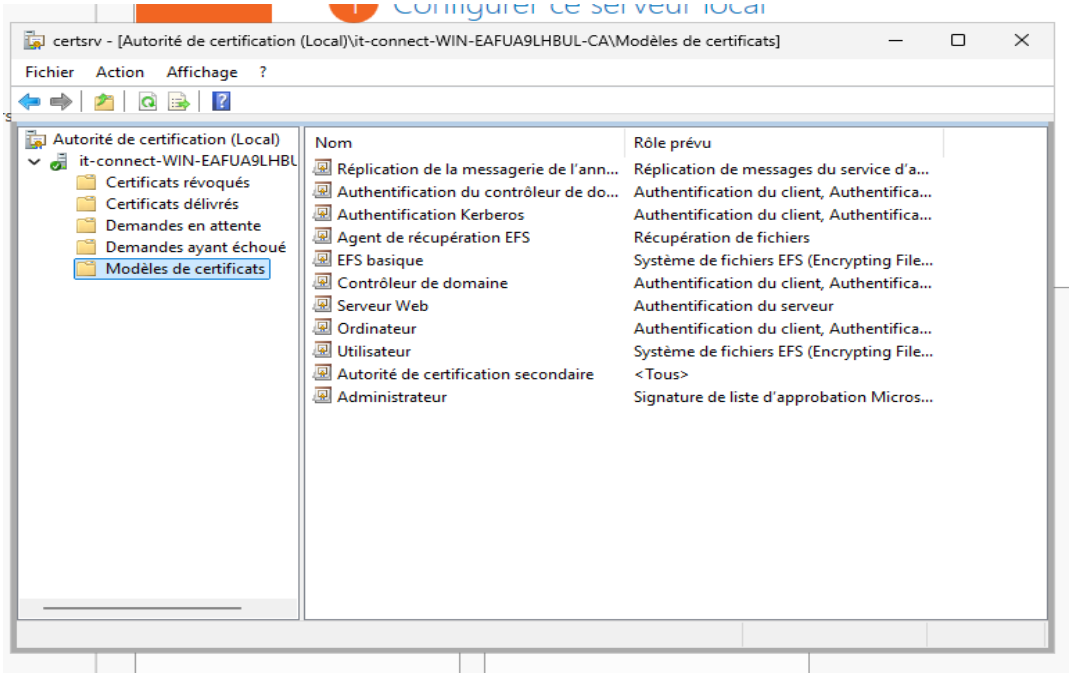


Il ne reste plus qu'à valider et après quelques minutes, vous devriez obtenir un message de succès avec le texte " Conguration réussie".

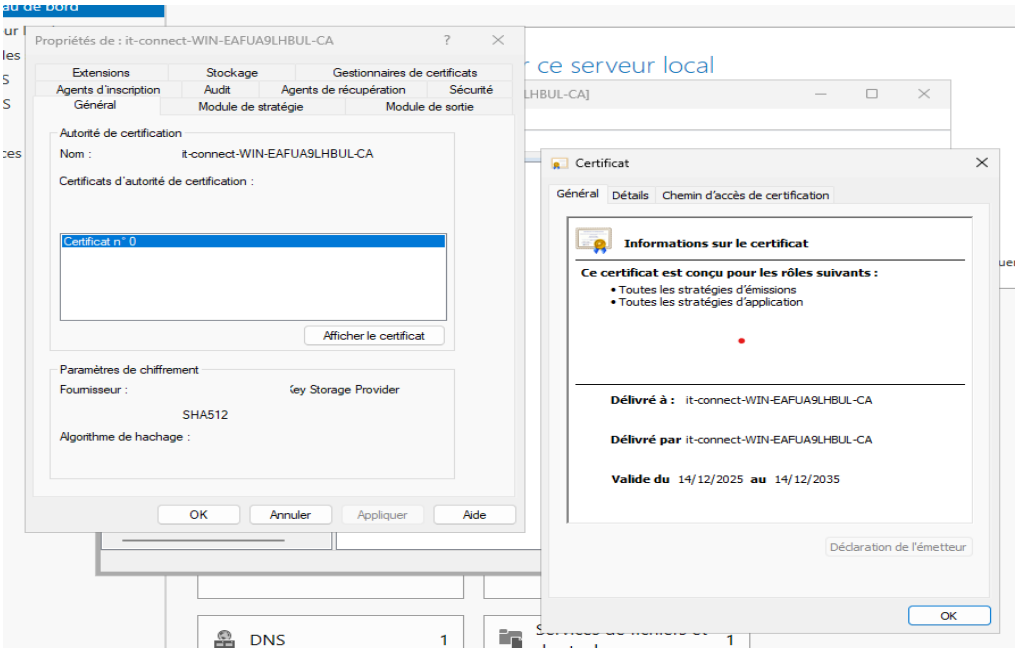




La console " Autorité de certi cation" disponible dans le menu " Outils" du Gestionnaire de serveur, vous permettra de gérer votre autorité de certi cation. PowerShell est également votre allié, comme l'outil en ligne de commande " certutil.exe"



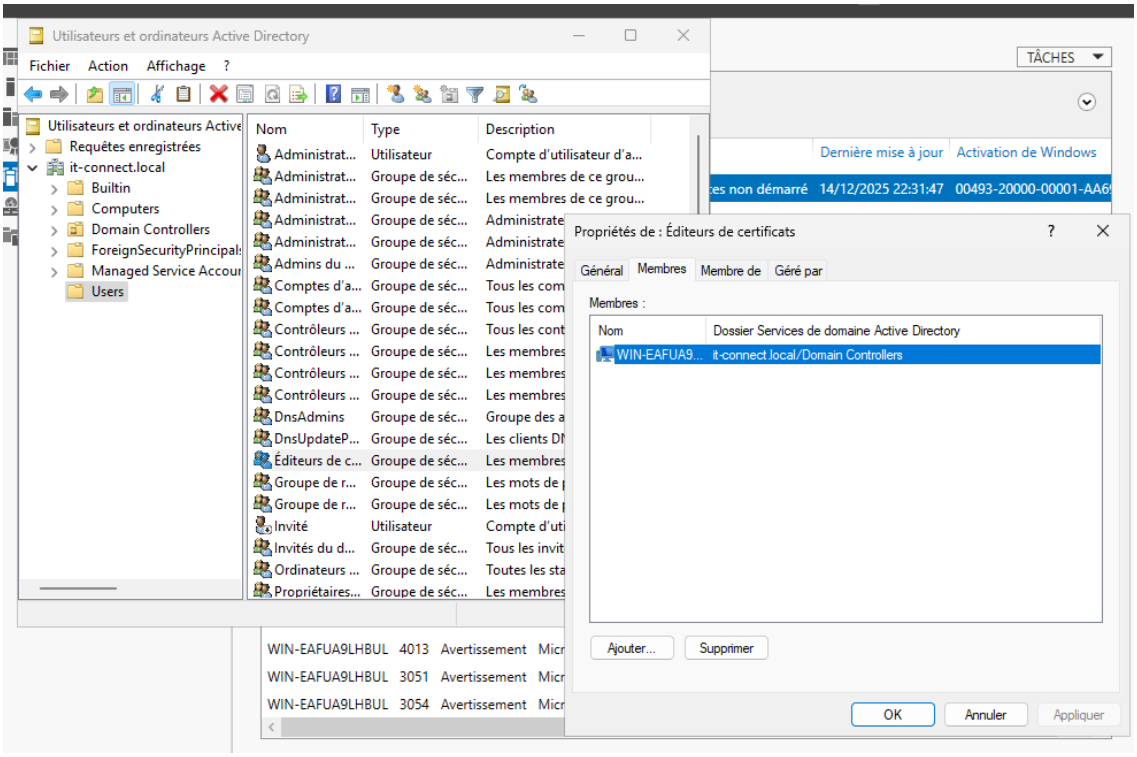
Effectuez un clic droit sur le nom de la CA, à savoir " Ensuite, cliquez sur le bouton " IT-Connect-CA-Root" puis cliquez sur " Propriétés". Af cher le certi cat". Ici, vous pouvez constater que le certi cat racine de la CA est bien valide 10 ans



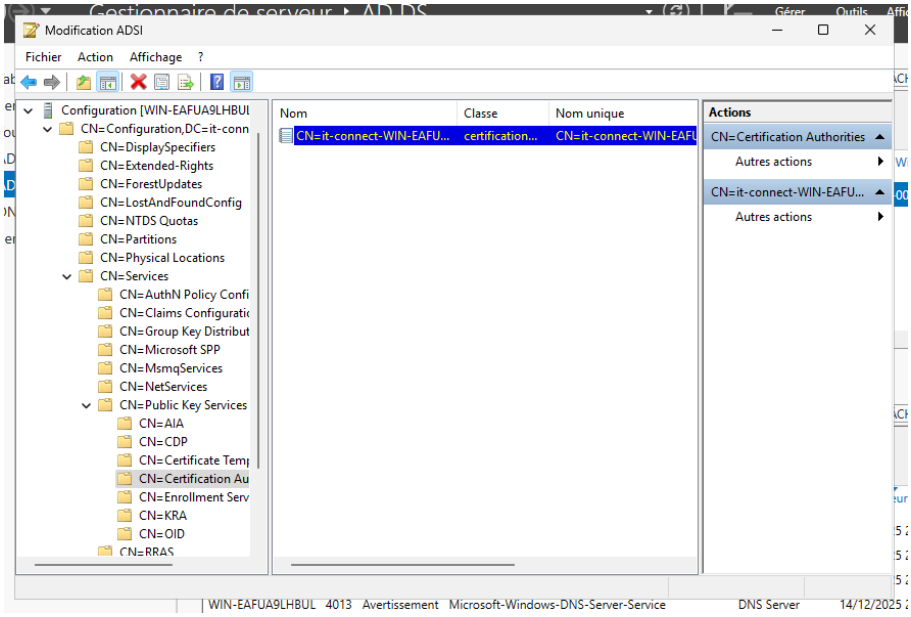
- L'autorité de certification est-elle inscrite dans l'AD ?

Puisque nous avons choisi de créer une autorité de certi cation d'entreprise, la CA est automatiquement inscrite dans l'AD lors de sa création. À l'inverse, ceci n'est pas le cas avec une CA autonome. Dans l'Active Directory, vous pouvez voir que le compte ordinateur de la machine " SRV-CA-ROOT" est désormais membre du groupe

de sécurité " Éditeurs de certi cats" (" Cert Publishers", en anglais). Vous pouvez en pro ter pour supprimer le compte ordinateur de ce groupe, car cette permission est utile uniquement le temps de l'installation.



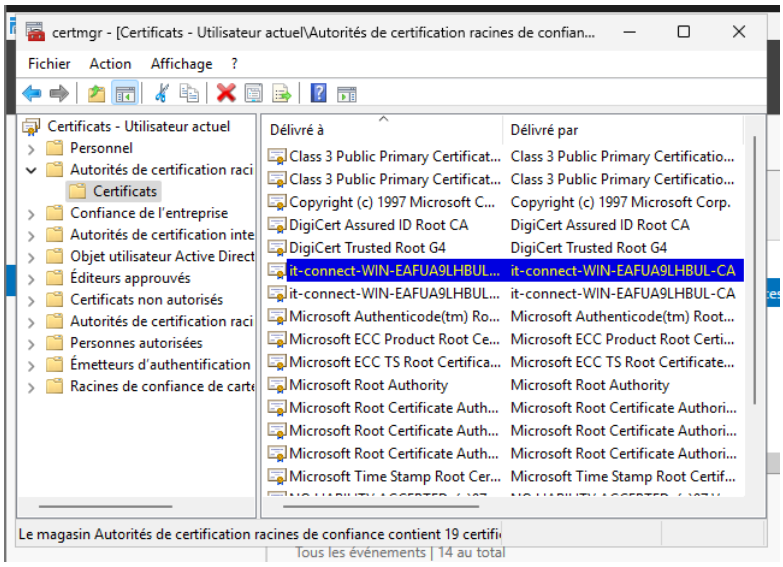
La CA est aussi inscrite dans l'annuaire au sein d'un conteneur nommé " Certi cation Authorities". Ouvrez la console " Modi cation ADSI" (adsiedit.msc) avec le contexte " Conguration", puis parcourez l'arborescence comme ceci : Conguration > Services > Public Key Services > Certi cation Authorities. Ici, notre CA apparaît



Faut-il déployer le certificat de l'autorité racine sur les machines ?

Nous avons créé une autorité de certi cation racine d'entreprise inscrit dans l'Active Directory. De ce fait, le certi cat de la CA sera automatiquement distribué aux postes de travail et aux serveurs membres du domaine AD. Nous pouvons le véri er assez rapidement…

Ouvrez la console " ⋯ certmgr.msc" sur une machine du domaine. Vous verrez ainsi que le certi cat de votre CA est placé dans le magasin nommé " Autorités de certi cation racines de con ance". Regardez :

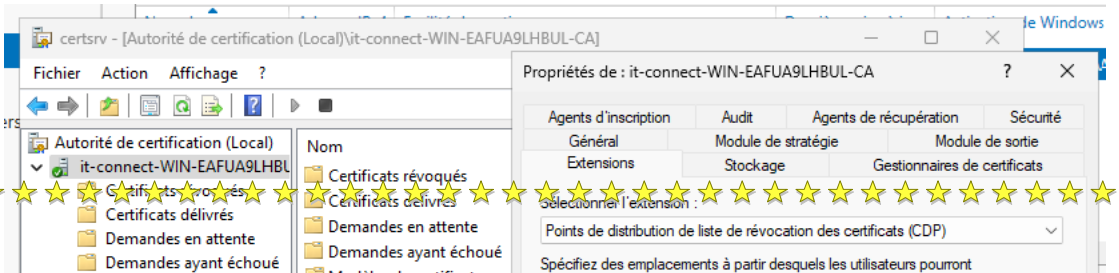


Il n'est donc pas nécessaire d'exporter ce certificat a n de le déployer par GPO.

La publication de la liste de révocation

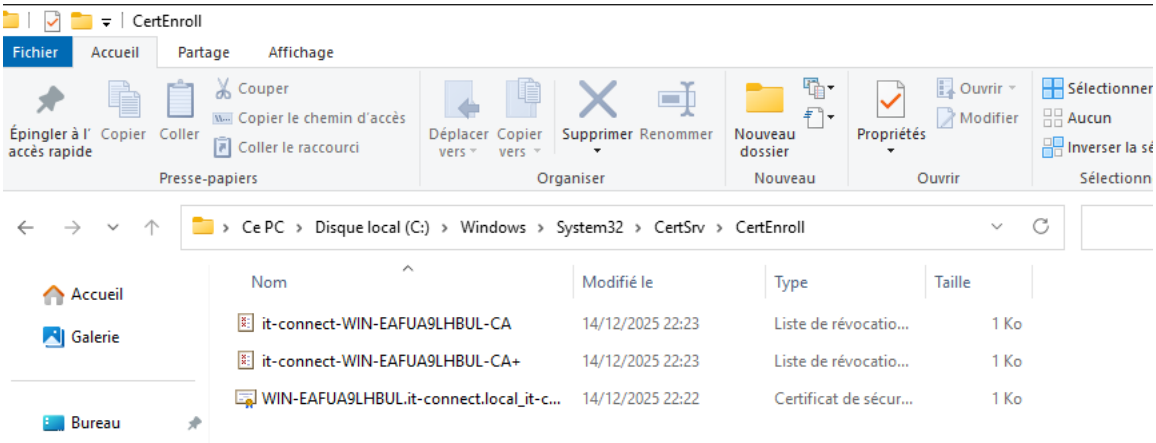
Chaque certi cat a une durée de vie limitée et un certi cat peut être révoqué à tout moment (suite à l'action d'un administrateur, par exemple). De ce fait, au-delà d'émettre des certi cats, l'autorité de certi cation doit aussi **mettre à disposition des machines la liste des certi cats révoquées**. Cette liste est appelée **CRL : Certi cate Revocation List**. Les emplacements où est stockée la CRL sont appelés **CDP : CRL Distribution Point**. À cela s'ajoute les emplacements des certi cats d'autorité de certi cation, que l'on appelle **AIA : Authority Information Access**, soit l'Accès aux informations de l'autorité. Par défaut, les informations sont publiées dans l'Active Directory et le chemin LDAP est précisé dans les certi cats délivrés par la CA. De ce fait, les machines du domaine AD pourront accéder à cette liste. En revanche, elle ne sera pas accessible aux machines qui ne sont pas membres du domaine. Ceci peut nécessiter la mise en œuvre d'un serveur IIS (de préférence différent du serveur ADCS) a n de publier la CRL et la rendre accessible via le protocole HTTP. La conguration s'effectue via les propriétés de la CA, à partir de l'onglet " **Extensions**".

Points de distribution de liste de révocation des certi cats (CDP) - Conguration par défaut



Accès aux informations de l'autorité (AIA) - Conguration par défaut

En plus d'une publication dans l'AD, la CRL est aussi publiée sur le disque local de l'autorité de certi cation.



Mission accomplie ! L'autorité de certi cation racine d'entreprise est désormais installée ! Désormais, vous êtes en mesure d'installer le rôle ADCS sur Windows Server. La prochaine étape sera la conguration de la CA et le déploiement de vos premiers certi cats, à partir d'un modèle existant ou d'un nouveau modèle personnalisé.

Prêtez une attention particulière aux permissions sur les modèles, car ils peuvent exposer la CA à des risques de compromission.

CONCLUSION FINAL :

Ce TP nous a permis de mettre en pratique les bases de la cryptographie avec OpenSSL. Nous avons travaillé sur le chiffrement symétrique et asymétrique, le hachage, la signature numérique ainsi que sur la gestion des certificats. Ces manipulations nous ont aidés à mieux comprendre comment les données peuvent être protégées et comment sécuriser les échanges.

La mise en place d'une autorité de certification racine sous Windows Server nous a permis de découvrir le fonctionnement d'une infrastructure PKI dans un contexte proche de celui de l'entreprise. La sécurisation d'un serveur web avec SSL/TLS montre concrètement comment ces notions sont utilisées dans le monde professionnel.

Les compétences acquises au cours de ce TP sont très importantes pour un futur administrateur systèmes et réseaux ou pour toute personne travaillant dans la sécurité informatique. Elles permettent d'assurer la confidentialité, l'intégrité et la fiabilité des communications.