

# Nät- och Systemövervakning

Underleverantör: IP-Solutions

## Datum

- 23-25 May, 2011  
Stockholm

Det här är en kurs med många praktiska övningar där eleverna lär sig införa eller förbättra övervakning av sina nät och system. Syftet med kursen är att man direkt efter avslutad kurs ska kunna införa ett övervakningssystem på företaget och själv kunna analysera de egna behoven av övervakning samt veta vad man tjänar på att använda det. Vi lär också ut vilken typ av övervakningsverktyg som finns att tillgå på marknaden, både kommersiella verktyg och open source-verktyg. Det är även en ögonöppnare för den som inte har tidigare erfarenhet av övervakning, där man lär sig om olika möjligheter och alternativ som finns.

## Målgrupp

Kursen riktar sig till alla som arbetar med system- och nätverksdrift.

## Förkunskaper

Grundläggande kunskaper om IP och nätverk motsvarande vår [TCP/IP in practice](#) samt praktisk erfarenhet av nätverksdrift.

## Övrigt

Denna kurs finns som schemalagd utbildning och presentationen ges på svenska. Under kursen blandas teoretiska presentationer med praktiska övningar. Vi kan även hålla denna kurs företagsinternt. Kontakta oss för att få reda på hur vi kan hjälpa er med anpassade kurser.

## Längd

3 dagar

## Svårighetsgrad



## Agenda

### Introduktion

- Möjligheter med övervakning
- Varför är övervakning viktigt?

### Terminologi

- Vad ska övervakas?
  - Identifiering av kritiska komponenter
- Hur ska det övervakas?
  - aktiv/passiv övervakning
  - binär/analog övervakning

- relationsmonitorering
- Implementation
- Intrångssäkerhet
- Test / mätning

## Jämförelse av olika övervakningssystem

### Genomgång av övervakningsprogram

- Nagios
  - Arkitektur
  - Lokala monitorer
  - Fjärrmonitorer
  - Plugins
  - Konfiguration
  - Accessnivåer
- Larmhantering
  - larmkanaler
  - filtrering
  - grupper
  - rutiner & jour
  - larmprocesser & ansvar
- Laboration Nagios
  - övervaka en webserver
  - övervaka en router
  - övervaka en switch
  - övervaka en filserver
  - övervaka en mailserver
- Uppsättning av olika metoder för larmgivning
  - mail
  - SMS

### SNMP

- vad är SNMP?
- hur fungerar SNMP?
- vad kan man göra med SNMP?
- Säkerhet/sekretess i SNMP
- Managers
- Agenter
- MIB
- Traps
- Net-SNMP
- GetIF SNMP Utility
- Laboration SNMP

### Statistikinsamling Cacti

- Vad är Cacti?
- Vad kan Cacti övervaka?
- Medföljande templates
- genomgång och konfigurationsexempel
- devices
- graphs
- användarhantering

- konfigurationsexempel

### Laboration Cacti

- övervakning av CPU-last på server
- övervakning av nättrafik hos router
- övervakning av diskutnyttjande på server
- skapa devices
- skapa graphs
- konfigurera presentation (graph trees)

### Övervaknings/analysverktyg

- Ping
  - svarstider – är det fördröjningar i nätet?
  - konnektivitet – kan jag nå mina destinationer?
- Telnet
  - servertest – svarar servern?
  - svarar den rätt?
- Traceroute
  - routinganalys – vilken väg går datapaketen?
- Dig/nslookup
  - Hur ser min namnuppslagings-information ut?
- Nmap
  - Vilka portar finns öppna på min server/i hela mitt nät?
- tcpdump & Wireshark/Ethereal
  - trafikanalys – vad går över det lokala nätet?
  - protokollanalys – vad säger servern till klienterna? NetSensory
  - passiv övervakning

### Laboration – Övervaknings/analysverktyg

### Summering