Naplózó rendszer syslog-ng alapon

Szigeti Szabolcs
Adamkó Péter
Gábor Ádám
BME (IT)[2]
Major Csaba
Balabit Kft.

INFORMATION TECHNOLOGY INNOVATION AND KNOWLEDGE CENTRE

MŰEGYETEM 1782

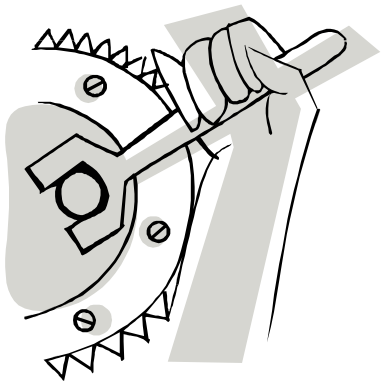
Tartalom

- A projekt
- $(IT)^2$ röviden
- Célok
- Megvalósítás
- Eredmények

MŰEGYETEM 1782

A projekt

- Cél:
  - syslog-ng alapon naplózó infrastruktúra keretrendszer kialakítása
  - Közös Balabit – BME fejlesztés
  - CeBIT 2007



MŰEGYETEM 1782

$(IT)^2$

- Információtechnológiai és Innovációs Tudásközpont
- 2006-ban indult, NKTH támogatás első 3 évben
- K+F projektek ipari partner és egyetem részvételével

INFORMATION TECHNOLOGY INNOVATION AND KNOWLEDGE CENTRE

MŰEGYETEM 1782

Igények

- Naplógyűjtő infrastruktúra
- Naplózni szükséges! Komplex integrált menedzsmentrendszerre nem mindig van szükség.
- Naplót elemezni sokféle módon lehet.
- Most csak naplózni akarunk!

MŰEGYETEM 1782

Követelmények

- Központilag menedzselhető naplózó infrastruktúra
- Skálázható, hierarchikus, nagyteljesítményű
- Könnyű használhatóság, fókuszált funkciók

MŰEGYETEM 1782

Felépítés

- Naplógyűjtés fa struktúrában.
- Fa gyökere a naplóesemények végső nyelője
- Fa csomópontjai és levelei: relay
  - naplóesemények fogadás
  - alapvető szűrések
  - appliance
  - távoli menedzsment

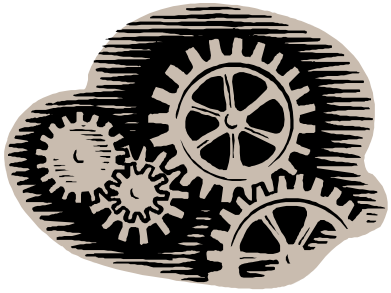
MŰEGYETEM 1782

Felépítés / 2

- Menedzsment központ
  - relay konfigurációk / firmware tárolása
  - központi konfiguráció tárolása
  - web felület
- Napló adatbázis
  - események gyűjtése
  - kapcsolat elemző rendszerek felé

MŰEGYETEM 1782

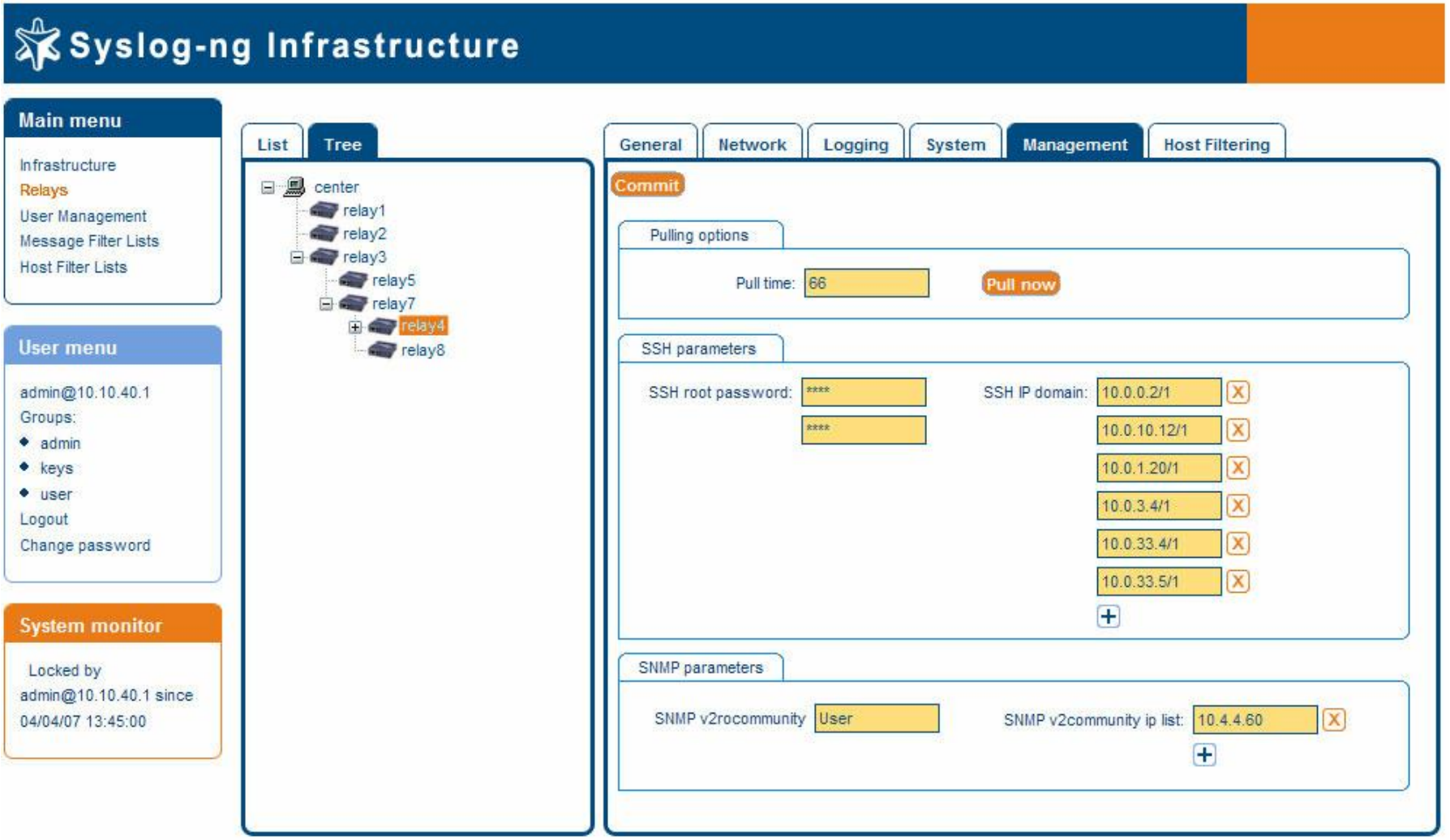
Komponensek



- syslog-ng
  - syslog protokoll kezelése
  - szűrések
- Web felület AJAX technológiával
- SQL adatbázis

MŰEGYETEM 1782

Kezelő felület



MŰEGYETEM 1782

Köszönöm a figyelmet

szigi@ik.bme.hu

Pázmány Péter program

A projekt a Nemzeti Kutatási és Technológiai Hivatal támogatásával valósult meg.

NKTH
Nemzeti Kutatási és Technológiai Hivatal

INFORMATION TECHNOLOGY INNOVATION AND KNOWLEDGE CENTRE