Migrationsanleitung FDS BCM

File Delivery Services

Umstellung auf die Standort-redundante FDS-Plattform

Herausgeber

Post CH AG
Informationstechnologie
Webergutstrasse 12
CH-3030 Bern (Zollikofen)

Kontakt

Post CH AG
Informationstechnologie
Webergutstrasse 12
CH-3030 Bern (Zollikofen)
IT261 FDS Betrieb
E-Mail: fds@post.ch

Version 2.1 / März 2016

Download der aktuellen Version: https://www.post.ch/fds

Inhaltsverzeichnis

1. Einleitung

Der File Delivery Services (FDS) ist ein Dienstleistungsangebot des Servicebereichs Informationstechnologie (IT) der Post CH AG.

FDS spielt die Rolle eines Gateways im IT-Sicherheitssystem zwischen dem Intranet der Post CH AG und den externen Netzwerken und ermöglicht den gegenseitigen Austausch von Dateien zwischen postinternen und externen Partnern sowie Applikationen.

Aufgrund von Revisions-Anforderungen an die Post CH AG wird ab Q1 2016 der Service mit Georedundanz betrieben.

Diese Anleitung hilft bestehenden Kunden auf die standort-redundante Lösung, nachfolgend „FDS BCM“ genannt, zu migrieren.

IT Post übernimmt für die Richtigkeit der hier gemachten Angaben keine Gewähr. Irrtum und Änderungen bleiben vorbehalten.

1.1 Architektur

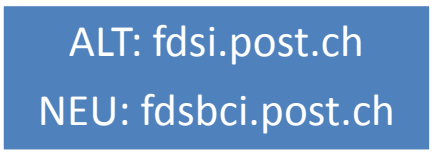
Der hochverfügbare Service wird um einen Standort erweitert, um den Ausfall eines Rechenzentrums abzudecken.

Die Verteilung der Kommunikation über beide Standorte wird mittels DNS Loadbalancing (Round-Robin) erreicht. Dies bedeutet, dass abwechselnd die IP-Adressen der beiden Standorte bei einer DNS-Auflösung zurückgegeben werden.

1.2 Neuerungen

Folgende grundsätzliche Neuerungen ergeben sich mit der neuen Architektur:

- Einführung sekundärer Standort
- Einführung DNS Loadbalancing (Round-Robin)
- Änderung DNS-Name
    - Integration



    - Produktion

- IPv4 und IPv6 Unterstützung

  Die Verwendung von IPv6 ist optional und erfordert durchgehende IPv6-Unterstützung in der Infrastruktur des Kunden.

An den Benutzer und Authentifizierungs-Informationen ändert sich nichts. Ebenso ändert es sich nichts an Verzeichnisse und an Dateien, die bereits in den Verzeichnissen gespeichert sind. Die durch Kunden durchzuführende Änderungen sind unter Kapitel 3 beschrieben.

1.3 Verbindungen

Der Kunde muss sicherstellen, dass die Kommunikation zu - oder ab „FDS BCM“ in seinem Netzwerk erlaubt ist. In vielen Fällen muss das Netzwerk-Team des Kunden die Verbindungen mit entsprechenden Firewall-Regeln erlauben.

Neu werden zwei IP-Adressen verwendet. Die IP-Adressen dürfen nur für die Konfiguration von Firewall-Regeln verwendet werden. Für den Verbindungsaufbau ist zwingend der DNS-Name (siehe Kapitel 1.2 und 5.1) verwendet werden.

Produktion und Integration

IP-Standort 1	Die IP-Adressen können jederzeit bei fds@post.ch angefragt werden.
IP-Standort 2	Die IP-Adressen können jederzeit bei fds@post.ch angefragt werden

Alternativ können die beiden IP-Adressen mittels DNS-Auflösung (zum Beispiel nslookup fdsbc.post.ch) durch mehrere Versuche ermittelt werden.

2. Einführung

Die Einführung von FDS BCM beinhaltet Änderungen der Plattform, die durch Post Informationstechnologie im Februar 2016 durchgeführt wurden. Für die Nutzung von FDS BCM durch die Schnittstellen sind die Kunden verantwortlich.

3. Migrationspfad

In diesem Kapitel werden die Migrationspfade pro Verbindungsart aufgezeigt. Die Verbindungen sind aus Sicht Kunde gerichtet.

3.1 Kommunikations-Protokolle

3.1.1 SFTP – Kunde zu Post

Die Kommunikation wird von der Kundenseite aufgebaut (Kunden-Applikation ist Client).

1) Sicherstellung, dass beide FDS Standorte erreichbar sind. (siehe Kapitel 1.3). Dies ist in der Verantwortung des Kunden.

2) Umstellung Kommunikationsaufbau zu Integration `fdsbci.post.ch` oder zu Produktion `fdsbc.post.ch` (Kunde)

   Ggf. ist beim erstmaligen Verbindungsaufbau auf den neuen DNS-Namen der Host-Key mit der IP-Adresse *IP-Standort2* zu akzeptieren.

   Bitte nicht die IP-Adressen(n) verwenden (siehe Kapitel 5.2)

3.1.2 SFTP – Post zu Kunde

Die Kommunikation wird von der Post aufgebaut (Kunden-Applikation ist Server).

1) Wenn der Kunde bei Inbetriebnahme von eingehenden und/oder ausgehenden Verbindungen Firewall-Regeln definieren muss:
   - Sicherstellen, dass beide FDS Standorte die Kunden-Systeme erreichen können (siehe Kapitel 1.3). Die Verantwortung liegt beim Kunden. Eine Information des Kunden an die Post Informationstechnologie ist nicht erforderlich.

2) FDS BCM baut Verbindungen von beiden Standorten zum Kunden-System auf. Dies stellt Post CH AG automatisch sicher, sobald Punkt 1) erfüllt ist.

3.1.3 Connect:Direct

Wenn Connect:Direct als Kommunikationsprotokoll verwendet wird, müssen Kunden sicherstellen, dass die Kommunikation zusätzlich zum Primary-Node auch auf den Alternate-Node aufgebaut werden kann.

Im Disaster-Fall wird automatisch der Alternate-Node verwendet. Wird die Kommunikation über eine Mietleitung geführt, funktioniert die automatische Umschaltung nur, wenn Mietleitungen zu beiden Standorten verfügbar und ständig aktiv sind (siehe Kapitel 3.2.2)

- **Alternate Node**
  konfigurieren mit neuer IP-Adresse *IP-Standort2*
- **Primary Node**
  konfigurieren von aktueller IP-Adresse *IP-Standort1*

Die Kunden sind gebeten, die Post über ihre Arbeiten zu informieren (per Mail an fds@post.ch).

Im Weiteren empfehlen wir den Kunden, Schnittstellen von Connect:Direct auf SFTP zu migrieren.

3.2 Kommunikations-Kanäle

Die Migrationspfade weichen je nach Verbindungsart ab.

3.2.1 Internet

Wird die Verbindung über das Internet geführt, sind die Informationen im Kapitel 3.1 relevant.

3.2.2 Mietleitungen

Damit im Disaster-Fall die Filetransfers weiterhin funktionieren, muss eine zweite aktive Mietleitung an den zweiten Standort bestehen. Die Mietleitung ist durch den Kunden zu bestellen.

Bei Anbindungen von Partner über die Fremdnetze (MPLS) sowie über Site-2-Site VPN wird auf Kundenseite häufig eine Adressübersetzung NAT eingesetzt, welche Post CH AG nicht beeinflussen kann.

- **FDS als Client muss im Disaster-Fall die IP Adresse ändern, um das Kunden-System durch die zweite Mietleitung zu erreichen.**
- **Bei Verbindungen zu FDS (FDS als Server) müssen die Partner im Disaster-Fall die andere IP-Adresse ansprechen.**

Wir bitten die Kunden der Post mitzuteilen (fds@post.ch) ob im Disaster-Fall auf der Kundenseite manuelle Konfigurations-Änderungen (nur bei Mietleitungen und Connect:Direct Verbindungen) vorzunehmen sind.

Informationstechnologie Post empfiehlt den Kunden, wenn möglich die Kommunikation übers Internet zu führen.

4. Vorgehen Disaster-Fall

Im Disaster-Fall sind nur bei Mietleitungen (siehe Kapitel 3.2.2) manuelle Interventionen bzw. Konfigurations-Änderungen notwendig.

Durch die Einrichtung einer entsprechenden Connect:Direct Konfiguration und der entsprechenden Mietleitung (ständig aktiv) sind die Vorbereitungen getroffen worden, dass im Desaster-Fall keine manuellen Aktionen notwendig sind.

5. Hinweise

5.1 DNS Caching

Die Plattform wird mit einer Active / Active Konfiguration über zwei Standorte betrieben. Der Failover-Mechanismus wird mit einer „Global Server Load Balancing (GSLB)„ Infrastruktur sichergestellt. Damit der Kunde von einem raschen Failover der Verbindung zu FDS profitieren kann, muss in seiner Umgebung sichergestellt werden, dass kein zusätzliches DNS-Caching durchgeführt wird. Die Time-To-Live (TTL) Angabe vom Post-DNS muss zwingend respektiert werden.

5.2 IP-Adressen

FDS BCM muss über den DNS-Namen angesprochen werden. Die IP-Adressen sind nur für die Erstellung von Firewall-Regeln zu verwenden, ausser in folgenden Fällen:

- Verwendung vom Protokoll Connect:Direct
- Mietleitungen