Bilag 3 Kundens tekniske plattform

xport

Tilpasningsavtale for
Ettellerannet

T Bilag 3
Kundens tekniske plattform

Innholdsfortegnelse

1 Innledning

Dette bilaget utgjør Kundens beskrivelse av den tekniske plattformen for leveransen. I dette bilaget er det ikke fremsatt krav.

2 Ordliste

NGK Neste Generasjon Kjernenett. Dette er nytt regionalt nettverk som blir levert av Norsk Helsenett.

NHNNorsk Helsenett SF

DS1	Regionalt datasenter1
DS2	Regionalt datasenter2

3 Dagens driftsmiljø

Helse Nord IKT forvalter, drifter og utvikler IKT-systemer for Helse Nord og regionens rundt 18000 brukere.

3.1 prosess

For å legge til rette for tverrgående ITIL-prosesser i Helse Nord IKT er det etablert et eget prosesstyret. Prosesstyret forvalter ITIL-prosessene med understøttende verktøy som er innført i organisasjonen.
For å håndtere og støtte opp arbeidsflyt for disse prosessene benyttes verktøyet HP Service Manager (HPSM). Verktøystøtten dekker per i dag ikke alle prosesser i prosesskartet.
I tillegg brukes det for Change Management i noen tilfeller en egenutviklet endringslogg gjeldende aktuell konfigurasjonsenhet.
Bestillinger (Request Management) håndteres i HPSM. Ved bestilling opprettes en egen change i HPSM for videre oppfølging. Disse sakene håndteres i dag primært manuelt.
For Access Management benyttes en egenutviklet løsning, BAS, for ressursprovisjonering og tilgangsstyring. BAS er integrert mot AD. I tillegg gjøres tilgangsstyring direkte i applikasjoner, der det er behov for det.
Service Asset & Configuration Management er etablert og man har automatisk fangst av Configuration items. Det arbeides med å få etablert innhold i en Configuration Management Database (CMDB) som vil støtte opp de andre ITIL-prosessene. For dokumentasjon og livssyklushåndtering av konfigurasjonsenheter (database, server, applikasjon, nett, linje, EDI, SAN) benyttes det primært egenutviklete løsninger.

3.2 Leverandørtilgang

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 (for databaser normalt kun lesetilgang, men utvidete rettigheter kan tildeles ved behov i særskilte tilfeller). Opprettelse av brukerkonto forutsetter at leverandøren har signert en databehandleravtale.

3.3 Drifts og overvåkingssenteret

Helse Nord IKT har et 24/7 drifts- og overvåkingssenter som benytter seg av Check_MK(Nagios) for å samle informasjon om konfigurasjonsenheten i CMDB.
Hendelser (events) som oppstår på forskjellige konfigurasjonsenheter fanges opp av overvåkningsverktøyet, som deretter blir manuelt registrert som incidents i HP Service Manager for videre håndtering.
Senteret overvåker i dag ca. 3000 enheter med rundt 75000 målepunkter.

4 Datasentre

Helse Nord sine datasenter skal sikre IKT-tjenester med høy sikkerhet, driftskvalitet og tilgjengelighet for å understøtte en slik strategi.
Det er opprettet to datasentre i regionen. Begge sentrene ligger i Tromsø og muliggjør en High Availability-løsning.
Lokale datasenter - på en del lokasjoner er det etablert lokale datasenter/datarom, men antallet skal reduseres i fremtiden. Lokale datasenter skal sikre minimumsfunksjonalitet på sykehuset i tilfelle feil på nettverk eller regionale datasenter. Hvilke funksjoner som skal etableres på de ulike sykehusene vil være avhengig av de ROS-analyser som gjøres for hvert enkelt sykehus.

5 Nettverk

5.1 Introduksjon til regionens nettverk

Helse Nord har stor geografisk spredning som dekker fylkene Finnmark, Troms og Nordland i tillegg til Svalbard. Stor geografisk spredning

medfører utfordringer med linjeføringer, tilgjengelighet og forsinkelser i nettverket.
Helse Nord har i overkant av 65000 nettverkspunkter på LAN som varier i båndbredde fra 10 megabit half duplex og oppover til 10 gigabit.
Helse Nord har i tillegg rundt 2800 trådløse nettverkspunkter, og vi antar at antallet vil øke en del.
Nettverk for spesialisthelsetjenesten i Helse Nord er knyttet sammen på regionalt og nasjonalt nivå med leveranser fra Norsk Helsenett (NHN).
Under finnes en oppsummering av nettverksstrukturen i regionen.
Regionalt nettverk:
Regionens klinikker og sykehus er koblet sammen i et regionalt nettverk (WAN) basert på en regional utbygging av Norsk Helsenett sitt nasjonale stamnett. Helse Nord sine elleve sykehus er koblet sammen i et regionalt nettverk levert på 10 Gbps samband. Antallet lokasjoner er rundt 100 og inkluderer alle klinikker i spesialisthelsetjenesten i Nord-Norge. Nettilkobling til disse er levert på en rekke forskjellige leveransetyper av regionens Internettleverandører.
Helse Nord IKT krypterer all trafikk over disse sambandene ved hjelp av GETVPN eller DMVPN.
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.

Lokalt nettverk

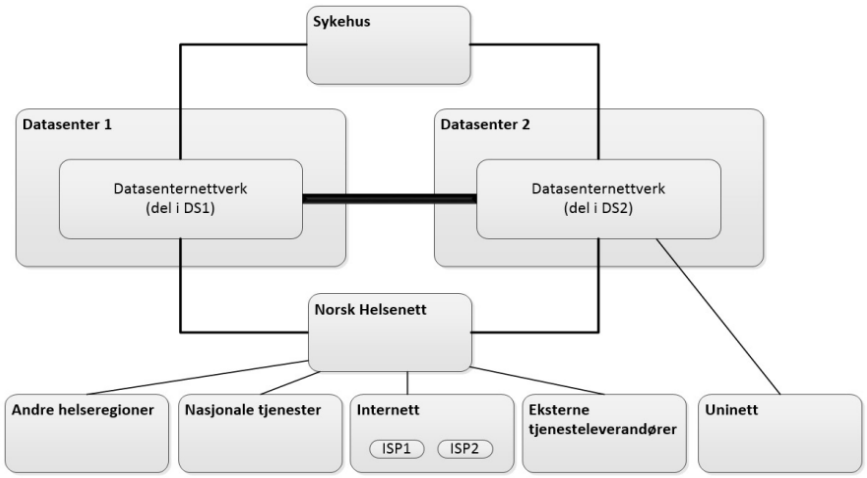
Lokale nettverk, som er nettverk inne på sykehusene, er bygget opp av switcher på flere nivå (LAN) i tillegg til trådløse aksesspunkt (WLAN), og basert på IPv4. Båndbredden på det kablede nettet varierer. IP-adresser i bruk er hovedsakelig RFC1918-adresser, men utstyr og tjenester må fungere med en blanding av private og offentlige adresser. IP-adresseplan er i henhold til Norsk Helsenetts nasjonale IP-plan.

Eksterne tilkoplinger

Tilkopling til eksterne nettverk gjøres gjennom datasenteret. Dette inkluderer:

- Tilgang til Internett via redundante tilkoblinger til internettleveranse fra NHN.
- Tilgang til NHN sine tjenester, samt regionale- og nasjonale tjenester, gjøres via én direkte tilkobling per datasenter til NHN sitt utstyr.
- Tilgang til eksterne tjenesteleverandører gjøres via NHN og én tilkobling per datasenter.
- Tilgang for forskningsenheter innenfor Helse Nord til Uninett gjøres via direkte tilkobling på Helse Nord IKT s rutere i datasenter. Sikkerhetsnivå på denne er lik internett.

I Figur 4 gis en oversikt over regionens nettverksstruktur.



Figur 4 Oversikt over regionens nettverksstruktur

5.2 Nettverksautentisering

Autentisering av brukere for drift av nettverksutstyr skjer ved hjelp av RADIUS, med mulighet for lokale brukerkontoer når RADIUS er utilgjengelig.

5.3 Lastbalansering

Helse Nord IKT benytter i dag F5 BIG-IP-enheter for lastbalansering av tjenester. Dette miljøet understøtter ulike produksjons-, QA- og testmiljøer.
F5 BIG-IP-miljøene har frem til nå i all hovedsak blitt implementert for å dekke ulike tekniske og funksjonelle behov:

- «Reverse Proxy»-funksjonalitet for internett-eksponerte tjenester (eks. for Microsoft ActiveSync eller Microsoft ADFS).
- Sømløs skalering av applikasjonsservere som støtter dette (Sectra, DIPS, Integrasjon/ESB og innsynstjenesten)

De forskjellige «gjestene» har provisjonert ulike F5-moduler ut ifra plassering og ytelsesbehov. Blant annet er enkelte gjester provisjonert med Lag7-brannmur (ASM) for sikring av bl.a. webtjenester.
All tilgang mellom klient og lastbalanserte tjenester mot de individuelle systemsonene gjøres ved hjelp av.
SNAT (Source Network Address Translation).
I tillegg har Helse Nord IKT to fysiske Citrix Netscaler appliancer som utelukkende er benyttet av Citrix-løsning.

5.4 Nettverkssoner

Soner er opprettet etter prinsippet om klassifiseringene Sikker sone, Intern sone, Åpen sone og Eksterne nett. Tilgang mellom disse må igjennom minst to tekniske barrierer. Typisk er brannmur et av disse.
Dette har gjort at tilnærmingen for nettverkstilgang til tjenestene har vært via virtuelle brannmurer på sentralt brannmur-cluster. Det er gjort samling av tjenester som er like av natur bak samme brannmur, f.eks. kliniske tjenester i produksjon. Mens det settes skille mellom enkelte soner selv om de har samme klassifisering. For eksempel vil det være brannmurer mellom kliniske tjenester og administrative tjenester selv om disse er definert til å være i Sikker sone.
En ny modell med soner/segmentering er under utarbeiding og er ventet ferdig ila. 2018.

6 Server

6.1 Eksisterende servermiljø

Helse Nord har en blanding av fysiske servere og virtuelle servere som kjører både som enkeltstående hoster og cluster. Som hypervisor kjører man VMware ESX. Helse Nord har i tillegg anskaffet et hyperkonvergert miljø, heretter omtalt som SKM (Sentralt KjøreMiljø), hvor man planlegger å migrere over tjenester i løpet av de neste årene.
Helse Nord opererer per i dag med rundt 3000 servere hvorav 2500 av disse er virtuelle. De fysiske serverne er en blanding av Dell og HP, med et par Sun-servere.

6.2 SKM

Helse Nord sitt sentrale kjøremiljø er en privat skytjeneste basert på VMware Validated Design for Software Defined Datacenter (VVD-SDDC 3.0), med hardware levert av HPE. Det er her Helse Nord skal kjøre mesteparten av serverne. SKM består av to tilgjengelighetssoner: DS1, og DS2. Nye tjenester som anskaffes forventes implementert her.
SKM kjører en full VMware stack med vSphere, vSan, og NSX.
Verktøy som brukes for å drifte de virtuelle komponentene av plattformen er vRealize operations manager, vRealize loginsight og vRealize network insight. Til hardware brukes HP ICM for nettverkskomponenter og HP oneview for fysiske servere.

6.3 Operativsystem

Som operativsystem på serverne benyttes hovedsakelig MS-Windows Enterprise server, og Red Hat Enterprise Linux. Det finnes et mindre antall av andre Linux-varianter som appliances og servere. Det finnes i tillegg noen få andre operativsystemer. Siste versjon av operativsystemet støttes.

7 Backup og arkivløsning

7.1 Backup

Helse nord bruker agentbasert backup for servere.

7.2 arkiv

I SKM benyttes Commvault som arkivløsning.

8 Andre tekniske tjenester

8.1 Katalogtjenester

Microsoft Active Directory (2016) benyttes som katalogtjeneste for brukere og tjenester samt som intern DNS og DHCP.
AD og DNS er satt opp som redundante tjenester på alle DC-noder. Hoveddomenet HN er en enkel forest hvor hver lokasjon er definert som en site. Det er replisering mellom sites er full-mesh.
DHCP er ikke redundant, og lokalt i hver enkelt site.
Alle ansatte og innleide må være definert som brukere og autentisere seg mot Active Directory for å få tilgang til tjenester og ressurser i Helse Nord IKT s nettverk.
Hvert helseforetak er lagt inn som en egen organisasjonsenhet (OU) hvor tilknyttede brukere og utstyr er plassert i underenheter (sub-OU).

8.2 Fjernaksess

Helse Nord IKT har en fjerntilgangsløsning basert på Citrix Xenapp
Tilgang eksternt, definert som utenfor Helsenettet, tilbys via Citrix Netscaler Gateway.
Sikker autentisering ivaretas med 2-faktor autentisering.

8.3 Databasetjenester

Databaseløsninger i regionen driftes av HN IKT i et standardisert stordriftsregime. Regionen har standardisert på tre databasemotorer (MSSQL, Oracle og MySQL) og disse støttes i siste sertifiserte hovedversjon, men med mulighet for bruk av forrige hovedversjon i unntakstilfeller.

8.4 Web tjenester

Helse Nord IKT tilbyr en standardisert, regional web-plattform for å hoste primært egenutviklede web-applikasjoner hos Helse Nord.
Man tilbyr webtjenester basert på IIS 10 og Apache Tomcat 7, med MSSQL og MySQL databaser. Som lastbalanserer/frontend benyttes F5 Big IP.
Alle servere tilknyttet løsningen kjøres virtuelt på SKM.

8.5 Fil- og Printtjeneste

8.5.1 Filtjenester

Filservere er i hovedsak virtuelle servere med lagring mot SAN/NAS.
Fillagring er basert på Windows OS SMB 1.1 og nyere.
Filtjenesten benyttes primært for felles- og hjemmeområder samt som programområde og for software-distribusjon. Helse Nord IKT har filservere på alle lokasjoner for å sikre rask responstid. Det benyttes DFS for noe data
Helse Nord IKT har pr. i dag ingen arkivløsning for filtjenesten.

8.5.2 Printtjeneste

Windows Print servere på alle lokasjoner. Det er ingen redundans for utskriftstjeneste. Printerobjektene er delt i Active Directory og printerne blir koblet opp automatisk via tilgangsstyring i AD. Alternativt brukerinitialisert oppkobling gjøres basert på særegne behov.
Helse Nord IKT har valgt Ysoft SafeQ som regional løsning for sikker utskrift.

8.6 Terminalservertjenester

Terminalservertjenesten er basert på Xenapp, og kjører på SKM. Serverene bruker Windows 2016 og applikasjonene er i hovedsak virtualisert med app-v.

8.7 Desktop infrastruktur

Helse Nord IKT har standardisert maskinvaren gjennom en nasjonal avtale for klientutstyr i regi av Helseforetakenes Innkjøpsservice AS (HINAS).

Helse Nord har rundt 16000 Stasjonære PCer hvorav det er management på 13000 av disse. I tillegg så har Helse Nord estimert rundt 3200 laptoper som per i dag ikke har noe management.
Maskinvaren er standardisert på følgende modeller: tre bærbare, en tablet, en desktop og en arbeidsstasjon. Tilbyderne på avtalen re-rangeres årlig, dermed kan man få et årlig modellskifte.
Klientene kjører per i hovedsak Windows 7 X64, men Windows 10 er planlagt innført i løpet av 2018. Komponenter som .Net og lignende kjøres alltid i siste versjon.
Klientene håndteres via Symantec Client Management Suite (CMS). Løsningen har en sentral infrastruktur og en desentralisert del på alle sykehus og større sentre.
Helse Nord IKT benytter Vpro som driftsverktøy og det er utført en stor mengde prosessautomatiseringer via Symantec Workflow.
Helse Nord benytter den antimalware som er på HINAS avtalen. Per i dag er det Symantec Endpoint Protection.
RealVnc benyttes til fjernstyring av klienter.

8.8 Integrasjonstjenesten

Integrasjonsplattformen i Helse Nord består i hovedsak av MS BizTalk og IIS. Den i brukes til å integrere fagsystemer med hverandre.
Integrasjonene benytter seg av standarder som HL7 v3, FHIR og KITH.XML.
Det er tre separate miljøer for Produksjon, Test og QA.

9 Støttetjenester

9.1 Service Desk

Helse Nord IKT har en regional servicedesk som single point of contact for Helse Nord.
Servicedesken er lokalisert i Tromsø og er bemannet kl. 08.00-15.30, i tillegg til en 24/7 driftsvakt. Ansatte er fordelt mellom generell brukerstøtte og spesialisert brukerstøtte på sykehusenes journalsystem (Dips).
ITIL er valgt som prosessrammeverk for håndtering av kundehenvendelser. HP Service Manager brukes som verktøy. Det mottas mellom 100 000-120 000 henvendelser til servicedesken pr. år.

9.2 Pakking og distribusjon av Software

På Windows 7 virtualiseres alle applikasjoner med Symantec Workspace Virtualization (XPF). Pakkene leveres så direkte til enhet med CMS eller strømmes til bruker med Symantec Workspace Streaming (SWS).
På Windows 10 og Citrix brukers Microsoft app-v som virtualiseringsteknologi.
I de få tilfeller hvor virtualisering ikke er mulig benyttes MSI eller annen scriptbasert installering.