Customer Technical Platform

This document describes the IT infrastructure existing in Helse Midt-Norge. The document aims to provide the potential supplier with an insight into what technologies and capabilities exists, which services the supplier must consider and what services the supplier can potentially rely on.

1 Network

This chapter describes the design of how networks connect technical infrastructure, network protocols in use and control mechanisms on traffic flow.

1.1 Wide Area Network

The WAN consists of a large number of high-capacity and redundant leased lines from various subcontractors. The level of capacity and redundancy varies between locations based on their size and role.

A connection to the network provided by Norsk Helsenett provides secure and high-performance messaging services and internet access. The network is built with Cisco routers that provide routing of IP-based traffic between locations.

1.2 Norsk Helsenett

Norsk Helsenett is owned by Helse- og omsorgsdepartementet (Ministry of Health and Care Services) and delivers network services, internet and other application services to all connected organizations within Norwegian health organizations.

1.3 Local Area Networking

Local Area Networks are built around high-capacity links (1 Gbps or more). Traffic is routed by a standardized layered architecture for edge switches, distribution switches and core networks.

All switches in distribution and edge layers are implemented on Cisco Catalyst switches.

Cisco Trustsec is implemented at hospitals St. Olavs Hospital and Sykehuset Nordmøre og Romsdal. This technology adds flexibility to what subnets and firewall rules can be distributed to the edge.

Software Defined Access network has been deployed to Sykehuset Nordmøre og Romsdal. SDA allows greater levels of automaton and policy level control of distribution networks.

1.4 Wireless networking

There are wireless networks available on all locations of Helse Midt-Norge. Clients offered by Helse Midt-Norge will automatically be granted access to the uniform and

secure enterprise class wireless network in Helse Midt-Norge. Helse Midt-Norge provides a guest network for devices brought by patients, consultants and other visitors.

The wireless network is built on devices from Cisco Catalyst series and is centrally managed by high-available wireless LAN controllers that control all distributed wireless access points. Managed clients is authenticated by IEEE 802.1X client authentication before being granted access to the wireless network.

1.5 Virtual networks

The physical network is partitioned into logical network zones using virtual networks (VLAN). The partitioning manages and transports data of different security classes on a functional and secure way.

PCs are authenticated by IEEE 802.1x. When connected to the network, PCs are automatically connected to their correct network zones. Where available, Trustsec is used to grant access to correct networking zones.

Figure 1 below shows how the network is partitioned into different logical networks using VLANs.

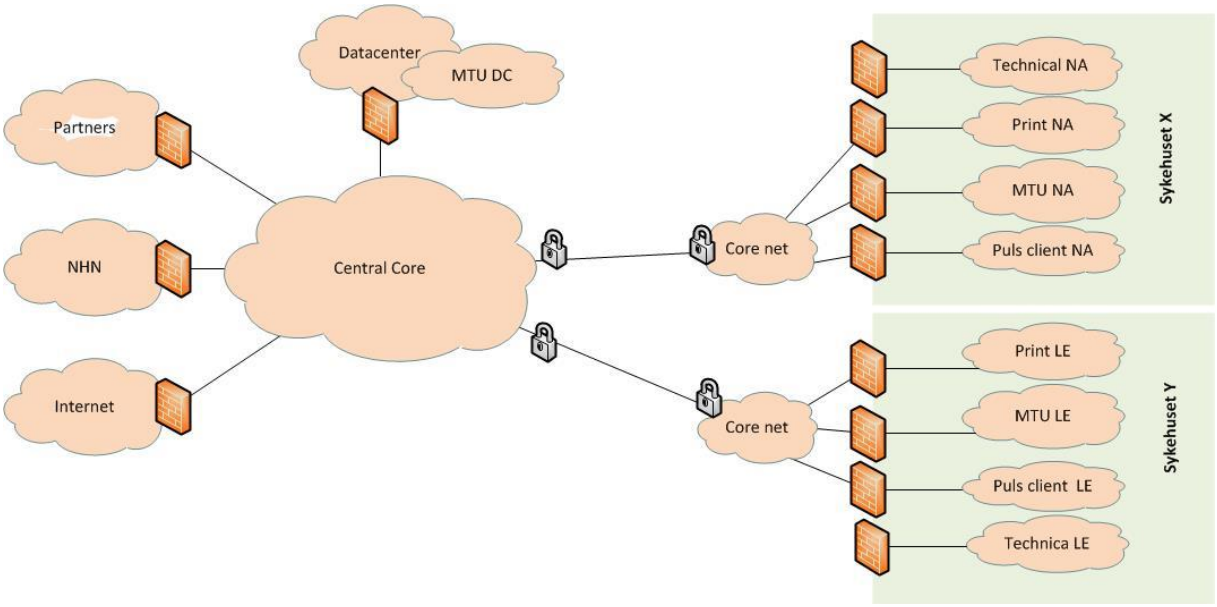


Figure 1 – Example of Virtual LANs

1.6 Firewalls

The network is partitioned by firewalls that control traffic flow and limits what services can communicate on the network and what traffic protocols can be used.

All network traffic through firewalls, both allowed and blocked traffic, are logged.

Helse Midt-Norge uses firewalls from Palo Alto and Cisco ASA-series.

1.7 Remote Access

Employees in Helse Midt-Norge are offered remote access directly from their Puls PCs using Microsoft Direct Access.

Helse Midt-Norge also offers remote access for employees using Virtual Desktop Infrastructure (VDI). This VDI solution is built on Omnissa Horizon (formerly named VMware Horizon).

Contracted suppliers of IT services and IT-support can be granted remote access through a Citrix terminal server solution.

1.8 Network protocol support

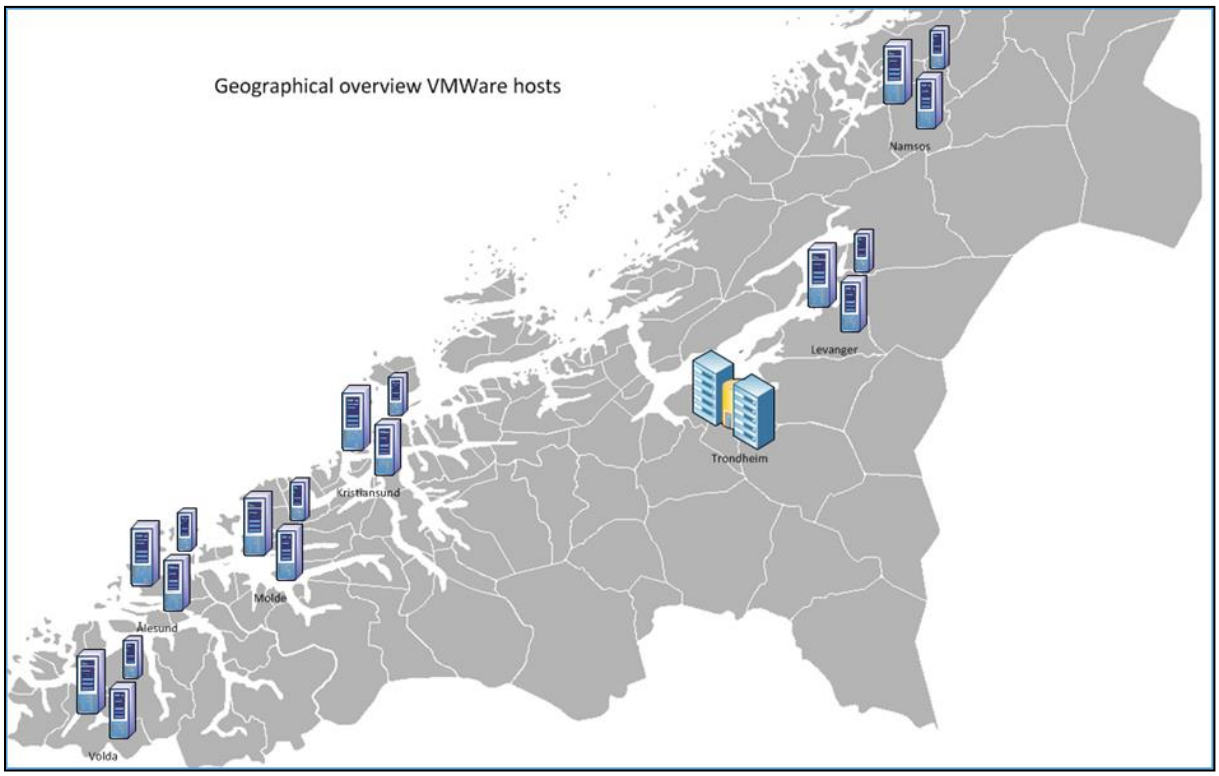
All networks are built on protocols from Internet Protocol version 4 (IPv4).

2 Servers

2.1 Virtual servers

Helse Midt-Norge has standardized on virtualization of servers. Virtualization rate is currently over 98% for Windows and Linux servers. Both Windows and Linux are supported on VMware ESXi.

2.2 Virtualisation of Servers



Figur 1 Server locations and virtualization

The production environment for servers consists of several geographically spread VMware farms placed in hospitals. Most production servers are placed in the central data center in Trondheim.

There is also a VMware VDI farm serving 6,000 VDIs. Please refer to chapter on clients for more details.

2.3 Operating systems

The standard server operating systems are Microsoft Windows Server or Linux servers. Standard server operating systems are regularly upgraded to meet service and support agreements.

The standard version of Windows server deliveries is currently Windows Server 2022.

The standard versions of Linux server deliveries are currently Redhat, CentOS and Ubuntu.

Servers delivered from Hemit are updated monthly with the latest patches published by their suppliers.

2.4 Databases

Helse Midt-Norge has standardized on Microsoft SQL Server as database platform. All SQL instances are running on a virtual platform on VMware. Hemit delivers consolidated instances for most cases but can deliver standalone instances where

strictly necessary. We offer both standalone servers, Microsoft Failover Clustering and Always On Availability Groups. Choice of standalone must be justified by the applications service level and other requirements.

The standard version is currently Microsoft SQL Server 2022. What is current standard version is regularly upgraded to meet service and support agreements. Every application must always meet requirements set by the latest Cumulative Update. SQL Server is updated to the latest Cumulative Update thrice a year.

There is a database cluster running Oracle version 12c on top of Windows Server to accommodate applications that only supports Oracle. Newer versions of Oracle can be delivered if the need arises.

2.5 Antivirus

All Windows servers are running anti-virus software and the internal Windows firewall is enabled.

2.6 Backup

Backup is done using various technologies. Snapshot technology performs backup and restore of data in the VMware environment, storing backups on NetApp and Rubrik. Backup and restore of physical servers are performed by Rubrik.

Backup and restore of SQL Server databases are performed by an SQL agent job (T-SQL) to a Data Domain device. Backup and restore of Oracle databases are performed by RMAN.

2.7 Software distribution for servers

Microsoft best practice for patching and updating are followed for Windows servers. Automated server patching is performed by Microsoft System Center Configuration Manager (SCCM).

Linus servers are automatically patched by using Rundeck and Ansible.

The automated regime patches approximately 90% of the servers and the remaining servers are patched manually due to special requirements.

3 Infrastructure services

This chapter describes what infrastructure services are delivered by Hemit to Helse Midt-Norge.

3.1 Active Directory (AD)

Helse Midt-Norge uses Microsoft Active Directory as its authoritative source for authentication and authorization into and inside its IT services.

Helse Midt-Norge's Microsoft Active Directory forest contains of domain controllers placed in the data centre in Trondheim. Domain controllers are on functional level 2016. The domain controllers are running on Windows server 2022.

A total of six domain controllers are located at the data center in Trondheim.

3.2 Federation services

Helse Midt-Norge offers Microsoft Entra ID where needed for federation services. Federation can enable access to remote web application services for local users and access to local web application services for remote users.

3.3 Email

Email services are delivered by Microsoft M365 and Exchange Online.

To support legacy systems and services not compatible with Exchange Online, a hybrid installation of Microsoft Exchange 2016 is deployed locally. Helse Midt-Norge offers SMTP, IMAP and POP3 protocols for services that produce or consume email.

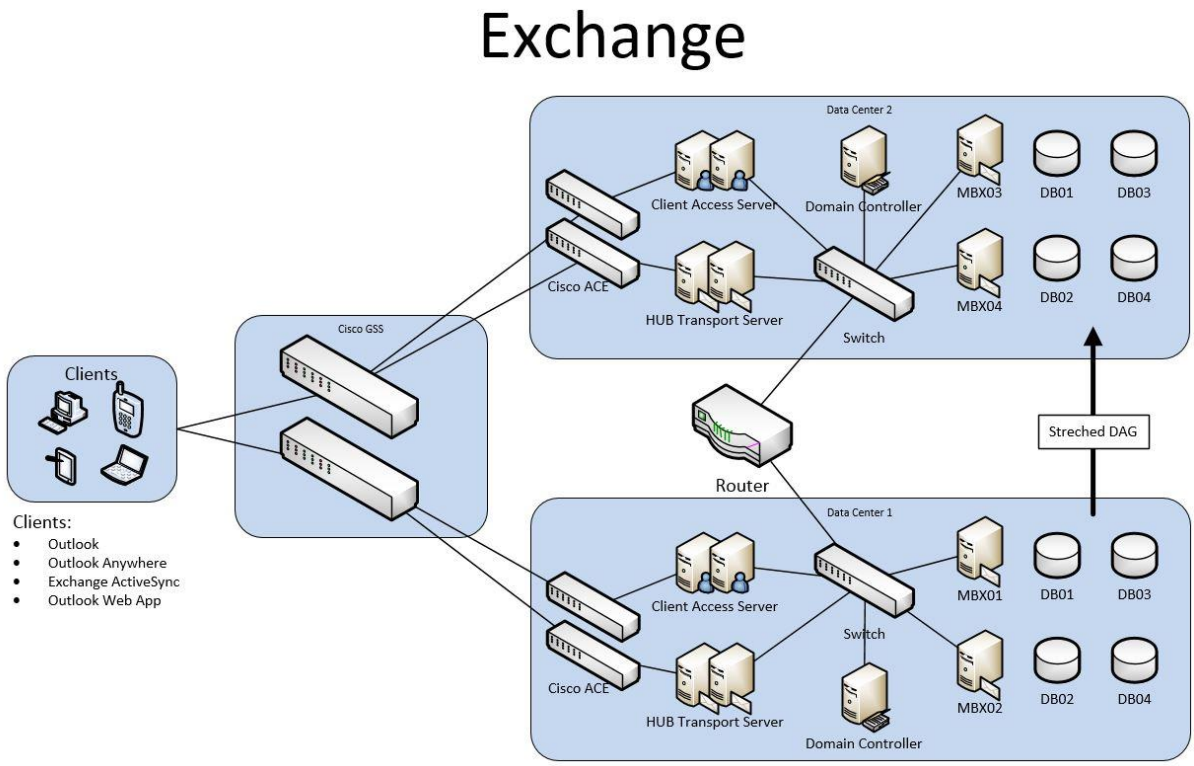


Figure 2 Overview over hybrid email services

4 Storage and Storage Area Network

Helse Midt-Norge offers Storage Area Networks on two levels: High-End and Mid-Range.

High-End storage is only delivered within the data centre in Trondheim. The high-end quality storage solution is Hitachi VSP F1500, configured with a synchronous mirroring between availability zones in the data center over a dedicated fiber network.

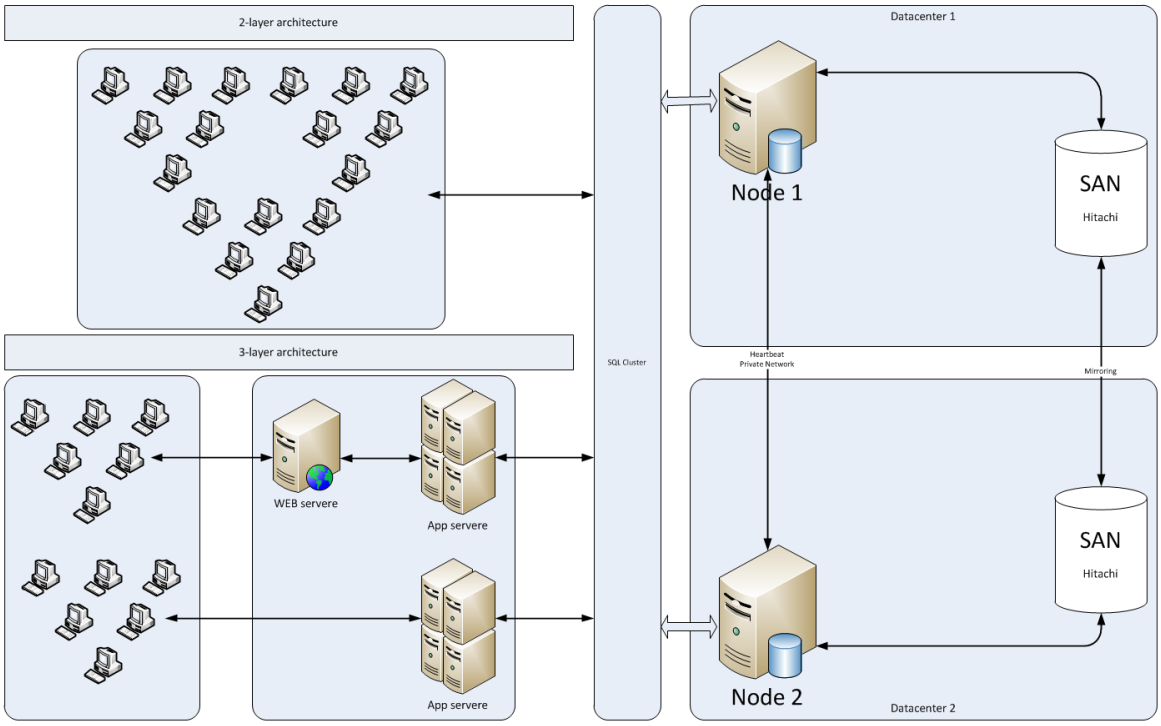


Figure 3 Usage example of High-End SAN

The mid-range quality storage solution is NetApp. NetApp delivers both block and file storage. Availability zones in the central data center in Trondheim are configured with asynchronous mirroring every hour over a dedicated fiber network.

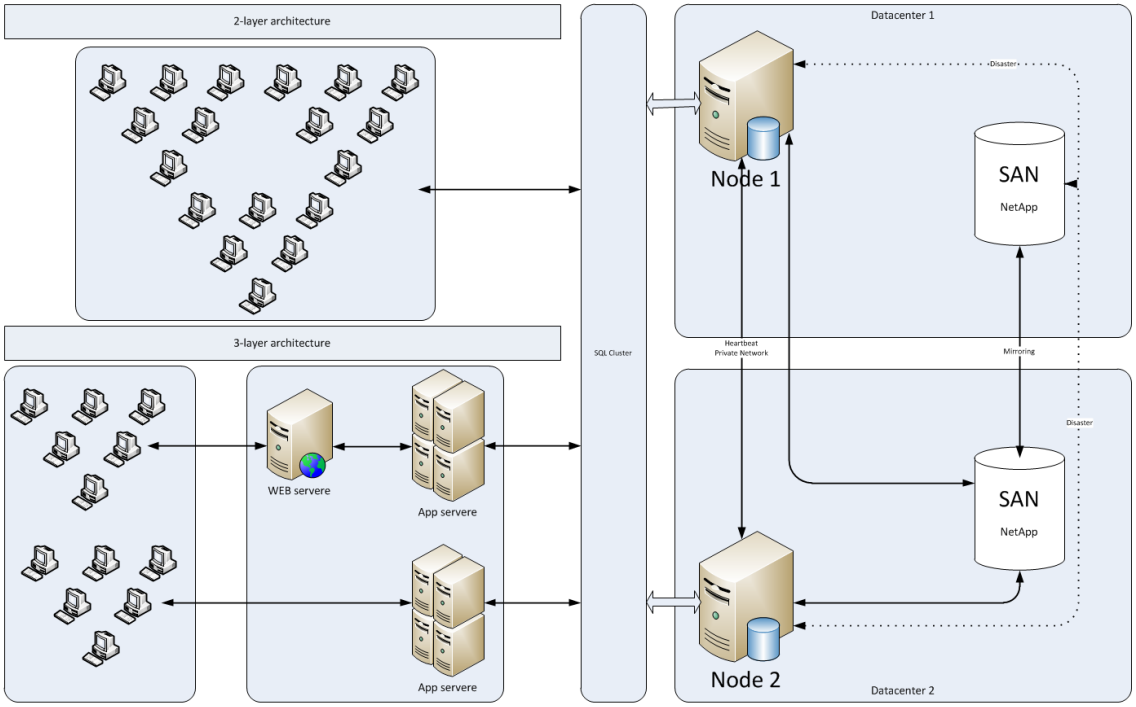


Figure 4 Usage example of Mid-Range SAN

5 Application integration

Helse Midt-Norge offers an enterprise service bus consisting of a Microsoft BizTalk 2022 CU5. The service provides both internal and external integrations.

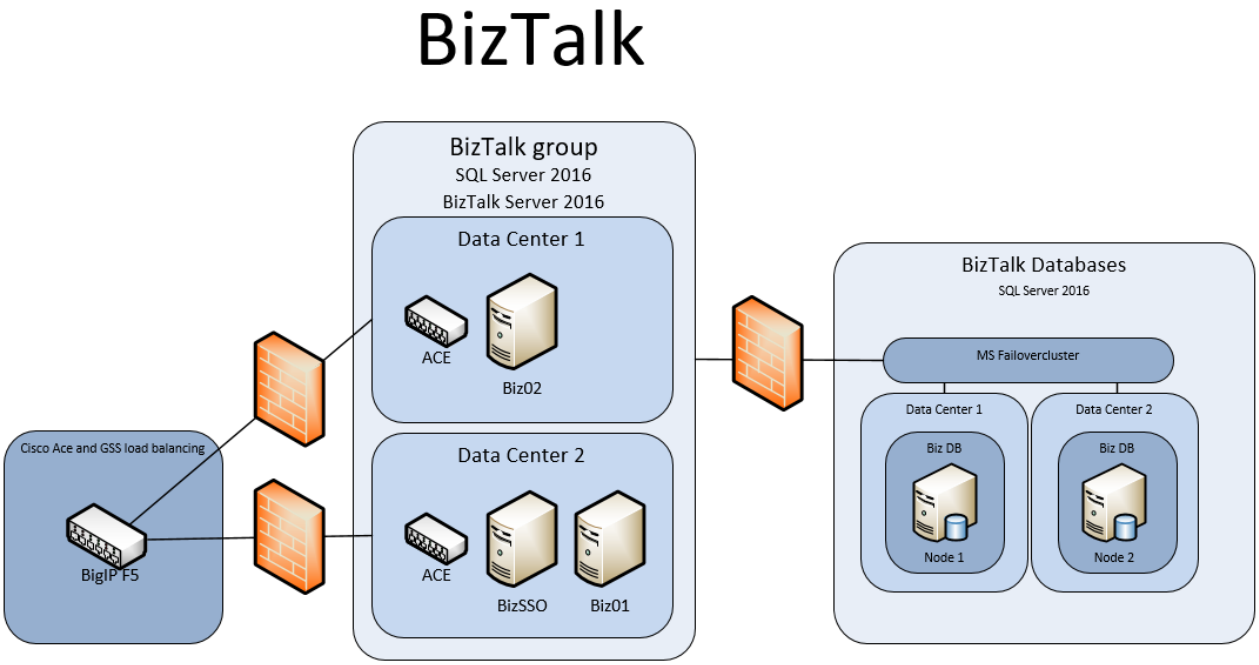
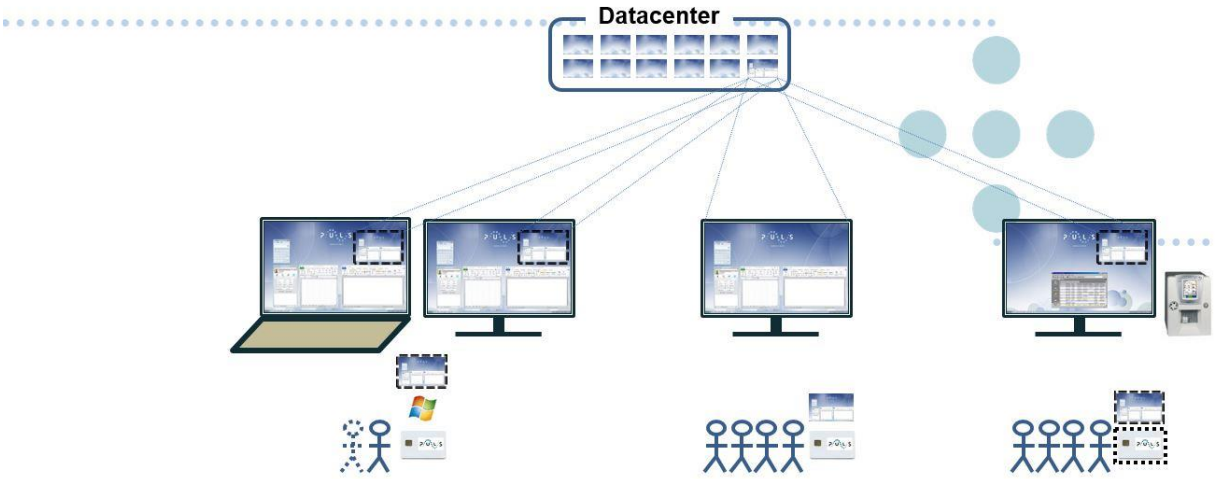


Figure 5 Overview of BizTalk

6 Clients

There are defined three different types of clients:

- Puls Standard
    - Standard Windows 10 and 11 client intended for regular clinical and administrative use, where the users logs on using a personal smart card. These types of clients are typically used where there are only one or two users sharing a computer, for example in an office.
- Puls Spesial
    - Standard Windows 10 and 11 client with automatic system user logon at startup. Intended for special use cases like interface clients connecting to analysis instruments or applications with special software or hardware requirements.
- Puls Sprint
    - Locked down Windows 10 and 11 installation, used as thin client endpoints for the Virtual Desktop Infrastructure (VDI). These clients are typically used where there are multiple users sharing the computer, for example in the clinics and wards. Users logs on and reconnects using a personal smart card and disconnects from the session when the smart card is removed.
- Ekstern Puls
    - Virtual desktop accessible from internet. User can log on to this desktop from other clients over internet, e.g., private PC’s.



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

Table 1 Types of PC clients

The Virtual Desktop Infrastructure is built on Omnissa (formerly VMware) Horizon View and is scaled for 6,000 concurrent users. VDIs are mainly used by clinical users with the need to log on to multiple computers on multiple locations during a workday. By disconnecting and reconnecting to the virtual desktops they save time and get to keep their session when they move from computer to computer.

Desktop pools are floating linked clones that refreshes once a week. Golden image is a Windows 10 and 11 installation, with a minimum set of basic applications and middleware installed, and best practice tuning for running in a VDI environment.

Laptops use standard a local user profile and have enabled functionality for offline sync of documents and email. Remote access from a laptop to internal networks in Helse Midt-Norge is provided by Microsoft Direct Access.

Clients are running System Center Endpoint Protection and the local Windows Firewall is enabled, centrally managed via Group Policy Objects (GPO). Patching and updates done according to Microsoft best practice recommendations to enhance security and stable operation. PC clients are patched monthly and virtual clients once every third month.

6.1 Client hardware

Helse Midt-Norge has a standardized client platform based on Windows 10 x64 and 11 x64, where approximately 30% are laptops and 70% are desktops, around 25,000 physical clients in total. The hardware lifecycle for PCs is 5-7 years.

Helse Midt-Norge offers handheld clients. The main platform offered are Apple iPhone and Myco 3. We also support Apple iPads and devices from Zebra android-devices. By January 2025 there are about 10,000 mobile devices deployed in Helse Midt-Norge.

6.2 Client software

The centrally managed clients are based on a Microsoft SCCM distributed client image and Active Directory GPO configuration.

The default PC image contains standard Microsoft products like Microsoft M365 or Microsoft Office 2016 and a set of standard utility tools. Helse Midt-Norge uses Microsoft Edge as the default web browser.

6.3 Client software distribution

Applications are distributed to computers and users either as a thick installed application or virtualized with Microsoft App-V. Software packages are streamed from a distributed file system where a local copy of all packages are stored for all hospitals.

Security groups in Active directory grants users' access to applications and builds machine collections for distribution in SCCM.

The goal is to App-V virtualize as many applications as possible. Microsoft SCCM distributes and installs applications that are not App-V virtualized.

6.4 Email client

Helse Midt-Norge uses Microsoft M365 and Microsoft Outlook 2016 as their email clients.

6.5 Client antivirus

Helse Midt-Norge currently uses Microsoft Defender Endpoint Protection as antivirus on client PCs.

7 Client workspace

Ivanti (formerly RES) Workspace Manager handles management of user environment and profile data. Application shortcuts, user settings, print- and drive mappings are distributed to the user based on the user and client context at the time of logon or reconnect.

On desktops and virtual clients, a custom created mandatory user profile is used, which is deleted from the client when the users log off. User profile settings are being preserved using Ivanti Workspace Manager and are applied to any client the user logs on to.

7.1 Client user logon

Users log on to a Windows domain and authenticates using a personal certificate stored on a smartcard. Applications authenticate users in different ways:

- Application defined username and password
- AD defined username and password
- Integrated authentication provides Single Sign On

7.2 User Accounts

Every user is allocated a unique user object in Active Directory. Applications which do not support Active Directory must handle authentication internally.

Users who need elevated authorizations will be allocated a separate user object in AD in addition to their regular user. This administrative user will receive the extended authorizations.