How To Use Deadpool In Nagios XI 5

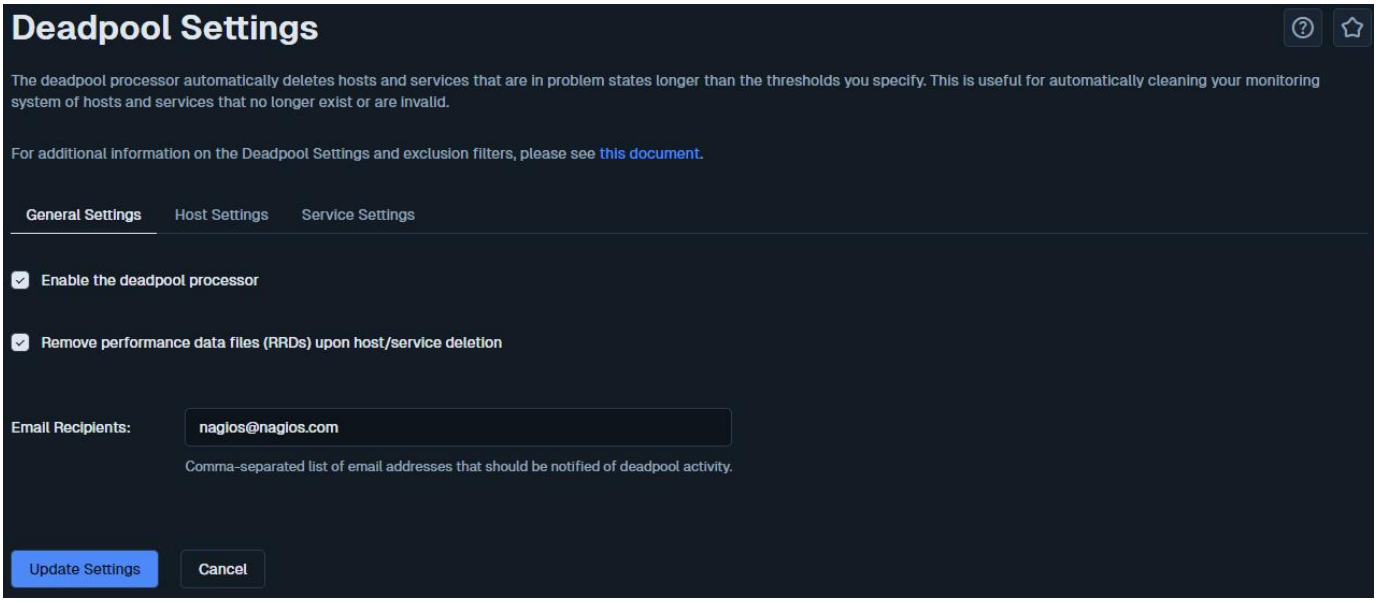
Purpose

This document describes how to use Deadpool settings to filter non-working hosts or services in Nagios XI 2024.

If you are using Deadpool in Nagios XI 2024, see How to use the Nagios XI 2024 Deadpool

How To Enable and Configure Deadpool Settings

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

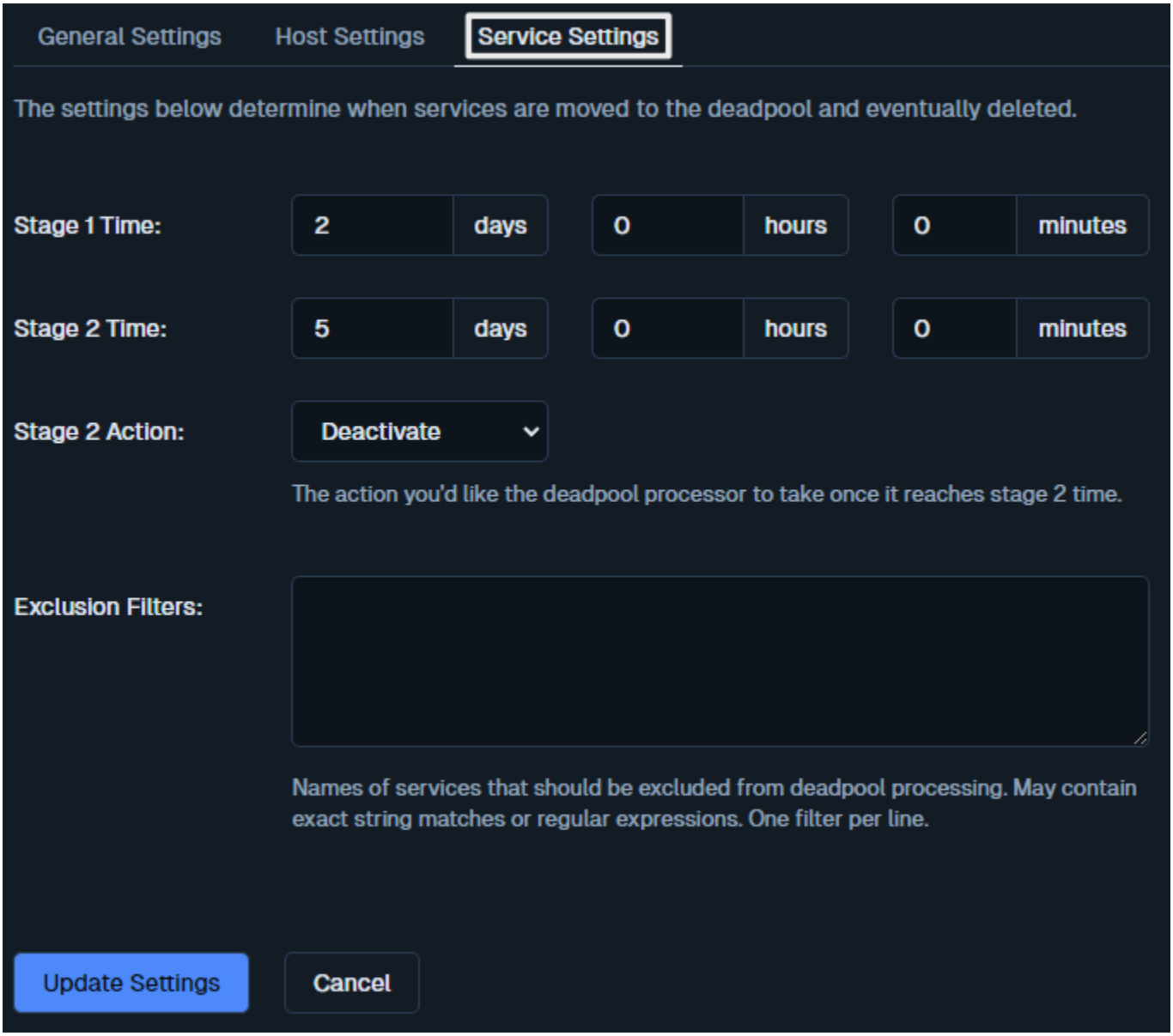


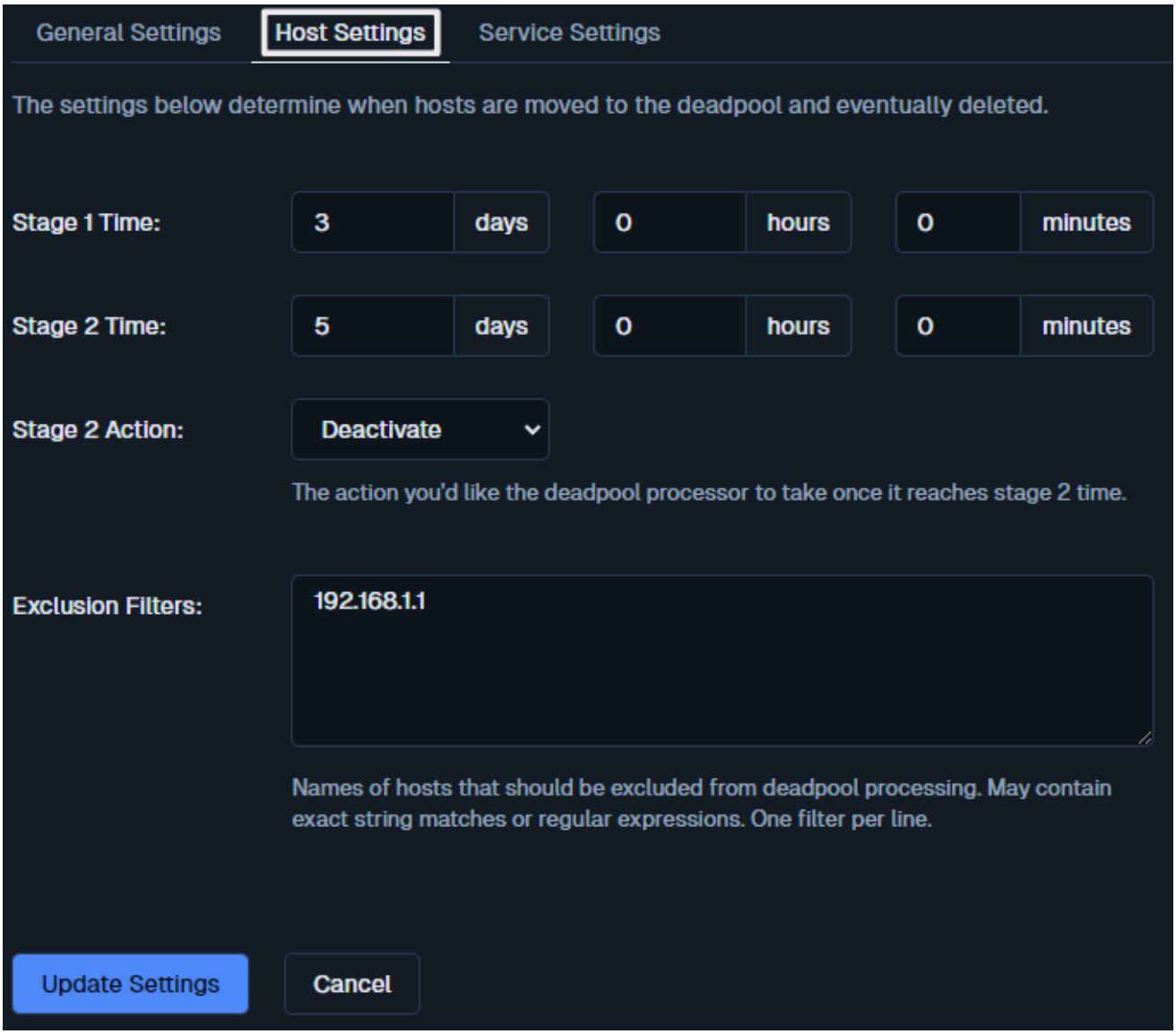
2. To enable the deadpool processor, click the **Enable the deadpool processor** checkbox.
3. Optionally, you can choose to remove performance data when a host or service is deleted and send email notifications of deadpool activity.
4. Enter a valid email address in the **Email Recipients** field. Email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

Host and Service Settings

There are two tabs: **Host Settings** and **Service Settings**.

The settings for both tabs are almost identical, in the following information the term object refers to either a host object or service object.





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

Stage 2 determines how long an object must be in a problem state before it is automatically removed from the deadpool and deleted/deactivated from the monitoring configuration.

Stage 2 Action allows you to define if you want an object to be deleted or deactivated when it reaches stage 2.

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.

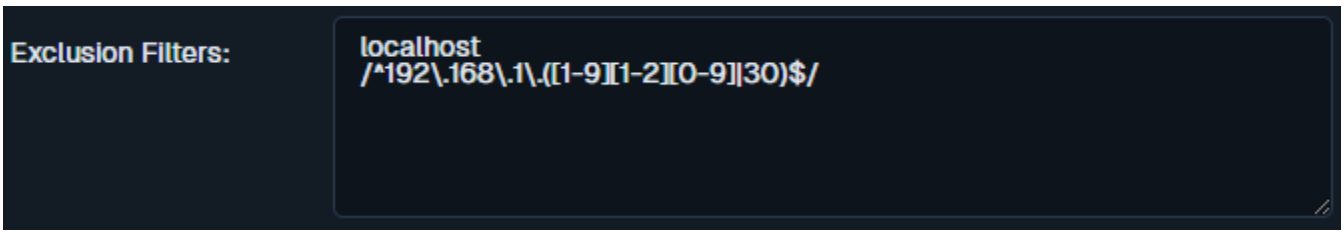
Regex expressions like \w, \d, \s, can be used but the backslash character must be escaped first. To do this, simply add another backslash to the beginning of the expression.

For example:
`/\w*/`
would become:
`/\\w*/`

Exclusion Filters:

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.

```
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.

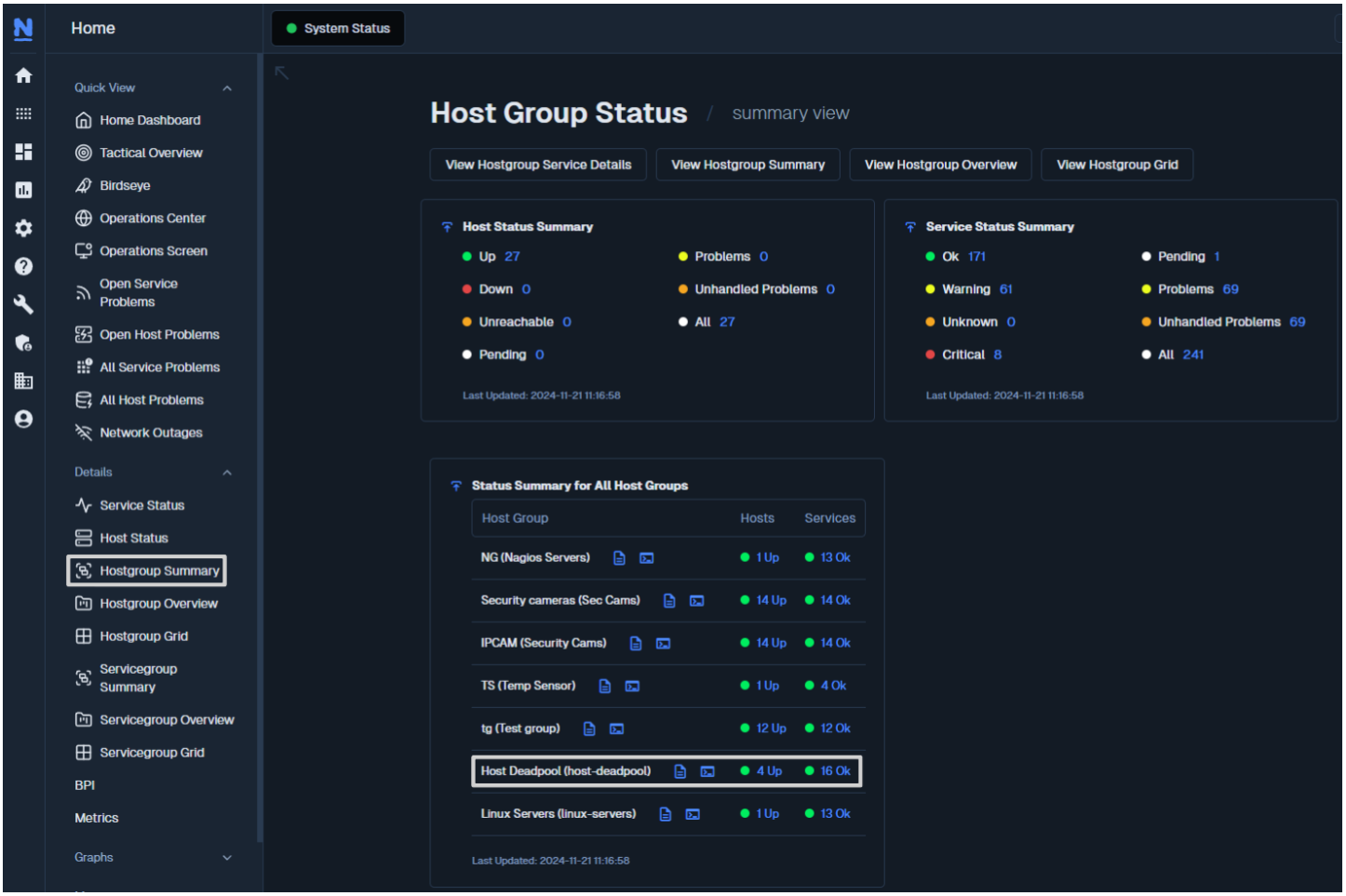
Regex should be used with some caution as expressions can be written in ways that require a long time to evaluate or may never finish evaluating. If you're not familiar with PCRE regex, a good resource is http://php.net/manual/en/book.pcre.php.

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

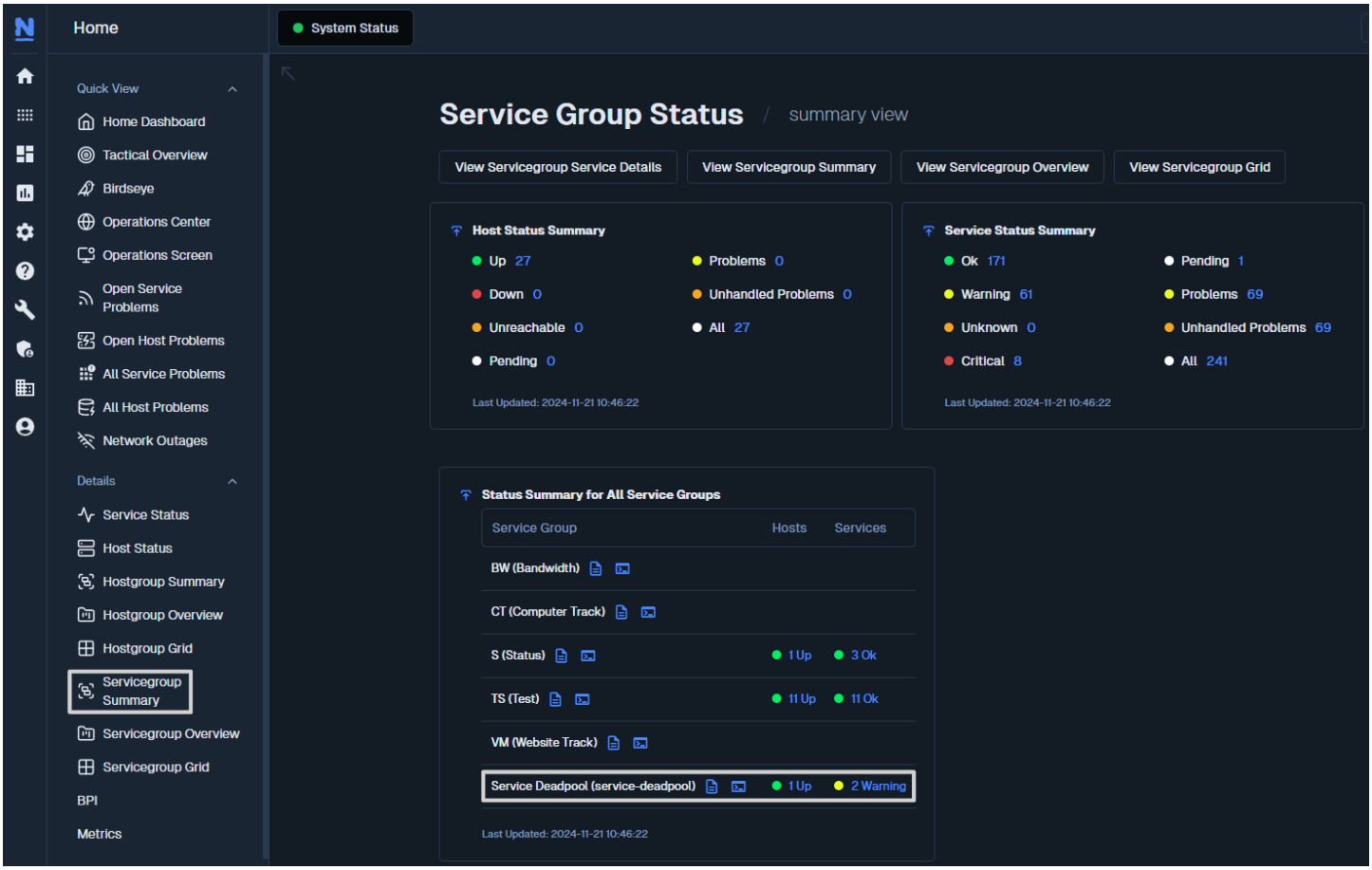
As soon as a host or service meets the stage 1 time criteria, Nagios XI will create a new hostgroup or servicegroup called **host-deadpool** or **service-deadpool**. All hosts and services that meet the stage 1 time criteria will be moved to the respective group.

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



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

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 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 Configuration Manager. To access this, navigate to **Configure** > **Core Config Manager** and then select either **Host Groups** or **Service Groups** under the **Monitoring** menu.

Finishing Up

This completes the documentation on using deadpool 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