Driftövervakning av Windows och Linux/Unix Servrar

MIKAEL FALK
och
MATIAS FERNANDEZ KARLSSON

KTH Information and
Communication Technology

Bachelor of Science Thesis
Stockholm, Sweden 2008

COS/CCS 2008-13

Driftövervakning av Windows och Linux/Unix Servrar

Slutrapport

Dokumenttitel	Dokumentnamn		Skapades
Slutrapport	Slutrapport.doc		2008-06-03
Dokumentansvarig och dokumentförfattare		Version	Sparades
Mikael Falk och Matias Fernandez Karlsson		1	2008-06-30

Sammanfattning

Ju fler servrar, med olika konfigurationer och olika system, som blir medlemmar i ett nätverk, desto svårare och osmidigare blir det att övervaka nätverksmiljön. Men om man använder sig av ett övervakningssystem, som tar emot information från flera servrar, blir det lättare att få en överblick om hur allt fungerar och samtidigt som det går snabbare att få information om felmeddelanden, som man sedan kan åtgärda.

I detta dokument tar vi upp olika typer av övervakningssystem som finns ute på marknaden idag, våren 2008. Bland dessa hittar vi t.ex. SCOM 2007, BigBrother, Nagios och Mon. Vi har inte begränsat oss till ett specifikt operativsystem, utan vi tar upp övervakningssystem som passar till Windows och/eller Linux/Unix.

Utifrån den information vi hittat om varje övervakningssystem och de kriterier som Valderas Consulting AB vill att systemen ska uppfylla, har vi valt ut tre stycken övervakningssystem som vi tycker passar bäst. Dessa system har vi sen, ett och ett, testat i ett litet nätverk där vi utsätter det för en del scenarior som kan hända ute på företag som t.ex. trasig anslutning, för full hårddisk och kraschat operativsystem.

De tre övervakningssystem vi tyckte höjde sig över mängden var SCOM 2007, Big Brother 4 och Nagios. Efter att ha testat vart och ett av dessa tre tycker vi att Nagios är det klart bästa. Det är användarvänligt i installationen, konfigurationen samt i övervakningen. En annan stor fördel med Nagios är att det är gratis, dvs. open source. Om ens datormiljö enbart innehåller Windows-datorer och en domän, passar SCOM 2007 bäst, då Nagios måste installeras på en Linux/Unix-dator. Big Brother 4 var bra det med, men faller bort pga. att det inte är gratis, färre testmöjligheter på nätverket och fungerade inte helt bra med att övervaka Linux/Unix-datorer.

Abstract

The more servers you install in your network, which utilize different types of configurations and operative systems, the harder it gets to monitor the entire network. But if you use a monitoring system to monitor the network it will get much simpler. The monitoring system gathers information from all of your hosts and servers on your network and warns you if something is wrong or not working properly.

In this document we will describe many of the monitoring systems that are out on the market today, spring 2008. Among these monitoring systems are: SCOM, BigBrother, Nagios, and Mon. We have not focused on a single operating system, but rather we have gathered information about monitoring systems that can be installed on Windows and/or Linux/Unix environments.

From the information, which we have gathered about each monitoring system, and the criteria that Valderas Consulting AB gave us, we have focused on three monitoring systems that seem to be the best. We have installed these systems, one at a time, on a server that's part of a small network, and run several tests, such as failure to the network and an operating system crash, to see how each system handles these failures in a real life environment.

We thought that SCOM 2007, Big Brother 4, and Nagios were the best amongst the systems we looked at. After testing each one of them, we think that Nagios is the best. It is user-friendly regarding installation, configuration, and monitoring. One big advantage with Nagios is that it is free of charge, open source. If you have a computer-environment that contain computers with Windows, and you only have one domain, then SCOM 2007 is the system for you to choose, because Nagios only works if it is installed on a computer with Linux/Unix. Big Brother 4 was also ok, but it had some issues. It is not free of charge, and it did not have as many tests, to run on the network-units, as Nagios. We also had some problem, with Big Brother 4, regarding monitoring computers with Linux/Unix.

Innehållsförteckning

1. Inledning

Detta dokument är en slutrapport av examensarbetet som vi, Matias Fernandez-Karlsson och Mikael Falk, utfört på företaget Valderas Consulting, våren 2008.

Syftet med examensarbetet och denna slutrapport är att ta fram information om alla de olika övervakningssystem för servrar, som finns ute på marknaden. Efter insamlandet av information ska vi, utifrån vissa fördefinierade kriterier, bestämma oss för vilka tre system som verkar vara bäst anpassade för just detta ändamål. Dessa tre övervakningssystem ska vi sen installera i ett litet nätverk, som vi satt upp här på företaget, och utföra en mängd tester för att se hur vart och ett av systemen reagerar på en del tänkbara fel som kan uppstå på ett företag.

Ju fler servrar, med olika konfigurationer och olika system, som blir medlemmar i ett nätverk, desto svårare och osmidigare blir det att övervaka nätverksmiljön. Men om man använder sig av ett övervakningssystem som tar emot information från flera servrar, blir det lättare att få en överblick hur allt fungerar och samtidigt som det går snabbare att få information om felmeddelanden, som man sedan kan åtgärda.

Målgruppen som vårt examensarbete och denna slutrapport vänder sig till är personer som på ett eller annat sätt är inblandade i vårt arbete. Detta innefattar författarna själva, handledare, examinator och andra intressenter. Självklart vänder sig detta dokument även till utomstående som inte har med examensarbetet att göra, utan som bara är intresserade av ämnet i sig. Kanske funderar de själva på att införa ett övervakningssystem hos sig och undrar vilket som passar dem.

Version	Datum	Anmärkning	Författare	Granskad av
1.0	2008-06-03	Preliminär slutrapport skapad	MFK MF	Oss själva
2.0	2008-06-23	Preliminär slutrapport klar	MFK MF	Gerald ”Chip” Maguire
3.0	2008-06-26	Slutrapport klar	MFK MF	Oss själva och G. Maguire
4.0	2008-06-30	Slutrapport helt klar	MFK MF	Oss själva

2. Kriterier för val av övervakningssystem

2.1. Användarvänlighet

- Det första kriteriet vi har är att det ska vara ett grafiskt gränssnitt på övervakningen.
- Man ska lätt kunna få en bra överblick över hela nätverket och dess hälsa, men även kunna få mer information om en specifik enhet.
- Det ska vara enkelt att lägga till nya enheter i nätverket, som t.ex. ny server, skrivare, etc. Det ska självklart även vara lätt att ta bort enheter som inte ska vara kvar på nätverket längre.
- Informationen om larm som inträffar, ska vara lätt att få tillgång till, och larmen ska vara enkla att tyda. Larmen ska helst bara ange själva rotproblemet, inte följdfelen som uppstår på grund av huvudproblemet och som förmodligen löser sig då rotproblemet åtgärdats. Exempel på detta är att om nätverket förlorar kontakt med en switch, vill vi endast ha information om den, inte om alla enheter som är kopplade bakom switchen, för dessa kommer ju självklart också ha tappat kontakten med resten av nätverket. Det finns olika ”paket” som hjälper till att hitta rotproblemet, som t.ex. System Management Arts (SMARTS) InCharge[16].
- Man ska själv kunna välja hur man vill få larmen presenterade för sig, exempelvis via mail, sms eller pop-upp rutor. Det ska även gå att välja så att rätt person/personer får rätt larm.

2.2. Installation/konfiguration

Installation och konfiguration av programvara ska inte vara för komplex. Installationen kan få vara krånglig, om alldagligt underhåll som att lägga till/ta bort enheter blir lättare. Om den dagliga konfigurationen är allt för svår kan det leda till att underhåll inte görs lika ofta, eller kanske inte görs alls.

2.3. Stöd för flera olika operativsystem

- Eftersom Valderas Consultings kunder framförallt använder sig av Windowsservrar och Linuxservrar, så ska vi välja ut minst ett övervakningssystem till varje operativsystem. Det bästa skulle vara om det finns ett övervakningssystem som är oberoende av vilken plattform som körs på servern.
- Det underlättar om övervakningssystemen kan övervaka flera olika operativsystem, så att det inte behövs ett övervakningssystem för Windowsenheterna och ett annat system som övervakar Linuxenheterna.

2.4. Antal enheter

Helst ska det inte vara ett begränsat antal enheter som kan övervakas. Det vill säga övervakningssystemet ska kunna övervaka ett nätverk, oberoende av dess storlek.

3. Övervakningssystem

I detta kapitel hittar ni en kortfattad presentation om några av de olika övervakningssystemen som finns ute på marknaden idag, våren 2008. Sist i kapitlet finns det en utförligare beskrivning av tre stycken övervakningssystem, de tre som vi kom fram till verkade bäst anpassade för Valderas Consulting AB. De utvalda systemen har vi testat ett och ett, i ett litet nätverk vi satte upp på Valderas, för att se hur de funkar ”in real life”. De tre övervakningssystemen vi valde är Microsoft Systems Center Operations Manager 2007, Quest Software’s Big Brother 4 och Nagios. Vi kommer att ta upp en mängd olika delar vad gäller varje övervakningssystem, som t.ex. systemkrav, installationsprocess och allmänna inställningar dvs. hur vi installerade dem och hur vi fick dem att fungera med övervakningen av ett gäng datorer/servrar.

3.1 Presentation av de olika övervakningssystemen

3.1.1. Microsoft Systems Center Operations Manager (SCOM)

System Center Operations Manager 2007[1], i texten förkortat till SCOM, är ett övervakningssystem som förenklar övervakningen och säkerheten av datornätverk och applikationer. SCOM varnar t.ex. direkt då ett problem uppstår och tillhandahåller ett svar på en passande lösning. Tanken med SCOM är att man lägger in en ”agent” på den utrustning, t.ex. en dator, man vill ha övervakad. Beroende på vad man sedan vill ha övervakat kollar agenten igenom datorn på alla tänkbara platser där fel kan uppstå, som t.ex. i Windows Event-log. Om ett fel uppstår skickas ett meddelande från agenten till den centrala SCOM -servern, som i sin tur skickar ut ett meddelande till den person som är ansvarig, detta meddelande kan vara en dialogruta som kommer upp på skärmen, ett mail, eller ett sms till personens mobil. SCOM tillhandahåller även så kallade ”Management packs” för många olika applikationer, även sådana som inte är tillverkade av Microsoft. Dessa ”management packs” används för att övervaka applikationer som är viktiga för ett företag, typ Outlook eller liknande. Om man har gjort en egen applikation som man vill ha övervakad, kan man ladda ner en mall på hur man gör ett eget ”management pack” på Microsofts hemsida.

3.1.2. Op5 Network Management Suite

Op5 Network Management Suite[2] är ett open source-baserat övervakningssystem som består av tre olika produkter som är till hjälp då man övervakar nätverk. Dessa tre är Op5 Monitor, Op5 Statistics och Op5 LogServer.

Med Op5 Monitor kan man övervaka all tänkbar IT-utrustning, passar alla produkter oavsett tillverkare. Övervakningen sker via ett webbgränssnitt, vilket betyder att inga klienter krävs. Exempel på saker som kan övervakas är servrar, skrivare, mailtjänster och virusprogram. Det går även att mäta hur mycket last en lina utsätts för på en specifik plats i nätverket. Op5 Monitor kollar hela tiden statusen för allt som den ska övervaka och larmar direkt då något händer. Larmet skickas ut till alla de personer som angetts som kontaktpersoner då något händer, detta sker antingen via SMS eller via e-post. Op5 är ett mycket intelligent system vad gäller larmhantering. Om det visar sig att en central router slutat fungera, skickas bara ett meddelande om denna specifika router, det skickas inget om att alla enheter som är kopplade bakom routern också tappat kontakten.

Op5 Statistics visar information om nätet uppdelat i timmar, dagar, veckor, månader och år. Detta är utmärkt då man ska planera och dimensionera sitt nät.

Op5 LogServer sparar alla loggar på en central punkt, för att lättare kunna granska och lagra.

Operativsystem som stöds är RedHat Linux(32 bitars) och CentOS(32 bitars). Har man en vanlig 3GHz dator så kan man som mest övervaka 1000 klienter och 5000 tjänster.

3.1.3. BMC Performance Manager

Det finns många olika typer av BMC Performance Manager[3] ute på marknaden, så beroende på vad det är du vill övervaka så kan du välja en som passar dig.
”BMC Performance Manager for servers” är till för dem som vill ha ett bra och pålitligt system för att övervaka sina servrar.

Övervakningen med BMC Performance Manager är inte beroende av ett speciellt operativsystem, utan man kan övervaka Windows, Linux och Unixmiljöer utan problem.
Men hjälp av BMC Performance Manager kan man ha remoteövervakning av servrar, webbservrar, loggfiler och databaser, detta sker utan att man behöver installera någon mjukvara på den övervakade maskinen.

Det finns olika huvuddelar inom BMC Performance Manager. Server Monitoring är precis som det låter, här övervakar man tillståndet på sin server, man kan även se sin servers prestanda och hur servern mår. I Process Monitoring ser man vilka processer som körs och hur mycket prestanda var och en kräver. Man kan ställa in så att om en process använder sig av för mycket CPU en längre tid, kan systemet automatiskt stänga ner just den processen. Man kan även stänga av processer som slutat fungera och laga dem så att allt är ok igen. Log File Monitoring tillåter att man letar igenom log-filerna på datorn och utifrån dem bestämmer rätt ”lagningsmetod”. Active Directory Operations Monitoring hjälper till att hålla koll på Active Directory. Windows Event Log Monitoring gör det möjligt för administratören att enkelt skapa olika filter för olika typer av alarm, som baserar sig på typ av event, källan, ID, användare och kategori.

3.1.4. Tadcom AB’s NetZonar

Tadcom AB’s NetZonar[4] är en färdig produkt som körs på egen hårdvara, för att lösa övervakningsproblemet. Övervakningen sker via ett webbgränssnitt, där fokus har lagts på att ge en överblick av nuläget. När man installerar NetZonar placeras hårdvaran på en central punkt i nätverket. Man kan lätt lägga till alla nätverkskomponenter man vill ha övervakade och även vilken typ av fel som ska larmas. Övervakningen sker via förfrågningar som skickas ut vid jämna mellanrum, för att säkerställa att allt fungerar som det ska. Om det visar sig att något är fel utlöses ett larm. Larmet skickar då ett meddelande till rätt person, antingen som sms, e-post eller röstuppringning. Meddelandena ökar i mängd beroende på vad för typ av larm som uppstått. Ju allvarligare fel, desto fler larm skickas.

3.1.5. Hyena

Hyena[5] förenklar och centraliserar nästan alla dagliga administrationsuppgifter. Den använder sig av en Explorer-liknande arbetsmiljö för hanteringen av användare, grupper, shares, domäner, datorer, tjänster, utrustning, events, filer, skrivare och processer.

Hyena kan användas på Windows NT/2000/XP/Vista klienter för att hantera Windows NT/2000/XP/Server 20003 installationer. Hyena har även stöd för Active Directory integration och Microsoft Access baserad rapportering.

För integration med Windows NT/XP/200x Event hanterare och Microsoft Management Console har Hyena sin egen event-hanterar-funktion som kan få vilken server/dators event log via context menyn. Det finns en mängd avancerade alternativ som kan göras med event-loggen, som t.ex. se flera eventloggar från flera olika datorer samtidigt, filtrera dem på olika sätt som efter datum, event ID, event typ, kategori och spara undan dem och se dem vid ett senare tillfälle.

3.1.6. Microsoft System Center Essentials 2007

Microsoft System Center Essentials 2007[6] används av IT-avdelningen på medelstora företag för att mer effektivt säkra, uppdatera, övervaka och felsöka sina nätverk från ett enda fönster.

Essentials kan maila information om nätverkets status till berörda personer, då ett fel uppstår. Det går även att få ett mail innehållande en helhetsbild av nätverkets hälsa varje morgon, oavsett om något är fel eller inte.

En Essentials-installation kräver Windows server 2003 med Active Directory, SQL-server 2005 och IIS 6.0.NET-framework.

3.1.7. Quest Software's Big Brother 4

Quest Software's Big Brother 4[7] är ett webb-baserat övervakningssystem för övervakning av ditt nätverk samt ditt system. Big Brother kan övervaka alla tänkbara delar i ett nätverk, så som routrar, switchar, skrivare, datorer, applikationer, databaser och servrar (fungerar på alla typer av servrar, Windows, Linux och Unix). Det finns två olika typer av programvara till Big Brother, ett för Windows och ett annat för Linux/Unix.

Det går alldeles utmärkt att ändra om i Big Brother, allt efter egen smak, så att man endast får med exakt de funktioner man själv vill. Big Brother är ett väldigt enkelt övervakningssystem att administrera och enkelt att komma igång med.
För att visa hur system och nätverk mår, visar Big Brother det på en webbsida. Statusen visualiseras med hjälp av ett färgkodnings-schema där man ser en viss färg beroende på hur en viss del mår.

Om det visar sig att ett fel uppstår, startas ett larm. Detta larm, där problemet beskrivs, skickas direkt, till ansvarig person, antingen som mail, sms eller personsökare, allt beroende på hur man själv vill ha det.

3.1.8. Intellipool AB's Network Monitor

Intellipool Network Monitor[8] (INM) är ett system för övervakning, notifiering och loggning av servrar utan att man behöver installera någon agent på den övervakade servern. INM installeras på en Windows dator och kan övervaka 14 olika operativsystem som Windows, Linux, Solaris och BSD. Enligt tillverkaren tar det tio minuter från det att man börjar installera tills det att man är klar och redo att börja övervaka. Man kan antingen göra ett egetskrivet test i INM för testning eller använda sig av något av de olika övervakningsmomenten som övervakar t.ex. Directory services, loggar, processer och

skript. Väljer man att övervaka loggarna kan man verifiera att processer körs, läsa från en log fil efter en viss text sträng eller ta emot syslog meddelanden.
När ett alarm sker kan man sätta den att visa larmet eller köra ett litet program.

3.1.9. ServersCheck Monitoring

ServersCheck Monitoring[9] är ett Windows-baserat övervakningsverktyg för övervakning, rapportering och notifiering av nätverkssystem. Man kan både övervaka Windows och Linux system utan att något behöver installeras på dem.
ServersCheck har över 60 olika ”checks” man kan välja bland, som övervakning av olika enheter på vilken TCP-port som helst eller göra en databas kontroll (ODBC, Oracle, My-SQL). Ett av ”checken” man kan göra är EVENTLOG, den meddelar administratören om när ett error hittats i event-loggen. När de händer kan man få de skickat till sig via mail eller sms.

3.1.10. Spong – Systems and Network Monitoring

Spong[10] är ett open source-baserat övervakningssystem för Linux/Unix.
Detta ”package” är skrivet i Perl och är ett mycket enklare övervakningssystem än t.ex. Tivoli och UniCenter. Men tanken var inte heller att konkurrera med alla de stora bolagen, utan tanken var att det skulle vara ett användarvänligt och någorlunda enkelt system.
Med hjälp av Spong kan man övervaka i princip allt som kan tänkas finnas i ett nätverk, som t.ex. routrar, servrar, datorer, skrivare etc. Man tillhandahåller även en klientbaserad övervakning av CPU, hårddiskarna, loggen osv. Övervakning kan även ske på olika typer av nätverkstjänster, så som SMTP, HTTP, ping, DNS mm.
Om ett problem uppstår skickas ett meddelande, i form av ren text eller via ett webb-baserat interface, till ansvarig person.
En utförlig lista med information, som innehåller alla tänkbara problem som kan uppstå, finns tillgänglig, så att det ska gå snabbt och enkelt att lokalisera och lösa problemet. Det är även möjligt att se tidigare problem samt hur man löste dessa.

3.1.11. Netplex’s SNIPS (Även kallat NOCOL)

SNIPS[11] (System & Network Integrated Polling Software) är ett Unixbaserat övervakningssystem för nätverksenheter. SNIPS kan övervaka DNS, NTP, TCP, webbportar, hosts, syslogg, radius servrar, osv.
SNIPS fungerar så att man har flera ”monitors” man övervakar, till dem sätter man egna tröskelvärden som sedan avgör om ett larm utlöses. När ett larm går kan den skicka en meddelande eller ett mail till den berörda personen.
SNIPS tillåter att flera tittar och övervakar samma data som tas in, istället för att varje användare behöver starta en egen ”monitor” som tar in samma sak, ifall de är så att man kan använda sig av samma information på olika sätt.

3.1.12. Linux System Group’s Mon

Mon[12] är ett enkelt Linuxbaserat open source-verktyg som hjälper till att övervaka tillgängligheten på olika tjänster och den ger ett meddelande när egenbestämda händelser sker. De olika tjänsterna kan vara vad som helst som man kollar på med ett ”övervaknings”-program. Ingen av de tester som körs hör till Mon, de är utomstående program som t.ex. ett skript som testar att pinga någonting. Att alla tester är utomstående program gör att Mon är väldigt enkelt och expanderbart. För att lägga till ett nytt test eller alarm behöver man inte ändra i någon kod, det enda man behöver göra är att skriva skriptet och referera det till Mons konfigurationsfil.

3.1.13. GFI Software's GFI EventsManager

GFI EventsManager[13] är en Windows-programvara som samlar in information om alla enheter som använder sig av Windows event-log, W3C och Syslog till en central plats. Detta förenklar eventuell backup.
GFI använder sina kriterier för att filtrera bort onödig data för att sedan presentera informationen på ett användarvänligt sätt, alltså översätter den kryptisk information från logg filen och gör att de går fortare och lättare att förstå vad som händer. Man kan välja ut kriterier för när GFI ska meddela en om att något har hänt. Detta meddelande kan skickas på flera olika sätt, via mail, pop-upp ruta på skärmen, nätverksmeddelande eller sms.

3.1.14. up.time 4

up.time[14] är en webb-baserad applikation till alla tillgängliga plattformar som övervakar allt tänkbart i ett datanätverk, så som servrar, databaser och även applikationer.
För att få en så bra inblick som möjligt i sitt nätverk behöver man installera en agent på alla de servrar man vill övervaka. Gör man det samlas 120 olika värden in från var och en av servrarna och utifrån dessa skapas sen olika grafer som visar detaljerad information om varje enskild server. Information samlas in från nätverket hela tiden, vilket gör det möjligt för administratören att söka efter felaktigheter, redan innan de uppstått. Men up.time varnar självklart den ansvarige om något skulle hända. Varningen kan komma till administratören på flera olika sätt, beroende på hur personen själv vill ha det. Man kan få en pop-upp ruta på skärmen, ett mail eller ett meddelande.

Up.time tillhandahåller en mängd olika övervakningsverktyg, för att övervaka alla olika delar av nätverket. Det går t.ex. att se hälsan på sitt IT-nätverk i realtid. Här kan man även se nätverkets status de senaste 24 timmarna. En annan sak man kan få se är hur ens servrar mår, med hänsyn till hur mycket cpu som används, hur mycket internminne som används och hur mycket som är lagrat på de olika hårddiskarna. Vill man ha översiktlig information om hur nätverket mår kan man självklart få det. Här får man se grundläggande information om de olika servrarna, ledigt minne, cpu-användning etc.

3.1.15. Nagios

Nagios[15] är ett övervakningssystem som är designat för operativsystemet Linux och det är även open source. Övervakningen sker, bland annat, genom att du anger vad för något du vill övervaka, som t.ex. klienter eller tjänster. När du har angivit vad du vill övervaka kör Nagios återkommande tester för dessa. Upptäcker den något fel, skickas ett meddelande till ansvarig administratör, detta kan skickas som sms, mail eller snabbmeddelande. Förutom övervakning av olika klienter och nätverkstjänster har du även möjlighet att se nätverkets status, tidigare problem samt vilka noteringar som tidigare gjorts, i ett webb-interface.

4. Testmiljön

4.1. Beskrivning av miljön

För att det ska vara möjligt att avgöra hur de tre utvalda övervakningssystemen beter sig på riktigt, har vi satt upp ett mindre nätverk på Valderas Consulting AB. Vi blev tilldelade två stycken datorer, som vi använde som servrar. Dessa datorer kunde vi använda hur vi ville för att utföra våra tester på. Förutom de två datorerna vi fick av Valderas, använde vi även våra egna bärbara datorer samt ett par datorer vi virtualiserat med hjälp av programmet VMware Server, som går att ladda ner på sidan *http://www.vmware.com/download/server/*.

På de virtualiserade datorerna installerade vi olika operativsystem på var och en, för att se om övervakningssystemen klarade av att övervaka dem oavsett operativsystem. De operativsystem vi testat är Windows XP Pro, Windows Server 2003, Windows Server 2008, Windows Vista, Fedora Core 6, Ubuntu 8.04 Server, Free BSD, Solaris 10 och SUSE10. Vi har även testat ett par av dessa operativsystem, i huvudsak Windows Server 2003, på de båda servrarna också. Lördagen den 7 juni 2008 kraschade en av våra bärbara datorer, på vilken vi hade VMware installerat och virtualiserat tre stycken datorer. Om ni märker att det finns datorer med på någon bild som ni inte hittar i nätverket nedan, beror det alltså på att det är en av dem som försvann i kraschen. Eftersom detta skedde blev vi tvungna att installera VMware på en av våra hemdatorer, därav förklaringen till att det finns två stycken nätverk på bilden nedan.

4.2. Nätverket

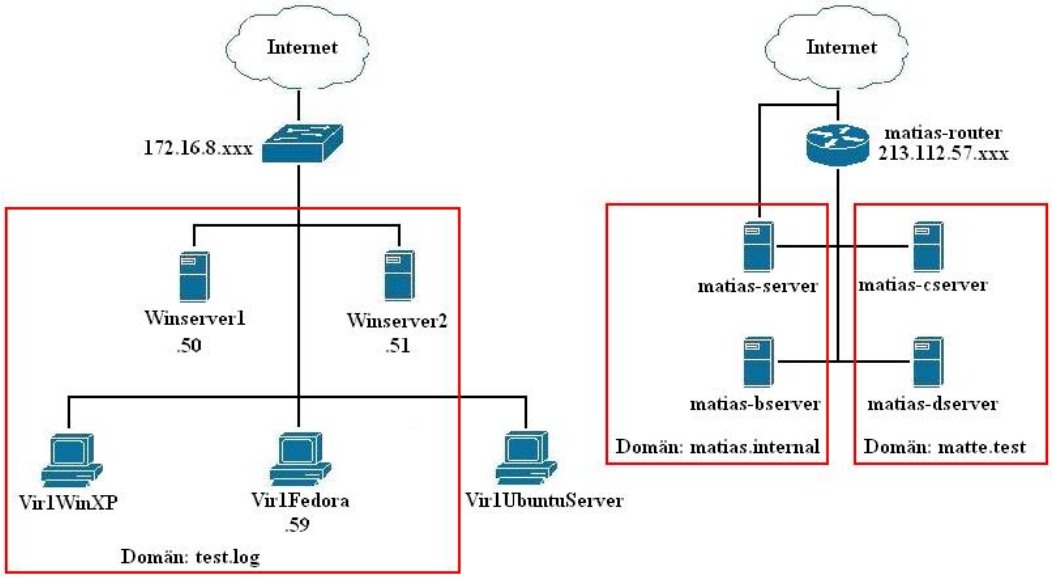

Fig.1 Bild föreställande vår testmiljö

På bilden föreställande nätverket kan ni se hur vår testmiljö såg ut. Denna bild är som nätverket såg ut då sista testet gjordes, det såg inte riktigt ut såhär förut, tack vare att en bärbar dator kraschade tidigare. Vi har även lagt till och tagit bort datorer allt eftersom, för att testa t.ex. om det går att övervaka alla typer av operativsystem, oavsett om datorn är medlem i en domän eller inte.

5. Omfattande presentation av SCOM, BB4 och Nagios

På Valderas Consulting AB blev vi tilldelade två stycken datorer som vi kunde få använda till att sätta upp ett litet nätverk på, för att kunna testa de olika övervakningssystemen ”in real life”.

5.1. Microsoft’s Systems Center Operations Manager 2007

5.1.1. Systemkrav

CPU:	1.8 GHz (Rek. 2.8 GHz)
RAM:	1 GB (Rek. 4 GB eller mer)

Hårddisk:	10 GB (Rek. 50 GB)
Operativsystem:	Windows Server 2003 SP1 eller SP2 (Edition-oberoende)
Mjukvara:	SQL Server 2005 SP1 eller SP2
	.NET Framework 2.0 och 3.0
	Microsoft Core XML Services (MSXML) 6.0
	Internet Information Services (IIS)
	ASP. NET

5.1.1.1. Begränsningar

Övervakad enhet	Rekommenderad gräns
Samtida Operations Konsoler	50
Agentdatorer per managementserver	2,000
Agentdatorer per gatewayserver	800
Agentlösa datorer per managementserver	25,000
Agentlösa datorer per managementgrupp	100,000

5.1.2. Installationsprocess för SCOM 2007 på Windows Server 2003

5.1.2.1. Det som behövs för en installation

För att kunna installera SCOM 2007 måste ni först göra en del saker innan ni börjar med själva installationen. Det första ni ska göra är att installera Windows Server 2003. När det är klart ska ni ladda hem och installera alla tillgängliga uppdateringar. Innan ni fortsätter till installationen av SCOM 2007 ska ni ändra IP-adresserna så att dessa är statiska. Det gör ni genom att gå till *Kontrollpanelen/Nätverksanslutningar/*. Sen högerklickar ni på den anslutningen ni har och väljer *Egenskaper*. Då kommer en ruta upp, *Egenskaper för anslutning*, där ska ni markera raden *Internet Protocol (TCP/IP)* och trycka på *Egenskaper*. Då kommer ytterligare en ruta upp, Egenskaper för Internet Protocol (TCP/IP). Ni ska där klicka i *Använd följande IP-adress* och sen fylla i er IP-adress, er nätmask och er Standard Gateway. Ni ska även klicka i *Använd följande DNS-serveradresser* och fylla i *Önskad DNS-server*. Nästa steg i denna förinstallation av SCOM 2007 är att installera Active Directory.

5.1.2.2. ”För-koll”

När ni ska installera Microsoft System Center Operations Manager är det rekommenderat att ni gör en s.k. ”för-koll” för att verifiera att datorn har alla program och tjänster som SCOM kräver. För att göra en ”för-koll” trycker ni, när ni startat installationen, på *Check Prerequisites*. När den är klar, vilket ska vara ganska direkt, kommer en lista upp med varningar och errors som behöver fixas till. För varje varning och error som kommer upp får man reda på vad som behövs ändras på.

5.1.2.3. Skapa grupper och konton

Om ”för-kollen” är klar, inga varningar eller error kommer upp, är det dags att skapa de rätta kontona och grupper som SCOM kräver. De som måste skapas är följande: En *Domänsäkerhetsgrupp,* ett s.k. *Actionkonto* som ska ha användarrättigheter, *SDK och Config Servicekonto* med systemadministratörsrättigheter.

5.1.2.4. Installation av SCOM 2007

För att installationen ska fungera måste ni vara inloggade på ett konto med administratörsrättigheter och ha ett likadant konto för SQL. Sen är det bara att starta igång installationen. Det första som kommer upp, när skivan sätts i, är en startsida på vilken ni ska välja *Install Operations Manager 2007*. Efter detta kommer det två stycken sidor där ni bara ska trycka på *Next*, dessa sidor är en *välkomstsida* och en *Licenssida*. Nästa steg är att leta reda på CD-nyckeln, för den behövs för att komma vidare till nästa steg i installationen. Skriv in nyckeln och tryck på *Next*. Ni kommer då till en sida där ni ska välja s.k. *Custom Setup*, denna ska ni låta vara som den är, ändra ingenting och tryck *Next*. På nästa sida ska ni ange ett namn för er *Management Group*, detta namn kan inte ändras senare så skriv något passande, vår döpte vi till Valderas. Efter ni valt namn ska ni sedan välja en grupp ni vill addera till administratörsrollen. Efter det ska ni trycka på *Next*. Nästa steg, på sidan *SQL Server Database Instance*, är att välja den SQL Server som ni vill installera SCOM's databas på. När detta är gjort trycker ni på *Next*. Sidan som följer är *Database and Log File Options*, där ni ska välja storlek på databasen som ska användas. Sen ska ni trycka *Next*. Nästa steg är att ni ska ange ett s.k. *Manager Server Action Account*, detta kan man göra på två olika sätt. Antingen väljer ni *Local System* och trycker på *Next*, eller så väljer ni *Domain or Local Computer Account* och anger användarkonto och lösenord samt väljer *Domain or local computer*. Vid nästa ruta, som heter *SDK and Config Service Account*, ska ni göra samma saker som på föregående ruta, dvs. antingen väljer ni *Local System* och trycker på *Next*, eller så väljer ni *Domain or Local Computer Account* och anger användarkonto och lösenord samt väljer *Domain or local computer* och sen trycker ni på *Next*. Rutan som nu kom fram heter *Web Console Authentication Configuration* och där är det meningen att ni ska ange hur ni vill att åtkomsten av konsolen ska vara. Välj *Use Windows Authentication* om ni endast vill använda konsolen från Intranätet, eller välj *Use Forms Authentication* om ni vill ha åtkomst till konsolen över Internet. Tryck sen på *Next*. På sidan *Operations Manager Error Reports* ska ni ange om ni vill skicka, de felmeddelanden som kan komma att dyka upp, till Microsoft eller inte och sen trycker ni på *Next*. Rutan som sen kommer fram heter *Customer Experience Improvement Program* och innebär att om ni vill medverka i att göra SCOM 2007 bättre väljer ni *Join the customer Experience Improvement Program* men vill ni inte delta i detta låter ni bli det och väljer *I don't want to join the program*. Sen trycker du på *Next*. Nu har vi kommit fram till själva installationen, för nästa ruta som kommer fram är *Ready to Install*. För att börja installationen klickar ni helt enkelt på *Install*. När installationen är klar kommer den sista rutan upp, *Completing the System Center Operations Manager 2007 Setup Wizard*, och för att starta SCOM direkt bockar ni i rutan *Start the console* och sen trycker ni på *Finnish*.

5.1.3. Konfiguration

När man ska konfigurera SCOM 2007 gör man det direkt i programfönstret, genom att klicka på knappen *Administration*. Från *Administration*-fönstret som då kommer upp kan man sen lägga till nya datorer och skapa nya tester som ska köras på datorerna man vill övervaka.

5.1.3.1. Lägga till fler datorer att övervaka

För att lägga till nya datorer att övervaka går ni till *Administration*-fönstret, sen hittar ni högst upp till höger en rubrik som heter *Actions*. I denna kolumn hittar ni, överst, en rad som heter *Configure computers and devices to manage*. När ni klickar på den kommer ett nytt programfönster upp som heter *Computer and device management wizard*. För att

komma vidare klickar ni helt enkelt på *Next*. För att SCOM ska börja söka efter nya datorer måste ni först välja hur ni vill att den ska söka efter dem, antingen väljer ni *Automatic computer discovery*, då söker SCOM efter windows-baserade datorer i det domän ni skrev in under installationen. Vill ni precisera sökningen, efter nya datorer, väljer ni det andra alternativet som är *Advanced discovery*. Då får ni välja vad för typ av enhet ni vill att SCOM söker efter, antingen söker den efter servrar och klienter, eller efter enbart klienter eller så kan den söka efter nätverksenheter så som routrar etc. Ni får även välja vilken management-server ni vill använda för övervakningen. Om ni t.ex. vill söka efter servrar och klienter, väljer ni det och klickar sen på *Next*. Då blir ni ombedd att ange vilket Active Directory konto ni vill använda för sökningen, antingen väljer ni att ni vill använda samma konto som ni angav vid installationen av Active Directory, ni kan även välja ett valfritt konto som ni skapat senare. När ni valt kontot att söka med, klickar ni på *Next* och då börjar sökningen efter nya enheter. Hittar SCOM enheter som ännu inte är övervakade får ni upp en lista med dessa och ni kan då välja vilka/vilken ni vill börja övervaka. När ni lägger till datorer att övervaka får ni ange om ni vill att SCOM installerar en agent på dessa datorer, för att få en mer överblickande övervakning, eller om ni enbart vill övervaka enklare tjänster. För att få en överblick av alla datorer som övervakas klickar ni på *Monitoring*, nere till vänster, och sen på *Computers*. Då kommer ni att se alla datorer som övervakas och vad som övervakas på dem. Om ni tittar på bilden nedan ser ni våra servrar och den dator vi testat, samt vilka tester vi valt att utföra.

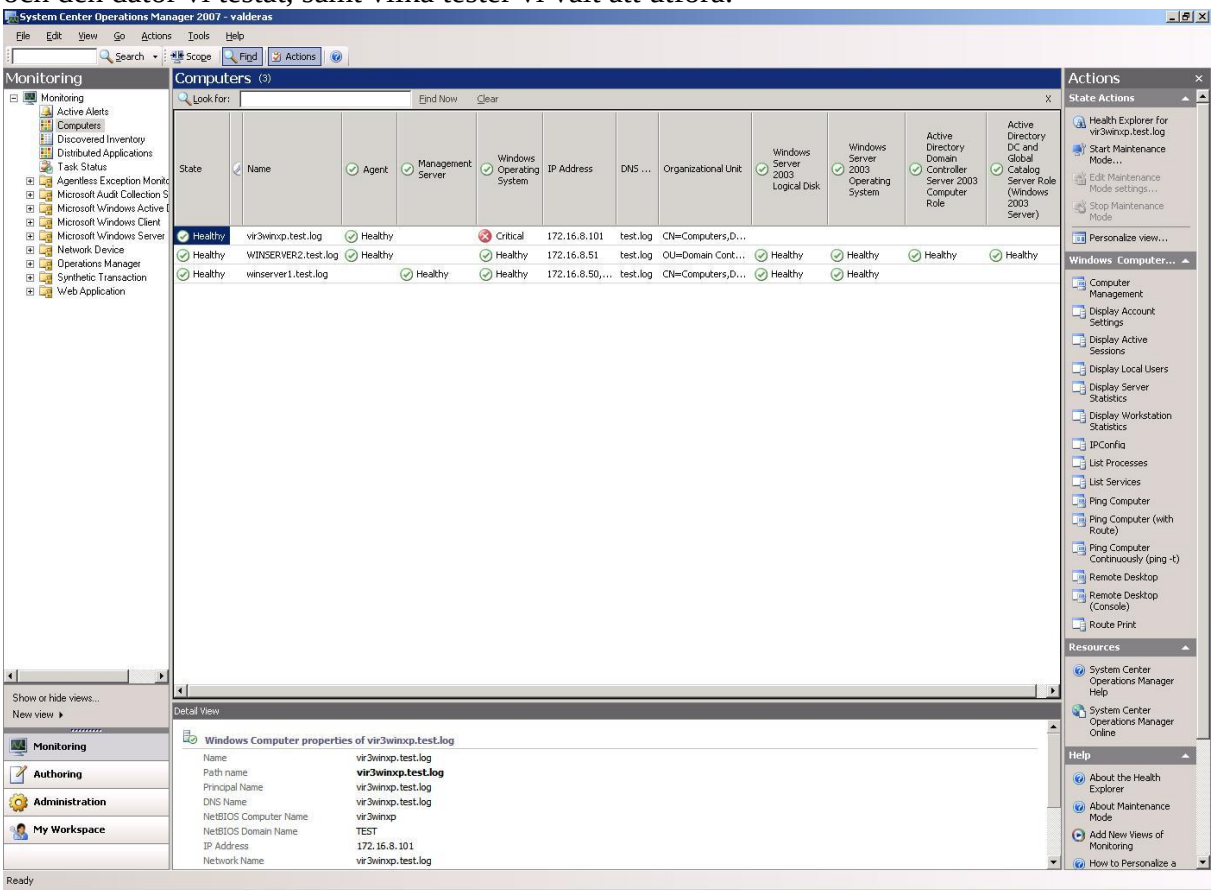

Fig.2 Bild föreställande övervakningen i SCOM 2007

När ni valt ut alla datorer ni vill ha övervakning på är det nu dags att lägga till tester ni vill utföra på dem.

5.1.3.2. Lägga till fler tester

För att lägga till fler tester i övervakningen klickar ni på *Administration*, nere till vänster, och sen på *Import management packs*, som finns under *Configure computers and devices to manage*, som ni gick in på då ni la till fler enheter till övervakningen. Management packs är de som utför själva testningen i SCOM 2007. När ni klickat på *Import management packs* får ni upp en ruta där ni ska välja vad för typ av management pack ni vill använda. På SCOM-skivan, i mappen ManagementPack finns det ett antal management packs som kan övervaka exempelvis Exchange Server 2003, Microsoft Office och SQL Server 2000/2005. Det går även att ladda ner andra management packs från Microsofts hemsida. Där finns det även mall för hur man kan göra egna management packs om man vill övervaka en enhet eller tjänst som det ännu inte finns ett management pack för. När ni valt de ni vill använda till er övervakning kan ni klicka på *Monitoring* och på *Computers* så ser ni att det kommit till fler tester som körs på datorerna ni övervakar.

5.1.4. Övervakning

Övervakningen med SCOM sker alltså med hjälp av så kallade management packs, som testar allt möjligt som t.ex. att Windows-operativsystemet fungerar som det ska. På bilden över vår övervakning kan ni där se att ett test ger svaret *Critical*, detta beror på att vår version av Windows XP ännu inte var registrerad. Det finns tre stycken olika tillstånd en enhet eller tjänst kan ha, *Healthy*, *Critical* eller *Warning*. *Healthy* betyder självklart att enheten/tjänsten fungerar som den ska, C*ritical* betyder att något ar fel och måste fixas så fort som möjligt, medans *Warning* betyder att något är fel eller inte riktigt fungerande, men att det inte är lika allvarligt. Vi fick *Warning* då det återstod någon dag innan vår version av XP slutade att gälla, om vi inte registrerade den och sen när registreringstiden gick ut byttes W*arning* ut mot *Critical*. För att ta reda på vad ett Warning- eller Critical-meddelande betyder, klickar ni på det så ser ni en förklaring på vad som är fel i rutan *Detail view*. Förklaringarna kan ibland vara lite svåra att tyda, så vi rekommenderar att ni gör som vi gjorde då vi inte förstod vad som var fel. Vi sökte efter felen på *www.google.com*.

När man befinner sig i *Monitoring* och *Computers* kan man, med hjälp av *Actions*-kolumnen längst till höger, administrera de övervakade datorerna direkt i SCOM. Det går t.ex. att ansluta till dem med *Remote Desktop*.

5.1.4.1. Meddelande till administratören

För att slippa sitta och hålla koll på övervakningen med SCOM kan man ställa in så att SCOM skickar meddelande då något händer, dessa meddelanden kan skickas via mail, sms eller personsökare. För att skicka meddelanden via mail måste man göra en del inställningar först.

Det första som ska göras är att skapa ett s.k. meddelandekonto, *Notification Action Account*. För att kunna skapa ett sådant konto ska ni vara inloggade på ett konto som har administratörsrättigheter på SCOM. Genom att sen klicka på *Administration*, sen högerklicka på *Security* och sen klicka på *Create Run As Account*, kan ni sen skapa ett nytt konto. Detta gör ni genom att ni väljer *Windows* under *Run As Account type* och sen skriver ni in *Notification action account* som *Display name*. Nästa steg är att skriva in användarnamn, lösenord och domän för kontot du vill skapa och sen trycka på *Create*. Nästa sak att göra är nu att klicka på *Run As Profiles*, i Administrationsrutan, I *Detail*-rutan, högerklicka på *Notification Account* och sen väljer ni *Properties*. I rutan som nu dök upp, *Run As Profile Properties*, klickar ni på *Run As Accounts*-fliken. Där klickar ni på

New och sen väljer ni *Notification Action Account*. Under *Matching Computers* dubbelklickar ni på *Root Management Server (RMS)*.

Nästa steg, för att få mailen att fungera, är att starta den mailtjänsten. Det gör ni genom att, i *Administration* klicka på *Settings* och sen högerklicka på *Notifications* och sen klicka på *Properties*. Klicka nu på fliken *Email* och sen väljer ni *Enable email notification*. På *SMTP servers* klickar ni på *Add* och sen anger ni hela ert domännamn till SMTP-servern, samt anger portnummer och vilken metod SMTP-servern ska använda för autentifiering. Sen klickar ni på *OK*. Efter det anger ni *Return Address*, vilken adress som ska vara mottagare, och ni ska även ange *Retry primary* after, dvs. ni ska ange ett visst antal minuter ni vill att SCOM ska vänta innan den åter skickar samma meddelande om något skulle gå fel med det första. Sen, under *Default email notification format*, fyller ni i mailets ämne samt ett meddelande. När allt är korrekt ifyllt klickar ni på *OK*, om nu alla inställningar som gjorts är ok, ska nu meddelanden skickas på mailen om ett fel uppstår i SCOM.

5.1.5. Våra synpunkter om SCOM 2007

Vårt första intryck av SCOM 2007 var att det verkade som ett rätt så svårt övervakningssystem att komma igång med. Det var många program och tjänster som krävdes för att en SCOM-installation skulle fungera. Fast det var inte svårt att veta vad som krävdes, då en mycket bra ”för-koll” fanns med, som man körde innan man började installera. Denna ”för-koll” gick igenom datorn och kollade att allt var inställt och installerat som det ska. Var det något som saknades fick man reda på vad det var och hur man skulle göra för att fixa problemet.

Att lägga till datorer, från samma domän, att övervaka gick rätt smidigt, då SCOM sökte efter enheter som ännu inte var övervakade och visade dem i en lista som vi sen kunde välja ifrån. Ett fel/problem vi stött på, då vi lagt till nya datorer i övervakningen, är att vi inte kunnat lägga till datorer som inte är med i någon domän, eller om datorn är med i en annan domän än vårt test.log. För när SCOM ska söka efter nya datorer att övervaka söker den enbart i det domän den själv är med i.

Att lägga till fler management packs i SCOM gick rätt så smidigt, förutsatt att de följde med i programmet. Ville man däremot ha andra management packs, för att övervaka andra tjänster på sitt nätverk, blev det genast svårare. Vi hittade t.ex. inget management pack för att övervaka Windows Server 2008 och dess tillägg.

En negativ sak med SCOM var att vi stötte på en hel del problem som vi inte visste vad det var och där vi inte blev klokare av SCOMs förklaring av felet. Tack vare det blev det svårt att veta vad som behövdes göras för att lösa problemet. Enda lösningen då var att söka efter felet i olika supportforum på Internet.

Huvudintrycket av SCOM 2007 är att det verkar vara ett bra men rätt så komplicerat övervakningssystem, men som när det fungerar, är ett mycket kraftfullt och användbart sådant. Vi har inte lyckats övervaka datorer från andra domän och om man inte ska kunna göra det, vilket verkar konstigt, så tycker vi det är en väldigt dålig begränsning och då inte passar Valderas, som ska övervaka sina kunders nätverk och därför är med i flera olika domäner.

Vi tycker att SCOM 2007 passar företag, oavsett storlek, som behöver övervakning på enstaka domän. För om det enbart går att övervaka en domän per SCOM-server, behövs

det en dator, med SCOM installerat, i varje domän. Företaget i fråga ska även vara medveten om att installation och konfiguration av SCOM tar längre tid, än t.ex. Big Brother…

5.2. Quest Software's Big Brother 4

5.2.1. Systemkrav

5.2.1.1. Windows

Processor: Pentium II 400MHz eller snabbare
Minne: 4GB ledigt diskutrymme
OS: Windows XP
Windows 2000 Server
Windows 2000 Pro
Windows 2003 Server
Nätverk: TCP/IP
Annat: Microsofts IIS webbserver eller annan webbserver

5.2.1.2. Linux/UNIX

OS: RedHat Enterprise Server 3.0, 4.0 eller 5.0
SUSE Enterprise Linux 9.0 eller 10.0
Solaris 8 eller nyare
HP-UX 11.0 eller 11i
AIX 5.1, 5.2 eller 5.3
Annat: Apache eller annan webbserver
CGI-scripts måste fungera
BBPAGER-servern måste kunna skicka mail så att mailvarningar kan skickas.

Vi kommer endast att ta upp hur Big Brother 4 fungerar på en Windows-server.
Anledningen till detta är att vi tror att Big Brother 4, kan fungera som ett bra komplement till SCOM 2007.

5.2.2. Installation av webbserver och Big Brother 4 Server

5.2.2.1. Webbserver

För att Big Brother 4 ska fungera måste det finnas en webbserver installerad på den server som Big Brother ska installeras på. Det går alldeles utmärkt att använda sig av Windows egen webbserver *IIS, Internet Information Server*. Det kan vara så att *IIS* redan är installerad på datorn.

Såhär kontrollerar du om IIS redan finns
Klicka på: *START, Kontrollpanelen, Lägg till/Ta bort program.*
Klicka på: *Lägg till/Ta bort Windows-komponenter*.
Sen kollar du om rutan vid *IIS* är ikryssad, är den det så är *IIS* redan installerat. Är den inte det så klickar ni i den och trycker på *Nästa*. Sen är det bara att följa instruktionerna vidare.

5.2.2.2. Big Brother 4

Gå till Quest's hemsida för Big Brother 4: *http://www.bb4.com/* och ladda ner programmet. För att kunna ladda ner programmet måste ni skapa ett konto hos Quest Software, detta är gratis. När ni ska ladda ner det så är det viktigt att ni väljer rätt operativsystem att ladda ner till. När nedladdningen är klar stänger ni ner webbläsaren och går till den mapp där ni sparade filen. Vi laddade ner en testversion av Big Brother 4 Server, så vår fil heter *BigBrotherforWindowsServerInstaller_40.exe*, vi har inte testat vad den heter om man köpt programmet, men det skulle kunna vara *bbntdpe-400.exe*, denna nämns i Quest's guide för installation av Big Brother 4 Server. Oavsett vad filen heter ska man dubbel-klicka på den för att starta installationen. Under installationen kommer du få göra följande saker: Acceptera licensavtalet, ange namn och företag, ange var du vill installera Big Brother någonstans samt ange var databasen *BBVAR* ska installeras. När installationen är klar ska ni kolla två saker som ska ha lagts till. Det första ni ska kolla är om *IIS* har lagt till Big Brother. För att kolla det klickar ni på *Start, Kontrollpanelen, Administrationsverktyg* och sen på *IIS*. Om allt är ok ska det se ut på såhär:

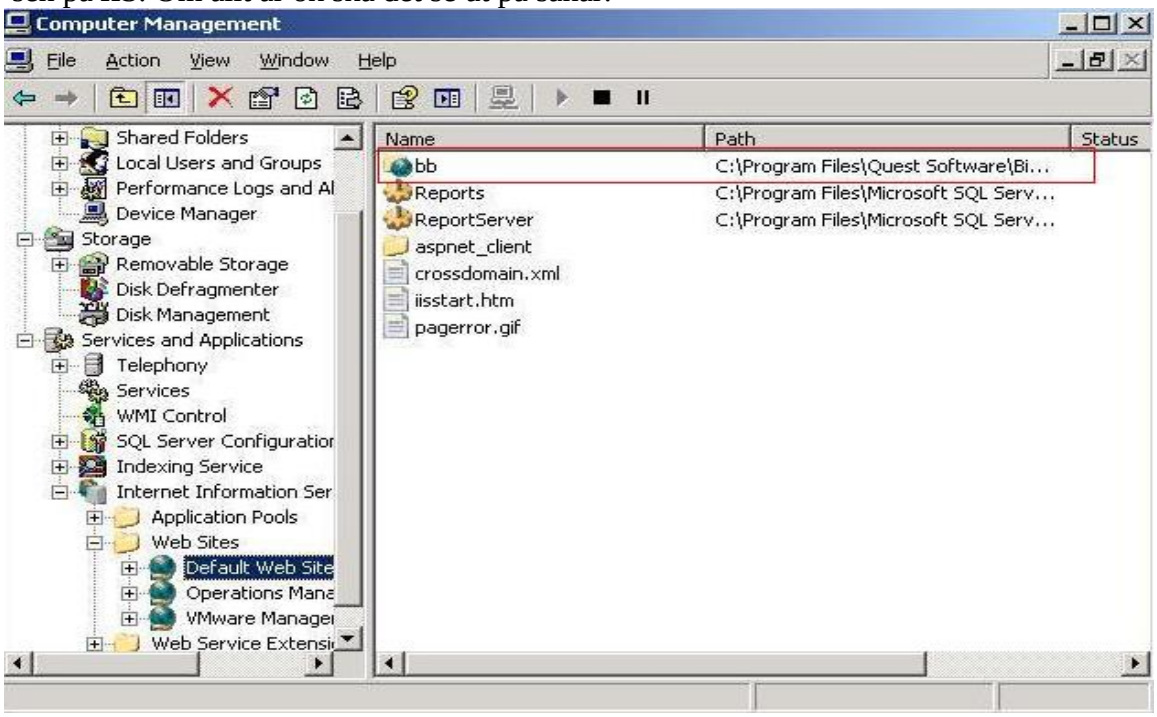

Fig.3 Kontrollera att IIS lagt till Big Brothers webbtjänst

Det andra ni ska kolla är om Big Brother har lagts till som en Tjänst (Service), det gör du genom att klicka på *Start, Kontrollpanelen, Administrationsverktyg* och sen på *Tjänster*. Det ska se ut på följande sett:

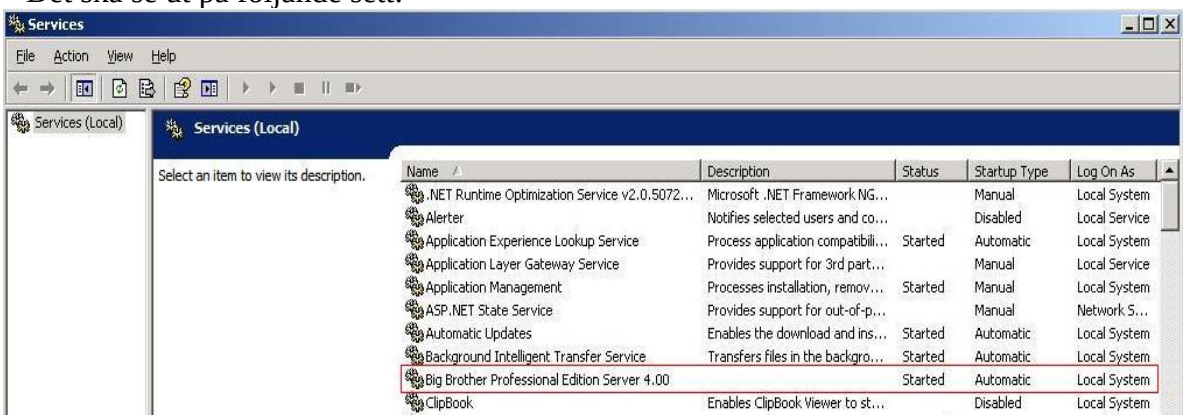

Fig.4 Kontrollera att servicen Big Brother lagts till som tjänst

Det ni ska se till är att Big Brother startar automatiskt när datorn startas.

5.2.3. Uppstarten

Big Brother 4 är ett webbaserat övervakningssystem, så för att kunna se allt som Big Brother övervakar måste ni öppna en webbläsare och ange adressen till programmet Big Brother. Detta kan man göra på två olika sätt, antingen *http://servernamnet/bb/* eller *http://ip-adressen.till.BigBrother-servern/bb/*.
När vi installerade Big Brother och skrev *http://172.16.8.51/bb/* fick vi upp följande:

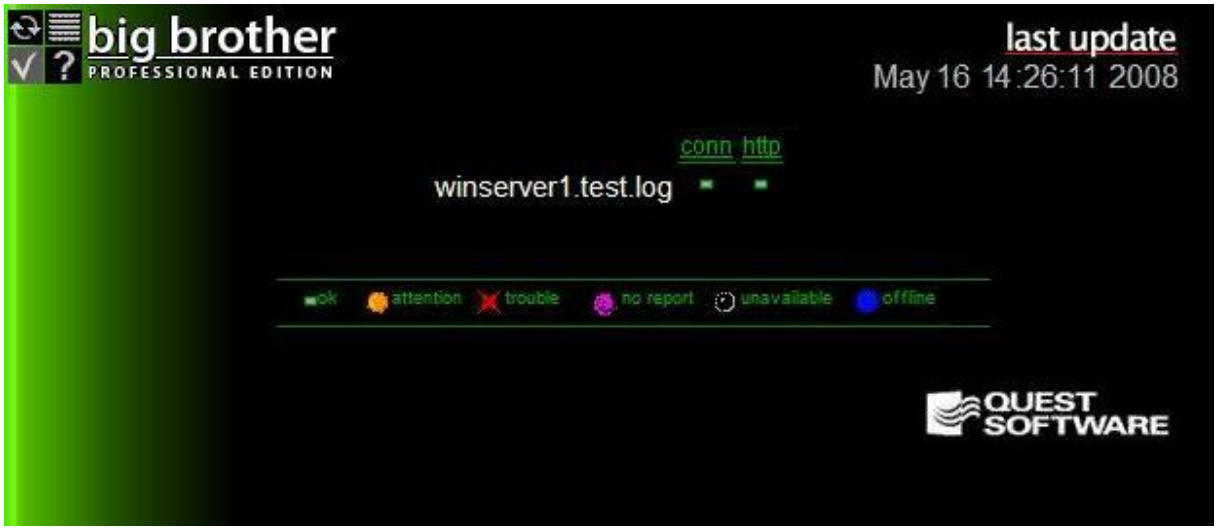

Fig.5 Big Brothers övervakning, i uppstarten

I vårt exempel kan vi se att servern, winserver1, är med i domänet test.log samt att den klarar av Big Brothers två grundtest. Testet ”*conn*” visar om Big Brother har kontakt med servern, testet ”*http*” visar om webbservern fungerar som den ska.

För att administrera Big Brother finns det ett verktygsfält, man kan använda sig av, uppe i det vänstra hörnet. Verktygsfältet består av fyra stycken olika ikoner:

- Klickar man på denna bläddrar man mellan huvudfönstret och fönstret som visar senaste händelserna.
- Här kan man välja att göra en tillgänglighetsrapport för sitt system. Man väljer en viss tidsperiod och sen visas det hur mycket av den tiden alla enheter har varit tillgängliga.
- Detta är administrationssidan. Här kan man, om man har installerat den funktionen, skicka meddelande till administratorn angående ett brådskande fel. Det går även att ta bort vissa meddelanden, om man vet om ett fel men att det inte är viktigt, så kan man göra så att inga fler meddelanden skickas om just det felet på den enheten. Det går även att komma åt konfigurationsfilerna och ändra i dem, självklart krävs ett lösenord för att göra detta.
- Klickar man på frågetecknet öppnas Quest’s egna hjälpfil för hur man administrerar Big Brother 4.

5.2.4. Konfiguration

För att kunna övervaka fler enheter än själva servern som Big Brother 4 är installerat på, ändrar man i två stycken konfigurationsfiler. Dessa två filer heter *bb-hosts.cfg* och *bbdef.cfg*. Har man installerat Big Brother 4 med de grundinställningar som ges som förslag ligger de två filerna i mappen *C:\Program Files\Quest Software\Big*

Brother\BBNTD\4.00\etc. Innan ni ändrar i de två filerna är det bäst att ta en backup på dem, för att kunna återställa allt, om något mot all förmodan, går fel. För att lägga till flera enheter att övervaka samt lägga till vad som ska övervakas på dessa, ändrar man i filen *bb-hosts.cfg*. Filen *bbdef.cfg* ändrar man i för att ställa in värden på till exempel hur länge en notis ska vara synlig i senaste händelser. För att Big Brother ska använda sig av de nya inställningarna måste Big Brother stoppas och startas om, vilket lättast görs via *Start, Alla Program, Quest Software, Big Brother, Server, Stop/start.*

5.2.4.1. bb-hosts.cfg

För att lägga till enheter, som ska övervakas av Big Brother, öppnar ni filen *bb-hosts.cfg* i en lämplig texteditor, exempelvis Anteckningar. I filen syns det 4 stycken rader som är bortkommenterade, dessa är till för att förklara lite om hur filen fungerar. Efter kommentarerna står det:
127.0.0.1 somehost.quest.com # testip BBPAGER BBNET BBDISPLAY http://somehost.quest.com/bb/
Det första som står är IP-adressen till enheten som ska övervakas, efter det följer enhetsnamnet och sen står det vad som ska övervakas, det återkommer vi till senare. Sist på raden är Internetadressen till den sida där man kan följa övervakningen.
När vi lagt till alla de servrar och datorer som vi ville övervaka såg vår *bb-hosts.cfg* ut på följande sätt:

```
172.16.8.50     winserver1.test.log  # testip BBPAGER BBNET BBDISPLAY http://winserver1.test.log/bb/
172.16.8.51     winserver2.test.log  # dns
172.16.8.101    vir3winxp.test.log   #
172.16.8.57     vir3ubuntu.test.log  #
172.16.8.58     Vir3Solaris
172.16.8.156    vir1winxp            #
172.16.8.161    vir1winxp2.test.log  #
```

IP-adress | Enhetsnamn | Vad som ska övervakas | Adress till Big Brother

Fig.6 Exempel på vår *bb-host.cfg*-fil

Enhetsnamnet är namnet på den dator/server ni vill övervaka, om maskinen är ansluten till ett domän ska hela domännamnet stå med. Det går att övervaka datorer även om de inte är med i någon domän, vi har t.ex. övervakning på datorerna Vir3Solaris och Vir1WinXP fast de inte är med i vår domän test.log.

Testet testip betyder att servern winserver1 testar kontakten till alla IP-adresser som finns skrivna i *bb-hosts.cfg*. *BBPAGER* indikerar att Winserver1 är rapporteringsservern. Winserver1 har även blivit tillsagd att utföra alla nätverkstester till varje enhet som finns med i *bb-hosts.cfg*, det är det som *BBNET* betyder. Winserver1 är även ”visnings”-server, *BBDISPLAY*, som visar alla meddelanden från alla tester. En Big Brother-server tar emot inkommande loggar innehållande alla enheters status och gör det möjligt för oss att se detta på webbsidan för servern, dvs. *http://ip-adressen.till.BigBrother-servern/bb/*.

När ni lagt till alla datorer och servrar, ni vill övervaka, i filen *bb-hosts.cfg*, sparar ni den och går till sidan *http://ip-adressen.till.BigBrother-servern/bb/* och väntar ett tag så ska ni se att Big Brother har lagt till alla enheter ni vill övervaka. När vi sparade vår *bb-hosts.cfg* såg det ut såhär på sidan *http://ip-adressen.till.BigBrother-servern/bb/*

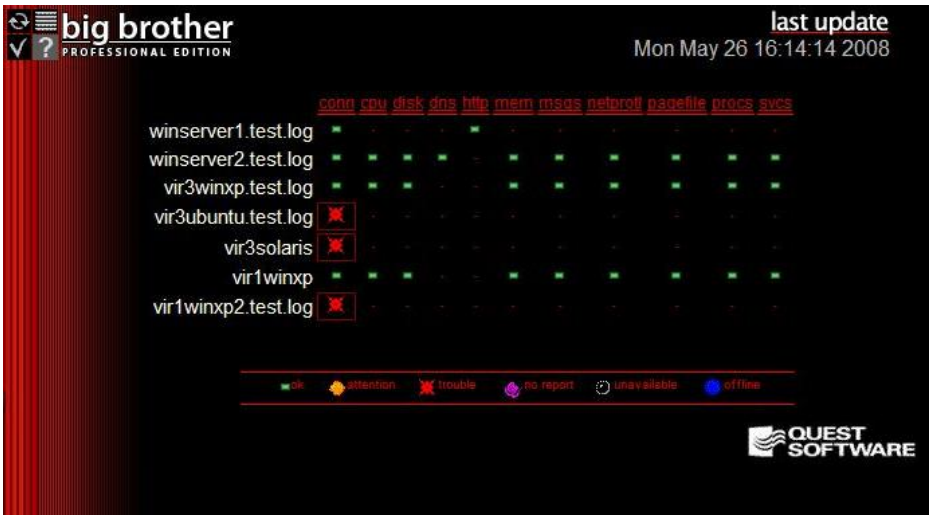

Fig.7 Bild föreställande Big Brothers övervakning då fler tester och datorer lagts till

Som ni märker på bilden har vi flera tester än vad som nämnts tidigare, dessa tester tar vi upp senare i detta dokument. På bilden syns även tre datorer som inte klarar testet *conn*, detta beror helt enkelt på att de inte är påslagna. På bilden ser ni också att Big Brother har ändrat färg, från grönt till rött. Anledningen till färgbytet är att Big Brother, förutom att varna med ikoner då något är fel, varnar med att byta färg på hela övervakningssidan beroende på hur allvarligt felet är. När vi startade datorerna, som var avstängda, vilka gjorde att Big Brother visade rött, blev alla tester ok och sidan ändrade sig till grönt, dvs. allt är ok, vilket ni kan se på nästa bild.

5.2.5. Lägga till fler tester

För att Big Brother ska kunna utföra fler tester än de som går i *bb-hosts.cfg*, måste man installera ett Big Brother-Client program på den dator som ska övervakas. Anledningen till att ett klientprogram måste installeras på alla datorer, som ska övervakas, är för att de tester som görs, som t.ex. CPU och använt hårddiskutrymme, är tjänster som endast kan testas på varje enskild dator.

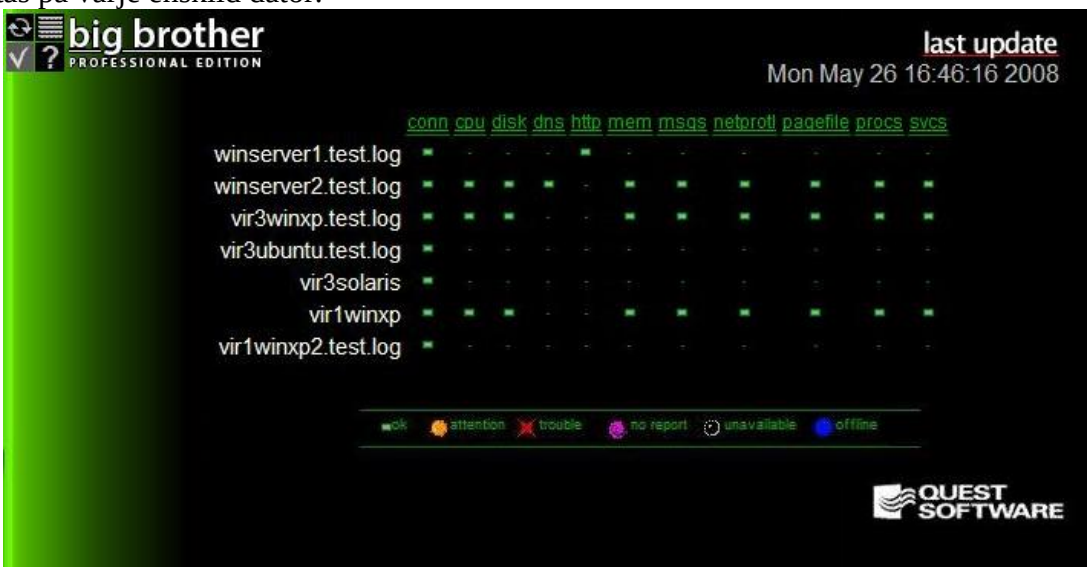

Fig.8 Bild föreställande Big Brothers övervakning då allt fungerar korrekt

5.2.5.1. Installera och konfigurera Big Brother-Client

Big Brother-Client kan installeras på alla datorer som har Windows som operativsystem, men om datorn som ska övervakas har Linux/Unix kan Big Brother-Client endast installeras på några av dessa. De Linux/Unix operativsystem som stöds är HP-UX 11, IBM AIX5.1 – 5.3, Red Hat Enterprise Server 3.0 – 5.0, Sun Solaris 5.8, 5.9 och 10, SUSE 9 och SUSE 10. Vi hade, på den bärbara datorn som kraschade, installerat Solaris10 på en av de virtuella datorerna just för att testa hur Big Brother-Client övervakade en icke Windows-maskin. Innan datorn kraschade hann vi komma igång med installationen av Big Brother-Client, men vi fastnade en bit in. Vi följde guiden som finns på *http://www.bb4.com/download.asp*, men när vi kom till punkt 6 så klagade den på att vi skrivit fel och ville inte fullfölja installationen. Innan vi sen hann ta reda på vad som kan varit fel, så kraschade bärbara datorn. Så vi har inte testat hur Big Brother-Client övervakar datorer som inte har Windows som operativsystem, tiden räckte helt enkelt inte till.

Det första som ska göras är att ladda ner Big Brother-Client från deras hemsida *http://www.bb4.com/download.asp*. När nedladdningen är klar dubbel-klickar ni på filen, för oss hette den *bbntpe-400.exe*, då kommer det upp en ruta som frågar om ni vill installera programmet, där trycker ni *Yes*. Licens avtalet ska ni acceptera. Efter det blir ni ombedda att skriva in ert namn och företagets namn. Nästa steg är att välja var på hårddisken ni vill installera Big Brother-Client. När allt är ifyllt korrekt är det bara att klicka *Yes*, så att installationen startas. När installationen är klar trycker ni på Finish, blir ni ombedda att starta om datorn kan ni välja *No*, för detta är inte nödvändigt. När allt är klart ska det dykt upp en ny rad under *Start* och *Alla Program*, som heter *Quest Software*. Om ni klickar på den och sen på *Big Brother Professional Edition* kommer *Client* fram, klickar ni på den så får ni upp fyra stycken olika val, *Configure*, *Help*, *Start* och *Stop*. Ni ska klicka på Configure för att konfigurera Big Brother-Client. Då ni klickar på den kommer följande ruta upp:

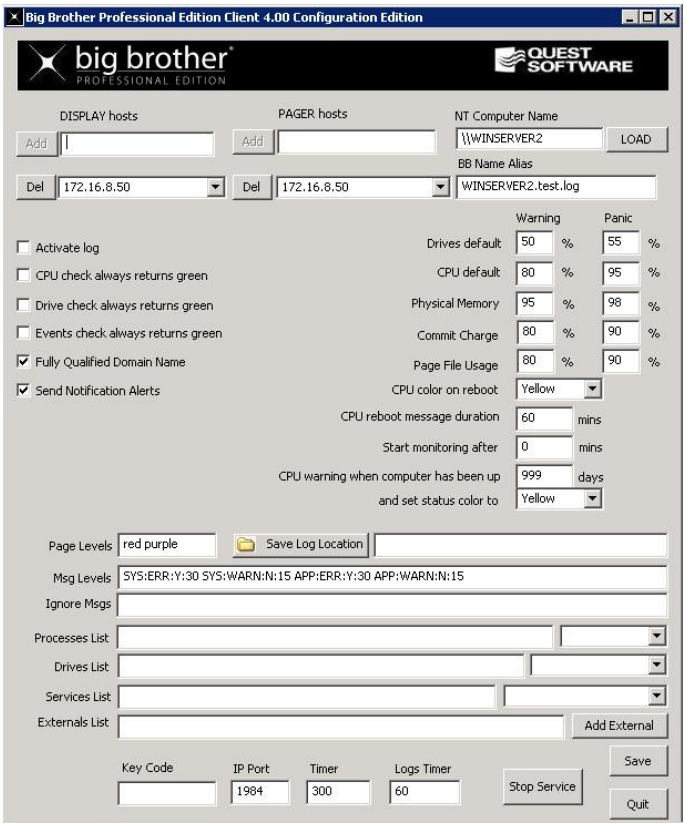

Fig.9 Bild föreställande Big Brother Client, för Windows

Det som ni måste ändra i Client, för att övervakningen ska börja, är att ni måste ange IP-adressen till servern/servrarna som fungerar som DISPLAY host/hosts, dvs. BBDISPLAY, samt IP-adressen till servern/servrarna som fungerar som PAGER hosts, dvs. BBPAGER. För att kunna lägga till dessa adresser måste ni först ta bort det som finns där nu. Det gör ni genom att välja den adress som står där och sen trycke på *Del*. För att sen lägga till de nya adresserna skriver ni in dem i fältet bredvid *Add-knappen* och sen trycker ni på *Add*. Ni kan även välja, på de test som finns, vilken procent som ska uppnås innan Big Brother börjar varna, det finns två fält att fylla i för hur Big Brother varnar. Det ena är vid vilken procent som måste passeras innan Big Brother skickar ett varningsmeddelande och det andra är vid vilken procent som Big Brother ska skicka ut ett panicmeddelande.

5.2.6. Övervakning med Big Brother

För att Big Brother ska börja använda sig av inställningarna som görs i Big Brother-Client, gäller även då du ändrar i dem i framtiden, måste ni stoppa och starta tjänsten. Detta gör ni genom att gå till *Start/Alla program/Quest Software/Big Brother Professional Edition/Client* och sen trycker ni på *Stop* respektive *Start*. För att detta ska fungera krävs det att ni lagt till de datorer ni installerat Big Brother-Client på i filen *bb-hosts.cfg,* det går även att lägga till en del tester direkt i filen, men vi har valt att endast testa DNS på Winserver2. Om allt verkar ok, kommer Big Brother, efter ett litet tag, för oss är det efter 2min, att uppdatera webbsidan och visa de nya datorerna samt de nya testerna. Om nu alla tester blir gröna, fungerar allt korrekt. Blinkar något gult eller rött betyder det att något inte är som det ska och kräver administration. Här nedan syns ett exempel på en varning.

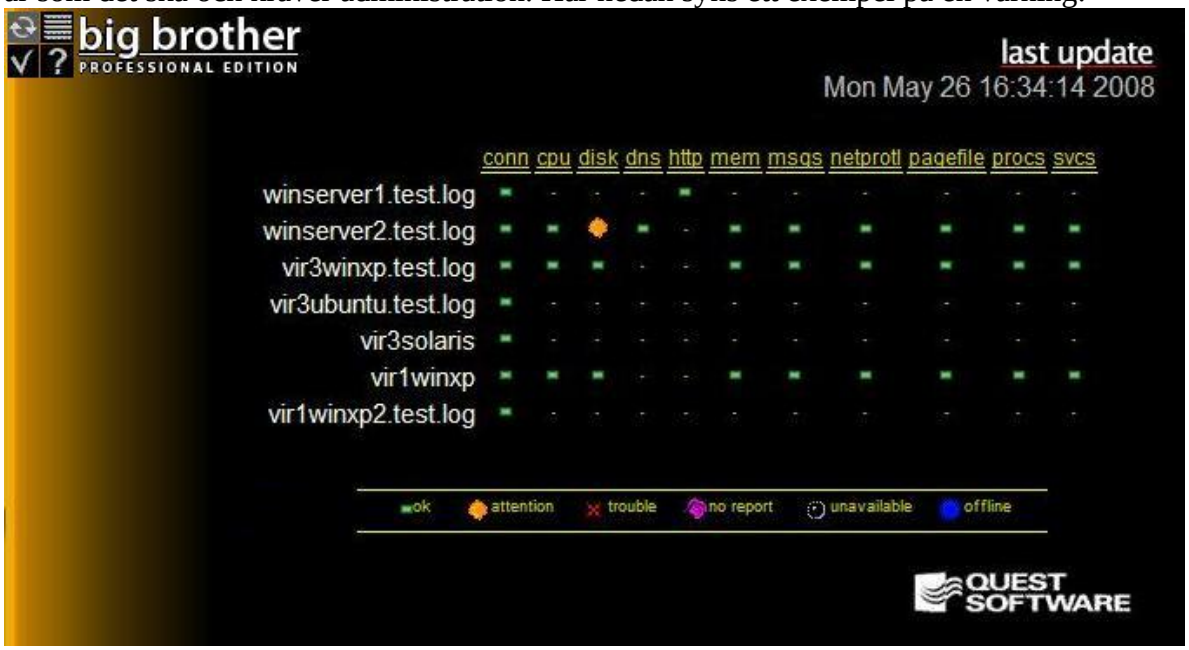

Fig.10 Bild föreställande Big Brother övervakning då endast finns en varning

För att ta reda på vad som är fel, vad varningen betyder, dubbelklickar ni på den gul/orangea runda ikonen. Då kommer ni till en ny sida där endast den datorn, som varningen gäller, och även det testet som skickar varningen.

Fig.11 Bild föreställande varningens beskrivning

I vårt fall är det servern, Winserver2, som har fått en varning. Varningen gäller hårddiskutrymmet på C: som har passerat den gräns vi valt som varningsgräns, 50 %. Denna gräns väljer man i programmet Big Brother-Client, som vi gick igenom tidigare. Winserver2 har, som det är på bilden fyllt C: till 52 %, Skulle Winserver2 lagra ytterligare 3 % kommer Big Brother att skicka ut ett panicmeddelande då gränsen för detta är 55 %.

5.2.6.1. Meddelande till administratören

För att man inte ska behöva besöka *http://ip-adressen.till.BigBrother-servern/bb/* hela tiden, för att se om något är fel, har Big Brother 4 som finess att den kan skicka mail, sms eller meddelande till personsökare då något händer. Vi har endast konfigurerat så att vi får mail om något händer. För att konfigurera Big Brother 4 till att skicka mail då ett eller flera problem uppstår öppnar ni en fil som heter *bbwarnrules.cfg*. Den filen finns i mappen *…\Quest Software\Big Brother\ BBNTD\4.00\etc*. Längst ner i den filen finns det en rad som det står *Enter your rules here*. Här är det meningen att ni ska skriva in följande uppgifter: Vilken/vilka datorer ni vill ha mail om, *hosts*, vilken/vilka datorer ni inte vill ha mail om, *exhosts*, vilka tjänster ni vill få mail om på de datorerna, *services*, vilka tjänster ni inte vill få mail om på de datorerna, *exservices*, om ni endast vill ha panicmeddelanden eller om ni även vill ha varningsmeddelanden, *colors*, vilka veckodagar ni vill få mail om, *day*, vilken tid på dygnen mailen ska skickas, *time* och till sist vilka som ska få dessa mail, *recipients*. Såhär ser vår *bbwarnrules.cfg* ut:

```
#################################################################
#
# Enter your rules here
#


winserver1.test.log;;*;;*;0-6;0000-2359;matiasfk@test.log administrator@test.log
winserver2.test.log;;*;;*;0-6;0000-2359;administrator@test.log
#hosts;exhosts;services;exservices;colors;day;time;recipients
#*;;*;;*;*;*;bbadmin@localhost
```

Fig.12 Exempel på hur vår *bbwarnrules.cfg* ser ut

Vi har valt att Big Brother 4 endast ska skicka mail angående servrarna Winserver1 och Winserver2. Nästa val har vi lämnat blankt, detta beror på att eftersom vi specificerade två

stycken enheter vill vi inte utesluta någon av dessa. Hade vi däremot valt att ta emot mail från alla övervakade enheter, då anger man en * i fältet istället, hade vi kunnat exkludera de enheter vi inte vill få mail angående. Nästa fält är *services*, där har vi angivit en *. Detta betyder att vi får mail, från Winserver1 och Winserver2, oavsett vilken tjänst som får problem. Vill man inte ha mail angående t.ex. hårddiskutrymme, anger det man i nästa val, *exservices* annars lämnas även detta fält tomt. Ska mailen skickas oavsett typ av fel, dvs. varning eller panic, skriver man in en * i fältet för *colors*. Sen ska det anges på vilka dagar man vill få dessa mail och vid vilken tidpunkt, vill man ha mail alla dagar och oavsett tidpunkt sätter man in en * i fälten *day* och *time*. Som ni kanske ser har vi valt att skriva ut dagarna och tiderna i ren text, detta fungerar också. Nästa val att göra är att ange vilka eller vem man vill ha som mottagare av mailen. Vi har valt att skicka mail angående Winserver1 till administratören och till användaren matiasfk, medans mail angående Winserver2 enbart skickas till administratören.

För att det ska vara möjligt för Big Brother 4 att över huvud taget skicka de varningsmail och panicmail som den vill måste en del inställningar göras först. På den server som Big Brother 4 är installerat på, måste även en fungerande mailserver vara installerad, vi valde att använda oss av POP3 och SMTP. Självklart måste det skapas konton för var och en av personerna som ska kunna ta emot mail och sen ska det även finnas ett lämpligt mailprogram, exempelvis Microsofts Outlook.

5.2.7. Våra synpunkter om Big Brother 4

För att vara första gången, för oss två, att installera, konfigurera och testa övervakningssystem har Big Brother 4 upplevt som ett mycket bra system att använda vid övervakning av sitt eget eller ett företags nätverk. Som det stod i beskrivningen av Big Brother 4, på deras egen hemsida *http://www.bb4.com*, var det mycket enkelt att installera och komma igång med övervakningen och från det att vi ladda ner Big Brother 4 tills det att vi var igång med övervakningen tog det ungefär 20 minuter. Att sen konfigurera och lägga till andra enheter till övervakningen upplevdes också som enkelt, det som behövdes då var programmet Big Brother-Client som var bra gjort och lätt att förstå. Övervakningen kan följas via ett webbaserat gränssnitt och kan åtkommas från alla datorer med en Internetuppkoppling, som har tillåtelse att nå den datorn.

Det negativa vi har att säga om Big Brother 4 är att om man vill övervaka fler tjänster än enbart nätverkskontakt, på en enhet som har Linux/Unix installerat, blir det genast mycket svårare. Vi fick det inte att funka, vi följde en guide på hur man skulle göra, men efter punkt sex i den guiden så kommer vi inte vidare. Det som skulle göras i punkt sex var att välja vilken server som skulle agera BBDISPLAY och BBPAGER. Big Brother föreslog att Linux/Unix-datorn skulle agera BBPAGER, medan vi ville att servern skulle vara båda delarna, men detta gick tydligen inte att göra, vi provade en massa olika alternativ men inget ville fungera. Vi hann som sagt inte utforska om varför vi inte kom vidare, för det ska fungera, det vet vi. En orsak till att vi inte kom vidare kan vara att vi endast hade Trial-version av Big Brother 4. En annan sak som var lite negativt var, att informationen om vilka olika tester man kan göra på de olika enheterna, var lite bristfällig. Vi vet egentligen inte hur mycket mer som kan övervakas på enheterna, som t.ex. disk, DNS, http etc., förutom de tester vi gjort nu, dvs. de som följde med i huvudinstallationen och i Big Brother-Client.

Huvudintrycket av Big Brother 4 är, från båda oss, mycket positiva. Det var, som sagt, väldigt användarvänligt i såväl installation, konfiguration och övervakning. Installationen

samt konfigurationen gick väldigt smidigt och snabbt och själva övervakningen var mycket enkel att följa. När det dök upp ett fel fick man lätt reda på vad som var problem, och på så sätt kunde vi hitta en lämplig lösning.

Vi anser att Big Brother 4 passar bäst till små eller medelstora företag som i första hand vill övervaka Windows-maskiner och enstaka Linux/Unix-maskiner. Vad som Big Brother 4 är bra på att övervaka är olika typer av tjänster, vi har inte hittat något tillägg för att kunna övervaka exempelvis Event-loggen eller liknande. Det vore alltså bra om företaget lägger tyngdpunkten på tjänstövervakning. Med tanke på att installation, konfiguration och övervakning går smidigt och enkelt behöver företagen inte oroa sig över att Big Brother 4 kostar för mycket, i hänsyn till tid och resurser. Självklart passar Big Brother 4 även stora företag om dessa endast behöver övervakning på de tjänster som Big Brother 4 kan övervaka.

5.3. Nagios

5.3.1. Systemkrav

Nagios har inga systemkrav vad gäller CPU, RAM etc. Det enda Nagios kräver är en dator som har ett Linux-operativsystem installerat, ska även fungera med en del Unix-operativsystem. Kräver även en C kompilator. Det vore bra om datorn hade TCP/IP konfigurerat korrekt, med tanke på att de flesta servicetesterna sker över nätverket.

5.3.2. Installationsprocess

Vi kommer här att beskriva hur en installation av Nagios, version 3.0.2, går till på en maskin som har Fedora Core 6 installerat.

5.3.3. Mjukvarukrav

För att kunna installera Nagios måste en del mjukvaror vara installerade innan. Det som krävs är en Apache-server, en GCC-kompilator och GD utvecklingsbibliotek. För att installera dessa tre anger man följande i terminalfönstret: *yum install httpd* för Apache-servern, *yum install gcc* för GCC-kompilatorn, *yum install glibc glibc-common*, för GD utvecklingsbibliotek och även *yum install gd gd-devel*, för GD utvecklingsbibliotek.

5.3.4. Skapa ett nytt konto och en grupp

Det första ni ska göra är att göra er till root-användare, om ni inte redan är det dvs. För att bli root-användare skriver ni, i terminalfönstret, *su -1***.** Nu när ni är root har ni rättigheterna till att skapa ett nytt användarkonto och ge det ett lösenord. För att skapa en ny användare, som heter nagios, skriver ni, i terminalfönstret, */usr/sbin/useradd nagios* och för att ange ett lösenord för det nyligen skapade kontot skriver ni *passwd nagios*. Då blir ni ombedda att skriva in ett lösenord och sen upprepa lösenordet igen, sen är det klart. Nu ska ni skapa en ny grupp och lägga till användaren nagios och apache till den gruppen. Ny grupp, som heter nagcmd, skapar ni genom att skriva */usr/sbin/groupadd nagcmd* och för att sen lägga till användarna nagios och apache skriver ni */usr/sbin/usermod G nagcmd nagios* respektive */usr/sbin/usermod G nagcmd apache*.

5.3.5. Ladda ner Nagios och tillhörande tillägg

Nästa steg är nu att ladda ner Nagios och dess tillägg, detta kan göras på två olika sätt, antingen besöker ni hemsidan *http://www.nagios.org/download/* och laddar ner dem där, eller så skriver ni, i terminalfönstret:
wget http://osdn.dl.sourceforge.net/sourceforge/nagios/nagios-3.0.2.tar.gz för själva Nagios 3.0.2 och *wget http://osdn.dl.sourceforge.net/sourceforge/nagiosplug/nagios-plugins-1.4.12.tar.gz* för tilläggen. Dessa två länkar går till de senaste versionerna som fanns ute, den 11 juni 2008, så de kommer att ändra sig då nyare versioner släpps, för att ta reda på gällande version besök Nagios hemsida *http://www.nagios.org.*

5.3.6. Packa upp, kompilera och installera Nagios

Det som ska göras nu är att ni ska packa upp och kompilera Nagios för att sen installera det. Öppna ett terminalfönster och navigera er till den plats ni sparade filen *nagios-3.0.2.tar.gz*. Sen skriver ni *tar xzf nagios-3.0.2.tar.gz* för att packa upp. Gå sedan in i mappen *nagios-3.0.2*. Väl där inne ska ni nu konfigurera Nagios med den grupp ni tidigare skapade, dvs. gruppen nagcmd, det gör ni genom att ange *./configure --with-command-group=nagcmd*. Innan vi kan installera Nagios måste vi först kompilera Nagios. Detta görs genom att skriva *make all* förutsatt att ni fortfarande befinner er i mappen *nagios-3.0.2*. När detta är klart måste ni även installera init script med mera. Nu ska ni alltså skriva *make install, make install-init, make install-config och make install-commandmode*.

5.3.7. Konfiguration

Innan Nagios kan startas måste en del ändringar göras.

5.3.7.1. contacts.cfg

För att Nagios ska skicka mail till rätt person, om något problem uppstår, måste man ändra mailadressen i filen *contacts.cfg.* Den finns i mappen */usr/local/nagios/etc/objects/*. Det ni gör är att ni öppnar filen och ändrar till den adress ni vill att mailen kommer till. För att se hela vår fil *contacts.cfg*, titta i bilaga 11.3.

5.3.7.2. Konfigurera webb-interfacet

Nagios är ett webbaserat övervakningssystem och för att få övervakningssidan att fungera måste man ange följande, i terminalfönstret: *make install-webconf*. När detta är installerat är det dags att skapa en användare som används för att logga in på övervakningssidan. Vi skapade ett konto som hette nagiosadmin, med följande kommando: *htpasswd –c /usr/local/nagios/etc/htpasswd.users nagiosadmin*. När kontot skapas blir ni ombedd att ange ett lösenord för kontot. För att dessa inställningar ska fungera korrekt krävs det att Apache startas om, vilket ni gör genom att skriva *service httpd restart*.

5.3.7.3. Nagios plugins

Nu är det dags att kompilera och installera de olika plugins ni ladda ner i början. Detta gör ni genom att skriva, i mappen *downloads*, *tar xvf nagios-plugins-1.4.12.tar.gz*. För att sen installera dem måste ni först gå in i mappen *nagios-plugins-1.4.12*, sen där skriver ni *./configure --with-nagios-user=nagios –with-nagios-group=nagios*, förutsatt att ni skapade en grupp samt användare som hette nagios. Efter det skriver ni *make* och sen *make install*.

5.3.7.4. Starta Nagios

För att Nagios ska starta då datorn startas måste ni ange det själv. Detta görs genom att skriva *chkconfig –add nagios* och *chkconfig nagios on.* Innan ni nu kan starta Nagios måste ni se till så att allt är ok med alla inställningar som gjorts, det gör man genom att skriva */usr/local/nagios/bin/nagios –v /usr/local/nagios/etc/nagios.cfg*. Om nu allt är som det ska borde ni inte fått varken varningar eller fel, stämmer detta är det dags att starta Nagios, skriv *service nagios start*.

Fedora innehåller SELinux, som kan medföra att Nagios stöter på problem då man försöker komma till övervakningssidan, för att lösa detta ska man skriva *chcon –R –t httpd_sys_content-t /usr/local/nagios/sbin/* och även *chcon –R –t http_sys_content-t /usr/local/nagios/share*.

När detta är gjort ska Nagios fungera och man kan logga in via webben. För att komma till övervakningssidan öppnar ni en webbläsare och skriver in *http://localhost/nagios/.* Ni kommer att bli ombedd att ange användarnamn och lösenord för att komma vidare.

5.3.7.5. Lägga till Windows-datorer att övervaka

För att lägga till datorer som har operativsystemet Windows installerat måste ni först ändra i en fil som heter *nagios.cfg* som finns i mappen */usr/local/nagios/etc/*. Det ni ska göra är att ändra så att Nagios letar efter Windows-datorer att övervaka och det gör ni genom att ta bort # före raden *cfg_file=/usr/local/nagios/etc/objects/windows.cfg*. Sen sparar ni filen och stänger den.

5.3.7.6. Installation av Windows agenten NSClient++

För att Nagios ska kunna övervaka Windows-maskiners interna tjänster, som t.ex. använt hårddiskutrymme, måste en agent installeras på var och en av dessa maskiner. Vi använde oss av agenten NSClient++ som finns att ladda ner på *http://sourceforge.net/projects/nscplus.* Det som behövs göras är att ladda ner agenten, sen packa upp den till mappen *C:\NSCLient++*. För att installera programmet öppnar ni kommandotolken och går till den mappen. Väl där skriver ni *nsclient++ /install*, samt *nsclient++ SysTray*.

För att se om NSClient++ är konfigurerat på rätt sätt ska ni kolla en del saker. Först ska ni gå till *Start, Kontrollpanelen, Administrationsverktyg* och sen till *Tjänster.* Där ska ni leta reda på ett inlägg som heter NSClientpp och öppna den och kryssa i, om det inte redan är det, rutan för *Allow service to interact with desktop*. En till sak som måste göras är att öppna filen *NSC.INI*, som finns i mappen *C:\NSClient++*, med en texteditor. Ni ska leta reda på ett avsnitt som heter *[modules]* och ta bort # före alla rader, förutom där det står *CheckWMI.dll* och *RemoteConfiguration.dll*. Ni måste även göra en ändring i avsnittet *[settings]* och ta bort # före *allowed_hosts* där ska ni istället lämna tomt så att alla kan ansluta till den. Ni ska även ta bort # före *port*, i avsnittet *[NSClient]* och se till att det portnumret *12489* står där. När alla ändringar är gjorda kan ni nu starta NSClient++ genom att skriva, i kommandotolken, *nsclient++ /start*. Om allt fungerade som det ska borde en ny ikon kommit fram längst ner till höger, bredvid klockan.

5.3.7.7. windows.cfg

För att Nagios överhuvudtaget ska kunna hitta dessa Windows-maskiner ni konfigurerat måste ni redigera en fil som heter *windows.cfg*. Det ni ska göra här är att ange information om varje dator, var för sig, som ni vill övervaka. Ni ska ange *host_name*, *alias* och *address*. Då vi la till en dator angav vi följande:

```
define host{
        use             windows-server  ;
        host_name       winserver1.test.log     ;
        alias           Windows övervaknings server
        address         172.16.8.50
        }
```

Fig.13 Exempel på hur man ska definiera en ny dator i filen *windows.cfg*

Detta måste anges för varje enskild dator ni vill ha övervakad.

När alla datorer som ni vill övervaka, är inlagda, är det dags att börja lägga till vad ni vill ha övervakat på dessa datorer. Detta görs också i filen *windows.cfg*. Ni måste ange ett test per dator i taget. Ett exempel på hur man kan skriva är:

```
define service{
        use                     generic-service
        host_name               winserver1.test.log
        service_description     NSClient++ Version
        check_command           check_nt!CLIENTVERSION
        }
define service{
        use                     generic-service
        host_name               winserver2.test.log
        service_description     NSClient++ Version
        check_command           check_nt!CLIENTVERSION
        }
```

Fig.14 Exempel på hur man kan definiera nya tester i filen *windows.cfg*

Här kollar Nagios vilken version av NSClient++ som finns installerat på servrarna *winserver1* och *winserver2*. Det finns självklart fler tester att göra på alla datorerna och dem kan ni läsa mer om på Nagios hemsida *www.nagios.org*.

När ni varit inne och ändrat i windows.cfg måste Nagios kontrolleras, vilket ni gör genom att skriva, i terminalfönstret:
/usr/local/nagios/bin/nagios –v /usr/local/nagios/etc/nagios.cfg och sen startar ni om Nagios med *service nagios restart*. För att se hela vår fil *windows.cfg*, titta i bilaga 11.5.

5.3.7.5. Lägga till Linux/Unix-datorer att övervaka

För att, på en Linux/Unix-dator, kunna övervaka exempelvis CPU och RAM-minnet måste en s.k. NRPE Daemon installeras på varje sådan dator, går att jämföra med NSClient++ för Windows-datorerna. Vi kommer gå igenom hur man gör för att lägga till en Fedora Core 6-dator till övervakningen med Nagios. Men det är liknande inställningar som görs på de flesta av Linux-distributionerna.

5.3.7.6. Installation av NRPE

För att övervakningen av Linux/Unix-datorer ska fungera måste följande göras på var och en av klienterna. Det första ni ska göra är att ni ska byta till root-användaren, genom att skriva *sudo –s* eller *su –l*. Detta för att ni ska få privilegier att skapa ett nytt konto. Ni ska skapa ett konto som heter nagios och som har lösenordet nagios, det gör ni med */usr/sbin/useradd nagios* och *passwd nagios*. Innan ni kan ladda hem och installera NRPE måste ni ladda hem plugins till Nagios.
Skriv *wget http://osdn.dl.sourceforge.net/sourceforge/nagiosplug/nagios-plugins-1.4.12.tar.gz*. Nästa steg är att packa upp dem och det gör ni med *tar xvf nagios-plugins-1.4.12.tar.gz*. Sen för att kunna kompilera och installera dem går ni in till mappen: *cd nagios-plugins-1.4.12.tar.gz*. För att nu kompilera filen skriver ni *./configure* och för att installera den skriver ni *make* och sen *make install*. En sak till måste göras innan pluginsen är klara, det är att ändra dess rättigheter. Det gör ni genom att skriva *chown nagios.nagios /usr/local/nagios* och *chown -R nagios.nagios /usr/local/nagios/libexec*. Beroende på Linux-distribution, kan det hända att xinetd inte är installerat och detta måste finnas. För att installera det skriver ni yum install xinetd.

För att ladda ner NRPE skriver man
wget http://osdn.dl.sourceforge.net/sourceforge/nagios/nrpe-2.12.tar.gz. Nästa steg är att packa upp det, ange då *tar xvf nrpe-2.12.tar.gz*. För att sen kunna kompilera och installera NRPE måste ni gå in i mappen *nrpe-2.12*, alltså *cd nrpe-2.12*. Kompilerar gör man med *./configure* och *make all*. Om allt verkar ok kan ni installera det med *make install-plugin, make install-daemon* och *make install-daemon-config*. Nästa steg är att installera NRPE till en service i xinetd, med hjälp av *make install-xinetd*. Om allt fungerar så här långt återstår ett fåtal saker att göra innan övervakningen kan börja. Filen */etc/xinetd.d/nrpe* måste redigeras så att IP-adressen till er Nagios server står skriven på raden *only_from*, raden ska se ut såhär:
only_from = 127.0.0.1 <Nagios-serverns IP-adress>.
En sak som också måste skrivas in, men i filen */etc/services/* är raden:
nrpe 5666/tcp #NRPE
Om allt är skrivet korrekt måste xinetd startas om, detta görs med *service xinetd restart*. När xinetd har startat är det säkrast om man testar att allt verkligen funkar som det ska, detta görs med *netstat –at | grep nrpe*, fungerar allt ok ska följande svar skrivas
*Tcp 0 0 *:nrpe *:* LISTEN*
Ett ytterligare test som kan göras är att skriva */usr/local/nagios/libexec/check_nrpe -H localhost* och funkar det ska ett svar komma som säger vilken version av NRPE som är installerat.

Om allt fungerar är nu klienterna konfigurerade klart. Det som måste göras nu är att konfigurera Nagios-servern. Först måste ni byta till root-användaren, genom att skriva *sudo –s* eller *su –l*. Sen ska ni ladda ner NRPE, detta görs genom att skriva
wget http://osdn.dl.sourceforge.net/sourceforge/nagios/nrpe-2.12.tar.gz.
Nästa steg är att packa upp det, ange då *tar xvf nrpe-2.12.tar.gz*. För att sen kunna kompilera och installera NRPE måste ni gå in i mappen *nrpe-2.12*, alltså *cd nrpe-2.12*. Kompilerar gör man med *./configure* och *make all*. Installerar gör man genom att skriva *make install-plugin*. För att nu testa att installationen av NRPE fungerade kan ni köra följande test */usr/local/nagios/libexec/check_nrpe -H <Klientens IP-adress>*. Om det fungerar ska ni få ett svar som visar vilken version av NRPE ni har, alltså *NRPE v2.12*. För att nu kunna använda NRPE måste ni definiera den i filen *commands.cfg*, som finns i mappen */usr/local/nagios/etc/*. Följande rader måste läggas till för att NRPE ska fungera:

```
define command{
        command_name    check_nrpe
        command_line    $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$
        }
```

Fig.15 Det som ska läggas till för att definiera NRPE, i filen *commands.cfg*

För att se hela vår fil *commands.cfg*, titta i bilaga 11.2.
När ni har definierat NRPE måste ni skapa en ny fil i mappen *objects*, som finns i */usr/local/nagios/etc/*. För att övervakningen av Linux/Unix-datorer ska fungera måste man definiera varje dator för sig, vilket man gör i den filen, som vi döpte till *linuxs.cfg*. För att göra det skriver man såhär:

```
define host{
        use                     linux-datorer
        host_name               Vir1UbuntuServer
        alias                   Ubuntu server 8.04
        address                 172.16.8.208
        }
```

Fig.16 Exempel på hur man lägger till en Linux/Unix-dator

För att se hela vår fil *linuxs.cfg*, titta i bilaga 11.4.

För att utföra olika tester på de datorer som lagts till måste de skrivas ett åt gången och för en dator i taget. För att testa hur mycket CPU som används på datorn Vir1Ubuntu skrev vi följande:

```
define service{
        use                     generic-service
        host_name               Vir1UbuntuServer
        service_description     CPU Load
        check_command           check_nrpe!check_load
        }
```

Fig.17 Exempel på ett test på en Linux/Unix-dator

För att sen Nagios ska veta att den ska söka efter enheter och tjänster, i den filen, måste ni ange sökvägen till den filen, i filen */usr/local/nagios/etc/nagios.cfg*. Det som vi la till för att Nagios skulle hitta filen var följande:

```
# Linux hosts
cfg_file=/usr/local/nagios/etc/objects/linuxs.cfg
```

Fig.18 Vår sökväg till *linuxs.cfg* filen, i filen *nagios.cfg*

Varje gång som någon av filerna redigeras måste ni köra dessa två kommandon, annars kommer inte Nagios att använda sig av de ni skrivit in:
/usr/local/nagios/bin/nagios –v /usr/local/nagios/etc/nagios.cfg och *service nagios restart*

5.3.8. Övervakning med Nagios

Övervakningen med Nagios är webbaserat, dvs. för att studera övervakningen går man in på en webbläsare och anger adressen *http://localhost/nagios*. Denna adress gäller om man sitter på datorn med Nagios installerat, annars byter man ut *localhost* mot IP-adressen till Nagios-servern. När man skrivit in adressen blir man tillsagd att skriva in användarnamn och lösenord, det som vi gjorde i punkt *5.3.7.2. Konfigurera webb-interfacet*. Då ni kommer in till Nagios-sidan ser ni att era datorer och tester, som ni lagt till, finns listade här och ni kan se statusen för varje enhet. I listan till vänster kan man välja vad för något man vill se. Om man t.ex. vill se statusen för alla datorer, går man in på *Host Detail*. Där visas en lista med datorerna, som man övervakar, och dess status. Om varje dator fungerar

och är påslagen står det *UP* på Statusen, men om en dator inte är nåbar står det istället *DOWN*.

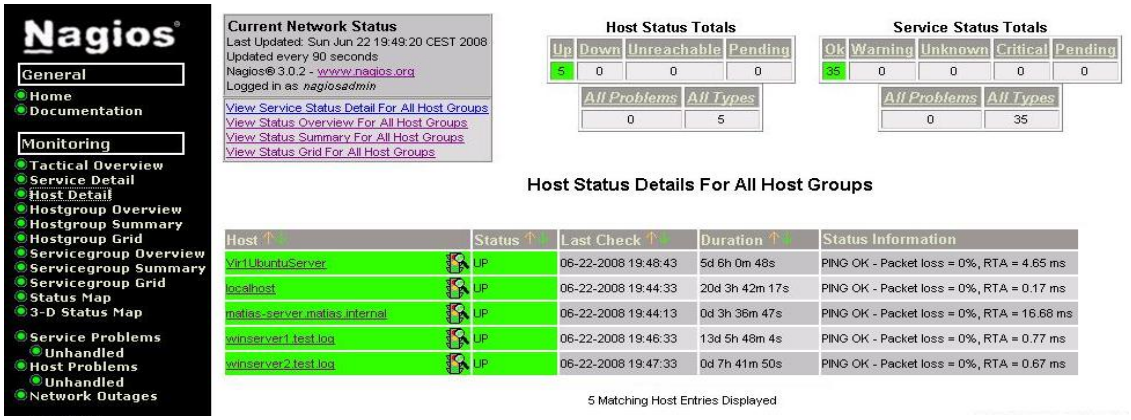

Fig.19 Statusen för våra övervakade datorer

För att se själva övervakningen, alla tester som körs på varje dator, trycker ni på *Service Detail* i listan till vänster. Rutan som då kommer upp visar datorerna, testerna samt lite information om varje. Om det skulle vara så att en tjänst inte fungerar som den ska, blir det *CRITICAL* istället för *OK*. Sker detta står det en förklaring om varför i kolumnen för *Status Information*.

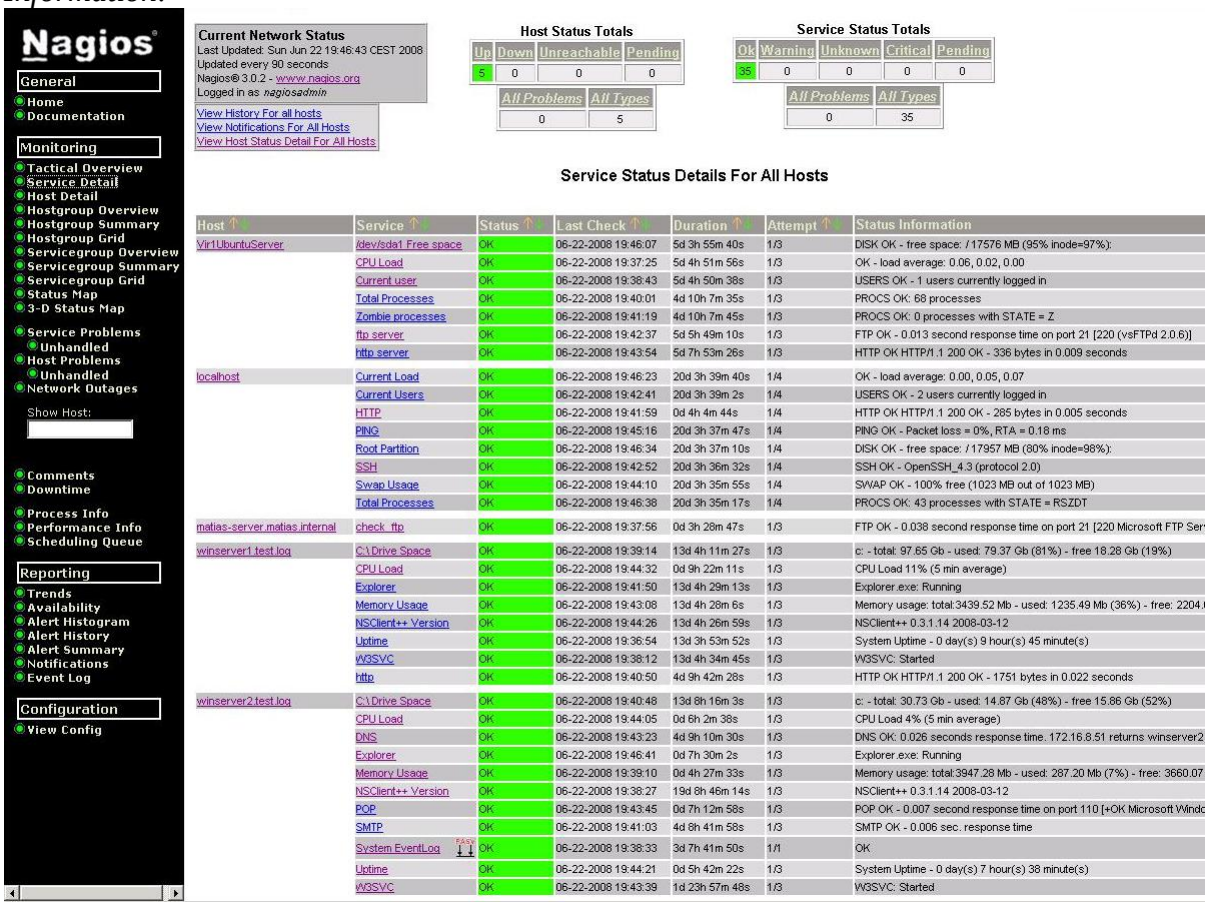

Fig.20 Bild på våra datorer samt de tester som körs på var och en av dem

5.3.8.1. Meddelande till administratören

För att inte behöva sitta inne på övervakningssidan hela tiden kan man ställa in att Nagios skickar meddelande till berörda personer, då något problem uppstår. Dessa meddelanden

kan skickas antingen via mail eller SMS. Vi har ställt in att vi får mail varje gång ett problem dyker upp. För att ställa in det i Nagios redigerar man filen:
/usr/local/nagios/etc/objects/contacts.cfg. Det som ska läggas till för att mailen ska fungera är följande:

```
define contact{
        contact_name                    nagiosadmin
        use                             generic-contact
        alias                           Nagios Admin

        email                           administrator@test.log
        }
```

Fig.21 Hur man ställer in så att mail skickas i Nagios

För att det överhuvudtaget ska fungera att låta Nagios skicka iväg mail, till den angivna adressen, måste det finnas en fungerande mailservice.

5.3.9. Våra synpunkter om Nagios

För att vara ett Linux-baserat övervakningssystem tycker vi att Nagios har varit det övervakningssystem som fungerat bäst av dem som vi provat på. Det har varit smidigast att installera klientverktyg, både på Windows-datorerna och på andra Linux/Unix-datorer.

Nagios är, precis som Big Brother, webbaserat vilket är en bra fördel, då man har åtkomst till övervakningssidan från Internet, förutsatt att man har den tillåtelsen.

En annan fördel med Nagios, som vi tycker är väldigt bra, är att Nagios är Open Source. Dvs. det är gratis att ladda ner och använda, till skillnad från de andra två övervakningssystemen vi testade.

Testerna som kan utföras av Nagios är väldigt bra, det går att testa det vanligaste, exempelvis DHCP, FTP och DNS men det går även att övervaka Windows Event-log. Detta är bra för att om Nagios inte skulle kunna övervaka en viss tjänst, på en Windows-dator, kan Nagios övervaka Event-loggen och rapportera om något är fel i den istället, detta har vi dock inte lyckats få att fungera, men det ska gå och det finns manualer att följa på Internet om hur man gör.

En fördel med Nagios, om man jämför det med SCOM 2007, är att det går att övervaka datorer som är med i olika domän eller inte med i någon domän alls.

Vi tror att Nagios passar ganska bra till alla typer av företag, oavsett storlek och vad för typ av operativsystem som används mest. Men det vore bra om företaget har åtminstone en person som är duktig på Linux/Unix, så att denne kan installera och konfigurera Nagios så att det funkar. Det är egentligen bara övervakningsdatorn som har Nagios som måste ha Linux/Unix, alla datorer som den i sin tur övervakar kan ju enbart bestå av Windows-operativsystem.

6. Slutsats

Vi har kommit fram till att SCOM 2007 fungerar bra om man enbart vill övervaka en domän innehållande nästan bara Windows-datorer. Medan Big Brother 4 och Nagios inte är beroende av om datorerna, som övervakas, är med i någon domän eller inte. De båda kan även övervaka flera olika typer av operativsystem, så som Windows, Linux eller Unix. Datorn som SCOM installeras på kräver betydligt mer prestanda än en installation av Big Brother 4 eller Nagios. Något som är bra med Nagios och Big Brother 4 är att de använder sig av mindre prestanda som medför att datorn inte belastas lika hårt.

När vi har testat alla tre övervakningssystemen har vi kommit fram till att vi tycker att SCOM 2007 innehåller allt för mycket saker att välja mellan, så att det blir svårt att få ett bra grepp om det.

Jämför man Big Brother 4 och Nagios tycker vi att Nagios verkar vara det som är lite bättre. Detta tack vare att det går att övervaka flera olika tjänster och det fungerade bättre att övervaka Linux/Unix-datorer. Men vi tyckte däremot att installationen av Big Brother 4 gick smidigare än den i Nagios, då Big Brothers installation går att genomföra genom att enbart trycka Next, Next, Next… Och var på så sätt fungerande inom 15 minuter, men då var det enbart övervakning på Big Brother-servern som var igång.

Om man vill ha övervakning på ett företags datormiljö innehållande Microsoft Windows Active Directory med dess olika komponenter, tycker vi att den bästa lösningen är att använda sig av både av SCOM 2007 och Nagios alternativt Big Brother 4, om man inte vill ha en Linux-dator. Vi tycker att dessa övervakningssystem kompletterar varandra genom att SCOM 2007 kan övervaka väldigt många olika Microsoft-tjänster medans Nagios har en mer simplare koll på att alla tjänster, oberoende av om det är Microsoft-produkter eller inte, svarar som de ska. Nagios kan även övervaka Linux/Unix-datorer, samt datorer på flera olika domäner, vid behov.

Vi tycker att de bästa vore att börja med att övervaka sitt nätverk med Nagios, till att börja med. Visar det sig att det räcker kan man nöja sig med enbart Nagios. Om Nagios inte räcker till kan man senare komplettera med SCOM 2007. Det är onödigt att först betala för SCOM 2007, om det sen visar sig att Nagios räcker, med tanke på att Nagios är gratis.

7. Fortsättning av eventuella efterföljande studenter

När vi har arbetat med detta examensarbete har en del frågor dykt upp som vi inte haft tid att få svar på. Vi tänkte att om det kommer efterföljande studenter, som är intresserade av övervakningssystem och detta examensarbete, att de kan ta reda på lite mer om vart och ett av dessa och kanske få svar på de frågor vi inte hann med.

7.1. SCOM 2007

Det som störde oss mest var att vi inte lyckades få till övervakning på datorer som befann sig i en annan domän, eller inte var med i någon domän alls. Finns det något tillägg att ladda ner och installera för att detta ska fungera? Om det inte finns, kanske det finns ett annat övervakningssystem från Microsoft som klarar detta.

En till sak som vi inte riktigt hunnit testa är om det finns stöd för att övervaka datorer som har operativsystemen Linux eller Unix installerat.

7.2. Big Brother 4

Det var egentligen inte mycket vi störde oss på vad gäller Big Brother 4, förutom att vi tyckte det fanns lite väl få tjänster att övervaka.

7.3. Nagios

Med Nagios tycker vi att en djupare undersökning om hur övervakningen av Windows Event-log fungerar, då vi inte haft tid att göra detta och få det att fungera som det ska.

8. Enkel sammanställning av alla övervakningssystem

Övervakningssystem	**Installation** Stödda operativsystem	**Övervakning** Stödda system	**Open source**	**Övervaknings begränsningar**	**Kostnad**	**Installationstid**	**Övrigt**
SCOM 2007	Microsoft Windows Server 2003, Kan nog även installeras på Windows Server 2000. Senare lär det även gå att installera på Windows Server 2008.	Microsofts produkter, Linux, Oracle, SAP.	Nej	2000 agenter per server och 5000 agenter per grupp kan övervakas. 25000 agentlösa datorer kan övervakas.	180 dagars trial. En licens kostar $573.	N/A	Handelsbanken, Banverket använder sig av SCOM.
Op5 Network Management Suite	CentOS 5, RedHat Enterprise 5.	Windows och Linux/Unix system.	Ja	Max 1000 hosts och 5000 tjänster.	Trial finns. En licens kostar från 937kr till 5225kr/månad, beroende på licenslängd och antal övervakade klienter.	10 min	Aftonbladet, tullverket och Volvo använder Op5. Bygger på Nagios.
BMC Performance Manager	Windows och Linux/Unix	SUSE, RedHat, AIX, Solaris, TRU64 och Windows server.	Nej	N/A	N/A	N/A	Swedbank IT använder BMC Softwares produkter.
Tadcom AB's NetZonar	Det är på egen hårdvara.		Nej	N/A	Ingen trial, medföljande hårdvara krävs.	N/A	Kommer med separat hårdvara.
Hyena	Windows NT/2000/XP/Vista	Windows NT/2000/XP/Server 2003	N/A	N/A	30 dagars trial. Licens kostar $200-$12000 beroende på hur många licenser man köper.	N/A	N/A

Microsoft System Center Essentials 2007	Windows Server 2003 SP1 med IIS 6.0 och BITS 2.0	Windows 2000 SP4 (PRO och server), XP SP2, Vista, Server 2003 SP1	Nej	N/A	90 dagars trial. En licens kostar $2000.	Mindre än 1 timme.	Kan uppdatera datorerna på nätverket.
Quest Software's Big Brother 4	Red Hat Enterprise Server 3.0/4.0, SUSE Enterprise Linux 9.0/10.0, Sun Solaris 6 eller senare, HP-UX 11.0 or 11i, AIX 5.1, 5.2 or 5.3, Windows 2000 Server eller Professional, Windows 2003 Server, Windows XP.	Windows och Linux/Unix	Nej	N/A	Trial finns. Inga uppgifter på vad en ev. licens kostar.	15-30 minuter	Webbaserad övervakning.
Intellipool AB's Network Monitor	Windows 2000, Windows XP, Windows 2003.	AIX (4.2 and above), CentOS, Debian, Fedora, FreeBSD, HP-UX, OpenBSD, OpenSUSE 10.2, Red Hat Enterprise Server, Solaris, Ubuntu, Windows NT, 2000, XP, 2003 och Vista.	Nej	Max 2500 objekt.	En licens kostar mellan $100 och $4369 beroende på licenstid och till hur många objekt.	N/A	N/A
ServersCheck Monitoring	Windows 2000/XP/Server 2003	Windows och Linux	Nej	N/A	21 dagars trial. En licens kostar från €399 till €2399.	N/A	Finns att installera på 38 olika språk.
Spong – System and Network Monitoring	Linux/ Unix med Pearl	Linux/Unix	Ja	N/A	Gratis	N/A	N/A

Netplex's SNIPS	Unix system med Pearl	Unix system plus dina egenskrivna monitors i Pearl/C	Nej	Ca 2000 enheter.	Gratis	N/A	N/A
Linux System Group's Mon	Med Pearl	W3C, Windows events, Syslog	Ja		Gratis	N/A	N/A
GFI Software's GFI EventsManager	Windows 2000/XP/2003/VISTA/Server 2008		Nej	> 500	30 dagars trial. En licens kostar från $767 till över $30000 beroende på hur många enheter.	N/A	N/A
Up.time 4	Windows och Linux/Unix	Windows och Linus/Unix		5 till 5000+ servrar	Ingen trial då medföljande hårdvara krävs.	15 min	Kommer med separat hårdvara.
Nagios	Linux/Unix	Windows och Linux/Unix	Ja	N/A	Gratis	15 min	Webbaserad övervakning.

(Informationen om övervakningssystemen är hämtade från deras egna hemsidor, 2008-04-22)

9. Sammanställning av SCOM 2007, Big Brother 4 och Nagios

9.1. Microsoft System Center Operations Manager 2007

	Installation	**Konfiguration**	**Övervakning**	**Kostnad (Tid/Resurser)**	**Fördelar**	**Nackdelar**	**Passande företag**
SCOM 2007	Innan installationen kan starta måste man köra en s.k. ”för-koll” för att fastslå att alla program och tjänster, som SCOM kräver, är installerade och korrekt konfigurerade. Saknas något får man reda på hur man går tillväga för att rätta problemet. Installationen är rätt så enkel och lätt att förstå, men tar rätt så lång tid. Kräver en del andra program och tjänster, men SCOM visar vilka dessa är.	Relativt lätt att lägga till nya datorer om de är medlemmar i samma domän. Svårare att lägga till datorer utanför domänet, vi har inte lyckats. Tar för givet att det ska gå. Kan heller inte lägga till datorer som inte är med i någon domän alls, när sökningen efter nya datorer i nätverket görs, måste man ange ett domännamn för att det ska fungera… Vi tycker att även detta borde fungera att lägga till men vi har inte haft någon lycka med att hitta en lösning på hur man ska gå till väga.	Att komma igång med övervakningen med SCOM 2007 är rätt så komplicerad. Det tar väldigt lång tid innan allt är ”up and running” Övervakningen med SCOM täcker det mesta tänkbara som en övervakning ska innehålla Förutom tester som DNS och PING finns även tester för t.ex. Active Directory och att Windows fungerar som det ska.	Tar lång tid att installera och få igång alla tillägg som krävs innan en fungerande övervakning finns. När fel uppstår är det relativt lätt att förstå vad som är fel och vad som ska göras för att lösa felet. Det går att lösa de flesta problem via SCOM-fönstret, då det går att ansluta till den felande datorn direkt i programmet.	Bra med en ”för-koll” innan installation, så att alla program och tjänster som krävs, är installerade och fungerande. Omfattande övervakning som klarar det mesta. Blir något fel, kan man för det mesta fixa det direkt i SCOM, med hjälp av inbyggda program som *Computer Management* och *Remote Desktop*.	Vi stötte på problem med installationen, fast än att allt var ok på den s.k. ”för-kollen”. När sen installationen fastnade var det svårt att veta vad som var fel och hur man skulle göra för att få det att fungera. Komplicerat att lägga till enheter som är utanför domänet SCOM är inte gratis. En licens kostar, den 19 juni 2008, $573.	SCOM passar de företag som har tid och resurs för ett lite mer komplext övervakningssystem. Då det väl är igång är det ett mycket bra övervakningssystem som övervakar det mesta i ett nätverk. Om det stämmer att endast datorer i samma domän kan övervakas och ett företag har flera olika domän, måste de kunna ha en dator, som fungerar som övervakare, för vart och ett av domänen.

9.2. Quest Softwares Big Brother 4

	Installation	Konfiguration	Övervakning	Kostnad (Tid/Resurser)	Fördelar	Nackdelar	Passande företag
Big Brother 4	Mycket simpel installation. Kräver at en fungerande webbserver finns, det går alldeles utmärkt at använda sig av Microsofts egen webbserver *IIS*. Från installationsstart till fungerande övervakning tog det ca 20 minuter, men då övervakas enbart datorn som Big Brother installerades på.	Lätt att lägga till/ta bort enheter/tjänster att övervaka. Finns det en fungerande mailserver går det ganska lätt att konfigurera så att Big Brother skickar mail till ansvariga personer, då något hänt.	Webbaserad övervakning som är lätt att överskåda och förstå. Eftersom övervakningen är webbaserad kommer man åt övervakningssidan från vilken dator som helst, förutsatt att den är tillåten att ansluta sig till den datorn via nätet. Vi hade problem med övervakning av Linux/Unix-maskiner. Big Brother-Client fanns endast till ett fåtal Linux/Unix distributioner, vilket var ett klart minus.	Att komma igång med Big Brother 4 går snabbt och är lättskött. Övervakningen går smidigt och är lätt att förstå, vad gäller typ av fel och hur man löser problemet. Då det går att komma åt övervaknings-sidan från Internet, är inte ansvarig person/personer låste till en specifik dator, vilket är mycket bra.	Enkelt att installera, konfigurera och övervaka. Webbaserad övervakning som kan överblickas från vilken dator som helst, om den har tillåtelse. Meddelande om fel skickas enkelt via mail, fungerar även via sms och personsökare, det är alltså lätt att få reda på om något är fel.	Kan övervaka endast ett begränsat antal Linux/Unix-distributioner, vanliga Linux-distributioner som Fedora Core 6 och Ubuntu fungerar inte med Big Brother-Client. Vad vi vet går det inte att övervaka exempelvis Event-loggen. Big Brother är inte gratis, fast vi har tyvärr inte hittat vad det kostar att köpa en licens.	Små och medelstora företag som vill övervaka tjänster som t.ex. DNS, http, mail osv. Passar såklart även stora företag som vill göra detta. IT-avdelningen behöver inte alls vara stor för att sköta Big Brother 4, då det är simpelt att överblicka. Passar företag som i första hand har datorer med Windows som operativsystem, då det var komplicerat att övervaka Linux/Unix. Vi inte kunde utföra en del av de tester, vi ville göra, på datorer med Linux/Unix.

9.3. Nagios

	Installation	Konfiguration	Övervakning	Kostnad (Tid/Resurser)	Fördelar	Nackdelar	Passande företag
Nagios	Nagios har inga speciella systemkrav vad gäller CPU, RAM-minne etc. Det enda Nagios kräver är en dator med ett Linux-operativsystem installerat, fungerar även på en del Unix. För att installationen ska fungera måste en del saker vara installerade, som t.ex. en fungerande Apache-server. En sak till som behövs är en speciell användare samt en till grupp. Dessa används senare i installationen. Installationen går hyfsat smidigt, förutsatt att kunskaperna om hur Linux fungerar, är relativt bra. För hela installationen sker via terminalfönstret.	Konfigurationen sker, som installationen, via terminalfönstret. För att lägga till de datorer, man vill övervaka, öppnar man speciella filer i Nagios-mappen. I dessa filer lägger man även in vad som man vill ha övervakat på var och en av datorerna. För att Nagios ska använda sig av de nya inställningarna startar man och stoppar tjänsten, då får man även reda på om något av de man skrivit var fel och hur man rättar till det.	Övervakning med Nagios är webbaserad, vilket betyder att man kan kolla sin övervakning från vilken dator som helst, förutsatt att den har Internet och har tillåtelse att ansluta till datorn via nätet. Övervakningen är lätt att förstå och uppstår ett problem med någon dator får man reda på det direkt via t.ex. mail. Med Nagios går det att övervaka alla datorer, oavsett vilket domän de är med i. Det går även att övervaka datorer som inte är med i någon domän alls.	Då Nagios är gjort för att installeras på en Linux-maskin krävs det att de ansvariga är kunniga på detta. Det tar ett tag att installera, konfigurera och starta övervakningen, då det måste ändras i en del filer. Alla tester som ska göras på datorerna skrivs in ett och ett på varje enskild dator, vilket tar lång tid att göra.	En av de största, kanske till och med den största, fördelen med Nagios är att det är Open Source, dvs. det är gratis att ladda ner och använda. Eftersom Nagios är webbaserat kan man, som redan nämnt, komma åt övervakningssidan från vilken dator som helst. Övervakningssidan är enkel att tyda och det är lätt att ta reda på vad som är fel, då något händer, och vad som behövs göras för att laga det. Går att övervaka alla datorer, oavsett om de är med i en domän eller inte. Går även att övervaka datorer som är med i olika domän.	Tar rätt så lång tid att komma igång med själva övervakningen, då man måste redigera filerna manuellt. Testerna som ska göras måste skrivas in för varje enskild dator. Testerna som skrivs in är mycket mer komplexa i Nagios än om man jämför med de tester som skrevs i Big Brother 4.	Nagios passar ganska bra till alla typer av företag, oavsett storlek och vad för typ av operativsystem som används mest. Men det vore bra om företaget har åtminstone en person som är duktig på Linux/Unix, så att denne kan installera och konfigurera Nagios så att det funkar. Det är egentligen bara övervakningsdatorn som har Nagios som måste ha Linux/Unix, alla datorer som den i sin tur övervakar kan ju enbart bestå av Windows-operativsystem.

10. Källförteckning

10.1 Här hittades informationen

1) SCOM 2007
Namn: System Center Operations Manager 2007
Adress: www.microsoft.com/systemcenter/opsmgr/default.mspx
Senast besökt: 2008-04-21

2) Op5
Namn: Op5, Nätverksövervakning, Övervakningssystem
Adress: www.icron.se/produkter/natovervakning.htm
Senast besökt: 2008-04-21

3) BMC
Namn: BMC Software Products
Adress: www.bmc.com/products
Senast besökt: 2008-04-21

4) NetZonar
Namn: TadCom - NetZonar - Driftövervakning
Adress: www.tadcomab.se/index.php?option=com_content&task=view&id=22&Itemid=1
Senast besökt: 2008-04-21

5) Hyena
Namn: SystemTools Software NT/XP/200x System Management Software
Adress: www.systemtools.com/hyena/index.html
Senast besökt: 2008-04-21

6) SYScenter
Namn: System Center Essentials 2007
Adress: www.microsoft.com/systemcenter/essentials/default.mspx
Senast besökt: 2008-04-21

7) BigBrother 4
Namn: System and Network Monitoring Software, BigBrother
Adress: http://bb4.com/
Senast besökt: 2008-04-21

8) Intellipool
Namn: Intellipool | Network Monitoring and Server Monitoring Software
Adress: www.intellipool.se/
Senast besökt: 2008-04-21

9) ServersCheck
Namn: Monitoring Software for Server Room Monitoring and Network Monitoring
Adress: www.serverscheck.be/monitoring_software/
Senast besökt: 2008-04-21

10) Spong
Namn: Spong – Systems and Network Monitoring
Adress: http://spong.sourceforge.net/
Senast besökt: 2008-04-21

11) SNIPS
Namn: SNIPS- Network Management and Server Monitoring Software
Adress: www.netplex-tech.com/snips/
Senast besökt: 2008-04-21

12) Mon
Namn: Main Page - Mon Wiki
Adress: http://mon.wiki.kernel.org/index.php/Main_Page
Senast besökt: 2008-04-21

13) GFI
Namn: Centralized event log management, security and monitoring
Adress: www.gfi.com/eventsmanager/
Senast besökt: 2008-04-21

14) up.time
Namn: up.time software
Adress: www.uptimesoftware.com/hpux.php
Senast besökt: 2008-04-21

15) Nagios
Namn: Nagios: Home
Adress: www.nagios.org/
Senast besökt: 2008-04-21

16) SMARTS InCharge
Namn: SMARTS InCharge - Network System Architects, Inc.
Adress: http://www.nsai.net/products/incharge-asm.shtml
Senast besökt: 2008-06-25

10.2 Demo av valda produkter finns här

1) SCOM
Namn: Utvärdera Microsoft System Center Operations Manager 2007 SP1
Adress: http://technet.microsoft.com/sv-se/bb738014.aspx
Senast besökt: 2008-04-21

7) BigBrother 4
Namn: Request FREE Trial of the NEW Big Brother Professional Edition 3.3
Adress: www.quest.com/landing/?ID=592
Senast besökt: 2008-04-21

15) Nagios
Namn: Nagios: Downloads
Adress: http://www.nagios.org/download/
Senast besökt: 2008-04-21

11. Bilagor

11.1 Företagen som var med i undersökningen

En av metoderna vi använde oss av då vi sökte efter vad för övervakningssystem som finns ute på marknaden, var att vi mailade ett antal företag och helt enkelt frågade vad de använde sig av. I spalten ”Företag” listar vi de företag som vi har kontaktat. I spalten ”Kontakt” anger vi hur vi tog kontakt med respektive företag. Under ”Svarat” har vi angivit om vi har fått ett svar eller inte. I spalten ”Använder” så beskriver vi vad vi har fått för svar, oavsett om svaret blivit att företaget inte lämnar ut sådan information eller om vi fått ett specifikt produktnamn.

Företag	Kontakt	Svarat	Använder
Microsoft	carinae@microsoft.com (Personalchef)	Ja	SCOM 2007 + en del mindre system.
Cisco	info-sverige@cisco.com	Nej	----------
AMS	ams-it-enhet@ams.amv.se	Nej	----------
Logica (WM-Data)	PR och informationsansvarig Mats Nilsson Hahne	Ja	Använder ett internutvecklat system.
Kista Science City	Projektansvarig Tomas Bennich	Nej	----------
SYSteam	info@systeam.se	Ja	Sekretess.
Svenska Pass	mats.sonnerup@svenskapass.se	Ja	Sekretess.
SundIT	info@sundit.se	Nej	----------
Cypoint	info@cypoint.se	Nej	----------
Invid	stockholm@invid.se	Ja	Ingen övervakning.
Securia	tekniker@securia.se	Nej	----------
Rikspolisstyrelsen	rikspolisstyrelsen@polisen.se	Ja	Hade inte tid att svara, men skulle återkomma snarast möjligt.
Pocket Mobile	info@pocketmobile.se	Nej	----------
TimeBiz	info@timebiz.se	Nej	----------
Bomankerer	info@bomankerer.se	Nej	----------
Scania	it@scania.com	Nej	----------
Stomp	info@stomp.se	Nej	----------
IT-Hantverkarna	IT chef Magnus Olsson	Nej	----------
N2a	info@n2a.se	Nej	----------
Emric	info@emric.com	Ja	Hänvisades till Anders Carlsson, men han svarade inte.
Sun	Professional Services Delivery Manager Ulf Bylund	Ja	Undrade vad för typ av information vi ville ha. Efter det har han inte svarat.
Pc city	kundcenter@pccity.se	Ja	Sekretess
Datainspektionen	datainspektionen@datainspektionen.	Ja	Använder ingen

	se		övervakning.
Swedbank IT	Mats Falk (Swedbank IT)	Ja	BMC Softwares produkter
Nordea	info@nordea.se	Ja	TWS (Tivoli)
Ericsson	Frågeformulär på hemsidan	Ja	Outsourcad till HP
Omicron	ceti@omicron.se	Nej	----------
Netsafe	info@netsafe.se	Nej	----------
Piratebay	Frågeformulär på hemsidan	Ja	Har ingen övervakning.

11.2 commands.cfg

```
##############################################################################
####
# COMMANDS.CFG - SAMPLE COMMAND DEFINITIONS FOR NAGIOS 3.0.2
#
# Last Modified: 05-31-2007
#
# NOTES: This config file provides you with some example command
definitions
#        that you can reference in host, service, and contact definitions.
#
#        You don't need to keep commands in a separate file from your other
#        object definitions.  This has been done just to make things easier
to
#        understand.
#
##############################################################################
####


##############################################################################
#####
#
# SAMPLE NOTIFICATION COMMANDS
#
# These are some example notification commands.  They may or may not work
on
# your system without modification.  As an example, some systems will
require
# you to use "/usr/bin/mailx" instead of "/usr/bin/mail" in the commands
below.
#
##############################################################################
#####


# 'notify-host-by-email' command definition
define command{
        command_name    notify-host-by-email
        command_line    /usr/bin/printf "%b" "***** Nagios
*****\n\nNotification Type: $NOTIFICATIONTYPE$\nHost: $HOSTNAME$\nState:
$HOSTSTATE$\nAddress: $HOSTADDRESS$\nInfo: $HOSTOUTPUT$\n\nDate/Time:
$LONGDATETIME$\n" | /bin/mail -s "** $NOTIFICATIONTYPE$ Host Alert:
$HOSTNAME$ is $HOSTSTATE$ **" $CONTACTEMAIL$
        }

# 'notify-service-by-email' command definition
define command{
        command_name    notify-service-by-email
        command_line    /usr/bin/printf "%b" "***** Nagios
*****\n\nNotification Type: $NOTIFICATIONTYPE$\n\nService:
$SERVICEDESC$\nHost: $HOSTALIAS$\nAddress: $HOSTADDRESS$\nState:
$SERVICESTATE$\n\nDate/Time: $LONGDATETIME$\n\nAdditional
Info:\n\n$SERVICEOUTPUT$" | /bin/mail -s "** $NOTIFICATIONTYPE$ Service
Alert: $HOSTALIAS$/$SERVICEDESC$ is $SERVICESTATE$ **" $CONTACTEMAIL$
        }
```

```
##############################################################################
#####
#
# SAMPLE HOST CHECK COMMANDS
#
##############################################################################
#####


# This command checks to see if a host is "alive" by pinging it
# The check must result in a 100% packet loss or 5 second (5000ms) round
trip
# average time to produce a critical error.
# Note: Five ICMP echo packets are sent (determined by the '-p 5' argument)

# 'check-host-alive' command definition
define command{
        command_name    check-host-alive
        command_line    $USER1$/check_ping -H $HOSTADDRESS$ -w 3000.0,80% -
c 5000.0,100% -p 5
        }

define command{
       command_name    check_nrpe
       command_line    $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$
       }


##############################################################################
#####
#
# SAMPLE SERVICE CHECK COMMANDS
#
# These are some example service check commands.  They may or may not work
on
# your system, as they must be modified for your plugins.  See the HTML
# documentation on the plugins for examples of how to configure command
definitions.
#
# NOTE:  The following 'check_local_...' functions are designed to monitor
#        various metrics on the host that Nagios is running on (i.e. this
one).
##############################################################################
#####

# 'check_local_disk' command definition
define command{
        command_name    check_local_disk
        command_line    $USER1$/check_disk -w $ARG1$ -c $ARG2$ -p $ARG3$
        }


# 'check_local_load' command definition
define command{
        command_name    check_local_load
        command_line    $USER1$/check_load -w $ARG1$ -c $ARG2$
        }


# 'check_local_procs' command definition
```

```
define command{
        command_name    check_local_procs
        command_line    $USER1$/check_procs -w $ARG1$ -c $ARG2$ -s $ARG3$
        }


# 'check_local_users' command definition
define command{
        command_name    check_local_users
        command_line    $USER1$/check_users -w $ARG1$ -c $ARG2$
        }


# 'check_local_swap' command definition
define command{
        command_name    check_local_swap
        command_line    $USER1$/check_swap -w $ARG1$ -c $ARG2$
        }


# 'check_local_mrtgtraf' command definition
define command{
        command_name    check_local_mrtgtraf
        command_line    $USER1$/check_mrtgtraf -F $ARG1$ -a $ARG2$ -w $ARG3$
-c $ARG4$ -e $ARG5$
        }


################################################################################
#####
# NOTE:  The following 'check_...' commands are used to monitor services on
#        both local and remote hosts.
################################################################################
#####

# 'check_ftp' command definition
define command{
        command_name    check_ftp
        command_line    $USER1$/check_ftp -H $HOSTADDRESS$ $ARG1$
        }


# 'check_hpjd' command definition
define command{
        command_name    check_hpjd
        command_line    $USER1$/check_hpjd -H $HOSTADDRESS$ $ARG1$
        }


# 'check_snmp' command definition
define command{
        command_name    check_snmp
        command_line    $USER1$/check_snmp -H $HOSTADDRESS$ $ARG1$
        }


# 'check_http' command definition
define command{
        command_name    check_http
        command_line    $USER1$/check_http -I $HOSTADDRESS$ $ARG1$
        }
```

```
# 'check_ssh' command definition
define command{
        command_name    check_ssh
        command_line    $USER1$/check_ssh $ARG1$ $HOSTADDRESS$
        }


# 'check_dhcp' command definition
define command{
        command_name    check_dhcp
        command_line    $USER1$/check_dhcp $ARG1$
        }


# 'check_ping' command definition
define command{
        command_name    check_ping
        command_line    $USER1$/check_ping -H $HOSTADDRESS$ -w $ARG1$ -c
$ARG2$ -p 5
        }


# 'check_pop' command definition
define command{
        command_name    check_pop
        command_line    $USER1$/check_pop -H $HOSTADDRESS$ $ARG1$
        }


# 'check_imap' command definition
define command{
        command_name    check_imap
        command_line    $USER1$/check_imap -H $HOSTADDRESS$ $ARG1$
        }


# 'check_smtp' command definition
define command{
        command_name    check_smtp
        command_line    $USER1$/check_smtp -H $HOSTADDRESS$ $ARG1$
        }


# 'check_tcp' command definition
define command{
        command_name    check_tcp
        command_line    $USER1$/check_tcp -H $HOSTADDRESS$ -p $ARG1$ $ARG2$
        }


# 'check_udp' command definition
define command{
        command_name    check_udp
        command_line    $USER1$/check_udp -H $HOSTADDRESS$ -p $ARG1$ $ARG2$
        }


# 'check_nt' command definition
define command{
```

```
        command_name    check_nt
        command_line    $USER1$/check_nt -H $HOSTADDRESS$ -p 12489 -v $ARG1$
$ARG2$
        }

#check dns
define command{
        command_name    check_dns
        command_line    $USER1$/check_dns -H $HOSTADDRESS$
        }

#check log
define command{
        command_name    check_log
        command_line    $USER1$/check_log -F $ARG1$
        }

define command{
        command_name    check_dummy
        command_line    $USER1$/check_dummy $ARG1$
        }

#define command{
#       command_name    check_nrpe
#       command_line    $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARGS1$
#       }

###############################################################################
#####
#
# SAMPLE PERFORMANCE DATA COMMANDS
#
# These are sample performance data commands that can be used to send
performance
# data output to two text files (one for hosts, another for services).  If
you
# plan on simply writing performance data out to a file, consider using the
# host_perfdata_file and service_perfdata_file options in the main config
file.
#
###############################################################################
#####

# 'process-host-perfdata' command definition
define command{
        command_name    process-host-perfdata
        command_line    /usr/bin/printf "%b"
"$LASTHOSTCHECK$\t$HOSTNAME$\t$HOSTSTATE$\t$HOSTATTEMPT$\t$HOSTSTATETYPE$\t
$HOSTEXECUTIONTIME$\t$HOSTOUTPUT$\t$HOSTPERFDATA$\n" >>
/usr/local/nagios/var/host-perfdata.out
        }

# 'process-service-perfdata' command definition
define command{
        command_name    process-service-perfdata
        command_line    /usr/bin/printf "%b"
"$LASTSERVICECHECK$\t$HOSTNAME$\t$SERVICEDESC$\t$SERVICESTATE$\t$SERVICEATT
EMPT$\t$SERVICESTATETYPE$\t$SERVICEEXECUTIONTIME$\t$SERVICELATENCY$\t$SERVI
CEOUTPUT$\t$SERVICEPERFDATA$\n" >> /usr/local/nagios/var/service-
perfdata.out
        }
```

11.3. contacts.cfg

```
##############################################################################
####
# CONTACTS.CFG - SAMPLE CONTACT/CONTACTGROUP DEFINITIONS
#
# Last Modified: 05-31-2007
#
# NOTES: This config file provides you with some example contact and
contact
#        group definitions that you can reference in host and service
#        definitions.
#
#        You don't need to keep these definitions in a separate file from
your
#        other object definitions.  This has been done just to make things
#        easier to understand.
#
##############################################################################
####



##############################################################################
####
##############################################################################
####
#
# CONTACTS
#
##############################################################################
####
##############################################################################
####

# Just one contact defined by default - the Nagios admin (that's you)
# This contact definition inherits a lot of default values from the
'generic-contact'
# template which is defined elsewhere.

define contact{
        contact_name                    nagiosadmin          ; Short name
of user
       use                            generic-contact        ; Inherit
default values from generic-contact template (defined above)
        alias                           Nagios Admin         ; Full name of
user

        email                           administrator@test.log       ;
<<***** CHANGE THIS TO YOUR EMAIL ADDRESS ******
        }



##############################################################################
####
##############################################################################
####
#
# CONTACT GROUPS
#
```

```
##############################################################################
####
##############################################################################
####

# We only have one contact in this simple configuration file, so there is
# no need to create more than one contact group.

define contactgroup{
        contactgroup_name       admins
        alias                   Nagios Administrators
        members                 nagiosadmin
        }
```

11.4. linuxs.cfg

```
define host{
        name                    linux-datorer           ;namn
        use                     generic-host            ;Inherit default
values
        check_period            24x7
        check_interval          5
        retry_interval          1
        max_check_attempts      10
        check_command           check-host-alive
        notification_period     24x7
        notification_interval   30
        notification_options    d,r
        contact_groups          admins
        register                0                       ;dont register
        }

#Vir1UbuntuServer
define host{
        use                     linux-datorer
        host_name               Vir1UbuntuServer
        alias                   Ubuntu server 8.04
        address                 172.16.8.208
        }

define service{
        use                     generic-service
        host_name               Vir1UbuntuServer
        service_description     http server
        check_command           check_http
        }
define service{
        use                     generic-service
        host_name               Vir1UbuntuServer
        service_description     ftp server
        check_command           check_ftp
        }
define service{
        use                     generic-service
        host_name               Vir1UbuntuServer
        service_description     CPU Load
        check_command           check_nrpe!check_load
        }
define service{
        use                     generic-service
        host_name               Vir1UbuntuServer
        service_description     Current user
        check_command           check_nrpe!check_users
        }
define service{
        use                     generic-service
        host_name               Vir1UbuntuServer
        service_description     /dev/sda1 Free space
        check_command           check_nrpe!check_hda1
        }
define service{
        use                     generic-service
        host_name               Vir1UbuntuServer
```

```
        service_description    Total Processes
        check_command          check_nrpe!check_total_procs
        }
define service{
        use                    generic-service
        host_name              Vir1UbuntuServer
        service_description    Zombie processes
        check_command          check_nrpe!check_zombie_procs
        }
#Vir1UbuntuServer slut
```

11.5. windows.cfg

```
##############################################################################
####
# WINDOWS.CFG - SAMPLE CONFIG FILE FOR MONITORING A WINDOWS MACHINE
#
# Last Modified: 06-13-2007
#
# NOTES: This config file assumes that you are using the sample
configuration
#        files that get installed with the Nagios quickstart guide.
#
##############################################################################
####



##############################################################################
####
##############################################################################
####
#
# HOST DEFINITIONS
#
##############################################################################
####
##############################################################################
####

# Define a host for the Windows machine we'll be monitoring
# Change the host_name, alias, and address to fit your situation

#define host{
#       use             windows-server ; Inherit default values from a
template
#       host_name       winserver       ; The name we're giving to this host
#       alias           My Windows Server       ; A longer name associated
with the host
#       address         192.168.1.2     ; IP address of the host
#       }
define host{
        use             windows-server ;
        host_name       winserver1.test.log    ;
        alias           Windows Ã¶vervaknings server
        address         172.16.8.50
        }
define host{
        use             windows-server ;
        host_name       winserver2.test.log    ;
        alias           dc fÃ¶r test.log ;
        address         172.16.8.51
        }
define host{
        use             windows-server ;
        host_name       matias-server.matias.internal
        alias           Hemma Win 2008 server
        address         213.112.57.86
        }

##############################################################################
####
```

```
##############################################################################
####
#
# HOST GROUP DEFINITIONS
#
##############################################################################
####
##############################################################################
####


# Define a hostgroup for Windows machines
# All hosts that use the windows-server template will automatically be a
member of this group

define hostgroup{
        hostgroup_name  windows-servers; The name of the hostgroup
        alias           Windows Servers; Long name of the group
        }



##############################################################################
####
##############################################################################
####
#
# SERVICE DEFINITIONS
#
##############################################################################
####
##############################################################################
####


# Create a service for monitoring the version of NSCLient++ that is
installed
# Change the host_name to match the name of the host you defined above

define service{
        use                     generic-service
        host_name               winserver1.test.log
        service_description     NSClient++ Version
        check_command           check_nt!CLIENTVERSION
        }
define service{
        use                     generic-service
        host_name               winserver2.test.log
        service_description     NSClient++ Version
        check_command           check_nt!CLIENTVERSION
        }


# Create a service for monitoring the uptime of the server
# Change the host_name to match the name of the host you defined above

define service{
        use                     generic-service
        host_name               winserver1.test.log
        service_description     Uptime
```

```
        check_command           check_nt!UPTIME
        }
define service{
        use                     generic-service
        host_name               winserver2.test.log
        service_description     Uptime
        check_command           check_nt!UPTIME
        }


# Create a service for monitoring CPU load
# Change the host_name to match the name of the host you defined above

define service{
        use                     generic-service
        host_name               winserver1.test.log
        service_description     CPU Load
        check_command           check_nt!CPULOAD!-l 5,80,90
        }
define service{
        use                     generic-service
        host_name               winserver2.test.log
        service_description     CPU Load
        check_command           check_nt!CPULOAD!-l 5,80,90
        }


# Create a service for monitoring
# Change the host_name to match the name of the host you defined above

define service{
        use                     generic-service
        host_name               winserver1.test.log
        service_description     Memory Usage
        check_command           check_nt!MEMUSE!-w 80 -c 90
        }
define service{
        use                     generic-service
        host_name               winserver2.test.log
        service_description     Memory Usage
        check_command           check_nt!MEMUSE!-w 80 -c 90
        }


# Create a service for monitoring C:\ disk usage
# Change the host_name to match the name of the host you defined above

define service{
        use                     generic-service
        host_name               winserver1.test.log
        service_description     C:\ Drive Space
        check_command           check_nt!USEDDISKSPACE!-l c -w 85 -c 90
        }
define service{
        use                     generic-service
        host_name               winserver2.test.log
        service_description     C:\ Drive Space
        check_command           check_nt!USEDDISKSPACE!-l c -w 80 -c 90
        }

# Create a service for monitoring the W3SVC service
```

```
# Change the host_name to match the name of the host you defined above

define service{
        use                     generic-service
        host_name               winserver1.test.log
        service_description     W3SVC
        check_command           check_nt!SERVICESTATE!-d SHOWALL -l W3SVC
        }
define service{
        use                     generic-service
        host_name               winserver2.test.log
        service_description     W3SVC
        check_command           check_nt!SERVICESTATE!-d SHOWALL -l W3SVC
        }


# Create a service for monitoring the Explorer.exe process
# Change the host_name to match the name of the host you defined above

define service{
        use                     generic-service
        host_name               winserver1.test.log
        service_description     Explorer
        check_command           check_nt!PROCSTATE!-d SHOWALL -l Explorer.exe
        }
define service{
        use                     generic-service
        host_name               winserver2.test.log
        service_description     Explorer
        check_command           check_nt!PROCSTATE!-d SHOWALL -l Explorer.exe
        }


#ftp server
define service{
        use                     generic-service
        host_name               matias-server.matias.internal
        service_description     check_ftp
        check_command           check_ftp
        }

#http
define service{
        use                     generic-service
        host_name               winserver1.test.log
        service_description     http
        check_command           check_http
        }

#DNS
define service{
        use                     generic-service
        host_name               winserver2.test.log
        service_description     DNS
        check_command           check_dns!test.log
        }

#Mail (smtp och pop)
define service{
        use                     generic-service
        host_name               winserver2.test.log
```

```
        service_description    POP
        check_command          check_pop!test.log
        }
define service{
        use                    generic-service
        host_name              winserver2.test.log
        service_description    SMTP
        check_command          check_smtp!test.log
        }

#Windows eventLog

define service{
        use                    generic-service
        service_description    Application
        active_checks_enabled  0
        passive_checks_enabled 1
        flap_detection_enabled 0
        register               0
        is_volatile            0
        check_period           24x7
        max_check_attempts     1
        normal_check_interval  5
        retry_check_interval   1
        check_freshness        1
        freshness_threshold    1500
#       contact_groups
        notification_interval  120
        notification_period    24x7
        notification_options   w,u,c,r
        stalking_options       w,c,u
        name                   Application
        }

define service{
        use                    Application
        service_description    System EventLog
        host_name              winserver2.test.log
        check_command          check_dummy!0
        }
```

COS/CCS 2008-13

www.kth.se