Helse Nord IKT

IKT infrastruktur i Helse Nord

Generelle krav for tilknytning til IKT infrastruktur i Helse Nord
Ver 0.8
24.01.2017

Innholdsfortegnelse

Innledning

Helse Nord består av 11 sykehus, over 100 utelokasjoner, og over 10,000 ansatte. For å best mulig utnytte regionens felles IKT ressurser er Helse Nord IKT (HN IKT) etablert som en felles IKT-driftsorganisasjon for hele regionen. All IKT-infrastruktur i regionen driftes og forvaltes av HN IKT, og etableres i et stordriftsregime utviklet for å mest mulig effektivt understøtte regionens kjernevirksomhet.

Dette medfører at leverandører av utstyr og systemer som har en IKT-komponent, eller som er avhengig av å virke i eller integreres mot, regionens IKT-infrastruktur må oppfylle en del generelle krav, samt levere en del standard dokumentasjon. Siden enkelte kategorier IKT-infrastruktur og IKT-utstyr skal leveres og driftes av HN IKT (e.g. nettverksutstyr, servere, og databaser) er det derfor kritisk at alle leverandører tydelig oppgir kompatibilitet med og behov for slike komponenter og tjenester, slik at et fullstendig og korrekt kostnadsbilde for tilbud løsning kan evalueres.

Der en tilbudt løsning forutsetter bruk av tjenester som ikke er tilgjengelig som standard, eller typer eller versjoner av standardiserte komponenter, vil dette medføre en øket kostnad for regionen som vil måtte tas med i evaluering av aktuelt tilbud. Enkelte krav er ufravikelige (f.eks. krav til oppdatert antivirusløsning, operativsystem på server og klient m.m.). System som ikke etterlever de mest sentrale kravene vil ikke kunne innføres i regionen.

Dokumentet tar kun for seg de mest allment anvendelige krav og en overordnet beskrivelse av regionens IKT-infrastruktur for å bistå prosjekter og leverandører med å tilpasse seg denne med minst mulig uforutsette hindringer. Der informasjon om et gitt emne ikke er tilgjengelig, eller er uklart, i dette dokumentet, må de nødvendige tiltakene for å innhente eller avklare nødvendige opplysninger påregnes.

Generelle krav for IKT infrastruktur

1 Sikkerhet og lovkrav

Helseforetakene i Helse Nord er underlagt krav til informasjonssikkerhet i en rekke lov- og forskrifter, Norm for informasjonssikkerhet i helse- og omsorgssektoren (Normen) og felles styringssystem for informasjonssikkerhet i Helse Nord. Normen er juridisk bindende for HN IKT og helseforetakene gjennom avtale med Norsk Helsenett SF. Virksomheter som følger Normen vil i utgangspunktet ivareta alle krav til informasjonssikkerhet som følger av lovverket. Felles styringssystem for informasjonssikkerhet beskriver blant annet Helse Nords felles sikkerhetspolicy, sikkerhetsmål og sikkerhetsstrategi. Den er førende for å ivareta sikkerhetskravene i regionen. Leverandører av utstyr og tjenester må til enhver tid være kjent med og etterleve alle Helse Nords krav til informasjonssikkerhet.

2 Fjerntilgang

All fjerntilgang til utstyr eller tjenester plassert i Helse Nords IKT-infrastruktur, og da særlig utstyr eller systemer som er pasientnære eller som er logisk plassert i et sykehus' sikrede sone, skal skje gjennom Helse Nords standard løsning for fjerntilgang. Denne løsningen består av en standard IPSec VPN klient (i "Remote Access" modus, ikke i "LAN to LAN" modus) som kobler opp til regionens VPN-mottak, samt en Citrix ICA-basert terminaltjenerklient som kobler opp til en dedikert terminaltjener for fjerntilgang. Fra VPN-klienten er det kun tilgang til nevnte terminaltjener og det er eksplisitt ikke tillatt med direkte IP forbindelse fra eksterne nettverk og til utstyr plassert i sikret sone. Både VPN og terminaltjener autentiseres med en personlig brukerkonto tildelt av HN IKT, og forutsetter undertegnet taushetserklæring.

Se for øvrig også Normen's "Veileder for fjernaksess".

3 Nettverk

Regionens nettverk driftes av HN IKT.

Lokalnettverk (LAN) er basert på Ethernet og IPv4. Eksisterende nettverkspunkter har varierende grensesnitthastighet fra 10 Mbps, 100 Mbps, og 1000 Mbps. Nye nettverkspunkter etableres som 10/100/1000Mbps. Alle nettverkspunkter termineres i standard RJ45 modulærkontakter. Power over Ethernet (PoE) basert på IEEE 802.3af-2003 er tilgjengelig som standard på alle nettverkspunkter. Utstyr som skal knyttes til LAN må kunne fungere i henhold til denne standarden. PoE basert på IEEE 802.3at-2009 ("PoE+") kan være tilgjengelig, mens nyere utstyr også vil støtte UPoE – begrenset tilgjengelighet inntil videre. Alle access-porter i LAN er satt opp med sikkerhetsfunksjonalitet som vil blokkere porten dersom ikke-tillatt trafikk eller oppførsel

detekteres. Dette inkluderer, men er ikke begrenset til, mottak av BPDU'er, uautoriserte DHCP pakker, tilsynelatende looper, eller uautoriserte nettverksenheter (e.g. switcher el.).

Regionens WAN er basert på det norske Helsenettet (se http://www.nhn.no/ for mer informasjon) og applikasjoner og tjenester må til enhver tid forholde seg til de kvalitets- og funksjonelle egenskaper som er gjeldende for dette. Dette gjelder særlig egenskaper som roundtrip delay ("Latency"), Jitter, og pakketap. Aksesshastighet for de fleste sykehus er 1Gbps redundant, men denne båndbredden er delt mellom alle applikasjoner og tjenester.

QoS er ikke tilgjengelig eller støttet i regionens nettverk.

Multicast er ikke støttet i regionens nettverk.

Bruk av broadcast, ut over det som er normalt og forventet for IP-baserte applikasjoner, er ikke støttet i regionens nettverk.

IPv6 er ikke støttet i regionens nettverk.

Tildeling av IP-adresser for annet utstyr enn servere levert av Seksjon for basistjenester skjer dynamisk gjennom DHCP, men en fast IP adresse kan tilbyes gjennom reservasjoner i DHCP. Servere settes opp med fast IP adresse og DNS innslag (både A og PTR RR).

IP adresser i bruk er hovedsakelig RFC1918 adresser, men utstyr og tjenester må fungere med en blanding av private og offentlige adresser. IP adresseplan er i henhold til Helsenettets nasjonale IP plan.

All kommunikasjon over WAN, inkludert mellom lokasjoner innen samme helseforetak, krypteres på nettverksnivå med bruk av GET VPN (IPSec i Transport mode). Dette medfører at MTU og MSS ikke kan forutsettes å ha noen spesiell defaultverdi, og at nettverket kan transparent endre MSS verdien i pakker som traverserer nettverket.

All trafikk som forlater en lokasjon tvinges gjennom et sentralt demarkasjonspunkt og underlegges trafikkontroll, som hovedregel i form av en brannmur med ACL og protokollinspeksjon. ACL'er bygges opp slik at trafikk per default blokkeres, og kun eksplisitte porter og destinasjoner tillates. Protokollinspeksjon gjør at pakker som ikke er i samsvar med relevant standard vil forkastes. Det er derfor kritisk viktig at alle kommunikasjonsprotokoller som er i bruk i en gitt tjeneste eller utstyr dokumenteres nøye, med spesiell oppmerksomhet til at dokumentasjonen skal benyttes for å utforme brannmurregler. En større range av dynamisk tildelte porter (e.g. diverse RPC-protokoller med en portmapper funksjon) tillates normalt ikke.

Direkte IP kommunikasjon ut over grensene for en juridisk enhet (i.e. et helseforetak) tillates ikke, og da spesielt ikke mot Internett eller andre eksterne nettverk. Direkte IP kommunikasjon mellom lokasjoner innenfor samme juridiske enhet (e.g. mellom sykehusene i samme Helseforetak) tillates etter Risikoanalyse dersom andre krav er oppfylt.

Applikasjoner som krever kommunikasjon mot internett må gjøre dette via felles HTTP/HTTPS-proxy (webproxy) med autentisering. HTTP CONNECT (tunnelering over proxy) gjøres kun over port TCP/80, TCP/443 eller TCP/22 om applikasjonen støtter proxyautentisering. HTTPS-trafikk som går via proxy vil være gjenstand for dekryptering/inspeksjon for malware/virussjekk.

4 Server

Maskinvare og operativsystem med tilhørende standard tjenester anskaffes, monteres, installeres, konfigureres, og driftes av HN IKT / Seksjon for basistjenester. Type og spesifikasjon av maskinvare er standardisert i regionen, og utstyr monteres i et av regionens datarom (herunder i noen tilfeller i sentraliserte datasenter geografisk fjernt fra det aktuelle sykehus).

Standard oppsett er virtuell server. Dersom en applikasjon eller et system har spesielle krav til maskinvare og derfor ikke kan benyttes på en virtuell server, så må dette dokumenteres. I slike tilfeller må egen godkjenning innhentes og økte driftskostnader vil påløpe.

4.1 VMWare

HN IKT benytter VMware vSphere som standard virtualiseringsplattform.
Maskinvare (server og tilhørende komponenter) som anskaffes må være godkjent på VMware's HCL-liste (Hardware Compability List) for siste versjon, pr. dags dato vSphere 5.5.

Systemer og applikasjoner som skal benyttes må støtte virtualisering og være supportert på siste versjon av vSphere.

4.2 Sertifiserte serveroperativsystem

Følgende serveroperativsystemer er sertifisert for bruk:

a. Microsoft Windows Server 2012 R2 (Datacenter)
b. ~~Microsoft Windows Server 2008 R2 (Standard, Enterprise og Datacenter)~~
c. Red Hat Enterprise Linux 6 og 7

4.3 Sertifiserte filsystem

Godkjente filsystem for både system og datalagring er NTFS for Windows Server samt ext4 og XFS for Red Hat Enterprise Linux. Rå tilgang til disk devices støttes ikke.

4.4 Generelle krav til serveroperativsystem

a. Sertifiserte versjoner av serveroperativsystem inkluderer alltid implisitt siste tilgjengelige servicepack eller vedlikeholdsoppdatering
b. Patcher og feilrettinger fra leverandør av serveroperativsystem (i.e. Microsoft, Red Hat) installeres fortløpende av HN IKT basert på operative driftshensyn. Patching vil som oftest kreve en omstart av server som utføres automatisk rundt kl 03:00 påfølgende døgn. HN IKT krever automatisk patching og avvik fra dette krever manuell patching hvilket tillates kun i unntaksfall.
c. Alle servere inngår i regionens Active Directory og underlegges felles Group Policy, herunder også sentralisert policystyring av Linux-servere
d. All tilgang til servere skjer ved hjelp av domene-konto (i.e. ingen lokale brukerkontoer)
e. Lokal brannmur på serveren må være slått på, med eksplisitte unntak kun for nødvendige porter brukt til management og applikasjoner og tjenester
f. Windows-servere må støtte å ha siste versjon av Internet Explorer og .Net Framework installert
g. Alle applikasjoner og tjenester må kunne kjøre uten at noen er pålogget konsollet; i.e. som en Windows Service
h. Dersom en service må kjøre i brukerkontekst skal denne kontoen ikke ha administrator rettigheter
i. Seksjon for basistjenester ivaretar sikkerhetskopiering (backup) i henhold til bestilling forutsatt nødvendig dokumentasjon (herunder forventet datavolum og endringsrate) og med regionens felles backupsystem (for tiden Symantec NetBackup)
j. Alle applikasjoner og tjenester bør kunne autentisere brukere mot regionens Active Directory
k. Applikasjoner må være environment variable aware. Som et minimum for alle Microsoft standard variabler.
l. Forventet behov for lagring og vekst i dette behovet må dokumenteres
m. Installasjon og lagring av alt som ikke er OS-spesifikt må skje mot andre volumer enn systemdisk
n. Eventuell kommunikasjon mot Internett (e.g. for henting av supplerende data) skal skje via Helse Nords web proxy løsning, inkludert autentisering med en Active Directory konto
o. Fjernstyring av server skal, der aktuelt, skje ved hjelp av RDP og autentisering skjer ved bruk av personlige kontoer i regionens Active Directory
p. Applikasjonen eller tjenesten må fungere selv om det er en antivirusløsning installert på serveren
q. Alle servere konfigureres med fast IP adresse. WINS og broadcast blir disablet
r. Lisensdongler må ha støtte for IP (f.eks. USB over IP) slik at de kan fungere i et virtuelt miljø.
s. VMWare Tools skal installeres på alle virtualiserte operativsystemer og alltid holdes oppdatert. På Red Hat Enterprise Linux 7 installeres Open VM Tools.

4.5 Generelle krav til webservere

- Systemet må benytte enten Microsoft Internet Information Services (IIS) for Windows Server (minimum 8.5) eller Apache webserver (minimum tomcat7)
- Systemrammeverk for websystem (MS .Net, PHP, Java osv.) må kunne oppdateres til nyeste versjoner.
- Tjenester må kunne kjøre under restriktive servicekontoer

4.6 Antivirus på servere

Alle servere må installeres med antivirus programvare i henhold til enhver tid gjeldende standard hos HN IKT.

5 Database

Databaseløsninger i regionen driftes av HN IKT i et standardisert stordriftsregime. Regionen har standardisert på tre godkjente databasemotorer og disse støttes i siste sertifiserte hovedversjon, men med mulighet for bruk av forrige hovedversjon i unntakstilfeller. Systemer som benytter databaser skal i hovedsak støtte bruk av en sentralisert databasemotor (i.e. ikke kreve bruk av en sk. "embedded" databasemotor); kunne sameksistere med andre applikasjoner på den samme databasetjeneren; og må støtte å kjøre mot en databaseklynge (cluster).

Masterpassord og administratorkontoer (e.g. sysadmin/administrator for MS SQL, sys/system for Oracle, etc.) gjøres normalt ikke tilgjengelig for leverandøren. Tilgang for vedlikehold eller feilsøking skjer ved hjelp av en dedikert brukerkonto for aktuell leverandør og system med de nødvendige tilganger (normalt kun lesetilgang, men utvidete rettigheter kan tildeles ved behov i særskilte tilfeller).

Sikkerhetskopi (backup) og programvareoppdateringer ivaretas av Seksjon for basistjenester i HN IKT.

5.1 Sertifiserte databasemotorer

Følgende databasemotorer er sertifiserte for bruk:

a. Microsoft SQL Server 2012 eller 2014 (2014 er foretrukket), kun Standard Edition eller Enterprise Edition. I løpet av første halvår 2017 vil MS SQL Server 2016 være sertifisert og foretrukket
b. Oracle 12c, kun Enterprise Edition
c. MySQL 5.6

5.2 Alternative databasemotorer

Følgende databasemotorer er sertifiserte men under utfasing, eller er av andre årsaker ikke en del av standard driftsplattform for nye installasjoner:

a. Microsoft SQL Server 2008 R2 (R1 er ikke støttet)
b. Oracle 11g

5.3 Utgåtte databasemotorer

Følgende databasemotorer er, eller blir, faset ut av standard driftsplattform og tillates følgelig ikke brukt i Helse Nord.

a. Microsoft SQL server 2005 eller eldre
b. Oracle 10g eller eldre
c. MySQL 5.5 eller eldre
d. Sybase

5.4 Generelle krav til databaser

a. Leverandør skal angi filsystem, operativsystem og databaseplattform som databasedelen av løsningen kan kjøre på
b. Angi oppgraderingsplan for databaseplattform som løsningen skal kjøre på
c. Databaseløsningen skal ha design basert på høy tilgjengelighet som inkluderer bruk av klyngeteknologi. Databaser som krever standalone servere er et unntak og vil medføre høyere kostnader til etablering og drift
d. Databaseløsninger som krever egne servere for den gitte applikasjonen, skal kunne være skalerbar
e. Databaseløsningen skal kunne installeres adskilt fra applikasjonsserverløsningen og andre applikasjonsspesifikke komponenter
f. Databasen skal håndtere skandinavisk og samiske tegnsett korrekt både ved registrering og søking
g. Databasen skal håndtere ulike typer spesialtegn (for eksempel α, β, γ, μ) korrekt både ved registrering og søking
h. Tilbudt løsning skal ved installasjoner og oppgraderinger ikke kreve tilgang via brukere eller rettigheter tilsvarende sa, sys eller system
i. Overvåkning og backup gjøres etter interne rutiner ved Seksjon for basistjenester i Helse Nord IKT
j. Seksjon for basistjenester ivaretar oppgradering av databasemotor og databaser i samråd med leverandør

6 Lagring

HN IKT har standardisert på lagringsløsninger fra EMC.

Ved alle sykehus benyttes det SAN løsninger (EMC CX4 eller EMC VNX) for blokk lagring (gjennom FC-FibreChannel). FC-switchene er levert av Cisco.

I datasentrene benyttes det NAS lagring (EMC Isilon) for ustrukturerte fildata. Protokollene som brukes her er SMB/CIFS og NFS. Løsningen har også støtte for HDFS (Hadoop Distributed File System). EMC VMAX benyttes for high-end blokk lagring.

Totalt har HN IKT ca. 4000TB data samlet i hele regionen.

7 Klienter

7.1 Krav til fysisk maskinvare

Tilbudt løsning skal kunne benyttes opp mot Helse Nords standard maskinvare.
Om et tilbydd produkt ikke kan benyttes på standard maskinvare må dette dokumenteres, egen godkjenning innhentes, og resulterende økte driftskostnader vil iberegnes totalkostnad for tilbudt løsning.

7.2 Krav til operativsystemer på klienter

Det vil enhver tid være flere klientoperativsystem drift i regionen. Det er et ufravikelig krav at «tilbydd produkt» skal kunne benyttes på minst et operativsystem med status: «Produksjon» eller «Under innføring». I tillegg skal tilbydere angi når støtte for operativsystem med status «Ide» kan forventes.

Operativsystem i Drift	**Status**	**Merknader**
Windows XP 32-Bit	Avviklet	Tillates ikke i Helse Nord
Windows 7 Pro 64-Bit	Produksjon	
Windows 10 Pro 64-Bit	Under planlegging	Må støttes av programvare leverandører

7.3 Oppsett av maskiner (tanking)

Tilbudt løsning skal kunne benyttes opp mot Helse Nord standard plattform oppsett.
Om et tilbydd produkt ikke kan benyttes på standard plattform må dette dokumenteres, egen godkjenning innhentes, og resulterende økte driftskostnader vil iberegnes totalkostnad for tilbudt løsning.

7.4 Regulære oppdateringer av klienter

Helse Nord følger anbefalt oppdateringsfrekvens for operativsystem og klientene blir oppdatert minst en gang i måneden. Det er et ufravikelig krav at tilbudt løsning fortsatt supporteres selv operativsystem og eventuell standard programvare oppdateres av Helse Nord.

7.5 Applikasjonsdistribusjon

Programvare distribueres per maskin eller per bruker ved hjelp av Helse Nords verktøy for applikasjonsdistribusjon. Det er et krav at tilbudt løsning som skal benyttes på >1 klient lar seg automatisere for installasjon. Det er ikke aktuelt å benytte egne løsninger for oppdatering eller installasjon av klientprogramvare.

7.6 Applikasjonsvirtualisering

Helse Nord benytter primært applikasjonsvirtualisering ved distribusjon av programvare. Alle applikasjoner som skal installeres på >1 klient bør dermed la seg virtualisere for distribusjon. Det vil være mulig å distribuere enhetsdrivere som MSI uten trekk i kvalitet.

Dersom en programvare ikke lar seg virtualisere må dette dokumenteres, egen godkjenning innhentes, og resulterende økte driftskostnader vil iberegnes totalkostnad for tilbudt løsning. Helse Nord forbeholder seg retten til å avvise tilbudt løsning som av installasjonstekniske årsaker er uegnet for distribusjon.

7.7 Avhengigheter og konflikter

Tilbudt løsning som er avhengig av annen programvare, biblioteker eller rammeverk må oppgi dette i tilbudet.

Dersom tilbudt løsning benytter avhengigheter (rammeverk, støtteprogrammer, biblioteker eller tilsvarende) som ikke er i Helse Nord standard oppsett må dette dokumenteres, egen godkjenning innhentes, og resulterende økte driftskostnader vil iberegnes totalkostnad for tilbudt løsning. Helse Nord forbeholder seg retten til å avvise tilbudt løsning hvor påkrevde avhengigheter av kompatibilitetsårsaker ikke lar seg sameksistere med Helse Nord standard driftsmiljø.

7.8 Administratortilgang

Tilbudt løsning skal kunne kjøres på klient uten at bruker av systemet har administrator privilegier.

7.9 Applikasjonslisensiering

Rapporter på forbruk av lisenser overvåkes daglig og rapporter genereres via våre lisensovervåkings systemer. Det er ikke anledning til å installere andre agenter for lisensovervåking.

I de tilfeller hvor tilbudt løsning må aktiveres mot internett eller intern lisenstjener må dette dokumenteres, egen godkjenning innhentes, og resulterende økte driftskostnader vil iberegnes totalkostnad for tilbudt system. Tilbudt løsning som krever aktivering via internett og som ikke støtter «helse nord proxy» vil avvises.

7.10 Antivirus

Alle klienter har installert Antivirusprogramvare med sentral styring og rapportering. Tilbudt løsning må ha støtte for gjeldene Antivirus programvare, kravet er ufravikelig.

Siste versjon av Symantec Endpoint Protection (SEP) er til enhver tid installert.

7.11 Verktøy oversikt

Funksjon	Produkt	Versjon	Merknad
Klienthåndtering	Altiris Client Management Suite	7.6	
Applikasjonsdistribusjon	Altiris Client Management Suite	7.6	Per maskin
Applikasjonsdistribusjon	Symantec Workspace Streaming	7.6	Per bruker
Lisensovervåking	Symantec Asset Management suite	7.6	Overvåker all programvare på HN Klientmaskiner.

7.12 Standard avhengigheter på alle klienter

Msxml	4.0sp2 & 6.0
Microsoft Silverlight	5.x (alltid nyeste)
Microsoft .NET	2 til 4
Vcred c++	2005 x86
Vcred c++	2005 x64
Vcred c++	2008 x86
Vcred c++	2008 x64
Vcred c++	2010 x86

8 Integrasjoner

Integrasjonstjenesten i regionen driftes av HN IKT. Tjenesten er todelt i en DINA-tjeneste og en Integrasjonsplattforms tjeneste.

8.1 Tjenester i tjenesteområdet DINA

- Applikasjonsserver
- Arena Applikasjonsserver
- Message Broker
- AR Connector
- SOLR Søkeservere
- DIPS Publisher
- DINA Dataguard
- Rapportserverløsning
- HL7 Connector
- Service Broker

Viser til DIPS ASA's teknisk dokumentasjon for tekniske krav for tjenesteområdet DINA.
Overvåking gjøres av driftspersonale i Samhandlingstjenesten i HN IKT. Oppgradering og test gjøres av Integrasjonstjenesten i samarbeid med EPJ-tjenesten i HN IKT.

8.2 Tjenesteområdet Integrasjonsplattform

Plattformen følger en integrasjonsstrategi som gir klare retningslinjer for integrasjonsstandarder og implementasjonsmønstre. Integrasjonsplattformens arkitektur vil fjerne bruken av punkt til punktintegrasjoner ved Integrasjonsprosjektet slutt. Plattformen består av BizTalk og web-tjenester. For hver integrasjonstjeneste som vil tilbys gjennom plattformen, vil det stilles spesifikke krav til hver enkelt applikasjon som knyttes opp. Disse kravene vil være endelige, men vil evalueres jevnlig.

Drift og overvåking av gjøres av Integrasjonstjenesten i HN IKT. Integrasjonstjenesten må involveres i testing og oppgradering av alle applikasjoner som har integrasjonstjenester tilknyttet Integrasjonsplattformen.

Egenskaper for Integrasjonsplattformen:

- God redundans i alle ledd, som sikrer et totalt system som har svært høy oppetid.
- Gode sikkerhetsmekanismer, som skal sikre integriteten og konfidensialiteten til informasjon som blir behandlet av Tjenestebuss, og som kan bli byttet ut når og hvis det blir avdekket problemer med eksisterende sikkerhetsregime.
- Veldefinerte roller og grensesnitt, som sikrer at nye tjenester kan legges inn i eksisterende regime på en god og enkel måte som opprettholder de reine linjene til Tjenestebuss.
- Enkel utskalering og oppskalering, for at produksjonsmiljøene skal kunne følge med i teknologiutviklingen og få tildelt tilstrekkelige ressurser på en så automatisk måte som mulig.
- Lastbalansering, som sikrer en god gjennomstrømning av meldinger i de forskjellige formatene som Tjenestebuss skal støtte.

- God mulighet for rapportering og logging, som sikrer at pålagt logging blir oppfylt samtidig som at en kan få produsert rapporter som viser eventuelle produksjonsproblemer med hensyn på flaskehalser, skadet eller uhensiktsmessig infrastruktur, og liknende.
- Sterk isolering på produksjons-Tjenestebuss i forhold til QA og test-Tjenestebuss, for å sikre at videreutvikling av Tjenestebuss i QA og test ikke kan påvirke den tjenestebussen som står i faktisk produksjon.

Integrasjonsplattformen består av tre miljø:

- Produksjonsmiljøet er den reelle Tjenestebussen, hvor meldinger fra reelle randsystemer og konsentratorer blir mottatt via lastbalanserere og behandlet i forhold til forretningslogikken definert for meldingstypen.
- QA er et nedskalert produksjonsmiljø. Nedskaleringen er ned til to noder for hver rolle, slik at en beholder muligheten for å kunne simulere svikt av maskinvare eller trafikkruting for å sjekke failover. QA må bruke uanonymisert testbase for å kunne simulere kompleksiteten til reelle produksjonsdata. Dette sikrer at nye tjenester og nye versjoner av tjenester blir testet i et miljø så nær faktisk produksjon som mulig.
- Test er et nedskalert produksjonsmiljø. Nedskaleringen er ned til to noder for hver rolle, slik at en beholder muligheten for å kunne simulere svikt av maskinvare eller trafikkruting for å sjekke failover. Test må bruke uanonymisert testbase for å kunne simulere kompleksiteten til reelle produksjonsdata. Dette sikrer at overgangen fra Test til QA og deretter produksjonssetting skal være så smertefri som mulig.
- QA og test deler klynge for lastbalansering mens produksjon har egen klynge på lastbalansering. Dette sikrer isolasjonen mellom QA og test fra faktisk produksjon, slik at uforutsette effekter av justering av konfigurasjon på lastbalansering i QA eller test ikke kan ta ned produksjonsmiljøet uansett hva justeringen i konfigurasjon medfører.

8.3 Integrasjoner mot AD

Kommer i en senere versjon

9 Samhandling

Kommer i en senere versjon

10 Kobling mot Metavision (Kurve)

Kommer i en senere versjon

11 Drifts- og overvåkingssenter

Kommer i en senere versjon