Manuale FDS

File Delivery Services

Filetransfer SFTP

Editore

Posta CH SA
Informatica
Webergutstrasse 12
CH-3030 Berna (Zollikofen)

Contatto

Posta CH SA
Informatica
Webergutstrasse 12
CH-3030 Berna (Zollikofen)
IT17.34 FDS
E-mail: fds@posta.ch

Versione 8.5 / gennaio 2023

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

Indice

1. Introduzione

Il File Delivery Services (FDS) è un'offerta di servizi dell'unità Informatica della Posta CH SA.

FDS ha il ruolo di gateway nel sistema di sicurezza IT tra l'intranet della Posta CH SA e le reti esterne e consente lo scambio reciproco di file tra partner interni ed esterni alla Posta nonché di applicazioni.

Il presente manuale descrive le modalità per scambiare file con il server FDS della Posta CH SA. Il servizio è a disposizione di tutti gli utenti che dispongono sul proprio computer di un client di trasferimento dati o del relativo account.

IT Posta non garantisce la correttezza di quanto qui riportato. Si fa riserva di modifiche ed eventuali errori.

2. Il modello FDS della Posta CH SA

2.1 Panoramica

Il modello FDS è stato creato nel 1993. È stato introdotto nell'ambito del progetto C TTD dell'organizzazione PostFinance di allora. I primi trasferimenti di file vennero effettuati tramite Kermit, FTP e FTAM. Nel 1995 il servizio per il trasferimento di file è stato ampliato con CONNECT:Direct™. Nel 2002 l'FDS è stato potenziato con il sistema FDS SSH (FTP mediante SSL, detto anche Secure FTP); nel frattempo i protocolli FTAM e Kermit non venivano più offerti.

Il 2007 è stato l'anno della svolta tecnologica e generazionale grazie all'introduzione di SFTP (SSH File Transfer Protocol). Con questa introduzione il servizio FDS SSH non aveva più motivo di esistere e non è più disponibile dalla metà del 2010.

L'uso del protocollo FTP traverso l'Internet per nuovi utenti non è più consentito a partire da giugno 2015 per motivi di sicurezza (trasmissione di dati, nome utente e password non criptati). Gli utenti esistenti avranno tempo fino al primo dicembre 2018 per passare al protocollo SFTP.

2.2 Protocolli supportati

- SFTP (SSH File Transfer Protocol)

2.3 Tipi di connessione

Vengono offerti tre tipi di connessione:

- internet
- MPLS/IPSS — Linee noleggiate, rete IPSS di Swisscom
- intranet — per partner/applicazioni interni/e alla Posta

Per quanto riguarda la data desiderata per le nuove linee noleggiate e per gli MPLS occorre tener conto dei tempi d'installazione previsti dal provider della rete. Si ricorre alle linee noleggiate quando altri tipi di collegamento risultano più costosi o se determinati requisiti in materia di sicurezza lo rendono necessario. I collegamenti ADSL sono possibili solo via internet tramite un provider. Se il protocollo SFTP viene usato con chiavi sufficientemente lunghe, l'uso di linee affittate e le connessioni VPN sono superflue e non portano alcuna sicurezza aggiuntiva.

3. Il servizio FDS

3.1 Il File Delivery Service

Il File Delivery Service si basa su uno speciale sistema di mailboxing capace di soddisfare gli elevati requisiti di sicurezza nell'ambito di internet, extranet e intranet.

3.2 Dove si collocano i servizi di File Delivery?

L'FDS è formato da un server di trasferimento dati, da un server di banca dati e vari server di perimetro. Tutti i componenti sono collocati in zone diverse (DMZ) della piattaforma IX. La piattaforma IX è la zona di sicurezza protetta da firewall tra la rete della Posta (intranet) e le reti esterne (internet, linee noleggiate). I server di trasferimento file e di banca dati si trovano all'interno di una zona altamente protetta e ad accesso estremamente limitato. I server di perimetro si trovano in zone meno protette cui è possibile accedere utilizzando dei client. I collegamenti client/server dalle reti esterne e dalla rete interna della Posta passano sempre attraverso i server di perimetro. Il servizio FDS e progettato geograficamente ridondante, cosicché resti disponibile anche in caso di guasto di un data center.

3.3 Protocolli di trasferimento file

Informazioni più dettagliate sono disponibili nel «Manuale d'esercizio File Transfer Client» su https://www.post.ch/fds.

3.3.1 SFTP

L'SFTP (SSH Secure File Transfer Protocol) è un protocollo di trasferimento dati sicuro. Tra client e server viene infatti stabilito un collegamento ininterrotto e cifrato tramite il quale i dati e i nomi utente risultano illeggibili per eventuali intrusi. L'autenticazione mediante public key garantisce l'integrità e la confidenzialità dei dati scambiati e consente, inoltre, ai client privi d'interazione utente di effettuare il login sul server. L'SSH garantisce la trasmissione completa e integrale dei dati dal mittente al destinatario. È supportato solo l'SSH-2 (versione 2) e l'autenticazione avviene esclusivamente tramite public key.

Con un client **SFTP** è possibile stabilire un collegamento con il server SFTP FDS ed eseguire i comandi necessari.

Attenzione: l'SFTP non va confuso con l'FTPS (FTP mediante SSL) o con l'FTP mediante SSH (detto talvolta Secure FTP).

3.4 Consegna e ritiro da server esterni

Se si desidera che il servizio FDS trasmetta i file o li ritiri presso il cliente, occorre che siano soddisfatti alcuni presupposti. Tali condizioni preliminari sono riportate nel capitolo 6. Le specifiche possono essere richieste a Esercizio FDS (fds@post.ch).

La consegna e la ripartizione di un file avvengono per evento. All'arrivo di un file, il server FDS lo invia alle destinazioni predefinite. Non è possibile stabilire quando tale azione debba essere eseguita.

3.5 Utilizzo del File Delivery Service

Gli utenti che si collegano al server FDS dall'esterno della rete della Posta devono utilizzare ulteriori misure di sicurezza a seconda del tipo di collegamento utilizzato (linee noleggiate, internet).

La richiesta amministrativa per l'utilizzo del servizio FDS avviene tramite il servizio clienti della competente unità aziendale o di servizi della Posta CH SA.

Per problemi urgenti che si dovessero presentare dopo la messa in servizio, è possibile rivolgersi alla nostra hotline (+41 (0)848 800 030).
Per chiarimenti in merito all'FDS è possibile scrivere al seguente indirizzo e-mail: fds@post.ch

4. Sicurezza

4.1 Nome utente (login)

Gli utenti esterni ricevono un proprio nome utente a seconda dell'unità servizi e aziendale. In caso di utilizzo da parte di un cliente dello stesso nome utente per più unità della propria azienda, la Posta CH SA declina qualsiasi responsabilità per danni derivanti dall'accesso esteso a dati del server di trasferimento dati della Posta.

4.2 Cifratura dei link

La cifratura dei link non è un servizio standard del sistema FDS. Può comunque essere utilizzata come opzione di rete. Se il protocollo SFTP viene usato con chiavi sufficientemente lunghe, una crittografia del collegamento non è più necessaria. La connessione può essere fatta senza perdita e la sicurezza traverso l'Internet.

4.2.1 Per tutti i tipi di collegamento

Per una cifratura client-to-server è disponibile il protocollo SFTP per tutti i tipi di collegamento.

4.2.2 MPLS/IPSS

Con MPLS/IPSS si può realizzare la cifratura dei link.

4.2.3 LAN-LAN

Nei collegamenti LAN-LAN può essere stabilita la cifratura dei link con entrambi i router.

5. Configurazioni

5.1 Configurazione dell'FDS Client-Server

5.1.1 Filetransfer Server

Zona	Hostname
internet / linee noleggiate	fdsbc.post.ch
Rete postale/DMZ	fdsbc.pnet.ch

La distribuzione delle connessioni su due sedi è realizzata per mezzo di Loadbalancing DNS (round-robin). Ciò significa che gli indirizzi IP dei due siti saranno restituiti alternativamente.

Occorre garantire che la comunicazione verso o da FDS sia consentita nella vostra rete. In molti casi, i specialisti della rete devono consentire le connessioni traverso le regole del firewall. Vengono utilizzati due indirizzi IP. Gli indirizzi IP possono essere utilizzati solo per la configurazione delle regole del firewall. Per stabilire la connessione bisogna assolutamente usare il nome DNS.

I due indirizzi IP possono essere determinati per mezzo di risoluzione DNS traverso diversi tentativi (nslookup fdsbc.post.ch).

FDS supporta IPv4 e IPv6. L'uso di IPv6 richiede un supporto completo di IPv6 nella vostra infrastruttura.

5.1.2 DNS caching

La piattaforma viene gestita con una configurazione Active / Active tra due sedi. Il meccanismo di failover viene assicurato con una infrastruttura „Global Server Loadbalancing (GSLB)". Per poter usufruire di una connessione di failover rapida, bisogna assicurarsi che nessun cache DNS aggiuntivo sia configurato nella vostra rete. Il Time to Live (TTL) specificato dal DNS della posta deve essere rigorosamente rispettato.

5.1.3 Porte

I protocolli FDS utilizzano le porte standard (22 per SFTP).

5.1.4 Nome utente (login)

Il nome utente sarà comunicato nel contesto dell'ordine di servizio.

5.1.5 Directory

I nomi delle directory sul server FDS sono sempre in lettere minuscole e contemplano le limitazioni seguenti

- Caratteri: [a-z], [0-9], [. -] (punto, trattino)
- Inizio: il primo carattere deve essere [a-z], [0-9]

5.1.6 Nomi dei file

Per i nomi dei file nelle directory dei server FDS bisogna attenersi alle seguenti disposizioni

- Caratteri: [A-Z], [a-z], [0-9], [. - _] (punto, trattino, trattino basso)

5.2 SFTP

5.2.1 Aspetti generali

Informazioni dettagliate sono disponibili nel «Manuale d'esercizio File Transfer Client» su https://www.post.ch/fds.

5.2.2 Invio della public key a IT Posta

Una copia della public key deve essere inviata alla Posta per e-mail (fds@post.ch). Affinché la Posta possa verificare con il mittente la chiave ricevuta, la chiave va inviata della persona di contatto (o la persona deve risultare dallo scambio di e-mail).

Volendo esiste la possibilità di configurare più public key per lo stesso nome utente. La stessa chiave può essere usata da più utenti.

5.2.3 Gestione delle chiavi

Si prega di gestire le private key come se si trattasse della propria carta di credito. Si prega di proteggerle da accessi non autorizzati.

Le chiavi generate devono avere una lunghezza di minimo **4096** bit.

6. Allegato A. Informazioni per l'uso di FDS

La presente nota informativa descrive lo scambio di dati e le funzioni di FDS e presenta le regole e i requisiti fondamentali per la trasmissione di file tramite i server di filetransfer FDS. Si rivolge agli utenti FDS delle unità aziendali e delle società del gruppo della Posta CH SA e ai loro clienti esterni.

6.1 Condizioni quadro/limitazioni

a) FDS non è un sistema di archiviazione. I file da scaricare non ancora cancellati dal cliente vengono in ogni caso cancellati automaticamente dal server dopo 9 giorni.

b) Ciascun file può essere scaricato al massimo 20 volte.

c) FDS ha un ritmo di elaborazione di un minuto. I file trasmessi figurano un minuto dopo il trasferimento dei file nella mailbox del destinatario. Se la configurazione prevede che i file vengano trasmessi ad un determinato elaboratore destinatario, il processo di trasmissione può durare di più a seconda delle dimensioni dei file.

d) I file di grandi dimensioni (normalmente file ASCII) devono essere trasmessi in formato compresso. Mittente e destinatario (end-to-end) stabiliscono il metodo di compressione (es. ZIP, GZIP).

e) Per trasmettere molti file è necessario ricorrere a un numero corrispondente di filetransfer (put/get) per sessione/login FTP/SFTP. Ad esempio per 1200 file: 10 collegamenti/login FTP, ognuno con esecuzione di 120 filetransfer. Se il numero di login durante una determinata unità temporale è troppo elevato, l'Intrusion Prevention System della Posta CH SA blocca automaticamente il Source IP Adress incriminato. per 15 minuti

f) FDS non conferma al mittente il trasferimento dei file. La creazione e l'invio di ricevute di conferma è compito del destinatario e non è garantita da FDS.

g) Al trasferimento dei file, in caso di inoltro non è garantita alcuna sequenza di trasmissione. I file di diverse dimensioni possono sovrapporsi in una sequenza parallela. Il sistema di ricezione della relazione end-to-end è responsabile per la riproduzione della corretta sequenza dei pacchetti trasmessi.

h) L'inoltro e la distribuzione dei file è controllata per evento. Non è possibile utilizzare un controllo temporale.

i) IT deve essere tempestivamente informata sulle dimensioni, la frequenza e le variazioni di volume dei file per tutti i trasferimenti di file che avvengono tramite il server FDS. Solo in questo modo si può garantire la necessaria capacità al momento opportuno.

j) IT deve essere tempestivamente informata sulla priorità in caso di escalation per tutti i trasferimenti di file che avvengono tramite il server FDS. Per tutti gli altri casi si applicano gli standard SLA.

6.2 Limitazione della trasmissione dei dati (client → server FDS)

- In caso di upload (put) da parte di un client di trasferimento file in una casella FDS (cartella), i file vengono direttamente elaborati dai processi sul server FDS alla conclusione del trasferimento. Le registrazioni dei file nelle mailbox di upload rimangono tuttavia visualizzabili dal cliente per due minuti (visualizzazione dei file tramite "dir" e "ls"). **La cancellazione o la rinomina di un file trasmesso non ha senso: il file viene inoltrato al destinatario con il nome di file originario.**
- FDS assicura che vengano elaborati solo file trasmessi integralmente. In caso di interruzione del collegamento, il file incompleto viene respinto.
- Con FDS non è inoltre possibile modificare gli attributi del file dopo il trasferimento.

6.3 Requisiti nell'ambito della trasmissione dei dati (server FDS → sistema target)

I destinatari esterni e interni della Posta devono rispettare questi requisiti per poter ricevere file dal servizio FDS:

– connessioni di rete permanenti come WAN-Access (MPLS) o internet
– sistema disponibile 7 giorni su 7, 24 ore su 24
– assicurazione di un centro di elaborazione dati operativo
– i punti di contatto per le attività di supporto (numeri di telefono, indirizzi e-mail) e la reperibilità sono garantiti

6.4 Requisiti e limitazioni nel recupero dei dati

L'FDS può prelevare automaticamente file con FTP e SFTP da sistemi di terzi.
Questa funzione va tuttavia utilizzata soltanto in via eccezionale.

Requisiti:
– connessione di rete permanente, come WAN-Access (MPLS) o internet
– sistema disponibile 7 giorni su 7, 24 ore su 24
– assicurazione di un centro di elaborazione dati operativo
– i punti di contatto per le attività di supporto (numeri di telefono, indirizzi e-mail) e la reperibilità sono garantiti

Restrizioni:
– il servizio non viene offerto per recuperare dati con tempi critici in un intervallo inferiore a 30 minuti
– i dati da recuperare devono trovarsi in directory definite in maniera fissa; non viene supportato il recupero in directory variabili (per esempio nomi di directory che comprendono la data odierna)

7. Allegato B. Glossario

D	DMZ	Zona demilitarizzata – Una DMZ si trova in una connessione LAN separata di un firewall tra una rete interna e una rete esterna non sicura, ad es. internet. Nella DMZ vengono spesso messi a disposizione server che offrono servizi agli utenti di internet (es. www o e-mail). Una DMZ si trova di preferenza tra due firewallsseparati fisicamente. Il firewall esterno protegge dagli attacchi dall'esterno e controlla ogni accesso internet alla DMZ. Il firewall interno controlla l'accesso dalla DMZ alla rete interna e viceversa. Costituisce così una seconda linea di difesa nel caso in cui il firewall esterno dovesse essere violato. Ciò presenta il vantaggio di proteggere la rete interna anche nel caso che un'aggressione raggiunga il server Web.
	DNS	Il Domain Name System (DNS) è uno dei servizi più importanti in internet. Il suo compito principale è quello di commutare gli «indirizzi internet» nei relativi indirizzi IP.
E	End-to-End	Relazione tra un'applicazione (ad es. VEA-I) di un'unità aziendale della Posta CH SA (ad es. PostFinance SA) e l'applicazione del cliente esterno.
F	FDS	Il File Delivery Services è un servizio dell'unità di servizio Tecnologia dell'informazione (IT) della Posta CH SA. FDS ha il ruolo di proxy nel sistema di sicurezza IT tra l'intranet della Posta CH SA e le reti esterne e consente lo scambio reciproco di file tra partner interni ed esterni alla Posta nonché di applicazioni.
	FTP	Il File Transfer è un protocollo di rete specificato nell'RFC 959 del 1985 per la trasmissione dei file attraverso le reti TCP/IP. È un protocollo, quindi, che consente lo scambio di file tra computer diversi, indipendentemente dalla loro ubicazione e dal sistema operativo.
I	IPSS	LAN Interconnect over IPSS è un servizio di Swisscom. È in grado di collegare reti locali a un'unica infrastruttura di comunicazione aziendale. IPSS è una soluzione propria di Swisscom e che fa capo alla tecnologia più moderna. La tecnologia MPLS (Multi Protocol Label Switching) utilizzata consente una grande flessibilità in rapporto alla larghezza di banda. Il servizio è assicurato da Swisscom Enterprise Solution. http://www.swisscom.com/es/
M	MPLS	Il Multiprotocol Label Switching (MPLS) è un'implementazione del Label Switching. In questo processo si riduce il carico dei router utilizzati per il trasporto dei pacchetti dati, poiché il livello di complessità del processo è ridotto a un semplice switch. Ciò è possibile perché all'inizio della trasmissione dei dati viene creato un percorso di connessione fisso. I router su questo percorso non devono individuare il destinatario dei pacchetti in transito, ma li trasferiscono senza elaborazioni secondo il percorso impostato.
S	SFTP	SSH File Transfer Protocol (abbreviato SFTP) è uno sviluppo ulteriore dell'SCP e permette la trasmissione di e l'accesso ai dati da un client su un sistema remoto. Il protocollo non comprende né autenticazione né cifratura. Queste funzioni devono essere affidate al protocollo SSH sottostante. SFTP non deve essere confuso con Secure FTP o con FTP tramite SSL.
	SSH	SSH consente una comunicazione crittografata sicura su reti protette o non protette. Offre un elevato livello di sicurezza. La reciproca autenticazione dei partner è affidabile, come pure l'integrità e la riservatezza dei dati scambiati. L'SSH garantisce la completa trasmissione e l'integrità dei dati dal mittente al destinatario.