

- ASFA -

Statistiques TIS

Plateforme SFTP

Références du document		
Nom document / révision :	TIS_Statistiques_TC-TSP_Proc_Plateforme-ASFA_V06_Valide-20231220.docx	
Date de création :	26 février 2020	
Auteur(s) :	Jérôme NOURICHARD	
Nombre total de pages :	9	
Diffusion :	ASFA, SCA, émetteurs Liber-t, émetteurs TIS SET, 6TM	
Classification :	Diffusable : <input checked="" type="checkbox"/>	Confidentiel : <input checked="" type="checkbox"/>
Etat du document	Draft : <input type="checkbox"/>	Validé : <input checked="" type="checkbox"/>

Versions

Version	Date	Objet de la modification
V01	02/02/2020	Première diffusion
V02	06/05/2020	Précision sur l'extension des archives compressées Support à venir du format .gz Palliatif en cas de renommage impossible des fichiers en fin de transmission Modification de la procédure d'initialisation pour tenir compte des cas : - De plateformes de transmission partagées par plusieurs acteurs - De comptes SFTP d'acteur partagés par deux plateformes de transmission
V03	04/06/2020	Corrections mineures
V04	05/08/2020	Mise à jour suite au passage en production du support du format .gz Inclusion d'un .csv contenant les indicateurs en erreur dans le compte-rendu d'erreur de contrôle d'intégrité
Vs05	28/10/2020	Ajout d'un environnement de test sur la plateforme SFTP Nouvelle version du schéma XML
V06	08/12/2023	Mise à jour des exemples pour le TIS SET (3.4) Mise à jour de la référence au schéma XML

Documents de référence

Nom du document	Référence
<i>TIS_Statistiques_TC-TSP_Spec_Schema-XML_V13_Valide-20231220.xsd</i>	[D1]

Sommaire

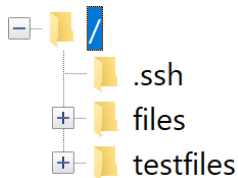
1. Structure de la plateforme SFTP	3
2. Connexion à la plateforme SFTP.....	3
2.1. Première connexion à la plateforme	3
2.2. Génération d'une paire de clés privée et publique.....	4
2.3. Transfert de la clé publique sur la plateforme	5
2.4. Connexions suivantes.....	6
3. Echanges de fichiers avec la plateforme.....	7
3.1. Arborescence SFTP pour les échanges et les traitements en environnement de production..	7
3.2. Arborescence SFTP pour les échanges et les traitements en environnement de test	7
3.3. Format et nom des fichiers.....	7
3.3.1. Flux statistiques à traiter	7
3.3.2. Compte-rendu de traitement OK	8
3.3.3. Compte-rendu de traitement en erreur	8
3.4. Transmission des flux et récupération des comptes-rendus.....	8

1. Structure de la plateforme SFTP

Sur la plateforme, chaque acteur dispose d'une racine et d'un login spécifiques à son rôle (TC ou TSP).

Un acteur à la fois TC et TSP (concessionnaire et émetteur Liber-t) dispose donc de deux logins permettant d'accéder à deux racines SFTP distinctes pour déposer les flux correspondants à ses rôles respectifs sur la plateforme.

La racine SFTP de chaque acteur contient trois répertoires dont l'utilisation est décrite dans les chapitres qui suivent :



Cinq autres fichiers système y sont également présents, ils n'ont pas d'utilité pour l'acteur, ne sont ni effaçables ni utilisables et doivent être ignorés.

2. Connexion à la plateforme SFTP

La connexion à la plateforme nécessite d'être initialisée manuellement par l'acteur à partir de la machine qui effectuera les transmissions, afin de permettre l'automatisation des connexions futures (par script ou application de transfert).

2.1. Première connexion à la plateforme

La première connexion est obligatoirement manuelle et doit se faire :

- Avec le **login** et le **mot de passe** propre à l'acteur et à son rôle et qui lui auront été transmis par l'ASFA de manière sécurisée ;
- Sur la machine qui effectuera les transmissions de flux statistiques ;
- Avec le compte utilisateur local sous lequel le script ou l'application de transfert s'exécutera.

Avec une ligne de commande Windows ou Linux :

```
sftp login_acteur@srv2871.sd-france.net
The authenticity of host 'srv2871.sd-france.net (188.130.11.101)' can't be established.
ECDSA key fingerprint is SHA256:6zBJQTD7f6ou04LonvuLU8MAjiqIl3ThtaW5n7KEEM0.
Are you sure you want to continue connecting (yes/no)?
```

Répondre **yes**

```
Warning: Permanently added 'srv2871.sd-france.net,188.130.11.101' (ECDSA) to the list of
known hosts.
```

```
login_acteur@srv2871.sd-france.net's password:
```

Entrer le **mot de passe** transmis par l'ASFA pour le login *

```
Connected to login_acteur@srv2871.sd-france.net.
sftp>
```

Taper **exit** pour sortir

```
sftp> exit
```

* : si utilisation du copier/coller, ne le faire qu'à la souris, pas au clavier (le mdp serait rejeté).

Relancer la connexion pour vérification :

```
sftp login_acteur@srv2871.sd-france.net
login_acteur@srv2871.sd-france.net's password:
```

Entrer le **mot de passe** transmis par l'ASFA pour le login

```
ConConnected to login_acteur@srv2871.sd-france.net.
sftp>
```

Fermer la connexion :

```
sftp> exit
```

2.2. Génération d'une paire de clés privée et publique

Si la génération a déjà été réalisée une première fois (cas d'une plateforme de transmission partagée par plusieurs acteurs ou qui a déjà une clé privée), **passer directement à l'étape 2.3.**

Cette opération utilise OpenSSH, elle est obligatoirement manuelle et doit se faire :

- Sur la machine qui effectuera les transmissions de flux statistiques ;
- Avec le compte utilisateur local sous lequel le script ou l'application de transfert s'exécutera.

Avec une ligne de commande Windows * :

```
ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\compte_local\.ssh\id_rsa):
```

Confirmer par **Entrée**

```
Enter passphrase (empty for no passphrase):
```

Confirmer par **Entrée** (ne pas saisir de passphrase)

```
Enter same passphrase again:
```

Confirmer par **Entrée**

```
Your identification has been saved in C:\Users\compte_local\.ssh\id_rsa.
Your public key has been saved in C:\Users\compte_local\.ssh\id_rsa.pub.
The key fingerprint is:
SHA256:U+K6zaGJwlkdeCdf/6CKYpJg40a4QqCimP6oUu1rvVs compte_local@nom_machine_locale
The key's randomart image is:
+---[RSA 2048]-----+
|
| . . .
| o . +..o.
|= . o =S. .
|+=. o .... o
|X= = .. E . o
|B.B =..O .. .
|B+.*ooBo+.
+---[SHA256]-----+
```

Avec une ligne de commande Linux * :

```
ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/compte_local/.ssh/id_rsa):
```

Confirmer par **Entrée**

```
Enter passphrase (empty for no passphrase):
```

Confirmer par **Entrée** (ne pas saisir de passphrase)

```
Enter same passphrase again:
```

Confirmer par **Entrée**

```
Your identification has been saved in (/home/compte_local/.ssh/id_rsa.
Your public key has been saved in (/home/compte_local/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:U+K6zaGJwlkdeCdf/6CKYpJg40a4QqCimP6oUu1rvVs compte_local@nom_machine_locale
The key's randomart image is:
+---[RSA 2048]-----+
|
| . . .
| o . +..o.
|= . o =S. .
|+=. o .... o
|X= = .. E . o
|B.B =..O .. .
|B+.*ooBo+.
+---[SHA256]-----+
```

* : les caractères affichés à la génération de la clé dépendent de la clé et de la machine.

2.3. Transfert de la clé publique sur la plateforme

Cette opération est obligatoirement manuelle et doit se faire :

- Avec le **login** et le **mot de passe** propre à l'acteur et à son rôle et qui lui auront été transmis par l'ASFA de manière sécurisée ;
- Sur la machine qui effectuera les transmissions de flux statistiques ;
- Avec le **compte utilisateur local** sous lequel le script ou l'application de transfert s'exécutera.

Copie de la clé publique dans le fichier *authorized_keys* en ligne de commande Windows :

```
copy C:\Users\compte_local\.ssh\id_rsa.pub authorized_keys
1 fichier(s) copié(s).
```

Copie de la clé publique dans le fichier *authorized_keys* en ligne de commande Linux :

```
cp /home/compte_local/.ssh/id_rsa.pub authorized_keys
```

Dans le cas d'un même login d'acteur utilisé par deux plateformes de transmissions distinctes, après exécution de cette étape 2.3 sur la première machine, il faut récupérer puis compléter, sur la seconde machine, le fichier *authorized_keys* généré sur la première :

Compléter le fichier *authorized_keys* en ligne de commande Windows :

```
type C:\Users\compte_local\.ssh\id_rsa.pub >> authorized_keys
```

Compléter le fichier *authorized_keys* en ligne de commande Linux :

```
cat /home/compte_local/.ssh/id_rsa.pub >> authorized_keys
```

Suite de la procédure dans tous les cas de figures : transfert du fichier *authorized_keys* sur plateforme ASFA avec la même ligne de commande Windows ou Linux :

```
sftp login_acteur@srv2871.sd-france.net
login_acteur@srv2871.sd-france.net's password:
```

Entrer le **mot de passe** transmis par l'ASFA pour le login *

```
ConConnected to login_acteur@srv2871.sd-france.net.
sftp>
```

Entrer les commandes suivantes ** :

```
sftp> cd .ssh
sftp> pwd
Remote working directory: /.ssh
sftp> put authorized_keys
Uploading authorized_keys to /.ssh/authorized_keys
authorized_keys 100%
393 0.4KB/s 00:01
sftp>
```

Vérifier le bon transfert du fichier *authorized_keys* * :

```
sftp> ls -l
-rw-r--r-- 1 1036 1036 393 Feb 28 12:34 authorized_keys
sftp>
```

Fermer la connexion :

```
sftp> exit
```

* : si utilisation du copier/coller, ne le faire qu'à la souris, pas au clavier (le mdp serait rejeté).

** : les valeurs affichées pour le fichier dépendent de la clé, de la machine et du login SFTP.

2.4. Connexions suivantes

A partir de ce moment, la connexion à la plateforme ne demande plus le mot de passe et se fait uniquement avec le **login** propre à l'acteur et par contrôle des clés générées. Elle peut être automatisée, dans un script Windows ou Linux ou via une application de transfert, sous réserve :

- Que les transmissions de flux statistiques s'exécutent sur la machine sur laquelle les opérations précédentes ont été réalisées ;
- Que le script ou l'application de transfert s'exécute avec le compte utilisateur local sous lequel les opérations précédentes ont été réalisées.

Connexion en une ligne de commande Windows ou Linux :

```
sftp login_acteur@srv2871.sd-france.net  
Connected to login_acteur@srv2871.sd-france.net.  
sftp>
```

Fermer la connexion :

```
sftp> exit
```

Pour une connexion avec une application de transfert, il sera nécessaire d'importer préalablement dans l'application la clé privée générée en 2.2 :

- C:\Users\compte_local\.ssh\id_rsa sous Windows,
- /home/compte_local/.ssh/id_rsa sous Linux.

Mode opératoire pour FileZilla : <https://tecadmin.net/import-private-key-in-filezilla/>

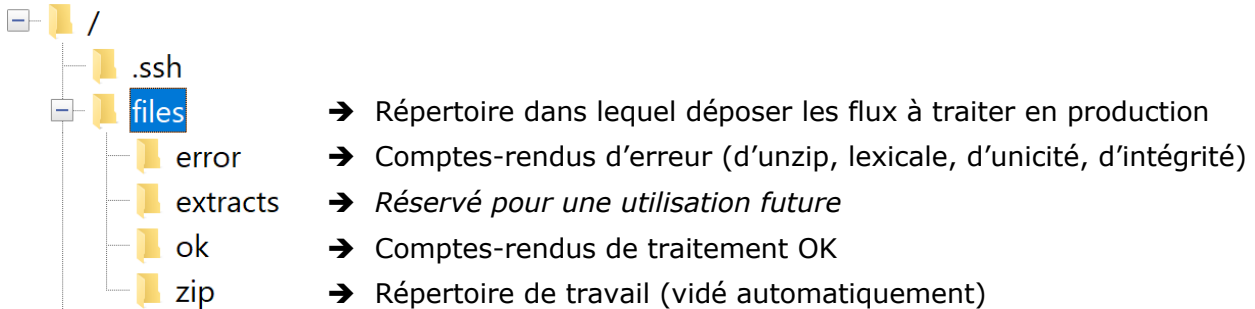
Mode opératoire pour Gateway :

- https://docs.axway.com/bundle/Gateway_6172_UsersGuide_allOS_en_HTML5/page/Content/Managing_Security/Certificates_and_keys/managing_keys_CLI.htm#secadm_import_key
- https://docs.axway.com/bundle/Gateway_6172_UsersGuide_allOS_en_HTML5/page/Content/Managing_Security/SSH/SSH_Security_profiles_GUI_.htm

3. Echanges de fichiers avec la plateforme

3.1. Arborescence SFTP pour les échanges et les traitements en environnement de production

Le répertoire **files** dans la racine de chaque acteur contient l'arborescence suivante :

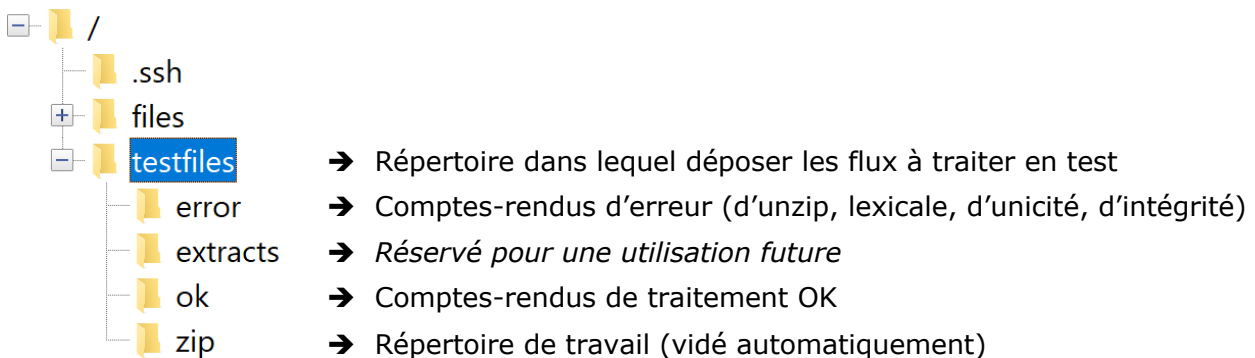


Une fois le flux traité par la plateforme, il est supprimé du répertoire **files** et son compte-rendu de traitement est déposé dans le sous-répertoire **ok** ou **error** selon le résultat du traitement.

Il appartient à chaque acteur de récupérer régulièrement les comptes-rendus de traitement dans les sous-répertoires **ok** et **error** et de les vider.

3.2. Arborescence SFTP pour les échanges et les traitements en environnement de test

Le répertoire **testfiles** dans la racine de chaque acteur contient l'arborescence suivante, analogue à celle de l'environnement de production :



Une fois le flux traité par la plateforme, il est supprimé du répertoire **testfiles** et son compte-rendu de traitement est déposé dans le sous-répertoire **ok** ou **error** selon le résultat du traitement.

Il appartient à chaque acteur de récupérer régulièrement les comptes-rendus de traitement dans les sous-répertoires **ok** et **error** et de les vider.

A partir du 1^{er} janvier 2021 (fin de la période de VABF), l'utilisation de l'environnement de test sera obligatoire pour tous les flux de tests transmis à la plateforme.

3.3. Format et nom des fichiers

3.3.1. Flux statistiques à traiter

Les flux doivent être au format xml et conformes au schéma [D1].

Ils doivent être transmis dans des archives compressées : sont supportés les formats **.zip** et **.gz**. Aucun autre format n'est supporté (entre autres, .tar.gz n'est pas supporté).

Il ne doit y avoir qu'un seul flux xml par archive compressée.

Plusieurs archives compressées peuvent être transmises simultanément.

Aucune convention de nommage n'est imposée aux acteurs : la seule contrainte à respecter est que le nom de chaque flux et de chaque archive zip soient **uniques**, pour éviter tout écrasement de fichiers dans les transmissions et la décompression.

Il peut néanmoins être utile (mais non obligatoire) que les noms des flux et des archives compressées incluent les valeurs qui constituent la clé unique de chaque flux (cf. les champs de l'élément WeekPublication du flux xml : *StatType*, *StatIssuer*, *Domain*, *OpArea*, *Year*, *WeekNum*, *PublicationTime*) : en plus de faciliter leur identification, cela garantit aussi l'unicité des noms des fichiers.

Les archives compressées, une fois transmises, doivent avoir une extension **.zip** ou **.gz** (selon le format retenu).

Pendant la transmission, il est recommandé que les archives compressées aient une extension **.tmp** (qui garantira que ces archives ne seront pas traitées par la plateforme en cours de transmission) et soient renommées par l'acteur une fois leur transmission terminée.

Le traitement des flux transmis s'exécute toutes les quarts d'heure. Pour diminuer les risques de traitement avant la fin de transmission, une archive compressée détectée par la plateforme ne sera pas prise en compte par le premier traitement mais par celui du quart d'heure suivant.

3.3.2. Compte-rendu de traitement OK

Le compte-rendu de traitement OK est l'archive compressée traitée (.zip ou .gz) dont le nom a été préfixé par « **Accepted-AAAA-MM-DD-hhmmss-** », AAAA-MM-DD-hhmmss étant le timestamp du traitement OK.

3.3.3. Compte-rendu de traitement en erreur

Le compte-rendu de traitement en erreur est une archive .zip dont le nom est composée de celui de l'archive traitée préfixé par ce qui suit et qui contient le log de la cause du rejet ainsi que l'archive compressée traitée :

- « **ERR-Rejected-AAAA-MM-DD-hhmmss-** » pour les erreurs de décompression, de contrôle lexical ou d'unicité du flux
- « **ERR-Integrity-AAAA-MM-DD-hhmmss-** » pour les erreurs de contrôle d'intégrité,

AAAA-MM-DD-hhmmss étant le timestamp du traitement en erreur.

Les comptes-rendus d'erreur de contrôle d'intégrité incluent également un .csv qui contient les indicateurs en erreur d'intégrité.

Un traitement en erreur entraîne le rejet du flux : le flux corrigé devra être retransmis par l'acteur.

3.4. Transmission des flux et récupération des comptes-rendus

La connexion se faisant maintenant par contrôle de clés sans saisi de mot de passe, la transmission des flux et la récupération des comptes-rendus peut être automatisée dans un script de commandes Windows, Linux ou dans une application de transfert qui le permet.

Pour les automatisation par script, SFTP pourra être utilisé en mode batch avec un **fichier de commandes** SFTP (cf. <https://man.openbsd.org/sftp>).

Lancement en mode batch en ligne de commande Windows ou Linux :

```
sftp -b command_file login_acteur@srv2871.sd-france.net
```

La connexion est automatiquement fermée lorsque les commandes SFTP contenues dans le fichier de commandes ont été exécutées.

Exemple (TC) d'un fichier de commandes SFTP pour transmettre des flux en environnement de production :

```
cd files
put TCxxx_202322_LIBERT_20230529093000.tmp
put TCxxx_202322_TISPL_20230529093005.tmp
put TCxxx_202322_TISVL_20230529093010.tmp
rename TCxxx_202322_LIBERT_20230529093000.tmp TCxxx_202322_LIBERT_20230529093000.zip
rename TCxxx_202322_TISPL_20230529093005.tmp TCxxx_202322_TISPL_20230529093005.zip
rename TCxxx_202322_TISVL_20230529093010.tmp TCxxx_202322_TISVL_20230529093010.zip
```

Exemple (TSP TIS-VL) d'un fichier de commandes SFTP pour transmettre des flux en environnement de production :

```
cd files
put TSPxxx_202322_TISVL_OPA1_20230529100000.tmp
put TSPxxx_202322_TISVL_OPA2_20230529100005.tmp
rename TSPxxx_202322_TISVL_OPA1_20230529100000.tmp TSPxxx_202322_TISVL_OPA1_20230529100000.zip
rename TSPxxx_202322_TISVL_OPA2_20230529100005.tmp TSPxxx_202322_TISVL_OPA2_20230529100005.zip
```

Exemple (TC ou TSP) d'un fichier de commandes SFTP pour récupérer les comptes-rendus en environnement de production :

```
cd files/ok
-get *.zip
-rm *.zip
cd ../error
-get *.zip
-rm *.zip
```

Exemple (TC) d'un fichier de commandes SFTP pour transmettre des flux en environnement de test :

```
cd testfiles
put TCxxx_202322_LIBERT_20230529093000.tmp
put TCxxx_202322_TISPL_20230529093005.tmp
put TCxxx_202322_TISVL_20230529093010.tmp
rename TCxxx_202322_LIBERT_20230529093000.tmp TCxxx_202322_LIBERT_20230529093000.zip
rename TCxxx_202322_TISPL_20230529093005.tmp TCxxx_202322_TISPL_20230529093005.zip
rename TCxxx_202322_TISVL_20230529093010.tmp TCxxx_202322_TISVL_20230529093010.zip
```

Exemple (TSP TIS-VL) d'un fichier de commandes SFTP pour transmettre des flux en environnement de test :

```
cd testfiles
put TSPxxx_202322_TISVL_OPA1_20230529100000.tmp
put TSPxxx_202322_TISVL_OPA2_20230529100005.tmp
rename TSPxxx_202322_TISVL_OPA1_20230529100000.tmp TSPxxx_202322_TISVL_OPA1_20230529100000.zip
rename TSPxxx_202322_TISVL_OPA2_20230529100005.tmp TSPxxx_202322_TISVL_OPA2_20230529100005.zip
```

Exemple (TC ou TSP) d'un fichier de commandes SFTP pour récupérer les comptes-rendus en environnement de test :

```
cd testfiles/ok
-get *.zip
-rm *.zip
cd ../error
-get *.zip
-rm *.zip
```

===== Fin du document =====