HELSETJENESTENS DRIFTSORGANISASJON
Nødnett

10

Hendelsesrapport

fra

Helsetjenestens driftsorganisasjon for nødnett HF (HDO)

Vedrørende

SL1 – Nasjonalt utfall av et større antall operatørplasser.

Hendelsesdato:	**23.01.2025**
Rapport dato:	**10.02.2025**
Versjon:	1.05
Vedlegg:	1

Innholdsfortegnelse

Referansenummer	Kategori
INM054068	SL1

Feil registrert		Feil rettet	
Dato	**Tid**	**Dato**	**Tid**
23.01.2025	14.15	23.01.2025	18.30

Rotårsak

Fullstendig rotårsak er p.t. ikke etablert.

Arbeidsteorien for hendelsen er foreløpig at Splunk (system for innsamling av system- og sikkerhetslogger) agenter på operatørplasser (MWP'er) ikke takler å miste forbindelse til Splunk-indexer over en lengre periode. Når nettverksforbindelse gjenopprettes observeres det at maskiner går i 100% CPU, nettverksadapter slutter å respondere, og brukere blir kastet ut av brukergrensesnitt / PC Dispatcher.

Det er ikke avklart selve årsaken til at Splunk agentene oppfører seg slik og/eller om det foreligger manglende eller feilaktig konfigurasjon, variasjoner på software, bios, firmware, drivere eller lignende. Dette arbeidet pågår.

Konsekvens

I perioden kl.14.13 – kl.15.25 mistet 129 av totalt 513 operatørplasser (MWP | kontrollromsplasser) nettverksforbindelse, og ble automatisk logget ut av PC Dispatcher / brukergrensesnitt. Tallene inkluderer ikke kurs-, lab- og testplasser.

Feilen oppstod på kontrollromsplasser fordelt over hele Norge.

- Ingen nødanrop gikk tapt som følge av feilen.
- Ingen AMK-sentraler ble fullstendig rammet.
- Pågående samtaler for berørte kontrollromsplasser ble brutt, og automatisk satt tilbake i kø.
- Enkelte inkommende anrop ble rutet over til samarbeidende AMK-sentral eller reserveløsning.

AMK Oslo aktiverte nødprosedyre kl.15.30, og er bekreftet over på nødløsning kl.16.00. Nødløsning deaktiveres igjen kl.18.14 etter at alle operatørplasser igjen er på nett.

Hendelse (hvordan rotårsaken oppsto)
Den 23.01.2025 kl.07.41 utføres en konfigurasjonsendring i rutingen på en sentral brannmur hos HDO, nærmere bestemt i H3 og på VDOM-NHN. *(se vedlegg 1 – Prinsippskisse, Spunk trafikk)* Arbeidet var av rutinemessig karakter, og omfattet i utgangspunktet kun et test-kontrollrom (339). Arbeidet ble av den grunn ikke varslet eller Change-behandlet. Konfigurasjonsendringen skulle endre ruting mellom nevnte test-kontrollrom (339) og de sentrale systemene som ligger i CR507. Konfigurasjonsendringen inklderte opprettelse av en blackhole-rute. Blackhole-ruten var spesifikk nok til å trumfe alle eksisterende ruter til CR507, som førte til at all trafikk i VDOM-NHN med destinasjon til CR507 ble droppet (sendt til blackhole). Denne ruting-feilen førte blant annet til at Splunk-trafikken mellom alle operatørplasser (MWP'er) og Splunk Heavy Forwarder (HF) i CR507 stoppet. Dette skyldes at Splunk Heavy Forwarder (i CP1), som fungerer som en proxy, mistet kontakt med Splunk index-clusteret i HDO-domenet. Operatørplasser (MWP'er) på SDWAN mistet også kontakten med Heavy forwarder, i tillegg til andre servere tilknyttet CR507. Selve feilkonfigurasjonen påvirket ikke operatørplassens hovedfunksjonalitet, og dennes mulighet til å besvare samtaler. Det var når ruting-feilen ble rettet, og kommunikasjon mellom MWP'ene og Splunk Indexer (via Splunk HF) ble gjenopprettet, at operatørplassen krasjet.

Hendelsesforløp		
Tid	**Kilde**	**Hendelse/tiltak**
Dato: 23.01.2025:		
07.41	PT Datasenter	Feilkonfigurasjon i ruting på brannmur medfører stans i nettverkstrafikk mellom 507 og HDO, og påvirker blant annet trafikk mellom Splunk Forwarder og Splunk Indexer.
08.00	SD	Oslo LV mister flere plasser - trolig grunnet lokal nettverksfeil/endring. Vi ser at det ikke er mulig å få kontakt med disse maskinene fra forskjellige servere.
13.15	SD	Foruten Oslo LV er det ingen pågående feilsituasjoner. Alle kontrollromsmaskiner (MWP'er) er operative.
13.19	SD	SD mottar feilmelding fra 3 operatørplasser om at kontrollromsmaskin ikke kan koble/logge på domene. SD starter feilsøk sammen med PT Datasenter og PT Server og Arbeidsflate som er på Grand Hotell Gjøvik ifm et felles HDO arrangement.
14.13	PT Datasenter	Disabler blackhole-rute i brannmurkonfig. Kommunikasjonen mot 507 rutes igjen riktig. Dette gjenoppretter kommunikasjonen mellom splunk og indexxer (via proxy), samt klienter på SDWAN mot 507.
14.16	SD	Zabbix melder at mange operatørplasser/kontrollromsmaskiner både på CICCS og AMK uforventet går ned. Teamet som feilsøker får beskjed fra 1.linje om at det nå er flere plasser som går ned per kontrollrom, og at situasjonen er eskalerende. Glenn og Jan Thomas blir sendt opp til HDO for bistand til SD.
14.17	PT Datasenter	Blackhole-rute enables på nytt i et forsøk på å stabililsere situasjonen. Har ingen effekt.

14.21	PT Datasenter	Blackhole-rute disables igjen siden dette er den eneste riktige konfiguasjonen.
14.30	PT Datasenter	Det blir etablert et beredskapsteam med ansatte fra PT Datasenter, ServArb, Kontrollrom og SD, samt øvrige støttepersonell og ledelse. Teamet flytter inn til et egnet møterom.
14.40	SD	SL1 varsling sendes ut både internt og eksternt.
14.46	SD	AMK Innlandet og AMK Oslo bekrefter at de har blitt kastet ut på flere plasser.
15.00	SD	Beredskapsteamet finner symptomer på at en mulig feil på klokkesynkronisering i nettverket kan være er en potensiell årsak til påloggingsproblemer. Manuell omstart av kontrollromsmaskinen på operatørplass løser situasjonen, og SD informerer alle som melder feil at dette er metoden for å gjenopprette operatørplassen.
15.05	SD	ServiceDesk starter å kontakte samtlige AMK'er for å manuelt restarte alle kontrollromsmaskiner som opplevde feil.
15.10	SD	Ny løsning er å slå av og på nettverksporten på switch som kontrollrommaskin er tilkoblet.
15.15	SD	AMK Haugesund og AMK Finnmark melder om samme feil, og omstart av maskiner gjøres fortløpende.
15.20	SD	ServiceDesk informerer beredskapsteam om at pressen har ringt på 08915 og at adm.dir Lars Erik Tandsæther bør ta telefonen.
15.25	SD	Alle AMK-sentraler blitt kontaktet, og retteprosedyre iverksatt.
15.30 - 16.00	SD	Vi finner ut i etterkant at AMK Oslo har iverksatt nødprosedyre og gått over til reserveløsning med hjelp av Sykehuspartner
15.45	SD	Pressen ringer igjen til SD – henvises til adm.dir.
15.50	Emergency Handler	EH kontakter beredskapsvakta hos Helsedirektoratet og hos alle 4 RHF og informerer om den pågående og delvis uavklarte situasjonen.
15.59	Emergency Handler	EH kontakter beredskapsvakta hos Helsedirektoratet på nytt med ny informasjon om at situasjonen nå er under kontroll, og korrigerende tiltak rulles ut.
16.00	SD	MSI informerer HDO at media melder om problemer i Nødnett – dette er ikke riktig. Adm.dir. Lars Erik Tandsæther snakket med pressen og gitt korrekt informasjon vedrørende feil og konsekvens.
16.03	Emergency Handler	EH sender e-post til beredskapsvakta hos Helsedirektoratet, samt beredskapsvaktene hos RHFene, med oppdatert informasjon.
16.20	SD	Ekstra ressurs kalles inn til ServiceDesk for å være ekstra beredskapsbemanning ut kvelden.
18.00	SD	Det ser ut som at alle operatørplasser er OK utenom 4 stk. Disse LV/AM som gjenstår har blitt informert om at det må gjøres en manuell restart på disse for å få de i drift igjen.
18.10	PT Datasenter	Det etableres en arbeidsteori om at Splunk-agent utløser problemet etter først å ha mistet kontakt med Splunk-indexer (via proxy).
18.14	SD	Nødprosedyre hos AMK Oslo blir deaktivert og samtaler blir rutet tilbake til ICCS.
21.00	SD	Ekstra beredskapsbemanning på SD avsluttes – normal driftsituasjon og bemanning.
22.20	PT Datasenter	Etter nøye søk i nettverkslogger konkluderes det foreløpig med at Splunk-agenten forårsaker at nettverkskortet på klienten krasjer etter først å ha mistet kontakt med Splunk-indexer (via proxy). Det besluttes å teste ut teorien på 337 neste dag.
Dato: 24.01.2025:		
08.00	PT Datasenter	Etablerer test på 337. Diverse feilsøk og testing pågår ut dagen.
15.00	PT Datasenter	Mistanken mot Splunk-agent og krasj av lokelt nettverkskort styrkes etter flere tester og ytterligere søk I logger.

15.30	HDO	Vurdering av hvorvidt det er nødvendig å rulle ut en haste endring hvor Splunk-agent på MWP'er disables. Konkluderes med at dette medfører en større endring med påfølgende risiko enn det er å fortsatte as-is.
Dato: 27.01.2025:		
09.00	PT Datasenter	Test med 337 bekrefter teorien at Splunk-agent på MWP'er ser ut til å krasje klientens nettverkskort når den mister forbindelse til Splunk-indexer (via forwarder/proxy).

Hvordan ble feilen rettet
Feilen ble rettet ved å kjøre tilbake tidligere fungerende running-config på aktuell brannmur. Deretter måtte alle berørte operatørplasser (MWP'er) foreta en hard omstart. HDO Servicedesk kontaktet alle berørte kontrollrom via telefon, og forklarte løsning for å gjenopprette funksjonalitet på operatørplass.

Annen viktig informasjon

Betraktninger fra HDO ServiceDesk (SD):

- AMK Oslo aktiverer nødprosedyre og re-ruter telefoni til sin til reserveløsning uten å avklare med HDO ServiceDesk. Cirka tidspunkt for når dette skjer finner vi ut i etterkant (mellom 15.30-16.00), og på denne tiden har HDO allerede funnet en god løsning/fiks. Aktivering av nødprosedyre kunne vært avverget dersom partene hadde hatt bedre og tettere dialog/kommunikasjon underveis.

- HDO finner ut at det er omtrentlig 120 maskiner som går ned i et tidsrom mellom kl.14.15 – 14.30. Når HDO informerer kunder om at feilen kan løses ved manuell omstart så måtte kunde selv ta initiativ for å få sin maskin i gang igjen. Denne beskjeden blir videreformidlet så godt ServiceDesk (1.linje) kunne gjøre ved å si ifra til hver og en som ringte inn til oss, og gi beskjed til dem vi har vært i kontakt med tidligere på dagen. ServiceDesk brukte også overvåkningsverktøy for å finne ut hvilke maskiner som enda ikke var skrudd på, og ta kontakt med kontrollrom for å videreformidle informasjon. Kl.18.00 gjenstår det kun en håndfull med maskiner som enda ikke er påskrudd, disse kontrollrommene var informert, manglet bare initiativ fra kunde.

Fra HDO PT Datasenter:

- Samtlige 129 berørte MWP-er kjørte Splunk. Av 209 klienter uten Splunk ble ingen berørt. 175 klienter med Splunk ble heller ikke berørt.
- Av ca 10 sjekkede klienter, rapporteres det i samtlige splunk-logger om at tilkoblingen mot Splunk indexer er gjenopprettet 15-25 sekunder før den slutter å respondere på nettverkstrafikk.
- Feilen er reprodusert to ganger på 337 (MWP 5 og 6). Dette er gjort ved å blokkere all trafikk mot Splunk HF (heavy forwarder) i en lengre periode (flere dager) for så å åpne den igjen. Vi har også hatt aktive samtaler på MWP, men uvisst om det er relevant. Dette er har ført til at nettverkstrafikken på klienten dør ila ca 10 sekunder etter at trafikken er gjenåpnet. Det ble også observert at klienten begynner å sende gjentagende ARP-forespørsler etter default GW, men den får ikke svar. Vi har wireshark-capture fra den ene hendelsen (tatt fra MWP).

Læringspunkter
PT Datasenter: • PT Datasenter oppretter en felles logg for pågående infrastruktur endringer som ikke er Change-behandlet.

Tiltak - korte beskrivelser	Ansvarlig	Frist
Etablere rutine/automatikk som varsler ServiceDesk når endringer på Fortinet bokser gjøres. Med mål om bedre og raskere kunne oppdage sammenheng mellom utførte endringer og oppståtte feilsituasjoner.	PT Datasenter v/Thomas Norgaard	20/2-25
Få assistanse fra ekstern Splunk spesialist til å se på hendelsen + vurdere arkitektur på nytt.	Event v/Geir Henning Joten	20/2-25
Vurdere oppgradering til nyeste versjon av Splunk agenter, forwardere og indekser.	Event v/Geir Henning Joten ServArb v/Anders Johnsgaard	20/2-25
Melde sak til SPLUNK – be om assistanse til å lese og tolke logger.	Event v/Geir Henning Joten	20/2-25
Vurdere avinstallasjon av Splunk-agenter på alle MWP'er	ServArb v/Anders Johnsgaard	20/2-25
Etablere oversikt over samtlige MWP'er som feilet – hw, sw, bios, firmware, nettverkskort, revisjoner, splunk versjon etc. Sammenstille dette med klienter som IKKE feilet, og heretter dra noen konklusjoner vedrørende rotårsak og videre aksjoner.	ServArb v/Anders Johnsgaard	20/2-25
Intern gjennomgang og informasjon om roller, emergency management og krisehåndtering for å sikre gode prosesser ved tilsvarende situasjoner.	Kvalitet v/Ann Kristin Lundby Emergency Manager v/Anita Østlund	20/2-25

Vedlegg 1: Prinsippskisse, Splunk-trafikk