

Storitve nadzora in upravljanja informacijske infrastrukture

Boštjan Lavuger
COMTRON d.o.o.

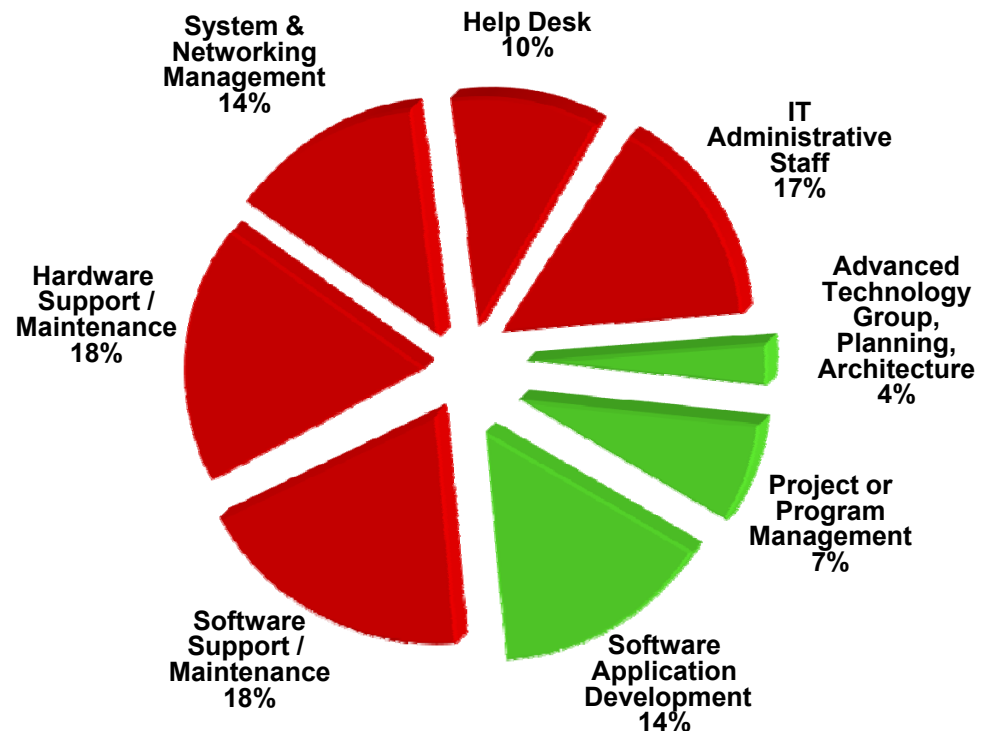
Vsebina

- OSI model nadzora in upravljanja virov IT
- Upravljanje storitev (service management)
- Upravljanje z dogodki
- Orodja za nadzor in upravljanje omrežij
- NET Inspector in Performance monitoring
- Storitve nadzora in upravljanja omrežij ter sistemskih virov

Fokus na izboljšanju učinkovitosti IT je ključ do obvladovanja stroškov. In kje smo?

Za 77% podjetij je izboljšanje učinkovitosti IT najvišja prioriteta v 2007

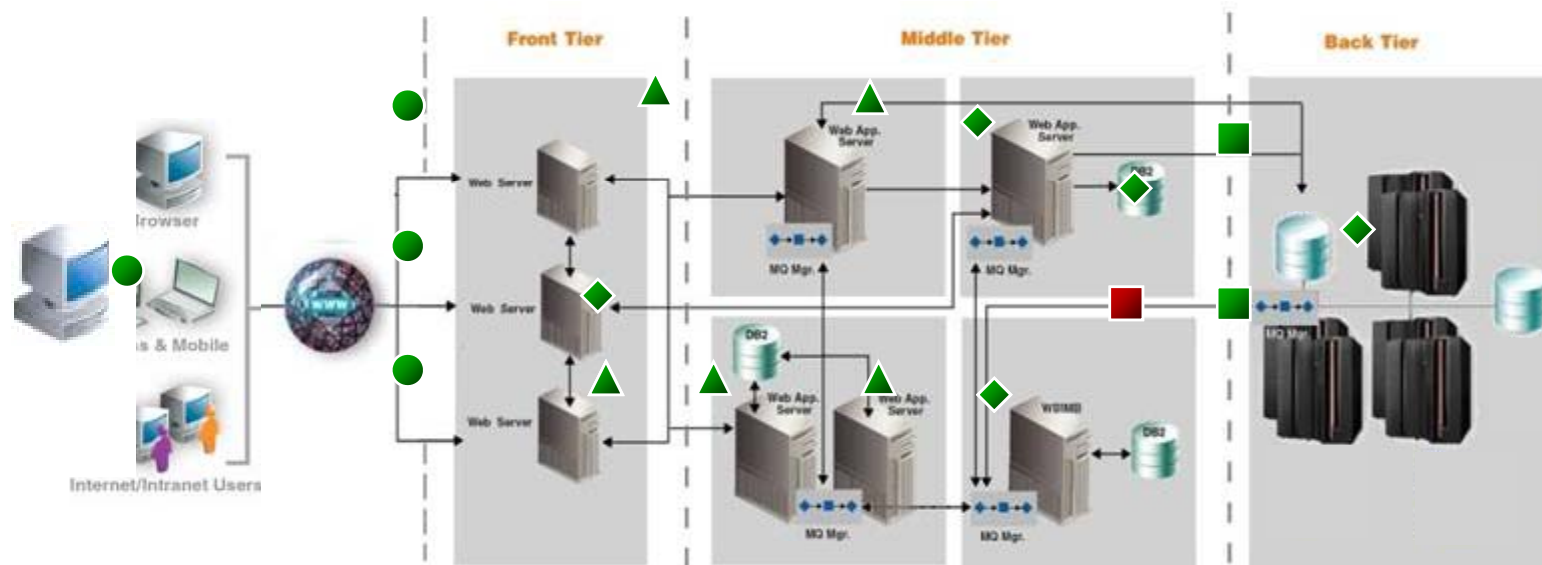
Kljub fokusu na učinkovitosti IT se v realnosti ni veliko spremenilo. Struktura sredstev za IT je zadnjih 5 let ostala enaka.



Skupna poraba na IT osebju v letu 2006

Teško vprašanje

Ko se uporabniki pritožujejo nad slabo odzivnostjo oz "počasno" aplikacijo, se v IT postavljajo tri osnovna vprašanja:



1. "Vsi sistemi so zeleni, kljub temu pa je nekje težava?"
2. "Kateri dogodki kažejo na izvor težav?"
3. "Zakaj ne moremo identificirati potencialnih težav, preden do njih pride?"

Vloga celovitega nadzora v IT

- Upad težav, ki izvirajo iz IT (iz 59% na 37%)
 - Programska oprema iz 4% na 19%
 - Strojna oprema iz 55% na 18%
- Porast težav, ki izvirajo iz stavbne infrastrukture – (iz 35% na 63%)
 - Okolje – sistemska infrastruktura iz 4% na 18%
 - Telekomunikacije iz 37% na 44%

OSI model nadzora in upravljana virov

- Upravljanje zmogljivosti (Performance management)
- Upravljanje konfiguracij (Configuration management)
- Upravljanje pravic (Accounting management)
- Upravljanje napak in izpadov (Fault management)
- Upravljanje varnosti (Security management)

Performance management

- Osnovni namen je merjenje in predstavitev različnih zmogljivostnih kazalnikov
 - Procesorska obremenitev, obremenitev pomnilnika, utilizacija vmesnikov, jitter, zakasnitve, ...
- Zajema tri osnovne korake:
 - Zajem podatkov iz različnih virov
 - Analiza podatkov za določitev sprejemljivih meja
 - Primerjava trenutnih podatkov s določenimi normalnimi vrednostmi
- Zmogljivosti moramo spremljati tudi med napravami

Configuration management

- Cilj je spremljanje trenutnih nastavitev z namenom obvladovanja vseh sprememb na napravah
- Vsaka naprava ima različne verzije informacij, ki se spremljajo
 - OS, verzije mikrokode, verzije konfiguracij,...
- Configuration management hrani vse informacije o vseh, za delovanje naprave bistvenih nastavitvah, na centralnem mestu

Account management

- Cilj upravljanje je nadzorovati dostop in potrebe po omrežnih virih in s tem omogočati njihovo pravočasno zagotavljanje
- Izvajamo s pomočjo spremljanja porabe omrežnih virov in določitev potrebnih virov za posameznika ali delovno skupino
- Upravljanje je zelo sorodno z performance managementom, le da so vpleteni viri glede na posameznika

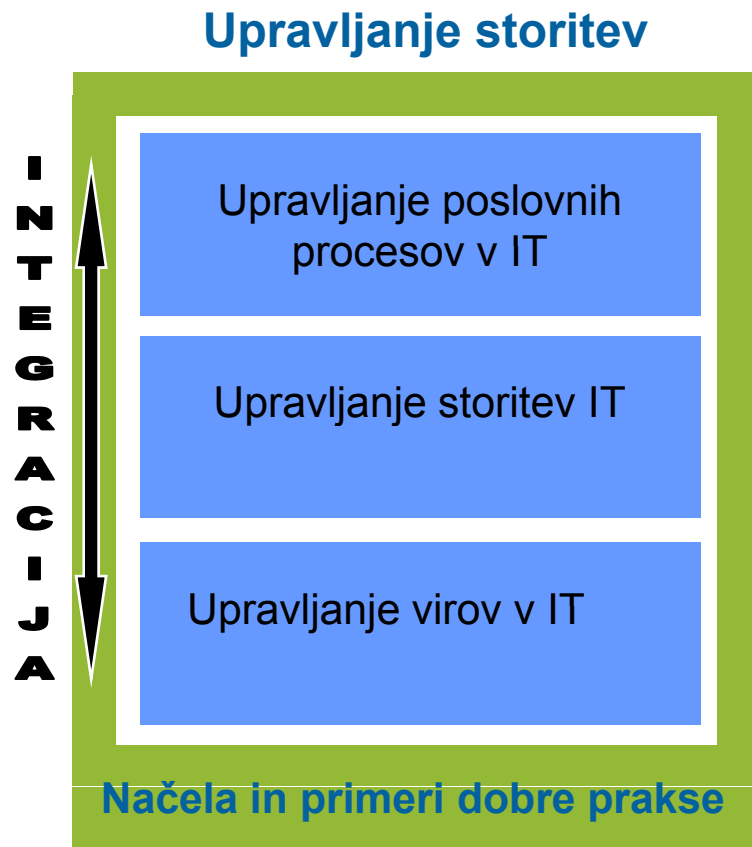
Fault management

- Osnovni cilj je zaznavanje in beleženje napak, obveščanje skrbnikov ter avtomatska odprava napak
- Fault management zajema
 - Prepoznavanje simptomov
 - Izolacijo problema
 - Odpravo napake
 - Testiranje delovanja
 - Zapis napake in postopkov za njihovo odpravo

Security management

- Cilj je nadzor nad celovitimi politikami za dostop do vseh omrežnih virov
- Na omrežjih se cilj omeji na preprečevanje nepooblaščenega dostopa do omrežnih storitev in virov
- Deloma zajema tudi spremljanje in beleženje varnostnih dogodkov v celotnem sistemu

Pristop k celovitemu upravljanju storitev



- Integriran in avtomatiziran procesni tok za procese v IT
- Upravljanje sprememb in konfiguracij
- Avtomatizirano upravljanje aplikacij, sistemov, omrežij, naprav, varnosti,...
- Načela dobre prakse, razvita orodja za implementacijo, svetovanje in pomoč pri implementaciji

Upravljanje virov

Upravljanje storitev

Upravljanje poslovnih procesov v IT

Upravljanje storitev IT

Upravljanje virov IT

Upravljanje strežnikov, omrežnih in drugih naprav

Upravljanje razpoložljivosti in zmogljivosti virov

Upravljanje poslovnih aplikacij

Optimizacija zmogljivosti, razpoložljivosti kompozitnih aplikacij

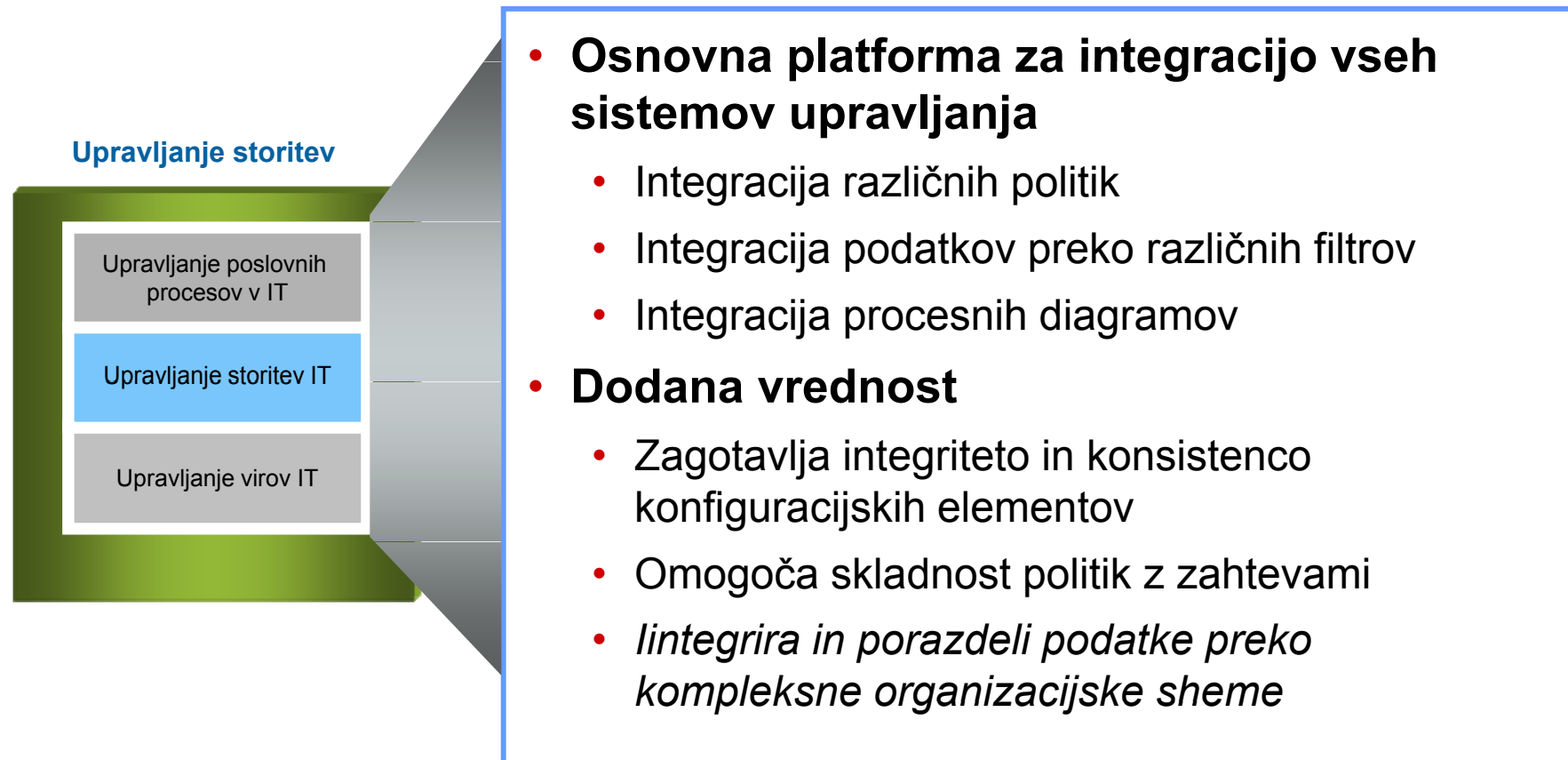
Upravljanje z diskovnimi sistemi

Backup, restore, zaščita podatkov ter optimizacija kapacitet

Upravljanje z varnostjo

zagotavljanje identitete, dostopne kontrole,...

Upravljanje storitev



Upravljanje poslovnih procesov

Upravljanje procesov

Upravljanje poslovnih
procesov v IT

Upravljanje storitev IT

Upravljanje virov IT

- WEB aplikacije, ki omogočajo implementacijo standardnih procesov v IT
- Temeljijo na izkušnjah ter uporabljajo načela dobre prakse (ITIL, eTOM, CoBIT, CMMI, and IBM PRM-IT)
- Dodana vrednost z integracijo delovnih procesov posebej za IT

Kje začeti? Kje smo sedaj in kam bi radi šli?

Tradicionalni pristop ↑ Zahtevni pristop

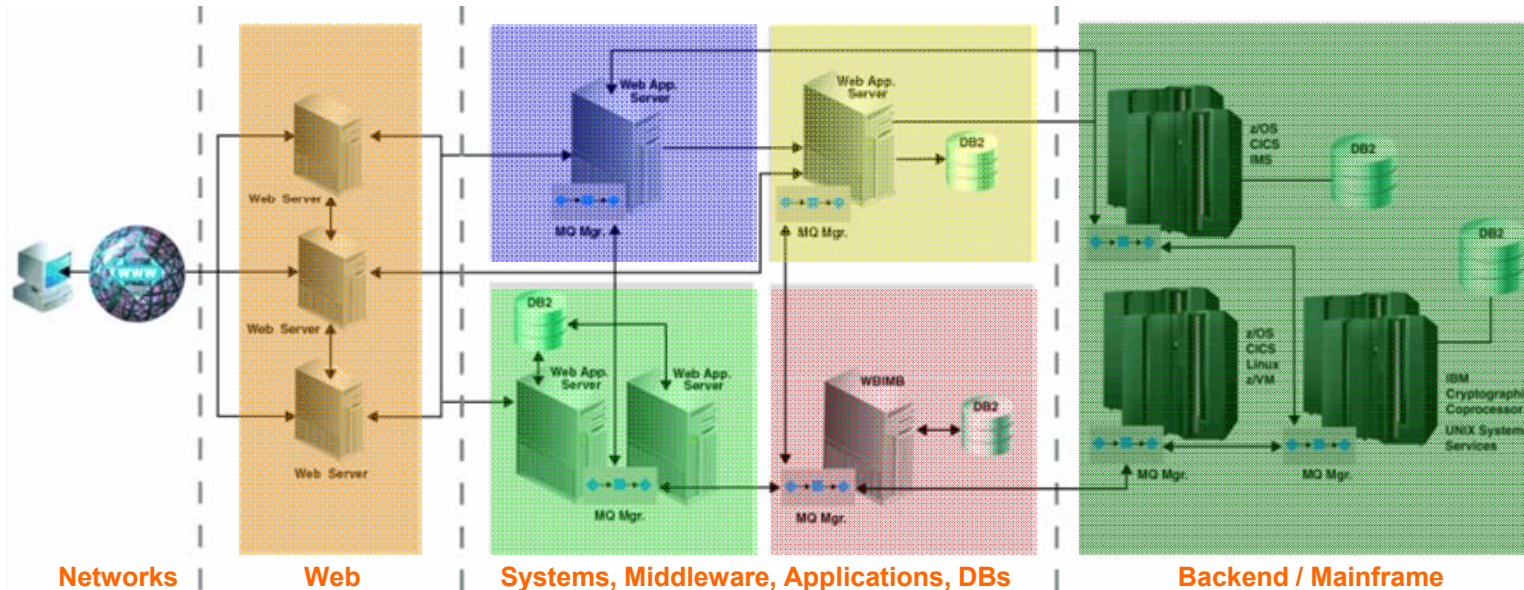


<ul style="list-style-type: none"> ✓ Delovna intenzivnost ✓ Ročno zaznavanje težav in njihova odprava 	<ul style="list-style-type: none"> ✓ Upravljanje in nadzor nad osnovno infrastrukturo ✓ Ukrepanje na osnovi dogodkov 	<ul style="list-style-type: none"> ✓ Napoved dogodkov preden do njih pride ✓ Ukrepi na osnovi analize trendov ✓ Koordinirani ukrepi 	<ul style="list-style-type: none"> ✓ Sistemi zaznajo simptome in določijo priporočene ukrepe ✓ Nadzorni sistem inicira ukrepanje 	<ul style="list-style-type: none"> ✓ Nadzorni sistem ukrepa na osnovi vnaprej določenih poslovnih politik in prioritet ✓ Avtonomno delovanje
--	--	---	---	--


 Večina podjetij je tukaj!

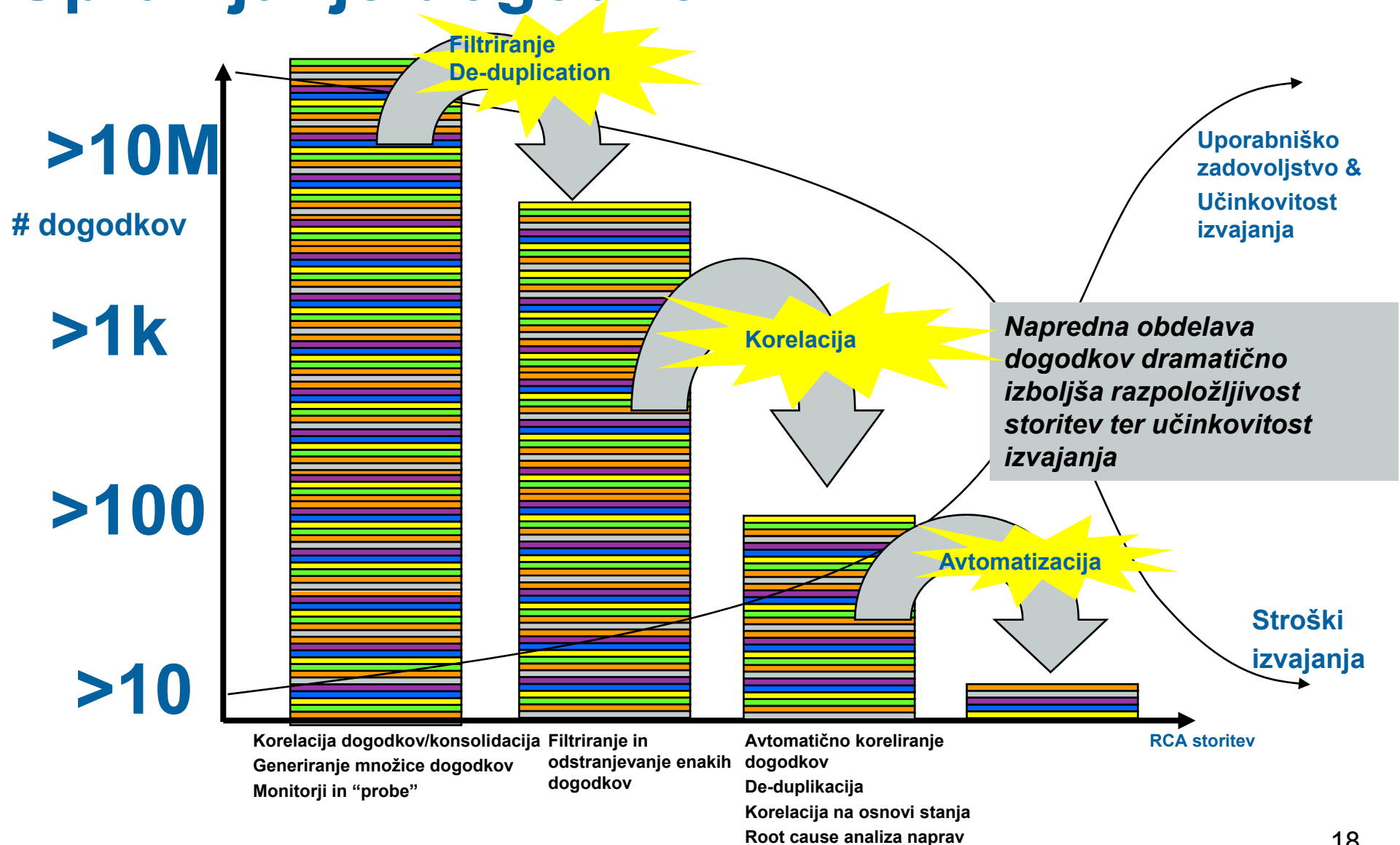


Kaj je upravljanje z dogodki?



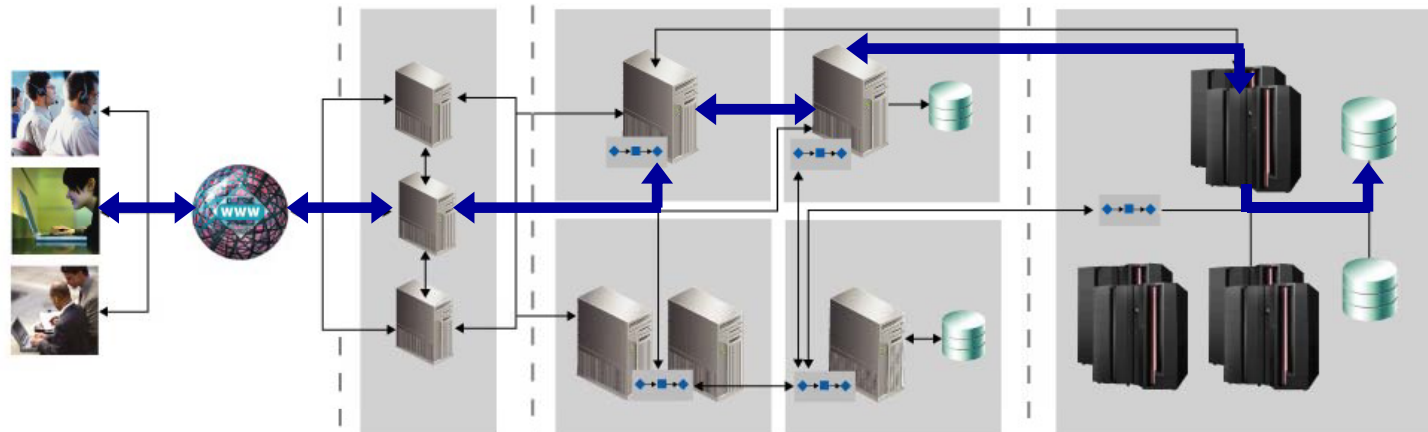
- Posamezna težava v IT infrastrukturi generira simptome v različnih komponentah infrastrukture
- Določanje konkretnega razloga za težave zahteva razumevanje dogodkov na različnih področjih in komponentah infrastrukture
- Velika, kompleksna okolja lahko generirajo velikansko število konsolidiranih dogodkov
- **Cilj upravljanja z dogodki je konsolidacija dogodkov, “root cause” analiza z identifikacijo ključnih – izvirnih težav ter, če je to mogoče, avtomatizirana odprava težav oz odgovor na težave v infrastrukturi**

Upravljanje dogodkov

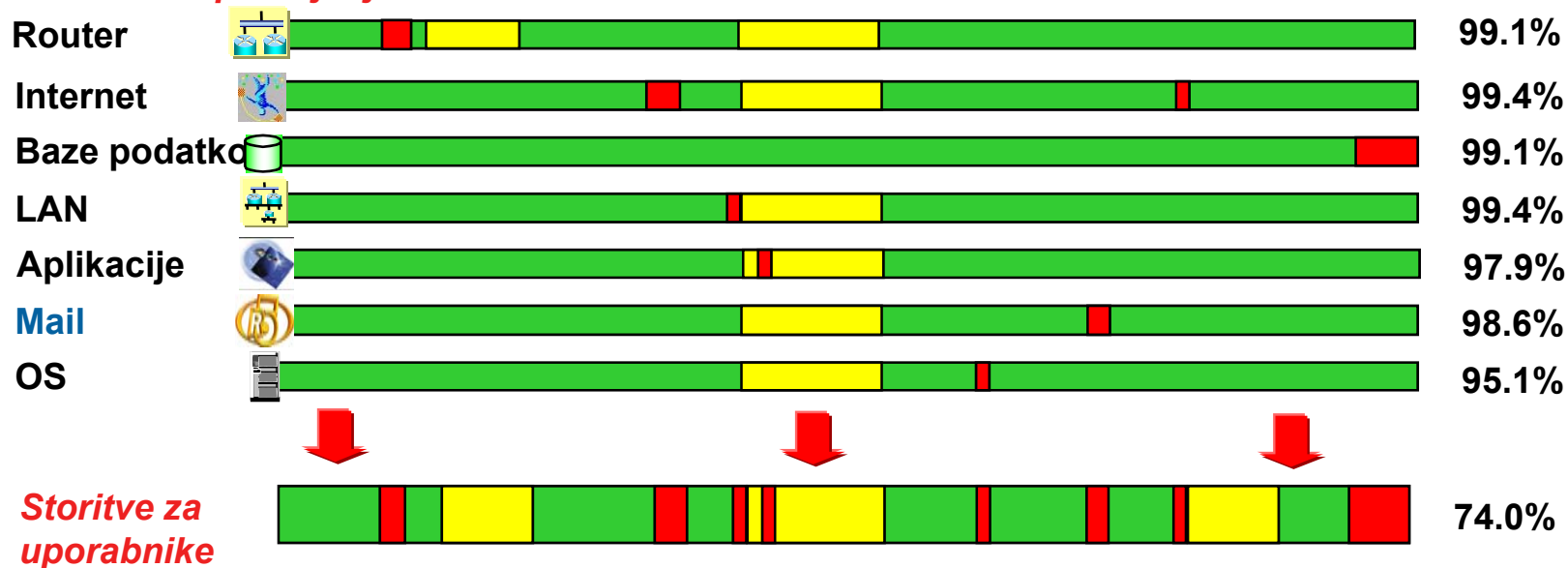


Jedro problema... nadzor nad viri IT

Uporabniška izkušnja



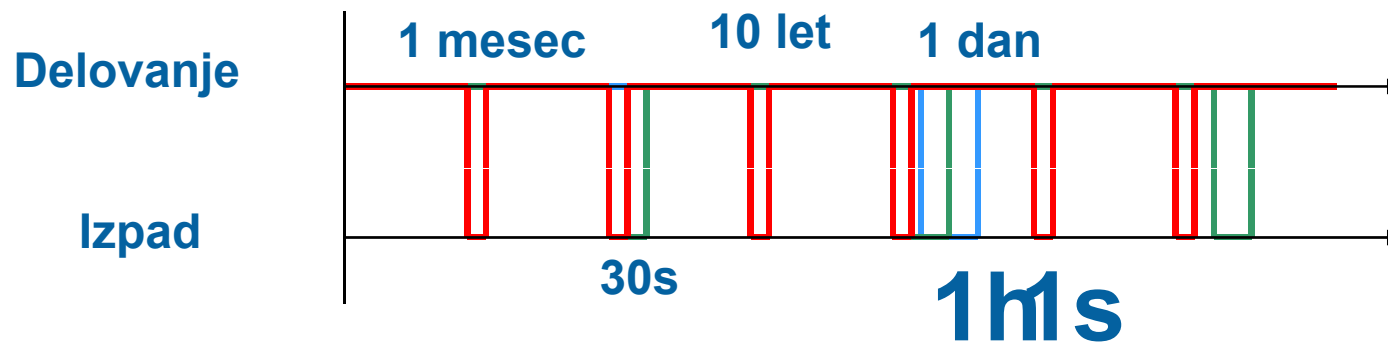
Nadzor in spremljanje virov



Zanesljivost in MTBF?

IT naročniki zahtevajo “Pet devetk” 99.999%

Primer: zanesljivost strežniškega sistema 99.99885%



■ Zanesljivost brez upoštevanja MTBF ne pomeni nič

Učinkovit nadzor in upravljanje virov

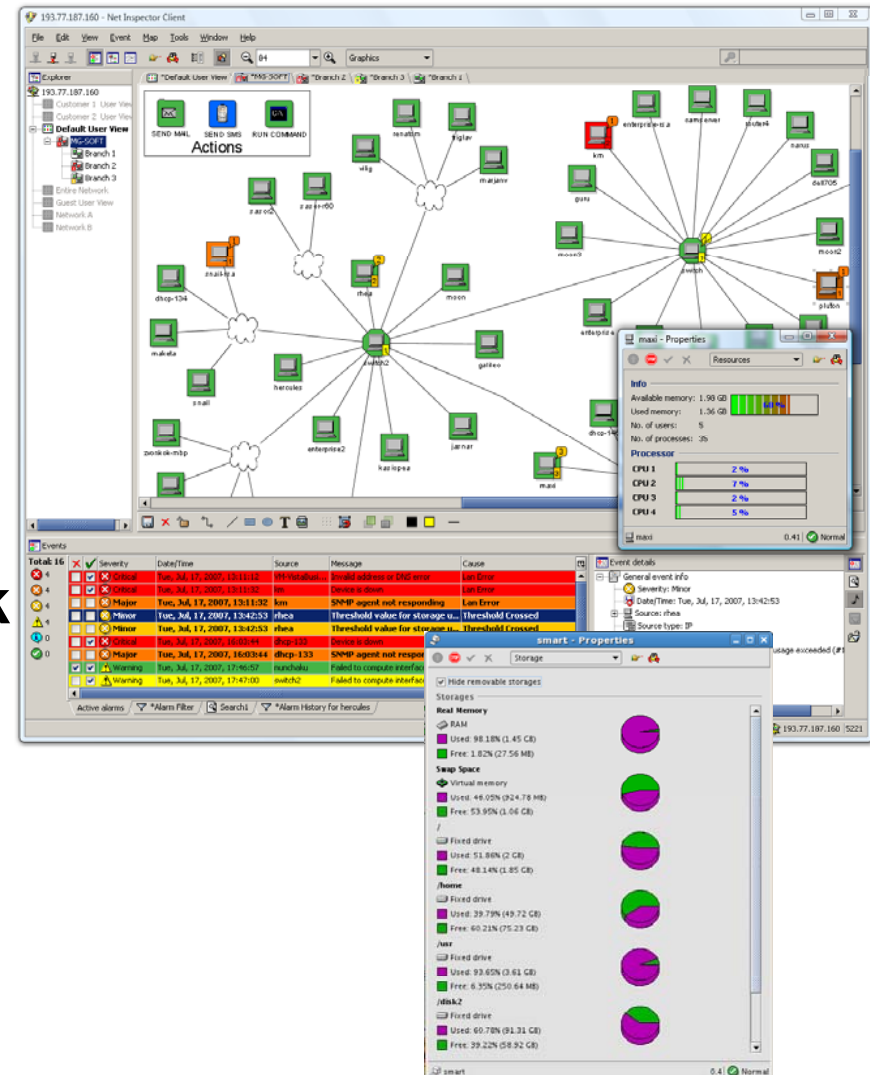
- **Nadzorljive naprave, aplikacije in storitve**
- **Orodja za nadzor in upravljanje**
- **Integracijo različnih sistemov**
- **Za vsak sistem izšolano in izkušeno osebje**
- **Stalno prisotnost osebja**
- **Učinkovite in beležene posege**

Orodja za nadzor in upravljanje

- Celovit nadzor in upravljanje procesov in storitev
 - IBM Tivoli (Netcool platforma)
 - HP Open View
 - ...
- Nadzor in upravljanje virov
 - Specifični za proizvajalce naprav in SW opreme
 - Generična, ki temeljijo na SNMP...

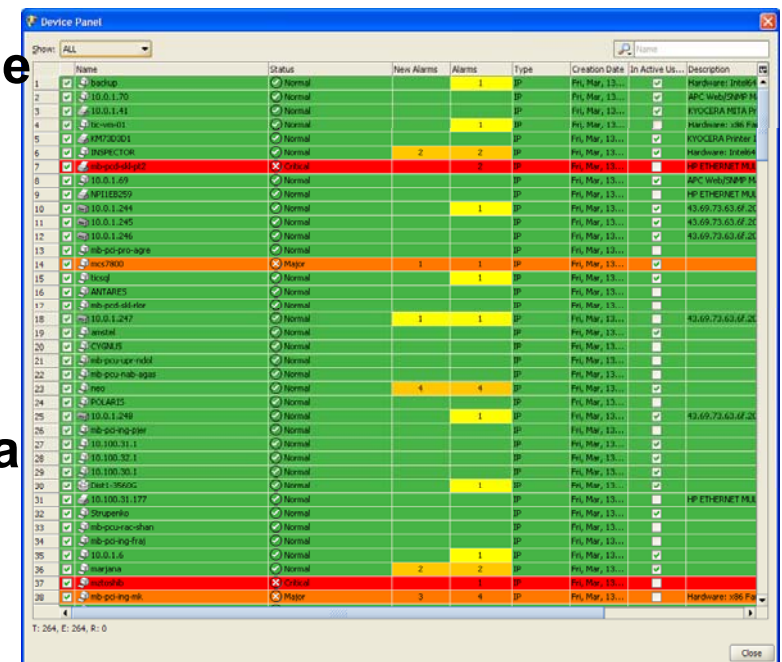
MG Soft Net inspector

- Združuje Fault in performance management
- Enostaven nadzor in upravljanje sistemskih virov – sredstev:
 - takojšnjo zaznavo napak
 - nadzor obremenjenosti
- Generiranje alarmov
- Inteligentni sistem upravljanja z alarmi
- Integrabilnost z drugimi sistemi



Glavne funkcionalnosti

- Osnova je polling preko ICMP (Ping) in SNMP protokola
- Sprejema SNMP Trap in Inform sporočila o dogodkih
- Proži dogodke in alarme (z ITU X.733 skladen alarmni sistem)
- Omogoča napredno obdelavo alarmov
- Omogoča nadzor 19 well-known omrežnih storitev ter nadzor TCP in UDP storitev, ki jih definira uporabnik
- Podpira hierarhične uporabniške poglede
- Izvaja akcije ob dogodkih:
 - zagon poljubnih aplikacij
 - pošiljanje el. pošte, SMS sporočil
 - zvočno opozarjanje na dogodke
- Nadzira naprave ne glede na proizvajalca
- Podpira zasebne MIB datoteke

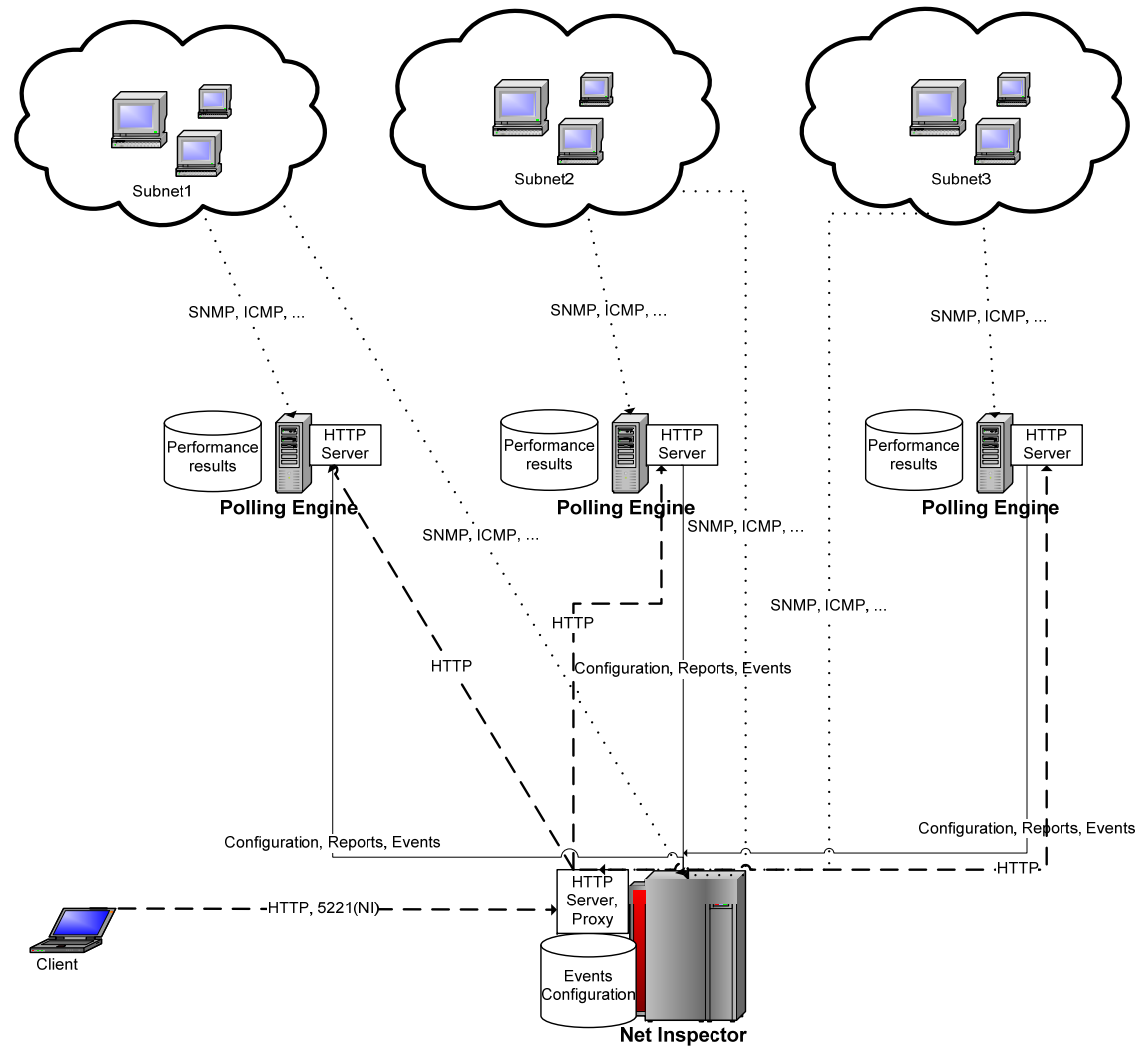


Name	Status	New Alarms	Alarms	Type	Creation Date	In Active Us...	Description
1 backup	Normal		1	IP	Fri, Mar, 13...		Hardware: Intel®
2 10.0.1.70	Normal			IP	Fri, Mar, 13...		APC Web/SNMP M...
3 10.0.1.41	Normal			IP	Fri, Mar, 13...		HYCCDA MIB TA P...
4 10.0.1.101	Normal		1	IP	Fri, Mar, 13...		Hardware: 386 P...
5 10.0.1.100	Normal			IP	Fri, Mar, 13...		HYCCDA MIB TA P...
6 10.0.1.100	Normal		2	IP	Fri, Mar, 13...		Hardware: Intel®
7 10.0.1.100	Critical	2	2	IP	Fri, Mar, 13...		HP ETHERNET M...
8 10.0.1.69	Normal			IP	Fri, Mar, 13...		APC Web/SNMP M...
9 10.0.1.245	Normal			IP	Fri, Mar, 13...		HP ETHERNET M...
10 10.0.1.244	Normal		1	IP	Fri, Mar, 13...		43.69.73.63.07.25
11 10.0.1.245	Normal			IP	Fri, Mar, 13...		43.69.73.63.07.25
12 10.0.1.246	Normal			IP	Fri, Mar, 13...		43.69.73.63.07.25
13 10.0.1.246	Normal			IP	Fri, Mar, 13...		43.69.73.63.07.25
14 10.0.1.246	Minor	1	1	IP	Fri, Mar, 13...		43.69.73.63.07.25
15 10.0.1.247	Normal		1	IP	Fri, Mar, 13...		43.69.73.63.07.25
16 10.0.1.247	Normal	1	1	IP	Fri, Mar, 13...		43.69.73.63.07.25
17 10.0.1.247	Normal			IP	Fri, Mar, 13...		43.69.73.63.07.25
18 10.0.1.247	Normal	1	1	IP	Fri, Mar, 13...		43.69.73.63.07.25
19 10.0.1.247	Normal			IP	Fri, Mar, 13...		43.69.73.63.07.25
20 10.0.1.247	Normal			IP	Fri, Mar, 13...		43.69.73.63.07.25
21 10.0.1.247	Normal			IP	Fri, Mar, 13...		43.69.73.63.07.25
22 10.0.1.247	Normal			IP	Fri, Mar, 13...		43.69.73.63.07.25
23 10.0.1.247	Normal	4	4	IP	Fri, Mar, 13...		43.69.73.63.07.25
24 10.0.1.247	Normal			IP	Fri, Mar, 13...		43.69.73.63.07.25
25 10.0.1.249	Normal		1	IP	Fri, Mar, 13...		43.69.73.63.07.25
26 10.0.1.249	Normal			IP	Fri, Mar, 13...		43.69.73.63.07.25
27 10.0.1.249	Normal			IP	Fri, Mar, 13...		43.69.73.63.07.25
28 10.0.1.249	Normal			IP	Fri, Mar, 13...		43.69.73.63.07.25
29 10.0.1.249	Normal			IP	Fri, Mar, 13...		43.69.73.63.07.25
30 10.0.1.249	Normal		1	IP	Fri, Mar, 13...		43.69.73.63.07.25
31 10.0.1.249	Normal			IP	Fri, Mar, 13...		HP ETHERNET M...
32 10.0.1.249	Normal			IP	Fri, Mar, 13...		HP ETHERNET M...
33 10.0.1.249	Normal			IP	Fri, Mar, 13...		HP ETHERNET M...
34 10.0.1.249	Normal			IP	Fri, Mar, 13...		HP ETHERNET M...
35 10.0.1.249	Normal		1	IP	Fri, Mar, 13...		HP ETHERNET M...
36 10.0.1.249	Normal		2	IP	Fri, Mar, 13...		HP ETHERNET M...
37 10.0.1.249	Critical	2	2	IP	Fri, Mar, 13...		HP ETHERNET M...
38 10.0.1.249	Major	3	4	IP	Fri, Mar, 13...		Hardware: 386 P...

Client – server arhitektura

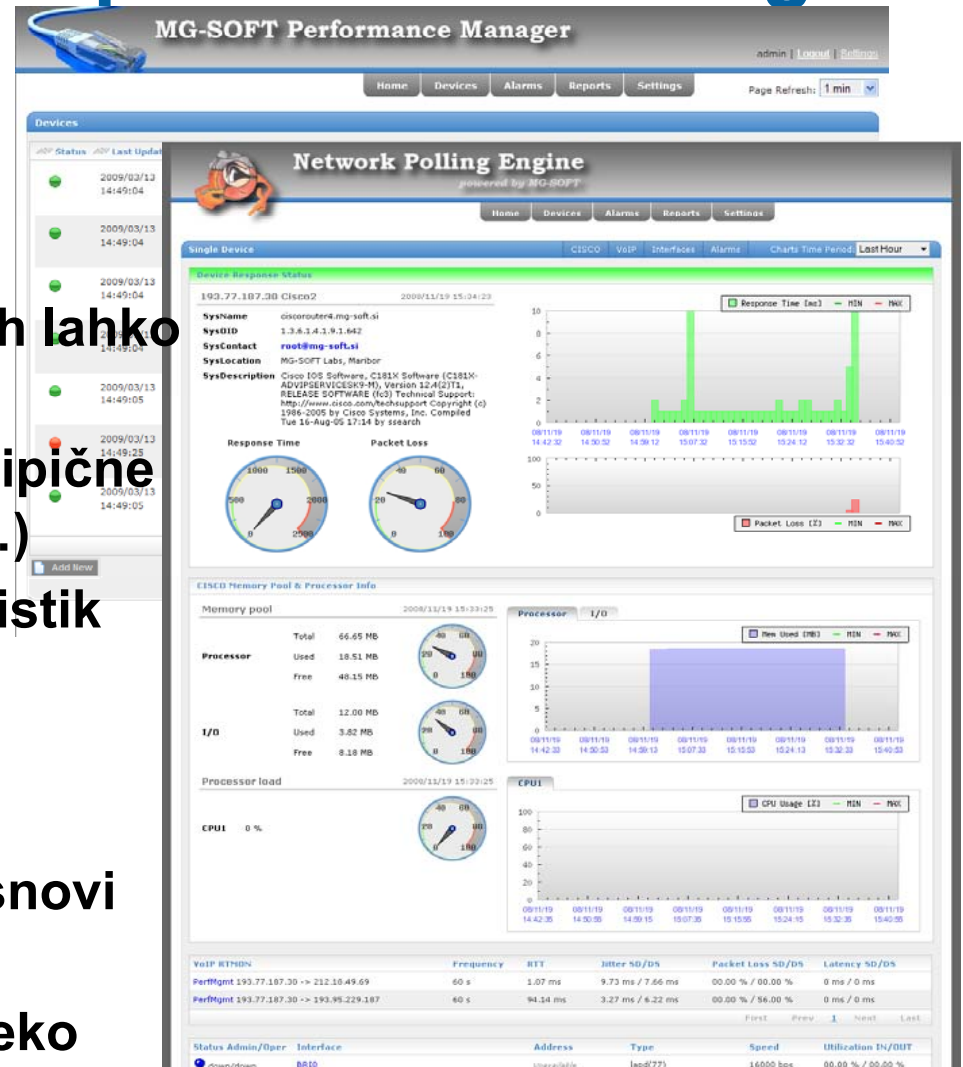
- Strežnik izvaja celoten nadzor omrežja, proži, hrani in obdeluje alarme, izvaja akcije,
- Odjemalec omogoča prikaz in modeliranje omrežja, manipulacijo alarmov ter konfiguriranje strežnika in odjemalca,
- Strežnik je na voljo za Linux in Win32/64 okolja,
- Odjemalec je Java aplikacija (neodvisna od platforme)
- Prenos in zagon odjemalca neposredno s strežnika (Java Web Start).

Več porazdeljenih pooling engine-ov



MG Soft Net inspector – performance mngt.

- Orodje za nadzor zmogljivosti sistemskih sredstev
- SNMP kot osnovni protokol
- Nadzor nad vsemi parametri, ki jih lahko spremljamo preko SNMP
- Vnaprej pripravljena poročila za tipične naprave (cisco stikala, routerje,...)
- Že vgrajeno spremljanje karakteristik QoS za potrebe VoIP
- Orodje je lahko integrirano v Net inspector
- Možno generiranje alarmov na osnovi prekoračenih vrednosti
- Dostop do konzole je mogoče preko brskalnika



Storitve nadzora in upravljanja

- **Pritisk na stroške v podjetjih je vedno večji**
- **Za vsak sistem potrebujemo izšolano osebje**
- **Osebje mora biti ves čas na voljo**

Zunanje izvajanje - outsourcing

Storitve nadzora in upravljanja

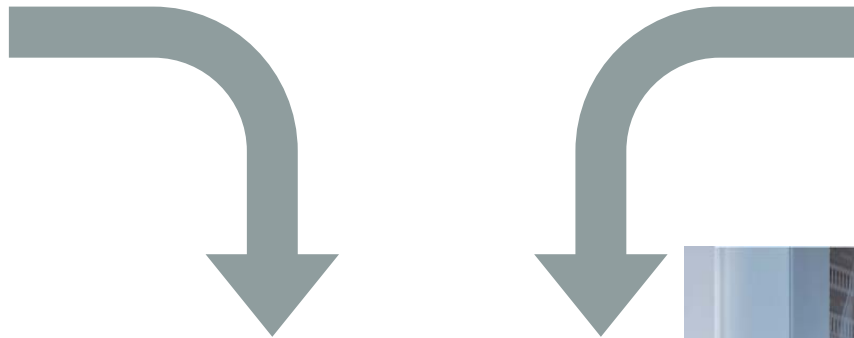
- **Zajemajo**
 - **Fault management**
 - **Performance management**
 - **Vzdrževanje naprav**
 - **Configuration management**
 - **Podporo uporabnikom**
- **Uporabnik ima samostojni dostop do vseh informacij in konzol**

Storitve nadzora in upravljanja

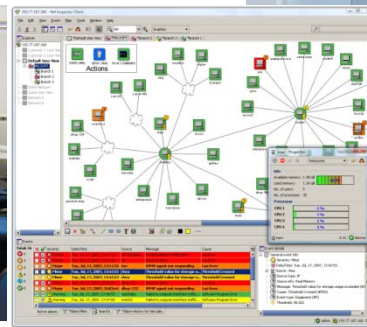
Help desk



Izšolano osebje



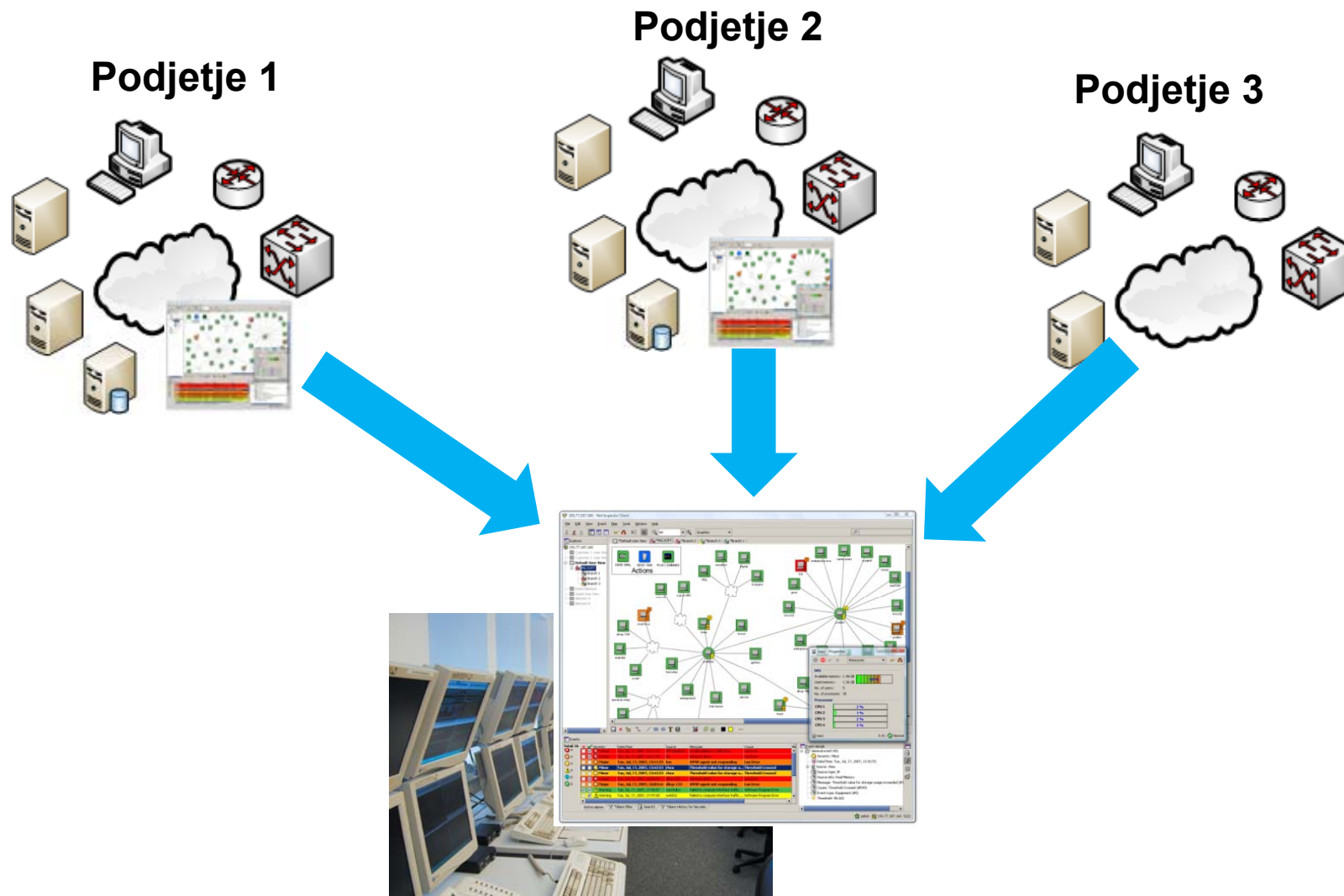
Nadzorni center z opremo



Storitve nadzora in upravljanja

- **Nadzor omrežja, strežnikov, aplikacij ...**
- **Alarmiranje in odprava napak (odzivni čas pod 15 minut)**
- **Spremljanje razpoložljivosti naprav**
- **Analiza dogodkov na napravah**
- **Analiza zmogljivostnih parametrov**
- **Vzdrževalni posegi**
- **Implementacijo servisnih popravkov na naprave**
- **Administracija naprav**
- ...

Način postavitve





Boštjan Lavuger
Comtron d.o.o.