

# Instructions pour la migration de FDS BCM

## File Delivery Services

Passage à la plateforme FDS redondante entre sites

# Editeur

Poste CH SA  
Technologies de l'information  
Webergutstrasse 12  
CH-3030 Berne (Zollikofen)

# Contact

Poste CH SA  
Technologies de l'information  
Webergutstrasse 12  
CH-3030 Berne (Zollikofen)  
IT261 FDS Exploitation  
E-mail: [fds@poste.ch](mailto:fds@poste.ch)

Version 2.1 / Mars 2016

Télécharger la version actuelle: <https://www.poste.ch/fds>

# Table des matières

<b>1. Introduction .....</b>	<b>4</b>
1.1 Architecture.....	5
1.2 Nouveautés .....	5
1.3 Connexions .....	6
<b>2. Introduction .....</b>	<b>7</b>
<b>3. Processus de migration .....</b>	<b>7</b>
3.1 Protocoles de communication .....	7
3.1.1 SFTP – Client vers la Poste .....	7
3.1.2 SFTP – Poste vers le client .....	7
3.1.3 Connect:Direct .....	8
3.2 Canaux de communication .....	8
3.2.1 Internet .....	8
3.2.2 Lignes louées.....	8
<b>4. Procédure en cas de sinistre .....</b>	<b>9</b>
<b>5. Remarques .....</b>	<b>9</b>
5.1 Cache DNS .....	9
5.2 Adresses IP .....	9

## 1. Introduction

File Delivery Services (FDS) est une offre de prestations de l'unité de services Technologies de l'information (IT) de Poste CH SA.

FDS joue le rôle de passerelle dans le système de sécurité IT entre l'intranet de Poste CH SA et les réseaux externes. Il permet l'échange de fichiers entre partenaires et applications internes et externes à la Poste.

En raison des exigences de révision à l'égard de Poste CH SA, le service est exploité de manière géographiquement redondante depuis le premier trimestre 2016.

Ces instructions aident les clients existants dans leur migration vers la solution redondante entre sites, appelée ci-dessous «FDS BCM».

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

## 1.1 Architecture

Un site est ajouté au service à haute disponibilité afin de compenser la défaillance d'un centre de calcul.

La répartition de la communication par l'intermédiaire des deux sites est obtenue à l'aide d'un DNS de répartition de charge (round-robin). Cela signifie que les adresses IP des deux sites sont retournées par alternance en cas de résolution DNS.

## 1.2 Nouveautés

La nouvelle architecture génère les innovations générales suivantes:

- Introduction d'un site secondaire
- Introduction d'un DNS de répartition de charge (round-robin)
- Modification du nom DNS
  - o Intégration

ANCIEN: fdsi.post.ch  
NOUVEAU: fdsbci.post.ch

- o Production

ANCIEN: fds.post.ch  
NOUVEAU: fdsbc.post.ch

- Support d'IPv4 et IPv6

L'utilisation d'IPv6 est facultative et nécessite un support d'IPv6 immédiat dans l'infrastructure du client.

L'identité de l'utilisateur et les informations d'authentification ne changent pas. Les répertoires et les fichiers déjà enregistrés dans les répertoires restent aussi identiques. Les modifications à réaliser par les clients sont indiquées au chapitre 3.

### 1.3 Connexions

Le client doit s'assurer que la communication vers ou à partir de «FDS BCM» est permise dans son réseau. Dans de nombreux cas, l'équipe en charge du réseau du client doit autoriser les connexions avec les règles de pare-feu correspondantes.

Deux adresses IP sont désormais utilisées. Les adresses IP ne doivent être utilisées que pour la configuration de règles de pare-feu. Le nom DNS (cf. chapitre 1.2 et 5.1) doit impérativement être utilisé pour l'établissement de la connexion.

#### Production et intégration

*Site IP 1* Les adresses IP peuvent à tout moment être demandées auprès de [fds@poste.ch](mailto:fds@poste.ch).

*Site IP 2* Les adresses IP peuvent à tout moment être demandées auprès de [fds@poste.ch](mailto:fds@poste.ch).

Les deux adresses IP peuvent aussi être transmises par la résolution DNS (p. ex. nslookup fdsbc.post.ch) au bout de plusieurs tentatives.

## 2. Introduction

L'introduction de FDS BCM implique des modifications de la plateforme qui ont été réalisées en février 2016 par Technologies de l'information Poste. Les clients sont responsables de l'utilisation de FDS BCM par l'intermédiaire des interfaces.

## 3. Processus de migration

Le présent chapitre aborde les processus de migration pour chaque type de connexion. Les connexions sont établies du point de vue du client.

### 3.1 Protocoles de communication

#### 3.1.1 SFTP – Client vers la Poste

La communication est établie par le client (l'application client correspond au client).



- 1) Garantie que les deux sites FDS sont joignables (cf. chapitre 1.3). Cela relève de la responsabilité du client.
- 2) Passage de l'établissement d'une communication vers l'intégration `fdsbci.post.ch` ou la production `fdsbc.post.ch` (client)

Il est le cas échéant nécessaire d'accepter le nouveau nom DNS de la clé hôte avec l'adresse IP *site IP 2* lors du premier établissement de connexion.

**Veillez ne pas utiliser l'adresse/les adresses IP (cf. chapitre 5.2)**

#### 3.1.2 SFTP – Poste vers le client

La communication est établie par la Poste (l'application client correspond au serveur).



- 1) Si le client doit définir des règles de pare-feu en cas de mise en service de connexions entrantes et/ou sortantes:
  - o S'assurer que les deux sites FDS peuvent accéder aux systèmes client (cf. chapitre 1.3). La responsabilité incombe au client. Le client n'est pas tenu d'informer Technologies de l'information Poste.
- 2) FDS BCM établit les connexions des deux sites avec le système client. Poste CH SA assure cette procédure dès que le point 1) est satisfait.

### 3.1.3 Connect:Direct



En cas d'utilisation de Connect:Direct à titre de protocole de communication, les clients doivent s'assurer que la communication est aussi établie sur le nœud alternatif en plus du nœud primaire.

En cas de sinistre, le nœud alternatif est automatiquement utilisé. Si la communication a lieu par l'intermédiaire d'une ligne louée, la commutation automatique ne fonctionne que si les lignes louées vers les deux sites sont disponibles et actives en permanence (cf. chapitre 3.2.2).

- **Nœud alternatif**  
configuration avec la nouvelle adresse IP *site IP 2*
- **Nœud primaire**  
configuration de l'adresse IP actuelle *site IP 1*

Les clients sont priés d'informer la Poste à propos des travaux prévus (par e-mail à [fds@poste.ch](mailto:fds@poste.ch)).

Nous recommandons de plus aux clients de migrer les interfaces de Connect:Direct vers le protocole SFTP.

## 3.2 Canaux de communication

Les processus de migration divergent en fonction du type de connexion.

### 3.2.1 Internet

Les informations indiquées au chapitre 3.1 s'appliquent à la connexion par Internet.

### 3.2.2 Lignes louées

Afin de permettre la poursuite du fonctionnement des transferts de fichiers en cas de sinistre, une deuxième ligne louée vers un autre site doit être installée. La ligne louée doit être commandée par le client.

Les connexions de partenaires par l'intermédiaire de réseaux tiers (MPLS) ainsi que via un VPN site-2-site impliquent souvent une conversion d'adresses NAT de la part du client sur laquelle Poste CH SA n'a aucune influence.

- **FDS à titre de client doit modifier l'adresse IP en cas de sinistre afin d'avoir accès au système du client par l'intermédiaire de la deuxième ligne louée.**
- **En cas de connexions avec FDS (FDS en tant que serveur), les partenaires doivent recourir à l'autre adresse IP en cas de sinistre.**

**Nous prions les clients d'indiquer à la Poste ([fds@poste.ch](mailto:fds@poste.ch)) si des modifications de configuration manuelles (uniquement en cas de lignes louées et liaisons Connect:Direct) doivent avoir lieu du côté du client en cas de sinistre.**

**Technologies de l'information Poste recommande aux clients de gérer si possible la communication par Internet.**



## 4. Procédure en cas de sinistre

En cas de sinistre, des interventions manuelles ou des modifications de la configuration ne sont requises que pour les lignes louées (cf. chapitre 3.2.2).

L'établissement d'une configuration Connect:Direct correspondante et d'une ligne louée appropriée (active en permanence) permettent de rendre inutile toute action manuelle en cas de catastrophe.

## 5. Remarques

### 5.1 Cache DNS

La plateforme est exploitée sur deux sites dans une configuration active/active. Le mécanisme de basculement est assuré par une infrastructure «Global Server Load Balancing (GSLB)». Afin que le client puisse profiter d'un basculement rapide de la connexion au FDS, il convient de s'assurer de l'absence d'exécution de cache DNS supplémentaire dans son environnement. Les indications relatives au «time to live» (TTL) du DNS de la Poste doivent être impérativement respectées.

### 5.2 Adresses IP

Il est nécessaire d'accéder au FDS BCM par l'intermédiaire du nom DNS. Les adresses IP ne doivent être utilisées que pour l'élaboration de règles de pare-feu, sauf dans les cas suivants:

- Utilisation du protocole Connect:Direct
- Lignes louées