Linnéuniversitetet
Institutionen för datavetenskap, fysik och matematik

Fördjupningsarbete

Nagios

The Industry Standard in IT Infrastructure Monitoring

Författare: Filip Roskvist
Handledare: Marcus Wilhelmsson
Termin: VT13
Kurskod: 1DV427

Innehåll

1 Inledning

Detta fördjupningsarbete kommer att vara en undersökning av verktyget Nagios som används för att övervaka nätverk. Fokus kommer att ligga på vad det är för något, vad det används till, vilka funktioner det har och vilka olika produkter som finns.

2 Nagios bakgrundshistoria

1999 lanserades opensource projektet Nagios för första gången under namnet NetSaint, utvecklat av Ethan Galstad från Minnesota. Idén föddes dock redan 1996 när densamme skrev en applikation till MS-DOS som använde externa tredjepartsapplikationer för att göra checkar och hämta information från Novell Netware-servrar. 1998 börjar han sedan att arbeta på en applikation till Linux som sedan lanserades som NetSaint-projektet. Namnet kom dock att ändras till Nagios år 2002 som påföljd av legala problem med namnet NetSaint. Nagios är en rekursiv akronym, och står för ”Nagios Ain’t Gonna Insist on Sainthood”, en anspelning på dess ursprungliga namn.

Över de kommande åren så vinner Nagios en mängd med utmärkelser, både communitybaserade genom röstning och från diverse IT-journalister, som bland de viktigaste, bästa och mest användningsbara säkerhetsverktygen som skapats, och blir nedladdat hundratusentals gånger. År 2009 lanseras sedan den första kommersiella produkten baserad på Nagios, och kontrakt för support börjar även erbjudas. Ethan Galstad vinner år 2011 priset för utomstående åstakommelse från organisationen SAGE, ett pris som tidigare delats ut till bland annat skaparen av Perl och utvecklingsteamet bakom Samba.

I dagsläget fortsätter Nagios att vara välanvänt av systemadministratörer, och det uppdateras fortfarande kontinuerligt (I skrivande stund kom senaste uppdateringen den 30 november 2012). Det rankas även som ett av nätverkssäkerhetscommunityts favoritverktyg på SecTools.org.[1][2][3][4]

3 Nagios Användningsområden

Nagios kan används för att monitorera hela system, vilket inkluderar serverar, hypervisors, nätverksenheter, temperaturer från mätinstrument och så vidare. På dessa enheter kan man monitorera essensiellt vad som helst som går att mäta. Olika typer av metrik i systemet, protokol, applicationer, tjänster och så vidare. Tack vare detta kan Nagios användas för att planera uppgraderingar av ett system baserat på hårdvarustatistik. Man kan sanbbt svara på problem som uppstår då man har en bra konstant överblick av hela systemet. Det är möjligt att åtgärda problem innan de blir kritiska genom att kontinuerligt hämta ut statistik från alla maskiner i systemet. Det går även att skapa Service Level Agreements (SLAs) för att skapa en baseline över vad för nivå av funktionalitet som garanteras, och visa på att denna hålls.

Tack vare en bra skalbarhet så kan Nagios användas såväl för enorma system som mindre system med endast en handfull eneter som övervakas om så önskas.[5]

Flera företag har lämnat fallstudier som beskriver hur de har använt Nagios i sina nätverk. Sunrise Community Banks behövde en lösning som var enkel att sätta upp, konfigurera och hålla uppe, och kapabel att monitorera flera platformar och enheter, och budgeteffektivt. Med hjälp av dokumenation från Nagios hemsida kunde en fungerande miljö sättas upp och modifieras för att möta Sunrises krav, vilket har ledit till att man minskat tiden på att fixa problem. Jared Bird från företaget konstaterade att man med hälp av Nagios har kunnat lösa problem innan användare och kunder ens hade märkt av något.[6]

Burlington Coat Factory var i behov av att upgradera mjukvara för att snabbare kunna identifiera trender i försäljning, snabbare kunna svara till uppkommande marknader, bättre hjälpa kunder och så vidare. Man hade tidigare hemmabjorda lösningar för att monitorera data, och bytte till Nagios för att skapa en mer fullständig och ensamstående lösning. De monitorerar över 1700 noder i dagsläget, och finner fler användningar ju mer tekniker lär sig om mjukvaran.[7]

4 Olika produkter av Nagios

Det finns flera olika produkter som är släppta i Nagios namn för olika ändamål, och med olika funktioner. Nedan går jag igenom dessa.

4.1 Nagios Core

Nagios Core är standardversionen av Nagios, och är gratis för nedladdning. Med Core kan man göra det mesta. Man kan övervaka hela nätverksmiljön, applikationer, tjänster, protokol och liknande. Man kan få notifikationer av fel genom mail eller SMS, skapa data över kapaciteten på ens infrastruktur för att kunna planera uppgraderingar och så vidare. Man kan även skapa tillgänglighetsrapporter och se till så att ens Service Level Agreement hålls, stöd för failover finns, och man kan övervaka mer än 100000 noder utan att behöva betala någon licenskostnad. Källkoden är öppen och fullt tillgänglig, och det finns en hel del community-utvecklade tillägg som man kan använda.

När det gäller support så kan man antingen hålla kontakt med communityt för Nagios geom mailinglistor, eller så kan man köpa support från Nagios själva. Detta är den enda kostnaden för Core, och ligger på 2495$ om året. Detta ger en tillgång till support genom dokumentation från nagios, supportforum och email, och gäller för Nagios Core 3.x, officiella Nagios Plugins, NRPE, NSCA och NagVis [8][9]

4.2 Nagios XI

Nagios XI är en kraftfullare version av Nagios, tänkt att användas i en enterprise-miljö. I helhet är XI tänkt att ha fler möjligheter än Core, vara mer användarvänligt och anpassningsbart.

XI har ett kraftfullare GUI som tillåter att man skräddarsyr utsendet och inställnngar efter egen preferens, vad för information man vill ska vara tillgänglig och dylikt, och separerat inställningarna mellan användare så att varje användare har sina egna inställningar. Varje enskillt användare kan även bestäma vad de vill få notifikationer om, vad för information dessa ska inehålla och hur dessa ska mottagas. Produkten har också integrerad möjlighet för att automatiskt skapa grafer vid monitorering av infrastruktur för att underlätta kapacitetsplanering.

Konfiguration har underlättats betydligt, med ett integrerat webgränssnitt för administrering av övervakningskonfiguration och systeminställningar, vilket gör det enklare att ge kontroll till andra användare att konfigurera programvaran. Administratören har också full möjlighet för att konfigurera programvaran via webinterfacet, och det finns ävern möjlighet att importera konfiguration från äldre Nagios Core-system.

Programet blir också mer tillgängligt för personer med en lägre nivå av förståelse för övervakningstekniker och mer avancerad konfiguration genom att införa konfigurationswizards som hjälper vid addering av nya enheter och tjänster som ska övervakas. Det finns även möjlighet att skapa egna wizards om man har behov för detta.

Priset på Nagios XI baseras på antalet noder som man vill övervaka, och hur många servrar man vill köra Nagios på, då varje licens endast gäller för en maskin. Programvaran är gratis att använda sålänge som man inte övervakar fler än 7 noder. För övervakning av upp till 100 hosts är priset $1995, och årlig förnyelse av kontraktet för underhåll och support kostar $1650. I detta ingår 3 supportärenden. För 100-200 hosts är priset $2995, 2000 för förnyelse av underhåll och support och 5 supportärenden ingår. För obegränsat antal hosts är priset $4995, 4000$ för förnyels och 10 supportärenden ingår. Om man köper flera licenser så minskas priset med 10% för 2-4 licenser och 20% för 5 eller fler. Värt att notera är att priset verkar ha ökat nyligen, då information from ett par år sedan säger att en obegränsad licens kostade $2495.

XI disturberas med insallation antingen via image för virtuella maskiner som kör under VMWare Player, ESX, Workstation eller vSphere, och även som installation på fysisk maskin för Redhat eller CentOS.[10][11][12]

4.3 Nagios Fusion

Nagios Fusion är en produkt som är tänkt att ge en centraliserad överblick av hela ens övervakningsinfrastruktur. Det vill säga att den ger information om status för alla hosts, tjänster och liknande som övervakas av alla sina Nagios Core och Nagios XI maskiner.

Poängen är att ge möjlighet för olika kontor att hantera separata servrar för övervakning av den hårdvara som relaterar till deras kontor, samtidigt som man kan få en komplett överblick av allt som övervakas i hela nätverket. Detta innebär även att lasten från övervakningen och grafritning balanseras mellan de olika övervakningsservrarna, medan den centrala noden inte behöver lida av prestandabrist eller kräva mer underhåll. Flera Fusion-servrar kan även användas för failover och för att skapa en total överblick av nätverket från flera olika platser. Ingen VPN krävs heller för att få fusion att fungera med alla övervakningsservrar i nätverket, utan HTTP/HTTPS räcker.

Licensen för Fusion kostar per maskin som man vill köra Fusion på, men man behöve r ingen dyrare licens för att kunna övervaka fler Nagios Core och XI maskiner, utan Fusion kan alltid övervaka hur många som helst. Priset för licensen är $995 per maskin, och detta inkluderar support för 5 ärenden.

Fusion distruberas med installation för virtuella och fysiska maskiner, med 32-bitars versioner av Red Hat eller CentOS.[13][14]

4.4 Nagios Mobile

Nagios Mobile är en applikation som installeras på ens Nagiosservrar för att tillandhålla ett webinterface för mobiltelefoner. Tanken är att man konstant ska kunna hålla sig uppdaterad på systemets status, och den fungerar både med Nagios Core och XI, och fungerar inte bara på smartphones, utan på alla telefoner med en webläsare. Produkten är tillgänligt för gratis nedladdning och har inga licenskostnader.[15]

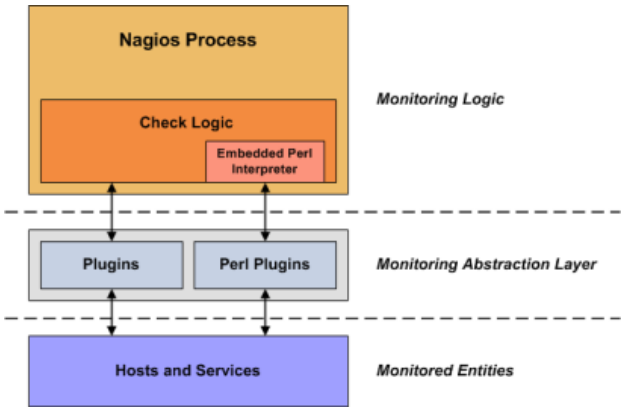
5 Plugins och addons

Mycket av funktionaliteten i Nagios beror på diverse plugins oc h addons till programet som används för olika ändamål, nedan går jag igenom några av dessa.

5.1 Plugins

Nagios har ingen egentlig intern funktionalitet för att utföra checkar mot noder i ett nätverk, utan måste förlita sig på externa program för att kunna hämta ut informationen och få den levererad till sig i ett format som den kan läsa av. Dessa program kallas för plugins.

Plugins agerar essensiellt som ett lager mellan Nagios och tjänsterna som ska övervakas. De är skript baserade på valfria skripningsspråk, som antingen exekveras lokalt eller via remote på maskinerna där checken ska utföras, och som sedan uftör sin check och skickar tillbaka datan till Nagios. Nagios i sig har därför ingen faktisk aning om vad det är som den övervakar, utan skapar endast data och notifikationer utifrån de parametrar som man har satt ut.



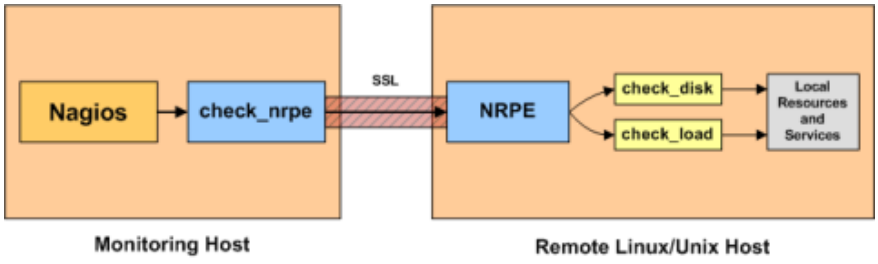
Plugins kan man skriva själv, använda sig av de runt 50 officiella plugins som nagios-teamet arbetar med eller några av tusentals plugins skapade av användarbasen. Man kan essensiellt övervaka vad som helst, den enda gränsen är vad för information man kan få från datorn man vill övervaka.[16][17]

5.2 Addons

Det finns en mängd addons till Nagios som kan utöka möjligheterna med programet. Addons kan även de skrivas själv, och det finns tusentals som är skapade av användarbasen. Addons kan anvädas för att utöka möjligheterna i notifikationer, konfigurera Nagios genom webinterfacet (även för Core), utföra checkar remote och så vidare. Nedan går jag igenom några som ofta används.

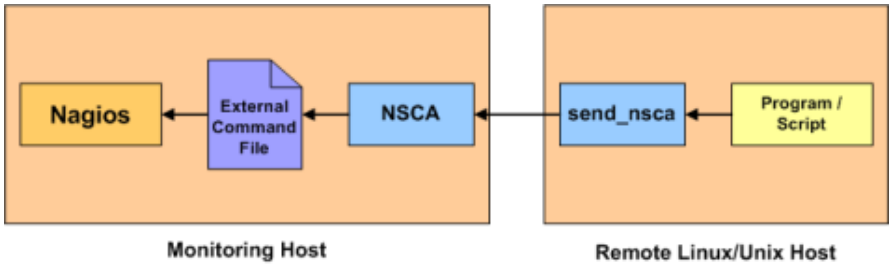
NRPE

Genom NRPE kan man exekvera skript på avlägsna hosts, vilket gör det möjligt att övervaka lokala resurser på dessa maskiner som man annars inte skulle kunna hämta data om. Detta görs genom att köra check_nrpe pluginen som körs på Nagios och via SSL går till den avlägsna hosten och exekverar skriptet som där lagras lokalt.[18]



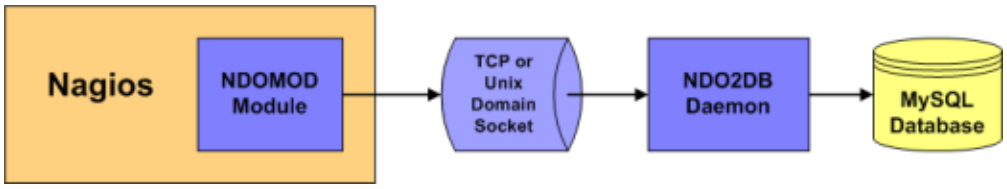
NSCA

Med NSCA kan man initiera checkar från avlägsna maskiner, som alltså skickar information till Nagios själva istället för att Nagios initierar checken själv. Detta kan till exempel vara nyttigt när det kommer till saker som det inte är effektivt att checka vid regelbundna intervaller, till exempel SNMP-traps. NSCA fungerar genom att ha en daemon igång på Nagios-maskinen, och en NSCA-klient som körs från den avlägsna maskinen, där daeomonen lyssnar efter och tolkar information som skickas från klienten.[18][19]



NDOUtils

Med NDOUtils kan man lagra all information från Nagios i en SQL-databas, och samma databas kan användas för alla Nagios-servrar man har i nätverket, vilket kan skapa en centraliserad informationsbas.[18]



6 Referenser

[1] *Nagios History*
http://www.nagios.org/about/history
[2] *Nagios Core Version Histroy*
http://www.nagios.org/projects/nagioscore/history
[3] *Traffic monitoring tools – SecTools Top Network Security Tools*
http://sectools.org/tag/traffic-monitors/
[4] *Nagios Founder Ethan Galstad Receives Outstanding Achievement Award*
http://www.prweb.com/releases/2012/1/prweb9148265.htm
[5] *Nagios Overview*
http://www.nagios.org/about/overview
[6] *Sunnrise_Community_Bank.pdf*
http://www.nagios.com/supportMedia/files/casestudies/Sunrise_Community_Bank.pdf
[7] *Burlington_Coat_Factory.pdf*
http://www.nagios.com/supportMedia/files/casestudies/Burlington_Coat_Factory.pdf
[8] *Nagios Core*
http://www.nagios.com/products/nagioscore
[9] *Nagios Core Support Plans*
http://www.nagios.com/services/support/coresupportplans
[10] *Nagios XI Features*
http://www.nagios.com/products/nagiosxi/features
[11] *Nagios XI Review (Free Nagios Core vs Nagios XI)*
http://www.thegeekstuff.com/2010/02/nagios-xi-review-free-nagios-core-vs-nagios-xi/
[12] *Nagios XI Pricing*
http://www.nagios.com/products/nagiosxi/pricing
[13] *Nagios Fusion*
http://www.nagios.com/products/nagiosfusion
[14] *Nagios Fusion Pricing*
http://www.nagios.com/products/nagiosfusion/pricing
[15] *Nagios Mobile*
http://www.nagios.com/products/nagiosmobile
[16] *Nagios Plugins*
http://nagios.sourceforge.net/docs/3_0/plugins.html
[17] *Nagios – Nagios Plugins*
http://www.nagios.org/projects/nagiosplugins
[18] *Nagios Addons*
http://nagios.sourceforge.net/docs/3_0/addons.html
[19] *Passive Checks*
http://nagios.sourceforge.net/docs/3_0/passivechecks.html