initMAX

Webinar

Advanced Windows monitoring part 2

all your microphones are muted

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

use Chat for discussion, networking or applause

initMAX

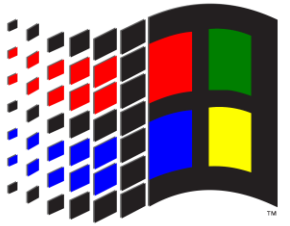
Windows server

Windows Server 2016

Windows Server 2025

Windows Server 2012

Windows Server 2022



Windows Server 2019

Advanced Windows monitoring part 2

Agenda

- Windows Process diagnostics
- Windows Defender (Antivirus) monitoring
- Active Directory – content monitoring

1

Out of the box

Advanced Windows monitoring part 2

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.	

2

Windows process diagnostics

initMAX

Advanced Windows monitoring part 2

Windows OS Process Diagnostics

Task: Process monitoring

- Diagnose problematic server with high memory consumption

Windows Process:

- Dynamic
- Monitoring technologies:
  - Zabbix agent built-in Items
  - Zabbix agent Performance counters
  - Master Item, LLD, Item prototypes

initMAX

Zabbix agent Out-of-the-box items

Item proc.get[]

Zabbix doc:

- https://www.zabbix.com/documentation/current/en/manual/config/items/itemtypes/zabbix_agent#proc.get
- JSON result
  - LLD rule
  - Dependent Item prototypes


```
[{
        "pid": 7296,
        "ppid": 700,
        "name": "zabbix_agent2.exe",
        "user": "SYSTEM",
        "sid": "S-1-5-18",
        "vmsize": 42276,
        "wkset": 52704,
        "cputime_user": 5.140625,
        "cputime_system": 36.484375,
        "threads": 20,
        "page_faults": 474602,
        "handles": 665,
        "io_read_b": 31052273,
        "io_write_b": 8884,
        "io_read_op": 1906,
        "io_write_op": 58,
        "io_other_b": 8256975,
        "io_other_op": 137261
    },
```

initMAX

Zabbix agent(2) - Performance counters

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

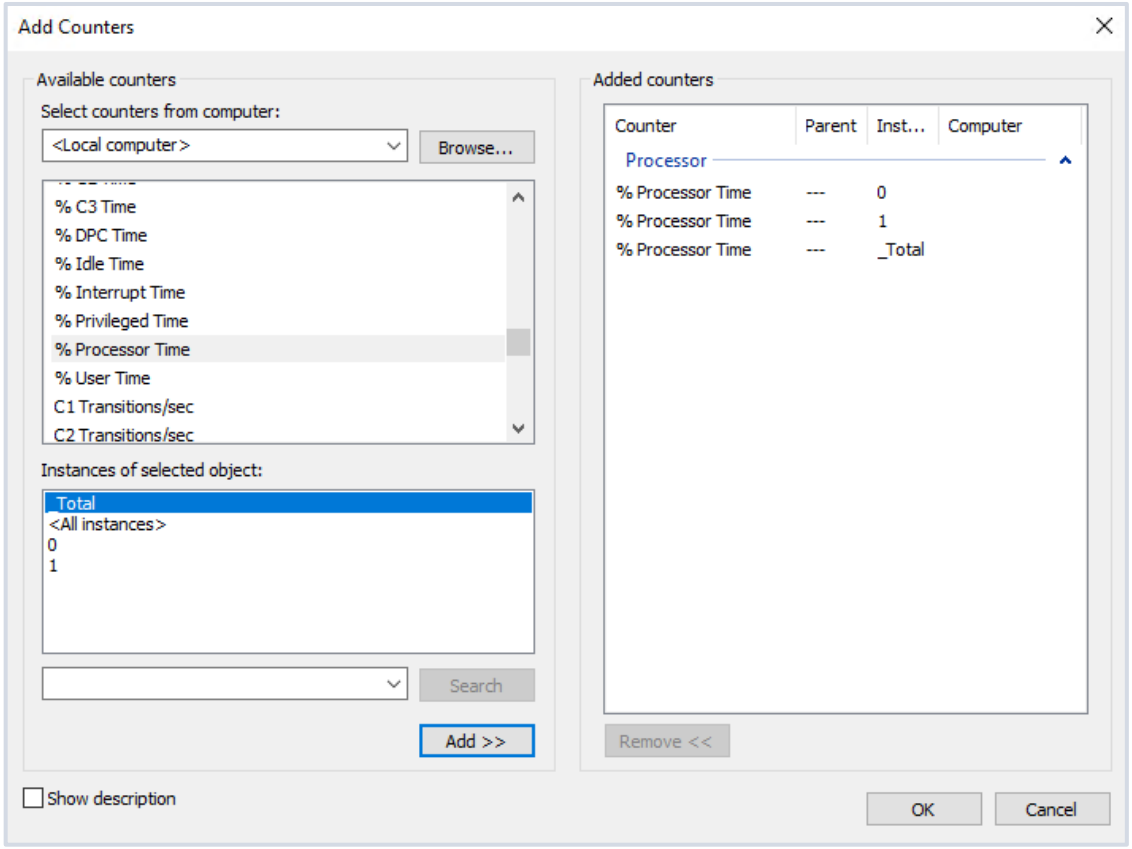
- perf_counter- The value of performance counter.
- perf_counter_en

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



initMAX

Zabbix agent Performance counters

Item perf_instance_en.discovery[Process V2]

Zabbix doc:

- https://www.zabbix.com/documentation/current/en/manual/config/items/itemtypes/zabbix_agent/win_keys#perf.instance.en.discovery
- JSON result
  - LLD rule
  - Zabbix agent Item prototypes
  - perf_counter_en[counter,<interval>]

```
[
    "{#INSTANCE}": "AggregatorHost:4476"},
    "{#INSTANCE}": "AzureArcSysTray:7568"},
    "{#INSTANCE}": "cmd:6384"},
    "{#INSTANCE}": "conhost:732"},
    "{#INSTANCE}": "csrss:476"},
    "{#INSTANCE}": "csrss:564"},
    "{#INSTANCE}": "csrss:5844"},
    "{#INSTANCE}": "ctfmon:6560"},
    "{#INSTANCE}": "dfsrs:3344"},
    ...
]
```

initMAX

Zabbix agent Performance counters

Process x Process V2

Item perf_instance_en.discovery[Process]

- JSON result
  - LLD rule
  - Zabbix agent Item prototypes
  - perf_counter_en[counter,<interval>]
  -

```
[
    "{#INSTANCE}": "Idle"},
    "{#INSTANCE}": "System"},
    "{#INSTANCE}": "Registry"},
    "{#INSTANCE}": "smss"},
    "{#INSTANCE}": "csrss"},
    "{#INSTANCE}": "wininit"}
]
```

```
[
    "{#INSTANCE}": "AggregatorHost:4476"},
    "{#INSTANCE}": "AzureArcSysTray:7568"},
    "{#INSTANCE}": "cmd:6384"},
    "{#INSTANCE}": "conhost:732"},
    "{#INSTANCE}": "csrss:476"}
]
```

initMAX

Zabbix agent Performance counters

LLD Workload

- LLD disadvantages
  - Running only on Zabbix server
  - Problem for dynamic changes
  - perf_counter_en[counter,<interval>]

- Lost resources consideration
  - Delete lost resources
  - Disable lost resources

3

Windows Defender

initMAX

Advanced Windows monitoring part 2

Windows Defender

Task: Microsoft Defender monitoring

- Monitor Status of Defender Component
- Monitor Defender Events

Windows Defender:

- GUI, Powershell, **WMI**
- Monitoring technologies:
  - Zabbix agent wmi Items
  - Master Item – Dependent Items

initMAX

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\microsoft\windows\defender -Query "select * from MSFT_MpComputerStatus"
```

Advanced Windows monitoring part 2

Windows Defender

Monitor Windows Defender status and events

- Defender Overall status

```
wmi.get["root\microsoft\windows\defender","select ComputerState from MSFT_MpComputerStatus"]
```

- All Defender metrics

```
wmi.getall["root\microsoft\windows\defender","select * from MSFT_MpComputerStatus"]
```

- Defender Events
- Eventlog

```
eventlog[Microsoft-Windows-Windows Defender/Operational,,,{$AV_SOURCE},1006|1116,,skip]
```

4

Active directory objects

Advanced Windows monitoring part 2

Active directory objects

Task: Monitor or analyze objects in Active Directory

- Many tasks:
  - Monitor OU or Group changes
  - Create New Groups in Zabbix based on AD
  - Create New Hosts based on AD computers
  - Compare Computers in AD and Hosts in Zabbix

- AD Access:
  - LDAP
  - PowerShell
  - Other, Zabbix native?

initMAX

Active directory – Reading AD objects

- **Standard approach:**
- external script:
  - Python, bash, …
  - LDAP connection

```
basedn = "OU=Computers,OU=Company,DC=lab,DC=local"
searchFilter = "(&(objectClass=computer)(cn=*))"
searchAttribute = ["cn","description"]
#this will scope the entire subtree under UserUnits
searchScope = ldap.SCOPE_SUBTREE

#Bind to the server
try:
    l.protocol_version = ldap.VERSION3
    l.simple_bind_s(binddn, pw)
except ldap.INVALID_CREDENTIALS:
  print ("Your username or password is incorrect.")
  exit(0)
try:
    ldap_result_id = l.search_s(basedn, searchScope, searchFilter, searchAttribute)
```

initMAX

Active directory – Reading AD objects

- **Zabbix „native“ solution (without external scripting)**
- Zabbix agent WMI items on DC

- Get Computer query:

```
wmi.getall["root\directory\ldap","select DS_name from DS_Computer where ADSIPath like
'%OU=Computers,OU=Company,DC=lab,DC=local%‘“]
```

- Get Group query:

```
wmi.getall["root\directory\ldap","select DS_name from DS_Group where ADSIPath like
,%OU=GroupsOU=Company,DC=lab,DC=local%‘“]
```

initMAX

Active directory – Reading AD objects

- Get User query:

```
wmi.getall["root\directory\ldap","select DS_name from DS_User where ADSIPath like
,%OU=Users,OU=Company,DC=lab,DC=local%'"]
```

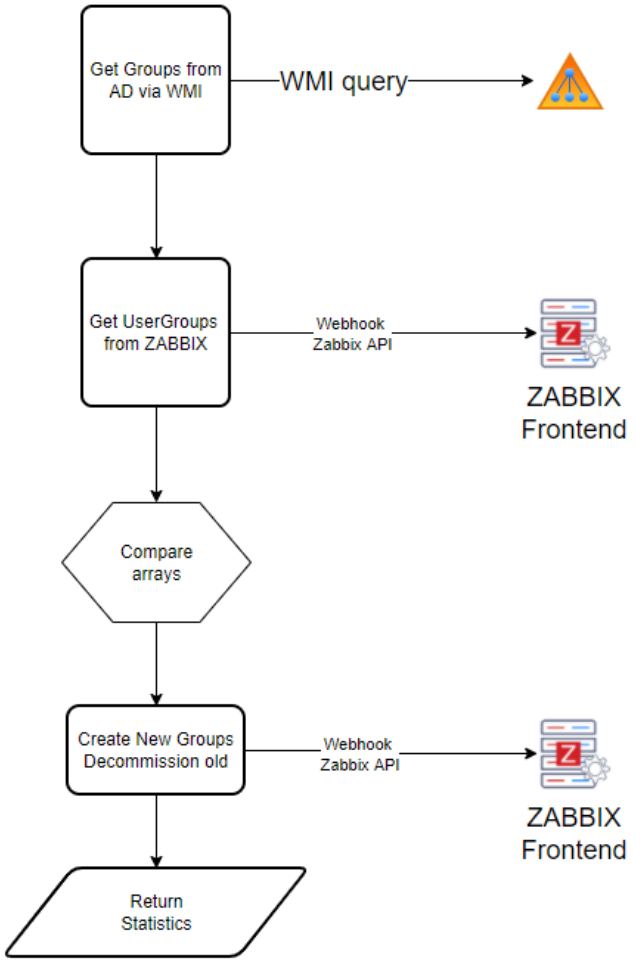
initMAX

Active directory – Reading AD objects

Next steps?

- Javascript preprocessing

1. Connect to Zabbix API
2. Get objects to compare from Zabbix API
3. Compare objects
4. Create missing
5. (delete remaining)
6. Return result statistics and status



initMAX

Questions?

initMAX

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