Nagios XI - WMI Troubleshooting

Article Number: 579 | Rating: Unrated | Last Updated: Mon, May 6, 2019 at 6:20 PM

Overview

This KB article provides contains troubleshooting steps for Windows Management Instrumentation (WMI) problems.

Permission Denied

You might experience this error message even though the plugin tests are successful in a terminal session:

This text indicates an error message:

```
UNKNOWN - Permission denied when trying to store the state data. Sometimes this happens if you have been testing the plugin from the co
as a different user to the Nagios process user. You will need to change the permissions on the file or remove it. The actual error text
can't create /tmp/cwpss_checkcpu__1025143___.state: Permission denied at /usr/local/nagios/libexec/check_wmi_plus.pl line 2460
```

The text does explain that this is a file permission issue. A very common problem that occurs is when you have been experimenting with a new command at the command line as the r

Check the permissions of the files with this command:

```
ls -ls /tmp/*.state
```

Here you can see that the `root` user/group is the owner of the file:

```
-rw-r--r-- 1 root root 91 Apr 24 16:10 /tmp/cwpss_checkcpu__1025143___.state
```

The simplest option is to delete the files with this command:

```
rm -rf /tmp/*.state
```

After **Nagios** executes the WMI service command you can see that the `nagios` user/group is the owner of the file:

```
-rw-rw-r-- 1 nagios nagios 105 Apr 24 16:24 /tmp/cwpss_checkcpu__1025143___.state
```

Need at least 2 WMI samples%

You see this error message even after executing the command repeatedly:

```
OK (Sample Period 17 sec) - Average CPU Utilisation Need at least 2 WMI samples%
```

The reason for the message is that the WMI user account does not have sufficient permissions. This can be resolved by adding the user account to the **Performance Log Users** se

Debug

Enabling debugging will produce extra output that can help diagnose the source of the issue. There are two different types of debugging options available, the `check_wmi_plus.pl`

`check_wmi_plus.pl` Plugin Debugging

This method of debugging is for the plugin itself.

When executing a command, using **`-d`** will produce extra debug information. For example:

```
/usr/local/nagios/libexec/check_wmi_plus.pl -H 10.25.14.3 -u wmiagent -p wmiagent -m checkcpu -w '80' -c '90' -d
```

The is the first and last few lines of output that is produced:

```
Base Dir: /usr/local/nagios/libexec
Conf File Dir: /usr/local/nagios/libexec
Loaded Conf File /usr/local/nagios/libexec/check_wmi_plus.conf
Starting Keep State Mode
STATE FILE: /tmp/cwpss_checkcpu__1025143___.state
...
UNKNOWN - The WMI query had problems. You might have your username/password wrong or the user's access level is too low. Wmic error tex
[librpc/rpc/dcerpc_util.c:1290:dcerpc_pipe_auth_recv()] Failed to bind to uuid 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57 - NT_STATUS_NET_WRI
[librpc/rpc/dcerpc_connect.c:790:dcerpc_pipe_connect_b_recv()] failed NT status (c0000022) in dcerpc_pipe_connect_b_recv
[wmi/wmic.c:196:main()] ERROR: Login to remote object.
NTSTATUS: NT_STATUS_ACCESS_DENIED - Access denied
```

WMI Debugging

This method of debugging will produce WMI API debugging output. The `--extrawmicarg` argument passes native WMI arguments which can help identify issues.

When executing a command, using **`--extrawmicarg "--debuglevel=4"`** will produce extra debug information. For example:

```
/usr/local/nagios/libexec/check_wmi_plus.pl -H 10.25.14.3 -u wmiagent -p wmiagent -m checkcpu -w '80' -c '90'  --extrawmicarg "--debugl
```

The is the first and last few lines of output that is produced:

```
UNKNOWN - The WMI query had problems. You might have your username/password wrong or the user's access level is too low. Wmic error tex
[param/loadparm.c:587:init_globals()] Initialising global parameters
[param/loadparm.c:2462:lp_load()] lp_load: refreshing parameters from /dev/null
[param/params.c:556:pm_process()] params.c:pm_process() - Processing configuration file "/dev/null"
[param/loadparm.c:2471:lp_load()] pm_process() returned Yes
...
[auth/ntlmssp/ntlmssp.c:72:debug_ntlmssp_flags()] Got NTLMSSP neg_flags=0x60088205
  NTLMSSP_NEGOTIATE_UNICODE
  NTLMSSP_REQUEST_TARGET
  NTLMSSP_NEGOTIATE_NTLM
  NTLMSSP_NEGOTIATE_ALWAYS_SIGN
  NTLMSSP_NEGOTIATE_NTLM2
  NTLMSSP_NEGOTIATE_128
  NTLMSSP_NEGOTIATE_KEY_EXCH
[librpc/rpc/dcerpc_util.c:1290:dcerpc_pipe_auth_recv()] Failed to bind to uuid 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57 - NT_STATUS_NET_WRI
[librpc/rpc/dcerpc_connect.c:790:dcerpc_pipe_connect_b_recv()] failed NT status (c0000022) in dcerpc_pipe_connect_b_recv
[wmi/wmic.c:196:main()] ERROR: Login to remote object.
NTSTATUS: NT_STATUS_ACCESS_DENIED - Access denied
```

FQDN vs IP Address

You see error messages similar to this:

```
[librpc/rpc/dcerpc_connect.c:329:dcerpc_pipe_connect_ncacn_ip_tcp_recv()] failed NT status (c00000b5) in dcerpc_pipe_connect_ncacn_ip_t
[librpc/rpc/dcerpc_connect.c:790:dcerpc_pipe_connect_b_recv()] failed NT status (c00000b5) in dcerpc_pipe_connect_b_recv
CLASS: Win32_ComputerSystem
```

It has been observed that this problem never occurs when querying a Windows machine via IP address, it only occurs when using a FQDN DNS record (intermittently). A solution was

https://support.nagios.com/forum/viewtopic.php?f=6&t=41864&start=30#p212361

Perform A Raw Query

Sometimes it can be helpful to perform a query directly on the windows machine to confirm that WMI is working and the data actually exists. The first step is identifying the query being

```
/usr/local/nagios/libexec/check_wmi_plus.pl -H 10.25.14.3 -u wmiagent -p wmiagent -m checkcpu -d
```

In the output the following is the information you are after:

```
Round #2 of 2
QUERY: /usr/bin/wmic '-U' 'USER%PASS' '--namespace' 'root/cimv2' '//10.25.14.3' 'select PercentProcessorTime,Timestamp_Sys100NS from Wi
```

Now that you have that information, open PowerShell on your Windows machine and execute the following command:

```
Get-WmiObject -Query 'select PercentProcessorTime,Timestamp_Sys100NS from Win32_PerfRawData_PerfOS_Processor where Name="_Total"'
```

The following output is an example of successful output:

```
__GENUS              : 2
__CLASS              : Win32_PerfRawData_PerfOS_Processor
__SUPERCLASS         :
__DYNASTY            :
__RELPATH            :
__PROPERTY_COUNT     : 2
__DERIVATION         : {}
__SERVER             :
__NAMESPACE          :
__PATH               :
PercentProcessorTime : 51966897119
Timestamp_Sys100NS   : 131374922305304314
```

The last two lines indicate the objects being queried and that they actually have values. If there were problems with WMI within Windows then you would not get this output and any e

Additional Permissions

When you run the WMI Configuration Wizard, on Step 2 you receive the error:

```
UNKNOWN - The WMI query had problems. The error text from wmic is: [wmi/wmic.c:212:main()]
ERROR: Retrieve result data.
NTSTATUS: NT code 0x80041003 - NT code 0x80041003
```

Some additional permissions need to be applied to your Windows machine.

> ⚠ **Warning**
>
> The following commands have the potential to cause problems with your Windows server if not followed correctly. The following Microsoft article provides more information the steps being p
>
> https://msdn.microsoft.com/en-us/library/aa374928.aspx

On the Windows machine in a command prompt (with Administrator permissions) execute the following command:

```
wmic useraccount where name='wmiagent' get sid
```

That command assumed the user account for WMI is `wmiagent`.

The output will be something like:

```
SID
S-1-5-21-2343277006-4046424753-211511363-1002
```

That `SID` number is what you need to use in an upcoming command.

Now execute the following command to get the current security descriptor (SD) for `SCMANAGER`.

```
sc sdshow SCMANAGER
```

The output will be something like:

```
D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)
```

This SD string will be used in an upcoming command, it is specific to your Windows machine and you will need to use it.

You need to **add** an entry to the `SD` that contains your `SID`, for example using the `SID` above:

```
(A;;CCLCRPRC;;;S-1-5-21-2343277006-4046424753-211511363-1002)
```

This needs to be inserted to the beginning of the `SD` after the `D:`, using the example above it looks like:

```
D:(A;;CCLCRPRC;;;S-1-5-21-2343277006-4046424753-211511363-1002)(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;
```

Now that you have altered the SD, execute the following command using your new SD to apply the SD:

```
sc sdset SCMANAGER D:(A;;CCLCRPRC;;;S-1-5-21-2343277006-4046424753-211511363-1002)(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;C
```

After executing the command you should re-run the configuration wizard and see if the problem is resolved.

Administrative Permissions

Sometimes the standard permission levels defined in the Monitoring Windows Using WMI documentation do not expose all the monitoring capabilities of the WMI plugin. In these case

- Performance Monitor Users
- Administrators

Access Denied When Using Domain Account

You might receive an error message like the following when authentication with a Windows domain account:

```
UNKNOWN - The WMI query had problems. You might have your username/password wrong or the user's access level is too low. Wmic error tex
[librpc/rpc/dcerpc_util.c:1290:dcerpc_pipe_auth_recv()] Failed to bind to uuid 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57 - NT_STATUS_NET_WRI
```

```
[librpc/rpc/dcerpc_connect.c:790:dcerpc_pipe_connect_b_recv()] failed NT status (c0000022) in dcerpc_pipe_connect_b_recv
[wmi/wmic.c:196:main()] ERROR: Login to remote object.
NTSTATUS: NT_STATUS_ACCESS_DENIED - Access denied
```

The solution to this problem is to use a forward slash `/` to separate the domain name and user account, for example:

```
/usr/local/nagios/libexec/check_wmi_plus.pl -H 10.25.14.3 -u your_domain/wmiagent -p wmiagent -m checkcpu
```

Force NTLMv2

You may be required to force the plugin to use NTLMv2, this can be changed globally. Open the `check_wmi_plus.conf` file in the vi editor with the following command:

```
vi /usr/local/nagios/libexec/check_wmi_plus.conf
```

*When using the **vi** editor, to make changes press **i** on the keyboard first to enter insert mode. Press **Esc** to exit insert mode.*

Jump to line 85 with the following command:

```
:85
```

Locate the following line:

```
our @opt_extra_wmic_args=(); # extra arguments to pass to wmic
```

Add "**--option=client ntlmv2 auth=Yes**" in between the brackets as follows:

```
our @opt_extra_wmic_args=("--option=client ntlmv2 auth=Yes"); # extra arguments to pass to wmic
```

When you have finished, save the changes in vi by typing:

```
:wq
```

and press **Enter**.

Service Not Listed In Wizard

When running the Windows WMI wizard it does not find all of the services on the server. One solution available is that on Step 1 of the wizard there is a field called **Truncate Output**

Another reason for this is that the user account used for WMI does not have `SERVICE_QUERY_STATUS (LC)` permissions on the service. The following steps will show you how to ad

> ⚠ **Warning**
>
> The following commands have the potential to cause problems with your Windows server if not followed correctly. The following article provides more information the steps being performed
>
> https://blogs.msmvps.com/erikr/2007/09/26/set-permissions-on-a-specific-service-windows/%E2%80%8B/

On the Windows machine in a command prompt (with Administrator permissions) execute the following command:

```
wmic useraccount where name='wmiagent' get sid
```

That command assumed the user account for WMI is `wmiagent`.

The output will be something like:

```
SID
S-1-5-21-3480785720-802978297-2857457638-1002
```

That `SID` number is what you need to use in an upcoming command.

Now execute the following command to get the current security descriptor (SD) for the service, this command is going to query the `WinDefend` service.

```
sc sdshow WinDefend
```

The output will be something like:

```
D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464)(A;OICIIO;GA;;;S-1-5-80-956008885-341
```

In the SD string you can see it begins with `D:` and has sets of access control lists (ACL) which are separated by round brackets `()`.

You will also see there is an `S:` section that also has ACLs which are separated by round brackets `()`.

Here is that same output broken down:

```
D:
(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464)
(A;OICIIO;GA;;;S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464)
(A;;CCLCSWRPWPDTLOCRRC;;;SY)
(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)
(A;;CCLCSWRPLOCRRC;;;IU)
(A;;CCLCSWRPLOCRRC;;;SU)
S:
(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)
```

You need to **add** an entry to the end of the `D:` section that contains your `SID`:

```
(A;;LC;;;<SID>)
```

For example using the `SID` above:

```
(A;;LC;;;S-1-5-21-3480785720-802978297-2857457638-1002)
```

This needs to be inserted to the end of the `SD` after the last ACL before `S:`, using the example above it looks like:

```
D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464)(A;OICIIO;GA;;;S-1-5-80-956008885-341
```

Now that you have altered the SD, execute the following command using your new SD to apply the SD on the `WinDefend` service:

```
sc sdset WinDefend D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464)(A;OICIIO;GA;;;S-1
```

After executing the command you should re-run the configuration wizard and see if the problem is resolved.

If this does not resolve your problem then you may need to look at an alternative agent like NCPA to perform your monitoring.

Firewall Problems

When you run the WMI Configuration Wizard, on Step 2 you receive the error:

```
UNKNOWN - The WMI query had problems. The error text from wmic is: [wmi/wmic.c:196:main()]
ERROR: Login to remote object.
NTSTATUS: NT code 0x800706ba - NT code 0x800706ba
```

It's possible that the Windows Firewall is not allowing the traffic through. In **Windows Firewall** under **Allowed Programs** check to make sure that **Windows Management Instru**

Documentation - Monitoring Windows Using WMI

WMI Plugin Not Installed Correctly

If the status information on the **Service Detail** page is empty (null) or states "Install wmic", the problem is that the WMIC plugins were not installed properly. Please refer to the insta

Documentation - How To Install The WMI Client For Nagios XI

Final Thoughts

For any support related questions please visit the Nagios Support Forums at:

http://support.nagios.com/forum/

Posted by: **tlea** - Mon, Apr 24, 2017 at 1:51 AM. This article has been viewed 5529 times.

Online URL: https://support.nagios.com/kb/article/nagios-xi-wmi-troubleshooting-579.html