

Atelier : Serveur web sécurisé

1. Objectif

Dans l'atelier pratique de ce chapitre, nous allons implémenter un serveur web sécurisé utilisant le protocole SSL. Pour cela notre serveur web devra obtenir un certificat auprès de notre autorité de certification puis le lier au protocole HTTPS. Nous testerons ensuite le fonctionnement du protocole SSL en détail.

Les ordinateurs virtuels utilisés dans cet atelier sont les suivants :

S1 : contrôleur de domaine (Corp.lan)

S2 : autorité de certification (CorpRootCA)

S3 : serveur web du domaine (Corp.lan)

W10 : ordinateur client du domaine (Corp.lan)

2. Créer un serveur web IIS (Internet Information Services) (S3)

Nous allons installer dans un premier temps un serveur web opérationnel sur le serveur s3.

a. Installer le rôle

- Ouvrez la console de gestion Gestionnaire de serveur, développez le menu **Gérer** et sélectionnez le menu **Ajouter des rôles et fonctionnalités**.
- Dans la fenêtre Avant de commencer de l'assistant, cliquez sur le bouton **Suivant**.
- Dans l'assistant Ajout de rôles et de fonctionnalités, dans la fenêtre Sélectionner le type d'installation, sélectionnez **Installation basée sur un rôle ou une fonctionnalité** et cliquez sur le bouton **Suivant**.
- Dans la fenêtre Sélectionner le serveur de destination, sélectionnez **Sélectionner un serveur du pool de serveurs** et sélectionnez le serveur s3.corp.lan.
- Dans la fenêtre Sélectionner des rôles de serveurs, cochez **Serveur Web IIS**.
- Dans la fenêtre Assistant Ajout de rôles et de fonctionnalités, cliquez sur le bouton **Ajouter des fonctionnalités** puis cliquez sur le bouton **Suivant**.
- Dans la fenêtre Sélectionner des fonctionnalités, cliquez sur le bouton **Suivant**.
- Lisez la description de l'écran Rôle Web Server (IIS) et cliquez sur le bouton **Suivant**.
- Dans la fenêtre Sélectionner des services de rôles, cliquez sur le bouton **Suivant**.
- Dans la fenêtre Confirmer les sélections d'installation, validez les éléments qui seront installés puis cliquez sur le bouton **Installer**.
- Attendez que l'installation soit complète puis cliquez sur le bouton **Fermer**.

b. Valider l'installation

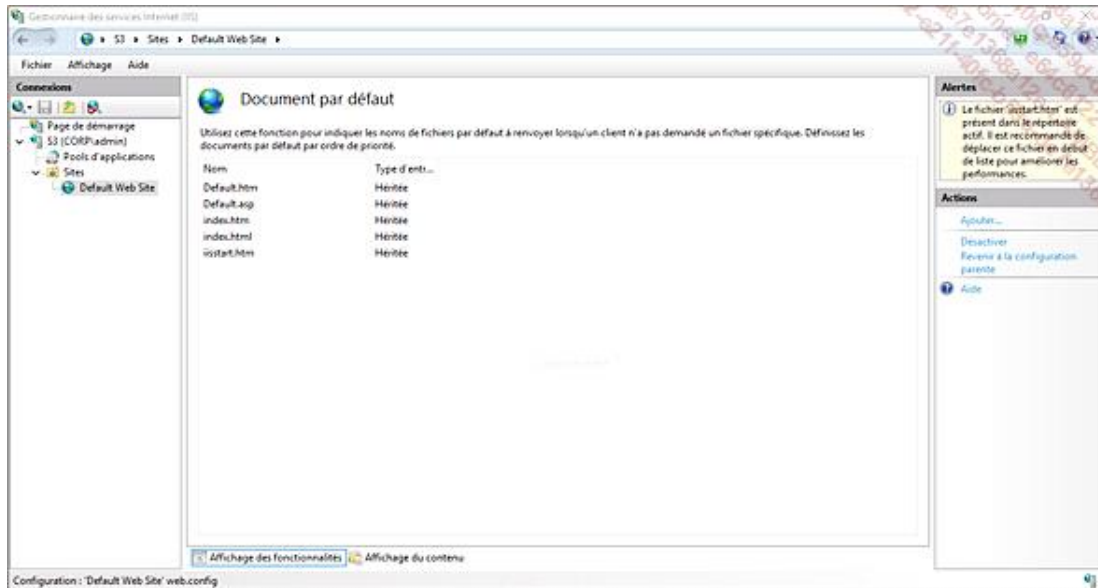
Dans la console de gestion Gestionnaire de serveur, développez le menu **Outils** et sélectionnez **Gestionnaire des services Internet (IIS)**.

La console de gestion Gestionnaire des services Internet (IIS) s'ouvre, profitez-en pour l'épingler à la barre de tâches afin d'éviter de la rechercher à nouveau (menu **Outils** du Gestionnaire de tâche (bouton droit sur l'icône de la console sur la barre de tâches), sélectionnez le menu **Épingler à la barre de tâches**).

- Dans la console Gestionnaire des services Internet (IIS), développez **S3 (Corp\admin)\Sites\Default Web Site**.

Default Web Site correspond au site web créé par défaut lors de l'installation du service IIS.

- Dans la zone centrale, double cliquez sur l'icône **Documents par défaut**.



Les documents par défaut présentés ici sont les premières pages chargées par défaut qui correspondent aux fichiers default.htm, default.asp, index.htm, index.html, iisstart.htm.

c. Créer le document par défaut

- Ouvrez l'explorateur de fichier et développez le disque C:.

Notez l'apparition du nouveau dossier inetpub.

- Créez un nouveau document texte nommé default.htm dans le dossier c:\inetpub\wwwroot.
- Modifiez le document pour ajouter le texte **Site Web de la société CORP** puis enregistrez le document.

Il est maintenant nécessaire de modifier l'extension par défaut .txt en .htm.

- Sélectionnez le menu **Affichage** et cochez **Extensions de noms de fichiers**.
- Supprimez l'extension .txt du document default et remplacez-la par l'extension .htm.

L'icône par défaut du fichier maintenant est remplacée par l'icône Internet Explorer.

d. Tester l'accès au site depuis le navigateur Internet

Créer un nom DNS pour le site

- Sur le contrôleur de domaine s1, ouvrez la console de gestion DNS.
- Développez **s1\Zones de recherche directes\corp.ian**.
- Faites un clic droit sur la zone **corp.ian** et sélectionnez le menu **Nouvel hôte (A ou AAAA)**.
- Dans la fenêtre Nouvel hôte, saisissez **www** dans la zone **Nom** et saisissez **10.0.0.3** dans la zone **Adresse IP**.
- Cliquez sur les trois boutons **Ajouter un hôte**, **OK** et **Terminé**.

Tester la bonne résolution du nom

- Ouvrez une invite de commande PowerShell et exécutez la commande **Ping www.corp.ian**.
- Validez que la résolution s'effectue bien en 10.0.0.3.

Tester l'accès au site depuis le navigateur Internet en saisissant l'URL www.corp.ian

- Ouvrez le navigateur Internet Explorer.
- Dans la zone d'adresse, saisissez **www.corp.ian** et validez.

S'il s'agit de la première utilisation du navigateur, un message s'affiche dans la fenêtre Installer Internet Explorer 11. Dans ce cas, acceptez les paramètres par défaut et cliquez sur le bouton **OK**.

- Validez l'accès au site par défaut (le texte **Site Web de la société CORP** s'affiche).

3. Sécuriser l'accès au site avec SSL

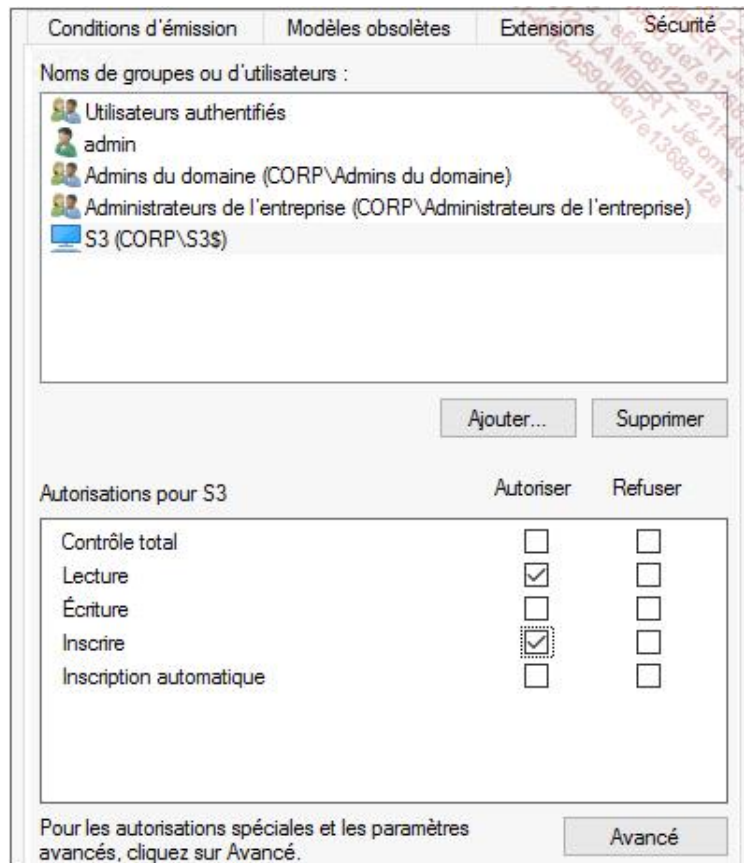
a. Obtenir un certificat pour le serveur web

Créer un modèle serveur web personnalisé

- Ouvrez la console de gestion Autorité de certification.
- Développez CorpRootEntCA.
- Faites un clic droit sur **Modèles de certificats** et sélectionnez le menu **Gérer**.

La console de gestion Modèles de certificats s'affiche.

- Faites un clic droit sur le modèle **Serveur Web** et sélectionnez le menu **Dupliquer le modèle**.
- Sélectionnez l'onglet **Compatibilité**, développez la liste déroulante **Autorité de certification**, sélectionnez **Windows Server 2016** et cliquez le bouton **OK** pour accepter les modifications résultantes.
- Développez la liste déroulante **Destinataire du certificat**, sélectionnez **Windows 10 / Windows Server 2016** et cliquez sur le bouton **OK** pour accepter les modifications résultantes.
- Sélectionnez l'onglet **Général**, saisissez **Corp Serveur Web** dans la zone **Nom complet du modèle**.
- Sélectionnez l'onglet **Sécurité**, cliquez sur le bouton **Ajoutez**, cliquez sur le bouton **Types d'objets** et cochez **Des ordinateurs** puis cliquez sur le bouton **OK**.
- Saisissez **s3**, cliquez sur le bouton **Vérifier les noms** puis sur le bouton **OK**.



Ici les autorisations permettant l'inscription du certificat sont attribuées à un compte d'ordinateur !

→ Cliquez sur le bouton **OK** et fermez la fenêtre de gestion Modèles de certificats.

Publier le nouveau modèle de certificat

- Dans la fenêtre Autorité de certification, faites un clic droit sur **Modèles de certificats** et sélectionnez les menus **Nouveau\Modèle de certificat à délivrer**.
- Dans la fenêtre Activer les modèles de certificats, sélectionnez le modèle de certificat **Corp Serveur Web** et cliquez sur le bouton **OK**.

Le nouveau modèle de certificat peut maintenant être distribué par l'autorité de certification.

Inscrire le certificat

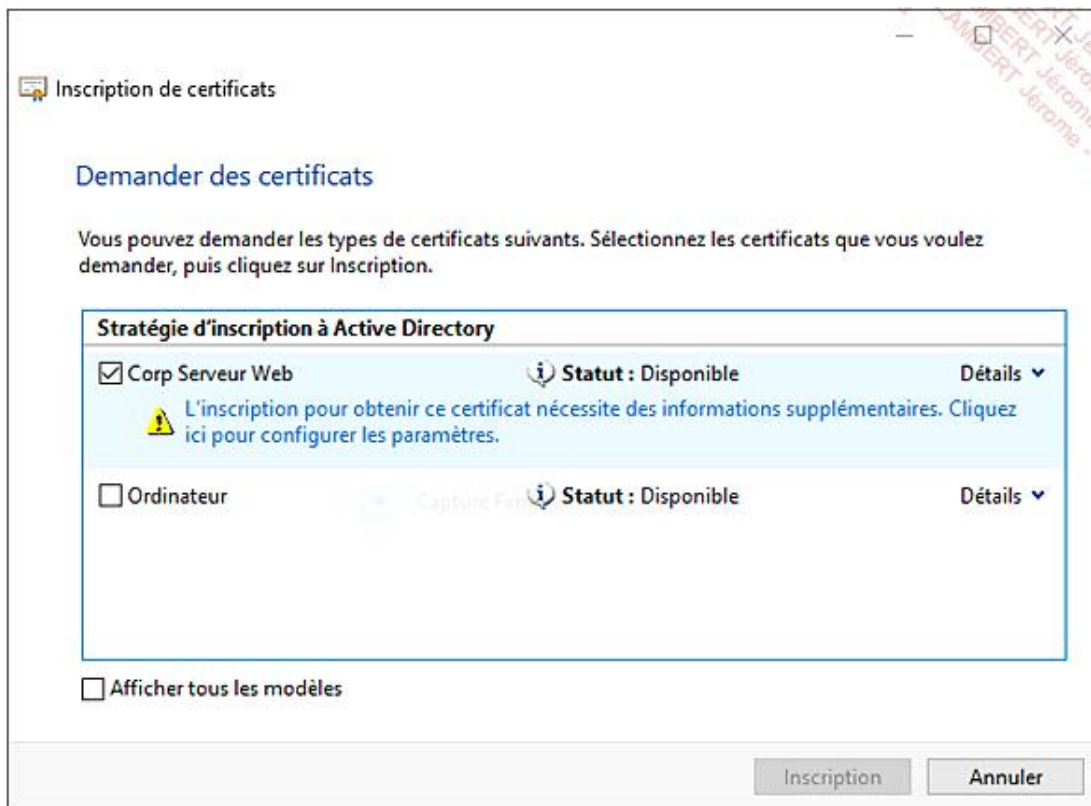
- Connectez-vous en tant que Corp/Admin sur le serveur s3.
- Ouvrez une invite de commande PowerShell et exécutez la commande `certlm.msc`.

Comme il s'agit d'inscrire un certificat pour un ordinateur (et non pas pour un utilisateur), la console utilisée ici pour inscrire le certificat est la console Certificat - Ordinateur local.

- Développez **Certificats-Ordinateur\Autorités de certifications de racines de confiance\Certificats** et validez la présence du certificat de l'autorité de certification CorpRootCA.

Si le certificat de l'autorité de certification CorpRootCA n'apparaît pas, exécuter la commande `certutil -pulse` ou redémarrez l'ordinateur et vérifiez à nouveau la présence du certificat.

- Dans la console Certificats-Ordinateur Actuel, faites un clic droit sur le dossier Personnel et sélectionnez les menus **Toutes les tâches et Demander un nouveau certificat**.
- Dans l'assistant Inscription de certificats, dans la fenêtre Avant de commencer, lisez les recommandations puis cliquez sur le bouton **Suivant**.
- Dans la fenêtre Sélectionner la stratégie d'inscription de certificat, validez que la sélection par défaut est bien **Stratégie d'inscription à Active Directory** puis cliquez sur le bouton **Suivant**.
- Dans la fenêtre Demander des certificats, cochez le modèle **Corp Serveur Web**.
- Cliquez sur le lien **L'inscription pour obtenir ce certificat nécessite des informations supplémentaires. Cliquez ici pour configurer les paramètres**.



➔ Des informations supplémentaires sont nécessaires pour former le nom du sujet du certificat !

- Dans l'onglet **Objet**, dans la zone **Nom du sujet**, développez la liste déroulante **Type** et sélectionnez **Nom commun**.
- Dans la zone **Valeur**, saisissez **www.corp.lan**.

Propriétés du certificat

Objet Général Extensions Clé privée Autorité de certification Signature

Le sujet d'un certificat est l'utilisateur ou l'ordinateur vers lequel le certificat est émis. Vous pouvez entrer des informations sur les types de noms de sujet et d'autres noms qui peuvent être utilisés dans un certificat.

Sujet du certificat
L'utilisateur ou l'ordinateur qui reçoit le certificat

Nom du sujet :

Type :
Nom commun

Valeur :
www.corp.lan

Ajouter >

< Supprimer

Autre nom :

Type :
Nom de répertoire

Valeur :

Ajouter >

< Supprimer

OK Annuler Appliquer

Il est fondamental ici que le nom commun corresponde à l'URL avec laquelle nous nous connecterons au site web (www.corp.lan) !

- Cliquez sur le bouton **Ajouter**.
- Sélectionnez l'onglet **Général**, dans la zone **Nom convivial** saisissez **Certificat SSL pour s3** et dans la zone **Description** saisissez **Certificat SSL pour le serveur Web de Corp**.

Propriétés du certificat

Objet Général Extensions Clé privée Autorité de certification Signature

Un nom convivial et une description facilitent l'identification et l'utilisation d'un certificat.

Nom convivial :
Certificat SSL pour S3

Description :
Certificat SSL pour le serveur Web de Corp

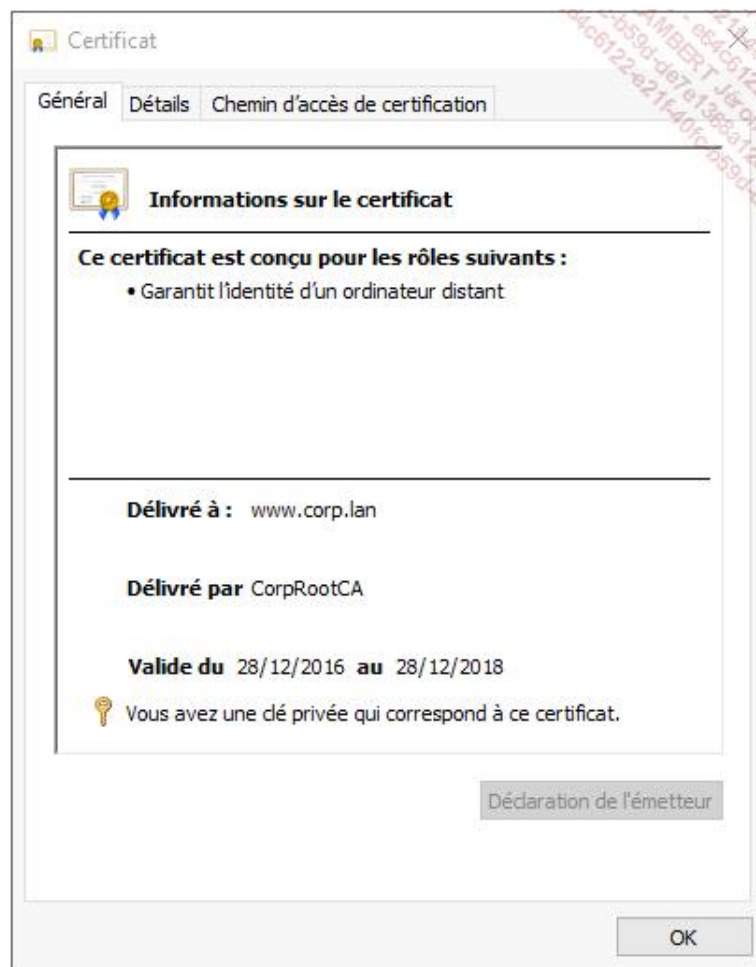
OK Annuler Appliquer

➤ L'ajout d'un nom convivial, même si cela n'est aucunement obligatoire, permet par la suite de repérer plus facilement un certificat.

- Cliquez sur les trois boutons **OK**, **Inscription** et **Terminer**.
- Validez l'inscription du certificat.

Valider les informations du certificat

- Double cliquez sur le certificat obtenu.
- Dans l'onglet **Général**, validez que le certificat est délivré à **www.corp.lan** par l'autorité de certification **CorpRootCA**.
- Sélectionnez l'onglet **Détails**, validez la présence du champ **Clé publique** et validez que le champ **Nom convivial** correspond bien à la valeur **Certificat SSL pour s3**.
- Sélectionnez l'onglet **Chemin d'accès de certification** et validez que le certificat est bien délivré par l'autorité de certification **CorpRootCA**.



Le certificat est bien délivré au site www.corp.lan par l'autorité de certification CorpRootCA.

b. Lier le certificat avec le service IIS

Nous allons maintenant lier le certificat SSL obtenu avec l'appliquatif IIS.

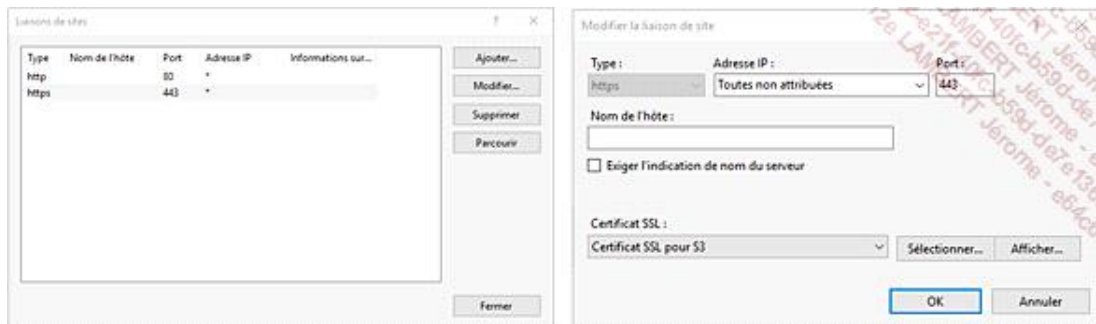
Lier le certificat SSL

- Ouvrez la console Gestionnaire des services Internet (IIS), développez **S3 (Corp\admin)**.
- Dans la partie centrale de la console, double cliquez sur l'icône **Certificats de serveur**.
- Validez la présence du certificat obtenu (le certificat est affiché avec son nom convivial).

- Dans la partie gauche de la console, développez **S3 (Corp\admin)\Sites**.
- Faites un clic droit sur **Default Web Site** et sélectionnez le menu **Modifier les liaisons**.
- Dans la fenêtre Liaisons de sites, cliquez sur le bouton **Ajouter**.
- Dans la fenêtre Ajouter la liaison de site, développez la liste déroulante **Type** et sélectionnez **https**.

Notez que la zone indiquant le port utilisé passe à la valeur 443 qui est le port par défaut du protocole SSL !

- Développez la liste déroulante **Certificat SSL** et sélectionnez le certificat précédemment obtenu (**Certificat SSL pour S3**).
- Cliquez sur les boutons **OK** et **Fermer**.



Le service IIS est maintenant lié au port 443 (HTTPS) grâce au certificat ordinateur obtenu.

Exiger une connexion sécurisée

- Connectez-vous sur le client w10 en tant Corp/Admin.
- Ouvrez le navigateur Internet Explorer 11 (depuis le menu **Accessoires Windows** du menu Windows).

Le navigateur Edge n'offre pas les mêmes informations.

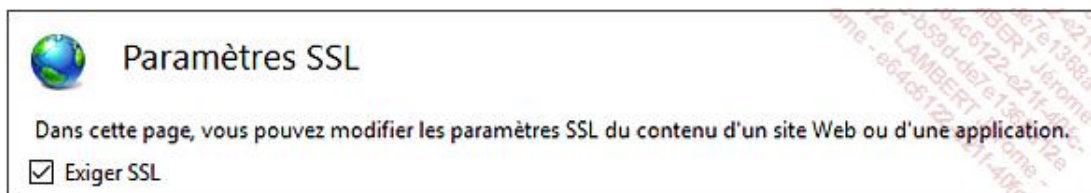
- Dans la zone d'adresse, saisissez **www.corp.ian** et validez.

S'il s'agit de la première utilisation du navigateur, un message s'affiche dans la fenêtre Installer Internet Explorer 11. Dans ce cas, acceptez les paramètres par défaut et cliquez le bouton **OK**.

- Validez l'accès au site par défaut avec l'URL **http://www.corp.ian**.

La connexion au site en HTTP (non sécurisée) reste fonctionnelle. Le site s'affiche.

- Dans la console Gestionnaire des services Internet (IIS), développez **S3 (Corp\admin)\Sites\DefaultWebSite**.
- Dans la partie centrale de la console, double cliquez sur l'icône **Paramètres SSL**.
- Dans la fenêtre Paramètres SSL, cochez **Exiger SSL**.
- Dans le volet **Actions** (volet de droite de la console), cliquez sur **Appliquer**.
- Validez l'apparition du message **Les modifications ont été correctement enregistrées**.
- Sur le client w10, essayez de vous connecter au site de façon non sécurisée avec l'URL **http://www.corp.ian** et validez que ce n'est plus autorisé (erreur 403).



➔ Forcer SSL permet d'interdire toute connexion non sécurisée au site (HTTP).

4. Valider la connexion SSL

➔ Sur le client w10, connectez-vous au site de façon sécurisée avec l'URL <https://www.corp.lan/> et validez l'accès au site.

Un cadenas apparaît après la zone de saisie de l'URL.

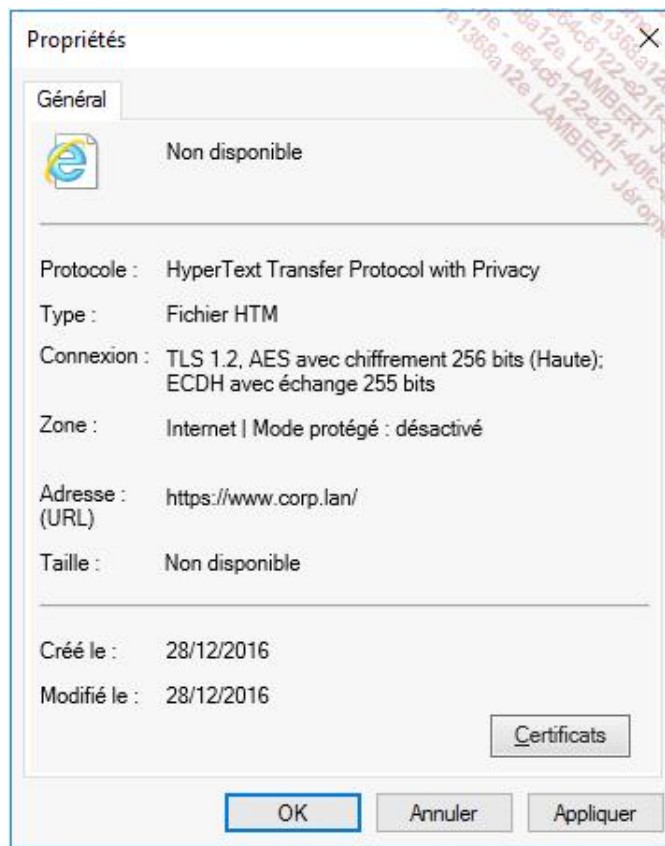
➔ Cliquez sur le cadenas affiché dans la zone de saisie puis cliquez sur le lien **Afficher les certificats**.

➔ Validez que le certificat présenté correspond bien à celui du site www.corp.lan.



➔ Faites un clic droit sur le fond blanc de la page web et sélectionnez le menu **Propriétés**.

➔ Validez que, dans la zone **Connexion**, la connexion est bien chiffrée en AES.



Les propriétés de la page web indiquent que la connexion est chiffrée en AES avec une taille de clé de chiffrement symétrique de 256 bits.

5. Tester les erreurs de connexion sécurisée au site web

Dans cette partie de l'atelier, nous allons tester les différents types d'erreurs de connexion au site sécurisé afin de mieux comprendre et savoir corriger ces erreurs.

a. Navigation SSL avec URL incorrecte

→ Essayez de vous connecter au site avec l'URL `https://10.0.0.3`.

Un message indique une erreur de certificat. En effet, le sujet du certificat (`www.corp.lan`) ne correspond pas à l'adresse saisie (`10.0.0.3`).

→ Cliquez sur le lien **Poursuivre avec ce site Web (non recommandé)** et validez l'accès au site web (la zone d'adresse est en fond rouge).



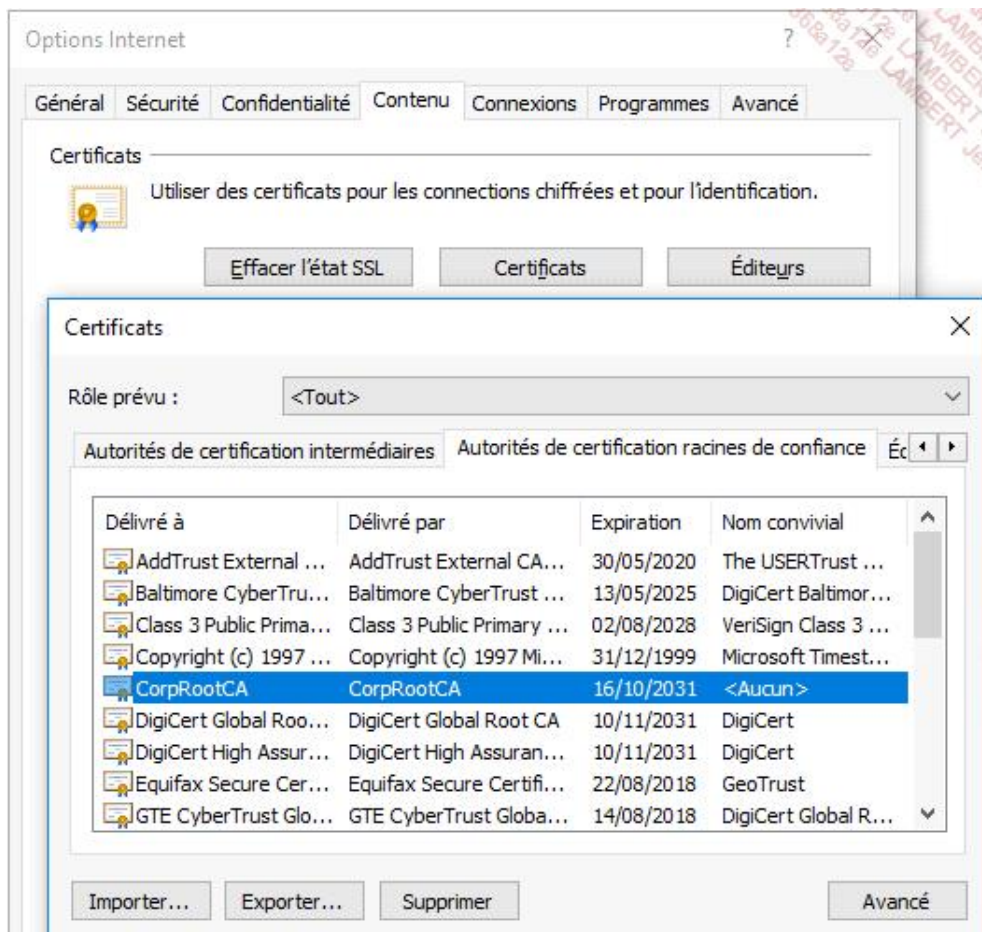
Le navigateur indique une erreur de certificat. Il est possible de poursuivre mais nous pourrions alors nous exposer à une menace d'hameçonnage (Phishing).

b. Navigation SSL sans certificat d'autorité de certification

→ Ouvrez la console de gestion des certificats de l'ordinateur en exécutant la commande :

```
certlm.msc
```

- Développez **Certificats-Ordinateur local\Autorités de certification racines de confiance\Certificats**.
- Validez la présence de l'autorité de certification CorpRootCA.
- Cliquez sur le bouton **Options du navigateur** (l'icône représentant une roue dentée à droite) et sélectionnez le menu **Options Internet**.
- Sélectionnez l'onglet **Contenu** et cliquez sur le bouton **Certificats**.
- Dans la fenêtre Certificats, sélectionnez l'onglet **Autorités de certification racines de confiance**.
- Sélectionnez le certificat de l'autorité de certification CorpRootCA puis cliquez sur le bouton **Supprimer**.
- Lisez le message d'avertissement de la fenêtre Certificats et confirmez la suppression en cliquant sur le bouton **OK**.
- Cliquez sur les boutons **OK** et **Fermer**.



Les certificats des autorités racines de confiance publiques et privées sont également visibles dans les propriétés du navigateur.

- Validez la suppression de l'autorité de certification CorpRootCA dans le conteneur **Autorités de certification racines de confiance\Certificats** de la console de gestion des certificats de l'ordinateur.
- Fermez et ouvrez à nouveau le navigateur Internet Explorer 11.
- Essayez à nouveau une connexion au site web avec l'URL <https://www.corp.lan>.

Une erreur est renvoyée. Le navigateur ne dispose plus du certificat de l'autorité de certification CorpRootCA pour valider l'authenticité du certificat présenté.

- Cliquez sur le lien **Poursuivre avec ce site Web (non recommandé)** et validez l'accès au site web (la zone d'adresse est en fond rouge).



Ici, l'URL saisie est correcte, mais il manque le certificat de l'autorité de certification dans le magasin local de l'ordinateur local.

6. Révoquer les certificats de serveurs web

Pour la réalisation de cet atelier, reportez-vous aux ateliers du chapitre Révocation de certificat dans l'entreprise (section Révocation d'un certificat de site web).

- Si vous souhaitez reporter cet atelier de révocation, effectuez un point de contrôle (nommé **SitesWebSécurisé**) sur tous les ordinateurs virtuels afin de pouvoir restaurer cet environnement lorsque vous réaliserez l'atelier.