

Remote Backup

Service Level Agreement

EnergiMidt og Front-safe har etableret et strategisk samarbejde, der betyder, at EnergiMidt formidler salget af de Remote Backup løsninger, som Front-safe leverer. Nærværende Service Level Agreement vedrører derfor den tekniske relation, der skabes mellem EnergiMidt's Slutkunde (i det efterfølgende benævnt Slutkunden) og Front-safe.

1. INDLEDNING

1.1 Formål

Service Level Agreement (SLA) beskriver de serviceydelser, som Front-safe A/S (i det følgende benævnt Front-safe) leverer til Slutkunden vedrørende Remote Backup. Denne SLA er bilag til aftalegrundlaget mellem EnergiMidt og Slutkunden, som ligeledes omfatter Slutkundeaftale om levering af Remote Backup samt Almindelige betingelser for Remote Backup.

1.2 Definitioner

I nærværende afsnit defineres nogle af de begreber, som anvendes i denne SLA.

Begreb	Definition
Backupanlægget	Betegnelse for det udstyr som bruges til serviceydelsen, herunder TSM servere, administrative servere samt disk og tape storage
Maskine	Server eller pc hos Slutkunden
Retentionperiode	Det antal dage, som slettede eller ændrede data bliver liggende i backuplageret hos Front-safe og dermed kan genskabes af Slutkunden
Versioner	Det antal ændringer tilbage i tid, som gemmes i backuplageret hos Front-safe, og som sikrer, at Slutkunden kan genskabe en tidligere version

2. SERVICEYDELSEN

2.1 Overordnet beskrivelse

Serviceydelsen omfatter afvikling, overvågning og forvaltning af backup og arkivering af filer og databaser fra Slutkundens maskiner, samt relaterede ydelser. Efter gennemført implementering af serviceydelsen godkender Slutkunden installationen ved underskrift, og ydelsen sættes i drift.

Til backup, arkivering samt genetablering af data anvender Front-safe IBM's Tivoli Storage Manager (TSM). Læs mere om TSM på:

<http://www-306.ibm.com/software/tivoli/products/storage-mgr/>
Såfremt Slutkunden vælger at installere softwaren selv eller via tredjepart, er det alene Slutkundens eller tredjeparts ansvar, at serviceydelsen fungerer.

2.2 Licens og ejerforhold

Software, leveret af Front-safe til Slutkunden, tilhører Front-safe. Slutkunden har som en del af serviceydelsen kun brugsret til det leverede i overensstemmelse med disse betingelser samt evt. licensbetingelser. Ved aftalens ophør leveres det lånte software retur til Front-safe.

Data, som Front-safe opbevarer for Slutkunden, tilhører alene Slutkunden. Data, der sendes fra Slutkunden i krypteret format, vil forblive krypterede.

2.3 Forudsætninger før installation

Følgende forudsætninger skal være opfyldt før installation af serviceydelsen:

- Der skal være en fast internetforbindelse fra Slutkundens netværk til Front-safes netværk, som anvendes til dataoverførsel mellem disse.
- Slutkundens netværk skal være åben for udgående trafik på TCP port 1500.
- Kapaciteten på Slutkundens internetforbindelse skal være tilstrækkelig stor i forhold til overførsel af Slutkundens backupdata. Front-safe kan stille krav til minimumskapacitet på Slutkundens internetforbindelse.
- Slutkunden skal aktivt tage stilling til, hvilke data der skal være omfattet af serviceydelsen.

2.4 Forudsætninger for serviceydelsen

Følgende forudsætninger er gældende for serviceydelsen:

- Der installeres software på de maskiner hos Slutkunden, som er omfattet af serviceydelsen.
- Den installerede software fra Front-safe opsættes til at tage backup af de ønskede filer, filtyper og mapper på de ønskede drev.
- Ved ændringer i maskinens filstruktur eller ved installation af nye datagenererende applikationer, hvoraf der ønskes backup, kan det være nødvendigt at tilpasse backupinstallationen. Det er Slutkundens ansvar at gøre leverandøren opmærksom på sådanne ændringer.
- Password bør ændres efter installation. Det er Slutkundens ansvar at gennemføre denne ændring.



- Hvis Slutkunden ønsker datakryptering, skal Slutkunden under installationen indtaste en krypteringsnøgle. Det er Slutkundens ansvar at indtaste og opbevare krypteringsnøglen.
- Umiddelbart efter den første backup skal Slutkunden kontrollere, at backup er foretaget korrekt, og at data kan genskabes. Dette sker ved, at Slutkunden henter et passende udvalg af data retur fra backup.
- Det er Slutkundens ansvar med jævne mellemrum at kontrollere, at data gemt hos Front-safe kan genskabes.

Ved backup af åbne databaser, skal en af nedenstående forudsætninger være opfyldt:

- Databasesystemet skal indeholde en funktion, så der kan genereres en backup af databasen på maskinens disk.
- Der skal være installeret software på Slutkundens system, så der kan genereres en fuld backup af databasen på maskinens disk.
- Der skal være installeret en Tivoli Data Protection (TDP) agent, leveret af Front-safe, så backup af databasen sendes direkte til Front-safes backupanlæg.

2.5 Backuppolitik

Med en backuppolitik sikrer Slutkunden, at data gemmes i backuplageret i det antal versioner (antal ændringer) og i det tidsrum (Retention perioden), som lever op til Slutkundens behov. Slutkunden er selv med til at definere sit behov før installation af løsningen.

Hvis Slutkunden ikke kan eller vil definere sit behov, anvendes Front-safes standardpolitik, som er fastlagt til 2 versioner og 180 dages Retention:

2 versioner: Denne del af politikken sikrer, at Slutkunden altid vil kunne genskabe filer én version tilbage i tid. Slutkunden vil dermed kunne fortryde de ændringer og rettelser, som Slutkunden har gennemført på et dokument i løbet af en dag, ved at genskabe den tidligere version af dokumentet en efterfølgende dag.

180 dages Retention: Dette sikrer, at en tidligere version af et dokument vil forblive i backuplageret i 180 dage, med mindre naturligvis, at dokumentet på Slutkundens computer ændres, hvorved versionen erstattes af en ny version. Retention perioden sikrer endvidere, at Slutkunden kan genskabe et slettet dokument på Slutkundens maskine i op til 180 dage efter, at sletningen er gennemført.

Skematisk illustration af Front-safes standard backuppolitik (2 versioner og 180 dages Retention)

Tidspunkt	Handling hos Slutkunden	Det sker i backuplageret
Tidspunkt 1	Navn.doc oprettes som nyt dokument	
	Der tages backup	1. version - aktiv status
Tidspunkt 2	Navn.doc ændres og gemmes	1. version - inaktiv status
		2. version - aktiv status
Tidspunkt 3	Navn.doc ændres og gemmes	1. version - slettes
		2. version - inaktiv status
		3. version - aktiv status
Tidspunkt 3 + 180 dage	Navn.doc har ligget stille siden Dato 3	2. version - slettes
		3. version - stadig aktiv
Tidspunkt 4	Navn.doc slettes	3. version - inaktiv
Tidspunkt 4 + 180 dage	---	3. version - slettes

2.6 Overvågning

Det er Slutkundens ansvar selv at kontrollere serviceydelsen ved at læse fremsendte statusmail. Statusmail sendes til en udvalgt mailadresse hos Slutkunden senest kl. 13.00 indeholdende det seneste døgns aktiviteter.

2.7 Support

Se serviceaftale for Remote Backup.

2.8 Konsulent

I forbindelse med første totalbackup eller ved genskabelse af data hos Slutkunden, kan Slutkundens data afhentes eller leveres via en mobil backupserver for at optimere processen. Denne ydelse afregnes særskilt efter faktisk timeforbrug.

3. SERVICENIVEAU

3.1 Driftstilgængelighed

Optimalt sikrer serviceydelsen, at Slutkunden har adgang til sine data 24/7/365, med undtagelse af planlagte serviceinduer, samt utilgængelighed som skyldes fejl hos Slutkunden.

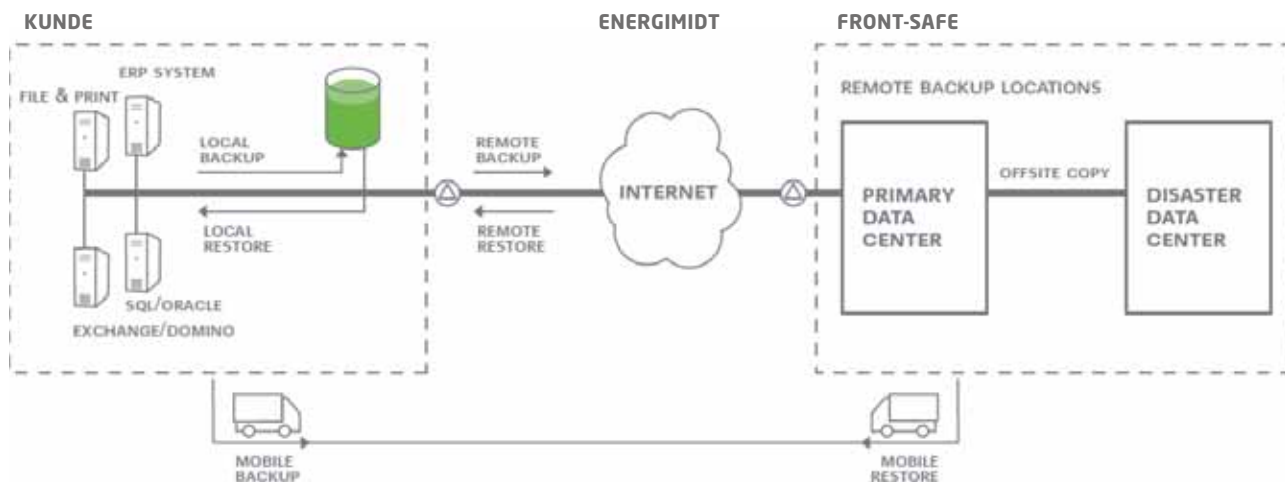
3.2 Oppetid

Følgende hændelser medgår ikke som nedetid ved beregning af oppetidsprocent:

- Planlagt serviceindue
- Nedetid, som skyldes fejl i udstyr hos Slutkunden
- Nedetid, som skyldes fejl på internetforbindelsen mellem Slutkunden og Front-safe.

3.3 Planlagt serviceindue

Front-safe vil en gang om måneden opdatere serviceydelsen for at sikre optimal drift. Det planlagte serviceindue placeres den anden torsdag i måneden i tidsrummet fra kl. 13.00 til kl. 16.00, hvor serviceydelsen ikke vil være fuld tilgængelig.



Kritiske opdateringer, anbefalet af Front-safes leverandører, vil kunne forekomme uden for det før nævnte tidsrum. Større opdateringer eller ændringer af serviceydelsen vil blive varslet med minimum 24 timer.

3.4 Garanteret opetid

Front-safe garanterer en opetid på 99 % på serviceydelsen. Ved opetid forstås fuld funktionalitet på Front-safes backup-anlæg, undtaget planlagt servicevindue. Ved eventuelle fejl på Front-safes backupanlæg vil Front-safe uden ophold påbegynde fejlretning straks 24/7/365.

4. SAMARBEJDSFORHOLD

4.1 Kontaktperson hos Slutkunden

Slutkunden navngiver over for EnergiMidt kontaktperson med telefonnummer, adresse og e-mail. Denne person skal have tilstrækkelig organisatorisk og faglig kompetence til denne funktion, ligesom vedkommende har ansvaret for at indholdet af serviceydelsen i almindelighed bliver kendt af alle, der skal arbejde med de af serviceydelsen omfattede enheder. Slutkunden er ansvarlig for at oplyse EnergiMidt om ændringer i kontaktinfo, ellers anvendes de senest kendte oplysninger.

4.2 Kontaktperson hos EnergiMidt

Slutkundens kontaktpunkt hos EnergiMidt er supporten.

4.3 Ændringshåndtering

Alle ændringer af servicebeskrivelsen eller de i serviceydelsen nævnte objekter skal ske efter skriftlig aftale mellem den kontraktansvarlige hos Slutkunden og den kontraktansvarlige hos EnergiMidt/Front-safe.

Front-safe har ansvar for at formidle opgraderinger af den til serviceydelsen installerede software. Slutkunden har ansvar for opgradering af den til serviceydelsen installerede software.

5. SIKKERHED

5.1 Formål

Formålet med dette afsnit er at beskrive det tekniske grundlag for serviceydelsen set fra et sikkerhedsmæssigt perspektiv.

5.2 Overordnet beskrivelse

Ovenstående princip skitse illustrerer sammenhængen mellem Slutkundens netværk og Front-safes backupanlæg. På skitsen er illustreret, hvorledes Slutkunden som option kan vælge at etablere en lokal backupkopi af data.

Front-safes backupanlæg er opbygget som en to-centret løsning, hvor data altid er online tilgængelig. I center 1 opbevares data på diske, og i center 2 opbevares data på tape. De to centre er forbundet med fiber og afstanden mellem centrene er minimum 3 km.

Front-safes backupanlæg er bygget, så det lever op til de angivne opetidskrav, samt at systemmæssige udvidelser kan foretages uden påvirkning af driften. Skalerbarheden sætter Front-safe i stand til at foretage nødvendige udvidelser, når der er behov for dette.

Backupanlægget overvåges 24/7/365.

5.3 Fysisk sikkerhed

Den fysiske sikkerhed omfatter fysisk beskyttelse af lokaler, anlæg og papirbaseret information, der vedrører serviceydelsen. Den fastlægger eksempelvis, at kun autoriserede personer har fysisk adgang hertil.

5.4 Ekstern fysisk sikkerhed

Front-safes backupanlæg er placeret i Hostingcentret hos søsterselskabet Front-data Danmark A/S. Nødstrømsanlæg opstartes ved eventuelt udfald eller fejl på den primære strømforsyning. Alt udstyr er endvidere forsynet med UPS, så normal drift fortsættes uden driftsstop.

Køl sikrer optimal temperatur i driftsmiljøet.

Krydsfelter og netværksudstyr er placeret i aflåste serverrum.

Der anvendes udelukkende systemnøgler.

Alarmanlæg anvendes til alle alarmovervågninger. Der føres log over alarmer.

Alle alarmer overføres til vagtcentral og/eller driftsvagt, som iværksætter og træffer de nødvendige aktioner.

Intern fysisk sikkerhed

Lokaler med fortrolig information er omfattet af adgangskontrol. Der anvendes udelukkende systemnøgler, så uautoriserede personer ikke får adgang dertil.

5.5 Logisk sikkerhed

Den logiske sikkerhed omfatter logisk beskyttelse af elektroniske systemer og information, der vedrører serviceydelsen. Fx fastlægger den, at kun autoriserede personer har elektronisk adgang hertil.

5.6 Sikkerhed for eksterne

Slutkunder har ikke mulighed for at se andre Slutkunder eller brugere på backupanlægget.

5.7 Sikkerhed for brugere

Forskelligt sikkerhedsniveau anvendes samtidig. Typisk skal brugere indtaste brugernavn og et unikt kodeord for at få adgang til serviceydelsen.

5.8 Sikkerhed for kommunikation

Der anvendes Cisco netværks udstyr i form af switche og firewalls. Al trafik mellem Slutkunden og Front-safe passerer som minimum gennem en firewall. For trafik via Internettet garanterer Front-safes udbyder 99,9% tilgængelighed.

5.9 Platform sikkerhed

Front-safes backupanlæg har ikke adgang til Internettet, undtagen de TCP porte serviceydelsen benytter, og er derfor beskyttet mod vira og andre angreb. Antivirus software opgraderes centralt og automatisk hver gang en ny version frigives. Der scannes fortløbende for virus.

5.10 System sikkerhed

Brugere garanteres en opetid på 99%. Ved opetid forstås fuld funktionalitet på Front-safes backupanlæg.

Der føres log over alle aktiviteter i backupanlægget hos Front-safe.

IT-udvikling og -afprøvning foregår i et isoleret testmiljø.

5.11 Informationssikkerhed

System- og driftsdokumentation opdateres efter hver ændring af systemer eller procedurer. System- og driftsdokumentation gemmes såvel elektronisk som fysisk i en ekstern boks.

Version 01 - Januar 2011