Od Nagiosu k Icinze na vlastní kůži

Michal Švamberg
svamberg@civ.zcu.cz

Výchozí stav

Softwarové vybavení:

- Nagios 3.5.1 (pozadu, k dispozici již 4.3.x),
- NConf 1.3.1 (aktivně již není vyvíjen),
- NRPE 2.15 (pozadu, k dispozici již 3.2.x),
- NSCA 2.9.2,
- nagiosgraph 1.5.2,
- NagVis 2.38.0,
- aNag (přístup pro mobilní klienty).

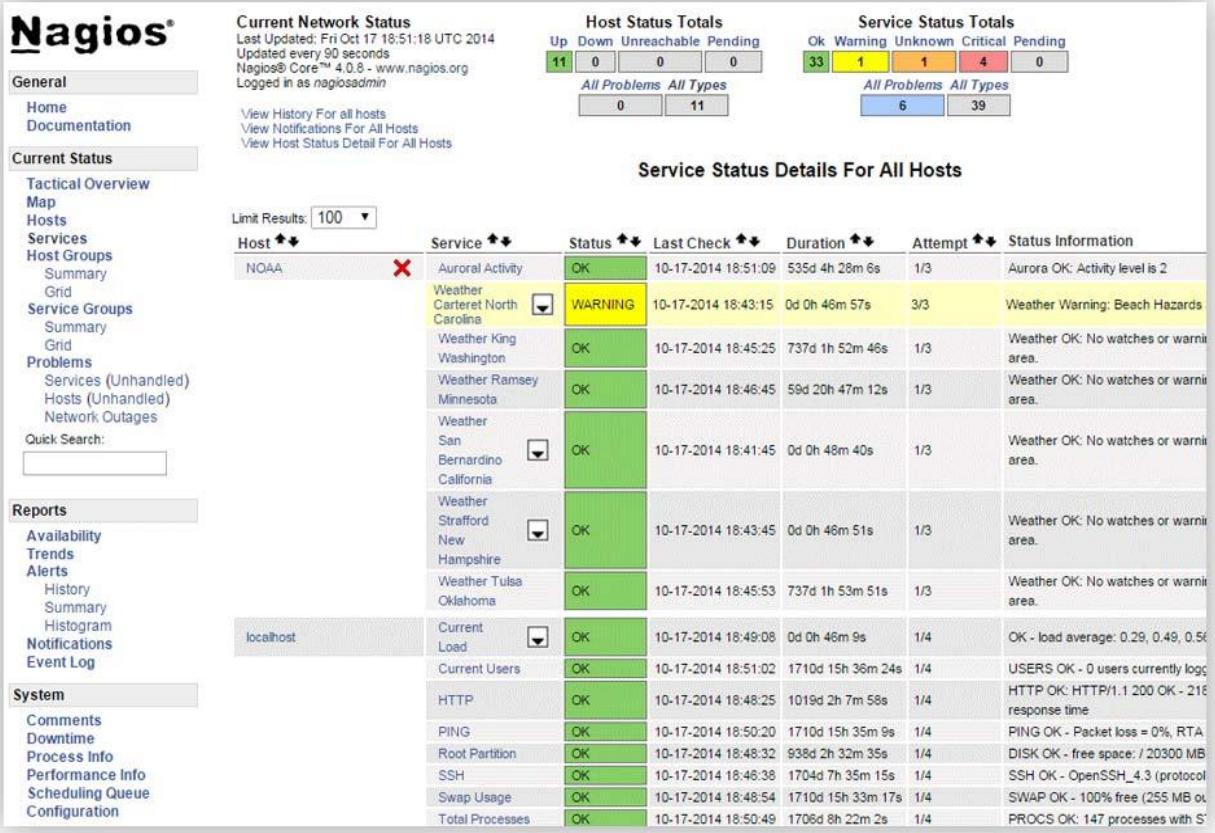
Nevýhody původního řešení

- Problematický upgrade operačního systému, navázáno mnoho rozdílného SW
- Nikdo neví, co se stane, pokud se aktualizuje nějaká komponenta
- Pomalé odezvy na uživatelské operace (recheck, grafy, deploy, ...)
- Nejednotnost uživatelského rozhraní (nconf, nagios, nagiosgraph, nagviz)
- Chybějící API pro konfiguraci
- Žádná automatizace zpracování vstupních dat
- Problémová autentizace/autorizace uživatelů (aNag přes sdílené jméno/heslo)
- Performance data uložená v RRD
- Distribuce konfigurace monitoringu jinými nástroji (ssh) + restart při změně
- Potíže s monitorováním za NATem nebo v chráněných sítích
- Logické vazby mezi službami se zpožděním (musí projít check command)

Nagios

Dobrý systém, ale

- pomalý vývoj,
- nemoderní prostředí,
- chybějící zastřešení ostatních komponent,
- konfigurační jazyk neumí dynamické zpracování (cykly, podmínky, ...), pouze proměnné, částečně řešil NConf formou šablon.



NRPE

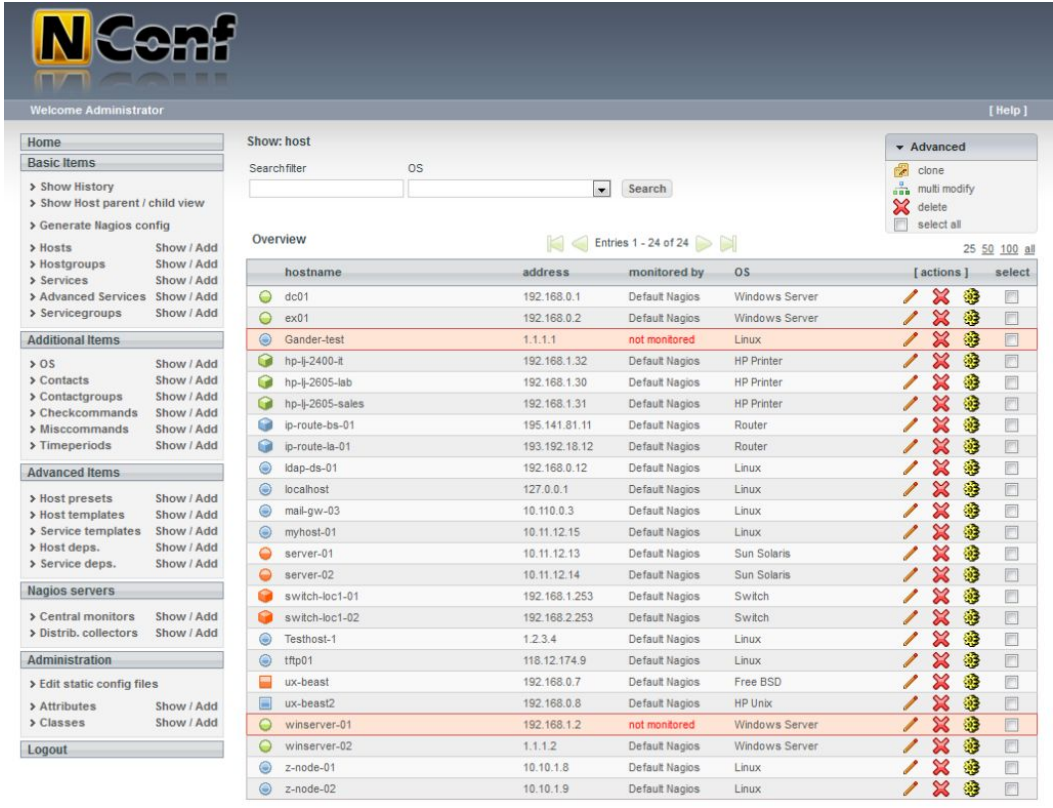
Funguje dobře, ale není to ono.

- Debian zakázal předávání proměnných z bezpečnostních důvodů, nutná vlastní kompilace a udržování v repozitáři.
- Nové NRPE vyžaduje SSL/TLS komunikaci, problémy s jejím nasazením, zůstáváme na staré verzi.
- Potíže s použitím za NATem (nagios server je NRPE klient), lze obejít samostatným obláčkem, pak ale potíže s distribucí konfigurace a komunikací mezi nagios servery.

NConf

Webová konfigurace přinesla velký nárůst služeb, zjednodušila přidávání a usnadnila správcům úpravy. NConf měl ale některé své neduhy:

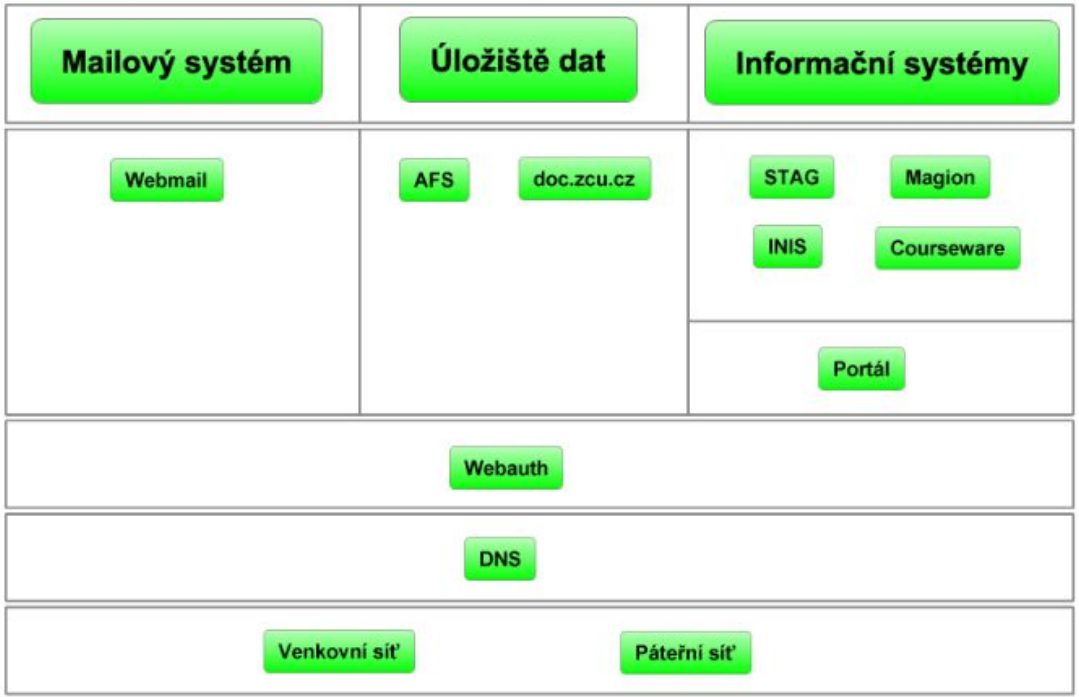
- šablony se používaly jen jednorázově, úprava šablony nemá vliv na již vytvořené hosty/služby,
- dlouhé generování konfigurace + deploy cronem + restart nagiosu,
- dobrý nástroj, ale bez dalšího vývoje,
- neřeší autorizaci, všichni mohou vše,
- horší hledání případných chyb při generování.



NagVis

Asi nejtajemnější část monitoringu, přitom se jí prezentujeme ven.

- Nasazeno v rámci jednoho projektu.
- Dokumentace nenalezena.
- Nikdo tomu nerozumí.
- Nikdo neví jak se tam dostat natož něco upravit.
- Neudržovaná konfigurace.
- Používá se check_multi => další zpoždění než se změna projeví.



Nagiosgraph & RRD

Nevýhody převážně vycházejí z formátu RRD a defaultního nastavení uložení performance dat:

- vykreslování grafů je pomalé
- při změně parametrů RRD je lepší stará data smazat
- nelze jednoduše využít data pro jiné nástroje (vhodné jen k vykreslení grafů)
- data nelze snadno zpracovávat a využít k další analýze (vytvářet dotazy)
- nagiosgraph se prakticky již nevyvíjí
- historie dat jen 1 rok
- velká agregace starších dat

Co požadujeme

- Integrovaný nástroj pro konfiguraci monitoringu skrze webové rozhraní
- Distribuce konfigurace monitoringu součástí komunikačního protokolu
- Integrace náhrady za NRPE/NCSA
- Lepší grafy a práce s performance daty
- Využít současné vlastní pluginy
- Autentizace a autorizace včetně mobilní aplikace
- Vizualizace dat
- API (nejlépe REST s JSON formátem) pro čtení i zápis konfigurace/stavu

Co roste na internetu?

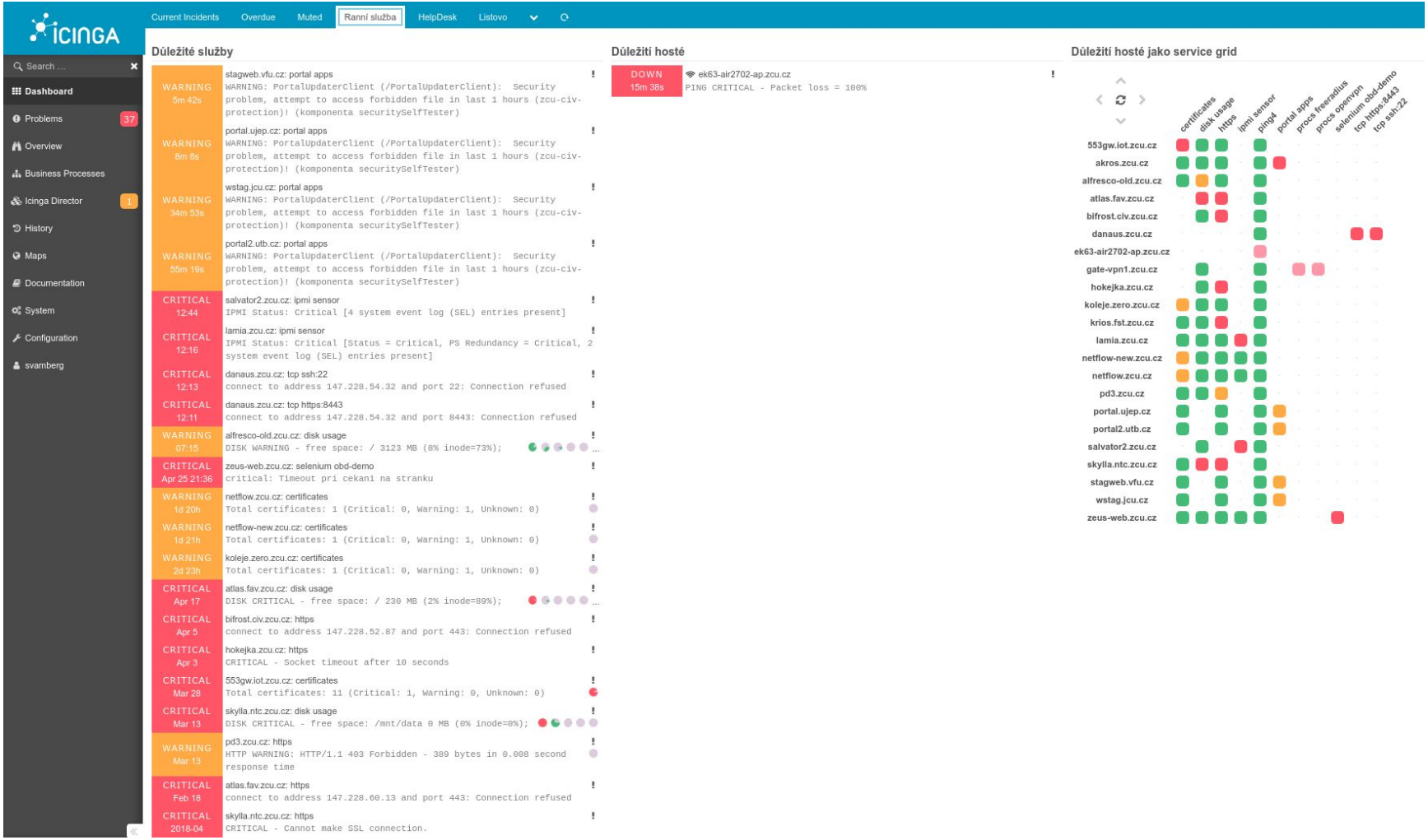
Je toho spoustu, mezi největší kandidáty patřili

- Zabbix,
- Icinga2 a
- Centreon.

Vybrali jsme Icinga2 s modulem Director. Líbil se nám zkrátka nejvíce a byl ze všech nejvíce rozjetý. Problémy při implementaci jsme čekali u každého řešení a i s Icingou se jich pár našlo. Pro grafy jsme vybrali nástroj Grafana s InfluxDB.

Nagios -> Icinga 2 + Icinga Web 2

- stará statická konfigurace zahozena, pouze zdroj nastavení sond
- vše nutno vymyslet znova (napřed se naučit možnosti)
- moderní webové prostředí
- modulární řešení
- zachována kompatibilita s Nagios pluginy včetně performance dat
- autentizace (používáme SSO s REMOTE_USER)
- autorizace na základě loginu a LDAP skupin

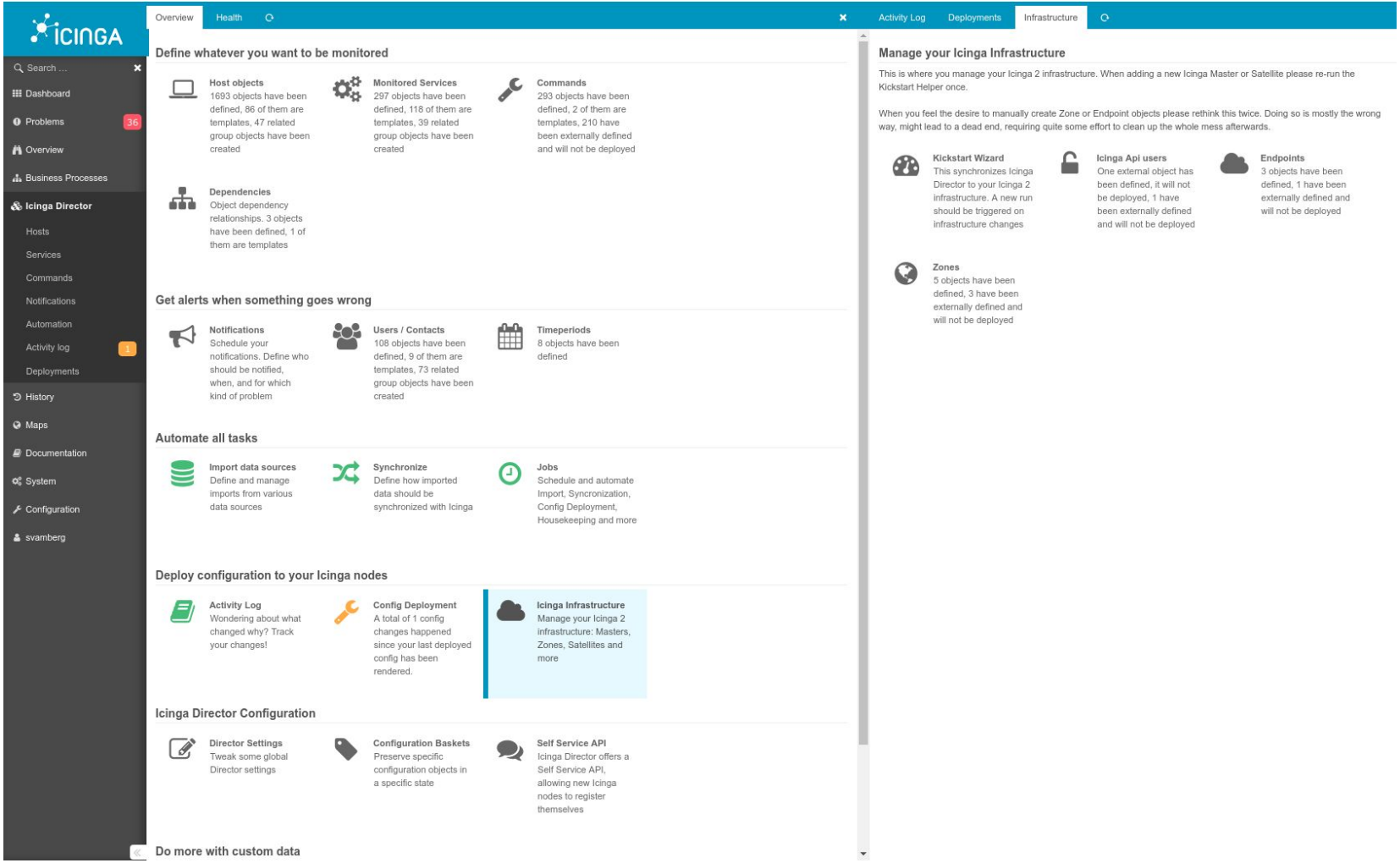

Current Incidents
Overdue
Muted
Ranní služba
HelpDesk
Listovo
Search ...
Dashboard
Problems 37
Overview
Business Processes
Icinga Director 1
History
Maps
Documentation
System
Configuration
svamberg
Důležité služby
WARNING 5m 42s
stagweb.vfu.cz: portal apps
WARNING: PortalUpdaterClient (/PortalUpdaterClient): Security problem, attempt to access forbidden file in last 1 hours (zcu-civ-protection)! (komponenta securitySelfTester)
WARNING 8m 8s
portal.ujep.cz: portal apps
WARNING: PortalUpdaterClient (/PortalUpdaterClient): Security problem, attempt to access forbidden file in last 1 hours (zcu-civ-protection)! (komponenta securitySelfTester)
WARNING 34m 53s
wstag.jcu.cz: portal apps
WARNING: PortalUpdaterClient (/PortalUpdaterClient): Security problem, attempt to access forbidden file in last 1 hours (zcu-civ-protection)! (komponenta securitySelfTester)
WARNING 55m 19s
portal2.utb.cz: portal apps
WARNING: PortalUpdaterClient (/PortalUpdaterClient): Security problem, attempt to access forbidden file in last 1 hours (zcu-civ-protection)! (komponenta securitySelfTester)
CRITICAL 12:44
salvator2.zcu.cz: ipmi sensor
IPMI Status: Critical [4 system event log (SEL) entries present]
CRITICAL 12:16
lamia.zcu.cz: ipmi sensor
IPMI Status: Critical [Status = Critical, PS Redundancy = Critical, 2 system event log (SEL) entries present]
CRITICAL 12:13
danaus.zcu.cz: tcp ssh:22
connect to address 147.228.54.32 and port 22: Connection refused
CRITICAL 12:11
danaus.zcu.cz: tcp https:8443
connect to address 147.228.54.32 and port 8443: Connection refused
WARNING 07:15
alfresco-old.zcu.cz: disk usage
DISK WARNING - free space: / 3123 MB (8% inode=73%);
CRITICAL Apr 25 21:36
zeus-web.zcu.cz: selenium obd-demo
critical: Timeout pri cekani na stranku
WARNING 1d 20h
netflow.zcu.cz: certificates
Total certificates: 1 (Critical: 0, Warning: 1, Unknown: 0)
WARNING 1d 21h
netflow-new.zcu.cz: certificates
Total certificates: 1 (Critical: 0, Warning: 1, Unknown: 0)
WARNING 2d 23h
koleje.zero.zcu.cz: certificates
Total certificates: 1 (Critical: 0, Warning: 1, Unknown: 0)
CRITICAL Apr 17
atlas.fav.zcu.cz: disk usage
DISK CRITICAL - free space: / 230 MB (2% inode=89%);
CRITICAL Apr 5
bifrost.civ.zcu.cz: https
connect to address 147.228.52.87 and port 443: Connection refused
CRITICAL Apr 3
hokejka.zcu.cz: https
CRITICAL - Socket timeout after 10 seconds
CRITICAL Mar 28
553gw.iot.zcu.cz: certificates
Total certificates: 11 (Critical: 1, Warning: 0, Unknown: 0)
CRITICAL Mar 13
skylla.ntc.zcu.cz: disk usage
DISK CRITICAL - free space: /mnt/data 0 MB (0% inode=0%);
WARNING Mar 13
pd3.zcu.cz: https
HTTP WARNING: HTTP/1.1 403 Forbidden - 389 bytes in 0.008 second response time
CRITICAL Feb 18
atlas.fav.zcu.cz: https
connect to address 147.228.60.13 and port 443: Connection refused
CRITICAL 2018-04
skylla.ntc.zcu.cz: https
CRITICAL - Cannot make SSL connection.
Důležití hosté
DOWN 15m 38s
ek63-air2702-ap.zcu.cz
PING CRITICAL - Packet loss = 100%
Důležití hosté jako service grid
certificates
disk usage
https
ipmi sensor
ping4
portal apps
procs freeradius
procs openvpn
selenium obd-demo
tcp https:8443
tcp ssh:22
553gw.iot.zcu.cz
akros.zcu.cz
alfresco-old.zcu.cz
atlas.fav.zcu.cz
bifrost.civ.zcu.cz
danaus.zcu.cz
ek63-air2702-ap.zcu.cz
gate-vpn1.zcu.cz
hokejka.zcu.cz
koleje.zero.zcu.cz
krios.fst.zcu.cz
lamia.zcu.cz
netflow-new.zcu.cz
netflow.zcu.cz
pd3.zcu.cz
portal.ujep.cz
portal2.utb.cz
salvator2.zcu.cz
skylla.ntc.zcu.cz
stagweb.vfu.cz
wstag.jcu.cz
zeus-web.zcu.cz

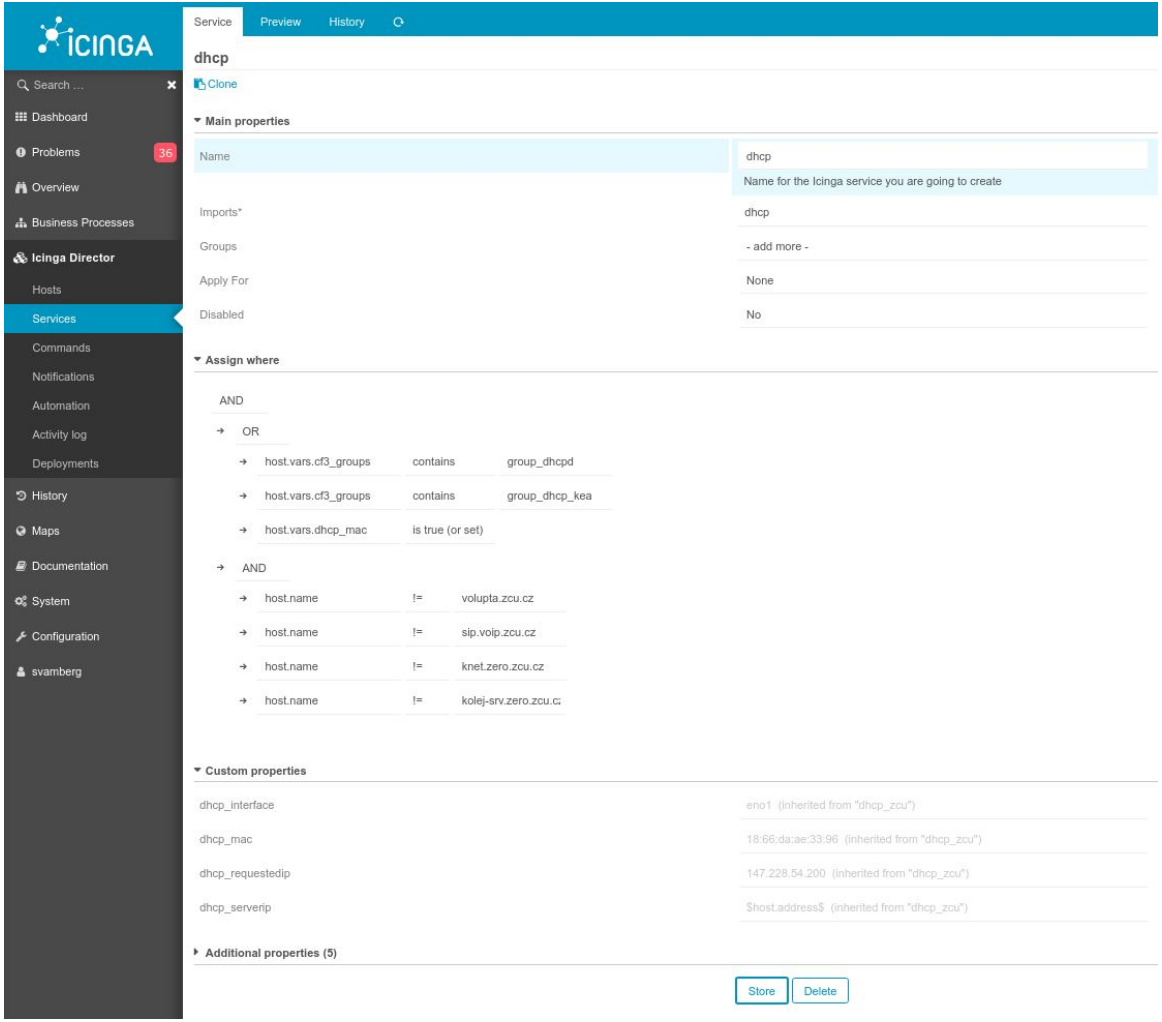
NRPE, NCSA -> Icinga 2

- komunikace součástí protokolu Icingy (konfigurace, parametry, spouštění)
- stačí jeden port (zjednodušení firewallů)
- spojení server-agent lze navázat z obou stran, záleží na konfiguraci

Nconf -> Icinga 2 / Director

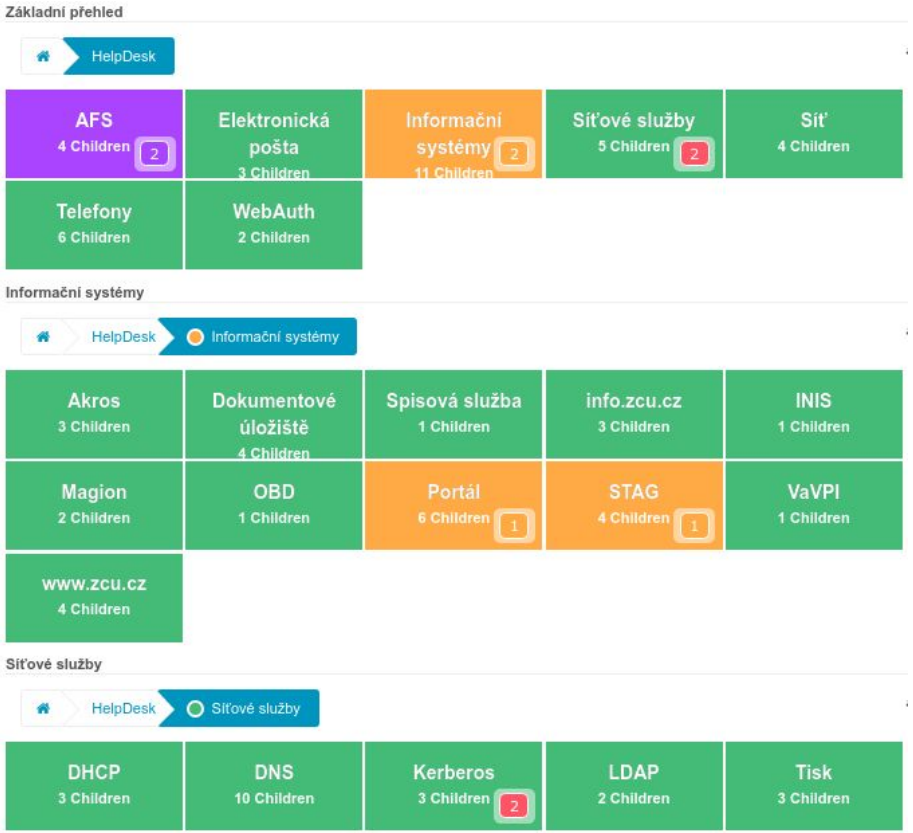
- nejtěžší je pochopit filozofii konfigurace (čti: zapomenout na Nagios)
- cokoliv jde automatizovat nebo využít API, pak to využij
- použij skupin, regulárních výrazů, hvězdičkové notace
- templaty se používají vždy
- parametry pro services mají nejvyšší prioritu, přebíjí hodnoty hosta
- historie změn
- možnost vrátit konfiguraci zpět (ne vždy funguje)
- snadné použití zónování
- ne vše je úplně průhledné, např. je třeba založit proměnnou než ji použiji


Overview
Health
Activity Log
Deployments
Infrastructure
Search ...
Dashboard
Problems
36
Overview
Business Processes
Icinga Director
Hosts
Services
Commands
Notifications
Automation
Activity log
1
Deployments
History
Maps
Documentation
System
Configuration
svamberg
Define whatever you want to be monitored
Host objects
1693 objects have been defined, 86 of them are templates, 47 related group objects have been created
Monitored Services
297 objects have been defined, 118 of them are templates, 39 related group objects have been created
Commands
293 objects have been defined, 2 of them are templates, 210 have been externally defined and will not be deployed
Dependencies
Object dependency relationships. 3 objects have been defined, 1 of them are templates
Get alerts when something goes wrong
Notifications
Schedule your notifications. Define who should be notified, when, and for which kind of problem
Users / Contacts
108 objects have been defined, 9 of them are templates, 73 related group objects have been created
Timeperiods
8 objects have been defined
Automate all tasks
Import data sources
Define and manage imports from various data sources
Synchronize
Define how imported data should be synchronized with Icinga
Jobs
Schedule and automate Import, Syncronization, Config Deployment, Housekeeping and more
Deploy configuration to your Icinga nodes
Activity Log
Wondering about what changed why? Track your changes!
Config Deployment
A total of 1 config changes happened since your last deployed config has been rendered.
Icinga Infrastructure
Manage your Icinga 2 infrastructure: Masters, Zones, Satellites and more
Icinga Director Configuration
Director Settings
Tweak some global Director settings
Configuration Baskets
Preserve specific configuration objects in a specific state
Self Service API
Icinga Director offers a Self Service API, allowing new Icinga nodes to register themselves
Do more with custom data
Manage your Icinga Infrastructure
This is where you manage your Icinga 2 infrastructure. When adding a new Icinga Master or Satellite please re-run the Kickstart Helper once.
When you feel the desire to manually create Zone or Endpoint objects please rethink this twice. Doing so is mostly the wrong way, might lead to a dead end, requiring quite some effort to clean up the whole mess afterwards.
Kickstart Wizard
This synchronizes Icinga Director to your Icinga 2 infrastructure. A new run should be triggered on infrastructure changes
Icinga Api users
One external object has been defined, it will not be deployed, 1 have been externally defined and will not be deployed
Endpoints
3 objects have been defined, 1 have been externally defined and will not be deployed
Zones
5 objects have been defined, 3 have been externally defined and will not be deployed


Service
Preview
History
dhcp
Clone
Main properties
Name
dhcp
Name for the Icinga service you are going to create
Imports*
dhcp
Groups
- add more -
Apply For
None
Disabled
No
Assign where
AND
OR
host.vars.cf3_groups contains group_dhcpd
host.vars.cf3_groups contains group_dhcp_kea
host.vars.dhcp_mac is true (or set)
AND
host.name != volupta.zcu.cz
host.name != sip.voip.zcu.cz
host.name != knet.zero.zcu.cz
host.name != kolej-srv.zero.zcu.c
Custom properties
dhcp_interface
eno1 (inherited from "dhcp_zcu")
dhcp_mac
18:66:da:ae:33:96 (inherited from "dhcp_zcu")
dhcp_requestedip
147.228.54.200 (inherited from "dhcp_zcu")
dhcp_serverip
$host.address$ (inherited from "dhcp_zcu")
Additional properties (5)
Store
Delete
Search ...
Dashboard
Problems
36
Overview
Business Processes
Icinga Director
Hosts
Services
Commands
Notifications
Automation
Activity log
Deployments
History
Maps
Documentation
System
Configuration
svamberg

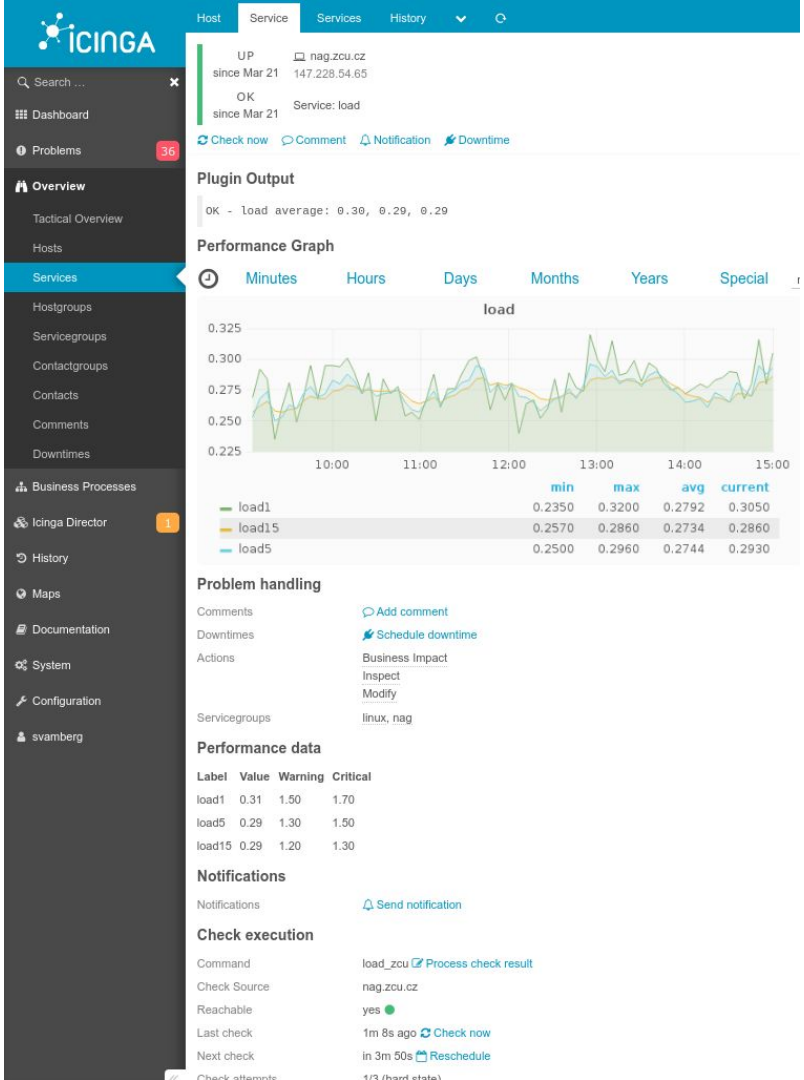
NagVis -> Icinga 2 / BusinessProcesses

- zdrojový soubor je textový, lze upravovat ručně
- neumí (zatím) fungovat dle skupin, každý host/služba se musí ručně přidat
- jednoduchý přehled pro uživatele, který lze strukturovat
- výstup na obrazovky (Chromecast vs. RPI)



Nagiosgraph -> Grafana

- rychle nasazené
- velká volnost při tvorbě přehledů
- integrace do webového rozhraní Icingy
- rychlé odezvy




icinga-host
Zoom Out
Last 6 months
Refresh every 1m
hostname
achlys.zcu.cz
DISK USAGE
MEMORY
Memory
37 GiB
28 GiB
19 GiB
9 GiB
0 B
11/1
11/16
12/1
12/16
1/1
1/16
2/1
2/15
3/1
3/16
4/1
4/16
min
max
Used 1.7 GiB 4.3 GiB
Total 31.3 GiB 31.3 GiB
Caches 3.8 GiB 27.7 GiB
Swap
1.2 GiB
954 MiB
715 MiB
477 MiB
238 MiB
0 B
Used 0 B 172 MiB
Max 975 MiB 975 MiB
SYSTEM
NTP
0 ns
-10 µs
-20 µs
-30 µs
-40 µs
-50 µs
-60 µs
-70 µs
offset -67 µs -4 µs
Load per CPU
2.0
1.5
1.0
0.5
0
load1 0.02 0.51
load15 0.02 0.51
load5 0.02 0.51
Temperatures
80 °C
70 °C
60 °C
50 °C
40 °C
30 °C
20 °C
10 °C
Disk Temperatures
39 °C
38 °C
37 °C
36 °C
35 °C
34 °C

RRD -> InfluxDB

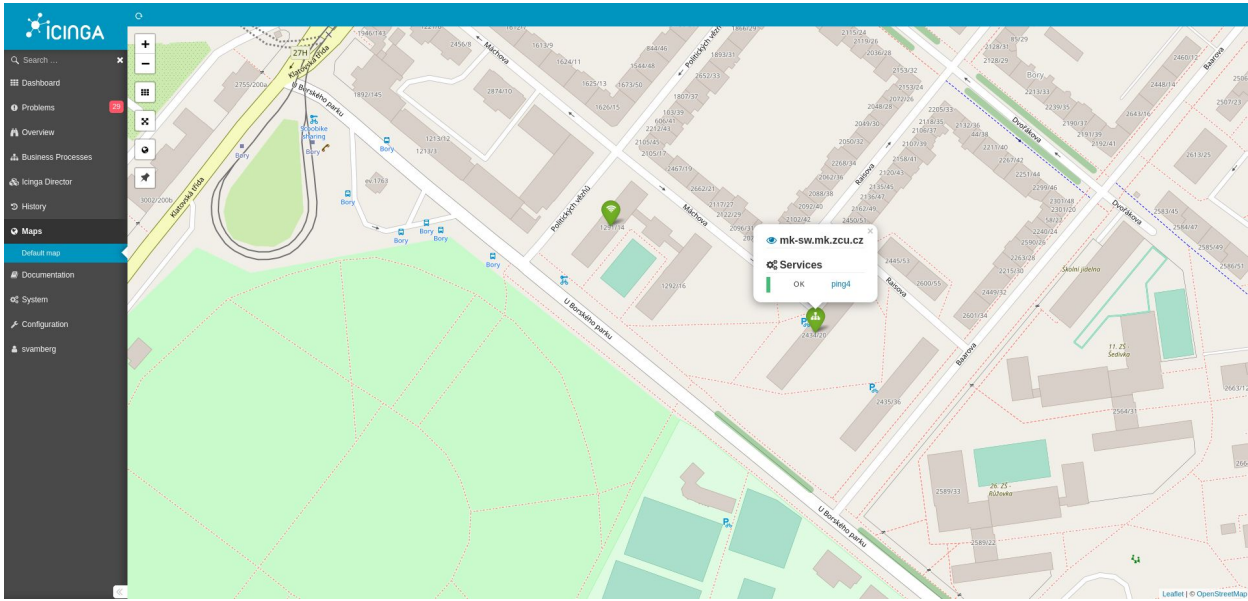
- používá Influx Query Language (InfluxQL)
- jedná se o databázi pro ukládání časových dat


icinga-host
Back to dashboard
Zoom Out
Last 6 months
Refresh every 1m
hostname
achlys.zcu.cz
MEMORY
Memory
33 GiB
28 GiB
23 GiB
19 GiB
14 GiB
9 GiB
5 GiB
0 B
11/1
11/8
11/16
11/23
12/1
12/8
12/16
12/24
1/1
1/8
1/16
1/24
2/1
2/8
2/15
2/22
3/1
3/8
3/16
3/24
4/1
4/8
4/16
4/23
min
max
Used
1.72 GiB
4.29 GiB
Total
31.33 GiB
31.33 GiB
Caches
3.80 GiB
27.73 GiB
Graph
General
Metrics
Axes
Legend
Display
Alert
Time range
Data Source
default
Options
Help
Query Inspector
FROM
default
mem_zcu
WHERE
hostname
=~
/^$hostname$/
AND
metric
=
USED
SELECT
field (value)
mean ()
GROUP BY
time ($__interval)
fill (none)
FORMAT AS
Time series
ALIAS BY
Used
B
SELECT mean("value") FROM "mem_zcu" WHERE ("hostname" =~ /^$hostname$/ AND "metric" = 'TOTAL') AND $timeFilter GROUP BY time($__interval) fill(none)
C
SELECT mean("value") FROM "mem_zcu" WHERE ("hostname" =~ /^$hostname$/ AND "metric" = 'CACHES') AND $timeFilter GROUP BY time($__interval) fill(none)
D
SELECT mean("value") FROM "mem_zcu" WHERE ("hostname" =~ /^$hostname$/ AND "metric" = 'FREE') AND $timeFilter GROUP BY time($__interval) fill(none)
E
Add Query

Icinga2 / Maps (mapDatatype)

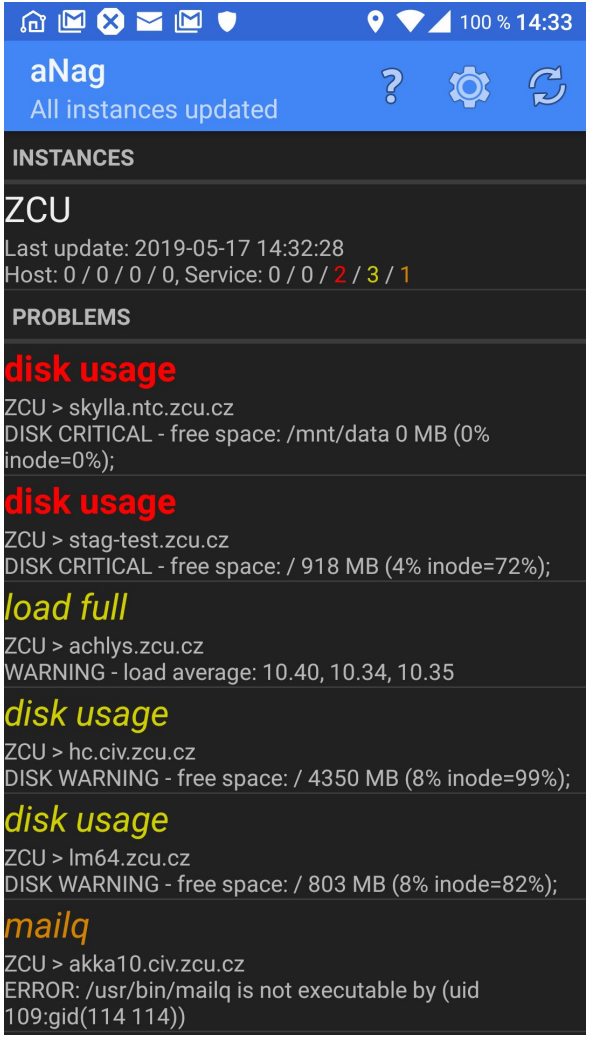
Modul pro zobrazování zařízení na mapě. Data pro lokaci máme nastaveno:

- přes API z evidence zařízení (rackmonkey) se předvyplní místnost,
- ručním zadáním místnosti (alias pro GPS souřadnici),
- ručním zadáním GPS souřadnice nebo
- kliknutím do mapy v modulu mapDatatype.

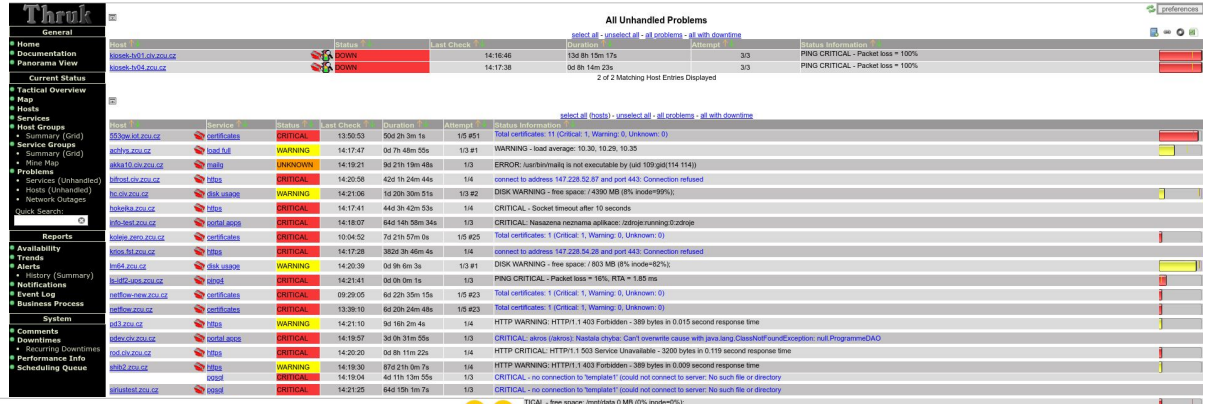


aNag

- Uživatelé ověřeni svým vlastním jménem a heslem vůči GSSAPI modulu.
- Apache má nastavenu proxy na jednoho uživatele vůči Icinze, s oprávněním pro čtení.
- V aplikaci si uživatelé sami nastavují vlastní filtry na základě skupin.



thruk.org



Alternativní uživatelské rozhraní pro monitorovací nástroje.

Automatizace

Konfigurační management

- CFE3 kontroluje nastavení stroje v Icinze, pokud se něco změní opraví to
- pokud stroj chybí založí jej, založený stroj ale neruší
- udržuje aktuální hodnotu proměnných (seznam certifikátů, disků, ...) stroje

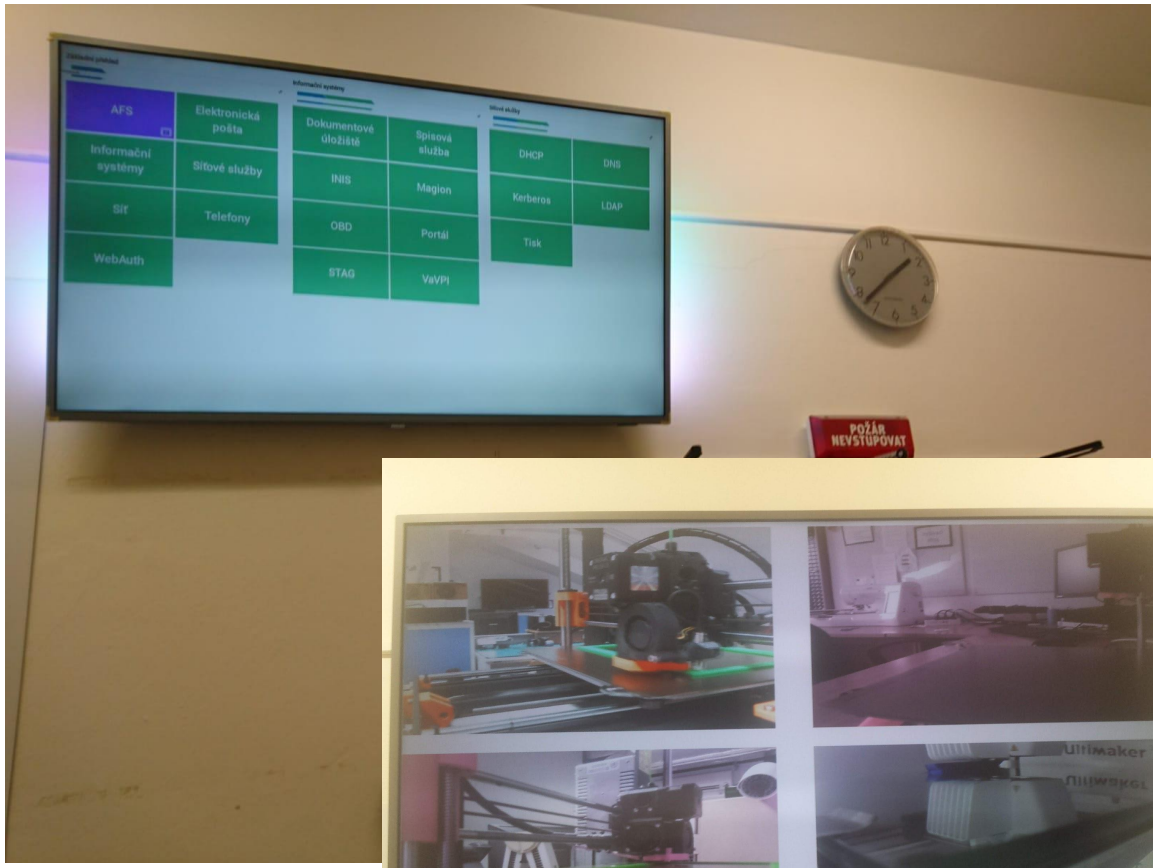
DNS

- síťové zařízení (switche, routery, AP, ...) dle DNS, export do CSV
- CSV načteno modulem Fileshipper (povoleno i rušení stroje)

Uživatelé zakládáni automaticky dle LDAP skupin (doplňuje se email, jméno)

Perličky

- utf8: trochu boj správně nastavit pro zobrazování češtiny v komentářích
- Chromecast je nepoužitelný pro servírování obsahu z webu, použito RPi
- Přesun monitoringu síťařů (Dude od MikroTiku) do Icingy
- Autentizace uživatelů přes SSO (WebAuth), povolení uživatelé generováni ze účtů v Icinze



Demo & tutoriál

https://icinga.com/demo

login / password: demo / demo

a nebo

Tutoriál ve středu dopoledne

(instalace, konfigurace, monitorování, diskuse)

Děkuji

Fond rozvoje CESNET, z.s.p.o.

Moderní monitoring IT infrastruktury

Projekt 626R1/2018