Kundens Tekniske Plattform

Dokumentadministrator: Nils Martin Fredriksen	Gyldig fra: 17.03.2020	Revisjon: 1.0
Godkjent av: Frode Opsahl	Revisjonsfrist: 17.03.2021	ID: 2960

Hensikt og omfang

Dette dokumentet skal fungere som støtte til anskaffelser av IT-systemer for Helse Midt-Norge. Teksten under kan brukes som beskrivelse av Kundens Tekniske Plattform, på engelsk Customer Technical Plattform, i anbudsdokumenter.

Teksten beskriver hvilken eksisterende teknisk infrastruktur som Leverandøren vil møte. Formålet er at Leverandøren lettere skal kunne forholde seg til hva denne infrastrukturen gir av muligheter og begrensninger for Leverandørens besvarelse.

Ansvar

Eier: Avdelingsleder Basisdrift
Gjennomføring: Utformer av anbud

Arbeidsbeskrivelse

Kopier tekst og bilder under kapitlet «Kundens Tekniske Plattform» inn i anbudsdokumentene.

Alternativt kopier samme tekst og bilder fra vedlegget «Kundens Tekniske Plattform» i denne EQS-artikkelen.

Kundens Tekniske Plattform

Dette dokumentet beskriver IT infrastrukturen til Helse Midt-Norge. Det søker gi Leverandøren et innblikk i hva som finnes og hvilke tjenester Leverandøren må ta hensyn til og eventuelt kan støtte seg på.

3.1 Nettverk

Dette kapitlet beskriver oppbygningen av nettverkene som knytter sammen den tekniske infrastrukturen, nettverksprotokollene som er brukt og kontrollmekanismene som styrer trafikkflyten.

3.1.1 Wide Area Network (WAN)

WAN-et består av et stort antall leider linjer med høy kapasitet og redundans. Linjene leies fra forskjellige underleverandører. Nivået på kapasitet og redundans varierer mellom lokasjoner basert på størrelsen og rollen til lokasjonen.

En forbindelse til Norsk Helsenett gir sikker og høytytende meldingsutvekslingstjenester og internett. Nettverket er bygd opp av Cisco-rutere som tilbyr ruting av IP-basert trafikk mellom lokasjonene.

3.1.2 Norsk Helsenett (NHN)

Norsk Helsenett er eid av Helsedepartementet og leverer internettforbindelser og andre applikasjonstjenester til de tilkoblede organisasjonene i norsk helsevesen.

3.1.3 Lokalnettverket (LAN)

Lokalnettverket er bygd opp med høykapasitetslinjer (1 Gbps eller mer) der trafikken er rutet av en standardisert lagdelt arkitektur for kantsvitsjer, distribusjonssvitsjer og kjernenettverk.

Alle svitsjer i distribusjon og kant kommer fra Cisco sin Catalyst-serie.

3.1.4 Trådløst nettverk (WLAN)

Trådløst nettverk er tilgjengelig på alle lokasjoner som tilhører Helse Midt-Norge. Klargjorte klienter får automatisk tilgang til det uniforme og sikrede enterprise-klasse trådløsnettverket. Et trådløst gjestenettverk er også tilgjengelig.

Det trådløse nettverket er bygd opp av teknologi fra Cisco og er sentralt styrt gjennom høytilgjengelige "Wireless LAN Controllers" (WLC) som kontrollerer de distribuerte trådløse aksesspunktene. Styrte klienter må autentiseres gjennom IEEE 802.1X maskinautentisering for å få tilgang til det trådløse nettverket.

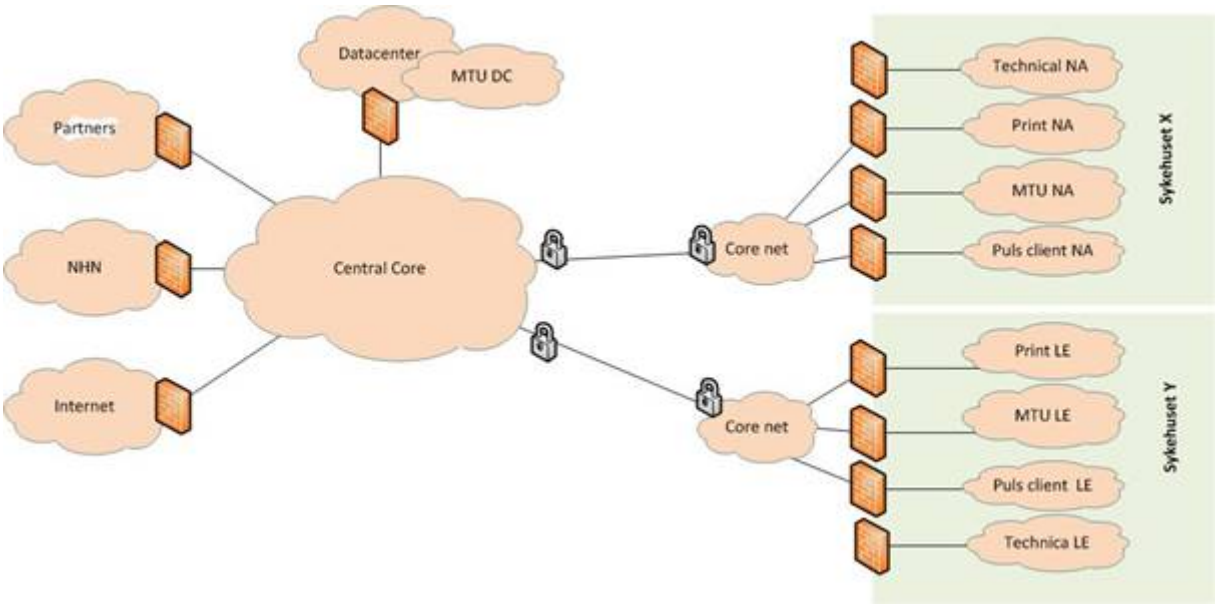
Aksesspunktene er fra Aironet-serien og WLC er av modell Cisco 8540.

3.1.5 Virtuelle nettverk (VLAN)

Det fysiske nettverket er partisjonert opp i logiske nettverkssoner ved hjelp av virtuelle nettverk (Virtual Local Area Network – VLAN). Partisjoneringen sikrer håndtering og transport av data av forskjellige informasjonsklasser på en funksjonell og sikkerhetsmessig trygg måte.

PCer autentiseres gjennom IEEE 802.1x og får tilgang til korrekte nettverkssoner.

Figur 1 under viser hvordan nettverket er partisjonert inn i forskjellige logiske nettverk ved hjelp av VLANs.



Figur 1 - Virtual LAN

3.1.6 Brannmurer

Brannmurer kontrollerer IP-trafikken og begrenser hvilke tjenester som får kommunisere på og hvilke trafikkprotokoller som kan brukes.

All nettverkstrafikk gjennom brannmurene, både tillatt og blokkert trafikk, blir logget.

Brannmurene som brukes er fra Cisco ASA-serie og fra Check Point.

3.1.7 Fjerntilgang

For ansatte i Helse Midt-Norge tilbys fjerntilgang direkte fra Puls-PCene ved hjelp av Microsoft Direct Access.

Hemit tilbys også fjerntilgang til en VDI-løsning. VDI-løsningen er bygd på VMware Horizon.

For leverandører og teknisk IT-personell tilbys en Citrix-basert terminalserverløsning.

3.1.8 Protokoller

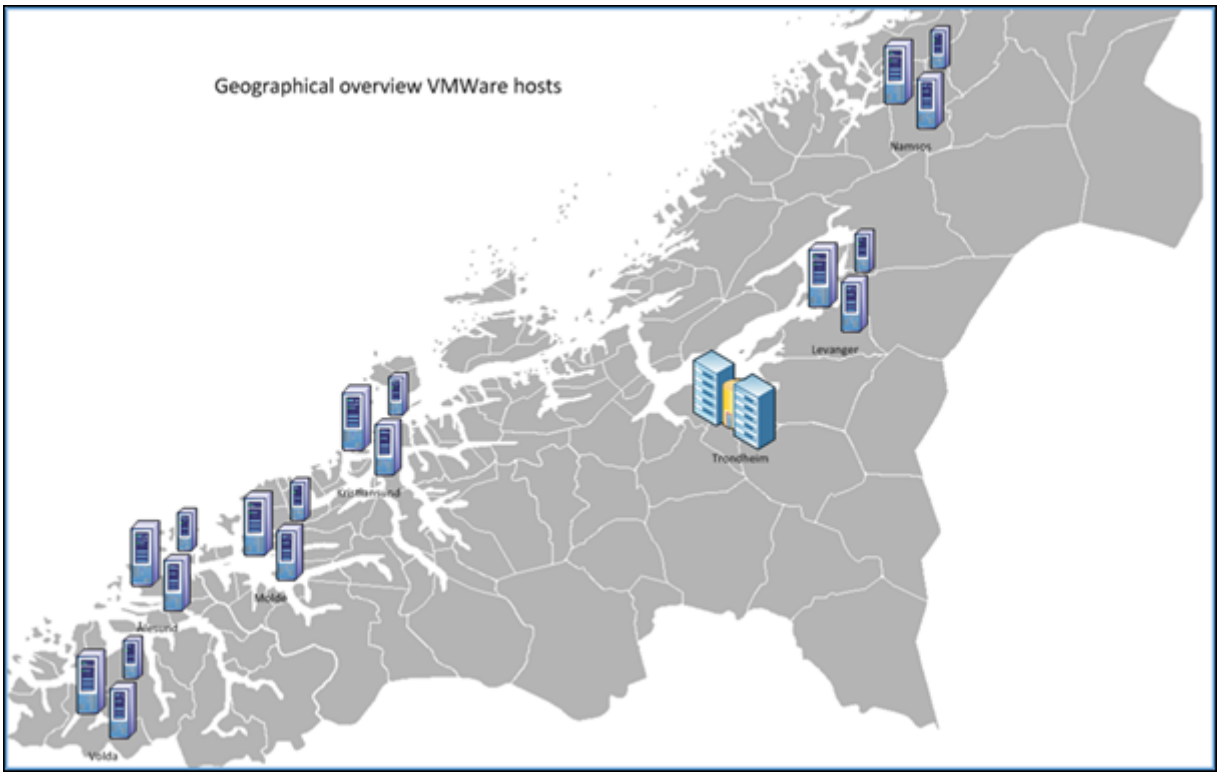
Nettverkene er bygd på kommunikasjonsprotokollene i IP versjon 4.

3.2 Servere

3.2.1 Virtuelle servere

Helse Midt-Norge har standardiser på virtualisert maskinvare. Virtualiseringsgraden av servere er over 95%. Windows- og Linux-servere kjører på VMware ESXi.

3.2.2 Virtualiseringsteknologi



Figur 1 Servervirtualisering

Produksjonsmiljøet for servere består av flere geografisk spredte VMware-farmer plassert på sykehusene. Til sammen består VMware-farmene av ca. 120 servere. Hovedvekten av VMware-serverne er plassert i datasenteret i Trondheim.

Det er i tillegg en VMware VDI-farm med ca. 40 servere for VDI'er. Se kapittel for klienter for mer informasjon.

3.2.3 Operativsystemer

En standard server bruker Microsoft Windows Server eller Linux som operativsystem. Hva som er standardsystem blir jevnlig oppdatert for å møte service- og supportavtaler.

Standardversjonen for Windows er for tiden Microsoft Windows Server 2016.

Støttede versjoner av Linux er for tiden Redhat, CentOS eller Ubuntu.

Leverte servere blir månedlig oppdatert med de siste partchsettene fra sine respektive leverandører.

3.2.4 Databaser

Helse Midt-Norge har standardisert på Microsoft SQL Server til databaser. Det er etablert flere failover clusters med flere databaseservere i hvert cluster. De forskjellige SQL instansene støtter et konsolidert produksjonsmiljø.

Standardversjonen er for tiden Microsoft SQL Server 2016. Hva som er standardversjon blir jevnlig oppdatert for å møte service- og supportavtaler.

Separate SQL-instanser eller dedikerte databaseservere, bade fysiske og virtuelle, blir allokert til systemer med spesielle ytelseskrav eller andre behov.

Det finnes et mindre databasecluster med Oracle versjon 12c. Oracle kjører på toppen av Windows Server 2012.

3.2.5 Antivirus

Windows-servere kjører antivirus-software og Windows-brannmuren er påslått.

3.2.6 Backup

Backup tas på forskjellige måter etter behov. I VMware-miljøet benyttes snapshot-teknologi til backup. For fysiske servere brukes NetBackup.

For SQL Server databaser brukes en SQL agent-jobb (T-SQL) med et filshare på dedikert Data Domain som mål. For Oracle databaser brukes RMAN.

3.2.7 Programvaredistribusjon til servere

Servere følger best practice for patching og oppdatert. For Microsoft Windows brukes Microsoft System Center Configuration Manager (SCCM) til automatisk serverpatching.

For Linux brukes Rundeck og Ansible som verktøy for å gjennomføre automatisk patching.

Den automatiske serverpatchingen dekker omtremt 90% av serverne og de resterende patches manuelt grunnet spesielle krav.

3.3 Infrastrukturtjenester

Dette kapitlet beskriver infrastrukturtjenester levert fra Hemit til Helse Midt-Norge.

3.3.1 Active Directory (AD)

Microsoft Active Directory er Helse Midt-Norges grunnleggende kilde til autentisering og autorisering inn til og inne i IT-systemene.

Helse Midt-Norges Microsoft Active Directory forest består av 10 domenekontrollere og kjører på 2016 funksjonalitetsnivå. Alle domenekontrollerne kjører Microsoft Windows Server 2016.

Fire av domenekontrollerne er lokalisert i datasenteret i Trondheim. Resten av domenekontrollerne er plassert på de andre sykehusene i regionene.

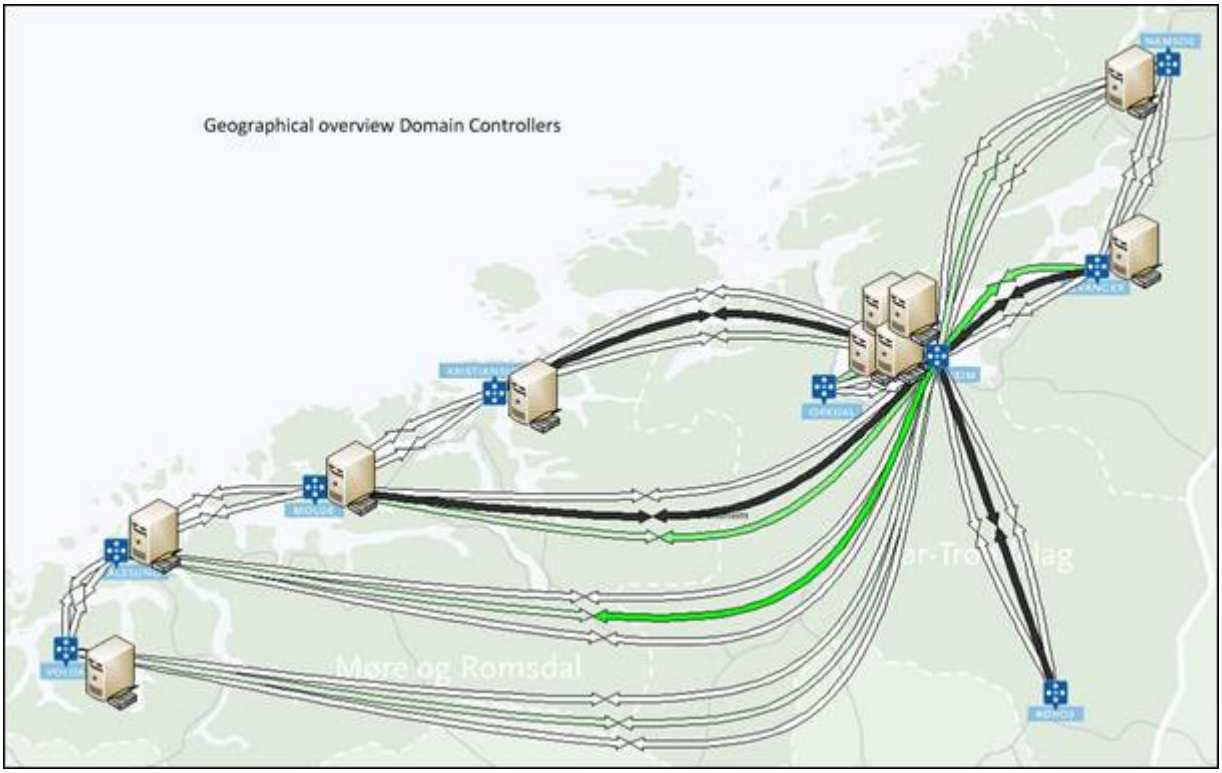


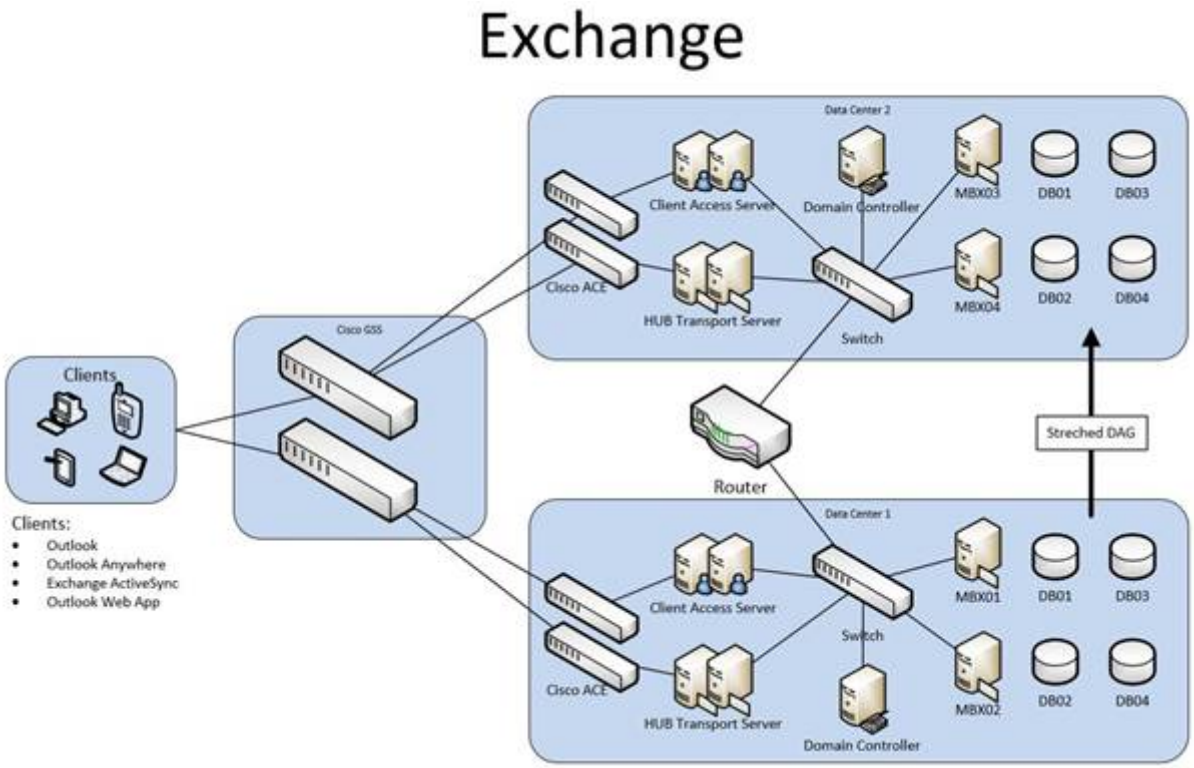
Figure 2 Active Directory

3.3.2 Federation services (ADFS)

Active Directory Federation Service er implementert for autentisering på tvers av organisasjonsgrenser. Det er den foretrukne måten å gi lokale brukere tilgang til eksterne webtjenester og eksterne brukere tilgang til interne webtjenester.

3.3.3 E-post

Eposttjenester leveres av Microsoft Exchange 2010 SP2 som kjører på virtuelle servere med Microsoft Windows Server 2008 R2

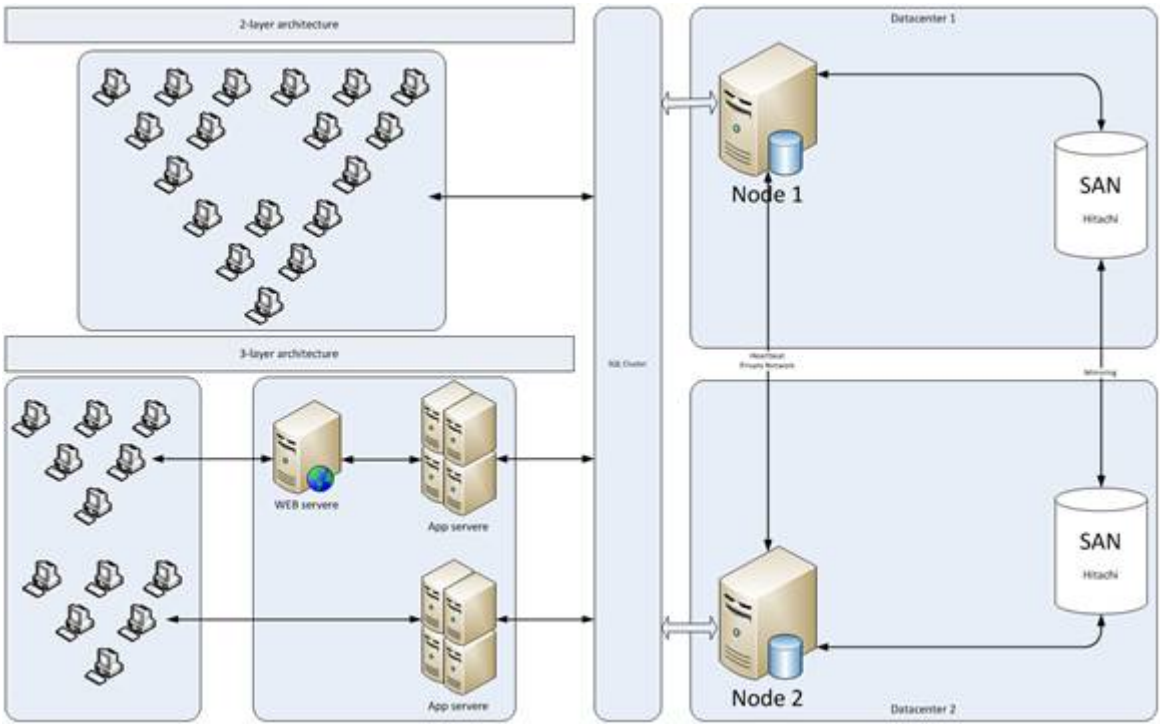


Figur 3 Eposttjenster

3.3 Lagring og Storage Area Network (SAN)

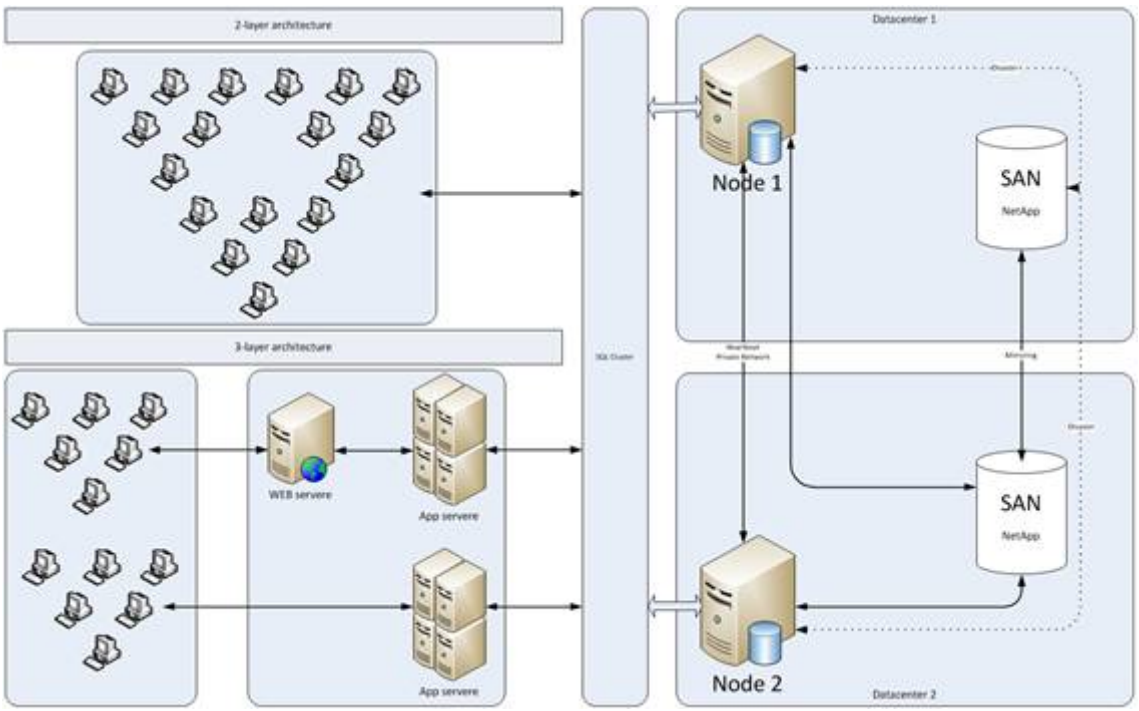
Helse Midt-Norge tilbyr Storage Area Networks i to nivåer: High-end og mid-range.

High-end lagring leveres kun i datasenteret i Trondheim. Tjenesten leveres av Hitachi VSP F1500 konfigurert med synkron speiling over et dedikert fibernettverk mellom de to datarommene som utgjør datasenteret.



Figur 4 High-End SAN

Mid-range lagring leveres av NetApp NAS. I datasenteret i Trondheim er de to datarommene konfigurert med asynkron speiling hver time over et dedikert fibernettverk.

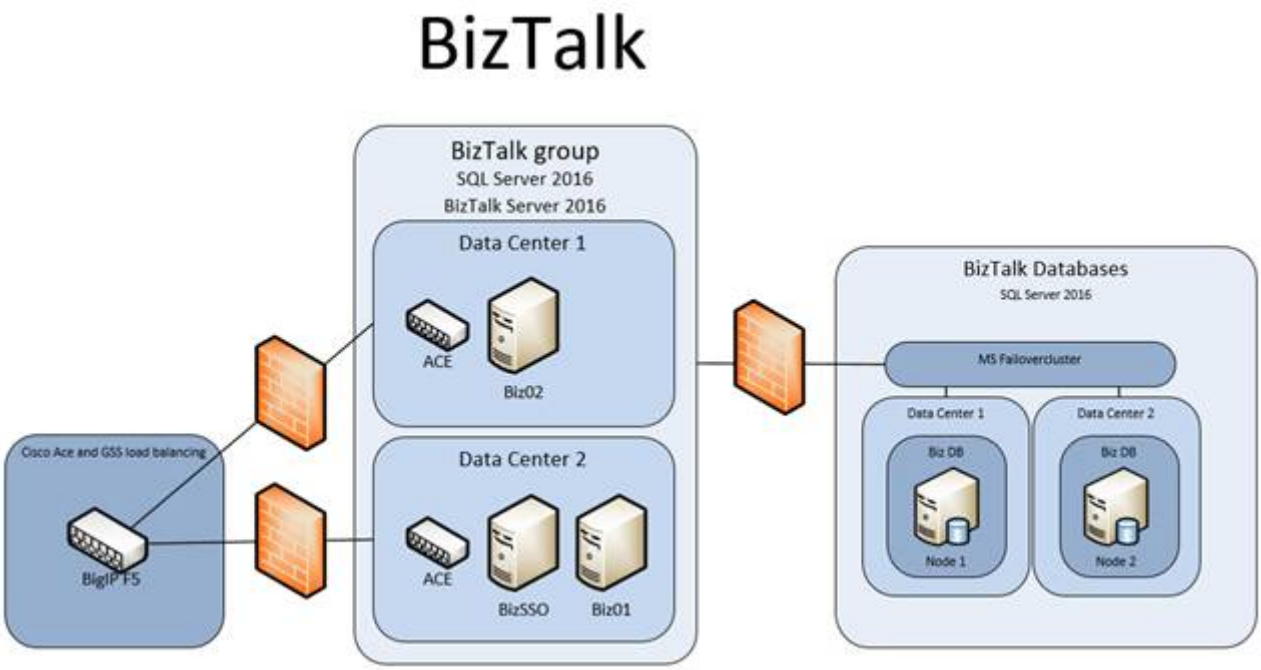


Figur 5 Mid-Range SAN

Til backupdata brukes EMC Data Domain, for tiden av serie DD2500.

3. 4 Integrasjoner

Helse Midt-Norge tilbyr en "enterprise service bus" (ESB) bestående av Microsoft BizTalk 2016 for integrasjonstjenester. Tjenesten betjener og tilbyr både interne og eksterne integrasjoner.

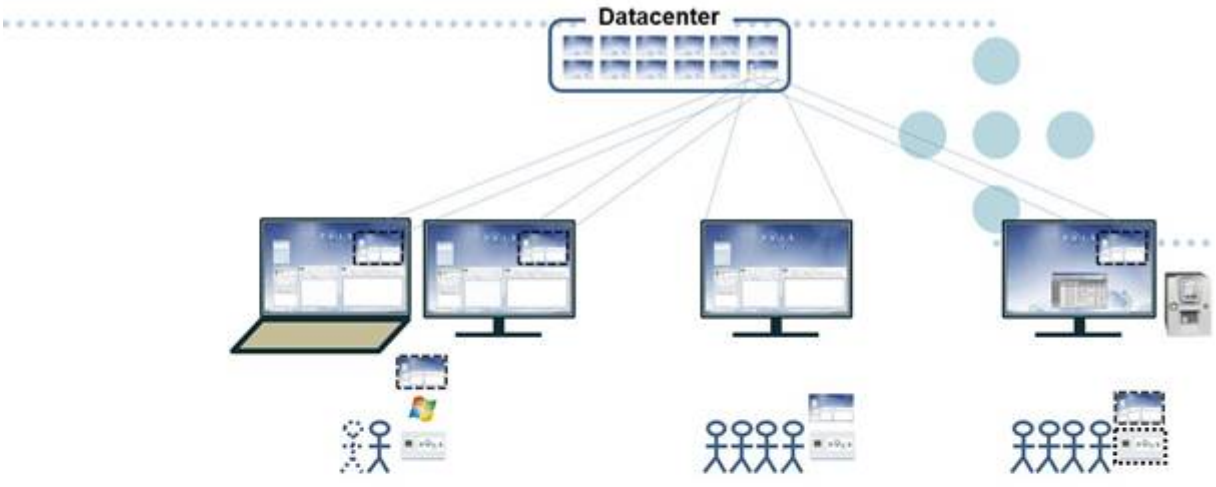


Figur 6 Overview BizTalk

3.5 Klienter

Helse Midt-Norge tilbyr tre forskjellige PC- baserte klienter:

- Puls Standard
  - Standard Windows 10-klient for klinisk og administrative bruk hvor brukeren logger på med et personlig smartkort. Disse klientene er beregnet for personlig bruk i kontormiljø. Hovedtyngden av PC-er er av denne typen.
- Puls Spesial
  - Standard Windows 10-klient med automatisk pålogging av systembruker ved oppstart. Denne klienten er beregnet tilkobling til analyseinstrumenter og applikasjoner med spesielle krav. Puls Spesial-klienten kan kun plasseres i adgangskontrollert område.
- Puls Sprint
  - Nedlåst Windows 10-klient brukt som tynnklient mot VDI-miljøet. Disse klientene er ideelle der flere brukere deler en datamaskin, for eksempel i klinikker og på sengeposter. Brukere logger på og re-connecter med et personlig smartkort. Sesjonen til VDI blir disconnected når smartkortet blir fjernet fra klienten og er klar for neste bruker.



PC Client	Standard	Sprint	Spesial
Locally installed apps	All your apps	No	Can be cutomized
Central clientapps (VDI)	*All your apps*	All your apps	*All your apps*
Windows local logon	Smartcard	No	No
Windows central logon (VDI)	*Smartcard*	Smartcard	*Smartcard*
Windows reconnect (VDI)	*Smartcard*	Smartcard	*Smartcard*
When removing smartcard	Lock desktop	Disconnect	*Disconnect (only VDI)*
Mobility	Laptop (VPN) / Workstation	Workstation	Workstation
Function when loss of network connection	Yes	No	Depend on application dependencies

Tabell 1 Typer av PC-klienter

En Virtuell Desktop Infrastructure (VDI) er bygd på VMware Horizon View og skalert for 4000 samtidige brukere. VDIer brukes hovedsakelig av helsepersonell med behov for å logge på flere arbeidsstasjoner i løpet av arbeidsdagen. Ved å disconnecte og så reconnecte kan de spare tid ved å beholde sin arbeidssesjon mens de beveger seg fra arbeidspost til arbeidspost.

Desktop pools er flytende linkede kloner som friskes opp en gang i uka. Alle sesjoner starter fra et «golden image» basert på Windows 10 med et standard sett av basisapplikasjoner og mellomvare og justert etter «best practice» for et VDI-miljø.

Bærbare PCer bruker lokale brukerprofiler og offline synkronisering av dokumenter og epost. Fjerntilgang til Helse Midt-Norges nettverk fra bærbare PCer skjer ved hjelp av Microsoft Direct Access.

Alle PC-klienter kjører Microsoft System Center Endpoint Protection, den lokale Windows Firewall er påslått og styres av Group Policy Objects (GPO). Patching og oppdateringer gjøres ifølge Microsofts «best practice» for å holde et høyt sikkerhetsnivå og høy stabilitet. PCene patches månedlig og VDI-imaget hver tredje måned.

3.5.1 Klienthardware

Helse Midt-Norge har en standardisert klientplattform basert på Microsoft Windows 10 x64, hvor omtrent 20% er bærbare PCer og 80% er stasjonære PCer. Totalt er det ca. 17 000 fysiske klienter. Livssyklusen for PCene er 4 år.

Mobiltelefoner og tablets har kun begrenset bruk innen den kliniske virksomheten i dag. Pr. i dag støtter Helse Midt-Norge kun synkronisering av epost. Noen applikasjonsspesifikke spesialløsninger med tablets finnes.

3.5.2 Programvare

De sentralt konfigurerte PCene får konfigurasjonen sin fra et distribuert klientimage fra SCCM og innstillinger i GPOer fra Active Directory.

Følgende programvare er en del av klientimaget og er tilgjengelig fra alle klienttyper:

- Microsoft .Net Framework 4.7
- Microsoft Silverlight 5.1.5 (on thick clients, but not on VDI)
- Microsoft Office 2016
- Microsoft Internet Explorer 11
- Skype® for Business 2016
- 7-Zip 19.00
- Adobe Reader DC 19
- Java 8 Update 202
- Citrix Receiver 4.9.7
- VLC Media Player 3.0.6
- Microsoft Virtual C++ 2005-2017 Redistributable packs
- Net iD 6.6
- RES Workspace Manager 10.3.60
- Netop Remote Control 12.60

3.5.3 Fjernhjelp

Netop Remote Control 12.60 brukes til fjernhjelp og feilretting på klienter.

3.5.4 Programvaredistribusjon

Programvare distribueres til datamaskiner og brukere enten som tradisjonelt installerte applikasjoner (tykt installert) eller som virtualiserte installasjoner med Microsoft App-V. Programvarepakker strømmes fra et distribuert filsystem der lokale kopier av alle pakker er lagret på alle sykehus.

Sikkerhetsgrupper i Active Directory styrer hvilke applikasjoner brukerne får tilgang til og er basis for distribusjon av programvare fra SCCM.

Målet er å virtualisere så mange applikasjoner gjennom App-V som mulig. For tiden er omtrent 80% av applikasjonene virtualisert. De applikasjonene som ikke kan virtualiseres blir distribuert og installert med SCCM.

3.5.4 Epostklient

Epostklienten som brukes I Helse Midt-Norge er Microsoft Outlook 2016.

3.5.5 Antivirus

For tiden brukes Microsoft System Center Endpoint Protection som antivirus på PCene. Det pågår arbeide for å skifte til Trend Antivirus på klientene.

3.6 Klient workspace

Avanti Workspace Manager (tidligere RES Workspace Manager) håndterer brukermiljøet og profilene på PCene. Programvareikoner, brukerinnstillinger og drive mappinger distribueres til brukerne basert på brukerens gruppetilhørighet og klientens kontekst ved pålogging og reconnect.

På stasjonære PCer og virtuelle klienter brukes en tilpasset påkrevet brukerprofil (mandatory user profile) som slettes fra klienten når brukeren logger av. Brukerens profil tas vare på av Avanti Workspace Manager og legges på neste klient som brukeren logger på.

3.6.1 Brukerpålogging

Brukere logger på et Windows domene og autentiseres med et personlig sertifikat lagret på et smartkort. Applikasjoner autentiserer brukerne på forskjellige måter:

- Brukernavn og passord definert internt i applikasjonen
- Brukernavn og passord definert i Active Directory
- Integrert autentisering tilbyr Single Sign On

3.6.2 Personlig brukerkonto

Alle brukere tildeles et dedikert brukerobjekt i Active Directory, Der applikasjoner ikke er integrert med AD må brukerens identitet håndteres internt i applikasjonen.

Brukere som skal ha administrative privilegier får et separat brukerobjekt i AD i tillegg til sin normale bruker.

Relaterte vedlegg:

Kundens Tekniske Plattform