Manuel FDS

File Delivery Services

Transfert de fichiers SFTP

Editeur

La Poste CH SA
Informatique
Webergutstrasse 12
CH-3030 Berne (Zollikofen)

Contact

La Poste CH SA
Informatique
Webergutstrasse 12
CH-3030 Berne (Zollikofen)
IT17.34 FDS Betrieb
Courriel : fds@post.ch

Version 8.5 / janvier 2023

Télécharger la version actuelle : https://www.post.ch/fds

Table des matières

1. Introduction 4
2. Le modèle FDS de La Poste Suisse 5
2.1 Vue d'ensemble 5
2.2 Protocole pris en charge 5
2.3 Types de connexion 5
3. Les services FDS 6
3.1 Les File Delivery Services 6
3.2 Où se trouvent les File Delivery Services? 6
3.3 Protocoles de transfert de fichiers 6
3.3.1 SFTP 6
3.3.2 Logiciels clients recommandés ..... **Error! Bookmark not defined.**
3.4 Livraison et récupération sur des serveurs externes 6
3.5 Utilisation du File Delivery Service 6
4. Sécurité 7
4.1 Nom d'utilisateur (login) 7
4.2 Cryptage de liaison 7
4.2.1 Pour tous les types de connexions 7
4.2.2 MPLS/IPSS 7
4.2.3 LAN-LAN 7
5. Configuration 8
5.1 Configuration FDS client-serveur 8
5.1.1 Serveur de transfert de fichiers 8
5.1.2 Cache DNS 8
5.1.3 Ports 8
5.1.4 Noms d'utilisateur (login) 8
5.1.5 Répertoires 8
5.1.6 Noms des fichiers 8
5.2 SFTP 8
5.2.1 Généralités 8
5.2.2 Envoyer une clé publique à IT Poste 9
5.2.3 Gestion des clés 9
6. Annexe A. Informations sur l'utilisation de FDS 10
6.1 Conditions-cadres/Restrictions 10
6.2 Restrictions concernant la livraison de fichiers (serveur → FDS client) 10
6.3 Exigences pour la transmission des données au client (serveur FDS → système de destination) 10
6.4 Exigences et restrictions concernant le téléchargement de données sur des systèmes tiers 11
7. Annexe B. Glossaire 12

1. Introduction

Les File Delivery Services (FDS) sont une offre de prestations de l'unité de services Informatique de La Poste CH SA.

FDS joue le rôle d'une passerelle dans le système de sécurité informatique entre l'Intranet de La Poste Suisse et les réseaux externes. Il permet l'échange mutuel de fichiers entre partenaires et applications internes et externes à la Poste.

Ce manuel décrit comment les fichiers peuvent être échangés avec le serveur FDS de la Poste Suisse. Ce service est à la disposition de tous les utilisateurs qui ont installé sur leur ordinateur un client sftp de transfert de fichiers et qui disposent du compte requis.

Informatique Poste décline toute responsabilité quant à l'exactitude des indications données dans ce document. Des erreurs et des modifications sont toujours possible.

2. Le modèle FDS de La Poste Suisse

2.1 Vue d'ensemble

L'origine du service FDS remonte à 1993. Il fut lancé dans le cadre du projet TTD-C de l'organisation PostFinance de l'époque. Les premiers transferts de fichiers furent effectués au moyen des protocoles Kermit, FTP et FTAM. En 1995, le service de transfert de fichiers fut complété par le protocole CONNECT:Direct™. Puis en 2002, on y ajouta le système FDS-SSH (FTP via SSH également appelé Secure FTP), alors que les protocoles FTAM et Kermit avaient déjà été retirés de l'offre.

En 2007, un changement de technologie et de génération eut lieu avec l'introduction de SFTP (SSH File Transfer Protocol). Le service FDS-SSH devint alors obsolète et fut retiré de l'offre en milieu de l'année 2010.

Depuis juin 2015, l'utilisation du protocole FTP est interdite pour les nouveaux utilisateurs pour des raisons de sécurité (les données ainsi que le nom de l'utilisateur et son mot de passe transitent en clair sur le réseau). Les utilisateurs actuels ont été migrés sur le protocole SFTP jusqu'à fin 2018.

2.2 Protocole pris en charge

- SFTP (SSH File Transfer Protocol)

2.3 Types de connexion

Trois types de connexion sont proposés :

- Internet
- MPLS/IPSS — lignes louées, réseau IPSS de Swisscom
- Intranet — pour partenaires/applications internes à la Poste

Pour les nouvelles lignes louées et MPLS, la mise en service sera fixée compte tenu du délai d'installation de l'opérateur de réseau concerné. On utilise une ligne louée lorsqu'un autre raccordement se révèle plus onéreux ou suite à des impératifs particuliers en matière de sécurité. Les connexions ADSL sont possibles uniquement sur Internet avec un fournisseur d'accès. Il est à souligner que l'utilisation de lignes louées ou de connexions VPN est rendue superflue par l'emploi du protocole SFTP et que ces premières nommées n'amènent aucune sécurité supplémentaire.

3. Les services FDS

3.1 Les File Delivery Services

Les File Delivery Services sont basés sur un système spécial de messagerie qui répond aux exigences accrues en matière de sécurité sur Internet, Extranet et Intranet.

3.2 Où se trouvent les File Delivery Services?

Les services FDS se composent de plusieurs serveurs applicatifs, serveurs de bases de données et de plusieurs serveurs de périmètre. Tous ces composants se situent dans des zones différentes (DMZ) de la plate-forme IX. Cette dernière constitue la zone de sécurité protégée par des pare-feu entre le réseau de la Poste (Intranet) et les réseaux externes (Internet, lignes louées). Les serveurs de transfert de fichiers et de bases de données sont situés dans une zone hautement protégée, dont l'accès est strictement limité. Les serveurs de périmètre sont placés dans des zones un peu moins protégées, dont l'accès avec des logiciels clients est autorisé. Les connexions client-serveur provenant des réseaux externes et du réseau postal interne passent toujours par les serveurs de périmètre. Les services FDS sont dimensionnés de telle manière qu'ils restent disponibles même en cas de la défaillance totale d'un centre de calcul.

3.3 Protocoles de transfert de fichiers

De plus amples informations sont à disposition dans notre « Manuel des logiciels de transferts de fichiers » à l'adresse https://www.post.ch/fds

3.3.1 SFTP

SFTP (SSH Secure File Transfer Protocol) est un protocole de transfert de fichiers sécurisé. Une connexion cryptée de bout en bout est établie entre le client et le serveur, rendant les données et noms d'utilisateurs illisibles en cas de piratage. Grâce à l'authentification par clé publique, l'intégrité et la confidentialité des données échangées sont assurées. En outre, l'authentification par clé publique rend possible la connexion des clients sur le serveur sans interaction de l'utilisateur. SSH garantit la transmission complète et inchangée des données de l'expéditeur au destinataire. Seuls sont pris en charge SSH-2 (version 2) et l'authentification par clé publique.

On utilise un client **SFTP** pour établir une connexion avec le serveur SFTP FDS et exécuter les commandes nécessaires.

Attention : SFTP ne doit pas être confondu avec FTPS (FTP via SSL) ou FTP via SSH (parfois nommé SecureFTP).

3.4 Livraison et récupération sur des serveurs externes

Certaines conditions doivent être remplies dans le cas où l'on souhaite que FDS distribue les fichiers ou les récupère auprès du client. Ces conditions sont mentionnées au chapitre 6.

La livraison et la distribution d'un fichier se déroule en fonction des événements. Après la réception d'un fichier, celui-ci est transféré du serveur FDS aux destinations prévues. Il est impossible de déterminer un moment précis pour l'exécution d'une action.

3.5 Utilisation du File Delivery Service

L'inscription administrative pour utiliser les services FDS s'effectue auprès du service à la clientèle de l'unité de services ou de l'unité d'affaires de La Poste Suisse concernée.

Hotline: +41 (0)848 800 030
Pour toute demande concernant File Delivery Services, l'adresse électronique suivante est à votre disposition : fds@post.ch

4. Sécurité

4.1 Nom d'utilisateur (login)

Les participants externes reçoivent un nom d'utilisateur par unité de services et unité d'affaires. Si un client utilise pour plusieurs unités d'affaires de son entreprise un seul et même nom d'utilisateur, La Poste CH SA décline toute responsabilité pour les dommages pouvant résulter de l'accès global, ainsi possible, aux données du serveur de transfert de fichiers de la Poste.

4.2 Cryptage de liaison

Le cryptage de liaison n'est pas une prestation standard des services FDS. Il peut toutefois être utilisé comme option de réseau. Il est à souligner que le cryptage de la liaison est rendu superflu par l'emploi du protocole SFTP et n'amène aucune sécurité supplémentaire.

4.2.1 Pour tous les types de connexions

Le protocole SFTP est disponible pour le cryptage client à serveur de tous les types de connexions.

4.2.2 MPLS/IPSS

MPLS/IPSS permet de réaliser un cryptage de liaison.

4.2.3 LAN-LAN

Pour les connexions LAN-LAN, un cryptage de liaison peut être établi avec les deux routeurs.

5. Configuration

5.1 Configuration FDS client-serveur

5.1.1 Serveur de transfert de fichiers

Zone	Nom de l'hôte
Internet et lignes louées	fdsbc.post.ch
Réseau postal/DMZ	fdsbc.pnet.ch

La répartition de charge (load balancing) sur deux sites s'effectue au moyen d'un DNS round-robin. Cela signifie que les adresses IP des deux centres de calcul sont renvoyées à tour de rôle.

Il faut s'assurer que la communication vers ou depuis FDS est autorisée dans votre réseau. Dans la majorité des cas, l'équipe responsable du réseau doit autoriser les connexions avec des règles correspondantes sur votre pare-feu (firewall). Les deux adresses IP correspondantes à la plateforme FDS ne doivent être utilisées que pour la configuration du firewall. Pour la connexion depuis votre application de transfert de fichiers, il est essentiel d'employer l'adresse DNS.

FDS supporte aussi bien IPv4 que IPv6. L'utilisation d'IPv6 requiert un support continue d'IPv6 dans votre infrastructure.

5.1.2 Cache DNS

La plateforme FDS est exploitée sur deux sites dans une configuration active/active. Le mécanisme de basculement est assuré par un „Global Server Load Balancing (GSLB)„. Afin de profiter d'un basculement rapide de la connexion à FDS en cas de problèmes, vous devez vous assurer qu'il n'existe pas de cache DNS supplémentaire dans votre environnement. Les indications concernant le Time to live (TTL) du DNS de la Poste doivent être respectées.

5.1.3 Ports

Le protocole SFTP est atteignable sur son port standard (22).

5.1.4 Noms d'utilisateur (login)

Les noms d'utilisateurs sont communiqués lors de la mise en service de la prestation.

5.1.5 Répertoires

Les noms des répertoires sur le serveur FDS sont toujours écrits en minuscules, avec les restrictions suivantes :

- caractères : [a-z], [0-9], [. -] (point, trait d'union)
- début : le premier caractère doit être [a-z], [0-9]

5.1.6 Noms des fichiers

Concernant les noms des fichiers placés dans les répertoires du serveur FDS, les directives suivantes doivent être respectées :

- caractères : [A-Z], [a-z], [0-9], [. - _] (point, trait d'union, underscore)

5.2 SFTP

5.2.1 Généralités

De plus amples informations sont à disposition dans notre « Manuel des logiciels de transferts de fichiers » à l'adresse https://www.post.ch/fds

5.2.2 Envoyer une clé publique à IT Poste

Une copie de la clé publique doit être envoyée à Informatique Poste par courriel (fds@post.ch). Afin d'éviter une fraude éventuelle, la clé publique doit être envoyée par la personne de contact de l'entreprise concernée ou à tout le moins, le nom de cette personne doit apparaître dans l'échange de courriel.

Si cela est souhaité, plusieurs clés publiques peuvent être configurées pour le même nom d'utilisateur. De la même manière, plusieurs noms utilisateurs peuvent employer la même clé.

La clé SSH doit avoir une longueur minimale de 4096 bits.

5.2.3 Gestion des clés

Traitez votre clé privée comme votre propre carte de crédit ! Protégez-la contre tout accès non autorisé.

6. Annexe A. Informations sur l'utilisation de FDS

La présente information résume les règles et les prescriptions à validité générale pour la transmission de fichiers avec les serveurs FDS. Il s'adresse aux utilisateurs FDS des unités d'affaires et des sociétés du groupe de la Poste Suisse et leurs clients externes.

6.1 Conditions-cadres/Restrictions

a) FDS n'est pas un système d'archivage. Les fichiers à récupérer, que le client n'a pas encore supprimés, seront dans tous les cas automatiquement effacés du serveur au bout de 9 jours.

b) Chaque fichier peut être téléchargé 20 fois au maximum.

c) Le cycle de traitement de FDS est de 1 minute. Les fichiers délivrés arrivent 1 minute après la fin du transfert de fichiers dans la boîte de réception du destinataire. Si la configuration exige que les fichiers soient transférés à un serveur de destination, cela peut prendre plus de temps, selon la taille et le nombre des fichiers.

d) Les gros fichiers doivent, si possible, être transmis après avoir été compressés. L'expéditeur et le destinataire (de bout en bout) s'accordent sur le type de compression (p.ex. GZIP).

e) Pour transmettre un grand nombre de fichiers, on effectuera un grand nombre de transferts (put/get) par session FTP/SFTP. Exemple pour 1200 fichiers : 10 connexions/logins FTP avec chacun 120 transferts de fichiers. Si le nombre de logins durant une unité de temps déterminée est trop grand, le système de prévention des intrusions de La Poste CH SA bloque automatiquement les adresses IP sources durant 15 minutes.

f) FDS ne confirme pas à l'expéditeur le transfert de fichiers. La création et l'envoi de confirmations incombent au destinataire et ne sont pas effectués par les services FDS.

g) En cas de retransmission à d'autres destinataires, l'ordre des fichiers transférés n'est pas garanti. Des fichiers de tailles différentes peuvent se doubler sur le trajet en cas de transmission en parallèle. Le système de réception de la relation de bout en bout est responsable de rétablir l'ordre correct des fichiers transmis.

h) Le transfert et la distribution des fichiers s'effectuent en fonction des événements. Une gestion temporelle est impossible.

i) Informatique Poste doit être informée au préalable de la taille, de la fréquence et des modifications de volumes des fichiers pour tous les transferts passant par les serveurs FDS. Cela est indispensable pour garantir la disponibilité de la capacité nécessaire au moment souhaité.

j) Informatique Poste doit être informée des priorités en cas d'escalade pour tous les transferts de fichiers passant par les serveurs FDS. Le SLA standard s'applique à tous les autres cas.

6.2 Restrictions concernant la livraison de fichiers (serveur → FDS client)

- Si un client de transfert de fichiers exécute une fonction de livraison (put) dans une boîte de messagerie FDS (répertoire), les fichiers sont traités par les processus sur le serveur FDS sitôt le transfert terminé. Les fichiers restent cependant visibles pour le client durant deux minutes dans les boîtes de messagerie «upload» (affichage des fichiers avec «dir» et «ls»). **La suppression ou le changement de nom d'un fichier envoyé est sans effet : celui-ci sera toujours retransmis au destinataire avec son nom initial.**
- FDS garantit que seuls les fichiers transférés de manière complète sont traités. Dans le cas d'une interruption de la connexion, les fichiers incomplets sont éliminés.
- Une modification des attributs du fichier après son transfert est impossible sur le serveur FDS.

6.3 Exigences pour la transmission des données au client (serveur FDS → système de destination)

Pour que le service FDS puisse transmettre les fichiers ou clients, les exigences suivantes doivent être remplies par les destinataires internes et externes à la Poste:

– connexions permanentes au réseau, telles qu'un accès WAN (MPLS) ou Internet,
– système disponible 24 heures sur 24 et 7 jours sur 7,
– exploitation garantie du centre de calcul,
– interlocuteurs pour le support (numéros de téléphone, courriels) définis et joignables.

6.4 Exigences et restrictions concernant le téléchargement de données sur des systèmes tiers

FDS peut automatiquement télécharger des fichiers avec SFTP sur des systèmes tiers.
Cette fonctionnalité ne devrait toutefois être utilisée que dans des cas exceptionnels.

Conditions préalables:
- connexion permanente au réseau, telle qu'un accès WAN (MPLS) ou Internet,
- système disponible 24 heures sur 24 et 7 jours sur 7,
– exploitation garantie du centre de calcul,
– interlocuteurs pour le support (numéros de téléphone, courriels) définis et joignables.

Restrictions:
- Ce service n'est pas proposé si des données urgentes doivent être téléchargées dans un intervalle inférieur à 30 minutes.
- Les fichiers à télécharger doivent se trouver dans des répertoires ayant des noms invariables. FDS n'effectue pas de téléchargement depuis des répertoires à noms variables (par exemple un répertoire contenant la date du jour actuel).

7. Annexe B. Glossaire

D	DMZ	Zone démilitarisée– Une DMZ se trouve à un raccordement LAN séparé d'un pare-feu, entre un réseau interne et un réseau non sûr, p. ex. Internet. Dans la DMZ, se trouvent fréquemment des serveurs fournissant des services pour utilisateurs Internet (p. ex. www ou messagerie).. Dans l'idéal une DMZ se situe entre deux pare-feu physiquement séparés l'un de l'autre. Le pare-feu externe protège des attaques de l'extérieur et contrôle chaque accès Internet à la DMZ. Le pare-feu interne contrôle l'accès depuis la DMZ au réseau interne et inversement. Il représente ainsi une deuxième ligne de défense, au cas où le pare-feu externe céderait aux attaques Cela présente l'avantage que le réseau interne reste protégé même si un agresseur parvient jusqu'au serveur web.
	DNS	Domain Name System (DNS): un des services les plus importants sur Internet. Sa tâche principale est la conversion de noms d'adresses Internet en adresses IP correspondantes.
E	End-to-End	De bout en bout. Relation entre une application (p.ex. VEC-I) d'une unité d'affaires de la Poste CH SA (p.ex. PostFinance SA) et l'application du client externe.
F	FDS	File Delivery Services est une offre de prestation de l'unité de services Technologies de l'information (IT) de La Poste CH SA. FDS joue le rôle de proxy dans le système de sécurité IT entre l'Intranet de La Poste Suisse et les réseaux externes. Il permet l'échange de fichiers entre partenaires et applications internes et externes à la Poste.
I	IPSS	LAN Interconnect over IPSS est un service de Swisscom, qui peut interconnecter des réseaux locaux en une unique infrastructure de communication pour toute une entreprise. IPSS est une solution «propre à Swisscom» caractérisée par une technologie des plus modernes. La technologie MPLS (Multi Protocol Label Switching) utilisée pour IPSS permet une grande flexibilité en ce qui concerne la bande passante. Le service est entièrement fourni par Swisscom Enterprise Solution. http://www.swisscom.com/es/
M	MPLS	MPLS (Multiprotocol Label Switching) est une implémentation du Label Switching, qui permet de décharger fortement les routeurs impliqués dans le transport d'un paquet de données, car il réduit le niveau de complexité à celui d'un commutateur (switch). Il obtient cette réduction en établissant un chemin fixe au début de la transmission des données. Les routeurs se trouvant sur ce chemin ne doivent plus rechercher quel est le destinataire des paquets de données à transférer, mais transmettent ces paquets, sans autre traitement, le long du chemin connecté au préalable.
S	SFTP	SSH File Transfer Protocol (abrégé: SFTP) est un perfectionnement du protocole SCP et permet à un ordinateur client de transférer ses données de manière sûre sur des systèmes distants ainsi que d'accéder en toute sécurité aux fichiers qui s'y trouvent. . Ce protocole ne comprend ni l'authentification ni le cryptage, fonctions devant être prises en charge par le protocole SSH sous-jacent. SFTP ne doit pas être confondu avec le protocole Secure FTP (FTP via SSH) ou avec FTP via SSL.
	SSH	SSH permet une communication sécurisée de manière cryptographique sur des réseaux non sécurisés et sécurisés. Il offre un niveau de sécurité élevé: authentification mutuelle fiable des partenaires ainsi qu'intégrité et confidentialité des données échangées. SSH garantit la transmission complète et inchangée des données entre l'expéditeur et le destinataire.