Nagios Alerting Plugin

This plugin allows **dynaTrace to send alerts to a Nagios server** using NSCA. Alerts can be posted locally or remotely to Nagios. This plugin based on the jsendnsca java library and tested with Nagios, OP5, Icinga.

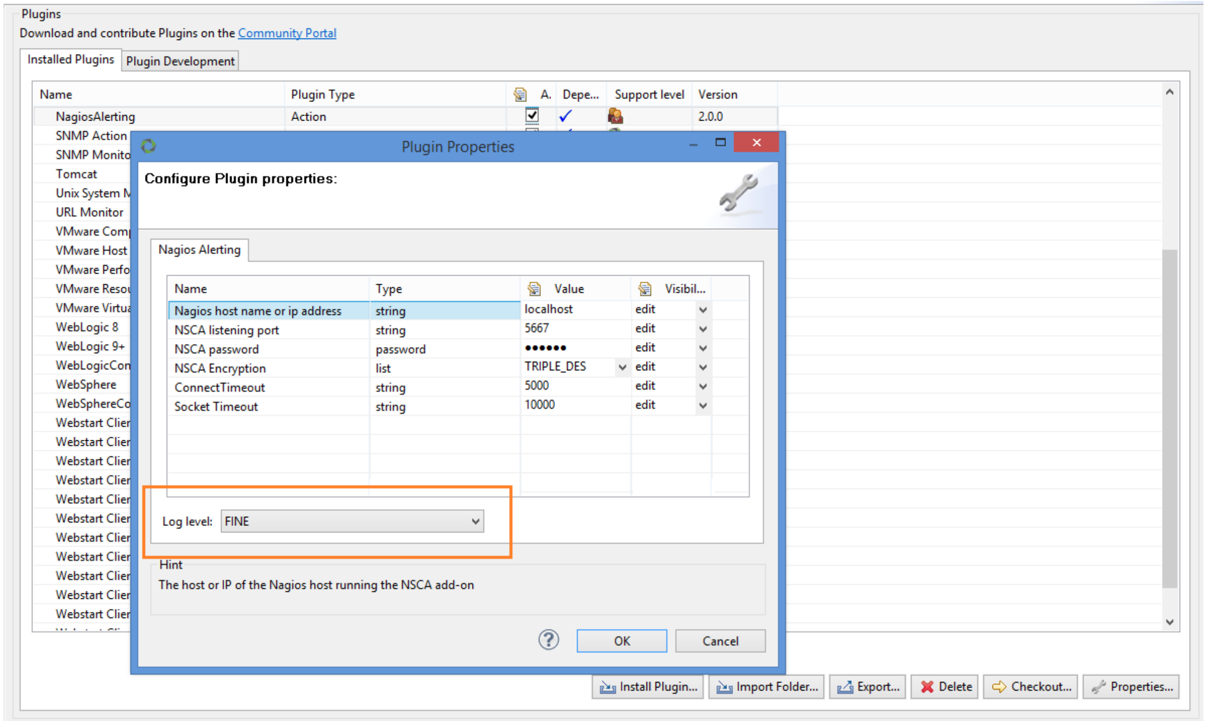
Special thanks to Peter Szegedi, who helped me in connection with Nagios and NSCA configuration.

Name	**Nagios Alerting Plugin 3.0**
Version	3.0.0 (2016.12.20)
dynaTrace Version	>= 6.0
Download	hu.bakaibalazs.dynatrace.nagios.NagiosAlerting_3.0.0.jar
Github	https://github.com/dynaTrace/Dynatrace-Nagios-Alerting-Plugin
License	LGPL v3
Support	Not Supported
Author	Balázs Bakai (balazs.bakai@telvice.hu) www.bakaibalazs.hu www.bakailab.hu Telvice Kft.
Release Notes	**3.0 - 2016.12.20** - remove not alphanumeric characters from the incident rule name - add description using this plugin with RedHat7/Centos7 - xinetd based nsca support - Nagios core, Nagios XI and OP5 support is tested with dynaTrace 6.3 **2.0 - 2015.03.26** - Easier configuration - The additional helper scripts are removed thanks to jsendnsca - Supports local and remote Nagios server - Timeouts added as parameter **1.0 - 2014.06.26** - Send "ok" notification to Nagios when the incident ends

Plugin installation

- Use dynaTrace client to install (Settings/dynaTrace Servers/Plugins/Install Plugin) the attached plugin binary jar file and activate the plugin
- Click on the properties button and setup the NSCSA and Nagios related parameters of the plugin. (TRIPLE_DES NSCA Encryption is suggested)
- If you need more information select the FINE log level else the INFO log level. Logs are available at System Information/dynaTrace

Server/Support Information/Log Files



Name	Plugin Type	A.	Depe...	Support level	Version
NagiosAlerting	Action	☑	✓		2.0.0
SNMP Action					
SNMP Monito					
Tomcat					
Unix System M					
URL Monitor					
VMware Comp					
VMware Host					
VMware Perfo					
VMware Resou					
VMware Virtu					
WebLogic 8					
WebLogic 9+					
WebLogicCon					
WebSphere					
WebSphereCo					
Webstart Clier					
Webstart Clier					
Webstart Clier					
Webstart Clier					
Webstart Clier					
Webstart Clier					
Webstart Clier					
Webstart Clier					
Webstart Clier					
Webstart Clier					
Webstart Clier					

Configure Plugin properties:

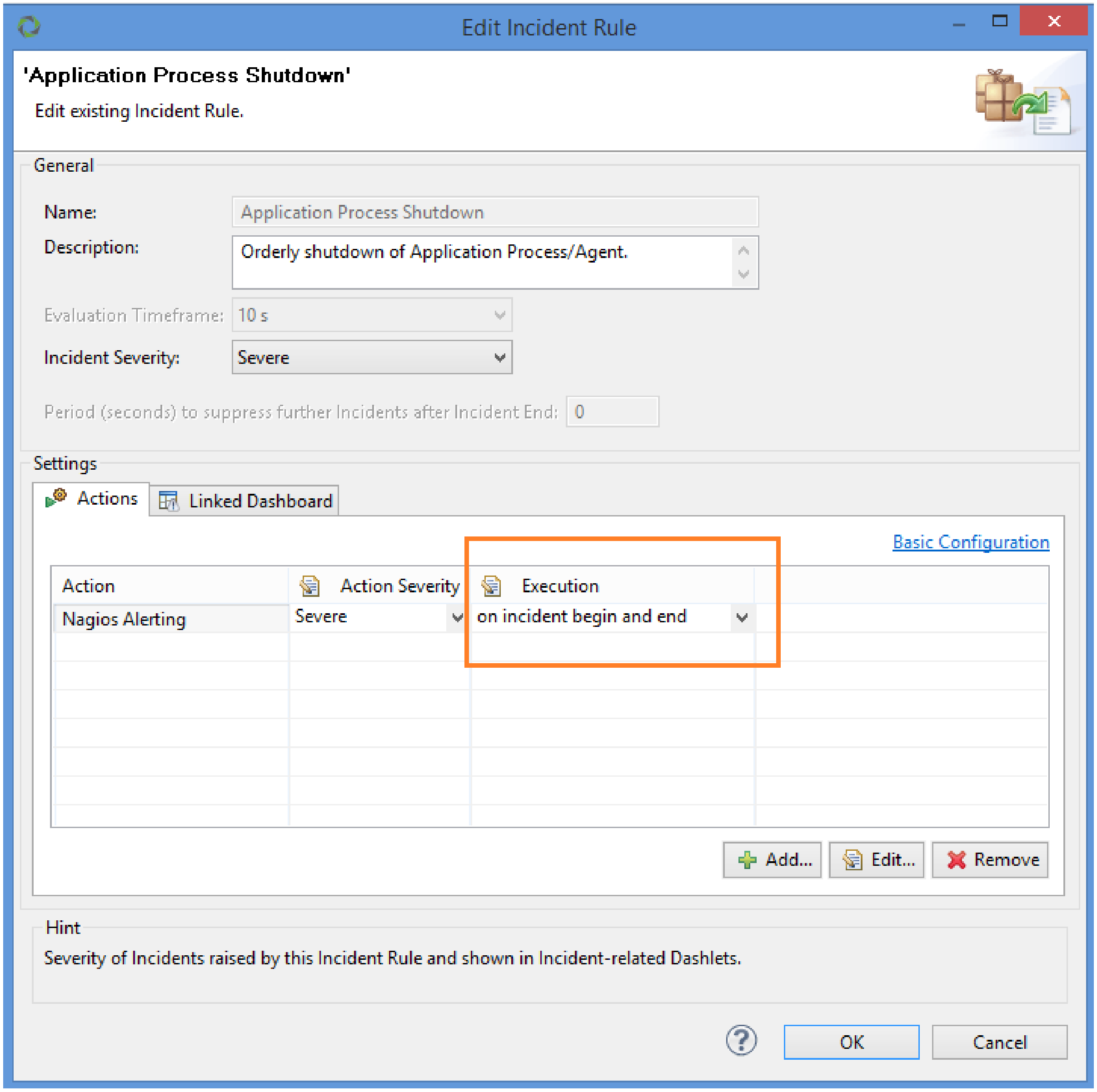
Name	Type	Value	Visibil...
Nagios host name or ip address	string	localhost	edit
NSCA listening port	string	5667	edit
NSCA password	password	••••••	edit
NSCA Encryption	list	TRIPLE_DES	edit
ConnectTimeout	string	5000	edit
Socket Timeout	string	10000	edit

Log level: FINE

Hint
The host or IP of the Nagios host running the NSCA add-on

Incident Configuration

- Add the Nagios Action Plugin of each of the incident rule you want to generate Nagios alerts for. (System Profile/Incidents/select an Incident Rule/Edit/Advanced Configuration/add/Nagios Alerting)
- Important to set up the execution list to: **on incident begin and end**, so dynaTrace can informs Nagios when an incident starts and finishes.
- The value of the **Action Severity** will be sent to the Nagios Server when the inident begins.
  - dynaTrace Servere => Nagios Critical
  - dynaTrace Warning => Nagios Warning
  - dynaTrace Informational => Nagios OK
- The value of the **Incident Severity** will be shown on the dynaTrace Incident dashlet



'Application Process Shutdown'

Edit existing Incident Rule.

General

Name: Application Process Shutdown

Description: Orderly shutdown of Application Process/Agent.

Evaluation Timeframe: 10 s

Incident Severity: Severe

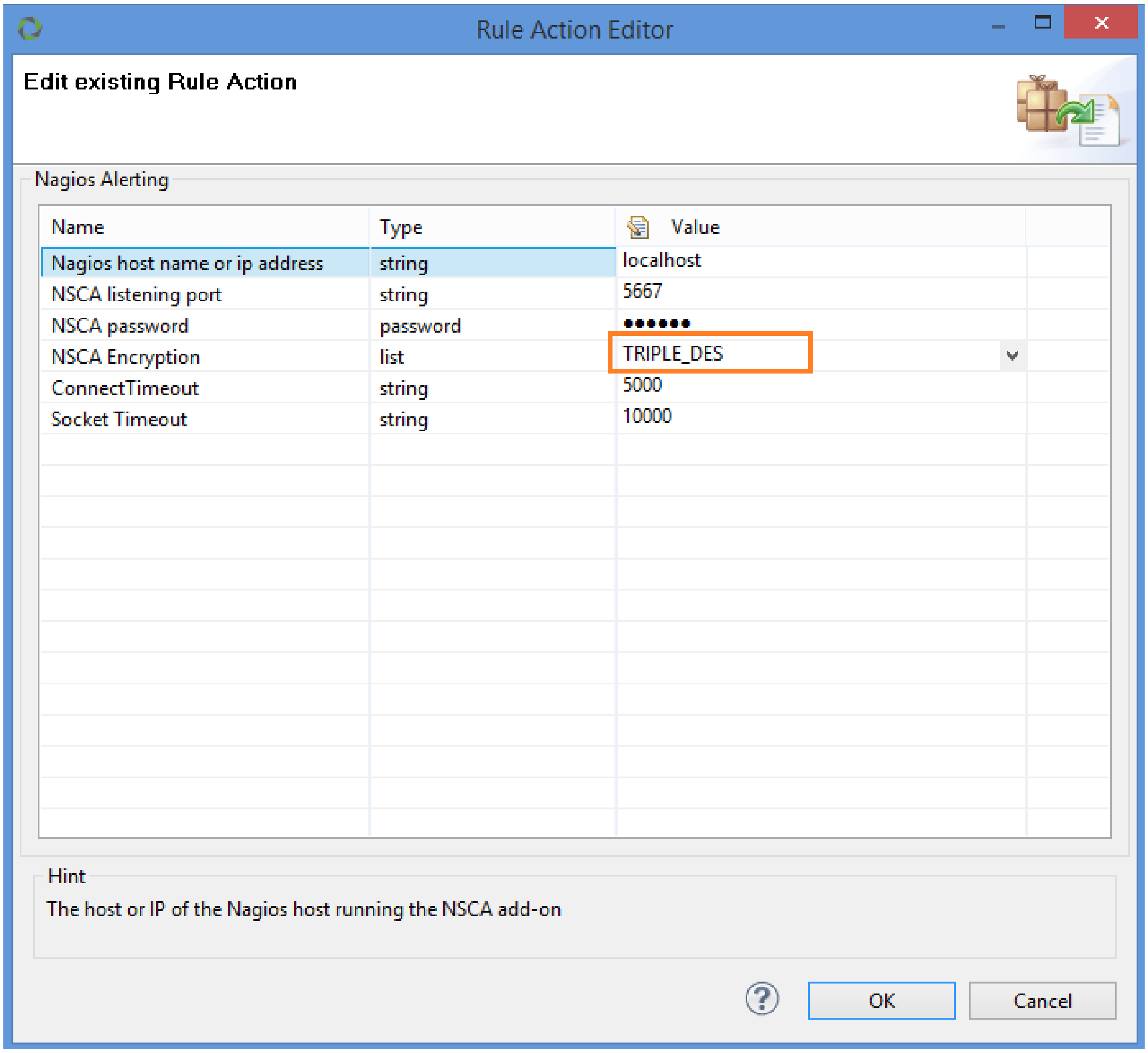
Period (seconds) to suppress further Incidents after Incident End: 0

Action	Action Severity	Execution
Nagios Alerting	Severe	on incident begin and end

Hint

Severity of Incidents raised by this Incident Rule and shown in Incident-related Dashlets.

- You can deviate from the default parameters pressing the edit button, however, TRIPLE_DES encryption is suggested to use.



Edit existing Rule Action

Nagios Alerting

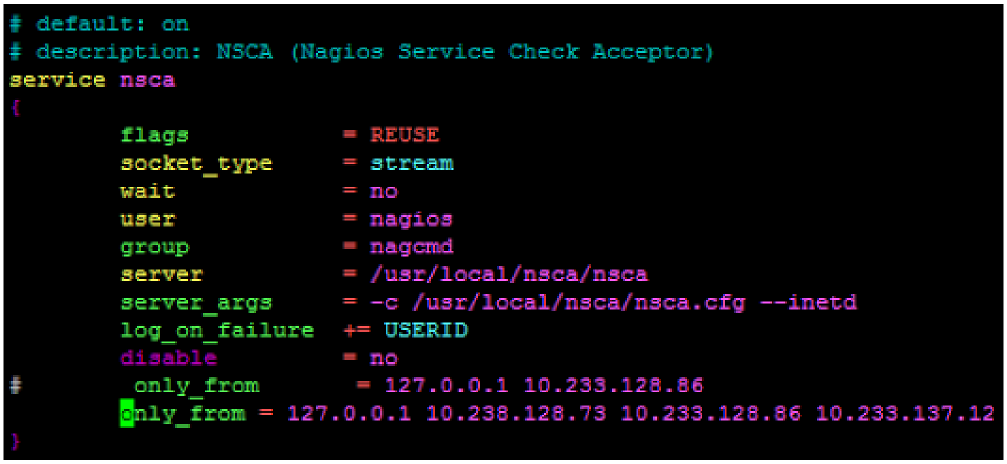
Name	Type	Value
Nagios host name or ip address	string	localhost
NSCA listening port	string	5667
NSCA password	password	••••••
NSCA Encryption	list	TRIPLE_DES
ConnectTimeout	string	5000
Socket Timeout	string	10000

Hint

The host or IP of the Nagios host running the NSCA add-on

RedHat7 (Centos7) xinetd - nsca support

- You have to define the IP address of the dynaTrace server at the **only_from** part of the **/etc/xinetd.d/nsca** configuration file.



```
# default: on
# description: NSCA (Nagios Service Check Acceptor)
service nsca
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = nagios
        group           = nagcmd
        server          = /usr/local/nsca/nsca
        server_args     = -c /usr/local/nsca/nsca.cfg --inetd
        log_on_failure  += USERID
        disable         = no
#        only_from       = 127.0.0.1 10.233.128.86
        only_from = 127.0.0.1 10.238.128.73 10.233.128.86 10.233.137.12
}
```

- You have to comment out the **server_address** in the **/usr/local/nsca/nsca.cfg** file

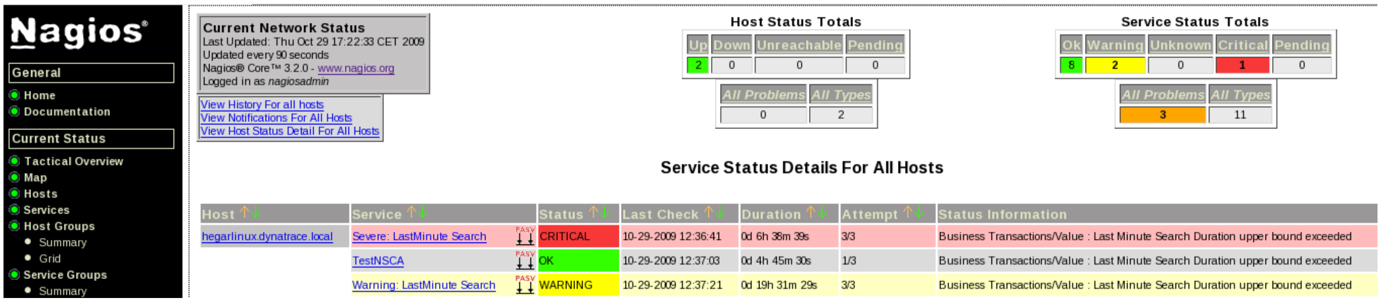
```
#server_address=192.168.1.1
```

Nagios Service/Host configuration

- On the Nagios side, you need to declare the host and the services which you will generate alerts for. The host is arbitrary as you will be able to configure it for each alert you will generate from dynaTrace. The service description on the other hand must match the name of the incident that will trigger the alert.

```
# HOST DEFINITION
define host{

    use                            default-host-template
    host_name                      dynaTrace_SystemProfileName
    alias                          dynaTrace_SystemProfileName
    address                        myfqdntodynatrace
    stalking_options               n
}

# SERVICE TEMPLATE DEFINITION
# Template for the service : dynaTrace alerts from the command file

define service {
        name                       passive_checkservice
        use                        generic-service
        active_checks_enabled      0
        passive_checks_enabled     1
        normal_check_interval      1
        check_period               24x7
        check_interval             1
        retry_interval             1
        }

# SERVICE DEFINITION
# Define each dynaTrace alert that we want to be processed by Nagios

define service {
        use                        passive_checkservice
        host_name                  dynaTrace_SystemProfileName  ; MATCH THE HOST
DEFINED EARLIER
        service_description        Warning: LastMinute Search   ; MATCH THE IINCIDENT
NAME
        register                   1
        check_command              check_ping                   ; Not used  but
mandatory command
}
```

Nagios Overview



Current Network Status
Last Updated: Thu Oct 29 17:22:33 CET 2009
Updated every 90 seconds
Nagios® Core™ 3.2.0 - www.nagios.org
Logged in as *nagiosadmin*

View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
2	0	0	0

All Problems	*All Types*
0	2

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
8	2	0	1	0

All Problems	*All Types*
3	11

Service Status Details For All Hosts

Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
hegarlinux.dynatrace.local	Severe: LastMinute Search PASV	CRITICAL	10-29-2009 12:36:41	0d 6h 38m 39s	3/3	Business Transactions/Value : Last Minute Search Duration upper bound exceeded
	TestNSCA PASV	OK	10-29-2009 12:37:03	0d 4h 45m 30s	1/3	Business Transactions/Value : Last Minute Search Duration upper bound exceeded
	Warning: LastMinute Search PASV	WARNING	10-29-2009 12:37:21	0d 19h 31m 29s	3/3	Business Transactions/Value : Last Minute Search Duration upper bound exceeded