BR4RB

Be ready for real business

AKO NAINŠTALOVAŤ ICINGA1 MONITORING

VZDELÁVACÍ VÝSTUP ZO ŠTUDENTSKEJ STÁŽE V PROJEKTE BE READY FOR REAL BUSINESS

Erasmus+

Projekt je financovaný zo zdrojov EÚ v rámci programu Erasmus+

Obsah

1 Úvod

V tomto dokumente som sa zameral na open source monitoring ICINGA presnejšie

ICINGA 1.Povieme si čo to vlastne monitoring ICINGA 1 je a ako funguje.

2 Čo je to ICINGA 1 monitoring ?

ICINGA je populárny open source systém pre automatizované sledovanie stavu siete.

Jeho použitie je primárne smerované na operačný systém Linux, avšak funguje na všetkých UN*X kompatibilných systémoch, ako aj solaris a HP-UX.

Sleduje sieťové služby, upozorňuje užívateľa keď je problém v sieti a tiež ho upozorňuje keď je problém vyriešený.

Projekt **ICINGA** vznikol ako fork projektu **NAGIOS** s ktorým je konfiguračne kompatibilný.

3 Možnosti kontrol

V štandardnom distribučnom balíčku **ICINGA** neponúka žiadne monitorovacie pluginy.

Tieto pluginy je nutné stiahnúť zo stránky **NAGIOS**.

Monitoring štandardných sieťových služieb :

- Monitorované pokusom o spojenie so službou a komunikácia so službami (SMTP,POP3,IMAP,HTTP,...)

Sledovanie stavu servera :

- **Hardware** – Pomocou protokolu SNMP sa ICINGA pýta na parametre HW, to je dostupné prevažne u Enterprise zariadení (teplota komponentov,odber prúdu,...)
- **Software** – Monitoring operačného systému, vyťaženie pamäte, CPU, počet spustených procesov, voľné miesto na disku

4 Architektúra

Icinga je rozdelená na niekoľko modulov. Hlavným modulom je Icinga Core, ktorý sa stará o prevedenie jednotlivých kontrol. Výsledky týhto kontrol sú ukladané cez komponent IDOMOD do IDO2DB a prezentované sú vrstvou ICINGA Web.

ICINGA Core – Hlavným motorom celého systému je modul ICINGA Core, ktorý vykonáva jednotlivé kontroly pomocou pluginov. Spúštanie kontrol rieši integrovaný plánovač úloh, ktorý riadi jednotlivé kontroly do fronty. Výsledky kontrol sú ukladané jednak do cache v ktorej je aktuálny obraz siete, tak pomocou IDOMOD do perzistného úložiska.

Core dokáže z tohto úložiska generovať reporty (SLA).

Plugin Architektúra – Architektúra pluginu je postavená na vykonávaní príkazov z príkazového riadku a preberanie výsledkov z štandarného výstupu. Vďaka tomuto prístupu je možné napísať plugin v akomkoľvek jazyku, ktorý je možne potom vykonať na príkazovom riadku.Notifikácie o problémoch fungujú úplne rovnako, takže napríklad odosielanie e-mailom je riešené skriptom, ktorý zavolá príkaz mail s potrebným parametrom.

IDOMOD – Je komponent, ktorý je zodpovedný za ukladanie výsledkov kontrol vykonávaných modulom ICINGA Core do perzistného uložiska. Podporuje celú radu úložisk

Od najjednoduchších textových súborov po relačné databázy. Do relačnej databázy zapisuje ICINGA pomocou modulu IDO2DB. Modul IDO2DB v súčasnej dobe podporuje databázu MySQL, PostgreSQL, Oracle.

ICINGA Web – Je webovým rozhraním pre zobrazenie stavu monitorovanej siete.Serverová strana Web je naprogramovaná v jazyku PHP a využíva framework Agavi. Klientská strana je takmer celá realizovaná javascriptovým frameworkem ExtJS.

Pre prenos živých dat medzi serverom a klientom sa používa štandard JSON.

NAGIOS Remote Procedure Execution (NRPE) – ICINGA spolupracuje s NRPE. Tento software nie je súčasťou distribúcie ICINGA a je potrebné ho prevziať z distribučného balíčka NAGIOS NRPE.

NRPE umožňuje vykonávať kontroly lokálne na vzdialených strojoch. Tento mechanizmus umožňuje kontrolovať veľmi zabezpečené stroje. Systému stači iba jeden otvorený TCP port.

Monitorovací server zašle žiadosť na kontrolu, v tejto žiadosti je poslaný iba názov kontroly. Obsah tejto kontroly je zakonfigurovaný lokálne na servery, takže nehrozí nebezpečenstvo kontrolovaneho stroja. Na strane monitorovacieho servera sa kontrola vykonáva pluginom check_nrpe s dvoma parametrami – IP adresa kontrolovaného stroja a názov kontroly na kontrolovanom stroji.

5 Inštalácia Step-by-step

1. Ako prvým krokom začneme stiahnutím „ICINGA“ a to pomocou príkazu wget.

```
[root@localhost ~]# wget http://packages.icinga.org/epel/ICINGA-release.repo -O /etc/yum.repos.
d/ICINGA-release.repo
```

2.

```
[root@localhost ~]# yum makecache
```

3. Je potrebné nainštalovať nasledujúce balíčky

```
[root@localhost ~]# yum install icinga icinga-gui icinga-doc icinga-idoutils-libdbi-mysql
```

4.Tiež je veľmi doležité nainštalovať NAGIOS plugins

```
[root@localhost ~]# yum install nagios-plugins*
```

5. Ak používate cent OS 6.* tak použit prikaz „**a**“ ak používate cent OS 7.* tak použiť príkaz „**b**“.

a:

```
[root@localhost ~]# yum install mysql-server mysql-client libdbi libdbi-devel libdbi-drivers li
bdbi-dbd-mysql
```

b:

```
[root@localhost ~]# yum install mariadb-server mariadb libdbi libdbi-devel libdbi-drivers
```

6. Je potrebné aby služba fungovala na cent OS 6.* to je služba MySQL a na cent OS 7.* to je mariaDB.Príkaz „**a**“ je pre MySQL a príkaz „**b**“ je pre mariaDB.

a:

```
[root@localhost ~]# service mysqld start
```

b:

```
[root@localhost ~]# systemctl start mariadb
```

7. Prihlásime sa do našej databázy a je jedno či používame cent OS 6.* alebo cent OS 7.* použijeme rovnaký príkaz.

```
[root@localhost ~]# mysql
```

8. Ako prvé si vytvoríme databázu pod menom „icinga“ a pridelíme práva uživatelovi icinga na nasledujúce príkazy.

```
MariaDB [(none)]> CREATE DATABASE icinga;
Query OK, 1 row affected (0.00 sec)
```

```
MariaDB [(none)]> GRANT USAGE ON icinga.* TO 'icinga'@'localhost'
    -> IDENTIFIED BY 'icinga' WITH MAX_QUERIES_PER_HOUR 0
    -> MAX_CONNECTIONS_PER_HOUR 0 MAX_UPDATES_PER_HOUR 0;
```

```
MariaDB [(none)]> GRANT SELECT, INSERT, UPDATE, DROP,
    -> CREATE VIEW, INDEX, EXECUTE ON icinga.* TO 'icinga'@'localhost';
```

```
MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)
```

```
MariaDB [(none)]> quit
Bye
```

9. Bude potrebné vypnúť SELINUX. Položku zmeníme na „disabled“ a reštartujeme stroj.

```
[root@localhost ~]# vim /etc/selinux/config
```

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of three two values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected pr
d.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

```
[root@localhost ~]# reboot
```

10. Po reštarte zapneme databázu pre cent OS 6.* použijeme príkaz „**a**“ pre cent OS 7.* použijeme príkaz „**b**“

a:

```
[root@localhost ~]# service mysqld start
```

b:

```
[root@localhost ~]# systemctl start mariadb
```

11. Teraz importneme nainštalovanú schému podľa toho akú verziu máme viď cestu /usr/share/doc/icinga-idoutils-libdbi-*-$version/db/mysql

```
[root@localhost ~]# cd /usr/share/doc/icinga-idoutils-libdbi-mysql-1.13.3/db/mys
ql/
[root@localhost mysql]# ls
mysql.sql  upgrade
[root@localhost mysql]# mysql icinga < mysql.sql
```

12. Koreň „ICINGA“ sa začína :

```
[root@localhost mysql]# cd /etc/icinga/
conf.d/   modules/  objects/
```

13. Skontrolujte či tento idoutils.cfg súbor vyzerá presne ako môj ak áno potom môžme prejsť na nasledujúci krok.

```
[root@localhost mysql]# vim /etc/icinga/modules/idoutils.cfg
```

```
define module{
        module_name     idomod
        module_type     neb
        path            /usr/lib64/icinga/idomod.so
        args            config_file=/etc/icinga/idomod.cfg
        }
```

14. Skontrolujte údaje ktoré su uvedené nižšie či sedia.

```
[root@localhost mysql]# vim /etc/icinga/ido2db.cfg
```

```
db_servertype=mysql
#db_servertype=pgsql
db_host=localhost
db_port=3306
#db_port=5432
db_name=icinga
db_prefix=icinga_
db_user=icinga
db_pass=icinga
```

15. Spustíme httpd službu ak ste inštalovali cent OS minimal tak ju bude potrebné najprv nainštalovať. Pre cent OS 6.* použijeme príkaz „**a**“ a pre cent OS 7.* použijeme príkaz „**b**“ a zároveň vypneme firewall.

a:

```
[root@localhost ~]# service httpd start
```

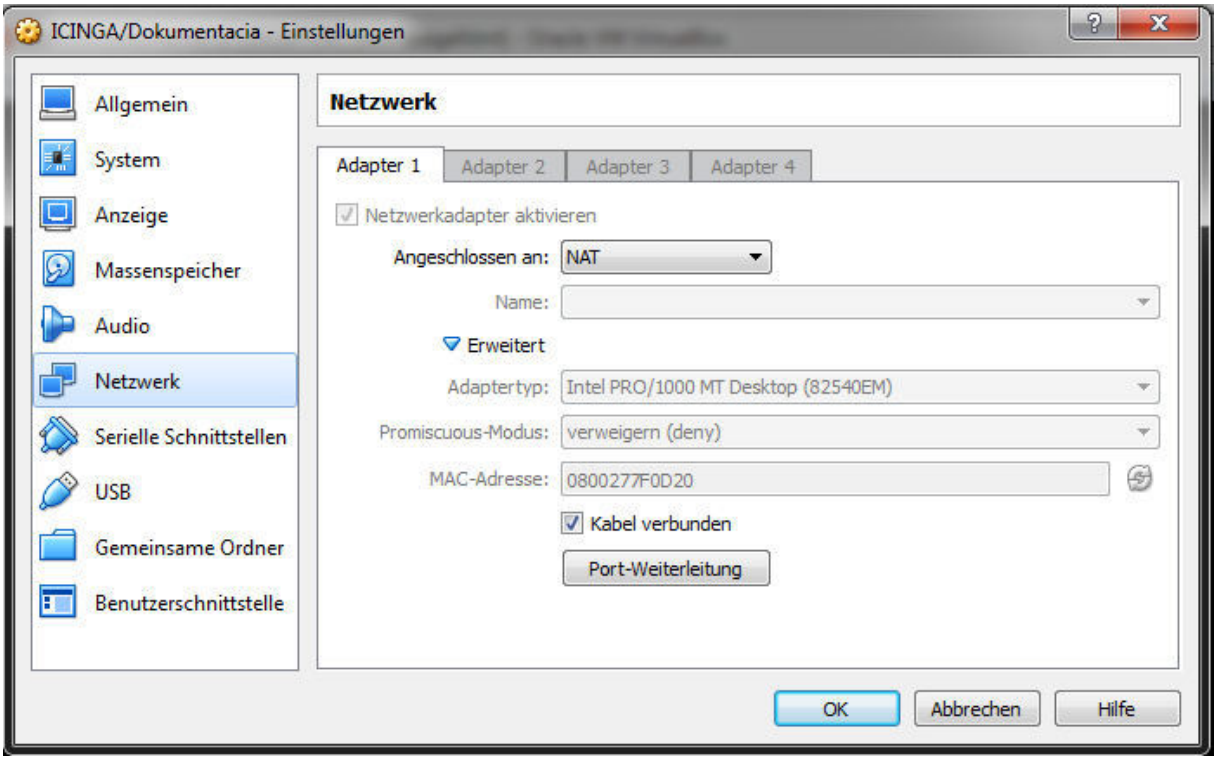
```
[root@localhost mysql]# service iptables stop
```

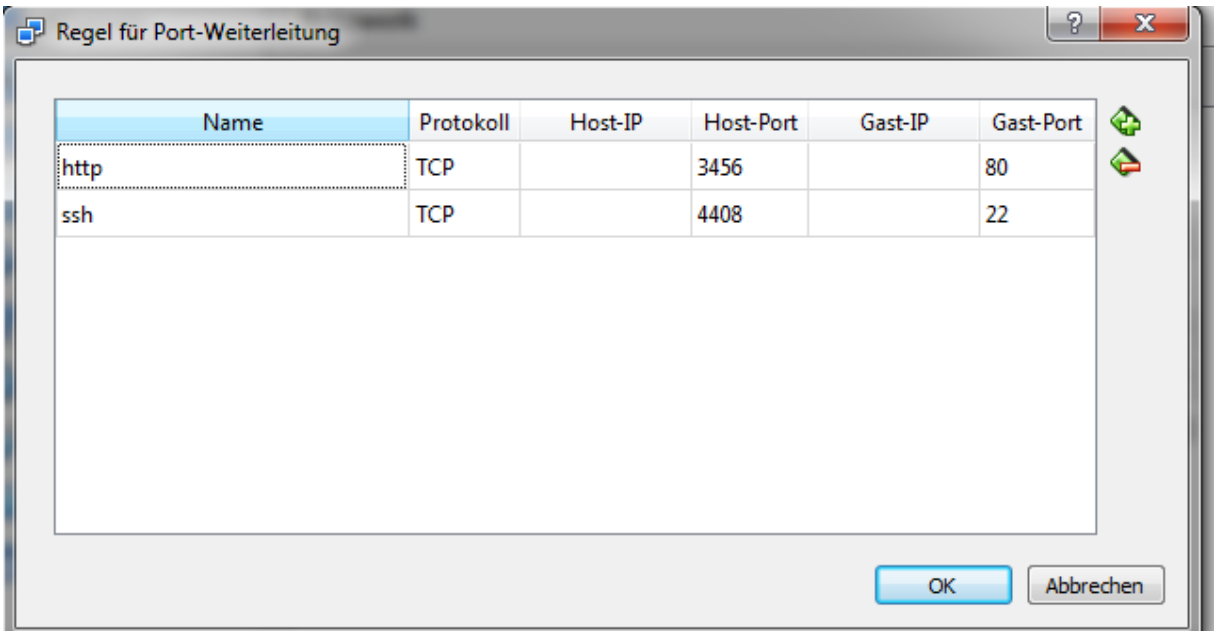
b:

```
[root@localhost mysql]# systemctl start httpd
```

```
[root@localhost mysql]# systemctl stop firewalld
```

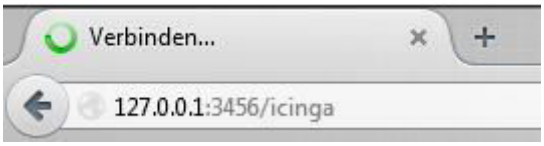
16. Vo VirtualBoxe si nastavíme port forwarding. „**Port-Weiterleitung**“. Port číslo 80 som si presmeroval na 3456.

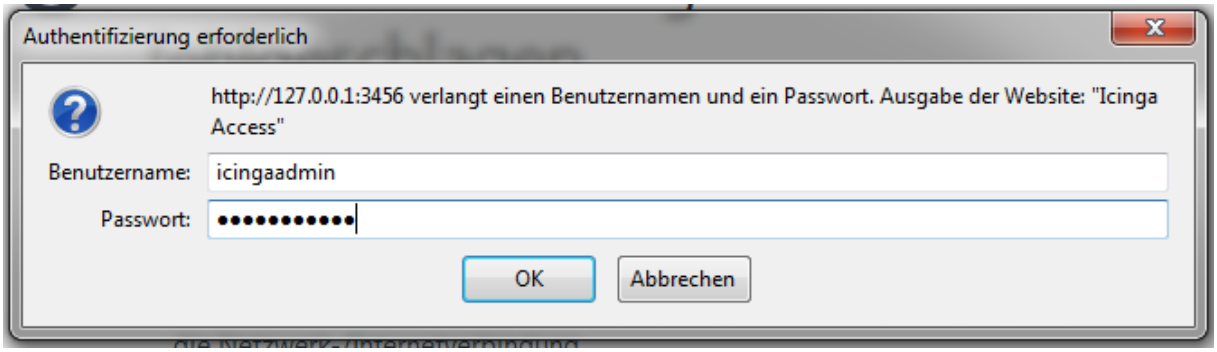




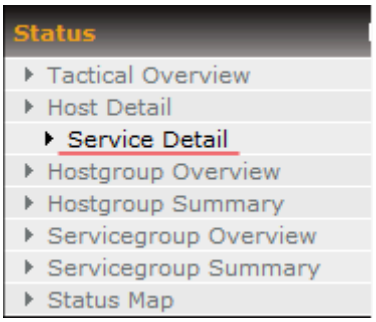
17. Otvoríme si prehliadač a pripojíme sa na localhost „**127.0.0.1:3456/icinga**“

Použijeme defaultny login name: „**icingaadmin**“ a heslo: „**icingaadmin**“





18. Na ľavej strane klikneme na tlačidlo „Service Detail“ a vidíme prehľad služieb, ktoré sú monitorované.



Set Filters

Service Status Details For All Hosts

Page 1 of 1 Results: 50

Host	Service	Status	Last Check	Duration	Attempt	Status Information
localhost	Current Load	OK	09-03-2015 18:36:18	0d 10h 3m 4s	1/4	OK - load average: 0.00, 0.01, 0.05
	Current Users	OK	09-03-2015 18:36:51	0d 10h 2m 31s	1/4	USERS OK - 2 users currently logged in
	HTTP	WARNING	09-03-2015 18:35:25	0d 8h 38m 57s	4/4	HTTP WARNING: HTTP/1.1 403 Forbidden - 5204 bytes in 0.001 second response time
	Icinga Startup Delay	OK	09-03-2015 18:37:58	0d 10h 1m 24s	1/4	OK: Icinga started with 0 seconds delay
	PING	OK	09-03-2015 18:38:31	0d 10h 0m 51s	1/4	PING OK - Packet loss = 0%, RTA = 0.13 ms
	Root Partition	OK	09-03-2015 18:39:05	0d 10h 0m 17s	1/4	DISK OK - free space: / 6880 MB (79% inode=99%):
	SSH	OK	09-03-2015 18:34:38	0d 9h 59m 44s	1/4	SSH OK - OpenSSH_6.6.1 (protocol 2.0)
	Swap Usage	OK	09-03-2015 18:35:11	0d 9h 59m 11s	1/4	SWAP OK - 100% free (1027 MB out of 1027 MB)
	Total Processes	OK	09-03-2015 18:35:45	0d 9h 58m 37s	1/4	PROCS OK: 101 processes with STATE = RSZDT

Page 1 of 1 Results: 50

Displaying Result 1 - 9 of 9 Matching Services

19. Na tomto obrazku vidite cestu kde sa nachádzajú nagios pluginy, alebo možme ich nazvať aj scripty.

```
[root@localhost plugins]# ls /usr/lib64/nagios/plugins/
check_apt        check_icmp            check_nrpe         check_snmp
check_bacula     check_ide_smart       check_nt           check_spop
check_breeze     check_ifoperstatus    check_ntp          check_ssh
check_by_ssh     check_ifstatus        check_ntp_peer     check_ssmtp
check_clamd      check_imap            check_ntp.pl       check_swap
check_cluster    check_ircd            check_ntp_time     check_tcp
check_dbi        check_jabber          check_nwstat       check_time
check_dhcp       check_ldap            check_openmanage   check_udp
check_dig        check_ldaps           check_oracle       check_updates
check_disk       check_linux_bonding   check_overcr       check_ups
check_disk_smb   check_load            check_pgsql        check_uptime
check_dns        check_log             check_ping         check_users
check_dummy      check_mailq           check_pop          check_wave
check_file_age   check_mrtg            check_procs        downtimes
check_flexlm     check_mrtgtraf        check_radius       negate
check_fping      check_mysql           check_real         urlize
check_ftp        check_mysql_query     check_rpc          utils.pm
check_game       check_nagios          check_sensors      utils.sh
check_hpjd       check_nntp            check_simap
check_http       check_nntps           check_smtp
```

20. Ak pridáme nový script je potrebné ho zadefinovať v commands.cfg. Je potrebné mať zadefinované command_name a command_line ako v príkladoch (w – warning , c- critical) :

```
# 'check_ping' command definition
define command{
        command_name    check_ping
        command_line    $USER1$/check_ping -H $HOSTADDRESS$ -w $ARG1$ -c $ARG2$
-p 5
        }
```

```
# 'check_ssh' command definition
define command{
        command_name    check_ssh
        command_line    $USER1$/check_ssh $ARG1$ $HOSTADDRESS$
        }
```

21. V tomto bode si ukážeme ako zmeniť monitorovacie parametre ktoré nám momentálne warning ukáže, ak bude prihlásených viac ako 20 užívateľov a keď ich bude 50 tak už bude critical. Tieto parametre zmeníme z 20 na 10 a z 50 na 40 a taktiež zmeníme popis služby.

```
[root@localhost plugins]# vim /etc/icinga/objects/localhost.cfg
```

Pred úpravou:

```
define service{
        use                             local-service         ; Name of service template to use
        host_name                       localhost
        service_description             Current Users
        check_command                   check_local_users!20!50
        }
```

Po úprave:

```
define service{
        use                             local-service         ; Name of service template to use
        host_name                       localhost
        service_description             Prihlaseny uzivatelia
        check_command                   check_local_users!10!40
        }
```

```
[root@localhost plugins]# service icinga restart
```

22. Ak si otvoríme prehliadač a klikneme na Service Detail tak vidíme, že zmena sa prejavila.

Host	Service	Status	Last Check
localhost	Current Load	OK	09-03-2015 19:26:18
	HTTP	WARNING	09-03-2015 19:25:59
	Icinga Startup Delay	OK	09-03-2015 19:22:58
	PING	OK	09-03-2015 19:23:31
	Prihlaseny uzivatelia	OK	09-03-2015 19:26:32
	Root Partition	OK	09-03-2015 19:24:05
	SSH	OK	09-03-2015 19:24:38
	Swap Usage	OK	09-03-2015 19:25:11
	Total Processes	OK	09-03-2015 19:25:45

6 Zdroje

Wikipedia : https://cs.wikipedia.org/wiki/Icinga
Icinga : https://www.icinga.org/