Restarting Windows Services with NCPA in Nagios XI 2024R1

Purpose

This document describes how Nagios XI Administrators can use the Nagios Cross-Platform Agent (NCPA) to automatically restart problematic services on Windows machines. A basic understanding 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 NCPA Installation Instructions documentation.

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:

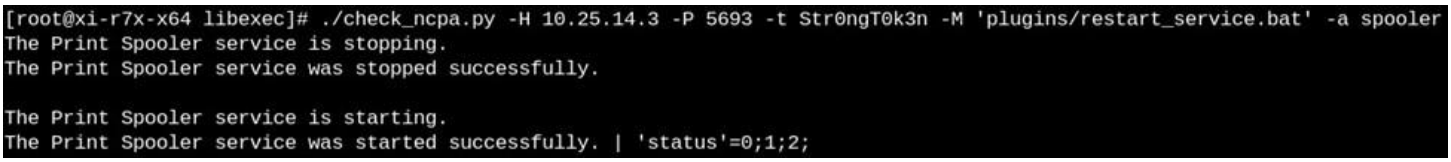
```
C:\Program Files\Nagios\NCPA\plugins\
C:\Program Files (x86)\Nagios\NCPA\plugins\
```

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
```



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/Oracle

```
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.

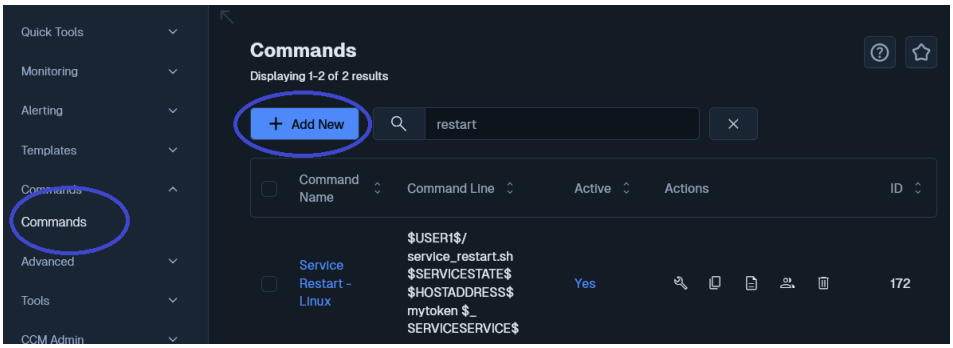
$4 = The name of the service being restarted.

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 create an event handler on the Nagios XI server to be used by your services.

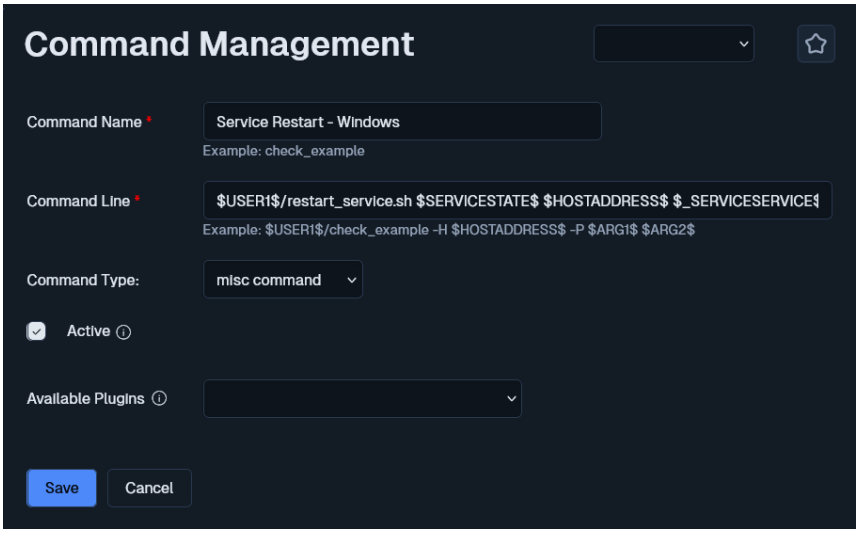
1. Navigate to **Configure > Core Config Manager > Commands > Commands**.
2. Click **Add New**.



3. You will need to populate the fields with the following values:
   - **Command Name:** Service Restart - Windows
   - **Command line:**

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

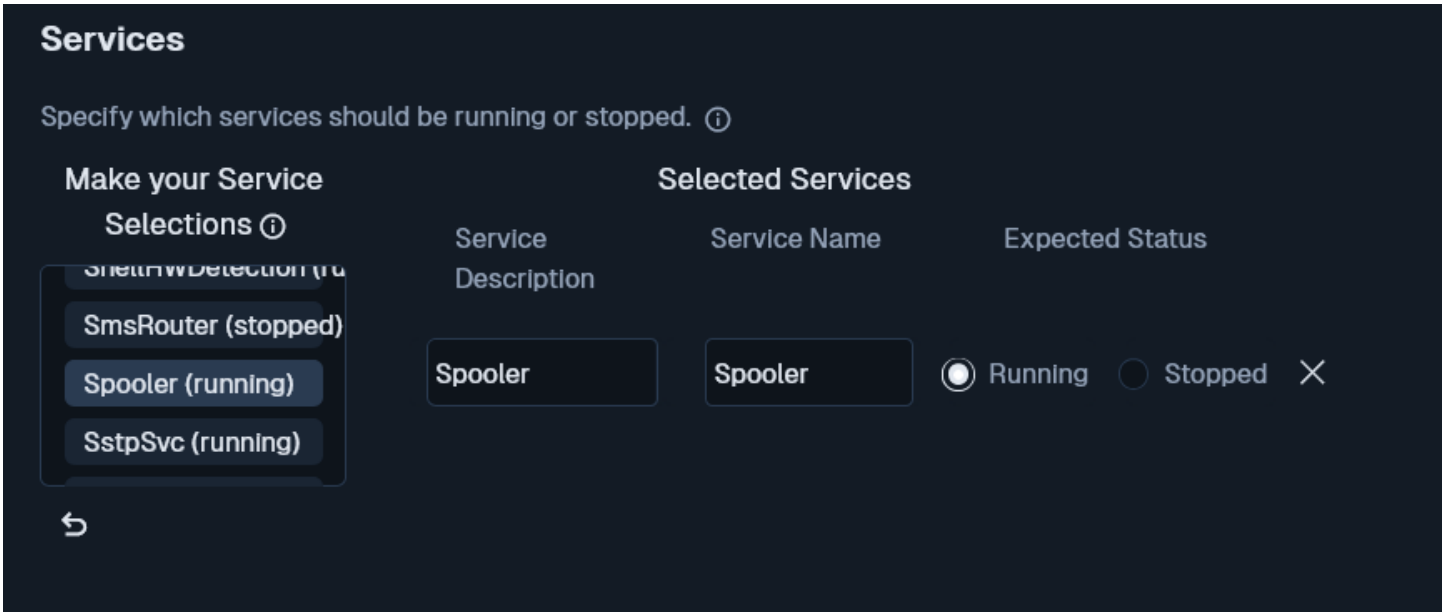
   - **Command type: misc command**
   - Check the **Active** box.
   - Click **Save** and then **Apply Configuration**.



Adding a Service Check

Now we will need to create a service using the **NCPA Configuration Wizard**. This guide will not go into the entire steps required, please refer to the steps in the following documentation for more details: Monitoring Devices Using NCPA

On Step 2 of the wizard, select the **Spooler** service from the list of **Services**.



Finish the wizard to create the new service.

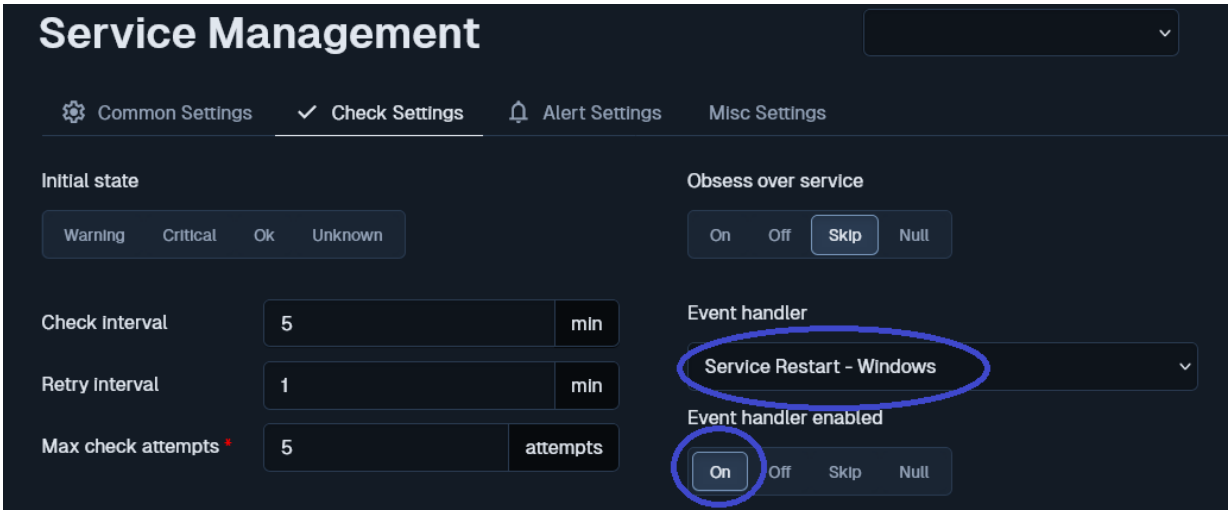
Update Service with Event Handler

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

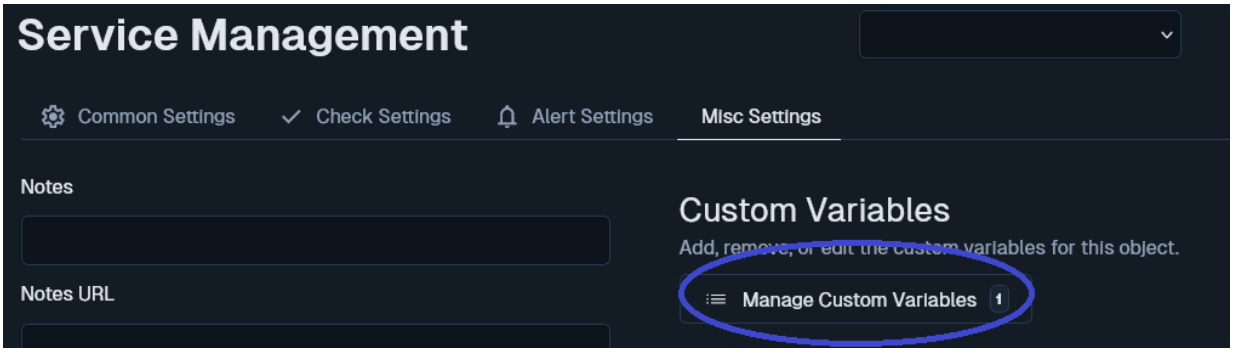
- Select Event Handler
- Add the name of the service we want to restart as a custom variable to the service object and add the NCPA token used to contact the NCPA agent on the windows system. This is how the event handler knows what the name of the service is to restart.

1. Navigate to **Configure > Core Config Manager > Monitoring > Services**.
2. Click the **Config Name** with the **Service Description** labeled as **Service status for: Spooler** to edit the service.

3. Click the **Check Settings** tab.
4. From the **Event handler** drop down list select the option **Service Restart - Windows**.
5. Under **Event handler enabled** click **On**.



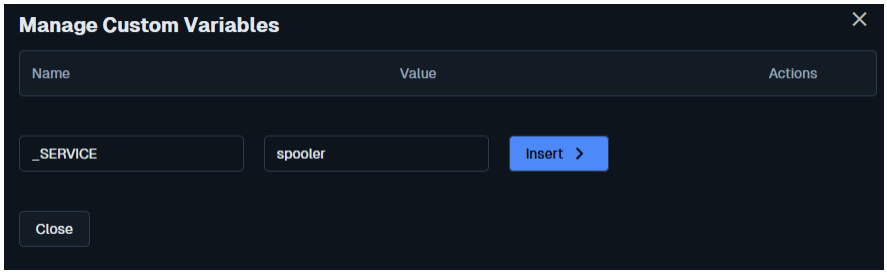
6. Click the **Misc Settings** tab and then click **Manage Custom Variables**.



7. We will be adding two custom variables so that the event handler knows the name of the service to restart and the token that is defined in the NCPA agent on the Windows Host.

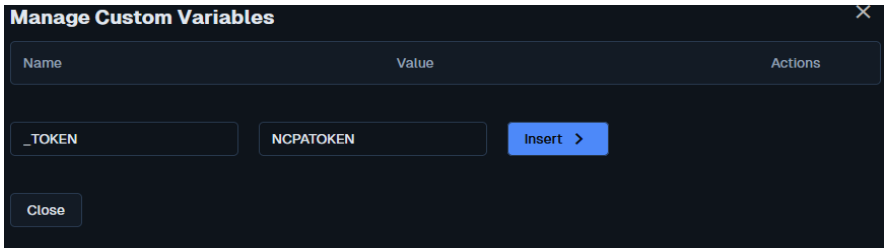
   Name: `_SERVICE`

   Value: `spooler`

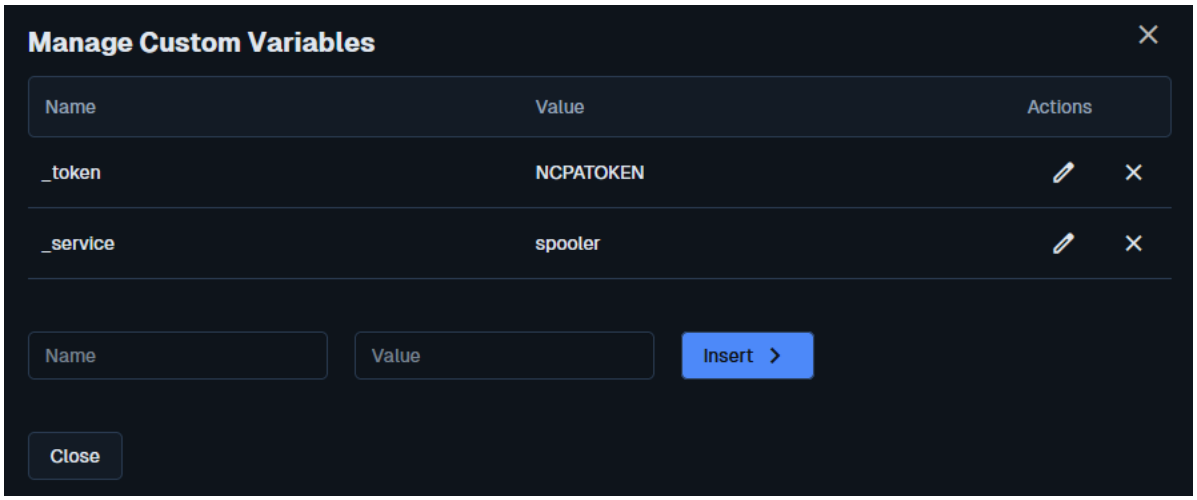


   Name: `_TOKEN`

   Value: `<The token used in the NCPA Agent>`



8. For each variable, enter the **Name** and **Value** then click **Insert**. The variable will then be added to the list. It should look like this when you have finished adding them both.



9. Click **Close** and then click **Save**. Click **Apply Configuration** for the changes to take effect.

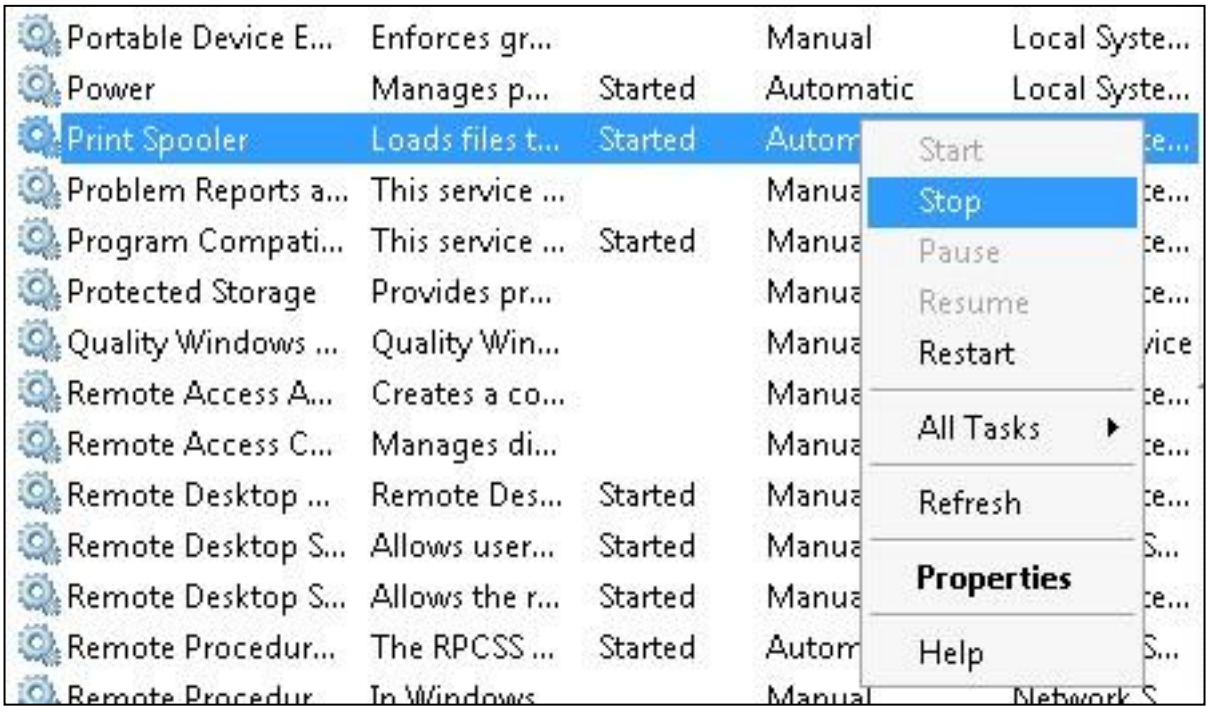
In the event handler command you created, you can see the macro `$_SERVICESERVICE$` and `$SERVICETOKEN` were used. This is how a service macro is referenced by the Nagios Core engine. More information on custom variables can be found here:

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

Testing the Event Handler

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

1. Open the **Services** console as an **Administrator**.
2. Right click the **Print Spooler** service and select **Stop**.



3. Wait for the Nagios service to go to a critical state or force the next check.
4. 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 restarting Windows services with NCPA in Nagios XI. If you have additional questions or other support-related questions, please visit us at our Nagios Support Forum, Nagios Knowledge Base, or Nagios Library:

Visit Nagios Support Forum Visit Nagios Knowledge Base Visit Nagios Library