0. Installation Open-Prod

Procédures internes pour l'installation d'Open-Prod

Sécuriser votre installation avec HTTPS

Importance de la sécurisation https pour Open-Prod et procédures de mise en oeuvre

0. HTTPS et les types de certificats

Par défaut, votre installation d'Open-Prod 10 est disponible sur le port **8069** (8068 pour Open-Prod 9). Si votre installation est prévue pour un accès public, ou pour être déployée dans un environnement sensible, il est fortement recommandé de sécuriser son accès web avec le protocole HTTPS (HTTP + TLS/SSL). C'est ce protocole qui vous permet de garantir des échanges de données sécurisés entre les utilisateurs et votre serveur, en les chiffrant via un échange de clés et des informations de certificat. De cette manière les données échangées ne peuvent être ni lues, ni altérées par un tiers pendant leur transit sur le réseau.

> Si vous souhaitez utiliser Open-Prod sur un terminal mobile (Zebra, Android, iOS, etc.) en version PWA (Progressive Web Apps), **l'utilisation d'HTTPS est obligatoire**.

Rappel :

L'utilisation d'HTTPS repose sur l'échange d'un certificat entre le serveur et le client. Ce certificat contient notamment une clé publique et des informations sur l'identité du serveur, afin de garantir son authenticité. Chaque certificat doit être signé par une autorité de certification, qui peut être votre serveur, un serveur de votre infrastructure (AD CS), ou une entité externe comme Let's Encrypt, Sectigo, Digicert, etc. Il existe donc deux grands types de certificats :

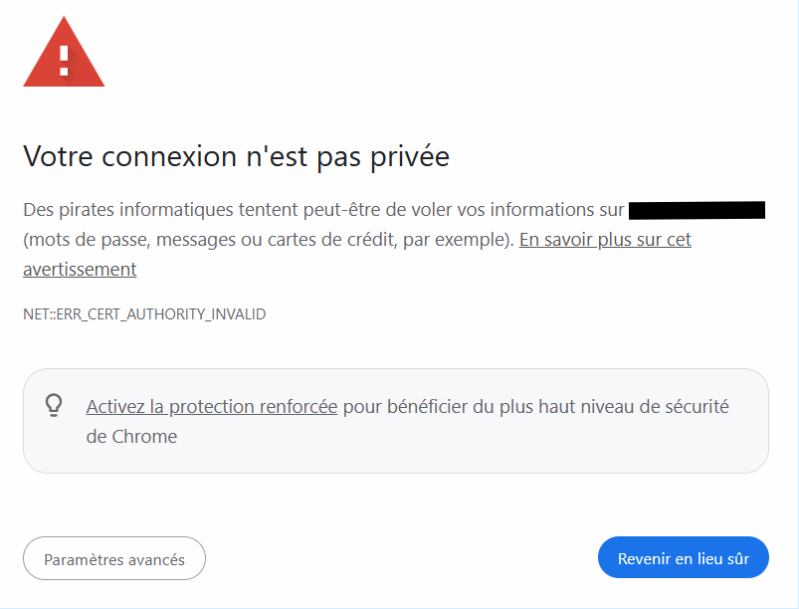
1. Auto-signés : Le certificat est signé par une autorité de certification interne de confiance *(fourni par défaut par 1Life)*

2. Signés : Vous signez le certificat par une entité externe de confiance

1. Certificats auto-signés

Un certificat auto-signé est gratuit. Aucune étape intermédiaire est nécessaire pour qu'il soit valide. Cependant pour que le client puisse valider l'authenticité du serveur, le certificat auto-signé doit être également déployé sur les postes client. Vous avez donc pour ce type de certificat, un déploiement en deux temps, automatisé ou manuel :

1. Génération de la paire de clés, génération du certificat et signature par la CA
2. Déploiement du certificat sur les postes clients, manuellement, via GPO ou via un AD CS local

> Le déploiement du certificat sur les postes clients vous permet aussi de vous affranchir de l'alerte de sécurité sur votre navigateur :
>
> 
>

> Par défaut, Open-Prod est livré avec un certificat auto-signé d'une durée de validité de 10 ans. Ce certificat est présenté aux clients par Nginx, configuré en reverse proxy et installé automatiquement lors du déploiement.

2. Certificats signés

Un certificat signé est considéré en tant que tel lorsqu'il est signé par un organisme externe **publiquement reconnu**. Il est gratuit ou payant en fonction de l'autorité de certification choisie (CA : Certificate Authority).

Si vous optez pour le choix payant, vous devrez acheter votre certificat auprès d'un registrar ou d'un fournisseur tiers. En fonction du registrar ou du fournisseur tiers, vous serez soumis à une DCV (Domain Control Validation) qui nécessite l'exposition d'une de ces ressources les plus fréquentes :

- Enregistrement DNS public (TXT, CNAME)
- URL accessible publiquement
- Adresse mail de validation
- Numéro de téléphone de votre société

Vous devrez également avoir une requête de signature de certificat (CSR) déjà prête pour pouvoir entamer vos démarches.

> 1Life vous simplifie la génération d'une CSR en mettant à disposition l'outil **MyHelp** et sa commande `https-config`

Si vous optez pour le choix gratuit, comme Let's Encrypt ou ZeroSSL, vous serez également soumis à une DCV qui nécessite une URL accessible publiquement par l'API de l'autorité de certification. Pour un accès à votre installation d'Open-Prod via un nom de domaine (Exemple : https://openprod.masociété.com) vous devrez en amont avoir un enregistrement DNS sur votre domaine local.

3. Configuration

La sécurisation de votre environnement avec HTTPS est simplifié grâce à l'outil MyHelp. Sa commande `https-config` couvre chacun des cas de figure évoqués précédemment (auto-signé, certificat signé gratuit ou payant). Vous trouverez les détails de son utilisation dans les pages de cette catégorie.

> Cette commande est applicable aussi bien sur Open-Prod 9 qu'Open-Prod 10

Les équipes du support technique 1Life sont également là pour vous accompagner si besoin au travers de votre contrat de TMA.

4. Récapitulatif des différents modes de certification

Type de certificat	Coût	Validité	Accès public	Déploiement sur les postes clients	DCV

Autosigné	Gratuit ✔	Étendue	✘	✔	✘
Signé - Gratuit	Gratuit ✔	45 à 90 jours	✔	✘	✔
Signé - Payant	Payant ⚠	1 à 3 ans	✔	✘	✔

1. HTTPS avec certificat auto-signé

Dans cette section, vous verrez comment installer pas à pas un certificat autosigné grâce à l'outil MyHelp en ligne de commande. Vous devrez au préalable :

- Intégrer le serveur Open-Prod dans son réseau interne en s’assurant de la bonne résolution du nom de la machine sur son réseau local (nom de machine fixée et IP statique en place, DNS fonctionnel)
- Vérifier que le serveur Open-Prod n’est pas en production lors de la procédure. Prévoir également de communiquer la nouvelle URL de connexion à l’ensemble des utilisateurs une fois la procédure terminée.

Présentation :

La commande `https-config` de l'outil MyHelp intègre les fonctionnalités suivantes :

- Installer Nginx en Reverse Proxy sur le port 443 (HTTPS)
- Générer un certificat autosigné
- Générer une CSR
- Importer un certificat signé
- Configurer Nginx :
  - Changer le chemin d'accès du certificat utilisé
  - Changer le chemin d'accès de la clé privée utilisée
  - Editer le fichier de configuration en direct
- Partager le certificat autosigné ou la CSR (dossier local / partagé)
- Supprimer l'installation de Nginx et les fichiers générés

> **Attention :** si vous utilisez le service Apache (pour l’outil pgadmin version web par exemple) l'installation va désactiver Apache. En effet Nginx est incompatible avec la présence du service Apache sur le même port d'écoute (TCP : 443). Vous pouvez remplacer le service pgadmin web par son utilisation via un client distant.

Etape 1 - Installation d'Nginx :

```
openprod@srvopp-jlv9t01:~ $ https-config
Etat de l'installation de Nginx: Desinstallé
Etat de Nginx : Inactif

==== INSTALLATION NGINX & HTTPS ====

1. Installer / Réinstaller Nginx avec la configuration minimale
2. Installer Nginx et configurer HTTPS
3. Gérer les certificats SSL/TLS

Entrez votre choix [1/2/3] : 2
Désactivation d'Apache...
Installation en cours...
```

Lancer la commande `https-config`. Le script vérifie la présence ou non d'Apache et Nginx pour préparer le déploiement. Sélectionner l'option 2 pour lancer l'installation et configurer le certificat auto-signé. Une fois l'installation d'Nginx terminée, vous obtiendrez les modes de certification suivants :

```
==== MODE DE CERTIFICATION ====

1. Générer un certificat auto-signé
2. Générer une CSR (Certificate Signing Request)
3. Importer un certificat signé par une CA reconnue

Votre choix [1/2/3] : 1
Saisie des informations du certificat :
Common Name (CN) [défaut: srvopp-jlv9t01]:
Subject Alternative Names (SAN) [défaut: DNS:srvopp-jlv9t01,IP:192.168.70.67]:
Organisation (O) [défaut: Openprod]:
Saisir les champs optionnels (OU, L, ST, C) ?
appuyez sur la touche O pour "Oui" ou sur la touche N pour "Non" :
n

==== Récapitulatif ====
CN  : srvopp-jlv9t01
O   : Openprod
SAN : DNS:srvopp-jlv9t01,IP:192.168.70.67
======================

Confirmer ?
appuyez sur la touche O pour "Oui" ou sur la touche N pour "Non" :
```

Utiliser la première option et répondre aux questions sur les caractéristiques du certificat auto-signé :

- Common Name (CN) : voir ci-dessous la valeur SAN. Par défaut mettre ou laisser la même valeur que le champ SAN (normalement le SAN est prioritaire)
- Subject Alternative Name (SAN) : mettre obligatoirement le nom réseau de cette machine sur le domaine ainsi que son adresse IP fixe. Ces informations sont essentielles pour intégrer manuellement ou via GPO le certificat sur chaque poste (Si besoin, modifier ces informations en utilisant la syntaxe précise : DNS:[nom environnement], IP:[adresse IP environnement],
- Organisation (O) : par défaut laisser Open-Prod (pas d'impact de ce paramètre sur le fonctionnement du https),

- Champs optionnels (OU, L, ST, C) : par défaut laisser vide (pas d'impact de ce paramètre sur le fonctionnement du https).

NOTA : Les champs O, OU, L, ST, C sont surtout utilisés dans les **certificats EV/OV** ou en interne (**PKI entreprise**). Ils ne sont normalement pas importants pour un simple certificat auto-signé.

Confirmer ensuite la génération du certificat par Oui en tapant `o` :

```
==== MODE DE CERTIFICATION ====

1. Générer un certificat auto-signé
2. Générer une CSR (Certificate Signing Request)
3. Importer un certificat signé par une CA reconnue

Votre choix [1/2/3] : 1
Saisie des informations du certificat :
Common Name (CN) [défaut: srvopp-jlv9t01]:
Subject Alternative Names (SAN) [défaut: DNS:srvopp-jlv9t01,IP:192.168.70.67]:
Organisation (O) [défaut: Openprod]:
Saisir les champs optionnels (OU, L, ST, C) ?
appuyez sur la touche O pour "Oui" ou sur la touche N pour "Non" :
n

==== Récapitulatif ====
CN  : srvopp-jlv9t01
O   : Openprod
SAN : DNS:srvopp-jlv9t01,IP:192.168.70.67
======================

Confirmer ?
appuyez sur la touche O pour "Oui" ou sur la touche N pour "Non" :
```

Choisir ensuite d'exporter le certificat dans un dossier local au serveur Linux avec partage Windows (ou non) de ce dossier. Le certificat peut ainsi être récupéré directement via le voisinage réseau depuis son poste Windows si le dossier est partagé. Sinon il est toujours possible de le récupérer depuis son navigateur après s'être connecté en Https sur le serveur Open-Prod (voir § suivant sur l'installation du certificat client).

Indiquer le chemin et nom du dossier de stockage du certificat, le nom de partage du dossier si besoin, sinon laisser par défaut.

Indiquer l'utilisateur autorisé à se connecter s'il y a un partage réseau du dossier (laisser sinon par défaut l'utilisateur connecté).

Indiquer le mot de passe pour accéder à ce partage réseau (obligatoire si le dossier est partagé). Nota : ce mot de passe est propre au partage réseau. Il n'est pas lié au mot de passe de session du compte utilisé.

```
PASS - Certificat TLS généré avec succès (CN=srvopp-jlv9t01)

==== EXPORT DES FICHIERS DE CERTIFICAT (.crt ou .csr) ====

1. Exporter dans un dossier local
2. Exporter dans un dossier de partage réseau (Samba)

Votre choix [1/2, défaut: 1] : 2
Répertoire à partager [défaut: /srv/share/certificates] :
Nom du partage réseau [défaut: certificates] :
mkdir: cannot create directory '/srv/share/certificates': Permission denied
Création du dossier de partage avec l'utilisateur courrant : openprod
Vérification de l'installation de Samba...
INFO - L'utilisateur Samba 'openprod' existe déjà.
Voulez-vous redéfinir le mot de passe de cet utilisateur ?
appuyez sur la touche O pour "Oui" ou sur la touche N pour "Non" :
o
New SMB password:
                Retype new SMB password:
                                        INFO - Partage Samba "certificates" déjà présent

Partage réseau configuré.
Accès Windows  : \\192.168.70.67\certificates
Accès Linux    : smb://192.168.70.67/certificates
Les fichiers seront exportés dans : /srv/share/certificates
Utilisateur Samba : openprod
Certificat pour les postes clients : /srv/share/certificates/deploy.crt
PASS - Installation de Nginx avec HTTPS terminée
```

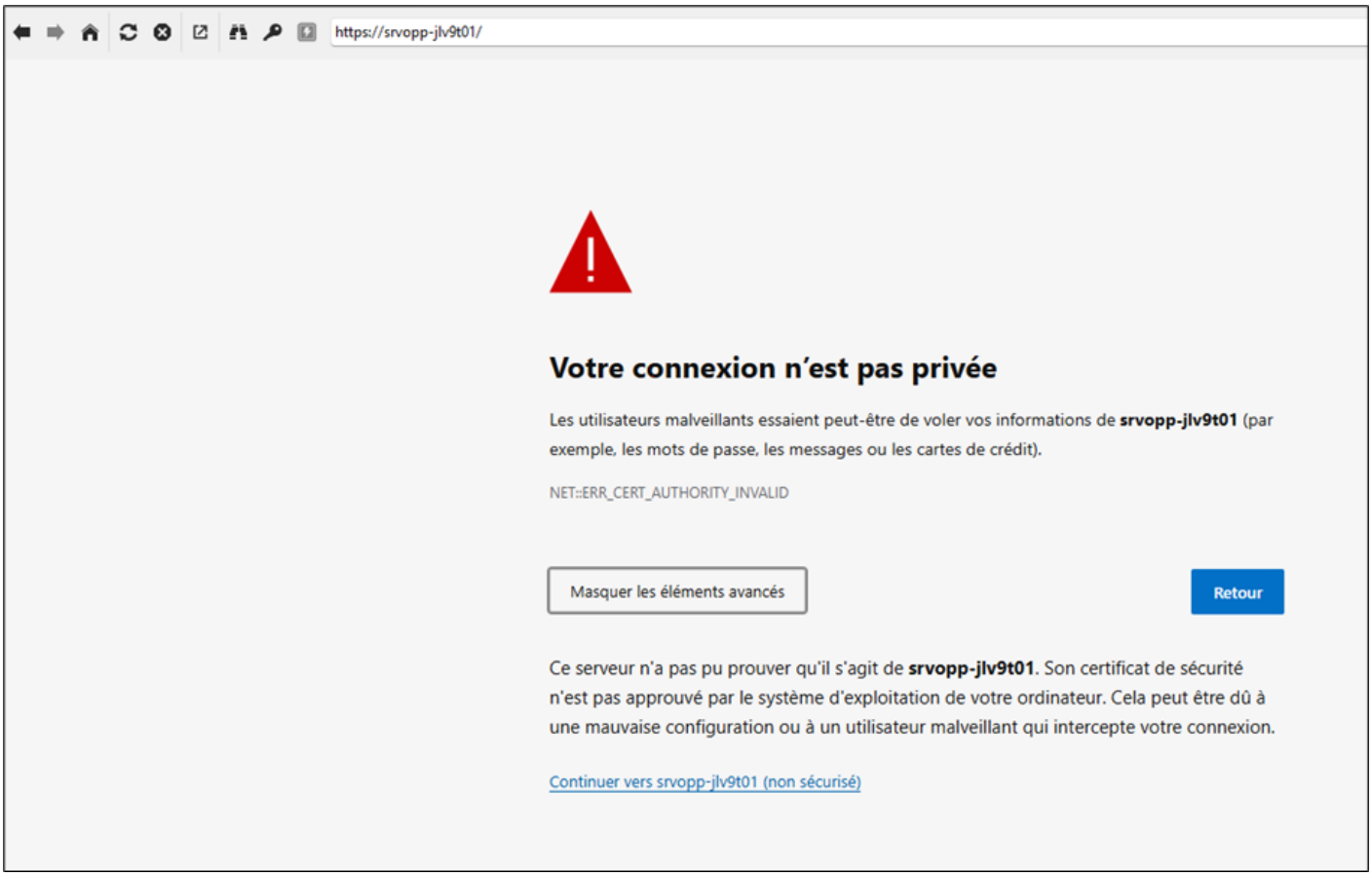
L'installation du Https pour Open-Prod en certificat auto-signé est maintenant terminée. Le service est disponible en se connectant sur https://[nom_de_machine_ou_IP] au lieu de http://[nom_de_machine_ou_IP:806(8/9)].

> SI jamais le processus ne va pas jusqu'au bout, sortir de la commande en cours (Ctrl + C). Relancer le script `https-config`. Une nouvelle option N°4 doit apparaitre et permet de désinstaller complètement Nginx, les composants associés et le certificat. Relancer ensuite une nouvelle installation avec l'option N° 2 en suivant à nouveau les instructions ci-dessus.

```
openprod@srvopp-jlv9t01:~ $ https-config
[sudo] password for openprod:
Etat de l'installation de Nginx: Installé
Etat de Nginx : Actif

==== INSTALLATION NGINX & HTTPS ====

1. Installer / Réinstaller Nginx avec la configuration minimale
2. Installer Nginx et configurer HTTPS
3. Gérer les certificats SSL/TLS
4. Désinstaller complètement Nginx et ses composants associés
5. Modifier la configuration de Nginx

Entrez votre choix [1/2/3/4/5] : 4
```

Etape 3 :

Par défaut l'accès Https est maintenant disponible pour tous les utilisateurs. La connexion à Open-Prod affiche une alerte de sécurité dans le navigateur pour indiquer à l'utilisateur que le certificat installé est propre à une structure interne de votre réseau et ne peut pas être reconnu par une autorité de certification externe (serveur de certification sur le web).



Cliquer dans votre navigateur sur « Paramètre avancé » puis sur « Continuer vers [nom_de_votre_environnement] (non sécurisé). L'accès est maintenant sécurisé au travers de https et tous les flux d'échange est crypté.

> Obligatoire : pour finaliser le déploiement du https et terminer la sécurisation de l'accès au service vous devez interdire l'accès au service Open-Prod au travers du service http sur les url http://[nom_de_machine_ou_ip]:8068 pour la V9 ou http://[nom_de_machine_ou_ip]:8069 pour la V10. Cette interdiction est à faire directement sur le boitier de sécurité réseau d'entreprise ou par filtrage d'URL directement sur l'environnement Linux (ufw par exemple) ou les services réseau de votre hyperviseur (cas d'une machine virtuelle locale ou hébergée). Consulter votre administrateur système pour cette mise oeuvre.

Etape 4 :

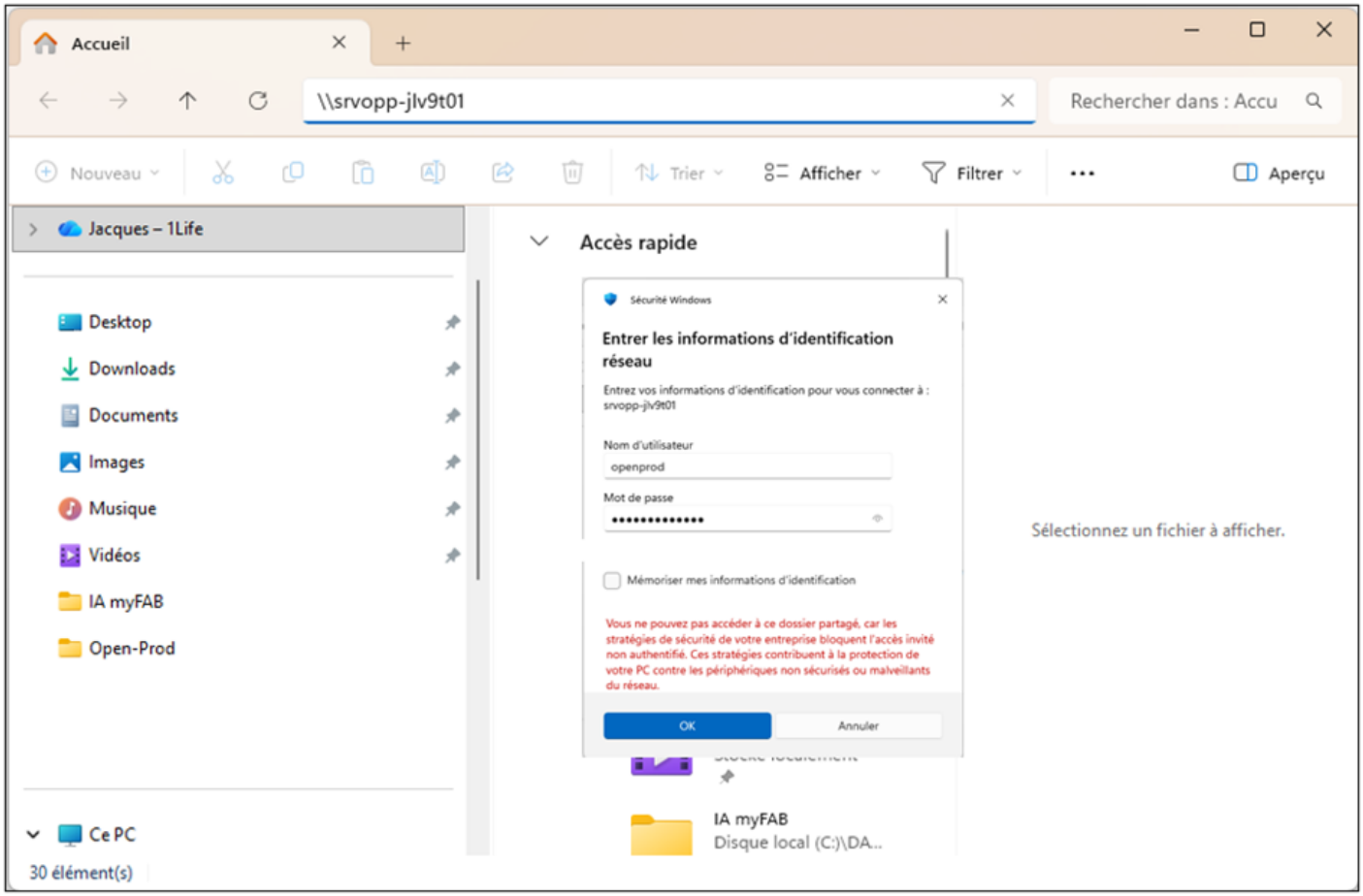
Suppression de l'alerte de sécurité dans le navigateur par intégration manuelle du certificact

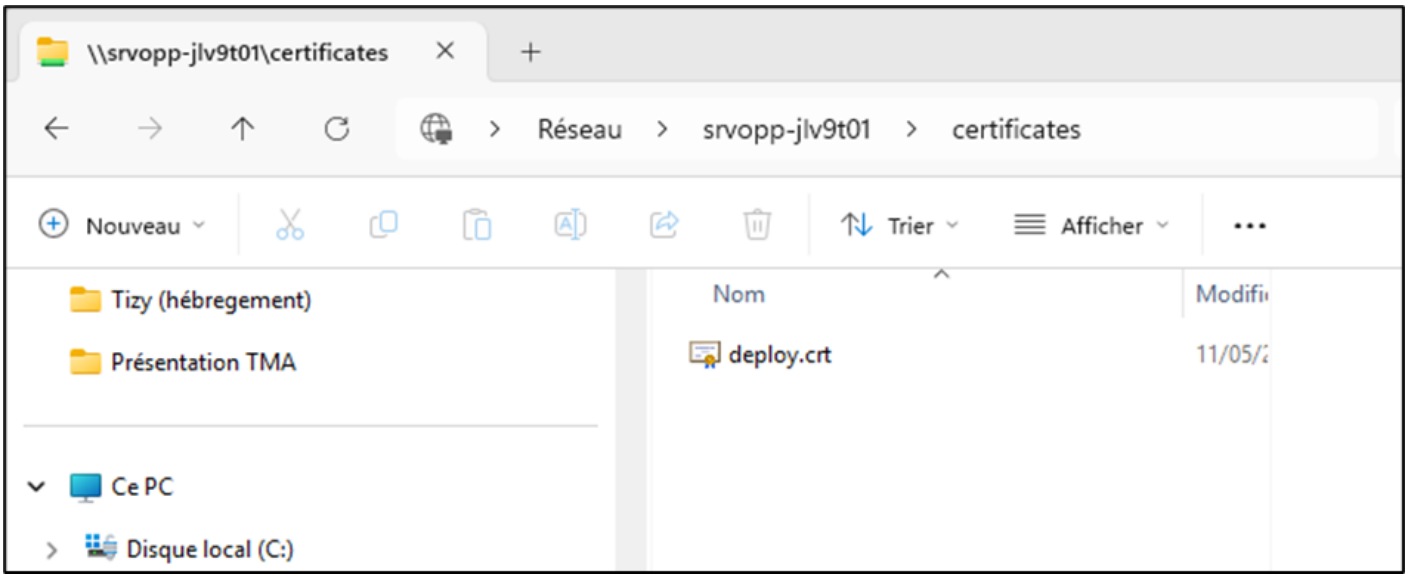
> Les opérations décrites ci-dessous sont présentées à titre informatif. Se rapprocher de son adminsutrateur système et réseau pour en adapter leur mise en oeuvre aux caractéristiques du système et réseau de chaque entreprise.

Si on ne souhaite pas visualiser l'alerte de sécurité dans le navigateur il faut installer le certificat https auto-signé manuellement ou automatiquement (via automatisme PGO d'un domaine Windows par exemple) sur chaque poste client qui utilise Open-Prod.

Pour cela, récupérer le certificat auto-signé sur le serveur Open-Prod :

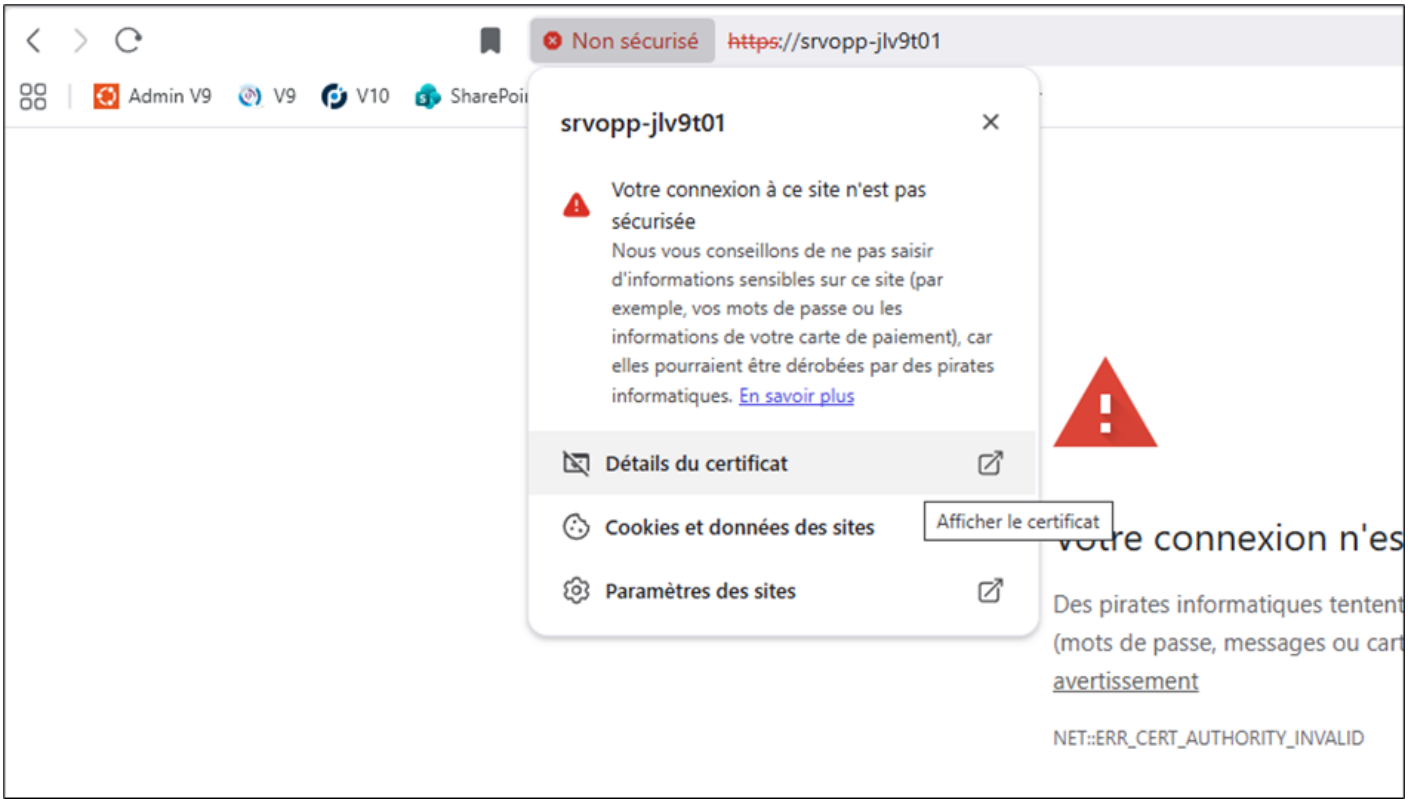
- Via le protocol SCP (Secure Copy Protocol) par exemple si le certificat est dans le dossier du serveur Linux et qu'aucun partage réseau n'a été créé.
- Via le dossier partagé créé lors de la génération du certificat. Utiliser depuis un poste Windows le voisinage réseau pour se connecter sur le serveur Open-Prod (via son IP ou son nom sur le domaine). S'identifier ensuite avec le user / password de partage réseau créé lors de la génération du certificat pour accéder au répertoir de stockage.



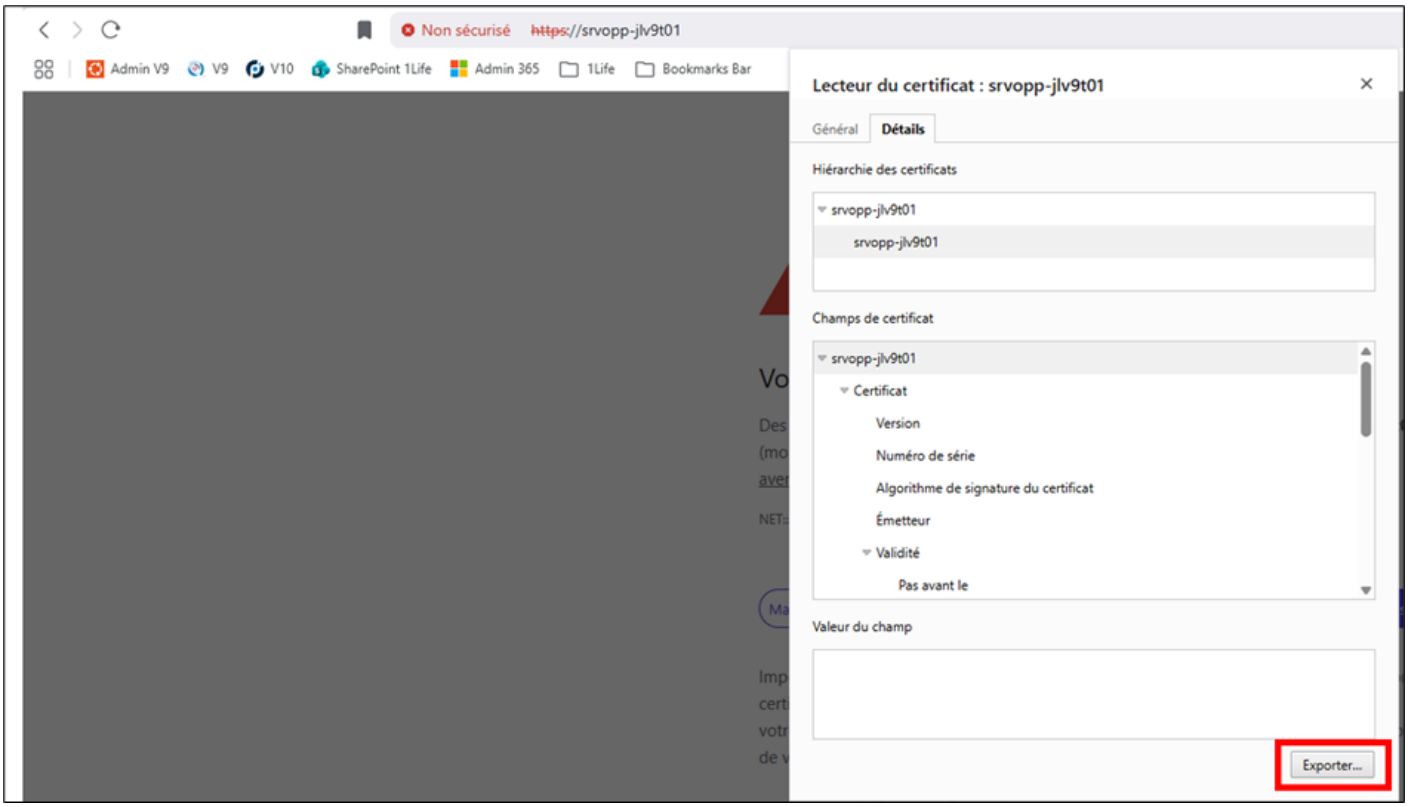


Récupérer sur son poste le certificat créé dans le répertoire sous le nom définit lors de sa génération (par défaut dans le dossier « certificates » avec le nom « deploy.crt »).

- Sinon via le navigateur Web, en se connectant depuis n'importe quel poste client sur Open-Prod par l'url https https://[nom_de_machine_ou_IP].

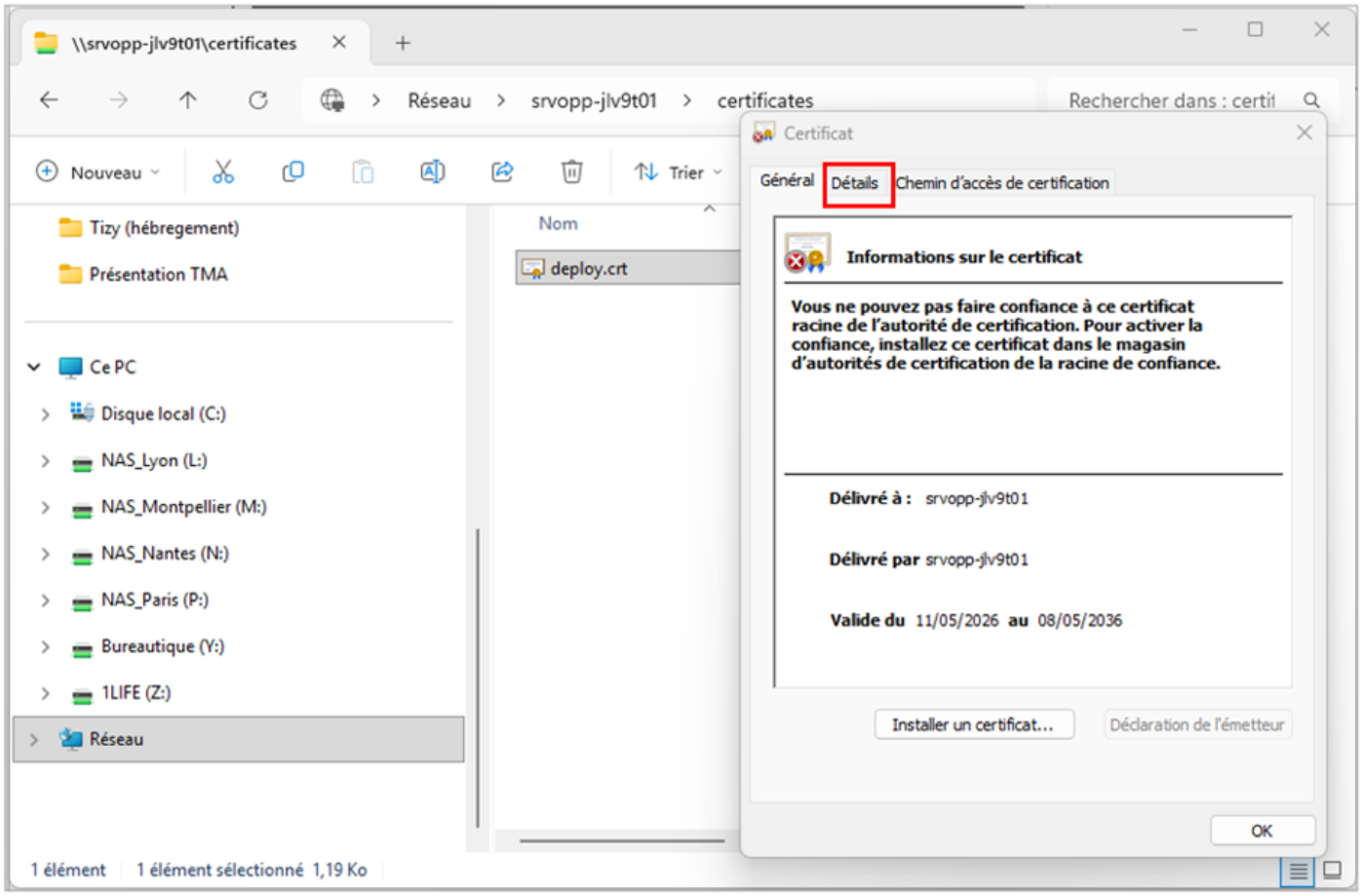


Trouver comment visualiser le certificat sur son navigateur, afficher les détails du certificat (options à trouver selon votre navigateur).

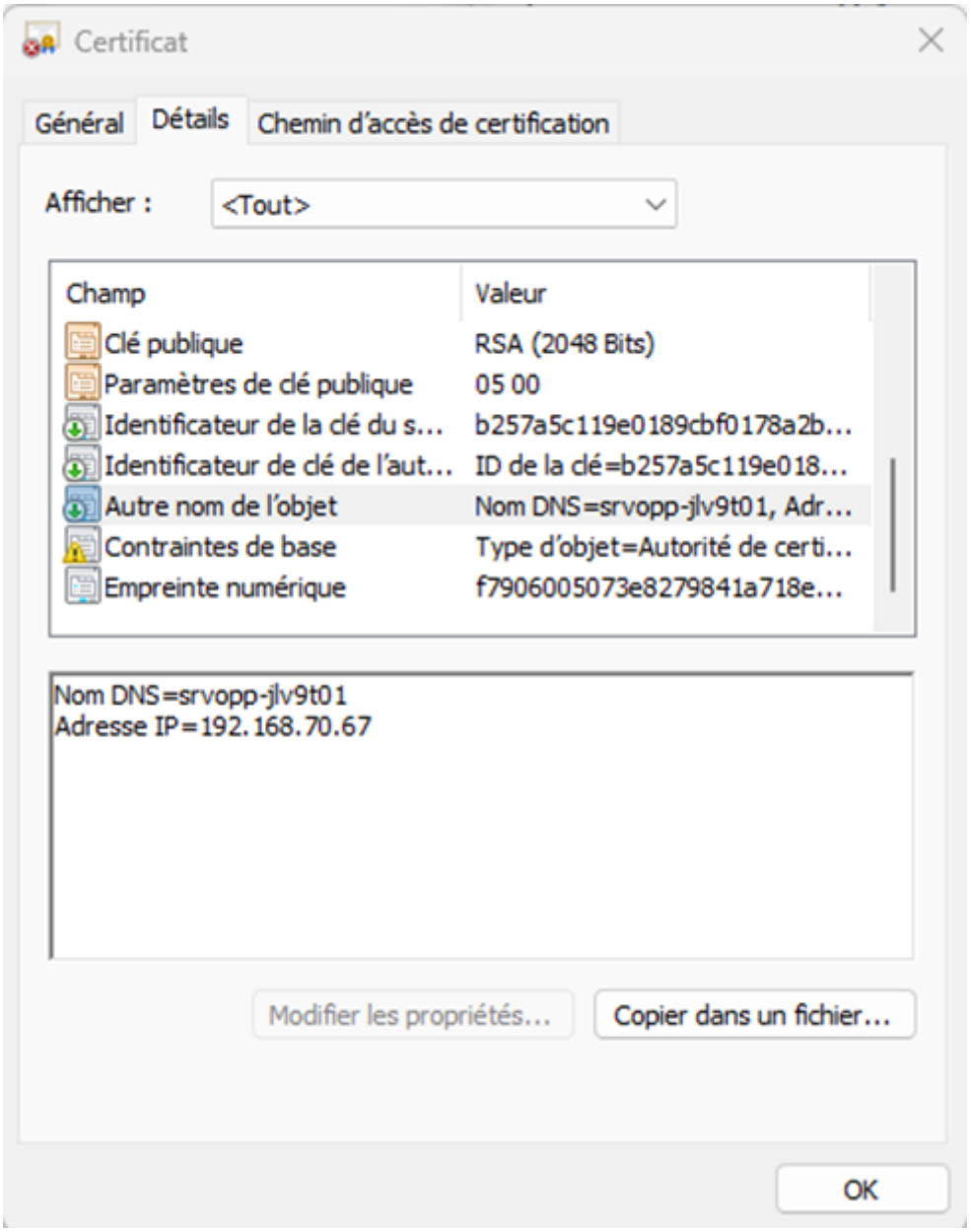


Cliquer sur « Exporter » pour récupérer le certificat en local sur votre poste (options à trouver selon votre navigateur).

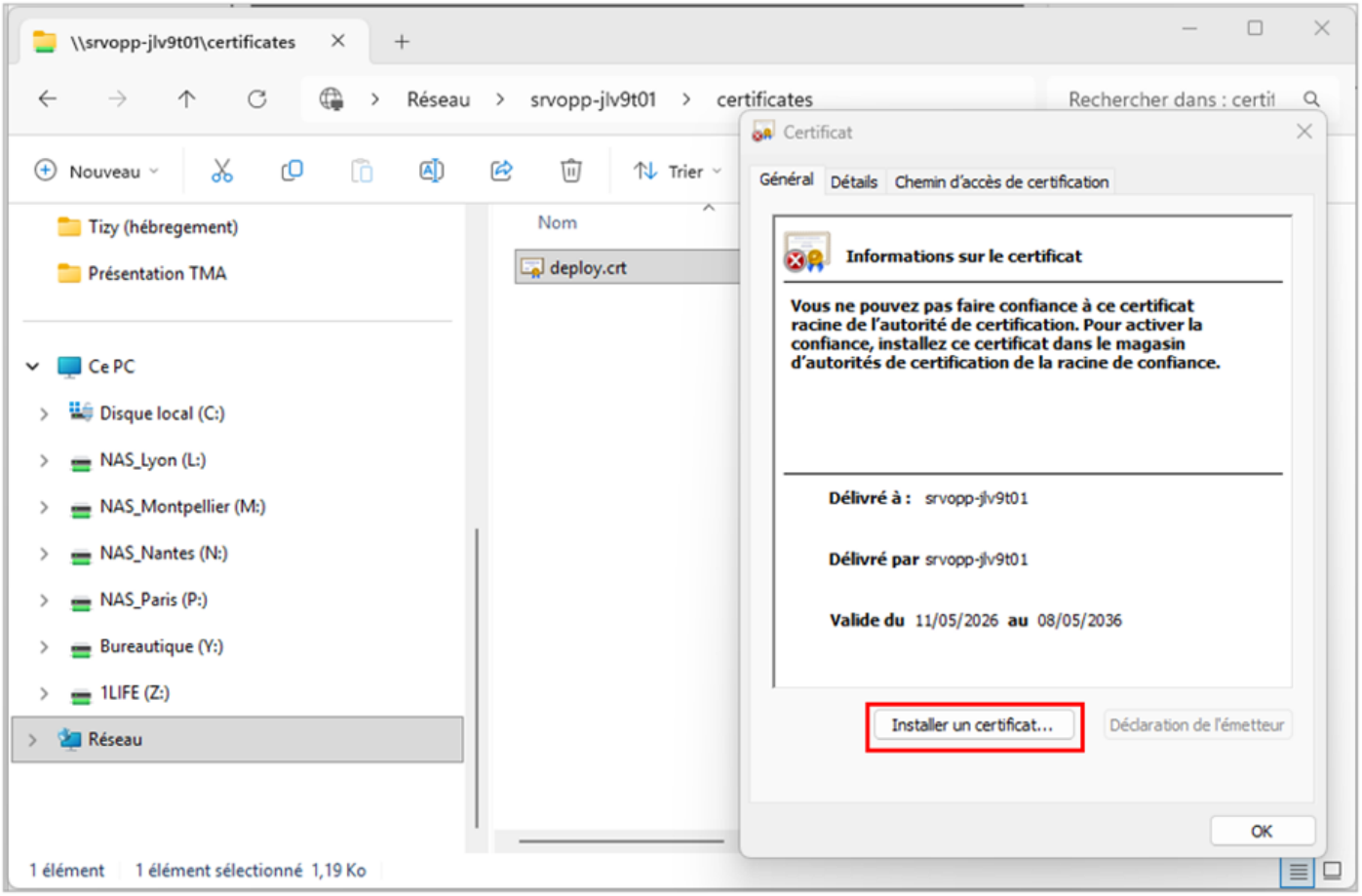
Installer maintenant le certificat sur son poste dans en l’important dans le magasin des certificats :



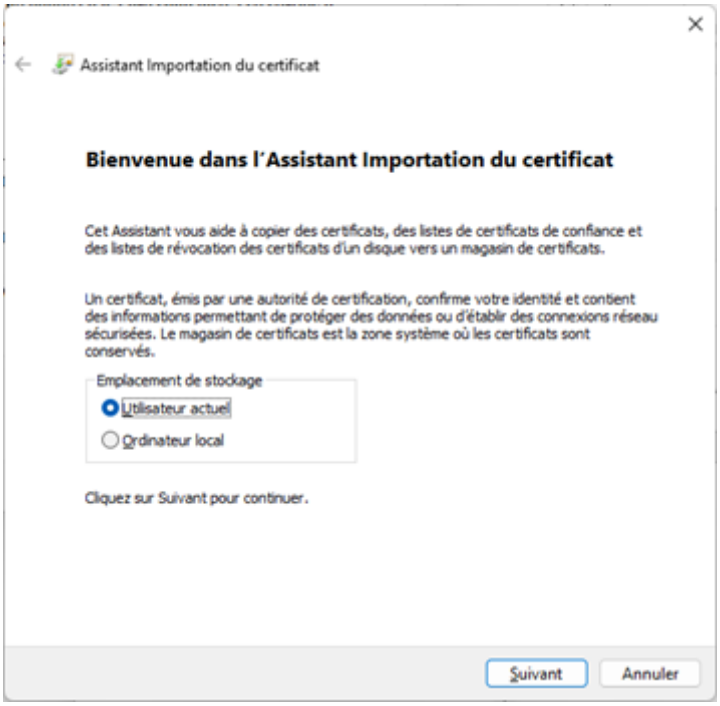
Double cliquer sur le certificat récupéré.



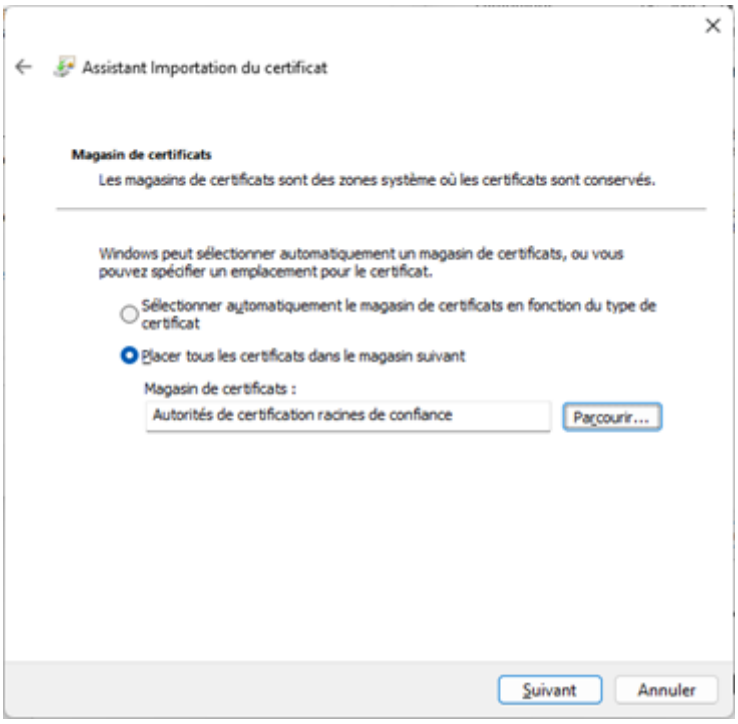
Vérifier dans l'onglet « détails » que la valeur « Autre nom de l'objet » correspond bien aux valeurs SAN saisies lors de sa génération et au vrai nom et IP de la machine sur votre réseau local. Si ce n'est pas le cas recommencer sr l'environnement Linux Open-Prod la création d'un nouveau certificat.



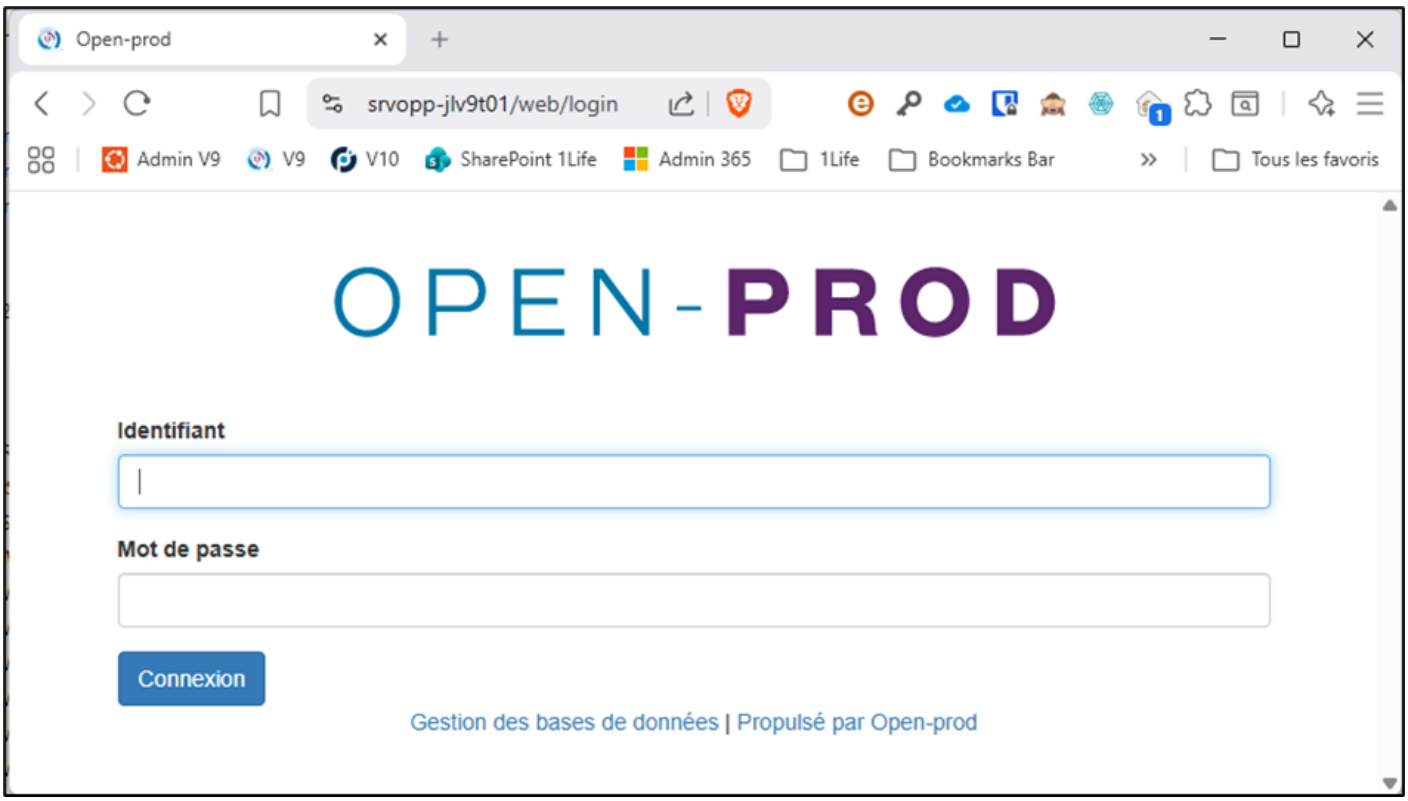
Si les valeurs sont correctes, revenir sur l'onglet Général » et sélectionner « Installer un certificat ».



Sélectionner « Utilisateur actuel » et « suivant »



Choisir « Placer tous les certificats dans le magasin suivant » et sélectionner « Autorités de certification racines de confiance » puis « suivant » et « terminer ». Confirmer par « Oui » l'alerte de sécurité pour finaliser l'installation du certificat. Le message « importation réussie » doit s'afficher.



Suite à cette intégration de certificat l'accès à Open-Prod via le navigateur au travers du nom de la machine ou de son ip (https://srvopp-jlv9t01 ou https://192.168.70.67 dans notre exemple) ne doit

plus lever d’alerte de sécurité sur ce poste.

> Répéter manuellement cette manipulation sur le poste de chaque utilisateur qui accède à Open-Prod via son navigateur.

> **Déployer automatiquement ce certificat sur tous les postes du réseau interne de l’entreprise.** Il est envisageable de déployer automatiquement ce certificat sur tous les postes de l’entreprise et d’éviter l’intégration manuelle sur chaque poste (au travers de la gestion des GPO sous Windows Active Directory par exemple). Contacter votre administrateur système pour étudier avec lui cette mise en place.

Https avec certificat signé

Https avec certificat signé gratuit