

The Industry Standard in IT Infrastructure Monitoring

Purpose

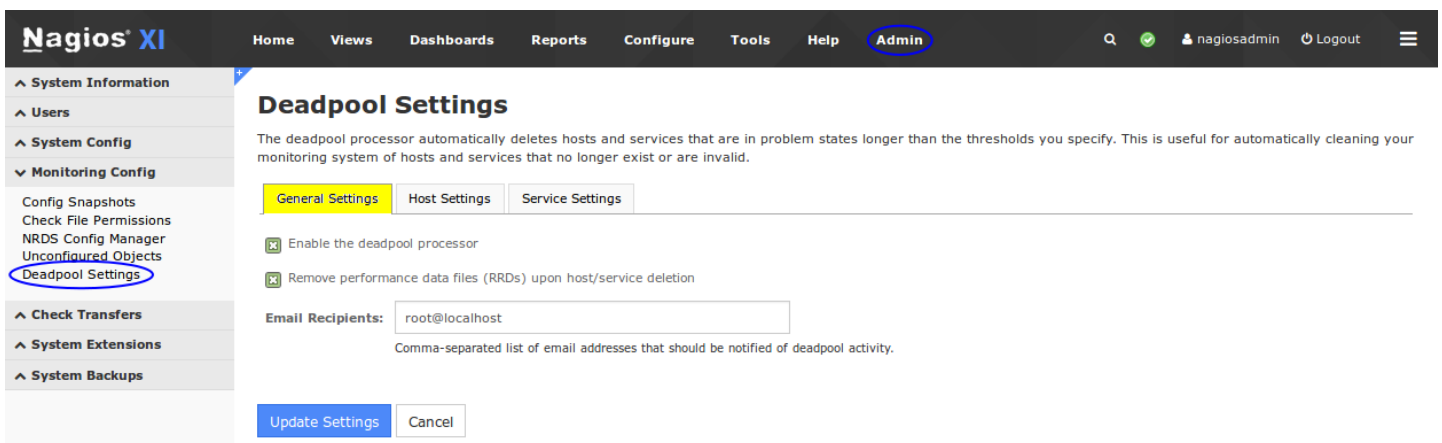
This document will describe how to use the Deadpool feature in Nagios XI.

Target Audience

This document is intended for use by Nagios XI Administrators who want XI to automatically remove failed hosts and/or services from the Nagios monitoring configuration.

How To Enable and Configure Deadpool Settings

Using the top menu bar, navigate to **Admin > Monitoring Config > Deadpool Settings** (this opens the General Settings tab).



To enable the deadpool processor, click the **Enable the deadpool processor** checkbox. Optionally, you can choose to remove performance data when a host or service is deleted and send email notifications of deadpool activity. Enter a valid email address in the **Email Recipients** field. Email notifications will be sent when the host or service has been added to the deadpool or when they have been deleted from the Nagios XI config.

Host and Service Settings

There are two additional tabs; **Host Settings** and **Service Settings**. The settings for for both tabs are almost identical, in the following information the term **object** refers to either a host object or service object.

Deadpool Settings

The deadpool processor automatically deletes hosts and services that are in problem states longer than the thresholds you specify. This is useful for automatically cleaning your monitoring system of hosts and services that no longer exist or are invalid.

General Settings **Host Settings** Service Settings

The settings below determine when hosts are moved to the deadpool and eventually deleted.

Stage 1 Time: days hours minutes
The amount of time a host must be in a problem state before notifications for it are automatically disabled and it is added to the host deadpool.

Deletion Time: days hours minutes
The amount of time a host must be in a problem state before it is automatically removed from the host deadpool and deleted from the monitoring configuration.

Exclusion Filters:

Names of hosts that should be excluded from deadpool processing. May contain exact string matches or regular expressions. One filter per line.

Deadpool Settings

The deadpool processor automatically deletes hosts and services that are in problem states longer than the thresholds you specify. This is useful for automatically cleaning your monitoring system of hosts and services that no longer exist or are invalid.

General Settings Host Settings **Service Settings**

The settings below determine when services are moved to the deadpool and eventually deleted.

Stage 1 Time: days hours minutes
The amount of time a service must be in a problem state before notifications for it are automatically disabled and it is added to the service deadpool.

Deletion Time: days hours minutes
The amount of time a service must be in a problem state before it is automatically removed from the service deadpool and deleted from the monitoring configuration.

Exclusion Filters:

Names of services that should be excluded from deadpool processing. May contain exact string matches or regular expressions. One filter per line.

Stage 1 Time determines how long an object must be in a problem state before notifications are disabled and the object is added to the deadpool.

Deletion Time determines how long an object must be in a problem state before the objects are removed from the monitoring configuration.

Exclusion Filters are used to exclude objects from the settings above. Exact string matches or [PRCE regular expressions](#) can be used.

Behavior and Exclusion

Problem states are “DOWN” for hosts and “CRITICAL” or “UNKNOWN” for services.

A host or service must meet the first stage 1 criteria before the second criteria (deletion time) is evaluated and the deletion time must be at least 5 minutes greater than stage 1 time.

The deletion time setting evaluates the total amount of time a host or service has been in a problem state. In the example above, a service would be moved to the service deadpool after 1 day of being unreachable and removed from the Nagios monitoring configuration after 3 days.

Deadpool does not work retroactively. For example, if a service has already been down for 4 days and then deadpool is activated with its default setting to delete after 3 days, the service will not be deleted.

Regex expressions like `\w`, `\d`, `\s`, can be used but the backslash character must be escaped first. To do this, simply add another backslash to the beginning of the the expression. For example:

```
/\w*/
```

would become:

```
/\\w*/
```

Here is an example of a Host Exclusion Filter where the hosts 192.168.1.1 to 192.168.1.30 are being excluded. The regex expression will only be matched against the name of the host object, not the address.

Exclusion Filters: localhost
/^192\.168\.1\.([1-9][1-2][0-9]|30)\$/

Here is an example of a Service Exclusion Filter where any service with HTTP is being excluded. The second line is a regex example that excludes SSH and FTP, these could be separate lines but it's here to demonstrate regex.

Exclusion Filters: HTTP
/SSH|FTP/

Regex should be used with some caution as expressions can be written in ways that require a long time to evaluate or may never finish evaluating. If you're not familiar with PCRE regex, a good resource is <http://php.net/manual/en/book.pcre.php>. Many online regex testers are also available. A good one is at <https://regex101.com/>.

How To Check Hosts And Services That Have Been Moved To A Deadpool

As soon as a host or service meets the stage 1 time criteria, Nagios XI will create a new hostgroup or servicegroup called host-deadpool or service-deadpool. All hosts and services that meet the stage 1 time criteria will be moved to the respective group.

The current status of the host deadpool can be seen by navigating to **Home > Details > Hostgroup Summary**.

Host Group	Hosts	Services
Host Deadpool (host-deadpool)	2 Down	2 Critical
Linux Servers (linux-servers)	1 Up	14 Ok

Last Updated: 2017-03-02 14:19:58

The current status of the service deadpool can be seen by navigating to **Home > Details > Servicegroup Summary**.

Service Group	Hosts	Services
Service Deadpool (service-deadpool)	2 Up	2 Critical

Last Updated: 2017-03-02 12:16:29

Details regarding the hosts and services that have been moved into deadpools can be gathered by clicking the links found in the **Status Summary** tables.

Troubleshooting

Host and service check failures are logged to `/var/log/messages` and `/usr/local/nagios/var/nagios.log`.

Deadpool status information is logged to `/usr/local/nagiosxi/var/deadpool.log`. This file is rewritten each time `deadpool.php` is run, which is currently every minute. It will contain the the current status of the deadpool including stage 1 and stage 2(deletion) settings, what hosts or services are currently in the dead pool, and when notification and deletions occur. You can watch the log file by executing the following command in a terminal session on your Nagios XI server:

```
tail -f /usr/local/nagiosxi/var/deadpool.log
```

Host and services can be removed from their respective deadpool groups manually through the CCM. To access this, navigate to **Configure > Core Config Manager** and then select either **Host Groups** or **Service Groups** under the **Monitoring** menu.

Finishing Up

If you have any questions about the deadpool feature in Nagios XI, you can contact our support team on the Nagios Support Forums:

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