Övervakning av switchar och övrig nätverksutrustning

Dynamo Net

Jimmy Björknäs

Examensarbete för ingenjör (YH)-examen

Utbildningsprogrammet för Elektroteknik

Vasa 2015

EXAMENSARBETE

Författare: Jimmy Björknäs

Utbildningsprogram och ort: Elektroteknik, Vasa

Inriktningsalternativ: Automations teknik

Handledare: Kaj Wikman

Titel: Övervakning av switchar och övrig nätverksutrustning

Datum: 16.9.2015 Sidantal: 21 Bilagor: -

Abstrakt

Mitt examensarbete har gått ut på att förena trafikgrafer och alarmering av nätverksutrustning som inte är nåbar till samma ställe, samt underlätta processen att lägga till eller ta bort en enhet från övervakningen. Tidigare har två olika program använts för uppgifterna, vilket betyder enheterna ska läggas till på två olika ställen samt att en del enheter inte har varit möjliga att övervaka där. I arbetet jämförde jag programmen Nagios, Icinga, openNMS och Observium. Vissa av dessa program var tänkta för övervakning medan andra var tänkta endast för loggning och grafer. Programmen testades i nätet och övervakade ca 20 enheter under testskedet för att se belastningen på programmen. Efter en tids testande och ett internt beslut tog vi i bruk Observium och vid ibruktagandet övervakades ca 200 enheter. Vid bytet fick Dynamo Net även Active Directory autentisering, d.v.s. alla kommer åt Observium med egna användarnamn. Då syns det vem som har lagt till enheterna eller vem som har ändrat något där och inte som tidigare när alla har använt samma användare.

Språk: Svenska Nyckelord: Nagios, Icinga, opennms, observium, nätverk, övervakning

---

BACHELOR'S THESIS

Author: Jimmy Björknäs

Degree Programme: Electrical Engineering, Vasa

Specilization: Automation

Supervisors: Kaj Wikman

Title: Monitoring of switches and other network equipment

Date: 16.9.2015 Number of pages: 21 Appendices: -

The main purpose of this Bachelor's Thesis was to link traffic graphs and alarm of network devices that are not reachable to same place and to facilitate adding or removing a device. Previously this has been done in two diffrent places which meant that some of the device had to be added twice and that some of the devices were not being monitored. In this Bachelor's Thesis I tested the management softwares Nagios, icinga, openNMS and Observium. Some of these programs were made to monitor the traffic and others to monitor the accessibility. The software were tested with 20 diffent devices in our network to see the load of them. When we started commissioning Observium there were 200 devices in the system. As a result of this change Dynamo Net was given Active Directory authentication which means all users are able login into Observium with individual usernames and also, this enables users to identify the devices added by other users.

Language: Swedish Key words: Nagios, Icinga, openNMS, Obersvium, Network management

---

OPINNÄYTETYÖ

Tekijä: Jimmy Björknäs

Koulutusohjelma ja paikkakunta: Sähkötekniikka, Vaasa

Suunatutumisvaihtoehto: Automaatio

Ohjaajat: Kaj Wikman

Nimike: Seurantaa kytkimet ja muut verkon laitteet

Päivämäärä: 16.9.2015 Sivumäärä: 21 Liitteet: -

Opinnäytetyöni tarkoitus on ollut kerätä liikennekaavioita ja hälytyksiä samaan paikkaan ja lisäksi helpottaa laitteen lisäämistä ja poistamista. Aiemmin käytettin kaksi eri sovellusta datalle eli laitteet lisättiin kahdessa eri paikassa eikä ollut mahdollista seurata eri yksiköitä.

Työssäni olen verrannut ohjelmat Nagios, Icinga, openNMS ja Observium keskenään. Osa näistä ohjelmista on tarkoitettu valvontaan kun taas toiset ovat tarkoitettuja vain lokitietoa ja graafeja varten. Ohjelmat testattiin verkossa ja valvottiin noin 20 laitetta, sekä tarkastettiin ohjelmien kuormitusta.

Testauksen jälkeen tehtiin sisäinen päätös ottaa Observium käyttöön. Käyttöönoton jälkeen seurattiin noin 200 laitetta. Vaihdon yhteydessä Dynamo Net sai Active Directory autentikoinnin, eli kaikki pääsevät omalla tunnuksella sisään. Nyt kaikki pääsevät katsomaan kuka on lisäännyt laitteita ja onko joku vaihtanut jotakin siellä, eikä tarvitse enää käyttää samaa käyttäjää.

Kieli: Ruotsi Avainsanat: Nagios, icinga, openNMS, Observium, verkon valvontaa

---

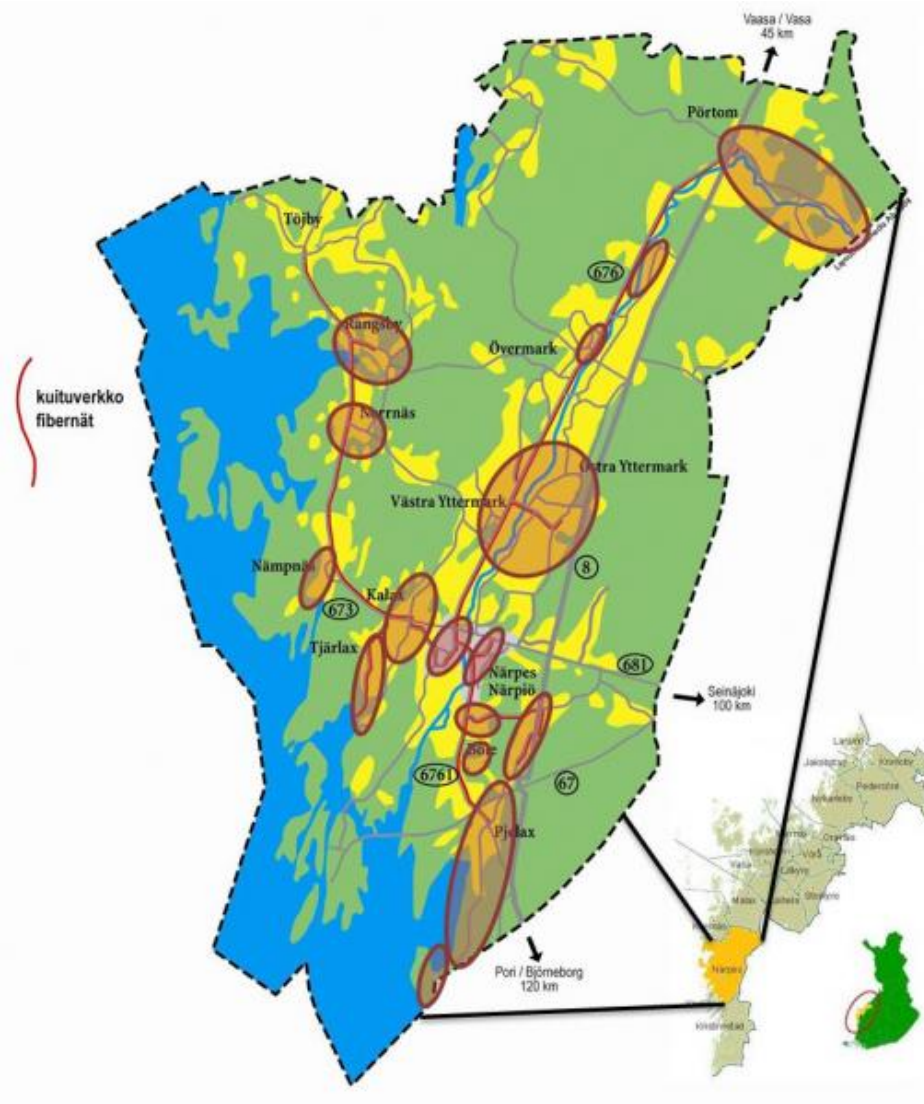
INNEHÅLLSFÖRTECKNING

1. Inledning

Det här examensbetet handlar om planering, uppställning och ibruktagande av ett övervakningssystem för Dynamo Net. Dynamo Net har sedan tidigare ett övervakningssystem uppbyggt på Nagios och ett på cacti för trafikövervakning. I mitt examensarbete kommer jag att gå igenom det befintliga system och jämföra dem för att kolla vilket som passar bäst. Det nya systemet är tänkt att bygga på Nagios, Icinga eller openNMS och ska ersätta befintliga för trafikövervakning och enhetsövervakning. Jag kommer att beskriva varför det blev det systemet som det blev och hur vi kom fram till den bästa lösningen. Eftersom det existerande systemet har byggts på i flera omgångar och blivit uppdaterat några gånger är det inte hållbart att uppdatera det längre. Det nya systemet önskas ha funktioner som det gamla inte har (t.ex. möjlighet att lägga till en enhet/service genom ett webbgränssnitt).

1.1. Dynamo Net

Dynamo Net är ett företag som ägs av Närpes stad och Företagshuset Dynamo. Företaget grundades 2002 för att driva ett regionalt datanätverk i Närpes med omnejd. Förutom detta ansvarar även företaget idag för Närpes stads IT-verksamhet, skolorna togs över 2010, staden 2012 och hvc 2014. Dynamo Net har idag fiber till de största byarna i kommunen, och finns inte fiber går det att få en trådlös anslutning dit. Företaget har ett eget stamnät av fiber och äger egen fiber ända till Vasa. Vid byggande av nya byanät har Dynamo Net samarbete med Närpes centralantenn som är det största tv-bolaget i nejden. Dynamo Net ansvarar för övervakning, drift och underhåll av nätet medan installationer köps av underleverantörer. Företaget har idag 7 anställda.



Figur 1: Dynamo Nets byanät.

1.2. Hur övervaka?

För att övervaka t.ex. att en viss port i en växel är aktiv, vilken hastighet den är ansluten med och hur mycket trafik som går igenom där kommer SNMP att användas. I nuvarande system kontrolleras endast svarstiden för en enhet för att kontrollera om den är tillgänglig eller inte samt om det tar extra länge. D.v.s. när man börjar använda flera portar mellan två växlar så märker man inte om en av portarna går sönder. Om något händer, d.v.s. en port ändrar status är det meningen att det nya programmet ska sända ut mail eller sms beroende på vad som är kopplat till porten. Mailen kommer att gå till en epost som samtliga personer har tillgång till och sms till företagets supporttelefon.

1.3. Varför övervaka?

Man övervakar sina nät för att lättare felsöka eventuella problem, ex. en växel går sönder, något i växeln går sönder eller störningar i nätet. Ett annat scenario är om något använder mycket nätverkstrafik och kapaciteten till växeln räcker inte till och då behöver man flera matnings portar till växeln.

1.4. Topologi

Innan jag började med mitt arbete ritade jag upp en topologi bild av nätet. D.v.s. vilka enheter som finns och hur allt är ihop kopplat. Det kan alltså vara till stor hjälp att ha en topologi bild av ett nät om man felsöker någonstans där man inte känner till hur allt är ihop kopplat. Detta gick ganska enkelt eftersom jag kände till alla kopplingar från tidigare och inte behövde dokumentera upp det. Topologi bilden ritade jag i programmet GNU Dia. Programmet är skapat för just dessa ända mål. Ett annat alternativ till GNU Dia hade varit Microsoft Visio som finns i Microsoft Office paketet, orsaken till att de inte blev använt var att det är licensbelagt.

2. OSI-modellen

2.1. Lager1 – Physical layer

Definierar mekaniska och elektriska komponenter. Siktet ser till att ettor och nollor går åt rätt håll. Exempel på vad som hör till Lager1: IrDA (infrarött, används vanligtvis i fjärrkontroller), Bluetooth (används t.ex. mellan telefon och handsfree) och RS-232 (används vanligtvis för att styra automationer av olika slag).

2.2. Lager2 – Data link layer

Hanterar dataöverföring och fel kontroll av en enskild länk. Det förhindrar att två meddelanden sänds samtidigt på samma kanal. Det planerar dock inte meddelandets väg i nätverket. Ex. Ethernet (det som används i datanätverk idag), token ring (det som man byggde datanät i tidigare) och FDDI (en utveckling på token ring).

2.3. Lager3 – Network layer

Hanterar uppkoppling och överföring i nätverket. Fastställer rutt. Hanterar enklare problem vid överföringen. T.ex. IP och ICMP.

ICMP (Internet Control Message Protocol). Används endast på få ställen, t.ex. ping som används för att fastställa svarstiden till en enhet och Traceroute som används för att kontrollera vilken väg datapaketet går till destinationen.

2.4. Lager4 – Transport layer

Hanterar uppkoppling, multiplexering och felkorrigering t.ex. TCP och UDP. Siktet ser alltså till att meddelandet kommer fram från sändare till mottagare utan att förstöras.

TCP (Transmission Control Protocol) används vid kommunikation på internet, d.v.s. Epost, web surfing och filöverföringar. Ett TCP packet kontrolleras alltid att det har kommit fram samt att paketet inte är korrupt. Är det något fel på paketet skickas ett nytt.

UDP (User Datagram Protocol) används vid spel eller där snabba överföringar krävs. Ett UDP packet kontrolleras inte när det kommer fram så är paketet ofullständigt eller saknas helt kommer inte ett nytt att skickas.

2.5. Lager5 – Session layer

Används för att inleda, genomföra och avsluta kommunikation mellan två noder. Hanterar också flödeskontroll som halv respektive full duplex, alltså att allt flyter på.

2.6. Lager6 – Presentation layer

Lagret ser till att information når den mänskliga mottagaren i den form som avsändaren tänkt sig. Lagret hanterar alltså kryptering av tecken och dokumentstruktur. Standardiserar datapresentation för applikationer. Exempel på System Protokoll: ASCII. SSL och MIME.

2.7. Lager7 – Application layer

Hanterar och stöder kommunikation mellan applikationer: HTTP, SNMP, SMTP, FTP, Telnet och DNS. Gör att program kan utbyta information via nätverket.

HTTP (Hypertext Transfer Protocol) används för att hämta websidor från en server. Det ursprungliga syftet var att överföra htmlsidor.

SNMP (Simple Network Management Protocol) och används främst för att läsa statistik och konfigurationer från stationer och även ändra konfigurationerna. SNMP använder oftast UDP för att skicka sitt paket men man kan också använda TCP. För en SNMP enhet finns något som heter MIB (Management Information Base), som är en databas som beskriver de parametrar som stationen kan utföra. En MIB är hierarkiskt organiserad med huvudgrupper och undergrupper. De högsta nivåerna i MIB:en är standardiserade av ISO/IEC medan de lägre nivåerna standardiseras av organisationerna för utrustningen. Det finns alltså standarder för vilka parametrar en viss typ av utrustning bör stödja förutom dessa kan tillverkaren själv lägga till parametrar som de vill ha med. De olika funktionerna som ingår i SNMP är: Get, Set, Get Next och Trap i version 2 finns även Inform och Get Bulk.

Ex. Iso.org.dod.internet.mgmt.mib-2.system.sysname eller 1.3.6.1.2.1.1.5 är en OID som ger eller ställer in namnet för enheten.

SNMP v1 som lades fram 1988 och innehåller inga säkerhetsfunktioner. Efterföljaren (v2) som lades fram 1993 (våren) och kom med säkerhetsfunktioner och en del nya kommandon. SNMP v3 lades fram 1999 men godkändes som internetstandard först i mars 2002.

P.g.a. säkerhetsfunktionerna bör man använda minst SNMP v2.

Man kan definiera vilka användare/stationer som är auktoriserade att utföra vilka funktioner. Man kan också skydda sig mot användare som med ”packet spoofing”, d.v.s. någon utger sig för att vara någon annan. Ett skydd mot icke auktoriserade användare kopierar ett meddelande och skickar dem vid ett senare tillfälle.

SMTP (Simple Mail Transfer Protocol) är det vanligaste sättet att leverera elektronisk post. Protokollet kan bara överföra 7-bitars tecken.

FTP (File Transfer Protocol) är det första filöverföringsprotokollet. Används för att överföra text och binära datafiler.

Telnet är ett nätverksprotokoll avsett för textbaserad inloggning på olika datorer men också för annan textbaserad kommunikation. Har till stor del ersatts av SSH som ger krypterad trafik.

DNS (Domain Name System). En DNS-server har till uppgift att översätta ett adressnamn till en IP-adress, ex. aftonbladet.se till 144.63.250.10. Det spelar alltså ingen roll om man skriver in aftonbladet.se eller 144.63.250.10 i webbläsaren så får man upp samma sida.

3. Enheter och beteckningar

3.1. Hubb

Består egentligen av flera bryggor som gör att man kan koppla ihop flera segment på ett nät. Förstärker inte signalen utan repeterar den. Sänder samma data till allt i samma hastighet. En hubb jobbar i OSI 1.

Figur 2: En vanlig bordsmodell av en hubb.

3.2. Växel

Kopplar ihop flera stationer på ungefär samma sätt som en hubb men ger de olika stationera full tillgång till hela bandbredden. En hubb repeterar vilket innebär att stationera delar på bandbredden. En växel jobbar i OSI 2.

Figur 3: En typisk växel.

3.3. Brygga

Används för att koppla ihop två segment av ett LAN. En brygga är kortsagt en svart låda med två kablar in, en från det ena LAN:et och en från det andra. Den brukar vidarebefordra broadcast till ”andra sidan”. En brygga jobbar i OSI 2.

Figur 4: En brygga som används för att omvandla Ethernet till FDDI.

3.4. Router

En router används för att vidarebefordra paket till andra segment. Vanligtvis används den för att koppla ihop LAN och WAN. Vidarebefordrar inte broadcast. På så sätt minskas trafiken i nätet. En router befinner sig i OSI 3.

Figur 5: En typisk router av märket TP-Link.

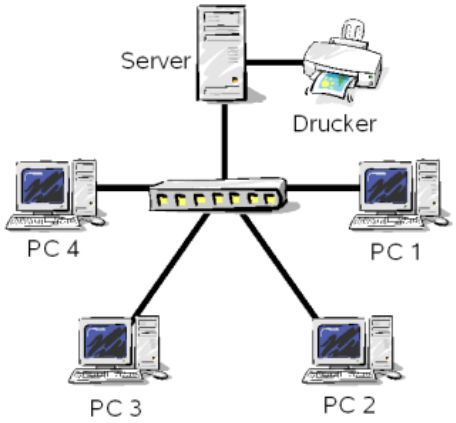
3.5. Brandvägg

Kan konfigurera vilka tjänster som ska kunna passera och därmed vilka som inte ska kunna passera. T.ex. SMTP, TELNET, FTP, NFS. Skyddar inte mot virus och brister i epost. Används alltså för att skydda det lokala nätet mot obehörig åtkomst. En brandvägg jobbar i OSI 4.

Figur 6: Ett vanligt utseende av en brandvägg.

3.6. LAN- Local Area Network

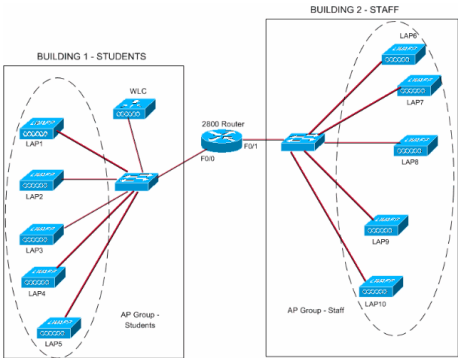
Ett lokalt nätverk. Nätverk i samma byggnad, kontor eller mindre företag. Det kan vara allt från två datorer som är ihop kopplade till flera hundra.



Figur 7: En bild på ett LAN bestående av 4 datorer och en server som har en skrivare kopplad till sig.

3.7. VLAN – Virtual Local Area Network

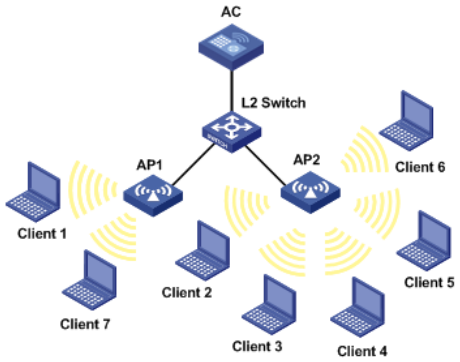
Baseras på en logisk konfiguration av ett fysiskt nät. Ett VLAN består i regel av ett stort nätverk som man delar upp i skilda VLAN (subnät).



Figur 8: Här ser vi två LAN kopplade till samma router och blir därmed olika VLAN i routern.

3.8. WLAN – Wireless Local Area Network

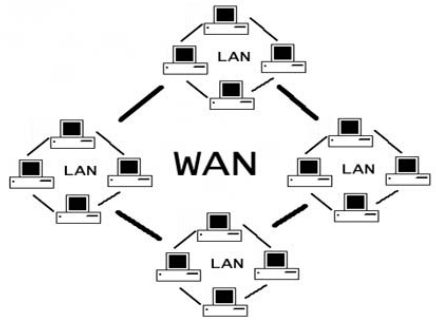
Används på 2400-2483,5MHz men finns också på frekvensbandet 5150-5300MHz. Arbetet med standard frekvenserna startade 1990 i Europa med att ERC publicerade ett förslag som bland annat angav frekvensområde för WLAN. Sänd effekt på 100mW i Europa. Räckvidden inomhus varierar mellan 20 och 50 meter.



Figur 9: Ett WLAN är alltså ett LAN trådlöst, bilden föreställer ett WLAN bestående av 7 klienter.

3.9. WAN – Wide Area Network

Sträcker sig över ett stort område. Oftast två eller flera LAN. Används bland stora företag och universitetsområden. Används vanligen för att dela olika typer av resurser eller för att byta stora mängder information mellan olika datorer. Fysisk koppling mellan LAN:en.

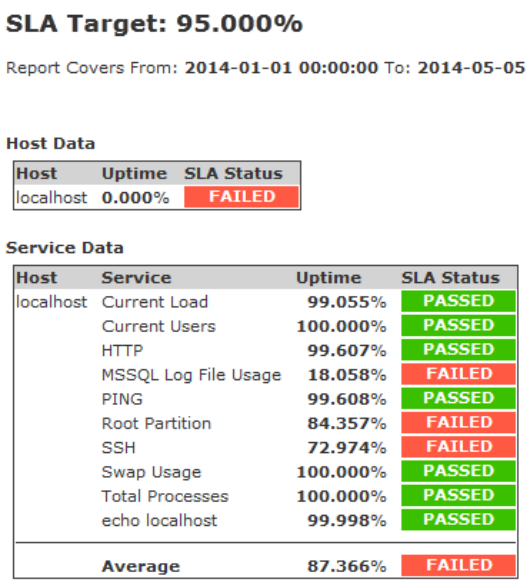


Figur 10: Ett WAN bestående av 4 olika LAN.

4. Övervakningsprogram

4.1. Nagios

Nagios är ett system som tagits fram för företags ska kunna identifiera och få en översikt över sina IT-strukturer. Det hjälper dessutom till att identifiera var problemen finns. Nagios övervakar så att tjänsterna fungerar och alarmerar ifall de inte skulle göra det. Alarmen från nagios går att konfigurera via email, sms eller något annat skript som man önskar. Ifall man underhåller något och önskar att det inte ska generera larm från nagios under tiden finns självklart också en funktion som tillåter detta. Man kan även ta ut rapporter härifrån när man använt systemet en tid för att se var man har problem eller svagaste länken i sin struktur. I nagios får man enkelt sina enheter sorterade när man lägger till dem i olika grupper, dock är problemet att varje enhet behöver en enskild konfigurationsfil för att nagios ska veta vart enheten hör och vilka tjänster som finns på den samt vem som ska få larmen det genererar. Man kan alltså ha en person som kontaktperson för en grupp medan en annan får larmen för enheter som hör till en annan grupp. Grupperna behöver inte vara delade så servrarna finns i en och övrig nätverksutrustning i en annan utan man kan fritt dela in sina enheter i grupper. Nagios används också av stora bolag så som AT & T, DHL, MTV, Telia, Ubisoft, Sony och Siemens. Den första versionen av nagios släpptes 14 mars 1999.



SLA Target: 95.000%

Report Covers From: **2014-01-01 00:00:00** To: **2014-05-05 13:35:45**

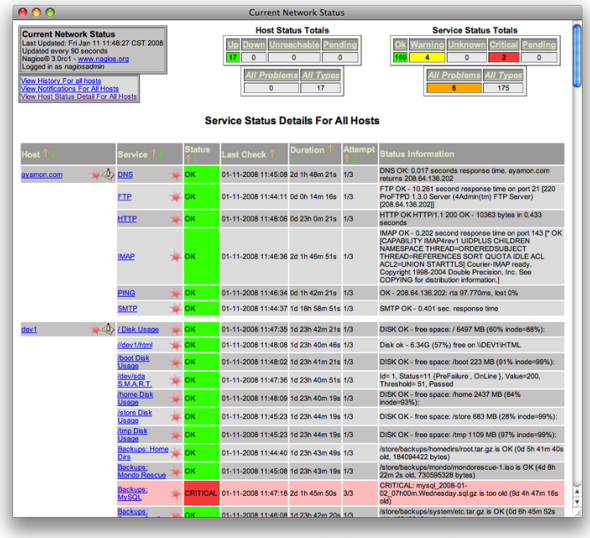
Host Data

Host	Uptime	SLA Status
localhost	0.000%	FAILED

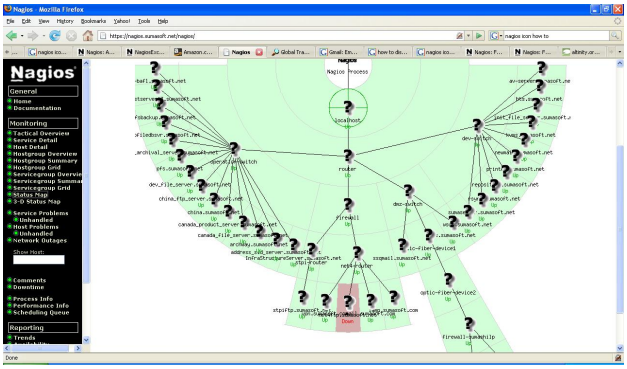
Service Data

Host	Service	Uptime	SLA Status
localhost	Current Load	99.055%	PASSED
	Current Users	100.000%	PASSED
	HTTP	99.607%	PASSED
	MSSQL Log File Usage	18.058%	FAILED
	PING	99.608%	PASSED
	Root Partition	84.357%	FAILED
	SSH	72.974%	FAILED
	Swap Usage	100.000%	PASSED
	Total Processes	100.000%	PASSED
	echo localhost	99.998%	PASSED
	Average	87.366%	FAILED

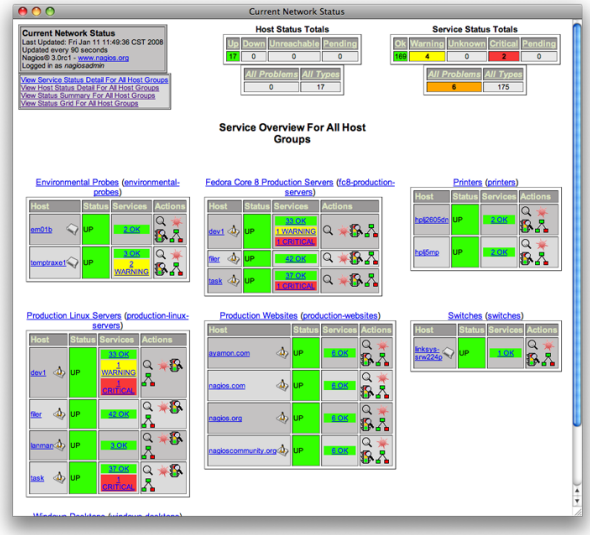
Figur 11: Här är en rapport på Nagios hur olika tjänster och enheten har klarat tillgänglighetstestet.



Figur 12: Service status översikt i Nagios. Här ser om endast något är fel eller om det är systemfel.



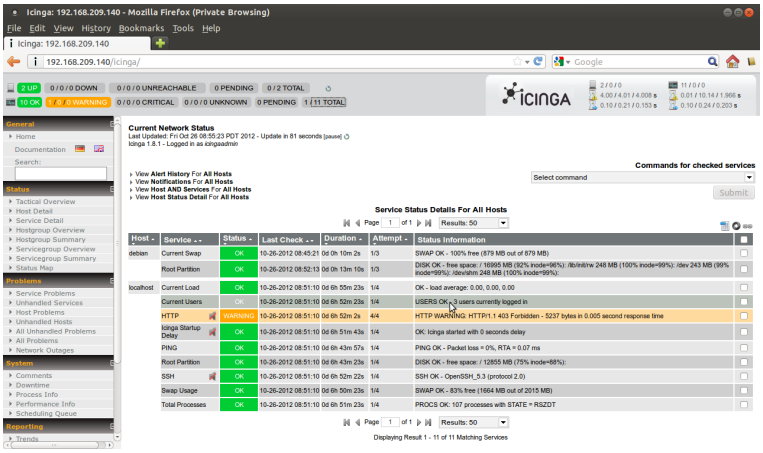
Figur 13: En topologi bild i Nagios. Här ser man alltså hur nätet är uppbyggt.



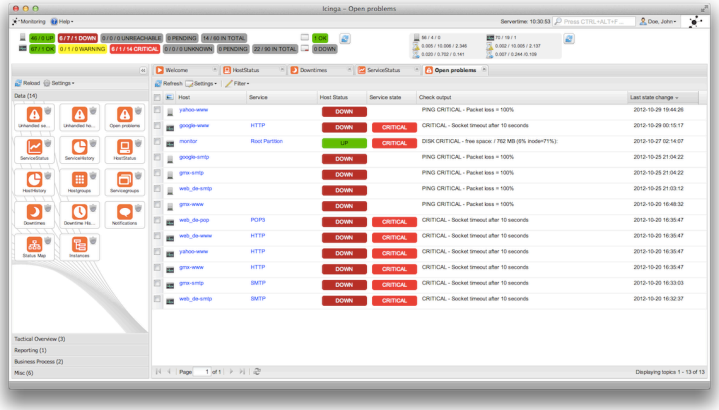
Figur 14: En grupp översikt i Nagios.

4.2. Icinga

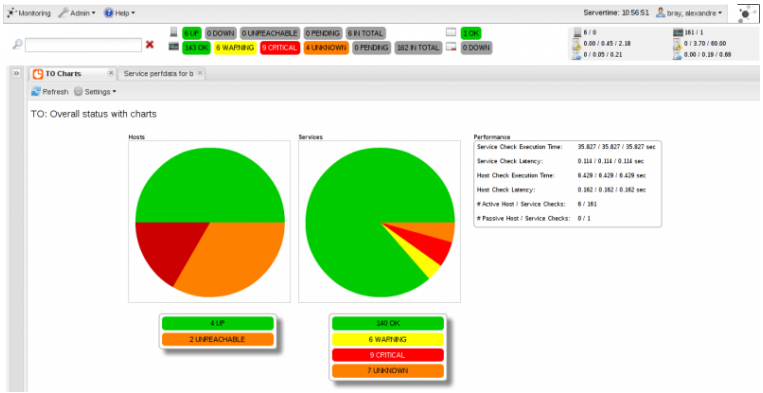
Icinga är en gratis utveckling av Nagios med fler funktioner. Icinga erbjuder två typer av webbgränssnitt. Ett som påminner väldigt mycket om Nagios samt ett som är mer avancerat och erbjuder mer funktioner. Icinga kan t.ex. övervaka följande nätverkstjänster SMTP (utgående mailservern fungerar), POP3 (inkommande mail servern fungerar), http (webb-servern fungerar), NTP (tidsserver fungerar) och PING (svarstiden inte är för lång eller för många packet faller bort på vägen). Förutom detta kan det också övervaka CPU belast-ningen, diskanvändningen, o.s.v. på servrar. Även Icinga används också av stora bolag, så som Audi, Debian och RIPE. Första versionen av Icinga släpptes 15 maj 2009.



Figur 15: En serviceöversikt i Icinga. Här ser man vilka tjänster som körs och fungerar på enheten. Här ser man även det är problem med webbservern men den är igång.



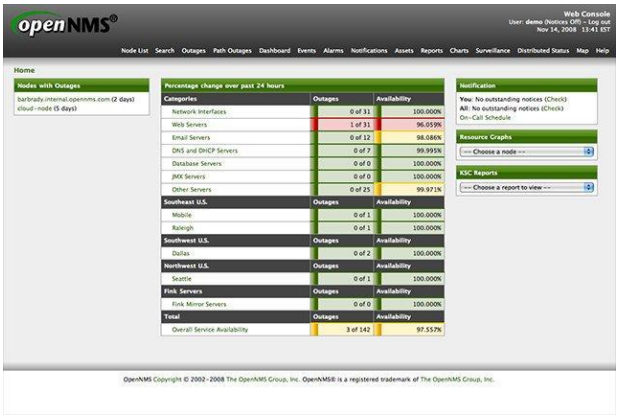
Figur 16: En servicelista i Icinga, innehåller bara tjänster eller enheter som har problem.



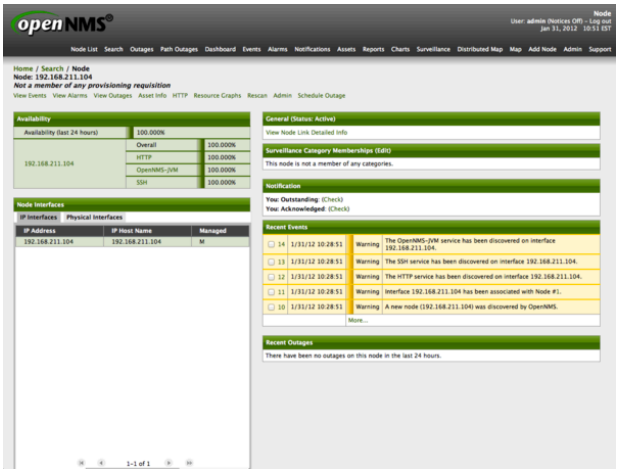
Figur 17: En rapport över enheter i Icinga. Här ser man att hälften klarade testet, en fjärde del klarade inte testet och de resterande klarande inte testet eftersom en fjärde del var ur funktion.

4.3. OpenNMS

OpenNMS står för Open Network Management System och är ett övervakningsprogram som fungerar på liknande sätt som Nagios och Icinga. Fördelen här är att man inte behöver något plugin för att få grafer utan finns färdigt i programmet. En annan fördel med OpenNMS är att man får enheterna bra grupperade och hastigt en bra överblick och bra möjligheter att konfigurera hurudana larm man vill ha. OpenNMS lägger också till webblänkar till en enhet om det t.ex. finns webbserver där eller om det finns möjlighet att fjärrstyra den. Det finns dock en nackdel med OpenNMS också, det är nämligen java baserat och därför trögt. OpenNMS har stöd för både topologi bilder samt geografiska kartor när man vill se var en enhet befinner sig. Man får också enkelt fram senaste händelserna på en enhet enkelt om man vill kontrollera om det har hänt något speciellt på senaste tiden. För att få en graf är det en del klickande men inget invecklat. Det går också att konfigurera OpenNMS så att det hittar nya enheter automatiskt om det finns inom en IP-rymd man anger.



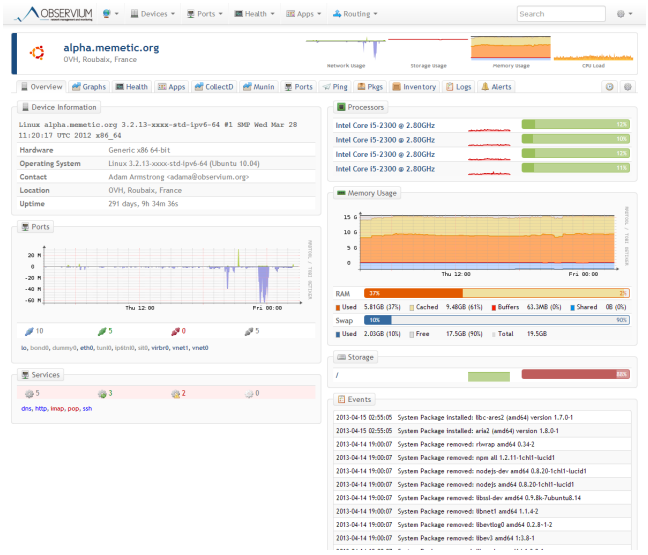
Figur 18: Överblick i OpenNMS.



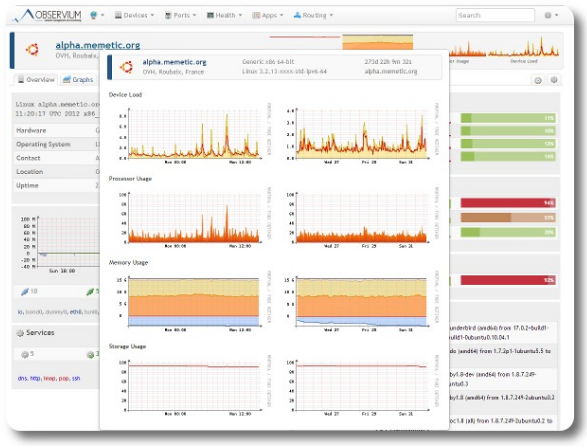
Figur 19: Enhetsöverblick i OpenNMS

4.4. Observium

Observium är ett annat övervakningsprogram som också erbjuder möjligheten att upptäcka och lägga till växlarna och brandmurar automatiskt. Ett problem med Observium är att det kräver dns lookup för att fungera. Man kan dock lägga till växlar och brandväggar manuellt men har man samma namn i dnsen och i SNMP hittar Observium enheten själv och lägger till den automatiskt om man har funktionen aktiverad. Det kräver dock man har en dns där alla enheter finns med om man inte lägger till dom manuellt på maskinen som kör Observium. Observium känner igen över 177 olika modeller av växlar och brandväggar. Det känner även ingen de kändaste Linux distributioner och Windows 2000-2012. Det ritar automatiskt grafer över minnesanvändning, processor belastning osv i enheten. Graferna i Observium är också enklare att få fram än openNMS. Under enhets-menyn får man även en snabb graf över hur mycket trafik som en växel har hanterat under senaste dygnet. Programmet stöder också realtidsövervakning. Det erbjuder även en karta (i Google maps) där man ser punkter som är gröna eller röda beroende på statusen på enheterna man har. I Observium finns även möjligheten att söka på ett portnamn i någon växel för att snabbt och smidigt få fram den information man vill ha. Observium används hos större bolag så som eBay, Paypal, Yahoo och Spotify.



Figur 20: En överblick över en enhet i Observium. Här ser man mängden trafik som gått senaste dygnet, nuvarande belastning på processorn, minnesanvändningen och hur mycket som är ledigt på hårddisken. Man får även det senaste notiserna över vad som hänt med enheten.



Figur 21: En snabb överblick av en specifik enhet i Observium. I graferna finns belastningen, minnesanvändningen och hur mycket som är ledigt på hårddisken. Graferna till vänster är senaste dygnet medan man får grafer för hela veckan på högersidan.

Figur 22: Detaljerad bild över hur många processer som körs på enheten ”localhost”.

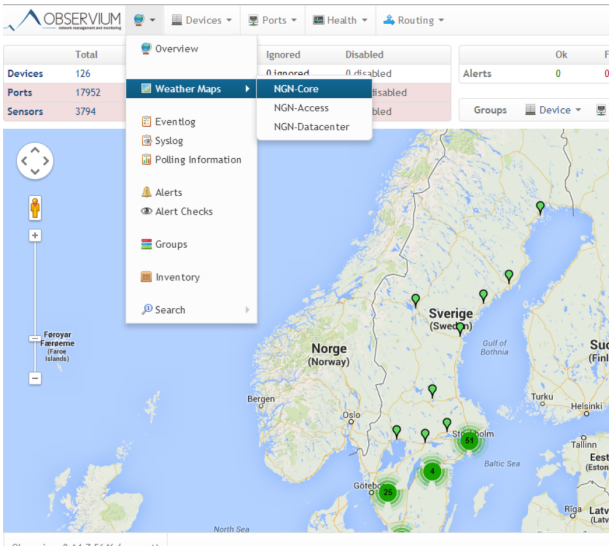


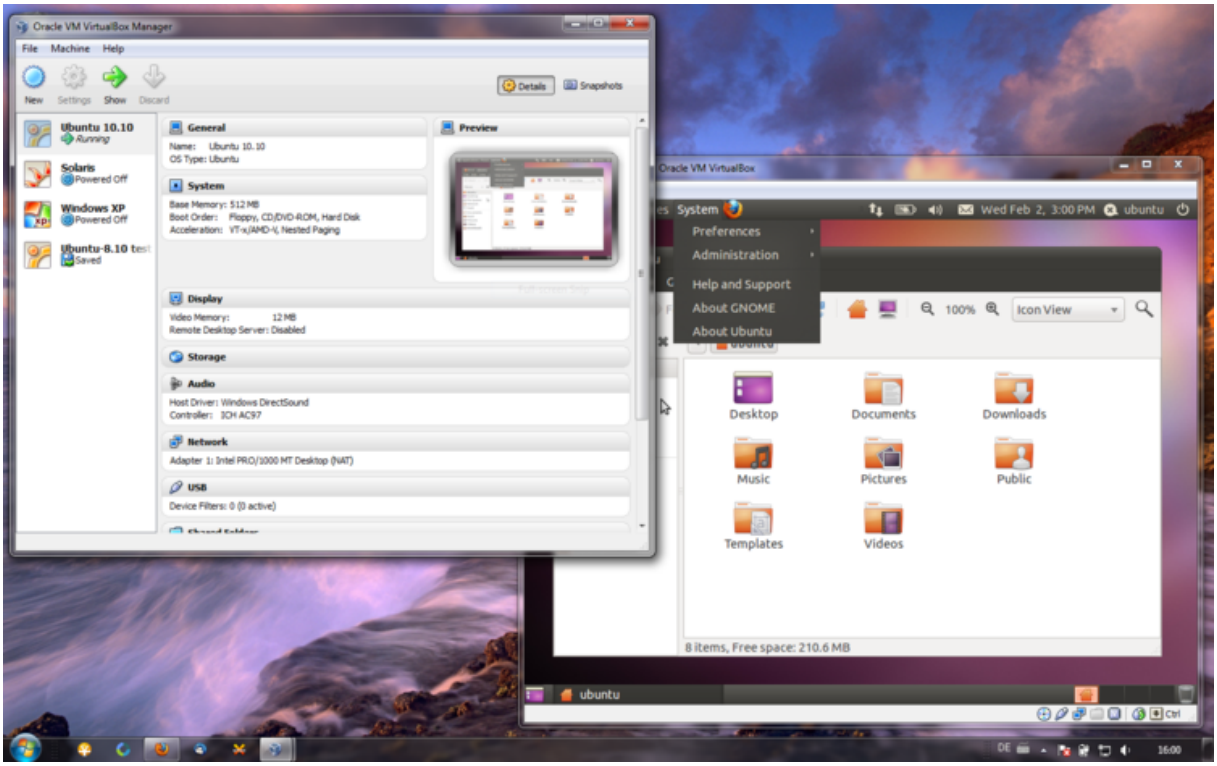
Bild 23: En karta över var enheterna finns i verkligheten i Observium.

5. Resultat och Diskussion

Det här arbetet har varit intressant och lärorikt. Jag har testat system och byggt upp konfigurationerna ensam och diskuterat och visat hur det har fungerat för kollegorna. Alla system hade sina för och nackdelar. Eftersom Dynamo Net hade två olika system från tidigare och jag hade jobbat i båda visste jag vad som önskades.

Inom Dynamo Net valde vi att använda Observium som övervakningsprogram. Orsaken till att Nagios och Icinga blev bortvalda var att vi slapp använda något plugin. OpenNMS valdes delvis bort p.g.a. java och vid test med 20 enheter gick belastning på ~ 50 % av testdatorn. I ett läge kördes Observium med ca 200 enheter med 80 % belastning på samma dator. Förutom detta kände Observium igen största delen av enheterna som vi använder, d.v.s. modellen så alla grafer över minnesanvändning och processor belastning kom med i graferna. Endast tre tillverkares enheter kändes inte igen men jag har lagt in en MIB för en grupp så endast två återstår.

Under testen valde jag att testa programmen under Debian, en gratis Linux distribution som är känd som en av de stabilaste som finns och till webbserver valdes Apache. När jag testade systemen valde jag att testa dem virtuellt, d.v.s. jag skapade en virtuell dator för varje program. Orsaken till att jag valde att testa dem virtuellt var för att jag fick köra alla parallellt med varandra utan att något påverkade något annat och det var enkelt att byta mellan olika system utan att tappa några inställningar eller behöva kopiera något. En annan orsak var också att när jag körde dem virtuellt var det enkelt att flytta hela systemet jag byggt upp bl.a. till våra servrar eftersom jag valde virtualbox som virtualiseringsprogram och våra servrar som kör vmware har möjlighet att köra en sådan här server direkt. Vanligtvis används det här programmet tvärt emot alltså när man vill köra Windows på Linux.



Figur 24: En virtuell dator med operativsystemet ubuntu körs på Windows 7 i virtualbox.

Funktion	Nagios	Icinga	OpenNMS	Observium
Autodiscover	Via plugin	Via plugin	Ja	Ja
Gränssnitt att lägga till enheter	Via plugin	Via plugin	Ja	Ja
Grafisk karta på enheterna	Via plugin	Via plugin	Ja	Ja
Realtidsövervakning	Via plugin	Via plugin	Ja	Ja
Håller ett register över enheterna	Via plugin	Via plugin	Ja	Ja
Kräver MySQL	Nej	Nej	Ja	Ja
Sökfunktion	Nej	Nej	Ja	Ja
Igen känning av enheterna	Nej	Nej	Ja	Ja
Topologi funktion	Ja	Ja	Ja	Nej
Går att övervaka utan SNMP	Ja	Ja	Ja	Nej
IPv6	Ja	Ja	Ja	Ja
Programmeringsspråk	c/php	c	Java	php

5.1. Kvar att göra

SMS-funktionen har inte ännu aktiveras och därefter kommer endast larmen via email. Förutom detta har enheterna matats in manuellt i servern för att dns lookupen ska fungera så en lösning på detta kvarstår också, ett alternativ är att också köra en liten dnsserver där Observium körs. Nackdelen är då att man måste lägga till enheten två gånger men det går dock att göra det via webbgränssnitt. Ett annat alternativ är att lägga till enherna i en dnsserver som man kan använda på arbetsstationerna också, fördelen med det är man behöver inte kolla upp en ip adress när man ska kontrollera en enhet.

6. KÄLLFÖRTECKNING

Ewert M, 2001. *Data kommunikation Nu och i Framtiden (3 Uppl.)*. Studentlitteratur.

Hedemalm G, 1999. *Nätverk och kommunikation från grunden (4 Uppl.)*. Pagina Förlags AB.

Hedemalm G, 1994. *Nätverk från grunden*. Pagina Förlags AB.

Lundström J & Lindström M, 2002-2003. *Nätguiden*. Bokförlaget Dn.

Nyhus J 2002. *Små pc-nätverk*. Pagina Förlags AB.

Mayer K, 2001. *Datakommunikation i praktiken*. Pagina Förlags AB.