Monitoring sítě, ZABBIX

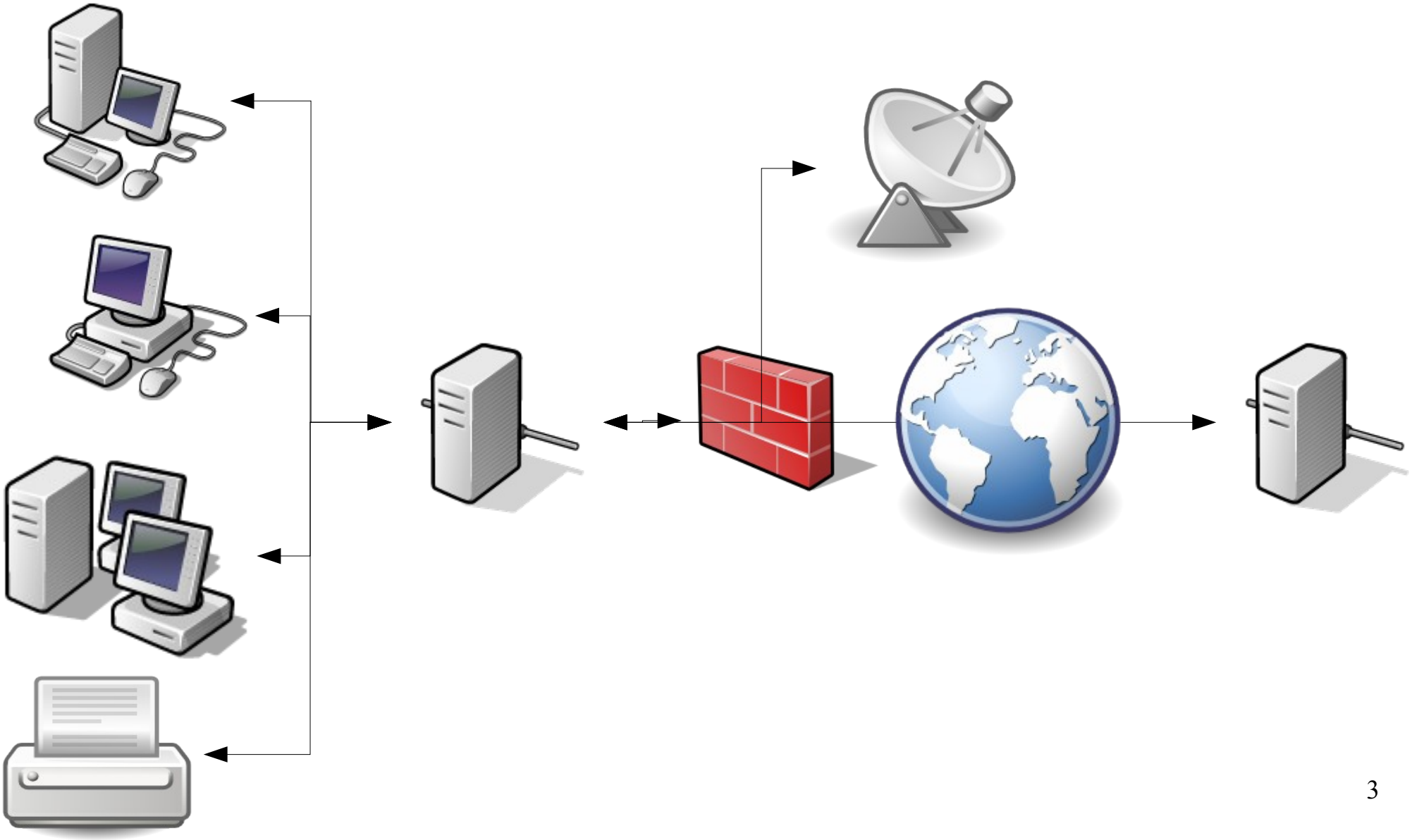
InstallFest 2005

Jaroslav Vorlíček
LOGIOS s.r.o.
jaroslav.vorlicek@logios.cz

Monitoring ?

- dostupnosti vzdálených serverů a zařízení
- služeb na vzdálených strojích
- hardwarových prostředků
- aktivních síťových prvků

Monitoring sítě

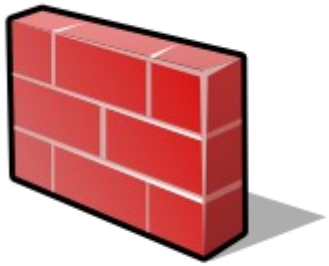


Monitoring dostupnosti

- Fyzická paměť
- Místo na disku
- Místo na swap
- Integrita souborů :
  - Konfigurační soubory
  - Soubory s hesly
  - Dokumentace

Monitoring výkonu

- Využití procesoru
- I/O operace na disku a diskových polích
- Síťová aktivita
- Aktivita odkládacího souboru



Proč monitoring ?

- součást bezpečnostních směrnic a standardů
- upozorňování při výpadcích
- plánování upgrade
- analýza dostupnosti IT služeb

ZABBIX

- je systém na monitorování aplikací a sítě
- principy :
  - Co nejjednodušší
  - Otevřený a uživatelsky přívětivý systém
  - Používat co nejméně systémových prostředků

Proč ZABBIX ?

- Snadná instalace
- Snadná konfigurace – Web rozhraní
- Žádné nutné pluginy
- Mnoho monitorovatelných systémových parametrů

Proč ZABBIX ?

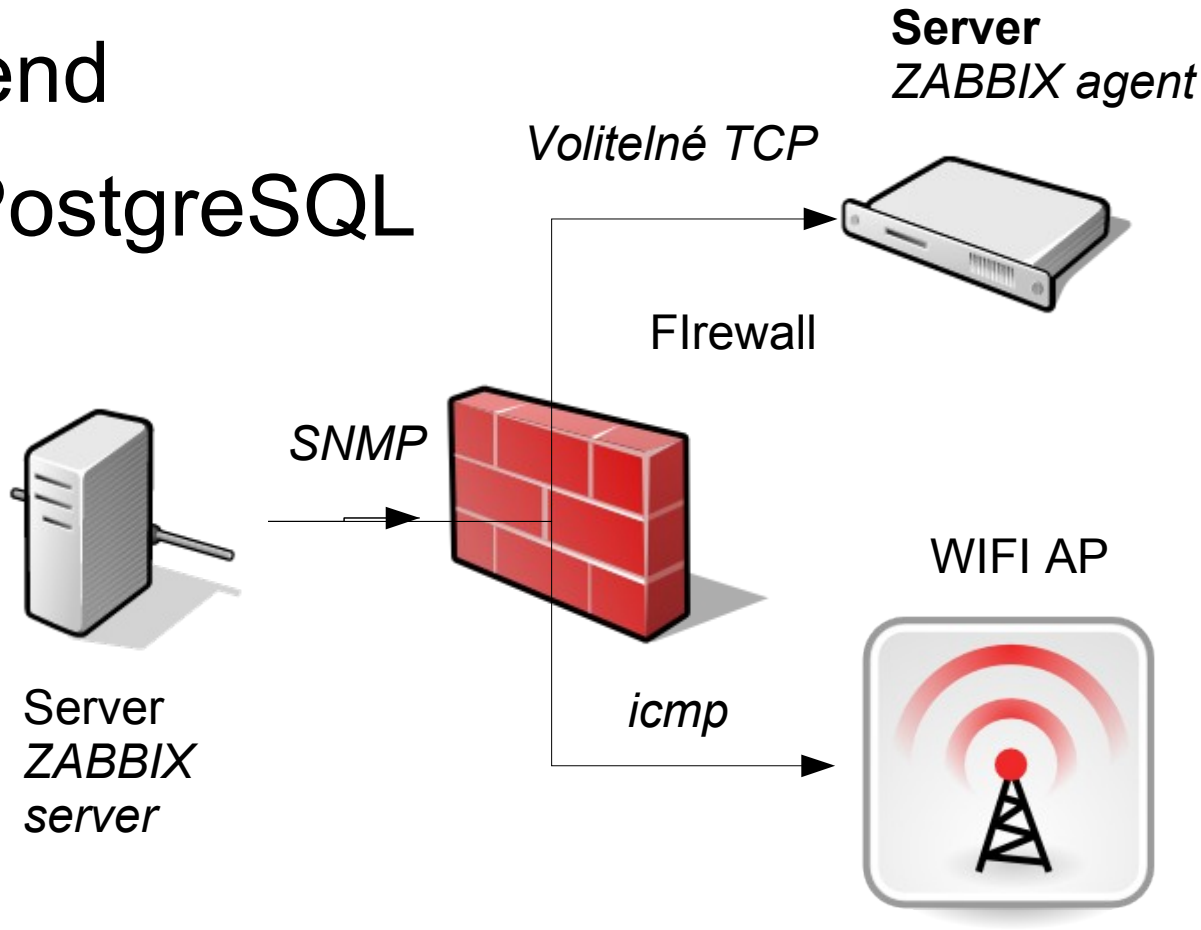
- Oznamování událostí (email,SMS)
- Hierarchie IT služeb
- Síťové mapy
- Monitoring Míry dostupnosti služeb (SLA)
- Uživatelsky definovatelné grafy :-)

Proč ZABBIX?

- Vše na jednom místě v databázi
- Stabilní
  - léta používaný mnoha společnostmi (banky , telekomunikační společnosti)
- Rozšířitelný
  - možnost spuštění na klientovi vlastních detekčních skriptů a aplikací
  - Open Source

Architektura

- Centralizovaný monitoring
- Architektura klient-server
- PHP frontend
- MySQL | PostgreSQL backend

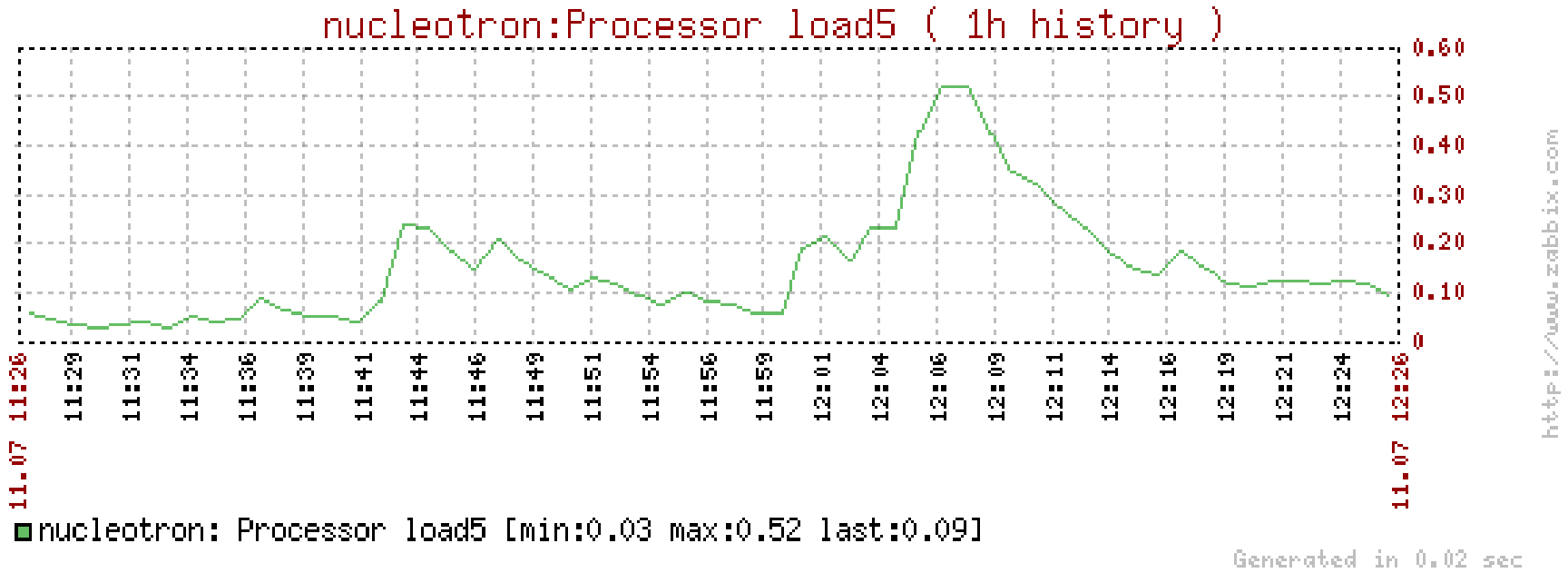


Podporované platformy - klienti

- Linux – Red Hat, SuSe, Debian, Gentoo, Fedora Core .....
- BSD (OpenBSD, FreeBSD, NetBSD)
- Microsoft Windows (XP, 2000, 2003)
- Cokoliv, co podporuje SNMP (SNMPv1, SNMPv2)
- HP – UX, Solaris, AIX, AS/400, Novell Netware,

Grafy

- Motto: zobrazit v grafu vše, co se monitoruje
- Velká možnost volby
  - několik měřených hodnot v jednom grafu



Web - Konfigurace

- Média
  - email
  - Script
- Úklid starých a nepotřebných záznamů

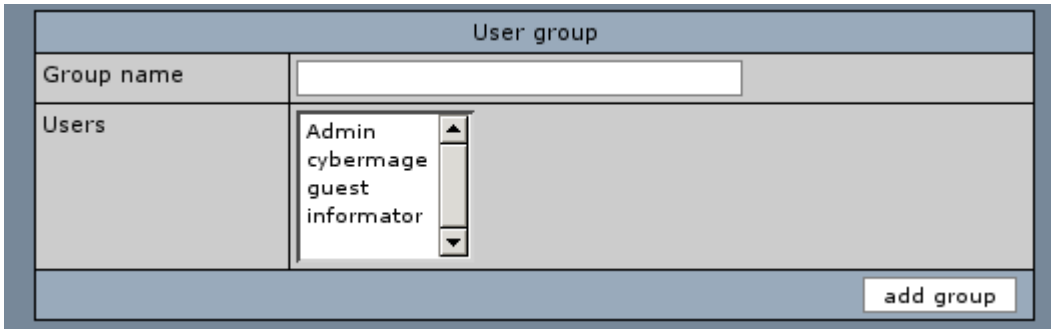
Configuration	
Do not keep alerts older than (in days)	365
Do not keep alarms older than (in days)	365
	update

Media	
Description	
Type	Email
SMTP server	localhost
SMTP helo	localhost
SMTP email	zabbix@localhost
	add

AVAILABLE MEDIA TYPES			
Id	**Type**	**Description**	**Actions**
1	Email	Email	Change
2	Script	Notifikace skriptem	Change

Web - Users

- Skupiny uživatelů
- Přístupová práva
- Kontaktní média
- Doručování zpráv dle důležitosti



CONFIGURATION OF USER GROUPS

Name	Members	Actions
Database administrators	Admin, cybermage, informator	Change

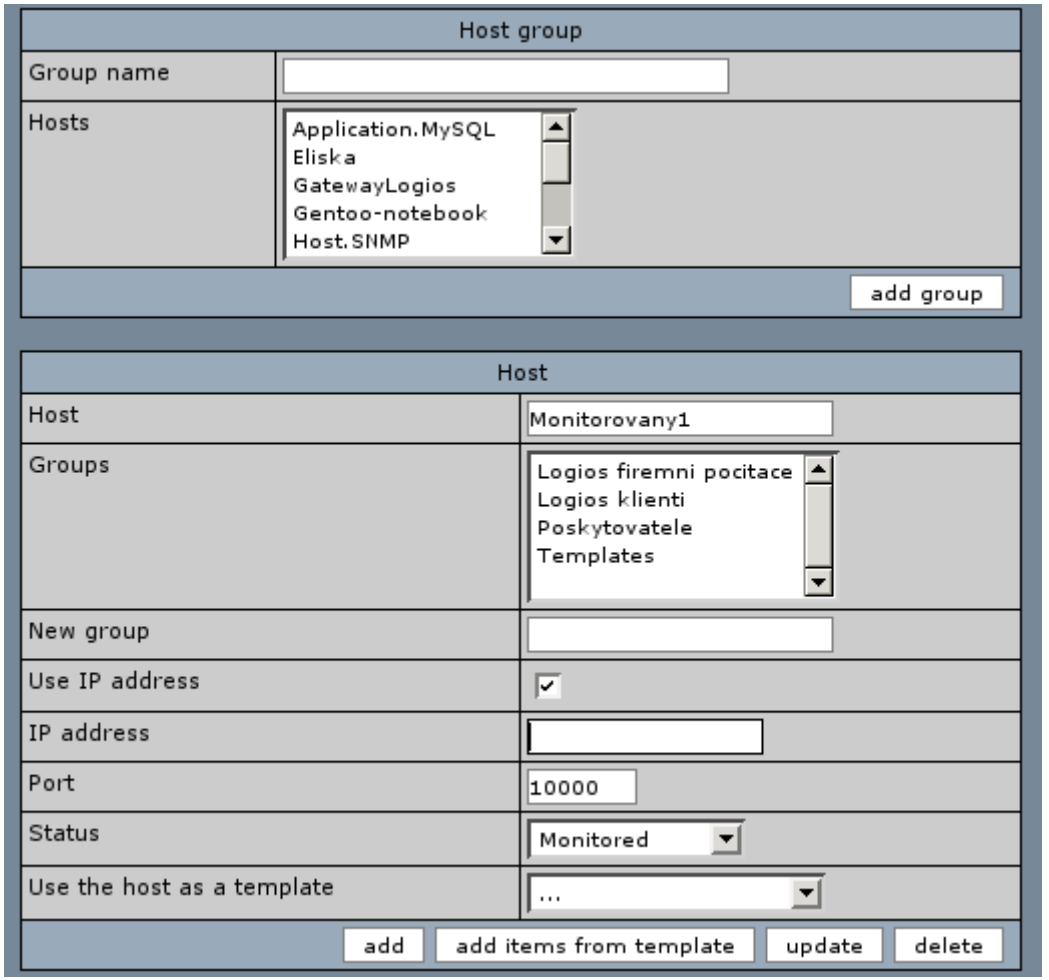
CONFIGURATION OF USERS

Alias	Name	Surname	Is online?	Actions
Admin	Zabbix	Administrator	Yes	Change - Media
cybermage	Jaroslav	Vorlicek	Yes	Change - Media
guest	Default	User	No	Change - Media
informator	Informator	Informaticny	No	Change - Media

Web - Hosts

- Definice jednotlivých monitorovaných hostů
- Definice šablon
- Definice skupin

CONFIGURATION OF HOST GROUPS		
Id	**Name**	**Actions**
2	Logios firemni pocitace	Change
3	Logios klienti	Change
4	Poskytovatele	Change
1	Templates	Change

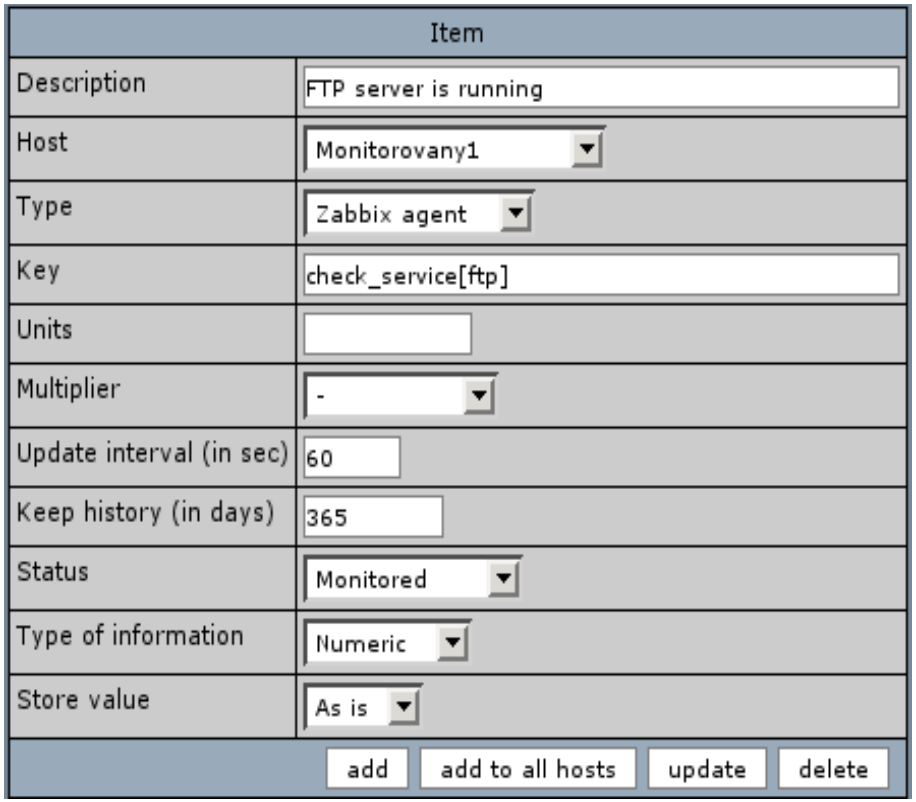


Web - Items

- Definice monitorovaných parametrů pro jednotlivé hosty
- Způsoby testování

  Agent, Simple check,

  SNMPvX agent
- Key parametr



Web - Triggers

- Například :

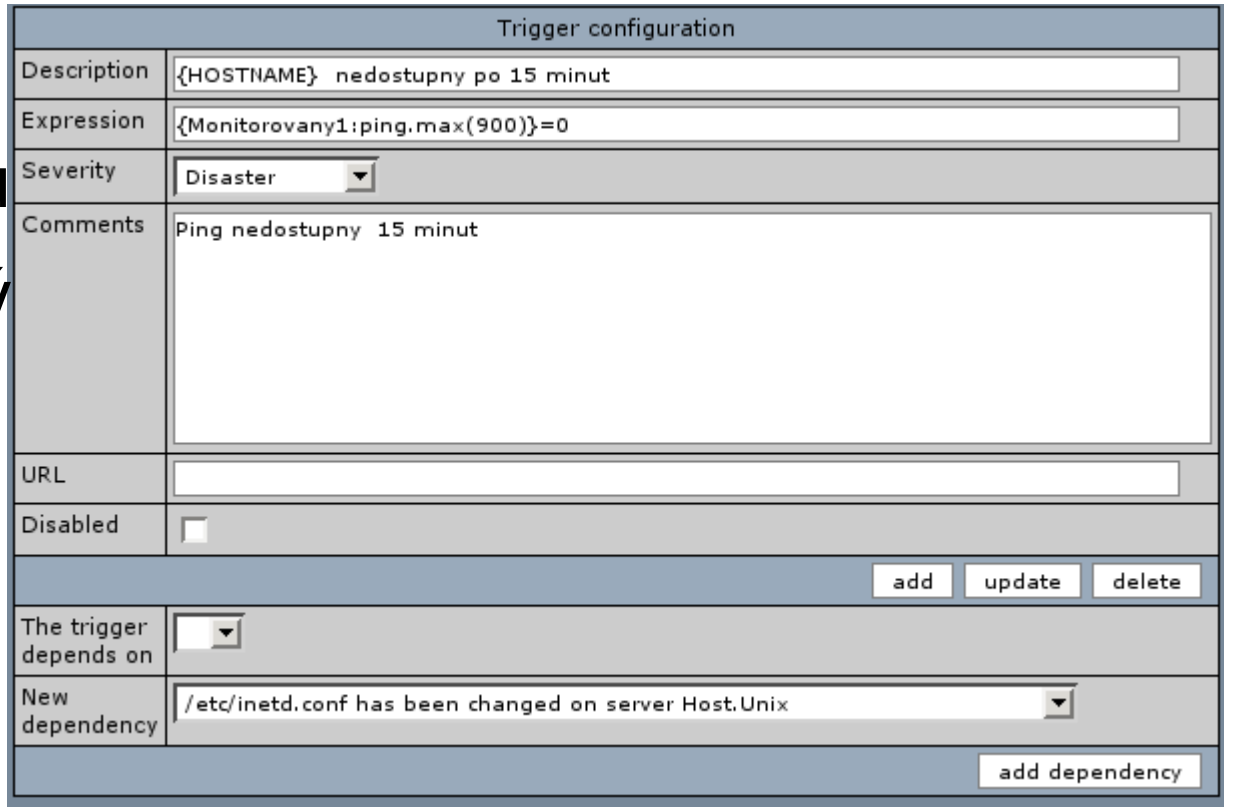
  Pokud půl hodiny

  není místo na disku

  Server nedostupný

- Výrazy
  - max, min, avg,

    delta ..
  - +, -

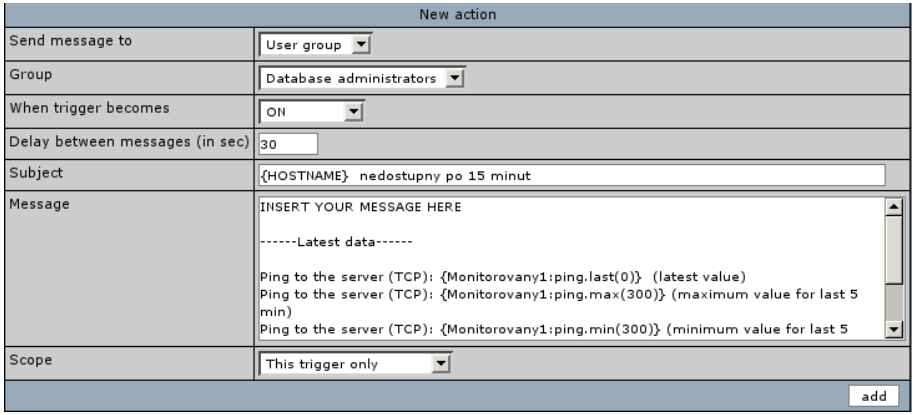


Upozornění

- Události
- Oznámení

skupině uživatelů,uživateli

- Uživatelská média
  - Email, skript ....



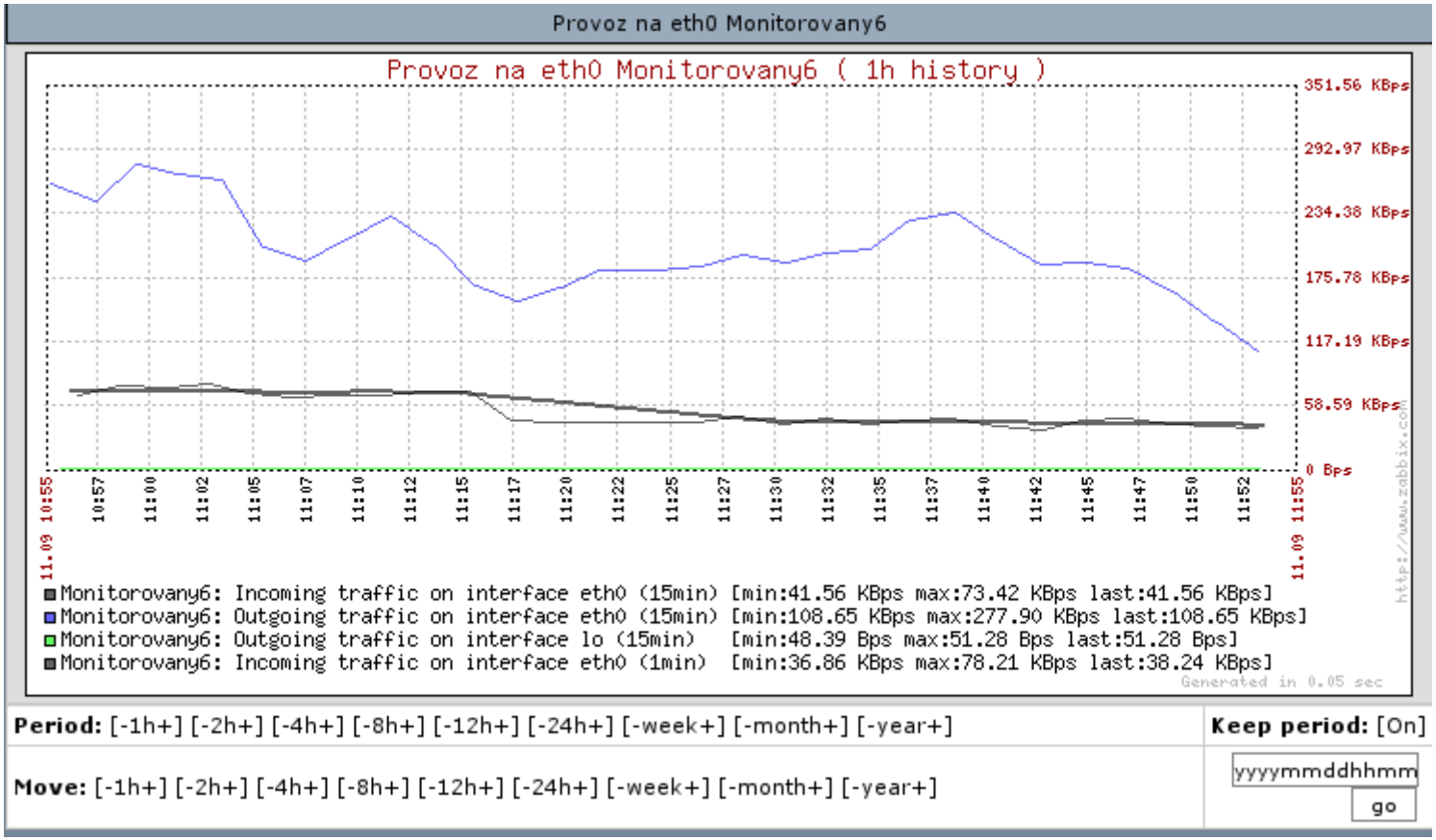
Monitorovany1 nedostupny po 15 minut
{Monitorovany1:ping.**max**(900)}=0

Scope	Send message to	When trigger	Delay	Subject	Actions
Trigger	Database administrators	ON	30	{HOSTNAME} nedostupny po 15 minut	Change

Web – Graphs

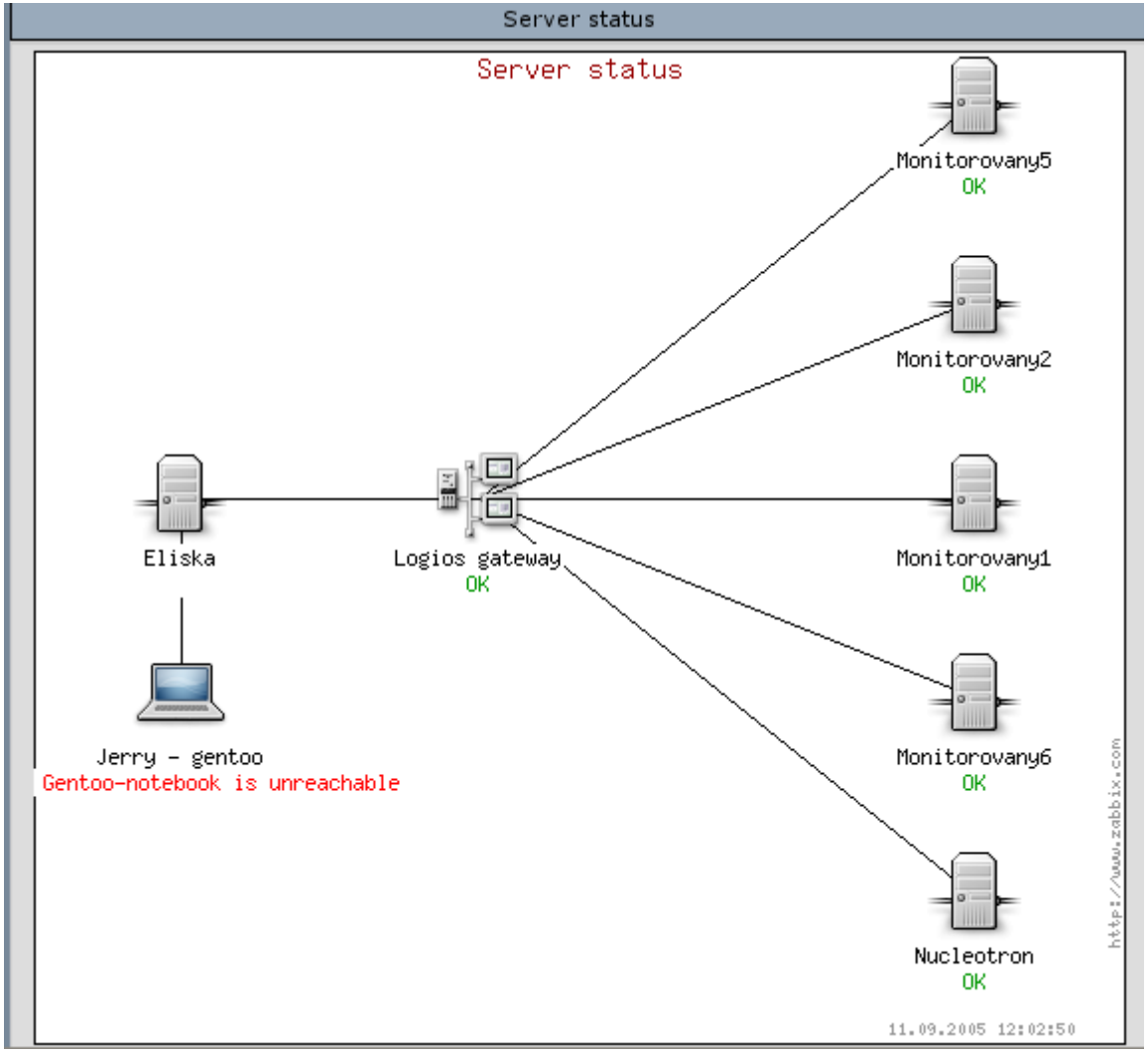
- Tvorba grafu
- Typy grafů
- Zdrojová

  data



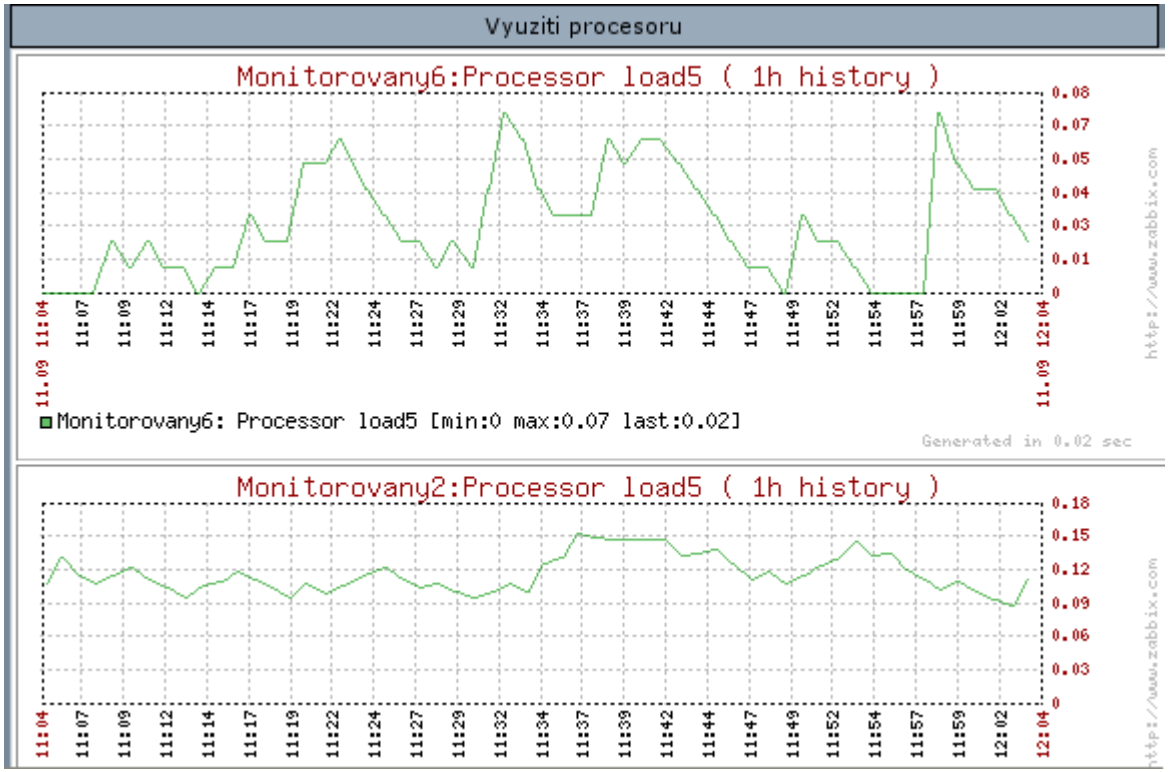
Web – Network maps

- Definice map
- Definice závislostí



Web - Screens

- Cokoliv na jedné obrazovce :
  - Vytvořené grafy
  - Mapy
  - Grafy z hodnot



Web – IT services

- Definice

IT SERVICES AVAILABILITY REPORT
Gentoo-notebook

2003 2004 **[2005]**

From	Till	OK	Problems	Percentage	SLA
27 Dec 2004	03 Jan 2005	7d 0h 0m	0d 0h 0m	100.00%/0.00%	9.99%
03 Jan 2005	10 Jan 2005	7d 0h 0m	0d 0h 0m	100.00%/0.00%	9.99%
10 Jan 2005	17 Jan 2005	7d 0h 0m	0d 0h 0m	100.00%/0.00%	9.99%
17 Jan 2005	24 Jan 2005	7d 0h 0m	0d 0h 0m	100.00%/0.00%	9.99%
24 Jan 2005	31 Jan 2005	7d 0h 0m	0d 0h 0m	100.00%/0.00%	9.99%
31 Jan 2005	07 Feb 2005	7d 0h 0m	0d 0h 0m	100.00%/0.00%	9.99%
07 Feb 2005	14 Feb 2005	7d 0h 0m	0d 0h 0m	100.00%/0.00%	9.99%
14 Feb 2005	21 Feb 2005	7d 0h 0m	0d 0h 0m	100.00%/0.00%	9.99%
21 Feb 2005	28 Feb 2005	7d 0h 0m	0d 0h 0m	100.00%/0.00%	9.99%
28 Feb 2005	07 Mar 2005	7d 0h 0m	0d 0h 0m	100.00%/0.00%	9.99%
07 Mar 2005	14 Mar 2005	7d 0h 0m	0d 0h 0m	100.00%/0.00%	9.99%
14 Mar 2005	21 Mar 2005	7d 0h 0m	0d 0h 0m	100.00%/0.00%	9.99%
21 Mar 2005	28 Mar 2005	7d 0h 0m	0d 0h 0m	100.00%/0.00%	9.99%
28 Mar 2005	04 Apr 2005	7d 0h 0m	0d 0h 0m	100.00%/0.00%	9.99%
04 Apr 2005	11 Apr 2005	7d 0h 0m	0d 0h 0m	100.00%/0.00%	9.99%
11 Apr 2005	18 Apr 2005	7d 0h 0m	0d 0h 0m	100.00%/0.00%	9.99%
18 Apr 2005	25 Apr 2005	7d 0h 0m	0d 0h 0m	100.00%/0.00%	9.99%
25 Apr 2005	02 May 2005	7d 0h 0m	0d 0h 0m	100.00%/0.00%	9.99%
02 May 2005	09 May 2005	7d 0h 0m	0d 0h 0m	100.00%/0.00%	9.99%
09 May 2005	16 May 2005	7d 0h 0m	0d 0h 0m	100.00%/0.00%	9.99%

Web – informace o stavu

- Triggers
- Queue
- Alarm
- Alerts

TRIGGERS [12:12:35]

Description	Status	SEVERITY	Last change	Comments
Server Gentoo-notebook is unreachable	TRUE	High	31 Oct 14:36:16	Add

QUEUE OF ITEMS TO BE UPDATED

Next time to check	Host	Description
11.09.2005 12:13:48	Monitorovany5	Outgoing traffic on interface eth0 (15min)
11.09.2005 12:13:48	Monitorovany5	Outgoing traffic on interface lo (5min)
11.09.2005 12:13:48	Monitorovany5	Incoming traffic on interface eth0 (5min)

ALARMS

Time	Description	Value	Severity
2005.Nov.09 11:54:29	SSH server is down on Monitorovany5	OFF	Average
2005.Nov.09 11:53:28	SSH server is down on Monitorovany5	ON	Average
2005.Nov.09 11:47:30	Gentoo-notebook minutu nedostupny	UNKNOWN	Average

ALERTS

Time	Type	Status	Recipient(s)	Subject	Message
2005.Nov.09 11:53:29	Email	sent	jaroslav.vorlicek@logios.cz	SSH server is down on Monitorovany5	INSERT YOUR MESSAGE HERE ------Latest data------ SSH server is running: 0 (latest value) SSH server is running: 0 (maximum value for las SSH server is running: 0 (minimum value for las ---------End--------

Co mi ZABBIX přinese ?

- Aktuální a srozumitelný přehled dění
- Přehled o historii
- Možnost srovnání
- Možnost plánování
- Možnost včasné reakce

Kde hledat a kde se ptát ?

- Web

  http://www.zabbix.com

- IRC

  irc.freenode.net

  kanál #zabbix

  (Nejvice tam ví James_Wells a alexei :o))

Dotazy

Ptejte se mne na co chcete, na co chci já odpovím ...

Děkuji za pozornost