

ZABBIX

DEPLOYING AND CONFIGURING ZABBIX AGENT ON WINDOWS

ARTŪRS LONTONS
TECHNICAL MARKETING ENGINEER

ZABBIX

TOPICS FOR TODAY

- ⚡ Downloading and Installing the Zabbix agent on Windows
- ⚡ Windows specific agent configuration
- ⚡ Windows specific Zabbix agent item keys
- ⚡ Windows monitoring templates
- ⚡ Extending the Zabbix agent on Windows
- ⚡ Zabbix Agent on Windows questions and troubleshooting

ZABBIX

Deploying and configuring Zabbix agent on Windows

DOWNLOADING AND INSTALLING ZABBIX AGENT

DOWNLOADING THE **ZABBIX AGENT**

Both Zabbix agent and Zabbix agent 2 are available for download on Windows

- ⚡ MSI and archive packaging is provided
- ⚡ The precompiled agent binaries support amd64 and i386 CPU architectures
- ⚡ Available with and without OpenSSL encryption support

Wish to compile Zabbix agent or Zabbix agent 2 on Windows?

- ⚡ It is also possible to compile Zabbix agent and Zabbix agent 2 on Windows*
 - ✓ This requires quite a few more manual steps compared to compiling on a Unix based OS

*https://www.zabbix.com/documentation/current/en/manual/installation/install/building_zabbix_agent_2_on_windows

*https://www.zabbix.com/documentation/current/en/manual/installation/install/win_agent

DOWNLOADING THE ZABBIX AGENT

Download and install pre-compiled Zabbix agents

Show legacy downloads



OS DISTRIBUTION	OS VERSION	HARDWARE	ZABBIX VERSION	ENCRYPTION	PACKAGING
Windows	Any	amd64	6.0 LTS	OpenSSL	MSI
Linux		i386	5.4	No encryption	Archive
macOS			5.2		
AIX			5.0 LTS		
FreeBSD			4.4		
OpenBSD			4.2		
Solaris			4.0 LTS		
			3.0 LTS		

DOWNLOADING THE ZABBIX AGENT

Zabbix Release: ▼

Zabbix agent v6.0.2

[Read manual](#)

Packaging: Archive
Encryption: OpenSSL
Linkage: Dynamic
Checksum: sha256: d3877a56450b6c41cc506d32a83bcb63d743f8fe82096be52dfb63ac381cf5e2
sha1: 4141714db964120074205d8e2315c6561ea1a1ca
md5: d737999f6363e4c4a9c6be316b3be1c0

DOWNLOAD

https://cdn.zabbix.com/zabbix/binaries/stable/6.0/6.0.2/zabbix_agent-6.0.2-windows-amd64-openssl.zip

Zabbix agent 2 v6.0.2

[Read manual](#)

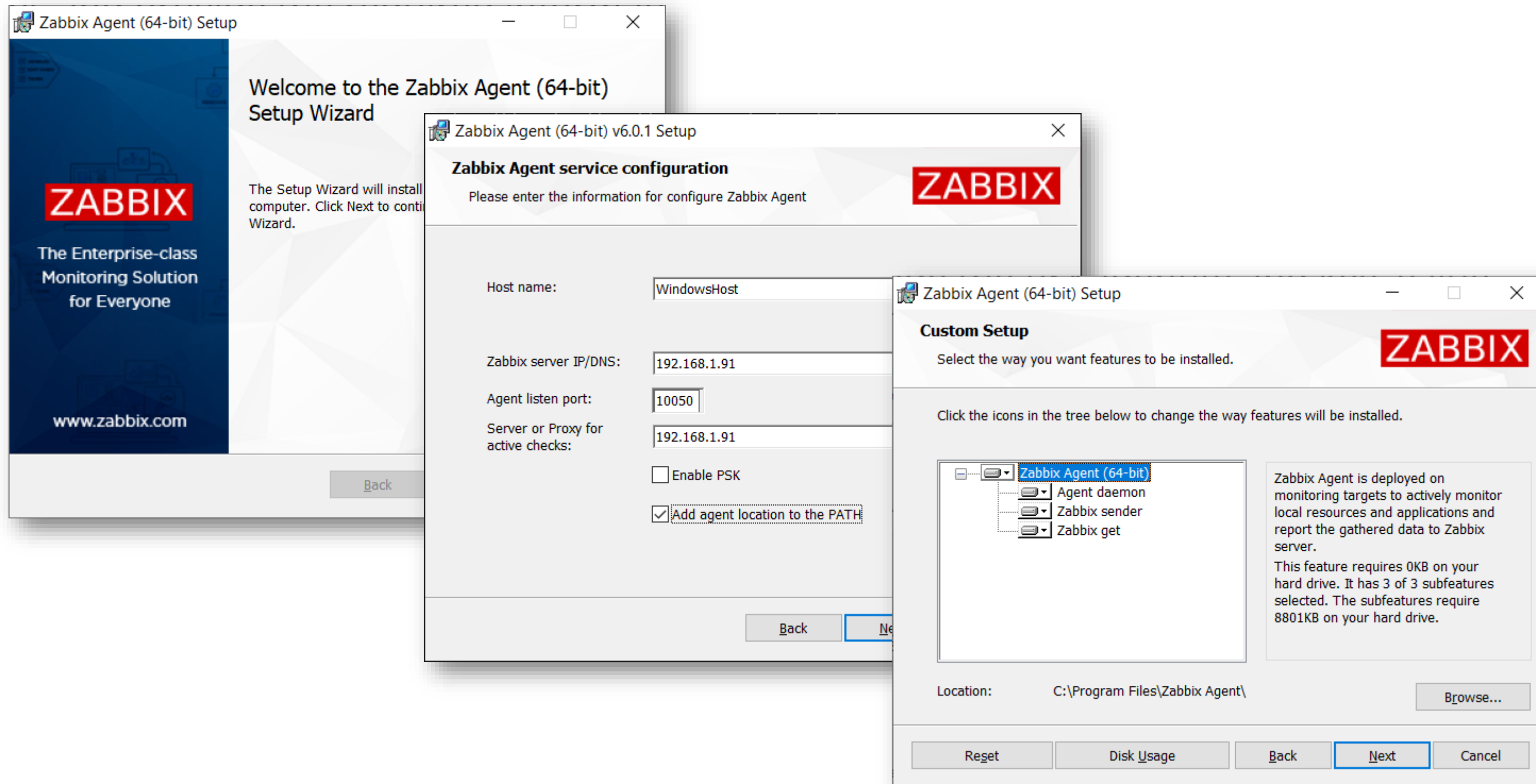
Packaging: Archive
Encryption: OpenSSL
Linkage: Static
Checksum: sha256: b850ac6b104bf889556c12d949b52e2959a0f446e47b3759cd4fcdefcaac04c1
sha1: 95b90518cad1f364baa30f5ad2b790c38eb6c7dc
md5: ae84a763065cca0f58e525266cd2321b

DOWNLOAD

https://cdn.zabbix.com/zabbix/binaries/stable/6.0/6.0.2/zabbix_agent2-6.0.2-windows-amd64-openssl-static.zip

INSTALLING FROM THE MSI PACKAGE

Follow the instructions and provide the required information



INSTALLING FROM THE MSI PACKAGE

Optionally, also provide the PSK identity and key value

Zabbix Agent (64-bit) PSK Setup

Zabbix Agent pre-shared key configuration ZABBIX

Please enter the PSK information for configure Zabbix Agent

Pre-shared key identity:
WindowsDemo

Pre-shared key value:
e560cb0d918d26d31b4f642181f5f570ad89a390931102e5391d08327ba434e9

Please, set minimum required permission to access the psk.key file

Back Next Cancel

- ⚡ The PSK will be stored in the agent directory, in the *psk.key* file
- ⚡ The PSK identity will be passed to the Zabbix agent configuration file
- ⚡ The value of *TLSCConnect* and *TLSAccept* parameters will be set to *psk*

INSTALLING FROM THE **MSI PACKAGE**

The Zabbix agent MSI package also supports a command-line based installation

⚡ Ability to configure additional parameters during the installation, such as:

- ✓ TLS parameters
- ✓ Log parameters
- ✓ Timeout parameters
- ✓ Persistent buffer parameters (*Agent 2 only*)
- ✓ Allow and Deny keys
- ✓ And more

⚡ This way Zabbix agent can be distributed in an advanced fashion by using Windows Group Policy

*https://www.zabbix.com/documentation/6.0/en/manual/installation/install_from_packages/win_msi

INSTALLING FROM THE **MSI PACKAGE**

```
SET INSTALLFOLDER=C:\Program Files\za
msiexec /l*v log.txt /i zabbix_agent-6.0.0-x86.msi /qn^
LOGTYPE=file^
LOGFILE="%INSTALLFOLDER%\za.log"^
SERVER=192.168.6.76^
LISTENPORT=12345^
SERVERACTIVE=::1^
HOSTNAME=myHost^
TLSCONNECT=psk^
TLSACCEPT=psk^
TLSPSKIDENTITY=MyPSKID^
TLSPSKFILE="%INSTALLFOLDER%\mykey.psk"^
TLSCAFILE="c:\temp\f.txt1"^
TLSCRLFILE="c:\temp\f.txt2"^
TLSSERVERCERTISSUER="My CA"^
TLSSERVERCERTSUBJECT="My Cert"^
TLSCERTFILE="c:\temp\f.txt5"^
TLSKEYFILE="c:\temp\f.txt6"^
ENABLEPATH=1^
INSTALLFOLDER="%INSTALLFOLDER%"^
SKIP=fw^
ALLOWDENYKEY="DenyKey=vfs.file.contents[/etc/passwd]"
```

INSTALLING FROM **THE ARCHIVE**

The archive contains two directories – *conf* and *bin*

- ⚡ The *conf* directory contains the Zabbix agent configuration file
- ⚡ The *bin* directory contains the binary files for Zabbix agent, Zabbix sender, and Zabbix get

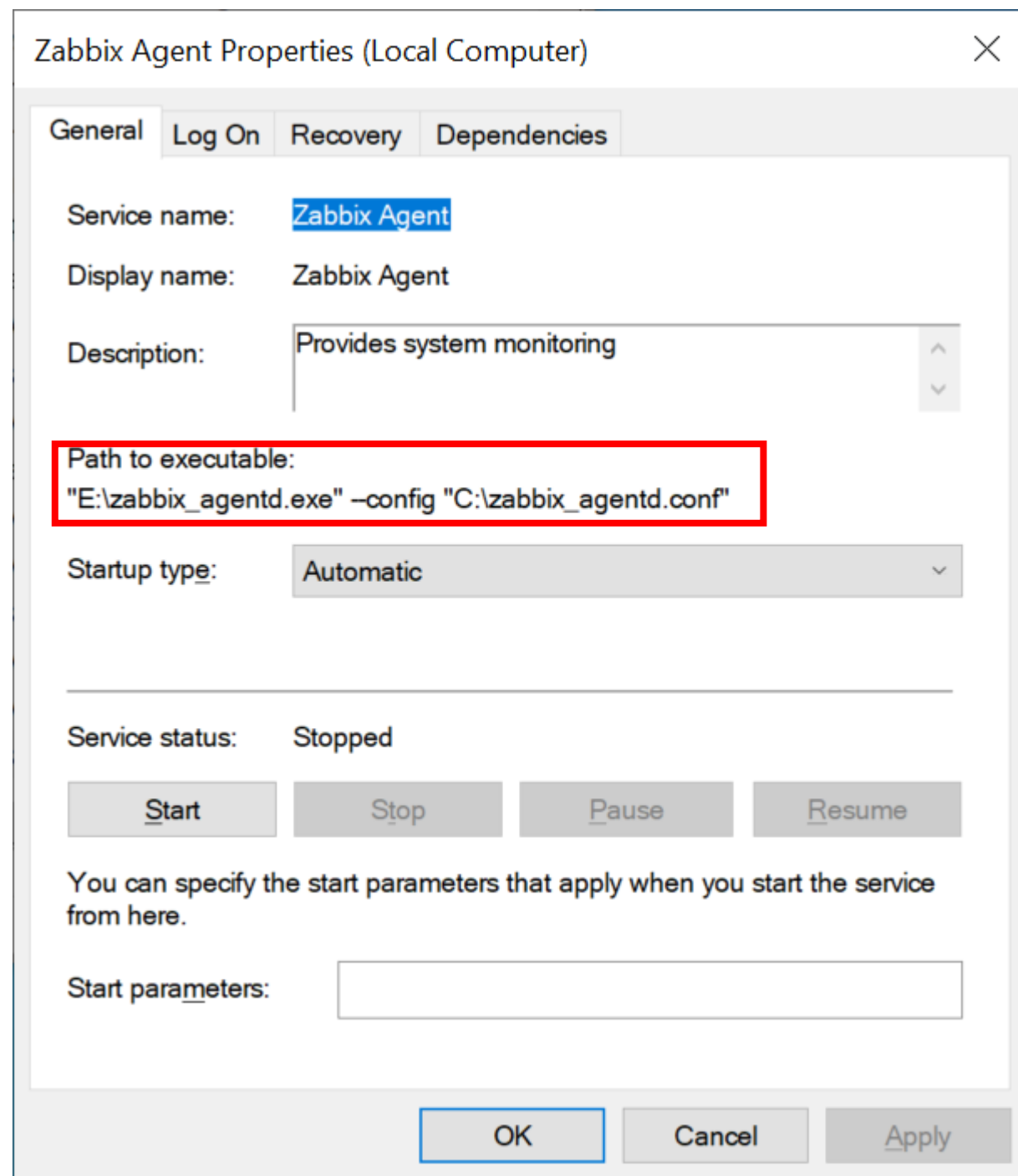
To install Zabbix agent, we must pass the *install* option to the `zabbix_agentd.exe`

```
zabbix_agentd.exe --install
```

- ⚡ By default, Zabbix agent will create a log file in the root of the C: drive

INSTALLING FROM THE ARCHIVE

By default, Zabbix agent will try to locate the Zabbix agent configuration file in the root of the C:\ drive



To change the location of the Zabbix agent configuration file, you must pass the `--config <your_configuration_file>` option to the agent binary

```
zabbix_agentd.exe --config "C:\Program Files\Zabbix\conf\zabbix_agentd.conf" --install
```

ZABBIX

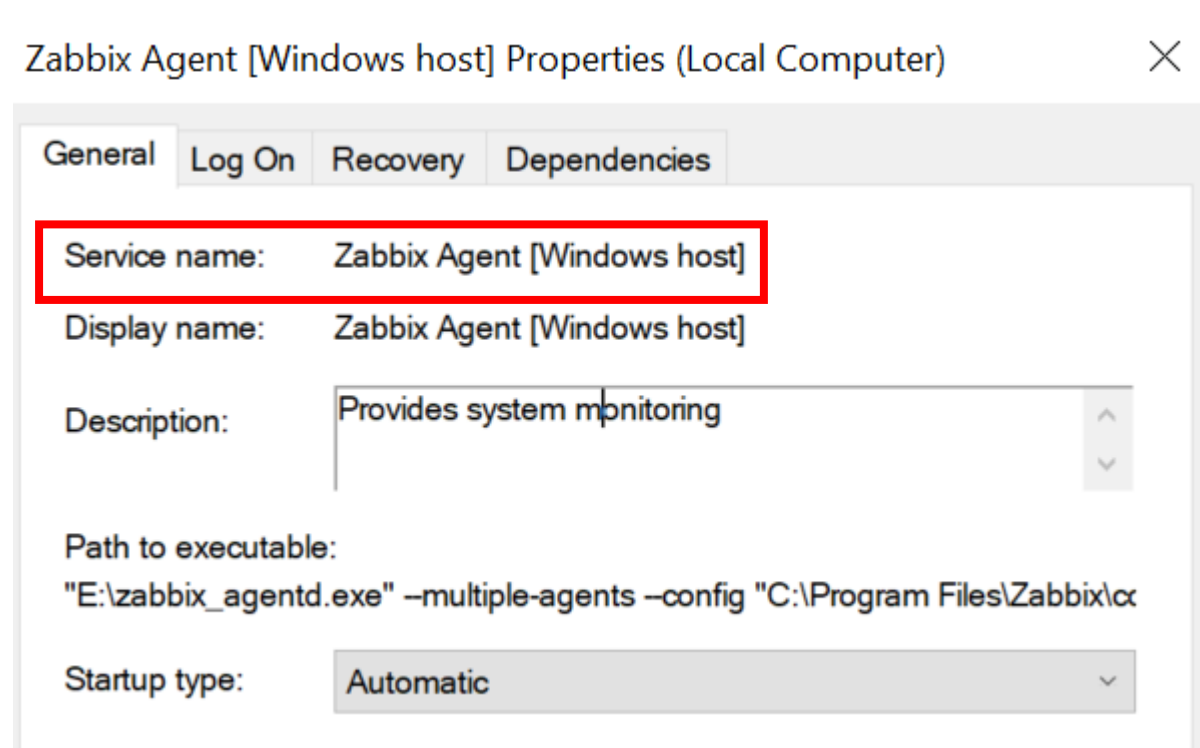
Deploying and configuring Zabbix agent on Windows

ZABBIX AGENT SERVICE

ZABBIX AGENT SERVICE

On Windows Zabbix agent runs as a service named *Zabbix agent* (by default)

- ⚡ It is also possible to Install multiple Zabbix agent services if you wish to run multiple agent instances (*this is an extremely rare use case*)
- ⚡ By passing the *--multiple-agents* option, the service name will contain the Agent host name (obtained from the configuration file)



ZABBIX AGENT SERVICE

- ⚡ The Zabbix agent service can be started/stopped either from the command line or from the *Services* section
- ⚡ By default, the Zabbix agent service startup type is set to *Automatic*
- ⚡ By default, the Zabbix agent service runs under the *Local system account*
- ⚡ The Zabbix agent service can be uninstalled by passing the *--uninstall* command-line option

Many of these settings can be changed on the service level, such as – the service user, startup type, recovery settings and more.

ZABBIX AGENT SERVICE

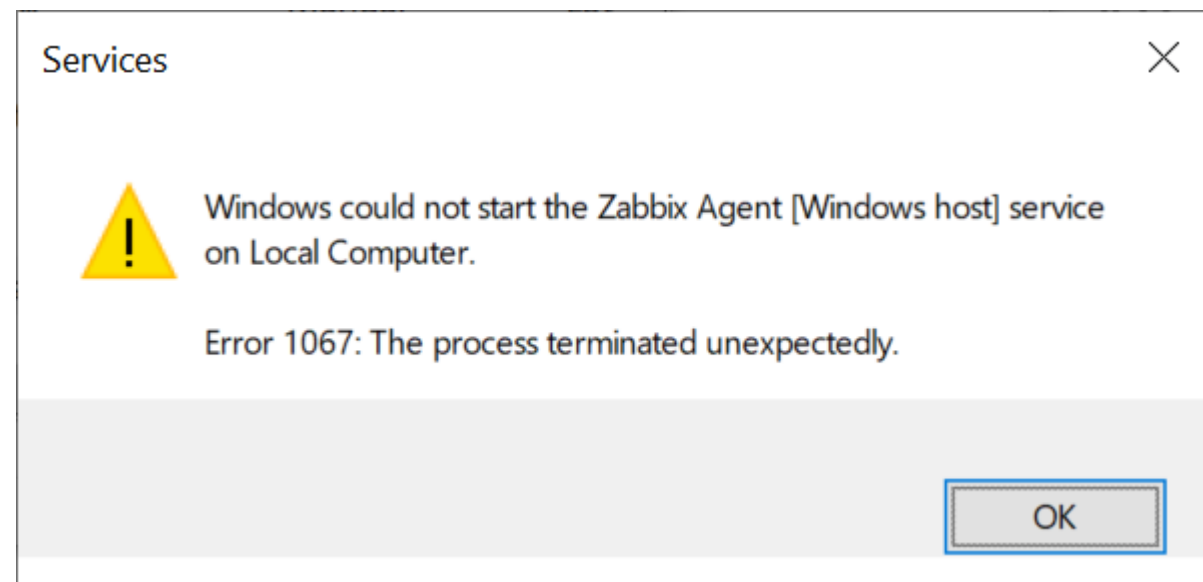
It is possible to run the Zabbix service under a different user

- ⚡ Make sure that the user can read the Zabbix agent configuration file
- ⚡ Make sure that the user has sufficient permissions to manage the Zabbix service
- ⚡ Make sure that the user has sufficient permissions to collect the required metrics (*for example – read a file, read a performance counter*)

ZABBIX AGENT SERVICE - TROUBLESHOOTING

An example of a performance counter permission issue

⚡ Error when starting the service



⚡ Error from Zabbix agent log file


```
27440:20220321:161515.011 RegQueryValueEx() failed at getting buffer size, 0x5
27440:20220321:161515.011 cannot initialize performance counter collector: cannot initialize
built-in counter indexes
27440:20220321:161515.011 Zabbix Agent stopped. Zabbix 6.0.2 (revision d726a4d916).
```

ZABBIX AGENT SERVICE - TROUBLESHOOTING

An example of lacking permissions to read file contents

 Error when testing the item


Test item ✕

 Cannot open file: [13] Permission denied ✕


Get value from host

* Host address Port

Proxy ▼

Value  Time

Not supported

Previous value  Prev. time

End of line sequence LF CRLF



Deploying and configuring Zabbix agent on Windows

WINDOWS SPECIFIC ITEM KEYS

ZABBIX AGENT SERVICE - TROUBLESHOOTING

There is a number of Zabbix item keys that are OS-specific. Windows is no exception*

Description	Key
Event log monitoring	eventlog[name,<regexp>,<severity>,<source>,<eventid>,<maxlines>,<mode>]
Performance counter value	perf_counter[counter,<interval>]
Information about a process	proc_info[process,<attribute>,<type>]
Windows service discovery	service.discovery
Windows service information	service.info[service,<param>]
Obtain WMI query result	wmi.get[<namespace>,<query>]
Virtual memory size	vm.vmemory.size[<type>]

*https://www.zabbix.com/documentation/current/en/manual/config/items/itemtypes/zabbix_agent/win_keys

WMI MONITORING

Windows management instrumentation – *WMI*, provides a standardized model to access management information.

- ⚡ Zabbix agent can obtain information about a WMI instance by using the WMI Query Language
- ⚡ Item keys like *wmi.get* and *wmi.getall* can be used to obtain WMI information
- ⚡ *wmi.get[<namespace>,<query>]* returns the first selected object
- ⚡ *wmi.getall[<namespace>,<query>]* returns the whole response as a JSON object

Example:

wmi.get[root\cimv2,select status from Win32_DiskDrive where Name like '%PHYSICALDRIVE0%'] - returns the status of the first physical disk

PERFORMANCE COUNTER MONITORING

Windows performance counters provide an interface for collecting various OS-level metrics such as metrics related to CPU, memory, and disk usage

- ⚡ Zabbix agent can monitor individual performance counters and a list of performance counter objects for Low-level discovery
- ⚡ Performance counter string names can vary between languages – use the *perf_counter_en* and *perf_instance_en.discovery* keys to monitor English performance counters
- ⚡ Bullet point

Example:

perf_counter_en["\System\Processor Queue Length"] – Processor Queue length

ZABBIX

Deploying and configuring Zabbix agent on Windows

WINDOWS MONITORING TEMPLATES

WINDOWS MONITORING TEMPLATES

Zabbix provides a vast selection of out of the box Windows templates that can be linked to any Windows host:

- 📶 Windows CPU by Zabbix agent
- 📶 Windows filesystems by Zabbix agent
- 📶 Windows generic by Zabbix agent
- 📶 Windows memory by Zabbix agent
- 📶 Windows network by Zabbix agent
- 📶 Windows physical disks by Zabbix agent
- 📶 Windows services by Zabbix agent
- 📶 *Windows SNMP (For SNMP agents deployed on windows hosts)*

WINDOWS MONITORING TEMPLATES

The templates utilize a mix of standard agent keys, WMI queries, and performance counter information

- ⚡ Some templates contain mostly static items, while others rely on Low-level discovery rules
 - ✓ For example, Windows service template fully relies on the Windows services discovery LLD rule and creates one item per service

Item prototypes

All templates / Windows services by Zabbix agent Discovery list / Windows services discovery

Item prototypes 1 Trigger prototypes 1 Graph prototypes Host prototypes

Item prototype Tags 1 Preprocessing

* Name

Type

* Key

Type of information

WINDOWS MONITORING TEMPLATES

Check the documentation to find what Low-level discovery macros can be used in the item prototypes

- ⚡ wmi.getall does not define any LLD macros
- ✓ The Zabbix administrator should define them by using the LLD macros tab of the LLD rule or use Javascript preprocessing

Discovery rules

All hosts / Windows host Enabled **ZBX** Discovery list / Network interfaces discovery Item prototypes 9 Trigger prototypes 4 Graph prototypes 1 Host prototypes

Discovery rule Preprocessing 1 **LLD macros** Filters 6 Overrides

LLD macro	JSONPath	
{#IFALIAS}	\$.NetConnectionID	Remove
{#IFDESCR}	\$.Description	Remove
{#IFGUID}	\$.GUID	Remove
{#IFNAME}	\$.Name	Remove

[Add](#)

[Update](#) [Clone](#) [Execute now](#) [Test](#) [Delete](#) [Cancel](#)

WINDOWS MONITORING TEMPLATES

As with every LLD – don't forget to check the LLD filters!

⚡ Are unnecessary services getting discovered? Check your filters!

✓ Official template filters use User macros – update the macro values to update the filters!

Discovery rules

All templates / Windows services by Zabbix agent / Discovery list / Windows services discovery

Item prototypes 1 / Trigger prototypes 1 / Graph prototypes / Host prototypes

Discovery rule / Preprocessing / LLD macros / **Filters 4** / Overrides

Type of calculation: And (A and B) and (C and D)

Filters	LabelMacro		Regular expression	Action
A	{#SERVICE.NAME}	matches	{\$SERVICE.NAME.MATCHES}	Remove
B	{#SERVICE.NAME}	does not match	{\$SERVICE.NAME.NOT_MATCHES}	Remove
C	{#SERVICE.STARTUPNAME}	matches	{\$SERVICE.STARTUPNAME.MATCHES}	Remove
D	{#SERVICE.STARTUPNAME}	does not match	{\$SERVICE.STARTUPNAME.NOT_MATCHES}	Remove

[Add](#)

[Update](#) [Clone](#) [Test](#) [Delete](#) [Cancel](#)



Deploying and configuring Zabbix agent on Windows

EXTENDING ZABBIX AGENT ON WINDOWS

EXTENDING ZABBIX AGENT ON WINDOWS

There are multiple ways how we can extend Zabbix agent on both Windows and Unix-like operating systems

- ⚡ Executing scripts and commands with User parameters
- ⚡ Collecting and sending custom metrics with Zabbix sender
- ⚡ *system.run[command,<mode>]* item
 - ✓ Can be used in HostnameItem or HostMetadataItem
- ⚡ Modules for Zabbix agent
- ⚡ GO plugins for Zabbix agent 2

CUSTOM SCRIPTS AND COMMANDS ON WINDOWS

Zabbix agent is language-agnostic when executing custom scripts

🔴 On Windows, we can utilize PowerShell to obtain a lot of useful information

Example: Obtaining number of days since last Windows update has been performed

```
$date = Get-Date
$diff = (Get-HotFix | Sort-Object -Property InstalledOn)[-1] | Select-Object InstalledOn
$diff3 = New-TimeSpan -Start $diff.InstalledOn -end $date
write-host $diff3.days
```

```
UserParameter=UpdateDays, powershell.exe -file C:\ZabbixTest\DaysSinceLastUpdate.ps1
```

CUSTOM SCRIPTS AND COMMANDS ON WINDOWS

Example: Obtaining number of days since last Windows update has been performed

The image shows a Zabbix web interface. The top navigation bar includes 'All hosts / Windows host', 'Enabled' status, 'ZBX' logo, and counts for 'Items 20', 'Triggers 8', 'Graphs 2', 'Discovery rules 1', and 'Web scenarios'. Below this, there are tabs for 'Item', 'Tags', and 'Preprocessing'. The main configuration area for an item is visible, with the following fields:

- * Name: Days since last update
- Type: Zabbix agent
- * Key: UpdateDays
- Type of information: Numeric (unsigned)
- * Host interface: 192.168.1.140:10050
- Units: !days
- * Update interval: 1d

A 'Test item' dialog box is overlaid on the configuration. It contains the following fields:

- Get value from host:
- * Host address: 192.168.1.140
- Proxy: (no proxy)
- Value: 12 (highlighted with a red border)
- Not supported

ZABBIX

Deploying and configuring Zabbix agent on Windows

ZABBIX AGENT ON WINDOWS – QUESTIONS AND TROUBLESHOOTING

ZABBIX AGENT TROUBLESHOOTING

- ⚡ If you're getting *Interrupted system call* errors, check your Windows firewall
- ⚡ Check your log file for errors (*By default stored in the root of the C: drive*)
- ⚡ Make sure that your Zabbix agent service is started
- ⚡ Don't forget – not every item key is supported on every OS
- ⚡ If Windows performance counters are reporting wrong values – try rebuilding them!*

*<https://docs.microsoft.com/en-us/troubleshoot/windows-server/performance/manually-rebuild-performance-counters>

ZABBIX AGENT COMMON QUESTIONS

Q: Can I run multiple instances of Zabbix agent on a single machine?

A: Yes, but each agent needs to use their own configuration file and listen on a unique port.

Q: Can I define UserParameters in a separate configuration file?

A: Yes, but you need to include the file in the *Include* option in the Zabbix agent configuration file

Q: Can I automate Zabbix agent deployment?

A: Yes, try using logon scripts or Group policy with the Zabbix agent MSI package

ZABBIX

QUESTIONS?

ARTŪRS LONTONS
TECHNICAL MARKETING ENGINEER

ZABBIX