initMAX

Webinar

Advanced Windows monitoring

all our microphones are muted

ask your questions in Q&A, not in the Chat

use Chat for discussion, networking or applause

initMAX

Advanced Windows monitoring

Windows server

- Out of the Box monitoring
- Agent extension
- What?
- How?

Advanced Windows monitoring

Agenda

Out of the box Windows items and templates

- Windows registry
- Performance counters
- Scripts

Windows Services and applications

- Active Directory
- DHCP
- DNS
- MSSQL
- Exchange server
- And more …

1

Out of the box

Windows Out-of-the-box templates

OS Templates

- Windows by Zabbix agent
- Windows by Zabbix agent active
- Windows SNMP
- Agent less monitoring

Microsoft APP Templates

- MSSQL by ODBC
- MSSQL by Zabbix agent 2
- Exchange server
- IIS server
- Sharepoint server

Tested versions

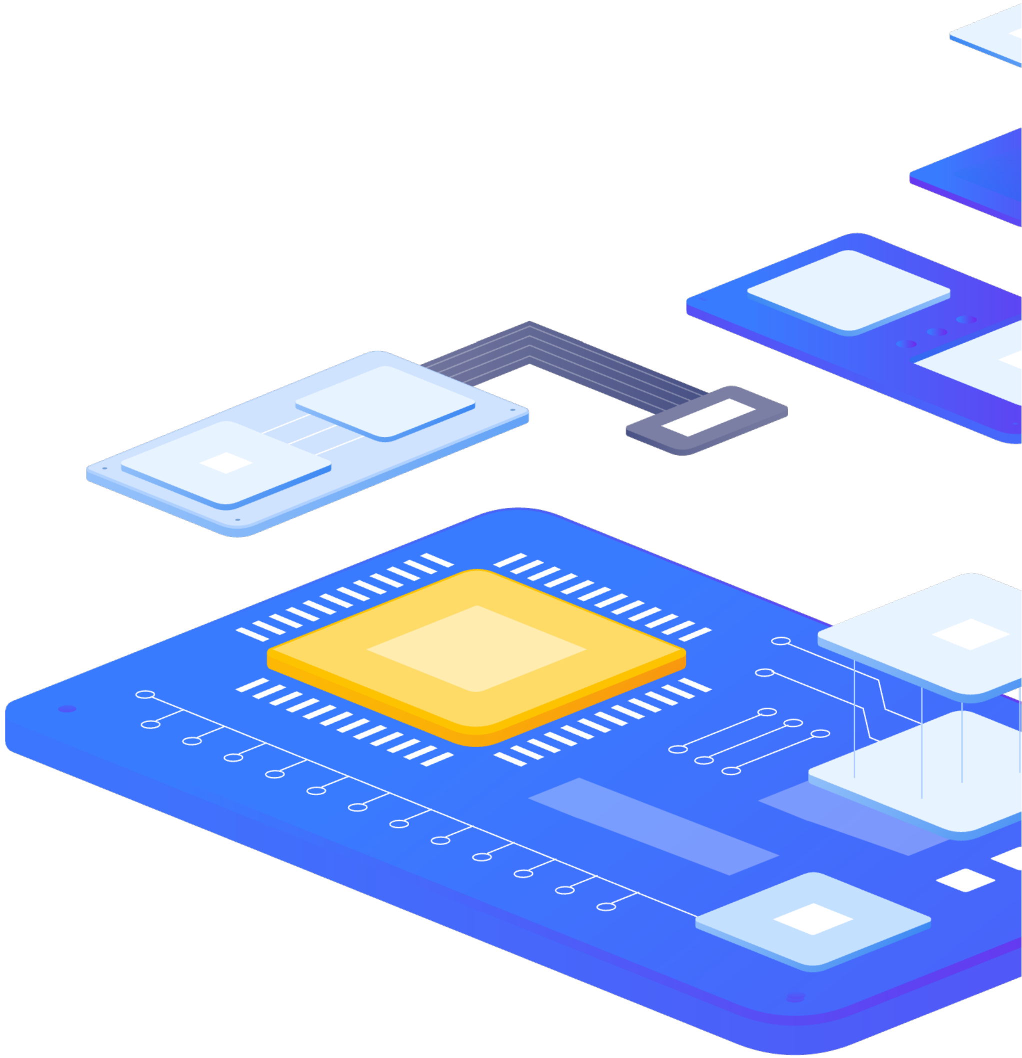
- Windows 10 and newer.
- Windows Server 2016 and newer.

Advanced Windows monitoring

Windows by Zabbix agent

Components

- Availability
- Performance
- Security
- Inventory



Advanced Windows monitoring

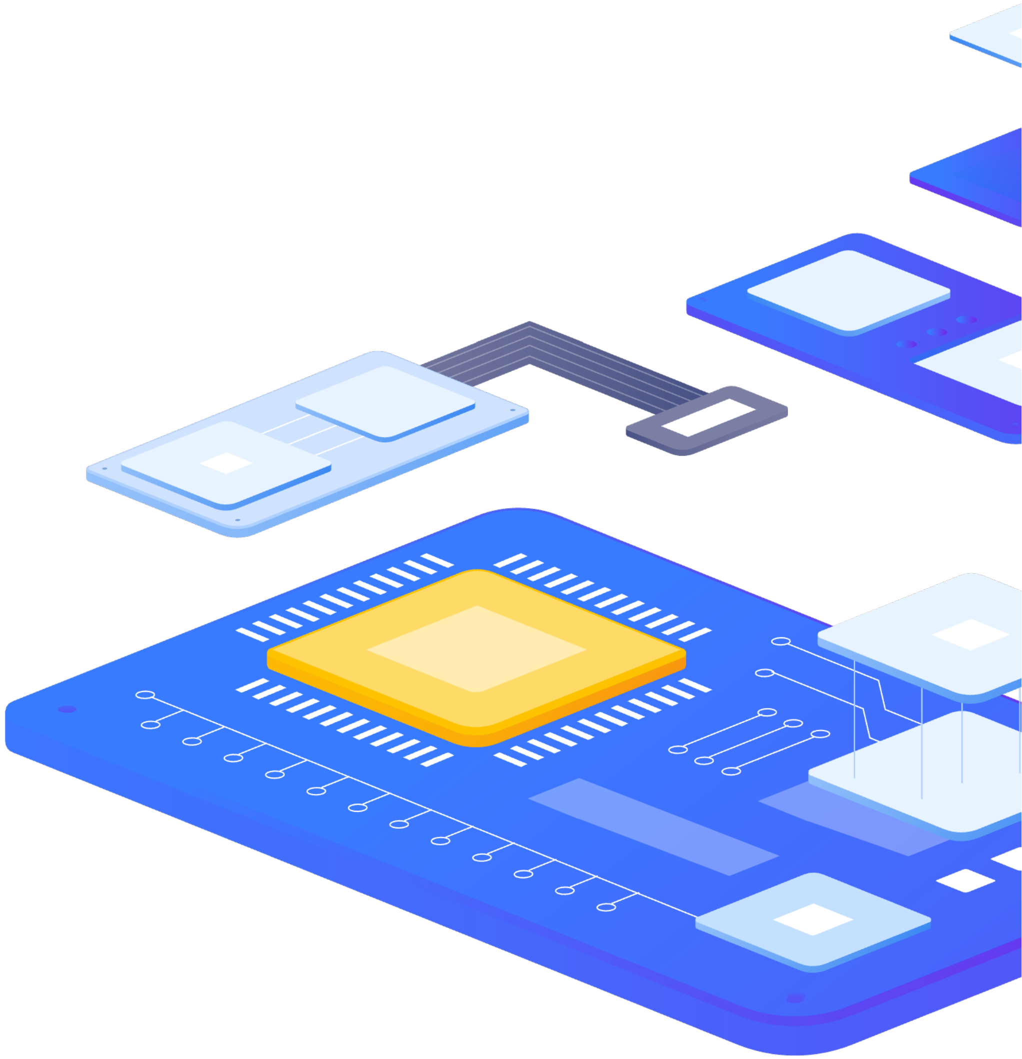
Windows by Zabbix agent

Performance

- CPU
- Memory
- Processes
- Filesystems
- Network interfaces
- Physical disks
- Windows Services

Inventory

- OS info
- Agent info



Zabbix agent(2) for windows - items

Windows-specific items

Eventlog	The Windows event log monitoring.	Log monitoring
net.if.list	The network interface list (includes interface type, status, IPv4 address, description).	Network
perf_counter	The value of any Windows performance counter.	Performance counters
perf_counter_en	The value of any Windows performance counter in English.	
perf_instance.Discovery	The list of object instances of Windows performance counters.	
perf_instance_en.discovery	The list of object instances of Windows performance counters, discovered using the object names in English.	
proc_info	Various information about specific process(es).	Processes
registry.data	Return data for the specified value name in the Windows Registry key.	Registry
registry.get	The list of Windows Registry values or keys located at given key.	
service.discovery	The list of Windows services.	Services
service.info	Information about a service.	
services	The listing of services.	
vm.vmemory.size	The virtual memory size in bytes or in percentage from the total. Virtual memory	
wmi.get	Execute a WMI query and return the first selected object.	WMI
wmi.getall	Execute a WMI query and return the whole response.	

Zabbix agent(2) for windows - items

Performance counters

- Windows Performance Counters provide a high-level abstraction layer that provides a consistent interface for collecting various kinds of system data such as CPU, memory, and disk usage.

perf_counter

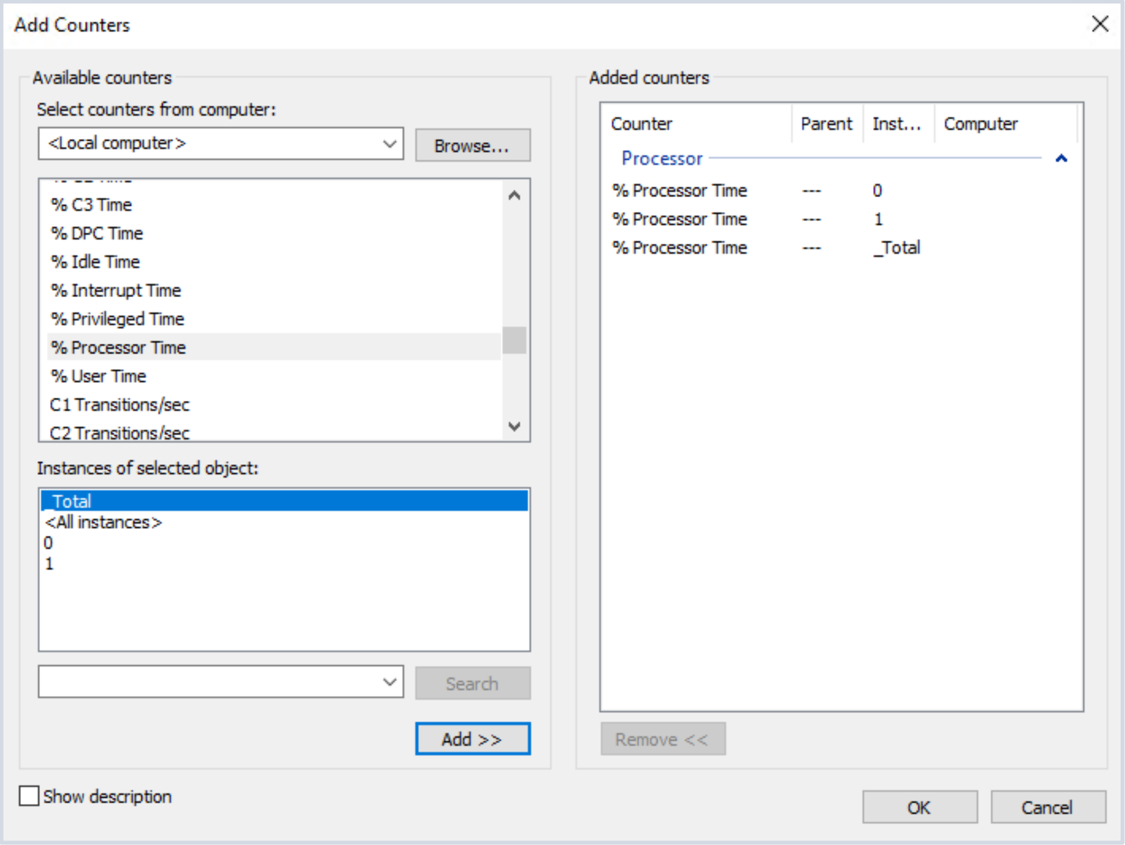
- perf_counter- The value of performance counter.
- perf_counter_en

perf_instance.Discovery

- perf_instance.Discovery - The list of object instances.
- perf_instance_en.discovery

List Performance Counters on server

- TypePerf.exe -q > counters.txt



Counter	Parent	Inst...	Computer
Processor			
% Processor Time	---	0	
% Processor Time	---	1	
% Processor Time	---	_Total	

Windows Out-of-the-box items

Windows Management Instrumentation - WMI

- Windows Management Instrumentation (WMI) is the infrastructure for management data and operations on Windows-based operating systems.

Tools:

- SimpleWMIView
- Powershell

Zabbix Items:

- wmi.get
- wmi.getall

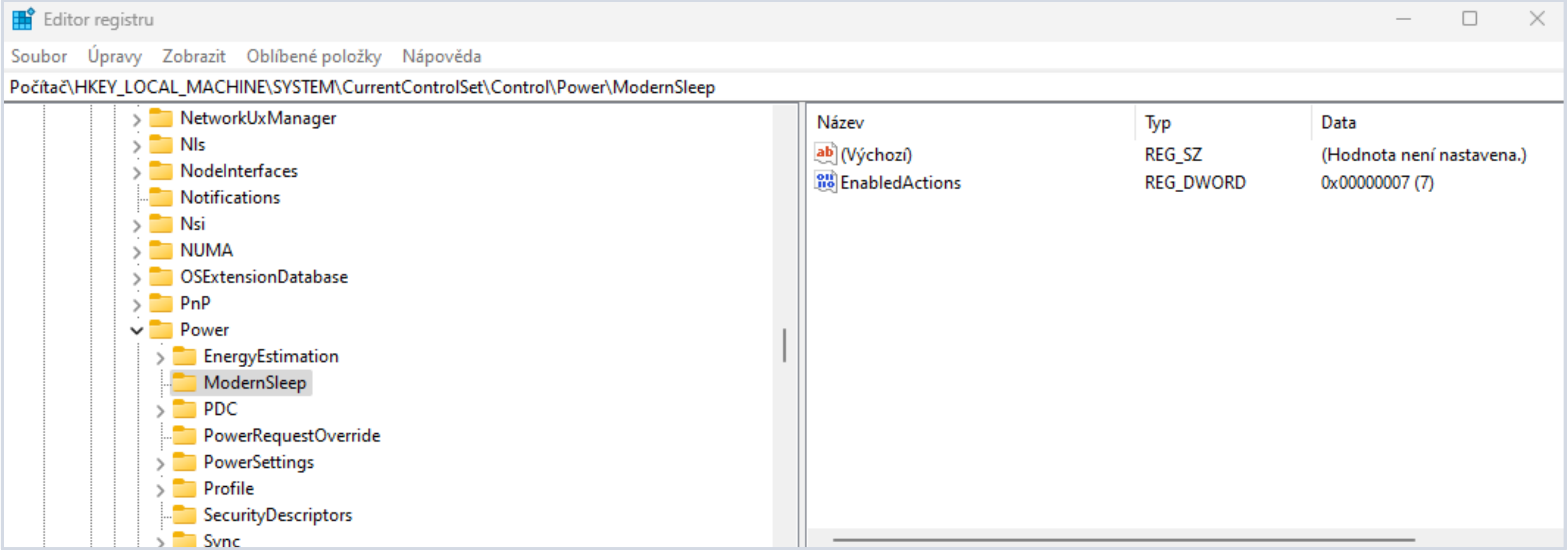
```
Get-WmiObject -Namespace root/cimv2 -Query "SELECT Name,UserName,Manufacturer
FROM Win32_ComputerSystem"
```

Advanced Windows monitoring

Windows Out-of-the-box items

Registry

- A central hierarchical database used in systems to store information that is necessary to configure the system for one or more users, applications, and hardware devices.
- registry.data
- registry.get



Počítač\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\ModernSleep

NetworkUxManager
Nls
NodeInterfaces
Notifications
Nsi
NUMA
OSExtensionDatabase
PnP
Power
EnergyEstimation
ModernSleep
PDC
PowerRequestOverride
PowerSettings
Profile
SecurityDescriptors
Sync

Název	Typ	Data
(Výchozí)	REG_SZ	(Hodnota není nastavena.)
EnabledActions	REG_DWORD	0x00000007 (7)

Windows Out-of-the-box template tunning

Timing

- Update Interval
- Discovery intervals

Throttling

- Discard Unchanged
- Discard Unchanged with Heartbeat

History and Trends

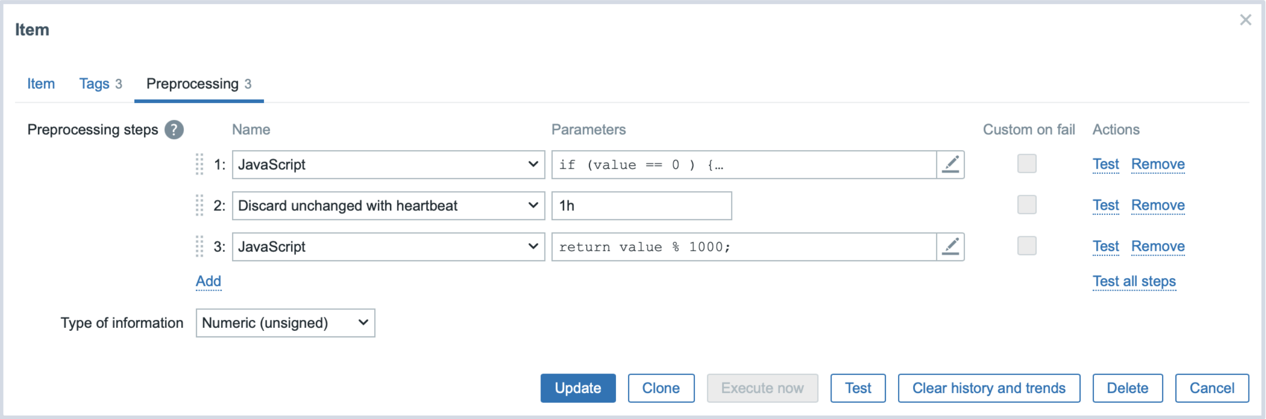
- History storage period
- Trend Storage

Advanced Windows monitoring

Windows Out-of-the-box template tunning

Throttling

- Throttling Services



Item

Item | Tags 3 | Preprocessing 3

Preprocessing steps

	Name	Parameters	Custom on fail	Actions
1:	JavaScript	`if (value == 0 ) {…`	□	Test Remove
2:	Discard unchanged with heartbeat	1h	□	Test Remove
3:	JavaScript	`return value % 1000;`	□	Test Remove

Add

Test all steps

Type of information: Numeric (unsigned)

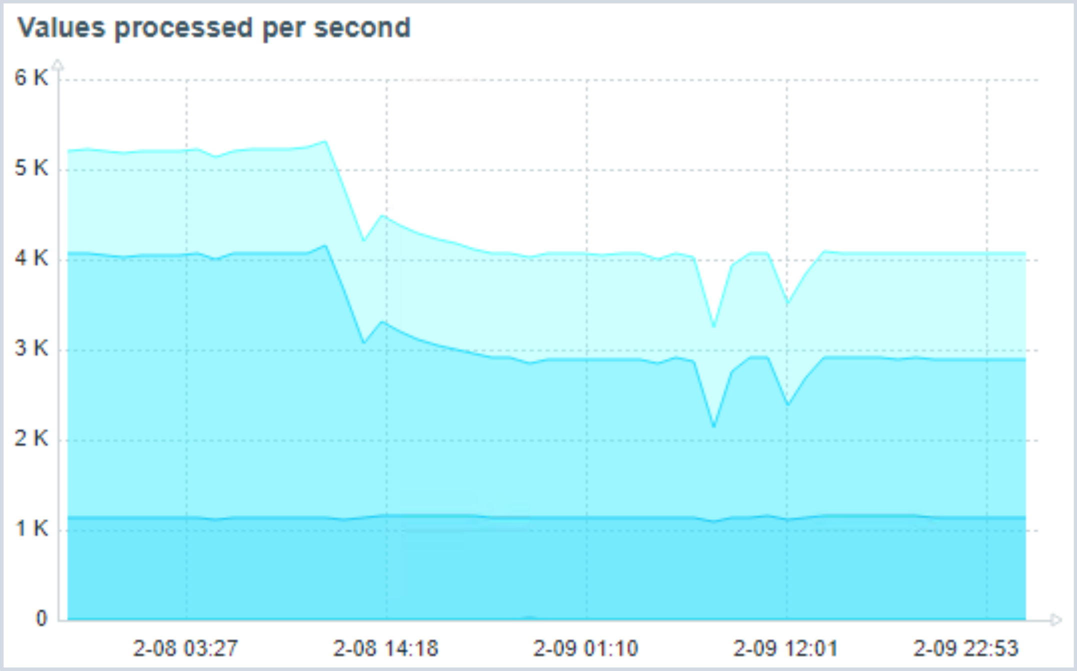
```
if (value == 0 ) {
  return value;
} else {
  return (Math.floor(Date.now() / 1000) - 1707000000 )*1000 + value;
}
```

```
return value % 1000;
```

Windows Out-of-the-box template tunning

Throttling

- Throttling Services Result:



- Wiki cz: https://www.initmax.cz/wiki/throttling-a-ochrana-pred-falesnymi-alerty-pomoci-min-max-avg/
- Wiki en: https://www.initmax.com/wiki/throttling-and-false-positives-protection-using-min-max-avg/

2

What & How

Advanced Windows monitoring

Server types

Server type

- Domain controllers
- Member servers
- Standalone servers

Components

- Availability
- Performance
- Security
- Inventory

Advanced Windows monitoring

Technologies to monitor

- AD
- DHCP
- DNS
- DFS
- File server + Quotas
- CA
- MSSQL
- Exchange
- IIS
- WSUS
- And more…

Technologies to use

- Out of the box monitoring
- System.run key
  - **Syntax: system.run[command,<mode>]**
  - command: command that should be executed, i.e., cmd or PowerShell

- User parameters
  - **Syntax: UserParameter=key,[<command>]**
  - Shell commands
  - Custom scripts

- Webinar cz: https://www.initmax.cz/webinar/rozsireni-funkci-zabbixu-7-0/

User Parameters

UserParameter examples:

- AD forest information – check FSMO roles
- Calculate GPO running time

```
### Option: UserParameter

UserParameter=getADForestFSMO[*],powershell -Command "Get-ADForest $1 |
select SchemaMaster,DomainNamingMaster |ConvertTo-Json"

UserParameter=GPORunTime[*],powershell -File "C:\Program Files\Zabbix Agent
2\scripts\GPORunTime.ps1"
```

Advanced Windows monitoring

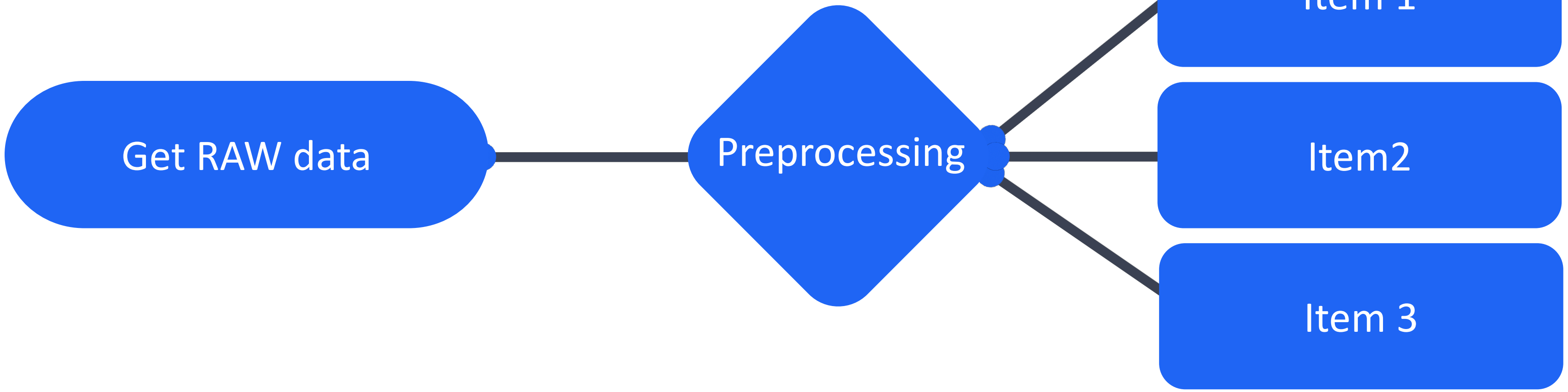
Active directory - Domain Controller

- Availability
  - FSMO role owners
  - DC diag errors
  - LDAP ports status
  - GC ports status
  - DNS availability
- Performance
  - NTDS.dit filesize
  - EDB.log filesize
  - Deleted object count
  - Replication status
- Security
  - Eventlog monitoring
- Inventory

Advanced Windows monitoring

DHCP server

- Availability
  - Service
- Performance
  - Scopes statistics
- Security
- Inventory



- Webinar cz: https://www.initmax.cz/webinar/jak-na-preprocessing-dat-7-0-2024/

Advanced Windows monitoring

DNS server

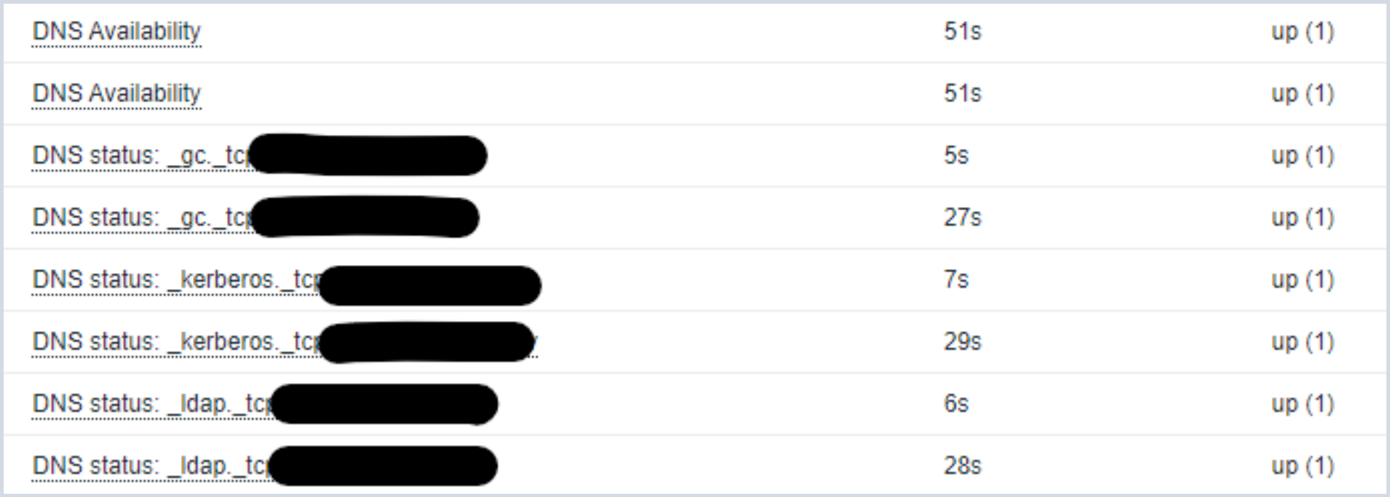
- Availability
  - Service state
  - DNS record availavility
- Performance
  - Response time
- Security
  - Eventlog security

Agent Items

- net.dns
- net.dns.record

Verze 7.0

- net.dns.perf
- net.dns.get



DNS Availability	51s	up (1)
DNS Availability	51s	up (1)
DNS status: _gc._tc[redacted]	5s	up (1)
DNS status: _gc._tc[redacted]	27s	up (1)
DNS status: _kerberos._tc[redacted]	7s	up (1)
DNS status: _kerberos._tc[redacted]	29s	up (1)
DNS status: _ldap._tc[redacted]	6s	up (1)
DNS status: _ldap._tc[redacted]	28s	up (1)

DFS server

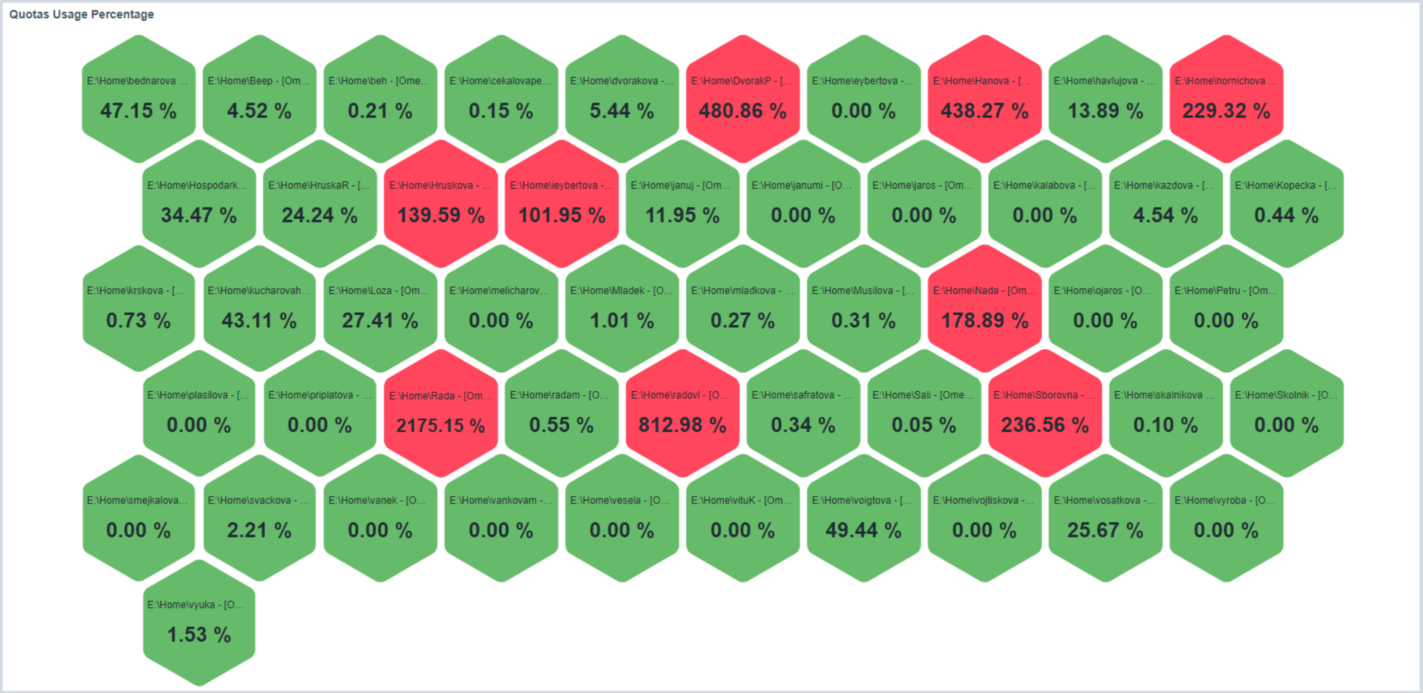
- Availability
  - Service
  - DFS-N status
  - DFS-R status
- Performance
  - ?

```
### Get DFS Namespace Folders
(Get-DfsnRoot -Domain <domain>).Path |
     % { (Get-DfsnFolder -Path (Join-Path -Path $_ -ChildPath "\*")).Path } |
     % { Get-DfsnFolderTarget -Path $_ | select Path, TargetPath, State } |
     sort Path | ConvertTo-Json
```

Advanced Windows monitoring

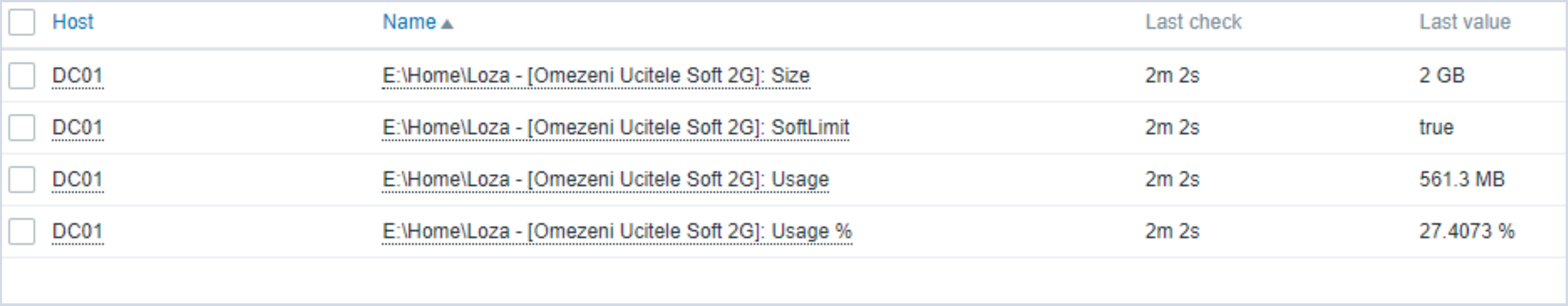
File server

- Availability
  - Service, Shares
- Performance
  - Quota monitoring
  - I/O Stats
  - Network traffic



Quotas Usage Percentage

E:\Home\bednarova ...	47.15 %
E:\Home\Beep - [Om...	4.52 %
E:\Home\beh - [Ome...	0.21 %
E:\Home\cekalovape...	0.15 %
E:\Home\dvorakova -...	5.44 %
E:\Home\DvorakP - [...	480.86 %
E:\Home\eybertova -...	0.00 %
E:\Home\Hanova - [...	438.27 %
E:\Home\havlujova - ...	13.89 %
E:\Home\hornichova ...	229.32 %
E:\Home\Hospodark...	34.47 %
E:\Home\HruskaR - [...	24.24 %
E:\Home\Hruskova - ...	139.59 %
E:\Home\ieybertova -...	101.95 %
E:\Home\januj - [Om...	11.95 %
E:\Home\janumi - [O...	0.00 %
E:\Home\jaros - [Om...	0.00 %
E:\Home\kalabova - [...	0.00 %
E:\Home\kazdova - [...	4.54 %
E:\Home\Kopecka - [...	0.44 %
E:\Home\krskova - [...	0.73 %
E:\Home\kucharovah...	43.11 %
E:\Home\Loza - [Om...	27.41 %
E:\Home\melicharov...	0.00 %
E:\Home\Mladek - [O...	1.01 %
E:\Home\mladkova - ...	0.27 %
E:\Home\Musilova - [...	0.31 %
E:\Home\Nada - [Om...	178.89 %
E:\Home\ojaros - [O...	0.00 %
E:\Home\Petru - [Om...	0.00 %
E:\Home\plasilova - [...	0.00 %
E:\Home\priplatova - ...	0.00 %
E:\Home\Rada - [Om...	2175.15 %
E:\Home\radam - [O...	0.55 %
E:\Home\radovl - [O...	812.98 %
E:\Home\safratova - ...	0.34 %
E:\Home\Sali - [Ome...	0.05 %
E:\Home\Sborovna - ...	236.56 %
E:\Home\skalnikova ...	0.10 %
E:\Home\Skolnik - [O...	0.00 %
E:\Home\smejkalova...	0.00 %
E:\Home\svackova - ...	2.21 %
E:\Home\vanek - [O...	0.00 %
E:\Home\vankovam -...	0.00 %
E:\Home\vesela - [O...	0.00 %
E:\Home\vituK - [Om...	0.00 %
E:\Home\voigtova - [...	49.44 %
E:\Home\vojtiskova -...	0.00 %
E:\Home\vosatkova -...	25.67 %
E:\Home\vyroba - [O...	0.00 %
E:\Home\vyuka - [O...	1.53 %



□	Host	Name ▲	Last check	Last value
□	DC01	E:\Home\Loza - [Omezeni Ucitele Soft 2G]: Size	2m 2s	2 GB
□	DC01	E:\Home\Loza - [Omezeni Ucitele Soft 2G]: SoftLimit	2m 2s	true
□	DC01	E:\Home\Loza - [Omezeni Ucitele Soft 2G]: Usage	2m 2s	561.3 MB
□	DC01	E:\Home\Loza - [Omezeni Ucitele Soft 2G]: Usage %	2m 2s	27.4073 %

Certificates and Certificate authority

- Published certificates
  - Out of the box certificate monitoring
    - web.certificate.get[hostname,<port>,<address>]
  - Multi-certificate template
    - https://git.initmax.cz/initMAX-Public/multiple-website-certificate-by-zabbix-agent-2

- Stored certificates
  - Microsoft cryptoapi
  - File stored certificates

- Certificate Authority
  - Availability
  - Service
  - Certificate status
- Performance

Advanced Windows monitoring

MSSQL Server news!!!

MSSQL by Zabbix agent 2

- 6.4.12, 6.0.27, 7.0.0.beta2
- Zabbix agent 2 plugin extension

MSSQL Server news!!!

- mssql.availability.group.get Returns availability groups. MSSQL
- mssql.custom.query Returns the result of a custom query.
- mssql.db.get Returns all available MSSQL databases.
- mssql.job.status.get Returns the status of jobs.
- mssql.last.backup.get Returns the last backup time for all databases.
- mssql.local.db.get Returns databases that are participating in an Always On availability group and replica (primary or secondary) and are located on the server that the connection was established to.
- mssql.mirroring.get Returns mirroring info.
- mssql.nonlocal.db.get Returns databases that are participating in an Always On availability group and replica (primary or secondary) located on other servers (the database is not local to the SQL Server instance that the connection was established to).
- mssql.perfcounter.get Returns the performance counters.
- mssql.ping Test if a connection is alive or not.
- mssql.quorum.get Returns the quorum info.

MSSQL Server news!!!

mssql.quorum.member.get	Returns the quorum members.
mssql.replica.get	Returns the replicas.
mssql.version	Returns the MSSQL version.
mysql.custom.query	Returns the result of a custom query.
mysql.db.discovery	Returns the list of MySQL databases.
mysql.db.size	The database size in bytes.
mysql.get_status_variables	Values of the global status variables.
mysql.ping	Test if a connection is alive or not.
mysql.replication.discovery	Returns the list of MySQL replications.
mysql.replication.get_slave_status	The replication status.
mysql.version	The MySQL version.

Advanced Windows monitoring

MSSQL Server

MSSQL by ODBC

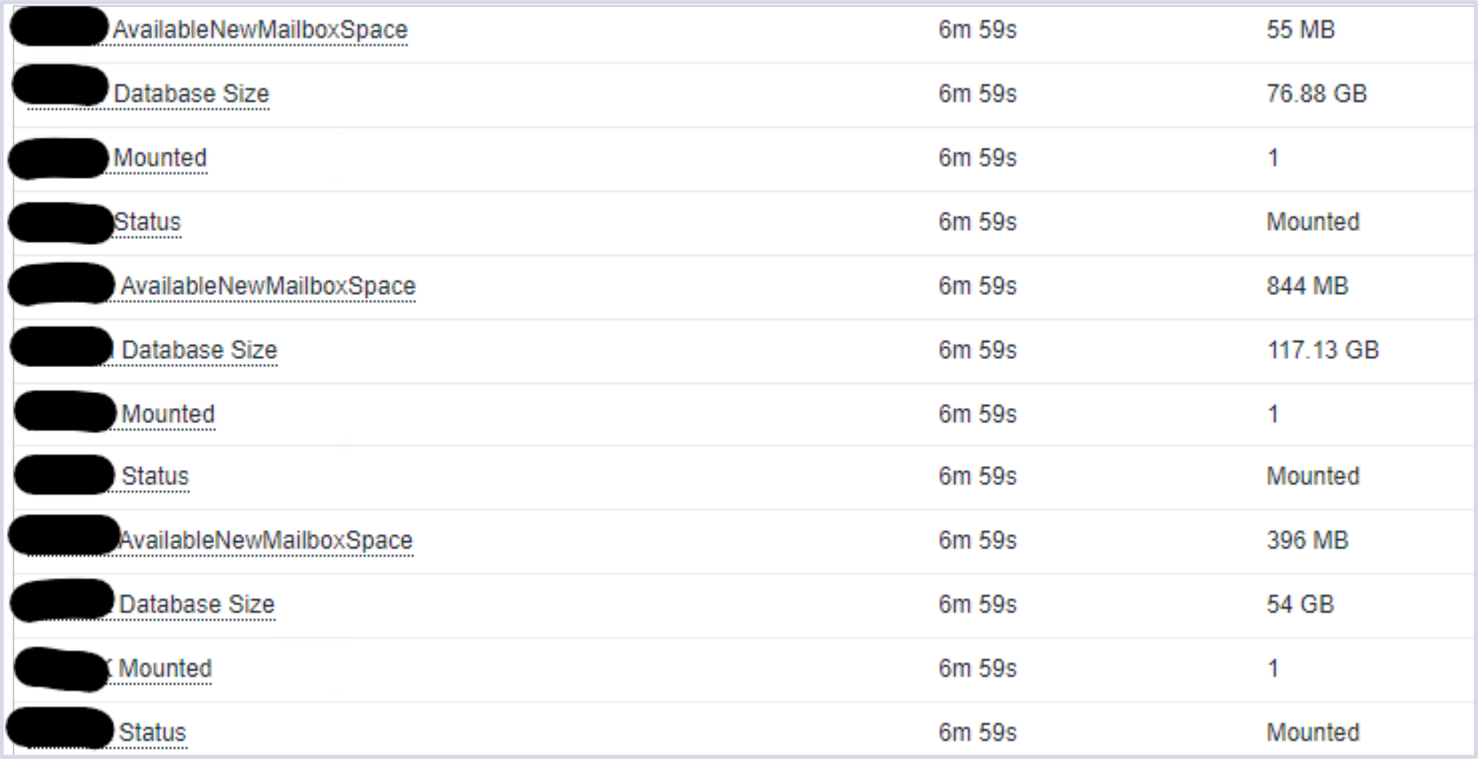
- Availability
  - Service
- Performance
  - Scopes statistics
- Security
- Inventory

Advanced Windows monitoring

Exchange Server

Microsoft Exchange Server 2016 by Zabbix agent

- Availability
- Performance
  - Server Counters
  - Discovery
    - Databases
    - LDAP
    - Web Services
- Statistics
  - Powershell + UserParameters



[redacted] AvailableNewMailboxSpace	6m 59s	55 MB
[redacted] Database Size	6m 59s	76.88 GB
[redacted] Mounted	6m 59s	1
[redacted] Status	6m 59s	Mounted
[redacted] AvailableNewMailboxSpace	6m 59s	844 MB
[redacted] Database Size	6m 59s	117.13 GB
[redacted] Mounted	6m 59s	1
[redacted] Status	6m 59s	Mounted
[redacted] AvailableNewMailboxSpace	6m 59s	396 MB
[redacted] Database Size	6m 59s	54 GB
[redacted] Mounted	6m 59s	1
[redacted] Status	6m 59s	Mounted

IIS Server

IIS by Zabbix agent

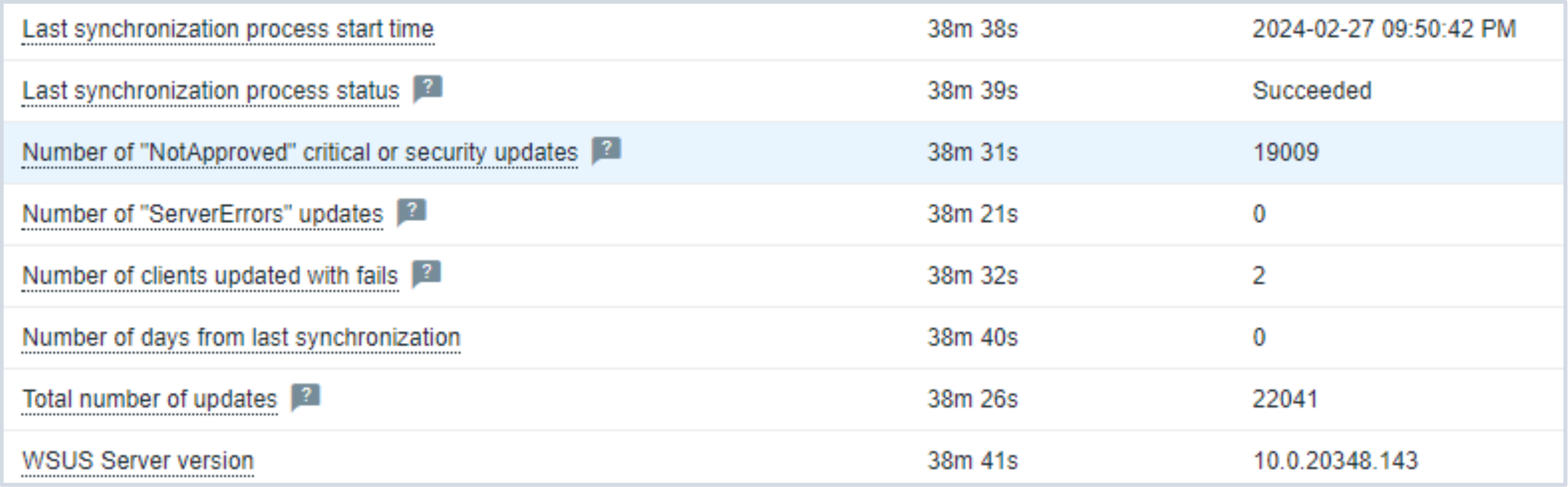
- Availability
    - service.info[WAS]
    - service.info[W3SVC]
    - net.tcp.service[{$IIS.SERVICE},,{$IIS.PORT}]
- Performance
    - perf_counter_en["\Web Service(_Total)\Bytes Received/sec", 60]
    - …
    - Application pools Discovery
        - Pool prototypes – perf_counter_en

Advanced Windows monitoring

WSUS Server

Community template

- Availability
  - service.info[WsusService]
- Performance
  - Application pools Discovery



Last synchronization process start time	38m 38s	2024-02-27 09:50:42 PM
Last synchronization process status	38m 39s	Succeeded
Number of "NotApproved" critical or security updates	38m 31s	19009
Number of "ServerErrors" updates	38m 21s	0
Number of clients updated with fails	38m 32s	2
Number of days from last synchronization	38m 40s	0
Total number of updates	38m 26s	22041
WSUS Server version	38m 41s	10.0.20348.143

3

Summary and recommendations!

Summary and recommendations!

Use Zabbix agent 2

- Use Zabbix Agent 2 – internal items (performance counters, WMI checks, registry)
- Extend agent functionality with userparameters and system.run keys
- Use dependent items
- Do not overload powershell
- Customize update interval
- Customize History and Trend storage

4

Demonstration

initMAX

Questions?

Contact us:

Phone:	+420 800 244 442
Web:	https://www.initmax.cz
Email:	tomas.hermanek@initmax.cz
LinkedIn:	https://www.linkedin.com/company/initmax
Twitter:	https://twitter.com/initmax
Tomáš Heřmánek:	+420 732 447 184