EXAMENSARBETE
våren 2015

Sektionen för hälsa och samhälle
Programområdet för datavetenskap
IT-drifttekniker programmet

Apple OS X i AD-miljö

Möjligheter och begränsningar

Författare
Henrik Kristoffersson
Victor Månsson

Examinator
Fredrik Jönsson

Högskolan Kristianstad | www.hkr.se

Dokumentblad

Högskolan Kristianstad
291 88 KRISTIANSTAD

Författare, program och år

Henrik Kristoffersson, IT-driftteknikerprogrammet 2013
Victor Månsson, IT-driftteknikerprogrammet 2013

Handledare

Martin Nilsson, teknisk utbildare, HKR

Examinator

Fredrik Jönsson, universitetslektor i datavetenskap och teknik, HKR

Examen

Detta examensarbete på 7,5 högskolepoäng ingår i examenskraven för *Högskoleexamen i System Management*.

Titel

Apple OS X i AD-miljö – Möjligheter och begränsningar

Språk

Svenska

Godkännande

Detta examensarbete är godkänt av ovan nämnda examinator 2015-03-31.

Sammanfattning

Apples datorer med operativsystemet OS X blir allt vanligare på arbetsplatserna. För att företagets IT-avdelning ska kunna upprätthålla en stabil och säker miljö strävar man efter att standardisera system och hårdvara. Verkligheten stämmer inte alltid överens med IT-avdelningens strävan och anställda vill i ökande grad använda sig av produkter de valt själva. Arbetet har undersökt möjligheterna och begränsningarna med att integrera Apple OS X i Microsofts Active Directory.

För att kunna besvara de frågor som använts som avgränsning inleddes arbetet med att metodiskt studera litteratur och på internet publicerade artiklar. Därefter har laborationer med och utan tredjepartsmjukvarorna ADmitMac och Centrify genomförts med inriktning på arbetets avgränsningar. Parallellt med detta har intervjuer av organisationer med olika bakgrund genomförts.

Intervjuer och laborationer gav ett resultat som sedan diskuterades i rapportens avslutande del. I analysen gjordes en jämförelse av resultaten från intervjuer samt laborationer. Från detta kunde bland annat följande slutsats dras; För att integrera en dator med Apple OS X i Active Directory fungerar det inbyggda stödet men med begränsad funktionalitet. Med hjälp av tredjepartsmjukvaror utökas stödet och fler funktioner i Active Directory kan användas.

Innehållsförteckning

1 Introduktion

1.1 Bakgrund

Apples datorer med operativsystemet OS X blir allt vanligare i hemmen men också på arbetsplatserna [1]. För att företagets IT-avdelning ska kunna upprätthålla en stabil och säker miljö strävar man efter att standardisera system och hårdvara och till sin hjälp tar man ofta Microsofts Windows Server. Verkligheten stämmer inte alltid överens med IT-avdelningens strävan och anställda vill i ökande grad använda sig av Apples produkter även på arbetet [2]. Mellan de båda operativsystemen saknas fullständig kompabilitet och detta skapar problem för företagen som inte får samma kontroll över sina datorer i form av t.ex. policys och rättigheter. Examensarbetet kommer undersöka möjligheterna och begränsningarna med att integrera Apple OS X i Microsofts Active Directory[1].

1.2 Målsättning och syfte

I vårt arbete vill vi få svar på följande frågor:

- Vilka möjligheter finns att ansluta Apples datorer till en Active Directory-miljö (AD)?
- Vad krävs från klient respektive server?
- Vilka utmaningar står IT-avdelningen inför?

1.3 Metodik

Det inledande skedet av arbetet fokuserades på inhämtning av information via litteratur och på internet publicerade artiklar. Detta för att få en bild över vilka verktyg och metoder som finns på marknaden idag för att AD-integrera Apple-datorer. Därefter kontaktades organisationer som implementerat eller har kompetens kring Apple OS X i AD-miljö. I samband med detta genomfördes två intervjuer. Efter intervjuerna gjordes en sammanställning och analys av resultatet. Parallellt genomfördes laborationer baserat på avgränsningar i avsnitt 1.4.

[1] Active Directory är en katalogtjänst som samlar information om objekt t.ex. skrivare, fillagring och användare.

1.4 Avgränsningar

Arbetet avgränsas till att omfatta följande tjänster i AD:

- Active Directory Domain Services – används bl.a. till att autentisera och auktorisera användare och datorer inom domänen.
- Group Policy – reglerar behörigheter, rättigheter samt inställningar för användare och datorer.
- Nätverkslagring – på nätverket utdelad lagring via olika protokoll och tjänster t.ex. SMB-share och DFS Namespace

Avgränsningarna är gjorda på grund av sina centrala roller i en Active Directory-miljö. Användarhantering och Group Policy då de är några av grundanledningarna till användandet av AD. Nätverkslagring för att undersöka vilka möjligheter Apple-datorer har att nå gemensam lagringsyta.

1.5 Arbetets innehåll i korthet

Det utredande kapitlet ger läsaren grundläggande information och historia om relationen mellan Microsoft och Apple, katalogtjänsten Active Directory, Group Policy, nätverkslagring samt operativsystemet Apple OS X. Informationen ges för att introducera eller repetera områden som är centrala för avsnitten med intervjuer och framförallt laborationerna.

I genomförandekapitlet redovisas först sammanställning av intervjuerna med resultatet i direkt anslutning. Därefter följer redogörelse för genomförda laborationer samt de resultat som uppnåtts.

Diskussionsavsnittet knyter samman resultatet av arbetet och läsaren får ta del av författarnas analyser och slutsatser. Kapitlet avslutas med en sammanställning av förslag till fortsatt arbete med intressanta sidospår och ämnen som går utanför arbetets avgränsningar.

2 Utredning

2.1 Microsoft och Apple – nu och då

Apple OS X och Microsoft Windows är ursprungligen utvecklade ur helt olika filosofier. Som exempel kan nämnas att Microsoft jobbat med att licensiera sitt operativsystem till olika dator-tillverkare medan Apple slagit vakt om sin idé med att leverera en helhet där operativsystem och hårdvara skapats för varandra. Båda filosofierna har sina för- och nackdelar men ur ett historiskt perspektiv har Microsoft varit mer lyckosamma med sin licensieringsmodell vilket gett dem en position som marknadsledande.

Under 1990-talet var skillnaderna mellan systemen stora vilket försvårade för organisationer att använda båda systemen i samma nätverk. Apple använde sig t.ex. av ett annat nätverksprotokoll: AppleTalk, jämfört med Microsoft som redan då använde dagens standard: TCP/IP. I tabell 2.1 påvisas några fler historiska skillnader mellan systemen [3].

	Apple	**Microsoft**
Nätverksprotokoll	AppleTalk	TCP/IP
OS-kärna	Sluten källkod / UNIX	MS-DOS
Systemarkitektur	Power-PC	X86

Tabell 2.1 – Historiska differenser mellan Apple och Microsoft

I och med releasen av Mac OS X Snow Leopard 2009 upphörde supporten för AppleTalk [4]. Övergången till TCP/IP skedde dock långt tidigare. Sedan mitten av 2000-talet har Apple genomfört ett par radikala förändringar vilket medfört ökad möjlighet till integration med andra system. Den största skillnaden var övergången till Intel-baserad systemarkitektur 2006 [5]. Förändringen till TCP/IP och Intel-arkitektur gjorde att man i releasen av Mac OS X 10.5 ”Leopard” 2007 kunde införa visst stöd för AD-integration direkt i operativsystemet. [3].

2.2 Presentation av miljö och tjänster

I detta kapitel ges en kort introduktion till de produkter och tjänster som avgränsar detta arbete. Vidare presenteras operativsystemet Apple OS X.

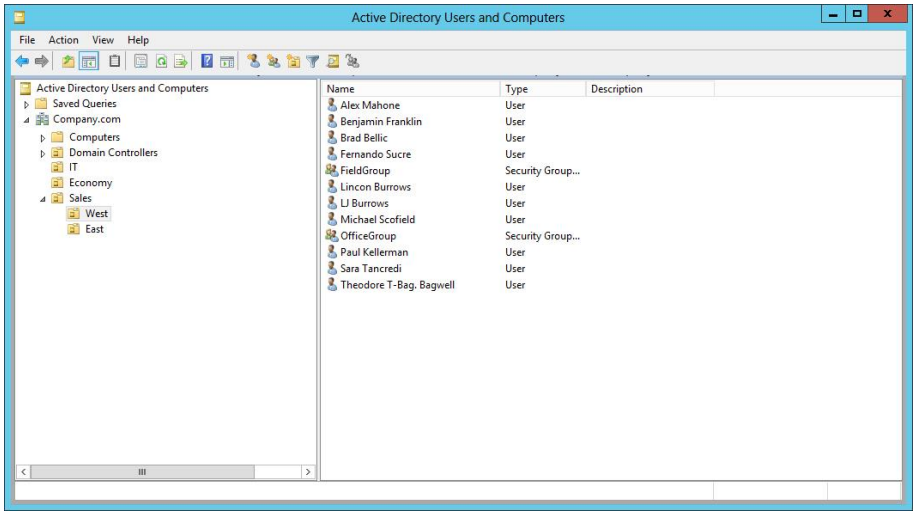
2.2.1 Vad är en katalogtjänst?

En katalogtjänst centraliserar och hanterar lagringen av bland annat användare, datorer och tjänster anslutna till ett nätverk. Man kan med tjänsten styra rättigheter för användandet av resurser som är gemensamma för nätverket t.ex. skrivare och utdelade mappar [6].

2.2.2 Active Directory Domain Services

Active Directory är en katalogtjänst från Microsoft som introducerades med Windows 2000 Server. Med hjälp av Active Directory kan man hantera autentisering och rättigheter för objekt[2] inom domänen. Detta görs enligt *best practice*[3] genom gruppindelning av objekt. Därefter appliceras rättigheter på gruppnivå istället för på ett enskilt objekt. Vid autentisering använder sig Active Directory av Kerberos[4]. Domänen är den yttersta gränsen som avgränsar den hierarki som byggts upp. Det finns undantag från detta men det behandlas inte i detta arbete [6].

Figur 2.1 – ADUC Domänstruktur



[2] Ett objekt kan t.ex. vara en dator eller en användare.
[3] Av tillverkaren rekommenderad arbetsmetod.
[4] Kerberos är ett nätverksprotokoll för säker autentisering mellan klient och server eller mellan servrar [7].

2.2.3 Group Policy

Group Policy Management Console är ett verktyg för hantering av operativsystems-inställningar för datorer och användare. I verktyget skapas ett Group Policy Object (GPO) som sedan kan länkas till en grupp eller organisatorisk enhet (OU). Med hjälp av GPO:er kan man standardisera och kontrollera sin miljö för att underlätta genom ett generiskt användargränssnitt. Man kan också erbjuda administratörer möjligheter att optimera systemanvändandet ur ett säkerhets- och resursperspektiv [6].

2.2.4 Nätverkslagring

Genom användandet av centraliserad lagring kan användare spara och komma åt sina filer oberoende av vilken dator man arbetar från. Det ger också säkerhetsfördelar genom att information inte finns lokalt på t.ex. en bärbar dator som kan försvinna. Sköts lagringen av filer centralt innebär det också att backup underlättas då den bara sker från ett ställe. I takt med att lagringsbehoven ökar är det också lättare och mer kostnadseffektivt att utöka den centrala lagringen. Med hjälp av nätverkslagring erbjuds administratörer kontroll över vem som sparar vad och vem som får åtkomst till lagrad data. Detta innebär större kollaborationsmöjligheter samt möjlighet att skydda känslig data [6]. För att öka kontrollen och tillgängligheten till nätverkslagringen kan man använda Microsofts tjänster File Server Resource Manager (FSRM) och Distributed File System (DFS) [7].

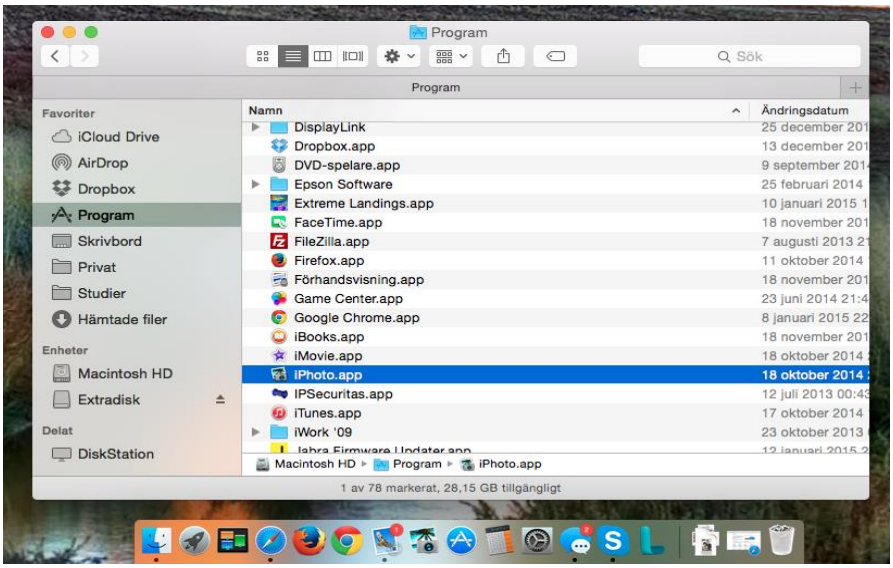
Figur 2.2 – Nätverkslagring [8]

2.2.5 Apple Mac OS X

Apples operativsystem för datorer heter numera OS X, tidigare Mac OS X och släpptes i sin första generation 2001 som Mac OS X 10.0 ”Cheetah” [9].

Den nya familjen, vilken nu var UNIX-baserad, lever kvar än idag och är framme vid version 10.10 ”Yosemite”.

Figur 2.3 - GUI Apple OS X 10.10 “Yosemite”



2.3 AD-integration

Som tidigare nämnts så introducerades visst inbyggt stöd för Active Directory i Mac OS X ”Leopard” (2007). I nuvarande version, OS X 10.10 ”Yosemite” är stödet utvecklat så långt att man direkt i operativsystemet kan ansluta datorn till Active Directory. Därefter kan man logga in på datorn med ett domänanvändarkonto och får då bland annat tillgång till de nätverksresurser som användaren har tilldelats rättigheter till. Administratörer kan välja om användarens unika hemkatalog[5] ska sparas lokalt på datorn eller i Active Directory. Lagras hemkatalogen centralt i AD följer den användaren oberoende av vilken dator man loggar in från. Likt Windows använder sig även Apple OS X av Kerberos vid autentisering. Detta innebär att en domänanvändare vid inloggning kan auktoriseras för flera tjänster utan att separat behöva logga in till dessa, så kallad Single Sign-on. Användandet av Kerberos innebär också att administratörer kan styra lösenordskrav på längd och komplexitet för användare i AD. För att kunna utnyttja fler Active Directory-funktioner till Apple OS X finns tredjepartsverktyg tillgängliga [10].

[5] Hemkatalogen är den mapp där den enskilde användarens skrivbord, dokument, favoriter och inställningar m.m. sparas [19]

2.3.1 Thursby ADmitMac

Ett populärt verktyg som rekommenderas av Apple är Thursbys ADmitMAC. [10] Detta tredjepartsverktyg installeras direkt på klientsidan utan någon extra konfiguration eller installation på serversidan. Med hjälp av verktyget får man ett ökat stöd för vissa funktioner i AD. Apple OS X kan idag inte tolka de GPO:er som levereras av Microsofts AD, men med hjälp av verktyget ADmitMAC kan OS X läsa in Mac-specifika GPO:er som skapats från Microsofts Group Policy Management Console. Detta sker helt utan förändringar av AD-schemat. Vidare ger ADmitMac fullt stöd för bland annat SMB och DFS [11].

2.3.2 Centrify User Suite, Mac edition

Genom Centrifys lösning för att integrera OS X i Active Directory får administratörer möjlighet att hantera Macdatorer utan att det innebär nya gränssnitt att arbeta i. Verktyget använder Windows egna program Group Policy Management Console för att hantera GPO:er. Centrifys egna policies importeras hit för att begränsa Mac-specifika funktioner som t.ex. dockan[6] och begränsningar för Mac App-store. Centrify User Suite, Mac edition, ger också stöd för automatiserad certifikathantering och stöd för Smart Card. Genom att använda befintlig kunskap hos administratörer och befintlig infrastruktur kan man effektivisera administrationen och därigenom spara pengar [12].

2.3.3 Beyondtrust Powerbroker Identity Services ”AD Bridge”

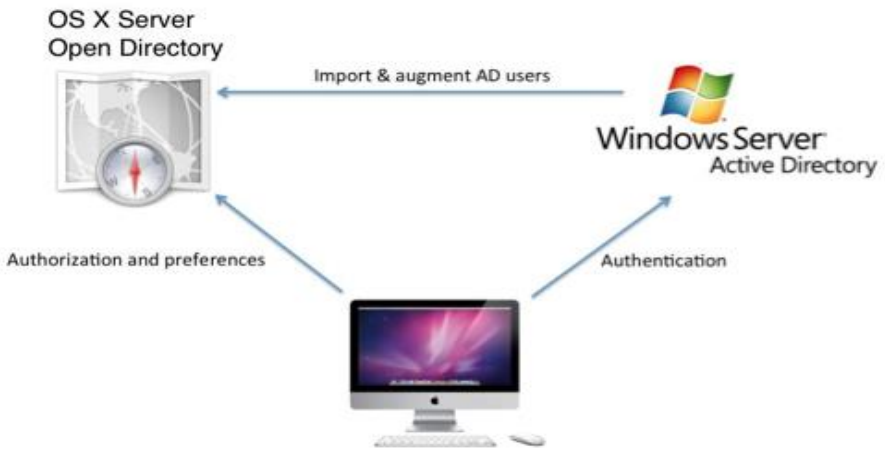
Beyondtrust erbjuder två versioner av sin mjukvara, den fria versionen är öppen källkod vilket innebär att man kan själv modifiera mjukvaran efter behov. I sitt grundläggande utförande erbjuder mjukvaran möjlighet att autentisera användare mot AD från plattformarna UNIX, Linux och Mac. Tidigare gick denna fria mjukvara under namnet Likewise Open [13]. Betalversionen erbjuder utöver den fria versionen även funktioner för hantering av klienter via Group Policy. Denna version använder Windows egna GPO:er men tillför även unika GPO:er anpassade för respektive plattform [14].

[6] Ikonrad på skrivbordet för snabb åtkomst till applikationer och filer.

2.3.4 Mac OS X Server

Vid integration av Apple OS X i en Microsoft AD-miljö finns framförallt två vägar att gå om man vill använda sig av GPO:er. Den ena vägen är genom tredjepartsverktyg som nämnts i tidigare avsnitt och den andra är genom Apples OS X Server med katalogtjänsten Open Directory [15]. Genom att använda sig av Apple och Microsofts katalogtjänster tillsammans kan man skapa något som kallas ”Magic Triangle”. Principen innebär att autentiseringen från OS X-klienten sker mot AD, medan auktorisering till nätverksresurser sker genom Open Directory. Användarkontot hanteras i AD och kan logga in på samtliga maskiner oberoende av operativsystem, medan datorn med OS X hanteras genom Open Directory [16] [10]. Från OS X Servern kan regler (Preferences) levereras genom Apples Profilhanterare. Reglerna kan vara allt från hur miljön ska se ut till inställningar samt vilka resurser som ska användas. Profilhanteraren erbjuder även möjlighet att distribuera program och uppdateringar till OS X-klienter [17].

Figur 2.4 – Magic Triangle [16]



3 Genomförande

3.1 Allmänt om genomförande

Verktygen för detta avsnitt består av intervjuer och laborationer, de utfördes med intention att besvara frågorna som ställdes i kapitel 1.2:

- Vilka möjligheter finns att ansluta Apples datorer till en Active Directory-miljö (AD)?
- Vad krävs från klient- respektive server?
- Vilka utmaningar står IT-avdelningen inför?

Intervjuobjekten bestod av en IT-avdelning inom en statlig myndighet och ett privat konsultföretag, detta för att få svar ur olika synvinklar.

Laborationerna avgränsade sig till att kontrollera funktionalitet för:

- Active Directory Domain Services
- Group Policy
- Nätverkslagring t.ex. SMB-share och DFS Namespace

Funktionaliteten har utvärderats med och utan tredjepartsmjukvara. Respektive mjukvara presenteras i kapitel 2.3.1 samt 2.3.2. Då tillgång till Apple OS X server saknades kunde ingen laboration utföras för att undersöka Magic Triangle, begreppet introduceras i kapitel 2.3.4

I detta kapitel redovisas först sammanställning av intervjuerna direkt följt av resultatet. Därefter följer redogörelse för genomförda laborationer samt de resultat som uppnåtts.

3.2 Intervjuer

3.2.1 Intervju med IT-chef Matts Behrens

Högskolan i Kristianstad har ca 15000 studenter, 48 program och 400 kurser, allt samlat på samma campus [18]. IT-avdelningen hanterar ca 1000 klienter med tillhörande mjukvaror samt serverinfrastruktur.

På Högskolan i Kristianstad (HKR) har man alltid haft en viss del Mac-datorer, just nu utgör Mac-datorer ca 5% av det totala antalet klienter men det är först de senaste två åren som man i mindre skala börjat integrera dem

i AD-miljön. Personal inom den akademiska sfären förväntar sig, och tillåts få, en större grad av frihet i valet av arbetsdator. Tidigare har varje institution själva köpt in sin IT-utrustning och sen var det IT-avdelningens uppgift att få det att fungera. Numera är alla IT-inköp centraliserade till HKR IT. Detta innebär inte att HKR-IT bestämmer vad som ska köpas in men ges möjlighet att se till att inköpet sker på för myndigheten legal väg.

HKR är statligt och lyder därför under lagen om offentlig upphandling (LOU) detta innebär också att det inte som tidigare går att ”köpa datorer på stan” utan att HKR måste verka för fri konkurrens och upphandla utrustning. Numera har man kunnat standardisera och centralisera IT vilket för användarna medfört att det vid nyanställningar på högskolan automatiskt levereras en ”personaldator”, färdigkonfigurerad och klar att användas.

IT-chef Matts Behrens ser inte Mac-integration som en teknisk fråga, snarare en ekonomisk eller strategisk fråga. Detta förklarar Matts beror på de lagar som HKR ska följa som statlig institution. Man har krav på sig att inventera och dokumentera hårdvara, mjukvara och ta backup på miljön. För varje unikt operativsystem man lägger till i miljön genererar det kostnader både för central hantering och för respektive avdelning samt utbildning av personal. Kostnaden uppgår till, grovt uppskattat, två pedagoger per år. Detta innebär att Mac-integration blir en ekonomisk fråga, är den extra valfriheten värd merkostnaden av två pedagoger per år?

Matts belyser också skillnaderna jämfört med privata företag som inte har samma krav på sig som en statlig institution. Avsaknaden av kostnads-drivande krav, t.ex. juridiska, medför att kostnaderna för att erbjuda ytterligare operativsystem i ett privat företag blir marginella i jämförelse.

3.2.2 Intervju med Christer Persson och André Ekholm, QSi

QSi är ett konsultföretag med många års erfarenhet från den bransch de verkar i. Genom att tillsammans med sina kunder arbeta med de frågeställningar och lösningar som finns i vardagens IT-miljö hos små och stora företag har de blivit det företag de är idag.

Christer menar att det idag är kunden som styr QSi´s utbud genom sina utmaningar och önskemål samt utvecklingen av ”Bring Your Own Device” (BYOD) på olika företag. Från att länge enbart varit en Microsoft-partner har

man på senare tid plockat upp Apples produkter i sitt sortiment efter större efterfrågan från sina kunder. Många av QSi´s kunder sitter i blandmiljöer med både PC och Mac. Majoriteten av företaget använder Windows och enskilda avdelningar t.ex. marknad och reklam använder sig av Apples datorer. André flikar in att Apples utveckling har exploderat med start i iPhone och iPads och fått till följd att många användare önskar arbeta med Apples datorer. Från att tidigare nästan bara använts inom reklam och tryck ser man nu Apples datorer hos allt från banker till sjukhus.

Utifrån sina egna erfarenheter anser Christer att det inte går att fullt ut integrera Macar i AD-miljö. Christer påpekar samtidigt att antalet Macar hos deras kunder inte är så många att det har funnits anledning att titta på mer omfattande lösningar för central hantering av Macar i AD. Idag administrerar man till stor del Mac-datorer manuellt men intåget av molntjänster har medfört att många AD-tjänster minskat i relevans eftersom många funktioner idag återfinns i molnet eller är webbaserade. Christer nämner fillagring som ett exempel genom Microsofts OneDrive och framförallt Sharepoint som båda finns i molntjänsten Office 365.

Eftersom det saknas stöd i Apple OS X för central hantering via t.ex. GPO:er sker mycket administration manuellt på respektive dator och detta är mer tidskrävande. På en PC hade arbetet i stor mån kunnat automatiseras. För Mac-integration används idag mest basala funktioner i AD, såsom autentisering, DNS och DHCP. Man saknar bättre stöd för kontroll av lösenordslängd och komplexitet samt GPO:er för att skjuta ut mjukvaror och inställningar till klienterna.

3.2.3 Resultat intervjuer

Intervjuerna gav en inblick i några av de utmaningar som en IT-avdelning står inför vid AD-integration av Apple OS X. Även om intervjuobjekten skiljde sig åt i storlek, förutsättningar samt antalet Macdatorer som hanteras fanns det likheter i synsätt och erfarenheter. De likheter som uppdagats och återkommit i båda intervjuerna är att stödet hos respektive operativsystem har förbättrats över tid för att underlätta integrationen. På grund av att Apple saknar stöd för många av Active Directorys funktioner är det båda intervjuobjektens erfarenhet att integrationen av Mac i AD kräver mer resurser i form av tid och pengar jämfört med en ren Windows-miljö.

Då Högskolan i Kristianstad är en offentlig verksamhet är man tvingad att följa diverse lagar och förordningar vilket bl.a. medför ansvar för inventering och kontroll av klienter. HKR verkar i en stor PC-miljö med inslag av Apple-datorer och har behövt utreda vilka tekniska möjligheter som finns för central hantering av Apple OS X eller andra operativsystem för den delen. Man har hittat lösningar på detta och ser därför inte längre detta som en teknisk fråga utan som en ekonomisk- eller strategisk fråga.

QSi hanterar även de ett stort antal klienter men uppdelat på många unika kundmiljöer. Detta innebär att andelen Macar i varje miljö är relativt låg och man har därför inte sökt verktyg för mer omfattande central administration. Många uppkomna hinder har kunnat lösas genom användandet av molntjänster såsom Microsofts Office 365. Eftersom QSi inte är en offentlig verksamhet har man inte samma krav på sig att följa specifika lagar som gäller för HKR utan är mer fria att välja lösning efter kundens behov.

3.3 Laborationer

3.3.1 Apple OS X inbyggda stöd för Microsoft Active Directory

Den första laborationen som utfördes utgick från en miljö med en domänkontrollant med Windows Server 2012 samt rollerna ADDS, DNS, DHCP och DFS samt en klient med Apple OS X 10.10 ”Yosemite”. Grundläggande funktionalitetstester utfördes för att utvärdera det inbyggda stödet i OS X för att ansluta datorn till AD. Efter att datorn anslutits till domänen genomfördes test genom att det lokala kontot loggades ut och en domänanvändare användes för att logga in på datorn. Därefter gjordes kontroll på domänkontrollanten så att datorobjektet hade skapats.

Laborationen gick vidare med att skapa en GPO och kontrollera huruvida dess inställningar slog igenom på datorn med Apple OS X som operativsystem. GPO:n innehöll inställningar för skrivbordsbakgrund, skärmsläckare och automatiskt skapande av mapp. Klienten startades om för att kunna läsa in GPO:n men ingen av inställningarna ändrades.

Apple OS X 10.10 har inbyggt stöd för att ansluta till nätverksmappar och detta kontrollerades genom att ansluta till en av domänkontrollanten utdelad mapp. Test gjordes också för att automatiskt mappa upp densamma efter

omstart av datorn. Testet gick bra men kräver handpåläggning på varje Mac dator, stöd för att centralt hantera detta saknas i OS X.

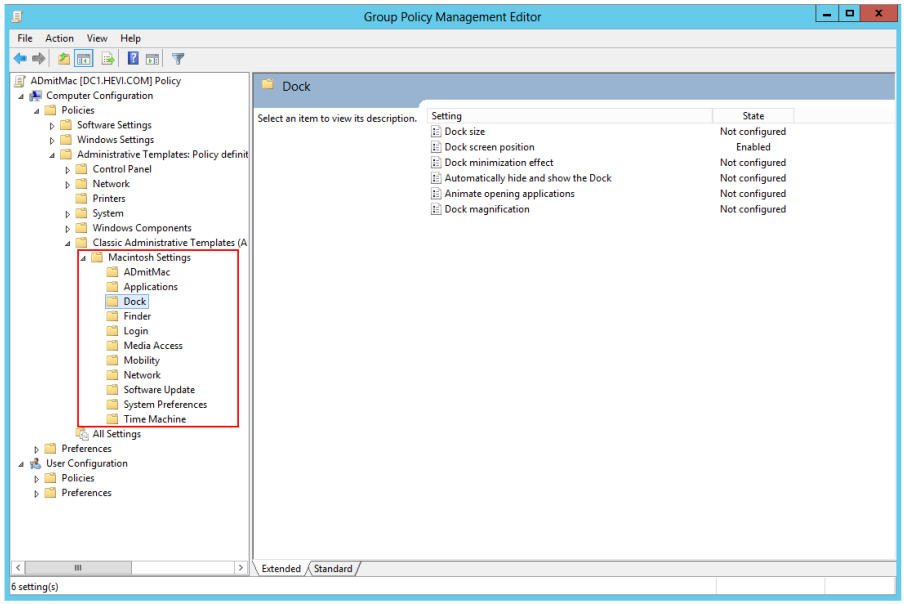
3.3.2 ADmitMac

För laborationen med tredjepartsverktyget ADmitMac installerades och konfigurerades två virtuella maskiner. En domänkontrollant med Windows Server 2012 samt rollerna ADDS, DNS, DHCP och DFS, och en klient med Apple OS X 10.10 ”Yosemite” samt verktyget ADmitMac. I AD skapades vanliga användare som kunde användas som test under laborationens gång. Målet med laborationen var att testa de tre avgränsande punkter som anges i 3.1, dvs. ansluta datorn mot ett AD, Group Policy samt nätverkslagring med SMB och DFS namespace.

Laborationen började med att klientdatorn anslöts till Active Directory genom tredjepartsverktyget ADmitMac. Processen att gå med i domänen var lik Apples inbyggda funktion. Båda alternativen gick ut på att ange vilken domän som skulle anslutas till och därefter autentisera sig med kontouppgifter för en användare som hade rättigheter att gå med i domänen. Utöver detta fanns det i ADmitMac möjlighet att välja vilket datornamn som skulle användas samt vilket OU i AD datorobjektet skulle lagras i.

Efter att klienten var ansluten kunde alternativet att flytta den lokala användarens hemkatalog till AD väljas, i denna laboration valdes inte detta alternativ. Vi loggade ut det lokala administratörskontot från klientdatorn och loggade istället in med ett domänkonto. Genom detta steg kunde vi verifiera att datorn var ansluten mot Active Directory. I verktyget finns där även en inbyggd funktion för att testa så anslutningen mot AD fungerar.

Figur 3.1 - Group Policy Management Editor, ADmitMac



Figur 3.2 - Kontroll GPO

När datorn var med i domänen och inloggad med ett domänkonto skulle Group Policy testas. Detta gjordes från domänkontrollanten. I Group Policy Management Editor adderades OS X-specifika mallar från ADmitMacs installationsmedia.

I dessa Group Policies fanns bland annat inställningar för vilka applikationer som fick köras, hur dockan skulle se ut, om Bluetooth skulle vara aktivt eller inaktivt samt systeminställningar. Några olika ADmitMac Group Policies ändrades samt länkades till ett OU där klientdatorn med OS X fanns. Därefter gjordes en omstart av klientdatorn så att de nya reglerna kunde läsas in. För att visuellt kunna se att reglerna hade slagit, ändrades vart dockan skulle placeras, från nederkant till vänsterkant.

Vidare testades om några Windowsspecifika GPO:er fungerade även på Apple OS X. De som testades var bakgrundsbild och skärmsläckare men ingen av dessa lästes in.

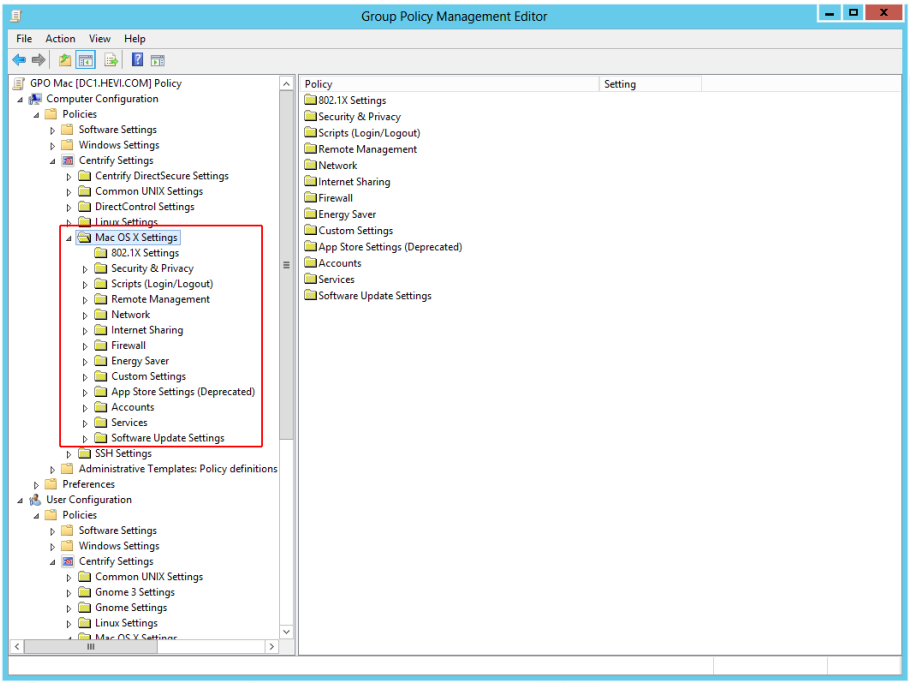
ADmitMac erbjuder i sitt program möjlighet att mappa upp nätverkslagring automatiskt när en användare loggar in. Detta testades genom att det på domänkontrollanten skapades en SMB-share som anslöts till ett DFS namespace. Från klientdatorn och genom ADmitMac verktyg valdes att en specifik nätverksmapp skulle automatiskt mappas upp på skrivbordet när en autentiserad domänanvändare loggade in. En ny domänanvändare som inte tidigare varit inloggad på OS X-klienten loggades därefter in för att kontrollera så att nätverksmappen fanns där.

3.3.3 Centrify User Suite, Mac edition

Likt ADmitMac i avsnitt 3.3.2 startades laborationen med en Microsoft Server 2012 med rollerna ADDS, DNS, DHCP och DFS samt en klient med OS X 10.10 ”Yosemite”. Målet med laborationen var precis som tidigare att testa de tre avgränsande punkter som anges i 3.1, dvs. ansluta datorn mot ett AD, Group Policy samt nätverkslagring med SMB och DFS namespace.

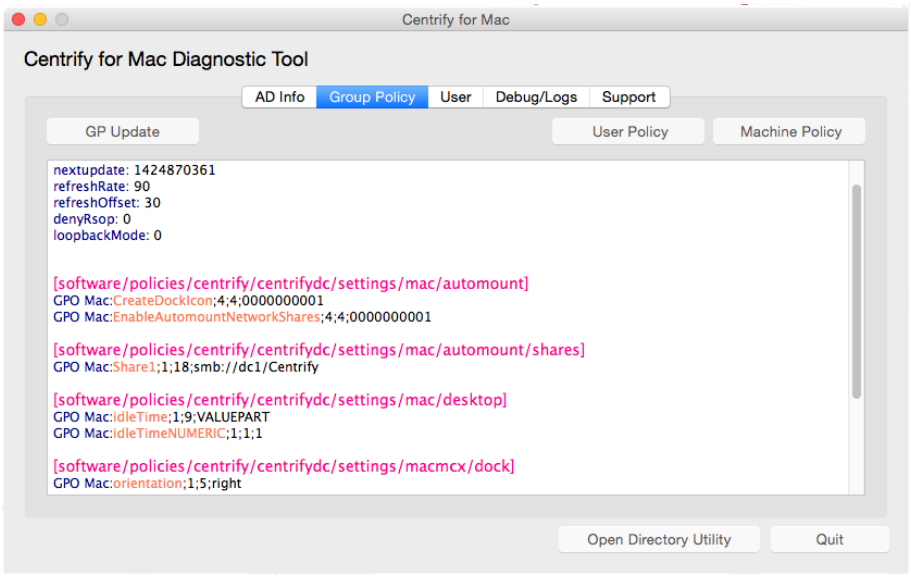
Laborationen inleddes med att Centrifys servermjukvara installerades på domänkontrollanten. Installationsförfarandet var enkelt med några kompletterande installationer t.ex. .Net Framework 3.5. Efter att installationen på servern var klar övergick laborationen till Mac-klienten där kontroll av DHCP, DNS och tid följde. Därefter installerades Centrifys klientmjukvara. Med hjälp av denna anslöts datorobjektet till domänen genom att ange administratörskontots uppgifter samt domänens namn. Det fanns även möjlighet att anpassa vilket OU datorobjektet skulle placeras i. På domänkontrollanten verifierades sedan att klienten anslutits korrekt och placerats i avsett OU. Därefter importerades Centrifys mallar för Apple OS X-specifika GPO:er.

Figur 3.3 Group Policy Management Editor, Centrify



När mallarna var importerade skapades policies för att ändra inloggningsfönstrets utseende med specifik välkomsttext, placering av dockan till höger på skärmen och automatisk uppmappning av en nätverksmapp. Centrify erbjuder två verktyg för att direkt kunna uppdatera GPO på klienten. Dels introduceras kommandot `adgpupdate` som kan köras direkt i OS X Terminal. Centrify har också ett mindre felsökningsprogram: Centrify for Mac Diagnostic Tool. Programmet ger möjlighet till att kontrollera anslutningen till AD men ger framförallt grafisk hjälp för att uppdatera GPO och kontrollera vilka GPO:er som är aktiva på användar- respektive datorobjektet.

Figur 3.4 Centrify for Mac Diagnostic Tool



3.3.4 Resultat laborationer

Efter att ha utfört tre laborationer med och utan tredjepartsverktyg hittades både likheter och skillnader mellan de olika alternativen. Generellt erbjöd tredjepartsverktygen högre funktionalitet.
Processen att ansluta klienten med OS X till AD påminde om varandra och ett av tredjepartsverktygen använde till stor del OS X inbyggda verktyg; Directory Utility, vidare erbjöd tredjepartsverktygen möjlighet att direkt vid anslutning välja vilket OU datorobjektet skulle placeras i.

Apple OS X i sig har inget stöd för Windows GPO:er men kan med hjälp av tredjepartsmjukvara hantera OS X-specifika GPO:er levererade från en domänkontrollant.

Stödet för nätverkslagring är utbyggt i OS X till den grad att man stödjer nätverksprotokollet SMB och kan hantera nätverkslagring publicerad via Windows DFS Namespace. Tillägget av tredjepartsverktyg ger i olika grad större möjligheter till central administration av resurser. För att återkoppla mot de avgränsningar i Active Directory som gjorts för detta arbete, presenteras resultatet av laborationerna i tabell 3.1 nedan.

	Apple OS X	ADmitMac	Centrify
AD-integration	Ja	Ja	Ja
Stöd för Group Policy	Nej	Ja*	Ja*
Anslutning till nätverkslagring	Ja	Ja	Ja
Hantering av nätverkslagring	Manuell handpåläggning per maskin och användare	Manuell handpåläggning per maskin	Central hantering via Group Policy

Tabell 3.1 – Överblick resultat laborationer

* Enbart GPO:er från respektive tredjepartstillverkare.

Apple OS X kan i nuvarande version utan problem autentisera mot Active Directory och domänanvändare kan på så sätt logga in på datorn, detta möjliggör för organisationen att enbart använda centrala konton och slipper därmed att hantera lokala konton. Vill samma organisation använda sig av GPO:er för att centralt hantera Macdatorer låter detta sig inte göras. Eftersom OS X har stöd för SMB och DFS Namespace kan man ange att automatisk anslutning av valda nätverksmappar sker vid inloggning. I OS X benämns detta Login Items. Detta måste göras på varje dator och för varje användare som vill nyttja funktionen.

ADmitMac gav möjlighet att till stor del genomföra de funktioner som arbetet avgränsats till. Mjukvaran installerades på klientsidan och erbjöd hjälp för anslutning till Active Directory. I samband med detta kunde man välja typ av autentisering, till exempel NTLMv2 eller Kerberos samt var i domänens struktur datorobjektet skulle placeras. Verktyget gav möjlighet att centralt distribuera OS X-specifika GPO:er. Detta gjordes genom att på domänkontrollanten importera mallar från ADmitMacs installationsmedia. Exempel på GPO:er som testades och fungerade var:

- Körbara applikationer
- Hantering av dockans utseende och placering
- Inställningar för Finder[7]
- Inställningar för automatisk systemuppdatering och backup

[7] Apple OS X motsvarighet till Windows Utforskaren.

ADmitMac har i sin mjukvara stöd för att automatiskt ansluta till nätverksmappar vid inloggning med en autentiserad användare. Denna inställning kan inte göras centralt eftersom ADmitMacs mjukvara endast installeras på klienten, således måste inställningen göras på varje Apple OS X-klient.

Centrify's user suite, Mac edition, innehöll mjukvara för både server och klientsida. Detta gav möjlighet att fullt ut använda de funktioner som avgränsar detta arbete. Klientmjukvaran användes för att ansluta till Active Directory. Det gavs möjlighet att välja i vilket OU datorobjektet skulle placeras, detta underlättades genom att Centrify's mjukvara redan läst in domänens struktur och kunde presentera den grafiskt.
Då mjukvara även installerades på servern i denna laboration medförde detta att central administration kunde ske i större utsträckning än med ADmitMac. Som exempel kunde en GPO skapas för att automatisk ansluta domänanvändare till nätverksmappar.

4 Diskussion

4.1 Analys av resultat

Är det möjligt att integrera Apples datorer i Active Directory inom de avgränsningar som gjorts för detta examensarbete?

Efter att ha utfört laborationer och intervjuer anser vi det fullt möjligt att genomföra detta. Precis som laborationerna visat finns det grundläggande stöd inbyggt i OS X. Apple OS X erbjuder stöd för att autentisera AD-användare och att ansluta mot nätverksmappar men där slutar mer eller mindre det inbyggda stödet. För ökad funktionalitet som påminner om Windows möjligheter anser vi det behövas tredjepartsmjukvara av något slag.

Både ADmitMac och Centrify gav oss möjlighet att applicera GPO:er på vår OS X-klient. Efter att ha utvärderat de båda anser vi Centrify´s lösning vara bättre och mer välutvecklad då Centrify User Suite Mac edition är del av en större familj. Det finns verktyg för bl.a. mobile device management men också för andra operativsystem såsom Linux. Centrifys verktyg gav oss fler GPO:er men erbjöd utanför vårt arbete också möjligheter till molnintegration av klienter utanför hemnätverket. Både Centrify och ADmitMac importerar mallar för GPO:er på domänkontrollanten men vi ser det som en nackdel att ADmitMac inte har någon central hantering utöver ovan importfunktion, utan all administration och konfiguration sker på klientsidan.

Båda tredjepartsverktygen erbjuder stöd för att varaktigt mappa upp nätverksmål men återigen erbjuder Centrify, enligt oss, mer utvecklad funktionalitet genom att kunna styra detta centralt genom GPO. Detta sparar tid jämfört med ADmitMac’s lösning där varje klient kräver manuell konfigurering.

Eftersom vi genom att använda tredjepartsmjukvara uppfyller de tre avgränsningar som arbetet omfattar är vi till viss del beredda att hålla med HKR´s IT-chef Matts Behrens i hans ståndpunkt att Apple OS X i AD inte är en teknisk fråga. Vi anser dock att hantering av tekniska frågor kvarstår vid jämförelse av integration av Apples datorer kontra en vanlig Windows-PC. Detta har också vår utredning och laborationer påvisat. Det krävs någon

form av tredjepartsverktyg eller användandet av ”Magic Triangle” för att uppnå likvärdig central hantering.
Frågans tekniska relevans är också något som Christer Persson på QSi tog upp. Han menade att eftersom de alltmer jobbar med fokus på molntjänster, som oftast är plattformsoberoende, har också betydelsen av många AD-funktioner minskat.
Tredjepartstillverkarna erbjuder sina lösningar i prenumerationsform per månad och användare. Vi tror att QSi och deras kunder kan erbjudas ökade möjligheter till bättre och mer samlad administration av OS X-klienter genom användandet av tredjepartsverktyg. På så sätt kan man effektivisera något som tidigare tagit stora resurser i anspråk.

4.2 Förslag till fortsatt arbete

Under detta examensarbetes fortskridande har vi vid fler tillfällen funnit flera intressanta stickspår som vi känner har underlag till och förtjänar vidare utforskning. I vår utredande del av arbetet behandlar vi tredjepartstillverkare samt Apple OS X Server, vi tycker att det skulle vara intressant att titta närmare på den ekonomiska skillnaden mellan mjukvarorna kontra OS X Server. Var finns brytpunkter för lönsamhet i olika lösningar beroende på hur många klienter som finns i miljön?

Arbetet har saknat förutsättningar för att utföra laborationer med OS X Server, vi hade gärna sett vilka möjligheter som ”Magic Triangle” medför när OS X Servers Open Directory integreras med Active Directory.

Vi har begränsade kunskaper i Microsofts System Center men det har dykt upp information kring användandet av System Center Configuration Manager (SCCM) och dess funktioner för bland annat utrullningslösningar som även kan hantera Apple OS X.

Under laborationen med Centrifys lösning kom vi även i kontakt med deras övriga produktutbud och insåg att de hade lösningar för så många andra användningsområden, bland annat en molnlösning för att hantera mobila enheter och även bärbara datorer. Denna kunde i sin tur integrera mot Active Directory. Centrifys helhetslösning hade varit intressant att titta närmare på.

5 Källförteckning

[1] ”www.theregister.co.uk,” 15 mars 2014. [Online]. Available: http://www.theregister.co.uk/2014/03/15/windows_desktop_and_laptop_market_share_dips_below_90_per_cent/. [Använd 15 december 2014].

[2] ”www.informationweek.com,” 11 juni 2014. [Online]. Available: http://www.informationweek.com/infrastructure/pc-and-servers/mac-enterprise-adoption-grows/d/d-id/1269595. [Använd 15 december 2014].

[3] W. Miller, december 2008. [Online]. Available: http://technet.microsoft.com/sv-se/magazine/2008.12.interacting(en-us).aspx. [Använd 21 januari 2015].

[4] 04 september 2009. [Online]. Available: http://www.macworld.com/article/1142631/snowleopard_printing.html. [Använd 21 januari 2015].

[5] 05 juni 2005. [Online]. Available: http://www.apple.com/pr/library/2005/06/06Apple-to-Use-Intel-Microprocessors-Beginning-in-2006.html. [Använd 21 januari 2015].

[6] C. Zacker, Exam 70-410 Installing and Configuring Windows Server 2012, John Wiley & Sons, 2013.

[7] C. Zacker, Exam 70-411 Administering Windows Server 2012, John Wiley & Sons, 2013.

[8] ”Networkstoragetips,” 27 januari 2015. [Online]. Available: http://networkstoragetips.com/.

[9] M. Moretti, ”Businessinsider,” 10 juli 2012. [Online]. Available: http://www.businessinsider.com/mac-os-i-through-x-2012-7?op=1&IR=T. [Använd 21 januari 2015].

[10] 02 januari 2013. [Online]. Available: http://training.apple.com/pdf/wp_integrating_active_directory_ml.pdf. [Använd 22 januari 2015].

[11] ”Thursby.com,” [Online]. Available: http://www.thursby.com/products/admitmac. [Använd 29 januari 2015].

[12] ”Centrify,” [Online]. Available: http://www.centrify.com/mac/active-directory-authentication-for-mac-os-x.asp. [Använd 29 januari 2015].

[13] [Online]. Available: www.powerbrokeropen.org. [Använd 23 februari 2015].

[14] ”Beyondtrust.com,” [Online]. Available: http://www.beyondtrust.com/Products/PowerBrokerIdentityServicesADBridge/. [Använd 23 februari 2015].

[15] 22 februari 2012. [Online]. Available: http://techworld.idg.se/2.2524/1.433858/sa-far-du-mac-att-trivas-pa-jobbet. [Använd 02 februari 2015].

[16] [Online]. Available: https://it.uoregon.edu/Magic-Triangle-setup. [Använd 02 februari 2015].

[17] [Online]. Available: https://www.apple.com/se/support/osxserver/profilemanager/. [Använd 02 februari 2015].

[18] [Online]. Available: http://www.hkr.se/sv/om-hkr/. [Använd 6 april 2015].

[19] ”Apple.com,” 08 maj 2014. [Online]. Available: http://support.apple.com/kb/PH13983. [Använd 22 januari 2015].

6 Bilagor

6.1 Intervju med företag

1:A Intervju med QSi

1:A Intervju med QSi

Intervju med QSI (2015-02-27)

Intervjun börjar med att vi berättar vad vi läser och vad och varför vi skriver examensarbete.

Vi tänkte börja med att fråga: Får vi spela in detta?

Christer: *Ja*

Får vi namnge QSI, Christer och André

Christer och André: *Ja*

Vill ni presentera QSi lite, varför ni finns och ert erbjudande?

Christer: *Egentligen är det kunden som styr utbudet och det är lite därför vi har tagit in Apple också. Vi är i grund och botten en Microsoft-partner och inriktning mot PC men idag så är det ju kunden eller köparen som väljer lite vad man vill jobba med och då har ju Apple blivit mer och mer en klient i arbetslivet och då är det för oss att följa efter och erbjuda även Apple-biten parallellt med PC-biten. Väldigt många kunder sitter med blandmiljöer idag, så det behöver inte vara den rena Apple kunden det kan vara en mixkund där en avdelning sitter med PC och kanske media och reklam avdelningen sitter med Mac. Då såg vi det som ett försök och ett drag att ta in Mac också i vårt utbud. Så det är kundefterfrågan som har gjort att vi tar in det också. Och därav vårt erbjudande. Så att PC, mix eller bara Mac det spelar ingen roll längre. Och det är lite därför att integrationen mellan dem har blivit bättre med tanke alla molntjänster. Idag så gör du väldigt mycket genom en internetläsare oavsett, då spelar inte klienten lika mycket roll.*

André: *Insteg är ju iPhone eller iPad och det har ju bara exploderat och vi ser ju mer och mer, som Christer säger, det är ju blandmiljöer i stort sätt vart som idag. Innan vart det mer inriktat mot marknadsföringsföretag på Apple sidan. Idag är det allt ifrån banker till sjukhus.*

En följdfråga: Har ni kunder som integrerar Macar i sin AD-miljö eller hanterar man dem separat?

Christer: *Integrera dem fullt ut vill jag påstå att det går inte, det är därför att katalogtjänster och sånt inte riktigt harmonierar, nu pratar jag lite utifrån egna erfarenheter också. Man kan integrera dem till vissa delar och det gör vi. Men som jag sa innan, väldigt mycket idag läggs upp i molntjänster och då är de inte lika mycket beroende av att ta in dem i ett AD heller. Därför att då har du en egen inloggning till webbtjänsten. Sen så kanske man då kan ifrågasätta det här med single-sign-on och liknande men det blir ju ett merarbete med att det blir lite mer inloggningar på webbtjänsterna men då har du inget AD med dig. På så sätt behöver du inte lika mycket in i AD. Men om man då tittar på katalogstrukturen när det gäller shares och delade mappar och sånt, där är det ett större problem. Det går att göra statiska kopplingar, precis som att du kopplar en enhet, tex en G:, så kan du göra en sån koppling på en Mac också men det är inte riktigt samma integration med sin inloggning och sitt lösenord som de är med en PC, så där är det inte helt utbyggt. Likadant Group Policys, man trycker ut mycket i PC-världen det kan man inte göra lika mycket i Mac-världen ifrån ett AD. Så går man djupare in i funktioner och tjänster i ett AD så finns det inte integration fullt ut av att hantera Macarna som klienter. Men att nå resurser och sånt, ja, mail idag, sen Office 365 kom finns de inga som helst bekymmer med dokumenthantering via en share-point, därför du har lika mycket stöd från en Mac-klient som från en PC. Ska du ha dokumenthantering via mappstruktur då är där en brist. Och det är det jag*

menar, nu har tjänsterna kommit upp så mycket att man byggt bort lite av AD-beroendet och det gör att dem mixar ihop bättre bland-miljöerna. Men lever man kvar i de gamla traditionella AD-mappstrukturmiljön då är det svårare att få in en Mac. Lika så att trycka ut skrivarinställningar, trycka ut installationer i PC så kan man köra med MDT, det är ju automatisk installationstjänst kan man säga, allt sånt finns ju inte för integration mot Mac. Så att ifrån de vinklarna får man ju se det som att de är fristående Mac-klienter. Till 35-40% kan man integrera dem ihop med miljön, resten är dem med egna påloggningar, man har mer handpåläggning. Du kan inte automatisera lika mycket.

Vi kom in på det lite nu, upplever ni att de kräver mer i tid, personella resurser?
Christer: *De är mer tidskrävande för att de går inte att automatisera lika mycket, i dagsläget. Man ser ju tecken på att PC och Mac närmar sig varandra. De har ju TCP/IP i grunden, innan var det AppleTalk. Microsoft släpper Office-paket till Mac. Vi har ganska många miljöer där man kan på en Mac komma åt sin tjänster men sen så kan du köra en RDP-klient och logga på så får du ditt PC-fjärrskrivbord och gör resten i. Så att de finns ju lösningar med dagens grejor som gör att du kan integrera dem ganska mycket. I annat fall kan man ju köra en Parallell, men då är de ju inte en Mac längre, då är de en PC i ett Mac-skal, så då tycker jag man har fuskat. Då har du inte integrerat Macen, då har du integrerat den virtuella PC. Då kan du lika gärna sitta och köra en PC.*
Men kör med de tjänster som går att köra som webbtjänster och resten har du RDP-fjärrskrivbord. Vi har en hel del lösningar där vi bygger en PC-baserad fjärrskrivbordsplattform så kan man komma åt den med en padda, en Macbook eller PC. Så då spelar de ingen roll vad du har för klient mot den. På så sätt kan man integrera ganska mycket.

Vilka funktioner i Microsoft Active Directory används?
Christer: *Autentisering, DNS och DHCP. Vi är ganska nya med Mac i PC-mijö, så de är dem erfarenheter vi har.*

Ser ni att behovet/efterfrågan på nätverkslagring minskar i takt med Office365, OneDrive osv?
Christer: *Ja, de är framförallt SharePointen som har gjort att man har lämnat traditionella mappstrukturen. Därför att mappstruktur, påstår jag, att det fungerar upp till 10 anställda, sen bygger du gyttja. De finns inte riktiga versionshanteringar, du har inte koll på vilka som har läs/skrivrättigheter. Så att blir man större än 10 så måste man lyfta det till någon annan funktion, då finns det bl.a. SharePoint och det finns andra tredjeparts webbaserade ”dokumenhanterings-portaler”. Och de har ju gjort att man har lämnat DFS och shares och mer tittar på någon form av webbtjänster. Då spelar det ingen roll om det är en Mac eller PC. De är det jag menar att man har närmat sig varandra i funktioner.*

Används funktioner främst för att underlätta för användare eller för kontroll av anslutna enheter?
André: *Användaren*
Christer: *Användaren, i första hand. Det är användaren som ställer önskemålen och kraven på klienten och sen därefter ställer de kravet på management att leva upp till det. Tidigare har ju management eller ledningen ställt policies och kraven, ”det här gäller; take it or leave it!”. Men med den nya generationen och*

den nya ”bring your own device-trenden” som har blivit så blir det, jag tar min egen dator istället för den är mycket bättre. Så det har vänt lite att det har gått till att det är slutanvändaren som ställer kraven eller tunga önskemålen. Och då har ju företagen fått börja anpassa sina system och tjänster efter det. Och i sin tur har de ju då ställt kraven på Microsoft och de andra stora leverantörerna att börja se det utifrån det. Men innan så skulle de ju inte ha släppt in en Mac. Men idag finns de ju mycket program med stöd för Mac. De tjänar ju pengar på licenserna på Office, och har hälften börjat köra Mac så vill de ju fortsätta tjäna pengar på Office. Så svaret slutar med att det är slutanvändarna som ställer kraven.

De kunder som ni har som kör Mac i AD, vilka verktyg används för att administrera dem?
Christer: *De flesta mix-kunder vi har är det mestadels PC, så dem friadministreras. Vi har inte så stora kunder så att man har 100-talet Macar. Vi står inte inför det problemet.*

Vilka funktioner saknas jämfört med Windows-klienter när de gäller AD och Mac?
Christer: *Kontrollen av autentiseringsbiten, man har inte koll på byta lösenord, svårighetsgrad på lösenord. GPO:er för att kunna trycka ut program, skrivare och annat. Annars är det inget så specifikt.*