

## Windows-specific item keys

### Item keys

The table provides details on the item keys that you can use with Zabbix Windows agent only.

Key			
Description	Return value	Parameters	Comments
<b>eventlog[name,&lt;regexp&gt;,&lt;severity&gt;,&lt;source&gt;,&lt;eventid&gt;,&lt;maxlines&gt;,&lt;mode&gt;]</b>			
Event log monitoring.	Log	<p><b>name</b> - name of event log</p> <p><b>regexp</b> - regular expression describing the required pattern</p> <p><b>severity</b> - regular expression describing severity</p> <p>This parameter accepts the following values:  <i>"Information", "Warning", "Error", "Critical", "Verbose"</i> (since Zabbix 2.2.0 running on Windows Vista or newer)</p> <p><b>source</b> - regular expression describing source identifier (regular expression is supported since Zabbix 2.2.0)</p> <p><b>eventid</b> - regular expression describing the event identifier(s)</p> <p><b>maxlines</b> - maximum number of new lines per second the agent will send to Zabbix server or proxy. This parameter overrides the value of 'MaxLinesPerSecond' in <a href="#">zabbix_agentd.win.conf</a></p> <p><b>mode</b> - possible values: <i>all</i> (default), <i>skip</i> - skip processing of older data (affects only newly created items that have not returned any data yet).</p>	<p>The item must be configured as an <a href="#">active check</a>.</p> <p>Examples:                      ⇒ eventlog[Application]                      ⇒ eventlog[Security,,"Failure Audit",,^(529 680)\$]                      ⇒ eventlog[System,,"Warning Error"]                      ⇒ eventlog[System,,,,^1\$]                      ⇒ eventlog[System,,,,@TWOSHORT] - here a <a href="#">custom regular expression</a> named <b>TWOSHORT</b> is referenced (defined as a <b>Result is TRUE</b> type, the expression itself being <b>^1\$ ^70\$</b>).</p> <p>The mode parameter is supported since Zabbix 2.0.0.                      "Windows Eventing 6.0" is supported since Zabbix 2.2.0.</p> <p>See also additional information on <a href="#">log monitoring</a>.</p>
<b>net.if.list</b>			

Key			
Description	Return value	Parameters	Comments
Network interface list (includes interface type, status, IPv4 address, description).	Text		<p>Supported since Zabbix agent version 1.8.1. Multi-byte interface names supported since Zabbix agent version 1.8.6. Disabled interfaces are not listed.</p> <p>Note that enabling/disabling some components may change their ordering in the Windows interface name.</p> <p>Some Windows versions (for example, Server 2008) might require the latest updates installed to support non-ASCII characters in interface names.</p>
<b>perf_counter[counter,&lt;interval&gt;]</b>			
Value of any Windows performance counter.	Integer, float, string or text (depending on the request)	<p><b>counter</b> - path to the counter</p> <p><b>interval</b> - last N seconds for storing the average value.</p> <p>The <code>interval</code> must be between 1 and 900 seconds (included) and the default value is 1.</p>	<p>Performance Monitor can be used to obtain list of available counters. Until version 1.6 this parameter will return correct value only for counters that require just one sample (like \System\Threads). It will not work as expected for counters that require more than one sample - like CPU utilisation. Since 1.6, <b>interval</b> is used, so the check returns an average value for last "interval" seconds every time.</p> <p>See also: <a href="#">Windows performance counters</a>.</p>
<b>proc_info[process,&lt;attribute&gt;,&lt;type&gt;]</b>			

Key			
Description	Return value	Parameters	Comments
Various information about specific process(es).	Float	<p><b>process</b> - process name</p> <p><b>attribute</b> - requested process attribute.</p> <p><b>type</b> - representation type (meaningful when more than one process with the same name exists)</p>	<p>The following attributes are supported:</p> <p><i>vmsize</i> (default) - size of process virtual memory in Kbytes</p> <p><i>wkset</i> - size of process working set (amount of physical memory used by process) in Kbytes</p> <p><i>pf</i> - number of page faults</p> <p><i>ktime</i> - process kernel time in milliseconds</p> <p><i>utime</i> - process user time in milliseconds</p> <p><i>io_read_b</i> - number of bytes read by process during I/O operations</p> <p><i>io_read_op</i> - number of read operation performed by process</p> <p><i>io_write_b</i> - number of bytes written by process during I/O operations</p> <p><i>io_write_op</i> - number of write operation performed by process</p> <p><i>io_other_b</i> - number of bytes transferred by process during operations other than read and write operations</p> <p><i>io_other_op</i> - number of I/O operations performed by process, other than read and write operations</p> <p><i>gdiobj</i> - number of GDI objects used by process</p> <p><i>userobj</i> - number of USER objects used by process</p> <p>Valid types are:</p> <p><i>avg</i> (default) - average value for all processes named &lt;process&gt;</p> <p><i>min</i> - minimum value among all processes named &lt;process&gt;</p> <p><i>max</i> - maximum value among all processes named &lt;process&gt;</p> <p><i>sum</i> - sum of values for all processes named &lt;process&gt;</p> <p>Examples:</p> <p>⇒ <code>proc_info[iexplore.exe,wkset,sum]</code> - to get the amount of physical memory taken by all Internet Explorer processes</p> <p>⇒ <code>proc_info[iexplore.exe,pf,avg]</code> - to get the average number of page faults for Internet Explorer processes</p> <p>Note that on a 64-bit system, a 64-bit Zabbix agent is required for this item to work correctly.</p> <p>Note: <i>io_*</i>, <i>gdiobj</i> and <i>userobj</i> attributes are available only on Windows 2000 and later versions of Windows, not on Windows NT 4.0.</p>

Key			
Description	Return value	Parameters	Comments
<b>service_state[service]</b>			
State of a service.	0 - running 1 - paused 2 - start pending 3 - pause pending 4 - continue pending 5 - stop pending 6 - stopped 7 - unknown 255 - no such service	<b>service</b> - a real service name or its display name as seen in MMC Services snap-in	
<b>services[&lt;type&gt;,&lt;state&gt;,&lt;exclude&gt;]</b>			
Listing of services.	0 - if empty  Text - list of services separated by a newline	<b>type</b> - <i>all</i> (default), <i>automatic</i> , <i>manual</i> or <i>disabled</i> <b>state</b> - <i>all</i> (default), <i>stopped</i> , <i>started</i> , <i>start_pending</i> , <i>stop_pending</i> , <i>running</i> , <i>continue_pending</i> , <i>pause_pending</i> or <i>paused</i> <b>exclude</b> - services to exclude from the result. Excluded services should be listed in double quotes, separated by comma, without spaces.	Examples: ⇒ services[,started] - list of started services ⇒ services[automatic, stopped] - list of stopped services, that should be run ⇒ services[automatic, stopped, "service1,service2,service3"] - list of stopped services, that should be run, excluding services with names service1, service2 and service3  The exclude parameter is supported since Zabbix 1.8.1.
<b>wmi.get[&lt;namespace&gt;,&lt;query&gt;]</b>			
Execute WMI query and return the first selected object.	Integer, float, string or text (depending on the request)	<b>namespace</b> - WMI namespace <b>query</b> - WMI query returning a single object	This key is supported starting with Zabbix 2.2.0.  Example: ⇒ wmi.get[root\cimv2,select status from Win32_DiskDrive where Name like '%PHYSICALDRIVE0%'] - returns the status of the first physical disk

## Monitoring Windows services

This tutorial provides step-by-step instructions for setting up the monitoring of Windows services. It is assumed that Zabbix server and agent are configured and operational.

To monitor the up/down status of a service you need to perform the following steps:

## Step 1

Get the service name.

You can get that name by going to the services mmc and bringing up the properties of the service. In the General tab you should see a field called 'Service name'. The value that follows is the name you will use when setting up an item for monitoring.

For example, if you wanted to monitor the “workstation” service then your service might be: **lanmanworkstation**.

## Step 2

Configure an item for monitoring the service, with:

- *Key*: service\_state[lanmanworkstation]
- *Type of information*: Numeric (unsigned)
- *Show value*: select the *Windows service state* value mapping

From:  
<https://www.zabbix.com/documentation/2.4/> - **Zabbix Documentation 2.4**

Permanent link:  
[https://www.zabbix.com/documentation/2.4/manual/config/items/itemtypes/zabbix\\_agent/win\\_keys](https://www.zabbix.com/documentation/2.4/manual/config/items/itemtypes/zabbix_agent/win_keys)

Last update: **2016/11/15 06:30**

