Linnéuniversitetet
Institutionen för datavetenskap, fysik och matematik

Effektiviserad drift av datorsystem

Agenter för op5

Författare: Simon Blixt
Handledare: Marcus Wilhelmsson
Termin: HT12
Kurskod: 1DV427

Innehåll

Inledning

I denna uppsats går jag igenom agenter som finns att använda när man kör op5. Agenter installeras på klienter, vilket möjliggör att man kan övervaka klienterna på ett effektivt och snabbt sätt via op5. På så vis behöver op5 enbart ta hand om att förfråga och presentera den data som agenten skickar till op5, själva exekveringen görs på klienten. Det finns en drös olika agenter för op5 som man delar in under agentbaserade övervakning samt agentlös övervakning. Jag har valt att fokusera på dessa och förklara när man bör använda de, installationsguide och kort hur de är uppbyggda.

Agentbaserad övervakning

NSClient++

NSClient++, även kallat nscp, är en kraftfull och säker övervaknings-daemon och används på enheter som kör ett Windows-operativsystem, dock ska det även fungera under vissa Linux-distrobutioner[2]. Daemonen har tre huvudfunktioner:

- Den klassika funktionen att en fjärrserver, övervakningsservern, skickar förfrågningar som ska köras på klientmaskinen, som då får ut ett värde av kommandot som kördes.
- Skickar ovanstående värde till en övervakningsserver.
- Vidta åtgärder och utföra uppgifter.

Nscp är en sammanslagning av vanliga NSClient kombinerat med att den kan exekvera scripts på den övervakade enheten i sig. Man får helt enkelt NSClient och NRPE_NT funktionalitet. Ursprungligen gjordes nscp för Nagios och Icinga, men ingenting i daemonen är just Nagios- eller Icinga-specifikt.[1][2]

Installationen av nscp är väldigt enkelt. Filen finns att ladda ner på op5's hemsida[1] .
Installera sedan filen. Det rekommenderas att man editerar filen NSC.ini i mappen där nscp installerades. Det man borde ändra är `allowed_hosts=`. Om värdet är tomt får vilken server som helst kommunicera agenten. Därav bör man skriva in IP-adressen till sin op5-server.[3]

[1] http://www.op5.com/download/OP5_NSClientpp-0.3.9.328-x64.msi

NRPE

NRPE, Nagios Remote Plugin Executor, används på Unix-enheter för att kunna exekvera plugins/få ut information på remote-enheter, och därefter skicka värdet till en övervakningsserver. Exempel på saker man kan övervaka via NRPE är CPU-lasten, minnesanvändning, diskutrymme etc. NRPE kan installeras via RPM eller via den portabla källkoden på de flesta Unixsystemen. NRPE används i kombination med ett antal lokala plugins. Övervakningsservern använder sig av kommandot check_nrpe, varpå kommunikationen görs via SSL till en klient som kör NRPE. NRPE kör kommandot som förfrågas, exempelvis check_disk, och får ut det lokala värdet som sedan returneras till övervakningsservern.[4][5]

Installationen bör göras manuellt av det allra senaste packetet för att få bästa funktionalitet. Att använda sig av exempelvis `nagios-nrpe-plugin` är inte att rekommendera då det säkerligen inte är det senaste paketet för NRPE i repository. Istället kan man ladda ner NRPE OP5's hemsida [2] och sedan kompilera själv:[15]

1. Ladda ner filen och gå till dess nedladdningsmapp
2. Installera paketet via dpkg
   a. `dpkg -i <filnamn>.deb`
3. Öppna filen nrpe.cfg och ändra allow_hosts
   a. `nano /etc/nrpe.cfg`
   b. `allowed_hosts=<IP-adress_OP5_1>,<IP-adress_OP5_2>`
4. Starta om NRPE
   a. `service nrpe restart`
5. Klart!

Windows Syslog Agent

Windws Syslog Agent, även kallat op5 SyslogAgent, kan användas på Windows 2000, Windows XP samt Windows 2003 där agenten körs som en tjänst. Agenten formaterar alla fem typer som Windows Eventlog har till syslog-format som sedan skickas till en syslog host, antingen en op5-server eller en OP5 logserver. Agenten har även stöd för att skicka logfiler i klartext.[6] op5's SyslogAgent är en ompacketerad version av Datagram SyslogAgent, som i sin tur är en version som fixat diverse buggar för Sabre Net's gamla NT_Syslog[7].

[2] http://www.op5.com/get-op5-monitor/download/

Själva installationen av op5's Syslog Agent är simpel. Ladda ner filen från op5's hemsida[3] . Installera sedan paketet och välj att konfigurera det. För att få igång de grundläggande funktionerna i SyslogAgent är det följande som gäller:

1. Tryck på "Install"-knappen för att installera SysLogAgent som en tjänst.
2. Skriv in IP-adressen till op5/log-servern i fältet för "Syslog Server.
3. Kontrollera att "Enable forwarding of event logs" är ibockat.
4. Tryck nu på "Start Service"-knappen.

SyslogAgent ska nu vara igång och skickar loggar till din op5/log-server.[7]

Nagstamon

Nagstamon är ett plugin som körs på Desktops för att få en överblick av värderna från en övervakningsserver, direkt på skrivbordet eller i systemfältet. Det som presenteras är en enkel summering av kritiska, varningar, okända, onårbara och avstängda hosts och tjänster som hämtas från övervakningsservern. Om man vill ha en detaljerad version av statusen kan man enkelt föra musen över det. Man kan även aktivera att ett ljud ska spelas vid en speciell status. [11]

För att installera Nagstamon på klienten som ska få informationen presenterad är det följande som gäller:[11]

1. Ladda ner Nagstamon för ditt operativsystem från op5's hemsida[4].
2. Packa upp och installera filen.
3. Starta programmet.
4. Högerklicka på systemfälts-ikonen och välj inställningar.
    a. Server Type: Ninja
    b. Server URL: https://<server IP>/monitor
    c. Server CGI URL: https://<server ip>/monitor.old/cgi-bin
    d. Username: <username for gui>
    e. Välj att spara lösenordet eller ej och välj även lösenord.
5. Klart!

MRTGEXT

MRTGEXT är en agent för att övervaka Novell-system. Den skapades från början som en NLM, NetWare Loadable Module, för Novell Netware för att hämta värden som används med MRTG, Multi Router Traffic grapher, men det kan även "pollas" från övervakningsservern.[12] Med MRTGEXT kan man bland annat få ut följande värden[13]:

- CPU-användningens medelvärde senaste 1, 5 och 15 minuter

[3] http://www.op5.com/download/ntsyslog.zip
[4] http://www.op5.com/get-op5-monitor/download/

- Licensieringsanslutningar samt max antal licensieringsanslutningar
- Ledigt diskutrymme samt använt diskutrymme
- Antal öppna filer
- Tidssynkroneringsstatus
- Nuvarande samt max antal processer

Installationen görs genom att kopiera filen MRTGEXT.NLM till de NetWare servrar som man vill övervaka. Filen ska kopieras till SYS:SYSTEM. Därefter ska man editera AUTOEXEC.NCF och skriva in ”LOAD MRTGEXT” så att det laddas in varje gång servern startas om. Det krävs även att man har en fungerande IP-konfigurationen på servern. MRGEXT.NLM har tre kommandoparametrar som man kan specificera efter eget behov:[13]

- -port=<port> - för att ändra vilken port som ska användas av MRTGEXT. Som standard används port 9999.
- -debug – för att få ut debug till systemskärmen.
- -mla=<license> - Används för de som har en MLA licens.

Agentlös övervakning

SNMP
SNMP, Simple Network Management Protocol, är en samling enkla operationer för att kommunicera med SNMP-enheter. SNMP ger administratörer möjligheten att ändra tillståndet på vissa SNMP-enheter, exempelvis kan man stänga av ett interface på en router eller få information om temperaturen för en switch. SNMP brukar associeras med routrar eller switchar, men SNMP fungerar oftast med all utrustning som ansluts till nätverk, exempelvis Unix, Windows, skrivare, modem, PSU m.m. Alla enheter som har någon form av mjukvara som har stöd för att ta emot SNMP information kan hanteras. Detta innefattar inte enbart fysiska enheter utan även mjukvara i form av webbservrar eller databaser.[8]

SNMP kommunicerar via UDP, vilket ger låg overhead jämfört med TCP vid stor användning. Nackdelen är att man inte får någon form av bekräftelse med UDP, exempelvis vid användning av SNMP traps. SNMP traps fungerar som så att klienten skickar information till op5-servern utan att op5-servern gjort en förfrågan, istället för att op5-servern skickar en förfrågan om information som SNMP vanligen gör. Det finns tre olika versioner av SNMP, v1, v2c samt v3. V1 är den första versionen SNMP. Säkerheten där är dock låg då den enbart är communitybaserad och data skickas utan kryptering. Det finns tre olika communitys: read-only, read-write samt traps. De fungerar så som det låter, read-only är tillåter enbart läsning, read-write tillåter läsning och skrivning medan traps enbart tillåter traps.

V2c är en sammanslagning av version v2u och v2*. Skillnaden mot v1 är förbättrad säkerhet samt bättre felhantering. Allt utom destinationen i paketet är krypterat. V3 har ännu högre säkerhet där all kommunikation är krypterat. Man har även applicerat en form av autentisering i v3 samt meddelandeintegritet.[8]

För att få ut information om SNMP på enhet kan man göra en så kallad SNMPwalk med exempelvis mjukvaran The Dude. När man har gjort en SNMPwalk får man fram mängder av OIDs, Object Identifier. Ett OID består av ett numeriskt värde som man inte förstår vad det är utan en MIB, Management Information Base, som översätter ett OID till klartext, varpå man förhoppningsvis kan förstå vad värdet innebär. Därefter kan man via op5 använda sig av check_snmp och kopiera OID:et för det värde man vill få ut, applicera rätt community-namn samt möjliga parametrar för att få ut uppgifter om servern.[8]

IPMI

IPMI, Intelligent Platform Mangement Interface, är ett öppet industristandardsinterface. Det skapades för att kunna möjliggöra hantering av serversystem över ett antal olika typer av nätverk. IPMIs funktioner är bland annat:[9]

- Systemövervakning
- Loggning av system-events
- Systemåterställning
- Utskick av varningar

Genom att integrera IPMI med OP5 kan man på så sätt få ut diverse information från systemet som kör IPMI, exempelvis temperatur, voltstyrka, fläktstatus, minne etc.

För att kunna övervaka IPMI krävs det lite konfiguration. Först och främst ska man se till att ha pluginet check_ipmi_sensor inlagt på OP5-servern. Pluginet har stöd att kontrollera IPMI sensorer lokalt eller via ”Serial over LAN”-anslutning. Därefter ska man aktivera IPMI Monitoring på den server man vill övervaka. Detta görs vid uppstart av servern och det kan skilja sig hur man kommer åt IPMI-konfigurationen. När man väl har kommit åt IPMI-konfigurationen via uppstarten ska man aktivera IPMI, sätta en statisk IP-adress och gateway samt sätta ett användarnamn och lösenord. Därefter startar man om servern. Det krävs även att man installerar op5 monitor community plugin-paketet, samt freeIPMI på op5-servern och konfigurerar den med korrekta uppgifter. Därefter ska man lägga till ett check command för den server som ska övervakas via IPMI och skriva in korrekt command line-uppgifter för att få det hela att fungera och presenteras via op5.

WMI

Genom att använda WMI, Windows Management Instrumentation, kan man utföra checkar från op5 på Windows-enheter utan att man behöver installera någon agent i Windows. WMI används i detta fall till att utföra förfrågningar på en Windows-enhet, ungefär som SNMP gör fast med mycket mer avancerade funktioner vilket ger möjlighet att övervaka betydligt mer med WMI än med SNMP på en Windows-enhet. WMI i sig består utav ett antal tillägg till Windows Driver Model som ger skapar ett gränssnitt för operativsystemet som sedan används av komponenter för information och notifikation.[16]

Installationen kräver att man har en användare på Windows-enheten som har tillåtelse att utföra WMI-förfrågningar. Sedan gäller följande[16]:

1. Uppdatera op5 med kommandot `yum upgrade` alt. `yum upgrade plugin*`.
2. Installera WMI-support på op5-servern: `yum install *wmic*`.
3. Testa så att installationen fungerade: `wmic -U DOMAIN/USER%PASSWORD //HOST "Select * from Win32_ComputerSystem"`

Det kan även vara bra att testa så att check_wmi-pluginen fungerar korrekt på op5[16]:

1. navigera till /opt/plugins/ på op5-servern.
2. Kör kommandot `./check_wmi_plus.pl -H [IP/Hostnamn] -u [användarnamn] -p [lösenord] -m checkmem -w 80 -c 90`

Man kan även konfigurera så att man inte behöver skriva in lösenordet i klartext för check_wmi-plugin, mer om detta på op5's sida för WMI[16].

Övrigt

op5 har även stöd för att presentera status på vissa externa tjänster utan att en agent en agent behövs[14]:

- FTP
- SSH
- HTTP
- DNS
- ICMP
- IMAP
- SMTP
- m.m.

Detta görs genom köra dess tjänsts check-plugin på op5-servern. Exempelvis check_http kontrollerar om adressen man anger returernar korrekt statuskod som innebär att det går bra att surfa till webbsidan.

Referenser

[1] op5 – ”NSClient++”, |Online|, available: http://www.op5.com/agents/nsclient/
[2] nsclient – ”About NSClient++”, |Online|, 2012, available: http://nsclient.org/nscp/wiki/doc/about
[3] op5 – ”User Manual NSClient++ 0.2.7.1”, |Online|, 2007, available: http://www.op5.com/manuals/extras/op5_NSClient++_0.2.7.1_manual.pdf
[4] Nagios@Sourceforge – ”Nagios Addons”, |Online|, available: http://nagios.sourceforge.net/docs/3_0/addons.html
[5] op5 – ”Nagios remote plugin executor (NRPE)”, |Online|, available: http://www.op5.com/agents/nagios-remote-plugin-executor-nrpe/
[6] op5 – ”Windows Syslog Agent”, |Online| , available: http://www.op5.com/agents/windows-syslog-agent/
[7] op5 – ”User Manual SyslogAgent v3.3.5”, |Online|, 2007, available: http://www.op5.com/manuals/extras/op5_SyslogAgent_3.3.5_manual.pdf
[8] D. Mauro and K. Schmidt, *Essential SNMP*, Sebastopol: O'Reilly & Associates, 2001, ch. 1
[9] Oracle – ”About IPM”, |Online|, 2012, available: http://docs.oracle.com/cd/E24707_01/html/E24528/z400000c1396369.html
[10] op5 – ”How-to monitor a server with enhanced IPMI sensor”, |Online|, available: http://www.op5.com/how-to/how-to-monitor-server-enhanced-ipmi-sensor/
[11] op5 – ”Nagstamon system tray status agent”, |Online|, available: http://www.op5.com/agents/nagstamon-system-tray-status-agent/
[12] op5 – ”Monitoring agent for Novell (MRTGEXT)”, |Online|, available http://www.op5.com/agents/monitoring-agent-for-novell-mrtgext/
[13] J.Drews – ”MRTG Extension Program for NetWare Server version 1.46b”, |Online|, available: http://www.op5.com/manuals/extras/mrtgext_1.46b_readme.txt
[14] op5 – ”List of plugins”, |Online|, available: http://www.op5.com/support/resources/list-of-plugins/
[15] op5 – ”User Manual op5 NRPE 2.7”, |Online|, 2006, available: http://www.op5.com/manuals/extras/op5_NRPE_2.7_manual.pdf
[16] op5 – ”Agentless monitoring of Windows using WMI”, |Online|, available: http://www.op5.com/how-to/agentless-monitoring-windows-wmi/