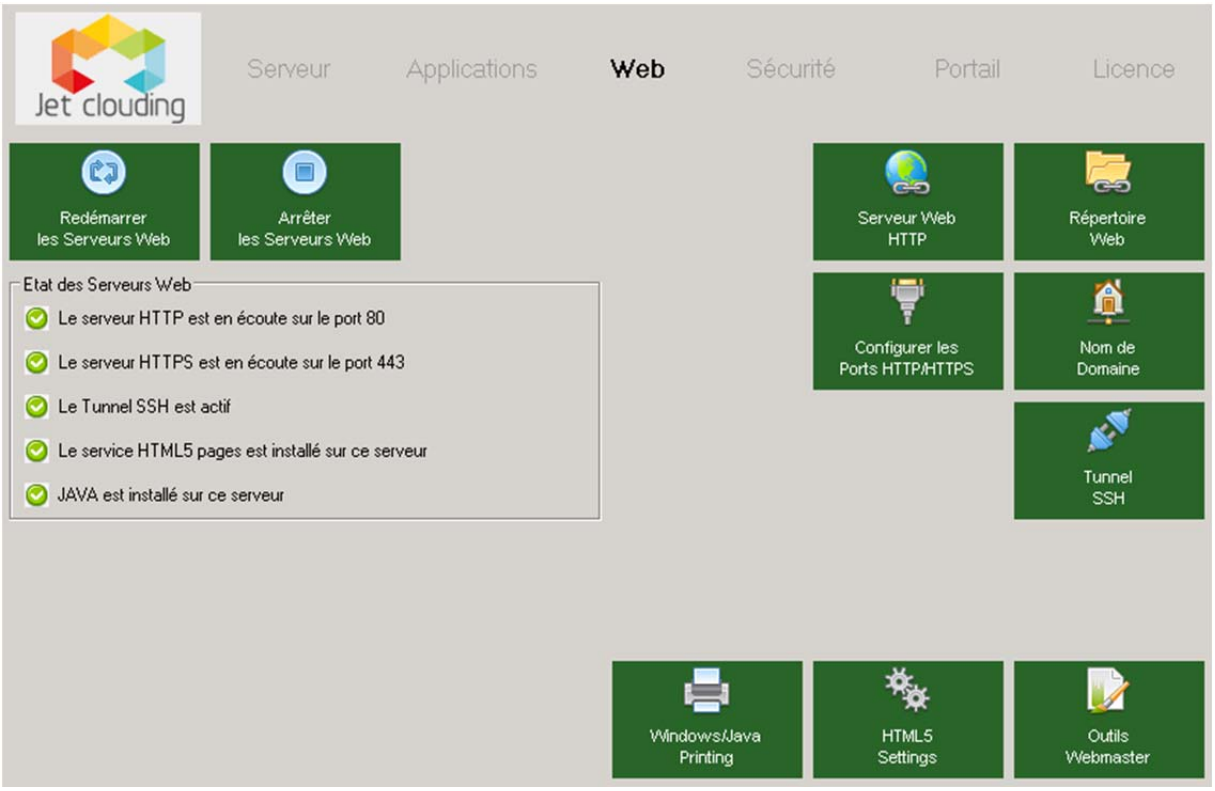
Tunnel SSH

1) Serveur Web et tunnel SSH, console d'administration

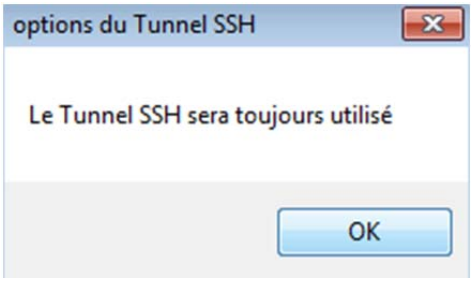
Une console de gestion est disponible dans l'outil d'administration

Cette console de gestion vous permet de configurer les services de JetClouding intégré dans le serveur Web, y compris les options tunnel SSH.



2) Toujours utiliser l'option tunnel SSH

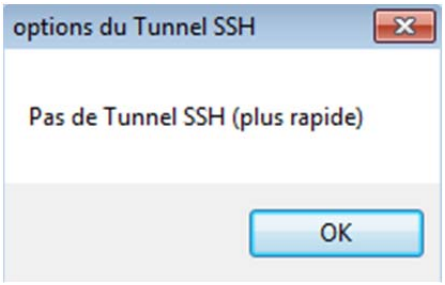
Lorsque vous sélectionnez « toujours utiliser le tunnel SSH », le tunnel SSH sera actif et vous permettra de créer un tunnel SSH sécurisé avant de se connecter pour créer une connexion VPN vers le serveur. Vous devez cliquer sur le bouton «sauver » pour continuer. Le message suivant s'affiche :



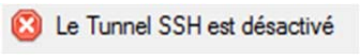
S'il vous plait cliquer sur le bouton « OK' pour continuer. Le « tunnel SSH est actif », l'option aura désormais un « + » vert :

3) Ne jamais utiliser l'option tunnel SSH

Lorsque vous sélectionnez « ne jamais utiliser un tunnel SSH » la connexion VPN ne sera pas établie. Vous devez cliquer sur le bouton « sauver » pour continuer. Le message suivant s'affiche :

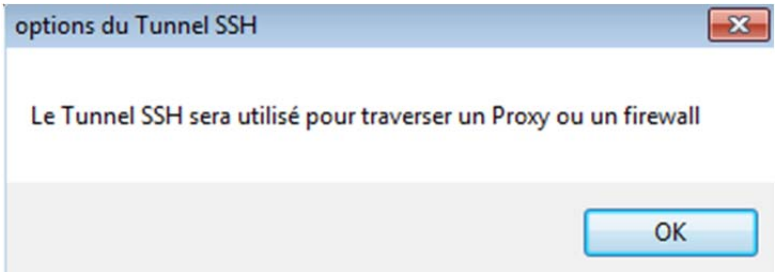


S'il vous plait cliquer sur le bouton « OK » pour continuer. Le tunnel SSH est désactivé et l'option aura désormais un « X » rouge :



4) Utiliser un tunnel SSH pour traverser un proxy

Lorsque l'option « utiliser un tunnel SSH pour traverser un proxy » est activée, le message suivant s'affiche :



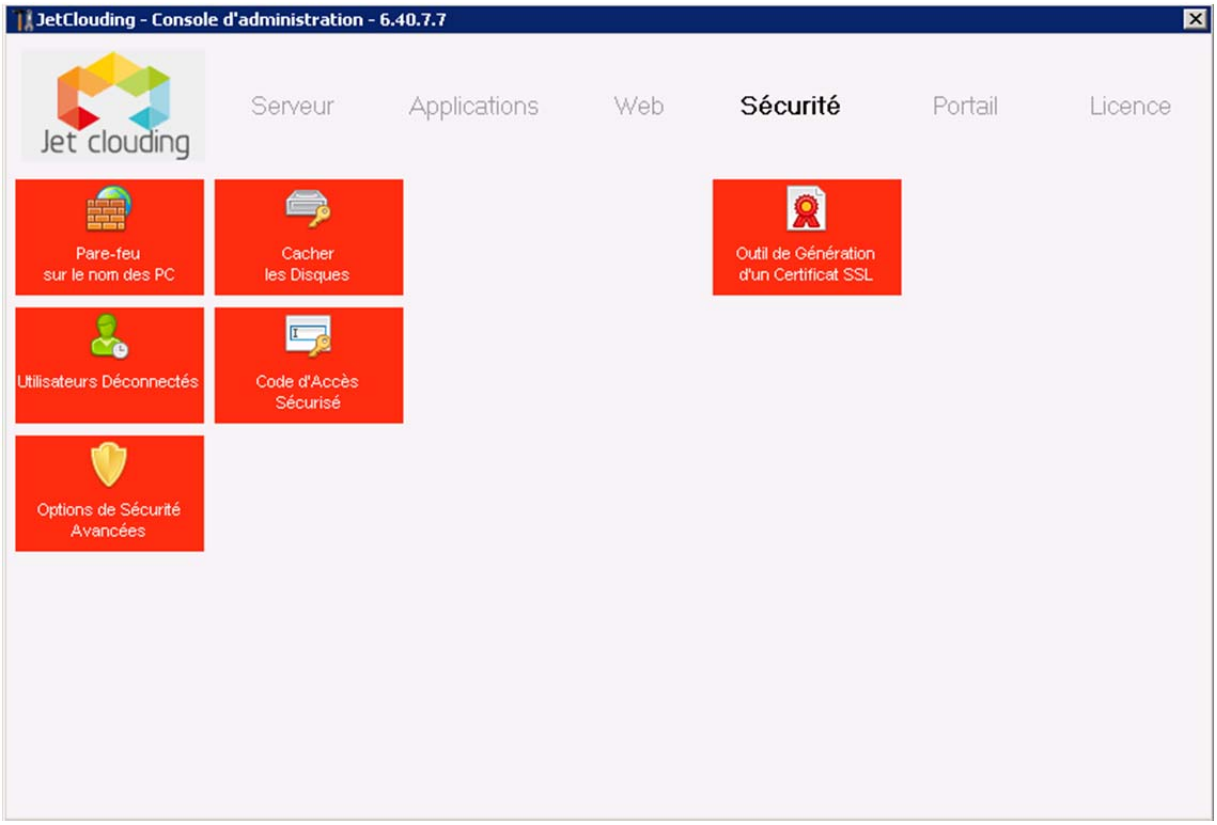
Cliquez sur le bouton « OK » pour continuer.

Certificat SSL

Server Web Console d'administration – Onglet sécurité

Un outil de génération de certificat SSL est disponible dans l'admin tool onglet sécurité.

Cet outil vous permet de configurer les certificats SSL avec les services JetClouding intégrés dans le Web Server :



Vue d'ensemble

Nous fournissons un certificat SSL auto signé 2048 bits RSA que vous pouvez utiliser « tel quel » dans notre serveur web HTTPS et dans notre serveur web SSH.

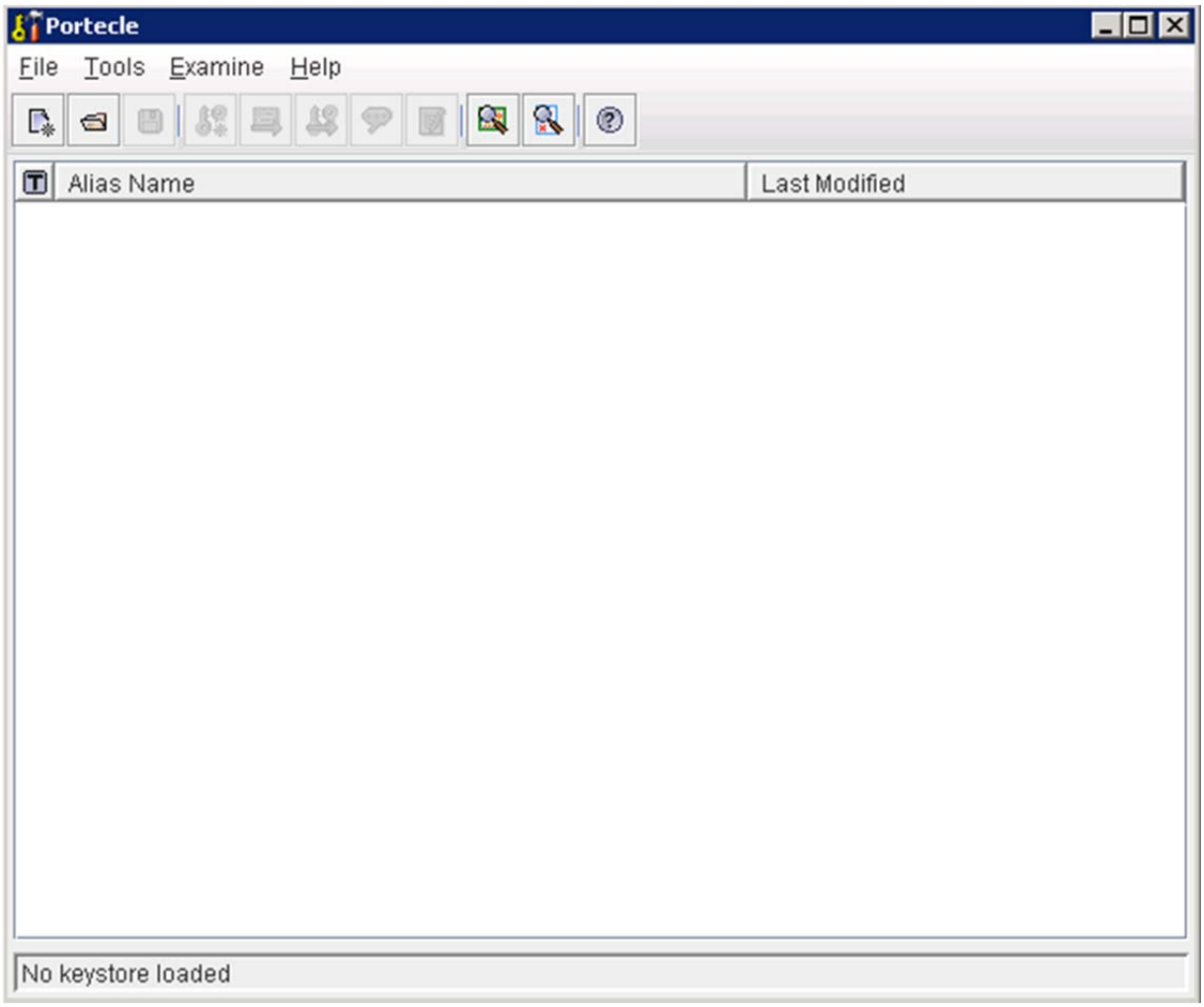
Si vous souhaitez créer votre propre clé ou importer un certificat 2048 bits, vous pouvez le faire en utilisant « PORTECLE ».

Notez que le mot de passe de cert.jks doit être : « secret »

PORTECLE est fourni tel quel et inclut de nombreuses fonctions utiles. Il permet également de générer une demande de certification.

Création d'un certificat SSL

S'il vous plaît cliquer sur le bouton « outil de génération d'un certificat SSL » pour ouvrir l'outil PORTECLE :



Le programme PORTECLE vous permettra de créer / importer et de modifier votre certificat 2048 bits pour votre serveur Web.

Pour trouver des informations sur « la génération du certificat » lancez le fichier README.TXT qui se trouve dans : *C:\Program Files\JetClouding\Clients\webserver*

S'il vous plait suivez les étapes ci-dessous pour générer votre certificat auto-signé et entrez correctement les informations dans votre certificat :

1. *Lancez Portecle*
2. *Ouvrez le menu « File » et cliquez sur « New Keystore »*
3. *Sélectionnez "JKS" puis cliquez sur "OK".*
4. *Lancez ensuite « Tools » et cliquez sur « Generate Key Pair ».*
5. *Choisissez "RSA" comme « Key Algorithm » et "2048" pour la « Key Size ». Puis cliquez sur « OK ».*

6. Dans la fenêtre suivante puis dans le menu « Signature Algorithm » choisissez au moins « SHA256withRSA »
6.1 Dans la case « Validity (days) », entrez « 36500 » qui signifie 100ans.
6.2 Dans la case « CN », entrez le domaine ou l'IP qui sera utilisé pour ouvrir le site. Par exemple si vous ouvrez : https://myserver.com alors le CN devrait être « myserver.com »
6.3 Remplissez ensuite les autres infos en fonction de vos besoins.
7. Dans la fenêtre suivante "Key Pair Entry Alias" entrez dans la case "Enter Alias" : « JWTS »
8. Dans la fenêtre suivante « Key Pair Entry Password » entrez dans la case « Enter New Password » : « Secret » et confirmer ce mot de passe.
9 Ensuite ouvrez "Tools" et cliquez sur "Set Keystore Password… " et entrez : « secret » et confirmer ce mot de passe.
10. Lancez « File » et cliquez sur « Save Keystore As », sauvegardez ce nouveau certificat « cert.jks » dans le dossier « WebServer » de JetClouding.
11. Redémarrez les serveurs Web.

Avertissement

- *Le certificat généré doit être nommé «cert.jks »*
- *Son mot de passe doit être «secret »*
- *Il doit être stocké dans le dossier : C:\Program Files\JetClouding\Clients\webserver*
-

Si la page Web n'est pas connectée via HTTP et n'est pas traitée en utilisant le protocole HTTPS, il est probable que votre fichier de certificat est erroné.

Nous vous recommandons d'effectuer une copie du certificat « cert.jks » fournie par défaut avant de générer votre propre certificat.

Lancer le client Windows ou JAVA sous les environnements avec proxy

Habituellement, le SSH intégré au serveur Web JetClouding supporte les proxys HTTP(S) et cela devrait être suffisant pour traverser la plupart des proxys connus.

Cependant, il y a des cas existants très dur, ou l'environnement proxy ne peut pas être reconnu car caché par un logiciel tiers ou sinon les serveurs cibles sont derrière des « reverse proxy ».

Pour ces cas difficile JetClouding contient une solution non-SSH appelé « mode de secours »

Si vous pouvez établir une connexion HTML5, vous pouvez être sûr que cette méthode va vous aider à établir des connexions via le WebSocket (Firefox, Chrome, Opéra, IE10 …) ou XHR (IE6-IE9).

Attention certains proxys permettent le trafic WebSocket / XHR uniquement via la couche HTTPS, donc utiliser HTTPS au lieu de HTTP.

Si le proxy ne demande pas d'authentification proxy pour accéder aux pages internet via un navigateur, suivez les étapes ci-dessous :

1. Lancez http(s)://votreserveur.com/software/html5/jwres/
2. Attendez « connexion réussie » (et autoriser l'éxécution JAVA si demandé)
3. Cliquez sur le texte rouge « OPEN THE LINK » pour ouvrir la page d'accès au portail WEB.
4. Utilisez l'accès JAVA / Windows comme d'habitude.

Si le proxy demande une authentification proxy pour accéder aux pages internet via un navigateur, suivez les étapes ci-dessous :

1. Lancez http(s)://votreserveur.com/software/html5/jwres/
2. Si une demande d'authentification proxy apparait pour les applets JAVA cliquez sur « Cancel ».
3. Cliquez sur « Download LocalWebServer » et exécutez-le après le téléchargement terminé. Le serveur http local va donc travailler sur le port 18888.
4. Cliquez sur « Force Applet Loading from http://localhost:18888 », ceci va recharger la page en chargeant les fichiers « JARS » à partir du serveur http locale.
5. Attendez pour « successful connexion »
6. Cliquez sur le texte rouge « OPEN THE LINK » pour ouvrir la page d'accès au portail WEB.
7. Utilisez l'accès JAVA / Windows comme d'habitude.

L’utilisation de serveurs derrière un Reverse Proxy

Il est possible d'utiliser les serveurs derrière un Reverse Proxy, sur certains Reverse Proxy via XHR-polling.

Websocket ne fait pas partie du protocole http. Les Reverse Proxys les plus connus ne supportent pas Websocket et rejettent la première demande de WebSocket.

Si vous savez que le serveur est derrière un reverse proxy, désactivez Websocket en mettant cette option dans Clients \ www \ software \ html5.html:

var disablewebsocket = true;

Cela va imposer l'utilisation de XHR-polling et éviter les retards de temps lors de la connexion.

Veuillez noter que l'utilisation de XHR-polling n'est pas aussi stable que Websocket en raison de sa nature de connexion.