Manuellt eller automatik
“Due care” ITSäkerhet

Jan Säll – Irial Ltd, YASK Systemkonsult AB, SNUS

Version: 1.0
Författare: Jan Säll

Jan Säll - Irial

- VD för irial
- Arbetat med Unix/Linux sedan 1983
- Unix/Linux konsult
  - Konstruktion av nätverk (LAN & WAN) - Säkerhet
  - Arkitektur av stora interaktiva Web applikationer
  - VOIP Arkitektur
- Internationell författare
- Internationell lärare i:
  - olika Unix-dialekter, olika programmeringsspråk (Java, C, Motif m.m.)
  - Avancerad. WEB design (Interaktiva Web sidor, Apache 2)
  - Internet Säkerhet, Brandväggar, Säkerhetsutvärderingar
- Ordförande för Svenska Unix föreningen - EurOpen.SE
- Email: jan@irial.com http://jan.saell.org/

Irial - Historia

- Skapades 1998 genom sammanslagning av resurserna i:
  - Yask Systemkonsult AB
  - Koala Systems
- Grundare
  - Jan Säll
  - Simon Kenyon
  - Andrew Macpherson
- Kontor i
  - Sweden (Stockholm, Kumla)
  - London, UK
  - Seattle, USA

- Projekt – då och nu:
  - Bokförningsprogram
    - Installerat i mer än 800 företag
    - Körde mer än 30,000 företag
  - conference management system
    - För hantering av konferenser upp till 25,000 delegater
  - Inköpssystem för Shell Oil
  - Reseräkningssystem for en organisation med mer än 15,000 anställda
  - web baserat membership directory för en stor europeisk medisinsk förening
  - Hotellbokningssystem för world athletics championship
  - Flerspråkigt diskussionsforum för EU Kommissionen
  - Aktiehandelssystem för Teletrade
  - Internet bank för en stro brittish bank
  - British Yellow Pages
  - Global VOIP Platform
    - För Flint Telecom

Irial – Erfarenhet/Kunskap

- internet/intranet/extranet
  - Design / utveckling / installation och driftstagning
  - nätverkssäkerhet / brandväggar / kryptering / utvärderingar
  - Voip Lösningar
- web programmering
  - HTML, CGI, javascript, Java
  - Web / databas integrering
- applikationsdesign / utveckling i:
  - Asm, C/C++, Java, Cobol, Perl, VB, Delphi, PHP, tcl, ASP, PL/1, Modula 2
- Databas design
- Reuters Utvecklare
- dCAP – Digium Certifed Asterisk Professional

- UNIX systemadministration
- Omfattande kursutbud
- OS erfarenhet:
  - Digital UNIX
  - HP/UX
  - Linux
  - FreeBSD, OpenBSD, NetBSD
  - BSD
  - Microsoft Windows
  - Solaris
  - SunOS
  - SCO, UnixWare

Irial – Kunder nu och då

- AOL Time Warner
- BP
- British Gas
- British Telecom
- BSDi
- Carlsberg
- Cellnet
- Chevron
- Citibank
- COI Communications
- Congrex
- DGXIII
- Digital
- Directline Insurance
- Energis
- Ericsson
- Flint Telecom
- HM Customs & Excise
- HP
- UKUUG
- IBM
- ICL
- Indy 500
- IPC Magazines
- Landis ICT Group
- LO
- Lucent
- Merrel Lynch
- Microsoft
- Nomura
- Nortel
- OCC
- Omicron
- PCG
- Price Waterhouse Coopers
- Saltmine
- Schlumberger
- SCO
- Scotland Yard
- Sequent
- Shell
- SITA
- Skanska
- Sony
- Swedish Police
- Teletrade
- Telia
- Total
- UBS
- UKUUG
- Unifocus
- Unisys
- USENIX
- Webtastic
- yell.com

Inledning

- Problemet
  - Hur validerar man de ”Svarta Lådorna i nätverket”
  - The Sarbone Oaxley act (section 404) – USA och
  - EU equivalent Basel II
    - Kräver insamling
    - Lagring
    - Analysering av data

Vårt Uppdrag

- Säkerställa data för Internal Audit
- Göra säkerhetsutvärderingen
- Köra på kundernas nätverk

- Inte ta fram verktyg

Initiala verktyg

- Gjordes av andra systerbolag
- Manuell hantering
- Ca 1-4 utrustningar i timmen
- Template dokuments fylldes i
- Dessa verifierades sedan

Processkrav

- Specificerad Customer Security Policy
  - Del av customer contract
- Varje kunds Security Policy är unik
  - Vad och hur saker ska kontrolleras skiljer mellan olika kunder
- Evidence måste samlas in
  - För audit processen

Nätverksutrustning

- Olika typer av network devices
  - Hubar, switchar, routers, concentratorer, content switches, firewalls, etc…
- Olika användarinterface
  - Kommandorad, VT100 menyer, web, diverse låsta konfigureringsprogramvaror
- Olika accessmetoder
  - Telnet, SSH, SNMP, HTTP, console port

Ett säkerhetsverktyg måste …

- Integreras smidigt I kundens nuvarande arbetsflöde
- Uppfylla kraven från corporate audit process
- Kunna hantera olika typer av Security policies
- Hantera alla typer av nätverksenheter
- Hantera all typ av access till nätverketenheterna
- Vara fristående och inte behöva ytterligare verktyg
- Skapa användbara “repair actions” för driftspersonalen
- Rapportera data för inmatning till andra system

Processen

- Hur gjorde vi

Krav

- 5 Huvudkunder
- Mellan 700 till 4000 enheter per kund
- 5 mans bemanning
- Körning var 3:e månad

- = Ca 10000 enheter var tredje månad
- = Manuellt ca 2500 mantimmar
- = 3.3 månader / man

Health check processen

- Inventory laddas in i verktyget
- Authentication data konfigureras
  - Usernames, passwords, proxy ids etc.
- Connectivity test utförs
  - Verifierar authentication data
  - Samlar in enhets information för valideringen av Inventory
- Enheternas konfigureringar samlas in
- Validerings parametrar sätts upp i verktyget
- Enheternas insamlade konfigureringar analyseras med de olika testar man satt upp
- Rapporter produceras
- Test och valideringsparametrarna kan ändras utan att man kör om insamlingen.
  - Mycket användbart vid startup av processen

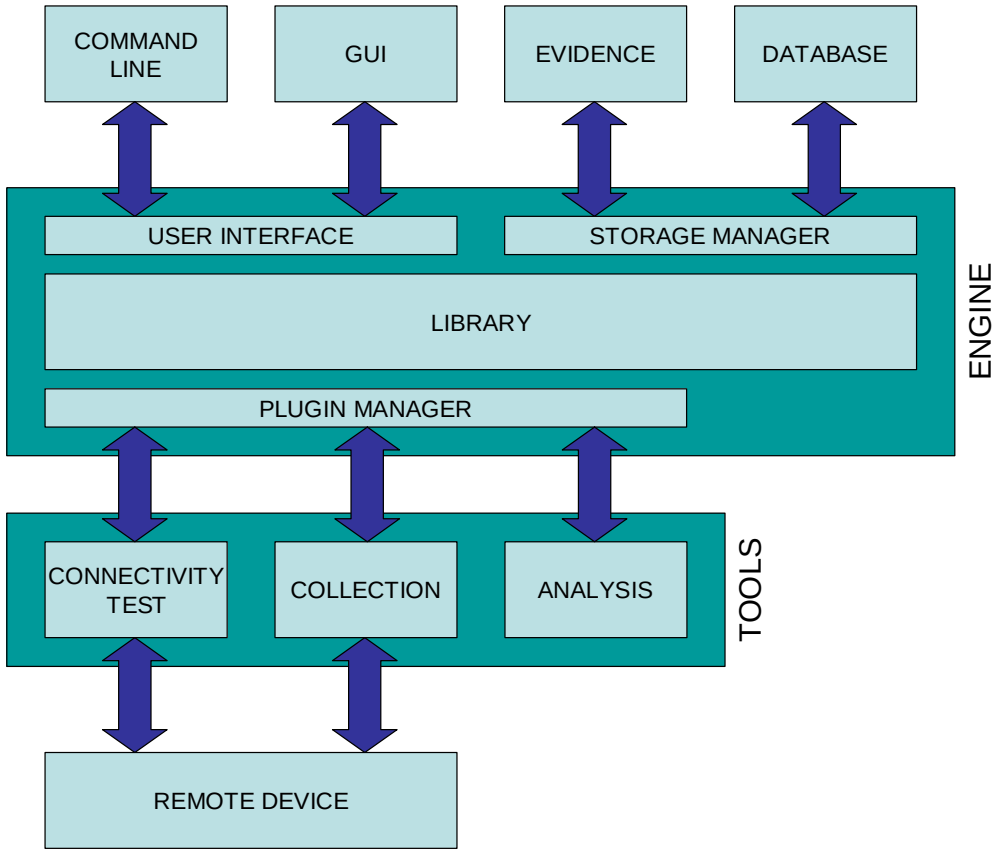
Verktyg

- Linuxbaserat
- OpenSource baserat

Health check verktyget

- Baserat på en vanlig laptop
  - Måste vara mobil för local LAN Access och console access
- Baserad på Linux
  - Fria programvaror = låg kostnad för deployment etc.
- Support för alla access methods som har krävts
  - Telnet, SSH, SNMP, HTTP, serial console och XML import
- Hantering av ett stort antal olika network device typer
  - Plug-in architecktur gör den enkel att utöka
- Skapar evidence filer för audit
  - Tidsstämplade

Block diagram



Rapporter

- Deviation matrices för Excel
- Deviation statistics
- Repair action rapporter
- Exportfiler i standardformat för vidare behandling
- Inventory deviation data
  - Användbar för att korrigera fel
- Specialanpassade rapporter for kunders egna verktyg och databaser
  - Många har egna RA systems

Supported network device types

- 3Com Superstack
- 3Com Linkbuilder
- 3Com Linkswitch
- Checkpoint Firewall-1
- Checkpoint secure platform Linux
- Cisco Aironet
- Cisco CatOS
- Cisco IOS
- Cisco IOS/700
- Cisco Kalpana
- Cisco PIX
- Cisco Vxworks
- Cisco WebNS
- IBM AIX
- IBM MRS
- Linux RedHat/Fedora
- Network Systems CDA
- Nokia AlchemyOS
- Nokia AP
- Nokia IPSO
- Nortel Baystack
- Nortel BCC
- Nortel Centillion
- Nortel MCP
- Nortel Passport
- Olicom
- Sun Solaris
- Symantec Enterprise Firewall
- Symbol AP
- … more are being added as needed

Performance

- Testat med en enstaka dator
  - IBM ThinkPad T23, 1.2 GHz Pentium, 512 MB
- Insamling / Collecting device configurations
  - 300 – 7,000 enheter per timme
- Analysering av konfigurationerna
  - 2,000 – 6,000 enheter per timme
- Mer datorer kan köras i paralell för mera prestanda
- Huvuddelen av tiden tas dock up I hantering av security policy och inventory och kvaliten på dessa

Tools and computers can be clustered

- Unlimited number of nodes in cluster
  - All nodes need TCP access to the master node
- Improves performance
- Nodes can perform different parts of the health check process
  - E.g. two nodes can collect data while a third is analyzing data
- Nodes can be permanently installed behind firewalls
- Data collecting nodes can be installed in customer networks
  - Operation performs collection while network team performs analysis
  - Efficient and still compliant with audit requirements

Avslut

- Tackar
- Frågor