Tangora™ Content Management Software

## Tangora™ White Paper:

# Tangora/DIR Drift

**Tangora Software tilbyder et kraftfuldt, IBM-certificeret driftsmiljø hos Dansk Internet Rådgivning, DIR. Såvel fysiske forhold omkring driftsmiljøet som procedurer og sikkerhed i forbindelse med drift og eventuelle krisesituationer lever op til IBM's standarder for IBM xSP Prime Hosting Providers. DIR er den eneste driftsleverandør i Danmark udover IBM, der er certificeret efter denne standard.**

Tangora driftsmiljøet hos DIR er konfigureret med henblik på at yde den højest mulige performance og oppetid, bl.a. ved at der på forhånd er taget højde for så mange former for nedbrudssituationer som muligt.

## Detaljer

Driftsmiljøet er opbygget med det formål at sikre redundans i videst muligt omfang samt sikre at 'disaster recovery' kan foregå så hurtigt og effektivt som muligt. Redundans betyder, at der er reservekomponenter klar til at tage over, hvis der opstår fejl på en eller flere komponenter, således at nedetid minimeres. Servermiljøets kapacitet bliver løbende overvåget for at sikre optimal performance på systemet, og gennem en foruddefineret skaleringsproces sikres denne performance vedvarende.

### Driftsmiljøet er baseret på et omfattende erfaringsmateriale

Hurtig reetablering fra alle tænkelige nedbrudsscenarier er det overordnede princip for driftsmiljøets opbygning. Der er således foretaget forebyggende foranstaltninger med henblik på at imødegå eksempelvis følgende nedbrudssituationer:

- brud på netkabel i forbindelse med anlægsarbejde
- problemer hos en netværksleverandør
- nedbrud på en transformatorstation
- en defekt harddisk
- et defekt bundkort
- en defekt RAID controller

- problemer med bandwidth controllere og/eller switche mellem disse
- installation af en fejlbehæftet fejlrettelse fra Microsoft

Hvis uheldet skulle ske, sikres det gennem faste procedurer og standby hardware, at det vil være muligt at komme i luften fra langt de fleste nedbrudsscenarier på kortest mulig tid.

### Hardware og software

Miljøet er opbygget omkring kraftige IBM x345 og IBM e326 servere med redundante disksystemer. Hardware overvåges konstant af IBM Director. Serverne er udstyret med enten Intel Xeon processorer med HyperThreading teknologi eller 64 bit AMD Opteron med Dual Core teknologi. Derved sikres optimal ydelse i et multithreaded webhosting miljø. Der anvendes udelukkende high performance SCSI diske i redundante RAID konfigurationer – for databaseservernes vedkommende et 14 disk redundant array. Ved eventuelle fejl på en disk overtages operationerne usynligt af de spejlede diske, og en fejlmelding sendes til overvågning, så den defekte disk kan skiftes uden driftsafbrydelse.

Der anvendes Microsoft Windows Server 2003 og Microsoft Windows Server 2003 x64 på alle servere i driftsmiljøet. Windows Server 2003 er udviklet med særligt henblik på høj oppetid og sikkerhed i webmiljøer. Databasesoftware er MS-SQL server 2000.

### Redundante internetforbindelser og strømforsyning

Driftscenteret er tilkoblet 2 uafhængige højkapacitets internetkredsløb. Det ene som trådløst radiolink, det andet som en fiberlinje til to forskellige internetleverandører. Det ene kredsløb er koblet direkte på DIXen, og det andet går direkte på et pan-europæisk backbone. Når begge kredsløb er kørende, vælges automatisk det hurtigste kredsløb i forhold til klientens placering (via BGP-routing). Hvis det ene kredsløb bryder ned, kører alt trafik over det andet kredsløb. Begge kredsløb er dimensioneret til at kunne håndtere fuld belastning.

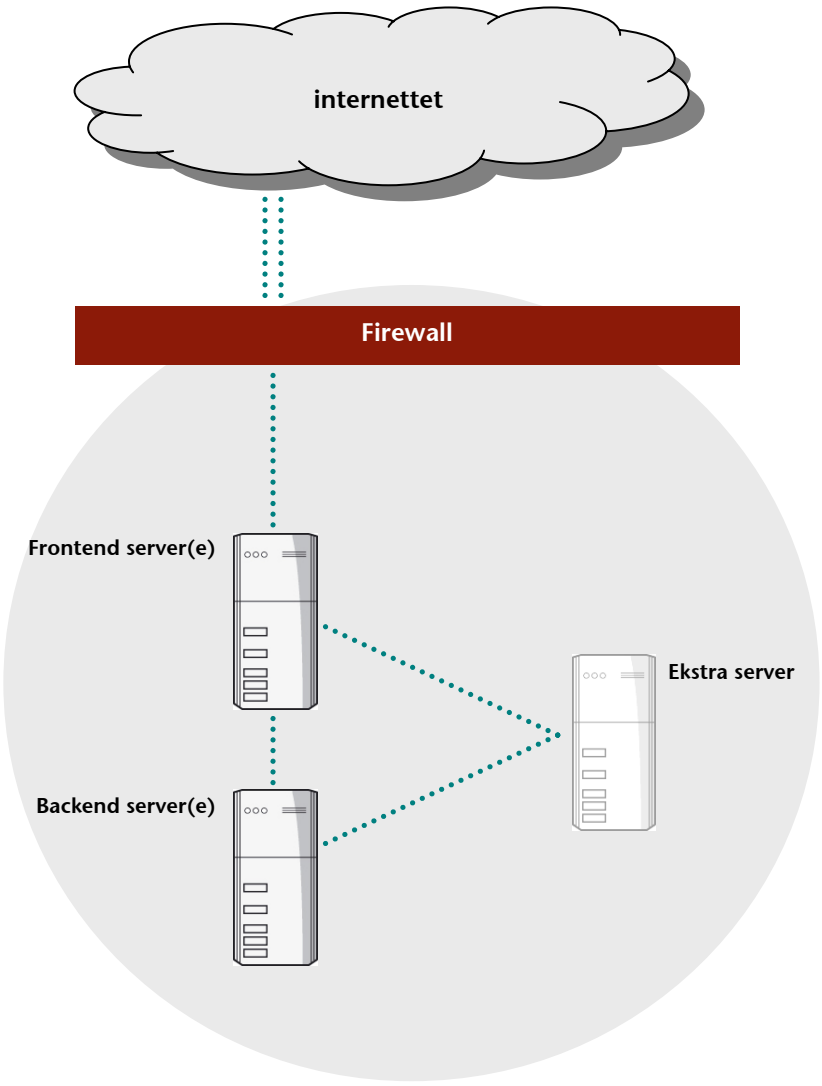
Driftscenteret er tilkoblet strøm fra to forskellige centraler for at sikre, at strømforsyningen til miljøet kan opretholdes selv ved fejl på én central. Desuden findes der nødstrømskapacitet, som kan klare strømafbrydelser af op til 1 times varighed.

### Firewall

Driftsmiljøets firewall er opdelt i 2 niveauer: Første filtrering sker i routeren (Cisco 7200), som filtrerer ICMP trafik til ping, traceroute osv. fra. Det gør det besværligt for hackere at finde ud af hvilke IP-adresser på DIR's net, der peger på servere, som kan angribes. Desuden filtreres alt unødig UDP trafik fra på dette niveau. Anden filtrering sker på de interne 'layer 3 switche' (Extreme Networks 48si) som alle servere er forbundet med. TCP trafik filtreres på dette niveau, så det kun er de services, den enkelte server skal stille til rådighed på

internet, der er åbne. Formålet med at benytte en layer 3 switch med firewall mellem alle servere er at separere de enkelte servere, således at skaden begrænses til én server, hvis denne servers systemintegritet skulle blive kompromitteret.

Lidt forenklet kan Tangora driftsmiljøet hos DIR illustreres således:




Alle servere er standardiserede, så den ekstra server vil uden videre kunne erstatte frontend eller backend server(e), hvis der skulle opstå problemer med en af disse.

### Fysisk sikkerhed

Driftscenteret indeholder ingen vinduer og er sikret med 2 ståldøre. Kun driftspersonale har fysisk adgang til servermiljøet. Alt personale har i øvrigt ren

straffeattest og har i forbindelse med ansættelsen underskrevet en fortrolighedserklæring.

Der er installeret 4 uafhængige klimaanlæg, som sørger for at holde temperatur og luftfugtighed på optimale værdier. Specielle kulfiltre renser luften, før den blæses forbi serverne. Anvendelsen af flere anlæg sikrer, at det ikke vil få væsentlig betydning, hvis et eller flere anlæg bryder sammen.

I tilfælde af røg-detektering starter et FireEater Inergen brandslukningsanlæg automatisk. Brandslukningsanlægget er CO2-baseret og kan således slukke eventuelle brande, uden at teknikken tager skade.

### Backup

Der tages backup hver nat. Backup fjernes til en fysisk adskilt lokation en gang om ugen. Der tages ligeledes komplet backup af systemdiske 1 gang om ugen, således at et reserve-setup hurtigt kan etableres, hvis der opstår fejl på operativsystem og/eller databasesoftware.

### Overvågning og nødprocedurer

Driftsmiljøet overvåges 24 timer i døgnet. Ved fejl sendes der automatisk en besked til døgnvagten hos DIR, som straks iværksætter fejlhåndtering. Før hver større opdatering af miljøet (fx ved installation af service packs eller opgraderinger af database software) tages en komplet diskkopi af operativsystem og databasesoftware således at en systemfejl under opgradering blot kræver en reboot med den gemte disk. Derved opnås hurtig recovery i tilfælde af fx fejl i sikkerhedspatches eller lignende.

Der er altid en komplet standby server klar i tilfælde af kritiske hardwarefejl. Dette sikrer, at meget alvorlige fejl – fx et afbrændt bundkort – blot vil resultere i en meget begrænset nedetid, mens diskene flyttes til standbyserveren, og denne startes op. Der findes en standby server til alle de anvendte servertyper i miljøet.

### Automatisk installation af sikkerhedspatches

Alle servere abonnerer på Microsoft Update hvilket sikrer, at sikkerhedspatches automatisk hentes og installeres, så snart de frigives fra Microsoft. Er en genstart nødvendigt, tidsfastsættes den automatisk til den førstkommende nat.

Patches og opgraderinger, som ikke kan installeres automatisk, vil blive søgt installeret i servicevinduet mellem 4 og 5 om morgenen.