Tentamensfrågor

1. **Förklara vad SNMP är och när det kan komma till användning.**
   Svar: 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.
   Genom att använda SNMP via op5 kan man på så sätt få ut information om exempelvis belastningen på ett interface för en router eller temperatur för någon viss komponent i en enhet.
2. **Nämn minst tre agenter och i vilka sammanhang de används.**
   Svar:
   1. NSCLIENT++ - NSClient++, även kallat nscp, är en kraftfull och säker övervaknings-daemon och används huvudsakligen på enheter som kör ett Windows-operativsystem. nscp ser till att man kan exekvera plugins/få ut information på remote-enheter, och därefter skicka värdet till en övervakningsserver som presenterar informationen.
   2. NRPE - 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.
   3. 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.
3. **Förklara vad SLA är och vid vilka situationer en SLA kan komma till användning.**

Svar: SLA står för Service Level Agreement och är ett avtal mellan beställare och tjänstförmedlare. Det bygger ofta på ITIL(Information Technology Infrastructure Librart) när det gäller IT-sidan. Kan exemplevis innehålla:

- Service strategy
- Service design
- Service Transition
- Service Operation
- Continual Service improvement

När man genererar en SLA i op5 får man snyggt och prydligt fram statistik på drifttiden för en IT-miljö, exakta tidpunkter då något inträffat, grafer över tjänster och hosts m.m. Detta kan sedan användas för att påvisa att man exempelvis ha följt avtalet för vilken upptid som skulle tillhandahållas för en viss host eller tjänst.

4. **Förklara hur man kan övervaka en enhet med hjälp av SSH.**

Svar: Det kräver att man har konfigurerat upp nycklar korrekt så att man inte behöver logga in som vanligt med användarnamn och lösenord på enheten som ska övervakas. Därefter körs ett valt plugin som sedan skickar tillbaka värdet via SSH till op5-servern.

5. **Nämn tre konkurrenter till op5 och en kort introduktion till varje konkurrent i förhållande till op5.**
   Svar:

- **Icinga** är en open source-mjukvara som övervakar nätverk och enheter, precis som op5. Icinga skapades till en börja som en fork av Nagios år 2009. Överlag har Icinga samma som funktioner som op5, med skillnaden att op5 är betydligt snabbare med utvecklingen och presterar bättre än Icinga. Dock strävar Icinga över att i princip månadsvis skicka ut nya patcher.

- **Zabbix** är en open source mjukvara som övervakar nätverk och enheter. Zabbix har en kommersiell support i form av företaget Zabbix SIA. Zabbix använder sig utav triggers medan man i op5 har plugins. op5 väger även här över med bättre funktioner och prestanda. Zabbix är inte baserat på något utan skrivet av Alexei Vladishev.

- **opsview** har tagit del av följande open source lösningar: Nagvis, Net-SNMP, RRDTool samt kärnan av Nagios och kört ihop detta till opsview. Mjukvaran körs i linux eller solaris. Opsview klarar av att övervaka de vanligaste operativsystemen, applikationer och andra typer av enheter. Kan rapportera fel via sms, e-post eller en atom-tråd.

6. **Förklara två skillnader mellan varje version av SNMP.**
   Svar:
   - SNMP v1->v2c – Om en förfrågan skickas men förfrågan innehåller fel så behandlas detta korrekt. Innehåller även förbättrad säkerhet då man exempelvis krypterar viss data.
   - SNMP v2c->v3 – Framförallt förbättrad säkerhet. Funktioner så som meddelandeintegritet, autentisering och full kryptering.
7. **Förklara vad MIB och OID är inom SNMP.**
   Svar: OID, Object IDentifier, är en siffersträng som för blotta ögat inte säger någonting alls. För att kunna läsa av ett OID krävs det att man finner enhetens MIB, Management Information Base. En MIB innehåller en mappning mellan OIDs med vad de betyder. Betydelsen av ett OID kan vara allt från fläkthastighet till antal inloggade användare på enheten. För att få reda på betydelsen läser man in MIB:en som används för enheten, varpå man kan förstå vad OID:et innebär. En MIB innehåller den hierarkiska strukturen av alla OIDs för ett fabrikat/enhet(?).
8. **Förklara hur man går tillväga för att skriva ett eget script till op5 för en linux-enhet som ska fungera via NRPE.**
   Svar: Först och främst ska man installera NRPE på klienten. Därefter ska man bestämma vilket språk man vill skriva scriptet i. Nästa steg är att få ut värdet/informationen som man vill ska presenteras via op5 genom sitt script. Den viktigaste delen är att få med exit-värderna som op5 förväntar sig att få beroende på vad som inträffar av scriptet:

- värde 3 – Okänt fel som inträffat.
- Värde 2 – Kritiskt värde.
- Värde 1 – Varningsvärde.
- Värde 0 – Allt är okej.

Dessa fyra värden ska returneras av scriptet till op5 beroende på vad som inträffar. Sist men inte minst gäller det även att skicka med grafvärden om man vill få en graf presenterad via op5. Texten som ska skrivas ut är "<rubrik> = värdets_parameter | <info_text>=$värdets_parameter;$varnings_värde;$kritiskt_värde;lägsta_siffra_för_grafstorleken;högsta_siffra_för_grafstorleken ". När scriptet är klart ska detta läggas i /opt/plugins/ på klienten. Man ska även editera filen /etc/nrpe.d/op5_commands.cfg och skriva in korrekt syntax med parametrar för sitt skapade plugin. Därefter kör man check_nrpe som check_command i op5 samt det namn på scriptet som valde i filen op5_commands.cfg som värde för check_command_args.

9. **Hur bör man göra om man har tänkt genomföra något som kan medföra att en tjänst presenteras som kritisk/nere i op5?**
   Svar: Man bör använda sig utav funktionen ”Schedule downtime” i op5. Om en host eller tjänst är schemalagd för nertid förhindrar op5 att checkar görs mot hosten eller tjänsten.
10. **Förklara de olika communities som finns i SNMP.**
    Svar: Med hjälp av SNMP communities sätter man upp relationer mellan managers och agenter. Det finns tre communities som tar hand om olika aktivititer:

    - Read-only – bara för att läsa värden
    - Read-write – läsa och modifiera värden
    - Trap – ta emot traps från agenter

    Det man ska tänka på är att döpa communityt till något ”säkert” då detta fungerar som lösenord. I SNMP v3 finns dock stöd för annan autentisering.