

Guida per la migrazione FDS BCM

File Delivery Services

Passaggio alla piattaforma FDS ridondante tra sedi

Editore

Posta CH SA
Tecnologia dell'informazione
Webergutstrasse 12
CH-3030 Berna (Zollikofen)

Contatto

Posta CH SA
Tecnologia dell'informazione
Webergutstrasse 12
CH-3030 Berna (Zollikofen)
IT261 Esercizio FDS
E-mail: fds@posta.ch

Versione 2.1 / marzo 2016

La versione attuale è disponibile su: <https://www.post.ch/fds>

Indice

1. Introduzione	4
1.1 Architettura	5
1.2 Novità	5
1.3 Collegamenti	6
2. Introduzione	7
3. Percorso di migrazione	7
3.1 Protocolli di comunicazione	7
3.1.1 SFTP – Dal cliente verso la Posta	7
3.1.2 SFTP – Dalla Posta verso il cliente	7
3.1.3 Connect:Direct	8
3.2 Canali di comunicazione	8
3.2.1 Internet	8
3.2.2 Linee noleggiate	8
4. Procedura in caso di disastro	9
5. Note	9
5.1 Caching DNS	9
5.2 Indirizzi IP	9

1. Introduzione

Il File Delivery Services (FDS) è un'offerta di servizi dell'unità Tecnologia dell'informazione (IT) di Posta CH SA.

Nel sistema di sicurezza IT, FDS ha la funzione di gateway tra l'intranet di Posta CH SA e le reti esterne, consentendo il reciproco scambio di file e applicazioni tra partner interni ed esterni alla Posta.

A fronte delle esigenze di revisione di Posta CH SA, dal primo trimestre 2016 il servizio viene gestito con ridondanza geografica.

La presente guida fornisce un aiuto ai clienti esistenti nel passaggio alla soluzione ridondante tra sedi, di seguito denominata «FDS BCM».

IT Posta non garantisce la correttezza di quanto qui riportato. Con riserva di inesattezze e modifiche.

1.1 Architettura

Il servizio a elevata disponibilità viene potenziato con una nuova sede per sopperire all'eventuale mancato funzionamento di un centro di calcolo.

La distribuzione della comunicazione sulle due sedi è realizzata per mezzo di DNS Load Balancing (round-robin). Ciò significa che, in caso di risoluzione DNS, saranno restituiti alternativamente gli indirizzi IP delle due sedi.

1.2 Novità

La nuova architettura porta con sé le seguenti novità fondamentali:

- introduzione sede secondaria
- introduzione DNS Load Balancing (round-robin)
- modifica del nome DNS
 - o integrazione

VECCHIO: fdsi.post.ch
NUOVO: fdsbci.post.ch

- o produzione

VECCHIO: fds.post.ch
NUOVO: fdsbc.post.ch

- supporto IPv4 e IPv6

L'utilizzo di IPv6 è facoltativo e richiede un relativo supporto costante nell'ambito dell'infrastruttura del cliente.

Per quanto concerne le informazioni sull'utente e per l'autenticazione tutto rimane invariato. Analogamente non cambia nulla per quanto riguarda directory e file che sono già salvati nelle directory. Le modifiche che devono essere eseguite dal cliente sono descritte nel capitolo 3.

1.3 Collegamenti

Il cliente deve accertarsi che nella sua rete sia consentita la comunicazione da e verso «FDS BCM». In molti casi il team di rete del cliente deve consentire la creazione dei collegamenti attraverso apposite regole del firewall.

D'ora in poi verranno utilizzati due indirizzi IP che possono essere utilizzati solo per configurare le regole del firewall. Per creare i collegamenti bisogna necessariamente utilizzare il nome DNS (cfr. capitolo 1.2 e 5.1).

Produzione e integrazione

IP sede 1 Gli indirizzi IP possono essere richiesti in qualsiasi momento a fds@posta.ch.
IP sede 2 Gli indirizzi IP possono essere richiesti in qualsiasi momento a fds@posta.ch.

In alternativa, i due indirizzi IP possono essere determinati per mezzo di risoluzione DNS (ad esempio nslookup fdsbc.post.ch), effettuando alcuni tentativi.

2. Introduzione

L'introduzione di FDS BCM include modifiche alla piattaforma che sono state eseguite da Tecnologia dell'informazione Posta nel mese di febbraio 2016. I clienti sono responsabili dell'utilizzo di FDS BCM attraverso le interfacce.

3. Percorso di migrazione

In questo capitolo vengono illustrati i percorsi di migrazione a seconda del tipo di collegamento. I collegamenti sono orientati dal punto di vista del cliente.

3.1 Protocolli di comunicazione

3.1.1 SFTP – Dal cliente verso la Posta

La comunicazione viene stabilita dal lato cliente (l'applicazione del cliente è il client).



- 1) Garantire che entrambe le sedi FDS siano raggiungibili (cfr. capitolo 1.3). Questo rientra nella responsabilità del cliente.
- 2) Passaggio da creazione della comunicazione a integrazione `fdsbci.post.ch` o a produzione `fdsbc.post.ch` (cliente).

Eventualmente, al primo tentativo di collegamento al nuovo nome DNS bisogna accettare l'host key con l'indirizzo *IP sede 2*.

Si prega di non utilizzare l'indirizzo / gli indirizzi IP (cfr. capitolo 5.2)

3.1.2 SFTP – Dalla Posta verso il cliente

La comunicazione viene stabilita dalla Posta (l'applicazione del cliente è il server).



- 1) Nel caso in cui all'attivazione di collegamenti in entrata e/o in uscita il cliente debba definire delle regole del firewall:
 - o garantire che entrambe le sedi FDS possano comunicare con i sistemi del cliente (cfr. capitolo 1.3); la responsabilità è del cliente e non è necessaria una comunicazione da parte sua a Tecnologia dell'informazione Posta
- 2) FDS BCM crea i collegamenti da entrambe le sedi verso il sistema del cliente, attività che viene garantita in automatico da Posta CH SA a condizione che il punto 1) sia soddisfatto.

3.1.3 Connect:Direct



Se Connect:Direct viene utilizzato come protocollo di comunicazione, i clienti devono garantire che la comunicazione possa essere stabilita, oltre che verso il primary node, anche sull'alternate node.

In caso di disastro viene utilizzato in automatico l'alternate node. Se la comunicazione viene gestita tramite una linea noleggiata, la commutazione automatica funziona solo se le linee noleggiate verso entrambe le sedi sono disponibili e sempre attive (cfr. capitolo 3.2.2).

- **Alternate node**
Configurare con il nuovo indirizzo IP *IP sede 2*
- **Primary node**
Configurare con l'attuale indirizzo IP *IP sede 1*

I clienti sono pregati di informare la Posta in merito alle loro attività (per e-mail all'indirizzo fds@posta.ch).

Inoltre, consigliamo ai clienti di trasferire le interfacce di Connect:Direct su SFTP.

3.2 Canali di comunicazione

I percorsi di migrazione variano a seconda del tipo di connessione.

3.2.1 Internet

Se la connessione viene gestita tramite internet, consultare le informazioni contenute nel capitolo 3.1.

3.2.2 Linee noleggiate

Affinché anche in caso di disastro il trasferimento di file continui a funzionare, presso la seconda sede deve essere presente una seconda linea noleggiata attiva. La linea noleggiata deve essere ordinata dal cliente.

Se un partner effettua collegamenti attraverso reti di terzi (MPLS) o anche attraverso VPN site-to-site, sul lato cliente viene spesso impiegata una traduzione degli indirizzi di rete (NAT) sulla quale Posta CH SA non ha alcuna possibilità di influire.

- **In caso di disastro, FDS con la funzione di client deve modificare l'indirizzo IP per poter comunicare con il sistema del cliente attraverso la seconda linea noleggiata.**
- **In caso di disastro per i collegamenti verso FDS (FDS con la funzione di server) i partner devono contattare l'altro indirizzo IP.**

Invitiamo i clienti a comunicare alla Posta (fds@posta.ch) se, in caso di disastro, devono essere apportate modifiche manuali alla configurazione sul lato cliente (solo in caso di linee noleggiate e collegamenti Connect:Direct).

Tecnologia dell'informazione Posta raccomanda ai clienti di gestire, se possibile, la comunicazione tramite internet.

4. Procedura in caso di disastro

In caso di disastro sono necessari interventi manuali e/o modifiche della configurazione solo per le linee noleggiate (cfr. capitolo 3.2.2).

Attraverso l'allestimento di un'apposita configurazione Connect:Direct e della relativa linea noleggiata (sempre attiva) sono state implementate le attività preparatorie che consentono di evitare interventi manuali in caso di disastro.

5. Note

5.1 Caching DNS

La piattaforma viene gestita con una configurazione attiva/attiva tra due sedi. Il meccanismo di failover viene garantito con un'infrastruttura «Global Server Load Balancing (GSLB)». Affinché il cliente possa usufruire di un rapido collegamento di failover a FDS, bisogna assicurarsi che nessun caching DNS aggiuntivo sia configurato nella sua rete. Il time-to-live (TTL) specificato dal DNS della Posta deve essere rigorosamente rispettato.

5.2 Indirizzi IP

FDS BCM deve essere contattato utilizzando il nome DNS. Gli indirizzi IP devono essere utilizzati solo per creare le regole del firewall, fatti salvi i seguenti casi:

- utilizzo del protocollo Connect:Direct
- linee noleggiate