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.

1 Nettverk

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

1.1 Wide Area Network

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

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

1.2 Norsk Helsenett

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

1.3 Lokalnettverket

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.

På sykehusene St. Olavs Hospital og Sykehuset Nordmøre og Romsdal brukes Cisco Trustsec. Det gir fleksibilitet til å definere hvilke subnett skal brukes og hvilke brannmurregler som kan brukes ute i spredenettene.

På Sykehuset Nordmøre og Romsdal er det også tatt i bruk SDA (Software Defined Access network). SDA gir større mulighet for automatisering og policystyring av spredenettene.

1.4 Trådløst nettverk

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.

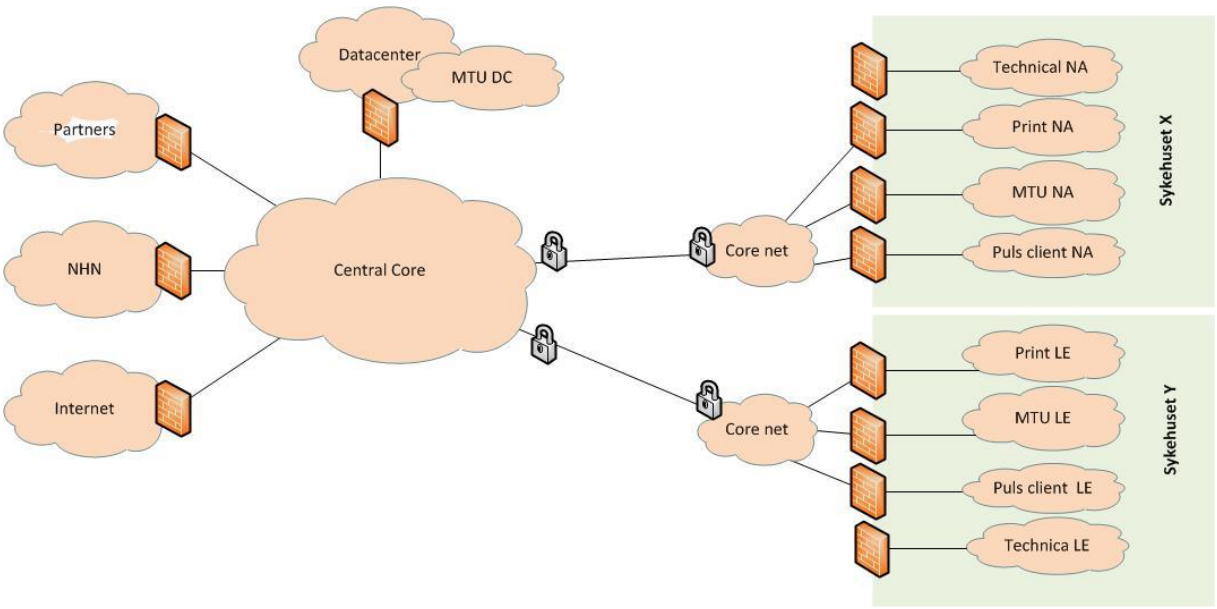
Aksesspunktene og WLC’er er fra Cisco.

1.5 Virtuelle nettverk

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. Her brukes også Trustsec for riktig tildeling i nettverkssoner.

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



Figur 1 – Eksempel på Virtuelle LAN

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 Palo Alto.

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.

1.8 Nettverksprotokoller

Nettverkene er bygd på kommunikasjonsprotokollene i IP versjon 4.

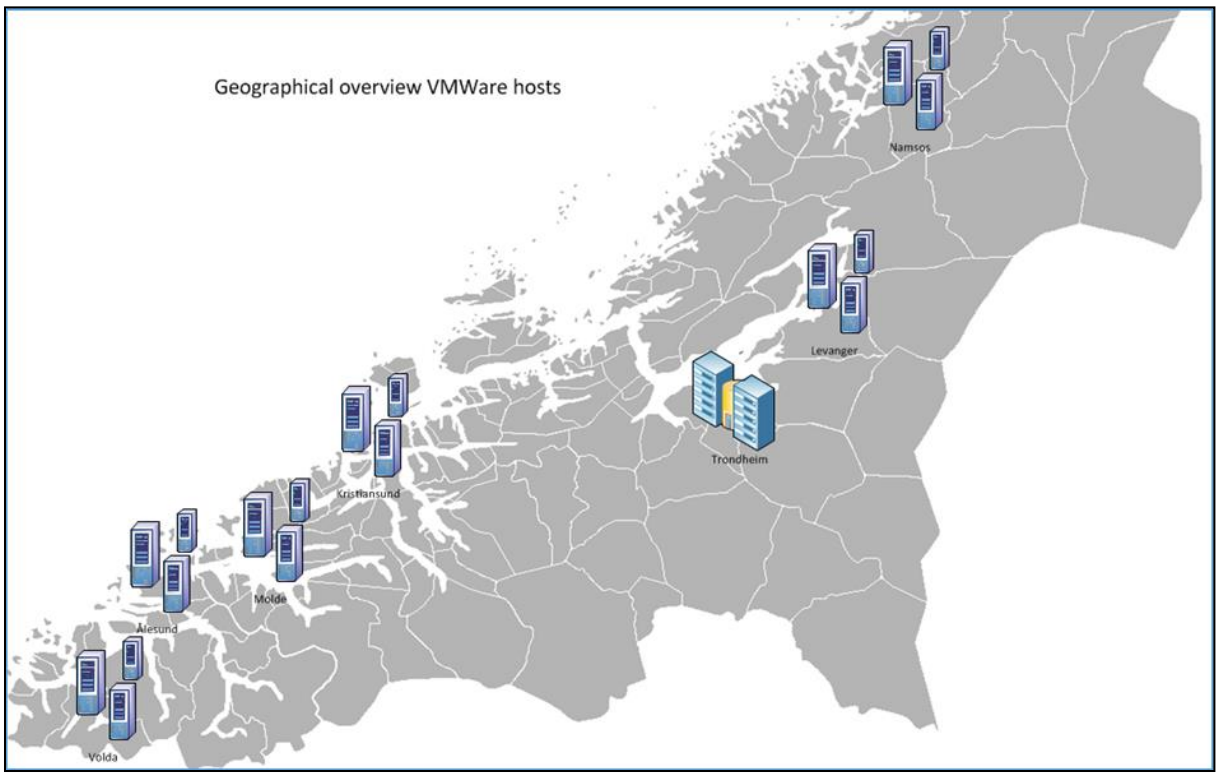
2 Servere

Servere i Helse Midt-Norge leveres som virtuelle servere. Det kan gjøres unntak om det finnes tungtveiende argumenter for hvorfor den aktuelle serveren kun kan leveres som fysisk server.

2.1 Virtuelle servere

Helse Midt-Norge har standardisert på virtualisert maskinvare. Virtualiseringsgraden av servere er over 98%. Windows- og Linux-servere kjører på VMware ESXi.

2.2 Virtualiseringsteknologi



Figur 2 Lokasjoner for servervirtualisering

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

Det er i tillegg en VMware VDI-farm som betjener 6 000 VDI'er. Se kapittel for klienter for mer informasjon.

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 2022.

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

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

2.4 Databaser

Helse Midt-Norge har standardisert på Microsoft SQL Server til databaser. Vi benytter virtuell plattform på VMware for våre SQL instanser. Vi benytter konsoliderte installasjoner i de fleste situasjoner, men kan vurdere å bruker standalone i tilfeller der det er nødvendig. Helse Midt-Norge tilbyr standalone servere, Microsoft Failover Clustering og Always On Availability Groups. Valg av standalone løsning må begrunnes og gjøres basert på applikasjonens tjenestenivå og behov.

Standardversjonen er for tiden Microsoft SQL Server 2022. Hva som er standardversjon blir jevnlig oppdatert for å møte service- og supportavtaler. Alle applikasjoner må støtte nyeste Cumulative Update til enhver tid, da vi kjører oppgradering av SQL Server med siste patch 3 ganger pr. år.

Det finnes et databasecluster med Oracle versjon 12c men vi kan levere nyere versjoner ved behov. Oracle kjører her på toppen av Windows Server.

2.5 Antivirus

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

2.6 Backup

Backup tas på forskjellige måter etter behov. I VMware-miljøet benyttes snapshot-teknologi til backup som lagres på NetApp og Rubrik. For fysiske servere brukes Rubrik.

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

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 omtrent 90% av serverne og de resterende patches manuelt grunnet spesielle krav.

3 Infrastrukturtjenester

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

3.1 Active Directory

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 domenekontrollere plassert i datasenteret i Trondheim. Domenekontrollerne kjører på 2016 funksjonalitetsnivå. Alle domenekontrollerne kjører Microsoft Windows Server 2022.

Det er totalt seks domenekontrollerne som er lokalisert i datasenteret i Trondheim.

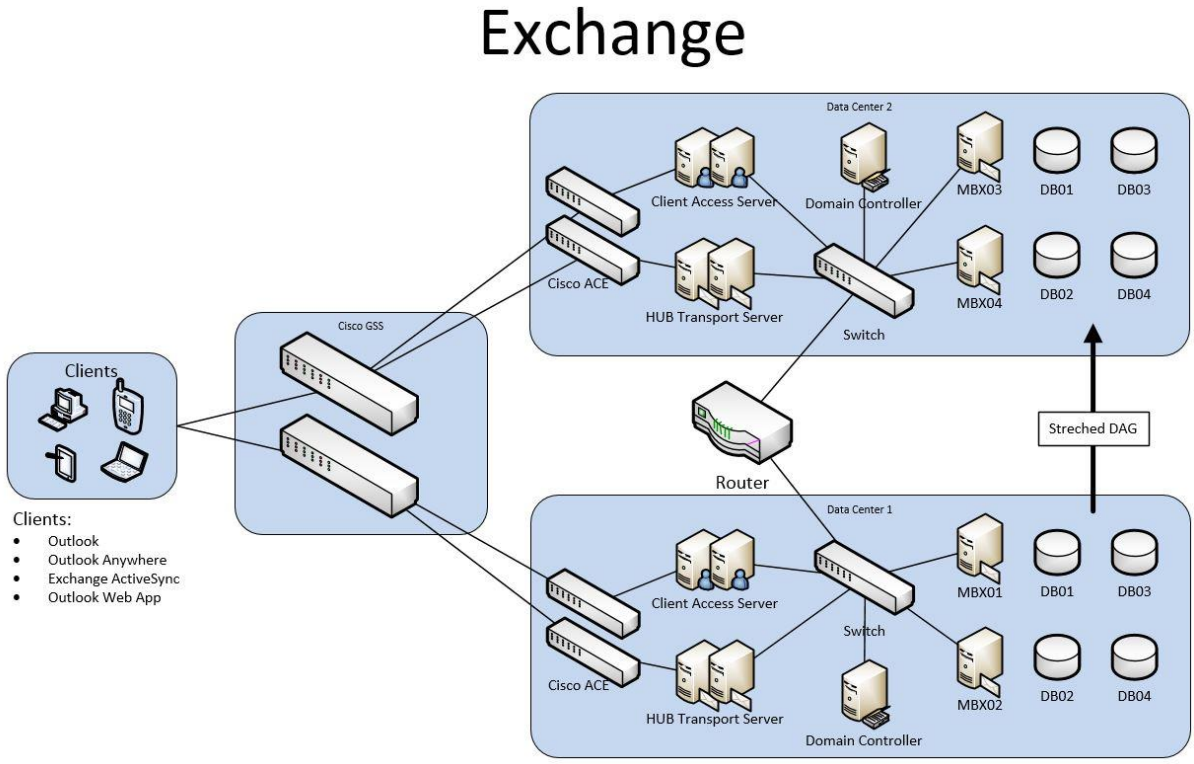
3.2 Federation services

Helse Midt-Norge bruker Microsoft Entra ID der det er behov for federeringstjenester. Det er en måte å gi lokale brukere tilgang til eksterne webtjenester og eksterne brukere tilgang til interne webtjenester.

3.3 E-post

Eposttjenester leveres av skytjenestene Microsoft M365 og Exchange Online.

Det finnes også en hybrid installasjon av Microsoft Exchange 2019 lokalt. Denne tar i mot epost fra systemer og tjenester som ikke støtter Exchange Online. Helse Midt-Norge støtter protokollene SMTP, IMAP og POP3 for tjenester som produserer eller forbruker epost.

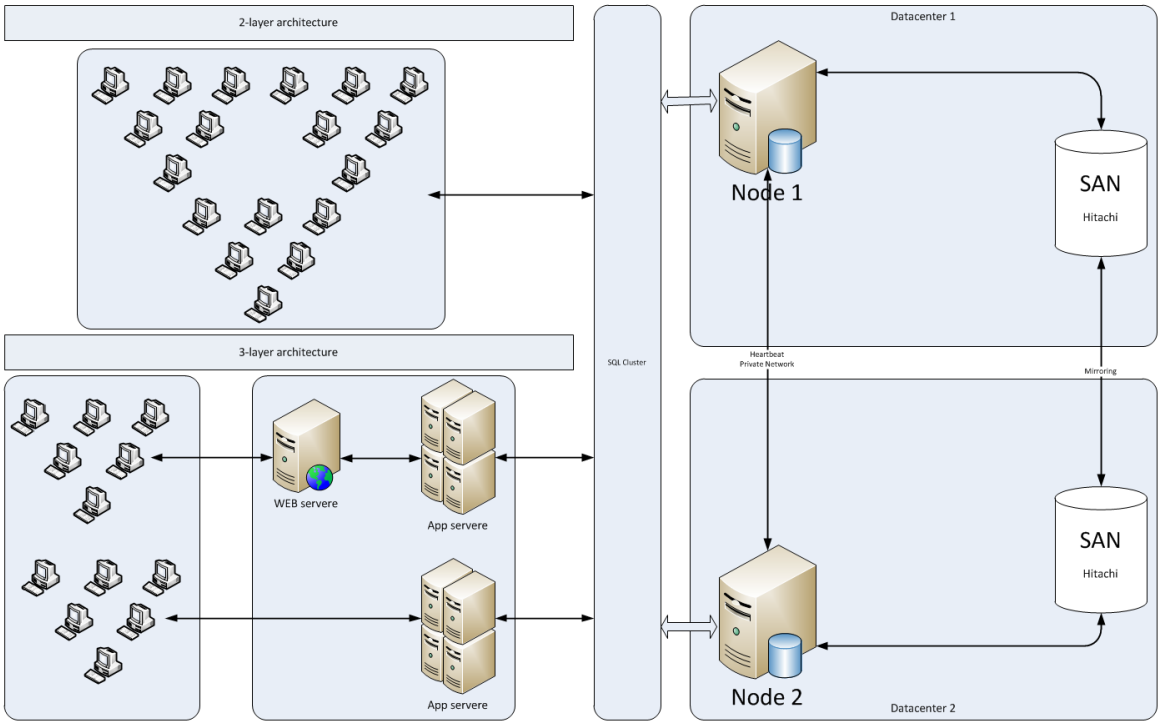


Figur 1 Oversikt over hybride eposttjenester

4 Lagring og Storage Area Network

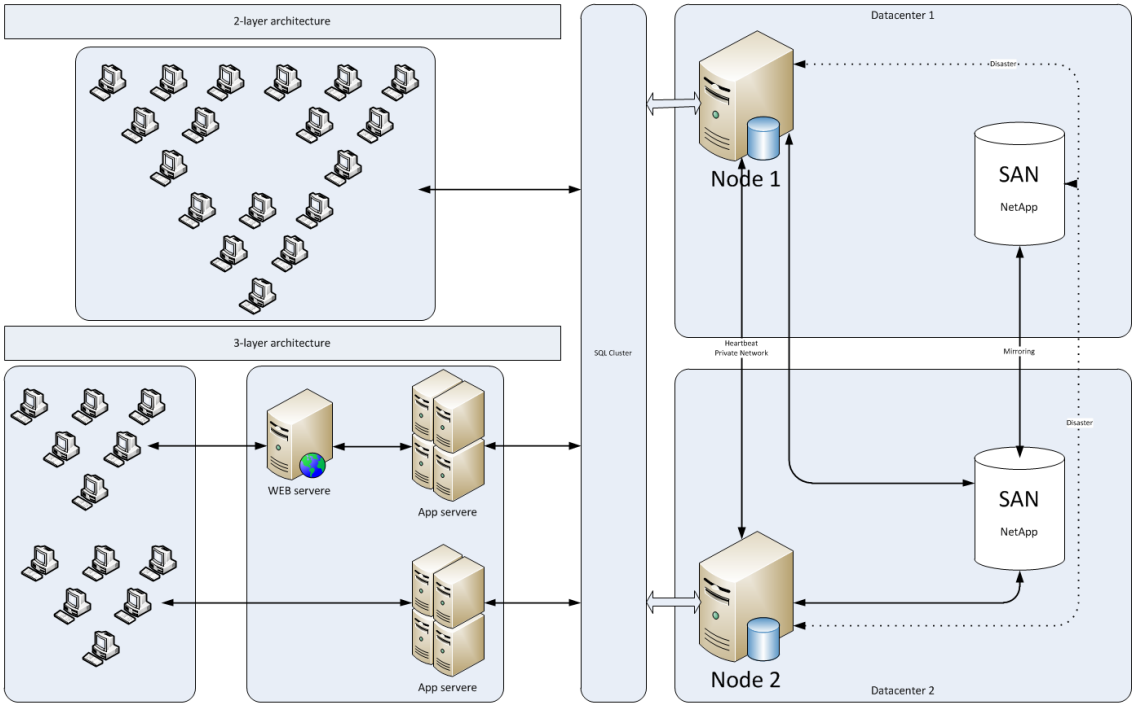
Helse Midt-Norge tilbyr Storage Area Networks i to nivåer: High-end og mid-range.

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 2 Eksempel på bruk av High-End SAN

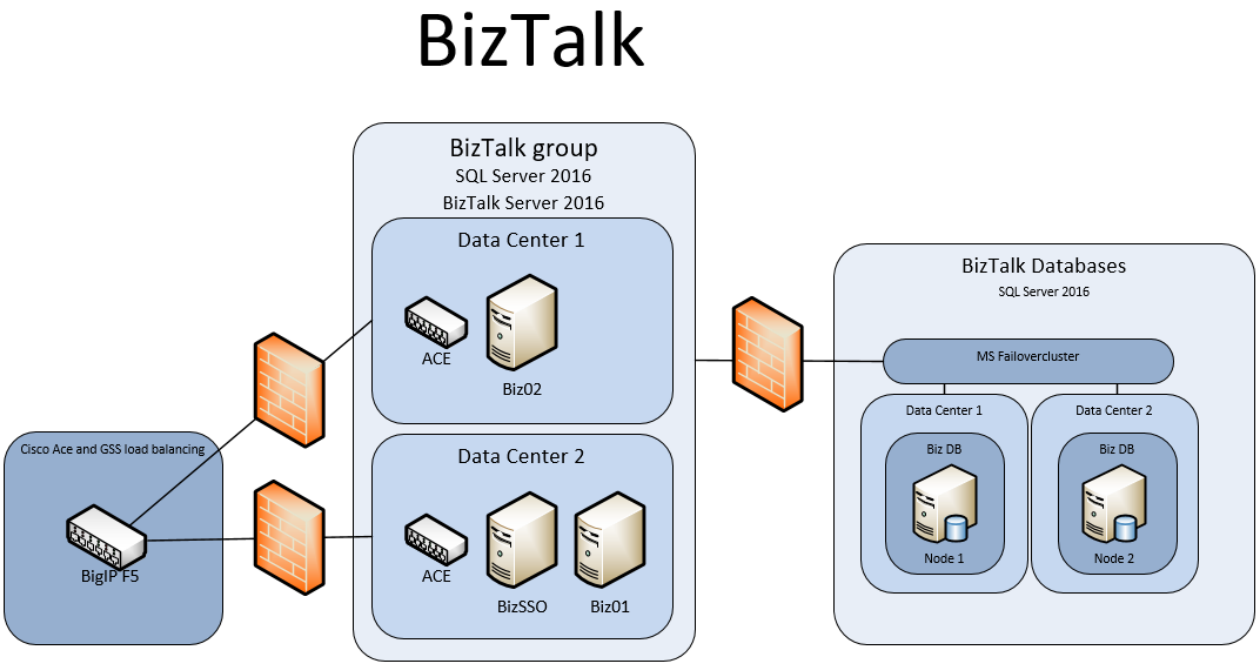
Mid-range lagring leveres av NetApp. NetApp leverer både blokk- og fillagring. I datasenteret i Trondheim er de to datarommene konfigurert med asynkron speiling hver time over et dedikert fibernettverk.



Figur 3 Eksempel på bruk av Mid-Range SAN

5 Integrasjoner

Helse Midt-Norge tilbyr en “enterprise service bus” (ESB) bestående av Microsoft BizTalk 2022 CU5 for integrasjonstjenester. Tjenesten betjener og tilbyr både interne og eksterne integrasjoner.



Figur 4 Oversikt over BizTalk

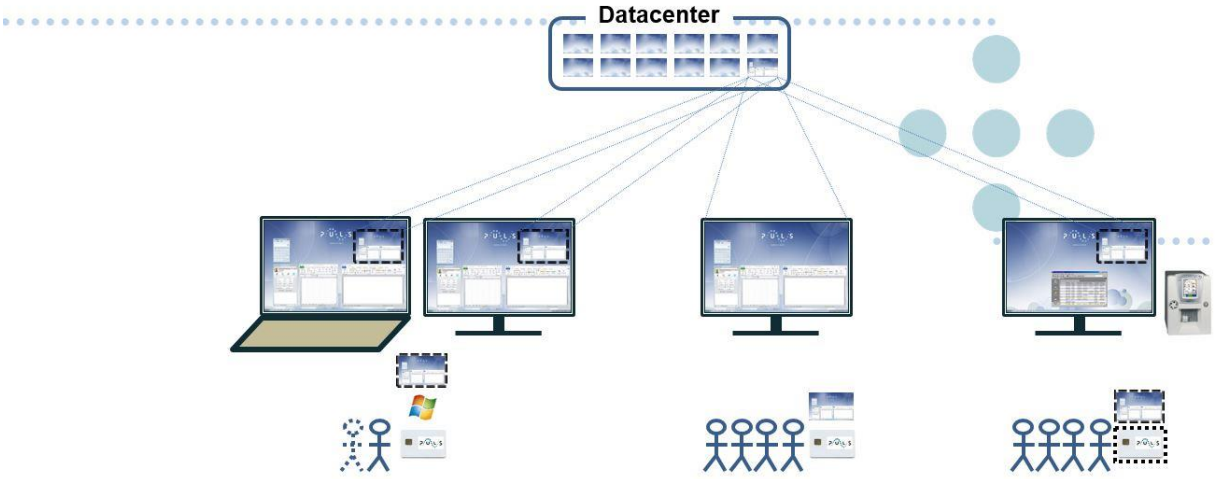
6 Klienter

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

- Puls Standard
  - Standard Windows 10- og 11-klienter 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- og 11-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- og 11-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.

I tillegg tilbys Ekstern Puls som er innlogging til VDI fra andre enheter over internett, som f.eks. fra privat PC.



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 Omnissa (tidligere VMware) Horizon View og skalert for 6 000 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 «instant clones» som slettes når brukeren logger av. 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 og VPN.

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.

Alle klienter er herdet etter Microsofts Security Baselines.

6.1 Klienthardware

Helse Midt-Norge har en standardisert klientplattform basert på Microsoft Windows 10 x64 og 11 x64, hvor omtrent 30% er bærbare PCer og 70% er stasjonære PCer. Totalt er det ca. 25 000 fysiske klienter. Livssyklusen for PCene er 5-7 år.

Helse Midt-Norge har et tilbud om håndholdt arbeidsflate. Den kan tilbys på hovedsakelig på Apple iPhone og Myco 3. Vi støtter også Apple iPad og enheter fra Zebra, som er android-baserte enheter. Til sammen er det pr januar 2025 ca 10 000 enheter i den håndholdte arbeidsflaten.

6.2 Programvare

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

Sammen med imaget distribuerer vi Microsofts standardprodukter som Microsoft M365 eller Office 2016 og et sett med standardprogramvare. Som nettleser har HMN standardisert på Microsoft Edge.

6.3 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. De applikasjonene som ikke kan virtualiseres blir distribuert og installert med SCCM.

6.4 Epostklient

Epostklientene som brukes i Helse Midt-Norge er Microsoft M365 og Outlook 2016.

6.5 Antivirus

For tiden brukes Microsoft Defender for Endpoint Protection som antivirus på PCene.

7 Klient workspace

Ivanti (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 Ivanti Workspace Manager og legges på neste klient som brukeren logger på.

7.1 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

7.2 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.