

Driftssikkerhet ved bruk av kritiske IT-systemer i helsevesenet

Katastrofeberedskap og
datalagring

Versjon 1.0
15. september 2002

KITH Rapport 21/02
ISBN 82-7846-146-5

KITH-rapport

Tittel

Driftssikkerhet ved bruk av kritiske IT-systemer i helsevesenet

Katastrofeberedskap og datalagring

KITH

Kompetansesenter for IT i helsevesenet AS

Postadresse

**Sukkerhuset
7489 Trondheim**

Besøksadresse

Sverresgt 15, inng G

Telefon

73 59 86 00

Telefaks

73 59 86 11

e-post

firmapost@kith.no

Foretaksnummer

959 925 496

Forfatter(e)

Arnstein Vestad
Magnus Alsaker
Olaf Trygve Berglihn

Oppdragsgiver(e)

Standardiserings- og samordningprogrammet (SSP)

Rapportnummer

R 21/02

URL

<http://www.kith.no/rapportarkiv/>

Prosjektkode

S-IS-DSIKK02

ISBN

82-7846-146-5

Dato

15. september
2002

Antall sider

43

Kvalitetssikret av

Bjarte Aksnes

Gradering

Godkjent av

Jacob Hygen
Adm. direktør

Sammendrag

Rapporten er en oppfølging av arbeidet omkring driftssikkerhet for elektroniske pasient-journalsystemer og andre kritiske systemer i helsevesenet, og er utarbeidet på oppdrag fra Standardiserings- og Samordningsprogrammet (SSP). Rapporten bygger videre på KITH-rapport 07/02 ” Driftssikkerhet ved bruk av elektronisk pasientjournal”.

Hovedtema for denne rapporten er katastrofehandling og utarbeiding av katastrofeplaner. Videre vurderes ulike typer lagringsteknologi som kan være teknologiske virkemidler for å bygge driftssikre IT-løsninger.

To casestudies gir videre konkrete eksempler på hvordan helseforetak og helsenett forholder seg til driftssikkerhet i sine løsninger både på infrastrukturnivå (helsenett) og tjenestnivå (EJP)

Innhold

KATASTROFEBEREDSKAP	3
Katastrofeberedskap	4
Hva skal sikres?	4
UTVIKLING AV KATASTROFEPLANER.....	6
Policy.....	6
Datainnsamling	6
Risikovurdering.....	7
Preventive kontroller.....	8
Konsekvensanalyse	9
Utarbeiding av katastrofeplan	10
Katastrofehåndtering.....	11
Kontinuitetsplan	11
Plan for midlertidig drift	12
Reetableringsplan.....	12
Etterarbeid	13
Testing av planer	13
Oppdatering av planer	13
Oppsummering	13
Realiserbare planer.....	14
DATALAGRING OG DRIFTSSIKKERHET	15
RAID	15
Electroning vaulting & remote journaling	15
Diskreplikering	16
Failover	16
Clustering	17
Server Load Balancing	17
AVANSERTE LAGRINGSSYSTEMER.....	18
Viktige begreper	19
Vurdering	20

DAS	21
SAN	22
NAS	24
SSP	25
Vurdering av iSCSI og FC-IP	25
Vurderinger angående IP lagring	26
Det intelligente lagringsnettverket	27
Konvergens av NAS og SAN	27
Anbefalinger	28
Lagring i fremtiden	29
Lagringssystemer for helsevesenet	29
SIKKERHETSKOPIERING AV DATA	31
Sikkerhetskopiering (backup)	32
Aktuelle spørsmål.....	34
Strategi for sikkerhetskopiering	36
Testing av sikkerhetskopiering	37
CASE STUDIES	38
Aust-Agder Sentralsykehus (ASA)	38
Generell beskrivelse	38
Systembeskrivelse	39
Målsetting.....	39
Strategier	40
Erfaringer	40
Midt-Norsk Helsenett	41
Innledning	41
Målsetning.....	42
Strategier	42
Erfaringer	43

Katastrofeberedskap

Helsevesenet er avhengig av IT-systemer på flere måter i sin daglige drift. Har helsevirksomheten planer for å håndtere for eksempel en oversvømmelse eller en brann på en avdeling? Katastrofeberedskap handler om hvordan en virksomhet skal kunne ivareta sine viktigste funksjoner ved en katastrofal hendelse. Generelt kan en si at virksomheter som ikke kan leve uten sine IT-systemer i 48 timer, trenger en katastrofeberedskap. Dette vil i praksis si de fleste virksomheter innen helsevesenet.

Å etablere en katastrofeberedskap har to hovedmål:

1. Redusere eller eliminere sjansene for at en ødeleggende skade vil oppstå
2. Redusere eller avgrense omfanget/konsekvensene dersom en skade skulle oppstå.

Mellvik [1] kommer med følgende definisjon av en katastrofe:

”En katastrofe er en brå, uventet og skjebnesvanger hendelse som setter organisasjonen ut av stand til å utføre kritiske virksomhetsfunksjoner for en gitt periode, og som resulterer i stor skade og/eller tap”

Å definere klart hva som er en katastrofesituasjon for helsevirksomheten er et viktig utgangspunkt for å kunne gå videre i prosessen med katastrofebehandling. Det er også viktig å vurdere tidsaspektet i forhold til om en har en katastrofesituasjon. En oversvømmelse vil umiddelbart kunne føre til at en har en katastrofe, mens for et strømbrudd kan det kanskje gå 1, 2 eller 6 timer før det fører til en katastrofesituasjon.

Hva som er en katastrofe vil kunne variere for ulike virksomheter, men innen helsesektoren vil virksomheter generelt ha strenge krav til hva som omfatter en katastrofe situasjon. Et strømbrudd i en time vil kunne ha store konsekvenser på et sykehus, det er derfor viktig å planer for hva som skjer i slike situasjoner.

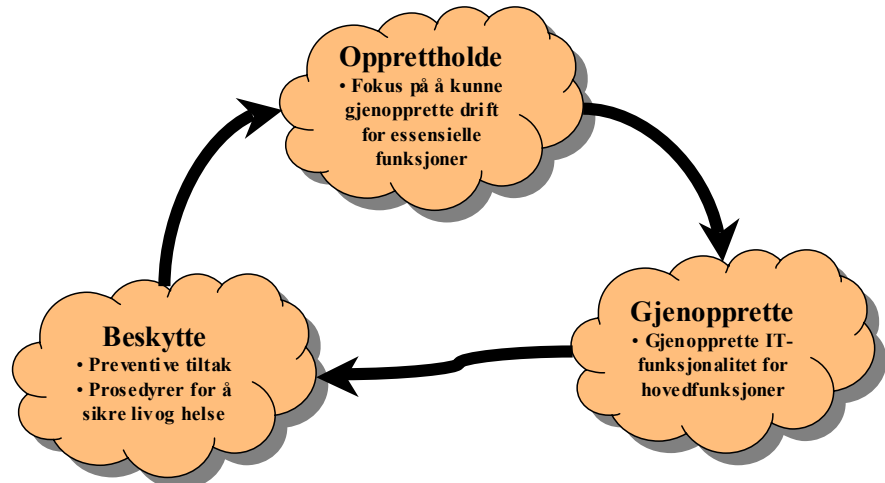
Hendelser som kan føre til katastrofer kan en stort sett gruppere i tre grupper:

1. **Menneskelige** - brukerfeil, sabotasje, ondsinnet programkode (virus), spionasje, terrorhandlinger
2. **Naturskader** - flom, brann, tornadoer, jordskjelv, storm, ras

3. **Teknologiske** - maskin/utstyrfeil, programvarefeil, strømbrudd, kommunikasjonslinjer

Katastrofeberedskap

En kan grovt sett dele katastrofeberedskap inn i en syklus med tre faser:



Figur 1: Sammenheng mellom fasene i katastrofeberedskap

Figuren over viser de tre hovedfasene ved katastrofeberedskap:

1. **Beskytte** - dette er den fasen som virksomheten befinner seg i til daglig. Her er hovedfokus på å beskytte seg mot hendelser som kan føre til katastrofer og iverksette tiltak som kan redusere konsekvensene av eventuelle katastrofale hendelser.
2. **Opprettholde** - denne fasen skal opprettholde midlertidig drift etter en katastrofal hendelse. Denne fasen setter fokus på å opprettholde de mest kritiske funksjonen i en virksomhet. Slik midlertidig drift må kunne fungere opptil et par måneder.
3. **Gjenopprette** - denne fasen skal føre virksomheten tilbake til normal drift etter en katastrofal hendelse.

Hva skal sikres?

Virksomhetens omfang og størrelse virker inn på hvilket IT-utstyr og IT-systemer som bør sikres i forbindelse med en katastrofesituasjon. Her er noen viktige deler:

- Desktop og mobile datasystemer (kan være bærbare PCer eller lommedatamaskiner)
- Webløsninger (dokumentere for eksempel software, hardware eller hvordan de er konfigurert)

- Servere
- Lokale nettverk (LAN)
- Globale nettverk (WAN)
- Distribuerte systemer
- Stormaskinsystemer
- Annet kritisk IT-utstyr

Vi vil ikke gå inn på hvordan de ulike delene best kan sikres for å opprettholde drift (for eksempel hva som er den beste måten å ta sikkerhetskopiering av innholdet på PCer på.) etter en katastrofesituasjon da dette bør være ivaretatt fra før gjennom sikkerhetsarbeidet i helsevirksomheten. Dersom for eksempel sikkerhetskopiering ikke er tilstrekkelig ivaretatt fra før, må i midlertidig også dette tas med som en del av planleggingen for katastrofeberedskap.

Sikring av pasientdata

Som en del av katastrofeberedskapen vil vi se på hvordan en fysisk kan sikre kritisk IT-utstyr mot for eksempel brann eller oversvømmelse. Det som er viktig ved en katastrofesituasjon, foruten å sikre fysisk utstyr, er å sørge for å ta vare på pasientdata (spesielt i forbindelse med elektronisk pasientjournaler - EPJ):

- Hindre tap eller ødeleggelse av data som er lagret i EPJ eller andre kritiske systemer, som følge av teknisk svikt eller materiell skade
- Sikre tilgjengelighet til data (herunder sikre at responstid og ytelse er akseptabel)

Sikring av pasientdata kan for eksempel gjøres ved å etablere drift på et eget alternativt sted, eller å flytte driften over til et annet sykehus i området. Andre tiltak kan være å benytte andre servere eller andre kommunikasjonslinjer dersom disse feiler.

Utvikling av katastrofeplaner

Det er viktig å gjøre forarbeid før en setter i gang med å utvikle selve planene for katastrofesituasjoner. Gjennom dette arbeidet skal en finne ut hvilke funksjoner/prosesser/prosedyrer som finnes i helsevirksomheten og prioritere hvilke som er viktigst å opprettholde ved en katastrofesituasjon. Gjennom dette forarbeidet bør en finne ut hvor kritiske og avhengige helsevirksomheten er av sine IT-systemer, og hvor mye ressurser en er villig til å bruke på katastrofeberedskap. I denne sammenhengen vil det kunne være nyttig å sette opp kost-nytte forhold for å se om ulike IT-ressurser er verdt å sikre for en katastrofe.

Policy

Å utarbeide en policy for en katastrofesituasjon er en god start for det videre arbeidet. En slik policy for katastrofesituasjoner bør gjelde for hele helsevirksomheten og inneholde blant annet følgende:

- Roller og ansvar (både i forhold til personer og avdelinger)
- Krav i forhold til øvelser
- Planer for testing/gjennomgang av en katastrofesituasjon
- Planer over vedlikehold av katastrofeplaner
- Frekvensen for sikkerhetskopiering og lagring av sikkerhetskopier

En bør ta hensyn til andre eksisterende planer som finnes når en utvikler katastrofeplaner. Dette kan for eksempel være planer for systemsikkerheten eller planer for kritisk infrastruktur. Dette er viktig slik at katastrofeplanene blir en del av den helhetlige sikkerheten for en helsevirksomhet.

Datainnsamling

Datainnsamlingen har til hensikt å skaffe oversikt over kritiske ressurser i helseorganisasjonen. Informasjonskilder i denne sammenhengen kan være målsetninger, policyer, regelverk, prosedyrer, strategier, handlingsplaner, og planer/tegninger knyttet til bygninger og bemanning.

Det en ønsker å finne ut er blant annet:

- Hvor dynamisk er informasjonen i helsevirksomheten?

- Hvor avhengig er helsevirksomheten av informasjonens tilgjengelighet for den daglige driften?
- Hvordan blir informasjonen lagret?

Disse parametrene vil til slutt fortelle hvordan informasjonen bør behandles (lagres) og dens prioritet i en krisesituasjon. Dersom fjernlagring av kritiske data allerede er på plass blir jobben i denne fasen blir å kontrollere at den er tilgjengelig innenfor de tidsrammer som helsevirksomheten definerer som akseptable. Dersom helsevirksomheten ikke har tilstrekkelige funksjoner/prosedyrer for å ivareta sikkerhetskopiering og fjernlagring av data bør dette inngå som en del av arbeidet med å utarbeide katastrofeberedskap.

Risikovurdering

En risikovurdering er en kritisk del av det å utarbeide planer for en katastrofesituasjon. Informasjonen fra en risikovurdering skal kunne fastsette krav og prioriteter for en katastrofeplan. Her kommer noen aktuelle punkter for en risikovurdering:

- Skaff til veie relevant informasjon som omhandler risiko for virksomheten
- Hele helsevirksomheten må dekkes, ikke bare en avdeling eller en bygning
- Få flere synspunkter på problemstillinger
- Identifiser kritiske IT-funksjoner
- Angi hvilke systemer som det er viktig å gjenopprette først
- Sett fokus på tid: havner en risiko på rett eller feil side av det som regnes som en katastrofe
- Kost/nytte er viktig: sett fokus på de skadene som er kritiske og/eller kostnadseffektive å sikre
- Identifiser preventive kontroller (se mer under)
- Identifiser konsekvenser av nede-tid for systemer og angi akseptable tidsrom for nede-tid

De ulike risikoene samles og systematiseres slik at en får oversikt over truslene. Flere parametere avgjør hvor stor trussel en risiko utgjør. Sannsynligheten, konsekvensene, hastigheten, varslingstid og varigheten er faktorer som avgjør hvilke trusler som er de mest aktuelle å beskytte seg mot. Det er ikke nødvendigvis truslene med størst konsekvens som utgjør den største risikoen. En trussel med mindre konsekvens kan ha større risiko for eksempel ved at den har større sannsynlighet for å inntreffe.

Risikovurderinger er et eget fagfelt og ofte bør ekstern hjelp benyttes. Det er likevel viktig at noen fra virksomheten er med på risikovurdering-

en, dette for å sikre at hele virksomheten blir vurdert og for å få kunnskap om hvordan en utfører risikovurderinger.

Det er godt mulig at virksomheten tidligere har utført risikovurderinger i forbindelse med sikkerheten til IT-systemer. Da kan en godt bruke disse som utgangspunkt, og så vurdere om ytterligere risikovurderinger behøves utført. For en nærmere beskrivelse av hvordan en gjennomfører risikovurderinger (eller risikoanalyser) kan KITH sin rapport ”*Risikoanalyse – Metodegrunnlag og bakgrunnsinformasjon*” være et godt utgangspunkt.

Preventive kontroller

Det er like viktig å vurdere preventive tiltak som å legge planer for håndtering av en katastrofesituasjon. Preventive kontroller er tiltak som kan forhindre at en hendelse ikke oppstår eller som gjør at konsekvensene av en hendelse reduseres til ikke å føre til en katastrofesituasjon.

En del av arbeidet med å redusere konsekvenser ved katastrofehendelser er å planlegge for drift ved et alternativt sted. Det finnes flere ulike typer steder å rekonstruere et system på:

- **Cold sites** - vil si at det finnes fysisk plass og infrastruktur for å støtte IT systemer som helsevirksomheten har.
- **Warm sites** - vil si at det finnes et delvis utstyrt sted som inneholder deler eller hele av nødvendig hardware, software, telekommunikasjonen og strømforsyning til IT systemer for helsevirksomheten.
- **Hot sites** - vil si steder med kapasitet til å støtte systemkrav og med nødvendig hardware, infrastruktur og supportpersonell.
- **Mobile sites** - er et transportabelt ”skall” som er utstyrt med nødvendig utstyr som skal til for å kunne støtte IT systemer som helsevirksomheten har.
- **Mirrored sites** - vil si at stedet er fullt ut redundant (gir samme muligheter) med det stedet hvor katastrofen inntraff.

Sikkerhetskopiering for en helsevirksomhet bør allerede være ivarettatt før en kommer så langt som å utrede katastrofeberedskap. Det er likevel en del punkter som det er relevant å vurdere i prosessen med katastrofeberedskap:

- Oppbevaring av sikkerhetskopier utenfor virksomheten
- Bruk av standard plattformer slik at det lettere lar seg gjøre å gjenopprette systemer etter stans
- Sikre redundans for (kritiske) IT-systemer
- Koordinering med sikkerhetstiltak

Konsekvensanalyse

Konsekvensanalysen vil si noe om konsekvensene av at ulike prosesser i helsevirksomheten blir utsatt for en katastrofesituasjon. Det overordnede målet er å få kunnskap nok til å kunne opprettholde kritiske funksjoner i en krisesituasjon.

Konsekvensanalysen setter fokus på hvilke prosesser som finnes i virksomheten, hvilke som er kritiske, hvordan henger de sammen, hvordan påvirker de hverandre og hva må til (ressurser) for å holde dem i gang?

En enkel handlingsplan for å etablere sammenhenger og konsekvenser kan se slik ut:

- Identifiser prosessene i virksomheten og kvalifiser deres betydning i kritiske sammenhenger
- Prioriter prosessene i forhold til hverandre og i henhold til behovene som må dekkes for å holde helsevirksomheten i gang
- Definer målsetninger og tidsrammer for hver enkelt av de mest kritiske prosessene: hvilke funksjoner må være i gang igjen etter X minutter og Y sekunder?
- Dokumenter det som er funnet på et format som passer helsevirksomheten og personene som er involvert

For hver kritiske prosess bør det dokumenteres følgende:

- Dens funksjon, rolle og grensesnitt mot omverden
- Nøkkelpersoner
- Hva som er kritisk
- Hvilke ressurser som kreves

Mens risikovurderingen i stor grad fokuserte på forebygging og skadereduksjon, handler konsekvensanalysen primært om restituering av drift. Dette vil si hvordan en skal komme seg i gang igjen etter en katastrofesituasjon. Mens en i denne fasen prøver å kartlegge prosessene innad i helsevirksomheten kan det være lett å overse selvfølghetene - for eksempel grensesnitt mot forsikringsselskaper, offentlig brannvern, lokale og sentrale myndigheter, presse/media og så videre.

Worst case situasjoner

Selv om konsekvensanalysene i utgangspunktet skal ta for seg de truslene med størst risiko, kan det være aktuelt å sette opp de verst tenkelige situasjoner som kan ramme helsevirksomheten. I denne sammenhengen kan aktuelle spørsmål være:

- Hva skjer dersom hele bygninger eller avdelinger blir totalskadd?
- Hva skjer dersom en eller flere personer fra katastrofegruppen ikke blir tilgjengelige i en katastrofesituasjon?
- Hva skjer dersom en ikke får tilgang til alternativt driftssted?

- Hva skjer dersom flere virksomheter i området blir rammet av samme katastrofe (kanskje flere virksomheter har avtaler med samme forhandler om støtte under en katastrofe), hvordan blir virksomheten prioritert?

Metoder

Intervjuer, spørreundersøkelser, arbeidsgrupper og diskusjoner er blant metodene som kan benyttes for å komme frem et tilfredsstillende resultat. Metodikk, omfang og dybde på disse metodene må tilpasses helsevirksomhetens størrelse, type virksomhet og omfang.

Når de kritiske prosessene er kartlagt og dokumentert må virkningene av ulike grader/former for katastrofer kartlegges, dette bør gjøres for hver enkelt prosess.

IT-beredskap

Analysene som nå er gjort danner grunnlag for å kunne sette opp en prioritert liste av IT-systemer og deres avhengigheter:

- Hvor lenge hvert enkelt av dem kan være ute av drift
- Hvem (brukergrupper og deres størrelse) som har den største avhengigheten
- Hvilke ressursbehov de har (også med hensyn på data og kommunikasjon)
- Minimum tilgjengelighet - hva kreves for å opprettholde drift

Denne oversikten gir helsevirksomheten grunnlaget for å definere ulike nivåer av beredskap og få en pekepinn om kostnader og nødvendige investeringer.

Handlingsplan

Arbeidet bør ende opp med en handlingsplan for etablering av beredskap. Denne handlingsplanen bør inneholde alle relevante forhold ved en katastrofesituasjon, selv opplagte/innlysende punkter bør blir tatt med. Grunnen for dette er at kaos/stress/panikk eller andre forhold ved en katastrofe ikke skal føre til at en glemmer opplagte punkter.

Nøkkelord for handlingsplanen er enkelhet, klare ansvarsforhold og en tilgjengelig toppledelse - som holder seg i bakgrunnen og ikke i frontlinjene.

Utarbeiding av katastrofeplan

Etter å ha gjort forarbeidet er neste fase å utarbeide selve planene for katastrofesituasjoner. Disse planene bør deles inn i flere faser som strekker seg fra det til å iverksette strakstiltak etter at en katastrofe er inntruffet til å bygge opp igjen normal drift av IT-systemene som ble berørt av hendelsene som førte til katastrofen.

Katastrofehåndtering

Katastrofehåndtering (øyeblikkelig hjelp) dekker de første timene (f.eks. 6/12//24/48) etter at en katastrofe har inntruffet. Målsetningen er å begrense fysiske, menneskelige og andre skader maksimalt, og bringe ansvarsforhold, informasjonsflyt osv. under kontroll. En hendelse kan oppstå både med og uten forvarsel (en flom er som regel mulig å forutsi, mens et virusangrep som regel kommer uten forvarsel) og det er viktig å ha dokumenterte prosedyrer for begge tilfellene.

Katastrofehåndteringen kan kort deles opp i to faser:

1. **Skadevurdering** - det er viktig å se på hvordan IT systemet har blitt skadet (eller kan bli), dette er avgjørende for hvordan beredskapsplanene vil bli implementert. Gruppen som avgjør skadeomfanget bør derfor være den første gruppen som blir informert ved en skade.
2. **Aktivisering av planer** - dersom er eller flere av kriteriene for en katastrofesituasjon er oppfylt, må de nødvendige tiltak i katastrofeplanen igangsettes.

Aktivitetene i denne fasen består av å fordele oppgaver og ansvar til personer, stoppe eller styre skadeutviklingen, sørge for at personell er utenfor fare og få de fysiske skadene under kontroll. Derom ikke hendelsen er direkte rettet mot IT-systemer er det lite i denne fasen som er rettet mot IT-siden utover å få sørge for at verken utstyr eller rekvisita kommer på avveie.

Et viktig punkt for denne fasen er å ha oppdaterte lister med prioriterte kontaktpersoner (kan lages som en trestruktur). Dersom en viktig kontaktperson ikke er tilgjengelig vil en slik liste vise hvem som er den neste som skal bli kontaktet.

Kontinuitetsplan

Kontinuitetsplanen skal sørge for at virksomheten kan opprettholde sin virksomhet på kort og lang sikt. Viktige punkter i denne fasen er:

- Skape trygghet
- Sørge for stabilitet
- Fokus på kritiske funksjoner i virksomheten
- IT-funksjoner og kommunikasjonssystemer må gjøres tilgjengelige slik at de kritiske funksjonene kan utøves
- Tilgang til konfigurasjonsinnstillinger (dette vil kunne være essensielt for å kunne sette i drift kritiske IT-systemer og IT-utstyr). Konfigurasjonen for følgende bør være dokumentert:
 - Hardware
 - Programvare

- Servere
- Databaser
- Rutere

Et viktig element som muliggjør slik kontinuitet er midlertidige lokaler med grunnleggende infrastruktur og tilgjengelige data. I denne sammenhengen er det relevant å vurdere:

- Distansen fra virksomheten til det alternative driftsstedet (distansen må være ”innen” rekevidde, men vil for eksempel flom, ras eller uvær også ramme det alternative driftsstedet dersom det ligger for nære?)
- Hvor tilgjengelige er dataene (tid det tar å gjøre de tilgjengelige)
- Kostnadene med å iverksette drift ved det alternative stedet

Ofte vil det være hensiktsmessig å etablere en kontinuitetsplan i samarbeid med tjenesteleverandører som tilbyr slike tjenester. Det er også tenkelig at for eksempel store sykehus kan tilby slike tjenester for mindre sykehus. Det er viktig å huske på at ikke hele driften for en helsevirksomhet skal berøres i en slik plan. Det er kun de mest kritiske funksjonene som skal ivaretas.

Et annet alternativ (men trolig dyrere) er å selv kjøpe inn utstyr og lagre det på en sikker plass.

Det er viktig at kontinuitetsplanen ikke bare er på papiret, men at den faktisk kan gjennomføres med tilgjengelig personell og økonomiske ressurser som virksomheten har tilgjengelig.

Plan for midlertidig drift

Denne fasen skal få virksomheten raskt i gang igjen og på en måte som gjør at driften kan fungere tilfredsstillende på i verste fall en periode over flere måneder. Her skal alle aktuelle medarbeidere kunne være i stand til å utføre arbeidet sitt med rimelig effektivitet.

Driften i denne fasen vil være mer kostbar og mindre effektiv enn til vanlig, men dette er noe som kan være delvis dekket av en forsikringspolise.

For helsevirksomheter er det aktuelt å kunne samarbeide med andre helsevirksomheter i området. For slike løsninger er det en fordel om de ulike helsevirksomhetene har samme policyer, prosedyrer, forsyninger og utstyr for lettere å kunne overføre pasienter, personell og data mellom helsevirksomhetene.

Reetableringsplan

I denne fasen blir midlertidig drift avsluttet og virksomheten ført tilbake til normal drift. Reetableringsplanen må ta høyde for at de opprinnelige

lokalene kan være fullstendig ødelagt. Det må altså være alternative løsninger avhengig av katastrofens art og omfang.

Etterarbeid

Etter at alle prosedyrer/planer er fastlagte må en finne ut om disse fungerer som ønskelig.

Testing av planer

Testing av planer er viktig for å oppdage og adressere feil/mangler som oppdages. Følgende bør bli testet:

- Systemgjenoppretting på en alternativ plattform fra sikkerhetskopier
- Intern og ekstern kommunikasjon
- Hvordan systemet fungerer med alternativt utstyr
- Gjenopprettingen av normale funksjoner

Resultater/erfaringer fra tester bør dokumenteres og gås igjennom av testdeltakere og annet relevant personale.

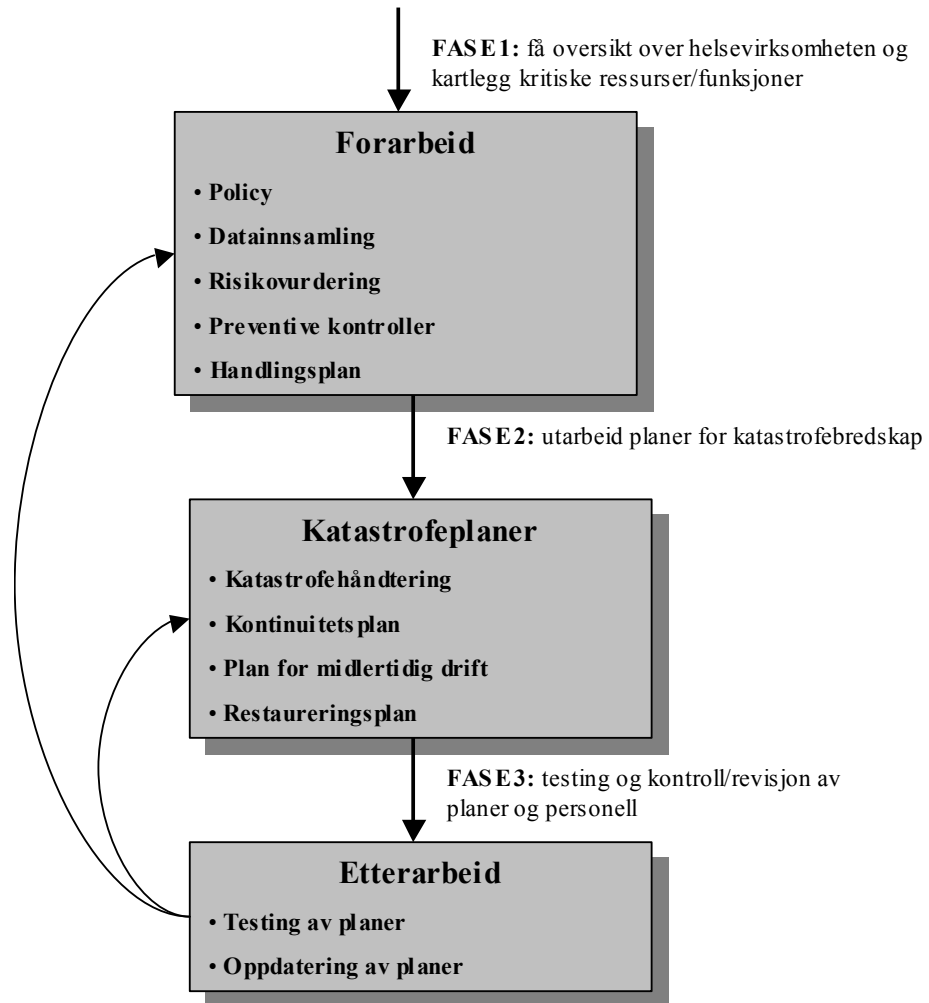
Oppdatering av planer

Planer må være oppdaterte slik at de dekker den situasjonen som helsevirksomheten befinner seg i. Følgende bør være fokus for planene:

- Operative krav (for eksempel hva kreves av utstyr ved et fullstendig strømbrudd for å tilfredstillende kommunikasjon)
- Sikkerhetskrav
- Tekniske prosedyrer
- Hardware, software og annet utstyr
- Navn og kontaktinformasjon av gruppemedlemmer
- Navn og kontaktinformasjon til leverandører, alternativt lagringssted og lignende
- Krav til fasiliteter hos alternativt lagringssted

Oppsummering

Figuren under viser en oversikt over arbeidet med katastrofeberedskap.



Figur 2: Oversikt over arbeidet med katastrofeberedskap

Det som er viktig med utarbeiding av beredskapsplaner er at en ikke ender opp med et statisk arbeid som en gjennomføres en gang for alle. Planene bør endres og oppdateres ettersom helsevirksomheten selv endres og utvikles.

Realiserbare planer

Planlegging av en katastrofesituasjon er viktig, men må ikke overdrives til å gå over i planlegging av detaljer og mindre viktige punkter. Det som er viktig er at planene er realistiske i forhold til helsevirksomheten og er gjennomførbare med tilgjengelige ressurser (personer, kunnskap, økonomi). Som nevnt tidligere er det viktig at planene er klare og at ansvarsforhold er klart definert.

Datalagring og driftssikkerhet

En virksomhets datalager er fra et arkitekturmessig synspunkt kanskje den mest sentrale IT-ressursen og må derfor vektlegges spesielt når tiltak for driftssikkerhet skal planlegges. Lagring tilrettelegges på en rekke ulike måter med varierende grad av redundans og pålitelighet. Dette kapitlet og det etterfølgende vil skissere ulike teknologiske elementer som er aktuelle. I dette kapitlet beskrives det ”enkle” metoder for lagringsløsninger som kan være med på å øke tilgjengeligheten til data i en virksomhet, mens neste kapittel fokuserer på mer avanserte løsninger.

RAID

RAID er en form for lagringsløsning som blant annet tilbyr diskredundans. Metoden skal også øke tiden mellom hver store feil (MTBF – Mean Time Between Failure). Kort forklart benytter RAID flere disker istedenfor en disk for bedre sikkerheten for lagrede data.

RAID bruker tre ulike metoder for dataredundans:

1. **Speiling** (mirroring) - skriver data samtidig til ulike disker. Fordelen med speiling er minimal nedetid, enkel gjenopprettelse av data og bedre lesing fra disk. Bakdelen med speiling er at systemytelse kan reduseres fordi at begge drev eller disker skriver data samtidig.
2. **Paritet** (Parity) - avgjør om data har blitt mistet eller skrevet over. Fordelen er at data kan bli beskyttet uten at en trenger å lagre en kopi av dataene slik som med speiling.
3. **Striping** - distribuerer data på ulike drives som finnes

Det finnes flere utgaver av RAID løsninger som er delt inn i seks nivåer fra RAID-0 til RAID-5, hvor RAID-0 er den enkleste løsningen.

Electroning vaulting & remote journaling

Dette er to metoder som ligner på RAID, men som gir noe bedre sikring ved blant annet kortere gjenopprettelsestid og mindre tap av data dersom en server skulle gjøre feil mellom sikkerhetskopiering. Dette gjøres ved at

sikkerhetskopier blir sendt over kommunikasjonslinjer til fjernlager utenfor virksomheten.

Metodene har funksjoner for automatisk sikkerhetskopiering til ”offsite” steder, og føring av transaksjonslogger og journaler slik at ved eventuelle feil skal det være enklere å kunne gjenopprette dataene.

For at metodene skal fungere kreves det at virksomheten har en lagringssted utenfor virksomheten som sikkerhetskopiene går til.

Diskreplikering

Denne metoden går ut på at data blir skrevet til to ulike diskere slik at det alltid finnes to kopier av dataene som er tilgjengelige. De to diskene er kalt beskyttet server (hovedserver) og replikasjonsserver (sikkerhetskopi-server).

To metoder:

1. **Synkronisert/speiling** - denne metoden bruker disk-til-disk kopiering og består av en replikasjon av databasen eller filsystemet ved å utføre endringer på replikasjonsserveren på samme tid som på den beskyttede serveren.
2. **Asynkronisert/skygging** (shadowing) - denne metoden inneholder en replikasjon av databasen eller filsystemet ved å føre endringer i en logg. Endringene i loggen blir så utført på replikasjonsserveren.

Failover

Failover kan gjelde både hardware og software. For hardware betyr det at dersom et system får en feil, så tar et annet system umiddelbart over. Brukere av slike systemer vil merke minimalt eller ingenting til en feil i et system.

Software failover betyr at softwaren er ”opperksom” på failover. Et nivå på slike software løsninger er at softwaren oppdager at det er en feil i et system og overfører automatisk operasjoner til et annet system. Et annet og mer vanlig nivå er at softwaren kan restartes på en annen maskin. Denne siste varianten fører til at brukere mister forbindelsen med softwaren og må koble seg opp på ny.

Aktiv - Aktiv

I en aktiv - aktiv failover konfigurasjon er det sekundære systemet alltid klar til å ta over dersom det skjer en feil i det primære systemet. Brukere vil ikke merke feil i denne typen systemer.

Aktiv - Passiv

I en aktiv - passiv failover konfigurasjon kan det sekundære systemet ta over ansvaret til det primære systemet. Brukere av denne typen systemet

vil merke feil ved at forbindelsen bryter og en må opprette ny forbindelse med systemet.

Clustering

Clustering (kan omtales som klynge på norsk) vil si at flere maskiner arbeider sammen og fungerer som en stor enhet. Silke systemer er som regel konfigurert for hardware failover, slik at dersom en maskin i klyngen feiler så kan en annen maskin ta over. Dette fungerer helt transparent for brukere av systemet. Dersom en maskin i klyngen ikke er tilgjengelig, håndterer softwaren dette og re-fordeler operasjoner innad i klyngen for å unngå avbrudd i operasjoner.

Det finnes tre hovedtyper clustering:

1. **Delt minne** - dette vil si at alle serverne i klyngen bruker det samme primære minnet hvor trafikken er rutet. Serverne deler også en enkel kopi av operativsystemet og I/O systemet.
2. **Delt disk** - dette vil si at hver server i klyngen har sitt eget minne, men at klyngen deler på diskene.
3. **Delt ingenting** (shared-nothing) - dette vil si at alle servere i klyngen har sitt eget minne og sine egne diskene. Systemer som er basert på diskspeiling bruker ofte denne modellen.

Kombinasjoner finnes som utnytter flere av modellene og den mest vanlige av disse er ”felles-disk” modell på toppen av en ”delt-ingenting” modell. Med denne modellen kan bare en server om gangen aksessere en disk, men dersom serveren feiler kan en annen server ta over.

Server Load Balancing

Denne metoden går i hovedsak ut på å fordele trafikk mellom servere som kjører en felles applikasjon. Trafikken blir dynamisk fordelt mellom serverne slik at ingen blir overbelastet med trafikk. Serverne fungerer som en serverenhet i nettverket, og brukere vil derfor merke minimalt til en slik løsning. Load balancing kan brukes for servere innenfor samme sted eller mellom servere på ulike steder. Ved å bruke metoden for servere på ulike steder kan et system være kjørende så lenge det finnes et sted hvor serverne fungerer.

Avanserte lagringssystemer

I dette kapitlet beskrives det ulike løsninger for mer avanserte lagringssystemer (og da spesielt nettverksbaserte lagringssystemer) enn de som ble beskrevet i forrige kapittel. De ulike løsningene har forskjellig arkitektur og egenskaper/funksjoner. De ulike systemene kan fortsatt benytte seg av de ulike lagringsmetodene (som RAID eller disk replikasjon) som ble beskrevet i forrige kapittel.

Nesten like viktig som selve lagringen av dataene er det å ha tilhørende systemer for organisering, søking og gjenfinning av data. Uten dette blir dataene fort en samling av kaos som i realiteten er verdiløs.

Den teknologiske utviklingen har ført til at lagring av data blir påvirket av mange faktorer. Tilgjengelig båndbredde til lav pris, billig lagringskapasitet, behov for stor dynamikk og skalerbarhet, høy pålitelighet, enkelhet, tilgjengelighet, effektivitet og lave administrasjonskostnader fører til at spørsmål om lagring av data ikke gjelder bare selve lagringen av data. Dette har ført til at lagringsteknologi har beveget seg bort fra grunnlagsteknologier og nærmere tjenester. I forbindelse med lagring snakker en sjeldnere om disk, RAID eller IDE, og heller oftere om lagringssystemer, SAN, NAS eller lagringsarkitektur.

Lagringssystemer som DAS/NAS/SAN er en samling av flere ulike fysiske lagringsenheter som er gjort om til en logisk virtuell lagringsenhet som kan bli håndtert sentralt, og også presentert til nettverksapplikasjoner, operativsystem og brukere som et stort lagringssystem.

Det finnes fire hovedtyper for lagringssystemer:

1. **DAS** (Direct attached Storage) - håndterer fysiske blokker av fast størrelse
2. **SAN** (Storage Area Network) - håndterer logiske blokker av vilkårlig størrelse
3. **NAS** (Network Attached Storage) - behandler filer med navn, attributter og rudimentær aksesskontroll
4. **SSP** (Storage Service Provider) - håndterer hele spekteret, inkludert avregning, replisering og sikkerhetskopiering. En SSP er rett og slett en leverandør som tilbyr lagringstjenester.



Figur 3: Lagringsløsningene fordelt på ulike nivåer (KILDE: Mellvik-rapporten nr. 85)

Figuren over viser på hvilket ”nivå” de fire lagringsløsningene jobber mot. Fra SSP som er en lagringstjeneste for objekter som et program kan forholde seg til, og ned til DAS som blant annet omfatter bit strømmen som leses og skrives på roterende magnetiske disk.

Viktige begreper

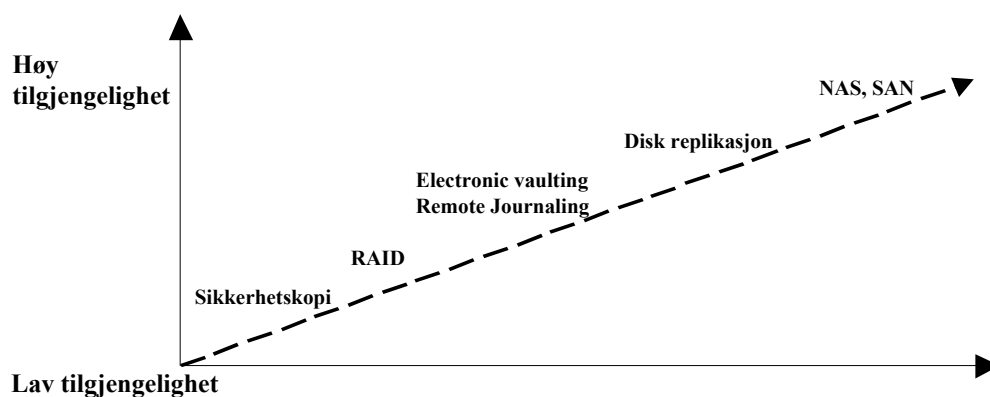
Det er tre begreper som er viktige i forbindelse med lagring

- **Konnektivitet** - hvordan prosessorer og lager fysisk er sammenkoblet:
 - **Direkte kobling** - dette vil si at en enkel prosessor er koblet sammen med en lagringsenhet. DAS er en type av direkte kobling.
 - **Nettverkskobling** - dette vil si at en eller flere prosessorer er koblet sammen med to eller flere lagringsenheter. NAS og SAN er typer av nettverkskoblinger.
- **Medium** - type kabling med tilhørende protokoller som er brukt for forbindelsen:
 - **Ethernet** begynte som medium for å danne LAN (lokale nettverk) i 1980-åra. IP-baserte protokoller som TCP/IP kjører som regel på toppen av Ethernet.
 - **Fibre Channel** er en teknologi utviklet på 1990-tallet og har blant annet av sin pålitelighet og ytelse blitt populær som prosessor-til-lager medium.
- **I/O henvendelser** (requests) - hvordan I/O (input/output) henvendelser er transportert over mediet:
 - **SCSI** (Small Computer System Interface) blir ofte kalt en ”blokk-nivå” protokoll fordi SCSI I/O kommandoer spesifiserer spesielle blokker (sektorer) på en gitt disk.
 - **NFS** (Network File System) er en fil-nivå protokoll for aksessering og deling av data.
 - **CIFS** (Common Internet File System) er som NFS en fil-nivå protokoll for aksessering og deling av data.

Vurdering

Her er hovedfordelene med de tre hovedtypene for lagringsteknologier:

- **DAS** er optimalisert for enkle (single) og isolerte prosessorer, og har lave kostnader før det kan settes i drift
- **SAN** er optimalisert for høy ytelse og skalerbarhet. Dette inkluderer blant annet høyhastighets fiberkanal (fibre channel) medium, støtte for behandling av flere disker/taper som en enhet med et kontrollpunkt, og spesielle sikkerhetskopifunksjoner.
- **NAS** er optimalisert for enkel håndtering og fildeling ved å bruke billige Ethernet-baserte nettverk. Installasjon er relativt rask og lagringskapasiteten blir automatisk tildelt brukere etter behov.



Figur 4: Tilgjengelighet for ulike lagringsløsninger (KILDE: NIST Special Publication 800-34)

Figuren over viser den relative tilgjengeligheten av ulike lagringsløsninger (det er også tatt med løsningene som ble beskrevet i kapittel 1). Høy tilgjengelighet i denne sammenhengen betyr at tap av data eller nedtid måles i minutter, mens for lav tilgjengelighet kan det ta dager å få opp igjen en server etter en feil.

EGENSKAP	DAS	NAS	SAN
Delt lagringsvolum	Nei	Nesten aldri	Ja
Fildeling		Ja	Nesten aldri
Robusthet	Veldig lav	Lav	Høy
Styrbarhet		Høy	Lav
Sikkerhetskopi/gjenoppretting	Veldig dårlig	Dårlig	God
Ytelse	God	Lav	Høy
Kostnader	Veldig lav	Lav	Høy
Skalerbarhet	Veldig lav	Lav	Høy
Nettverk		IP (vanlig)	Fiberkanal (uvanlig)

Tabell 1: Forskjeller i arkitekturen mellom DAS, NAS og SAN

Tabellen over viser de viktigste egenskapene og forskjellene mellom DAS, NAS og SAN. Denne kan fungere som en første pekepinn på hvilken lagringsløsning som passer best for ulike virksomheter.

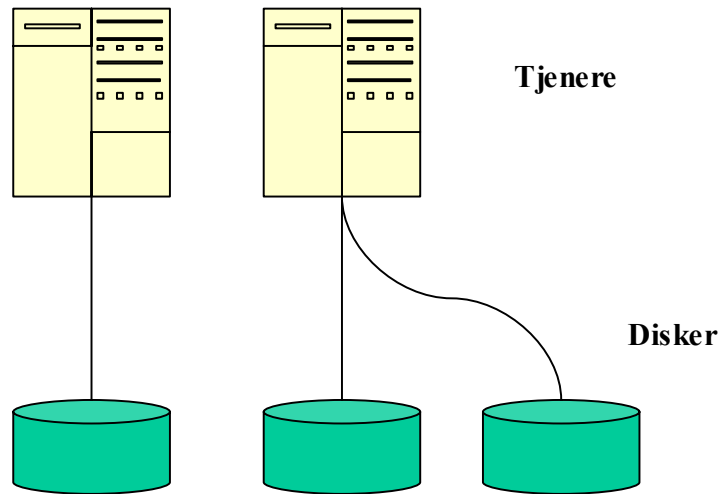
DAS

DAS (Direct Attached Storage) er den tradisjonelle formen for datalagring som innebærer at disker direkte er knyttet til systemene de tilhører. DAS er fortsatt den dominerende formen for lagring. DAS lagringssystem består av generelle tjenerer med lokale disker og aksesskontroll via tjenerens operativsystem.

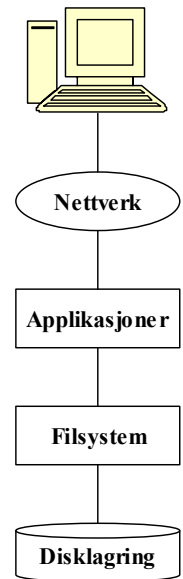
DAS sies å ha et ”blokk-nivå” grensesnitt. Med dette menes det at I/O henvendelser fra klienten spesifiserer spesielle blokker (eller sektorer) på spesielle disker.

Følgende karakteriserer et DAS lagringssystem:

- Kapasiteten er dedikert per tjener
- Sikkerheten håndteres av tjeneren
- Påliteligheten håndteres av tjeneren eller tjener/disk-system i fellesskap (for eksempel RAID)
- Utnyttelse av kapasiteten er avhengig av muligheten for å planlegge kapasiteten. Valget står ofte mellom overkapasitet eller å legge inn driftsavbrudd for å gjøre oppgraderinger.
- Endringer (konfigurasjoner, kapasitet etc) krever hardwareforandringer og driftsavbrudd
- Det kan ta tid før kapasitetsforandringer avdekkes til de kan tilfredsstilles
- Moderat effektivitet i og med at tjeneren sjelden er optimalisert for oppgavene



Figur 5: DAS lagringssystem



Figur 6: DAS arkitektur

Det finnes klare ulemper med DAS i og med at det ikke kan fungere som nettverkslagring:

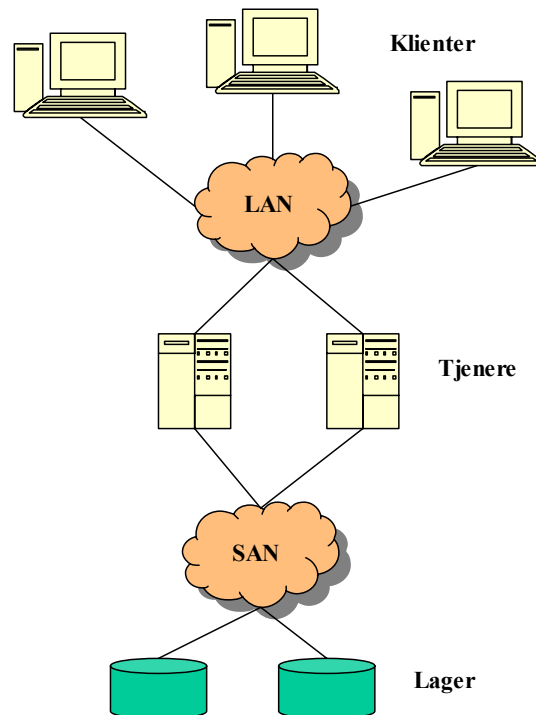
- Ikke mulig å dele data mellom applikasjoner
- Ikke like enkelt med sikkerhetskopiering og gjenoppretting
- Trenger flere operasjoner for å håndtere lagringen

DAS alternativet er fortsatt det enkleste for moderate behov, og vil på ingen måte forsvinne som lagringsmetode i nærmeste fremtid.

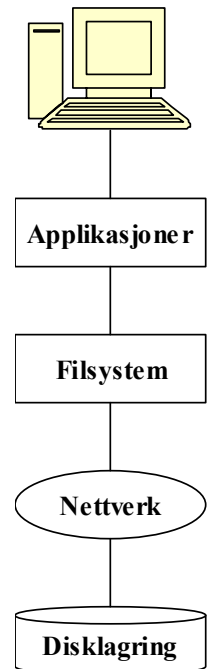
SAN

SAN (Storage Area Networks) ble utviklet tidlig på 1990-tallet som resultat av behovene for større fleksibilitet, pålitelighet og effektivitet knyttet til lagringssystemer. Et SAN er et eget dedikert nettverk for lagringsenhetene og prosessorene som aksesserer lagringsenhetene. Som for DAS utfører SAN "blokk-nivå" I/O fordi det håndterer spesielle blokker (sektorer) på spesifikke disker.

SAN ble utviklet først og fremst for store organisasjoner og sentraliserte omgivelser. Et SAN lagringssystem fjerner den fysiske en-til-en forbindelsen mellom tjenere og lager, noe som gir en rekke fordeler i forhold til kapasitetsutnyttelse, effektivitet, tilgjengelighet og skalerbarhet. FC (Fibre Channel) er det som har vært dominerende for sammenkoblingsteknologi for SAN. FC er kjent for høy effektiv hastighet, en etablert standard og høy robusthet og pålitelighet, og har med dette vært med å skape grunnlaget for at SAN har blitt en utbredt lagringsteknologi.



Figur 7: SAN lagringssystem



Figur 8: SAN arkitektur

SAN har normalt følgende egenskaper:

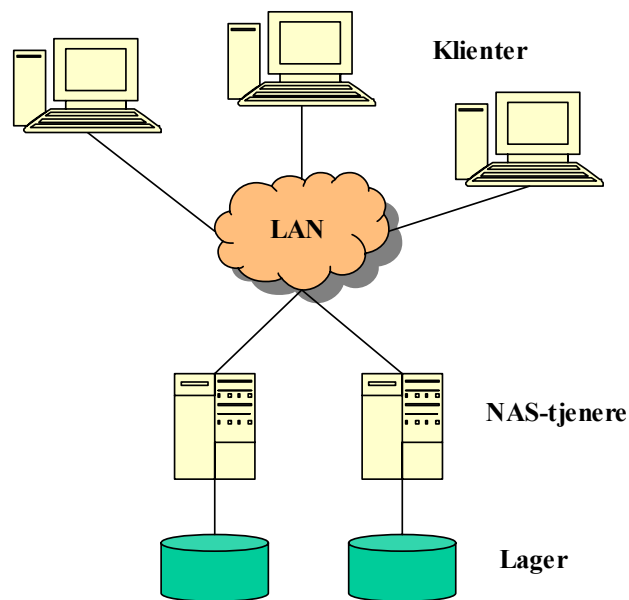
- Alle-til-alle konnektivitet, det vil si at alle tjenere får tilgang til alle lagringsressursene direkte
- Lagringsressursene kan konsolideres og optimaliseres, oppgraderinger og utvidelser kan foretas uten driftsforstyrrelser
- Kapasiteten kan økes raskt i takt med behovet
- Tjenere kan byttes, fjernes eller legges til med minimale driftsforstyrrelser
- Åpner for nye løsninger på gamle problemer: sikkerhetskopiering uten å gå via tjenere, virtuelle diskker av store proporsjoner osv.
- Egner seg for gjenoppretting fordi data relativt raskt kan bli speilet eller bli tatt sikkerhetskopi av til en alternativ lagringsplass
- Blokk-nivå I/O operasjoner gjør SAN bedre egnet enn NAS for databasemaskiner og store blokk I/O operasjoner

En ulempe med SAN er at det er laget for andre omgivelser enn det vi ser utviklingen av i dag: det er et økende behov for å kunne dele ressurser mellom grupper som ikke har noe med hverandre å gjøre, noe som fordrer fullstendig isolasjon med hensyn på aksess. På den andre siden øker kravene til sikkerhet over hele linja, og akkurat disse to utfordringene gir ikke SAN noe gode svar på per i dag.

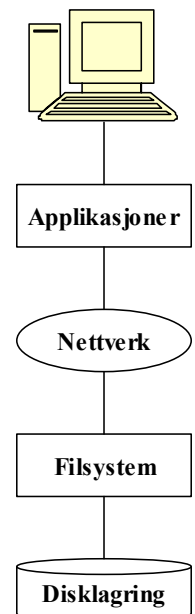
NAS

NAS (Network Attached Storage) blir ofte betraktet som det samme som SAN, men likhetene strekker seg egentlig bare til at begge er nettverksbaserte lagringsalternativer. Et NAS er en enhet som befinner seg på et nettverk som kan bli delt med ikke-lagrings trafikk. Dette nettverket er i dag som regel Ethernet, men kan i utgangspunktet være et hvilket som helst nettverk som støtter IP-baserte protokoller som NAS bruker. NAS er i motsetning til SAN ikke et egen nettverk, men kan kobles direkte mot det eksisterende IP nettverket som normalt finnes (LAN).

NAS oppsto som en videreutvikling av Unix-baserte filtjenere som fikk relativt stor utbredelse på slutten av 1980-tallet. NAS-tjenere er spesialiserte filtjenere som betjener klientene direkte og som selv har ansvaret for autentisering, låsing og så videre.



Figur 9: NAS lagringssystem



Figur 10: NAS arkitektur

Den store fordelen med NAS er at fordi den bruker det eksisterende IP nettverket, kan brukere av dette nettverket dele på filer som er lagret i NAS systemet. Dette kan en se av figuren over.

Som tilfellet var for SAN ser vi også at NAS ikke helt er tilpasset de behovene som har vokst frem gjennom det siste tiåret:

- NAS mangler SAN sine muligheter for å konsolidere den fysiske lagringskapasiteten på tvers av brukerplattformer
- Fordi NAS implementerer filsystemer blir responstiden høyere enn de typisk er for SAN. Responstiden tilbake til brukeren treng-

er nødvendig ikke å bli noe høyere, men dette avhenger av anvendelsen og arkitekturen.

- Løsningene dekker ikke situasjoner der separate miljøer skal konsolideres, dette fordi sikkerhetsmekanismer mangler
- Behandlingen av filsystemer er krevende, både teknisk og ressursmessig. Dette gjelder spesielt når flere filsystemtyper skal overlappes.

SSP

SSP (Storage Service Provider) er som navnet tilsier ikke noe ren lagringsteknologi på samme måten som DAS, SAN eller NAS. SSP er mer en samling tjenester som tilbyr ulike former for lagring med tilhørende tjenester.

Gjennom utviklingen fra DAS via SAN til NAS kan en se at en flytter grensesnittet bort fra selve lagringen med bits og bytes, og over til tjenester med høyere verdi. Dette samsvarer med andre trender i teknologimarkedet, og rene lagringsspesialister er på full fart inn i markedet. En kan også se i store prosjekter at lagringsdelen blir behandlet separat som en egen identifiserbar enhet. I denne sammenhengen blir derfor det neste naturlige steget å benytte seg av tredjeparter som spesielt tar seg av lagringen av data, og som kan utnytte det som en slik stordrifting vil kunne gi.

Som nevnt tidligere er SAN og NAS ikke tilpasset utviklingen som har skjedd de siste årene, så dagens teknologi egner seg ikke helt for slike tjenester som SSP tenkes å tilby. Det ideelle hadde vært å utnytte den høye ytelsen og stabiliteten til fiberkanaler sammen med mer fleksible og kostnadseffektive IP-baserte LAN/WAN. Dette har ført til at en har tatt til å bruke IP-baserte SAN og derfor har en sett konturene av to spesielt interessante IP-SAN baserte lagringsteknologier vokse frem:

- **iSCSI** - hvor en erstatter hele FC (Fibre Channel) med et IP basert nettverk
- **FC-IP** - hvor en allerede har et FC (Fibre Channel) basert SAN, men en fører SAN trafikk inn i det IP baserte nettverket for SAN-til-SAN kommunikasjon

Vurdering av iSCSI og FC-IP

Grunner for FC-IP fremfor iSCSI:

- FC (Fibre Channel) støtter høyere hastigheter (dette er i midlertidig i ferd med å endres, FC er i alle fall ikke klart raskere lenger)
- LAN trafikk kan involvere variabel forsinkelse, tap av pakker og overbelastning, noe som er uakseptabelt i et lagringssystem

- TCP og IP pakkeprosessering er ressurskrevende operasjoner som kan ta mye systemressurser

Det finnes eksisterende FC-IP løsninger, mens alternative iSCSI løsninger er relativt nye

Grunner for iSCSI fremfor FC-IP:

- Muligheter for å bruke et delt nettverk (LAN/WAN)
- Eksisterende IP svitsjer og nettverksrutere kan bli brukt uten at trengs endres
- Lagringssystemet kan kobles direkte til IP svitsjer
- iSCSI kan ha mange-til-mange forbindelser ved å utnytte mulighetene i rutere i IP nettverket

Vurderinger angående IP lagring

En vil sannsynligvis se at IP blir en sentral enhet for fremtidige lagringssystemer, men det er en del punkter en må vurdere før det tas i bruk. IP lagring har vært et "hot" tema i flere år og er en relativt ny og uferdig teknologi. Den siste tiden har leverandører/produsenter satset mye på IP lagring og en ser nå at IP lagring er i ferd med å slå gjennom og at løsninger kommer på markedet.

- **TCP offload** - fordi IP ikke kan garantere levering av data er det TCP som må sikre at data kommer riktig frem, dette gjelder både ved bruk av iSCSI og FC-IP. Dette kan føre til at TCP må gjøre en del ekstra arbeid for eksempel med å levere IP pakker i riktig rekkefølge til den høyereliggende protokollen (som vil være SCSI). Dette kan være en krevende prosess som kan ta en del CPU ressurser fra klientmaskinen og føre til forsinkelse for transaksjonen.

TCP Offload Engines

For å løse problemet med TCP Offload er det utviklet noe som heter TOE (TCP Offload Engines) som er spesialisert hardware som overtar protokollprosesseringen fra operativsystemet, eliminerer flaskehalser og forbedrer ytelsen vesentlig. Dette skal være med å gjøre IP lagring både sikrere og raskere.

- **Pris/ytelse** - selv om protokollen kjører på IP, er det godt mulig at en likevel må anskaffe hardware.
- **Sikkerhet** - ved IP baserte lagringssystemer hvor informasjonen blir fysisk tilgjengelig gjennom et standard IP-nettverk, blir sikkerheten et større problem enn ved SAN løsninger som ligger som egne "øyer" i datanettverket.

- **Samarbeid** (om systemet kan fungere sammen med andre) - selv om lagringssystemer bruker IP er det ikke automatikk i at det kan fungere mot andre systemer. Ulike leverandører eller andre systemer må kunne støtte de samme IP protokollene som lagringssystemet bruker, men IP er relativt utbredt så dette skulle gå greit i de fleste tilfeller.

Det intelligente lagringsnettverket

Gjennom utviklingen av SSP (Storage Service Provider) og integrering av IP-nett med SAN-nett, ser en kanskje konturene av hvordan lagringsløsninger vil være i fremtiden. Dette vil si et lagringsnett som er fullstendig teknologiavhengig og som en kan plassere der hvor det er mest optimalt, enten av økonomiske, sikkerhetsmessige eller andre årsaker. Det overordnede målet er at når som helst og hvor som helst kan brukere koble seg opp mot lagringssystemet og få tak i hvilken som helst type informasjon.

En slik intelligent lagringstjeneste vil kunne:

- Redusere kostnader
 - Lavere investeringer
 - Bedre ressursutnyttelse
 - Lavere driftskostnader (arbeidskraft, tilpasninger, integrasjon)
- Redusere kompleksitet
- Omdisponere ressurspersoner til viktigere oppgaver

Å få til et godt lagringssystem krever mye planlegging og etablering av en lagringsstruktur med klare grenselinjer: her er lagringssystemet, her er tjenestene som kan benyttes, og her er kanalene og grensesnittet. Dette innebærer at intelligensen i lagringssystemet flyttes fra endepunktene og til selve infrastrukturen. På denne måten kan en få teknologiavhengige lagringsnettverk.

Konvergens av NAS og SAN

En har sett at SAN og NAS er to ulike lagringsteknologier med hver sine fordeler og ulemper. En ser derfor at det skjer en konvergens av NAS og SAN for å utnytte alle de fordelene som de to systemene til sammen kan gi. Det er også mye som tyder på at iSCSI blir en del av den fremtidige utviklingen mellom NAS og SAN. Det er flere grunner til at en prøver å integrere SAN- og NAS-løsningene:

- **Skalerbarhet** - SAN med fiberkanaler (FC) gir en skalerbar arkitektur for nettverkslagring med høy ytelse. IP-baserte NAS har på den andre siden lang rekkevidde.

- **Lagringshåndtering** - en SAN arkitektur er i kontakt med lagringssystemet, sikkerhetskopianheter og servere, og tar med dette trafikk bort fra LAN.
- **Tilgjengelighet** - SAN sine høye tilgjengelighet kommer fra muligheter for "live" sikkerhetskopiering, gjenopprettingsfunksjoner og støtte fra redundante datastier og lagringssystemer. NAS har rask aksess til filer og høy tilgjengelighet gjennom bruk av etablerte nettverkstopologier. NAS har også funksjoner og replikasjon av data for å beskytte og sikre fillagring.
- **Serverkonsolidering** - i SAN løsninger er servere tilknyttet et datanettverk, noe som øker konnektiviteten til felles lagringstabeller (array) for en virksomhet.

NAS og SAN løsningene har altså hver sine fordeler som man ønsker å utnytte samtidig. En slik konvergert nettverksløsning mellom NAS og SAN vil blant annet kunne gi:

- Konsolidering av lagring
- Lagring med sentral databeskyttelse og administrasjon
- Deling av heterogen informasjon fra et enkelt databilde (data image)
- Muligheter for flere nivåer med tjenester for å oppnå kostnadsmål og ønsket nivå med tjenester
- Større lagringsutnyttelse i heterogene miljøer
- Kostnader for lagring blir spredd (UNIX og Windows servere kan utnytte fordeler av teknologi som har vært for kostbar frem til nå)
- Sentralisert og redusert håndtering

De fremste utfordringene med en integrering er at SAN må bli i stand til å operere over lengre avstander og med heterogen informasjonsdeling, mens NAS må bli i stand til å få sentralisert håndtering og den samme høye lagringsutnyttelsen som SAN har.

Trenden med å integrere SAN og NAS løsninger er relativt ny og lite etablerte løsninger finnes, og med få praktiske erfaringer av hvordan de egentlig fungerer. Der er i midlertidig stor sannsynlighet for at de to teknologiene vil smelte sammen. Dette ser en allerede konturene av, og vil nok skje i nær fremtid (trolig innen 2-4 år).

Anbefalinger

En del nyttige praktiske vurderinger i forbindelse med anskaffelse av nettverksbaserte lagringssystemer er:

- Effektiv hastighet er i mange tilfeller det samme som opplevd hastighet. Bruk av 2. eller 3. nivå hierarkisk lagring på magnet-

bånd eller CD-jukebokser skaper forsinkelser som brukerne alltid vil merke. Når klager kommer, er det med andre ord ikke alltid nettverket som er flaskehalsen.

- At defekte komponenter kan skiftes uten nedetid er kritisk for et moderne lagringssystem.
- Å etablere klare krav i henhold til aktuelle og forventede behov for sikkerhetskopiering, replisering og speiling er viktig for å kunne vurdere ulike produkter og tjenester i forhold til hverandre.
- SAN-teknologi er stort sett proprietær og kun unntaksvis samspillende mellom leverandører. Mix and match er derfor sjelden en mulighet.
- Kostbare, men effektive styringsverktøy er tilgjengelige fra de etablerte leverandørene i segmentet. Snakk med erfarne driftsmiljøer for å finne ut hva som er nødvendig og hva som er kjekt å ha. Pass på å sammenligne epler og epler, ikke minst med hensyn til behov: Erfaringer fra miljøer med helt andre karakteristika enn ens eget, kan være fullstendig misvisende.
- Redundans og pålitelighet er viktigere enn høy tetthet og lav kostnad per enhet.
- NAS er billigere, lettere tilgjengelig og lettere å administrere enn SAN, og skal vurderes når forholdene/behovene er av begrenset omfang.
- SAN-nettverk er aldri plug-and-play, slik vi er vant med på lokalnettsiden. Det tar tid å installere, konfigurere og få tingene på lufta. Det er en kostnad som må kalkuleres inn i ligningen.

Lagring i fremtiden

Det er kanskje spesielt to behov i forbindelse med lagring som vil bli viktige i fremtiden:

1. Større behov for lagringskapasitet
2. Større behov for skalering både i forhold til utvidelser og ytelse

Med disse to trendene vil det bli viktigere hvordan en greier å håndtere dataene som er lagret og i denne sammenhengen vil det bli viktigere å ha en sentralisert håndtering hvor en kan styre alle lagringsressursene som finnes i virksomheten.

Lagringssystemer for helsevesenet

Ved valg av lagringsløsning for en helsevirksomhet må en vurdere generelle problemstillinger som nevnt over for hva som passer best for den

enkelte helsevirksomhet. I tillegg må en vurdere punkter som er spesielt viktige for en helsevirksomhet:

- **Tilgjengelighet** - det kan være kritisk i en helsevirksomhet at informasjonen er tilgjengelig når det er behov for det. Dette betyr at for eksempel vedlikehold, utvidelser eller utskifting av utstyr ikke må føre til at lagringssystemet blir utilgjengelig.
- **Kapasitet** - det er viktig at lagringssystemet og tilhørende kommunikasjonskanaler kan håndtere store mengder data, for eksempel dersom det skjer en stor ulykke hvor en må ha tak i pasientjournalen til mange personer på en gang.
- **Hastighet** - det kan være kritisk at informasjonsuthenting fra et lagringssystem skjer raskt i en helsevirksomhet (og henger sammen med kapasiteten til lagringssystemet). Dette kan for eksempel være ved en akutsituasjon hvor en må vite hvilken blodtype en pasient har.
- **Fysisk uavhengighet** - det kan være behov for at ulike brukere har tilgang til lagringssystemet fra ulike fysiske steder (for eksempel en lege som rykker ut på hjemmebesøk som må ha tilgang til pasientjournalen).
- **Sikkerhet** - ved bruk av IP-baserte lagringsnettverk vil lagringssystemet være mer tilgjengelig enn for eksempel en SAN løsning som ligger som et eget nettverk for eksempel innad i et LAN til helsevirksomheten. Dette betyr at sikkerheten blir et viktigere tema for IP-baserte lagringsnettverk.

Generelt er det viktig å vurdere de kritiske IT-løsningene individuelt (EPJ, PAS, labsystemer) og vurdere de ulike behovene for tilgjengelighet, oppetid, gjenoppsettshastighet mm. for å komme fram til hvilke kriterier som er av størst betydning for det enkelte system.

Sikkerhetskopiering av data

Stabile og driftssikre lagringsløsninger bør ikke være en erstatning for gode rutiner og prosesser rundt sikkerhetskopiering. I dette kapitlet beskrives ulike metoder for sikkerhetskopiering av data og hva som er viktige punkter å vurdere i forbindelse med sikkerhetskopiering av data.

I en helsevirksomhet vil store mengder data måtte lagres, og da spesielt i forbindelse med elektroniske pasientjournaler (EPJ). Det er viktig at det er etablert sikre rutiner i forbindelse med lagring av pasientopplysninger fordi tap eller endring av slike data kan få katastrofale følger. I forbindelse med lagringsløsninger av informasjon bør en vurdere blant annet følgende punkter:

- Sikkerhetskopier og programvare bør lagres på et sikkert sted.
- Standardisere hardware, software og periferutstyr
- Dokumentere systemkonfigurasjon og utstyrinformasjon
- Koordinere med nettverkssikkerhetspolicy og systemsikkerhetskontroll

Årsaker til feil ved data:

Det finnes mange ulike årsaker til at det skjer feil ved data og her det listet opp de vanligste:

- Menneskelige feil
- Hardware- og softwarefeil
- Virus
- Strømsvikt
- Applikasjonsfeil

Andelen feilårsaker:

Årsakene til de ulike feilårsakene kan stort sett kategoriseres i tre hovedtyper:

1. Menneskelige feil 40%
2. Applikasjonsfeil 40%
3. Miljøfaktorer 20%

Sikkerhetskopiering (backup)

Lagring av informasjon i en helsevirksomhet vil kunne omfatte store mengder data (for eksempel elektroniske pasientjournaler). Dette er data som kan være kritisk at ikke går tapt, så det er viktig at en har løsninger som gjør at en har sikker lagring av informasjonen.

Sikkerhetskopiering av data er trolig den mest vanlige måten å sikre lagringen av data på. Dette er også trolig den beste måten å forsikre seg at dataene er forsvarlig lagret.

Det finnes tre hovedtyper av sikkerhetskopiering av data:

1. **Full backup** - inneholder alle filer på disker eller foldere som er valgt for sikkerhetskopiering. Dette kan være krevende fordi en tar full sikkerhetskopi av alle filer, og full sikkerhetskopiering av filer som ikke endres ofte (for eksempel systemfiler) kan være lite effektivt. Fordelen med denne metoden er at alle filer finnes inntakte siden siste fulle sikkerhetskopiering.
2. **Inkrementell backup** - inneholder filer som ble opprettet eller endret siden siste sikkerhetskopiering (uansett type). Dette er generelt raskere enn full sikkerhetskopiering, men kan kreve at data fra flere taper fra ulike sikkerhetskopieringer blir benyttet ved en gjenoppretting av et system.
3. **Differentiell backup** - inneholder filer som ble opprettet eller endret siden siste fulle sikkerhetskopiering. Dette er generelt raskere enn full sikkerhetskopiering og krever færre taper enn inkrementell sikkerhetskopiering. Bakdelen er at det kan gå lenger tid å utføre denne typen sikkerhetskopiering enn inkrementell fordi mengden av data øker etter hvert som tiden går siden siste fulle sikkerhetskopiering.

I tillegg finnes det to andre typer sikkerhetskopiering:

4. **Image backup** - er en fotografisk ”avlesing” av data, men uten hensyn til hvor filer er plassert. Dette gir en hurtigere sikkerhetskopi enn en full backup, men det tar lenger tid å gjenopprette enkelte filer.
5. **Inkrementell forever backup** - er en intelligent backup som krever en intelligent backup server og et tapebibliotek. Backup serveren holder selv styr på hvilke filer det er tatt backup av og når backupen ble gjort. Fordelen med denne metoden er at det rask både å ta backup og gjenopprette data etter en feil. Bakdelen er at det kan være store førstegangsinvesteringer med innføre denne metoden.

Det er vanlig, og også å anbefale, å kombinere flere av typene med sikkerhetskopiering. Den mest vanlige kombinasjonen er å benytte full backup for eksempel en gang i uken for så å kjøre inkrementell eller differentiell backup til daglig.

Fordeler med sikkerhetskopiering

Følgende fordeler kan oppnås ved at en virksomhet har gode rutiner for sikkerhetskopiering:

- **Reduserte kostnader** - brukere lagrer mer og mer data, og verdien av disse dataene bare øker. Å sikre seg mot tap av lagret data kan spare virksomheten for mye kostnader i forhold til om dataene skulle gå tapt og må gjenskaffes på annet vis enn fra sikkerhetskopier.
- **Høyere produktivitet** - med sikkerhetskopier kan en relativt raskt fortsette med arbeidet selv om en feil skulle oppstå. Ved fravær av sikkerhetskopier kan det timer eller dager/uker å gjenskape det en hadde før feilen inntraff.
- **Enkelt for sluttbrukere** - en virksomhet med rutiner for sikkerhetskopiering fratru sine ansatte mye arbeid som de eventuelt måtte bruke på å sikre sine data.
- **Mer sikkerhet i virksomheten** - flere og flere rutiner gjøres på datasystemer i dag. Ved å gjøre regelmessige sikkerhetskopier vil en dermed sikre mye av det arbeidet som gjøres i virksomheten.

Hva kan en miste

Følgende kan tenkes mistet dersom en virksomhet har manglende rutiner for sikkerhetskopiering:

- **Operativsystemer** - moderne operativsystemer har en rekke filer i ulike foldere som kan gå tapt. I tillegg kan det være drivere, kontrollpaneler eller andre systemrelaterte ressurser som kan gå tapt.
- **Applikasjoner** – re-installasjon fra disk, CDer eller Internett er stort sett mer tidkrevende og komplisert enn å gjenopprette applikasjonene.
- **Konfigurasjoner** - brukere kan ha lagret mange innstillinger eller konfigurasjoner for en rekke ulike applikasjoner. Går disse preferansene tapt kan det gå lang å stille de inn på nytt.
- **Nettverk** - et nettverk kan være oppsatt fra en rekke ulike bibliotek, kontrollpanel, datafiler og også applikasjoner. Dersom noen av disse går tapt eller blir endret kan det resultere i tap av deler eller hele nettverket.
- **Data** - en kan selvfølgelig miste data som en har lagret med et resultat at en må gjenopprette dem manuelt eller en må begynne å arbeide på nytt med det som ble tapt.

Aktuelle spørsmål

Her kommer aktuelle spørsmål som en bør vurdere i forhold til det å ha rutiner for sikkerhetskopiering.

Hvor ofte bør data sikkerhetskopieres?

Hvor ofte sikkerhetskopieringer bør skje har sammenheng med hvor ofte innholdet i objektet som skal sikkerhetskopieres endres. Dersom en fil endres hver dag bør sikkerhetskopiering skje minst en gang i døgnet, mens dersom en fil bare endres en gang i uken er det nok med sikkerhetskopiering en gang pr uke. For eksempel bør det tas sikkerhetskopi av siste dags endringer og full sikkerhetskopi for EPJ (elektronisk pasientjournal) systemer.

Hvor viktig innholdet i det som skal sikkerhetskopieres påvirker også frekvensen av sikkerhetskopieringer. En fil med kritisk innhold bør oftere sikkerhetskopieres enn en fil hvor innholdet ikke er så kritisk. Å utføre sikkerhetskopiering krever ressurser, så å prioritere for eksempel noen filer som viktigere enn andre kan gjøre at virksomheten får mer ressurser til å sikkerhetskopiere innholdet av det som virkelig er kritiske data.

Siden sikkerhetskopiering krever ressurser må det ses på hvor ofte det er hensiktsmessig å gjøre sikkerhetskopiering. En bør derfor finne en balanse slik at de ressursene som brukes på sikkerhetskopiering står i forhold til de tap som virksomheten får dersom data går tapt.

Når bør data sikkerhetskopieres?

Sikkerhetskopiering kan kreve ressurser både fra nettverk og de maskiner som utfører sikkerhetskopieringen slik at ytelse kan bli redusert når sikkerhetskopiering utføres. Sikkerhetskopieringen bør derfor, dersom det er mulig, legges til tidspunkter hvor det generelt er lite bruk av datasystemet. Dette vil typisk være om kveld/natt, eller i helgene.

Hvilket lagringsmedium bør brukes?

Hvilket lagringsmedium som bør benyttes avhenger først og fremst av volumet på sikkerhetskopieringen og med hvor stor hastighet sikkerhetskopieringen skal skje. Optiske disketter (for eksempel en CD-RW) er stort sett billige i innkjøp og drift, men har ikke stor lagringskapasitet eller hastighet. Magnetiske disketter har relativt stor kapasitet og hastighet, men er dyrere i drift en optiske disketter.

Hvor bør sikkerhetskopier oppbevares?

Sikkerhetskopiene bør lagres slik at det er minst mulig for at de kan bli skadet. Det er liten vits med en sikkerhetskopi dersom den ikke er mer sikker en det primære lagringssystemet. Det er tre forhold en bør vurdere med tanke på sikker oppbevaring av sikkerhetskopier:

1. Minst en sikkerhetskopi bør lagres på et annet sted enn hvor hoveddatasystemet befinner seg. Dersom hoveddatasystemet blir ødelagt av brann, flom eller andre skader vil da sikker-

hetskopien kunne være uskadet om den er lagret på et annet sted.

2. Kontroller aksess til sikkerhetskopiene slik at ikke uautoriserte får tilgang og kan gjøre skader på dem.
3. Sikkerhetskopiene bør lagres i et rent og støv-fritt miljø slik at ikke lagringsmediene for sikkerhetskopiene blir ødelagt.

Et forhold som må vurderes i forbindelse med sikkerhetskopier er hvor ofte sikkerhetskopiene tas ut og oppbevares på et annet geografisk sted. For EPJ systemer bør dette gjøres minimum en gang pr uke eller oftere.

Hvem vil utføre sikkerhetskopieringen?

I små virksomheter vil kanskje de ansatte selv måtte ta sikkerhetskopier, mens i de fleste større virksomheter er det sentrale rutiner for dette. Dersom det kreves at sikkerhetskopiering utføres ofte (for eksempel hvert døgn) kan prosedyrene automatiseres og styres fra sentralt holdt i virksomheten.

Hva skjer dersom data går tapt?

Virksomheten bør ha rutiner for hva som skjer dersom data går tapt og må gjenopprettes fra sikkerhetskopier. Rutinene bør beskrives i en plan som beskriver hvem som har ansvar for å gjøre hva. Rutinene bør også kjennes til av andre enn de som primært er ansvarlige for å utføre dem, i tilfelle de ikke er tilgjengelige når en feil i datasystemet skjer.

Hvor mange kopier bør en ha?

Flere kopier av sikkerhetskopiene øker sjansene for at data kan gjenopprettes etter en feil. For kritiske data bør en kanskje ha ”kopi av kopien” slik at dersom en sikkerhetskopi blir ødelagt så har en fortsatt en gyldig kopi av dataene.

Hvordan godkjenne sikkerhetskopiene?

En sikkerhetskopiering er en prosedyre som kan ende opp med feil i de dataene som ble kopiert. En bør derfor ha en eller annen funksjon slik at en kan godkjenne en sikkerhetskopi, slik at en vet at alle data har integritet i forhold til de originale dataene.

Et annet forhold er at dataene som skal sikres må være riktige. En kopi kan blir aldri bedre enn originalen, så tar en sikkerhetskopi av for eksempel konfigurasjonsinnstillinger som er feil så er sikkerhetskopien lite verdt.

Hvor lenge må sikkerhetskopiene bli lagret?

Et aktuelt spørsmål er hvor lenge en skal ta vare på dataene som en sikkerhetskopi har skapt. Dette avhenger i stor grad av hvilke type data det er snakk om. For noen typer data kan det være snakk om uker, mens for andre data kan det være snakk om måneder eller år som det er aktuelt å ta vare på sikkerhetskopiene.

Hvor lang tid tar det å gjenopprette siste sikkerhetskopi?

Hvor lang tid det tar å gjenopprette dataene etter en feil kan avhenge blant annet av datavolum, båndbredde eller lagringsmedium. Gjenopprettingstiden kan være kritisk under visse omstendigheter, slik at dette må vurderes ved valg av løsning for sikkerhetskopiering.

Kort sagt er det tre punkt som er viktige med sikkerhetskopiering:

1. Ha flere sikkerhetskopier
2. Sørg for at sikkerhetskopiene er riktige
3. Sikkerhetskopiene må lagres på et sikkert sted

Strategi for sikkerhetskopiering

En strategi for sikkerhetskopiering kan en grovt sett dele inn i fire ulike deler.

1. **Ta sikkerhetskopi** - dette innebærer selve sikkerhetskopieringen av dataene som skal sikres. Disse må så gjøres tilgjengelige slik at de kan brukes når det er behov for å gjenopprette data.
2. **Klargjør sikkerhetskopi for gjenoppretting** - dette innebærer å laste opp filer og transaksjonslogger slik at en gjenoppretting av de aktuelle filer kan skje. Her må en også sjekke at sikkerhetskopien har de riktige data slik at en eventuell gjenoppretting skaffer tilbake data med integritet i forhold til de filene som ble tapt.
3. **Gjenopprette data** - dette innebærer selve gjenopprettingen av de dataene er gått tapt.
4. **Testing av rutiner** - dette innebærer at en med jevne mellomrom tester om rutiner angående sikkerhetskopieringen fungerer. Her bør en simulere en feil og se om rutinene i de ulike trinnene i sikkerhetskopiprosessen fungerer tilstrekkelig og som tiltenkt.

I tillegg bør følgende gjøres i forbindelse med opprettelse av rutiner for sikkerhetskopiering:

- **Prosedyrer** - det bør utarbeides og dokumenteres prosedyrer som beskriver oppgavene til ansvarlig for sikkerhetskopieringen. Disse prosedyrene bør også omfatte beskrivelse av rensing av utstyret og når gamle medium skal tas ut av bruk.
- **Avtaler** - det bør etableres avtaler med leverandører eller lignende som kan støtte ved eventuelle problemer/feil ved sikkerhetskopieringen.
- **Loggbok** - det bør etableres en loggbok hvor ansvarlig for sikkerhetskopieringen kvitterer for det som er gjort i forbindelse med sikkerhetskopieringen. Loggboken bør for eksempel fortelle at

sikkerhetskopier er utført og verifisert korrekt, og at medium er skiftet ut.

- **Rutiner** - det bør etableres rutiner som beskriver hva som skjer for eksempel dersom ansvarlig person for sikkerhetskopieringen ikke er til stede eller det skjer en feil med sikkerhetskopieringen.

Testing av sikkerhetskopiering

En viktig del av arbeidet med å sikre seg mot tap av data er å teste de systemer en har lagring og sikkerhetskopiering. En ting er å ha planlagt og implementert planer/funksjoner/utstyr for å sikre data og systemer, men noe helt annet er hvordan de fungerer i praksis dersom en feil oppstår. ”*Jo da, vi har en backup løsning*” er det mange virksomheter som sier, men kanskje helt uten å vite hvordan det faktisk fungerer dersom det skjer en feil og en må bruke sikkerhetskopiene. Kan virksomheten gjenopprette alle dataene dersom en feil har skjedd? Dette og andre spørsmål er aktuelle for testing av backup løsninger:

- Fungerer backup løsningen som tiltenkt?
- Hvor gamle data greier en å gjenopprette og er dette tilstrekkelig?
- Hvor lang tid tar det å gjenopprette data etter en feil?
- Hva blir konsekvensene for brukere av en feil?
- Vet de riktige personer hvilket ansvar de har dersom en gitt feil oppstår?

Listen ovenfor viser aktuelle områder å ta for seg for i en eventuell test. Dersom det er mulig kan det være lurt å gjøre slike tester i liten skala og innenfor ”lukkede” områder av nettverket. For eksempel kan det å ta ut hovedserveren for å se om den sekundære serveren kobler inn få store konsekvenser dersom det ikke fungerer. Dersom det er mulig anbefales det derfor å teste dette ut i miljøer hvor konsekvensene ikke er fatale. Det kan være tøft å gjøre slike tester fordi å ta ut en server eller lignende kan virke som en rå og brutal metode for å teste backup systemene. Men det er gjennom slik testing en virkelig finner ut hva som skjer ved en feil i en viktig del av lagringssystemet.

Som en del av testingen bør en også verifisere at de data som blir gjenopprettet er riktige i forhold til de dataene som en tok kopi av.

Testing av rutinene for sikkerhetskopiering bør gjennomføres med jevne mellomrom, og da helst med en fullstendig sikkerhetskopi.

Case studies

For å sette driftssikkerhets spørsmål inn i en mer konkret kontekst har vi funnet det formålstjenlig å beskrive to konkrete case som viser hvordan virksomheter i Helse-Norge har forholdt seg til driftssikkerhets spørsmål i utviklingen av kritiske IT-systemer i sine organisasjoner. Først beskrives bruken av EPJ-systemet DIPS hos Aust-Agder Sentralsykehus, deretter innføringen av det første redundante helsenettet i Norge, MNH 100%.

Aust-Agder Sentralsykehus (ASA)

Generell beskrivelse

DIPS er et system hvor EPJ og PAS kan integreres. ASA tok i bruk DIPS januar 2000 til administrativ databehandling i somatikken. Høsten 2000 ble legenotater også inkludert i systemet. Alle nye papirdokumenter scannes og lagres elektronisk. Gamle papirjournaler ryddes etter mal fra "Norgesjournalen" og skilles etter viktighet i A- og B-journaler. A-journalene scannes til én bildefil pr hovedgruppe i Norgesjournalen.

Det scannes circa 700 journaler og opprettes 300 nye elektroniske journaler i måneden. Pr juli 2002 har 13.000 pasienter ved ASA journaler hvor hoveddelen er elektronisk, og 20.000-25.000 pasienter har journaler hvor deler er elektronisk. Målet til ASA er todelt: Å få effektive og sikre rutiner knyttet til forvaltning av journaler og tømme store deler av papirarkivet for å redusere arealbehovet arkiv med papirjournaler. Det benyttes fremdeles mapper for papirdokumenter som oppstår under en pasients opphold ved sykehuset. Dokumentene scannes og papirversjonen makuleres etter utskrivning.

Videre utvikling av systemet ved ASA tar sikte på å minimalisere behovet for å scanne papirdokumenter. For å oppnå dette vil det være behov for å koble til medisinsk teknisk utstyr som i dag produserer resultater i form av papirutskrifter, film og lignende. For informasjon fra slikt utstyr ser ASA det som en utfordring å tilfredsstille Riksarkivarens forskrifter med hensyn på godkjente formater for langtidsarkivering i elektronisk form (jmf. NOARK-4). PACS vil bli innført i oktober 2002.

Sommeren 2002 ble det også satt i gang et prøveprosjekt med bruk av PDA'er til journalføring. PDA'ene har en terminalløsning som kan koble

seg opp mot sentralt journalsystem over trådløst nettverk. I testfasen benyttes PDA-ene i hovedsak til å føre journal under visitt for å minimalisere behovet for tid og arbeidsoppgaver før og etter visitten.

Systembeskrivelse

ASA benytter systemet DIPS for å håndtere både elektroniske pasientjournaler, røntgenadministrasjon og pasientadministrasjon (EPJ, RIS og PAS). Sykehusets ansatte har tilgang til deler av systemet etter behov.

Teknisk beskrivelse

Applikasjon: DIPS 2000

Database: Oracle Enterprise ed. 9i, ikke replikert.

Maskinvare: En standalone Intel tjener for database med reservemaskin som må kobles opp manuelt. I løpet av høsten 2002 vil denne være skiftet ut til fordel for to HP (HP/UX) tjenere med real application cluster.

Lager: HP SAN, raid-5, dubblering av nettverk til database, redundante nettkort, kontrollere og strømforsyning, uavhengige UPS'er på hver strømforsyning. SAN er koblet til HP sin supportavdeling som monitorerer driften av SAN fortløpende. Det er i dag cirka 200 Gb med journaldata i systemet, og mengden vokser med 1,3 Gb daglig.

Backup: Taperobot som tar daglig fullstendig kopi av database. Test av restore fra backup utføres, men ikke ved faste intervaller.

Kjøling: Har to kjøleanlegg, hvorav det ene er vannbasert og ikke i drift på grunn av risiko for lekkasje og vannskade på tjenermaskiner. Dette anses som en større risiko. Problematisk dersom hovedkjøler feiler.

Nettverk: Mellom datarom og sykehus er det 1 Gbit ringnettverk for redundans.

Internet: ASA har tilgang til Internet via separat nettverk. Det benyttes to redundante brannmurer. Ansatte har tilgang til epost. Ytterlige sikkerhetsløsninger er under utprøving (blant annet hinder mot utilsiktet utlevering av epost).

Vaktordning: IT-avdelingen har døgnkontinuerlig vakt.

Målsetting

Krav til tilgjengelighet og servicekvalitet til sluttbrukerne er ikke fastsatt ut i fra andre kriterier enn at feil eller driftstans ikke skal gå ut over liv og helse. I praksis har målsettingen vært at det ikke skal forekomme stans på systemet på dagtid. Dagtid er definert som tidsrommet 0700-2100. Småstans for vedlikehold begrenses til 10 minutter. Andre krav til funksjon og design som er relevant for driftsikkerheten har i mindre grad blitt formulert skriftlig, men har blitt vurdert løpende. Vurderingene og valgene har blitt foretatt i henhold til utført risikoanalyse. Generelt har IT-

avdelingens avveininger vært gjort på bakgrunn av signaler og samtaler med brukere og ledere ved sykehuset.

Strategier

For ASA har det vært fokusert på å bygge opp kompetanse i IT-avdelingen som dekker sykehusets primære behov. IT-avdelingen har derfor personell som kan håndtere Oracle database og det meste av maskinvare. Unntaket er for SAN-løsningen fra HP som i stor grad vedlikeholdes av HP og deres servicepersonell. SAN-løsningen er koblet til HP sin supportavdeling og overvåkes kontinuerlig. Fjerndrifting av løsninger har vært sett på som uaktuelt av sikkerhetsmessige, økonomiske og funksjonelle årsaker. Internt i IT-avdelingen tilstrebes det å utveksle informasjon mellom de ansatte for å redusere sårbarhet forbundet med at kun en person kjenner et delsystem og kan håndtere dette. Det er også et tett samarbeid med leverandører, men ingen begrenset med responstidavtaler utenom for DIPS og SAN-løsning, i hovedsak fordi kostnadene er store og behovet har vært begrenset.

Ved innføringen av EPJ ble det lagt opp til en løsning med fail-over cluster for databasesystemet og DIPS frontend. Problemer med dette clusteret har ført til at det nå brukes en standalone server i en overgangsperiode til nytt cluster er på plass (se avsnitt om erfaringer). For kritiske systemer som hovedsvitsjer/routere og brannmurer er det full redundans i form av dublerede systemer. I og med at det benyttes VLAN, så rutes all trafikk gjennom et sentralt punkt, og redundans her blir nødvendig for å sikre oppetid i tilfelle en switch feiler.

Bruk av SAN gir stor fleksibilitet for lagring, og med nåværende løsning nås kapasitetsgrensen først ved 36 Tb. SAN'et er ikke dubleret ut over redundante kontrollere, nettkort og raid-5, og strømforsyninger. Redundansen i selve SAN-løsningen anses å gi tilstrekkelig sikring. Selve dataene er ikke replikert annet enn til backup. Det ses nå på en mulighet for å replikere deler av databasen for å dekke de viktigste data i tilfelle nedetid på databaseløsningen.

De foreligger ikke noen kriseplan for å håndtere de helt store krisesituasjonene i form av militære angrep, naturkatastrofer eller sabotasje. Replikering av de viktigste databaseelementer og fjernlager for backup kan sikre mot tap av data i mange av disse tilfellene, men for en større krisesituasjon er det sannsynlig at ved sykehuset vil bli lammet på en slik måte at nedetid på datasystemet på langt nær blir den viktigste trussel mot liv og helse til pasienter og ansatte. Det er ønskelig å få på plass rutiner og retningslinjer for hvordan personell skal opptre når datasystemet er ute av drift, men dette er foreløpig ikke en prioritert oppgave.

Erfaringer

I innføringsperioden for DIPS var det stor ustabilitet i Microsoft cluster. Dette førte til flere ikke planlagte stopp, og det ble besluttet å avvikle

clusteret til fordel for en standalone-løsning. Stabiliteten har etter det blitt vesentlig forbedret og oppetiden kumulativt for første halvår 2002 er målt til 99.98% innenfor dagtid (0900-2100). Fravær av cluster er midlertidig, og i løpet av høsten 2002 vil det være på plass et cluster på HP/UX-operativsystem bestående av to uavhengige maskiner.

Feil i programvare for tilgangskontroll (Microsoft Active Directory) førte til at brukere ble slettet på hovedserver. Dataene inkludert feilen ble replikert to andre servere for adgangskontroll. Restore fra backup ble foretatt. Feilen oppstod tidlig på natten og systemene var ikke tilgjengelige før kl. 11:00 neste formiddag. Noen brukere hadde problemer i en tid etter dette også.

En annen betydelig stans av DIPS 200 var i august 2001 under oppgradering av Oracle-database. Feilen den gang skyldtes feil i programvaren (Oracle) som leverandør ikke hadde opplyst ASA om.

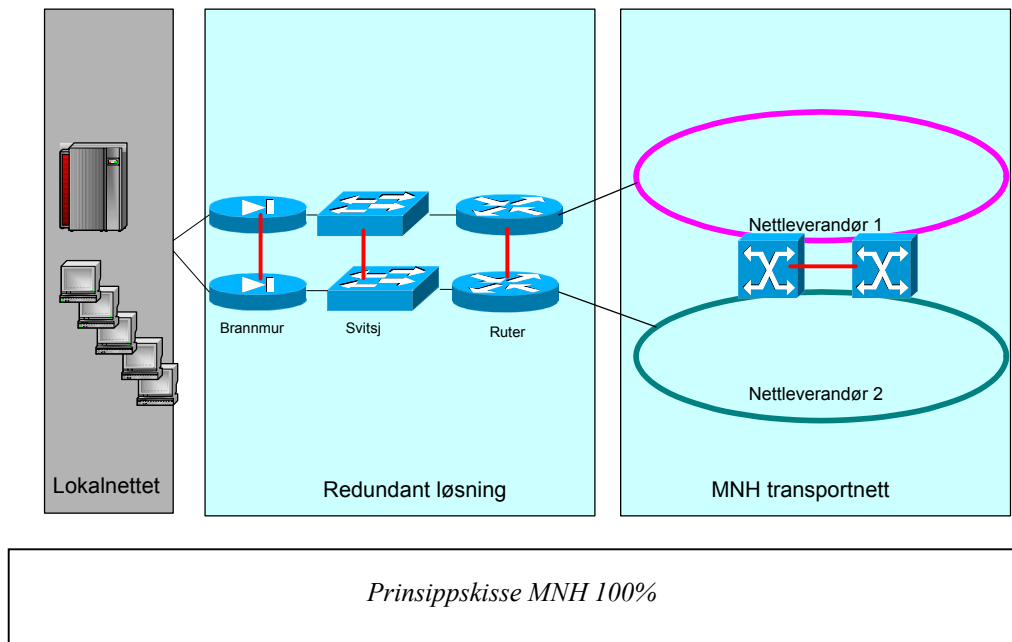
De største utfordringer ved innføring av EPJ og PAS har vært og er fremdeles knyttet til opplæring av personell på brukernivå. Overgangen har også stilt mye større krav til enhetlige rutiner og håndtering, spesielt rundt scanning av dokumenter. Nytilsatte får kursing, men mye av opplæringen foregår ved at ansatte hjelper hverandre. Store deler av innføringen har vært knyttet til organisasjonsutvikling og dokumentasjon av eksisterende rutiner. Ved IT-avdelingen er det avsatt betydelige ressurser for å følge opp rutiner og utnyttelse av IT-løsningen i avdelingene.

Midt-Norsk Helsenett

Innføringen av MNH-100%, Norges første redundante regionale helsenett.

Innledning

Prosjektet "100% MNH" var et delprosjekt i Midt-Norsk Helsenett med formål å oppnå tilnærmet 100% tilgjengelighet på nettverksinfrastrukturen i Midt-norsk helsenett. Prosjektet hadde sin hovedaktivitet i 2001 og resulterte i Norges første redundante regionale helsenett. Ved hjelp av uavhengige føringsveier, dublerne brannmurer, switcher og rutere er det skapt en infrastruktur med meget høy oppetid. På denne infrastrukturen kjøres det nå felles drift av systemer for pasientadministrasjon og laboratorievirksomhet og etter hvert felles drift av elektronisk pasientjournal for Midt-Norge.



Infrastrukturen baserer seg på leie av linjer fra to ulike nettleverandører som tilbyr uavhengige føringsveier til alle sykehusene i helsenettet, slik at linjebrydd hos en nettleverandør ikke skal kunne føre til brydd i kommunikasjonen. På hvert enkelt sykehus er det i tillegg utplassert dublerede brannmurer, svitsjer og rutere som har støtte for failover-funksjon seg i mellom. Dermed vil heller ikke feil i en av nodene medføre driftsavbrydd.

Målsetning

Målsetningen med 100% MNH har som navnet tilsier vært å tilby en infrastruktur for sykehusene i regionen som kan garantere tilnærmet 100 % oppetid. Regionen har som mål å kunne tilby sentral drift av tjenester som elektronisk pasientjournal og PACS og gjøre dette tilgjengelig for alle sykehus i regionen. Dette stiller høye krav til tilgjengelighet som gjenspeiles i en løsning hvor man har forsøkt å fjerne alle "single point of failure", punkter hvor feil vil føre til at tjenesten er utilgjengelig. Kravspesifikasjonen til MNH 100% hadde som et krav at ikke en enkelt feil på utstyr eller linjer skulle medføre at tjenesten ikke var tilgjengelig

Strategier

Redundans og failover-funksjoner har vært en nøkkelstrategi i utformingen av løsningen. 100% MNH er etablert som et redundant WAN basert på "hub & spoke"-arkitektur, hvor St. Olavs Hospital i Trondheim utgjør det sentrale navet. Fra før var det etablert en 155Mb kommunikasjonslinje mellom alle sykehusene. I tillegg ble det etablert en 34 Mb forbindelse levert av en annen leverandør.

Hvert av sykehusene er utstyrt med to rutere som er kraftige nok til å gi den ytelsen som er nødvendig for å kunne etablere lukkede nett bl.a. basert på aksess-lister. Ruterene er knyttet til hver sin svitsj som er koblet sammen for å la VLAN eksistere på begge svitsjene. I arkitekturen inngår det også et sett med redundante brannmurer som også støtter failover slik at den ene brannmuren tar over hvis den andre går ned. Brannmurene benytter såkalt "stateful failover" noe som gjør at sesjoner som allerede er aktive, ikke må etableres på nytt. Dette gjør at man unngår f.eks. ny oppstart av applikasjonen eller å miste siste data.

For å sikre at løsningen er skalerbar og også kan dekke regionens framtidige behov ble løsningen testet i lab med ytelser langt over dagens behov også når ressurskrevende tjenester som QoS, aksess-lister og Multicast video ble benyttet. Man har også valg utstyr som lar seg oppgradere, f.eks. med større prosesseringskapasitet og minne, noe som kan være aktuelt hvis nettverket skal inngå i en større sammenheng, f.eks. et nasjonalt helsenett.

Innføring av en såpass kompleks løsning stiller høye krav til koordinering og samkjøring av de enkelte aktørene som skal delta, det være seg leverandører, sykehus og andre. For å forberede overgangen ble det bl.a. utarbeidet en eget dokument som detaljert beskrev hvordan det enkelte sykehus skulle forberede innføringen av løsningen, bla. når leverandøren skulle ha tilgang til datarom, krav til datarommet, f.eks. hvilken størrelse utstyret som skulle installeres hadde, krav til strøm og kjøling samt rutine for feilmelding.

Erfaringer

Løsningen har ved flere anledninger vært effektiv i å opprettholde kommunikasjonen i situasjoner som ellers ville ha ført til brudd. Blant situasjoner som er opplevd er:

- Feil på kommunikasjonen fra/til et sykehus på den ene av de to linjene til helsenettet
- Feil på nettverkskort i en av brannmurene viste at failover-funksjonaliteten her fungerte som tiltenkt.
- Ved et sykehus ble strøm til både primær ruter og svitsj kuttet av elektriker. Løsningen sikret at dette knapt ble oppdaget annet enn via overvåkningssystemet
- Failover på brannmurer har i hovedsak skyldtes konfigurasjonsendringer / restart utført av IT-avdelingen
- Primær ruter på et sykehus sluttet å rute trafikk. Failover gjorde at sluttbruker ikke oppdaget situasjonen

En erfaring knyttet til den siste situasjonen var å la ruterene logge til lokalt buffer i tillegg til sentralt loggsystem, slik at logginformasjon ivaretas selv om ruterene ikke kan nå det sentrale systemet.