

FDS BCM migration user guide

File Delivery Services

Converting to a location-redundant FDS platform

Publisher

Post CH Ltd
Information Technology
Webergutstrasse 12
3030 Berne (Zollikofen)
Switzerland

Contact

Post CH Ltd
Information Technology
Webergutstrasse 12
3030 Berne (Zollikofen)
Switzerland
IT261 FDS Operation
E-mail: fds@swisspost.ch

Version 2.1 / March 2016

Download the latest version from: <https://www.swisspost.ch/fds>

Contents

- 1. Introduction4**
 - 1.1 Architecture.....5
 - 1.2 Innovations.....5
 - 1.3 Connections6
- 2. Introduction7**
- 3. Migration path.....7**
 - 3.1 Communication protocol.....7
 - 3.1.1 SFTP – customer to Swiss Post7
 - 3.1.2 SFTP – Swiss Post to customer7
 - 3.1.3 Connect:Direct8
 - 3.2 Communication channels8
 - 3.2.1 Internet8
 - 3.2.2 Leased connections8
- 4. System failure procedure.....9**
- 5. Notes9**
 - 5.1 DNS caching9
 - 5.2 IP addresses9

1. Introduction

File Delivery Services (FDS) is a service provided by the Information Technology (IT) service unit of Post CH Ltd.

FDS acts as a gateway in the IT security system between Post CH Ltd's intranet and external networks. It enables files and applications to be exchanged among internal and external partners.

Due to the audit requirements placed on Post CH Ltd, the service will be operated as geographically redundant from Q1 2016.

This user guide will help existing customers to migrate to the location-redundant solution, hereinafter referred to as "FDS BCM".

Swiss Post IT assumes no responsibility for the accuracy of the information in this user guide and reserves the right to correct errors and make changes.

1.1 Architecture

The high-availability service will be expanded to an additional location in order to cover the outage of a data center.

The distribution of communications over two locations is accomplished using DNS load balancing (Round Robin). This means that the IP addresses of both locations are returned alternately for DNS resolution.

1.2 Innovations

The following fundamental innovations will come with the new architecture:

- Introduction of a secondary location
- Introduction of DNS load balancing (Round Robin)
- DNS name change
 - o Integration

OLD: `fdsi.post.ch`
NEW: `fdsbci.post.ch`

- o Production

OLD: `fds.post.ch`
NEW: `fdsbc.post.ch`

- IPv4 and IPv6 support

The use of IPv6 is optional and requires continuous support of IPv6 in the customer's infrastructure.

The user and authentication information remain unchanged. Similarly, there is no change to the directories and the files that are already stored in the directories. The amendments to be made by the customer are described in section 3.

1.3 Connections

The customer must ensure that communication to or from "FDS BCM" is allowed in his/her network. Usually the network team has to allow connections with the appropriate firewall rules.

Two IP addresses will now be used. These IP addresses may be used only for configuring firewall rules. It is essential that the DNS name is used (see sections 1.2 and 5.1) for the connection setup.

Production and integration

- | | |
|----------------------|---|
| <i>IP location 1</i> | The IP addresses can be requested at any time from fds@swisspost.ch . |
| <i>IP location 2</i> | The IP addresses can be requested at any time from fds@swisspost.ch . |

Alternatively, both IP addresses can be determined with several DNS lookup requests (for example, nslookup fdsbc.post.ch).

2. Introduction

The introduction of FDS BCM includes the amendments made to the platform by Swiss Post Information Technology in February 2016. Customers are responsible for using FDS BCM via the interfaces.

3. Migration path

This section describes the migration paths for each connection type. The connections are based on the customer's point of view.

3.1 Communication protocol

3.1.1 SFTP – customer to Swiss Post

Communication is set up by the customer (the customer application is the client).



- 1) Ensure that both FDS locations are accessible. (See section 1.3). This is the customer's responsibility.
- 2) Convert the communication setup to integration `fdsbci.post.ch` or to production `fdsbc.post.ch` (customer)

For the initial connection setup using the new DNS name, accept the host key with the IP address *IP location2*, if required.

Please do not use the IP address(es) (see section 5.2)

3.1.2 SFTP – Swiss Post to customer

Communication is set up by Swiss Post (the customer application is the server).



- 1) If the customer needs to define firewall rules for incoming and/or outgoing connections during start-up:
 - o Ensure that both FDS locations can access the customer systems (see section 1.3). The responsibility lies with the customer. The customer is not required to notify Swiss Post Information Technology.
- 2) FDS BCM sets up connections from both locations to the customer system. Post CH Ltd automatically ensures this as soon as point 1) is complete.

3.1.3 Connect:Direct



If Connect:Direct is used as the communication protocol, customers must ensure that communication can also be set up for the primary node as well as the alternate node.

The alternate node will be used automatically in the event of a system failure. If communication is via a leased connection, automatic switching only functions if the leased connections are available to both locations and constantly active (see section 3.2.2)

- **Alternate node**
Configure with a new IP address *IP location2*
- **Primary node**
Configure from current IP address *IP location1*

Customers are requested to inform Swiss Post of their progress (by e-mail to fds@swisspost.ch).

We also recommend customers migrate interfaces from Connect:Direct to SFTP.

3.2 Communication channels

The migration paths differ depending on the type of connection.

3.2.1 Internet

If the connection is via the Internet, see the relevant information in section 3.1.

3.2.2 Leased connections

To ensure that file transfers continue to function in the event of a system failure, there must be a second active leased connection to the second location. The leased connection must be ordered by the customer.

For connections from partners via external networks (MPLS) and via site-2-site VPN, network address translation (NAT) is often used by the customer. This is beyond Post CH Ltd's control.

- **As the client, FDS needs to amend the IP address in the event of a system failure in order to access the customer system via the second leased connection.**
- **For connections to FDS (FDS as server), the partners must use the other IP address in the event of a system failure.**

We ask customers to inform Swiss Post (fds@swisspost.ch) if, in the event of a system failure, manual configuration changes have to be made by the customer (only for leased and Connect:Direct connections).

Swiss Post Information Technology recommends that customers communicate via the Internet if possible.

4. System failure procedure

In the event of a system failure, manual interventions or configuration changes are necessary only for leased connections (see section 3.2.2).

By setting up an appropriate Connect:Direct configuration and corresponding leased connection (constantly active), preparations have been made to render manual action unnecessary in the event of a system failure.

5. Notes

5.1 DNS caching

The platform operates in active/active mode at two locations. The failover mechanism is guaranteed by a Global Server Load Balancing (GSLB) infrastructure. In order to benefit quickly from this failover mechanism, the customer must ensure that no additional DNS caching is done in his/her environment. The Time to Live (TTL) specification given by Swiss Post's DNS must be respected.

5.2 IP addresses

FDS BCM must be used via the DNS name. The IP addresses are only to be used to create firewall rules, except in the following cases:

- Use of the Connect:Direct protocol
- Leased connections