Kundens IT miljø - Region Midtjylland

af Peder Thorsø Lauridsen, it-arkitekt, Arkitektur og Design. Revideret 16. maj 2011.

Overordnet beskrivelse af it-installationen i RM - OneRM

Al it drift i Region Midtjylland er besluttet samlet i en central organisation, der fungerer som it-leverandør for alle institutioner og funktioner under Region Midtjylland.

Fysisk samles it-drift i tre driftscentre - placeret i Horsens, Århus og Holstebro - således konsolideres hidtidige installationer på regionens institutioner centralt i moderne driftsmiljøer. Denne sammenlægning er ikke endeligt gennemført og forventes at løbe over mindst 2-3 år. Dette betyder at der fortsat er selvstændige installationer på en del af regionens institutioner uden tilknytning til det overordnede AD.

Der er indført tværgående it-systemer som post/kalender, EPJ, røntgenarkiv, sagsstyring, økonomi etc., ligesom der er indført et fælles “RegionsID” dvs. samordning af brugerID’er og passwords til centrale systemer.

Der er indført standarder for modeller af PC’er, printere, mobiltelefoner etc. gældende for nye indkøb. Der er et vist spænd af maskiner på alder, software versioner etc.

Alle nye systemer der indkøbes og idriftsættes, skal være fungerende i det centrale miljø og levere services til klienter på tværs af de eksisterende AD’er.

Arkitekturprincipper for Region Midtjyllands it-installation

Region Midtjylland sigter mod en systemarkitektur der kan bidrage til at realisere følgende mål:

- Sikker drift. Service skal kunne leveres, til rette tid på det rette sted i det rette omfang.
- Standardisering. Der anvendes åbne standarder i videst muligt omfang. Det tilstræbes at data kan anvendes på tværs af systemer. Det tilstræbes at data som f.eks. brugeroplysninger, CPR-register data hentes fra regionens fælles ressourcer. Målet bidrager til at undgå redundante inkonsistente data. Standardisering medvirker til at understøtte interoperabilitet mellem systemer.
- Skalerbarhed. Systemer skal kunne udvides i det omfang det kræves for at imødegå krav til større volumen i produktionen.
- Holdbarhed. Der bygges modeller, hvor data, forretningslogik og præsentation kan fungere uafhængigt og derved bevares i en form der fremtidssikrer adgangen til data.

Region Midtjylland tager udgangspunkt i ITIL ved opbygning af strukturer og processer i IT organisationen. Principper og terminologi fra ITIL kan derfor med fordel anvendes i forbindelse med beskrivelse dokumentation og design af systemet, samt opbygning af processer til udvikling, drift og vedligeholdelse af systemet.

Interoperabilitet

Interoperabilitet (populært at komponenter og delsystemer i arkitekturen kan 'snakke sammen') er en afgørende forudsætning realiseringen af den serviceorienterede systemarkitektur og for realiseringen af en række af de ovenfor anførte målsætninger.

Kravet om interoperabilitet indebærer en forudsætning om:

- At der på 'forretningssiden' findes åbne, dokumenterede datamodeller (datadefinitioner med definition af i hvilken kontekst data anvendes) og åbne, dokumenterede snitflader og protokoller for anvendelse/kommunikation af data.
- At der på den tekniske side tilsvarende findes åbne, dokumenterede definitioner af hvorledes komponenter i leverancens tekniske platform (middlewarelag og driftsplatform) interagerer defineret i form af standarder.

En åben standard er således en standard, der er dokumenteret (i tilstrækkelig detalje), frit tilgængelig (gratis) og forbliver frit tilgængelig.

En vigtig skelnen går mellem 'proprietære' standarder (har en ejer med mulighed for begrænsninger i standardens anvendelse), 'de facto' standarder (dominerende standarder uden at være offentligt vedtagne) og 'de jure' (offentlige) standarder (vedtaget af offentlige (danske eller internationale) standardiserings organer).

Region Midtjylland sigter, medmindre andre forhold taler imod, mod at anvende 'de jure'

standarder, og sekundært mod at anvende 'de facto' standarder med tilstrækkelig grad af åbenhed.

Målsætningen om anvendelse af åbne standarder, åbne snitflader og åbne datamodeller er en afgørende forudsætning for interoperabilitetskravet og dermed for realiseringen af en serviceorienteret systemarkitektur.

Anvendelse af åbne standarder, åbne snitflader og åbne datamodeller er endvidere afgørende for at kunne opnå større leverandøruafhængighed og realisere en flerleverandør strategi, for investeringens levedygtighed, samt for mulighederne for en fortsat videreudvikling og udbygning af systemløsningen i takt med ændrede behov og nye muligheder.

Overholdelse af fællesoffentlige standarder og anbefalinger

Region Midtjyllande ønsker at følge de fællesoffentlige anbefalinger videst muligt under hensyntagen til forvaltningsmæssige/forretningsmæssige krav.

Driftcenter opbygning

Region Midtjyllands it-installation er bygget op omkring tre driftscentre, der indbyrdes er forbundet med hurtige netværksforbindelser. Det er moderne driftscentre med central nødstrøm, køling, adgangskontrol og brandsikring/alarmering.

Fakta og krav vedr. servere:

- Primær serverdrift afvikles på Microsoft Windows på virtuelle servere i VMware. Server operativsystemer fra Microsoft installeres og vedligeholdes på en standardiseret måde og overvåges fra central side med værktøjer fra IBM og Microsoft.
- Servere er installeret med antivirus programmel fra McAffee.
- Der anvendes SAN og NAS til alle storage formål. EMC er primær leverandør af storagesystemer.
- Der er etableret fælles database server clustre baseret på MS-SQL og Oracle - disse skal anvendes til database afvikling for alle installationer.
- Der må ikke kræves fysiske tilknytninger til serverne - fx. licens dongles, da afviklingen af serverne flyttes mellem fysiske servere for sikring af driftsafviklingen.
- Der er centraliseret backup system baseret på Tivoli Storage Manager fra IBM.
- Der afvikles desuden drift på platforme fra IBM (AIX) og Oracle (Solaris) med tilhørende storagesystemer.

Eksisterende decentrale installationer på institutioner

Klienter, model for afvikling og installation af applikationer

Klienter er primært baseret på hardware fra Lenovo og kører Microsoft Windows XP SP2 og SP3. Der anvendes pt. Internet Explorer i versionerne 6 og 7. Der kan tilbydes alternative browsere som Mozilla Firefox og Google Chrome hvis der er behov for høj hastighed/ overholdelse af standarder.

Fakta og krav vedr. klienter:

- Klienter modtager IP adresse og netværkskonfiguration via DHCP
- Navne på servere opløses via DNS
- Brugere har ikke lokal administrator rettigheder
- Maskiner er tilmeldt AD og modtager politikker og rettigheder herfra
- Klient maskiner er ikke nødvendigvis i samme AD som centrale servere!
- Software afvikles primært via Citrix XenApp platformen, sekundært ved lokal installation
- Al klient programmel skal kunne scriptinstalleres silent via CAPA CMS værktøj
- Der må ikke kræves manuelle routiner ved installation - fx. licenser/aktivering mv.
- Der må ikke anvendes hardware licensdongles og licenser skal kunne styres centralt og automatisk.

BSK - brugerstyring og validering

Region Midtjyllands BrugerStamdataKatalog (BSK) har to primære funktioner:

- Vedligehold af stamdata om personer ansat i Region Midtjylland herunder deres adgang til ressourcer, jobfunktioner, ansættelser og rollestyring
- Validering brugernavn og password for brugere med RegionsID.

BSK er bygget på Novells Identity and Access Management platform. Det stiller en bred vifte af integrationsmetoder til rådighed for tilknyttede systemer, men fra It-udvikling, arkitektur og designs side anbefales det at de metoder der anvendes er i overensstemmelse med de principper for integration, der er beskrevet i dette dokument.

Metoderne er prioriterede for at understøtte de klienter og systemer, der oftest anvendes i Region Midtjylland.

Funktioner

Alle personer, der har et ansættelseslignende hos Region Midtjylland kan oprettes i BSK. En bruger der oprettes i BSK registreres med CPR-nummer og tildeles et unikt RegionsID.

Vedligehold af stamdata

I BSK opbevares en lang række oplysninger om ansatte, der enten er personlige data eller data der knytter sig personens ansættelser. Til disse data knyttes oplysninger om adgang til ressourcer, roller og rettigheder. Alle disse data kan ved integration bringes til anvendelse i eksterne systemer.

Validering af brugernavn og password

I BSK findes en flere metoder til direkte validering af brugernavn og password. Primært anvendes LDAP eller BSK's authentication webservice. Derudover er bruger i BSK repræsenteret med samme brugernavn og password i OneRM Active Directory der giver mulighed at anvende Microsofts standard metoder til validering af brugere.

Integrationer

De mulige scenarier for integration af BSK data i eksterne systemer er mangfoldige. De følgende fire metoder er dem der anbefales. Rækkefølgen er prioriteret for systemer, der kan anvende flere af metoderne. For hver metode opstilles en liste med nogle af de systemer der anvende metoden.

1. Validering bruger og dennes tilhørsforhold og roller direkte mod Active Directory
    a. Outlook
    b. Filsystemer
    c. ProNestor
2. LDAP eller webservice Integration direkte til BSK
    a. CIC (Digital Signatur klient til PC og Citrix)

b. Sygesikringen
c. Patologi
d. CPR opslag

3. Synkronisering af stamdata til integreret system og validering mod BSK eller Active Directory
    a. EPJ
    b. ESDH
    c. Synkronisering af stamdata inklusivt brugernavn og password til integreret system
    d. eDok
    e. ØS

Sikkerhedsmodel og funktionsopdeling

Systemet skal leve op til danske (og internationale) standarder for sikkerhed og overholde krav til sikkerhed og adgangskontrol i standarder på sundhedsområdet.

- Systemet skal overholde gældende "Lov om behandling af personoplysninger", "Sundhedsloven", samt overholde Region Midtjyllands informationssikkerhedspolitik. Dette bør ske i overensstemmelse med DS484:2005 afsnit 15 ”Overensstemmelse med lovbestemte og kontraktlige krav”. Derudover skal systemet overholde gældende regler indenfor dette område som foreskrevet i Danmark og EU. Herunder især håndtering af logning vedr. brugeradgang til person-henførbare oplysninger.
- IT-sikkerheden for den samlede løsning skal være i overensstemmelse med DS 484:2005 Standard for informationssikkerhed.
- Logdata være tilgængelig for Region Midtjylland.

Brugerrettigheder skal tildeles som roller i enten AD grupper eller via BSK.