



Purpose

This document describes how to automatically restart problematic services on Windows machines using the Nagios Cross-Platform Agent (NCPA).

Target Audience

This document is intended for use by Nagios XI Administrators who want to automate restarting of problematic services on their Windows machines. A basic knowledge of NCPA is recommended.

Prerequisites

You should already have NCPA configured on the Windows machine you would like to restart services on, please refer to the following documentation:

[NCPA Installation Instructions](#)

Background Information

In this guide you will be shown how to use an event handler to restart a service on a Windows machine. A script will be created to do this task that will be executed via NCPA.

Create A Batch File To Restart The Service

On your windows machine open **Notepad** and paste in the following code:

```
@echo off
net stop %1
net start %1
@exit 0
```

Once completed, save it as a batch file called **restart_service.bat** in your NCPA plugins directory:

```
C:\Program Files\Nagios\NCPA\plugins\  
C:\Program Files (x86)\Nagios\NCPA\plugins\  

```

The `%1` argument is the name of the service, this will be received from an event handler which will be created later in this document.

Test The Command From The Nagios XI Server

Now we will test from the Nagios XI server that the command you just added to NCPA is working. This example is going to restart the `spooler` service as it is unlikely to cause any issues. Establish a terminal session to your Nagios XI server and execute the following command:

```
cd /usr/local/nagios/libexec
./check_ncpa.py -H 10.25.14.3 -P 5693 -t Str0ngT0k3n -M 'plugins/restart_service.bat' -a spooler
```

```
[root@xi-r7x-x64 libexec]# ./check_ncpa.py -H 10.25.14.3 -P 5693 -t Str0ngT0k3n -M 'plugins/restart_service.bat' -a spooler
The Print Spooler service is stopping.
The Print Spooler service was stopped successfully.

The Print Spooler service is starting.
The Print Spooler service was started successfully. | 'status'=0;1;2;
```

You can see from the screenshot that we received back the results from the `restart_service.bat` script, it appears to be working.

Create Event Handler Script

Next we need to create a script that will be used by Nagios XI for the event handler. The script will be called `restart_service.sh` and will be located in the `/usr/local/nagios/libexec/` directory on the Nagios XI server. Execute the following command:

```
vi /usr/local/nagios/libexec/restart_service.sh
```

When using `vi`, to make changes press `i` on the keyboard first to enter insert mode and press `Esc` to exit insert mode.

Paste the code on the following page into the terminal session:

```
#!/bin/sh
case "$1" in
    OK)
        ;;
    WARNING)
        ;;
    UNKNOWN)
        ;;
    CRITICAL)
        /usr/local/nagios/libexec/check_ncpa.py -H "$2" -P 5693 -t "$3" -M 'plugins/restart_service.bat' -a "$4"
        ;;
esac
exit 0
```

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

```
:wq
```

and press Enter.

Now execute the following commands to set the correction permissions:

CentOS/RHEL

```
chown apache:nagios /usr/local/nagios/libexec/restart_service.sh
chmod 775 /usr/local/nagios/libexec/restart_service.sh
```

Debian/Ubuntu

```
chown www-data:nagios /usr/local/nagios/libexec/restart_service.sh
chmod 775 /usr/local/nagios/libexec/restart_service.sh
```

You can now test the script works by executing the following command:

```
/usr/local/nagios/libexec/restart_service.sh CRITICAL 10.25.14.3 Str0ngT0k3n spooler
```

When the script is run, it receives three arguments which are referenced as \$1, \$2, \$3, \$4 in the script.

\$1 = The state of the service.

\$2 = The host address of the Windows server.

\$3 = The NCPA Token on the Windows server.

\$4 = The name of the service being restarted.

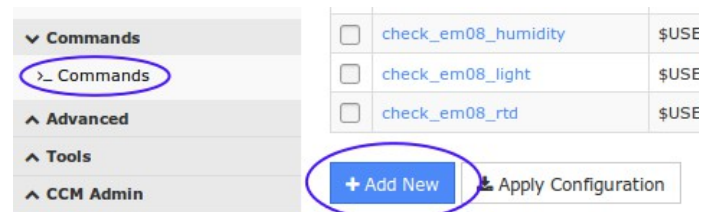
You can see from the script above that it's only when the service is in a CRITICAL state that the `restart_service.sh` command will be executed.

Create Event Handler

Now an event handler on the Nagios XI server will be created which will be used by your services.

Navigate to **Configure > Core Config Manager**.

Select **Commands** from the list on the left, click the **>_ Commands** link and then click the **Add New** button.



You will need to populate the fields with the following values:

Command

`Service Restart - Windows`

Command line

`$USER1$/restart_service.sh $SERVICESTATE$ $HOSTADDRESS$ $_SERVICE$SERVICE$`

Command type

`misc command`

Check the **Active** check box.

Click the **Save** button and then **Apply Configuration**.

Note: You will notice that the NCPA token `Str0ngT0k3n` has been hard coded in the command definition. This has been done to simplify this documentation, user macros is a better solution and is explained in the [Understanding The User Macros Component](#) documentation.

Command Management

Command Name *

Service Restart - Windows

Example: check_example

Command Line *

`$USER1$/restart_service.sh $SERVICESTATE$ $HOSTADDRESS$ Str0ngT0k3n $_SERVICESERVICE$`

Example: `$USER1$/check_example -H $HOSTADDRESS$ -P $ARG1$ $ARG2$`

Command Type:

misc command

Active ?

Available Plugins

Save

Cancel

Adding a Service Check

Now we will need to create a Service using the NCPA Monitoring Wizard. This guide will not go into the entire steps required, please refer to the steps in the following documentation:

[Monitoring Devices Using NCPA](#)

On **Step 2** of the wizard you need to select the **spooler** service from the list of **Services**.

Services

Specify which services should be running or stopped. Depending on the selected state you will receive an OK when the process is in the selected state and a CRITICAL if the process is not in the state selected.

Service Name	Expected Status
<input checked="" type="checkbox"/> Spooler	<input checked="" type="radio"/> Running <input type="radio"/> Stopped

[Add Another Service Check](#)

Running Processes

Specify which processes should be running, and how many should be.

Services listed by the NCPA Agent ✕

Select a service that is either running or stopped from the NCPA client host to automatically fill in the service name and the expected state.

Spooler (running)

Select this Service

Finish the wizard to create the new service.

Update Service With Event Handler

Now that the Nagios service is created we need to do two things:

- Select Event Handler
- Add the name of the service we want to restart as a custom variable to the service object. This is how the event handler knows what the name of the service is to restart.

Navigate to **Configure > Core Config Manager > Monitoring > Services**.

Click the service **Service status for: Spooler** to edit the service.

From the **Event handler** drop down list select the option **Service Restart - Windows**.

Service Management

Service Management

Common Settings | **Check Settings** | Alert Settings | Misc Settings

Initial state: Warning | Critical | Ok | Unreachable

Obsess over service: On | Off | Skip | Null

Check interval: 5 min

Event handler: Service Restart - Windows

Retry interval: 1 min

Event handler enabled: On | Off | Skip | Null

For **Event handler enabled** click **On**.

Click the **Misc Settings** tab and then click the **Manage Free Variables** button.

Service Management

Service Management

Common Settings | Check Settings | Alert Settings | **Misc Settings**

Notes: [Text Area]

VRML image: [Text Area]

Notes URL: [Text Area]

2D coords: x,y

3D coords: x,y,z

Manage Free Variables 1

We will be adding a custom variable so that the event handler knows the name of the service to restart.

Name:

`__SERVICE`

Value:

`spooler`

Click **Insert** and the variable will be added to the list on the right.

Name	Value	
_xiwizard	ncpa	✘
_SERVICE	spooler	✘

Click the **Close** button and then click the **Save** button. Click **Apply Configuration** for the changes to take affect.

In the event handler command you created, you can see the macro `$_SERVICE$SERVICE$` was used. This is how a service macro is referenced by the Nagios Core engine. More information on custom variables can be found here:

<https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/customobjectvars.html>

Test

To test simply stop the **Print Spooler** service on the Windows machine.

Open the **Services console** under **Administrative Tools**.

Right click the **Print Spooler** service and select **Stop**.

Service Name	Description	Status	Start Type	Path
Portable Device E...	Enforces gr...		Manual	Local System...
Power	Manages p...	Started	Automatic	Local System...
Print Spooler	Loads files t...	Started	Autom...	ce...
Problem Reports a...	This service ...		Manua...	ce...
Program Compati...	This service ...	Started	Manua...	ce...
Protected Storage	Provides pr...		Manua...	ce...
Quality Windows ...	Quality Win...		Manua...	ce...
Remote Access A...	Creates a co...		Manua...	ce...
Remote Access C...	Manages di...		Manua...	ce...
Remote Desktop ...	Remote Des...	Started	Manua...	ce...
Remote Desktop S...	Allows user...	Started	Manua...	ce...
Remote Desktop S...	Allows the r...	Started	Manua...	ce...
Remote Procedur...	The RPCSS ...	Started	Autom...	ce...
Remote Procedur...	In Windows		Manua...	Network S...

Wait for the Nagios service to go to a critical state or force the next check.

Once the Nagios XI **Print Spooler** service is in a **critical** state the event handler will be executed and the

Windows Print Spooler service will be restarted. The next time Nagios XI checks the **Print Spooler** service it will return to an **OK** state as the **Windows Print Spooler** service will now be running.

Troubleshooting

If the event handler does not appear to be working as expected, check the `/usr/local/nagios/var/nagios.log` file for any errors, for example:

```
[1481763272] SERVICE ALERT: 10.25.14.3;Print Spooler;CRITICAL;SOFT;1;spooler: Stopped
[1481763272] wproc: SERVICE EVENTHANDLER job 7 from worker Core Worker 12627 is a non-check
helper but exited with return code 13
[1481763272] wproc:   early_timeout=0; exited_ok=1; wait_status=3328; error_code=0;
[1481763272] wproc:   stderr line 01: execvp(/usr/local/nagios/libexec/restart_service.sh, ...)
failed. Errno is 13: Permission denied
```

In the log entries above you can see that the worker reported that it did not have permission to execute the `restart_service.sh` command.

Finishing Up

This completes the documentation on how to restart Windows services with NCPA and Nagios XI.

If you have additional questions or other support related questions, please visit us at our Nagios Support Forums:

<https://support.nagios.com/forum>

The Nagios Support Knowledgebase is also a great support resource:

<https://support.nagios.com/kb>