arcOpole PRO Serveur

Guide Installation - Annexes

Version 141.5

30/09/2026

Copyright © 2026, 1Spatial® by VertiGIS™. Tous droits réservés.

info@1spatial.com www.1spatial.com

A propos du Guide

Les informations contenues dans ce document pourront faire l'objet de modifications sans préavis de la part de 1Spatial.

Sauf mention contraire, les sociétés, les noms et les données utilisés dans les exemples sont fictifs.

Aucune partie de ce document ne peut être reproduite ou transmise à quelque fin ou par quelque moyen que ce soit, électronique ou mécanique, sans la permission expresse et écrite de 1Spatial.

Limitation de garantie et de responsabilité

1Spatial a réalisé tous les tests nécessaires et suffisants du Progiciel et a vérifié la conformité de son guide.

Le client reconnaît que dans l'état actuel de la technologie informatique, le fonctionnement du Progiciel est susceptible d'être interrompu ou affecté par des bogues. 1Spatial ne garantit pas que le Progiciel, le média d'installation, la clef ou la documentation livrés soient exempts d'erreurs, de bogues ou d'imperfections.

Ainsi, le client doit effectuer toutes les sauvegardes, prévoir et effectuer toutes les procédures de remplacement en vue d'éventuelles défaillances du Progiciel, prendre toutes les mesures appropriées pour se prémunir contre toute conséquence dommageable due à l'utilisation ou la non-utilisation du Progiciel.

Il est expressément convenu que 1Spatial ne sera en aucun cas responsable des dommages directs ou indirects dus à l'utilisation du Progiciel.

L'utilisation du Progiciel est soumise à la signature par le client du contrat de droit d'utilisation des logiciels de 1Spatial.

Marques déposées

Ce progiciel est une marque déposée de 1Spatial.

Ce progiciel, développé par 1Spatial, est une marque déposée et est la propriété exclusive de 1Spatial. Toutes les autres marques citées appartiennent à leurs propriétaires respectifs.

Copyright © 2026, 1Spatial® by VertiGIS™. Tous droits réservés.

TABLE DES MATIÈRES

1 PRÉSENTATION 4

2 EXEMPLE CRÉATION CLIENT ID SUR UN PORTAL FOR ARCGIS® 5

3 RÉCUPÉRATION D'UN CERTIFICAT EN FICHIER « .CRT ». 8

4 FICHIERS À CONFIGURER POUR PASSER EN MODE NON FÉDÉRÉ 10

4.1 Fichier ArcGISConnector.json 10
4.2 Fichier proxy.json 12

5 CRYPTER UN MOT DE PASSE POUR « AOPS » 14

6 RÉSUMÉ DE TOUS LES FICHIERS MODIFIABLES POUR UNE INSTALLATION « AOPS » 16

7 DÉCRYPTAGE DE QUELQUES MESSAGES D'ERREURS AU DÉMARRAGE 17

7.1 Etat HTTP 404 – Non trouvé 17
7.2 Invalid client_id 18
7.3 Not found 18
7.4 Ce site est inaccessible 18
7.5 État http 403 – Interdit 19
7.6 Connexion impossible : aucune page ne s'affiche 20
7.7 Connexion bloquée si serveur Apache installé sur un autre serveur que arcOpole PRO Serveur. 21

© 2026, 1Spatial® by VertiGIS™

1 PRÉSENTATION

Cette documentation vient en complément de la documentation d'installation d'arcOpole PRO Serveur.

Elle contient, entre autres les annexes citées dans la documentation principale et peut être considérée comme une FAQ.

Convention de nommage pour le reste de la documentation :

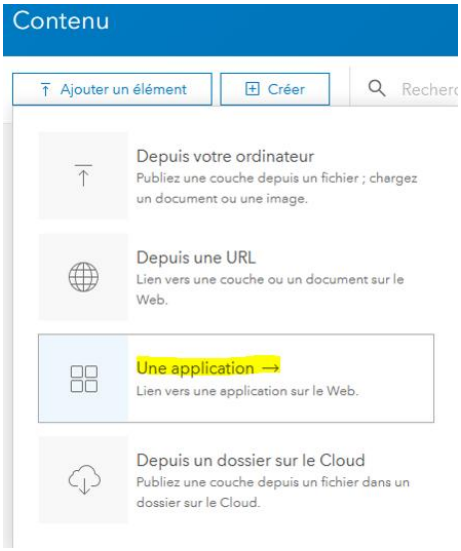
- arcOpole PRO Serveur : AOPS ;
- ArcGIS® Server : AGS ;
- Portal for ArcGIS® : PORTAL.

Dans la suite du document, tous les répertoires sont référencés par rapport à la racine d'installation (par défaut : « D:\1Spatial\aOpServeur »).

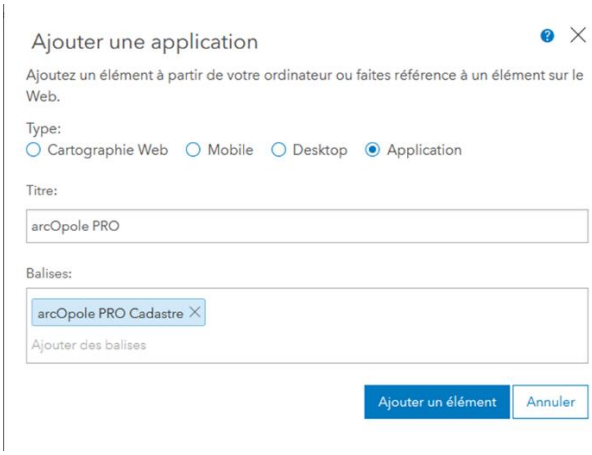
Par convention, ce répertoire est nommé : **<REPAOPS>**

2 EXEMPLE CRÉATION CLIENT ID SUR UN PORTAL FOR ARCGIS®

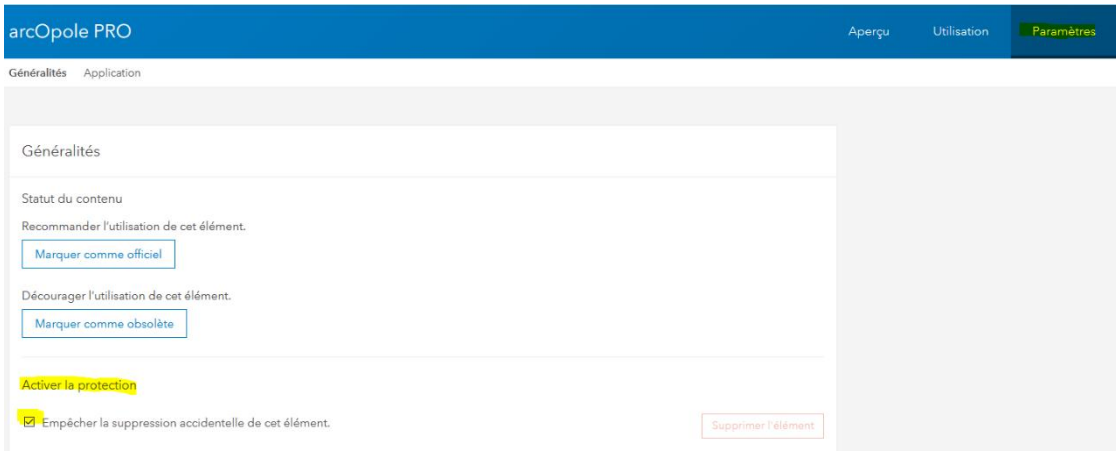
- Vous connecter sur votre « PORTAL » avec un compte ayant le droit de créer du contenu ;
- Aller dans la page de gestion des « contenus » ;
- Dans le menu « Ajouter un Élément », choisir « Une application » :



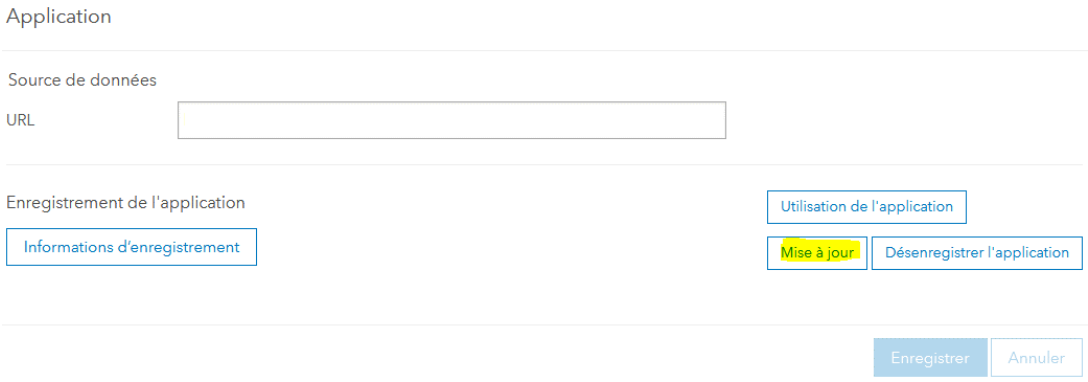
- Sélectionner « Application » dans Type, donner comme titre « arcOpole PRO », mettre une balise, puis valider en cliquant sur « Ajouter un élément » :

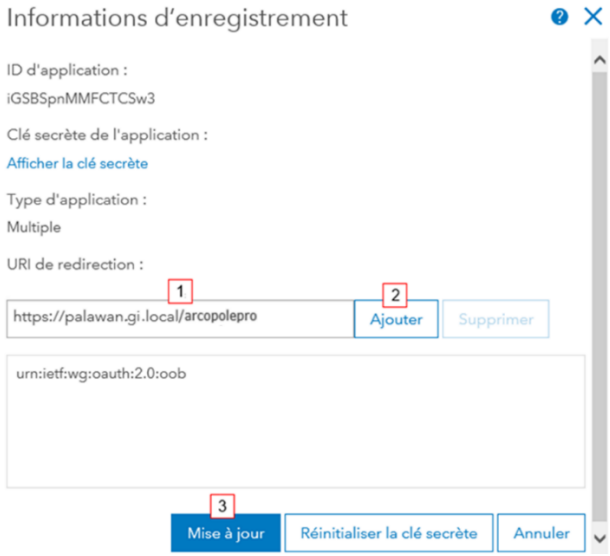


- Sur la page de l'application, aller dans l'onglet « Paramètres » :

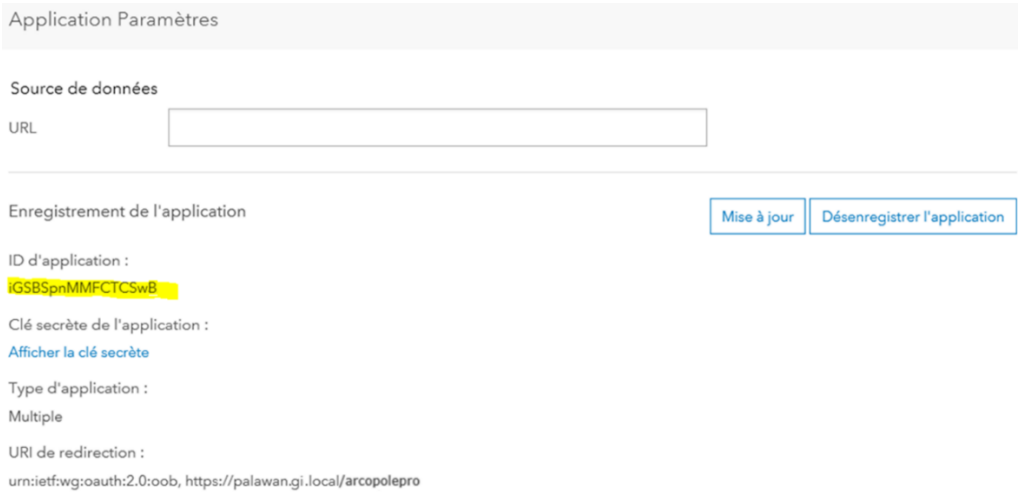


- Cocher « Empêcher la suppression accidentelle de cet élément », puis cliquer sur « Enregistrer » ;
- Descendre en bas de la page, puis dans la partie « Application » et cliquer sur « Mise à jour » :





- Saisir l'URI de votre serveur « arcOpole PRO Serveur » (celle que vous venez de créer à l'étape précédente) ;
- Cliquer sur « Ajouter » ;
- Cliquer sur « Mise à jour » :



La chaine « Client ID » attendue dans le fichier « ArcGISConnector.json » correspond à la ligne : « ID d'application ».

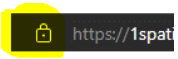
! **NE PAS SUPPRIMER CETTE APPLICATION DE VOTRE « PORTAL », SINON L'AUTHENTIFICATION D' « arcOpole PRO Serveur » NE FONCTIONNERAIT PLUS.**

! Si vous avez déjà une application « arcOpole PRO » ou une autre application dont vous voulez réutiliser le numéro « Client ID », il suffit d'ajouter votre url du contexte « arcOpole PRO » dans l'URI de redirection existante de cette application.

3 RÉCUPÉRATION D'UN CERTIFICAT EN FICHIER « .CRT ».

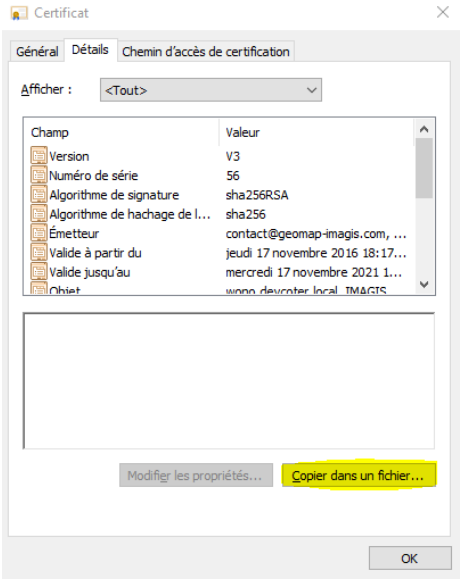
Pour récupérer un certificat en fichier « .crt », suivre la démarche suivante :

► Vous connecter au serveur avec « Internet Explorer » ;

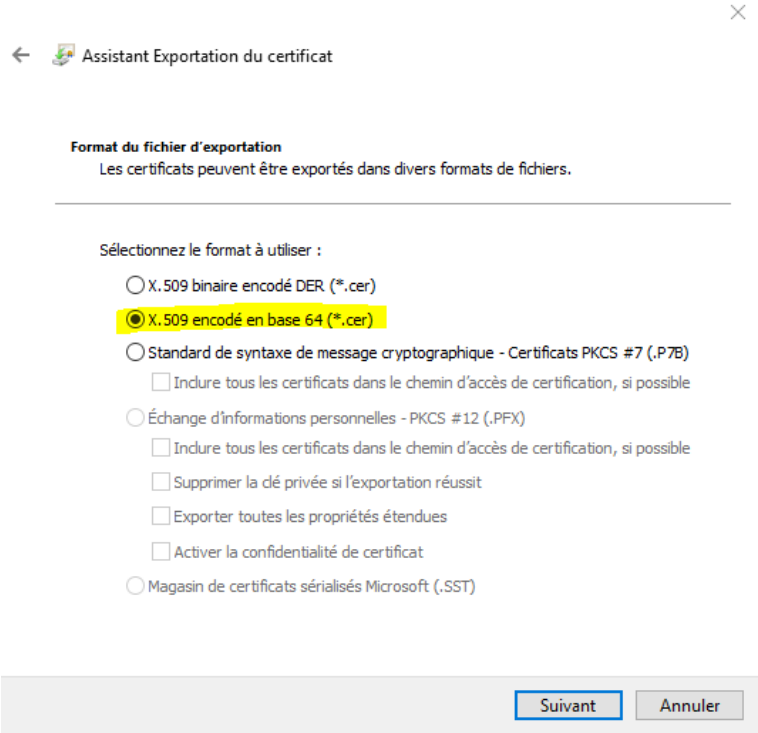
► Cliquer dans la barre d'adresse sur le cadenas 

et choisir « afficher les certificats » :

! Suivant les Navigateurs, le terme « afficher les certificats » peut varier.



► Aller dans l'onglet « Détails », puis choisir « Copier dans un fichier » qui va ouvrir un assistant pour exporter le fichier. Suivre les indications de l'assistant :



- Dans l'assistant, choisir le format d'export : « X.509 encodé en base 64 (*.cer) » ;
- Pour le nom du fichier à exporter, il est à votre convenance, seule l'extension doit avoir obligatoirement comme nom « .crt » ;
- Pour le chemin d'export, si vous êtes sur le serveur « AOPS », vous pouvez directement choisir comme dossier de destination le répertoire « \config\certificates » ;
- Si vous n'êtes pas sur le serveur « AOPS », copier le certificat sauvegardé dans le répertoire « \config\certificates » du serveur « AOPS ».

4 FICHIERS À CONFIGURER POUR PASSER EN MODE NON FÉDÉRÉ

Il est possible d'installer arcOpole PRO Serveur en mode non fédéré pour les applications (DVF, DTDICT, Intervention, DPA).

Vous trouverez ci-dessous les fichiers de paramétrages à modifier par rapport à une installation standard en mode fédéré.

4.1 FICHIER ARCGISCONNECTOR.JSON

Éditer le fichier « <REPAOPS>\config\ArcGISConnector.json » afin d'indiquer les connexions aux serveurs « PORTAL » et « AGS ».

```
{
  "portals": [
    {
      "name": "default",
      "url": "https://mon serveur portal/portal",
      "clientID": "<chaine Client ID de mon serveur portal>"
    }
  ],
  "servers": [
    {
      "name": "default",
      "url": "https://mon serveur ArcGIS_server/arcgis",
      "authUsername": "login",
      "authPassword": "mot de passe"
    }
  ],
  "certificatesDirectory": "./certificates",
  "validateCertificates": true
}
```

En plus de la configuration classique du fichier (voir documentation principale), vous devez indiquer pour « servers », un utilisateur et son mot de passe.

Pour « servers » (AGS), l'utilisateur doit avoir le droit d'usage du(des) service(s) qui seront utilisés pour le module métier installé.

! Pour des raisons de sécurité vous pouvez crypter vos mots de passes. Vous trouverez la méthodologie dans le chapitre « Crypter un login ou un mot de passe pour arcOpole PRO Serveur ».

Exemple : Avec une authentification via un portail non fédéré, et mot de passe crypté

```
{
  "portals": [
    {
      "name": "default",
      "url": "https://www.work.com/portal",
      "clientID": "raZcu2CoDj5msgC4",
    }
  ],
  "servers": [
    {
      "name": "default",
      "url": "https://www.work.com/arcgis",
      "authUsername": " portaladmin ",
      "authPassword": "~/5tbtorJmFnjlOX4TYX0jLyllNJhuPCh5ef8pXjZXqU="
    }
  ],
  "certificatesDirectory": "./certificates",
  "validateCertificates": true
}
```

Exemple : Avec une authentification uniquement sur ArcGIS® Serveur :

```
{
  "portals": [],
  "servers": [
    {
      "name": "default",
      "url": "https://www.work.com/ArcGIS/",
      "authUsername": "dtdict",
      "authPassword": "Th3qsfOs"
    }
  ],
  "certificatesDirectory": "./certificates",
  "validateCertificates": true
}
```

4.2 FICHIER PROXY.JSON

Le proxy permet de définir certaines redirections lors des appels au serveur « AOPS » vers des services externes comme le service de géocodage d'adresses, l'accès aux services de géométrie ou encore l'accès aux serveurs ESRI©.

Éditer le fichier « .\config\proxy.json » :

```
{
 "proxies": [
  {
   "name": "geocoder",
   "url": "https://api-adresse.data.gouv.fr/"
  },
  {
   "name": "geometry",
   "url": "https://arcgis_server/ArcGIS/rest/services/Utilities/Geometry/",
   "username": "login",
   "password": "mot de passe"
  }
 ]
}
```

En plus de la configuration classique du fichier (voir documentation principale), vous devez indiquer pour les proxys définis un utilisateur et son mot de passe.

! Pour des raisons de sécurité vous pouvez crypter vos mots de passes. Vous trouverez la méthodologie dans le chapitre « Crypter un login ou un mot de passe pour arcOpole PRO Serveur ».

Exemple : Définition du proxy en mode non fédéré, avec une définition d'accès aux services d'ArcGIS Sever nécessitant un login/mot de passe, et un accès un service public sur ArcGIS Online.

```
{
  "proxies": [
  {
    "name": "geocoder",
    "url": "https://data.geopf.fr/geocodage/"
  },
  {
    "name": "geometry",
    "url": "https://www.work.com/arcgis/rest/services/Utilities/Geometry/",
    "username": "arcopolepro",
```

```
      "password": "AdJf$24F"
    },
    {
      "name": "online",
      "url": "https://services.arcgisonline.com/ArcGIS/rest/services/"
    },
    {
      "name": "arcgis",
      "url": "https://www.work.com/arcgis/rest/services/",
      "username": "arcopolepro",
      "password": "~/5tbtorJmFnjlOX4TYX0jLyllNJhuPCh5ef8pXjZXqU=""
    }
    ]
}
```

5 CRYPTER UN MOT DE PASSE POUR « AOPS »

Pour ne pas mettre en clair les mots de passe, vous avez la possibilité de les crypter.

Pour indiquer à « AOPS » qu'une chaine est cryptée dans un fichier de configuration « .json », il faut préfixer la chaine par un tilde : **~.**

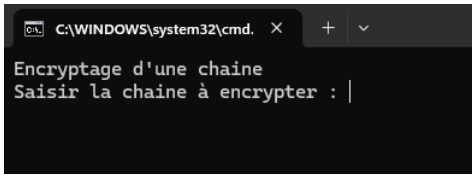
Il est possible d'encrypter les données sensibles figurant dans les fichiers de configuration suivants :

- Tous les fichiers *.properties des différents métiers ;
- Les fichiers : ArcGISConnector.json, proxy.json, acldatabase.json.

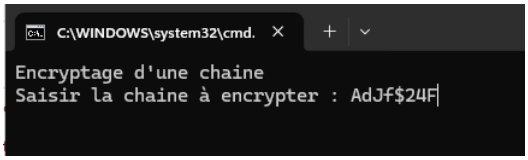
Un script « encrypte.bat » a été mis à disposition pour encrypter une chaine de caractères.

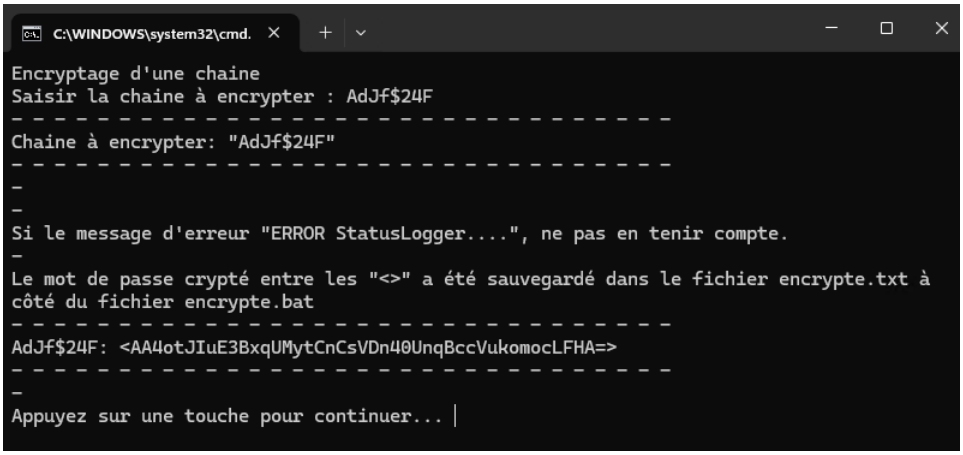
Il est disponible dans « <REPAOPS>\Ressources_Installation_outils » :

- Exécuter le fichier « encrypte.bat » :



- Saisir votre chaine à encrypter, puis valider par « entrée » :





La chaine encryptée est composée de tous les caractères entre les « **<>** ».

Vous trouverez la chaine dans le fichier « encrypte.txt » situé à côté du fichier « encrypte.bat ».

! Le fichier « encrypte.txt » est écrasé à chaque exécution du fichier « encrypte.bat ».
Si vous avez le caractère " (guillemet) dans votre chaine, il faut le doubler lorsque vous saisissez votre chaine.

- Ensuite, dans votre fichier « json », vous indiquerez la chaine de caractères pour un mot de passe ou un utilisateur, en commençant la chaine par un **tilde (~)**.

Exemple :

```
"servers": [
  {
    "name": "default",
    "url": "https://www.work.com/arcgis",
    "authUsername": "cadastre",
    "authPassword": "AdJf$24F »
  }
```

► Après encryptage du mot de passe :

Exemple :

```
"servers": [
  {
    "name": "default",
    "url": "https://www.work.com/arcgis",
    "authUsername": "cadastre",
    "authPassword": "~/5tbtorJmFnjlOX4TYX0jLyllNJhuPCh5ef8pXjZXqU="
  }
```

6 RÉSUMÉ DE TOUS LES FICHIERS MODIFIABLES POUR UNE INSTALLATION « AOPS »

Vous trouverez ci-dessous tous les fichiers qui sont potentiellement modifiables pour une installation d'arcOpole PRO Serveur.

- Installation standard :

  \config\ArcGISConnector.json

  \config\proxy.json

- Installation personnalisée :

  \server\tomcat\apache-tomcat\bin\aopServerInstall.bat

  \server\apache-tomcat\conf\Catalina\localhost\arcopolepro.xml

  \config\acldatabase.json

  \config\modules.json

  \config\mapprint.json

  \config\application.properties

  \config\orion.json

  \server\database\server\server.cfg

  \server\database\server\service_mongodb.bat

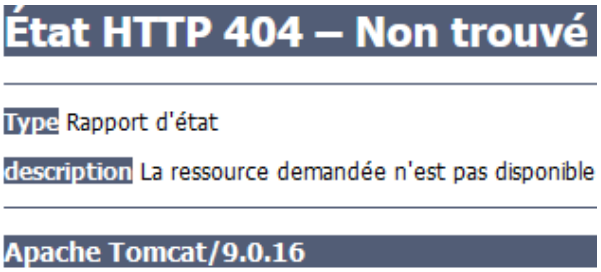
  \server\database\server\test_service_mongo.bat

7 DÉCRYPTAGE DE QUELQUES MESSAGES D'ERREURS AU DÉMARRAGE

Vous trouverez ci-dessous les principaux messages d'erreurs qui peuvent survenir au démarrage d'arcOpole PRO Serveur lors du test de validation avec l'adresse suivante :

https://monServeurAOPS/arcopolepro/rest/auth/oauth2/authorize?callback=arcopolepro:application

7.1 ETAT HTTP 404 – NON TROUVÉ



Ce message indique que le serveur arcOpole PRO n'est pas démarré.

Consulter les logs suivants pour connaître la raison :

- **<REPAOPS>\logs\arcopolepro.log ;**
- **<REPAOPS>\server\apache-tomcat\logs\arcopoleproserver-stderr.<date>.log.**

Pour savoir si c'est un problème lié au moteur arcOpole PRO Serveur ou à un module métier, désactiver tous les modules dans le fichier « **modules.json** », arrêter le serveur, effacer les fichiers « logs » et redémarrer le serveur.

Exemples de messages :
Ici le module DT-DICT est activé, mais n'a pas de licence :
27-Sep-2019 07:50:09.464 SEVERE [main] org.apache.catalina.startup.HostConfig.deployDescriptor Erreur lors du déploiement du descripteur de configuration [D:\1Spatial\aOpServeur\server\apache-tomcat\conf\Catalina\localhost\arcopolepro.xml] java.lang.IllegalStateException: Erreur lors du démarrage du conteneur fils … Plus bas dans le fichier : Caused by: java.lang.IllegalStateException: Pas de clé de licence pour le module DTDICT
Ici le contexte Tomcat d'arcOpole PRO Serveur est mal défini :
08-Nov-2019 16:07:44.883 SEVERE [main] org.apache.catalina.startup.HostConfig.deployDescriptor Erreur lors du déploiement du descripteur de configuration [D:\1Spatial\aOpServeur\server\apache-tomcat\conf\Catalina\localhost\arcopolepro.xml] java.lang.IllegalStateException: Erreur lors du démarrage du conteneur fils …

Plus bas dans le fichier : Caused by: java.lang.IllegalArgumentException: L'ensemble de ressources principal [D:\1Spatial\aOpServeur\web1] est invalide

7.2 INVALID CLIENT_ID

ArcGIS Portal Directory | Home

Error

Invalid client_id

Error: 400

Ce message indique que la clé « **clientID** » n'est pas valide.

Cela peut venir :

- D'un mauvais numéro de **clientID** dans le fichier « **ArcGISConnector.json** » ;
- D'une mauvaise déclaration de votre URI dans l'application du portail qui a générée le numéro de **clientID**.

7.3 NOT FOUND

Not Found

The requested URL /portale/sharing/rest/oauth2/authorize was not found on this server.

Le serveur arcOpole PRO Serveur a démarré, mais il ne trouve pas le « portail » défini dans le fichier « **ArcGISConnector.json** ».

Exemple de message dans le fichier de log : **<REPAOPS>\logs\arcopolepro.log.**

Exemple :
[WARN] 2019-09-26 14:52:19.229 [ags.RestConnector] - Unable to connect with portal default com.imagis.arcopolepro.ags.InvalidJsonRestException: AGSRestConnector.connect failed to connect to portal default

7.4 CE SITE EST INACCESSIBLE

Ce site est inaccessible

Impossible de trouver l'adresse IP du serveur de **pate.gi.local**.

✓ Essayez d'exécuter les diagnostics réseau de Windows.

DNS_PROBE_FINISHED_NXDOMAIN

Le serveur d'arcOpole PRO serveur est inaccessible.

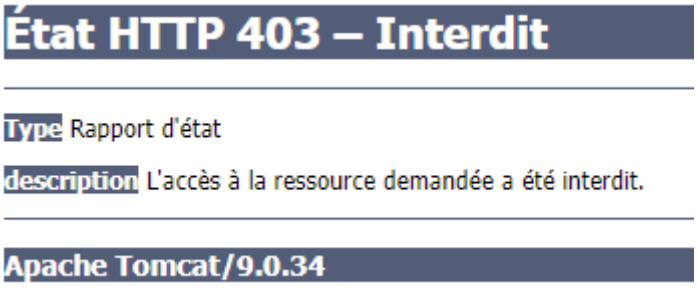
Le serveur « hôte » désigné dans la configuration n'est pas accessible.

Cela peut être une erreur dans le PareFeu, dans le fichier de configuration de Tomcat (server.xml), dans la définition du port de publication, d'une erreur de redirection dans le serveur Apache Frontal.

Exemple de message dans le fichier de log : **<REPAOPS>\logs\arcopolepro.log.**

Erreur :
[ERROR] 2019-09-26 15:30:41.962 [ags.RestConnector] - RestConnector.connect failed to connect to portal default java.net.UnknownHostException: Hôte inconnu (pate.gi.local)

7.5 ÉTAT HTTP 403 – INTERDIT



Ce cas peut arriver lors de la mise en place du mode de sécurité entre TOMCAT/APACHE, lorsque que le mot clé « secret » partagé entre les deux n'est pas bon.

CAS 1 : Le mot clé indiqué est bien différent entre TOMCAT et APACHE.	
aOpServeur\server\apache-tomcat\conf\server.xml	Apache24\conf\extra\httpd-ssl.conf
<Connector port="8029" protocol="AJP/1.3" URIEncoding="UTF-8" executor="tomcatThreadPool" keepAliveTimeout="20000" secretRequired="false" secret="AOPS-KeySecure" />	ProxyPass /arcopolepro ajp://localhost:8039/arcopolepro ttl=20 retry=0 nocanon secret=AOPS-Key
Solution : mettre le même mot clé de sécurité des deux côtés.	
CAS 2 : Version d'Apache trop ancienne pour le support des mots clés de sécurités.	
Si votre version d'Apache est inférieure à la version 2.4.42, les mots clés de sécurités ne sont pas supportés : ► (Recommandé) Mettre à jour votre Apache en version 2.4.42 ou supérieure ;	

► Si vous ne pouvez pas mettre à jour votre version d'Apache, dans ce cas supprimer l'attribut « **secret** » dans votre fichier « server.xml » et mettez « **secretRequired** » à « **false** ». ! Si l'attribut « secret » est présent, la valeur de l'attribut « secretRequired » (true, false) n'est plus pris en compte en Tomcat. L'attribut « secretRequired » est resté pour la compatibilité avec Tomcat 8. Donc vous aurez ceci dans le fichier :
<Connector port="8029" protocol="AJP/1.3" URIEncoding="UTF-8" executor="tomcatThreadPool" keepAliveTimeout="20000" secretRequired="false" />

7.6 Connexion impossible : aucune page ne s'affiche

Ouvrir le fichier log « arcopoleproserver-stderr.YYYY-MM-DD.log ».

Si vous avez ce message :

15-Oct-2021 14:20:08.499 SEVERE [main] org.apache.catalina.util.LifecycleBase.handleSubClassException Echec de démarrage du composant [Connector[AJP/1.3-8039]]

Avec un peu plus bas :

Caused by: java.lang.IllegalArgumentException: Le connecteur AJP est configuré avec secretRequired="true" mais l'attribut secret est soit null soit "", cette combinaison n'est pas valide.

Ce message indique que dans le fichier **« server.xml »**, l'attribut « **secret** » n'a pas été trouvé.

Cas possibles pour obtenir le message d'erreur évoqué :	
« secret » absent	ancien attribut « secure »
<Connector port="8029" protocol="AJP/1.3" URIEncoding="UTF-8" executor="tomcatThreadPool" keepAliveTimeout="20000" secretRequired="**true**" />	<Connector port="8029" protocol="AJP/1.3" URIEncoding="UTF-8" executor="tomcatThreadPool" keepAliveTimeout="20000" secretRequired="**true**" secure=" AOPS-KeySecure" />
Pour résoudre le problème :	
► Si vous voulez utiliser le mode de sécurité renforcé APACHE/TOMCAT, mettre l'attribut « secret » avec sa valeur, ou remplacer le nom de l'attribut « secure » par secret.	
<Connector port="8029"	

```
        protocol="AJP/1.3"
        URIEncoding="UTF-8"
        executor="tomcatThreadPool"
        keepAliveTimeout="20000"
        secretRequired="true"
        secret=" AOPS-KeySecure"
    />
```

► Sinon, mettre secretRequired="false" :

« secret » absent	ancien attribut « secure »
<Connector port="8029" protocol="AJP/1.3" URIEncoding="UTF-8" executor="tomcatThreadPool" keepAliveTimeout="20000" secretRequired="**false**" />	<Connector port="8029" protocol="AJP/1.3" URIEncoding="UTF-8" executor="tomcatThreadPool" keepAliveTimeout="20000" secretRequired="**false**" secure=" AOPS-KeySecure" />

7.7 Connexion bloquée si serveur Apache installé sur un autre serveur que arcOpole PRO Serveur.

Si votre serveur Apache est situé sur un autre serveur que le serveur arCOpole PRO Serveur, la connexion peut être bloquée dans certaine configuration lors de l'activation du protocole sécurisé de l'AJP.

Dans ce cas, il faut ajouter la ligne suivante dans la configuration de l'AJP dans le fichier « server.xml », après la ligne « protocol="AJP/1.3" » :

```
address="0.0.0.0"
```

Ce paramètre supplémentaire permet au serveur Tomcat d'écouter sur toutes les interfaces réseau du serveur Tomcat, avec le protocole IPv4.

Pour les explications détaillées de l'usage de ce paramètre ainsi que des autres paramètres de configuration du serveur Tomcat, vous reporter à la documentation officielle de Tomcat : Apache Tomcat 10 (10.1.54) - Documentation Index

Ce qui donne :

```
<Connector port="8029"
    protocol="AJP/1.3"
    address="0.0.0.0"
    URIEncoding="UTF-8"
    executor="tomcatThreadPool"
    keepAliveTimeout="20000"
```

```
  secretRequired="true"
   secret=" AOPS-KeySecure"
/>
```