Förslag till uppdatering av nätverksoperativsystem i Kökar kommun

Alex Forsman

Timothy Ekeblom

Examensarbete för Tradenom (YH)-examen

Utbildningsprogrammet i Informationsbehandling

Raseborg 2014

EXAMENSARBETE

Författare: Alex Forsman och Timothy Ekeblom

Utbildningsprogram och ort: Tradenom, Raseborg

Inriktningsalternativ/Fördjupning: Informationsbehandling

Handledare: Klaus Hansen

Titel: Förslag till uppdatering av nätverksoperativsystem i Kökar kommun

---

Datum: 25.11.2014 Sidantal: 85 Bilagor: 0

Abstrakt

Vårt examensarbete är avsett att vara ett förslag på hur man kan uppdatera den befintliga servermiljön till en modernare och tidsenligare servermiljö med hjälp av operativsystemet Windows Server 2012 Revision 2 för Kökar kommun i Ålands skärgård.

Vi utförde detta genom att skapa ett testlaboratorium, där vi satte upp en miljö med en servermaskin vilken vi skräddarsydde för att köra de processer och tjänster som behövs. För de empiriska experimenten hade vi två andra datorer inkopplade till vårt nätverk för att fungera som användare i vår domän.

Vi kom fram till att en server skulle räcka som DC (Domain Controller), tack vare att det är en kostnadseffektiv lösning och för att det är lätt att sköta och underhålla.

Servern skall fungera med alla funktioner som behövs: Active Directory Domain Services(AD DS), DNS, DHCP, Printer- och filserver, säkerhetskopiering, VPN mm. Vi går noggrant in på alla funktioner och tjänster, varför de behövs och hur de fungerar samt installeras i praktiken.

Resultatet av arbetet är att vi skapade en effektiv och fungerande servermiljö i ett relativt litet nätverk (under 100 pers.) som är installerad och konfigurerad färdigt för användning.

Språk: Svenska Nyckelord: windows server 2012, nätverk, nätverksstruktur, active directory ,servermiljö

BACHELOR'S THESIS

Author: Alex Forsman and Timothy Ekeblom

Degree Programme: Business Information Technology, Raseborg

Specialization: Information processing

Supervisors: Klaus Hansen

Title: A proposition for updating the network operating system for the municipality of Kökar

---

Date: 25.11.2014 Number of pages: 85 Appendices:0

Summary

Our thesis is intended to be a proposition for updating the current server environment for the municipality of Kökar, located in the Åland archipelago. The computer environment will be modernized and more time-saving by using Windows Server 2012 Revision 2.

We created a test lab where we set up an environment with a server machine which we commanded to run the exact processes and services that are needed. For the empirical experiments we had two other computers connected to our network to function as users in our domain.

Our conclusion was that just one server will be needed as a DC (Domain Controller), because that will be a cost-effective solution and because the system is easily operated and maintained.

The server must work with all features needed: Active Directory Services (ADSD), DNS, DHCP, Printer- and fileserver, backup, VPN and more. In our work we have penetrated all the features and services and explained why they are needed, how they work and how they are installed practically.

The result of our work is that we created an efficient and effective server environment for a relatively small network (less than 100 persons) which is installed and configured, ready to be used.

Language: Swedish Keywords: windows, server 2012, network, active directory, directory services, server environment

---

Innehållsförteckning

1 Ordlista

AD DS	Active Directory Domain Services. Det är en katalogtjänst som innehåller information om olika resurser i en domän (nätverk) t.ex. datorer, skrivare och användare.
CAL	Client Access Licenses. Dessa behövs för varje användare eller apparat som vill ha tillgång till en server
OU	Organisational Units (Organisationsenhet) är Active Directory behållare i vilken man kan placera användare, grupper, datorer och andra organisationsenheter.
GPO	Group Policy Objects, är ett objekt som innehåller styr-inställningar för datorer och användare.
DC	Domain-Controller. Domänkontrollanten är huvudsakligen den server som innehåller AD och andra katalogtjänster för domänen.
.WIM	Windows Imaging Format. Används vid distribuering av operativsystem med WDS till datorer inom domänet.
WDS	WIndows Deployment Service, är en servertjänst som gör det möjligt att massdistribuera Windows operativsystem via en nätverksbaserad installation.
VPN	Virtual Private Network, tillåter krypterad data att skickas mellan två datorer över Internet.
SHV	System Health Validator. Används vid konfigurering av NPS servern och hur man begränsar datorernas hälso när de vill ansluta sig till ett domän.
DNS	Domain Name System, fungerar som ett slags tolk som är kvalificerad att läsa domän eller värdnamn till IP-adresser.

2 Inledning

Iden bakom slutarbetet kom från Alex Forsman som har nära kontakt till Åland och speciellt Kökar för han har bott där länge. Sedan diskuterades idén med Kökars kommundirektör som blev intresserad och frågade oss om vi kunde komma fram till ett förslag till ett nytt datasystem och en infrastruktur genom en uppdatering av befintliga nätverket.

Efter att vi hade haft kontakt med kommunen och kommundirektören och de accepterade idén började vi planeringen. Alex Forsman hade tidigare jobbat med Active Directory i Windows Server 2008, vilket gjorde valet av verktyget för arbetet lätt.

Vi har båda också jobbat med Linux och Windows Server 2008 men vi valde Windows Server 2012 R2 som är nyaste upplägget eftersom vi tyckte att det skulle vara intressant att lära och fördjupa våra kunskaper i detta system, som vi fått gratis till förfogande från Microsoft Dreamspark då vi studerar i en yrkeshögskola.

Dreamspark är ett Microsoft-program som stöder teknisk utbildning genom att ge tillgång till Microsoft-programvara för lärande, undervisning och forskning.

Många företag föredrar Windows framom Linux operativsystem för deras servrar, speciellt gör större företag det därför att Active Directory gör det lättare och säkrare att hantera ett större antal användare och underlättar uppbyggnaden av en infrastruktur för ett nätverk.

Fokuset i vårt slutarbete kommer att ligga på själva praktiska utförandet av installationen och konfiguration av servern, men vi går också grundligt igenom vad vissa funktioner och tjänster i Windows Server 2012 gör och varför vi använder dem, samt tankegången bakom varför vi prioriterade vissa funktioner framom andra.

3 Mål

Det finns sex delar i arbetet:

1. Beskrivning av nuvarande situation och vårt förslag till lösning på den.
2. En grundlig introduktion av Windows Server 2012 och dess funktioner.
3. Beskrivning av behov
4. Planering och installation av nätverksoperativsystemet i en försöksmiljö
5. Konfiguration av funktioner och tjänster i en försöksmiljö
6. Konfiguration av en VPN server.

Vi beskriver hur vi byggde upp ett nätverk och en domän med hjälp av Windows Server 2012 i en försöksmiljö som motsvarar Kökar kommuns behov. Inledningsvis går vi emellertid noggrant igenom Windows Server 2012 R2 och alla dess funktioner.

Genomgången kommer vara grundlig men inte alltför nybörjarvänlig. Detta borde ändå göra det enklare så att man förstår alla termer och nyckelord samt de funktioner de leder till.

Vår lösning för att förbättra den nuvarande situationen kommer att vara fokuserad på kostnadseffektivitet. Detta betyder att kostnaderna skulle vara minimala och kommunens nuvarande utrustning skulle återanvändas. Vi kommer dock även med rekommendationer på uppgraderingar som borde göras för vissa tjänster som skulle kräva nyare hårdvara.

Vi kommer att beskriva Kökars nuvarande situation beträffande deras nätverksstruktur, vilka behov de har, och sedan hur man kunde förbättra situationen och optimera verksamheten.

Vi har analyserat vilka behov kommunen har för nätverket och sedan valt ut vilka processer och tjänster kommunens nätverk kommer att behöva.

4 Val av Windows Server 2012 R2

Eftersom varumärket Windows och alla dess komponenter hela tiden växer inom företagsvärlden ville vi använda den nyaste Windows Server versionen som nätverksoperativsystem för uppdraget.

Vi tyckte att Windows Server var ett intressant ämne och vi ville därför forska och lära oss mera om området för att på så sätt även uppnå en eventuell fördel inom framtida arbetsförhållanden. De personliga erfarenheter vi får kan naturligtvis användas i praktiken, i det riktiga arbetslivet.

Det finns särskilt stor efterfrågan på specialister som har kunskap inom Windows Server operativsystemen. Man kan även delta i anordnade kurser och avlägga ett prov och på så sätt få ett särskilt Microsoft certifikat som visar att man behärskar området.

Vi valde nyaste versionen av Windows Server framom de äldre versionerna, såsom den vanligare Windows Server 2008, därför att Windows Server 2012 baserar sig på Windows 8 och kommer förmodligen att bli standarden för företag och institutioner i framtiden. Windows Server 2012 innehåller också ett fullständigt grafiskt gränssnitt som man kan i princip göra allting i, medan man i Windows Server 2008 och dess äldre versioner måste använda sig av kommandoraden för att utföra en stor del av de kommandon som behövs.

Det finns nog fortfarande ändå möjlighet att använda kommandoraden och t.ex. PowerShell i Windows Server 2012, så man kan fortfarande göra allting “manuellt” om man vill skriva in kommandon för hand eller dylikt.

PowerShell är ett aktivitetsbaserat kommandoradsskal och skriptspråk. Det är speciellt gjort för systemadministration. PowerShell är byggt på Microsofts .NET ramverk (Framework). Man kan skapa “cmdlets” i PowerShell som innehåller kommandon, t.ex. kodexemplet som demonstreras i Kod 1. Kodexemplet demonstrerar ett skript som automatiserar installationen av Active Directory Domain Services och innehåller information om domänet och installationsplatsen för databaser osv.

Med dessa cmdlets kan man hantera datorer i nätverket, installera program och tjänster eller göra förändringar i registret mm. Cmdlets kan exempelvis skickas till andra datorer där Cmdlets sedan kan exekvera sina kommandon.

Kod 1. PowerShell skript för AD DS installation

```
#
# Windows PowerShell script for AD DS Deployment
#

Import-Module ADDSDeployment
Install-ADDSForest `
-CreateDnsDelegation:$false `
-DatabasePath "C:\Windows\NTDS" `
-DomainMode "Win2012R2" `
-DomainName "test.fi" `
-DomainNetbiosName "TEST" `
-ForestMode "Win2012R2" `
-InstallDns:$true `
-LogPath "C:\Windows\NTDS" `
-NoRebootOnCompletion:$false `
-SysvolPath "C:\Windows\SYSVOL" `
-Force:$true
```

En annan orsak att vi valde Windows Server 2012 är för att Microsoft oftast har bättre kundservice och support för sina kunder än t.ex. Linux. Även när man söker information på nätet, t.ex. när vi själva stötte på problem vid installationen av olika tjänster, så hittade vi lätt information på Microsofts egna sidor och hjälp till att lösa problemen.

4.1 Disposition

I arbetet ingår följande delar:

- Bakgrund och intervju
- Nuvarande nätverkssituation
- Förslag till förbättring
- Uppbyggnad av arbetet
- Nätverksstruktur
- Funktionalitet (Tillägg/Moduler)
- Praktiska arbetsprocessen förklarad / förverkligande
- Resultat och slutsatser.

Vi kommer att förklara ovanstående punkter genomförligt.

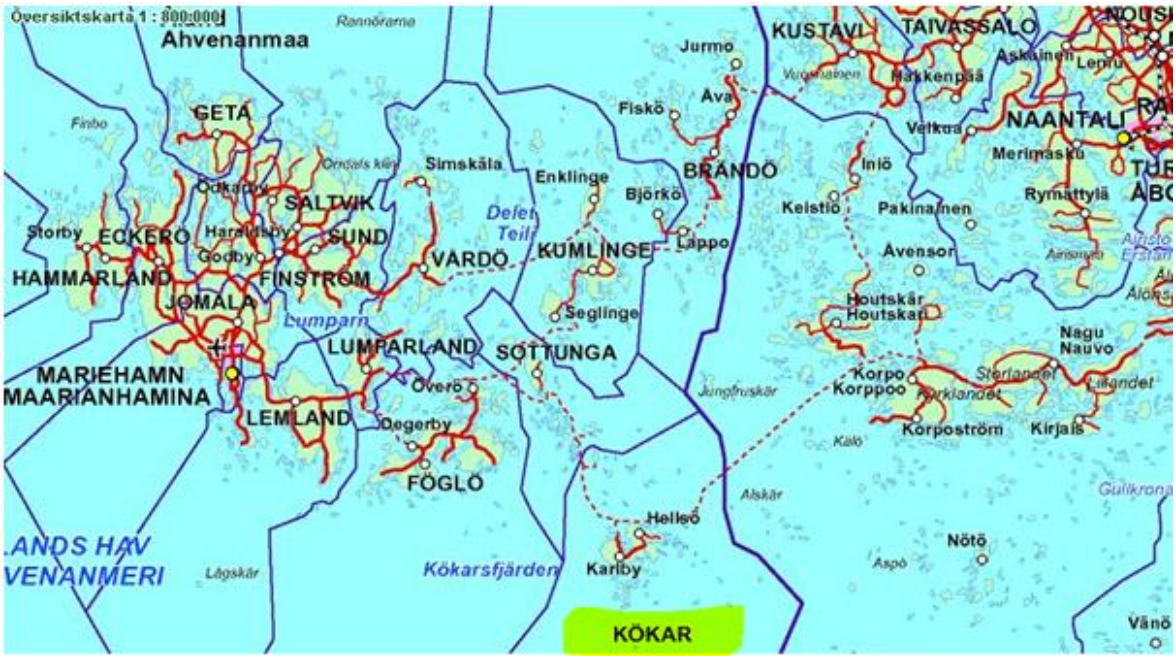
5 Bakgrund och intervju

Hela detta kapitel baserar sig på intervju med kommundirektören på Kökar, Kurt Forsman.

Kökar kommun

Kökar som hör till Åland är Finlands nästminsta kommun. Där bor ca 250 invånare men kommunen har alla organ som skall finnas i en kommun, både lagstadgade och en del frivilliga. Kökar ligger mitt i havet mellan fasta Finland och fasta Åland, som man kan se på kartan i figur 1.

Med färja tar det 2,5 timmar till fasta Åland och därefter 30 minuter med bil förrän man är i Mariehamn. Åker man österut till Korpo i så tar det också 2,5 timmar med färja. Figur 2 visar en karta över Ålandsskärgård.



Figur 1. Översiktskarta - Kökar.

Kommunen har verksamhetspunkter på flere ställen inom kommunen och även utanför själva kommungränserna. Förutom på Kökar finns skoldirektörsfunktionen i grannkommunen Sottunga och byggnadsinspektörsfunktionen i Jomala på fasta Åland. Lantbrukskansliet finns i Jomala och brandchefstjänsten sköts från Mariehamn.

Kökars kommunkansli

Kommunkansliet ligger i centrum (Karlby) av Kökar. I kommunkansliet finns ett ca 5 år gammalt lokalt nätverk med ca 5 år gammal utrustning. Man har en Dell-server, PowerEdge T310 Tower Chassis med speglade hårdskivor samt 4 stycken arbetsstationer, Dell OptiPlex 360 MT. Dessutom finns ett par Laptops som används av kommundirektören och socialsekreteraren vid resor och möten utanför Kökar.

I kommunkansliet kör man med Windows 7 som operativsystem allt sedan utrustningen skaffades för ca 5 år sedan. Man har officepaketet i alla maskiner och som e-postprogram används Microsoft Office Outlook. Mest används Word och Excelprogrammen, i viss mån Powerpoint och Publisher.

Kommunkansliet skulle vara en ideal plats för en central server och vårt förslag skulle vara att använda kansliets nuvarande utrustning för att skapa en huvudserver där.

Utrustningen och hårdvaran täcker kraven för Windows Server 2012 och de tjänster vi planerat tillsvidare. Om användarantalet växer måste det möjligtvis planeras en server till som körs vid sidan av huvudservern och som kan sköta om vissa tjänster.

Alternativt kan man eventuellt uppgradera hårdvaran i huvudservern så att den klarar av en mer omfattande trafik i domänen. Tack vare Windows Server och dess Deployment Services (WDS) kan man, förutom central lagring av dokument, också göra distribution och utdelning av ny programvara till användarna enklare än vad den är idag.

I nuläget har kommunen inget gemensamt upplägg av mjukvara på sina arbetsstationer, alla anställda har i princip installerat vad de anser sig behöva på sina datorer. Detta eventuella problem skulle lösas av den nya centrala servern som färdigt kunde skicka alla väsentliga program och uppdateringar mm. till användarna.

Övrig programvara som används är ekonomisystem och personaladministration (löneräkning). Här använder man sedan länge Abilita ekonomiförvaltning, rapportering och budgetering(www.abilita.fi).

Man har i ekonomiförvaltningen inte tagit i bruk cirkulation av fakturor. I dag sköts godkännandet av fakturor så, att när en räkning kommer in till kommunen så diarieförs den i kommunkansliet och matas in i inköpsreskontran.

Sedan läggs den i respektive enhets postfack i kansliet som någon från enheten tömmer ibland. Det kan vara samma dag eller först om en vecka, vilket leder till förseningar i betalningarna.

Cirkulation innebär att räkningen skannas in genast då den kommer till kommunen varefter den digitalt sänds till respektive enhet för godkännande och sedan returneras den godkända fakturan digitalt till kommunkansliet för betalning. Ibruktagandet av cirkulation kunde bli naturligt efter att Windows Server 2012 tagits i bruk.

5.1 Kommunens ekonomisystem

På Åland finns 16 kommuner. De allra flesta av kommunerna använder Abilitas ekonomisystem och program som är integrerade och fungerar bra ihop.

Från personalschemaläggning i omsorgshemmet kan uppgifterna integreras i löneräkningen som i sin tur har förbindelse med lönebokföringen som i sin tur har förbindelse med kommunens banksystem (Ålandsbankens Business-Line).

Endast några få kommuner och Ålands landskapsregerings alla enheter inklusive Ålands Hälso- och Sjukvård (ÅHS) använder programvara från österbottniska Norlic (www.norlic.fi). Nu har Abilita meddelat att man slutar utveckla och uppdatera de nuvarande ekonomi- och PA-systemen år 2016.

Norlic har meddelat att de också slutar med sin svenskspråkiga programvara och avser inte att översätta någon ny. Det här innebär att hela den offentliga sektorn står inför ett dilemma, man är tvungen att lösa problemet snabbt.

Abilita har istället för nuvarande programvara börjat samarbeta med svenska Agresso och säljer deras system. Unit 4 Agresso startade i Sverige 1995 och har nu verksamhet på många ställen i världen efter att ha köpt upp en hel del andra företag i samma bransch.

Agresso innehåller följande fullt integrerade moduler som fyller kommunernas behov:

- Ekonomi
- Budget, prognos, beslutstöd
- Lön/HR
- Projektadministration
- Inköp och e-handel
- Logistik, lager
- Service och underhåll

Antagligen kommer de flesta kommuner på Åland att övergå till Agresso, som antagligen kommer att upphandlas centralt av ett offentligt samägt bolag som bildas utan vinstsyfte.

Dessa ekonomisystem- och program kunde överföras till servern och skulle fungera även i nya nätverket och vara säkert tack vare krypteringsmetoden som VPN uppkopplingen emellan klienterna i nätverket använder sig av.

Ett annat alternativ som skulle underlätta användningen av olika slags affärssystem som Agresso är att använda dem i "molnet". Agresso erbjuder egen molntjänst (Cloud Computing) möjlighet vilket betyder att man kan använda programmet helt normalt oavsett vilket operativsystem man har eller vilket nätverk man använder.

I praktiken betyder utnyttjandet av molntjänsten att ingen programvara behöver installeras på datorerna. Användningen skulle inte vara låst till ett visst system, för att programmet körs webbaserat har alla användare med inloggningsrättigheter tillgång till programmet.

Molntjänsten av Agresso skulle vara en bra lösning, speciellt om alla kommuner i framtiden går över till Agresso som nämnts. Det nya nätverket och domänen skulle inte skapa några problem för övergången till det nya affärssystemet. Om man dessutom skulle använda Agresso via molntjänsten skulle det minska på kommunens serverbandbredd och resurser, vilket är att rekommendera.

Det offentligt samägda bolaget, ÅDA Ab, har bildats hösten 2014 och gör nu (december 2014) en riktad emission till kommunerna och övrig offentlig sektor på Åland. Bolaget skall vara praktiskt fungerande i januari 2015.

På Åland försiggår nämligen just nu en samhällsservicereform (SSR) som omfattar flere sektorer och vars syfte inte åtminstone i första hand är att sammanslå kommuner utan att

sammanföra funktioner och öka samarbetet inom den offentliga sektorn. Till målen för reformen hör att effektivera verksamheten, koncentrera sakkunskapen och uppnå ekonomiska inbesparingar.

Det kommer också att ställas krav på goda och effektiva IT-lösningar. Inom SSR finns något som kallas Ålands Digitala Agenda (ÅDA) som under 2013-14 utrett den offentliga sektorns fysiska IT-struktur och den mjukvara som används.

Det är Ålands Digitala Agenda och i synnerhet Ålands landskapsregering som står bakom det nämnda bolaget. Bolaget kommer också, förutom att sköta offentliga sektorns upphandlingar, att kunna erbjuda support, serverutrymme, m.m. Fysiskt kommer bolagets verksamhet att vara placerad i Mariehamn.

5.2 Platsundersökning

I Kökars kommunkansli finns idag Soneras ADSL-uppkoppling, 8/2 Mbps. Linjen används för e-post, internetsökning, överföring av bankfiler och dokument av varierande slag och varierande storlek. ADSL-abonnemanget har fungerat väl hittills men nu avser man att koppla in fiberoptik i kansliet med anslutning 100/100 Mbps.

Tjänsteleverantören i fibernätet är Ålcom (www.alcom.ax) som i stort sett har monopol på att leverera sådana tjänster i skärgården, där fibernäten byggts ut av kommunalt delägda bolag. Sonera har inga planer på att bygga egen fiber där.

Genom att dra in fiber med tillräcklig kapacitet så kan man bättre åstadkomma förutsättningar för telemedicin och skapande av virtuella mötesplatser för äldre och som i detta fall i kommunkansliet för att ordna och deltagande i videokonferenser. Ålands landskapsregering har nämligen för avsikt att köpa in och installera videokonferens utrustning till varje skärgårdskommun, eller använda Microsoft Lync för att nå liknande resultat.

Eftersom Ålands skärgård är spridd och omfattar sex skärgårdskommuner med sammanlagt ca 2400 invånare så är det viktigt att åstadkomma virtuella mötesplatser, deltagande i ett möte i Mariehamn tar en hel dag i anspråk om man utgår från Kökar eller Brändö.

Kökars grundskola

Kökars grundskola är en liten skärgårdsskola med 24 elever på årskurserna 1 – 9. Man har alltså eget högstadium. Skolan använder olika Linuxvarianter som operativsystem och Open Office programvara. Skolan har ända till oktober 2014 haft en 8/2 mbps ADSL uppkoppling från Sonera. Mest används e-post samt naturligtvis Internet för skolans administrations- och undervisningsbehov.

Nu har man dragit in fiberoptik med anslutning 100/100 mbps bl.a. för att bättre kunna delta i olika projekt, t.ex. ByskolE-projektet. Projektet har existerat drygt ett år och med ett mera konkret innehåll sedan januari 2014.

I korthet går projektet ut på att ge skolorna möjligheter till ökat samarbete via digital teknik och att utveckla metoder för distansundervisning.

Detta genom att fortbilda lärarkårerna i teknik och metodik, vilket delvis genomförs under hösten 2014 via Fortbildningscentralen vid Åbo Akademi med hjälp av ekonomiska medel från Ålands landskapsregering.

Ålands landskapsregering stöder överhuvudtaget digital utveckling i skärgårdsskolorna genom att tilldela medel för att kunna utveckla möjligheterna till att dela resurser, samarbeta, undervisa eller få undervisning på distans för de små skärgårdsskolorna.

I Kökars grundskola finns inom administrationen (lärarna) 4-5 datorer och i undervisningen ca 20 datorer av väldigt varierande ålder och kapacitet. Skolan har ett eget LAN(lokalt nätverk) från år 2000.

Kökars bibliotek

Kökars bibliotek finns i Kökars grundskola och använder numera samma LAN som skolan och samma uppkoppling, 100/100 mbps. I biblioteket har bibliotekarien två datorer, en vid utlåningsdisken och en i kansliutrymmet. Därtill finns två kunddatorer. Datorerna är av varierande ålder; en kunddator kör Windows XP medan de tre övriga har Windows 7.

Förutom Officepaketet använder bibliotekarien det biblioteksprogram, Book-It, som är svenskt och används av alla bibliotek på Åland. Uppkopplingen sker mot Sverige. Alla bibliotek på Åland är också med i den gemensamma biblioteksdatabasen Katrina där hela Ålands bokbestånd finns.

Katrina motsvaras i Finland av databasen Lucas. Biblioteket tillhandahåller även en trådlös öppen accesspunkt för biblioteksbesökare och andra, tex. turister, som därmed kan koppla upp sig även utanför skolbyggnaden då biblioteket är stängt.

Omsorgshemmet Sommarängen

Sommarängen i Hellsö by är ett effektiverat serviceboende för åldringar, där finns 12 rum och en hel del gemensamma utrymmen. Det är byggt 2009 och i anslutning till omsorgshemmet finns även 4 lägenheter för pensionärsboende.

Omsorgshemmet har 8/2 mbps ADSL uppkoppling, men man kommer inom kort att ansluta det till en 100/100 mbps anslutning via fiberoptisk kabel. I huset finns ett LAN med anslutningspunkter i alla klientrum och i alla gemensamma utrymmen samt förstås i kansli, personalrum och även i köket. I huset finns brandlarm via telefon samt klientlarm som går via telefon.

Nu när det finns fiberuppkoppling vill man utreda möjligheterna till IP-telefoni och att larmsystemen går via internet istället för via mobiltelefonabonnemang, om det kan vara en billigare lösning än den nuvarande.

I mars 2013 (18 mars) startade projektet Äldreomsorg på distans (ÄlDis) i Landskapet Åland, vars syfte är att införa en ny stödtjänst inom äldreomsorgen på Åland som ett kvalitativt och ekonomiskt lönsamt komplement till traditionell hemservice. Projektperioden är från 1.3.2013 till 28.2.2015.

ÄlDis har inte fungerat så bra på Kökar på grund av dålig internetkapacitet, men nu hoppas man att det ska bli bättre. Meningen med projektet är att utveckla en resursförstärkande metod för att på distans stöda hemmaboende äldre och utvecklas i samverkan med personal vid Högskolan på Åland, personal inom deltagande kommunernas äldreomsorg samt andra berörda samarbetspartners.

Via dator i hemmet (pekskärm) kan de äldre umgås med varandra eller kontakta omsorgshemmet Sommarängen eller t.ex. få information från Folkpensionsanstalten eller gå på olika kurser på distans. Metoden förverkligas via videokonferensteknik från Videra.

Videra Oy i Finland levererar den tekniska lösningen, som bygger på ett videokonferenssystem som kopplas till en VGU-skärm.

Med denna teknik kan användarna vara i kontakt med varandra via ”telefonkatalogen” eller delta i olika gruppsändningar/aktiviteter. I tekniken från Videra krävs också att användaren har internetanslutning. Vid projektets början var användarna anslutna internet via Videra, senare har man ingått avtal med Ålcom, Ålands telefonandelslag och Mariehamns telefon.

Daghemmet Barnängen

Daghemmet Barnängen ligger invid omsorgshemmet Sommarängen och kommer att använda deras uppkoppling. Daghemmet har bara ringa behov av dator och det är då främst inom administrationen.

6 Program och verktyg

Förutom av Windows Server 2012 använde vi oss av andra Microsoft standardprogram och undermoduler, även öppen källkod (OpenSource) program som vi berättar mera om senare i slutarbetet.

Då vi praktiskt byggde upp en kopia av en domän som vi teoretiskt beskriver i arbetet, använde vi oss av utrustning vi fått låna av Yrkeshögskolan Novia. Med hjälp av utrustningen som vi fått låna, byggde vi upp ett nätverkssystem med både klienter och servrar.

Hårdvaran som vi hade till förfogande var inte av den nyaste tekniken men täckte de absoluta minimi-systemkraven för en installation av Windows Server 2012 vilka är:

- 512 Mb RAM
- 1.4 GHz 64-bit processor
- 32 GB utrymme på hårdskivan

(System Requirements and Installation Information for Windows Server 2012 R2, 2013.*)*

Den utrustning vi hade täckte gott och väl minimi-systemkraven och hade 230 GB utrymme på hårdskivan, 2,4 Ghz 64-bit processor och 4 GB RAM. Med denna utrustning och några klientdatorer klarade vår server av alla uppräknade roller och tjänster utan stress. Problem uppstår först efter att man har över 50 användare som arbetar samtidigt med häftig belastning på nätverket, speciellt om VPN är anslutet.

I arbetet byggde vi upp nätverksstrukturen inom en fysisk försöksmiljö så att vi lätt kunde se vad som krävdes för just de ändringar vi beskriver i förbättringsförslagen.

Det är inte optimalt att ha alla tjänster och roller på samma server om den inte är väldigt modernt utrustad med den nyaste hårdvaran, alternativt bör man dela ut större roller till andra servrar. Vi rekommenderar, om Kökar besluter sig välja VPN, att kommunen i så fall investerar i en skild server för detta.

Om man beslutar att köra de flesta roller och tjänster på samma server kunde virtualisering vara på sin plats. Genom att dela ut RAM minne till en specifik tjänst, och en processorkärna (core) till tjänstens förfogande gör så att bara en kärna fokuserar sig på en specifik tjänst/roll och inte mera.

Virtualisering med Hyper-V använde vi dock inte oss av i arbetet men det kunde hjälpa balansera lasten på servern. Hyper-V är en roll i Windows Server 2012 som kan användas för att skapa virtuella instanser så som virtuella installationer av operativsystem.

Det är inte obligatoriskt att virtualisera, så som vi gjorde i arbetet fungerade det rätt bra i ett mindre nätverk, men om det är i fråga om större nätverk är det en bra idé att överväga virtualisering.

6.1 Mjukvara

Förutom Windows egna tjänster använde vi oss av olika typer av verktyg för att utföra vårt projekt. Ett av dem var Deployment Workbench som användes i samband med WDS och skapandet av skräddarsydda ”.WIM” avbildningar (images).

Workbench installerade vi i samband med MDT (Microsoft Deployment Toolkit). Dessa verktyg är alla nödvändiga förutsättningar för att WDS och distribution skall fungera överhuvudtaget.

Dessa verktyg är viktiga i det skedet när man skall skapa Capture images och skapa Installation images, och sedan distribuera dem på WDS servern för utdelning på domänen.

Vi använde oss även av vissa standardprogram på de testdatorer som fungerade som våra klienter i domänen.

Till dessa program hörde till exempel: Open Office, VLC Mediaplayer, drivrutiner till ljud och video mm. Anledningen av att vi använde oss av dessa standardprogram var att testa och undersöka hur bra det fungerade att distribuera hela operativsystem till andra datorer.

En annan anledning var att vi ville undersöka hur denna automatiserade distribuering av programvara och operativsystem kunde göra det lättare för Kökar kommun att administrera datorer i sitt nätverk.

7 Windows Server 2012 R2

Windows Server 2012 innehåller flera olika ”roller” som man kan installera, dessa roller (features/roles) är egenskaper med vilka man styr och utför systemfunktioner såsom säkerhetskopiering eller olika Active Directory tjänster.

Windows Server 2012 finns i olika versioner och egenskaperna i de olika versionerna varierar, därför bör man överväga vilken version man behöver.

Till exempel i de billigare versionerna som Windows Server 2012 Essentials och Foundation finns det inte möjlighet till Hyper-V, LDS(Lightweight Directory Services) och även antalet användare i systemet är begränsat.

En lista på de viktigaste rollerna i Windows Server 2012 är beskrivna i tabell 1 på nästa sida.

Tabell 1. Windows Server 2012 Roller.

Roll	**Beskrivning**
AD Certificate Services (AD CS)	Certifikattjänster
AD Domain Services (AD DS)	Tjänster för hantering av användare, resurser
AD Federation Services (AD FS)	Federation och enkel inloggning på webben
AD Lightweight Directory Services (LDS)	Katalogtjänst
AD Rights Management Services (RMS)	Tjänster för rättighetshantering
Application Server	Program/applikationsserver
DHCP Server	Dynamisk utdelning av IP-adresser
DNS Server	Domännamnssystem
FAX Server	Fax tjänst
File and Storage Services	Fil- och lagringstjänster
Hyper-V	Virtualisering
Network Policy and Access services (NPAS)	Nätverksprincip- och åtkomsttjänster
Print and Document Services	Tjänster för hantering av printrar och dokument
Remote Access	Fjärranvändningstjänster
Remote Desktop Services (RDS)	Fjärråtkomsttjänster
Volume Activation Services	Hantering av licenser
Web Server (IIS)	Webbservertjänst
Windows Distribution Services (WDS)	Distributionstjänst av Windows-Operativsystem
Windows Server Update (WSUS)	Uppdateringstjänst

Windows Server 2012 R2 finns i fyra olika versioner: Datacenter, Standard, Essentials, Foundation.

Skillnaden mellan virtualiseringsmöjligheterna i de olika versionerna är att de billigare versionerna Essentials och Foundations inte överhuvudtaget stöder virtualisering. Med virtualiseringsmöjligheter avses hur pass begränsade de olika versionerna av Windows Server är. Vi använde oss av Datacenter vilken kan skapa ett obegränsat antal virtuella instanser.

CAL (Client Access Licenses) är licenser som man behöver för att lagligt ansluta sig till en Windows server. Dessa licenser måste köpas skilt till Datacenter eller Standard versionen, men krävs inte för de andra versionerna eller om man ansluter sig anonymt via Internet till servern.

Själva operativsystemets licens ger inte alla användare rätt att koppla sig till servern fastän de är en del av samma organisation eller företag. Man behöv därför dessa CAL licenser för varje användare eller apparat som kopplar sig till servern.

I tabell 2 beskrivs de olika versionerna närmare samt vilka begränsningar de har. Priserna förändras så dessa räknade upp i tabellen nedanför är Microsofts egna riktpriser för produkterna.

Tabell 2. Översikt av Windows Server 2012 R2 versionerna.

Version	Egenskaper	Användare	Licensiering	Pris/licens
Datacenter	Obegränsad virtualisering. Alla tjänster.	per CAL	2x Processorer	6,155 $
Standard	Två virtuella instancer. Alla tjänster.	per CAL	2x Processorer	882 $
Essentials	Begränsad administration och tjänster. Ingen virtualisering	Max 25 användar-konton	Per server	501 $
Foundation	Begränsad administration och tjänster Ingen virtualisering.	Max 15 användar-konton	Per server	Enligt den slutliga försäljaren.

7.1 Roller och tjänster

I detta stycke kommer vi beskriva de viktigaste rollerna och tjänsterna som vi använde oss av i den praktiska delen av arbetet.

Dessa roller och tjänster är bara en del av alla de olika roller som finns i Windows Server 2012.

7.1.1 VPN (Virtual Private Network)

"Virtual Private Network" (VPN) är den teknik som används för att skapa en säker förbindelse, en "tunnel" av ett privat nätverk som kopplar ihop delade eller publika nätverk som t.ex. Internet. VPN tillåter data att skickas mellan två datorer över internet på ett sätt som emuleras av en punkt till punkt länk. (Tyson & Crawford, 2011.*)*

I dagens läge är Internet mer tillgänglig än någonsin då Internetleverantörerna utvecklar snabbare och mer tillförlitliga tjänster på löpande band. Då företag växer, kan de expandera till flera kontor eller t.ex. butiker över hela landet och runt om i världen.

Genom att komplettera med VPN anslutningar kan ett företag förlänga alla dess nätverksresurser till anställda som arbetar från avlägsna kontor eller på distans hemifrån.

VPN används också i hög grad som ett verktyg för att surfa anonymt på webben eller slingra sig undan blockeringar på nätverket. Man kan koppla sig till avlägsna VPN-servrar i t.ex. USA och därefter får man en ny, extern IP-adress ifrån USA. Det är bland annat tack vare VPN som t.ex. människor i Kina och andra diktaturer har kunnat undvika censurering av material på nätet.

För att hålla saker och ting igång effektivt, behöver de människor som arbetar på avlägsna platser ett snabbt, säkert och tillförlitligt sätt att dela information över datornätverk. Om de anställda dessutom t.ex. reser som säljare behöver de ett lika säkert och pålitligt sätt att ansluta till sitt företags datornätverk från avlägsna platser.

VPN tekniken använder sig att diverse olika protokoll för att skapa "tunnlar". De vanligaste protokollen är PPTP och L2TP som är baserade på det väldefinierade protokollet Point-to-Point Protocol (PPP).

L2TP är det protokoll som man föredrar då man använder sig av Windows server 2012 eftersom det kombinerar alla de bästa delarna av PPP med en teknik kallad Layer 2 Forwarding. (Morimoto et al. 2013 s. 495)

L2TP möjliggör inkapsling av data över flera nätverksprotokoll, inklusive IP, och kan användas som en tunnel över internet. Lasten (Payload) eller de data som skall överföras för varje L2TP ram (frames) kan komprimeras och krypteras för att spara bandbredd. (Morimoto et al. 2013 s. 495)

En VPN server kräver flera mindre roller och tjänster på DC servern, till dem hör: RAS-, NPS, Certifikat och Active Directory tjänsterna. Dessa kan vara på samma server så som vi gjorde i vår försöksmiljö. Det fungerade visserligen, men RAS (Remote Access Control) rekommenderas ändå att lokaliseras på en separat server. "NPS" står för Network Policy Server som är en annan tjänst som också krävs för att VPN skall fungera.

Med certifikat menar man att en server fungerar som en "CA" (Certificate Authority) vilket betyder att den skickar ut certifikat för andra servrar och klienter. Dessa certifikat behövs vid autentisering (inloggning på domänen) och krypteringen av t.ex. en VPN tunnel. Dessa olika tjänster och roller berättar vi om mera när vi kommer till praktiska delen av arbetet. (Morimoto et al. 2013 s. 464)

CA server rollen behövs främst när VPN skall tas i bruk. Rekommendationen är att detta installeras på en skild server av säkerhetsorsaker pga. att den innehåller alla certifikat som ett företag eller domän äger.

En VPN förbindelse skulle fungera perfekt för Kökars kommun då man i dagens läge pratar om eventuella sammanslagningar av små skärgårdskommuner och ökat samarbete överhuvudtaget.

En VPN förbindelse ger möjlighet att öppna en krypterad tunnel/länk mellan alla kommunens inrättningar. En anställd inom kommunen kan då vara stationerad på t.ex. omsorgshemmet Sommarängen och arbeta med en kollega i Kökars socialbyrå eller i en annan kommun och dela filer och information på samma sätt som om deras fysiska skrivbord skulle stå bredvid varandra. (VPN, En krypterad tunnel till företaget, u.å.)

Det är viktigt att kommunanställda kan använda sig av en säker förbindelse mellan kontoret och platsen där de själva jobbar ifrån. Många gånger kan det vara fråga om känslig information som berör personer, klienter, ekonomi eller överhuvudtaget konfidentiella uppgifter.

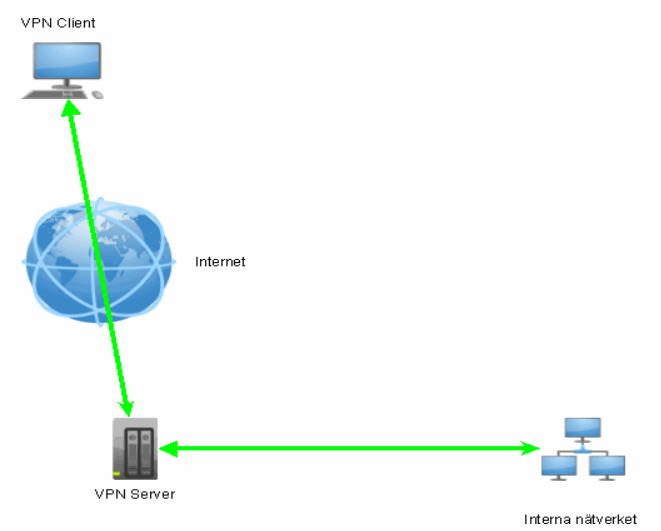
Genom VPN kan de anställda komma in på Kökars domän, via VPN tunneln, och sedan komma åt dokument, filer, printrar osv. var de än finns, förutsatt att de har tillgång till internet. Med en VPN, (illustrerat i figur 2) skapas en privat länk mellan klienten och VPN servern genom att kryptera data så att den blir konfidentiell.

Eftersom VPN kräver rätt hög kapacitet av servern så kan det uppstå problem med kapaciteten vid omfattande trafik, speciellt om kommunerna slås ihop och serviceställena därmed ökar väsentligt. I så fall kan användarantalet approximativt växa till flera hundra.

I så fall borde man överväga att anskaffa en skild server som enbart kör VPN tjänsten för att balansera belastningen på huvudservern. Alternativt kan man uppgradera hårdvaran i väsentlig grad på huvudservern för att klara av att köra så många tjänster inklusive VPN.

Det skulle finnas ett behov för en säker VPN uppkoppling pga. att kommunens anställda ofta rör på sig, och inte sitter vid sitt skrivbord vid en stationär dator hela tiden.

Med andra ord blir den data som skickas mellan servern och klienten oläsbar utan de korrekta krypteringsnycklarna, vilket gör att de data som skickas via länken blir säkrare, även data som rör sig genom Internet är oläsbara om man inte har krypteringsnyckeln. (Thyson och Crawford, 2011.)



Figur 2. Exempel på uppbyggnad av ett VPN.

7.1.2 DHCP

Vi började med att konfigurera DHCP servern i vår Windows Server 2012 miljö genom att planera vårt eget IP-adresschema. Det betydde att vi var tvungna att fundera ut hur många IP-adresser det skulle finnas, alltså hur många användare och apparater det skulle finnas i nätverket och utgående från det bestämma vilken klass av nätverk de behöver.

I och med att kommunen har rätt få anställda valde vi att använda oss av ett klass C nätverk vilket innebär att det skulle kunna finnas 254 användare (datorer eller utrustning med egen IP) där 192.168.0.0 står för lokala nät. Om sammanslagningar av kommuner genomförs så måste man fundera om. (Andersson, 1999)

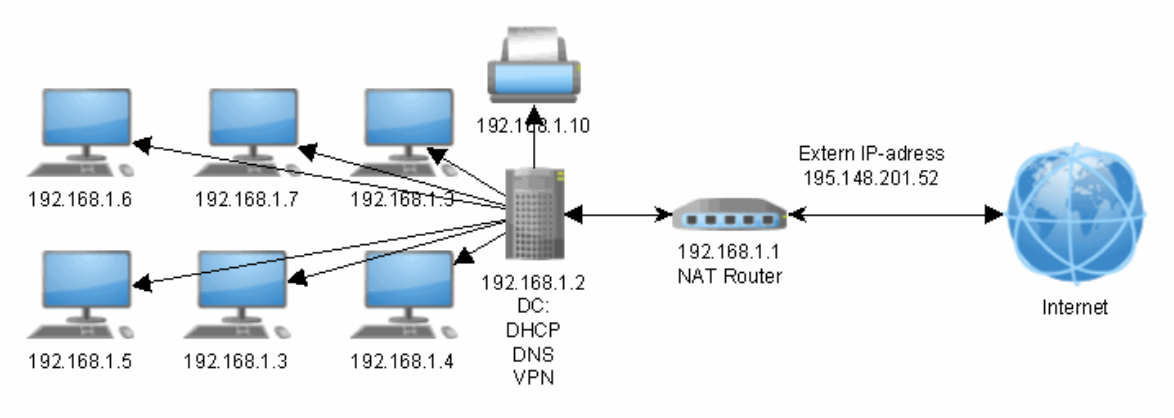
Eftersom kommunen i nuläget inte har mer än 50 anställda och endast vissa apparater behöver ha statiska (fasta) IP-adresser, kommer IP rymden att räcka mer än väl. Orsaken till att vanliga arbetsstationer kan ha dynamiska (rörliga) IP-adresser är att de inte kör några viktiga roller eller tjänster såsom DC servern eller bibliotekets server kör.

Till exempel måste själva DC servern ha en statisk IP-adress, eftersom man konfigurerar resten av nätverket att ha kontakt med och arbeta mot DC serverns specifika IP-adress.

Även printrar och andra server-roller kräver statisk IP-adress då programvara konfigureras till låsta IP-adresser. Övriga datorer och apparater kan ha dynamiska IP adresser i domänen. Det spelar ingen roll vilken IP-adress en enskild användare har för sin t.ex. dator eller läsplatta.

”192.168.1.1” var IP adressen i vår Default Gateway (router), men då använde vi oss av vår egen DHCP och DNS server vilka hade samma IP-adress (192.168.1.2) som vår DC. Det är också här som NAT kommer med in i bilden. I figur 3 beskriver vi strukturen för nätverket.

NAT (Network Address Translation) möjliggör för en apparat, till exempel en router, att fungera som representant mellan Internet och ett lokalt (eller "privat") nätverk. Detta innebär att endast en unik IP-adress behövs för att representera en hel grupp av datorer. (Tyson, 2001.)



Figur 3. Exempel på uppbyggnad av ett nätverk med DHCP server.

Vi ville att alla datorer, förutom övriga server-roller eller printrar, skall erhålla dynamiska IP-adresser av vår DHCP server. Detta innebär att IP- adressen inte är låst till en viss dator inom nätverket. DHCP-, DNS och AD rollerna kan vara på helt olika servrar eller boxar på nätverket om man tycker och rekommenderas. Om det besluts att sprida ut rollerna på olika servrar/DC kan man länka dem till huvud DC-servern och styra rollerna i från den.

Vi beslöt att arbeta med alla tjänster på samma server eftersom syftet med arbetet inte är ett enormt system för stora mängder användare, utan kanske för högst 50 användare. Kökar servers kapacitet kommer att räcka förutsatt att inte antalet användare stiger mycket.

En annan viktig sak att tänka på då man installerar en DHCP server är modemet eller ISP routern som vidarekopplar till Internet och gör så att vi kan bläddra mellan olika webbsidor på nätet.

Det finns ofta färdigt inställda eller installerade DNS- och DHCP tjänster i själva modemet. Dessa måste stängas av eftersom de kommer att installeras på servern. Om samma tjänst förekommer dubbelt kan det förorsaka problem då de stör varandra.

7.1.3 DNS

DNS är en viktig infrastrukturell komponent till en Windows-servers nätverksuppbyggnad. Man kan säga att DNS är grunden för det som binder ihop Internet och alla TCP-IP nätverk tillsammans.

DNS fungerar som ett slags tolk som är kvalificerad att läsa domän- eller värdnamn till IP-adresser. DNS huvudsakliga uppgift är alltså att översätta domännamn till IP-adresser.

Active Directory kräver att man har DNS inställt och installerat på servern för att det skall fungera korrekt, inte bara för AD utan för många andra tjänster.

I vårt fall kommer inte DNS servern översätta adresser ut över Internet utan bara på det interna nätverket för att underlätta åtkomst till printrar och diverse nätverksutrustning.

En dator bryr sig egentligen inte om domännamnet hos en internetadress, t.ex. ”www.google.com”, utan det som en dator refererar till är IP-adressen, tex. nummerserien ”192.168.1.1”. Användarna har däremot betydligt enklare att komma ihåg namnet på en webbsida, t.ex. ”www.Novia.fi” som är avsevärt lättare att komma ihåg än IP-adressen ”193.166.227.6”.

DNS servern kopplar alltså ihop domännamn med IP-adresser. Innan man kan skapa en Active Directory domänkontrollant måste man se till att DHCP körs på servern och att DNS är aktiverat.

7.1.4 Windows Deployment Services

Windows Deployment Services (WDS) är en servertjänst som gör det möjligt att massdistribuera Windows operativsystem via en nätverksbaserad installation, vilket betyder att man inte behöver installera varje operativsystem via CD/DVD eller USB.

Man kan även skräddarsy en egen windowsinstallation där man färdigt kan lägga till specifika program och eventuella drivrutiner för olika syften samt inställningar för domänen. (Rollen Windows Deployment Services, 2008)

Eftersom man kan automatisera processen så pass mycket underlättar det också arbetet för IT-administratörerna då de inte behöver konfigurera och installera datorer enskilt. I dagens läge har Kökars kommun inget standardsystem för varken program eller datorkonfigurationer. Med hjälp av WDS skulle man kunna effektivera både support och distribution av diverse funktioner och program.

För att WDS skall fungera korrekt behövs en del tilläggsfunktioner, t.ex. måste Windows Deployment Service-servern antingen vara medlem i AD DS-domänen eller vara en domänkontrollant för en AD DS-domän. Detta betyder att endast datorer som är med i domänen har tillgång till Deployment service-funktionerna.
(Rollen Windows Deployment Services, 2008)

Man måste också ha en fungerande DHCP-service eftersom WDS använder sig av PXE (Pre-Boot Execution Environment) med DHCP för att förse datorer med IP-adressering, vilket gör det möjligt att boota datorer med hjälp av ett nätverkskort utan att den fysiska maskinen är beroende av en lagringsenhet såsom t.ex. en hårddisk eller ett operativsystem.

Det här sker med hjälp av en dators BIOS som anropar WDS servern som i sin tur skickar ett svar till maskinen med en adress till en bootloader. WDS kräver även att DNS rollen skall vara installerad på server. (Preboot Execution Environment, *u.å*)

7.1.5 Typer av WDS Images

WDS i Windows Server 2012 innehåller flera typer av images. Med en image menar man en avbildning, i det här fallet systemavbildningar. Man kan använda images till att distribuera Windows installationer, säkerhetskopiering, kopiera program till DVD/CD mm. I WDS finns det tre olika typer av images: Boot, Installation och Capture images.

Boot images innehåller själva WDS klienten och Windows installationen, det kallas Windows Preinstallation Enviroment (Windows PE). Windows PE är ett s.k. “mini” operativsystem som används för att kontakta systemet till WDS servern och det ger en möjlighet att välja och sedan installera en WDS image. (Morimoto et al. 2013 s. 1025)

Dessa Boot images kan hittas bland filerna för operativsystemets installation eller CD/DVD-skivor. Boot imagen heter normalt “boot.wim” och en viktig sak att komma ihåg är att vi som i vårt experiment använde oss av Windows 7 som operativsystem för våra klientdatorer, var tvungna att använda oss av en boot image som är x64, alltså har 64bits arkitektur.

Det går alltså inte att använda en x86 image för att distribuera en x64 installation. En tumregel är att man använder en boot.wim som överensstämmer med, eller är nyare än, installationsavbildningens operativsystem.
(Introduktion till Windows Deployment Services, 2008.)

Installation images utgör hela Windows paketet som innehåller all installationsmedia som är insatt i en WIM fil. Dessa images kan skräddarsys för att innehålla även andra program och inställningar som man kan välja när man gör själva installationen av operativsystemet på en dator. (Morimoto et al. 2013 s. 1025-1026)

En WDS server behöver oftast bara en x86 och en x64 boot image, men man kan ha flera olika slags installationsimages beroende på vilket behov man har.

Om man till exempel vill ha en Windows 7 installation på en arbetsdator med stränga restriktioner så att den inte kan koppla sig till internet, eller en installation som har Windows 8.1 med alla rättigheter osv.

Capture images är skapade i från en boot image, men istället för att köra en installationsimage, så kör en capture image ett WDS Capture program. Detta program är ett verktyg som man skapar en installation image ifrån en referensdator. Verktyget klonar en dators operativsystem, samt installationer och även rättigheter man inställt i registret. (Morimoto et al. 2013 s. 1026)

För att skapa en Capture image måste man dock först förbereda en dator för det. Detta görs via ett verktyg som heter Sysprep (System Preparation tool). Man kan automatisera processen av förberedelsen genom att skapa Task Sequence (installationssekvens) som kan automatiskt köra Sysprep och klona operativsystemet.

Efter att man har kört Sysprep och gjort en Capture image så skickas den nyskapade “capture.WIM” filen till WDS servern över nätverket. Det är först efter att man har tillgång till Capture imagen på WDS servern som man kan börja skräddarsy den med specifika program, inställningar, licenser osv. som man sätter in i ”.WIM” filen.

Därefter är avbildningen färdig för distribution på servern och redo att delas ut till användare på nätverket.

Processen för distributionen är automatiserad. Detta betyder att man kan bygga en helt "tyst" installation av ett operativsystem som sköter allting själv, beroende på vad man har förinställt att avbildningen (Installation image) skall göra.

Som exempel kan man ha en installation där man i ett grafiskt gränssnitt förutom operativsystemet kan välja vilka program man vill ha inkluderat med operativsystemet.

Denna metod gör att en arbetstagare som första gången sätter sig vid sin arbetsdator bara behöver starta datorn och den tar då själv kontakt med WDS servern samt påbörjar Windows installationen automatiskt.

7.1.6 DC (Domain Controller)

Anledningen till att man skapar en domän och har domänkontrollanter är för att den håller kontroll över allting inom en Windows Server-domän. Man kan även använda dessa domänkontrollanter (domain controllers) till exempel för att ändra någon användares lösenord på nätverket, skapa olika användarkonton eller datorkonton och så vidare.

Active Directory fungerar med en sk. "Multiple-Master" modell. Den första domänkontrollanten man skapar i en domän blir den som har alla roller av Operations Master, vilken innehåller fem olika typer av roller: Schema master, PDC emulator, Domain naming master, Infrastructure master och Relative identifier (RID) master.
(Clines & Loughry, *u.å.*)

Dessa roller kan delas ut till olika domänkontrollanter i domänen men bara en DC kan ha en specifik roll åt gången. Alla roller kan även behållas på en DC, men det kan inte finnas flera olika av samma roller i domänen eller skogen.

8 AD DS (Active Directory Domain Services)

En AD domänkontrollant verifierar och godkänner alla användare/användning av datorer i en Windows-domän samt tilldelar och upprätthåller säkerhetsprinciper för alla datorer och användare.

Man kan säga att Active Directory är en säkerhetstjänst, det är den tjänst som tillåter administratörerna att skapa användare, grupper och organisationsenheter (Organisational Unit) och tilldela resurser till specifika användare och grupper.

Till exempel när en användare loggar in på en dator som är med i vår Windows-domän, kontrollerar Active Directory om användaren är med i användarregistret, kontrollerar lösenord och avgör sedan om användaren är en administratör eller vanlig användare vilket bestämmer vad användaren har för rättigheter. (Morimoto et al. 2013 s. 118-119)

Med hjälp av AD kan man ge användare tillstånd att använda olika apparater såsom en skrivare eller scanner på nätverket, eller t.ex. ge användarna tillstånd att använda en delad fil eller mapp.

Man kan också begränsa användarnas tillgång till diverse olika funktioner, t.ex. förhindra att en specifik användare eller grupp kan ändra bakgrundsbild eller ha åtkomst till kontrollpanelen eller mappar. (The Logical Structure of Active Directory, 2003)

8.1 Grupper och Organisationsenheter

En grupp är en samling av användar- och datorkonton och kan bestå av andra grupper som kan hanteras som en helhet. Användning av grupper skulle göra det lättare att administrera Kökars nätverk och användare, eftersom man med hjälp av grupper kan dela in användare och datorer enligt kategorier.

Införandet av grupper underlättar administrationen av nätverket, eftersom man kan kombinera användarnas datorer och till och med andra grupper i en enda grupp och sedan fördela specifika tillstånd och säkerhetsprinciper för den enskilda gruppen. (Så här fungerar gruppkonton, 2008.)

Grupper i AD DS är katalogobjekt som finns i en domän och i vad man kan kalla organisationsenhetsbehållare (Organizational units)**.** Organisationsenheter är Active Directory behållare i vilka man kan placera användare, grupper, datorer och andra organisationsenheter.

En organisationsenhet kan inte innehålla objekt från andra domäner. Med hjälp av organisationsenheter kan man skapa behållare inom en domän som representerar organisationens hierarkiska och logiska struktur.
(Så här fungerar organisationsenheter, 2008)

För att sedan kunna ge en viss OU speciella rättigheter används GPO (Group Policy Objects). Låt oss anta att Kökar skulle slås samman med andra kommuner och skulle ha tusen anställda i en omfattande kontorsmiljö och alla tusen anställda skulle ha samma behörigheter och säkerhetsaspekter för sina konton.

Istället för att behöva konfigurera varje användarkonto och tilldela rättigheter och säkerheter kan man enkelt tilldela rättigheter och säkerhet till en kontorsgrupp och sedan bara lägga till användarna i den gruppen.

Om man har administratörer i nätverket som man vill att skall ha behörighet att administrera datorer och skrivare och allt vad det innebär, kan man skapa en administratörsgrupp och sedan helt enkelt lägga till de specifika användarna till den gruppen.

Så i princip behöver man inte administrera varje användarkonto, man kan istället administrera grupper. Det innebär att då man gör ändringar i en grupp istället för att göra ändringar till ett användarkonto åt gången så kan man göra ändringar till sex eller varför inte 1000 användarkonton på en och samma gång.

Man kan alltså lägga till användare eller datorer eller till och med grupper in i en annan grupp och istället för att ge alla användare och datorer enskilda rättigheter ge en hel grupp alla de specifika rättigheterna på en gång. Detta sparar tid vid administrationen av nätverket och effektiverar verksamheten väsentligt.

8.2 Säkerhet

När man talar om säkerhet inom AD är det en helt annan sak än externa säkerhetsrisker, så som virusskydd och brandväggar osv. Säkerhet i det här fallet fokuserar på vilka rättigheter användarna har och vad de kan göra för ändringar på själva datorsystemet.

Till exempel: har användaren rätt komma åt kontrollpanelen, kan de ändra bakgrundsinställningar, kan de installera eller ta bort program. Till och med användningen av CD-stationen i en dator kan begränsas.

Dessa rättigheter kan delegeras via Group Policy Management konsolen i Active Directory. Detta kan förebygga problem om man har skapat en bra administrativ "template" som betyder en slags mall vilken innehåller inställningar, konfigurationer mm. för operativsystemet.

Det finns färdiga mallar man kan välja eller så kan man tillverka en egen så som vi gjorde i vår experimentmiljö och som vi beskriver närmare i praktiska delen av arbetet. Kökar har i dagsläget ingen liknande lösning på detta men vi anser att det finns ett behov av det eftersom det skulle minska säkerhetsriskerna i domänen.

Dessa rättigheter delas ut automatiskt i samband med att man loggar in på domänen, så om någon skulle försöka göra något intrång på någon annans dator eller rensa bort filer på datorn, skulle de inte helt enkelt få tillgång till det. Det beror förstås på hur man har inställt Group Policies och hur stränga de är.

8.3 Rättigheter

Då man talar om rättigheter avser man användarnas eller datorernas tillgång och användning av nätverksresurser. Dessa användarrättigheter delas oftast ut till olika Grupper (Security Groups), inte till specifika användare. Efter man tilldelat rättigheter till vissa grupper går det enkelt att placera användare i de grupper dit de passar.

I vårt arbete skapade vi flera grupper. Det fanns grupper för marknadsföring, vanliga arbetstagare och även en grupp för begränsad åtkomst på domänen. Den begränsade gruppen kan användas i ett företag till exempel för gäster eller för arbetstagare som kanske är föremål för samarbetsförhandlingar och riskerar att få lämna företaget.

Gruppen som är begränsad kan t.ex. inte komma åt vissa filer eller får kanske inte printa ut något, medan en annan grupp såsom till exempel marknadsföringsgruppen kan ha fullständig tillgång till alla funktioner.

En annan positiv sak med grupper är at då användarna är placerade i olika grupper kan de inte per automatik gå in på andra gruppers dokument eller filer. Det här kan naturligtvis variera beroende på vilka rättigheter man gett åt grupperna. Ofta har företag dock gemensamma och delade mappar som alla grupper i företaget kan komma åt. Dessa delade mappar kan naturligtvis också regleras och åtkomsträttigheterna begränsas.

Exempel på användarrättigheter: Har användarna rätt att se dokument, kan de läsa filer, har de rätt att se en delad mapp, skall de ha rätt att kunna komma åt en delad fil på nätverket, skall de ha rätt att kunna redigera den delade filen eller har de till exempel tillgång till en skrivare i nätverket.

8.4 Roaming Profiles

När man talar om "roaming profiles", alltså profiler, avser man alla inställningar och konfigurationsfiler och mappar för ett användarkonto i användarregistret för Active Directory.

Till exempel: vad finns det för programinställningar, vad finns inne i "Mina dokument", vilka filer och mappar finns på skrivbordet, vilken bakgrundsbild finns det, hur ser skärmsläckaren ut? Det här är alla exempel på typer av data som en profil kan innehålla.

Det som "Roaming-profiles" gör är att de låter användarna komma åt sina profiler oavsett vilken dator de loggar in med på nätverket. Det betyder att om användaren loggar in vid en specifik dator och ändrar bakgrundsbilden och sedan loggar ut och loggar in på en annan dator så kommer de få samma bakgrundsinställningar som de tidigare konfigurerat på den första datorn. (*Orfano, 2011.)*

Dessutom kommer användaren ha tillgång till alla sina mappar och alla andra konfigurationer de haft rättigheter att göra. "Roaming-profiles" gör att vi alltid har tillgång till vår skräddarsydda profil oberoende av vilken dator man loggar in med bara den är med domänen.

“Roaming-profiles” är ett utomordentligt användbart verktyg i en miljö där alla användare inte är “låsta” vid enskilda datorer utan fritt kan röra på sig och använda vilken dator de själva tycker.

Ett bra exempel är skolor eller kontor där det finns så mycket användare att alla inte har en bestämd arbetsplats eller dator. Tack vare “Roaming-profiles” kan användarna komma tillbaka till arbetsmiljön och bara sätta sig vid första bästa dator som inte är upptagen och fortsätta jobba.

Användarna sätta sig ner vid vilken som helst av datorerna i nätverket och logga in med sin egen anpassade profil och göra ändringar. När de sätter sig vid en annan dator följer alla dessa förändringar med dem. Det här är en anledning till att man kanske vill använda “Roaming-profiles” i dessa ovan nämnda miljöer.

En annan anledning till att vi valde att använda “Roaming-profiles” är att det avsevärt förbättrar arbetseffektiviteten hos de anställda och därmed även företagets kostnadseffektivitet då de anställda alltid har möjlighet att jobba utgående från den situation där man tidigare slutat.

Med “Roaming-profiles” kan vi ge den anställda vars dator har gått sönder en ny dator så de kan fortsätta jobba oavbrutet.

Om användare enbart har lokala profiler när de sätter sig vid en annan dator och loggar in i nätverket så kommer de att få upp en standardkonfiguration, oavsett vilken annan dator i nätverket de loggar in på, förutom den de ursprungligen gjorde inställningarna på. (*Orfano, 2011.)*

De kommer inte att ha andra mappar, ingen annan bakgrundsbild, bara Windows standardkonfiguration eftersom all profilinformation lagrades lokalt på den dator som de loggade in med från början.

En negativ sak med “Roaming-profiles” är att det inte sparar program i en profil. Med andra ord så kommer det som man installerat på en enskild dator inte att migreras med som en del av din profil. En annan negativ sak med “Roaming-profiles” är att desto större domän man har desto mera kapacitet kommer “Roaming-profiles” att använda eftersom “Roaming-profiles” sparar och laddar information varje gång en användare loggar in och ut från sin profil. (Morimoto et al. 2013 s. 1094)

Det här löste vi lokalt i vårt experiment genom att färdigt se till att alla datorer har standardapplikationer installerade på de enskilda arbetsstationerna. Användarna vet då att de har tillgång till de program som de behöver för att kunna jobba på sina datorer.

9 Förbättringar i nätverksoperativsystem

Huvudsakligen går vårt förbättringsförslag ut på att installera en central server som körs med Windows Server 2012 R2. Vi föreslår att denna server placeras på en central plats som t.ex. kommunkansliet. Denna server blir en så kallad. domain-controller "DC" som innehåller alla viktiga moduler och tjänster som: VPN, DCHP, DNS, säkerhetskopiering, fil-server osv.

Dessa olika tjänster kan också delas ut till andra serverdatorer vid behov. Det här skulle vi rekommendera för att minimera riskerna för långsamma anslutningar inom domänen och för att inte överbelasta bandbredden för servern vid hög trafikintensitet.

Vi tror att tack vare att det är så få användare kan allting tillsvidare skötas ifrån den befintliga servern, och vi testade också vårt arbete med bara en enda huvudserver som körde allt. Om kommunen besluter sig för att använda VPN i nätverket så rekommenderas det att ytterligare servrar skaffas pga. att VPN är kapacitetskrävande om antalet användare stiger.

Om trafiken ökar och antalet användare i domänen stiger, samt om systemen uppgraderas med ny hårdvara så kunde man köra tjänster som t.ex. en Lync-server (videokonferens) och/eller VPN. Den nuvarande servern skulle kunna hantera en VPN tjänst utöver de andra viktiga rollerna och tjänsterna, men den kanske bara kan hantera ett tiotal VPN anslutningar åt gången.

Att bygga ut systemet går enkelt eftersom det är möjligt att koppla en ny server till domänen, om det kommer fram att kommunen behöver t.ex. en Lync- eller SQL server.

En möjlighet är att en sådan installeras på en skild serverdator med Windows Server 2012 och Active Directory, och att det sedan skapas en förbindelse med centrala servern och den andra servern läggs till i domänen.

Därefter är de nya tjänsterna som tex. Lync videokonferenstjänsten klar för användning för alla användare i domänen. På samma sätt kan tex. VPN-tjänsten flyttas till en separat server vid behov, om inte kapaciteten på huvudservern räcker till. Därmed får man balanserad trafik, serverbelastningen minskar och tjänsterna fungerar bättre.

Kommunens hårdvara behöver inte nödvändigtvis uppdateras eftersom den stöder Windows Server 2012. De användare som efterhand ansluter sig till nätverket t.ex. via VPN opererar med Windows 7 eller äldre operativsystem så åtkomsten till nya servern och nätverket skulle inte vara något problem.

Denna förnyelse skulle initialt egentligen inte kosta så mycket för kommunen, förutom anskaffning av programvara, men vi tror att det skulle främja samarbetet och eventuella sammanslagningar av skärgårdskommunerna eller åtminstone göra det enklare att i framtiden bygga vidare på nätverket och infrastrukturen i kommunen och mellan kommunerna.

Detta skulle allting ske genom att vi skulle skapa en lokal domän (intranät) för Kökar som är säkrad med krypterade VPN anslutningar. På så sätt skulle alla anställda, oberoende var de finns, kunna ansluta sig till domänen och få tillgång till vissa program, material och nätverksresurser som är lagrade på den centrala servern i kommunkansliet.

Själva användningen skulle centraliseras och administrationen skulle minska betydligt då användarna har sina egna rättigheter “permission” och säkerhetspolicy ”security policy”. Det betyder att användarna har en specificerad åtkomst till filer eller har behörighet att ändra vissa saker på den lokala datorn och lagra filer på ett eget hemområde.

Detta skulle också betyda att t.ex. omsorgshemmet Sommarängens filer skulle sparas på den centrala servern i kommunkansliet istället för på den lokala dator de anställda har till förfogande idag, vilket i sin tur betyder mycket bättre datasäkerhet och fungerande säkerhetskopiering. Eftersom fiberanslutning finns till förfogande skall den datamängd som skickas inte vara något problem.

Denna nätverksstruktur skulle även minska på vissa kostnader såsom t.ex. ny programvara eftersom man kan installera ett program på centralservern som sedan kan delas ut till användare i domänen via WDS (Windows Deployment Services).

Som exempel kan man ta Office paketet som kan installeras på centralservern som en sk. “image” och som därefter kan distribueras ut till alla datorer i nätverket och installeras färdigt på deras datorer, allt fjärrstyrt från centralservern.

Ett annat exempel är att uppdateringar såsom Windows Updates kan skötas helt via Active Directory på servern, och därefter uppdateras alla datorer i domänen automatiskt.

Med samma teknik som ovanstående fungerar användarprofilerna för de som är registrerade på domänen. Alla dokument och all information sparas på centralservern. Man får tillgång till dem från vilken dator som helst så länge man är kopplad till nätverket och inloggad på domänen.

Även installation av nya arbetsstationer och deras programvara kan man skräddarsy. En färdig installation kan utföras genom att göra en s.k. “image” av operativsystemet som t.ex. kan innehålla standardprogram som alla datorer skall ha eller drivrutiner och olika konfigurationer.

Dessa förinstallationer, “images”, sparas på centralservern och kan sedan enkelt distribueras via nätverket till datorer inom domänen.

Med denna metod kan man automatisera installationerna av nya arbetsdatorer i domänen och även underhålla dem med uppdateringar osv. Detta har kommunen inte möjlighet till i nuläget men skulle, som vi ser det, absolut ha behov av det.

Vi tror att detta system skulle underlätta kommunens dataverksamhet betydligt. Det skulle bli både säkrare och mycket enklare i framtiden att lösa gemensamma dataproblem. Det skulle också underlätta om man vill bygga på nätverket och utvidga det med andra servrar, som tex. en egen E-postserver eller en Lync (video konferens) server och så vidare.

10 Skog- och domändesign

Före man börjar bygga upp en domän och ett nätverk måste man planera strukturen för dem. Kökar har för tillfället inget nätverksoperativsystem som styr nätverket eller någon domän så situationen kan bara förbättras för dem.

Active Directory strukturen som håller objekten kan betraktas på flera nivåer; Skogen, träd och domän är de logiska indelningarna i ett Active Directory-nätverk.

En ”skog” är en samling av ”träd” som delar en gemensam global katalog, katalogschema, logisk struktur och katalogkonfiguration. Ett träd är en samling av ett eller flera domäner och domänträd i ett sammanhängande namnområde sammanlänkade i en hierarki.

En domän definieras som en logisk grupp nätverksobjekt (datorer, användare, enheter) som har samma Active Directory databas.

Före man börjar bygga upp ett nätverk och domän, måste man planera strukturen för den. Det finns flera olika domäntyper. Den typ som skulle täcka behoven för Kökar kunde vara “Single Forest, Single Domain” modellen som illusteras i figur 4.

De fördelar som denna modell har jämfört med andra är säkerheten och kostnadseffektiviteten. Denna metod har också mindre säkerhetsrisker. Tack vare att det finns bara en domän behövs det inte lika mycket hårdvara som det skulle behövas för flere.

Kökar har inte något behov för flera olika domäner. Möjligtvis kan behovet uppstå i framtiden men det kan lösas genom att utvidga domänmodellen så som det illustreras i figur 5.

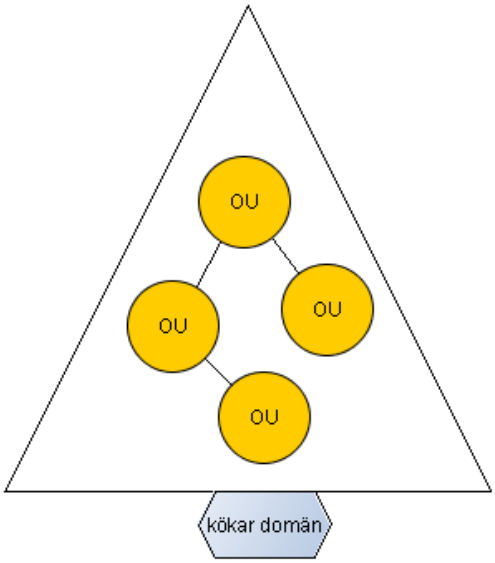
Figur 5 åskådliggör att vid eventuella sammanslagningar i framtiden, om exempelvis en annan kommun som Sottunga vill ha en egen domän, kan den anslutas till “Root” domänen (Kökar). I detta fall skulle de olika domänerna ha sina domännamn, DNS, AD men för att de befinner sig i samma skog så skulle den nya domänens AD vara länkad till den andra. Förutom att flera domäner skulle vara sammanlänkade i Active Directory, så finns det en eller flera fysiska servrar i en domän, vilket medför kostnader.

På den här nya servern i Sottunga “site” som man kallar den platsen där fysiska servrar ligger, skulle finnas en DC med AD installerat och de tjänster som behövs lokalt.

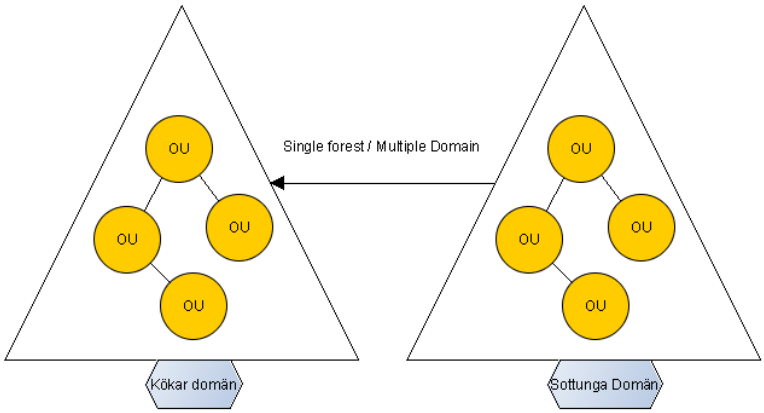
Men själva globala katalogen för hela skogen och andra inställningar styrs från domänen Kökar. En orsak till att domänerna behöver sina egna DC servrar är att det minskar bandbredden och replikationstrafiken mellan domänerna.

Med replikation avser man att delar av katalogträdet som innehåller data om domäntjänster replikeras mellan domänkontrollanterna. De alltså skickar information till varandra och alla domänkontrollanter blir sk. “peer”-datorer i en domän och hanteras som en enda enhet. (Förstå den logiska Active Directory-modellen, 2008.)

Replikation hjälper alltså att hålla data synkroniserat mellan domänkontrollanter och man kan planera en tidtabell för när de skall replikera, oftast blir det när det är lågtrafik i nätverket som sent på kvällen eller på natten.



Figur 4. Single Forest, Single Domain model.



Figur 5. Single Forest, Multiple Domain model

För detta projekt i vår försöksmiljö skapade vi en sådan struktur som skulle passa bäst för en kommun med ganska få användare, därmed skulle trafiken i nätverket bli ganska låg. Skog- och domänmodellen “Single Forest, Single Domain” passar bäst i detta fall.

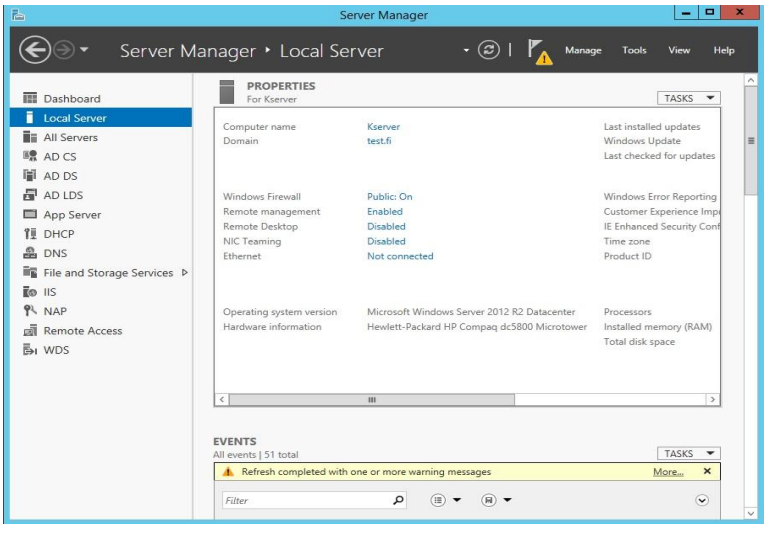
Även om det skulle slås samman kommuner behöver de eventuellt inte flera domäner. Möjligen behövs extra domänkontrollanter med uppgiften att balansera trafiken i nätverket genom replikation, eller kanske någon kommundel till exempel vill ha en SQL-server till sitt förfogande.

11 Installation och konfiguration

Vi började arbetet med att ladda ner Windows Server 2012 R2 mjukvaran från Dreamspark. Installationen av Windows Server 2012 kräver att en hårdskiva formateras och en ny “partition” skapas på hårdskivan där all mjukvara sparas.

Till vårt förfogande hade vi en hårdskiva med drygt 230 GB utrymme, vilket är mer än tillräckligt för själva operativsystemet. En basinstallation av Windows Server 2012 R2 kräver ca 11 GB utrymme på hårdskivan.

Det rekommenderas att man har mycket större hårdskivor i verkliga situationer på grund av att de olika Windows Server rollerna i sig själva har stora krav på hårddiskutrymme. Efter att Windows installationen var klar, skapade vi ett administratörskonto och lösenord till det. I figur 6 ser man hur Server Manager ser ut efter installationen av operativsystemet.

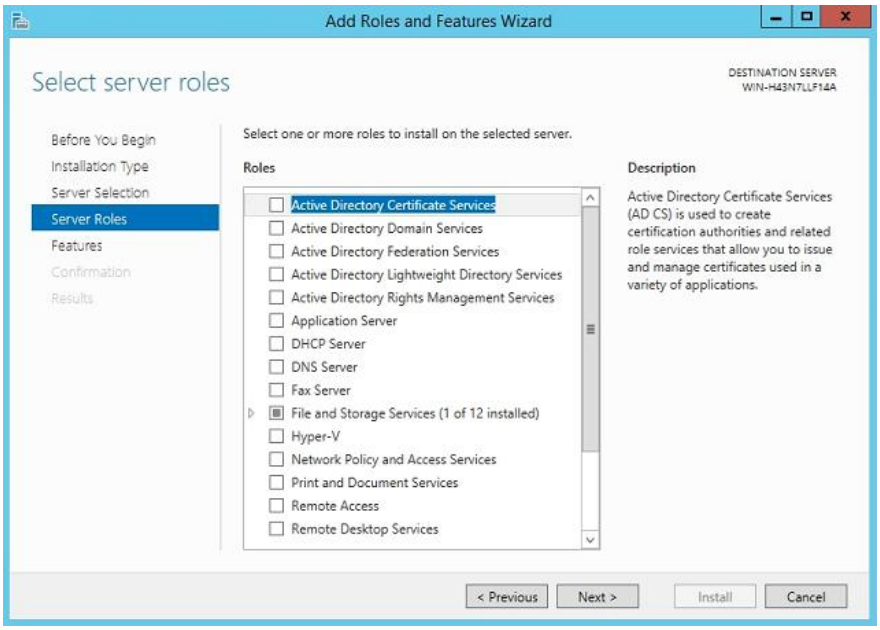


Figur 6. Windows Server 2012 R2 och dess Server Manager efter installation.

Då installationen var klar och administratörskontot skapat började vi installera alla de olika serverrollerna och -tjänsterna vi behövde. Då vissa roller kräver att andra roller är installerade i förväg måste vi inledningsvis ha installerat rollerna i en viss ordning.

Förrän man kan börja installera VPN eller någon annan roll måste DNS och DHCP rollerna vara installerade och konfigurerade. Det är väldigt viktigt att man har de olika mindre rollerna och tjänsterna i gång och rätt konfigurerade som krävs för att de större rollerna skall fungera.

För att installera roller i Windows Server 2012 börjar man med att öppna "Server Manager" och väljer "Add roles and Features" i verktygsmenyn (Tools). Efter att en ny ruta öppnats väljer man vilka roller man vill ha genom att trycka på dem. (Demonstreras i figur 7)



Figur 7. Installation av roller och tjänster.

I den nyskapade rutan väljer man de roller som man först vill installera, i vårt arbete valde vi inledningsvis DNS, DHCP, Fil- och lagringstjänster. Orsaken till valet av dessa roller är att de krävs för att komma igång med Active Directory Domain Services. Fil- och lagringstjänsterna är också nödvändiga eftersom vi skulle ha en fil-server på vår domänkontrollant.

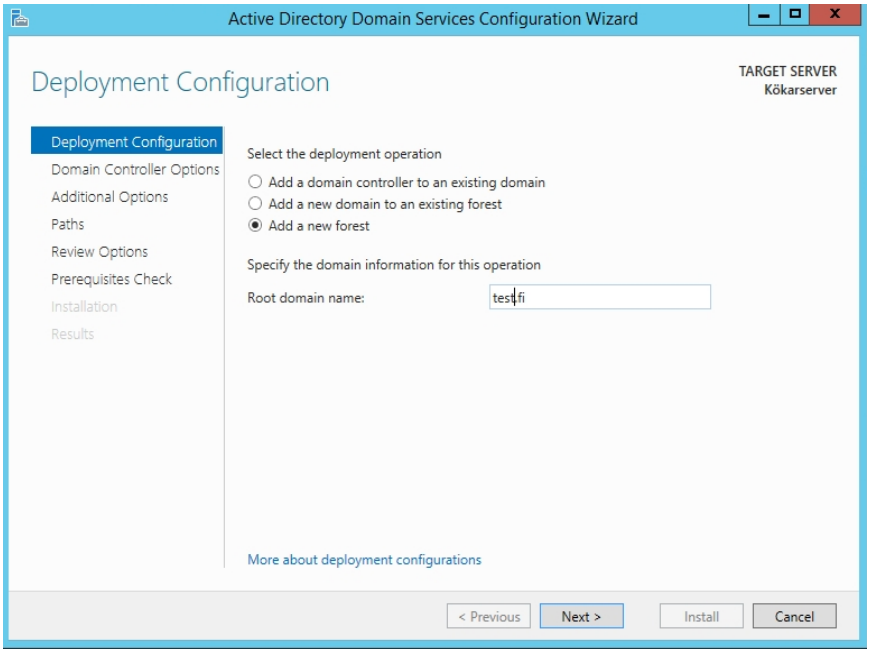
Man måste komma ihåg att roller kan vara installerade på servern men de fungerar inte förrän man har konfigurerat dem skilt för sig. Ofta kräver det också att man startar om servern eller själva tjänsten för att de skall komma igång.

Vi fortsätter arbetet med att gå igenom alla faser gällande installationerna och konfigurationerna av alla roller i den ordning vi gjorde det och som det rekommenderas att man gör.

11.1 Active Directory Domain Services

Eftersom vi inte hade någon domän eller skog från tidigare valde vi alternativet att skapa en helt ny skog och domän, vilket man ser i figur 8. Namnet på domänen har inte någon större betydelse eftersom vi arbetade inom ett testlaboratorium, dock måste namnet sluta med en domänbetecking t.ex. ".fi" eller ".com". I arbetslivet namnger man domänen oftast efter företagets namn.

Före Active Directory installationen föredras det att man ändrar namnet på datorn om inte den redan har ändrats. Vi döpte vår server till "Kökarserver". Detta blir också namnet för själva domänkontrollanten, så i framtiden blir det enklare att hålla koll på alla servrar om man har flera domänkontrollanter.



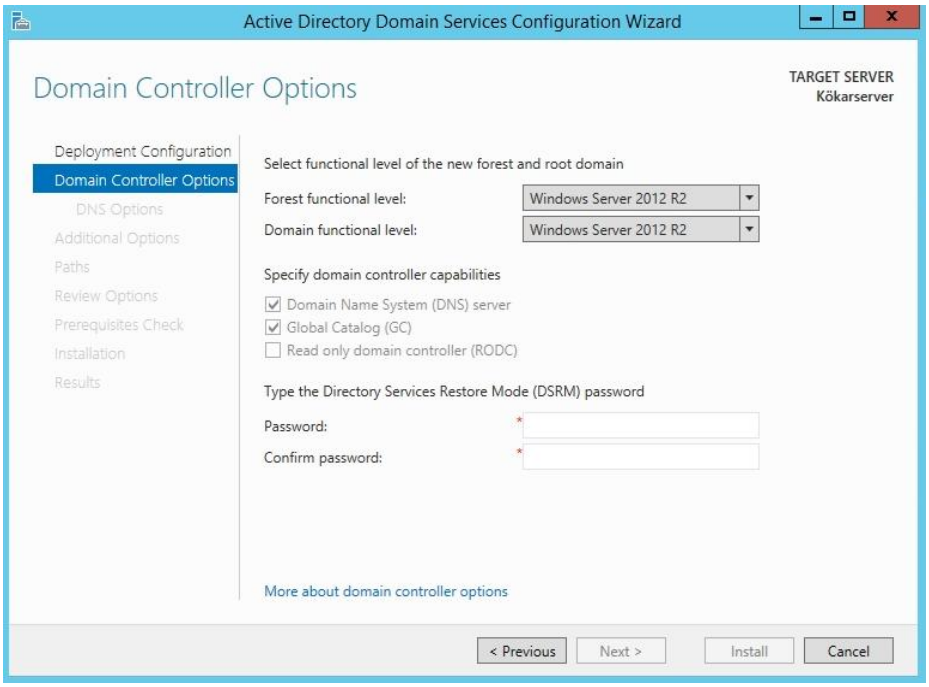
Figur 8. Skapande av domän och skog.

Nästa steg (figur 9) av konfigurationen är att man väljer funktionalitetsnivån (functional level) för både domän och skog. Orsaken till att man väljer en viss funktionalitetsnivå är att om man från tidigare har en server med t.ex. Windows Server 2008 så måste man sänka nivån så att den stöder den gamla servern om man vill ha den kopplad till domänen och AD.

Eftersom vi byggde ett helt nytt nätverk lämnade vi bara rutorna som de är, då vi endast använde oss av Windows Server 2012 R2. Det här är första servern och DC i domänen som betyder att det blir en sk. "Root domain", därför går det inte att trycka bort rutorna som är gråa. Av samma orsak, att det är den första servern i domänen, kan servern inte heller bli en RODC (Read-Only Domain Controller), och man vill att den skall kunna skriva också.

Ett DSRM (Directory Services Restore Mode) lösenord måste också anges i denna ruta. Det rekommenderas att man skriver ner lösenordet någonstans för det är viktigt att ha kvar om någonting går fel i framtiden.

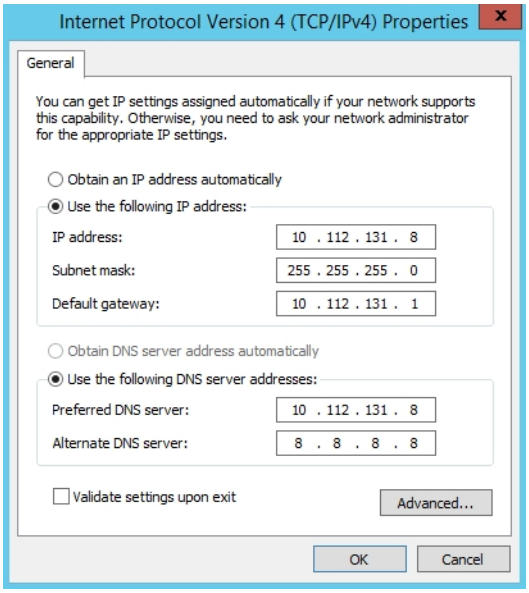
Efter man har fyllt i de ovanstående uppgifterna så trycker man på "nästa" och man behöver inte ändra på någonting annat. "DNS Options" behöver man inte heller bry sig om i det här skedet för vi konfigurerar DNS skilt.



Figur 9. AD DS - Funktionalitetsnivån.

11.2 DHCP

DHCP krävs för att man skall kunna installera Active Directory och skapa en domän. Inledningsvis måste man konfigurera en statisk IP-adress för servern. För att komma åt IP-adress inställningarna går man till kontrollpanelen i Windows och söker upp nätverksanslutningarna (Network Connections). I figur 10 ser man inställningarna för IP-adresserna där vi gjorde inställningarna för vår server.



Figur 10. Statisk IP-adress konfiguration.

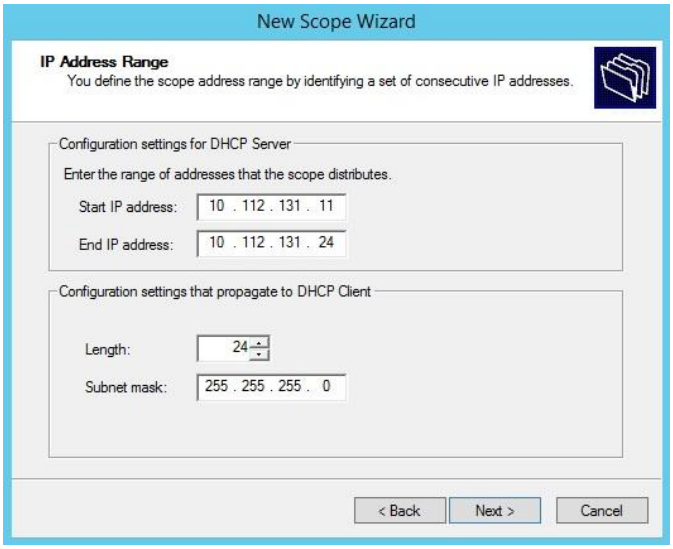
Om man jobbar med ett litet nätverk, såsom vi gjorde, är det viktigt att det bara finns en (1) aktiverad DHCP server, annars kan det uppstå problem med IP-adresserna. Det här betyder också att vi var tvungna att stänga av routerns inbyggda DHCP server, annars förorsakar det problem och vår skapade DHCP på servern skulle inte fungera.

I större nätverk kan man ha flera DHCP servrar som kommunicerar med varandra, men i mindre nätverk som i Kökars kommun skulle en DHCP server räcka till.

I vårt nätverk i vår försöksmiljö hade vår server IP-adressen “10.112.131.8”. Vårt modem (Default Gateway) hade IP-adressen “10.112.131.1”.

Som DNS adresser hade vi vår servers IP-adress som den primära DNS servern, för vi kommer att konfigurera den på vår server. Den sekundära DNS servern definierade vi till “8.8.8.8” vilket är IP-adressen till Googles öppna DNS server.

För att reservera IP-adresser skapade vi en sk. “Scope” vilken begränsar antalet IP-adresser som får delas ut i nätverket. IP-adresserna sparas i en adressbehållare “Address Pool”. Dessa IP-adresser som demonstreras i figur 11 är alla de IP-adresser som servern kan delas ut till andra datorer eller användare i domänen.



Figur 11. Exempel på IP-adress Scope.

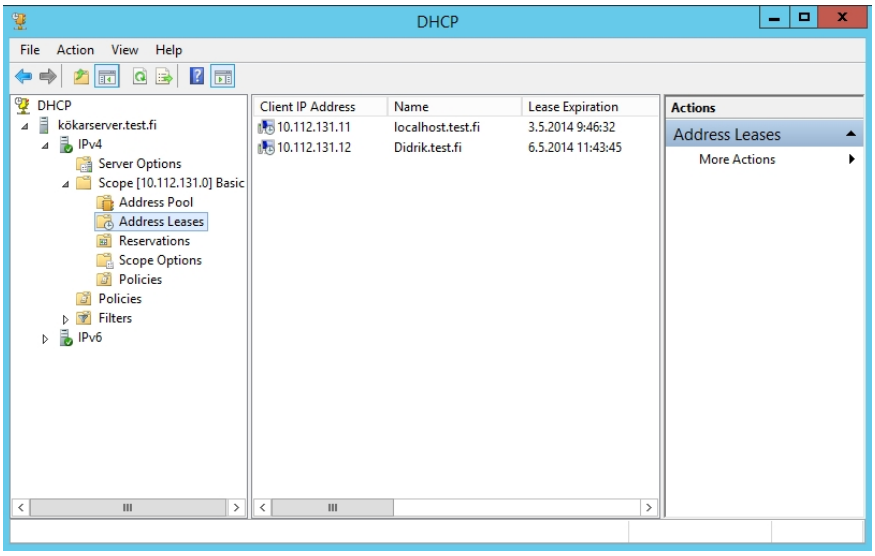
I figur 12 på nästa sida visas några anslutna klientdatorer i domänet som har fått en IP-adress utdelad av DHCP servern. Som man ser finns inte de statiska IP-adresserna för t.ex. servern eller printern med i listan. Orsaken att man vill hålla de statiska IP-adresserna utanför adressbehållaren är för att undvika konflikter med IP-adresser inom domänen.

Om man ändå väljer att ha de statiska IP-adresserna med i adressbehållaren så är det genomförbart genom att exkludera ett visst omfång av IP- adresser inom adressbehållaren.

Efter att man har konfigurerat adressbehållaren kan man välja IP-adressens utgångsdatum (Lease Expiration). Med “Lease Expiration” menar man hur länge IP-adresserna är i kraft för en viss dator eller andra mobila enheter som telefoner och läsplattor.

Det rekommenderas att dessa utgångsdatum sätts till ungefär så lång tid som man beräknar att en användare kommer att använda sin dator.

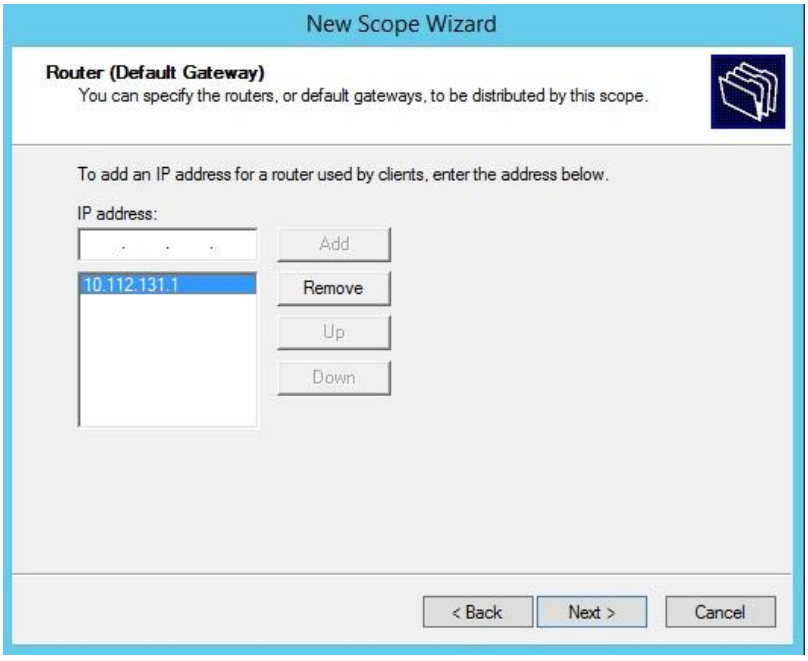
För mobila enheter gäller det att lägga ett kortare utgångsdatum (några timmar) så att man inte riskerar att adress behållaren blir full. För att skräddarsy utgångsdatum för enskilda enheter måste man skapa egna “Policies” för dem, det här beskriver vi dock inte i arbetet.



Figur 12. Användare anslutna till DHCP servern.

Efter att man valt utgångsdatum för IP-adresserna kommer följande steg där man blir frågad om man vill konfigurera dessa alternativ. I det här skedet skall man fylla i IP-adressen till den Default Gateway som skall användas.

I vårt fall hade Default Gateway IP-adressen “10.112.131.1”. Det finns även stöd för flera Default Gateways men i en liten miljö som vårt testlaboratorium behövde vi bara en Default Gateway. I figur 13 demonstreras Scope Wizard konfigurationen för Default Gateway.

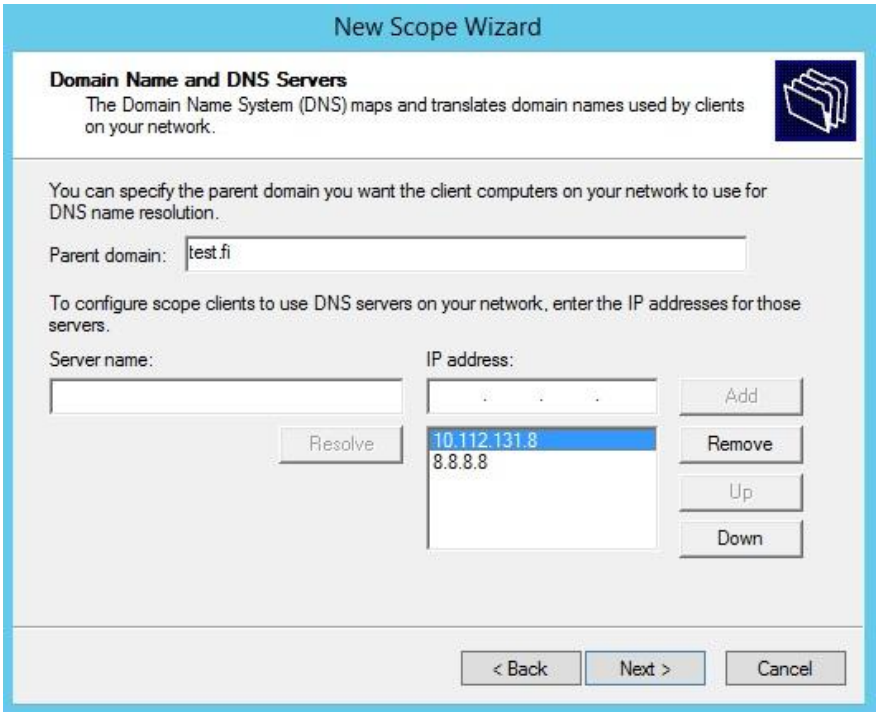


Figur 13. Default Gateway inställning.

I följande ruta som demonstreras i figur 14, skall man fylla i information om DNS servrarna. Dessa DNS servrars IP-adresser kommer att delas ut i samband med DHCP adresserna. Vi valde att den primära DNS servern skulle vara vår server som vi startat upp.

Som sekundär DNS server valde vi Googles öppna DNS server men man kan lika väl använda internetleverantörens DNS server.

I vanliga fall brukar man sätta ett modem eller en router som sekundär DNS server, om modemet stöder funktionen. Man har även möjlighet att lägga till nya DNS servrar om det finns flera i nätverket.



Figur 14. Konfiguration av DNS servrarna i Scope.

11.3 DNS

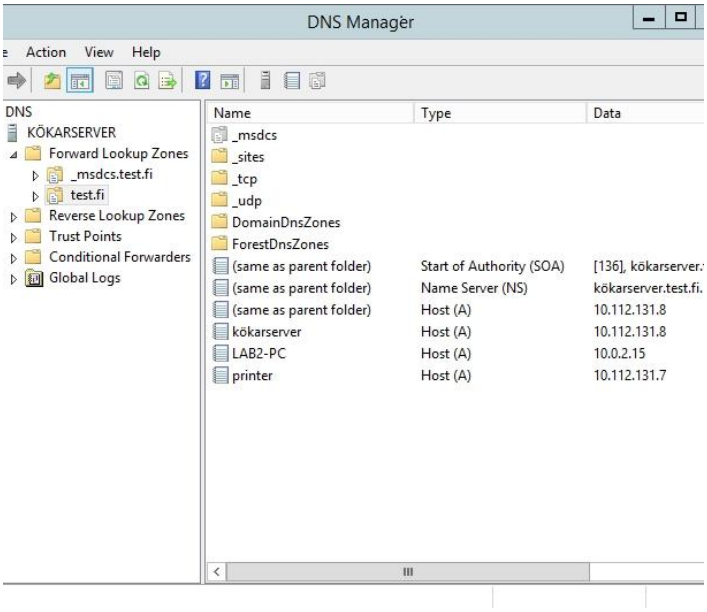
Efter att DHCP är konfigurerat färdigt, måste man konfigurera DNS. DNS inställningarna kommer man till genom att öppna Server Manager i Windows Server 2012, och välja "DNS" i verktygsmenyn.

I figur 15 på nästa sida visas hur DNS Manager rutan ser ut efter man öppnat den. Vår domän är i vänstra fältet "Test.fi" och den är markerad så innehållet visas i högra fältet.

Man kan lägga till eller ta bort enheter genom att högerklicka på domännamnet och välja "New Host". Serverns IP-adress och namn finns från början i listan. Vi valde att lägga till en nätverks-printer till domänen genom att specificera dess IP-adress och helt enkelt ge den namnet "Printer". "LAB2-PC" som finns i listan är en klientdator i form av en virtuell installation av Windows 7 på en laptop.

Det som DNS gör är att den associerar IP-adresser till domännamn så t.ex. printern vi lade till har nu en IP-adress som är "10.112.131.7" och domännamnet "printer.test.fi".

Det här betyder att en användare kan komma åt printern genom att ange IP-adressen eller "printer.test.fi" domännamnet. I figur 15 ser man vilka enheter som fanns i vår servers DNS Manager.



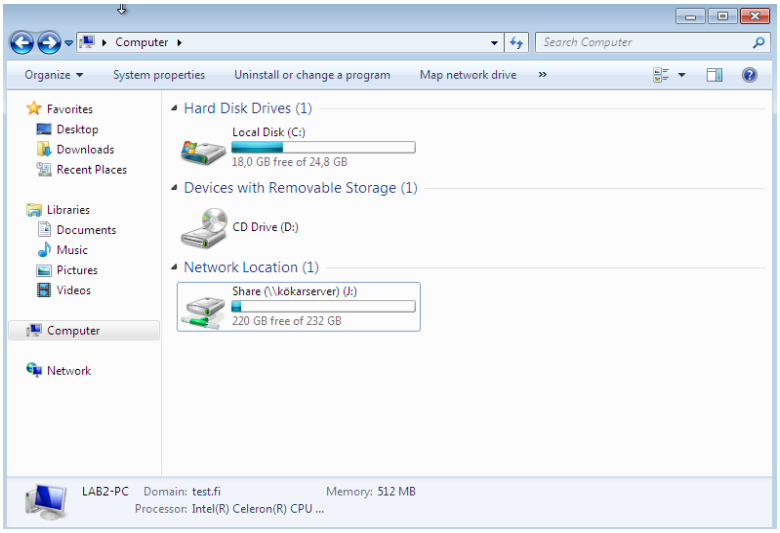
Figur 15. Exempel på hur DNS Manager ser ut.

Tack vare DNS kan användare nu ansluta sig till en printer och även till själva servern, "Kökarserver" som vår server hette. Man kan nu komma åt dokument och delade filer på t.ex. huvudservern genom att lägga till en nätverksenhet och ange IP-adressen "kökarserver.test.fi" eller skriva "\\kökarserver\ i adressfältet.

Man kan på samma sätt dela printern och sedan skulle man även kunna se printern när man försöker printa ut någonting. Det skulle bli dock jobbigt att alltid vara tvungen att göra detta manuellt på varje dator så man kan automatisera processen genom WDS.

I vår testmiljö skapade vi "Capture images" i WDS och konfigurerade dem färdigt så att de redan innehöll alla delade nätverksresurser och man hade automatiskt t.ex. printern till förfogande.

Exempel på det delande av nätverksresurser genom DNS i figur 16.



Figur 16. Exempel på en delad nätverksresurs.

11.4 Anslutning av datorer till domänet

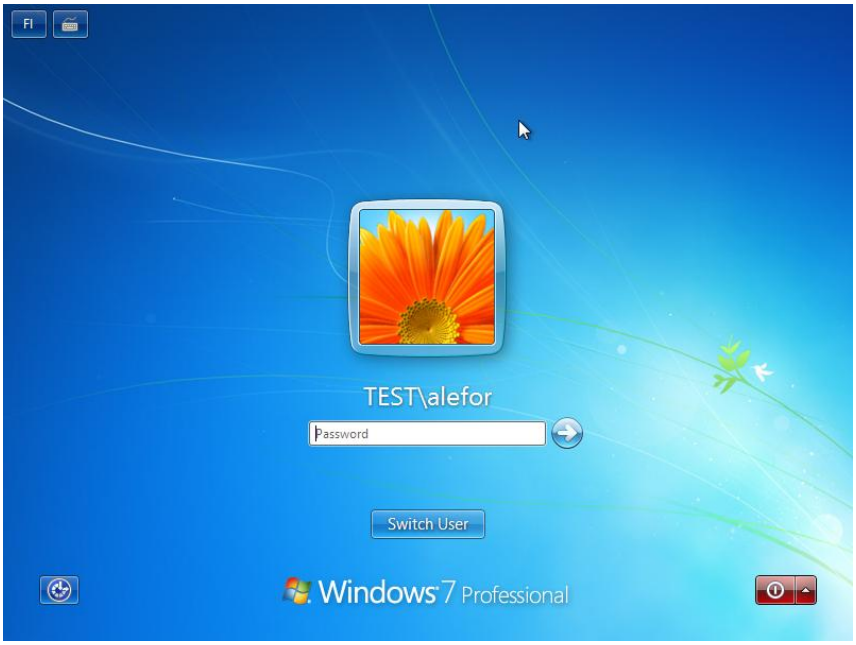
Då man skapar en domän måste man först ansluta klientdatorer till själva domänen istället för den standard "WorkGroup" som är färdigt konfigurerad på Windows operativsystemen.

Det här gör man genom att ha en Active Directory domänkontrollant och en dator med ett Windows operativsystem som har versionen Professional eller bättre. Datorn måste även vara ansluten i samma nätverk för att kunna ansluta till Windows Server domänen. I vårt fall anslöt vi några Windows 7 Professional datorer till vår "Test.fi" domän.

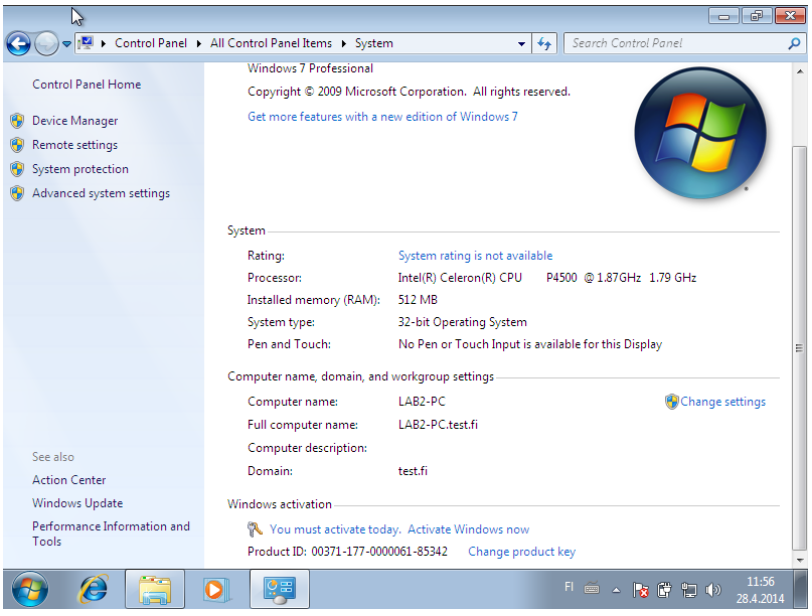
Anslutningsprocessen kan automatiseras via WDS, men i och med att det här var den första datorn vi anslöt till domänen, gjorde vi det manuellt. Det här gör man genom att klicka på kontrollpanelen och sedan på systemikonen.

Eftersom att datorn inte ännu är ansluten till domänen står det WorkGroup istället för domännamnet. Man klickar sedan på "Change settings" och fyller i uppgifterna för domänen. Då man har satt in rätt uppgifter startar datorn om.

Efter en omstart har användaren möjlighet att logga in med sina användaruppgifter på domänen. Figuren 17 nedanför demonstrerar hur det ser ut när en dator har anslutits till en domän och kan logga in. I figur 18 ser man hur system fönstret ser ut efter man anslutit en dator i domänet (Test.fi).



Figur 17. Exempel på inloggning till ett domän.



Figur 18. Exempelbild på en dator som har gått med i ett domän.

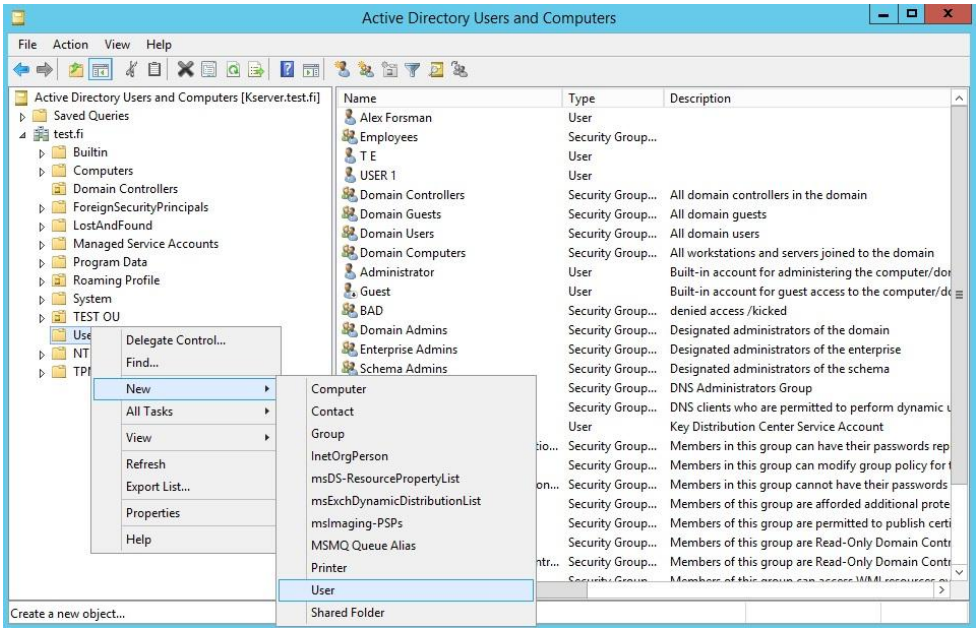
11.5 Användarkonton i Active Directory

Efter man har konfigurerat Active Directory och lagt till datorer till domänen måste det skapas användarkonton för samtliga användare. Man kan välja att skapa användarkonton på servern i Active Directory eller alternativt då man ansluter sig till domänen kan man använda den anslutande datorns användarkonto som sedan blir överförd till Active Directory.

I vår nyskapade domän beslöt vi att skapa alla användarkonton på servern i AD. För att börja lägga till nya användare går man till Server Manager och i verktygsmenyn klickar man på "Active Directory Users and Computers".

I Active Directory Users and Computers rutan ser man på högersida hela AD katalogen som innehåller domännamnet och alla datorer samt domänkontrollanter. I behållaren "Users" finns alla standard säkerhetsgrupper (Security Groups) och användarkonton. I behållaren kommer även alla nya användarkonton som skapas.

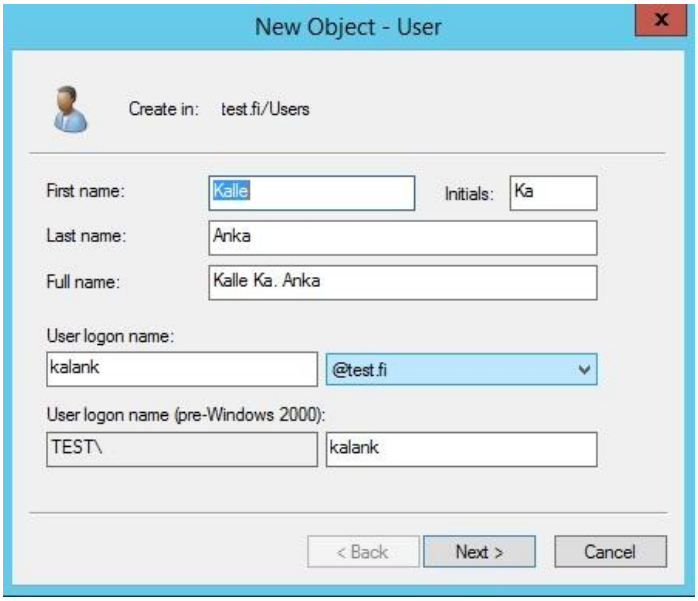
Om man högerklickar på "Users" och väljer "New User" i menyn kan man skapa ett användarkonto. I samma meny skapar man även grupp- och datorkonton mm. vilket illustreras i figur 19.



Figur 19. Exempel på skapandet av användarkonton i AD.

När man har valt att skapa en ny användare kommer en ruta upp där man skall skriva in namn och lösenord samt inloggningsnamnet.

Dessutom finns det möjlighet att välja om lösenordet måste ändras då användaren loggar in för första gången i domänen, detta rekommenderas av säkerhetsorsaker. I figur 20 nedanför demonstreras vilka uppgifter som skall fyllas i när man skapar ett konto.



Figur 20. Exempel på hur man skapar ett användarkonto.

Efter att användarkontot är skapat kan en användare logga in på domänen med sitt användarnamn och det lösenordet man ställt in. Det innebär att användarens dator har gått med i domänen på så sätt som beskrevs i förra kapitlet.

Man kan även automatisera detta för Kökar kommun med hjälp av WDS "images" som är färdigt konfigurerade med inställningarna för domänen. Vi gjorde försök med både WDS och vanlig anslutning till domänen och båda fungerade.

11.6 Grupper i Active Directory

Grupper är viktiga för användare i t.ex. ett företag eller i Kökars kommun eftersom det möjliggör bättre administrativ kontroll över användarnas rättigheter i domänen. Förutom att gruppera användarkonton i samma grupp enligt anställdas arbetsuppgifter eller

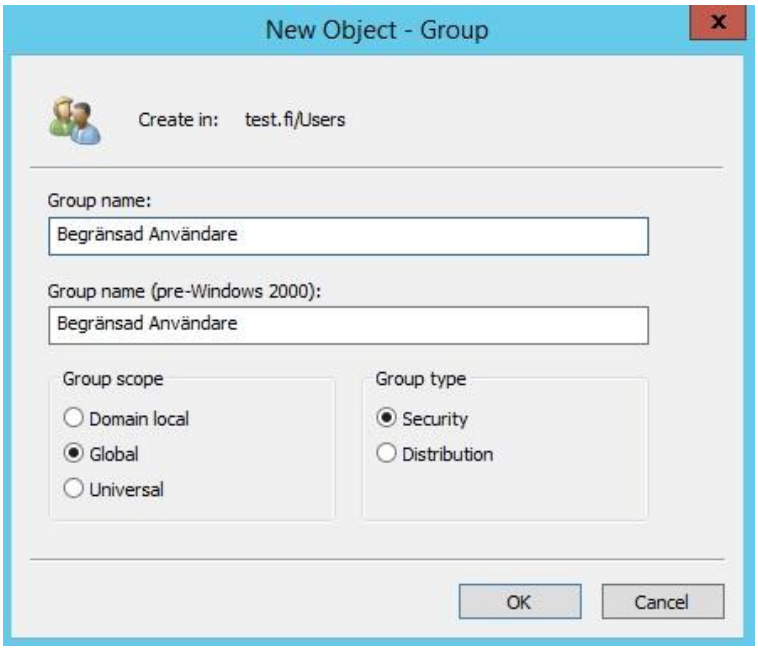
avdelning som t.ex. marknadsföring eller bokföring, kan man även begränsa användarnas åtkomst till olika nätverksresurser.

Det finns två typer av grupper: Security Groups och Distribution Groups. Man kan förbättra säkerheten med hjälp av säkerhetsgrupper (Security Groups). Det gör man genom att lägga in användarkonton eller andra grupper i Security Groups som kan innehålla specifika rättigheter eller begränsade åtkomsträttigheter till nätverksresurser.

Distribution Groups använder man främst för att samla användarkonton och information för att skicka e-post till användare inom domänen. För att dra nytta av Distribution Groups används t.ex. Microsoft Exchange. (Microsoft, 2005. Group types)

Vi jobbade för det mesta med säkerhetsgrupper. För att skapa en säkerhetsgrupp måste man gå till "Active Directory Users and Computers" i verktygsmenyn. Sedan går man till samma meny som i förra kapitlet men i detta fall väljer man att skapa en ny grupp.

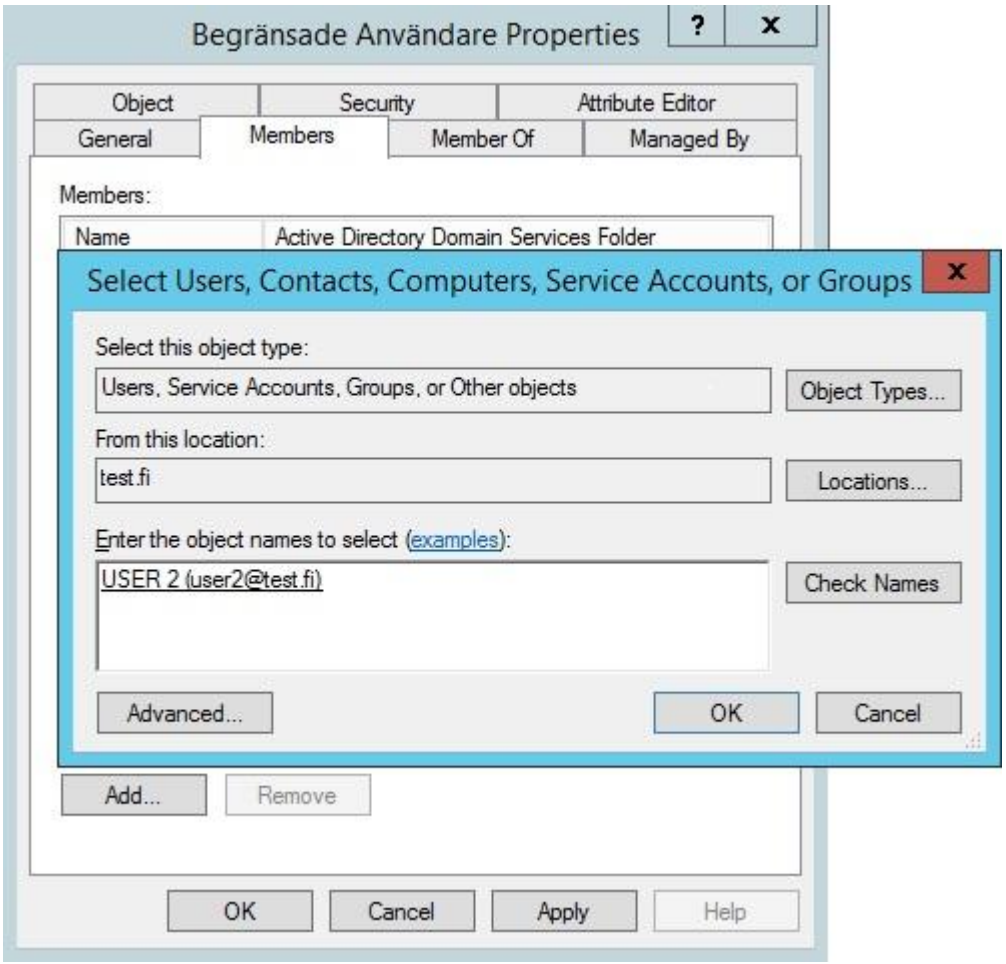
Efter man har valt att skapa en ny grupp öppnas en ny ruta i vilken man definierar vilket namn gruppen skall ha, gruppens "scope" och gruppens typ vilket man ser i figur 21. Det som menas med "Group scope" är hurudan räckvidd eller gräns som gäller för gruppen. (Microsoft, 2014. *Group scope.)*



Figur 21. Exempel på hur man skapar en säkerhetsgrupp.

Efter man har skapat en grupp kan man börja lägga till användarkonton eller andra grupper in i den nya gruppen. I figur 22 lägger vi som exempel till en användare (USER 2) till gruppen Begränsade Användare.

I vårt exempelfall gjorde vi en grupp som hade begränsad ankomst till nätverksresurserna på servern. Användarna i säkerhetsgruppen kunde t.ex. inte komma åt privata dokument och privata mappar på servern, utan enbart till de delade "Public" dokumenten.



Figur 22. Insättning av användare/objekt i en säkerhetsgrupp.

11.7 Skapa OU och GPO i Active Directory

För att underlätta administrationen av olika grupper och användare i ett domän kan man skapa organisationsenheter (OU) vilka fungerar som behållare för grupp- eller användarkonton.

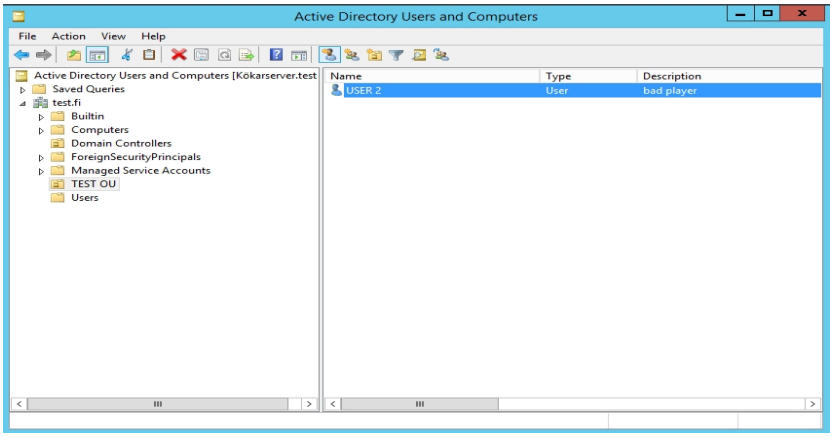
Även datorer och andra objekt kan sättas in i en organisationsenhet. Group Policy Objects (GPO) länkar man sedan till organisationsenheterna för att ge rättigheter och säkerhetsinställningar till en användare eller till en hel grupp. Som exempel kan man neka installation av vissa program eller användandet av vissa funktioner, användandet av CD-stationen och dylikt.

För att börja med skapandet av organisationsenheter öppnar man Server Manager och i verktygsmenyn väljer man "Group Policy Management". I Group Policy Management trycker man på domännamnet och väljer i menyn "Create a new OU".

I vårt arbete skapade vi en OU som hette "Test OU". Efter man har skapat en organisationsenhet måste man välja vilka användare eller datorer som skall höra till organisationsenheten. För att lägga till användare i organisationsenheten går man till "Active Directory Users and Computers" som finns i verktygsmenyn i Server Manager.

För att flytta användare till nya organisationsenheten som skapats går man till "Users" mappen och högerklickar på användaren eller gruppen och väljer "Move" i menyn. I "Move" menyn väljer man organisationsenheten.

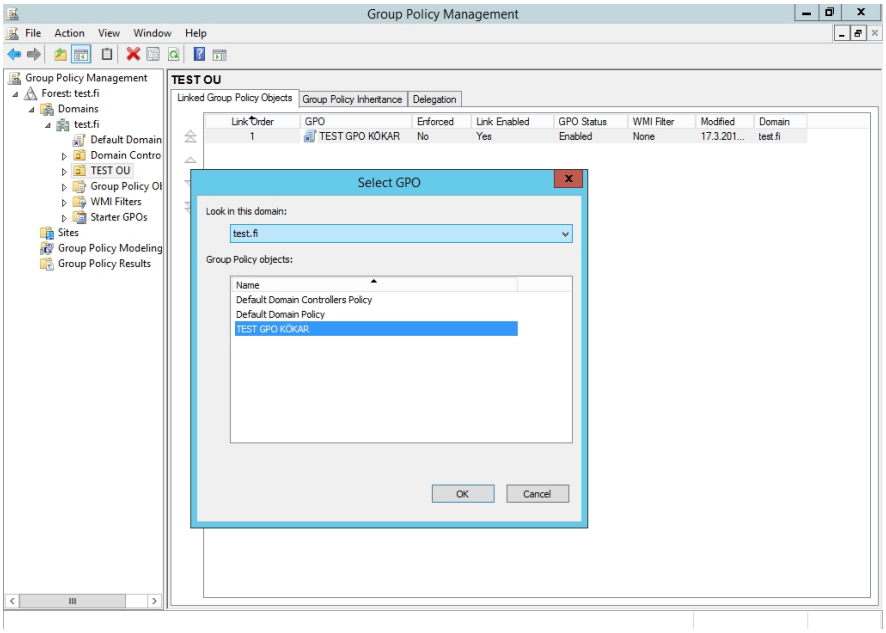
Vi lade in "USER 2"-användarkontot i vår organisationsenhet "Test OU", för att vi ville begränsa användandet för användarna i "Test OU" som demonstreras i figur 23.



Figur 23. Gruppering av användare i en OU.

Som nästa steg skall man skapa ett grupprincipsobjekt (GPO). Det gör man genom att öppna Group Policy Management rutan och välja "Group Policy Objects" i listan och högerklicka på den, och i menyn välja "New Organisational Unit".

Vi gav vår GPO namnet “Test GPO”. För att själva GPO skall fungera måste den länkas till en OU, det gör man genom att högerklicka “Test UO” som skapades och välja “Link to an existing GPO”. I rutan som öppnas väljer man den GPO som man vill ha från listan. Figur 24 visar processen där man skall välja grupprincipsobjektet.



Figur 24. Länkning av GPO till en OU.

I det här skedet gör GPO ingenting ännu. Man måste först lägga till säkerhetsinställningar och rättigheter för den. För att konfigurera GPO öppnar man Group Policy Management rutan och högerklickar på GPO och väljer “Edit”.

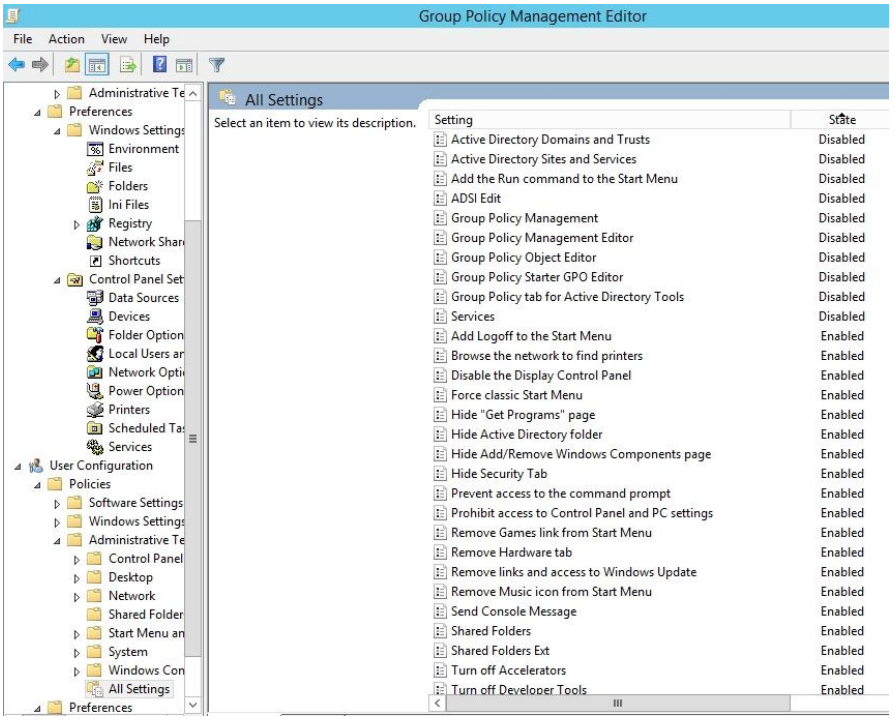
Efter man har klickat på “Edit” öppnar det en ny ruta som heter “Group Policy Management Editor”. I den här rutan kan man ändra på allting från specifika Windows-inställningar till administrativa säkerhetsinställningar som t.ex. gömma Task-Manager, ta bort alla spel, neka tillgång till kommandotolken eller att något skript/program skall köras automatiskt vid inloggning.

Det finns flera olika färdiga profiler (administrative templates) vilka innehåller inställningar som man kan också använda om man inte vill skapa egna inställningar.

För vårt testlaboratorium skapade vi flera olika begränsningar för användarna i domänen. Dessa GPO rättigheter och inställningar kommer i kraft vid inloggningen i domänen.

Man kan dock uppdatera och testa olika inställningar eller rättigheter utan att logga ut genom “gpudate /force”-kommandot som man kan skriva in i kommandotolken i Windows.

I figur 25 visas det olika konfigurationer som vi gjorde för att begränsa användarna i gruppen ”Begränsade användare”.



Figur 25. Rättighets- och säkerthetsinställningar för en GPO.

11.8 Roaming User Profiles

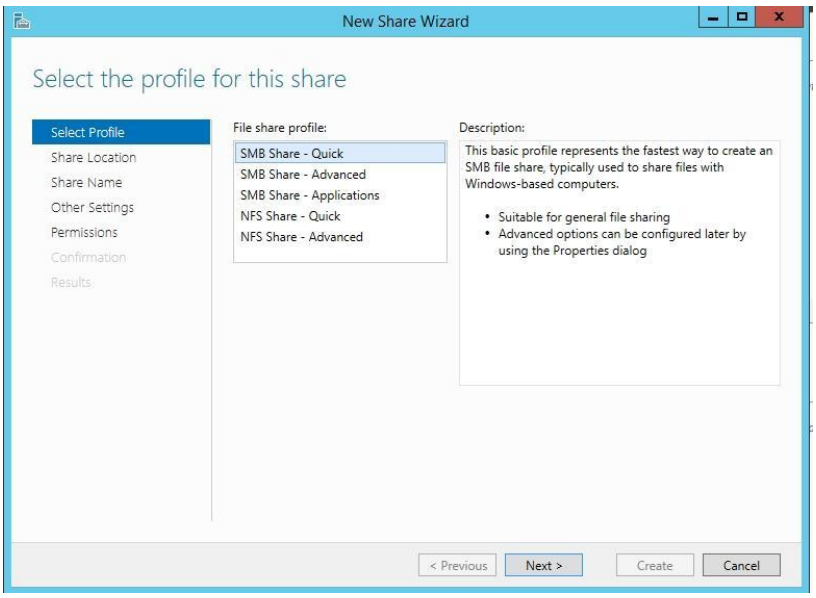
Roaming user profiles, eller Roaminganvändarprofiler, inom AD stöder endast klientdatorer som är anslutna till en Windows domän och använder sig av ett Windows operativsystem.

För att användarna skall få tillgång till profilerna måste de vara medlemmar av en säkerhetsgrupp som innehåller inställningar för centrala användarprofiler.

Man påbörjar ibruktagandet av roaminganvändarprofiler genom att navigera in på Active Directory Users and Computers. Sedan högerklickar man på den domän man vill skapa gruppen i och väljer “Create new group” samt väljer ett namn för gruppen och lägger till alla de medlemmar man vill att skall få tillgång till de rörliga profilerna.

Följande steg är att skapa en delad mapp som alla användare på nätverket har rättighet att skriva i och läsa. När de individuella profilerna sedan skapas kommer de att innehålla mera avancerad säkerhet, så att en användare bara har tillgång till sin egen individuella profil.

I Server Manager navigerar man sig till File and Storage Services och klickar sedan på Shares och väljer New Share. I det här skedet dyker en ny ruta upp med en så kallad Share Wizard, som fungerar som en guide. I Share Wizard väljer man profilen ”SMB Share - Quick” och fortsätter till nästa steg. Figur 26 demonstrerar Share Wizard guidens första steg där man skall välja profil.

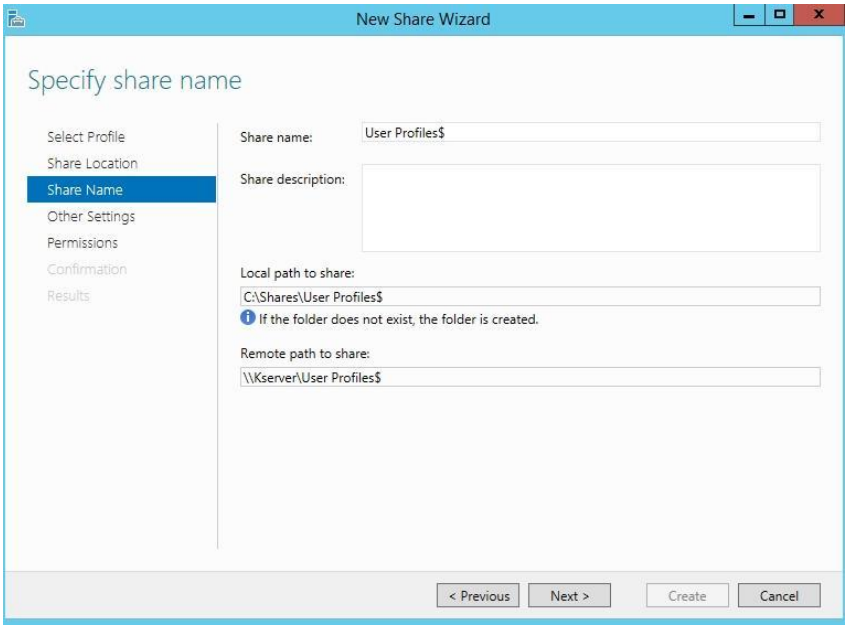


Figur 26. Val av profil i Share Wizard.

Efter att man har valt profil kommer man till “Share Location”. I det här fönstret väljer man var mappen skall sparas. I följande steg väljer man “Share Name” som är namnet på mappen som kommer att delas.

Om man skriver ett ”§” på slutet av namnet, kommer mappen att vara dold för vanliga användare som använder sig av en filhanterare.

Vi valde att mappen skulle heta User Profiles§ vilket man kan se i figur 27. Platsen vi valde att ha den delade mappen lokaliserad på, var vår server(Kserver). Då vi inte hade så många användare, valde vi det här alternativet istället för att spara profilerna på en annan plats i nätverket, t.ex. på en dedikerad filserver.



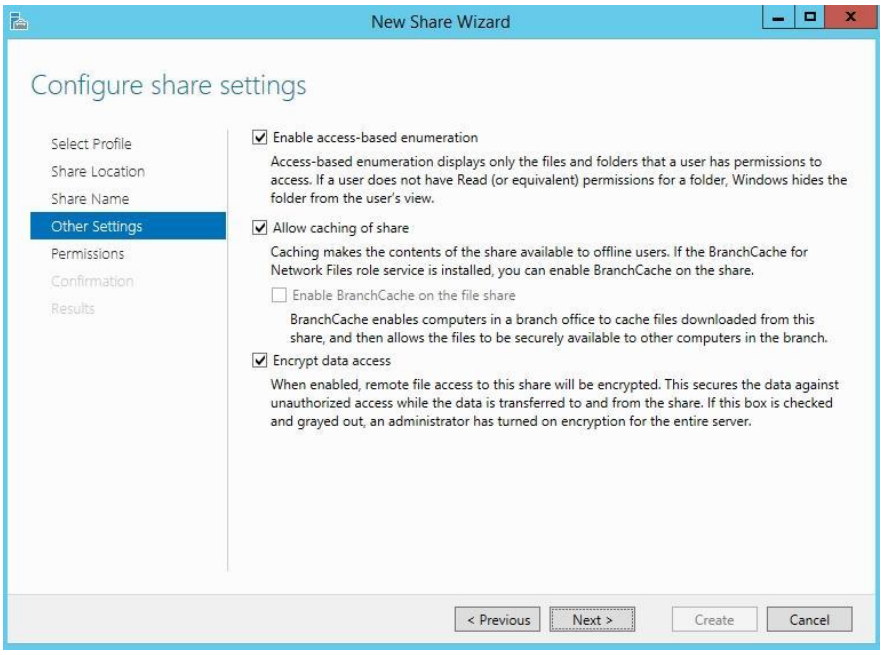
Figur 27. Namnge en delad mapp i Share Wizard.

På Other Settings fliken, som är följande steg, hittar man tre alternativ; Enable access-based enumeration, Allow Caching of share och Encrypted data access.

"Enable access-based enumeration" är en inställning som gör möjliggör att Windows visar de specifika mappar en användare har tillgång till (läsrättigheter eller motsvarande), medan användare utan läsrättigheter inte ser mapparna fysiskt.

"Allow Caching of share" gör det möjligt för användare att ha tillgång till innehåll även när de är bortkopplade från domänen ("Offline"). "Encrypt data access" gör att fjärråtkomsten till mappen kommer att vara krypterad, vilket säkrar data från obehörig åtkomst medan den skickas och tas emot från den delade mappen.

Vi valde att klicka i alla tre alternativ så som det demonstreras i figur 28. Användarna kommer att röra sig utanför domänen och därför bör de ha åtkomst till sina filer utan att obehöriga skall ha åtkomst till en annan användares filer.



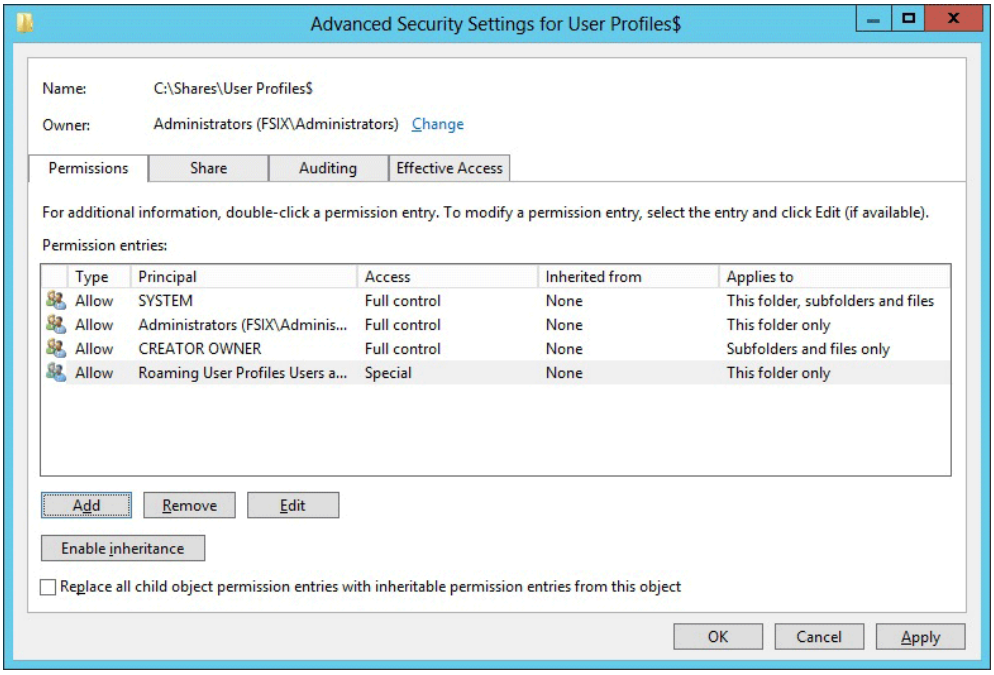
Figur 28. Konfiguration av nätverksresursen.

Följande steg i listan var "Permissions", vilket illustreras i figur 29. Här klickar man på "Customize permissions" för att få upp den avancerade dialogrutan över behörighets-inställningar.

Här väljer man "Disable inheritence" och klickar sedan på "Convert inherited permissions into explicit permissions on this object". Det här gör att under mapparna inte ärver behörigheterna från föregående objekt. Efter det här väljer man vilka rättigheter alla användare skall få.

I vårt fall valde vi att ge system "Full access" vilket är själva servern. Om man t.ex. har en administratörs grupp vill man högst troligt ge full kontroll över mappen åt dem. Sedan valde vi att skaparna av undermappar skall ha full kontroll över dem.

Till sist lade vi till den användargrupp vi tidigare skapat och gav dem rättigheten "Special" som gällde endast för huvudmappen. Efter det här är man klar med själva behörighetsdelen och kan gå vidare till följande steg.



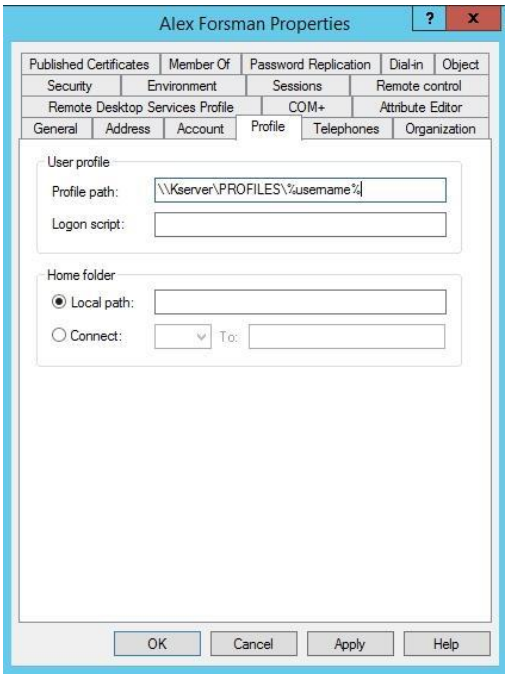
Figur 29. Behörigheter över Profil mappen.

Nästa fas är att tilldela själva roaming-användarprofilfunktionen till användarkonton, det här kan göras på flera olika sätt. Vi valde att använda oss av den varianten där man lokalt och individuellt ställer in Roaming User Profiles för enskilda användarkonton via AD.

Det här görs genom att navigera till "Active Directory Administration Center" och välja den säkerhetsgrupp som man tidigare skapat. Här markerar man alla användare man vill ge tillgång till den rörliga profilen och högerklickar på användarna och väljer sedan "Properties".

I fliken "Profile" anger man sedan sökvägen till den profilmappen vi tidigare skapat och där man vill att profilerna skall sparas och lägger till "%username%" (vilket ersätts med användarnamnet efter första inloggningen).

I vårt fall blev sökvägen "\\Kserver\User Profiles§\%Username%, eftersom vi skapade vår profilmapp där vilket man kan se i figur 30.



Figur 30. Roaming användarprofilens sökväg.

En annan variant som man kan använda sig av för att tilldela roaminganvändarprofiler är med hjälp av GPO. Den här varianten bygger på att man med hjälp av GPO tilldelar roaminganvändarprofiler till datorer.

Vi skulle rekommendera att använda profilerna via GPO om man vill utvidga systemet i framtiden, genom att lägga till t.ex. enskilda datorer, virtuella instanser av operativsystem eller dylikt.

Det här går allt att åstadkomma genom att länka datorer till grupprincipobjekt och därmed får alla användare som loggar in via dessa datorer en egen roaminganvändarprofil.

11.9 VPN och dess krav

För att lägga upp ett VPN, alltså ett virtuellt privat nätverk, krävs det en hel del server roller för att VPN skall fungera: RAS(Remote Access Services), NPS(Network Policy Server) och AD CS(AD Certificate Server).

Övriga systemkrav för att lägga upp en VPN i domänen är att servern helst har två nätverkskort.

Ett nätverkskort som är kopplat till det externa nätverket (Internet) och ett annat nätverkskort för det interna nätverket. Det fungerar även med bara ett nätverkskort men det rekommenderas att man har två stycken.

Förutom de fysiska systemkraven på hårdvara, kräver VPN även planering av hurudan VPN- struktur man kommer att använda. Vi använde i vårt testlaboratorium ett "L2TP/IPsec" protokoll för uppläggningen av vår VPN server, vi beskriver här hur det går till.

Ett annat krav för VPN är att öppna alla portar i brandväggen som krävs för att släppa igenom L2TP/IPsec trafik: UDP port 500, 4500 (inbound/outbound) och IP port 50 (inbound/outbound).

I vårt testlaboratorium ville vi förutom att skapa en VPN server, även ha en NPS server som undersöker en dators "hälsa" för att den skall kunna ansluta sig till domänen. Med en dators "hälsa" avses dess funktionsduglighet, att datorn har t.ex. virusskydd, brandvägg igång osv.

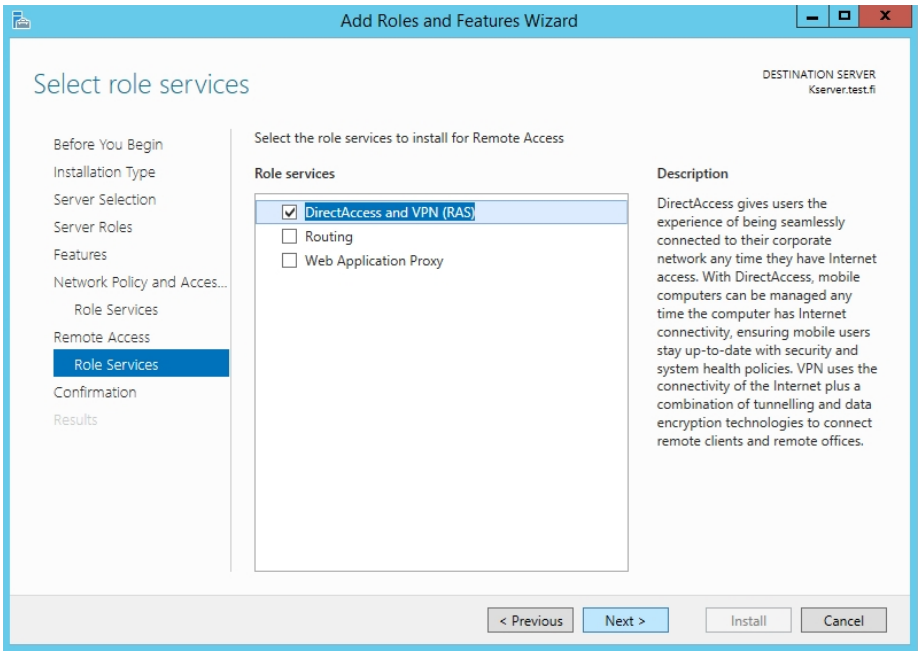
Efter att datorn har fått en positiv respons av NPS servern, ger servern lov åt datorn att koppla sig till domänen. Man kan konfigurera skilda "Health Policies" som innehåller hur stränga krav man vill ställa på datorernas hälsa för en domän.

Förrän datorn kan koppla sig i domänen måste den få ett certifikat av servern som behövs för att autentisera användaren som försöker ansluta sig till domänen. Certifikattjänsten kräver en AD CS roll som måste vara installerad på en server.

För en säker VPN server krävs att AD CS, NPS och RAS rollerna är installerade. Man börjar med att installera alla roller och tjänster på servern. Det rekommenderas att man installerar AD CS rollen på en helt skild server pga. Säkerhetsorsaker. Den skickar ut alla certifikat för alla datorer i domänen så den skall egentligen hållas separat och aldrig stängas av.

För att installera rollerna AD CS, RAS och NPS går man till Server Manager och i verktygsmenyn väljer man "Add Roles and Features". I fliken "Features" väljer man även "Routing" och under den finns "DirectAcces and VPN(RAS)" som man kryssar i. Processen för att installera DirectAccess and VPN(RAS) demonstreras ser man i figur 31.

Om man vill i framtiden använda DirectAccess kommer man få stöd för det också tillika när man konfigurerar VPN och RAS.



Figur 31. Installationen av roller och tjänster (NPS och Remote Access).

Efter man har valt rollerna och klickat nästa (Next) så följer man installationsguiden och servern installerar då rollerna och deras programvara. Efter att installationen är klar skall rollerna konfigureras.

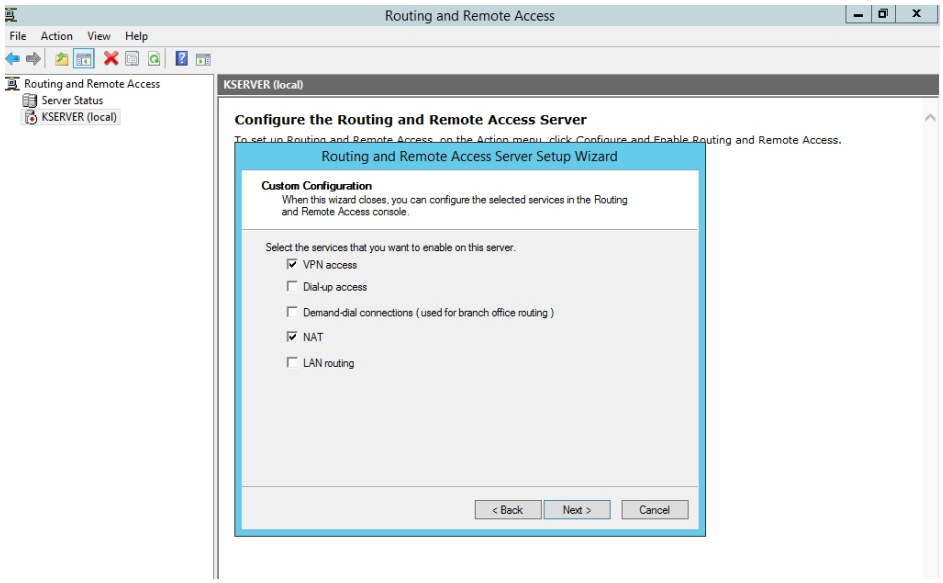
Vi började i våra försök med att ställa in "Remote Access" rollen.

I Server Manager i Windows Server har det i verktygsfältet nu kommit upp ett nytt menyobjekt som heter "RRAS" (Routing and Remote Access). Man trycker på RRAS i menyn och kommandot öppnar då ett nytt fönster där man ser lokala servern på högersida. Efter man har markerat "Routing and Remote Access" i fönstret, skall man i menyn välja "Add Server" och sedan väljer man den lokala servern man använder.

Efter att servern är vald och man lagt till "Routing and Remote Access" i fönstret, skall tjänsten sättas igång och konfigureras. Det här gör man genom att högerklicka på den valda serverns namn och i menyn välja "Enable Routing and Remote Access" under "Configure" menyobjektet.

Ett nytt fönster öppnas som är en "Setup Wizard" för RRAS vilket beskrivs i figur 32. I första fliken skall man välja vilken typ av fjärranslutningar som skall stödas av server. I

den här fliken väljer man “Remote access (dial-up or VPN)” och NAT (om man behöver det), sedan trycker man på “Next”. Man kan även senare ändra på dessa inställningar.



Figur 32. Konfiguration av Routing and Remote Access.

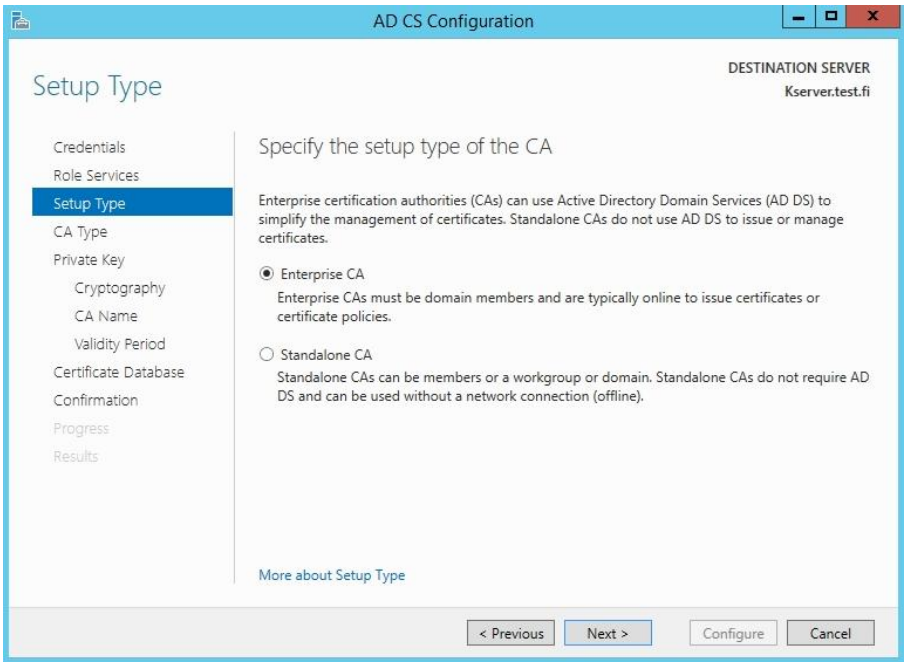
En viktig sak att göra i nästa flik är att välja rätt “VPN Connection”. Det här betyder att man skall välja vilket nätverkskort VPN anslutningarna skall komma ifrån. Det här är oftast det nätverkskortet som har kontakt till det externa nätverket (internet).

Efter man har valt nätverkskortet i listan går man till nästa flik som frågar vilka IP-adresser VPN klienterna kommer att få. De kan man lägga på automatiskt eller begränsa anslutningarna och manuellt ange en IP-adress “Scope” för dem. Nu är “Setup Wizard” guiden i princip färdig.

För att konfigurera AD CS rollen till nästa, har det i Server Manager fönstret kommit text i vilken det står att nya roller måste konfigureras, där väljer man AD CS och klickar på den.

I fönstret “AD CS Configuration” som öppnades följer man standardkonfigurationerna på de första stegen och i “Setup Type” steget är det viktigt att välja hurudan CA (Certificate Authority) servern skall ha.

Man bör i det här steget välja “Enterprise CA” som demonstreras i figur 33, för man vill att server skall skicka alla certifikat över nätverket och då måste servern vara med i domänen och uppkopplad till internet.



Figur 33. AD CS konfiguration av typen av CA.

I nästa steg skall man välja typen av "CA": Root eller Subordinate. Eftersom detta är den första certifikatservern i domänen, väljer man här "Root CA".

Efter att CA är inställt skall det skapas en nyckel, "Private Key", som fungerar som lösenord för certifikatservern. Då man har valt ett nytt lösenord frågas det efter hurudan kryptering av nyckeln man vill ha och hur länge lösenordet skall vara i kraft.

Nu är AD CS rollen installerad och man kan konfigurera den nya "Root CA" servern så att datorcertifikat skickas automatiskt via ett grupprincipobjekt (GPO) som heter "Cert Auto Enrollment Group Policy Object".

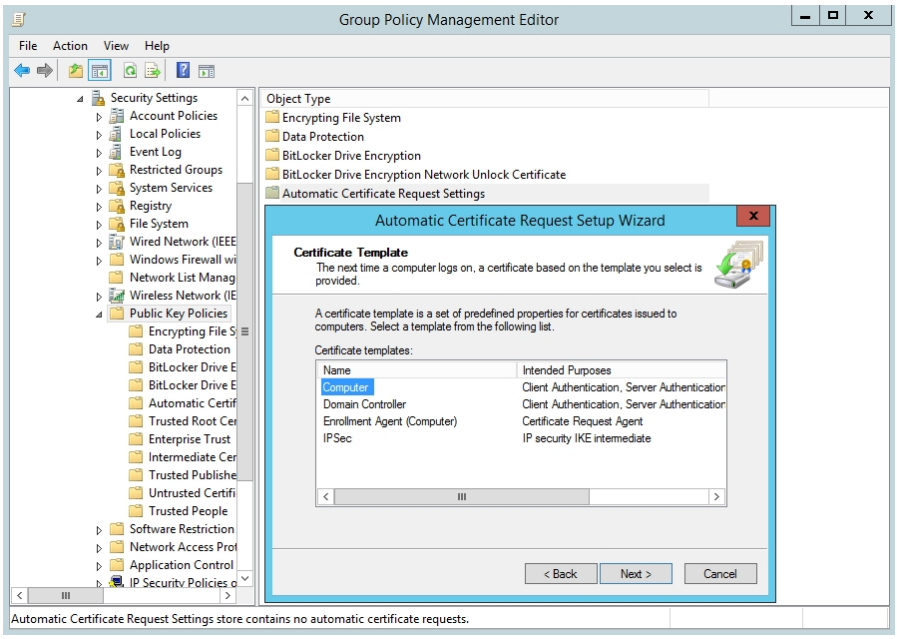
För att skapa det nya grupprincipobjektet måste man gå till Server Manager och välja "Group Policy Management" i verktygsmenyn. I det nya fönstret som öppnas väljer man domännamnet och högerklickar på det, sedan väljer man i menyn "Create a GPO in the Domain and Link It Here".

Efter man valt föregående inställning skall man namnge det nya grupprincipobjektet till "Cert Auto Enrollment Group Policy Object" och klicka "Ok". Nu har en ny GPO skapats och för att editera den högerklickar man den, och väljer "Edit".

Det öppnas då ett nytt fönster, “Group Policy Management Editor”, efter att man valt att editera grupprincipsobjektet. Det nya fönstret som är en s.k. “Console tree” innehåller flera mappar i en lista till vänster, och mapparnas innehåll finns på höger sida.

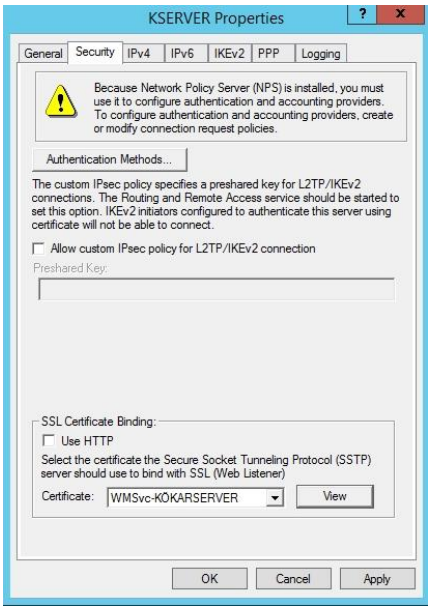
I listan till vänster väljer man “Computer Configuration”, därefter går man till undermappen “Security Settings” och i den hittar man “Public Key Policies”. I “Public Key Policies” mappen finns en mapp som heter “Automatic Certificate Request Settings”, den högerklickar man på och i menyn väljer man “New Automatic Certificate Request”.

Det öppnas en ny “Setup Wizard” ruta som demonstreras i figur 34, för att automatisera registreringen av certifikat till datorer eller andra domänkontrollanter i domänen. I rutan väljer man “Computer” och trycker på “Next” och sedan är grupprincipsobjektet för certifikat färdigt.



Figur 34. Skapa en ny "Automatic Certificate Request" GPO.

Efter certifikatet är skapat måste det väljas som standardcertifikat för datorerna i domänen. Det gör man genom att gå till “Routing and Remote Access” som finns i Server Manager under verktygsfältet. I det nya fönstret som öppnas markerar man serverns namn (Kserver i vårt fall) samt högerklickar och väljer egenskaper. Efter man kommit till egenskaperna för servern, väljer man rätt certifikat nere i listan vid “Certificate”, så som man ser i figur 35.



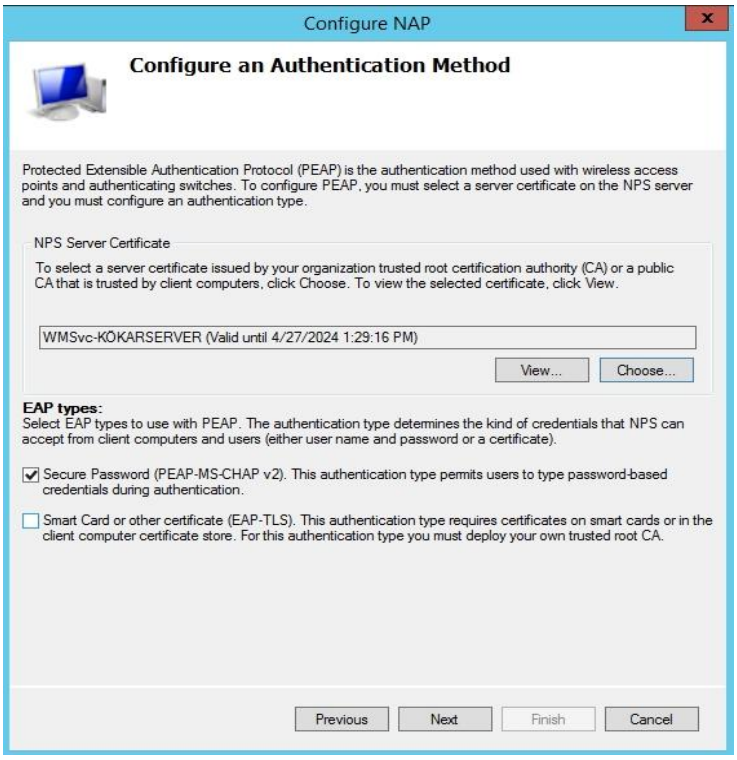
Figur 35. Val av ett certifikat för servern.

Före man kan börja konfigurera NPS måste NAP (Network Access Protection) tjänsten vara inställd. För att komma åt NAP konfigurationen klickar man på "Network Policy Server" som finns i de administrativa verktygen, i startmenyn.

I NPS fönstret trycker man på "Configure NAP". Ett nytt fönster som beskrivs i figur 37, öppnas där man skall välja vilka datorer eller användargrupper som konfigurationen skall gälla. I vårt testlaboratorium valde vi en säkerhetsgrupp som innehöll flera användare.

I nästa flik skall man välja serverns certifikat som man vill använda. Under "EAP Type" väljer man autentiserings typen, i vårt fall valde vi "PEAP-MS-CHAP-v2" och sedan trycker man på "Next".

Till nästa skall man välja vilken "Health policy" man vill använda, där väljer man "Windows Security Health Validator" och trycker på "Finish" för att spara konfigurationerna.



Figur 36. Konfiguration av NAP.

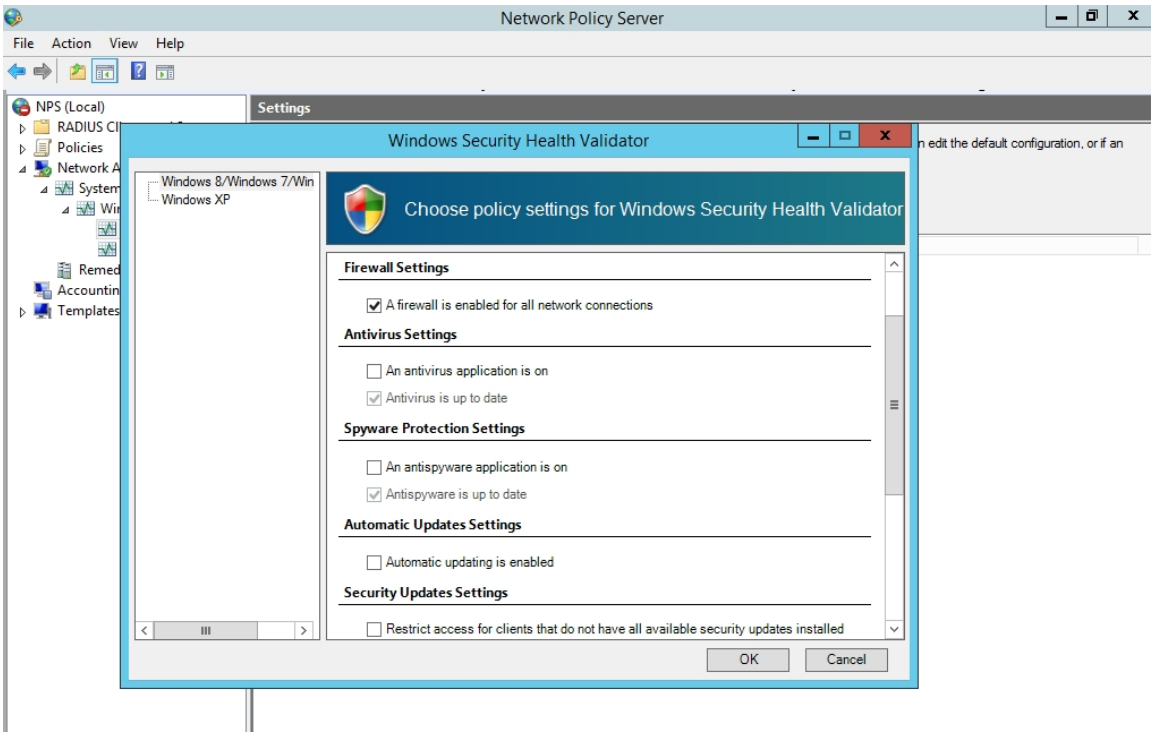
Efter att man har NAP tjänsten klar kan man börja konfigurera NPS (Network Policy Server) rollen på servern.

Till konfigurationsprocessen för NPS hör fem delar: “Health validators”, “Health policy”, “Network policy”, “Connection policy” och “RADIUS client”. På grund av att vissa delar är beroende av varandra bör man konfigurera NPS i den ordning som det beskrevs ovanför.

Det som alla dessa delar i NPS gör är ett slags “hälsogranskning” av datorer. NPS kollar vilka krav man ställt in att en dator minst skall ha för att få ansluta sig till domänen, sedan agerar NPS på ett visst sätt enligt hur man konfigurerat de olika “policies” inställningarna.

För att börja konfigurera “Health validators” öppnar man “Network Policy Server” som finns i de administrativa verktygen, i startmenyn. Under “Network Access Protection” i listan till vänster, högerklickar man på “Windows Security Health Validation”mappen.

I det nya fönstret som demonstreras i figur 37, som öppnas kan man välja hurudana inställningar datorerna bör ha för att ansluta sig till domänen. I vårt testlaboratorium satte vi som inställning bara att datorerna bör ha en brandvägg igång, men man kan konfigurera det mycket strängare om man så vill.



Figur 37. Skapa en Security Health Validator (SHV).

Efter att "Health Validator" inställningarna är konfigurerade måste man skapa "health policies" som krävs för att "Health Validator" skall fungera.

Dessa "policies" fungerar som ett slags profiler för hur systemet skall göra om en dator kommer igenom hälsogranskningen eller om den inte kommer igenom. Man måste även konfigurera "network policies" där man specificerar vilka anslutningar som är tillåtna osv.

För att skapa en ny "Health policy" går man tillbaka till "Network Policy Server" fönstret och högerklickar på "Health Policies" mappen som finns under "Policies" mappen, sedan väljer man "Create a new health policy".

Det första som skall göras för att skapa en ny "Health policy" är att namnge den. Den här "Health policy" ger man t.ex. namnet "Pass" eftersom den här konfigurationen skall beskriva hur NPS skall fungera för datorer som godkänns i hälsogranskningen.

Efter man har gett namnet skall man under "Client SHV checks" i listan välja "Client passes all SHV checks". Efter det skall man välja "Windows Security Health Validator".

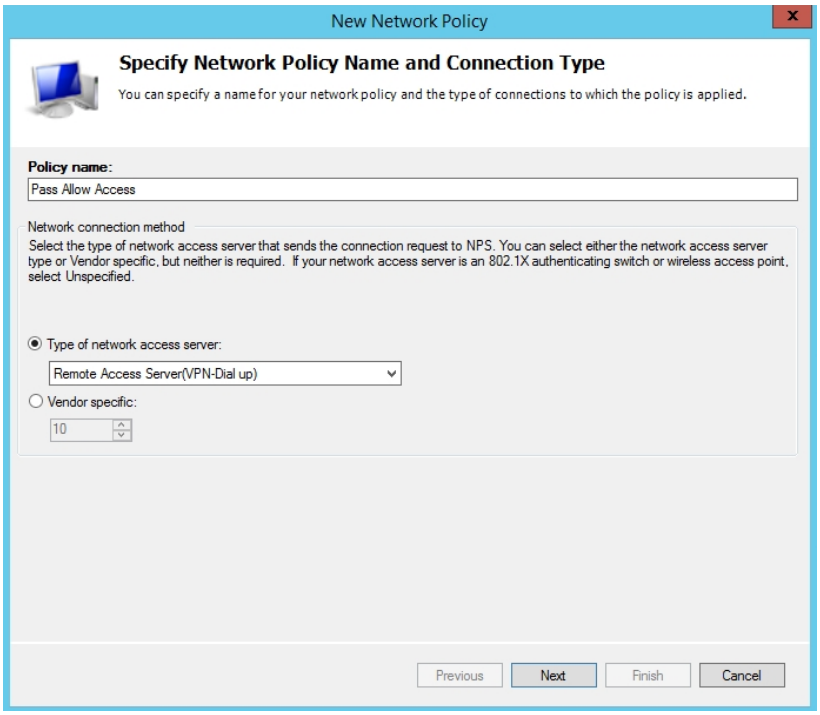
Därnäst skall man skapa en icke godkänd “Health policy”. Det gör man på samma sätt som föregående men man ger som namn t.ex. “Fail” och under “Client SHV checks” väljer man “Client Fails One or More SHV Checks”.

Nu har det skapats “Health policies”, en “Health validator” och nu måste det skapas en Network policy” för de olika Health policies som skapades tidigare.

För att skapa första “Network policy” för den godkända “Health policyn”, går man till “Network Policy Server” fönstret och trycker på Policies mappen för att expandera den. Det finns några standard ”Policies” i mappen som man kan ta bort eller inaktivera för de behövs inte pga. att det skapas nya specifikt för VPN.

Efter man har inaktiverat standard Policies, skapar man en ny genom att högerklicka på mappen och välja “Create new network policy”. Ett nytt fönster öppnas och man måste ge ett namn. I vårt fall gav vi namnet “Pass Allow Access” för den nya Network policyn.

I detta fönster är det viktigt att välja rätt typ av “network access server”, som skall vara “Remove Access Server (VPN-Dial up) vilket demonstreras i figur 38.



Figur 38. Skapa ett Network Policy.

I nästa flik skall man specificera hurudana tillstånd (conditions) som skall användas. Man skall här välja “Add” knappen, och i listan välja “Health Policies” och sedan trycka på “Add”. Efter man tryckt på “Add” kommer det upp en ny ruta där det finns en lista av “Health Policies”, i den listan väljer man “Pass”.

Därnäst skall det specificeras “Access Permissions”. Där kryssar man i “Access Granted” och trycker på “Next”. I nästa flik skall man definiera “Authentication Methods” där man kan välja hur säker autentisering man vill ha.

Vi valde i våra försök Microsoft: Protected EAP (PEAP). Efter att man valt Authentication Method, högerklickar man på den och trycker på Edit och en ny ruta öppnas. I den nya rutan skall man lägga till serverns certifikat, vilket man gör i listan ”Certificate Issued to”.

I nästa flik i konfigurationen skall man ställa in olika nätverksinställningar som t.ex. IP filter och IP inställningar. Men det som man främst ändrar här är att godkänna all åtkomst till nätverket: Allow full network access som man kryssar i under NAP Enforcement.

Nu är Network policy är färdig för de godkända Health policies. Det som måste göras nu är en icke godkänd Network policy som begränsar åtkomsten för användaren till nätverket som inte blir godkända i hälsogranskningen. Det här gör man på samma sätt som när man skapade den tidigare Network policyn, förutom att man nu väljer Allow limited access under NAP Enforcement.

Efter att man har begränsat nätverksåtkomsten kan man även lägga till ett IP filter, så att användarna som inte blivit godkända i hälsogranskningen bara kan komma åt en viss IP-adress. Det här är en bra lösning speciellt om man har satt som en “Health policy” att datorerna i domänen måste använda ett visst program eller drivrutin som kan sedan sökas ifrån den datorn/servern man har specificerat i IP filtret.

Nu fattas det bara Connection policies från servern att konfigurera. För att komma till Connection policies går man till Network Policy Server rutan. I Policies mappen högerklickar man på Action och Create new connection request policy och ger namnet “RAS Connections” till den.

I listan nedanför väljer man Remove Access Server (VPN-Dial up) och trycker på Next. I nästa flik väljer man Client IPv4-Address som en “condition” och går till nästa flik. I Specify Authentication Methods kan man lägga till olika metoder av autentisering.

I vårt testlaboratorium ville vi ha säkrare funktioner och lade till Microsoft: Protected EAP och även Microsoft: Secured Password (EAP-MS-CHAP-v2).

Efter man har konfigurerat de ovanstående inställningar är NPS färdigt konfigurerat och nu är nästa steg att konfigurera NPS servern som en "RADIUS" klient i det nyskapade NPS systemet.

För att skapa en RADIUS klient går man till "Network Policy Server" fönstret och expanderar "RADIUS Clients and Servers" mappen, sedan högerklickar man på "RADIUS Clients" och väljer "New RADIUS Client".

Efter man har skapat RADIUS klienten och namngett den till t.ex. "RAS1" måste man ange IP-adressen till den, i vårt fall blev det serverns IP-adress "10.112.131.8". Man måste även skapa ett lösenord, en s.k. "Shared Secret" och sedan man fyllt i lösenordet klickar man på "OK" och RADIUS klienten är då skapad.

Efter man har skapat certifikatet och konfigurationerna för NPS är gjorda, kan man börja med att konfigurera Remote Access rollen (RAS). RAS server rollen är den som sedan kopplar användaren till internet och skapar kontakten emellan VPN klienterna (förutsatt att NPS har autentiserat användarens anslutning till domänen).

I Server Manager på domänkontrollanten öppnar man Remote Access Management i verktygsfältet för att komma åt RAS tjänsten. Efter att man navigerat till Authentication fliken under VPN Configuration, skall man kryssa i "Use RADIUS Authentication" inställningen. I sektionen "RADIUS servers" skapar man sedan en ny server och anger NPS servern som tidigare skapats.

Efter att man har lagt till NPS servern skall man trycka på Change knappen för att ändra lösenordet "Shared Secret", som man ställde in tidigare i RADIUS konfigurationen. Efter man har ändrat på inställningarna sparar man den nya konfigurationen och trycker på "Finish". Efter man är klar så uppdateras Remote Access servern med nya inställningarna. Nu är RAS server konfigurerad och redo att acceptera VPN anslutningar.

Nu fattas det bara en sak för att användarna skall kunna ansluta sig via VPN. Man måste konfigurera användarkonton i Active Directory Users and Computers under Users, eller en organisationsenhet, genom att högerklicka på dem och välja egenskaper (Properties). I användarkonto finns det flera flikar vilket man sedan väljer Dial-in fliken. I fliken kryssar man i alternative "Control access through NPS Network policy".

Nu har användaren tillgång att ansluta sig via VPN till domänet. Användaren måste bara ställa igång en ny nätverksanslutning i Windows på sin dator genom att i Network and Sharing Center klicka på Set up a new connection or network.

Efter man har avklarat guiden för den nya nätverksanslutningen och konfigurerat rätt domännamn och användaruppgifter, kan användaren motta ett certifikat till sin dator och ansluta sig till domänet.

11.10 WDS

För att komma igång med WDS och kunna bygga en fungerande "Image" av en Windows XP, W7 eller W8 installation krävs förutom WDS rollen även följande program: Microsoft Deployment Toolkit (MDT) 2012 Update 1 och Windows Assessment and Deployment Kit (ADK) 8.0. MDT innehåller även Workbench som man även behöver för att konfigurera och skräddarsy installationsfilerna.

Dessa olika verktyg är gratis och kan hämtas från Microsofts hemsidor. Man behöver även installationsfilerna för ett eller flera operativsystem som kommer att behövas senare när man bygger de skräddarsydda operativsystem ".WIM" filerna. Man skall komma ihåg att vid installationen av ADK välja både Deployment Tools och Windows PreInstallation Environment.

Målet med WDS för Kökar kommun var att skapa skräddarsydda Windows installationer som kan installeras över internet, förutsatt att man är medlem i domänen. Efter att man har installerat WDS rollen på servern måste den konfigureras. För att konfigurera WDS öppnar man Windows Deployment Services som finns nu i verktygsmenyn.

I Windows Deployment Services fönstret expanderar man Servers och högerklickar på serverns namn och väljer Configure Server. I nästa steg skall man specificera platsen där man vill spara alla operativsystems avbildningar (images). Vi lämnade detta alternativ så som standardinställningen var: "C:\RemoteInstall" och gick vidare till nästa flik.

Då man har kommit till nästa flik skall man konfigurera PXE Server Initial Settings. Där kan man välja “Respond to all client computers” eller “Respond only to known client computers”. Vi valde det tidigare alternativet och gick till nästa flik. I nästa flik finns konfigurationen efter avbildningar men det skall inte läggas till nu.

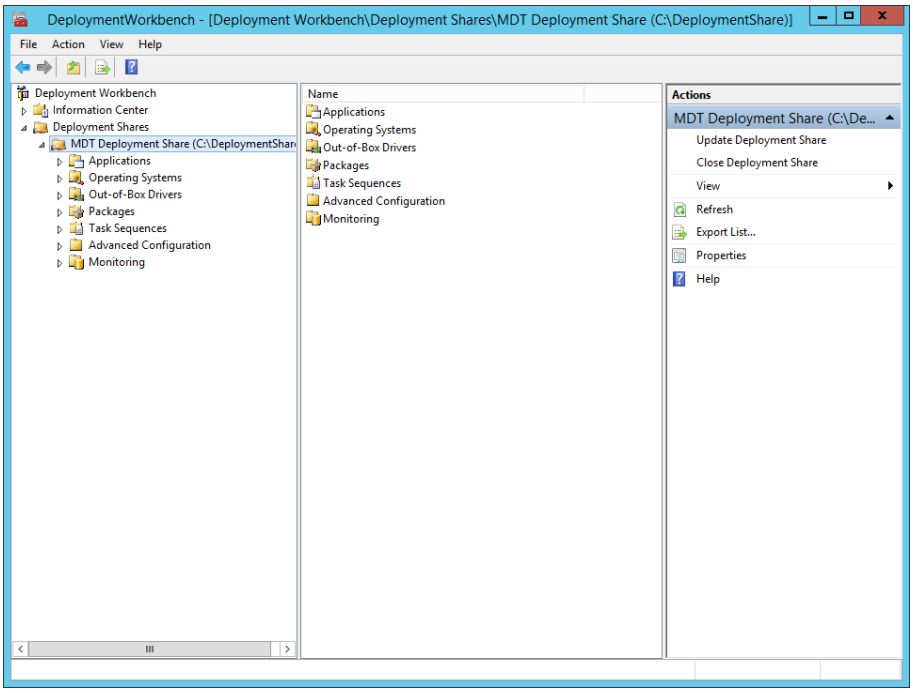
När man har gjort WDS konfigurationen skall man ännu tillåta vissa portar i DHCP så att användare kan kontakta servern över nätverket och få avbildningarna (images) sedan när de skall installera ett operativsystem.

För att öppna DHCP portarna för WDS går man och högerklickar på servern i “Windows Deployment Services” och väljer properties. I properties fönstret som öppnas går man till DHCP fliken och kryssar i alternativen Do not listen to port 67 och Configure DHCP option 60 to PXE Client.

Till processen att skapa Windows installationer (avbildningar) hör många steg som måste göras i ordningsföljd. Först importeras ett operativsystem på servern och en “Task Sequence” skapas. Denna process gör man genom att först installera verktygen.

Efter installation av verktygen (ADK och MDT) startar man Deployment Workbench programmet vilken man hittar i startmenyn på Windows servern. När man väl är inne i Deployment Workbench vilket demonstreras i figur 39, skall man skapa en ny Deployment Share.

Då det nya dialogfönstret startat skall man välja på vilken plats (sökväg) man skall dela ut de “shares” som man skapat. Resten av inställningarna kan man lämna som de är. För att sedan se vilka “shares” som finns tillgångliga expanderar man “Deployment shares” mappen.



Figur 39. Deployment Workbench efter man har skapat en ny Deployment Share.

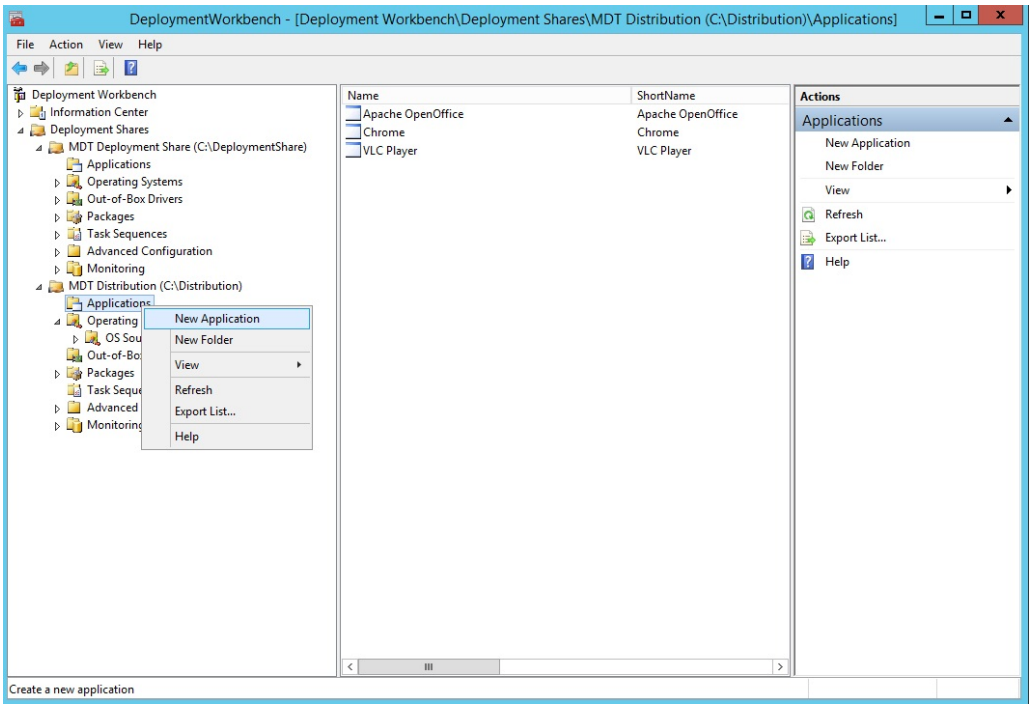
Nästa steg är att importera det operativsystem man vill distribuera. Till det behöver man originalversionen av installationsfilerna (DVD eller avbildning). Man högerklickar Operating Systems mappen och i menyn väljer man Import Operating System.

Det öppnas ett nytt fönster där man skall välja typen av operativsystem. För vårt arbete hade vi tillgång till originalversion av Windows 7 DVD-skivor så vi valde "Full set of source files" alternativet.

I nästa steg skall man definiera platsen där installationsfilerna finns och därefter börjar importprocessen. Importen kan ta ganska länge eftersom servern kopierar filerna för alla versioner av Windows 7 (Home, Professional osv) till "Deployment Share" mappen.

Nu har man lagt till operativsystemet som skall distribueras och då kan man lägga till program, drivrutiner eller andra konfigurationer som man vill ha med. Det här kan man göra genom att högerklicka t.ex. Applications och välja "New Application" och sedan specificerar man platsen där programmets installationsfiler finns.

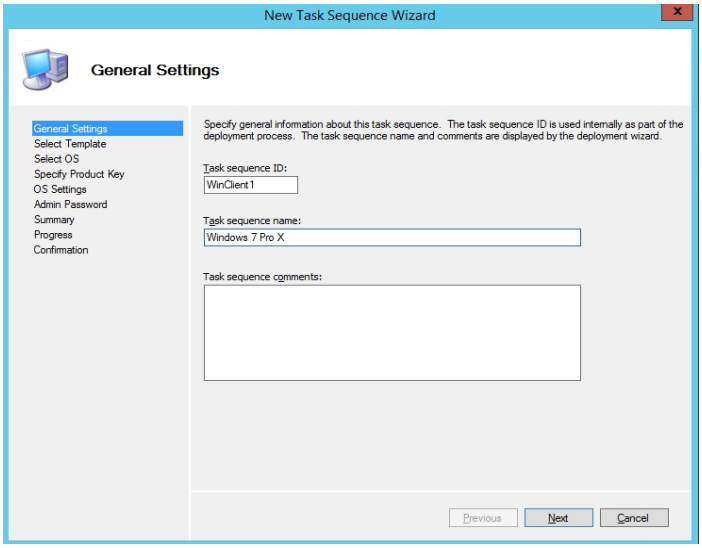
I figur 40 visas Deployment Workbench fönstret efter det har lagts några program till Deployment Shares.



Figur 40. Exempel på att lägga till program i en Deployment Share.

Som nästa steg skall man skapa en installationsprocess (Task sequence) vilket man gör genom att expandera Deployment shares mappen och klicka på “New task sequence”.

I följande fönster, som demonstreras i figur 41, skall man fylla i diverse information om installationsprocessen. I ”Task Sequence ID” alternativet, kan man lägga till t.ex. WinClient1 för att indikera att det är första versionen. I ”Task Sequence name” alternativet, kan man lägga till det namn som kommer att visas då man senare väljer sekvensen i “Deployment Wizard”.



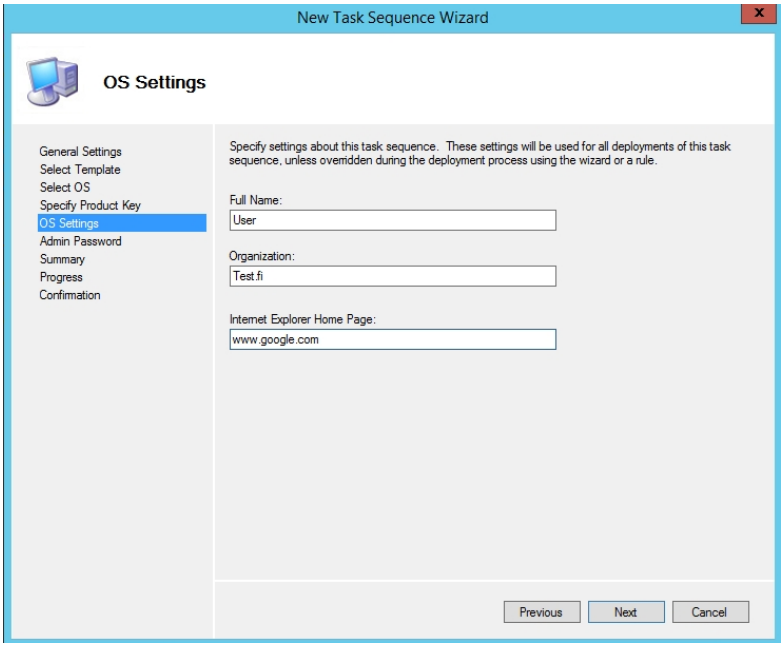
Figur 41. Skapa en Task Sequence för en Windows 7 installation.

Nästa steg är Select Template här väljer man den mall man vill använda sig av. I vårt fall valde vi Standard Client Task Sequence. Därefter klickar man på Nästa. I följande steg skall man välja vilket operativsystem man vill använda sig av.

Beroende på vilket operativsystem man importerat kommer det synas olika versioner av operativsystemet, t.ex. om vi importerat Windows 7 Ultimate så kommer också alla andra versioner av Windows 7 finnas med i listan. Här bör man välja "Windows 7 Professional" eller högre då AD inte fungerar med versioner under "Professional".

I följande steg får man välja om man vill ange en produktnyckel, här väljer man "Do not specify a product key at this time" eftersom att vi kommer att använda oss av sekvensen för flera licenser och inte bara en specifik.

I följande flik som demonstreras i figur 42, fyller man i information om namn och organisation. Sedan väljer man ett lösenord som krävs för att köra sekvensen och klickar på "Finish".



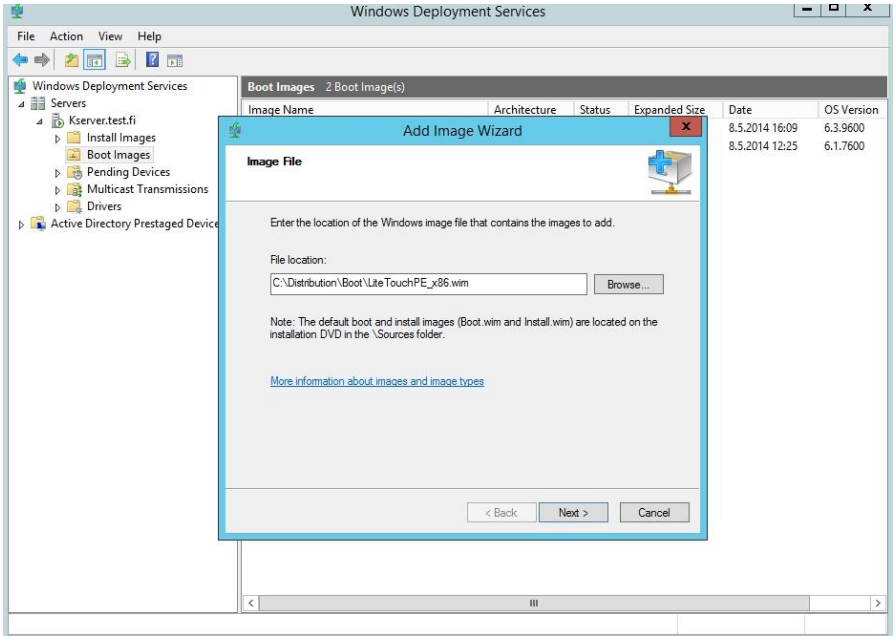
Figur 42. OS settings i skapandet av en Task Sequence.

Nu har det skapats en installationssekvens för en referensdator och nästa steg är att köra Update Deployment Share som man gör genom att högerklicka på MDT Deployment Share mappen och välja kommandot i menyn.

Uppdateringen tar ganska länge för programmet skapar en avbildning som innehåller alla installationsfiler av operativsystemet, installationssekvensen och alla program som har lagts i Deployment shares.

Efter att man har uppdaterat Deployment Share kan man börja att skapa en Capture image av referensdatorn. Man börjar med att gå till Windows Deployment Services och markerar "Boot images" och väljer "Add new image".

I figur 43 demonstreras processen. I rutan som öppnas bläddrar man till den nya avbildningen som skapades när man uppdaterade Distribution shares. I vårt fall hittade man filen i mappen "C:\Distribution\Boot\".



Figur 43. Lägga till en avbildning till WDS.

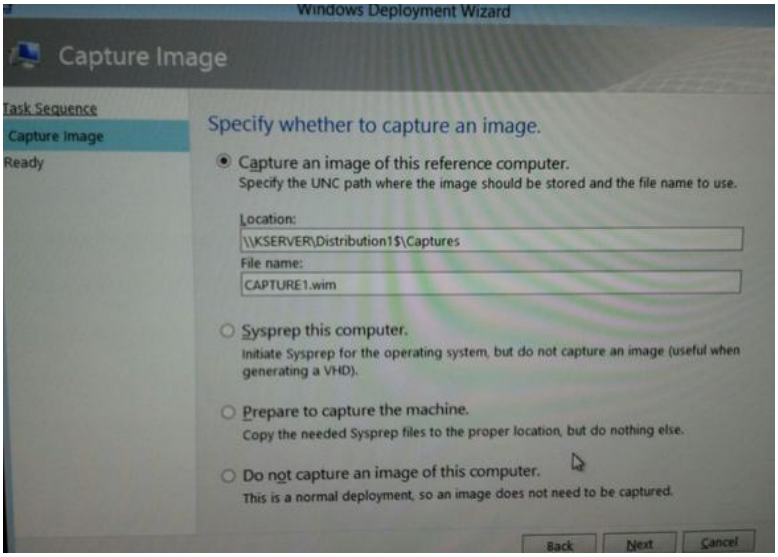
I detta skede skall man gå till referensdatorn och starta den i BIOS och så skall man trycka två gånger "F12" så den börjar med en s.k. "Network service boot (PXE)", vilket demonstreras i figur 44 på nästa sida. Referensdatorn måste vara i samma nätverk som servern.

Figur 44. Start av referensdatorn via PXE network boot.

Då man har kopplat referensdatorn till WDS-servern börjar en "Windows Deployment" installationsguide. I guiden väljer man "Run Deployment Wizard" och så följer man stegen.

Först skall man logga in på domänen med sitt användarkonto och även skriva in domännamnet, sedan går man vidare och väljer "Task Sequence" som skapades tidigare och som kommer att installera operativsystemet.

I nästa flik som demonstreras i figur 45 frågar guiden om man vill skapa en "Capture image" och det skall man kryssa i, sedan skall man också definiera på vilken plats på servern man vill spara "Capture image" avbildningen av referensdatorn.



Figur 45. Deployment Wizard konfigurationen.

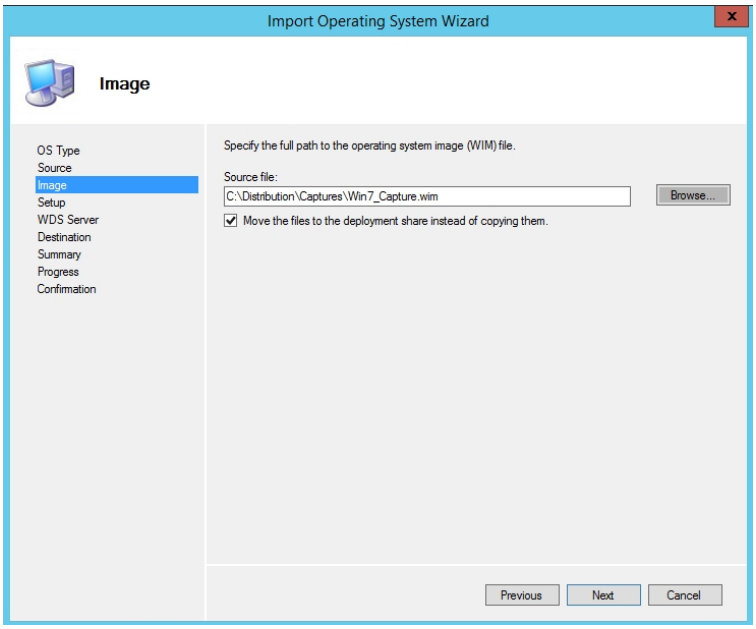
Efter man har kört Deployment Wizard guiden så installeras Windows operativsystemet och alla program, applikationer samt drivrutiner man lade till tidigare.

Installationen tar lång tid men när den är klar startar datorn om och man kommer in i Windows och installationen fortsätter ännu automatiskt.

Efter att alla program har installerats kör Windows Deployment programmet Sysprep och skapar en Capture image av operativsystemet och skickar avbildningen till servern genom nätverket.

Nu när Capture image avbildningen har skapats, skall man lägga till den till Deployment Workbench. Det här gör man genom att gå till Deployment Workbench och högerklicka Operating Systems under Deployment shares och där väljer man Import operating system.

I Import Operating Systems Wizard fönstret som visas i figur 46, väljer man i OS Type alternativet Custom Image file. Därefter skall man välja vilken avbildning (image) man vill använda och i detta fall skall man välja den avbildningen som skapades av referensdatorn som tidigare skapades.



Figur 46. Exempel på val av avbildningen vid import av ett OS.

I nästa flik frågar konfigurationen om man vill köra Sysprep men det vill man inte för det gjordes redan och efter det frågas vilket namn den skall ha. Nu identifieras avbildningen som ett operativsystem i Deployment Workbench.

Nu har det skapats en skräddarsydd Windows 7 installation, men det fattas ännu en Task Sequence som måste skapas för den. För att skapa Task Sequence gör man på samma sätt som tidigare beskrivet, men man namnger den t.ex. ”Deploy Windows Server to Target PC”. Efter man har gett namn och ID för Task Sequence skall man i nästa flik (Select Template) välja Standard Client Task Sequence.

Då man valt typen av Task Sequence skall man välja operativsystemet (Select OS). Vid detta alternativ är det viktigt att man väljer det operativsystem som importerades tidigare, sedan trycker man på “Finish” och så är det klart.

I detta skede har det skapats ett funktionellt Windows operativsystem som innehåller färdiga drivrutiner, program och applikationer mm. Nu kan man installera ett operativsystem på en dator i nätverket och gå med i domänen automatiskt samt få alla program och drivrutiner som användaren behöver.

12 Slutsatser

Man kan dra många positiva slutsatser utgående från det forskningsarbete vi utfört och den laboratoriemiljö vi byggt upp och använt oss av. Det står helt klart att användandet av Windows Server 2012 R2 i mindre (och även medelstora) företag och kommuner underlättar arbetet, ger kostnadseffektiva lokala lösningar och förbättrar datasäkerheten.

Kökars kommun skulle definitivt ha fördel av att ta i bruk Windows Server 2012 i sin verksamhet. Som kommunens situation är idag, är den både förlegad och osäker vad beträffar datafunktionerna.

Kommunen har, trots att den fysiska miljön är fem år gammal (eller i vissa fall mer än det), hyfsade förutsättningar att starta upp serverfunktionerna utan att uppgradera sin hårdvara.

Det skulle emellertid vara rekommendabelt att göra en uppgradering och samordning av hårdvaran förrän man startar upp serverfunktionen, eftersom man antagligen kommer att bli tvungen till förnyande av datorparken inom en snar framtid.

Tar man ytterligare i beaktande att avståndet till fasta Åland och därmed till teknisk support är väldigt långt tidsmässigt och beroende av färjtidtabeller, så är en uppgradering definitivt att rekommendera. Utbudet av teknisk support på Kökar är absolut väldigt begränsat.

Oberoende av hårdvaran så är slutsatsen att kommunen har stor nytta av ibruktagandet av Windows Server 2012. Det kommer att försnabba funktionerna väsentligt. Vi rekommenderar dock att våra rekommendationer tas i beaktande gällande anskaffning av flera servermaskiner, om det beslutas att VPN tjänsten tas i bruk på större skala.

Idag måste bokföraren vänta på att få in godkända fakturor från enheterna för att kunna betala dem. Genom att använda digitala hjälpmedel så försnabbas betalandet väsentligt. Kommunens bokföring är mer up to date och inga förseningsräntor uppstår. Kommunikationen mellan olika organ och olika tjänstemän i kommunen försnabbas och blir säkrare.

Genom att använda krypterad VPN kommer man att kunna hantera klientärenden inom socialvården på ett mycket snabbare och säkrare sätt än hittills. Dagvårdsärenden (barndaghemmet) kan skötas effektivt och okomplicerat. Socialsekreterarens och socialnämndens beslut kan vara uppdelade i kategorier och dessa kan vara tillgängliga för särskilda användare eller användargrupper.

Dokumenthanteringen centraliseras och blir tillgänglig för de grupper och användare man bestämmer internt i kommunen. Konfidentiell information kan tillhandahållas i digital form åt just de användare som har rätt att ta del av den.

Detsamma gäller för grundskolans del. Informationsflödet försnabbas och effektiveras utan att integriteten hos elever eller föräldrar försämras. Inom byggnadstekniska sektorn kommer serverfunktionerna att hjälpa till att försnabba ansökningsförfarandet, t.ex. beträffande byggnadslov eller miljötillstånd för avloppslösningar.

Ansökningsblanketter kan tillhandahållas digitalt och ifyllda delas till de personer som behöver uppgifterna och som har access till dem. Genom att knyta ihop ansökningsfunktionen med faktureringen av avgifter effektiverar man ytterligare.

E-identifiering skulle för sin del möjliggöra att kunderna (kommuninvånarna) skulle ha möjlighet att fylla i och lämna in blanketter digitalt när som helst på dygnet. Man kan

därför varmt rekommendera att kommunen överväger att gå in för det som ett komplement till övrig datautveckling.

Kommunkansli, skola, socialväsende, bibliotek och teknisk sektor kommer alla att kunna samarbeta både snabbare och bättre då användaren inte är bunden till sin egen arbetsstation utan kan använda vilken dator som helst i nätverket för att komma åt sin digitala plattform.

Det här kommer även att märkas väsentligt i fråga om de distansarbetare som kommunen har redan idag, brandchef, skoldirektör, lantbrukssekreterare.

Användarna kan logga in på kommunens server och ta del av innehållet, även ekonomisystemet. I dagsläget måste alla användare i ekonomisk ansvarsställning vänta på att en gång per månad få en utskriven budgetjämförelse för att se hur mycket budgeterade medel man använt och hur mycket man har kvar av årets budget. I det nya systemet kan alla logga in när som helst för att kontrollera läget.

Om det skulle bli verklighet av tankarna på kommunsammanslagningar, men även redan på basen av de samarbetssträvanden som finns, så skulle en utveckling mot ibruktagande av de beskrivna serverfunktionerna bli oundviklig.

De fysiska avstånden i skärgården måste i så fall kompenseras med datateknik och skapandet av bland annat virtuella mötesplatser om man skall kunna upprätthålla en fungerande närdemokrati.

Vi planerade detta arbete så att det föreslagna systemet kan byggas på och utvecklas vidare på ett enkelt sätt. När man t.ex. installerar VPN servern och bestämmer dess krav, så finns det möjlighet att förutom att skapa VPN anslutningar även börja använda DirectAccess anslutningar.

Man kan också enkelt installera en Web server och/eller Exchange (e-post) server och lägga dem till domänen samt länka dem till domänkontrollanten.

Detta slutarbete skulle kunna vidareutvecklas genom att gå djupare in på de vissa delar och berätta mera om NAP, NPS, RRAS och så vidare. Men vi tog med de tjänster och roller som vi främst jobbade med i försöksmiljön och som vi anser är de mest relevanta för vår uppdragsgivare.

13 KÄLLFÖRTECKNING

Andersson, G., 1999. *Nätverkskonfiguration.*
http://www.sslug.dk/artikler/gnulinux/node120.html [hämtat 28.10.2014]

Finn, Orfano., 2011 *The Difference Between Roaming Profiles and Local Profiles.*
http://www.brighthub.com/computing/smb-security/articles/9325.aspx [hämtat 13.11.2014]

Morimoto, R.,Noel, M.,Yardeni, G.,Droubi, O.,Abbate, A.,Amaris, C., 2013. *Windows Server 2012 - Unleashed*, USA, Sams Publishing.

Microsoft, 2013. *System Requirements and Installation Information for Windows Server 2012 R2***.**
http://technet.microsoft.com/en-us/library/dn303418.aspx [hämtat: 15.10.2014].

Microsoft, 2003. *The Logical Structure of Active Directory.*
http://technet.microsoft.com/en-us/library/cc759073(v=ws.10).aspx [hämtat: 17.10.2014].

Microsoft, 2012. *Deploy Roaming User Profiles.*
http://technet.microsoft.com/en-us/library/hh848267.aspx [hämtat: 17.10.2014]

Microsoft, 2012. *WDS.*
http://technet.microsoft.com/en-us/library/hh831764.aspx [hämtat: 23.10.2014

Microsoft, 2008. *Rollen Windows Deployment Services.*
http://technet.microsoft.com/sv-se/library/cc770628(v=ws.10).aspx [hämtat 28.10.2014]

Microsoft, 2008. *Introduktion till Windows Deployment Services*
http://technet.microsoft.com/sv-se/library/cc770667(v=ws.10).aspx [hämtat 3.11.2014]

Microsoft, 2008. *Så här fungerar organisationsenheter*
http://technet.microsoft.com/sv-se/library/cc771811.aspx [hämtat 3.11.2014]

Microsoft, 2008, *Så här fungerar gruppkonton*
http://technet.microsoft.com/sv-se/library/cc733001.aspx [hämtat 3.11.2014]

Microsoft, 2008. *Förstå den logiska Active Directory-modellen.*
http://technet.microsoft.com/sv-se/library/cc770319(v=ws.10).aspx [hämtat 6.11.2014]

Microsoft, 2014. *Group scope.*
http://technet.microsoft.com/en-us/library/cc755692%28v=ws.10%29.aspx [hämtat 21.11.2014]

Microsoft, 2005. *Group types.*
http://technet.microsoft.com/en-us/library/cc781446(v=ws.10).aspx [hämtat 21.11.2014]

Preboot Execution Environment, (u.å.).
http://sv.wikipedia.org/wiki/Preboot_Execution_Environment [hämtat 28.10.2014]

Steve Clines och Marcia Loughry, u.å. *Roles of the Active Directory Domain Controllers.*
http://www.dummies.com/how-to/content/roles-of-the-active-directory-domain-controllers.html [hämtat: 6.11.2014]

Tyson, Jeff och Crawford, Stephanie, 2011. *How VPN Works*
http://computer.howstuffworks.com/vpn.htm [hämtat: 17.10.2014]

Tyson, Jeff., 2001 *How Network Address Translation Works*.
http://computer.howstuffworks.com/nat.htm [hämtat 13.11.2014]

VPN, En krypterad tunnel till företaget, (u.å.).
http://www.omwlan.se/artiklar/vpn.aspx [hämtat 28.10.2014]

14 FIGURFÖRTECKNING