



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



gov.cz



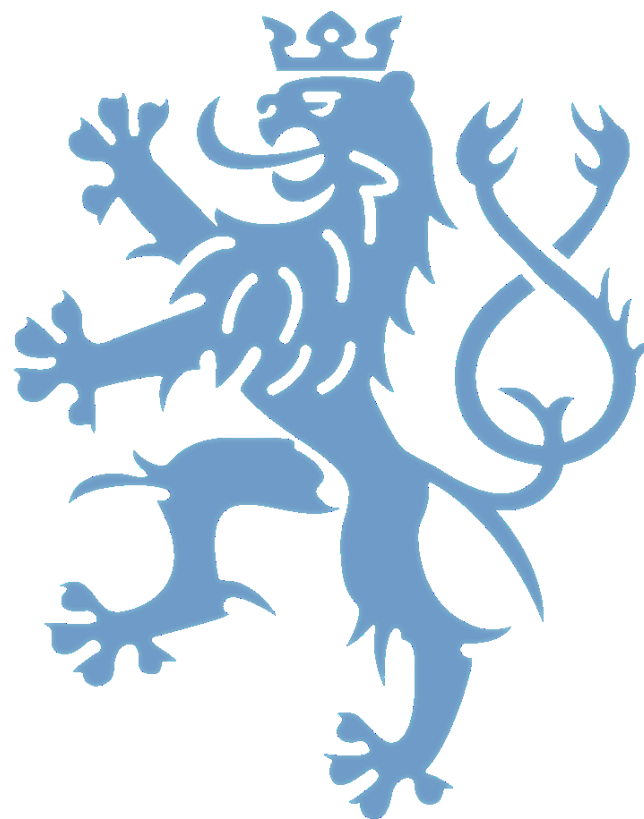
Zajištění provozu KII a VIS na odboru centrálních informačních systémů MV



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



NAKIT





➤ Úvod

- ❑ Představení prezentujících
- ❑ Představení OCIS infrastruktury

- Zákon o kybernetické bezpečnosti a jeho implementace na OCIS
- Centralizované open source řešení pro správu IT
- Technické a provozní standardy
- Směrování OCIS infrastruktury
- Závěr





MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



gov.cz



Představení prezentujících



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Ing. František Varmuža



Václav Krmenčík, Pavel Lejsek, Martin Svárovský

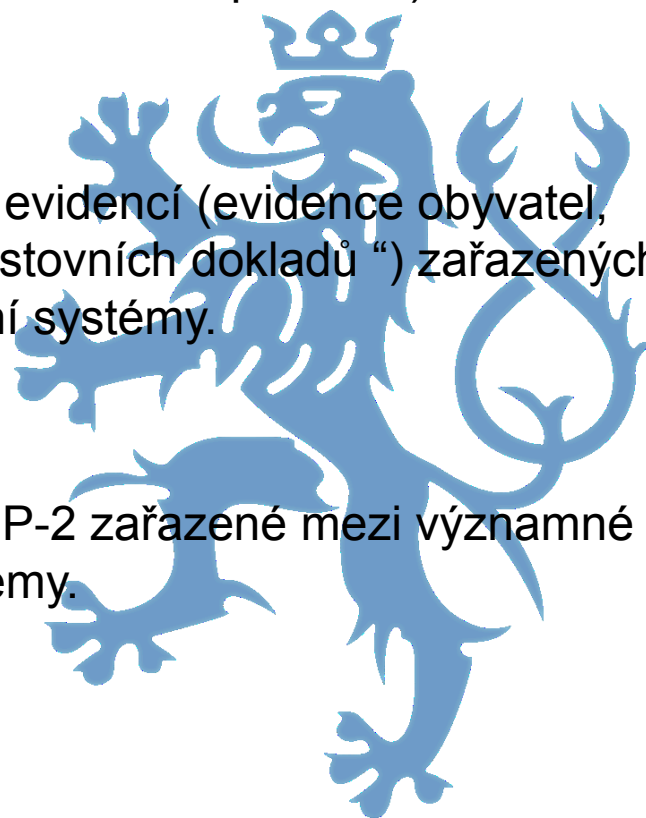




OCIS infrastruktura

Je složena ze správy kritických a významných informačních systémů zařazených v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

- ❑ Agendové informační systémy správních evidencí (evidence obyvatel, evidence občanských průkazů, evidence cestovních dokladů“) zařazených mezi kritické informační systémy.
- ❑ Systém spisové služby eSSL – GINIS a DP-2 zařazené mezi významné informační systémy.





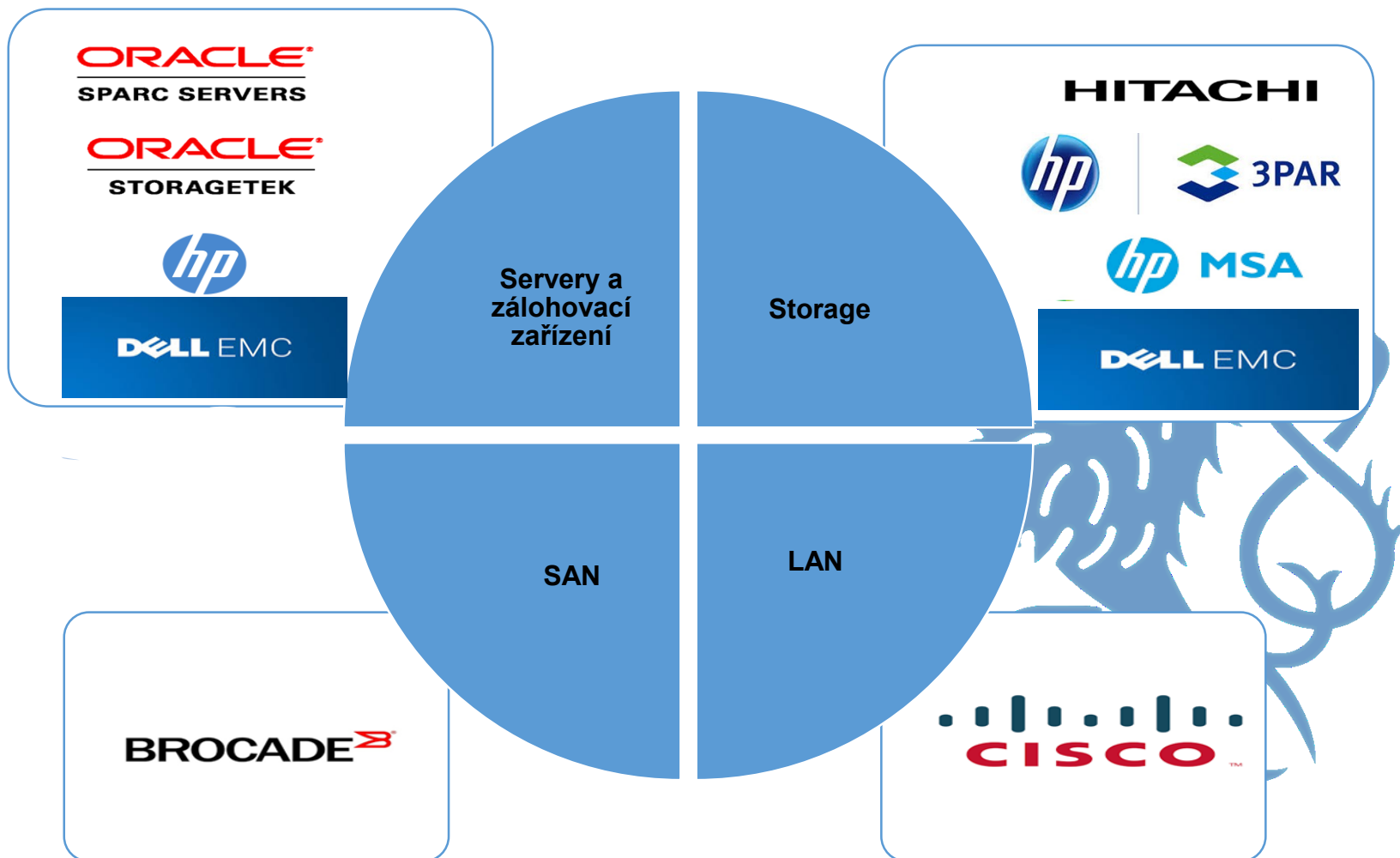
MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



gov.cz



Hardware

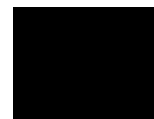




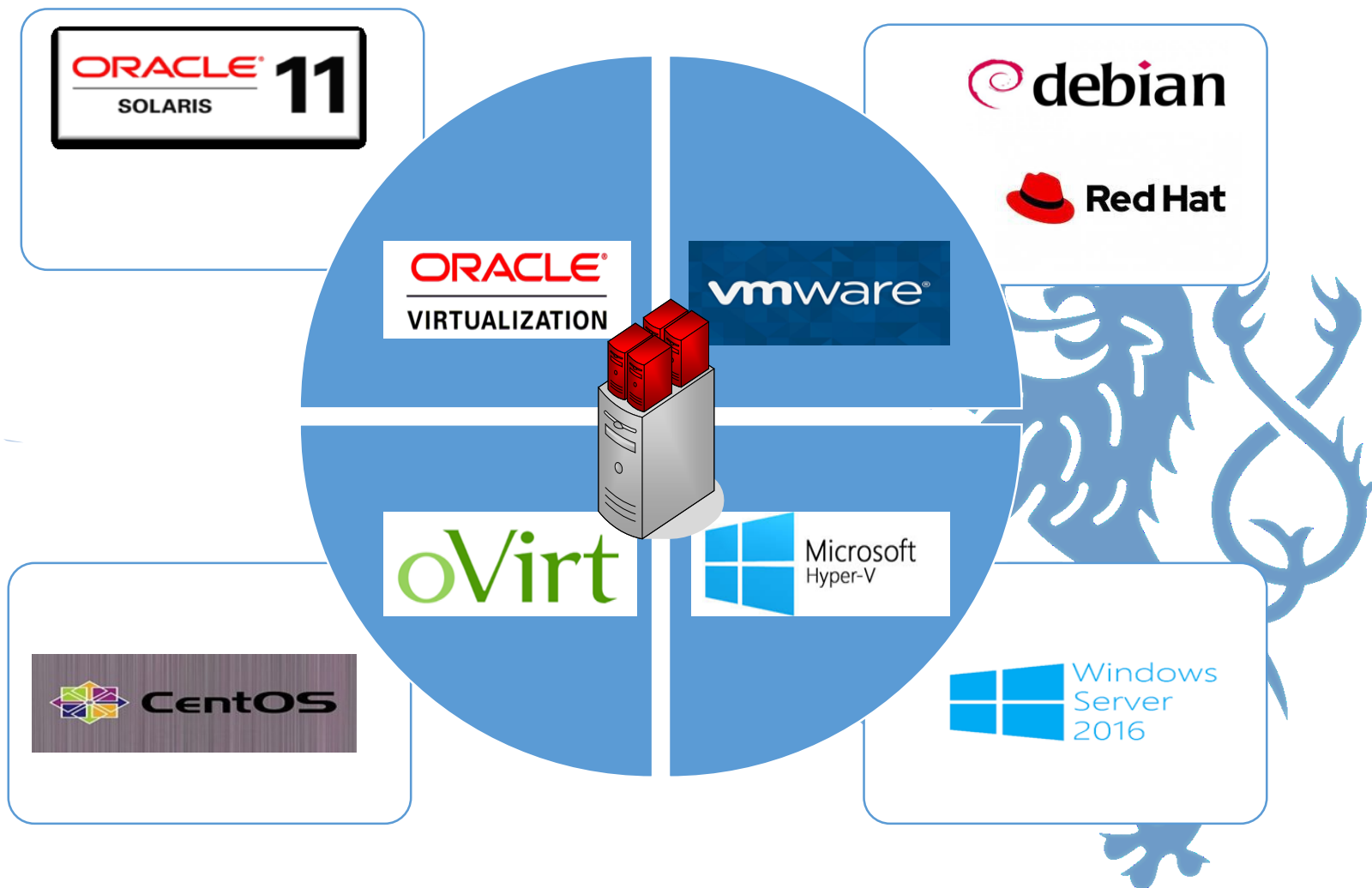
MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



gov.cz



Virtualizační technologie a operační systémy





MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



gov.cz



Databázové systémy

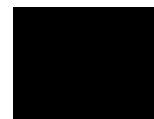




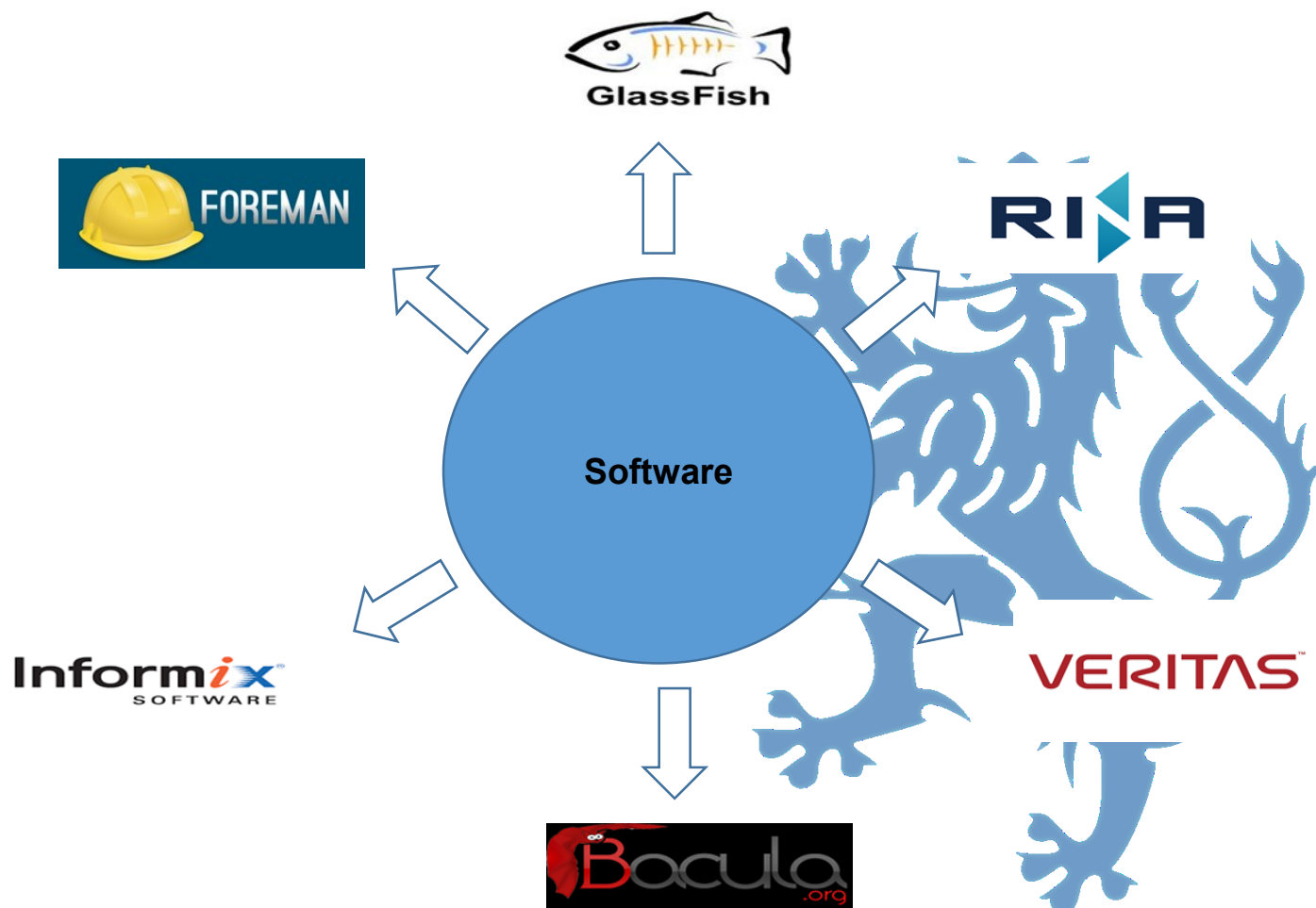
MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



gov.cz



Aplikační, zálohovací a cluster software

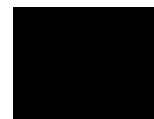




MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



gov.cz



Zákon o kybernetické bezpečnosti a jeho implementace na odboru centrálních informačních systémů MV, který zajišťuje provoz KII a VIS





MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

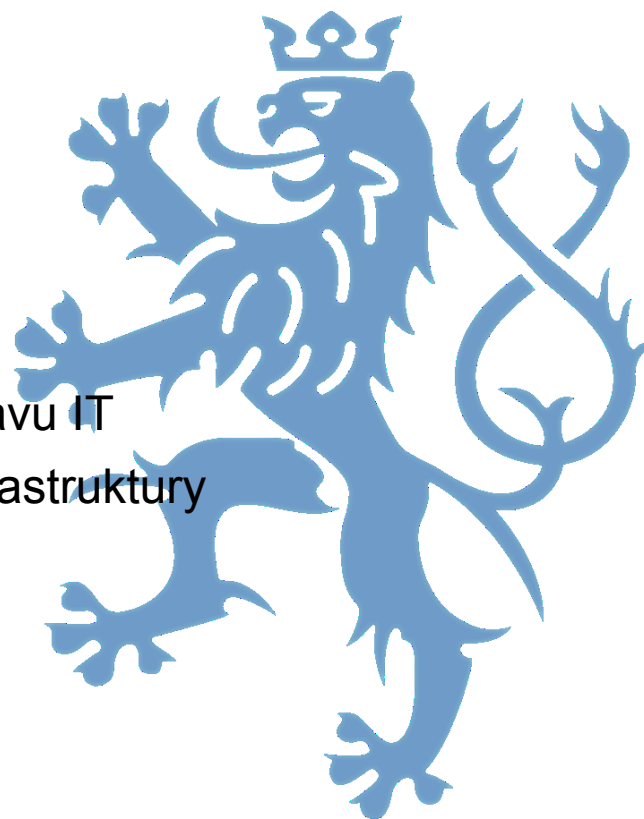


gov.cz



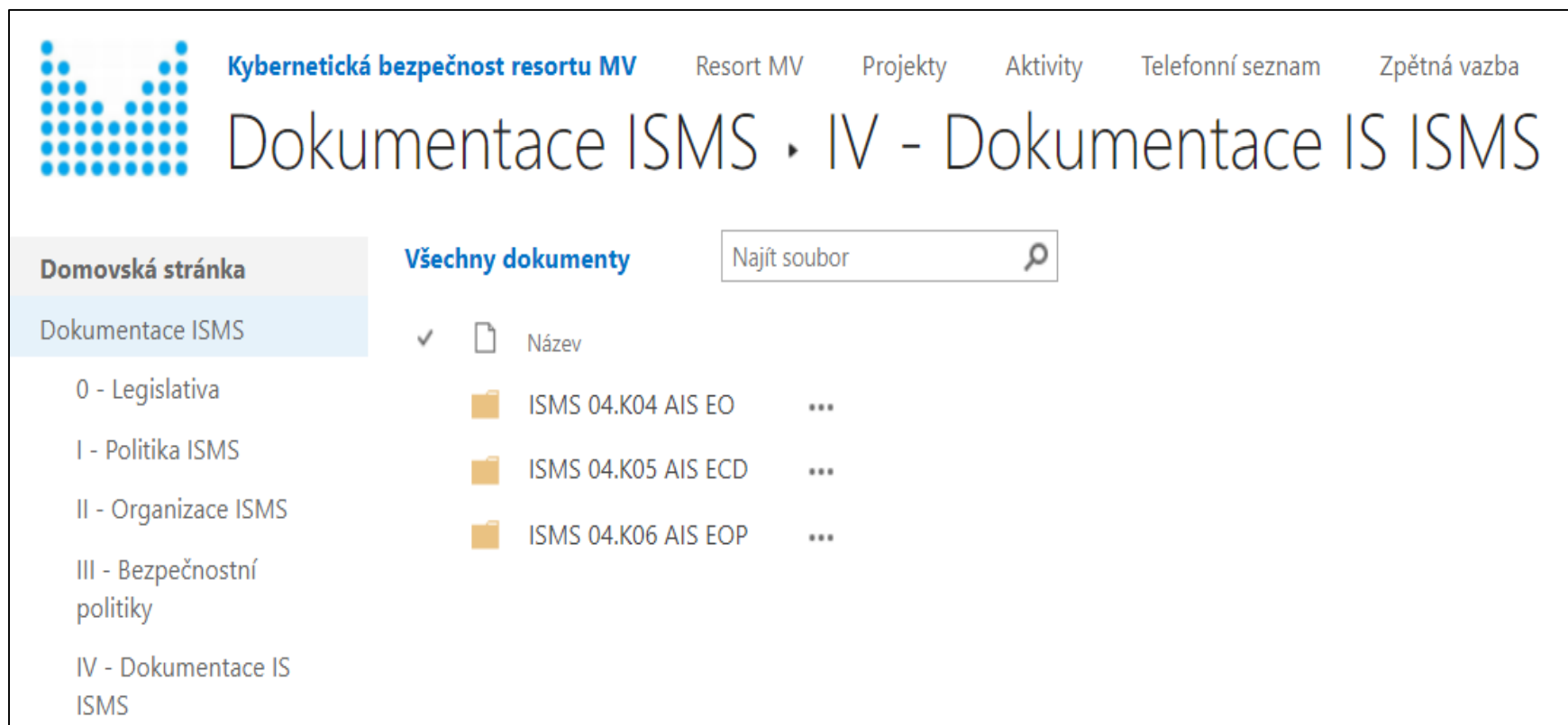
Obsah

- ISMS dokumentace
- Hardening
- Auditní politiky
- Centralizované open source řešení pro správu IT
Monitoring, dohled a podpůrné systémy infrastruktury





Vypracování dokumentů do Systému řízení informační bezpečnosti



The screenshot shows a web interface for the ISMS documentation system. At the top, there is a navigation bar with the following items: "Kybernetická bezpečnost resortu MV", "Resort MV", "Projekty", "Aktivity", "Telefonní seznam", and "Zpětná vazba". The main heading is "Dokumentace ISMS ▸ IV - Dokumentace IS ISMS". On the left, there is a sidebar menu with "Domovská stránka" and "Dokumentace ISMS". The "Dokumentace ISMS" menu is expanded, showing a list of folders: "0 - Legislativa", "I - Politika ISMS", "II - Organizace ISMS", "III - Bezpečnostní politiky", and "IV - Dokumentace IS ISMS". The "IV - Dokumentace IS ISMS" folder is selected, and its contents are displayed in a table. The table has a search bar "Najít soubor" and a magnifying glass icon. The table columns are "Název" and "..." (actions). The table contains three rows of folders: "ISMS 04.K04 AIS EO", "ISMS 04.K05 AIS ECD", and "ISMS 04.K06 AIS EOP".

Kybernetická bezpečnost resortu MV Resort MV Projekty Aktivity Telefonní seznam Zpětná vazba

Dokumentace ISMS ▸ IV - Dokumentace IS ISMS

Domovská stránka **Všechny dokumenty** Najít soubor 🔍

✓	📄	Název	
	📁	ISMS 04.K04 AIS EO	...
	📁	ISMS 04.K05 AIS ECD	...
	📁	ISMS 04.K06 AIS EOP	...





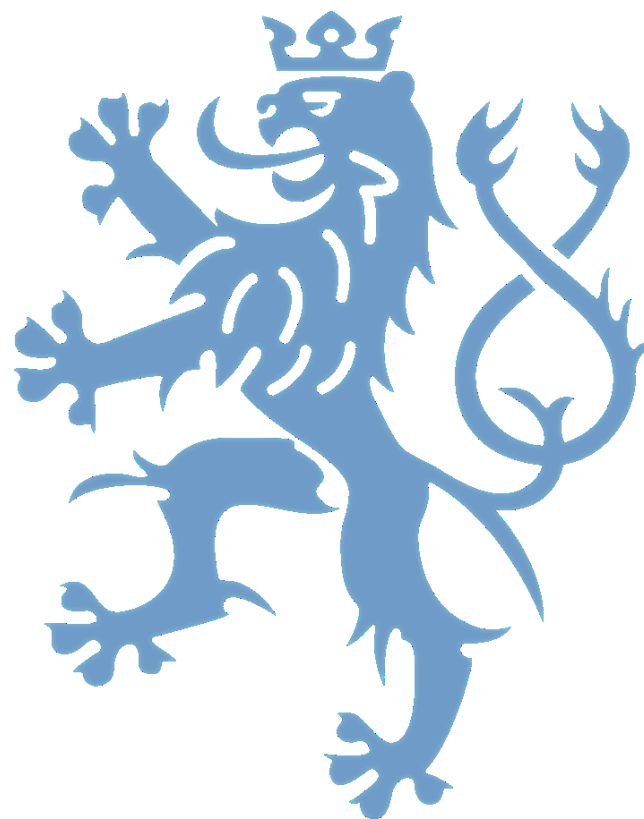
MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



gov.cz



Vytvoření procesu zabezpečení konfigurace systému takovým způsobem, který omezí výskyt zranitelností využitelných útočníkem. V IT terminologii je tento proces nazýván jako hardening.

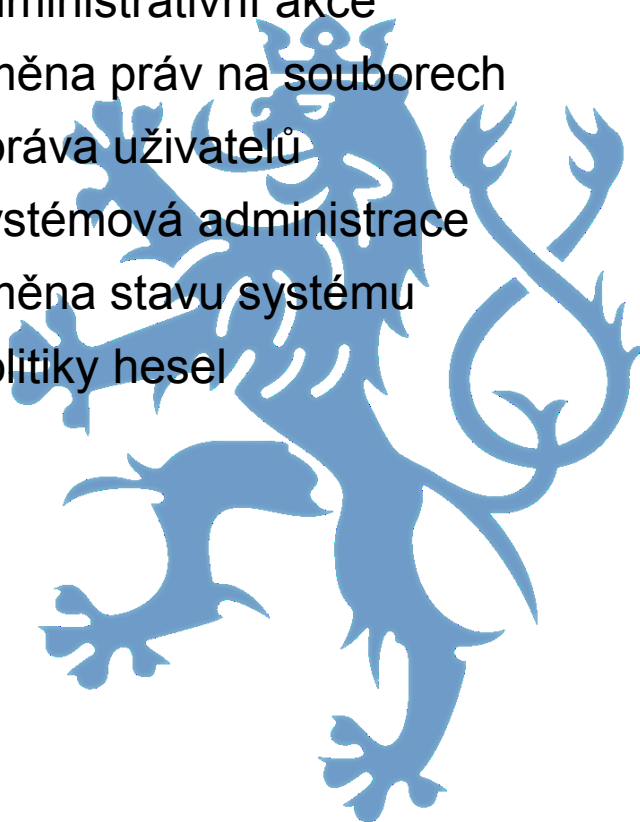


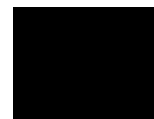


Nastavení politik auditingu systémů, aplikací a databází.



- Odhlášení, přihlášení uživatelů
- Administrativní akce
- Změna práv na souborech
- Správa uživatelů
- Systémová administrace
- Změna stavu systému
- Politiky hesel





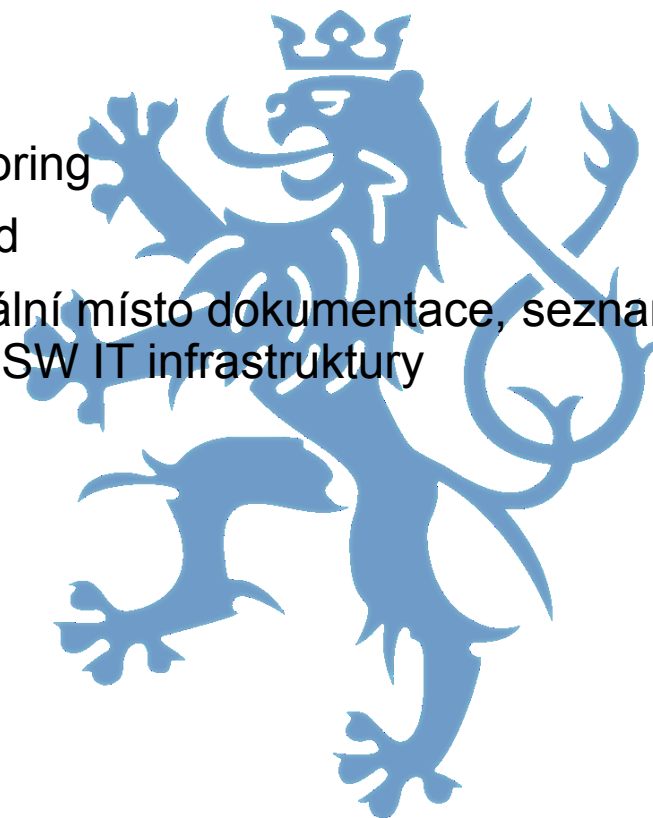
Centralizované open source řešení pro správu IT

Nezbytná a nutná součást pro naplnění požadavků kybernetického zákona.



open source

- Monitoring
- Dohled
- Centrální místo dokumentace, seznamu HW a SW IT infrastruktury





MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

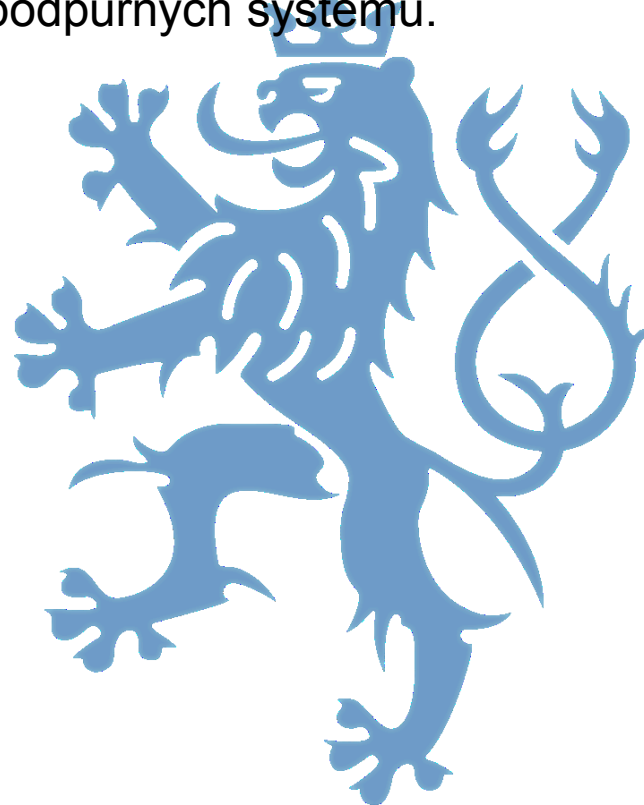


gov.cz



Monitoring, dohled a podpůrné systémy infrastruktury

Zajištění a zabezpečení služeb plné funkcionality „interního dohledu a monitoringu“ (automatické stahování provozních a systémových logů), vedení evidence změn a významných změn a dalších podpůrných systémů.





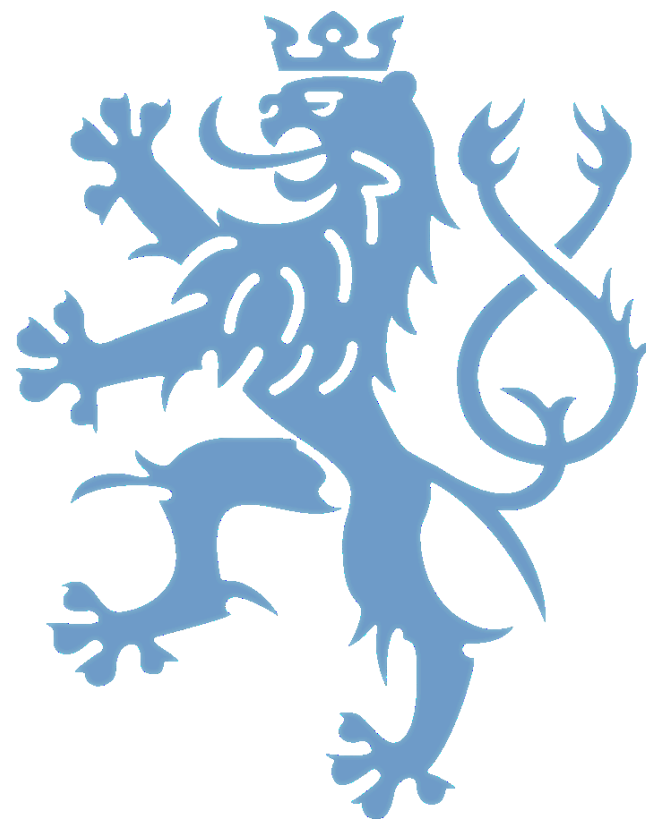
MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



gov.cz



Centrální monitoring OCIS IT infrastruktury

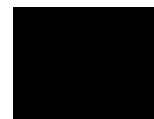




MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



gov.cz



Obsah

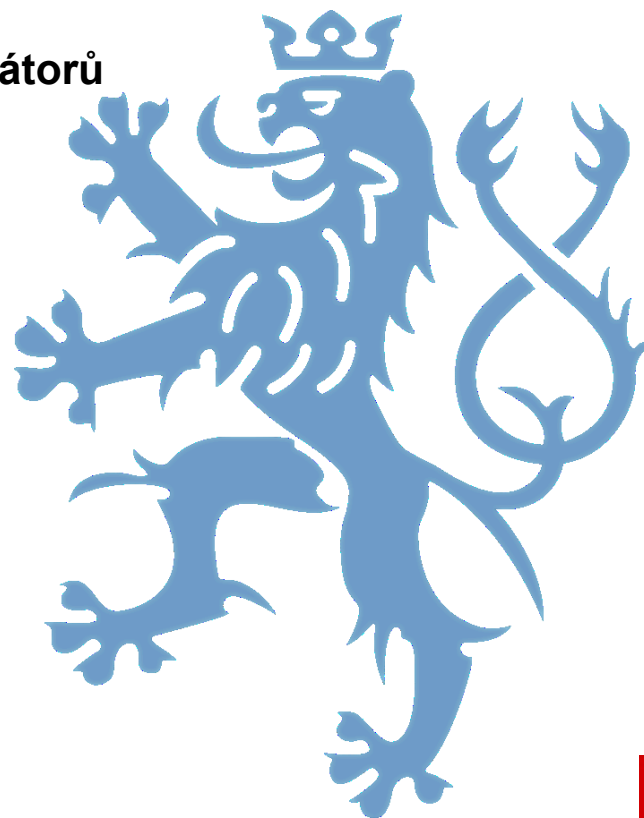
- Proč Zabbix
- Historie implementace monitoringu IT infrastruktury OCIS
- Ukázka provozního prostředí





Proč vůbec monitorovat?

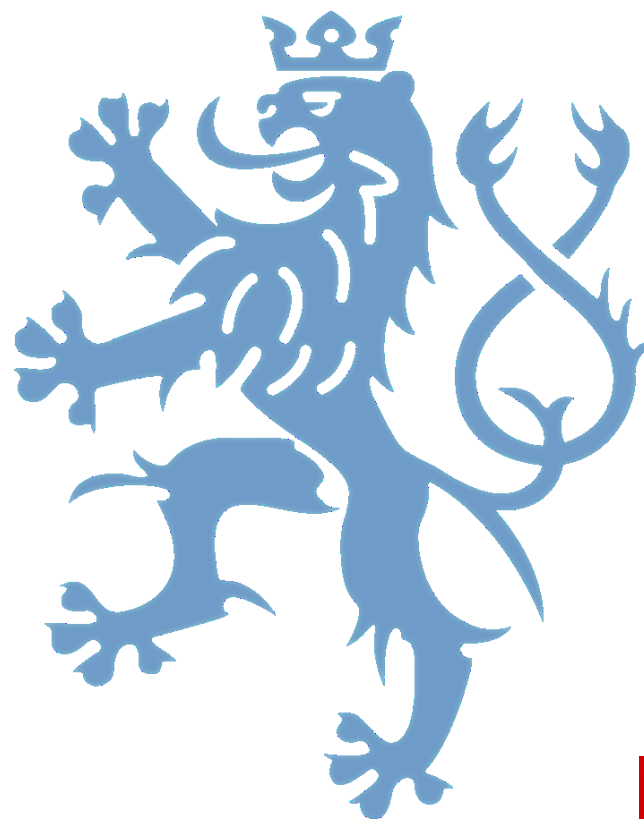
- **Identifikace a rychlé opravení problémů**
 - ❑ Rychlé rozpoznání bezpečnostní události = snížení negativního dopadu na provoz IT infra
- **Zvýšení produktivity systémových administrátorů**
 - ❑ Snížení administrativních nákladů
- **Měření dostupnosti a výkonnosti**
 - ❑ Ukládání historických a trend dat pro pozdější analýzu
- **Zlepšení kvality poskytovaných služeb**
- **Snížení nákladů**





Jaký monitorovací nástroj vybrat?

- **Open Source**
- **Podpora různých platforem**
- **Rozšiřitelný (monitorovaná zařízení/veličiny)**
- **Integrace vlastních skriptů/utilit**
- **Distribuovaný monitoring**
- **Dobrá vizualizace (grafy, mapy, dashboardy)**
- **Otevřený a přizpůsobitelný web frontend**
- **Aktivní a široká komunita**





MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

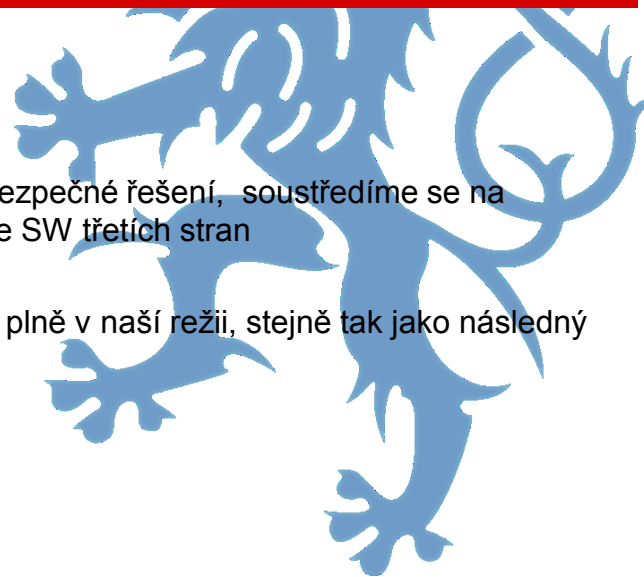


gov.cz



ZABBIX

- ❑ Od začátku se snažíme o co nejjednodušší a zároveň bezpečné řešení, soustředíme se na maximální využití nativních funkcí Zabbixu bez integrace SW třetích stran
- ❑ Jak navržená architektura, tak instalace i konfigurace je plně v naší režii, stejně tak jako následný provoz a rozvoj





Historie implementace monitoringu IT infrastruktury OCIS

Linux CentOS podpůrné systémy

HW

SunOS servery + VM

Informix DB

OCIS Appl

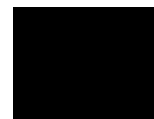
VMWare Hypervisors + VM

WIN servery/VM

Další org.složka/tým?

**CENTRALNÍ
MONITORING**





Eskalace / filtrování zpráv

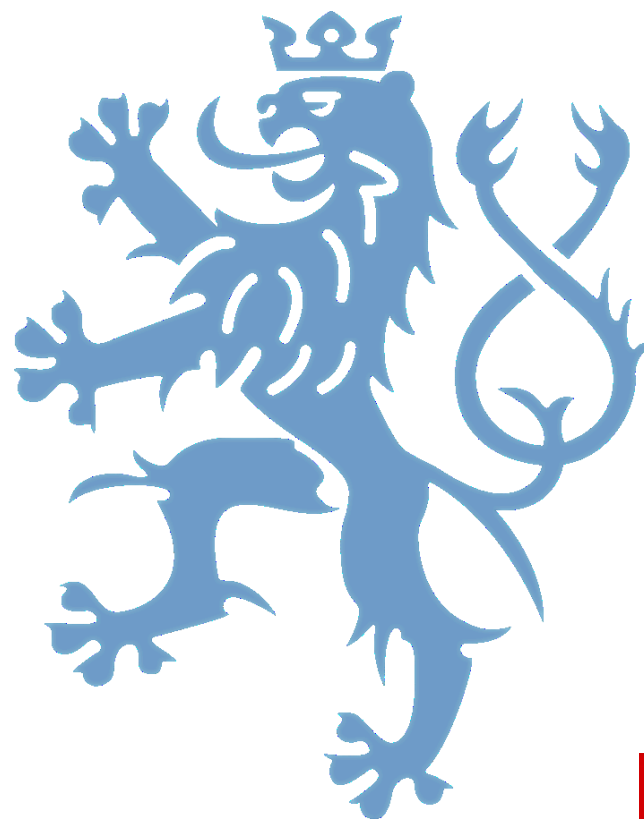
User Groups	Popis	Tags	Host Groups	Severity
D1 OCIS ADM SOLARIS	Správa OCIS SunOS	Service:OS/SAN, NAKIT:AVYK	D1 OCIS Solaris Servers (SunOS svět)	komplet vše
D1 OCIS ADM LINUX	Správa OCIS Linux OS	Service:OS/SAN, NAKIT:AVYK	D1 OCIS Linux Servers (LX svět)	komplet vše
D1 OCIS APPL/DB	Správa OCIS Appl	Service:APP/DB	D1 OCIS Solaris Servers	komplet vše
D1 OCIS LAN	Správa OCIS NET	Service:LAN	D1 OCIS Linux Servers	komplet vše
D2 OCIS ADM NT	Správa OCIS GINIS	WIN:OS/DB, NAKIT:AVYK	D2 OCIS NT (WIN svět)	komplet vše
D3 OCIS ADM	Dev&Test OCIS	Service:OS/SAN	D3 OCIS Servers (Vmware, HV)	komplet vše
Zabbix Administrators	Správa Zabbixu	žádný, tj. vidí vše	žádná, tj. vidí vše	komplet vše
Operators	Operátoři 24x7	Pouze Service:OPER_F	D1* + D2*	komplet vše





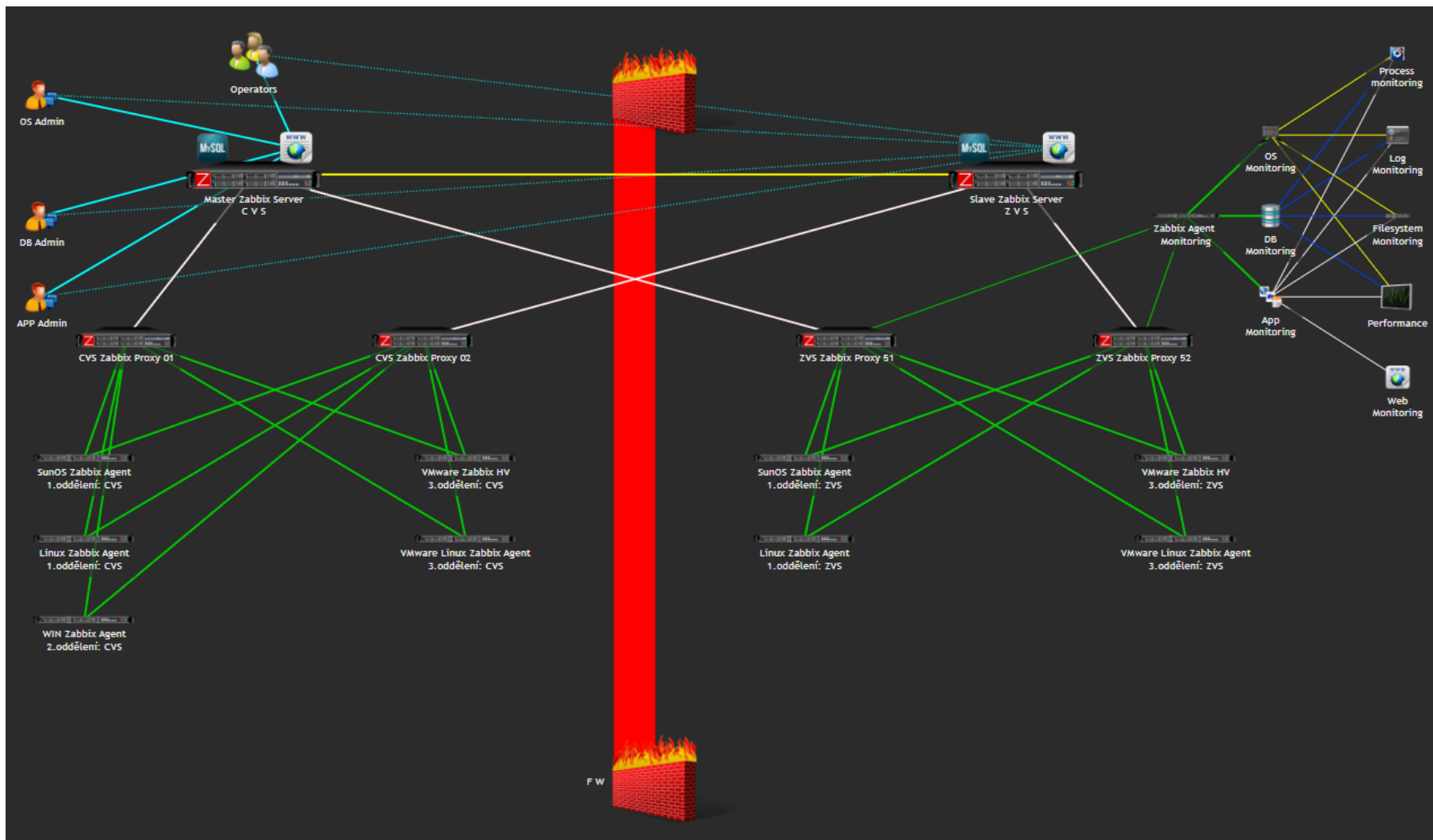
Jednotné názvosloví

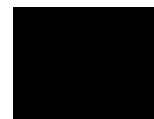
- **Uživatelské skupiny**
- **Dashboardy**
- **Skupiny serverů/VM**
- **Templaty (=šablony)**
- **SLA**
- **Mapy**





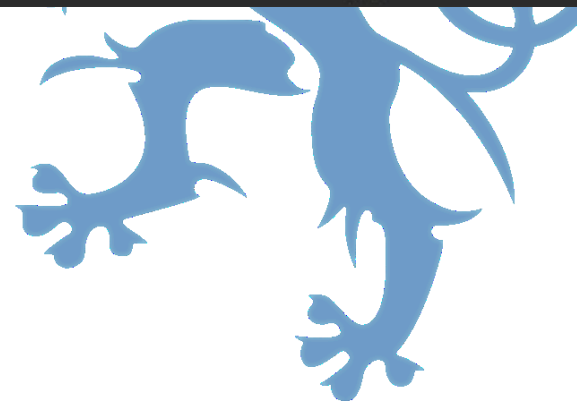
Zabbix mapa architektury





Zabbix provozní prostředí

Time	Severity	Recovery time	Status	Info	Host	Problem	Duration	Ack	Actions	Tags
08:21:05	Warning		PROBLEM		semapp223	Filesystem / na serveru semapp223 je zaplnen na 75 %	8m 58s	No		Service: APP, Service: DB, Service: OPER_F, ...
08:01:03	Critical		PROBLEM		semdb122	May 6 08:01:02 semdb122 sudo: [ID 702911 auth notice] operibx : TTY=pts/1 : PWD=/export/home/operibx : USER=informix : COMMAND=/export/home/inf ormix/helbackupid5_restore.sh semdb122crotcp sezdb122crotcp sezdb151bck CRO/varlog/auth log SX	29m	No		Service: OS
08:01:03	Normal		PROBLEM		semdb122	/export/home/informix/helbackupid5_restore.sh : START obnovy CRO do semdb122crotcp semdb122crotcp sezdb122crotcp sezdb151bck CRO/ITO_ER R log ids_restore	29m	No		Service: OPER_F, Service: OS
08:00										
00:36:38	Minor		PROBLEM		lvodog01.cse.mv.cz	May 6 00:36:37 192.168.12.16 687: May 6 00:36:36 CEST: %ILPOWER-3-CONTROLLER_PORT_ERR: Controller port error, Interface Gi0/5. Power given, but Power Controller does not report Power Good. syslog machine LAN	7h 53m 25s	No		Service: LAN, Service: OS
00:25:05	Normal		PROBLEM		CVS Zabbix server	Normal File May 6 00:25:05 CEST 2022 Zbx_BackupConfig_and_Move.sh: N. Zaloha Zabbix konfigurace probehla OK, soubor lvocbz01-Dump_ZbxDB_N Ohesl_2022_05_06.gz byl vytvořen N ITO_ERR_APP.log	8h 4m 58s	No		Service: APP, Service: OS
Today										
2022-05-05 15:06:05	Critical		PROBLEM		seddb1911	May 5 15:06:04 seddb1911 sshd[29345]: [ID 800047 auth info] Failed publickey for admjns from 10.74.40.38 port 56051 ssh2/varlog/auth log SX	17h 23m 58s	No		Service: OS
2022-05-05 14:39:37	Minor		PROBLEM		lvodog01.cse.mv.cz	May 5 14:39:36 hv1vso %ASA-3-106014: Deny inbound icmp src sw1_1-fw-hvs:10.73.64.208 dst sw1_1-fw-hvs:10.74.63.1 (type 8, code 0): syslog machine LAN	17h 50m 26s	No		Service: LAN, Service: OS





Zabbix provozní prostředí

Problem

Filesystem / na serveru semapn223 je zaplnen na 75 %

- TRIGGER
- Problems
- Description**
- Configuration
- HISTORY
- SunOS: FS Usage on / (percentage)



Trigger description

Description	Mimo pracovní dobu volejte pohotovost SUN-SOS.
-------------	--



Zabbix provozní prostředí

Host: semapp223
Problem: Filesystem / na serveru semapp223 je zaplnen na 75 %

SCRIPTS

- Kdo ma dnes pohotovost?**
- Ping
- Running processes
- Server Uptime
- Solaris: Zabbix Agent Stop
- Test monitoringu UX

GO TO

- Host inventory
- Latest data
- Problems
- Graphs
- Host screens



```
Kdo ma dnes pohotovost?  
  
/etc/zabbix/pom/kdo_ma_pohotovost.sh  
  
Datum          Skupina pohot.      Jmeno prijmeni      Telefon  
#####  
06.05.2022     INFRA-SOS           [redacted]  
-----  
06.05.2022     SUN-SOS             [redacted]  
-----  
06.05.2022     NT-SOS              [redacted]  
-----  
06.05.2022     SUN-DB              [redacted]  
-----  
06.05.2022     SUN-APP             [redacted]  
-----  
  
Kontakt na operatory OCIS [redacted]  
Kontakt na Hotline OCIS  [redacted]  
  
HOTLINE & SUPPORT  
#####  
AIS SE(Solaris prostredi)  
-----  
eSSL(Ginis), DP-2 [redacted]  
-----  
Monitoring a dohled  
-----  
DCeGOV
```





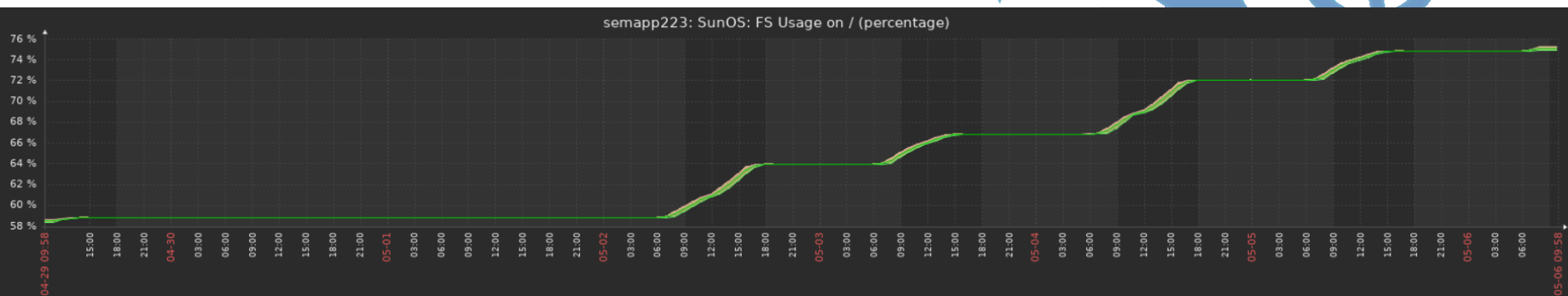
Zabbix provozní prostředí

Problem

Filesystem / na serveru semapp223 je zaplněn na 75 %

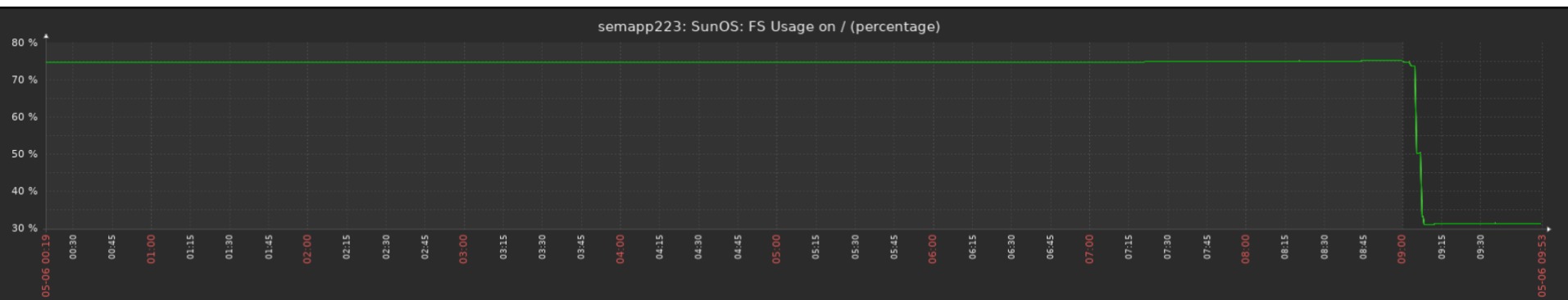
- TRIGGER
- Problems
- Description
- Configuration
- HISTORY

SunOS: FS Usage on / (percentage)

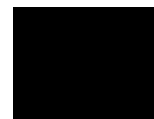




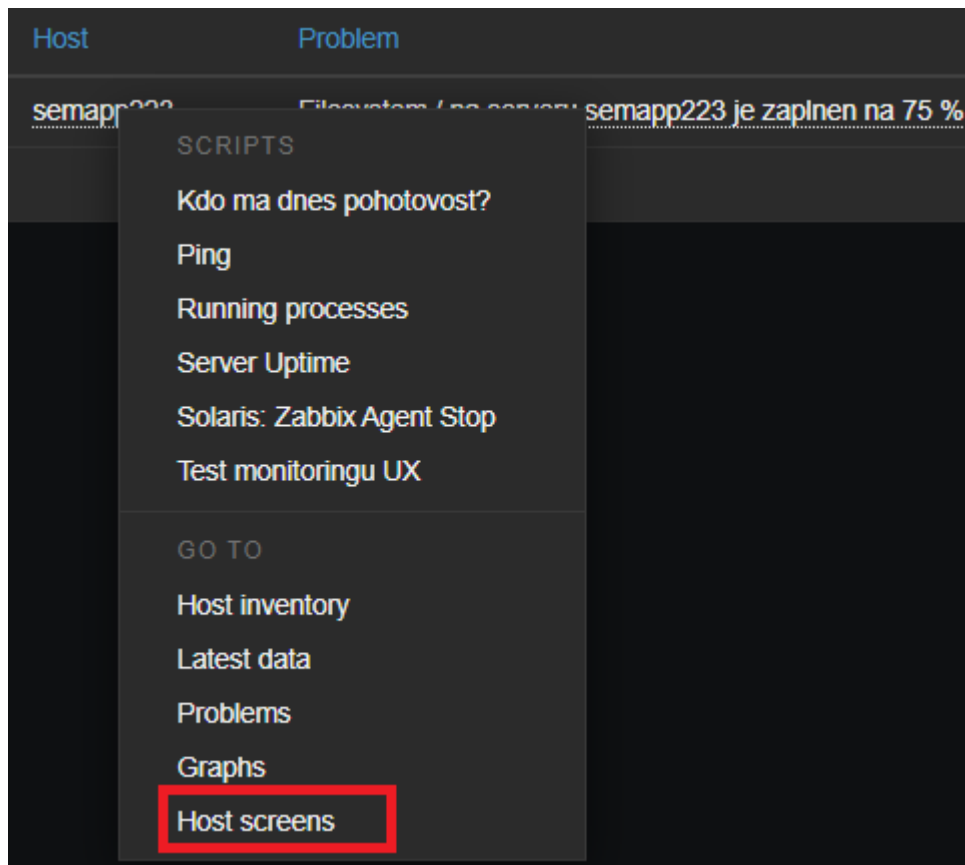
Zabbix provozní prostředí



Status	Info	Host	Problem
RESOLVED		semapp223	Filesystem / na serveru semapp223 je zaplnen na 75 %



Zabbix provozní prostředí

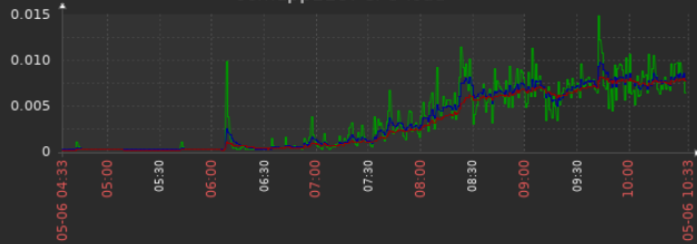




Zabbix provozní prostředí

Updated: 10:33:59

semapp223: CPU load



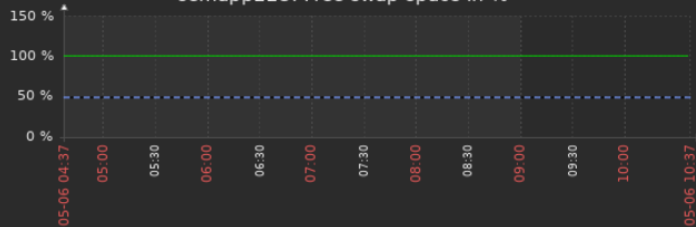
	[avg]	last	min	avg	max
Processor load (1 min average per core)	[avg]	0.0065	0.0002	0.0035	0.0149
Processor load (5 min average per core)	[avg]	0.0079	0.0002	0.0034	0.0097
Processor load (15 min average per core)	[avg]	0.0078	0.0001	0.0031	0.0081

semapp223: CPU utilization



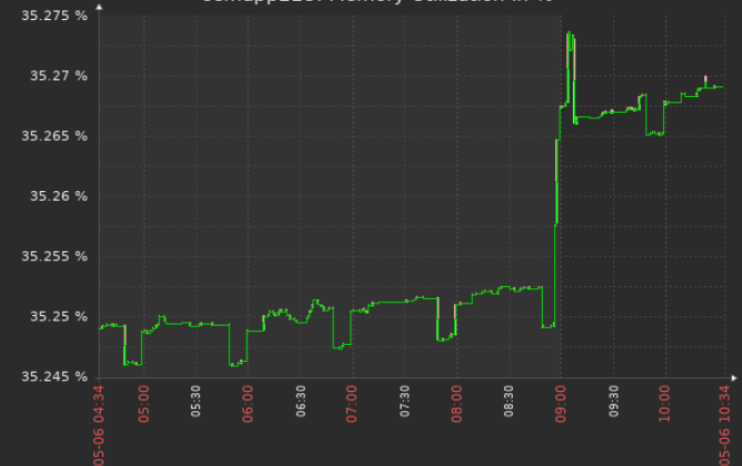
	[avg]	last	min	avg	max
CPU idle time	[avg]	99.3506 %	98.2831 %	99.6372 %	99.9714 %
CPU user time	[avg]	0.594 %	0.0107 %	0.2927 %	1.5194 %
CPU system time	[avg]	0.1179 %	0.0174 %	0.0697 %	0.2317 %
CPU await time	[avg]	0 %	0 %	0 %	0 %

semapp223: Free swap space in %



	[all]	last	min	avg	max
Free swap space in %	[all]	100 %	100 %	100 %	100 %

semapp223: Memory Utilization in %

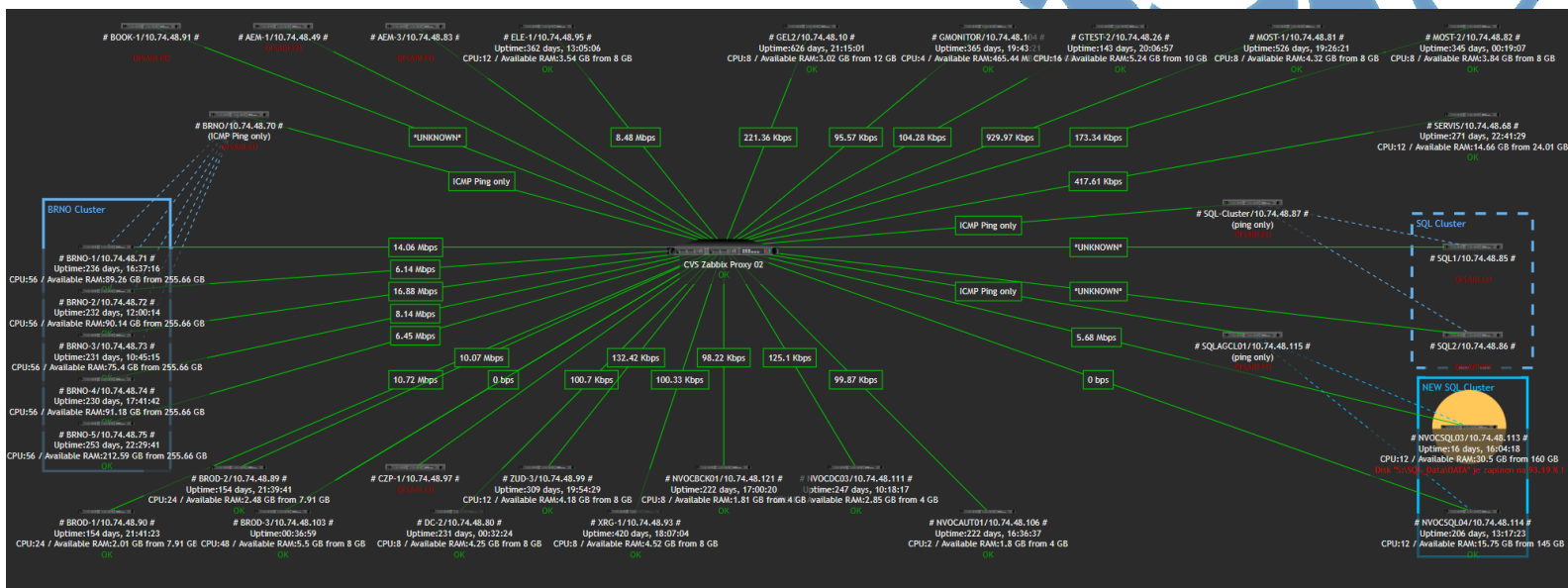
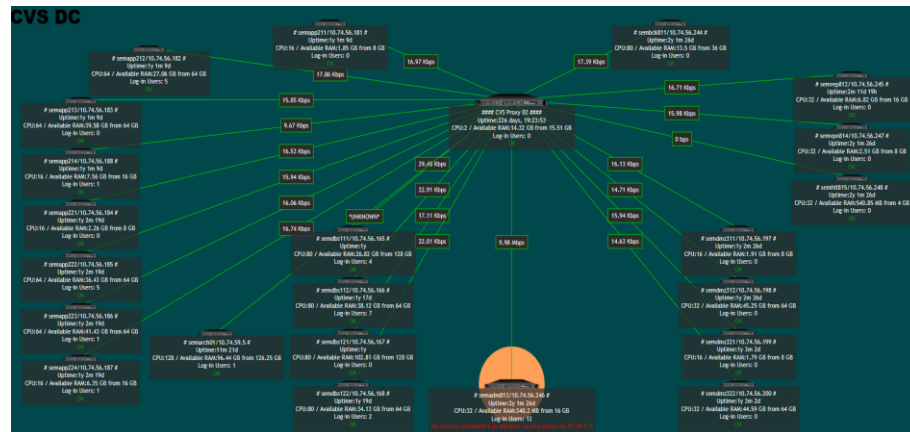
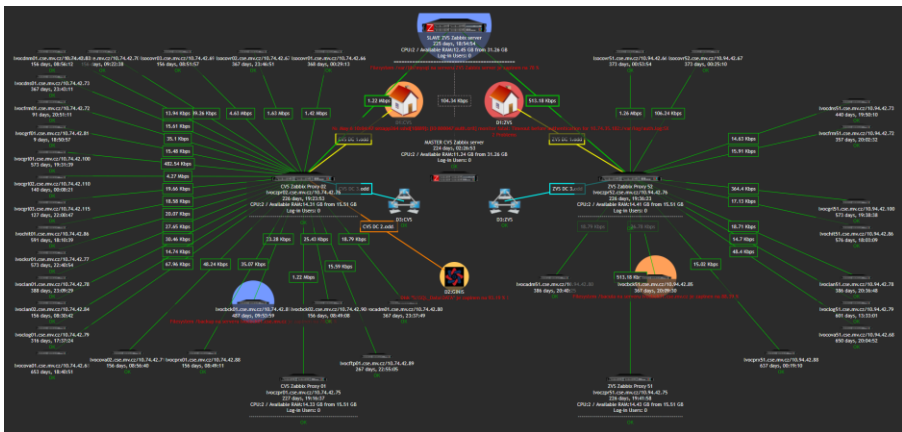


	[all]	last	min	avg	max
Memory Utilization in %	[all]	35.2691 %	35.2459 %	35.2546 %	35.2737 %
Trigger: Na serveru semapp223 je aktualne vyuzita pamet na 35.2691 % !!	[> 90]				





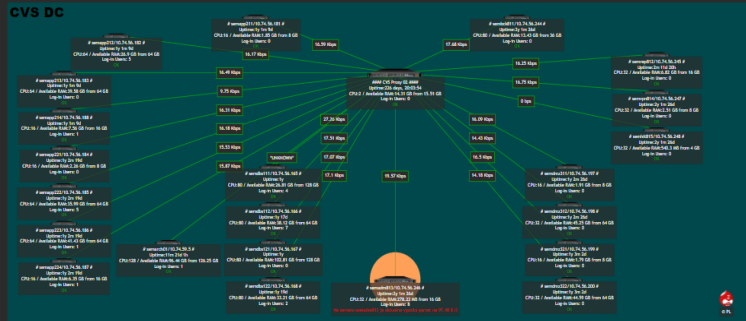
Zabbix Maps





Zabbix Dashboards

CVS OCIS Map



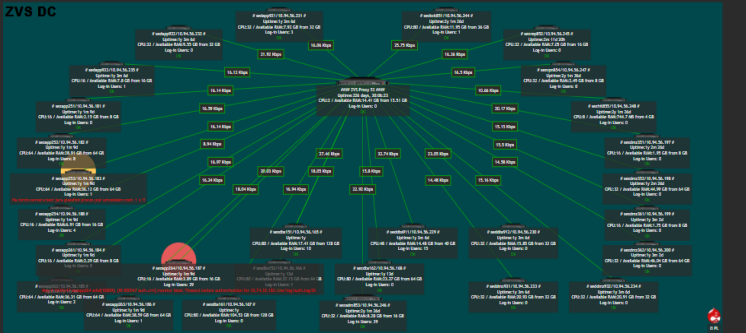
Problems by severity

Host group a	Critical	Major	Minor	Warning	Normal	Unknown
D1 OCIS Solaris Servers	1	1	1			

Problem hosts

Host group a	Without problems	With problems	Total
D1 OCIS Solaris Servers	47	3	50

ZVS OCIS Map



System information

Parameter	Value	Details
Zabbix server is running	Yes	localhost:10051
Number of hosts (enabled/disabled/templates)		
Number of items (enabled/disabled/not supported)		
Number of triggers (enabled/disabled/problem/ok)		
Number of users (online)		
Required server performance, new values per second		

Problems

Time w	Recovery time	Status	Info	Host	Problem / Severity	Duration	Ack	Actions	Tags
10:04:48		PROBLEM		sezapp264	May 6 10:04:47 sezapp264.ssh[10889]: jID:800047.auth.cri[monitor fatal]: Timeout before authentication for 10.74.35.182:/var/log/auth.log.SX	1h 13m 38s	No		Service: OS
09:55:46		PROBLEM		ZVS.Zabbix server	Filesystem /var/lib/mysql na serveru ZVS.Zabbix server je zaplnen na 78. %	1h 22m 40s	No		Service: OS
09:55:45		PROBLEM		lvocbk01.cse.mv.cz	Filesystem /backup na serveru lvocbk01.cse.mv.cz je zaplnen na 70.98 %	1h 22m 41s	No		Service: OS
09:55:28		PROBLEM		lvocbk51.cse.mv.cz	Filesystem /bacula na serveru lvocbk51.cse.mv.cz je zaplnen na 83.39 %	1h 23m	No		Service: OPER_F; Service: OS
09:54:42		PROBLEM		semadm813	Na serveru semadm813 je aktualne vyuzita pamet na 97.48 % !!	1h 23m 44s	No		Service: OS
2022-02-24 09:45:42		PROBLEM		sezapp253	Na tomto serveru bezí java glassfish proces pod uvcvatelem root. 1 x !!	2m 11d	No		Service: APP





Monitoring řešení není pouze o kvalitním monitorovacím nástroji, ale především o spolupráci všech týmů IT infrastruktury, srozumitelné definici a představě toho, co chci monitorovat.

Rozvoj a ladění monitoringu je a bude vždy postupné v závislosti na aktuálních provozních stavech a tím pádem nikdy nekončící!





MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



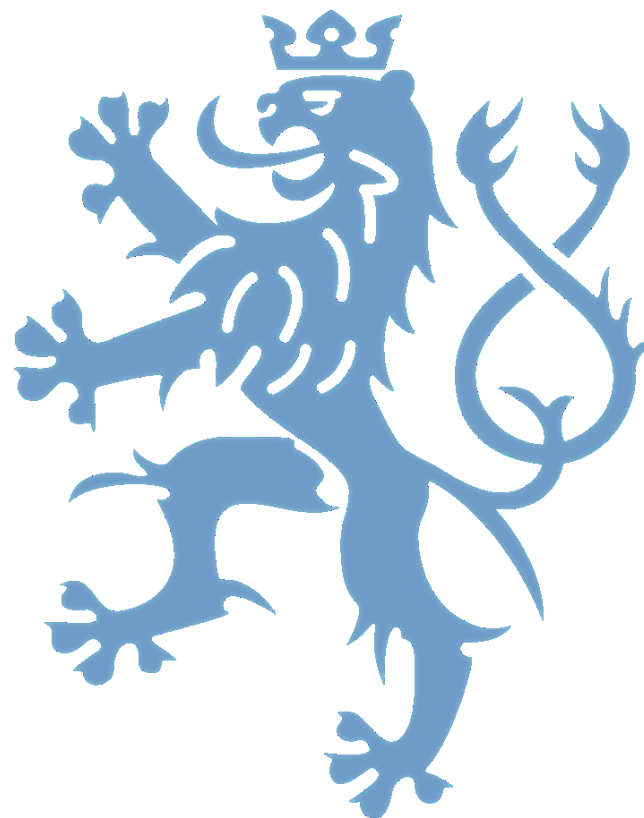
gov.cz



Centralizovaný dohled



graylog





MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



gov.cz



Obsah

- Stručný popis Graylog
- Schéma sběru dat
- Komunikační matice
- Dashboardy
- Ukázka odhalení incidentu

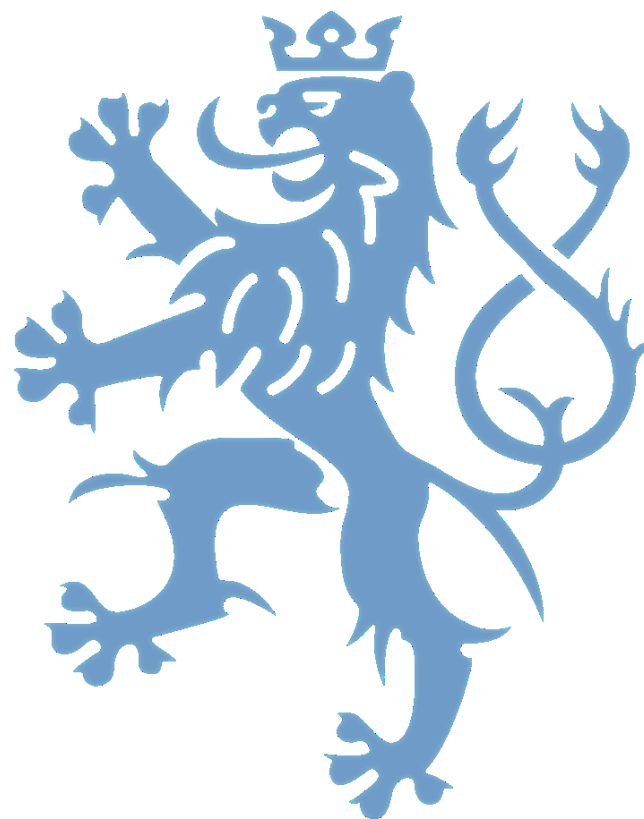
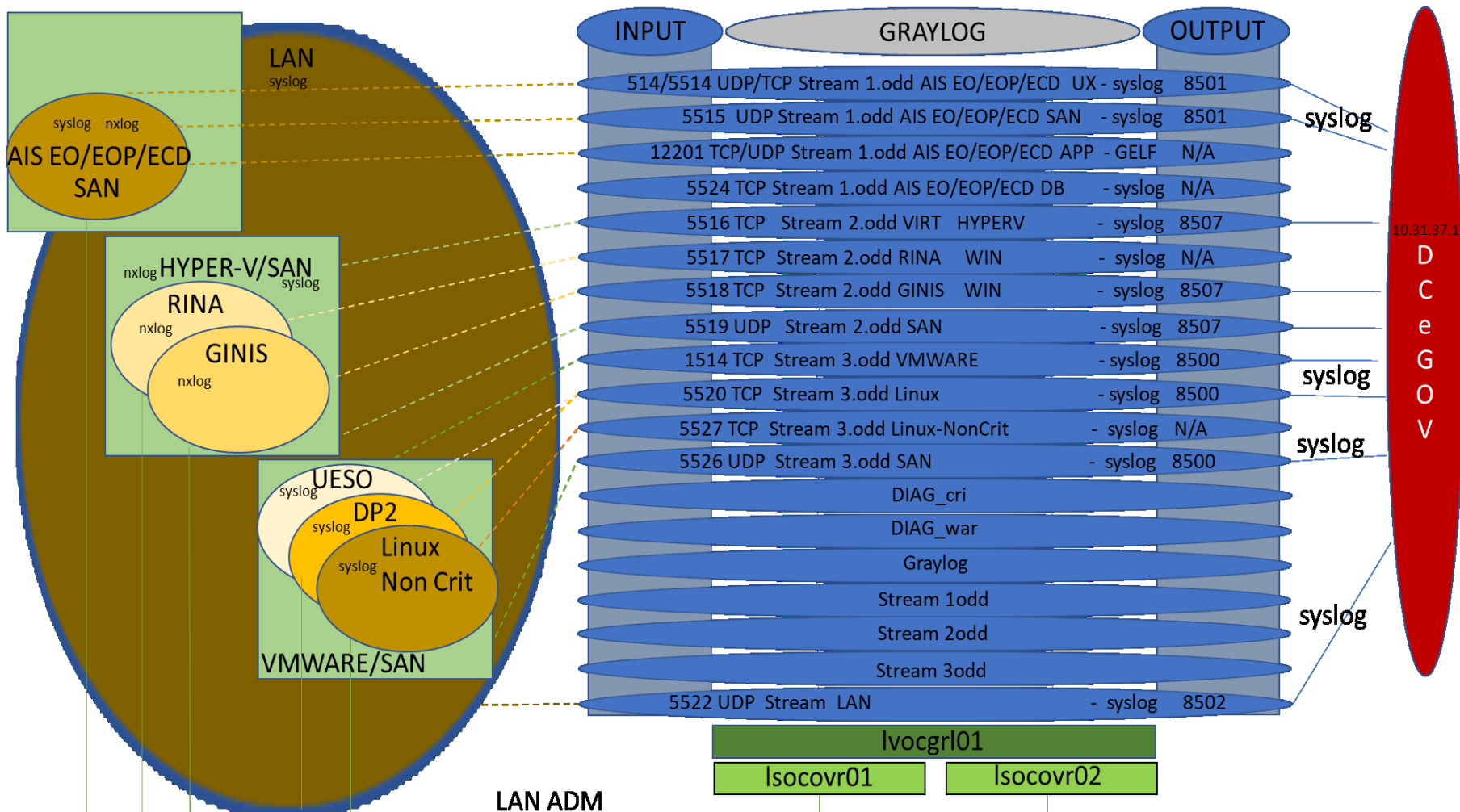
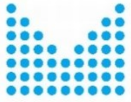


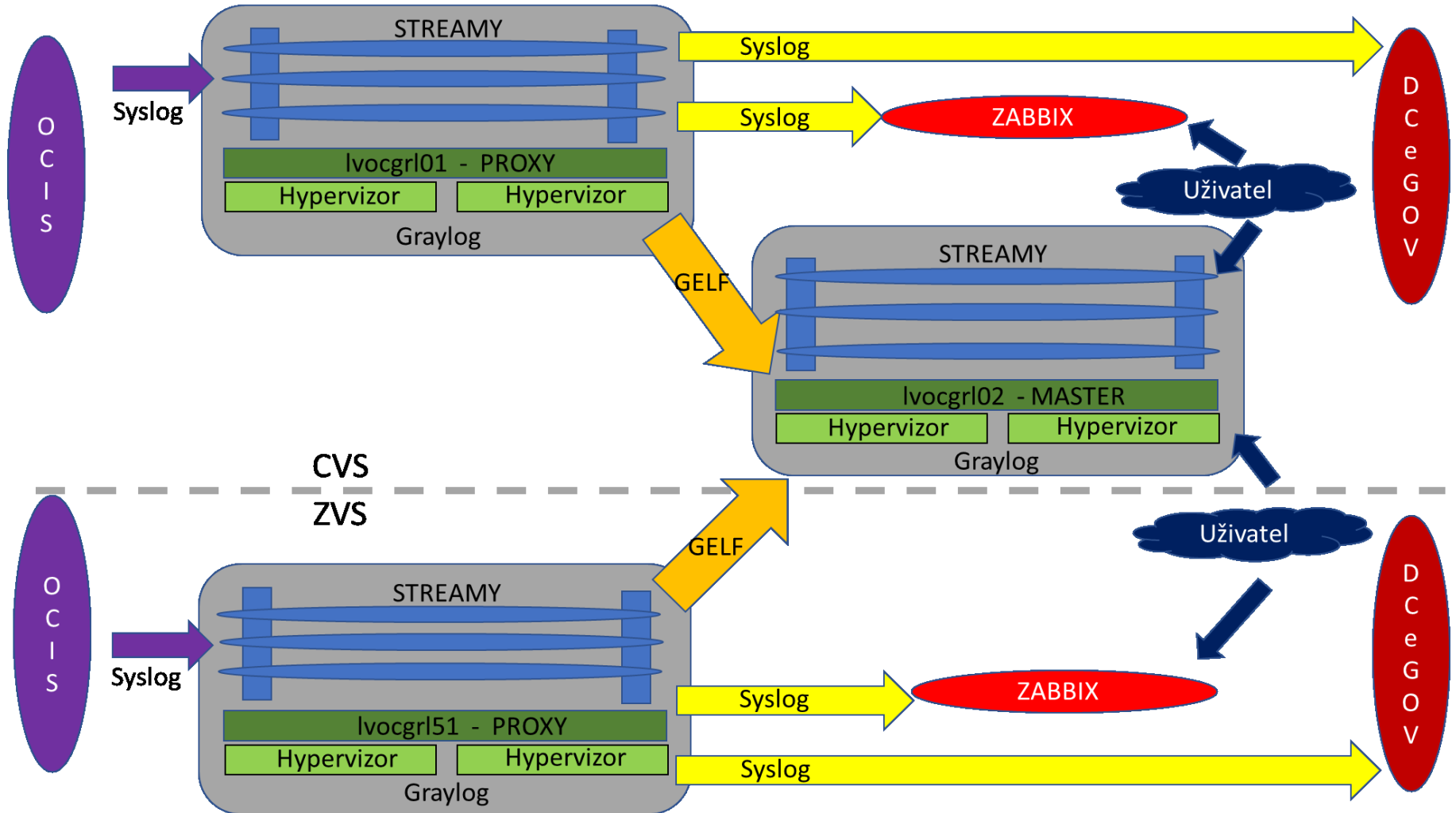


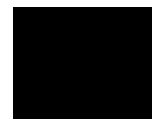
Schéma sběru dat



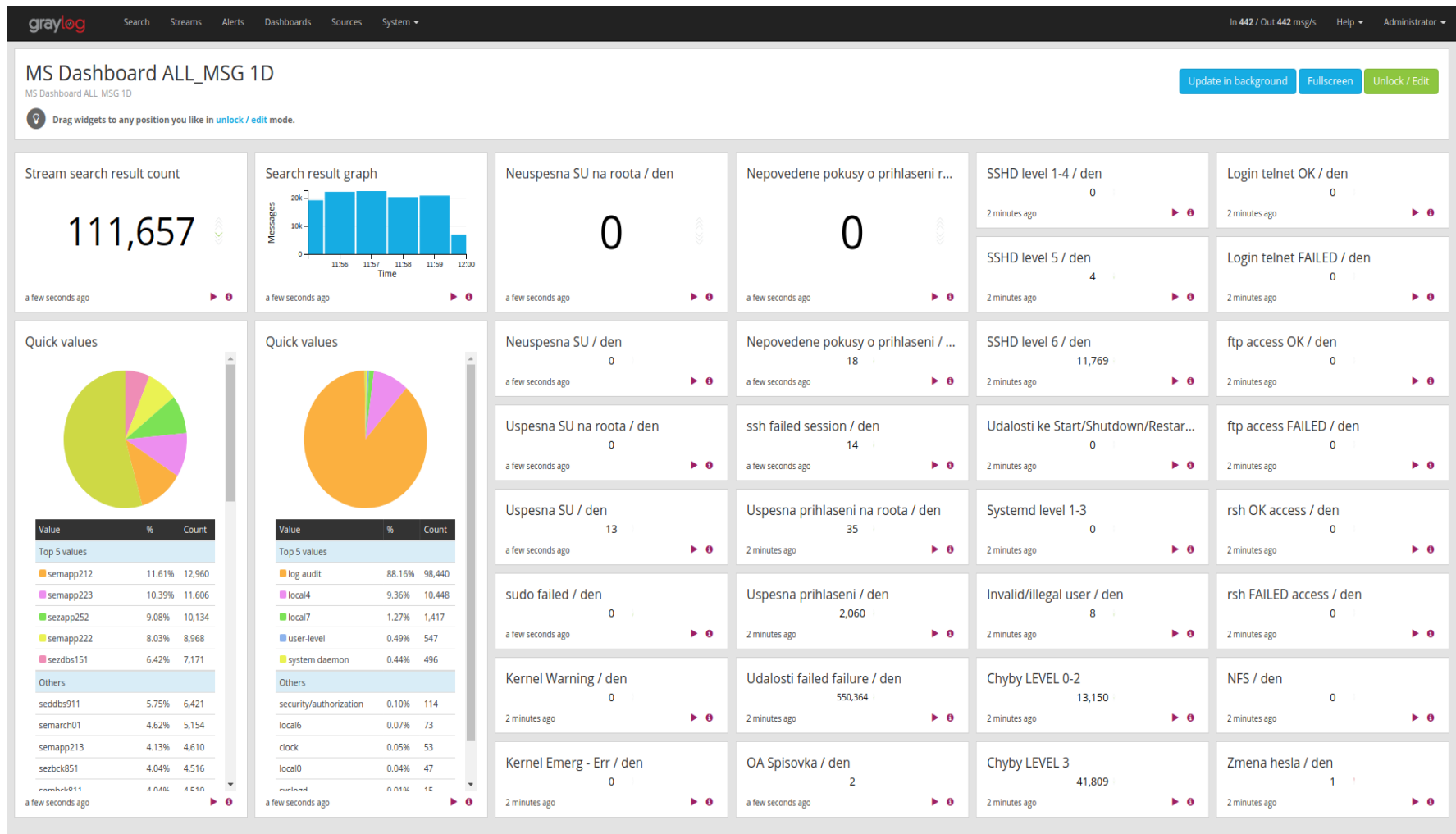


Komunikační matice





Dashboard OCIS infrastruktury





Dashboard síťových prvků

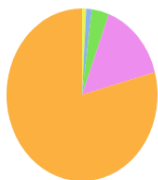
LAN_Dashboard

LAN_Dashboard

Update in background Fullscreen Unlock / Edit

Drag widgets to any position you like in [unlock / edit mode](#).

Facility



Value	%	Count
Top 5 values		
local7	79.23%	1,411
system daemon	14.99%	267
local6	3.71%	66
local0	1.18%	21
clock	0.90%	16

a few seconds ago

Zdroj zprav



Value	%	Count
Top 5 values		
fw1vso	61.26%	1,091
sw1_l	12.86%	229
lb1vso	8.25%	147
lb1vsc	7.41%	132
sw3	5.11%	91
Others		
sw101_1	2.30%	41
sw2	1.68%	30
2022	1.12%	20

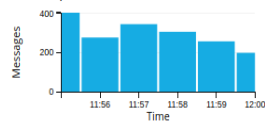
a few seconds ago

Pocet zprav / 5min

1,781

a few seconds ago

Pocet zprav / 5min



a few seconds ago

Deny_denied / 5min

381

a few seconds ago

Nejcasteji zamitnuta komunikace



Value	%	Count
Top 5 values		
10.74.56.139	43.83%	167
10.252.16.131	11.55%	44
10.94.56.139	9.19%	35
10.72.192.163	5.77%	22
10.74.96.73	5.25%	20
Others		
10.74.36.41	4.46%	17
10.72.192.161	2.89%	11
10.74.41.81	2.89%	11
10.74.59.7	2.36%	9

a few seconds ago

ACL



Value	%	Count
Top 5 values		
cvs-app-in	43.83%	167
fw1-gw1_access_in	18.64%	71
[lanadm-act-out]	13.39%	51
zvs-app-in	9.19%	35
admin-nakit-in	4.46%	17
Others		
cvs-essi-tst-in	2.89%	11
archokr-in	2.36%	9
cvs-essi-bck-in	1.84%	7
cvs-essi-bck-out	1.05%	4

a few seconds ago



Ukázka odhalení incidentu

The screenshot displays the Graylog web interface. At the top, there is a navigation bar with 'graylog' and menu items: Search, Streams, Alerts, Dashboards, Sources, System. On the right, it shows 'In 345 / Out 345 msg/s', 'Help', and 'Administrator'. Below the navigation bar is a search bar with a date range from '2022-03-02 17:34:57' to '2022-03-02 21:40:22'. A search query is entered: 'Type your search query here and press enter. (*not found* AND http) OR http_response_code:[400 TO 404]'. The main content area is divided into two panels. The left panel, titled 'Stream LAN', shows 'Found 40,411 messages in 95 ms, searched in 67 indices. Results retrieved at 2022-05-04 12:33:23.' It includes buttons for 'Add count to dashboard', 'Save search criteria', and 'More actions'. Below this is a 'Fields' and 'Decorators' section with a list of fields including facility, forwarder, GraylogName, GraylogTime, GraylogTime1, HOSTNAME, HOUR, id, level, message (checked), MINUTE, MONTH, MONTHDAY, SECOND, source (checked), SYSLOGTIMESTAMP, TIME, and timestamp. The right panel, titled 'Histogram', shows a bar chart of message counts over time. A tooltip indicates '155 messages Wednesday 2 March 2022, 18:12 +0100'. Below the histogram is a 'Messages' section with a table of search results. The table has columns for 'Timestamp' and 'source'. The messages are all from 'fw/vsso' and contain the same log entry: '%ASA-4-106023: Deny tcp src *gw1-fw-hvs:10.85.43.14/40385 dst sw1_1-fw-hvs:10.74.41.255/21 by access-group *fw1-gw1_access_in* [0x0, 0x0]'. The messages are timestamped at 2022-03-02 20:53:11.000, 2022-03-02 20:53:05.000, and 2022-03-02 20:53:03.000.



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

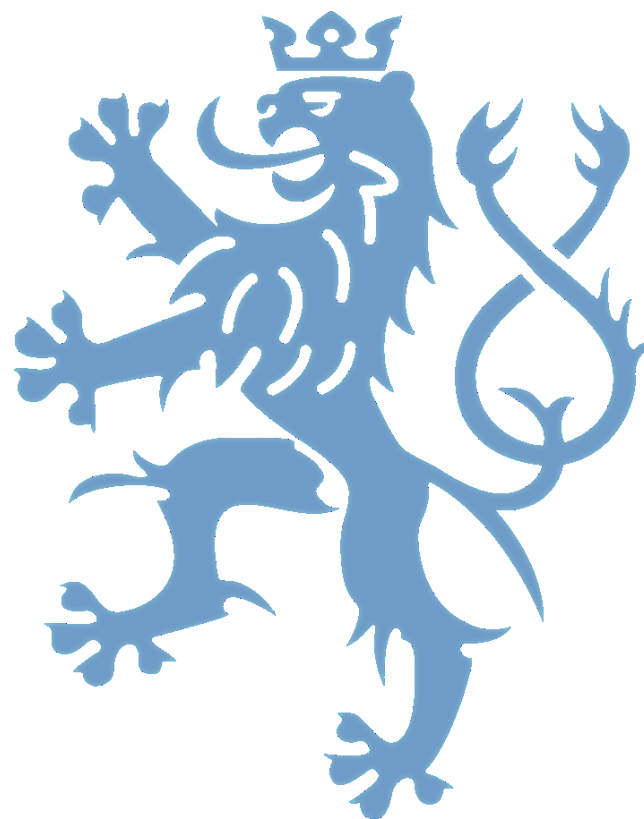


gov.cz



Centralizovaný systém evidence
(provozní deník, centrální místo dokumentace,
seznamu HW a SW) OCIS IT infrastruktury

Glpi





MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

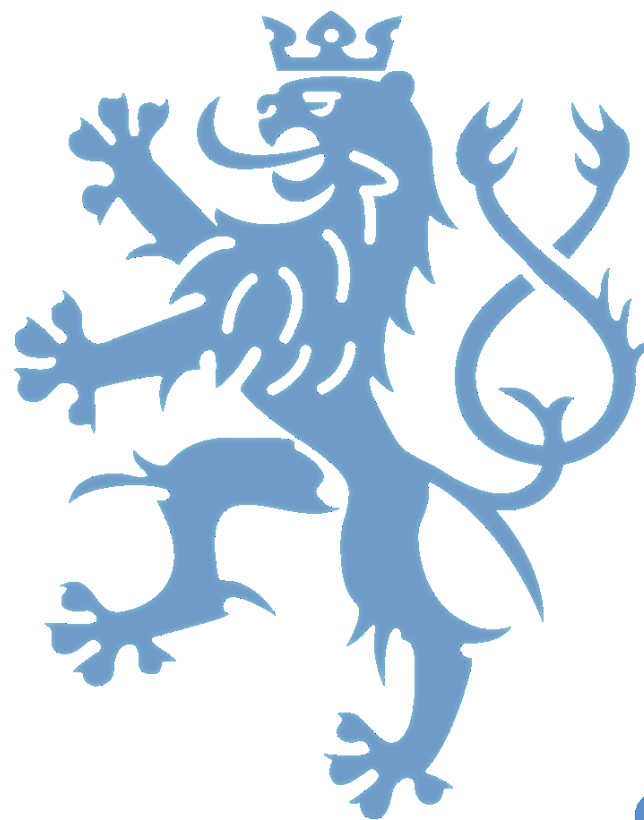


gov.cz



Obsah

- Stručný popis Glpi
- Provozní deník
- Depot dokumentace
- Seznam HW/SW
- Propojení s monitoringem





Popis Glpi

➤ **Open Source Software**

- Přizpůsobení dle vlastních potřeb
- Podporuje další nástroje a pluginy

➤ **Nástroj pro management a správu IT**

- Inventář HW/SW a všech přidružených komponent s maximální provázaností
- Depot dokumentace

➤ **Možnost nastavení entit**

- Právo vidět jen to, co spravuji, neboli omezit viditelnost datových zdrojů pro skupiny, uživatele či mezi organizačními jednotkami
- Jednoduché přidání další entity

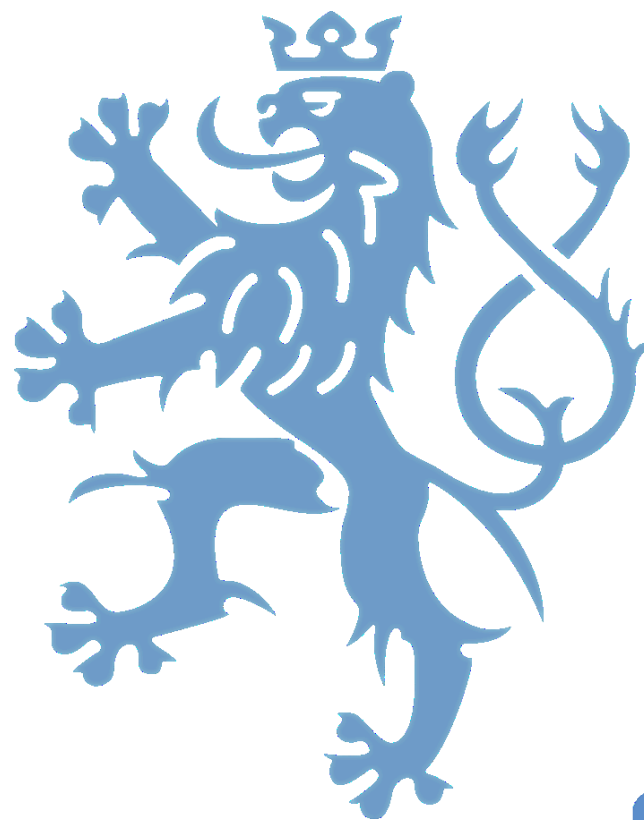


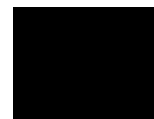


Provozní deník

➤ **U každé poznámky je smluvený TAG, značka**

- ZMENA (veškeré změny infrastruktury)
- VZMENA (významná změna infra)
- PORUCHA (porucha a opravy)
- INFO (ostatní informace)





Počítač	
Operační systémy	1
Komponenty	5
Svazky	
Software	1
Připojení	
Síťové porty	8
Smlouva	
Dokumenty	1
Virtualizace	
Antiviry	
Databáze znalostí	1
Požadavky	
Problémy	
Změny	
Odkazy na vnější zdr...	
Certifikáty	
Poznámky	16
Historie	96
Tasks / Groups	
Databáze	
Vše	

- ZABBIX ZMENA:** Posledně změnil **zabbix** v 2021-06-21 10:37 / Vytvořil **zabbix** v 2021-06-21 10:37

ADMIN: pridan lun do cvdopdg
- Jun 21 10:00:59 semdbs111 vxvm:vxconfigd: [ID 702911 daemon.notice] V-5-1-18928 config_enable_copy: enable config copy hitachi_vspgxo_041a:/var/adm/messages:C:5X
- ZMENA:** Posledně změnil **Krmenčík Václav** v 2021-05-08 11:21 / Vytvořil **Krmenčík Václav** v 2021-05-08 11:21

Patchování a test funkčnosti cluster řešení
- ZMENA:** Posledně změnil **Šindelář Jiří** v 2021-04-28 11:54 / Vytvořil **Šindelář Jiří** v 2021-04-28 11:54

- přidána routa pro zálohování CROISZR na lvocgrl02bck
route -p add 10.74.42.192/26 10.74.58.1
- informix klíč přenesen na informix@lvocgrl02bck
- INFO:** Posledně změnil **Muller David** v 2021-03-12 14:20 / Vytvořil **Muller David** v 2021-03-12 12:40

Destination Mask Gateway Interface
default 0.0.0.0 10.74.56.1 0
10.74.36.16 255.255.255.240 10.74.56.161 0
10.74.39.128 255.255.255.192 10.74.39.140 instalace1
10.74.40.0 255.255.255.0 10.74.56.161 0
10.74.42.64 255.255.255.192 10.74.56.161 0
10.74.56.0 255.255.255.192 10.74.56.16 db1
10.74.56.0 255.255.255.192 10.74.56.18 db1
10.74.56.0 255.255.255.192 10.74.56.19 db1
10.74.56.0 255.255.255.192 10.74.56.24 db1
10.74.56.0 255.255.255.192 10.74.56.22 db1
10.74.56.0 255.255.255.192 10.74.56.23 db1
10.74.56.0 255.255.255.192 10.74.56.21 db1
10.74.56.0 255.255.255.192 10.74.56.17 db1
10.74.56.0 255.255.255.192 10.74.56.20 db1
10.74.56.0 255.255.255.192 10.74.56.14 db1
10.74.56.0 255.255.255.192 10.74.56.8 db1
10.74.56.160 255.255.255.240 10.74.56.165 adm_db1
10.74.57.0 255.255.255.240 10.74.57.5 repo_db1
10.74.57.80 255.255.255.240 10.74.57.85 service_db1
10.74.58.0 255.255.255.192 10.74.58.16 backup_db1
10.74.58.0 255.255.255.192 10.74.58.18 backup_db1
10.74.58.0 255.255.255.192 10.74.58.19 backup_db1
10.74.58.0 255.255.255.192 10.74.58.24 backup_db1
10.74.58.0 255.255.255.192 10.74.58.22 backup_db1
10.74.58.0 255.255.255.192 10.74.58.23 backup_db1
10.74.58.0 255.255.255.192 10.74.58.21 backup_db1
10.74.58.0 255.255.255.192 10.74.58.17 backup_db1
10.74.58.0 255.255.255.192 10.74.58.20 backup_db1
10.74.58.0 255.255.255.192 10.74.58.8 backup_db1
10.74.58.192 255.255.255.240 10.74.58.1 0
10.94.58.192 255.255.255.240 10.74.58.1 0
169.254.182.0 255.255.255.0 169.254.182.77 net8
- ZMENA:** Posledně změnil **Šindelář Jiří** v 2021-03-01 15:38 / Vytvořil **Šindelář Jiří** v 2021-03-01 15:38

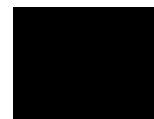
- přidána routa pro zálohování serveru do ZVS
route -p add 10.94.58.192/28 10.74.58.1
- změna zálohování na BS do ZVS



Depot dokumentace

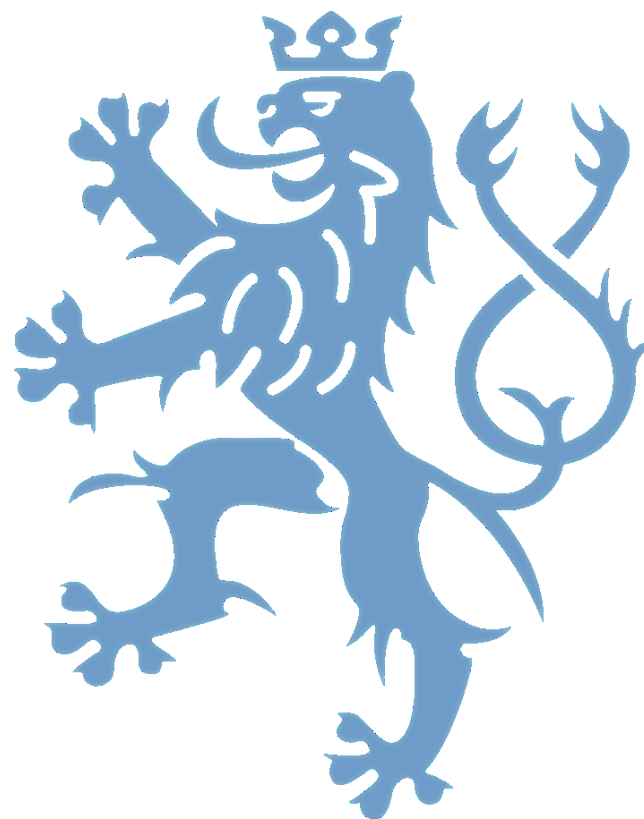
- **Glpi nám slouží i jako skladiště všech dokumentů IT infrastruktury**
 - Opět rozděleno dle entit – každé odd. vidí jen to svoje
- **Ukládáme nejenom dokumenty týkající se HW/SW, projektů, ale i např.:**
 - Výkazy práce
 - Antigenní testy
 - Pohotovosti/dosahy a další

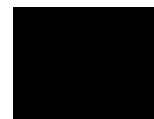




Seznam HW/SW

- **Evidence veškeré IT infrastruktury**
 - Servery / VM
 - SW / Appl
 - Databáze
 - Síťová zařízení
 - Další HW jako racky, disková pole ...





Počítač

Operační systémy 1

Komponenty 11

Svazky

Software 5

Připojení

Síťové porty 10

Smlouva

Dokumenty 3

Virtualizace

Antiviry

Databáze znalostí 1

Požadavky

Problémy

Změny

Odkazy na vnější zdr...

Certifikáty

Poznámky 41

Historie 173

Tasks / Groups

Databáze 9

Vše

Software ----- i

Nainstalovat

Software

Kategorie Všechny kategorie i

Zobrazit (počet položek) 50

Od 1 do 5 z 5

↓ Akce

	Název	Stav	Verze	Licence	Datum instalace	Automatizovaná inventarizace	Kategorie software	Platná licence
<input type="checkbox"/>	Informix	PROD	10			Ne	Database	Ano
<input type="checkbox"/>	Informix	PROD	12			Ne	Database	Ano
<input type="checkbox"/>	Informix	PROD	9.40.FC3			Ne	Database	Ano
<input type="checkbox"/>	Veritas InfoScale Enterprise		7.3.0.0			Ne	Volume manager + Cluster	Ano
<input type="checkbox"/>	Zabbix Agent		4.0.13			Ne	Dohled	Ano

↑ Akce

Licence

Licence -----

Přidat

Nebyla nalezena žádná položka



Propojení Glpi se Zabbixem

➤ Řetězec „GLPI“

- Domluvený řetězec díky němuž se CRITICAL Zabbix hláška, eskalovaná k operátorům OCIS, automaticky propíše do Glpi
- Usnadnění administrativy pro jednotlivé správce





Propojení Glpi se Zabbixem

Message

History

Time	User	User action	Message
2022-05-03 14:21:41	js600815 (Jiri Sindelar)	✓	GLPI - během obnovy instance došlo v NBU k uvolnění staging area - NBU bug
2022-04-29 21:09:33	js600815 (Jiri Sindelar)	✓	restore dokončen

Scope

Only selected problem

Selected and all other problems of related triggers 1 event

Change severity Unknown Normal Warning Minor Major Critical

Acknowledge

Close problem

* At least one update operation or message must exist.





Propojení Glpi se Zabbixem



semdb122 (MVCR OCIS > 1. odd OCIS)

6/11 > >

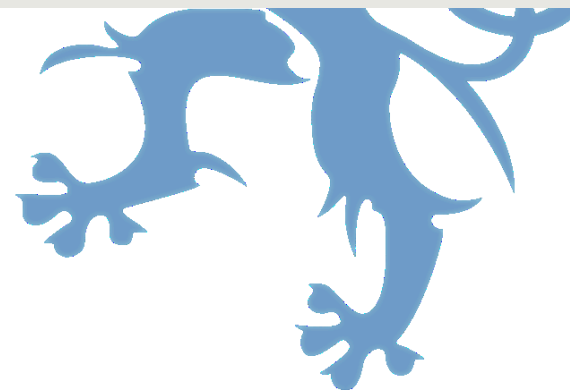
Přidat



ZABBIX ZMENA:

Posledně změnil **zabbix** v 2022-05-03 14:21 / Vytvořil **zabbix** v 2022-05-03 14:21

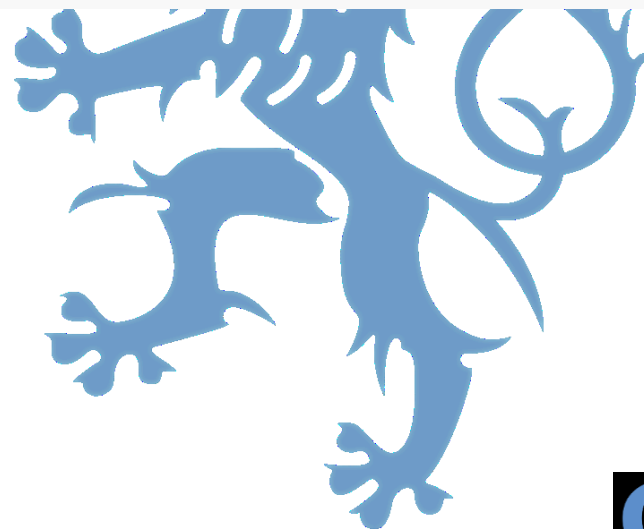
- GLPI
- během obnovy instance došlo v NBU k uvolnění staging area
- NBU bug
- /export/home/informix/netbackup/ids_restore.sh : KONEC obnovy CVDCD do semdb122cvdcctcp: CHYBA (Nevolat, vyresi SUN-OS v pracovni dobe):ITO_ERR.log ids_restore





Propojení Glpi se Zabbixem

<input type="checkbox"/> CSI: 23459119	MVCR OCIS > 1. odd OCIS	CSI	2021-03-08	36 měsíce	Servery pro Archiv okresů Centrotex
<input type="checkbox"/> Nákup 12.12.2017	MVCR OCIS	Archiv	2017-12-12	36 měsíce	3.odd : MSA + vsochyp02 + vsochyp52
<input type="checkbox"/> Smlouva ALWIL 3.odd	MVCR OCIS	support	2019-08-27	36 měsíce	Servery, Racky, Switche a Pole pro 3. odd Smlouva ALWIL - MV-94000-4/SIK6-2019 platí do 27.8.2022
<input type="checkbox"/> Smlouva ARCHIV OKRESŮ - MV-185902-25/VZ-2020	MVCR OCIS > 1. odd OCIS	support	2021-03-08	36 měsíce	Smlouva ARCHIV OKRESŮ - MV-185902-25/VZ-2020 platí do 8.3.2024
<input type="checkbox"/> Smlouva COMSYS - MV-139803-26/VZ-2020	MVCR OCIS > 1. odd OCIS	support	2020-12-23	60 měsíce	Podpora COMSYS-Oracle CVS ZVS platí do 23.12.2025
<input type="checkbox"/> Smlouva DATASYS - MV-26107-35/OPF-2020	MVCR OCIS > 1. odd OCIS	support	2020-06-25	36 měsíce	Smlouva DATASYS - MV-26107-35/OPF-2020 platí do 25.6.2023

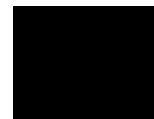




MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

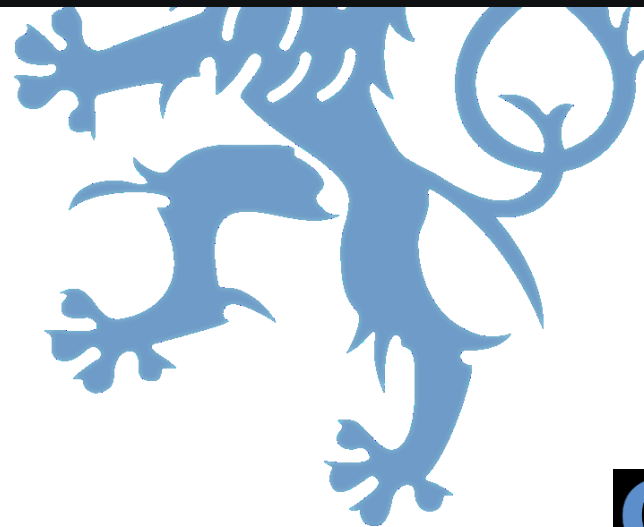


gov.cz



Propojení Glpi se Zabbixem

<input type="checkbox"/>	Severity	Recovery time	Status	Info	Host	Problem
<input type="checkbox"/>	Critical		PROBLEM		lvocksr01.cse.mv.cz	Support smlouva "support Alwil 3.odd" (Savery, Racky, Switche a Pole pro 3. odd) vyprsi za 4 mesicu!



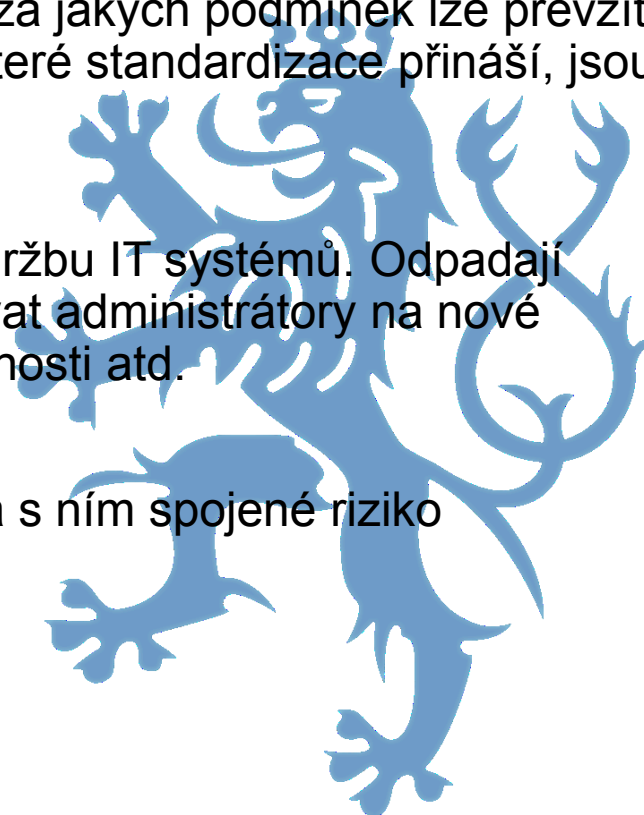


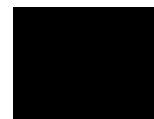
Technické a provozní standardy

Standardizace je jednou z klíčových podmínek pro dosažení garantované kvality a udržitelné ceny provozu IT Infrastruktury. Z tohoto důvodu má Odbor centrálních informačních systémů (OCIS) vypracované technické, provozní a bezpečnostní standardy, ve kterých je uvedeno, za jakých podmínek lze převzít HW, OS, aplikace atd. do jeho správy. Výhody, které standardizace přináší, jsou převážně v ochraně investic

Dodržováním standardů se snižují náklady na údržbu IT systémů. Odpadají problémy s nekompatibilitou, není třeba zaškolovat administrátory na nové technologie, udržuje se vysoký stupeň zastupitelnosti atd.

Absence standardů zvyšuje různorodost řešení a s ním spojené riziko komplikací, vícenákladů a časových ztrát.

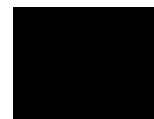




Řídící dokumenty

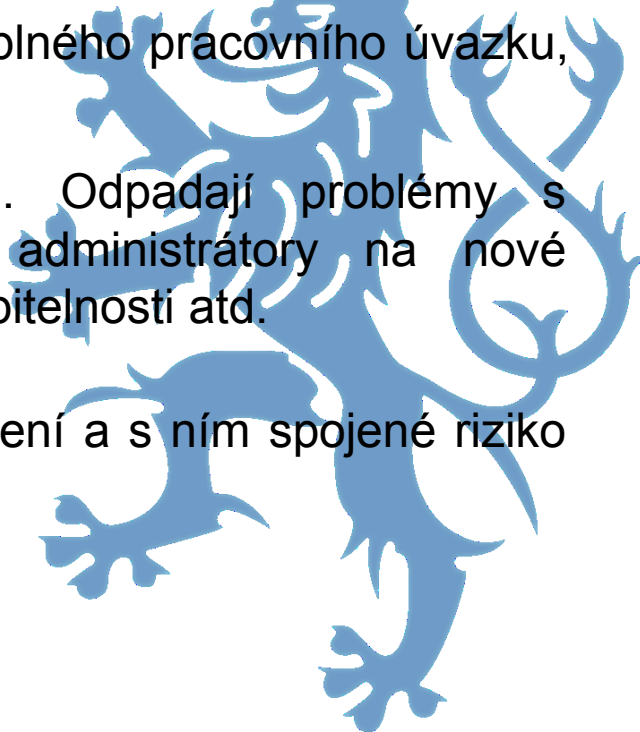
- Metodika postupu implementace prostředí do infrastruktury.
- Schválená konfigurace hardware a software.
- Bezpečnostní politiky, monitoring a dohled.





Finanční benefity

- ❑ Není potřeba investic do OS, licencí a SW pro monitoring a dohled. Přebíraná infrastruktura bude automaticky napojena na centrální dohledové, monitorovací a podpůrné systémy OCIS a zároveň je zajištěno napojení na dohledový systém DCeGOV. Konfiguraci a instalaci potřebných agentů provádí IT specialisté OCIS/NAKIT, s.p.
- ❑ Úspora na náboru dalších FTE (Ekvivalent plného pracovního úvazku, lidské práce).
- ❑ Snižují náklady na údržbu IT systémů. Odpadají problémy s nekompatibilitou, není třeba zaškolovat administrátory na nové technologie, udržuje se vysoký stupeň zastupitelnosti atd.
- ❑ Absence standardů zvyšuje různorodost řešení a s ním spojené riziko komplikací, vícenákladů a časových ztrát.





Směrování OCIS infrastruktury

- Dokončit centralizaci a konsolidaci
- Prevence vendor lock-in
- Využívat open source produkty tam, kde to umožňuje zákon





MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



gov.cz



Hyper-V
Windows
x86

Bez VM

Vmware
Linux
x86

Oracle VM for SPARC
Oracle Sun Sparc

Backup server
Oracle Sun Sparc

oVirt
Monitoring dohled
x86

LAN
konsolidace



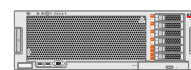
APP
TST



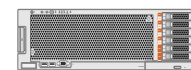
DB



APP
TST



DMZ



Škálovatelné
(např. HP, Dell)

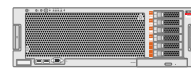
Škálovatelné
(např. HP, Dell)

Škálovatelné
(např. HP, Dell)

APP

Příprava na
konsolidaci záloh

Škálovatelné
(např. HP, Dell)



DB

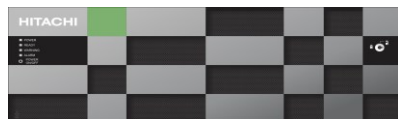


DEV/TST

Storage

SAN
konsolidovaná

Storage
konsolidovaná



LTO knihovna



FLEX
appliance



Škálovatelné



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



gov.cz



Závěr

Děkujeme za pozornost

V případě zájmu o detailnější technické a provozní informace jsme k dispozici



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Ing. František Varmuža



Václav Krměčık, Pavel Lejsek, Martin Svárovský

