YRKESHÖGSKOLAN NOVIA

Planering av rollbaserade mapprättigheter i Windows-miljö

Jan Bergman

Examensarbete för Tradenom (YH)-examen
Utbildningsprogrammet för Informationsbehandling
Raseborg 2014

EXAMENSARBETE

Författare: Jan Bergman

Utbildningsprogram och ort: Informationsbehandling Raseborg

Handledare: Klaus Hansen

Titel: Planering av rollbaserade mapprättigheter i Windows-miljö

Datum 9.12.2014 Sidantal 36 Bilagor 0

Abstrakt

Detta examensarbete beskriver utformningen av en plan att skapa ett rollbaserat mapprättighetssystem i Windows-miljö. Närmare sagt utvecklingsarbetet grundar sig på Active Directory. Jag använder mig av grupper i Active Directory för att möjliggöra rollbaserad administration av mapprättigheter.

Examensarbetet är indelat i tre delar: teori, utveckling och avslutning. Teoridelen börjar med att förklara olika begrepp som hör ihop med Active Directory. Jag förklarar begrepp som Domain Controller, Domain och Forest, m.m. Efter att jag beskrivit de olika begreppen kommer jag till RBAC. Role Based Access Control är principen att ge rättigheter till roller istället för till användare i ett system. Man kan skapa hierarkier med roller och detta beskrivs i slutet av teoridelen. Sedan kommer utvecklingsdelen, där jag beskriver det praktiska arbetet. Till denna del hör kartläggning, planering och implementering. Jag kartlägger Active Directory m.h.a. inbyggda verktyg och skript. Sedan planerar jag ramarna för rollbaserade mapprättigheter. Detta handlar om att göra upp planer för OU-struktur och gruppstruktur. Efter det beskriver jag den implementeringen. Dock är inte all implementering med.

Resultatet av detta examensarbete blev en plan för hur man skapar ett rollbaserat mapprättighetssystem. Jag beskriver hur man kan implementera ett sådant system i Windows-miljö. Dock anser jag att det finns andra sätt att hantera elektroniska dokument och dylikt i dagens moderna värld.

Språk: Svenska

Nyckelord: Active Directory, Rollbaserad, RBAC, mapprättigheter

---

BACHELOR'S THESIS

Author: Jan Bergman

Degree Programme: Business Information Technology

Supervisors: Klaus Hansen

Title: Planning of role-based folder permissions in a Windows environment

---

Date 9.12.2014 Number of pages 36 Appendices 0

Abstract

This thesis describes the design of a plan with which a role-based folder permission system can be created in a Windows environment. Specifically said the development is based on Active Directory. I use groups in Active Directory to enable role-based administration of folder rights.

The thesis is divided into three parts: theory, development, and conclusion. The theory part begins by explaining various concepts associated with Active Directory. I explain concepts such as Domain Controller, Domain, and Forest, etc. After describing the different concepts I come to RBAC. Role Based Access Control is the principle of providing rights to roles rather than to users of a system. Hierarchies of roles can be created and this is described at the end of the theoretical part. Then comes the development part, where I describe the practical work. This part includes mapping, planning, and implementation. I chart the Active Directory by means of built-in tools and scripts. Then I plan the framework for role-based folder rights. This involves making plans for the OU structure and the group structure. After that I describe the implementation. However, all of the implementation is not included.

The results of this thesis became a plan for the creation of a role-based system of folder rights. The implementation of such a system in a Windows environment has been described in my thesis. However, I believe that there are other ways to manage electronic documents and such in today's modern world.

Language: Swedish

Keywords: Active Directory, Role-based, RBAC, folder permissions

---

Innehållsförteckning

1 Inledning

Jag började under hösten 2013 att fundera ut vad jag skulle göra för mitt examensarbete. Jag höll semester under augusti månad och började söka ett ämne för examensarbetet under september. Jag hade gjort en praktik på sommaren för Crossdesigns så jag ringde till Carl-Johan Backman(dåvarande delägare av företaget) för att fråga om ett eventuellt examensarbete. Då fick jag höra att de hade ett Active Directory-projekt (Samtal på telefon under september månad 2013). Då talade vi om att man borde göra Active Directory:n (AD) mera aktuell och kolla att mapprättigheterna är aktuella. Jag började göra på examensarbetet den 9 september 2013. Christo (IT-assistent i Ingå kommun) och Carl-Johan gjorde upp ett konto i deras nätverk och jag fick tillgång till AD:n.

När jag tittade på Ingå kommuns nätverksmappar märkte jag att de var i ganska bra skick, de var endast föråldrade. Mapparnas rättigheter var inte aktuella. Mapparnas namn var för de mesta på engelska och t.ex. translatorn för kommunen tyckte inte om det. Förvaltningsspråket är svenska, så allt skall vara på svenska.

Ingå kommun är en liten kommun i västra Nyland med cirka 5500 invånare. Ingå är mest svenskspråkig, 55 % svenskspråkig och 42 % finskspråkig.(Kort om Ingå, 2012). Ingå är bekant för mig för att jag växte upp där.

2 Syfte

Examensarbetets syfte är att planera, utveckla och implementera ett roll-baserat mapprättighetssystem med utgångspunkt i Active Directory. Till examensarbetet hör också att granska rättigheterna till filresurserna är aktuella och säkra och en omstrukturering av nätverksmappstrukturen. Detta examensarbete innefattar inte dator- eller användarobjekt, utan koncentrerar sig på mapprättigheter och AD-grupper.

Själva examensarbetet är indelat i två stora sektioner: teori och tillämpning. Teoridelen innehåller bakgrundsteori för den teknologi som tillämpas i

utvecklingsarbetet. Till teknologin hör för det mesta olika begrepp anknutna till Active Directory. Utvecklingsdelen beskriver praktiska arbetet, som föregås av en planeringsprocess. Utvecklingen är indelad i tre delar: kartläggning, planering och implementering.

3 Teori

3.1 Active Directory

3.1.1 Beskrivning

Active Directory (AD) är en katalog på alla resurser i ett nätverk (Active Directory, 1999). Resurser kan vara datorer, användare eller skrivare. Dessa resurser kallas för objekt i Active Directory. Det finns andra sortens objekt också, t.ex. kontakter (Active Directory Users, Computers, and Groups, u.å.). Dessa objekt har olika attribut som är förknippade med dem (Active Directory Objects, u.å.). Attribut beskriver ett objekt, på ett eller annat sätt. I detta fall betyder det att man beskriver någonting om t.ex. en användare. Ett attribut hos ett användarobjekt skulle kunna vara förnamn eller telefonnummer. Dessa objekt och deras attribut är mera på gräsrotsnivå. Jag förklarar mera om AD:n i stora drag i ett senare skede.

Enligt Kivimäki (2009 s.651) är Active Directory en katalogtjänst som baserar sig på en Internetstandard. Dess uppgift är att minska olika register och på samma gång ge ett gemensamt gränssnitt för att hantera olika saker. Tidigare var det svårt att hitta alla resurser i ett nätverk. Det fanns inte en plats man kunde titta och hitta det man sökte. Tidigare fanns det olika verktyg för att hantera dessa saker men de förde olika problem med sig. Vissa kunde användas bara av administratörer och vissa hade klumpiga grafiska gränssnitt. Man hade också problem med att nätverken blev hela tiden större, vilket satt nya krav på programvaran. Active Directory skapades för att underlätta detta. Den första Active Directory kom med Windows 2000. (Active Directory, 1999).

Man kan utnyttja AD på olika sätt, t.ex. då en användare loggar in på nätverket (kallas i detta fall också till domän) kollas det i AD:n om denna användare finns. Om användarnamnet och lösenordet finns i registret tillåts inloggningen, annars

nekas den. För att AD nås på hela nätverket fungerar inloggning från alla datorer inom samma nätverk.

Man kan indela användarna i olika grupper och sedan kan man ge dessa grupper olika rättigheter (Active Directory Collection, u.å.). Active Directory kan användas också vid inventering av datorer och användare. Detta är speciellt viktigt i stora organisationer för att själva mängden av datorer är svårt att inventera och kan i vissa fall vara mycket tidskrävande. Man kan använda informationen i AD:n för att underlätta detta. Man kan säga att AD:n i vissa fall används som ett register över användare och datorer.

AD används i Ingå kommun för att hantera inloggning och rättigheter. Rättigheter till nätverksmappar hanteras m.h.a. AD. Utan AD kan man inte ha rättigheter inom ett nätverk, utan endast lokalt på datorer. AD möjliggör att man kan hantera rättigheter till nätverksmappar på ett effektivt sätt. AD kan användas till andra ändamål, men jag koncentrerar på mapprättigheter i detta examensarbete. Läs mera om mapprättigheterna i Ingå kommuns fall i kapitel 4 och framåt.

3.1.2 Struktur

Active Directory:s struktur består av fyra olika saker: Forest, Tree, Domain och Site. De är uppräknade i hierarkisk ordning, alltså Forest är största enheten, sedan kommer Tree osv. De tre första termer syftar på AD:ns logiska struktur, medan Site tillhör den fysiska strukturen. En domän kan sträcka sig över flera *Sites*. Med termen *Site* brukar man mena en fysisk plats, eller ett subnät i ett ip-adressområde. Domain, Tree och Forest förklaras mera i detalj i ett senare skede.

Det finns en logisk struktur och en fysisk struktur i AD.(Understanding the Active Directory Logical Model, u.å.). Dessa är två helt olika saker och är inte bundna till varandra. Men man måste ändå ta båda i beaktan när man planerar en AD-miljö.

3.1.3 Domain Controller

Domain Controller(DC) är en ytterst viktig del av Active Directory. AD skulle inte fungera utan en DC. Detta är en roll som installeras på ett Windows Server-operativsystem som heter Active Directory Domain Services (AD DS). Enligt Kivimäki:s bok om Windows Server 2008 R2 (2009 s. 651), betyder det att Active Directory inte är bara en ”directory”, utan har också ”services” anknutet till den. ”Directory” syftar på ”databasen” som förklarades i kapitel 3.1.1. och ”services” syftar på användarkontons administration.

Domain controller:n ansvarar primärt för domänens säkerhet. Den hanterar autentiseringen av användare i domänen och hanterar rättigheterna till delade resurser (Security information for Active Directory, u.å.). Dessa delade resurser kan vara nätverksmappar eller printrar. En användare kan ha fulla rättigheter till en mapp och någon annan kan bara ha läsrättigheter till mappen. Detta betyder att förrän en användare får tillgång till någon resurs på nätverket måste användaren autentisera sig till DC:n och DC:n ger användare de rättigheter som den besätter. Detta betyder att användaren i inloggningsskedet får sina mapprättigheter.

Examensarbetet baserar sig på Ingå kommuns Active Directory och i detta fall fanns det två DC:n. Dessa DC:n jobbar ihop, om den ena skulle sluta fungera skulle den andra ta över. Detta är för att säkerställa att det åtminstone finns en DC som är hela tiden uppe.

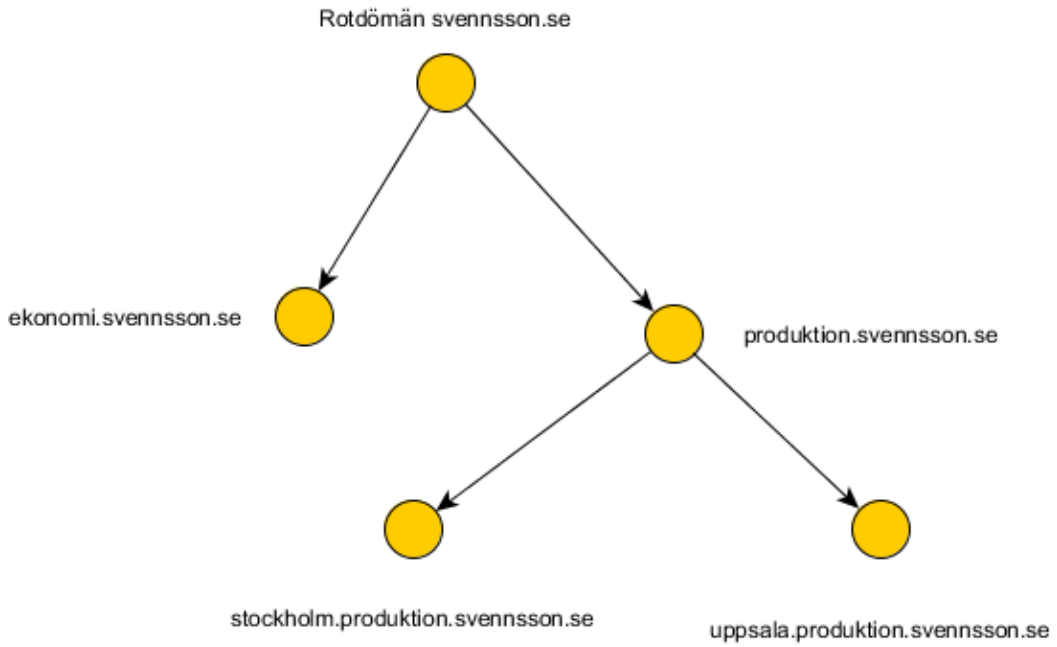
3.1.4 Domain

Domänen tillhör den logiska strukturen av AD. För att domänen är en del av den logiska strukturen kan en domän sträcka sig över flera sites (kapitel 3.1.2). M.a.o. kan en domän fungera i flera ip-adressrymder och därmed också på flera platser. I dagens läge är företagen ofta internationella, detta betyder att kontor är fysiskt spridda över hela världen. Men ett företag kan utöva liknande verksamhetsformer på olika platser. Ett företag som producerar mobiltelefoner kan producera olika telefoner på olika platser, tillsammans bildar alla dessa den totala produktionen. Då kan en domän fungera på alla dessa sites, man behöver inte göra en ny domän för varje fysisk plats. Varje Active Directory måste ha en rotdomän (kallas för forest root domain) och ifrån rot-domänen grenas de övriga domänerna. Man kan

tänka sig att rot-domänen är trästommen som det grenar sig till underdomäner (Se Figur 1).

Domän brukar ha ett beskrivande namn också, t.ex. ett företag som heter Svensson ab kunde ha en domän som skulle heta svensson.se (se Figur 1). Rot-domänen skulle då heta svennson.se, men en underdomän skulle heta t.ex. ekonomi.svennsson.se. Underdomän får oftast överliggande domänen till suffix. På så sätt kan bygga upp sin *forest*, mera om detta i nästa kapitel.

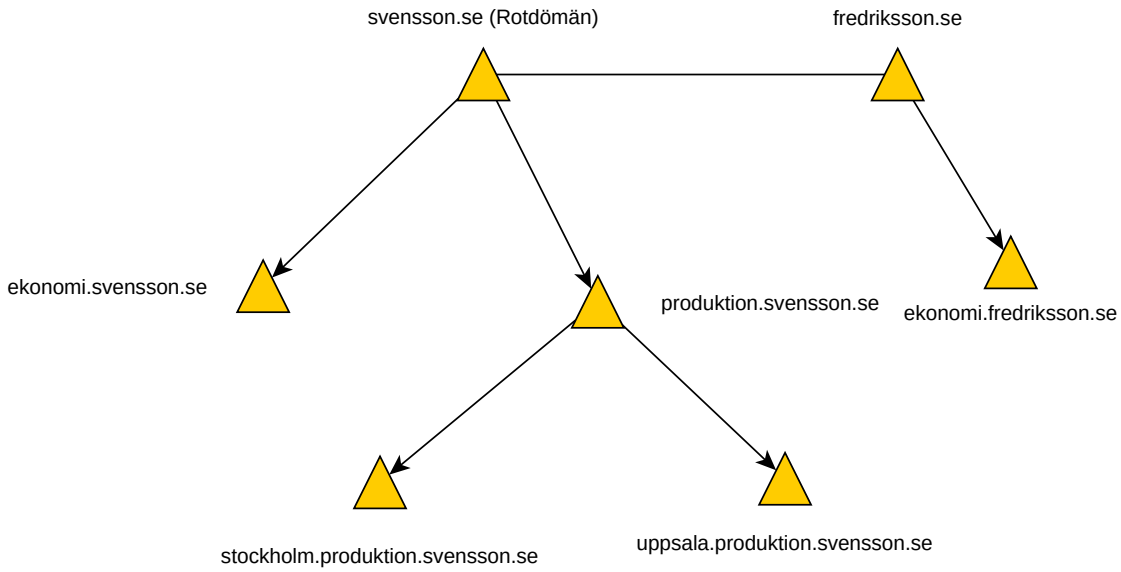
Figur 1 demonstrerar hur en domän kunde se ut. Detta är ett exempel hur domänstrukturen kunde se ut. Man kan göra upp sin domänstruktur på olika sätt, då när man gör upp en domänstruktur så är det viktigt att veta hur domänen fungerar i praktiken. Ibland kan det räcka med bara med en rot-domän, man kan i framtiden alltid tillägga underdomän om det så behövs.



Figur 1 Exempel på en domänstruktur

Om man bara har en domän delar man in det m.h.a. Organizational Units (OU), mera om OU:n i ett senare kapitel. Det är oftast lättare att administrera en domän än flera domäner.

Det som alla inte inser när det kommer till domänstruktur, är att man kan ha flera domänträd i en forest. Med forest menar man kort sagt hela AD. Domänträd börjar med trädrot-domän (Svensson.se i Figur 2) och sedan gör man en ny trädrot(fredriksson.se).



Figur 2 Exempel på en domänstruktur

Den nya trädroten kan heta något helt annat än forest-roten. T.ex. Svensson ab bildar ett dotterföretag som har samma fysiska nätverksstruktur som dess ägarföretag (Svensson Ab). Det nya företaget använder sig i stort sätt samma IT-personal som ägarföretaget. Då skulle man kunna göra en ny trädgren som heter t.ex. fredriksson.se (Se Figur 2). I detta sammanhang skall man märka att även om en ny trädrot finns, är det nya domänen (fredriksson.se) inte helt isolerat.

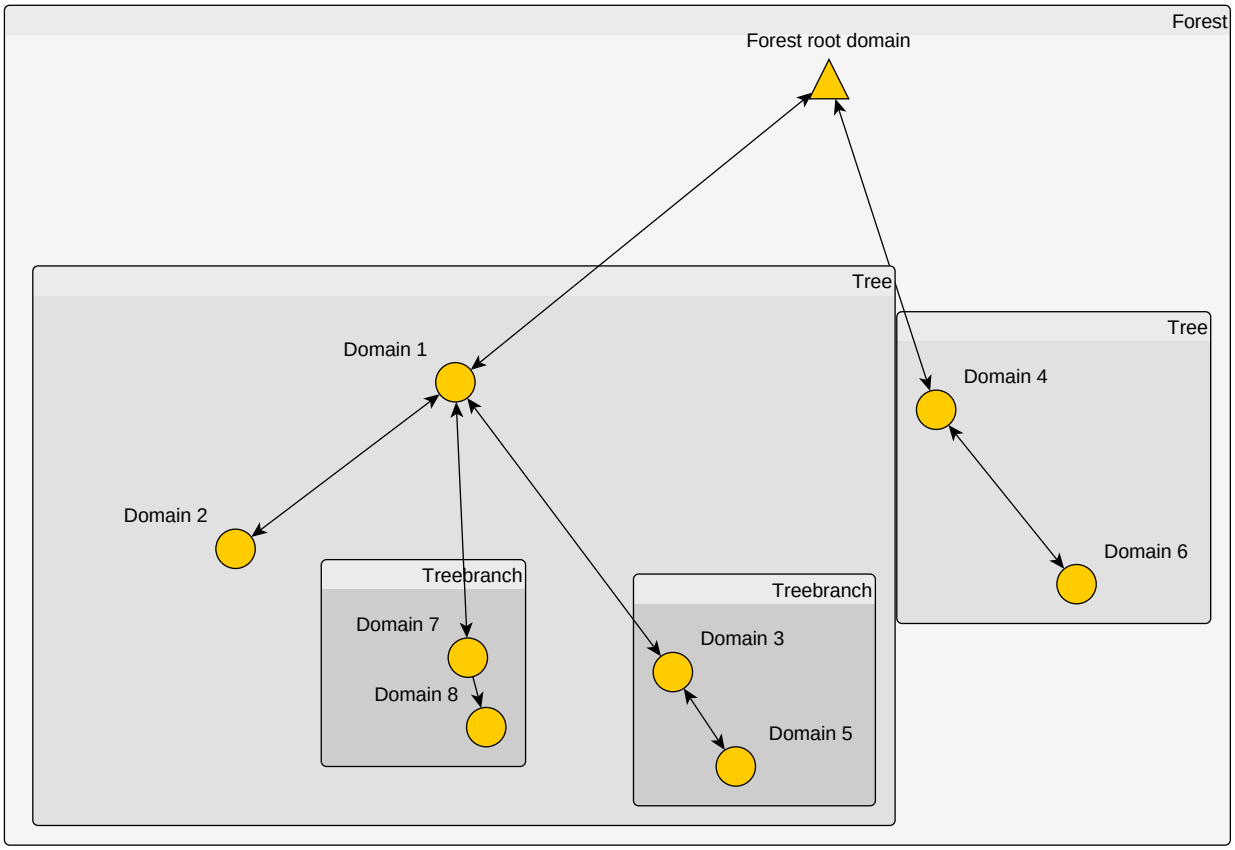
Domänen fungerar delvis som en sorts behållare, it-administrationen kan delas upp med m.h.a. domänstrukturering (What Are Domains and Forests? u.å.). Om vi tar som exempel ett internationellt företag, ett företag som har produktion i flera länder. Företaget har IT-personal på alla dessa platser. Då kan man göra en domän för varje fysisk plats och på sätt centralisera it-administrationen bara för en viss plats. Då kan man göra så att bara lokala administratörerna som är fysiskt på en plats hanterar den platsens domän. Indelningen skulle också kunna vara t.ex. ett dotterbolag, eller egentligen vad som helst.

Domän fungerar också som en säkerhetszon. D.v.s. användare tillhör en domän och kan därmed ges rättigheter eller privilegier i denna domän. Användare autentiseras i en domän och då ges användaren dess befogenheter. Domän används i denna bemärkelse också för att tillämpa policy. D.v.s. om man vill applicera en policy på t.ex. på en specifik geografisk plats och en annan policy på en annan plats, kan man urskilja dessa med att skapa respektive domän. Men det är också möjligt att urskilja dem med m.h.a. OU:n, som tidigare nämnts. (What Are Domains and Forests? u.å.). Dock skall man komma ihåg att domän inte fungerar som en absolut avgränsning med tanke på säkerhet. Man kan inte helt och hållet isolera domän ifrån varandra, utan istället urskiljer man *forests* istället. Isolering sker på s.k. *forest*-nivå och inte på domän-nivå.

3.1.5 Forest

En s.k. *forest* i detta sammanhang är en samling av olika domän (Terms and Definitions, u.å.). Forest är egentligen hela AD:n, men man kan ha flera *forests* ihopkopplade. Forest är den största enheten när man tänker på AD:ns logiska struktur. Det är också den absoluta avgränsningen i AD med tanke på säkerhet. Om t.ex. är man ”domain admin” i en domän kan man göra sig själv till Enterprise Admin och då har man full kontroll över alla domän i en forest. Men man kan inte få full kontroll över andra *forests* på detta sätt.

Forest representerar flera domäner som har gemensamma egenskaper. Varje forest som har flera underdomäner bildar s.k. träd (Se Figur 3). Dessa träd bildar grenar(tree branch) när ett träd delar på sig. Dessa grenar bildar ett ömsesidigt förtroende mellan alla domänerna som är kopplat ihop, det illustreras som pilar i Figur 3 (Trust transitivity, u.å.). Dock har en forest alltid en rotdomän (Achieving Autonomy and Isolation with Forests, Domains, and Organizational Units, u.å.).



Figur 3 En forest med flera underdomäner

3.1.6 Organizational unit

En s.k. organizational unit (OU) i Active Directory är en "container". Man kan tänka att organizational units är som mappar dit man kan sätta andra mappar och filer. I detta fall är mapparna organizational units och filerna är andra objekt (Organizational units, u.å.). Man kan på så sätt organisera objekten innanför en domän på ett logiskt sätt, en OU kan ha en annan OU innanför sig också. Man kan på det viset göra upp en struktur som är unik i det domänen som den befinner sig i. Denna OU-struktur ofta speglar organisationens struktur. OU-strukturen kan också hjälpa att organisera alla objekt innanför en domän.

Organizational units och dess struktur används för att applicera GPO:n (Group Policy-objekt) eller delegera administration (Delegating administration, u.å.). Man kan t.ex. tilldela en viss printer för användare inom en viss OU genom att applicera en GPO eller man kan göra andra inställningar via GPO. Man kan också delegera vissa administrativa rättigheter inom en OU åt en användare.

I ett senare skede kommer jag att göra upp nya OU:n i Ingå:s AD för de nya grupperna som jag skapar för att möjliggöra rollbaserade mapprättigheter. OU:n används i detta sammanhang som en urskiljning ifrån de OU:na som Ingå kommun hade från förut. Detta beskrivs i kapitel 4.1.2.

3.1.7 Group Policy

Microsoft beskriver Group Policy som ett system där man kan göra skräddarsydda konfigurationer för olika datorer och användare (Group Policy, u.å.). Man kan då t.ex. göra så att vissa printrar installeras på vissa datorer och vissa användare får tillgång till vissa nätverksresurser. Det är ett enkelt sätt att centralt implementera en ändring i it-resurserna. Om det inte skulle finnas Group Policy skulle man behöva göra varje ändring till varje dator och användare skilt för sig, vilket skulle ta överdrivet länge att göra.

Group policy sparas i s.k. Group Policy-objekt(GPO) och dessa förknippas sedan antigen med hela Active Directory, en domän eller en OU. Man kan också använda sig av s.k. ”Security filtering”, då kan man specificera att en GPO bara appliceras på en viss grupp (Security filtering using GPMC, u.å.). Det finns också WMI-filtrering, då kan man filtrera t.ex. enligt operativsystem eller datormodell (WMI filtering using GPMC, u.å.).

Jag kartlägger i detta examensarbete Ingå kommuns Group Policy-objekt för att kunna se vilka grupper i AD är sådana som måste sparas och vilka kan tas bort. Grupperna i AD:n förklaras till nästa och mera om kartläggningen av GPO:n finns i kapitel 4.1.3.

3.1.8 Grupper

Grupperna i Active Directory är ganska lika som OU:n. Enligt Microsoft kan man gruppera användare, datorer och kontakter (Groups, u.å.). Man kan också sätta grupper innanför andra grupper och på så sätt skapa hierarkier. Grupperna finns på två olika ställen, lokalt på datorn eller i Active Directory. Lokala grupper används endast lokalt på datorn, däremot används AD-grupper i hela AD:n.

Skillnaden mellan OU:n och grupper är att samma objekt kan finnas i flera grupper, men ett objekt kan finnas bara i en OU. Grupperna är bl.a. gjorda för att underlätta administration. Man kan ge rättigheter eller privilegier på gruppnivå istället för att ge dem på objekt-nivå. Rättigheter kan vara en rättighet till en nätverksmapp och privilegiet kan vara t.ex. att en grupp användare får lägga till GPO:n till en OU. Grupper kan också användas för att distribuera e-post, de kallas för ”Distribution Groups”. Man kan också sätta olika omfång eller ”scope” på grupper. Det finns tre olika omfång, de kallas för: Universal, Global och Domain local (Group scope, u.å.).

3.1.9 Groupscope

”Groupscope” beskriver gruppens räckvidd eller dess tillämpningsområde. Både ”security groups” och ”distribution groups” kan vara antingen en universal, global eller domain local-grupp. Tillämpningsområde definierar vilka objekt gruppen kan innehålla och vilka rättigheter kan appliceras på gruppen (Group scope, u.å.).

Domain local-grupper är grupper som är innanför en domän. Rättigheter kan appliceras bara innanför samma domän som gruppen finns på. Med andra ord om det finns en grupp på en domän som heter domainA.local och det finns användarobjekt som ligger på samma domän som sätts i denna grupp, kan man applicera rättigheter för dessa medlemmar bara innanför denna domän. Det kan också finnas grupper från andra domän i denna sorts grupp, men man kan bara applicera rättigheter till den domänen som föräldragruppen är i.

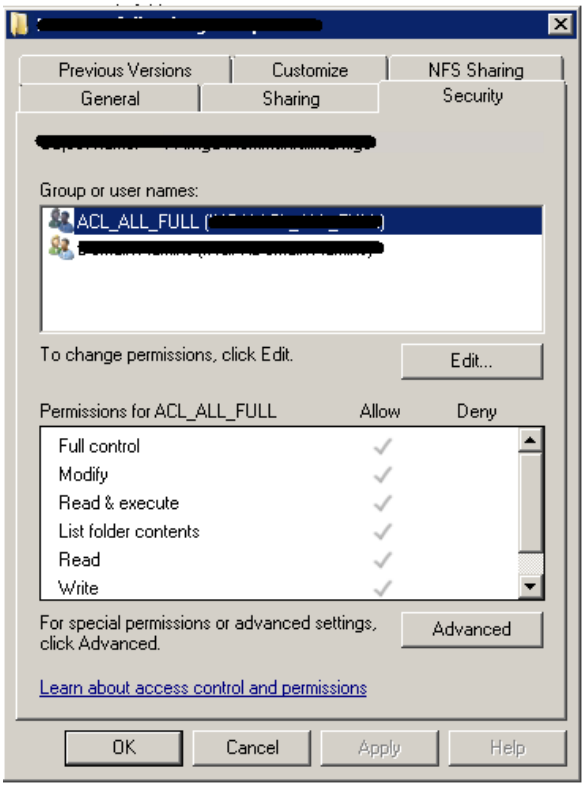
Global-grupper är grupper vars omfång omfattar alla domäner. Man kan applicera rättigheter till dessa grupper på vilken domän som helst. I dessa sortens grupper kan man sätta andra grupper som har samma omfång och finns i samma domän och användare eller datorer som finns i föräldragruppens domän. Den här gruppsorten är speciell på det viset att man kan applicera rättigheter till denna grupp på vilken domän som helst.

Universal-grupper är grupper med stor skala eller omfång. Omfånget på dessa grupper innefattar alla domänerna och alla Forests. Man kan sätta in alla datorer och användare som tillhör samma forest som gruppen befinner sig i. Andra universal-grupper och global-grupper kan sättas som medlem i grupper med universal-omfång. Man skall observera att man inte kan sätta Domain local-grupper i global-grupper.

3.1.10 Grupptyper

Security Group

En ”Security group” är en grupp för att hantera säkerhetsaspekter. Man kan ge t.ex. mapprättigheter till en sådan grupp (Se Figur 4). Man kan också hantera användarbefogenheter. T.ex. när man installerar AD DS skapas en grupp som heter Backup Operators (Understanding Group Accounts, u.å.) och medlemmar i denna grupp kan säkerhetskopiera och återställa filer och mappar på domänen. I detta examensarbete används dessa grupper för att hantera mapprättigheter.



Figur 4 Security group:en ACL_ALL_FULL används här för att ge fulla rättigheter till en mapp

Distribution Group

”Distribution groups” används för att distribuera e-post. T.ex. man kan göra en avdelning till en distribution group. Då kan man skicka e-post till en e-postadress och sedan skickas e-posten till alla inom avdelningen. Man kan också sätta dessa typens grupper innanför varandra. Man kan också sätta ”security groups” innanför ”distribution groups”.

3.1.11 Gruppärftlighet

Grupper i AD använder sig av gruppärftlighet, detta betyder att man kan sätta en grupp som medlem till en annan grupp. På så sätt kan man göra upp en hierarki m.h.a. grupper. Detta betyder att säkerhetsaspekterna ärvs. Detta betyder att om vi har en grupp som heter Grupp1 och Grupp2 är medlem i Grupp1. Då har Grupp2 samma mapprättigheter som Grupp1. Det är detta hela examensarbete bygger på. Dock skall man komma ihåg vilka grupper man kan sätta in i vilka grupper, detta är beskrivet i kapitel 3.1.9.

3.2 Mapprättigheter i Windows

Enligt Microsoft så ärvs mapprättigheterna, d.v.s. om det finns mapp A och innanför den finns en mapp som heter mapp B. Då ärver mapp B rättigheter av mapp A (What Are Permissions? u.å.). Men man kan också göra en inställning så att mapp B inte ärver rättigheterna, men detta behövs oftast endast i specialfall. Det är också viktigt att komma ihåg att användare som inte fått jakande eller nekande rättighet till en resurs får inte komma åt den. Alltså man behöver inte neka ett objekt för att neka den tillgång till en fil eller en mapp (File and Folder Permissions, u.å.). Detta examensarbete har mycket med mapprättigheterna att göra, man kan hantera dem m.h.a. gruppärftlighet.

3.3 PowerShell

Jag använder mig av en teknologi som heter Windows PowerShell. Den är en slags ny kommandotolk för systemadministratörer (Windows PowerShell, u.å.). Dess huvudsakliga uppgift är att underlätta administration i Windows-miljö. M.h.a. den kan man automatisera olika aktiviteter. Man kan t.ex. skriva kod som utgör underhållningsuppgifter, detta betyder att man inte behöver sätta tid på uppgifter

som är upprepande. Den innehåller s.k. cmdlets som är små program gjorda för att göra vissa aktiviteter. Jag använder en cmdlet i ett senare skede för att få en rapport på group policy-objekt.

3.4 Role based access control

”Roll based access control” (RBAC) är ett system för att hantera transaktioner eller rättigheter i ett datorsystem. Istället för att ge en rättighet till en användare ger man den till en roll. Sedan ges användarna en eller flera roller och därmed får vissa rättigheter (Sandhu, Ravi S., 1998, sida 237). Denna roll beskriver oftast en persons uppgifter inom en organisation t.ex. försäljningschef, bokförare eller revisor.

3.4.1 Fyra olika RBAC-modeller

Det finns fyra olika komponenter för RBAC. Dessa komponenter baserar sig på en standard av ANSI och INCI. Den heter ANSI INCITS 359-2004. De fyra komponenter definieras i standarden som: Core RBAC, Hierarchical RBAC, Static Separation of Duty Relations och Dynamic Separation of Duty (American National Standard for Information Technology, 2004, sida 2).

Core RBAC är den s.k. kärnan i RBAC, de element som finns i denna komponent behövs för att göra upp ett RBAC-system. Den består av fem viktiga element: användare, roller, objekt, operationer och tillstånd. Begreppen förklaras i tabellen nedan:

Tabell 1 Olika elementen i RBAC

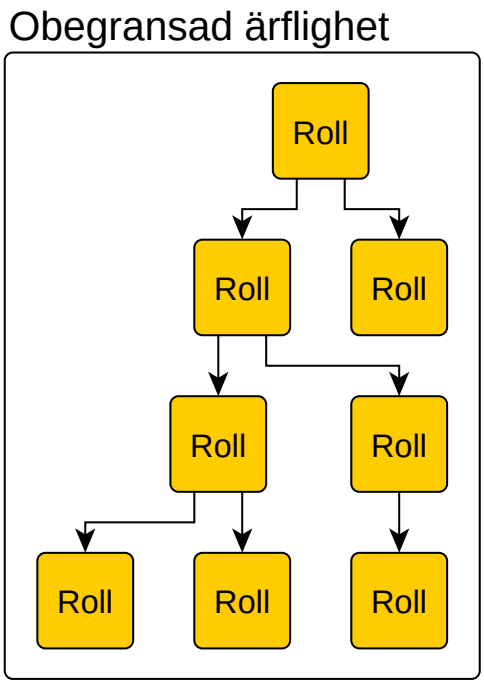
Användare	refererar oftast till personer, men kan också betyda andra saker i olika sammanhang. T.ex. en dator kan vara en användare i ett sammanhang som det finns inte personer.
Roll	är t.ex. arbetstitel, avdelning eller arbetsuppgift, exempel nämns tidigare i examensarbetet.
Objekt	är något som skyddas av RBAC. Detta är oftast information eller ett sätt att hämta information.

Operation	är en funktion som användaren exekverar.
Tillstånd	Det en roll måste ha för att göra en operation på ett objekt.

Förutom dessa element har Core-RBAC ett ytterligare element, sessioner. En session är ett sammanhang där en användare anknyts till en del av dess roller. Allt detta är grunden i RBAC.

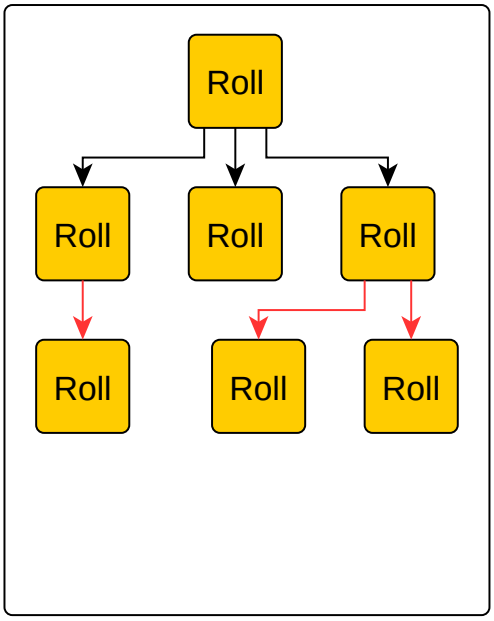
Hierarchical RBAC är till grunden samma som Core-RBAC. Men den har en ytterligare egenskap, rollhierarki. I denna rollhierarki introduceras också rollernas ärftlighet. Detta menar man att en roll kan ärva de roller som är under den i hierarkin (Se Figur 5). Detta kan göra rollerna tydligare att förstå och betydligt mindre till antal. Det finns en variant av detta där man får ärva bara en roll, inte alla underliggande roller (Se Figur 6). Dessa två metoder är de som används i standarden.

I detta examensarbete använder jag mig av ärftlighetsprincipen. Jag skapar grupper som ärver rättigheter av underordnade roller i hierarkin. Läs mera om detta i kapitel 4.2. Det jag tillämpar sätter inte restriktioner på hierarkin, utan ärftligheten sträcker över flera roller i samma gren i hierarkin. Till följande några bilder som tydligt illustrerar de ovannämnda två varianterna:



Figur 5 RBAC med obegränsad ärftlighet i en rollhierarki

Roll hierarki där rollerna ärvs bara till en nedanstående roll.
D.v.s. ärftligheten följer inte enda ner (röda pilarna).



Figur 6 RBAC med begränsad ärftlighet i en rollhierarki

Detta definierar Hierarchical RBAC, alltså rollerna gör upp en hierarki. Det finns ännu två mera avancerade modeller i standarden. Dessa heter Static Separation of Duty Relations och Dynamic Separation of Duty Relations. Ingendera av dessa tillämpar jag i detta examensarbete, men de tillhör standarden. Dessa två kategorier brukar kallas också för ”Constrained RBAC”. Med denna tillämpning vill man ha ett sätt att begränsa de operationer som en användare har tillstånd till. Detta betyder att man inte kan missbruka systemet utan att två eller flera personer är inblandade.

Ett scenario skulle vara t.ex. att ett företag skall köpa saker ifrån ett annat företag. Vanligtvis finns det flera personer inblandade i denna funktion. Men tänk dig en anställd med en hög post inom företaget, denna person skulle enligt RBAC ärva de roller som är nedan i hierarkin. Detta betyder att denna person som är högt uppe i hierarkin skulle kunna missbruka detta om den så ville. Men om man sätter en restriktion att denna person högt uppe skulle kunna göra beställningen men inte bekräfta den. Då kan inte denna person missbruka systemet och detta är Static Separation of Duty Relations. Man sätter restriktioner på att en användare kan få en viss roll, men då utesluts vissa andra roller. I exemplet ovan betyder det att personen får göra en beställning (rollen ”beställare”), men inte bekräfta beställningen (en roll som kan bekräfta). Detta är ett översimplifierat exempel för tydlighetens skull, i verkliga livet kan strukturen vara betydligt mera komplex.

Den andra är Dynamic Separation of Duty Relations, till skillnad till den statiska versionen får användare vissa roller beroende på dess session. Detta betyder att man inte kan använda roller som kan missbrukas samtidigt. Under olika sessioner besätter man olika tillstånd till samma operation och då kan man inte missbruka systemet. I exemplet ovan skulle det betyda att du inte kan ha rollen som kan bekräfta förrän din egen beställning är bekräftad av en annan roll som kan bekräfta. Detta betyder att din beställning måste bli bekräftad av någon annan under den tid du har rollen beställare. Detta är en omständighet som kan användas i ett RBAC-system som har Dynamic Separation of Duty Relations.

4 Utveckling

4.1 Kartläggning

För att kunna lyckas med projektet måste man kartlägga nuläget och hurdan AD:n skulle kunna se ut i framtiden, med användning av rollbaserad administration. Kartläggningen fokuseras på: Grupperna och deras medlemmar, Organizational Unit-strukturen, Group Policies och alla användare i AD:n. Datorerna är inte relevanta i detta examensarbete.

4.1.1 Grupperna och deras medlemmar

För att kunna eventuellt göra upp nya grupper måste man kartlägga nuvarande grupper. I början användes AD-grupperna i Ingå kommun för att dela kalendrar, ge mapprättigheter, tilldela GPO:n och ge rättigheter till programvara.

Det brukar oftast finnas många grupper i AD:n så det skulle ta länge om jag skulle gå igenom alla för hand. Så då började jag söka ett skript för att få ut grupperna och dess medlemmar. Jag hittade ett bra skript som gör precis det jag vill (Document Your Domain Groups, 2009). Skriptet skapar en Excel-fil där den på första fliken visar alla grupper. Gruppnamnen (nederst i tabell 2) är länkar till flikar i Excel-filen där dess medlemmar är, vilket underlättar märkvärdigt användarvänligheten. Skriptet separerar också på grupper med medlemmar och grupper utan medlemmar.

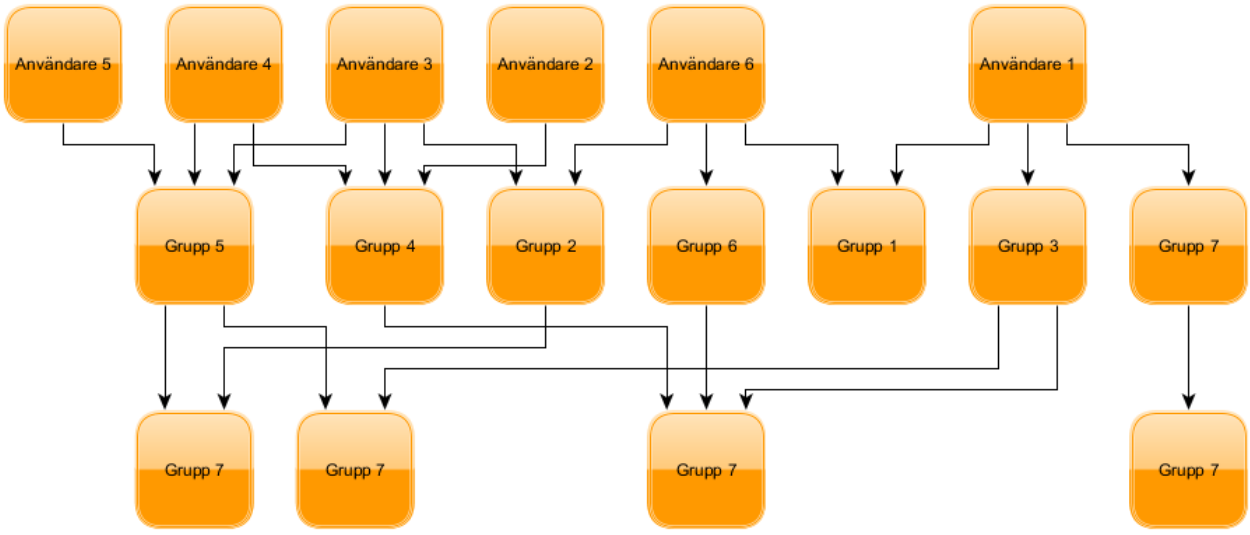
Tabell 2 Exempel på hur Excel-filen såg ut

Total Group Count	134			
Groups No Members	29			
Grupp1				
Grupp2				
Grupp3				
Grupp4				
	Grupp1	Grupp2	Grupp3	Grupp4

På basen av denna fil gjorde jag en ”mindmap” av alla grupper och dess medlemmar. ”Mindmappen” blev mycket bred, alltså det fanns många grupper, men de var inte inne i varandra. Man kunde jämföra det med en mapp med många mappar, men nästan inga undermappar. Jag beslöt mig för att inte använda ”mindmappen” för den var inte så särskilt bra. Den visade inte AD-gruppernas hierarki.

Jag hade en diskussion med IT-personalen och vi kom fram till att det skulle vara lättare om vi skulle göra upp en visuell bild av grupphierarkin. Det går helt enkelt lättare att se sambandet på grupperna om man ser dem visuellt hur de förhåller sig till varandra.

För att få en visuell bild använde jag mig av ett verktyg (Draw Nested AD Security Groups by MemberOf or Member Attributes, u.å). Det var ett skript som hette ”Graph-Nested-AD-Security”. Det var ett skript som gör upp en graf av ”security groups” i AD:n. Dess förmån var att den kunde visa grupphierarkier lätt. Skriptet gjorde en lättläst bild av hur grupphierarkin ser ut (Se Figur 7).



Figur 7 Exempel på resultatet av skriptet ” Graph-Nested-AD-Security”

Bilden blev jättestor och jag måste ta ut bara vissa delar av den för att kunna se hur grupperna ligger till förhållande till varandra. Man kunde ge vissa parametrar till

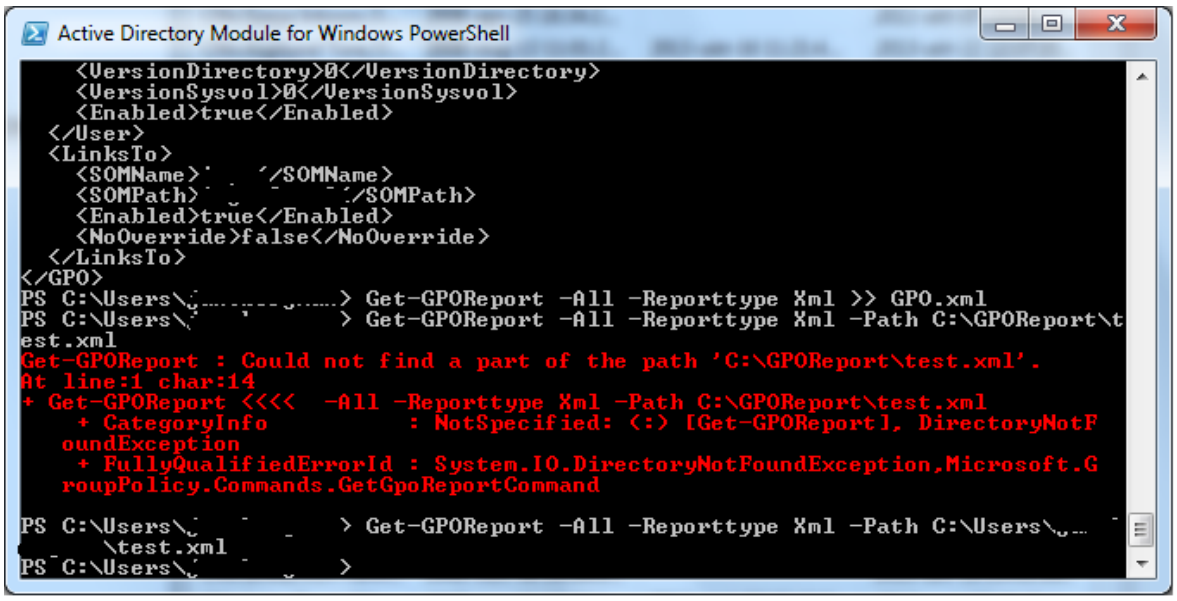
skriptet, m.h.a. dessa parametrar kunde man bestämma vad som den skulle rita upp. T.ex. det var möjligt att definiera att skriptet skulle utgå ifrån en OU och ta alla användare ifrån den och rita upp en karta på dem. Man kunde också t.ex. definiera att skriptet skulle läsa member-attributet istället för memberof-attributet. D.v.s. man kunde säga åt skriptet att utgå ifrån en OU där det fanns grupper och visa grupperna som är medlemmar till grupperna i specificerade OU:n. M.a.o. om det finns en OU som heter ”groups” och i den finns alla grupper, man kunde då lätt kartlägga vilka objekt är medlemmar av grupperna i OU:n.

4.1.2 OU-strukturen

OU-strukturen är ganska lätt att få fram. Man kan bara titta på översikten i ”Active Directory Computers and User”(ADUC) och de ser ut som mappar är OU:n (Se Figur 13 på sida 30). ADUC är ett verktyg för att administrera eller sätta in information till AD (Active Directory Users and Computers u.å.). Det finns säkert verktyg att få fram dem på ett annat sätt, men det behövdes inte i detta fall när det finns så få OU:n. Själva strukturen av OU:na var klar och förståelig, vilket lättade kartläggningen till sin del.

4.1.3 Group Policies

Group policy var ganska svårt att få ut. Det som jag var mest intresserad av var vilka grupper hade GPO:n associerade till dem. För att få ut denna information använde jag mig av en ”Powershell-cmdlet” som heter ”Get-GPOReport”. Enligt Microsoft genererar den en rapport antingen i XML-format eller i HTML-format (Get-GPOReport, u.å.). Rapporten är ganska stor och är ganska svår att läsa för att den har så många kolumner, men om man söker innanför filen så hittar man nog det som man söker.



Figur 8 Bild på när jag kör Powershell-cmdlet:en Get-GPOReport

M.h.a. denna rapport kunde jag kombinera informationen med grupper för att kunna urskilja grupper som är tillämpade GPO:n på. D.v.s. jag kunde urskilja de grupper som möjligen behövs också i framtiden ifrån de grupper som var onödiga.

4.1.4 Användare

En lista på användarna fick jag m.h.a. av ett program som hette AD INFO- Free edition (AD INFO - ACTIVE DIRECTORY REPORTING TOOL, u.å). Man kunde m.h.a. programmet välja vilken information man exporterar ifrån AD:n, det är oftast onödigt att exportera all information. Viktig information var t.ex. användarnas kontonamn, inloggningstidpunkt och olika attribut; så som avdelning, beskrivning och arbetstitel. Man kunde därefter sortera den i Excel enligt olika attribut. Jag använde denna information när jag började gruppera användare, mera om detta i kapitel 4.3.1 på sida 29.

4.1.5 Mapprättigheterna

Det finns inga inbyggda verktyg för att kartlägga mapprättigheterna på en filserver. Man skulle kunna gå in i alla mappar och se deras rättigheter, men det skulle ta orimligt lång tid. Därför måste man använda sig av skräddarsydda verktyg till detta. Verktygen gör också ofta så att man kan hantera informationen i Excel; vilket underlättar arbetet betydligt.

För att få reda på mapprättigheter använde jag mig av ett skript. (List Security of Folder and Subfolder, export information to CSV File, u.å). Skriptet går igenom alla mappar och ser vilka rättigheter en viss ”security group” har för den aktuella mappen. Sedan gör programmet en csv-fil av informationen. I csv-filen finns det mapplats, användare/grupp och dess rättigheter. Dessutom kan man ange en parameter till skriptet så att ärvda rättigheter inte kommer med i filen.

Denna information var viktig, för att se vilka grupper som har mapprättigheter applicerade till dem. Jag kunde kartlägga de grupper som har mapprättigheter med de som inte har. Då kunde jag se vilka grupper som är onödiga i miljön och vilka som måste sparas till övergångsskedet. D.v.s. för att kunna flytta det gamla materialet till det nya stället måste användarna ha rättigheter i gamla filsystemet.

4.2 Planering

4.2.1 Övergripande ram för att göra upp grupperna och OU:n

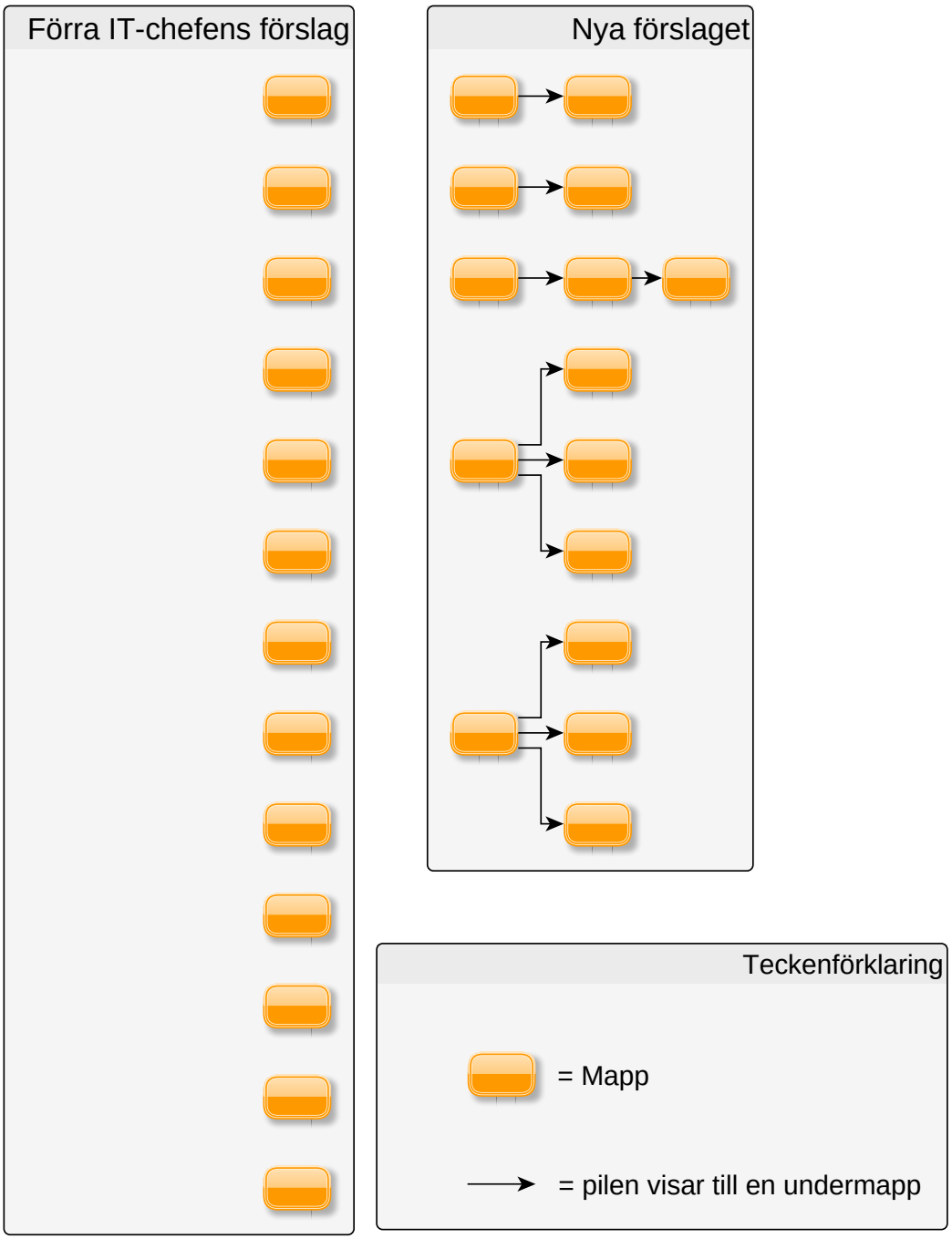
På basen av en video implementerade jag en s.k. ”Role based active directory”. (Role-Based Management Extreme Makeover for Active Directory, 2011). Det handlar om att ha mycket grupper innanför andra grupper. Man tilldelar användarna roller, en roll kan vara dess arbetstitel eller att den tillhör en viss avdelning. Sedan skulle man ge denna roll vissa rättigheter. I praktiken betyder det att alla användare tillhör en AD-grupp och man ger denna grupp motsvarande rättigheter som man skulle ge användaren. Man kan då sätta in nya användare till denna grupp eller ta bort användare och på så sätt lätt administrera rättigheterna.

Eftersom rättigheterna i systemet hanteras m.h.a. grupper betyder det att man behöver ett bra verktyg för att hålla reda på gruppernas hierarki. Denna hierarki är lättare att se om man ser den visuellt och till det behöver man verktyg för att kunna göra upp en sådan bild. I detta examensarbete använde jag ett verktyg som finns på Microsoft:s webbsidor. (Draw Nested AD Security Groups by MemberOf or Member Attributes, u.å.). Detta verktyg använde jag mig också för att visa till IT-assistenten de dåvarande grupperna och vi gick igenom tillsammans grupperna. Vi tittade igenom grupperna och gallrade bort onödiga grupper.

4.2.2 Mappstrukturen

Mappstrukturen ändrades på hösten 2014, till en mera snävare uppbyggnad. Den modellen som föregående IT-chef hade gjort ett år tidigare var simplare till strukturen. Strukturen var mycket bred och hade mindre undermappar, den nya strukturen som Ingå kommuns ledning föreslog var mycket djupare. IT-chefens ursprungliga mappstruktur liknade mera en sorts taggningssystem, alltså det fanns mycket mappar som var mycket specifika till sin natur. En mapp som var i roten kunde vara namn på en skola, vilket är mycket specifikt för att vara en rotmapp.

Jag talade med förvaltningschef Eija Taskinen och kommundirektör Jarl Boström om nätverksmapparna och de ville göra upp mapparna på ett annat sätt än hur de var nu. D.v.s. ändra på mappstrukturen som föregående IT-chef hade gjort tidigare (Se Figur 9). De ville gå enligt uppställningen i budgeten och dela in det på det sättet istället. Jag talade också med nuvarande IT-chefen och han godkände det nya förslaget.



Figur 9 Illustration på skillnaden mellan den förra IT-chefens mappstruktur och ledningens förslag

I praktiken betydde de att indelningen av mapparna är mera snäv och djupare, det skulle finnas färre rotmappar och många undermappar. Rättighetssystemet ändras också, närmare sagt rättighetsärftligheten i mapparna. Jag måste göra upp mera ACL_ grupper för att hantera rättigheterna. ACL-grupper förklaras närmare i kapitel 4.3.3 på sida 31.

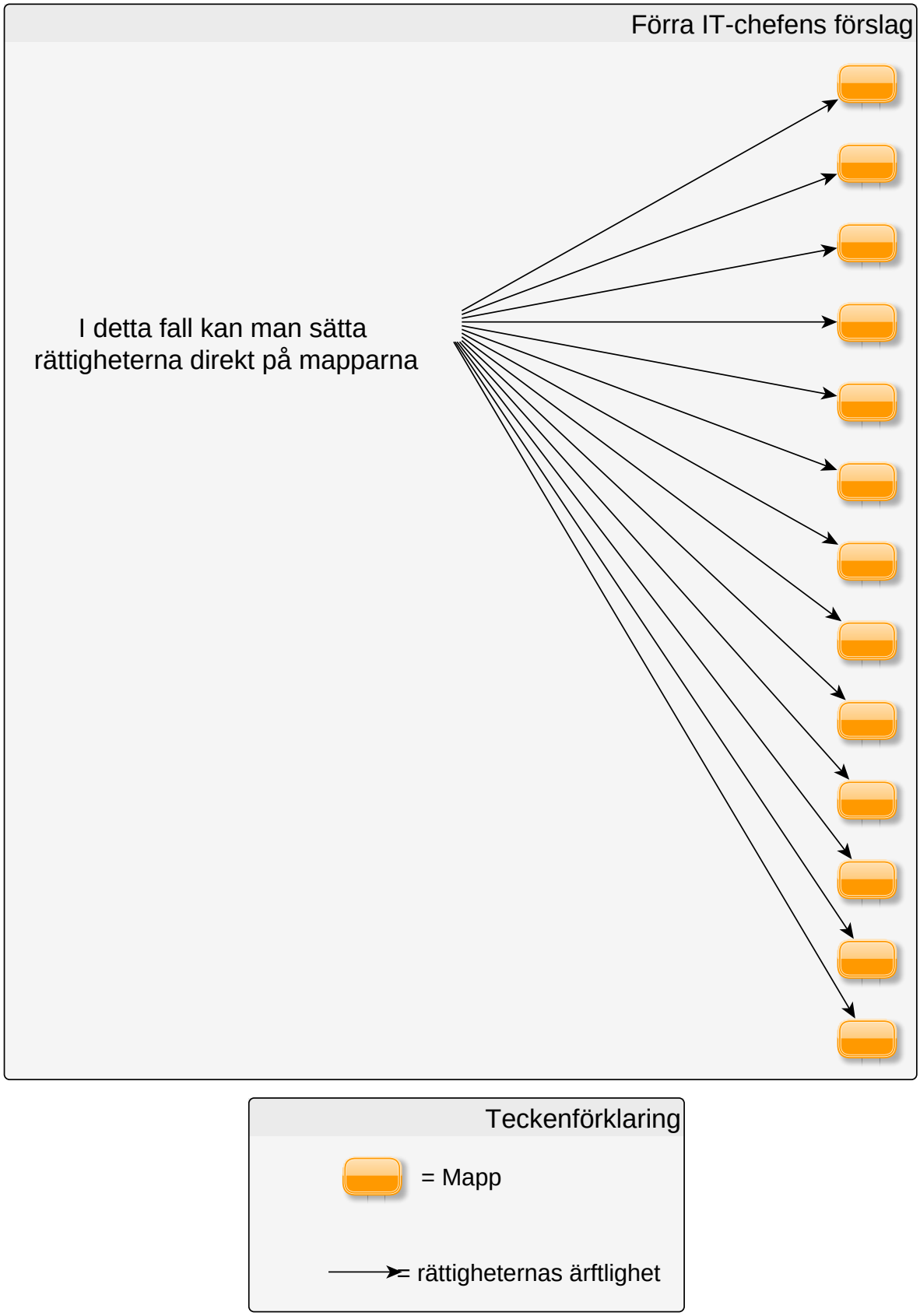
Det visade sig att uppställningen i budgeten inte räckte till. Många av avdelningscheferna ville ha undermappar under de s.k. ”huvudmapparna”. Till dessa mappar skall appliceras också olika rättigheter. D.v.s. parallella mappar skall ha olika rättigheter. Därför behöver jag göra mera ACL-grupper och att rättigheterna blir mera invecklade.

4.2.3 Mapprättigheterna

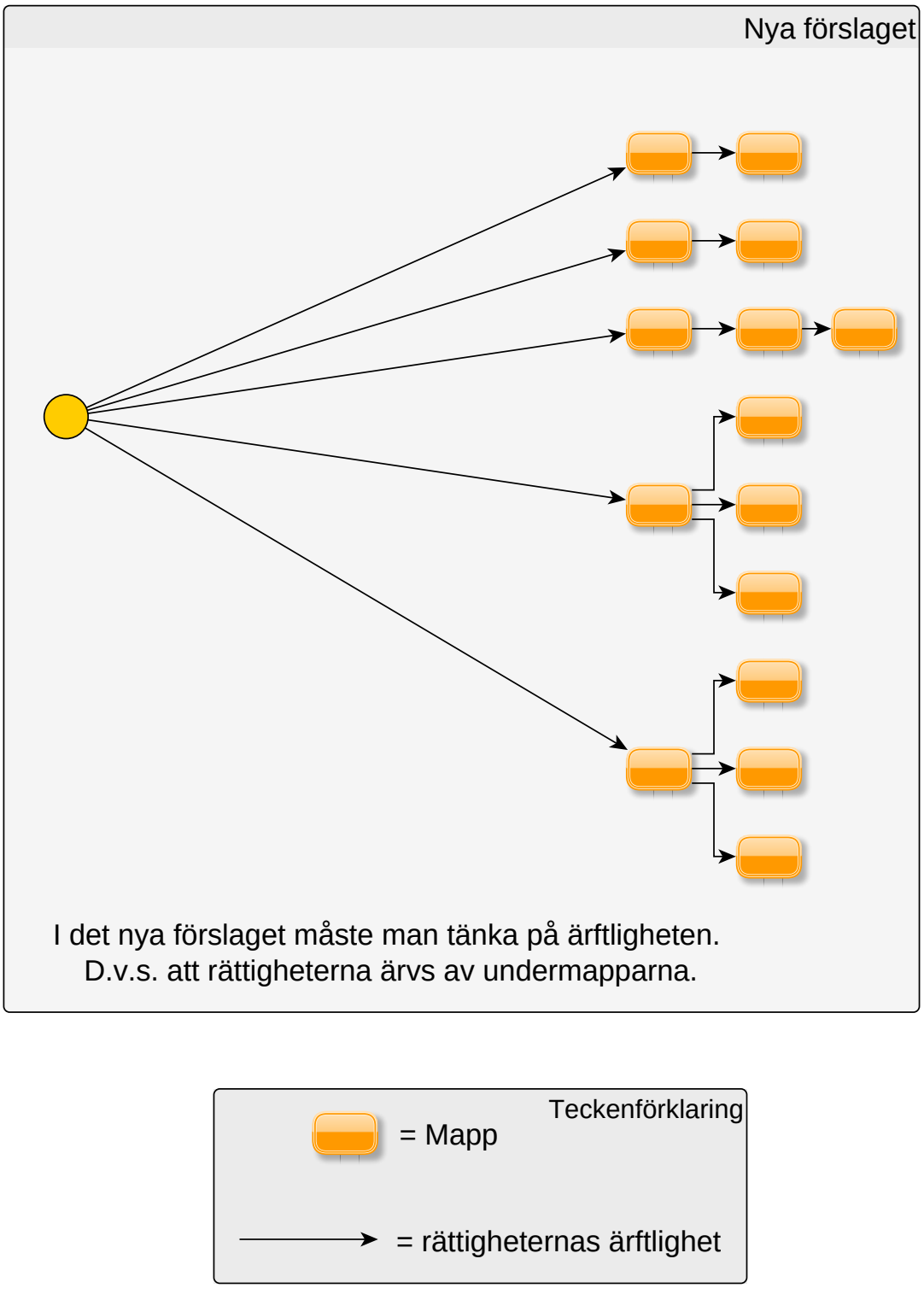
De krav som finns för mapprättigheterna fick jag ifrån intervjuer av de flesta arbetare på kommunen. Nätverksmappstrukturen gjorde IT-chefen förrän han bytte arbetsplats och jag såg inte orsak för att byta ut den, detta var på hösten/vintern 2013. Dock visste jag inte alltid till vilket ändamål mapparna gjordes för, men jag fick mera information av arbetstagarna på kommunen. De flesta mapparna var helt enkelt olika fysiska platser eller områden i kommunens verksamhet. En plats kunde vara en förskola eller en skola. Ett område kunde vara ekonomi eller tandvård.

Jag kunde inte utgå ifrån de tidigare rättigheterna för att de var åldrade och man kunde inte lita på dem. Man kan dra också den slutsatsen att mapprättigheterna förändras med åren, när arbetstagarnas uppgifter ändras. Därför är det bra att ha ett system som man kan lätt administrera, då kan man efter hand ändra på rättigheterna lätt.

Detta ändrades också på hösten 2014. Då mapparna fick en annan struktur behövdes mapprättigheterna också tänkas om. Jag fick som uppgift att fråga av de olika avdelningscheferna vilka rättigheter skulle vem få och på basis av denna information implementera den. I den tidigare strukturen var det enkelt att applicera mapprättigheter p.g.a. att man kunde applicera rättigheterna direkt på mapparna, utan att man behöver tänka på ärftligheten. Men nu när mappstrukturen har undermappar och dessa undermappar skall ha olika rättigheter applicerade måste man tänka på ärftligheten av rättigheter. D.v.s. om det finns t.ex. Mapp2 innanför Mapp1 och det finns en person som behöver komma åt Mapp2 och behöver inte ha eventuellt rättigheter till parallella mappar så då måste man begränsa ärftligheten av rättigheterna i Mapp1.



Figur 10 Förra IT-chefens mappar och hur rättigheterna skulle appliceras



Figur 11 Det nya förslaget

4.2.4 Grupperna

Vi diskuterade länge hur vi skulle göra de nya grupperna. Jag hade en idé att vi skulle göra grupper på basen av olika OU:n. Men då tyckte dåvarande IT-chefen att var lite för invecklat, det skulle ha skapat en djup OU-hierarki och skulle vara krånglig att administrera. De skulle ha betytt att varje OU skulle ha respektive ”Security group”, vilket skulle ha skapat jättemånga grupper. Så istället planerade vi att göra grupperna så som i videon, alltså grupperna har en hierarki istället för en platt struktur.

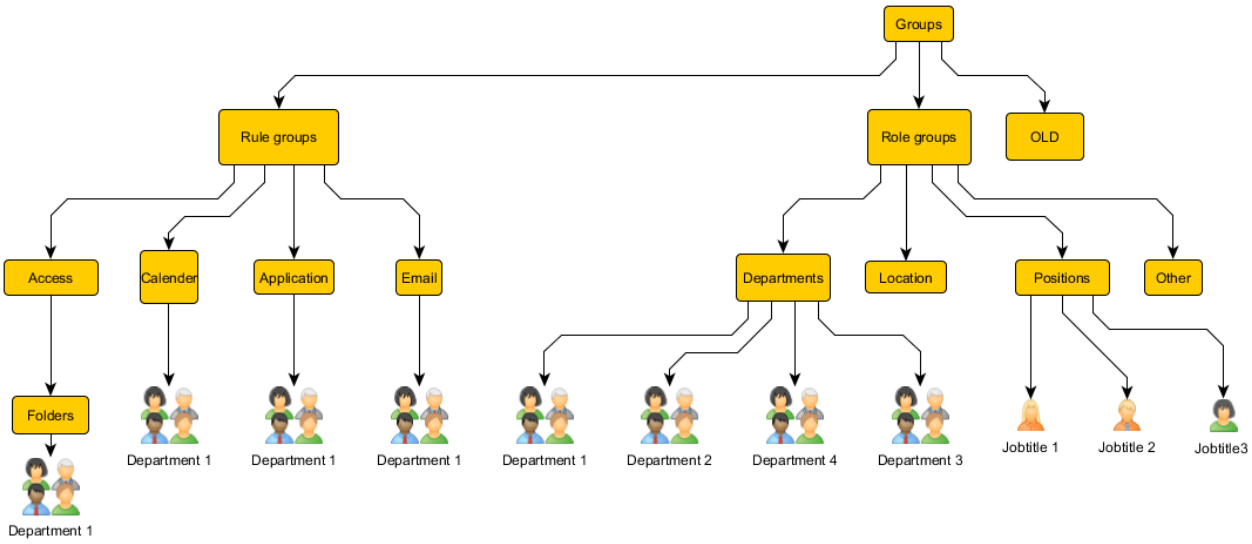
Vi diskuterade också om grupperna kunde vara skriptbaserade. Då skulle ett skript sätta användarna i rätta grupper utgående från deras attribut. Skriptet skulle gå igenom alla användare och sätta dem i rätta grupper. T.ex. ett skript skulle läsa Location-attributet och om attributet skulle vara t.ex. Kyrkjärdens skola skulle skriptet sätta denna i användare i LOC_Kyrkfjärden-gruppen. Jag talade med IT-chefen om saken och han tyckte att man inte kan lita på ett skript för en sådan sak (Samtal med Carl-Johan Backman under hösten 2013).

Grupphierarkin skulle vara likadan som organisationen har. Organisationen Ingå kommun är indelad i olika avdelningar och inne i dessa avdelningar har arbetstagarna egna titlar. Så jag tänkte att det bästa sättet är att indela Ingå kommun i avdelningar och titlar. För att alla arbetstagare i kommunen oftast har en avdelning och en titel. Det fanns dock människor som jobbade på flera avdelningar eller hade uppgifter som involverade flera avdelningar. Men dessa var dock undantag. Vad som gäller den tekniska implementeringen så hade det ingen skillnad fastän människor jobbar på olika ställen. Man kunde använda sig av titeln istället för avdelningen för att skapa unika grupper. D.v.s. för att hantera rättigheterna så gav man rättigheten till dess titel istället för avdelningen. Det fanns förmän som behövde mera rättigheter än andra och då var det mycket lätt att tilldela mera rättigheter till deras titel-grupp.

4.2.5 Ou-strukturen

I stora drag tog jag strukturen ifrån tidigare hänvisade videon. AD:n hade från tidigare en ganska bra basstruktur, jag ansåg att det inte fanns behov att ändra den. Däremot tänkte jag laga upp en ny struktur för de nya grupper som jag tänkte laga.

Först en rot OU som skiljer de nya OU:na ifrån de existerande och sedan under den två nya OU:n. Dessa skulle vara Role groups och Rule groups (Se figur 12). Role groups är rollerna och Rule group är ”rättighetsgrupperna”. Tekniskt sett sätter man in role groups innanför rule groups och på så sätt ger rättigheter till Role groups. Detta är i enlighet med RBAC, som förklarades i kapitel 3.4. Gruppärftligs-principen ifrån kapitel 3.1.11 tillämpas också i detta fall.



Figur 12 OU-strukturen för nya de nya grupperna

Man skall märka att det finns en skillnad mellan OU-hierarkin och grupp-hierarkin. OU-hierarkin är mest för att ha en klar visuell hierarki, främst för att lätt hitta det som man söker. Men själva grupphierarkin är den som används i tekniska sammanhang, t.ex. då när man ger ut mapprättigheter. Denna hierarki används då av AD för att ge rättigheter inom domänen.

4.3 Implementering

Jag utförde inte en test-fas p.g.a. tidsbrist och började direkt med implementeringen. Alla ändringar gjorde jag direkt i produktionsmiljön, detta är oftast inte önskvärt men det har sina fördelar. Systemet kommer direkt i bruk och eventuella problem upptäcks direkt och kan sedan korrigeras. Nackdelen är att allt händer i produktionsmiljö och därmed kan påverka den på ett negativt sätt. Första steget i implementeringen var att uppdatera attributen i AD:n för att hantera

objekt på ett lättare sätt; med objekt menas i detta fall användare.

4.3.1 Uppdatering av AD attribut för att underlätta gruppindelningen

För att underlätta skapande av grupper i AD:n måste jag få information om användarna och importera denna info till AD:n. Det fanns inte mycket information om användarna i AD:n, men den var ändå en bra utgångspunkt. Jag exporterade först den information som fanns i AD:n till en Excel-fil. Det gjorde jag m.h.a. ett program. (AD INFO - ACTIVE DIRECTORY REPORTING TOOL, u.å)

Programmet ”AD info free edition” gjorde en CSV-fil av informationen om användarna och denna fil importerade jag till Excel. Jag började kolla upp Excel-filen och började se efter vilken information som fattades. Den information som var mest relevant var avdelning, titel och arbetsplats. Denna information finns för alla arbetstagare och hjälper att effektivt gruppera användarna. Sedan när man visste vilken information som fanns var det lätt att se det som fattades.

Som bakgrundsinformation kan jag tillägga att i alla kommuner finns det mest personal inom bildning och grundtrygghet. P.g.a. att Ingå hade haft samarbete med Lojo gällande hälsovården hade inte hälsovårdspersonalen använt Ingå kommuns it-resurser. Detta ledde till att det fanns lite information i AD:n angående hälsovårdspersonalen. Men jag fick ganska snabbt informationen av förmän inom hälsovården. Det fattades också information angående personalen inom bildningen men den informationen fick jag också ganska snabbt.

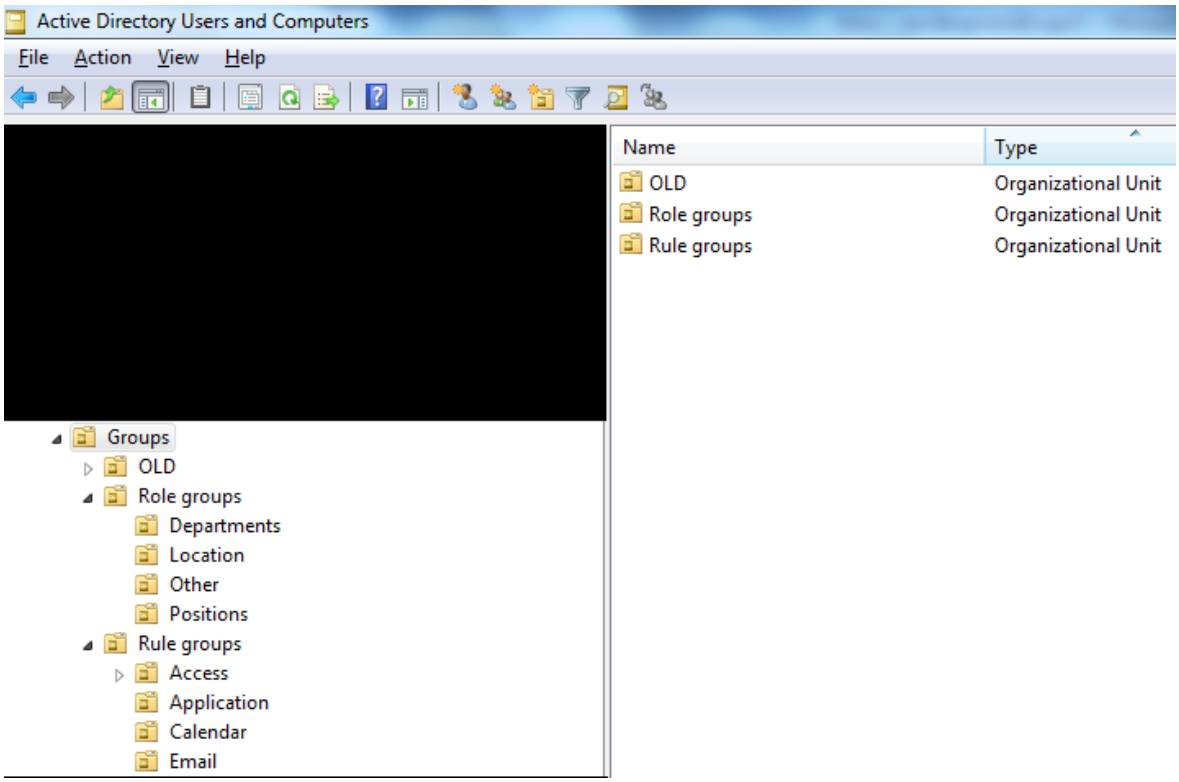
Jag började sammanställa all information. Jag fick nästan en fullständig bild av alla användare i kommunen. En del av information fick jag ifrån Ingås webbsidor. Jag gjorde en Excel-fil med alla användare och deras information. Sedan började jag göra en fil som jag skulle använda för att uppdatera flera användar-attribut i AD:n. Det fanns inte färdiga program för att uppdatera attribut för flera användare på en gång, d.v.s. jag måste söka ett. Ifrån lite sökning på nätet hittade jag AD Bulk Admin Tool (AD Bulk Admin Tool, u.å). M.h.a. verktyget uppdaterade jag flera attribut på användarna på en gång. Första gången som jag gjorde detta lyckades det inte så bra. Alla e-postattribut blev något helt annat som det skulle vara, men

det upptäcktes snabbt och korrigerades också relativt snabbt.

När infon sedan var inne i AD:n kan man gruppera människorna på ett lätt sätt. Jag fundera också på att sätta in användarnas telefonnumror, men gjorde det inte sedan p.g.a. tidsbrist. När infon är inne i AD:n kan man använda sig av ”Active Directory Users and Computers” (ADUC) för att skapa grupper. Man kan göra så att man filtrerar användare på basen av ett attribut. T.ex. för att göra en grupp på ekonomiavdelningen filtrerar man på Department-attributet och väljer sedan dessa användare och sätter in dem i en grupp.

4.3.2 OU strukturen för de nya grupperna

”OU:na” gjorde jag så att jag först gjorde en s.k. rotmapp för att urskilja de nya ”OU:na” ifrån de övriga. Detta leder också till tydlighet och därmed lättare administration. Den fick heta helt enkelt Groups. Inne i den gjorde jag en OU som hette OLD, där satt jag alla gamla grupper. Under Groups OU:n gjorde jag två huvud OU:n, Rule groups och Role groups. Innanför dessa hade jag sedan ytterligare indelning, nedan en bild som visar OU-strukturen.



Figur 13 OU-strukturen implementerad

4.3.3 Grupperna och deras namngivning

För att kunna lätt identifiera grupperna måste man hitta på namngivningsregler. Namngivningsreglerna definierar att om en grupp tillhör en viss kategori får den ett visst prefix. T.ex. om vi har en avdelning som heter IT, skulle detta betyda att gruppen till avdelningen skall heta DEP_IT. Vi har då definierat att alla avdelningsgrupper har ett prefix på DEP_. Följande tabell anger vilka prefix jag använde för att namnge grupperna.

Tabell 3 Prefix för "Role groups" i AD:n

Avdelning	DEP_
Titel	Inget prefix (Dessa hade en egen OU och är lätt att hitta om det behövs)
Program	APP_
Kalender	CAL_
Plats	LOC_
Epost	EMAIL_

Jag måste också definiera regler för de s.k. "Rule groups". Eftersom jag koncentrerar mig på mapprättigheter i detta examensarbete, gjorde jag en egen namngivningsregel för dessa. Denna regel lyder i kort såhär, ACL_*Resurs*_*Rättighet*. T.ex. om det fanns en mapp som hette Ekonomi och gruppen fick läs-rättigheter, då skulle gruppen heta: ACL_Ekonomi_READ.

Fördelen med namngivningsregler är det att man kan söka bara på viss sorts grupper. Om man t.ex. vill hitta bara ACL grupper är detta lätt att söka p.g.a. att alla dessa grupper börjar på ACL. Likaså fungerar det med de övriga grupperna.

Efter att jag hade gjort upp dessa regler var det bara att göra upp alla grupper. Jag gjorde först Role groups och sedan Rule groups. Det betyder att jag skapa en Rule group för alla de nya mappar som skulle komma i bruk. Det var ungefär 20 till

antalet och sedan skulle man sätta in Role groups i dem.

Först gick jag igenom alla mappar och satt in Rule groups i dem och gav grupperna respektive rättigheter. T.ex. Jag gav ACL_Ekonomi_READ läsrättigheter till Ekonomi-mappen och osv. Det var ganska mycket mappar så det tog sin tid.

Eftersom mappstrukturen ändrades hösten 2014 var jag tvungen att göra upp nya Rule groups. D.v.s. de grupper som används i tekniska sammanhang för att till dela rättigheter. Jag måste ta bort alla gamla ACL-grupper och göra nya för de nya mapparna.

4.3.4 Ändringar i implementeringen

Jag började på mitt examensarbete under september-december 2013, men fick inte allting gjort under denna tid. Det fattades själva implementeringen av det planerade och som tidigare nämnt började jag på hösten 2014 att göra den sista delen av examensarbetet. Då fanns det dubbla nätverksmappar för att de nya inte var tagna i bruk helt och hållet. De nya fanns där och hade mapprättigheterna applicerade till dem, men de var inte tagna i bruk. En orsak var att jag inte hann göra allt tidigare och en annan orsak var att hälsovården ännu inte hade börjat använda sig av Ingå kommuns IT-resurser. Så jag började på nytt under hösten 2014.

Så uppgiften var nu att flytta över gamla data till de nya mapparna. Vi kom också överens om en stegvis plan hur vi skall ta i bruk mapparna. Först skulle vi göra upp mapparna, sedan göra upp mapprättigheterna och sedan kopiera över allt material. Steg 1 är enkelt, göra upp mapparna och få dem godkända med Ingå kommuns ledning för att sedan fara till steg 2.

Eftersom de finns två olika mappstrukturer på Ingå kommun, de gamla och de ”nyare” eller de som föregående IT-chef hade gjort. Beslöt jag namnge de nyare mapparna. Jag namngav dem så att varje mapp hade ett _-tecken i början. Detta gjorde jag för att urskilja de nya mapparna ifrån de gamla, men de gamla kunde

ännu användas i detta skede.

Sedan skickade jag en förfrågan till alla avdelningschefer angående mapprättigheterna. Mapparna var de mappar som går enligt uppställningen i budgeten. M.a.o. den struktur som Ingå kommuns ledning hade godkänt hösten 2014. Förfrågan var en Excel-fil med en matris på mapprättigheterna (Se tabell 4).

Tabell 4 Exempel hur Excel-filen såg när jag gjorde förfrågan på mapprättigheterna. Man skall skriva i rutorna de personer som skulle få respektive rättigheter.

Bildningsnämnd	LÄSRÄTTIGHETER	SKRIVRÄTTIGHETER	FULLA RÄTTIGHETER
Barndagvård			
Bildningsnämndens förvaltning			
Kommunens skolväsende			
Kultur- och fritidsservice			
Övrig utbildningsverksamhet			

Exemplet ovan är för bildningens del, jag gjorde detta för alla avdelningar. Men de två största var grundtryggheten och bildningen. Min tanke var att göra den så enkel som möjligt. Då kunde man inte missförstå den på något sätt. Jag fick feedback till förfrågan. Vissa avdelningschefer önskade att de kunde specificera mapprättigheterna noggrannare. De ville specificera mapprättigheterna till undermappar till den struktur som jag hade tänkt mig. I detta skede är projektarbetet nu.

4.4 Resultat

Resultatet av arbetet blev en plan för rollbaserat system för att hantera mapprättigheter. Resultatet blev en plan för att det förekom ändringar i sista skedet och jag hann inte implementera allt. Ändringar blev i mappstrukturen och det kommer eventuellt ännu ytterligare ändringar.

Men jag vet hur jag skall hantera mapprättigheterna oberoende hur mappstrukturen blir. Projektet blev inte helt färdigt, men jag kommer att göra det till slut utanför detta examensarbete. Själva implementeringen är inte helt och hållet med i detta examensarbete, jag hann lite börja med implementeringen.

Det som är med i detta examensarbete är ett sätt att hantera mapprättigheter. En plan hur du kan m.h.a. AD-grupper hantera ett rollbaserat mapprättighetssystem. Detta system kan tillämpas på alla miljöer som använder sig av AD och har ett Windows-baserat filsystem.

5 Avslutning

5.1 Reflektion över arbetet med projektet

Detta examensarbete handlar om nätverksmappar och ett visst sätt att hantera mapprättigheter. Jag fick idén av tidigare nämnda videon och tänkte att rollbaserad administration är mycket lättare än vanlig rättighetsadministration. För att man inte baserade rättigheterna på en viss person eller användare, utan man utgick ifrån att denna person har en viss roll i en organisation. Detta betyder att man måste skapa så unika roller som möjligt. Detta betyder att i ett rollbaserat system måste alla användare vara unika. T.ex. det kan finnas två läkare i en hälsovårdsstation, men de kan ha unika arbetsuppgifter. Detta betyder att rollen läkare inte är tillräckligt noga för någondera läkaren. En av läkarna kan ha ett specialområde som de är experter på och andra läkaren kan vara expert på ett annat område. Då måste ytterligare två roller skapas bara för dessa två läkare. Systemet blir mera komplicerat desto mera roller det finns. Dessutom att rollerna blir mera gör att rollhierarkin blir mera invecklad, vilket i sig är en dålig sak. Så ett rollbaserat system kan bli komplex ganska snabbt om man inte beaktar

organisationens komplexitet. Detta är inte en brist, det är mera en sak som man måste tänka på när man implementerar rollbaserade rättighetssystem.

Med tanke på nätverksmappar och deras uppgift skulle man kunna tänka på ett annat system. Nätverksmappar börjar vara föråldrade, det börjar finnas mera avancerade system för att administrera innehåll, t.ex. dokumenthanteringssystem eller innehållshanteringssystem. Jag började bygga upp Ingå kommunens intranät strax efter att jag hade börjat på mitt examensarbete och detta intranät baserade på Sharepoint. Sharepoint är en plattform för intranät, innehållshantering eller dokumenthantering (SharePoint 2010 Is Poised for Broader Enterprise Adoption, 2009). Sharepoint skulle passa in som ett ställe där man kunde sätta in alla dokument. Den är webbaserad så det skulle vara lätt att använda sig av på olika operativsystem och plattformar. D.v.s. dokument skulle kunna vara tillgängliga ute på fältet. Jag blev introducerad till Sharepoint först då jag började skapa ett intranät. Jag skulle ha kunnat föreslå Sharepoint istället för nätverksmappar. Men jag var sent ute, för att jag redan hade börja göra upp mappsystemet då och jag visste inte Sharepoint:ens potential ännu. Dock vet jag inte om man skulle ha kunnat bygga upp ett rollbaserat rättighetssystem i Sharepoint, det skulle kunna vara ett intressant projekt. Så med tanke på framtiden tror jag att nätverksmappar börjar vara föråldrade. Det finns så mycket avancerade funktioner i Sharepoint, som skulle kunna göra arbetsdagen smidigare för många, men det är ett helt annat projekt.

5.2 Personlig utveckling och lärdomar ifrån examensarbetsprocessen

Jag började på hösten 2013 att göra på mitt examensarbete och jag började det med bråttom. Jag hade inte någonting planerat för hösten och jag hade bråttom att skaffa sysselsättning. Jag hade på sommaren 2013 gjort en praktik för Crossdesigns och tänkte att jag skulle fråga om de hade ett projekt till mig och de hade det. Först tänkte jag att det verkade intressant, men efter en tid tappade jag lusten till ämnet. Det är otroligt svårt att göra ett examensarbete som man inte är så intresserad av egentligen. Jag borde ha bytt ämnet direkt när jag märkte att detta inte är någonting för mig. Jag tänkte att jag gör det snabbt undan; så att jag får det gjort. Men som det är med många saker med livet, målet är inte det

viktigaste utan hur man kommer till det. Så det är min viktigaste lärdom av examensarbetsprocessen. Ta ett examensarbete som du är jätteintresserad av, lyssna inte alltid vad alla andra säger, utan lär dig att lyssna på dig själv i viktiga beslut.

En annan sak som jag tänker ta lärdom av är att göra upp klara mål. Jag hade inte alltid klart för mig att vad jag skulle göra. Det är jobbigt att du har en sak som du måste göra, men du vet inte alls hur du skall göra den. Jag är en sådan person som tycker om klara regler och strukturer i arbetet. Jag behöver någonting som styr mig, annars vet jag inte vad jag skall göra. Jag är inte ännu helt redo för självständigt arbete, jag behöver en förman som styr mig i vad jag skall göra. Sommararbetet lärde mig delvis att jobba självständigt, jag fick ganska fritt välja vad som jag skulle göra, detta motivera mig också i arbetet. Men att jobba självständigt är ett område jag skall jobba på i framtiden.

Källförteckning

Achieving Autonomy and Isolation with Forests, Domains, and Organizational Units (u.å.). [Online] http://technet.microsoft.com/en-us/library/bb727032.aspx [hämtat: 18.1.2014]

Active Directory Collection (u.å.). [Online] http://technet.microsoft.com/en-us/library/cc780036(WS.10).aspx#w2k3tr_ad_over_qbjd [hämtat: 27.12.2013]

Active Directory Objects (u.å.). [Online] http://technet.microsoft.com/en-us/library/cc977990.aspx [hämtat: 18.1.2014]

Active Directory Users and Computers (u.å). [Online] http://technet.microsoft.com/en-us/library/cc754217.aspx [hämtad 13.11.2014]

Active Directory Users, Computers, and Groups (u.å.). [Online] http://technet.microsoft.com/en-us/library/bb727067.aspx [hämtat: 18.1.2014]

Active Directory, 1999. [Online] http://technet.microsoft.com/en-us/library/bb742424.aspx [hämtat 23.10.2013]

AD Bulk Admin Tool (u.å.). [Online] http://sourceforge.net/projects/adbulkadmin/ [hämtat 11.1.2014]

AD INFO - ACTIVE DIRECTORY REPORTING TOOL (u.å). [Online] http://www.cjwdev.co.uk/Software/ADReportingTool/Info.html [hämtat 11.1.2013]

American National Standard for Information Technology, 2004. *Role Based Access Control*. New York: ANSI

Delegating administration (u.å.). [Online] http://technet.microsoft.com/en-us/library/cc778807%28v=ws.10%29.aspx [hämtat 24.10.2013]

Document Your Domain Groups, 2009. [Online] http://windowsitpro.com/scripting/document-your-domain-groups [hämtat 23.10.2013]

Draw Nested AD Security Groups by MemberOf or Member Attributes, (u.å.). [Online] http://gallery.technet.microsoft.com/scriptcenter/Graph-Nested-AD-Security-eaa01644#conte [hämtat 11.1.2014]

File and Folder Permissions (u.å.). [Online] http://technet.microsoft.com/en-us/library/bb727008.aspx [hämtat 16.10.2014]

Get-GPOReport, Windows Server (u.å.). [Online] http://technet.microsoft.com/en-us/library/ee461057.aspx [hämtat 30.12.2013]

Group Policy (u.å.). [Online] http://technet.microsoft.com/fi-fi/windowsserver/bb310732.aspx [hämtat 7.11.2013]

Group scope (u.å.). [Online] http://technet.microsoft.com/en-us/library/cc755692(v=ws.10).aspx [hämtat 2.12.2013]

Groups (u.å.). [Online] http://technet.microsoft.com/sv-se/library/cc739393%28v=ws.10%29.aspx [hämtad 26.10.2013]

Kivimäki, Jyrki, 2009. *Windows server 2008 r2 – tehokas hallinta*. Helsinki: Readme.fi

Kort om Ingå, 2012. [Online] http://www.inga.fi/hemsida/information/sv_FI/info/ [hämtat 10.10.2013]

List Security of Folder and Subfolder, export information to CSV File (u.å.). [Online] http://gallery.technet.microsoft.com/scriptcenter/List-Security-of-Folder-8f0487a9#content [hämtat 23.10.2014]

Organizational units (u.å.). [Online] http://technet.microsoft.com/sv-se/library/cc758565(v=ws.10).aspx [hämtat 10.10.2013]

***Role-Based Management Extreme Makeover for Active Directory*, 2011. [Online] http://technet.microsoft.com/en-us/video/hh134690.aspx (hämtat 17.10.2014)**

Sandhu, Ravi S., 1998. *Role based Access Control in Advances in Computers VOL 46*. London: Academic Press

Security filtering using GPMC (u.å.). [Online] http://technet.microsoft.com/en-us/library/cc781988(v=ws.10).aspx [hämtat 7.11.2013]

Security information for Active Directory (u.å.). [Online] http://technet.microsoft.com/en-us/library/cc779033(v=ws.10).aspx [hämtat 2.9.2014]

SharePoint 2010 Is Poised for Broader Enterprise Adoption, 2009, Gartner [Online] https://www.gartner.com/doc/1209350 [hämtat 29.10.2014]

Terms and Definitions (u.å.). [Online] http://technet.microsoft.com/en-us/library/cc773224(v=ws.10).aspx **[hämtat 18.1.2014]**

Trust transitivity (u.å.). [Online] http://technet.microsoft.com/en-us/library/cc739693(v=ws.10).aspx **[hämtad 18.1.2014]**

Understanding Group Accounts (u.å.). [Online] http://technet.microsoft.com/en-us/library/cc733001.aspx **[hämtat 30.10.2013]**

Understanding the Active Directory Logical Model (u.å.). [Online] http://technet.microsoft.com/en-us/library/cc770319%28v=ws.10%29.aspx **[hämtat 17.9.2014]**

What Are Domains and Forests? (u.å.). [Online] http://technet.microsoft.com/en-us/library/cc759073(v=ws.10).aspx#w2k3tr_logic_what_yokf **[hämtat 3.9.2014]**

What Are Permissions? (u.å.). [Online] http://technet.microsoft.com/en-us/library/cc771375.aspx **[hämtat 31.12.2013]**

Windows PowerShell (u.å.). [Online] http://technet.microsoft.com/sv-se/library/cc731851(v=ws.10).aspx **[hämtat 12.1.2014]**

WMI filtering using GPMC (u.å.). [Online] http://technet.microsoft.com/en-us/library/cc779036(v=ws.10).aspx **[hämtat 7.11.2013]**