

IT-RAPPORT: Automatisert fjerndrift

i 'IT-RAPPORTEN' gir vi hver måned et innblikk i relevante IT-erfaringer fra et utvalgt norsk miljø. Vi tegner først et bilde av miljøet og interessante erfaringer de har gjort på områder som drift, teknologi, plattformer og kommunikasjon. Deretter presenterer vi en oppsummering av almenlydige punkter som lett kan anvendes i andre sammenhenger. Vi har alle noe å lære hverandre og lære av hverandre. 'IT-RAPPORTEN' skal være en katalysator i denne prosessen.

Ensom og lønnsom nisje

Kan 200 distribuerte tjenermaskiner driftes av to personer? 'Javisst' sier Larvik-selskapet Bibliotek-Systemer, som samtidig hevder at grensen slett ikke er nådd. Det hele handler om planlegging, forenkling og sunn fornuft.

Norge er fullt av ukjente, små selskaper med nisjeløsninger for smale markedssegmenter. I mange tilfeller er løsningene både praktisk og teknisk av høy klasse, uansett sammenligningsgrunnlag. De bærer preg av å være utviklet av personer som vet hvor skoen trykker og hva som skal til for å effektivisere hverdagen for spesifikke brukergrupper. Når vi tar slike løsninger i øyesyn er det uunngåelig å bli slått av den store avstanden til generelle verktøy – for eksempel i kontorautomatjonskategorien – der en leverandør fokuserer mer på det de mener vil selge enn på det markedet har behov for.¹⁴

At løsningene er lite kjent utenfor sitt eget smale segment, passer leverandørene utmerket: De unngår mye av støyen som preger IT-markedet i sin alminnelighet, og kan fokusere på oppgavene i stedet for omgivelsene. Baksiden av denne medaljen er at kunnskapen og erfaringen de kontinuerlig samler inn, sjelden kommer andre til gode. I denne artikkelen – og i en rekke artikler fra ulike miljøer i månedene fremover, skal vi synliggjøre en del slike erfaringer, og gjøre dem anvendelige i en bredere sammenheng.

Bibliotek-Systemer er en glimrende representant for denne gruppen: Nisjeløsninger for norske biblioteker siden 1988, 15 ansatte, god lønnsomhet og stabil vekst gjennom mange år. Selskapet utvikler løsningene selv, og leverer nøkkelferdige systemer til kunder over hele landet – inklusive fjerndrift fra Larvik.

Mens selve løsningen i beste fall er av kuriøs interesse for oss som er utenfor segmentet, har driftsmodellen – hvordan selskapet fjerndrifter hundrevis av tjenere generell appell. Vi har besøkt selskapet ved flere anledninger – uten noen gang å finne spor av den hastige og stressede modus operandi vi vanligvis assosierer med 'driftssentraler' for hundretalls systemer. Sammenligningen med en annen driftsgruppe vi besøkte nylig, med ansvar for 20-30 interne tjenere og et hundretalls brukere, blir uvirkelig. Sistnevnte minnet mest om aksjebørsene i New York og Tokyo.

"Sammenligningen er kunstig", påpeker daglig leder Torkel Hasle. "Vi har et forholdsvis enkelt miljø med én enkelt hovedapplikasjon, ultrastabile systemer og forutsigbare brukere." Utsagnet impliserer at

¹⁴ Avstanden mellom behov og hva som selger er interessant i seg selv, og understreker at utfordringen ikke utelukkende skyldes kreative markedsførere på leverandørsiden, og at markedet må ta sin del av skylden for at situasjonen er som den er.

dette er en unormal situasjon – hvilket vi skal være de første til å underskrive. Samtidig er den ønskelig, og spørsmålet blir: “Hvordan kommer vi dit?”

Brukerne først

Og for å begynne med det siste – hvorfor er brukerne forutsigbare? Jo, fordi de har fått opplæring, de kjenner oppgavene og verktøyet, og opplever sjelden forandringer av vesentlig karakter.

Allerede her har vi et viktig element i oppskriften – som uten videre kan overføres til miljøer flest: *Driftsstabilitet er proporsjonal med brukernes innsikt i det de driver med og kunnskap om verktøyet de bruker.* Argumentasjonen blir som følger:

Alminnelige IT-brukere får generelt for lite opplæring, de har beskjeden innsikt i verktøyene som brukes, og sågar liten forståelse for oppgavene de er satt til å løse. Et godt eksempel er epost, som ikke engang IT-virksomheter bryr seg med å gi brukeropplæring på. Det burde ringe en klokke når nettopp epost-systemene er en vesentlig bidragsyter til ustabilitet, men evnen til å koble sammen årsak og virkning er ikke påtrengende. Når slike sammenhenger ikke fungerer for regulære IT-virksomheter, hvordan skal de kunne fungere for resten av markedet?

Sammenhengen mellom brukerkompetanse og stabilitet blir med andre ord:

- ✓ Brukere som kan sine verktøy og oppgaver er ‘snillere’ for systemene. De har lite behov for å eksperimentere, hvilket typisk skjer når brukere står fast. Vi unngår dermed den uforutsigbarhet som tilfeldig eksperimentering forårsaker.
- ✓ Belastningen på støtteapparatet blir beskjedent. [Støtteapparatet, dvs. *help desk* og driftsansvarlige blir altfor ofte misbrukt til å kompensere for manglende opplæring – en kostbar og ineffektiv bruk av ressurser.]

La systemene være i fred

‘Ultrastabile systemer’ var et annet element i Hasles observasjon. Slike systemer vil vi alle ha, men hvordan kommer vi til det forjettede land? Hva betyr uttrykket og hva er Larvik-bedriftens hemmelighet? Her dukker flere interessante observasjoner opp:

- ✓ ‘Ultrastabil’ betyr nettopp det. Det forekommer praktisk talt ikke at et system ‘går ned’ ukontrollert. Systemstopp kommer i tilknytning til planlagt vedlikehold – av programvare eller system.
- ✓ Oppdatering av applikasjonsprogramvare skjer automatisk – normalt utenfor arbeidstid, og forårsaker aldri nedetid. I nødstilfeller kan programvaren oppdateres mens systemet er i drift, og alt brukerne vil merke er dårlig respons i noen sekunder.

- ✓ Oppdatering av systemprogramvare skjer sjelden. Systemene er ikke sikkerhetsmessig utsatt. Kun nødvendige nettverks-tjenester er aktive, og systemene er beskyttet bak en brannmur. Dermed er det unødvendig å følge med på all verdens 'vulnerability reports'.
- ✓ Forebyggende vedlikehold består i rengjøring og test av utsatte komponenter og foretas årlig. Slike operasjoner er den normale årsaken til nedetid.
- ✓ Stabile systemer forblir stabile så lenge de får være i ro. Utvidelse av minne, diskkapasitet eller lignende er grunnlag for midlertidig ustabilitet – en erfaring som gjør at oppgraderte systemer overvåkes ekstra tett en periode.

Gjennomgangstonen er proaktive tiltak som i sin tur sørger for den roen vi allerede har nevnt: Det er en beskjeden utfordring å slukke en sporadisk brann eller to. Å slukke 10 eller flere samtidig er det motsatte.

Automatisk overvåking

Grunnstammen i den proaktive tankegangen er godt innarbeidede prosedyrer for automatisk systemovervåking. Alle systemer med driftsavtale er satt opp med rutiner som minst én gang per døgn sender en omfattende, ferdig formatert (HTML) statusrapport til en sentral maskin i Larvik. Her havner informasjonen i et nettleserbasert overvåkingssystem der de ansvarlige i flere nivåer kan inspisere status på de ulike systemene. Avvik fra det normale flagges umiddelbart, både via eksplisitte prosedyrer og ved at varsellamper blir røde eller gule i overvåkingssystemet.

Hele systemet er skreddersydd – av de samme programmererne som har laget selskapets hovedprodukt, og har utviklet seg i parallell med dette. Igjen har enkelhet vært en hovedmålsetting, sammen med utstrakt bruk av eksisterende Open Source komponenter der det har vært mulig.

Blant aktivitetene som automatisk kontrolleres på denne måten er aktivitetslogger fra backupsystemet. Sikkerhetskopiering til *tape* skjer hver natt, med tilhørende manuelle prosedyrer hos kunden for å sirkulere kassetene. Loggfilene sjekkes blant annet for signaler om *tape*-slitasje og brukerfeil (gal kassett er satt inn).

Videre inneholder de daglige rapportene kopi av viktige konfigurasjonsfiler fra hvert enkelt system, som kontrolleres før de arkiveres. Dermed kan utilsiktede endringer raskt avsløres og korrigeres, og enda viktigere: I et katastrofe-tilfelle kan driftsansvarlige raskt konfigurere opp et nytt system med utgangspunkt i oppdaterte konfigurasjonsfiler. De samme konfigurasjonsfilene finnes naturligvis på kundens backup, men det tar for lang tid å hente dem frem når katastrofen er et faktum. På mindre enn 4 timer kan Bibliotek-Systemer ha en ny tjener klar til innlasting av kundens backup. Innen 24 timer er en tjener alltid tilbake i normal drift, uansett feiltype. Og interessant nok: En katastrofal feil er sjelden forårsaket av hardware eller pro-

Virtuelle tjenere uten grenser

Virtuelle tjenere er et aktuelt tema i tiden – med VMware som primær eksponent på produktsiden. I konsolideringens navn sentraliseres fysiske tjenere til færre maskiner, mens fordelene med å separere funksjoner til egne maskiner opprettholdes.

Slik virtualisering har fordeler og ulemper hvis størrelse og konsekvenser kan diskuteres. To klare ulemper er at hver virtuelle maskin krever relativt mye ressurser fra vertsmaskinen og at de i mange tilfeller (og avhjulpet av verktøy fra leverandøren) må administreres individuelt.

Ukjent for de fleste er at det finnes enkle virtualiseringshjelpemidler for Linux, som utnytter eksisterende funksjoner i systemet, og lager virtuelle forekomster innenfor det eksisterende operativsystem. En annen variant gjør det motsatte, og virtualiserer et nærmest vilkårlig antall Linux-systemer til én kraftig maskin – en virtuell klynge så og si.

Førstnevnte variant er implementert gjennom et program som kalles 'virtuald'. Ca. 150 kodelinjer og kreativ bruk av mekanismer som finnes i systemet gjør at virtualiseringen ikke konsumerer merkbare ressurser i seg selv. På en hardwaremessig velutrustet maskin blir det dermed mulig å kjøre store mengder slike virtuelle maskiner samtidig, gjerne flere hundre.

Bibliotek-Systemer benytter denne mekanismen til å betjene mange separate kunder på én og samme maskin. Oppsettet er ideelt for små enheter, typisk skolebiblioteker med 1-2 brukere, som det finnes mange av i de fleste kommuner, og som dermed enkelt kan betjenes via en sentral kommune-tjener. Ikke minst driftsmessig er løsningen optimal: I motsetning til hva tilfellet er for de fleste andre virtuelle løsninger, er det kun én maskin som skal driftes – uansett hvor mange virtuelle forekomster som måtte være i drift.

[Se Web-tjenesten for referansemateriale om dette konseptet.]

gramvare. Den hyppigst forekommende 'katastrofen' er tyveri – av hele maskinen – som typisk befinner seg på et offentlig bibliotek eller en skole.

Her har vi en ny nøkkelparameter for konseptet: *Testing og kontroll av rutiner og prosedyrer – ikke én gang, men regelmessig*. Hvor mange eksempler kjenner ikke de fleste av oss på beredskap som har sviktet når det gjelder – fordi testingen har vært for dårlig eller for gammel. Spesielt det siste er typisk. Selv i et stabilt miljø vil forandringer som påvirker driftsrutinene forekomme – for eksempel økt disk-kapasitet. Mer skal det ikke til før justeringer i et ellers velfungerende automatisk oppsett er påkrevet.

Sikkerhet

Som vi var inne på ovenfor, holdes tjenerne stabile i programvaremessig forstand fordi de er beskyttet innenfor en brannmur, og dermed ikke er eksponert for 'den store verden'. Likeledes er de sikret i seg selv, slik at den interne eksponeringen er minimal. Tankegangen preges av den samme enkelheten vi allerede har nevnt ved flere anledninger: Fjernt alt som ikke trengs, hold god kontroll med det som trengs. Dermed blir de daglige eller ukentlige 'vulnerability reports' mange av oss strir med, overflødige og uinteressante. I tillegg hjelper det naturligvis at Linux-systemet som benyttes, er relativt lite utsatt for slike svakheter.

All kommunikasjon mellom den enkelte tjener og den sentrale driftsgruppen går via en SSH-basert VPN-tunnel. Igen enkelhet satt i system, og sikring på et nivå som lett kan karakteriseres som tilstrekkelig for formålet. SSH-teknologien har vært i bruk i over 10 år, og er ikke feilfri, men langt enklere og mer effektiv enn de fleste av dagens VPN-teknologier, hvilket både reduserer eksponeringen for feil og øker den totale påliteligheten.

For å øke sikkerheten ytterligere arbeider Bibliotek-Systemer i disse dager med en automatisk, regelmessig sikkerhetsskanning av systemene (egentlig nettverkene) de har ansvaret for. Nessus, som verktøyet heter, har vi diskutert ved flere anledninger tidligere i Mellvik-Rapporten,¹⁵ og er anerkjent som det beste og mest

¹⁵ Se Mellvik-Rapporten nr. 75 og 77.

omfattende i sin kategori. Rapporter fra denne tjenesten vil bli inkorporert i det eksisterende driftssystemet.

Oppsummering

Bibliotek-Systemer har klart det mange organisasjoner drømmer om: Å komme på offensiven i forhold til driftsmessig problemløsning, og å rasjonalisere løpende driftskostnader til et minimum. Selskapets driftsgruppe på 4 personer estimerer at grovt regnet halvparten av tiden går med til regulære driftsoppgaver. 2 årsverk for drift av over 200 tjenere er sjelden kost i våre dager.

Vel er det riktig at alle miljøer har sine unikiteter og at metoder og mekanismer sjelden kan overføres direkte fra én til den neste. Her er det imidlertid verken metodene eller mekanismene som er viktigst, men tankegangen: Ved å tenke riktig – i forhold til foreliggende situasjon, erfaring, tilgjengelige verktøy og kompetanse, har Bibliotek-Systemer etablert en driftsmessig suksess. Hovedelementene i og erfaringene bak suksessen kan oppsummeres slik:

- ✓ *Driftsstabilitet er proporsjonal med brukernes innsikt i det de driver med og kunnskap om verktøyet de bruker.*
- ✓ *Stabilitet betyr å la systemer og programvare være i ro. Unngå unødige forandringer, oppdateringer, oppgraderinger. Kvalifiser trusler og påståtte svakheter, reduser sikkerhetsrisiko gjennom et effektivt 'kringvern' (se "Hypersikring: Kostbart og ineffektivt" i Mellvik-Rapporten nr. 102).*
- ✓ *Innsikt og kompetanse, som gir god forståelse for teknologi, arkitektur og systemer, er en forutsetning for å komme over i et proaktivt forhold til drift.*
- ✓ *Enkelhet er en ufeilbarlig ledetråd, men det er ikke alltid innlysende hvilket valg som er det optimale: Å skaffe et sofistikert verktøy som dekker over kompleksitetene, eller å forenkle oppgaven først og dernest tilpasse verktøyet til den forenklede virkeligheten. Mens sistnevnte i de fleste tilfeller er å foretrekke, vil tilgangen på egen kompetanse avgjøre hva som er praktisk mulig.*
- ✓ *Testing og kontroll av rutiner og prosedyrer – ikke én gang, men regelmessig – er nødvendig.*
- ✓ *Å sikre data er ikke nok, det er også nødvendig å optimalisere veien fra total katastrofe til operativ drift.*
- ✓ *Det vi ikke vet har vi vondt av: En driftsgruppe skal vite (for eksempel) at en disk har generert feilmeldinger, at en bruker har vært aktiv om natten, at en lagringsenhet nærmer seg kapasitetsgrensen, at en ny nettverkstjeneste har dukket opp på en tjener som ikke skal ha den, og så videre.*