

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 uložena 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.

Nagios®

Current Network Status
Last Updated: Fri Oct 17 18:51:18 UTC 2014
Updated every 90 seconds
Nagios® Core™ 4.0.8 - www.nagios.org
Logged in as nagiosadmin

Host Status Totals

Up	Down	Unreachable	Pending
11	0	0	0

All Problems: 0 | All Types: 11

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
33	1	1	4	0

All Problems: 6 | All Types: 39

General
Home
Documentation

Current Status
Tactical Overview
Map
Hosts
Services
Host Groups
Service Groups
Problems
Quick Search:

Reports
Availability
Trends
Alerts
Notifications
Event Log

System
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Configuration

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
NOAA	Auroral Activity	OK	10-17-2014 18:51:09	535d 4h 28m 6s	1/3	Aurora OK: Activity level is 2
	Weather Carteret North Carolina	WARNING	10-17-2014 18:43:15	0d 0h 46m 57s	3/3	Weather Warning: Beach Hazards
	Weather King Washington	OK	10-17-2014 18:45:25	737d 1h 52m 46s	1/3	Weather OK: No watches or warn area.
	Weather Ramsey Minnesota	OK	10-17-2014 18:46:45	59d 20h 47m 12s	1/3	Weather OK: No watches or warn area.
	Weather San Bernardino California	OK	10-17-2014 18:41:45	0d 0h 48m 40s	1/3	Weather OK: No watches or warn area.
	Weather Strafford New Hampshire	OK	10-17-2014 18:43:45	0d 0h 46m 51s	1/3	Weather OK: No watches or warn area.
	Weather Tulsa Oklahoma	OK	10-17-2014 18:45:53	737d 1h 53m 51s	1/3	Weather OK: No watches or warn area.
localhost	Current Load	OK	10-17-2014 18:49:08	0d 0h 46m 9s	1/4	OK - load average: 0.29, 0.49, 0.56
	Current Users	OK	10-17-2014 18:51:02	1710d 15h 36m 24s	1/4	USERS OK - 0 users currently logged in
	HTTP	OK	10-17-2014 18:48:25	1019d 2h 7m 58s	1/4	HTTP OK: HTTP/1.1 200 OK - 216 response time
	PING	OK	10-17-2014 18:50:20	1710d 15h 35m 9s	1/4	PING OK - Packet loss = 0%, RTA = 0.00ms
	Root Partition	OK	10-17-2014 18:48:32	938d 2h 32m 35s	1/4	DISK OK - free space: / 20300 MB
	SSH	OK	10-17-2014 18:46:38	1704d 7h 35m 15s	1/4	SSH OK - OpenSSH_4.3 (protocol 2)
	Swap Usage	OK	10-17-2014 18:48:54	1710d 15h 33m 17s	1/4	SWAP OK - 100% free (255 MB of 256 MB used)
	Total Processes	OK	10-17-2014 18:50:49	1706d 8h 22m 2s	1/4	PROCS OK: 147 processes with 512K of memory

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 oblačkem, 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 nedostatky:

- 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.

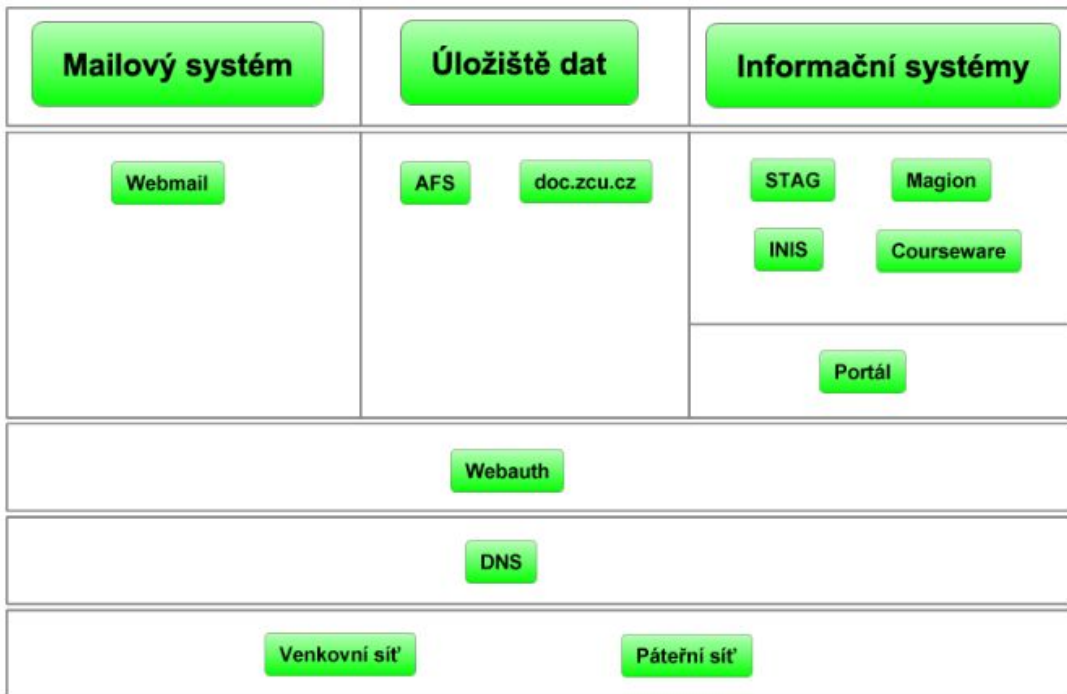
The screenshot displays the NConf web interface. At the top left is the NConf logo. Below it, a navigation menu is organized into sections: Home, Basic Items (with sub-items like Show History, Generate Nagios config, Hosts, Hostgroups, Services, Advanced Services, Servicegroups), Additional Items (with sub-items like OS, Contacts, Contactgroups, Checkcommands, Misccommands, Timeperiods), Advanced Items (with sub-items like Host presets, Host templates, Service templates, Host deps, Service deps), Nagios servers (with sub-items like Central monitors, Distrib. collectors), Administration (with sub-items like Edit static config files, Attributes, Classes), and Logout. The main content area is titled 'Welcome Administrator' and includes a search filter for 'OS'. Below this is an 'Overview' section showing a table of hosts. The table has columns for hostname, address, monitored by, OS, and actions. The 'Gander-test' and 'winserver-01' rows are highlighted in red, indicating they are 'not monitored'. The 'Advanced' menu on the right contains options like clone, multi modify, delete, and select all.

hostname	address	monitored by	OS	[actions]	select
dc01	192.168.0.1	Default Nagios	Windows Server	[edit] [delete] [select]	[checkbox]
ex01	192.168.0.2	Default Nagios	Windows Server	[edit] [delete] [select]	[checkbox]
Gander-test	1.1.1.1	not monitored	Linux	[edit] [delete] [select]	[checkbox]
hp-lj-2400-t	192.168.1.32	Default Nagios	HP Printer	[edit] [delete] [select]	[checkbox]
hp-lj-2605-lab	192.168.1.30	Default Nagios	HP Printer	[edit] [delete] [select]	[checkbox]
hp-lj-2605-sales	192.168.1.31	Default Nagios	HP Printer	[edit] [delete] [select]	[checkbox]
ip-route-bs-01	195.141.81.11	Default Nagios	Router	[edit] [delete] [select]	[checkbox]
ip-route-la-01	193.192.18.12	Default Nagios	Router	[edit] [delete] [select]	[checkbox]
ldap-ds-01	192.168.0.12	Default Nagios	Linux	[edit] [delete] [select]	[checkbox]
localhost	127.0.0.1	Default Nagios	Linux	[edit] [delete] [select]	[checkbox]
mail-gw-03	10.110.0.3	Default Nagios	Linux	[edit] [delete] [select]	[checkbox]
myhost-01	10.11.12.15	Default Nagios	Linux	[edit] [delete] [select]	[checkbox]
server-01	10.11.12.13	Default Nagios	Sun Solaris	[edit] [delete] [select]	[checkbox]
server-02	10.11.12.14	Default Nagios	Sun Solaris	[edit] [delete] [select]	[checkbox]
switch-loc1-01	192.168.1.253	Default Nagios	Switch	[edit] [delete] [select]	[checkbox]
switch-loc1-02	192.168.2.253	Default Nagios	Switch	[edit] [delete] [select]	[checkbox]
Testhost-1	1.2.3.4	Default Nagios	Linux	[edit] [delete] [select]	[checkbox]
ttf01	118.12.174.9	Default Nagios	Linux	[edit] [delete] [select]	[checkbox]
ux-beast	192.168.0.7	Default Nagios	Free BSD	[edit] [delete] [select]	[checkbox]
ux-beast2	192.168.0.8	Default Nagios	HP Unix	[edit] [delete] [select]	[checkbox]
winserver-01	192.168.1.2	not monitored	Windows Server	[edit] [delete] [select]	[checkbox]
winserver-02	1.1.1.2	Default Nagios	Windows Server	[edit] [delete] [select]	[checkbox]
z-node-01	10.10.1.8	Default Nagios	Linux	[edit] [delete] [select]	[checkbox]
z-node-02	10.10.1.9	Default Nagios	Linux	[edit] [delete] [select]	[checkbox]

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 spousta, 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 znovu (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

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	wstaj.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: top ssh22 connect to address 147.228.54.32 and port 22: Connection refused	!
CRITICAL 12:11	danaus.zcu.cz: top https8443 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	skylia.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	skylia.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	proc fsreadplus	selenium obd-demo	top https-a843	top ssh22
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	●	●	●	●						
skylia.ntc.zcu.cz	●	●	●	●						
stagweb.vfu.cz	●	●	●	●						
wstaj.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
- šablony 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

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, 116 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, Synchronization, 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

dhcp

[Clone](#)

Main properties

Name	dhcp <small>Name for the Icinga service you are going to create</small>
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.cz

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/slужba se musí ručně přidat
- jednoduchý přehled pro uživatele, který lze strukturovat
- výstup na obrazovky (Chromecast vs. RPI)

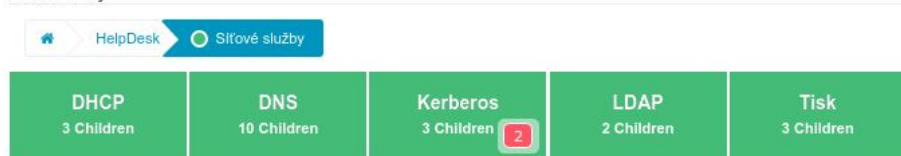
Základní přehled



Informační systémy

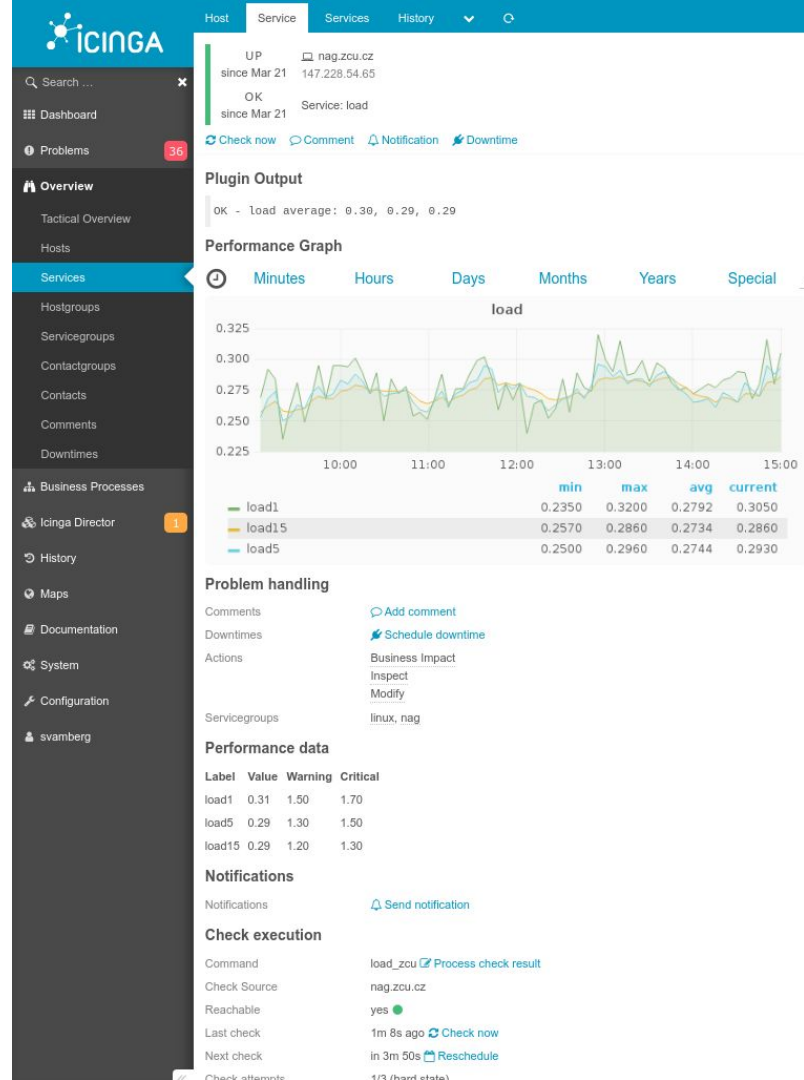


Síťové služby



Nagiosgraph -> Grafana

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

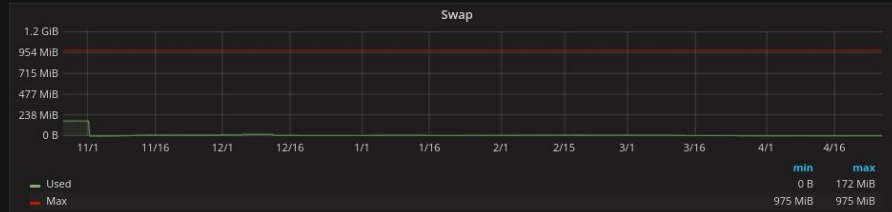




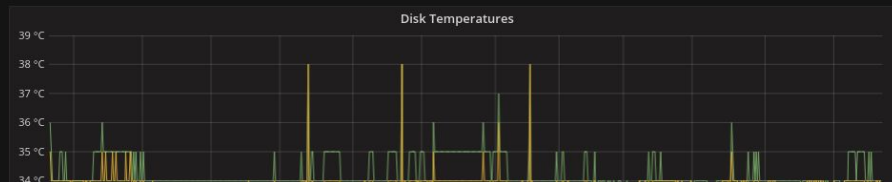
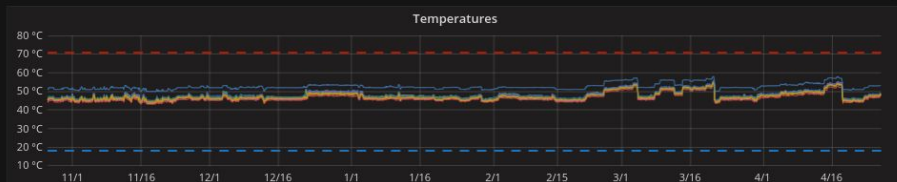
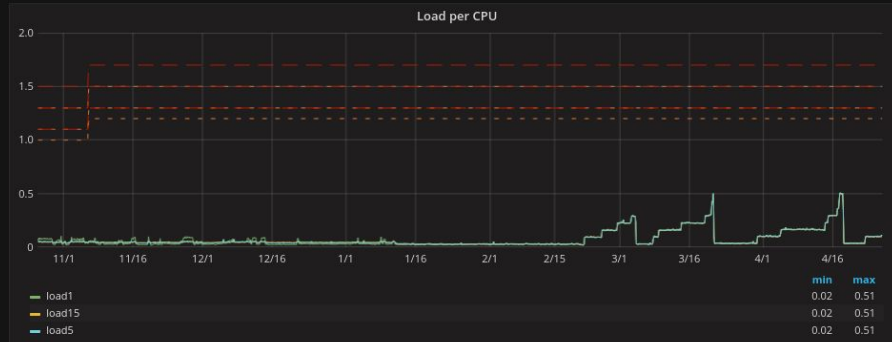
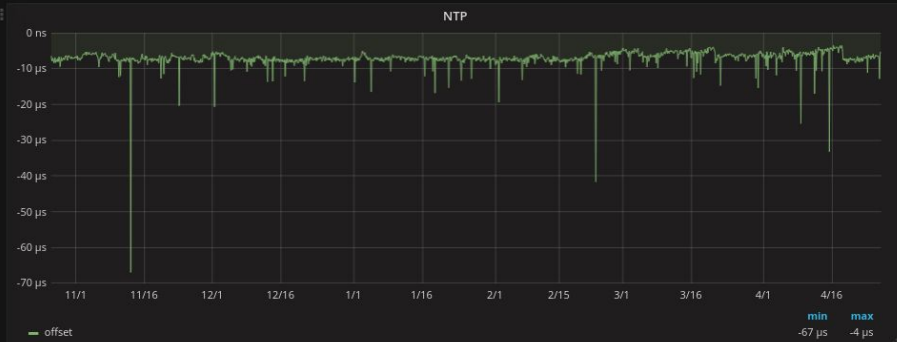
hostname achlys.zcu.cz

DISK USAGE

MEMORY



SYSTEM



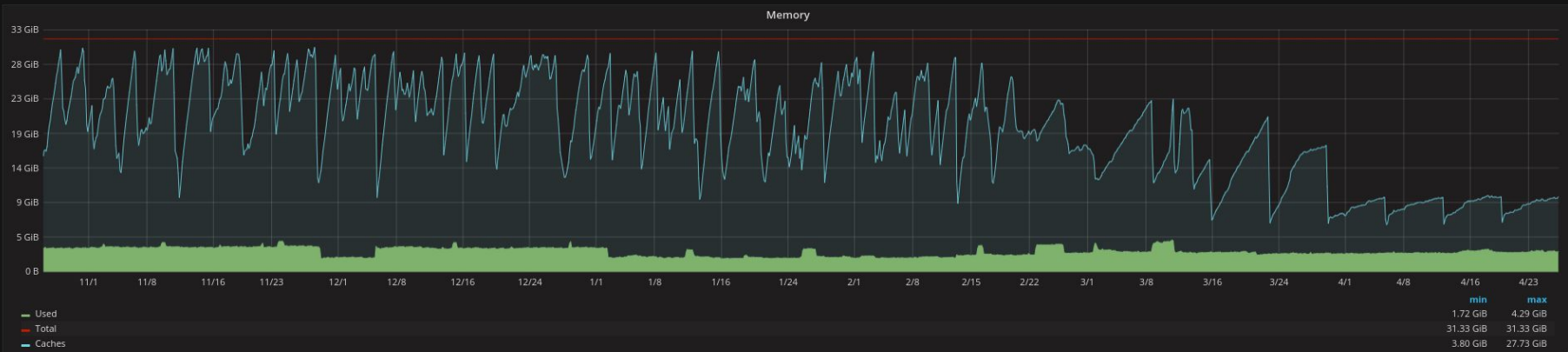
RRD -> InfluxDB

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



hostname achlys.zcu.cz

MEMORY



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)

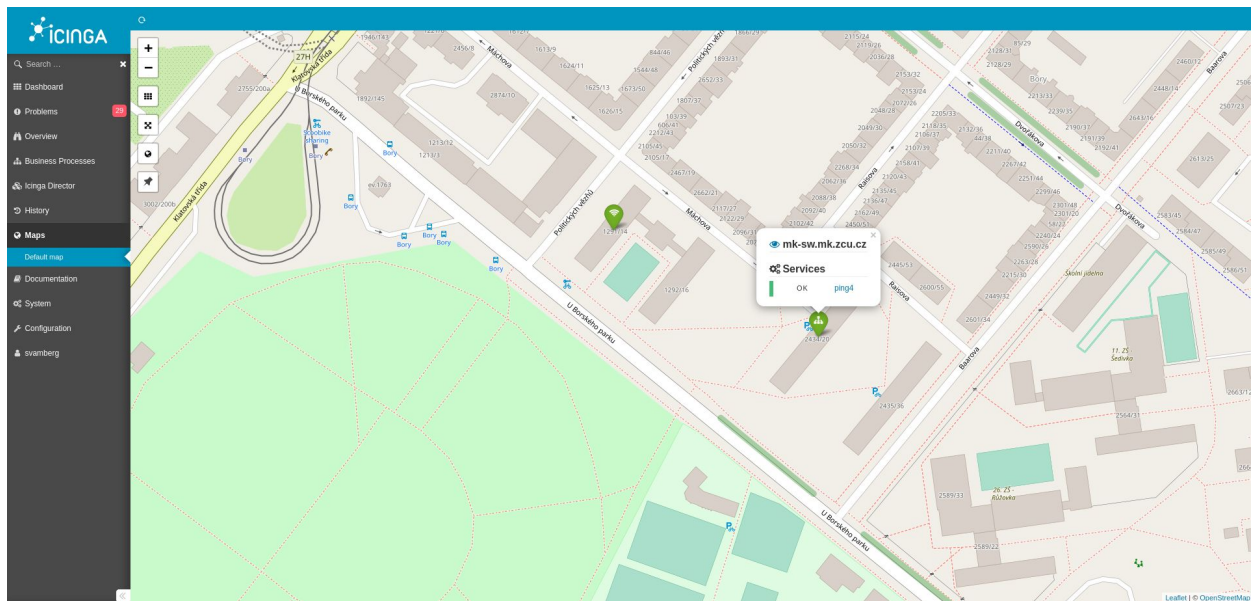
D SELECT mean("value") FROM "mem_zcu" WHERE ("hostname" =~ /\$hostname\$/ AND "metric" = 'FREE') AND \$timeFilter GROUP BY time(\$__interval) fill(none)

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 místnosti (alias pro GPS souřadnici),
- ručním zadáním GPS souřadnice nebo
- kliknutím do mapy v modulu mapDatatype.



aNag

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

aNag
All instances updated

INSTANCES

ZCU
Last update: 2019-05-17 14:32:28
Host: 0 / 0 / 0 / 0, Service: 0 / 0 / 2 / 3 / 1

PROBLEMS

disk usage
ZCU > skylla.ntc.zcu.cz
DISK CRITICAL - free space: /mnt/data 0 MB (0% inode=0%);

disk usage
ZCU > stag-test.zcu.cz
DISK CRITICAL - free space: / 918 MB (4% inode=72%);

load full
ZCU > achlys.zcu.cz
WARNING - load average: 10.40, 10.34, 10.35

disk usage
ZCU > hc.civ.zcu.cz
DISK WARNING - free space: / 4350 MB (8% inode=99%);

disk usage
ZCU > lm64.zcu.cz
DISK WARNING - free space: / 803 MB (8% inode=82%);

mailq
ZCU > akka10.civ.zcu.cz
ERROR: /usr/bin/mailq is not executable by (uid 109:gid(114 114))



General

Home Documentation Panorama View

Current Status

Tactical Overview

Hosts

Services

Host Groups

Service Groups

Summary (Grid)

- Map
- Alerts
- History (Summary)
- Notifications
- Business Process
- System
- Comments
- Downlines
- Recuring Downlines
- Performance Info
- Scheduling Queue

All Unhandled Problems

Host	Service	Status	Last Check	Duration	Attempt	Info
koosek-h01.civ.zcu.cz	ssh	DOWN	14:22:11	131 8h 19m 7s	3/3	PING CRITICAL - Packet loss = 100%
koosek-h04.zcu.cz	ssh	DOWN	14:23:06	0d 8h 18m 13s	3/3	PING CRITICAL - Packet loss = 100%

2 of 2 Matching Host Entries Displayed

select all (hosts) - unselect all - all problems - all with downtime

Host	Service	Status	Last Check	Duration	Attempt	Info
koosek-h01.civ.zcu.cz	ssh	CRITICAL	15:53:58	5d 2h 3m 1s	16/45	Total certificates: 1 (Critical: 1, Warning: 0, Unknown: 0)
koosek-h04.zcu.cz	ssh	WARNING	14:17:47	0d 7h 48m 55s	13/11	WARNING - load average: 10.30, 10.28, 10.35
koosek-h01.civ.zcu.cz	rsync	UNKNOWN	14:21:21	9d 21h 19m 48s	1/3	ERROR: libssh/malloc is not executable by (uid 109) (pid 114 114)
koosek-h01.civ.zcu.cz	rsync	CRITICAL	14:20:58	42d 1h 24m 44s	1/4	connect to address 147.228.52.87 and port 443: Connection refused
koosek-h01.civ.zcu.cz	disk usage	WARNING	14:21:06	1d 20h 30m 51s	13/82	DISK WARNING - free space / 4390 MB (8% inode=99%)
koosek-h04.zcu.cz	ssh	CRITICAL	14:17:41	44d 3h 42m 53s	1/4	CRITICAL - Socket timeout after 10 seconds
koosek-h01.civ.zcu.cz	portal apps	CRITICAL	14:18:07	64d 14h 58m 34s	1/3	CRITICAL - Sasazawa neznama aplikace: /zdne/runtime/zdne
koosek-h04.zcu.cz	certificates	CRITICAL	10:04:52	7d 21h 57m 0s	1/5 4/23	Total certificates: 1 (Critical: 1, Warning: 0, Unknown: 0)
koosek-h04.zcu.cz	ssh	CRITICAL	14:17:28	38d 3h 46m 4s	1/4	connect to address 147.228.54.28 and port 443: Connection refused
koosek-h04.zcu.cz	disk usage	WARNING	14:20:39	0d 9h 6m 3s	13/81	DISK WARNING - free space / 463 MB (8% inode=52%)
koosek-h01.civ.zcu.cz	rsync	CRITICAL	14:21:41	6d 59m 0m 1s	1/3	PING CRITICAL - Packet loss = 100%, TTL=1185 ms
koosek-h01.civ.zcu.cz	certificates	CRITICAL	09:29:05	6d 23h 35m 15s	16/423	Total certificates: 1 (Critical: 1, Warning: 0, Unknown: 0)
koosek-h01.civ.zcu.cz	certificates	CRITICAL	13:38:10	6d 22h 24m 49s	16/823	Total certificates: 1 (Critical: 1, Warning: 0, Unknown: 0)
koosek-h01.civ.zcu.cz	ssh	WARNING	14:21:10	9d 16h 2m 4s	1/4	HTTP WARNING: HTTP/1.1 403 Forbidden - 389 bytes in 0.015 second response time
koosek-h01.civ.zcu.cz	portal apps	CRITICAL	14:19:57	3d 0h 31m 55s	1/3	CRITICAL - sasazawa: Nastava chybte: Can't overwrite cause with java.lang.ClassNotFoundException: null.ProgrammeDAO
koosek-h01.civ.zcu.cz	ssh	CRITICAL	14:20:20	0d 8h 11m 22s	1/4	HTTP CRITICAL: HTTP/1.1 500 Service Unavailable - 3200 bytes in 0.119 second response time
koosek-h01.civ.zcu.cz	ssh	WARNING	14:19:30	87d 21h 0m 7s	1/4	HTTP WARNING: HTTP/1.1 403 Forbidden - 389 bytes in 0.009 second response time
koosek-h01.civ.zcu.cz	portal apps	CRITICAL	14:19:04	4d 11h 13m 55s	1/3	CRITICAL - no connection to "/tmp/arte" could not connect to server: No such file or directory
koosek-h01.civ.zcu.cz	portal apps	CRITICAL	14:21:25	64d 19h 7m 7s	1/3	CRITICAL - no connection to "/tmp/arte" could not connect to server: No such file or directory

1: Cannot make SSL connection.
 Codes: 1 (Critical: 1, Warning: 0, Unknown: 0)

2: Sasazawa neznama aplikace: /RozcestniPortlet/testing/6/RozcestniPortlet
 Codes: 139 (Critical: 0, Warning: 1, Unknown: 0)

3: shz_frontend (/shz_frontend): Exception java.io.IOException: Server returned HTTP response code: 500 for URL: https://stag-demo.zcu.cz/shz_frontend/TestServlet?actor=shzFront
 ANNING: HTTP/1.1 404 404 - 1337 bytes in 0.017 second response time

TICAL - free space / 918 MB (4% inode=72%)
 Codes: 1 (Critical: 1, Warning: 0, Unknown: 0)

4: Socket timeout after 10 seconds
 TICAL - Packet loss = 100%

5: Socket timeout after 10 seconds
 exceeded ==Terminated by signal 9 (Killed) >
 exceeded ==Terminated by signal 9 (Killed) >
 1: address 147.228.51.144 and port 443: Connection refused
 Codes: 1 (Critical: 1, Warning: 0, Unknown: 0)

6: Codes: 139 (Critical: 0, Warning: 1, Unknown: 0)

7: Socket timeout after 10 seconds
 exceeded ==Terminated by signal 9 (Killed) >
 exceeded ==Terminated by signal 9 (Killed) >
 1: address 147.228.51.144 and port 443: Connection refused
 Host not ok on the stranku

All Unhandled Problems

General

Home Documentation Panorama View

Current Status

Tactical Overview

Hosts

Services

Host Groups

Service Groups

Summary (Grid)

- Map
- Alerts
- History (Summary)
- Notifications
- Business Process
- System
- Comments
- Downlines
- Recuring Downlines
- Performance Info
- Scheduling Queue

All Unhandled Problems

Host	Service	Status	Last Check	Duration	Attempt	Info
koosek-h01.civ.zcu.cz	ssh	DOWN	14:22:11	131 8h 19m 7s	3/3	PING CRITICAL - Packet loss = 100%
koosek-h04.zcu.cz	ssh	DOWN	14:23:06	0d 8h 18m 13s	3/3	PING CRITICAL - Packet loss = 100%

2 of 2 Matching Host Entries Displayed

select all (hosts) - unselect all - all problems - all with downtime

Host	Service	Status	Last Check	Duration	Attempt	Info
593gw-lot.zcu.cz	certificates	CRITICAL	13:50:53	50d 2h 6m 51s	1/5 451	Total certificates: 11 (Critical: 1, Warning: 0, Unknown: 0)
anyka.zcu.cz	ssh	WARNING	14:22:47	0d 7h 52m 45s	13/81	WARNING - load average: 10.36, 10.16, 10.14
skiba10.civ.zcu.cz	rsync	UNKNOWN	14:24:21	9d 21h 23m 36s	1/3	ERROR: libssh/malloc is not executable by (uid 109) (pid 114 114)
brifrost.civ.zcu.cz	rsync	CRITICAL	14:20:58	42d 1h 24m 34s	1/4	connect to address 147.228.52.87 and port 443: Connection refused
hc.civ.zcu.cz	disk usage	WARNING	14:21:06	1d 20h 34m 41s	13/82	DISK WARNING - free space / 4390 MB (8% inode=99%)
koosek-h04.zcu.cz	ssh	CRITICAL	14:22:41	44d 3h 46m 43s	1/4	CRITICAL - Socket timeout after 10 seconds
koosek-h01.civ.zcu.cz	portal apps	CRITICAL	14:20:07	64d 15h 2m 24s	1/3	CRITICAL - Sasazawa neznama aplikace: /zdne/runtime/zdne
koosek-h01.civ.zcu.cz	certificates	CRITICAL	10:04:52	7d 23h 3m 55s	1/5 4/23	Total certificates: 1 (Critical: 1, Warning: 0, Unknown: 0)
koosek-h01.civ.zcu.cz	certificates	CRITICAL	14:20:28	38d 3h 46m 54s	1/4	connect to address 147.228.54.28 and port 443: Connection refused
koosek-h04.zcu.cz	disk usage	WARNING	14:20:39	0d 9h 5m 53s	13/81	DISK WARNING - free space / 463 MB (8% inode=82%)
netflow-new.zcu.cz	certificates	CRITICAL	09:29:05	6d 22h 39m 5s	1/5 4/23	Total certificates: 1 (Critical: 1, Warning: 0, Unknown: 0)
netflow.zcu.cz	certificates	CRITICAL	13:39:10	6d 20h 28m 38s	1/5 4/23	Total certificates: 1 (Critical: 1, Warning: 0, Unknown: 0)
pa3.zcu.cz	ssh	WARNING	14:21:10	9d 16h 5m 54s	1/4	HTTP WARNING: HTTP/1.1 403 Forbidden - 389 bytes in 0.015 second response time
pdm-cv.zcu.cz	portal apps	CRITICAL	14:24:56	3d 0h 35m 45s	1/3	CRITICAL - sasazawa: Nastava chybte: Can't overwrite cause with java.lang.ClassNotFoundException: null.ProgrammeDAO
koosek-h01.civ.zcu.cz	portal apps	CRITICAL	14:20:20	0d 8h 11m 22s	1/4	HTTP CRITICAL: HTTP/1.1 500 Service Unavailable - 3200 bytes in 0.120 second response time
koosek-h01.civ.zcu.cz	ssh	WARNING	14:24:30	87d 21h 3m 57s	1/4	HTTP WARNING: HTTP/1.1 403 Forbidden - 389 bytes in 0.011 second response time
koosek-h01.civ.zcu.cz	portal apps	CRITICAL	14:24:04	4d 11h 17m 45s	1/3	CRITICAL - no connection to "/tmp/arte" could not connect to server: No such file or directory
sinustest.zcu.cz	portal apps	CRITICAL	14:21:25	64d 19h 4m 87s	1/3	CRITICAL - no connection to "/tmp/arte" could not connect to server: No such file or directory
skyla-rtc.zcu.cz	disk usage	CRITICAL	14:22:42	64d 15h 0m 40s	1/3 8/85	DISK CRITICAL - free space / /mnt/data 0 MB (0% inode=0%)
koosek-h01.civ.zcu.cz	ssh	CRITICAL	14:23:13	38d 3h 46m 49s	1/4	CRITICAL - Cannot make SSL connection.
stag-demo-ub.zcu.cz	certificates	CRITICAL	12:44:00	0d 19h 23m 14s	1/5 8/18	Total certificates: 1 (Critical: 1, Warning: 0, Unknown: 0)
stag-demo.zcu.cz	portal apps	CRITICAL	14:23:36	64d 15h 6m 6s	1/3	CRITICAL - Sasazawa neznama aplikace: /RozcestniPortlet/testing/6/RozcestniPortlet
stag-demo.zcu.cz	portal apps	CRITICAL	14:24:06	13d 12h 19m 56s	1/3	CRITICAL - shz_frontend (/shz_frontend): Exception java.io.IOException: Server returned HTTP response code: 500 for URL: https://stag-demo.zcu.cz/shz_frontend/TestServlet
stag-experiments.zcu.cz	portal apps	CRITICAL	14:24:46	32d 3h 4m 48s	1/4	CRITICAL - PortalUpdaterClient (/PortalUpdaterClient). Security problem. sensitive files are potentially accessible (zcu-zp-protection) - security manager is not enabled at all.
stag-marbles.zcu.cz	ssh	WARNING	14:23:34	3d 0h 15m 53s	1/4	HTTP WARNING: HTTP/1.1 404 404 - 1337 bytes in 0.020 second response time
stag-new.zcu.cz	disk usage	CRITICAL	14:23:34	0d 7h 56m 58s	1/3	DISK CRITICAL - free space / 918 MB (4% inode=72%)
stag.zcu.cz	certificates	CRITICAL	14:23:44	57d 19h 5m 56s	1/4	CRITICAL - Socket timeout after 10 seconds
stag.zcu.cz	portal apps	CRITICAL	14:22:14	57d 19h 10m 35s	1/3	PING CRITICAL - Packet loss = 100%
stagweb-vfu.zcu.cz	ssh	CRITICAL	14:24:02	0d 1h 31m 46s	1/4 8/1	CRITICAL - Socket timeout after 10 seconds
stagweb.zcu.cz	portal apps	UNKNOWN	14:20:48	0d 1h 28m 55s	1/3	<Timeout exceeded ==Terminated by signal 9 (Killed) >
stagweb.zcu.cz	portal apps	UNKNOWN	14:24:08	0d 1h 29m 44s	1/4	<Timeout exceeded ==Terminated by signal 9 (Killed) >
tantaloze-test.zcu.cz	ssh	CRITICAL	14:24:58	87d 20h 15m 42s	1/4	connect to address 147.228.51.144 and port 443: Connection refused
tanvald.zcu.cz	certificates	CRITICAL	10:28:39	27d 22h 23m 11s	1/5 8/44	Total certificates: 1 (Critical: 1, Warning: 0, Unknown: 0)
web2.zcu.cz	certificates	WARNING	11:25:13	0d 9h 15m 53s	1/5 8/2	Total certificates: 129 (Critical: 0, Warning: 1, Unknown: 0)
wettag.zcu.cz	portal apps	CRITICAL	14:22:21	0d 0h 3m 11s	1/4	CRITICAL - StagPortlets:SR168 (/StagPortlets:SR168): Exception java.net.SocketTimeoutException: Read timed out
zeus-web.zcu.cz	portal apps	CRITICAL	14:22:55	0d 19h 12m 8s	1/3	critical: Timeout pri cekani na stranku

5d of 5d Evolution Service Status Historical

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

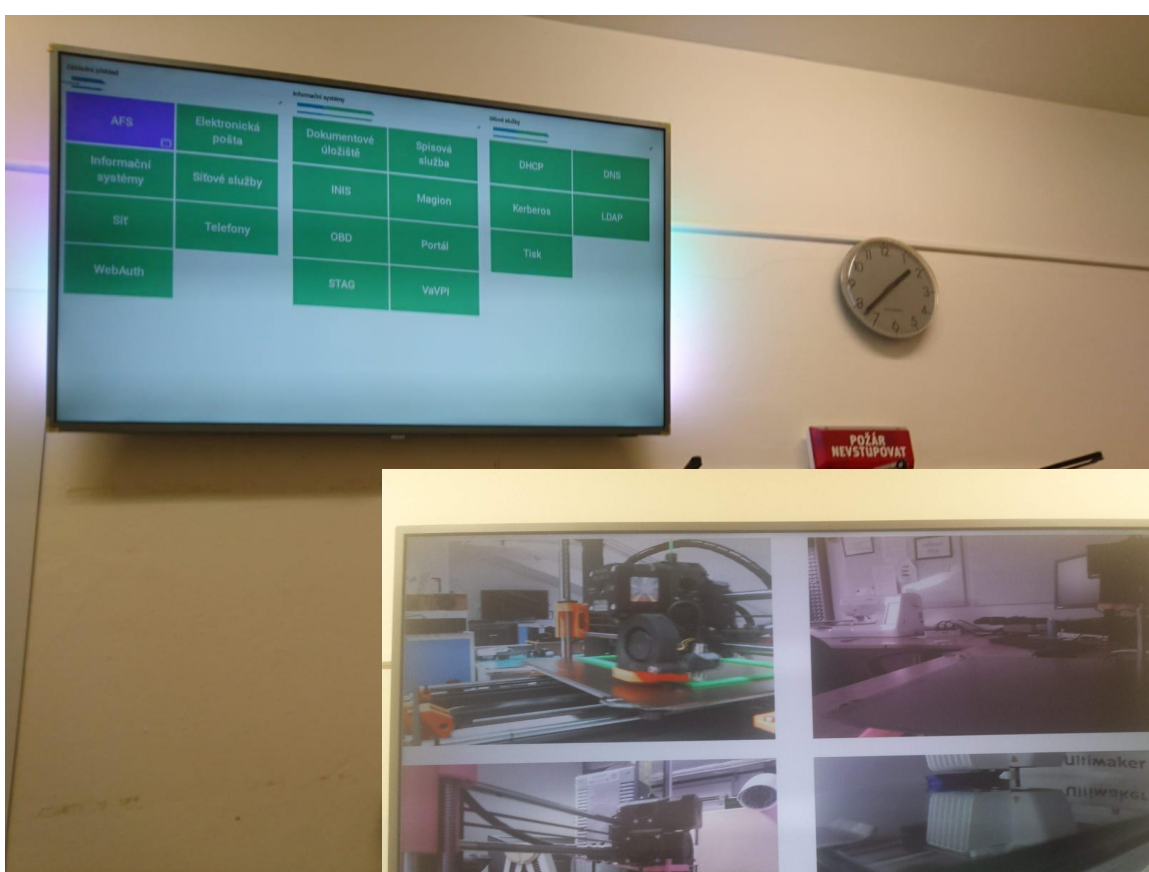
DNS

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

Uživatelé zakládání 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 síťů (Dude od MikroTiku) do Icingy
- Autentizace uživatelů přes SSO (WebAuth), povolení uživatelé generování ze účtů v Icinze



Demo & tutorial

<https://icinga.com/demo>

login / password: demo / demo

a nebo

Tutorial ve středu dopoledne

(instalace, konfigurace, monitorování, diskuse)

Děkuji

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

Moderní monitoring IT infrastruktury

Projekt 626R1/2018