Installation och underhåll av servrar i Aktias bankkontor

Leon Laude

Examensarbete

Informations- och medieteknik

2013

EXAMENSARBETE	
Arcada	
Utbildningsprogram:	Informations- och medieteknik
Identifikationsnummer:	4167
Författare:	Leon Laude
Arbetets namn:	Installation och underhåll av servrar i Aktias bankkontor
Handledare (Arcada):	Göran Pulkkis
Uppdragsgivare:	Aktia Abp

Sammandrag:

I detta examensarbete undersöks på vilket sätt man kan utarbeta ett effektivt och lätt system för installation och underhåll av bankkontorservrar på Aktia Bank, som påbörjar ett projekt för att förenkla sina nuvarande två olika IT-infrastrukturer till en gemensam. Eftersom serverantalet är stort bör installationerna automatiseras så långt som möjligt.
Programvaran System Center 2012 Configuration Manager (SCCM) används för att automatisera installation och underhåll av bankkontorservrarna.
Examensarbetet består av en teoretisk och en praktisk del. I teoridelen beskrivs hur man kan automatisera installation och konfiguration med hjälp av SCCM. Därefter presenteras serveroperativsystemet Windows Server 2008 R2, som kommer att användas för bankkontorsservrarna; och installationsprocessen. Den praktiska delen beskriver hur själva installationsprocessen gick till, hur servrarna testades efteråt och hur underhållet gjordes. Resultatet av testningen gällande installationsautomatiseringen med SCCM på en server-prototyp visade att installationerna kunde automatiseras rätt långt, förutom enstaka processer som måste göras manuellt. Beträffande underhållet kunde säkerhetskopieringarna helt automatiseras medan uppdateringarna måste hanteras manuellt p.g.a. Aktias datasäkerhetspolicy.

Nyckelord:	Aktia Bank, System Center 2012 Configuration Manager, Windows Server 2008 R2, Installering, Underhåll, Automatisering,
Sidantal:	50
Språk:	Svenska
Datum för godkännande:	17.6.2013

DEGREE THESIS	
Arcada	
Degree Programme:	Information and Media Technology
Identification number:	4167
Author:	Leon Laude
Title:	Installation and maintenance of Aktia bank's office servers
Supervisor (Arcada):	Göran Pulkkis
Commissioned by:	Aktia Plc

Abstract:

This thesis is examining in which way an efficient and easy system of installation and maintenance of servers in Aktia Bank could be developed. The bank will start a project to simplify their two IT Infrastructures into one united.
As there is a considerable amount of servers that need to be installed, there is a need to automate the installations as much as possible
The software System Center 2012 Configuration Manager (SCCM) is used to automatize the installations and the maintenance of the servers in the banks.
This thesis work is divided into a theoretical part and a practical part. The theoretical part describes how the installation and configuration using SCCM is automatized. The practical part describes the installation process itself, the procedure of testing the servers, and how the maintenance was organized.
The result of the testing on a prototype server showed that with SCCM the installations were possible to automatize to a great extent, except some processes which need to be done manually. Regarding the maintenance of the backup, automatization was possible to a full extent, while the updating needed to be done manually because of the security-policy of Aktia Bank.

Keywords:	Aktia Bank, System Center 2012 Configuration Manager, Windows Server 2008 R2, Installation, Maintenance, Automatization
Number of pages:	50
Language:	Swedish
Date of acceptance:	17.6.2013

INNEHÅLL

Figurer

Tabeller

Förkortningar

QS	Quick Step
ICT	Information and Communications Technology
SCCM	System Center Configuration Manager
SQL	Structured Query Language
CAS	Central Administration Site
MP	Management Point
SUP	Software Update Point
WSUS	Windows Server Update Services
DP	Distribution Point
GUI	Graphical User Interface
RAM	Random Access Memory
PXE	Pre-Boot Execution Environment
DHCP	Dynamic Host Configuration Protocol
VPN	Virtual Private Network
SSH	Secure Shell
LAN	Local Area Network
TPM	Trusted Platform Module
BIOS	Basic Input/Output System

FÖRORD

Jag vill först och främst tacka Aktia Abp för att jag fått en möjlighet att vara med i detta projekt och ytterligen för att ha fått göra detta som mitt avhandlingsarbete. Jag vill tacka Johan Wiik som varit min experthandledare på Aktia, det är tack vare honom som jag har lärt mig mycket och bra kommit igång med arbetet.

Jag vill uttrycka min tacksamhet till min handledare från min skola Arcada, Dr. Tech Göran Pulkkis för alla råd och hjälp jag fått gällande skrivprocessen för mitt avhandlingsarbete.

Detta examensarbete har gett mig mycket värdefull erfarenhet om vad ett större projekt i arbetslivet innebär. Detta var mitt sista steg under min högskoletid här på Arcada och jag ser fram emot alla nya utmaningar som väntar mig ute i arbetslivet.

Helsingfors, den 17 juni 2013

_____

Leon Laude

1 INLEDNING

Aktia Bank använder i dagens läge två olika programmiljöer, en egen miljö endast för bankkontoren runtom i landet och en annan programmiljö på huvudkontoret. Dessutom använder Aktia två olika separata nät inom ett gemensamt nätverk med två olika infrastrukturer motsvarande programmiljöerna, ett för bankkontoren och ett för huvudkontoret. Detta medför flera nackdelar och gör hela infrastrukturen onödigt komplicerad. Ett projekt har startats för att ändra infrastrukturen genom att ta i bruk Aktias nuvarande egna arbetsstationsinfrastruktur även i bankkontoren. För tillfället sköter flera olika tredje parter driften av den nuvarande kontorssystemsmiljön Quick Step (QS). Detta anses inte längre vara ändamålsenligt av följande orsaker:

- Svårigheter för affärsverksamheten att förstå de begränsningar konceptet medför vilket leder till osäkerhet gällande vad som är möjligt
- Felsökningen är mycket svår då ingen part har kontrollmöjlighet i hela infrakedjan
- Utvecklingsprojekt fördröjs och förlängs
- Driften har lagts ut till flera olika tredje parter vilket i sin tur gör situationen ännu mera komplicerad
- Svårt för leverantörer att tillämpa lösningar i en så komplicerad miljö
- Kostnadsmässigt är den nuvarande miljön inte effektiv
- Datasäkerhetsproblem uppstår då man splittrar ansvaret mellan de olika parternas nät samt skapar brandmursöppningar mellan de olika näten.

Av ovannämnda orsaker har man på Aktia gjort ett beslut att omvandla sina nuvarande infrastrukturer till endast en gemensam infrastruktur.

Projektet kommer till största delen att handla om automatisering av installation och underhåll av bankkontorsservrar med installationshanteringsverktyget SCCM.

1.1 Målsättning och metoder

Målet med detta examensarbete är att använda programvaran SCCM för att så långt som möjligt automatisera installation och underhåll av Aktias bankkontorsservrar. Eftersom Aktia har cirka 70 olika kontor i landet bör det finnas lika många fysiska servrar som det finns kontor. En manuell installationsprocess skulle kräva mycket tid och därför bör en automatiserad lösning utvecklas. Installationsprocessen och ibruktagande av de nya bankkontorsservrarna får inte heller vara för tidskrävande. En server-prototyp kommer att användas för testning av installation och underhåll.

1.2 Avgränsningar

Både installation och underhåll av servrar kommer endast att gälla bankkontoren, d.v.s. det kommer inte att gälla huvudkontoret. Arbetet kommer inte heller att gå in på hur en server används.

1.3 Frågeställningar

Med arbetet strävar man att svara på följande frågor:
På vilket sätt kan man utarbeta ett effektivt och lätt system för installation och underhåll av en större mängd Windows-servrar? Kan SCCM användas för att automatisera hela processen?

2 SYSTEM CENTER 2012 CONFIGURATION MANAGER

System Center 2012 Configuration Manager (SCCM), skapat av Microsoft, är ett hanteringsverktyg för att möjliggöra automatisering av installationer. SCCM:s uppgift är att förenkla hanteringen av underhåll och installationer av mjukvara. Den senaste versionen av SCCM lanserades i april år 2012 och tog över den tidigare versionen av SCCM (System Center Configuration Manager 2007) som lanserades år 2007 (Server & Cloud Blog, 2012).

Med hjälp av SCCM kan underhåll av mjukvara samt installation av olika program och uppdateringar skötas. Installationshanteringsverktyget SCCM är inriktat på medelstora och större organisationer för att underlätta underhåll och installationsarbete för IT-personalen. I Aktia-banken finns det närmare 1400 datoranvändare. Aktia anses därför vara en medelstor organisation där SCCM kan utnyttjas. SCCM används på Aktia mest för att installera nya bordsdatorer, bärbara datorer, programvara och uppdateringar.

2.1 Arkitektur

SCCM-arkitekturen kan variera beroende på organisationens storlek. SCCM är avsett för större företag där hantering av en större mängd av datorer är svår. Detta betyder att mindre företag inte nödvändigtvis har behov av SCCM eftersom det på mindre företag finns färre datorer att hantera och underhålla. IT-administratörer på mindre företag är oftast kapabla att sköta underhåll, uppdateringar och installationer manuellt då det är fråga om få datorer. Det är också viktigt att påpeka att själva SCCM-mjukvaran och licensieringen kan bli ganska dyr. Detta är också en orsak till att SCCM inte lämpar sig för mindre företag med liten budget.

2.1.1 Site-hierarki

En *Site* omfattar en server, klienter, system-roller och resurser. För att en *Site* skall fungera krävs det att en ”SQL Server”-databas finns tillgänglig (SCCM Basics & FAQ, 2010). Organisationer som använder en eller flera *Site*:s har en så kallad site-hierarki.

En site-hierarki kan uppdelas i tre olika nivåer. I den första nivån i hierarkin finns en *Central Administration Site* (CAS), vilken är den så kallade roten i arkitekturen. Dess uppgift är att hantera alla andra *Site*:s och kommunikationen mellan dem. En CAS måste finnas om man tänker använda flera primära *Site*:s (eng. Primary Site). En *Site* är nyckelrollen i SCCM:n. Mindre företag som använder endast en primär *Site* klarar sig utan CAS. På den följande nivån krävs det att man har minst en primär *Site*. Till den kan klienter sedan ansluta sig för att kunna bli administrerade via SCCM-programkonsolen.

En viktig sak att komma ihåg är att noggrant tänka efter hur många primära *Site*:s man behöver för organisationen, eftersom det inte är möjligt att senare lägga till dem till en CAS. En primär *Site* kan hantera upp till 100 000 klienter, vilket i Finland är mycket och därför kan man tänka sig att de flesta organisationer i Finland som använder sig av SSCM har endast en primär *Site*. Det finns också en annan typ av site, en sekundär *Site* (eng. *Secondary Site)* som egentligen fungerar under den primära *Site*:n som den är kopplad till. Om sekundära *Site*:s används kommer de att finnas på den tredje nivån i hierarkin. De kan endast administreras från den primära *Site*:n som de är kopplade till. Det är inte möjligt för klienter att ansluta sig direkt till en sekundär *Site*. (Meyler et al., 2012 s. 43-46).

2.1.2 Site-roller

En primär/sekundär *Site* kan också ha olika roller. Om man använder en server eller en helt vanlig dator som värddator för att utföra dessa roller, kallas värddatorn för en *Site System Server*. En del av dessa roller som finns krävs för att driva Site System Servern. De roller som Aktia använder i sitt SCCM-system är följande:

- **Site Database Server**
  Detta är en databasserver som har Microsoft SQL Server installerat. Servern används som värddator för SCCM:s site-databas
- **SQL Server Reporting Services (SSRS)**
  SSRS är en del av SQL-Server och är en valfri roll. Rollen måste dock finnas ifall en site-databas server används. SSRS ger möjligheten att skapa, distribuera och hantera rapporter.

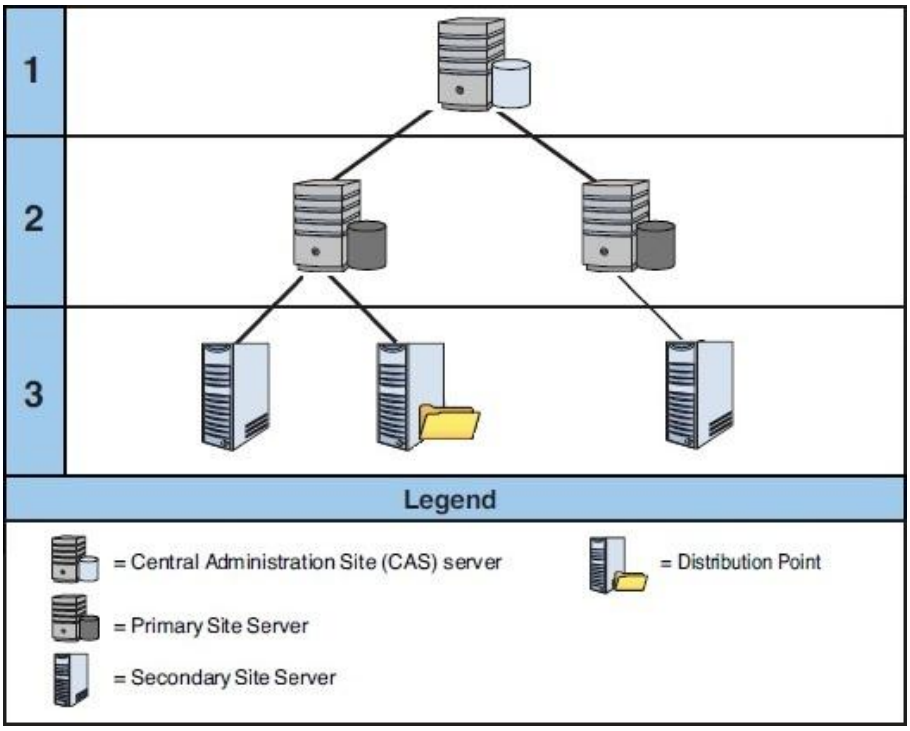
- **Management Point (MP)**

  För att kunna skapa policyn för klienter samt för att ta emot statusmeddelanden, inventering och annan data från klienterna krävs det att man har en MP
- **Fallback Status Point (FSP)**

  Om SCCM-klienterna inte kommer åt att kommunicera med MP:n, är FSP:n en alternativ väg för klienterna att skicka statusmeddelanden
- **Software Update Point (SUP)**

  SUP är en roll som ger möjlighet för SCCM-klienter att hantera uppdateringar genom Windows Server Update Services (WSUS)

För att kunna distribuera mjukvara krävs det att man har en s.k. Distribution Point (DP). DP:n finns på samma nivå som en sekundär *Site*. DP:ns uppgift är att göra mjukvaran tillgänglig för klienter och för andra datorer. I Fig.1. ser man hur en site-hierarki kan se ut i verkligheten.



Figur 1. Ett exempel på hur en Site-hierarki kan se ut

Vid planeringsskedet av SCCM-hierarkin bör man ta i beaktande hur det egna organisationsnätverket ser ut och hurdana krav organisationen har. När kraven är upp-

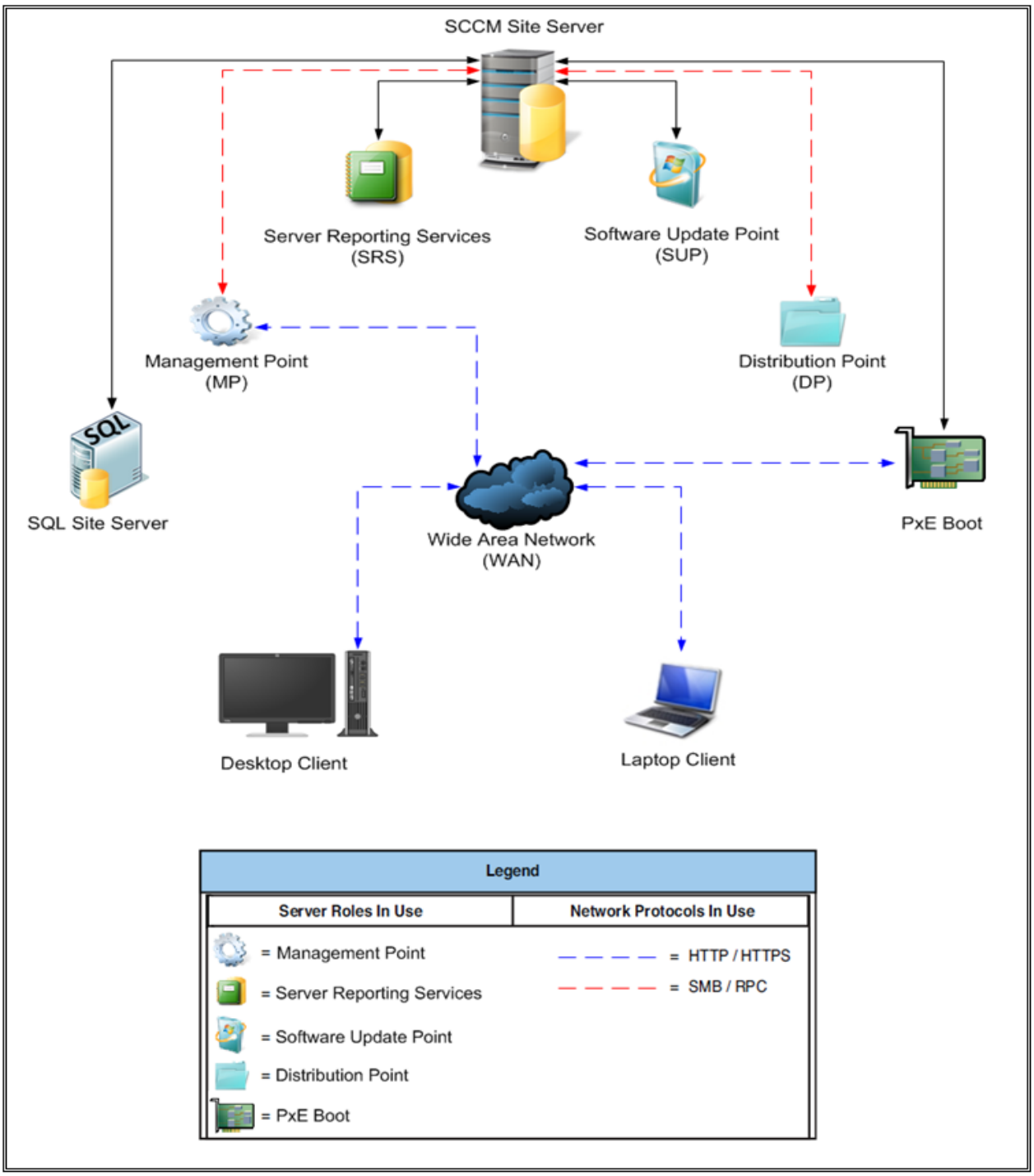
fyllda och nätverksstrukturen är gjord kan man fortsätta till nästa planeringsskede, som gäller implementeringen av SCCM. Vid implementeringsskedet tar man i bruk så lite hårdvara och mjukvara som möjligt men ändå tillräckligt för att uppfylla organisationens mål.

Site-hierarkin bör vara välplanerad för att SCCM skall fungera optimalt. För att framgångsrikt planera site-hierarkins olika egenskaper och delar gäller det att gå igenom de olika alternativen som finns och ta reda på vad man behöver till sin site-hierarki. Tabell 1 kan vara till god hjälp vid planering av en site-hierarki (Microsoft System Center, 2012).

Tabell 1. Kraven på en SCCM-hierarki (Microsoft System Center, 2012)

Server	Purpose	More information
Central Administration Site	The recommended location for all administration and reporting for the hierarchy.	• SQL Server is required. • Does not process client data. • Does not support client assignment. • Not all site system roles are available. • Participates in database replication.
Primary Site	A required site that manages clients in well connected networks. All clients are assigned to a primary site.	• SQL Server is required. • Additional primary sites provide support for a higher number of clients. • Cannot be tiered below other primary sites. • Participates in database replication.
Secondary Site	Manages clients in remote locations where network bandwidth control is required.	• SQL Server Express or a full instance of SQL Server is required. If neither is installed when the site is installed, SQL Server Express is automatically installed. • A management point and distribution point are automatically deployed when the site is installed. • Secondary sites must be direct child sites below a primary site, but can be configured to send content to other secondary sites. • Participates in database replication.

Aktias site-hierarki består endast av två nivåer, där det finns en CAS som är kopplad till endast en primär *Site*. En Distribution Point finns sedan kopplad till den primära *Site*:n. I Fig.2 visas hur Aktias SCCM-hierarki ser ut i verkligheten.



Figur 2. Aktias nuvarande SCCM-hierarki

Aktias SCCM består av endast en primär *Site* d.v.s. SCCM-siteservern i Fig.2. SCCM-siteservern har fem roller installerade som egentligen finns i själva siteservern. I Fig. 2 visas rollerna skilt för att ge en tydligare bild av hierarkihelheten. Ytterligare används en SQL-databassiteserver som är kopplad med SCCM-siteservern.

2.2 Skivavbildning

En skivavbildning är en virtuell fil som t.ex. kan föreställa en fysisk CD-skiva, hårddisk eller ett USB-minne. Tidigare användes den mera som backup av data och för kloning av hårddiskar. Nuförtiden kan man använda den för flera ändamål än endast backup och kloning. Vanligtvis använder man skivavbildningar som virtuella DVD eller Blu-ray-skivor, där de t.ex. kan vara en mjukvara såsom program, spel, operativsystem m.m. Skivavbildningen kan använda olika filformat och brukar oftast följa öppna standarder (wiseGEEK, 2008).

I dagens läge används skivavbildning relativt mycket istället för att använda fysiska DVD/Blu-Ray-skivor. Den är mycket viktig speciellt inom mjukvarudistributionen. T.ex. Linux, som är baserad på öppen källkod, har på sina hemsidor lagt upp på sina olika operativsystem skivavbildningar som kan laddas ner gratis. Ett av de vanligaste filformaten är ”.iso”. Namnet ISO är taget från ISO 9660-standarden, som i sin tur är ett standardiserat filsystem för CD-ROM-media (Microsoft Developer Network, 2012).

I SCCM används skivavbildning speciellt för att skapa färdigt konfigurerade eller installerade operativsystem för att underlätta både installation och konfigurering samt för att spara tid.

2.3 Distribution av mjukvara

En av SCCM:ens huvudsakliga uppgifter är distribuering av program och uppdateringar. Inom SCCM-terminologin talar man ofta om mjukvarupaket. Ett mjukvarupaket innehåller information om själva programvaran som skall distribueras. Det innehåller också information om tillverkaren, programversionen m.m. För att distribuera programvara eller enbart göra konfigurationsändringar använder SCCM dessa mjukvarupaket (System Center 2012 Configuration Manager Unleashed 2012, s. 533-534).

Mjukvarupaketen kan innehålla mera än ett program. Dessa program kan sedan utföra i princip nästan vad som helst såsom t.ex. installera programvara, uppdatera en klients

konfigurationer eller även köra ett antivirusprogram. Först efter att ett mjukvarupaket har skapats i SCCM kan man börja distribuera det. För att kunna distribuera ett mjukvarupaket krävs det att man har DP. (System Center 2012 Configuration Manager Unleashed 2012, s. 635-640).

Ifall det är fråga om en större organisation med användare runt hela världen kan man skapa en Distribution Point Group (DPG). Med hjälp av en DPG kan man skapa en grupp av flera DP:n som finns inom ett visst område. Om en organisation har en DPG i Asien, kan den exempelvis döpas till ”Asiens DP” och endast de klienter som finns i Asien har tillgång till den. (System Center 2012 Configuration Manager Unleashed 2012, s. 57-58). Det är också möjligt att ha en DP i flera olika DPG:n, t.ex. en DP som finns på andra sidan jordklotet som distribuerar all data till en annan DP som finns närmare belägen den klient som har behov av den. En annan orsak till att DPG:n är nyttig är att den kan underlätta nätförbindelsen och att man oftast får en högre hastighet om en DP ligger närmare.

Efter att ett mjukvarupaket har skapats kan man distribuera paketet över nätverket med hjälp av SCCM så att klienterna i samma nätverk kan komma åt programmen.

2.4 Distribueringsprocessen i praktiken

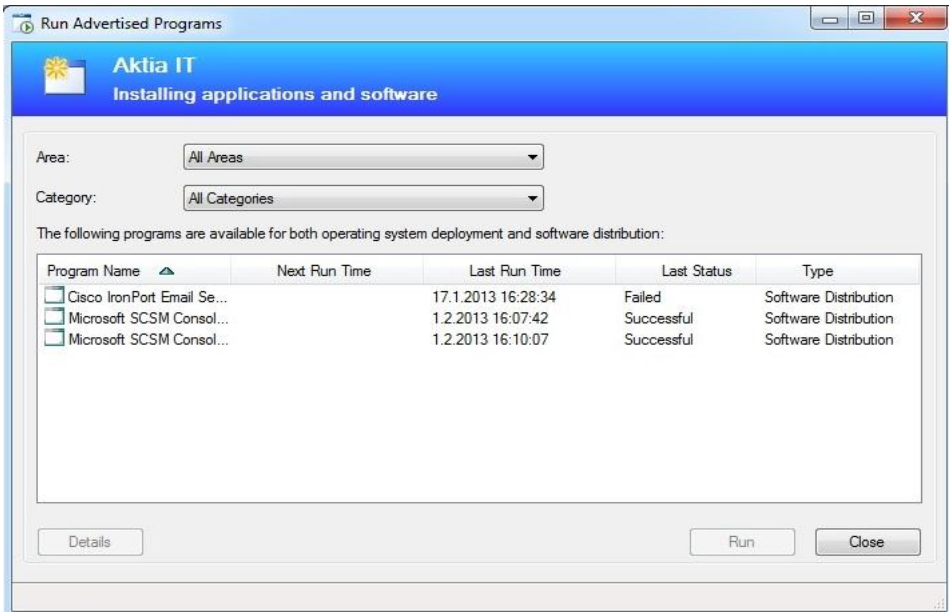
Processen börjar med att en IT-administratör först skapar ett mjukvarupaket i SCCM-konsolen som finns på SCCM:s siteserver, d.v.s. på en primär *Site*. I mjukvarupaketet skriver man in grundläggande information om programmet, såsom namn, version och hur mycket hårddiskutrymme programmet kräver. Efter att informationen har lagts in väljer man varifrån programmet hämtas, d.v.s. källan. Nästa steg är att välja vilken version av operativsystem detta program kan installeras på och om programmet behöver en 32 eller 64 bitars datorarkitektur. För att avsluta skapandet av mjukvarupaketet väljer administratören sedan vilka datorer som skall få tillgång till mjukvarupaketet.

Följande steg är att skapa en så kallad publicering (eng. *deployment*). Då man skapar en publicering väljer man först vilket mjukvarupaket man vill publicera. Nästa steg är att

välja datum och tidpunkt när man vill att paketet skickas till de på förhand utvalda klienterna. Då en publicering skapas går det att välja från vilken DP mjukvarupaketet tas, varefter det sedan är möjligt att välja både vilken prioritet paketet ges och hur det installeras. Efter att administratören skapat en publicering återstår ännu det slutliga steget i distributionsprocessen.

Innan en klient kan börja söka mjukvarupaket bör man ännu göra en så kallad uppgiftssekvens (eng. *Task Sequence*). En uppgiftssekvens är en process inom SCCM som möjliggör utförande av flera steg eller uppgifter på en server/klient. Denna process kräver inte att någon användare behöver vidta någon åtgärd. I uppgiftssekvensen definierar man vad som skall göras och vilka processer som skall köras då en klientdator skall installeras från SCCM. De vanligaste processerna är partitionering och formatering av hårddisk samt installation av operativsystem, drivrutiner och andra program som behövs.

Då ett mjukvarupaket har skapats och publicerats tar det alltid en stund innan klienten/klienterna kan ta emot det och börja installera. Tiden det tar för paketet är dock beroende av vilken prioritet administratören har lagt på paketet. Då mjukvarupaketet har kommit fram till klientens dator kan han/hon söka fram programmet som då finns tillgängligt för nerladdning/installering med hjälp av ett program som heter *Run Advertised Programs* som hittas i kontrollpanelen i Windows-operativsystem. Run Advertised Programs är ett program som SCCM installerar på alla klienter som finns i samma nätverk som SCCM-siteservern. Med detta program kan klienterna antingen ladda ner eller installera program som SCCM har distribuerat. I Fig. 3 visas hur Run Advertised Programs på en klient kan se ut. (Microsoft System Center Run Advertised Programs Overview, 2012)



Figur 3. Ett exempel på hur program söks från SCCM

3 INSTALLATION OCH KONFIGURERING AV SERVRAR

Installeringarna som kommer att utföras i detta examensarbete kommer att ske med serveroperativsystemet Microsofts Windows Server 2008 R2. Orsaken till varför Aktiabanken kräver att serveroperativsystemet Windows Server 2008 R2 skall användas är kompatibilitetsproblem som uppstår mellan Aktias nuvarande kontorssystem och nyare versioner av Windows Server, såsom t.ex. Windows Server 2012. Installationer av serveroperativsystem och mjukvara kommer endast att ske på distans. Dessutom kommer enbart fysiska servrar att användas. De fysiska kontorsservrar som kommer att användas i detta examensarbete är IBM:s System x3200 M3 servrar, (se Fig. 4).

Figur 4. IBM System x3200 M3

3.1 Windows Server 2008 R2

R2 står för leveransversion två. Serveroperativsystemet Windows Server 2008 R2 utkom den 22:a oktober 2009 (Microsoft, 2009). Windows Server 2008 R2 var Microsofts första operativsystem som enbart fanns i 64-bitars version (Windows Server Blog, 2008).

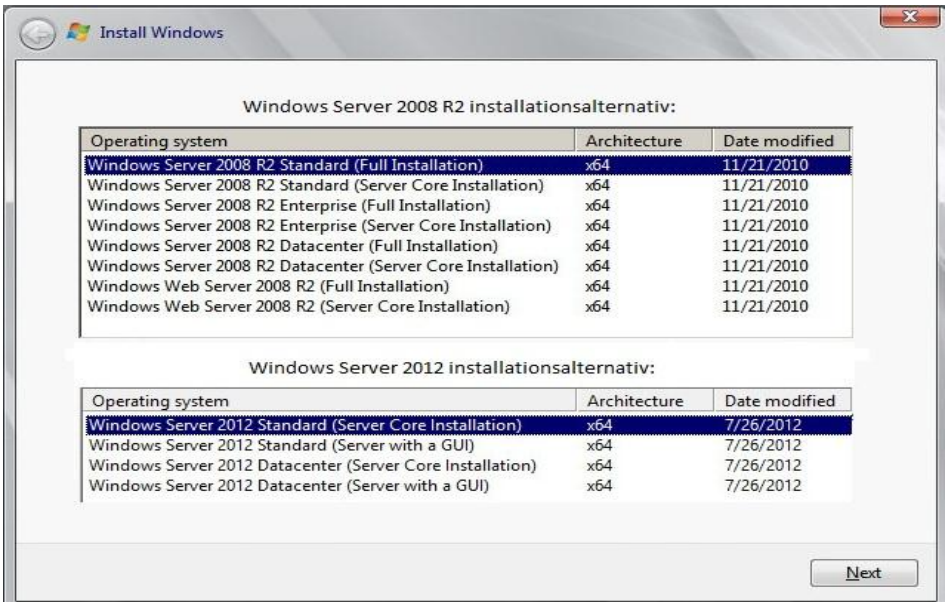
Vid installering av detta serveroperativsystem finns det åtta (8) olika installationsalternativ. I Microsofts nyaste serveroperativsystem Windows Server 2012 har Microsoft tagit i bruk en ny standard där de har bytt ut två av installationsalternativen från Windows Server 2008 R2, *Windows Web Server* och *Enterprise* mot två nya alternativ.
I det nyaste serveroperativsystemet Windows Server 2012 har Microsoft bestämt att fortsätta användningen av installationsalternativen *Standard* och *Datacenter* (ArsTechnica, 2012).

Ett helt nytt installationsalternativ har skapats, sedan Windows Server 2012 kommit ut, nämligen alternativet *Essentials*. I Fig. 5 har en jämförelse gjorts mellan de vanligaste installationsalternativen för Windows Server 2008 R2 och Windows Server 2012 för att visa skillnaderna. Alternativen *Essentials* och *Foundation* finns inte med i Fig. 5 eftersom de anses vara ovanligare än de andra alternativen.

Installationsalternativen för Windows Server 2008 R2 är, antingen *Full Installation*/*Full Installation Server* eller *Server Core Installation*. Innan man installerar en Windows Server bör man veta vilken version av installationsalternativet man vill ha. Kort sagt är *Full Installation/Full Installation Server* egentligen samma sak som en traditionell ”Windows Server”-installation. I en *Full Installation* har man möjlighet att använda alla funktioner som Windows Server 2008 R2 har att erbjuda (Windows Server, 2012). Beroende på vilket installationsalternativ man använder, får man tillgång till de specifika specialfunktionerna för det valda alternativet. De vanligaste mjukvarukomponenterna till serveroperativsystemet *Full Installation/Full Installation Server* installeras som administrativa verktyg och grafiskt användargränssnitt. De som har behov av att använda de flesta funktioner som ett installationsalternativ kan erbjuda väljer *Full Installation/Full Installation Server* versionsvalet (Hannifin, 2010 s.20). Vid val av versionen

Server Core Installation får man tillgång till endast de väsentliga komponenterna i serveroperativsystemet.

Med S*erver Core Installation* ligger fokus på datasäkerheten. Eftersom detta installationsalternativ helt saknar grafiskt användargränssnitt, betyder det att serveroperativsystemet måste administreras via en kommandotolk. En *Server Core Installation* är inte lika sårbar för datorintrång, eftersom den inte har ett grafiskt användargränssnitt och endast de allra nödvändigaste mjukvarukomponenter är installerade. Detta versionsval är ypperligt då man kräver en datasäkerhet på en högre nivå (Hannifin, 2010 s.21).



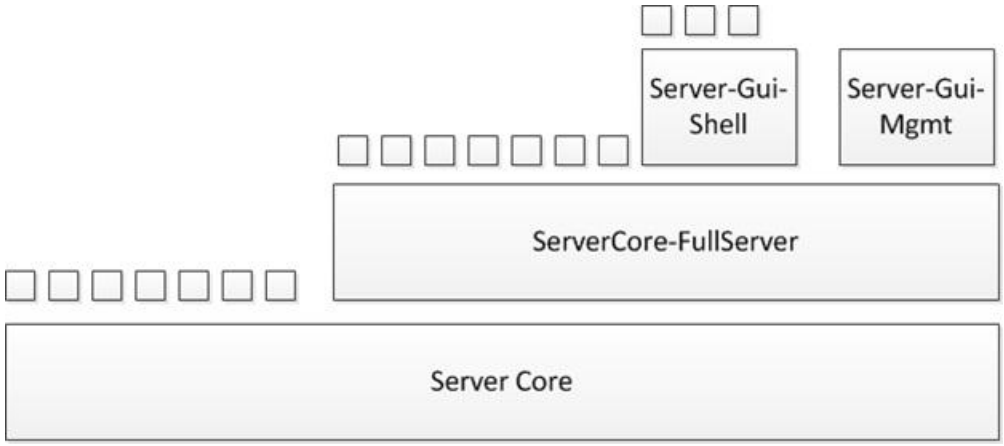
Figur 5. En jämförelse mellan Windows Server 2008 R2:s och Windows Server 2012:s installationsalternativ för serveroperativsystem

I den nyare versionen av Windows Server, d.v.s. Windows Server 2012 har man döpt om versionerna av installationsalternativ så att det framkommer vilka alternativ som har ett inbyggt grafiskt användargränssnitt (GUI) och vilka som är utan.

Skillnaden i installationsalternativen mellan Windows Server 2008 R2 och Windows Server 2012 är inte enbart namnen och antalet installationsalternativ, utan också en förbättring i den tekniska översikten av både *Full Server Installation/Full Installation Server* och *Server Core Installation*. I Windows Server 2008 R2 är det inte

möjligt att konvertera från en *Full Installation/Full Installation Server* till en *Server Core Installation*, utan man är tvungen att installera om serveroperativsystemet i sin helhet. I Windows Server 2012 har Microsoft förbättrat detta och där har man nu möjlighet att konvertera från en *Server Core Installation* till en *Full Installation*/*Full Installation Server* och vice versa vid behov. Fig. 6 och Fig. 7 visar hur Microsoft har förbättrat strukturen av dessa val (Windows Server, 2012).

Figur 6. Windows Server 2008 R2:s struktur för olika installationsalternativ (Windows Server. 2012)



Figur 7. Windows Server 2012:s förbättrade struktur för olika installationsalternativ (Windows Server. 2012)

Fig. 6 och Fig. 7 visar att vid installation av serveroperativsystemet Windows Server 2008 R2 är man tvungen att välja antingen en *Full Server* installation eller en *Server Core* installation. Därefter är det inte längre möjligt att ändra på det val man gjort. Ifall man behöver byta alternativet är man tvungen att installera om hela servern. Det som skiljer från Windows 2012 är att man har möjlighet att flytta från en *Full Installation* till en *Server Core* installation och vice versa. Detta betyder att man i Windows Server 2012 har möjlighet att byta till ett annat installationsalternativ utan att

behöva om installera hela servern. I Windows Server 2012 har Microsoft förbättrat detta genom att integrera installationsalternativen och nu finns det istället tre större tillvalsfunktioner, *Server Core*, *ServerCore-FullServer* och *Server-Gui-Shell*/*Server-Gui-Mgmt*. Detta betyder att IT-administratörer har möjlighet att installera eller avinstallera dessa tillvalsfunktioner för att sedan vid behov kunna byta mellan *Server Core* och *Full Server Installation*. (Windows Server, 2012).

Installationsalternativen som kommer att användas i detta slutarbete kommer främst att vara Windows Server 2008 R2 Standard (Full Installation) och Datacenter (Full Installation). Installationsalternativen Standard och Datacenter i Windows Server 2008 R2 och 2012 håller sig till samma principer. Alternativet Standard väljer man om servern skall köra program som går utöver en vanlig filserver eller printserver. Applikationer såsom Microsoft Exchange, ”SQL Server”-databaser, SharePoint serverapplikationer brukar vara vanliga för detta installationsalternativ. Ifall man vill köra virtuella servrar med t.ex. VMware, Hyper-V eller någon annan virtuell miljö är Datacenter det bättre installationsalternativet (ArsTechnica, 2012).

3.2 Installation

I arbetet skall ca 70 fysiska servrar installeras på ett automatiserat sätt. Microsofts lösning på detta är programvaran System Center 2012 Configuration Manager (*SCCM*). Planen är att använda skivavbildningar och med hjälp av dem börja med installationer som kommer att göras på distans. En grundläggande skivavbildning av en Windows Server 2008 R2 kommer att skapas.

En annan sak att tänka på då det gäller mjukvaruinstallationer är om programmet skall installeras för en 32-bitars eller 64-bitars arkitektur. I det här fallet installeras ett serveroperativsystem som endast kommer att utgå från en 64-bitars arkitektur. Systemkraven för Windows Server 2008 R2 visas i Tabell 2. Innan man börjar installera en mjukvara såsom ett operativsystem gäller det således att ta reda på systemkraven för den mjukvara man tänker installera.

Tabell 2. Systemkraven för Windows Server 2008 R2 (Microsoft Developer Network, 2007)

Component	Requirement
Processor	• Minimum: 1 GHz (x86 processor) or 1.4 GHz (x64 processor) • Recommended: 2 GHz or faster **Note:** An Intel Itanium 2 processor is required for Windows Server 2008 for Itanium-Based Systems.
Memory	• Minimum: 512 MB RAM • Recommended: 2 GB RAM or greater • Maximum (32-bit systems): 4 GB (Standard) or 64 GB (Enterprise and Datacenter) • Maximum (64-bit systems): 32 GB (Standard) or 1 TB (Enterprise and Datacenter) or 2 TB (Itanium-Based Systems)
Available Disk Space	• Minimum: 10 GB • Recommended: 40 GB or greater **Note:** Computers with more than 16 GB of RAM will require more disk space for paging, hibernation, and dump files.
Drive	DVD-ROM drive
Display and Peripherals	• Super VGA (800 x 600) or higher-resolution monitor • Keyboard • Microsoft Mouse or compatible pointing device

De fysiska kontorsservrarna som används i Aktia har följande tekniska specifikationer:

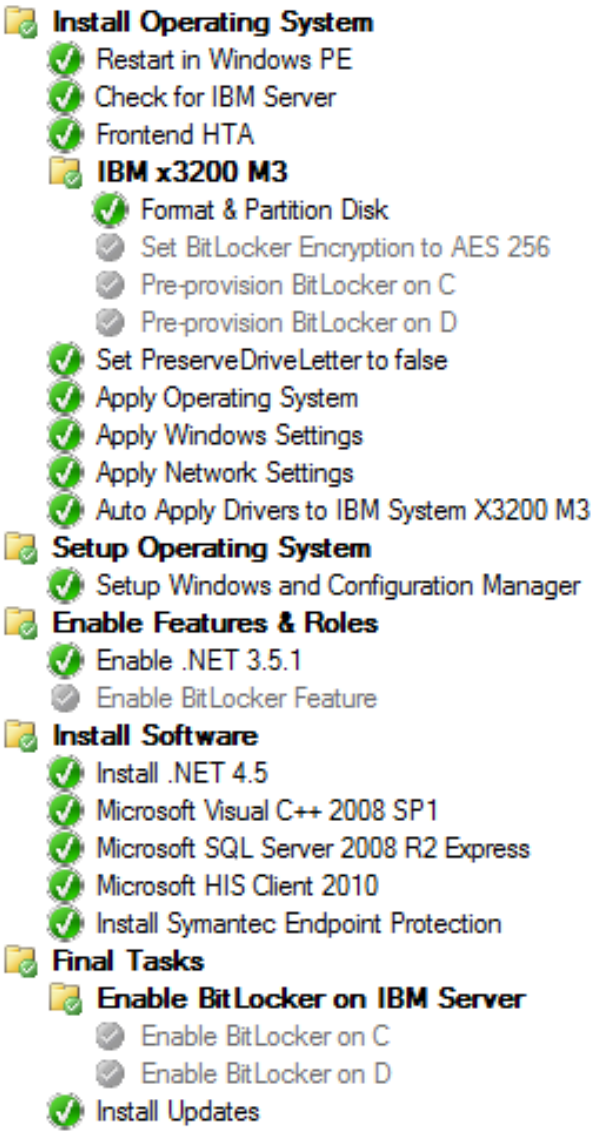
- **Processor:** Intel Xeon X3450 Quad-Core @ 2,67Ghz
- **Minne (RAM):** 8GB DDR3 ECC 800Mhz
- **Hårddisk:** 2st IBM 500GB SATA 3Gbps (RAID 1)
- **Nätkort:** 4st Intel 100/1000 Gigabit LAN
- **DVD-ROM station**

Modellen IBM System x3200 M3 uppfyller systemkraven i Tabell 2.

3.2.1 Installation av en bankontorsserver

Installationerna av bankkontorsservrarna sker med hjälp av en skivavbildning som har gjorts i SCCM och sedan distribuerats med hjälp av en uppgiftssekvens. En grundläggande skivavbildning som kommer att användas för alla serverinstallationer har skapats. Skivavbildningen innehåller alla drivrutiner som servern *IBM System x3200 M3* behöver. I samma skivavbildning sker också krypteringen, serverns hårddiskar krypteras innan serveroperativsystemsinstallationen sätter igång.

Uppgiftssekvensen som kommer att användas för Aktias bankkontorsservrar visas i Fig.8.



Figur 8. Illustration av bankkontorsserverns uppgiftssekvens

Hela installationsprocessen börjar med en PXE-startprocess (Pre-Boot Execution Environment). PXE är ett gränssnitt som kan användas av IT-administratörer för att på distans kunna konfigurera en server/dator som inte ännu har hunnit starta upp operativsystemet (SearchNetworking, 2005).

För att PXE-startprocessen kan startas krävs det att en IT-administratör är fysiskt närvarande för att starta bankkontorsservern. För att kunna starta upp PXE-startprocessen

krävs det att bankkontorsservern startas från nätverket (eng. network boot) och detta görs alltid genom att trycka på F12 då servern startas upp. Det som egentligen händer under PXE-startprocessen är att bankkontorsservern tar kontakt med en DHCP-server (Dynamic Host Configuration Protocol) genom att skicka en DHCP-begäran. DHCP är ett standard nätverksprotokoll som här används för att skicka information om var DP-servern finns, för att från den kunna ta emot en så kallad startskivavbildning (eng. boot image). Startskivavbildningen innehåller själva uppgiftssekvensen. Efter att DHCP-servern har tagit emot DHCP-begäran från bankkontorsservern, svarar den till bankkontorsservern genom att exekvera startskivavbildningen, vilket leder till att uppgiftssekvensen påbörjas (Oracle Enterprise Manager, 2013). Efter att PXE-startprocessen har utförts börjar uppgiftsekvensen gå igenom alla steg som illustreras i Fig. 8. Före uppgiftsekvensen börjar med de första installationsprocesserna utför den en kontroll som granskar om servern/datorn är exakt en IBM System x3200 M3. Ifall denna skulle vara någon annan modell såsom HP (Hewlett Packard) skulle hela uppgiftsekvensen avslutas. Eftersom denna uppgiftsekvens endast är gjord för modellen IBM System x3200 M3 granskar man att det är en sådan server före man börjar installera.

Den första installationsprocessen börjar med att partitionera servern/datorns hårddisk. Aktias bankkontorservrar har två partitioner, C-partitionen för serveroperativsystemet och D-partitionen för programvara.

Efter att partitioneringarna har gjorts var tanken att kryptera hårddisken med BitLocker:s 256 bitars AES-kryptering. För att kunna kryptera en hårddisk bör krypteringen först aktiveras i Windows. Man försökte aktivera krypteringen i Windows genom SCCM:s egen funktion, men det misslyckades. Sedan försökte man aktivera krypteringen med ett PowerShell-skript, som gjordes av en programmerare inom företaget Aktia, men det misslyckades också. Orsaken visade sig vara att det inte var möjligt att få kontroll över ett så kallat TPM-chipp (Trusted Platform Module) med varken SCCM:s egen inbyggda funktion eller med PowerShell-skriptet i uppgiftsekvensen. TPM-chippet är ett på moderkortet integrerat mikrochipp som är gjort för att ge olika säkerhetsfunktioner som innefattar krypteringsnycklar och det krävs att användaren har kontroll över detta chipp innan man kan börja kryptera med BitLocker. (Windows Trusted Platform Module Management Step-by-Step Guide, 2013). Man upptäckte att denna modell av IBM-servern har TPM-chippet inaktiverat i BIOS:en (Basic Input/Output System) från bör-

jan, vilket betyder att man manuellt var tvungen att aktivera den i BIOS:en och därefter var det möjligt att aktivera krypteringen i Windows. BIOS:en är ett chipp som finns integrerat på moderkortet i datorn. BIOS:en kommunicerar mellan hårdvaran och operativsystemet (MSI, 2011). I uppgiftssekvensen har man satt en inställning att om något fel uppstår, hoppar uppgiftssekvensen över felet och fortsätter till nästa steg. Eftersom hårddisken inte blev krypterad på förhand bör det göras manuellt efter att alla installationer är klara.

Därefter börjar installationen av operativsystemet, Microsoft Windows Server 2008 R2 i detta fall. Ifall servern/datorn kräver omstart kommer uppgiftsekvensen att sköta om det automatiskt och sedan fortsätta från samma processtillstånd.

Då inställningarna är konfigurerade fortsätter installationsprocesserna med att installera alla drivrutiner som servern/datorn behöver för att fungera. Drivrutinerna behövs för att servern/datorn skall kunna kommunicera med hårdvaran. IBM:s System x3200 M3 har närmare 70 olika drivrutiner som måste installeras.

I nästa steg installeras SCCM-klienten på servern/datorn. Efter att SCCM-klienten är installerad på en bankkontorsserver kan man enkelt distribuera programvara vid behov.

Efter att serveroperativsystemet och SCCM-klienten är installerade börjar installeringsprocesserna för bankkontorens egna programvaror. Med de egna bankkontorsprogrammen kommer också en del andra viktiga program samt ett antivirusprogram som bör installeras.

Då all programvara är installerad är uppgiftssekvensen klar och det krävs endast en åtgärd till, nämligen krypteringen. Eftersom det inte var möjligt att kryptera enligt planeringen bör det göras i slutändan istället. Före krypteringen kan börja bör man initiera TPM-chippet så att man kan få kontroll över det. Detta görs genom att klicka på *Start* som hittas i Windows-aktivitetsfältet, klicka sedan på *All Programs* och till sist klickar man på *Run*. I *Run*-fönstret skriver man in ”tpm.msc”, därefter öppnas TPM:s hanteringsprogram och där bör man sedan klicka på ”*Initialize TPM*”. Efter att ha valt att initiera TPM-chippet kommer ett fönster upp enligt Fig. 9.

Figur 9. Initiering av TPM-chippet

I följande steg gäller det för IT-administratören att följa instruktionerna enligt Fig. 9. Servern kommer att omstartas och från BIOS:en kommer ett fönster att dyka upp, som frågar ifall han/hon godkänner att ta kontroll över TPM-chippet.

Efter att ha svarat att han/hon godkänner dessa ändringar är det sedan möjligt att kryptera hårddisken. För att manuellt kryptera hårddiskpartitionerna bör IT-administratören öppna programmet *BitLocker Drive Encryption* och där väljer han/hon ”Turn On BitLocker” på den valda partitionen. Krypteringen av hårddiskarna tog två och en halv timme.

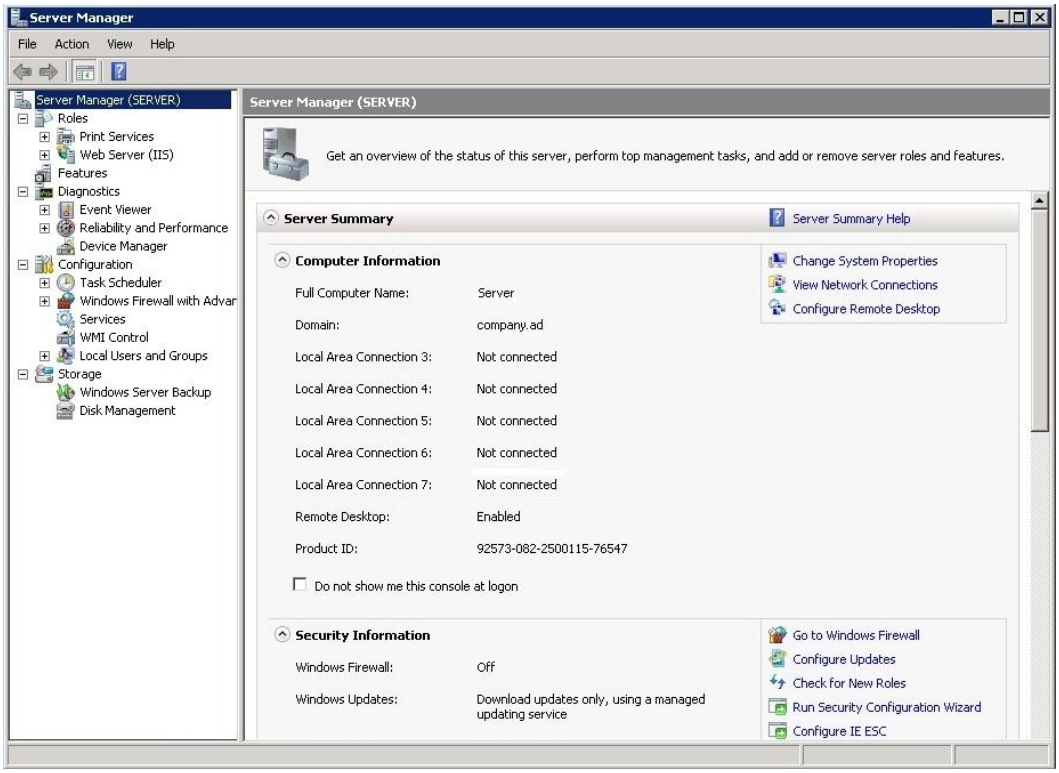
Efter att krypteringen har gjorts på både C och D-partitionerna är bankkontorsservern färdig och klar för användning.

3.3 Konfigurering

Konfigurationerna på en server med ett Windows Server operativsystem görs i ett program som heter *Server Manager*, en programvara skapad av Microsoft. Med hjälp av detta program kan IT-administratörer både se och hantera all information samt nå verktyg som påverkar en servers produktivitet. Vanligtvis kommer *Server Manager* med vid installation av ett Windows-serveroperativsystem, men det är också möjligt att ladda ner programmet från Microsofts hemsidor. Vid uppstart av en Windows-server kommer ”Server Manager”-konsolen upp automatiskt. ”*Server Manager”*-fönstret som visas i Fig. 10 är också en lämplig omgivning där man kan se de vanligaste konfigurationerna.

I *Server Manager* konsolen har man möjlighet att hantera

- Roller och rolltjänster
- Funktioner
- Diagnostik
- Konfigurering
- Lagring



Figur 10. ”Server Manager”-fönstret i Windows Server 2008 R2

För att få serverinstallationsprocesserna så långt som möjligt automatiserade försöker man få alla bankkontorsservrar färdigt konfigurerade så långt som möjligt. En stor del av servrarna kommer att ha en del gemensamma konfigurationer. T.ex. nätkortskonfigurationerna kommer att vara gemensamma konfigurationer som görs på alla bankkontorsservrar, men IP-adresserna (Internet Protocol) kommer att vara unika. Servrarna kommer att automatiskt läggas till bankkontorsdomänet samt till Domain OU:n (Organization Unit). En Domain OU är en underavdelning i AD:n (Active Directory). AD:n är en databas, där kataloger för användare, användargrupper, datorer och servrar finns (Win-

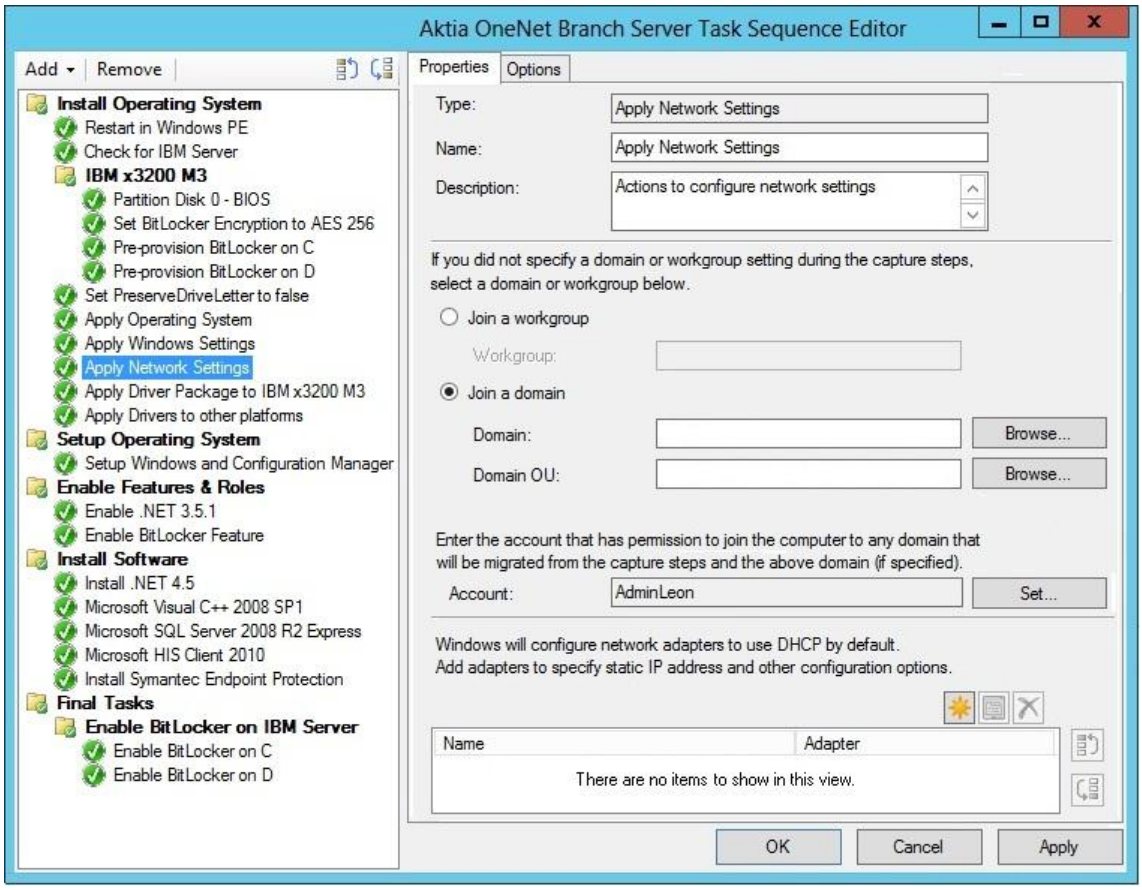
dows Dev Center, 2012). AD:n är konstruerad för att kunna hantera sök och läs-funktioner av en större mängd användare (Indiana University, 2013).

Alla servrar kommer dock inte att vara konfigurerade på samma sätt, vilket leder till problem vid användning av SCCM. Eftersom en del bankkontor kommer att ha olika konfigureringar kommer det inte vara möjligt att färdigt konfigurera en fullständig skiv-avbildning utan detta måste sedan göras manuellt.

3.3.1 Konfigurering av en bankkontorsserver

Efter att operativsystemet/serveroperativsystemet är installerat kan det konfigureras. För bankkontorsservrarna har man konfigurerat så att Windows-serveroperativsystemets brandväggar är inaktiverade eftersom Aktia använder egna brandväggar.

I uppgiftsekvensen är det möjligt att färdigt konfigurera några nätverksinställningar för serveroperativsystemet (se Fig.11).



Figur 11. Nätverksinställningar i en uppgiftssekvens

Bankkontorsservrarna kommer på detta sätt automatiskt att ansluta sig till Aktias kontorsdomän och Domain OU. Varje server får också en egen unik statisk IP-adress från en så kallad adresspool där man har reserverat en statisk IP-adress för varje bankkontorserver.

4 UNDERHÅLL AV SERVRAR

Underhållet av bankkontorsservrar kommer enbart att handla om uppdateringar och säkerhetskopior. För att en server skall vara säker bör den först och främst vara up-to-date med de senaste säkerhetsuppdateringar. Uppdateringen är en liten del av underhållet men är en sak som bör göras kontinuerligt. Den andra viktiga saken är säkerhetskopior. I vilken organisation som helst är säkerhetskopior viktiga, på Aktia finns det extremt mycket hemlig information som gör att säkerhetskopior är av största vikt.

4.1 Uppdateringar

Microsofts uppdateringar till serveroperativsystemet Windows Server 2008 R2 kommer att automatiseras. Då finns det en möjlighet att automatisera uppdateringarna på alla Windows servrar, men automatiseringen medför också en nackdel. Om t.ex. Microsoft ger ut nya uppdateringar för Windows-servrar och servrarna genast börjar hämta uppdateringarna från nätet så fort de finns tillgängliga, kan det leda till att en stor del av bandbredden används. Detta kan i sin tur minska hastigheten för datorernas användare. Microsoft har en lösning på detta problem. Lösningen är att använda sig av Windows Server Update Services (WSUS). Det är ett program som ger IT-administratörer möjlighet att distribuera uppdateringar för Microsoft Windows serveroperativsystem. Med hjälp av WSUS kan administratörerna hantera när och hur distribueringen av uppdateringar till Windows-servrar kommer att ske (Windows Server, 2013).

WSUS installeras ofta på en separat server som sedan används som en uppdateringsserver. På Aktia används en WSUS server för serveruppdateringar och denna server kommer att utnyttjas då bankkontorsservrarna behöver uppdateras.

IBM:s *UpdateXpress*-verktyg används för att ladda ner uppdateringar av drivrutiner och så kallad *firmware*. *UpdateXpress*-verktyget söker de senaste uppdateringar som finns för servern i fråga och säger också till ifall en uppdatering anses vara nödvändig eller inte.

4.2 Säkerhetskopior

Säkerhetskopior är kopior som görs av original filer och sedan lagras någon annanstans. Säkerhetskopior är viktigt att ha ifall en användare råkar t.ex. tappa bort eller raderar ett dokument av misstag. Säkerhetskopiorna kan lagras på många olika sätt, de två vanligaste sätten är på hårddiskar eller på ett magnetband med hjälp av en magnetbandenhet (Windows Säkerhetskopiera och återställa: vanliga frågor, 2013)

Alla bankkontorsservrar kommer att skapa säkerhetskopior på de filer och databaser som finns lagrade i själva servrarna. Även säkerhetskopior av servrarnas hårddiskpartit-

ioner skapas ifall en hårddisk från en bankkontorsserver går sönder. Bankkontorens säkerhetskopior lagras både på magnetband och på hårddiskar. Information som förvaras en längre tid, vanligtvis några år, sparas på magnetband, medan information som förvaras en kortare tid, d.v.s. några månader, sparas på hårddiskar. Säkerhetskopieringen på bankkontorsservrarna skapar kopior och synkroniserar filerna var 12:e timme, d.v.s. två gånger per dygn.

För att kunna få tillbaka filer som t.ex. förstörts eller blivit överskrivna kan man återskapa data, för att få tillbaka den information som försvunnit. Återskapande av data går mycket snabbare från hårddiskar än från magnetband, eftersom det tar längre tid för en magnetbandenhet att söka fram informationen. Magnetbandenheten har en återställningspunkt (eng. recovery point) varje veckoslut, medan återställningspunkten på hårddiskarna är varje morgon under vardagar. På detta sätt ser man till att bankkontorsservrarna har kopior av senast uppdaterade data och att kopiorna kan återställas från många olika versioner av filerna.

För att underhålla säkerhetskopieringar och återskapning av data, används programmet *Data Protection Manager* som hör till programpaketet Microsofts System Center 2012. Med hjälp av detta program har man konfigurerat så att säkerhetskopieringen av bankkontorsserverns filer, databaser och hårddiskpartitioner sker automatiskt vid vissa tidpunkter. Ifall något gått förlorat, behöver man endast skriva in namnet på de filer eller kataloger man vill återskapa och därefter välja datum och tidpunkt i sökningslistan.

5 DATASÄKERHET

Datasäkerheten indelas vanligen i fysisk, teknisk och administrativ datasäkerhet. Datasäkerhetens uppgift är att säkra användaren från datorvirus, datorintrång, förlorad information m.m. Med hjälp av en bra och aktuell datasäkerhet säkrar man datorer, servrar, nätverk, smarttelefoner, datorplattor och annan teknisk hårdvaruutrustning. Eftersom Aktia är en bank som hanterar privat ekonomisk information har datasäkerheten hög prioritet.

5.1 Fysisk datasäkerhet

Den fysiska datasäkerheten syftar oftast på hur säkrade servrar är i en byggnad och hur man skyddar sig mot eldsvådor eller naturkatastrofer. Trådbaserade nätförbindelser hör också till den fysiska datasäkerheten eftersom nätkablarna är fysiskt dragna från ett ställe till ett annat.

5.1.1 Hantering av intrång, eldsvådor och naturkatastrofer

Varje kontor kommer att ha ett skåp där kontorsservern finns i säkert förvar. Man kommer in i skåpet enbart med en fysisk nyckel. Endast IT-administratörer kommer att ha tillgång till de låsta skåpen där kontorsservrarna kommer att förvaras.

Naturkatastrofer och eldsvådor är inte något som man räknar med att händer så ofta. Då det gäller datasäkerheten är det viktigt att ta alla tänkbara olyckor i beaktande.
Då en naturkatastrof eller eldsvåda uppstår finns det en stor risk att t.ex. en server går sönder eller helt enkelt bara blir utan ström.

För att skydda bankkontorsservrarna i fall av eldsvåda har man på Aktia låst in dem i ett brandsäkert skåp. Vid större naturkatastrofer finns det egentligen inte mycket man kan göra åt saken. Ifall någon mindre naturkatastrof då t.ex. strömmen avbryts har Aktia säkerhetskopior på huvudkontoret.

5.1.2 Nätförbindelsen mellan bankkontorens och huvudkontorets servrar

Bankkontorsservrarna kommer att ha separata privata nät och servrarna är ytterligare länkade till huvudkontorets servrar. Internet kommer in till bankkontorens omkopplare och servrar med hjälp av kopparkablar. Beträffande datasäkerheten är kopparkabeln dock inte lika säker som fiberkabeln.

Fiberkabeln strålar inte ut magnetiska fält, vilket däremot kopparkabeln gör. De elektromagnetiska fälten för fiberkabeln förvaras inne i själva kabeln till skillnad från kopparkabeln som strålar ut dem. Detta gör det omöjligt att utifrån avläsa information som skickas inom fiberkabeln. För användare/organisationer som använder kopparkab-

lar är detta en stor datasäkerhetsrisk, eftersom de elektromagnetiska fälten kommer ut från kopparkabeln, vilket möjliggör att utomstående kan avläsa informationen som skickas inom kopparkablarna.

Bankkontorsnätförbindelsetrafiken mellan bankkontoren och huvudkontoret går aldrig genom det publika Internet. Orsaken till varför bankkontorsservrarnas nätförbindelsetrafik inte går till det publika Internet är för att det orsakar datasäkerhetsrisker och dessutom kan det enklare leda till att obehöriga försöker komma åt servrarna. Datatrafikkryptering sker endast på applikationsnivå vid behov. Nätförbindelserna som sedan går över Internet och till t.ex. samarbetspartner använder sig av en säkrad VPN-teknologi (Virtual Private Network). Ett VPN är en mycket säker anslutning som länkar ett privat nätverk till det publika nätverket såsom Internet (Netgear, 2013).

Ibland används också säkra förbindelsen, som är på applikationsnivå med hjälp av t.ex. SSH (Secure Shell), som är ett säkert sätt att ansluta sig till en dator på distans (Search-Security, 2005). En säker förbindelse fungerar som ett rör med två noder som kommer in i ett nätverk. I en säker förbindelse krypteras informationen i vanliga datapaket och sedan inkapslas datapaketen och överförs i Internet (VPN4ALL, 2013).

5.2 Teknisk datasäkerhet

Den tekniska datasäkerheten är minst lika viktig som den fysiska datasäkerheten. I den tekniska datasäkerheten hanterar man främst nätkommunikation, sabotageprogram och server/dator-intrång. För skydd mot datasäkerhetshot krävs det att man har krypterad datakommunikation, brandväggar och antivirusprogram.

5.2.1 Kryptering

Att kryptera något betyder att man ersätter, ändrar eller blandar ord i en text eller textrad. Lösenord är exempelvis något som man ofta krypterar nuförtiden. Det finns flera olika krypteringsalgoritmer, de tre vanligaste algoritmerna idag är *AES*, *RSA* och *MD5*. Dessa krypteringsalgoritmer använder krypteringsnycklar av olika längd, längden mäts i antalet bitar. Ju längre nyckellängd, desto svårare är det för utomstående att

knäcka krypteringen. Typiska krypteringsnycklar har längden 128…256bit. I Fig.12. visas ett hur en krypterad textrad kan se ut.

Figur 12. Exempel på 256-bitars AES-kryptering

På Aktia är all information konfidentiell och detta är orsaken till att allt bör krypteras. Informationen i alla bankkontorsservrar krypteras med en programvara som heter *BitLocker*. Krypteringen kommer vara av typen AES med 256 bitars nyckellängd. Före Windows Server 2008 R2 installeras på bankkontorsservrarna kommer hårddiskarna att krypteras. Orsaken till att servrarnas hårddiskar krypteras då man installerar serveroperativsystemet, är att det är en betydligt snabbare process att kryptera en hårddisk då den är tom. En hårddisk som innehåller data kräver mycket längre tid för kryptering och den skall göras på 70 servrar.

5.2.2 Antivirusprogram

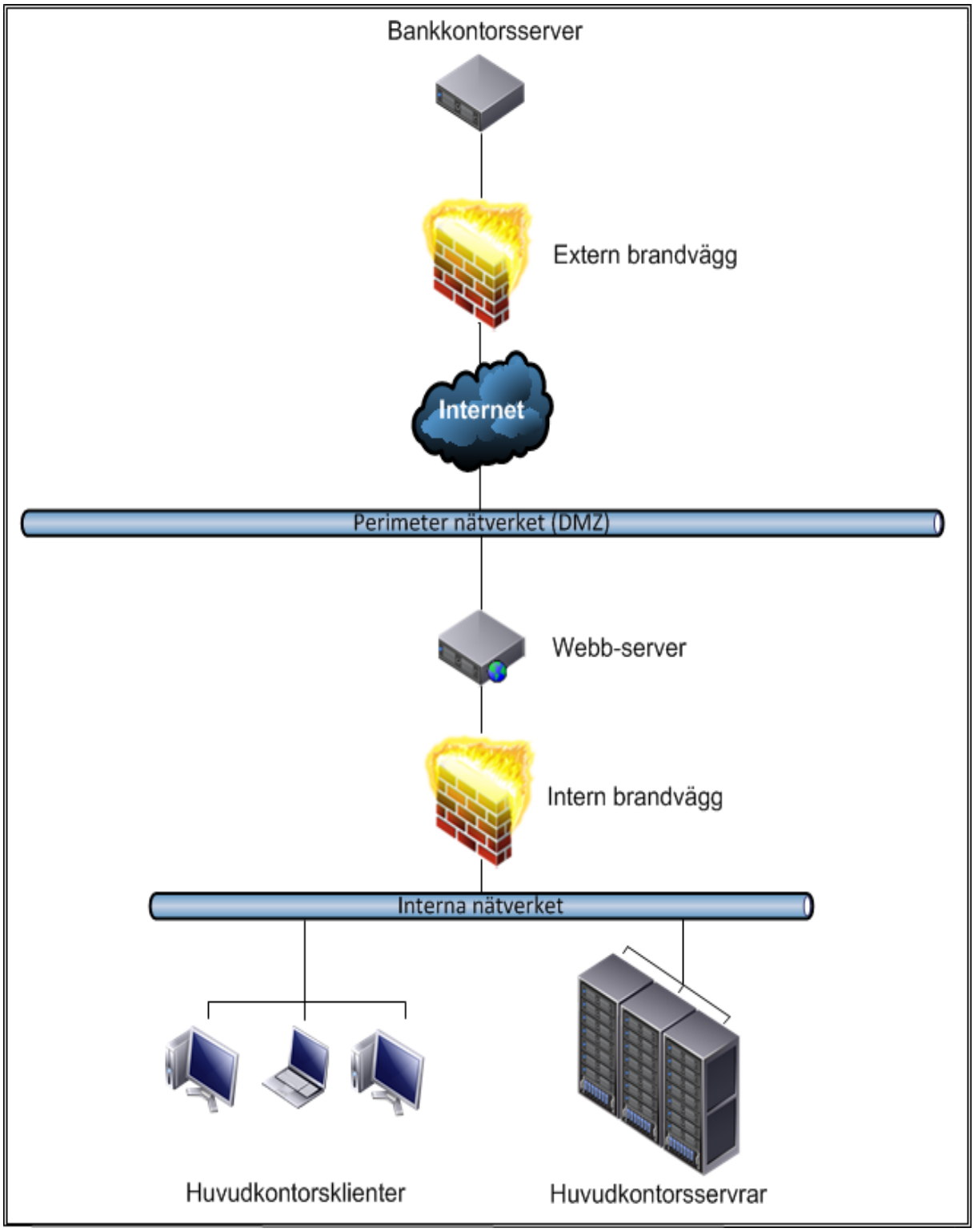
Ett antivirusprogram är en programvara för att skydda användaren mot skadliga program såsom virus, trojanska hästar, maskar mm. Antivirusprogrammet fungerar oftast i bakgrunden utan att man själv ens vet om att det är igång. Programmet skannar alla inkommande filer på en dator/server. Programmet läser en fil eller ett programs kodmönster och alarmerar direkt om det är ett mönster som verkar vara suspekt. Antivirusprogrammen är oftast automatiserade så att det direkt upptäcks om något verkar vara en risk för datorn/servern. I sådana fall läggs de misstänkta filerna i antivirusprogrammets karantän. (Computer Security Basics, 2nd Edition, 2006)

Varje bankkontorsserver kommer att ha ett antivirusprogram installerat. Alla bankkontorsservrar är kopplade till Internet via ett LAN (Local Area Network) och därför är det viktigt att ha ett antivirusprogram installerat. Både servrarna och klienterna som finns i samma nätverk på Aktia har antivirusprogram installerade.

5.2.3 Brandväggar

En brandvägg kan vara antingen en fysisk enhet eller en programvara som är installerad på en dator eller server. Brandväggen finns alltid mellan en dator/server och Internet. Dess uppgift är att skydda användaren genom att blockera nätförbindelser som användaren inte har begärt och på detta sätt kan man undvika att en dator/server skadas (Bleepingcomputer.com, 2004).

På Aktia ligger varje bankkontor bakom minst en brandvägg. I Fig.13. visas ett exempel på hur en bankkontorsserver kan vara kopplad. Brandväggarna skyddar respektive kontor, bankkontoren och huvudkontoret och man har konfigurerat brandväggarna så att de är öppna för nätförbindelsen mellan bankkontorsservrarna och huvudkontorsservrarna.



Figur 13. Ett sätt att lösa nätverksarkitekturen för bankkontoren

5.3 Administrativ datasäkerhet

Den administrativa datasäkerheten omfattar datasäkerhetspolicyn och kan indelas i följande kategorier

- **Planering och administrering av helhetens datasäkerhet**
  I denna kategori skapar man bl.a. organisationens datasäkerhetspolicy samt katastrofplaner. Man gör också riskanalyser samt övervakar anställda och organisationens system.
- **Daglig administrering av datasäkerhet**
  Denna kategori handlar enbart om en anställds användarprofiler. Här skapar man säkra användarprofiler för användarna. Man hanterar också hur ofta användarna bör byta lösenord på sin dator. Vid extrema fall kan man också hantera tidpunkter, d.v.s. när det är möjligt att logga in till sin arbetsdator.
- **Daglig systemadministrering**
  Den sista kategorin handlar främst om att hålla alla system igång. Till den dagliga systemadministreringen hör det också till att göra säkerhetskopior och att se till att alla system fungerar felfritt. (Computer Security Basics, 2nd Edition, 2006)

På Aktia har man en sträng datasäkerhetspolicy för alla användare, även IT-administratörer har en datasäkerhetspolicy. Administratörerna har dock tillgång till de system, programvara och servrar som hör till deras eget kostnadsställe. Datasäkerhetspolicyn innebär att en användare enbart har tillgång till de program och system han/hon behöver för sitt arbete. Beroende på användarens roll inom organisationen varierar också datasäkerhetspolicyn.

5.3.1 Datasäkerhetspolicyn Group Policy

Egentligen så är *Group Policy* en infrastruktur, som ger möjlighet för IT-administratörer att specificera hantering av användarnas konfigurationer samt deras datorer. Detta används oftast i medelstora och större företag som har ett större datornätverk. Med hjälp

av *Group Policy* kan man t.ex. definiera vilka användare som skall ha administrativa rättigheter i en specifik dator (Windows Server, 2012).

6 TESTNING OCH IBRUKTAGANDE

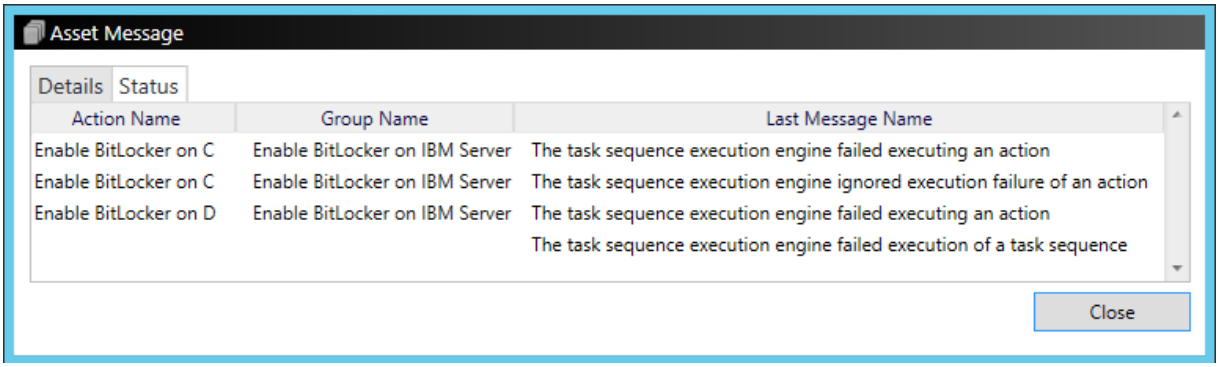
Eftersom detta examensarbete är en del av ett större viktigt projekt för företaget och resulterar i en stor förändring inom organisationen bör testning av bankkontorsservrarna göras före man kan ta servrarna i bruk. Testningen görs på huvudkontoret med hjälp av en server-prototyp. Prototypen tas också i testbruk för att testa att den fungerar och att klienterna kommer åt både information och databaser. Om problem uppstår kommer dessa att elimineras i detta testskede.

6.1 Prototyp

På Aktias huvudkontor har man använt en prototyp av en IBM System x3200 M3 server, som senare blir en bankkontorsserver. Eftersom ett Aktia kontor stängdes fick man därifrån en server, som är identisk med de servar som bankkontoren kommer att använda.

På prototypen har man kört tiotals installationer genom SCCM för att testa att installationsmiljön går igenom utan problem. Vid nästan varje installation under de tio första installationerna dök ett eller flera problem upp. Vid varje problem har man varit tvungen att göra en problemsökning av felen som uppstått.

Det första felet som uppstod vid uppgiftssekvensen var att få hårddiskpartitionerna krypterade före de egentliga installationsprocesserna (se Fig. 14).



Figur 14. Ett utdrag ur en loggfil från SCCM

De andra felen var att vissa bankkontorsprogram inte hade installerats fullständigt på grund av att en Windowsfunktion saknas.

För att söka problemen har man med hjälp av loggar i installationshanteringsverktyget SCCM kunnat hitta var och när i installationsprocessen ett fel har uppstått.

Eftersom det visade sig att det inte var möjligt att få kontroll över TPM-chippet med SCCM:s uppgiftssekvens, försökte man få kontroll över chippet med en annan metod. Ett ”PowerShell”-skript som skapades av en programmerare på Aktia lades in i uppgiftssekvensen för att försöka få kontroll över TPM-chippet. I skriptet försökte man aktivera TPM-chippet i Windows, men det gav samma oönskade resultat som uppgiftssekvensen, d.v.s. det tillät inte administratören att få kontroll över TPM-chippet. För att kunna kryptera en hårddiskpartition krävs det att man har kontroll över TPM-chippet. Efter att ha använt dessa två olika metoder drog man slutsatsen att TPM-chippet enbart går att kontrolleras via BIOS:en, vilket betyder att en IT-administratör bör vara fysiskt närvarande vid servern/datorn. Detta i sin tur betyder att hela installationsprocessen för varje bankkontorserver kommer att kräva mera tid.

Testarna fann också en orsak till att bankkontorsprogrammen inte installerades. Det visade sig bero på att en Windows-funktion, *Microsoft .NET Framework 3.5* inte var installerad på förhand. Bankkontorsprogrammen kräver att denna Windows-funktion redan är installerad.

6.2 Ibruktagande av en bankkontorsserver

Ibruktagandeprocessen av en bankkontorsserver är egentligen mycket enkel. Det första steget som görs då man tar i bruk en bankkontorsserver är att koppla den till Aktias kontorsnät. Då den är kopplad kan dess serveroperativsystem startas upp. Bankkontorsservern har egentligen ingen större uppgift än att fungera som en fil-server för bankkontorsanvändarna i fråga och lagra data i SQL-databaserna för bankkontorsprogrammen som använder sig av dem. Då bankkontorsservern startas upp, startas också SQL-servern och de andra databasprogrammen automatiskt. Eftersom dessa program är satta som tjänster i Windows, är det möjligt att färdigt konfigurera dem så att dessa tjänster startas upp automatiskt vid uppstart av serveroperativsystemet.

Då server-prototypen togs i bruk förekom det inga problem. Alla problem eliminerades redan under testningsskedet vilket var vad man strävade efter. I testmiljön användes några bankkontorsklienter som var kopplade i samma kontorsnät som server-prototypen. Server-prototypen hade nätskivor som man gjorde synliga för resten av kontorsnätverket. På detta sätt kunde man se om bankkontorsklienterna kunde komma åt filerna på server-prototypens nätskivor. Filåtkomsten för klienterna visade sig att inte vara något problem. Det slutliga steget var att se att databaserna fungerade. För att se till att bankkontorsklienterna kunde ansluta sig direkt till databaserna kontrollerade man helt enkelt om klienten fick en anslutning till databasen. För att få ut information från en databas användes ett bankkontorsprogram, som kräver att en databas finns ansluten. Eftersom informationen tas från databasen går det därefter att redigera informationen i själva programmet.

7 DISKUSSION OCH SLUTSATSER

Efter att ha läst mycket teori kom jag fram till att installationer samt konfigurationer av Windows Server 2008 R2 kunde automatiseras mycket långt och enkelt genom att använda installationshanteringsverktyget SCCM. Jag fortsatte att läsa teorin angående SCCM och hur det används. Efter att ha fått en klar uppfattning om hur installationshanteringsverktyget fungerar, förstod jag hur jag skulle förverkliga en automatisering av serverinstallationer.

Genom att i SCCM skapa en uppgiftssekvens som innehöll installationsprocesser av serveroperativsystem, drivrutiner, funktioner och programvara, kunde jag sammanslå de olika valda processerna till endast en större process, som automatiskt sköter alla installationer. Med hjälp av uppgiftssekvensen kunde jag sedan automatisera de valda processer som ingick i den. Om man jämför med manuella installationer av processerna som bör göras en i gången och som kräver både användarresurser och tid är SCCM:s uppgiftsekvens en mycket snabbare och automatiserad lösning.

Automatiseringen av installationerna har gått ganska långt enligt planerna. På vägen förekom det dock ett större hinder vilket gjorde att en process inte gick helt som planerat. Problemet gällde krypteringen, jag fick inte hårddiskspartitionerna krypterade före själva installationsprocesserna satte igång. Som jag tidigare skrev måste krypteringen först vara aktiverad i Windows för att sedan kunna kryptera hårddisken. Då jag försökte aktivera krypteringen i Windows genom SCCM.s egna funktion, misslyckades det. Därefter försökte jag aktivera krypteringen med ett PowerShell-skript som gjorts av en programmerare på Aktia, men det misslyckades också. Efter mycket forskande hittade jag orsaken till varför jag inte fick förhandskrypteringen gjord enligt planen. Det visade sig att denna modell av IBM-servern hade TPM-chippet inaktiverat enligt standardinställningen i BIOS. Detta betydde att jag inte lyckades få kontroll över av TPM-chippet genom SCCM, utan enda möjligheten var att aktivera chippet manuellt i BIOS:en. Därefter först blev det möjligt att aktivera krypteringen i Windows. Detta betyder att jag var tvungen att göra hela krypteringen manuellt efter att installationsprocesserna var klara. Det gick alltså inte att utföra en fullständig automatisering på grund av att krypteringen inte kunde automatiseras utan måste göras manuellt.

Hanteringen av underhåll handlar enbart om säkerhetskopieringar och uppdatering av bankkontorsservrar. I hanteringen av underhållet kunde säkerhetskopieringarna automatiseras enligt planen. Tack vare programmet som användes kunde man enkelt hantera tidpunkten för säkerhetskopieringen. Återställning av filer fungerade som önskat, man skrev in namnet på de förlorade filerna eller katalogerna och därefter valde man datum och tidpunkt i sökningslistan.

Beträffande uppdateringarna var själva nerladdningen och installeringen av dem automatiserade med hjälp av *Windows Update*. I uppdateringsprogrammet var det möjligt att automatisera hela uppdateringsprocessen, men i stället för att låta *Windows Update* hantera uppdateringarna helt automatiskt följdes Aktias datasäkerhetspolicy. Enligt den väljer IT-administratören själv vilka uppdateringar som skall installeras, eftersom det finns sådana som inte anses vara nödvändiga. Uppdateringsprocessen var alltså inte helt automatiserad, men man undvek datasäkerhetsrisker som kan orsakas av korrumperad uppdatering.

Underhållet var egentligen den enklare delen eftersom där inte dök upp några problem, vilket gav mig mera tid för att finslipa den automatiserade installationsmiljön.

Slutresultatet av det här examensarbetet är en nästan helt automatiserad miljö för serverinstallationer som används för ett projekt på Aktia. Med denna miljö har man kunnat spara mycket värdefull tid.

Med hjälp av installationshanteringsverktyget SCCM gick det att automatisera bankkontorsserverinstallationerna rätt långt, förutom någon enstaka installationsprocess som man var tvungen att göra manuellt. Underhållet av säkerhetskopieringen kunde hanteras automatiskt medan uppdateringarna gjordes manuellt p.g.a. en datasäkerhetspolicy.

KÄLLOR

ArsTechnica. 2012, First look: Windows Server 2012 brings the cloud down to earth, [www]. publicerad 4.9.2012.
Tillgänglig: http://arstechnica.com/information-technology/2012/09/windows_server_2012_first_look Hämtad 18.2.2013

Bleepingcomputer.com. 2012, Understanding and Using Firewalls, [www]. publicerad 20.4.2004.
Tillgänglig: http://www.bleepingcomputer.com/tutorials/understanding-and-using-firewalls/#intro Hämtad 3.4.2013

Indiana University. 2013, In Active Directory, what is an organizational unit?, [www]. publicerad 6.4.2013.
Tillgänglig: http://kb.iu.edu/data/atvu.html Hämtad 16.4.2013

Lehtinen, Rick; Russel, Deborah; G.T, Gangemi, Sr. 2006, *Computer Security Basics, 2nd Edition*, 2 uppl., Sebastopol: O'Reilly Media, Inc, 312 s.

Hannifin, Dustin. 2010, *Microsoft Windows Server 2008 R2 The Administrator's essential Reference,* 1 uppl., Burlington: Syngress, s.17-72.

Meyler, Kerrie; Holt, Byron; Oh, Marcus; Sandys, Jason; Ramsey, Greg. 2012, *System Center 2012 Configuration Manager Unleashed*, 1 uppl., Indianapolis: Sams Publishing, 1360 s.

Microsoft Developer Network. 2007, Windows Server 2008 System Requirements, [www]. publicerad 24.9.2007.
Tillgänglig: http://msdn.microsoft.com/en-us/windowsserver/cc196364.aspx Hämtad 13.3.2013

Microsoft Developer Network. 2012, Disc Formats (Windows), [www]. publicerad 26.10.2012.
Tillgänglig: http://msdn.microsoft.com/enus/library/windows/desktop/aa364836%28v=vs.85%29.aspx Hämtad 16.3.2013

Microsoft. 2009, Windows 7 and Windows Server 2008 R2 Timelines Shared at Computex, [www]. publicerad 2.6.2009.
Tillgänglig: http://www.microsoft.com/en-us/news/features/2009/Jun09/06-02SteveGuggenheimer.aspx Hämtad 3.3.2013

Microsoft System Center. 2012, Run Advertised Programs Overview, [www].
Tillgänglig: http://technet.microsoft.com/en-us/library/bb633225.aspx
Hämtad 4.3.2012

Microsoft System Center. 2012, Planning for Sites and Hierarchies in Configuration Manager, [www]. publicerad 1.1.2013.
Tillgänglig: http://technet.microsoft.com/en-us/library/gg712681.aspx Hämtad 17.3.2013

MSI. 2011, What is the BIOS and what does it do?, [www], publicerad 17.3.2011
Tillgänglig http://forum-en.msi.com/faq/article/what-is-the-bios-and-what-does-it-do Hämtad 22.4.2013

Netgear. 2013, What is VPN (Virtual Private Networking)?, [www]. publicerad 28.1.2013.
Tillgänglig: http://kb.netgear.com/app/answers/detail/a_id/1128/~/what-is-vpn-%28virtual-private-networking%29%3F Hämtad 18.4.2013

Oracle. 2013, *Understanding PXE Booting and Kickstart Technology*, [www]. Tillgänglig: http://docs.oracle.com/cd/E24628_01/em.121/e27046/appdx_pxeboot.htm#BABJDJAJ Hämtad 2.5.2013
Russel, Charlie. och Zacker, Craig. 2010, *Introducing Windows Server 2008 R2,* Redmond, Washington: Microsoft Press, 204 s.

SCCM Basics & FAQ. 2010, SCCM Basics & FAQ, [www]. publicerad 28.3.2010 Tillgänglig: http://sccmfaq.blogspot.fi/ Hämtad 6.5.2013

SearchNetworking. 2005, Preboot Execution Environment (PXE), [www]. Tillgänglig: http://searchnetworking.techtarget.com/definition/Preboot-Execution-Environment Hämtad 2.5.2013

SearchSecurity. 2005, Secure Shell (SSH), [www]. Tillgänglig: http://searchsecurity.techtarget.com/definition/Secure-Shell Hämtad 18.4.2013

Server & Cloud Blog. 2012, System Center 2012 Configuration Manager SP1 Beta and Windows Intune Update, [www]. publicerad 10.9.2012. Tillgänglig: http://blogs.technet.com/b/server-cloud/archive/2012/09/10/system-center-2012-configuration-manager-sp1-beta-and-windows-intune-update.aspx Hämtad 16.3.2013

VPN4ALL. How does the VPN technique work? How does a VPN tunnel work?, [www]. Tillgänglig: http://www.vpn4all.com/userportal/knowledgebase.php?action=displayarticle&id=530 Hämtad 18.4.2013

Windows. 2013, Windows Trusted Platform Module Management Step-by-Step Guide, [www].

Tillgänglig: http://technet.microsoft.com/en-us/library/cc749022%28v=ws.10%29.aspx Hämtad 22.4.2013

Windows. 2013, Säkerhetskopiera och återställa: vanliga frågor, [www]. Tillgänglig: http://windows.microsoft.com/sv-se/windows-vista/back-up-and-restore-frequently-asked-questions Hämtad 29.4.2013

Windows Dev Center. 2012, So What Is Active Directory?, [www]. publicerad 26.10.2012.
Tillgänglig: http://msdn.microsoft.com/en-us/library/windows/desktop/aa746492%28v=vs.85%29.aspx Hämtad 16.4.2013

Windows Server Blog. 2008, Announcing Windows Server 2008 R2!, [www]. publicerad 28.10.2008.
Tillgänglig: http://blogs.technet.com/b/windowsserver/archive/2008/10/28/announcing-windows-server-2008-r2.aspx Hämtad 18.2.2013.

Windows Server. 2008, How PXE Requests Work, [www]. *publicerad 8.5.2008. Tillgänglig: http://technet.microsoft.com/en-us/library/cc725614%28v=WS.10%29.aspx Hämtad 9.4.2013*

Windows Server. 2012, Server Core and Full Server Integration Overview, [www]. publicerad 29.2.2012.
Tillgänglig: http://technet.microsoft.com/en-us/library/hh831758.aspx Hämtad 14.3.2013

Windows Server. 2012, Group Policy Overview, [www]. publicerad 29.2.2012.
Tillgänglig: http://technet.microsoft.com/library/hh831791 Hämtad 6.4.2013

Windows Server. 2013, Windows Server Update Services, [www].
Tillgänglig: http://technet.microsoft.com/en-us/windowsserver/bb332157.aspx
Hämtad 28.3.2013

wiseGEEK. 2008, What is a Disk Image?, [www].
Tillgänglig: http://www.wisegeek.org/what-is-a-disk-image.htm Hämtad 7.3.2013