

How To Monitor Website Defacement In Nagios XI 2024

Purpose

This document describes how to use the Website Defacement Wizard to monitor your websites for defacement, modification, and malicious insertions with Nagios XI. The Website Defacement Wizard provides an automated method for monitoring your website for defacement and notifies you when your website contains undesirable content.

Considerations

To protect against web defacement attacks, using the Website Defacement Wizard can save you from damage and loss of classified information. This website defacement monitoring wizard uses the regular expression check to find a specific string that you do not want to appear on your website. You receive a critical response when the check finds one or more of the strings it was instructed to search for on the website. These strings can be organically created lists of words, loading a CSV file, or selecting from categories of terms (gambling, profanity, pharmaceutical, etc.).

When monitoring a website for defacement, consider the following:

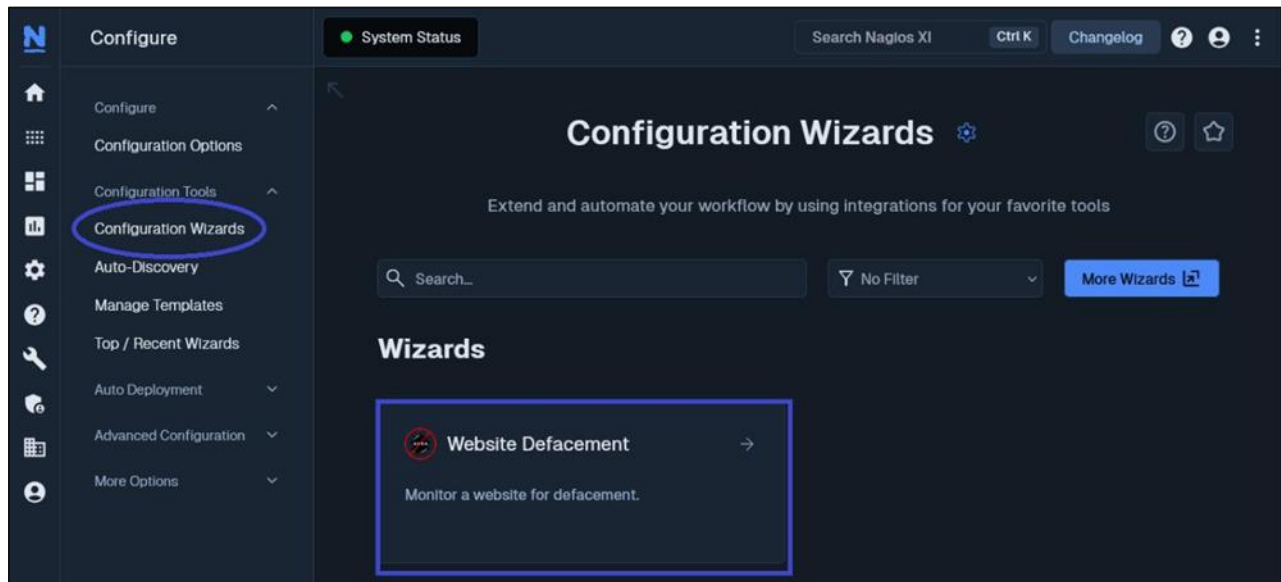
- The Website Defacement wizard uses a regular expression check to search for a specific string or multiple strings
- Strings do not have to be case sensitive, and each one should be separated by a new line
- There are a few pre-defined lists of words you may want to search for, sorted into categories
- You can also load a custom wordlist file into the wizard for each site you want to monitor
- There is also a regular expression match check to verify that the website you are monitoring is up and running, but this is strictly optional and may be redundant if you are already monitoring this website with Nagios XI

The Website Defacement Wizard

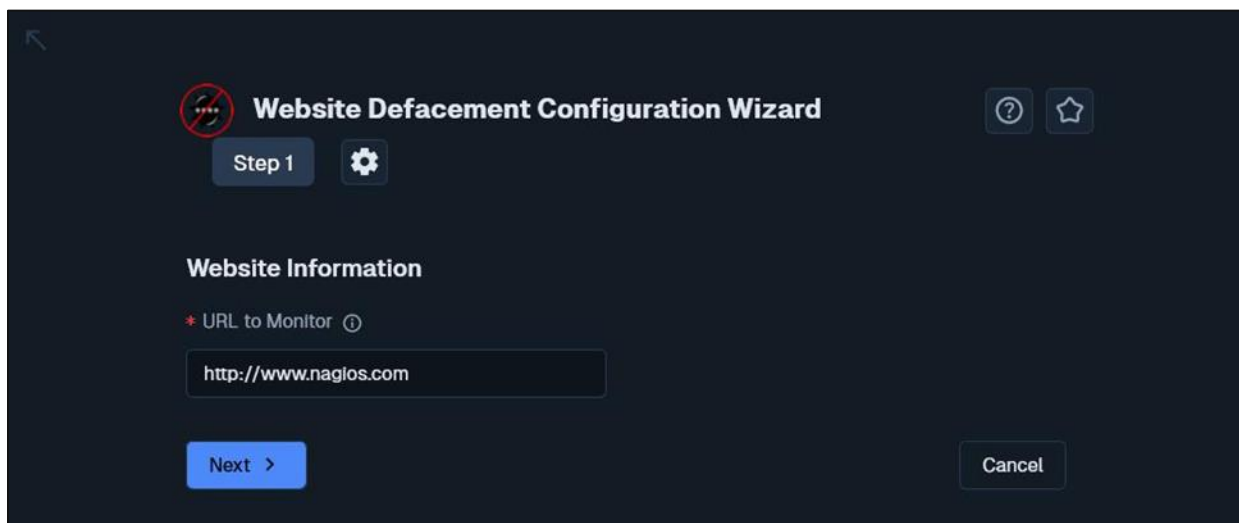
This Website Defacement wizard uses the regular expression check to find a specific string that you do not want to appear on your website. You receive a critical response when the check finds one or more of the strings it was instructed to search for on the website. To understand the capabilities of the wizard we will walk through an example.

To begin using the **Website Defacement wizard** navigate via the top menu bar to **Configure > Run a Configuration Wizard** and select the **Website Defacement wizard**. In the following screenshot you can see how the search field allows you to quickly find a wizard.

How To Monitor Website Defacement In Nagios XI 2024



1. In **Step 1**, enter the **URL of the website** you want to monitor into the **URL to Monitor field**.
 - a. This can be the main page of the website or any specific sub-page you want to monitor. Click **Next** to proceed to **Step 2**.



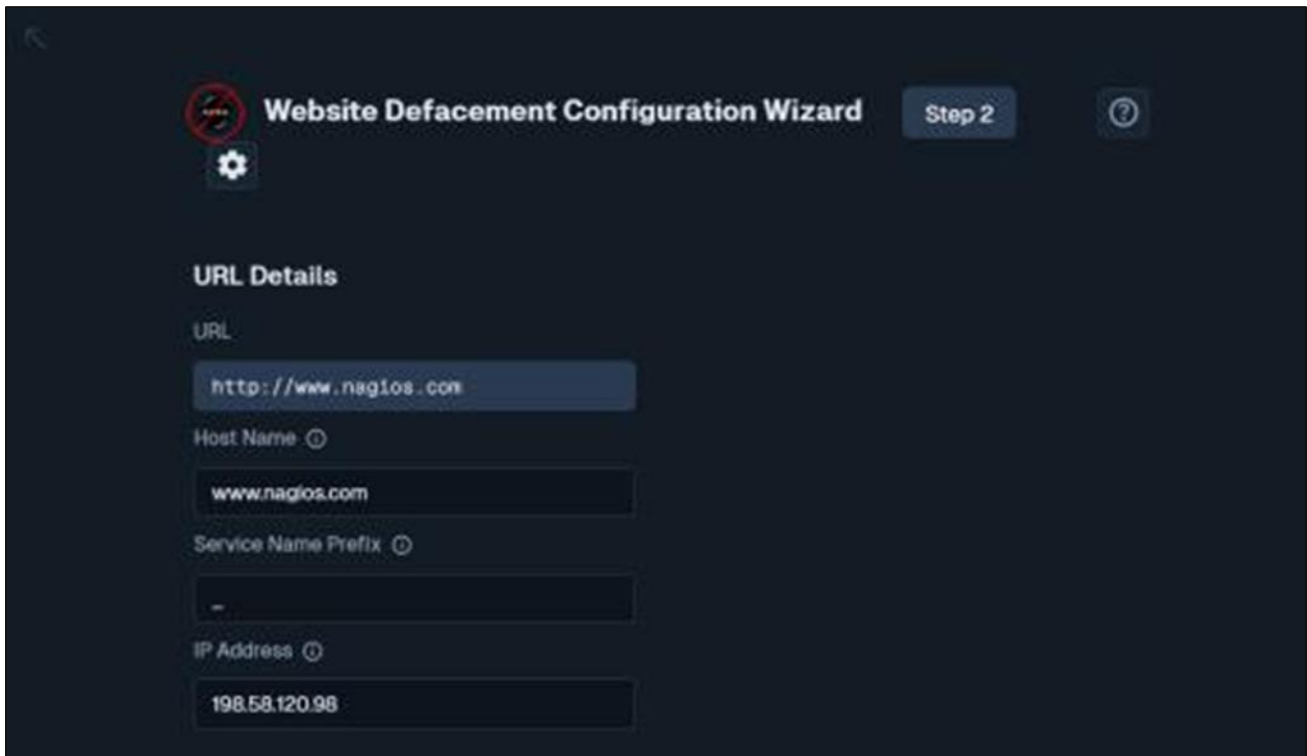
How To Monitor Website Defacement In Nagios XI 2024

2. **Step 2** is where most of the configuration takes place and is broken up into multiple sections.

a. **URL Details** specify the following:

- **Host Name** is the standard Nagios host name
- **Service Name Prefix** is a string that will be added to the beginning of any services created by the wizard for easier identification
- **IP Address** allows you to specify a different IP from the one that was auto-detected for the URL

Please refer to the screenshot below.

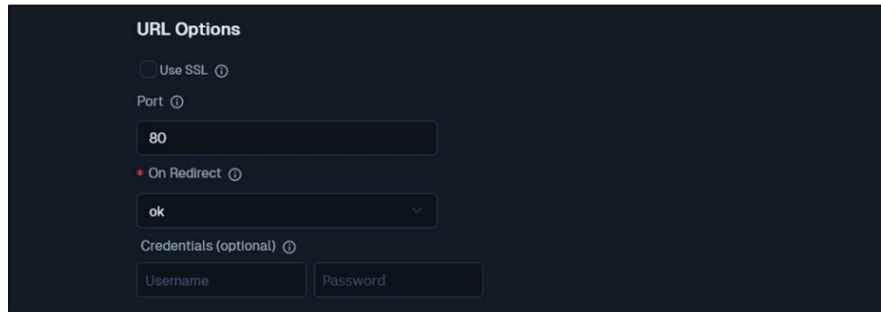


The screenshot displays the 'Website Defacement Configuration Wizard' interface, specifically 'Step 2'. The 'URL Details' section is visible, containing four input fields: 'URL' with the value 'http://www.nagios.com', 'Host Name' with 'www.nagios.com', 'Service Name Prefix' with a hyphen '-', and 'IP Address' with '198.58.120.98'. The interface is dark-themed with light-colored text and input boxes.

b. **URL Options** specify the following:

- Use **SSL and Port** can be configured in case HTTP/S are running on alternative ports
- On **Redirect** allows you to define how to handle redirected pages.
- **Credentials** allow you to specify a username and password for use in basic HTTP authentication

How To Monitor Website Defacement In Nagios XI 2024



URL Options

Use SSL ⓘ

Port ⓘ

80

On Redirect ⓘ

ok

Credentials (optional) ⓘ

Username Password

- c. **Defacement Monitoring Services** allows you to select which defacement methods you would like to use to monitor your website. If you check the box next to **Defacement Content Locator** then a **Website Defacement** service will be created.
- d. **The Defacement Content Locator** allows you to enter a list of words which should be considered "bad" if they appear on the page.
 - You can enter a list of words manually, one on each line
 - You can upload a custom text file of words, also one on each line
 - You can choose from the pre-defined lists of default words from various categories
- e. From the screenshot below you can see that the **Gambling** checkbox was selected, and the **Load Defaults** button was clicked. This loaded all the gambling related words to the text area input.

How To Monitor Website Defacement In Nagios XI 2024

Defacement Monitoring Services

Specify which defacement services you would like to monitor your website with.

Defacement Content Locator
Monitors the website to locate strings, as defined in the text box below.

Insert a list of strings, each separated with a new line (if using a single quote you must escape it).

```
gambling
holdem
holdempoker
holdemsoftware
online-gambling
onlinegambling-4u
poker
roulette
texas-holdem
slot-machine
```

Load File... Browse... No file selected. ⓘ

Marketing Profanity Gambling Pharmaceuticals

Load Defaults ⓘ

- f. **Web Page Regular Expression Match** allows you to check that the content of the webpage includes specific words or expressions. If you check the box next to **Web Page Regular Expression Match** then a **Web Page Regex Match** service will be created.
- g. You will then enter a string you wish to search for on the website. You will be alerted if the entered string does not appear on your website. You can also choose to invert the search by checking the **Invert Regex Search** check box. This will instead alert if the regex is found on your website.

Web Page Regular Expression Match
Monitors the website to ensure the specified regular expression is found in the content of the web page. A content mismatch may indicate that your website has experienced a security breach or is not functioning correctly. To include multiple expressions use the "|" after each expression with no spaces

Regular Expression

Invert Regex Search

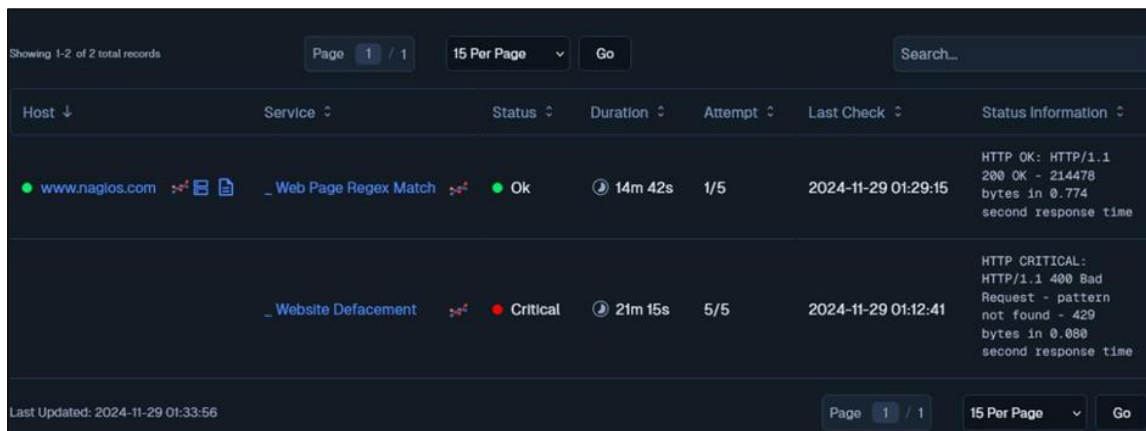
< Back Next > Cancel

How To Monitor Website Defacement In Nagios XI 2024

3. Once you've finished making your selections, click **Next** and then complete the wizard by choosing the required options in **Step 3 – Step 5**.

To finish, click on **Finish** in the last step of the wizard, this will create the new hosts and services and begin monitoring.

Once the wizard applies the configuration, click the **View status** details for your web server link to see the new host and services that were created.



Host ↓	Service ↓	Status ↓	Duration ↓	Attempt ↓	Last Check ↓	Status Information ↓
www.nagios.com	_ Web Page Regex Match	Ok	14m 42s	1/5	2024-11-29 01:29:15	HTTP OK: HTTP/1.1 200 OK - 214478 bytes in 0.774 second response time
	_ Website Defacement	Critical	21m 15s	5/5	2024-11-29 01:12:41	HTTP CRITICAL: HTTP/1.1 400 Bad Request - pattern not found - 429 bytes in 0.080 second response time

In the screenshot you can see that the **Web Page Regex Service** is in a critical state with the error "301 Moved Permanently - pattern not found". This will be resolved in the following troubleshooting section.

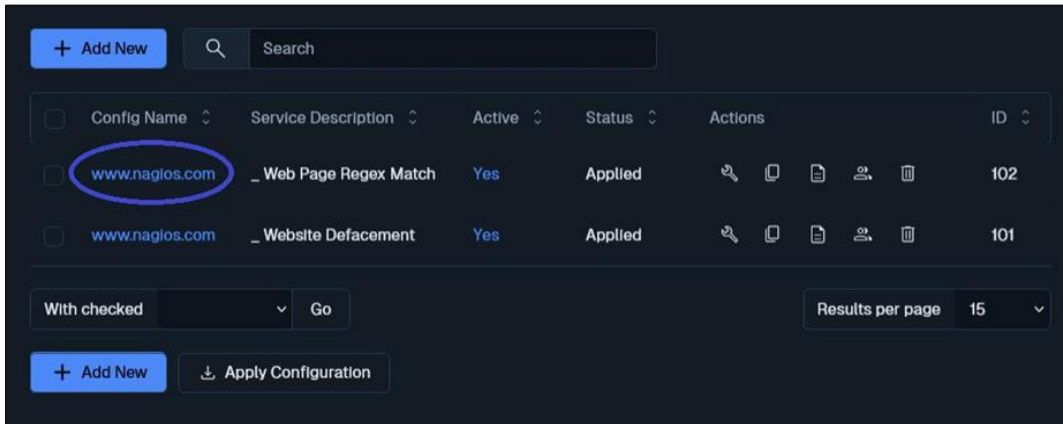
It's also worth mentioning that while the **Website Defacement Service** is in an OK state, it is also reporting "301 Moved Permanently - pattern not found" and will need to be corrected for the service to function properly.

Troubleshooting

Some sites will issue a HTTP 301 code which is just a simple redirect and can cause some issues with the check_http plugin (as seen in the previous screenshot). You will need to adjust the "-f xxxx" switch on the services to use the follow argument.

1. Locate the services by navigating to **Configure > Core Config Manager > Monitoring > Services**.

How To Monitor Website Defacement In Nagios XI 2024

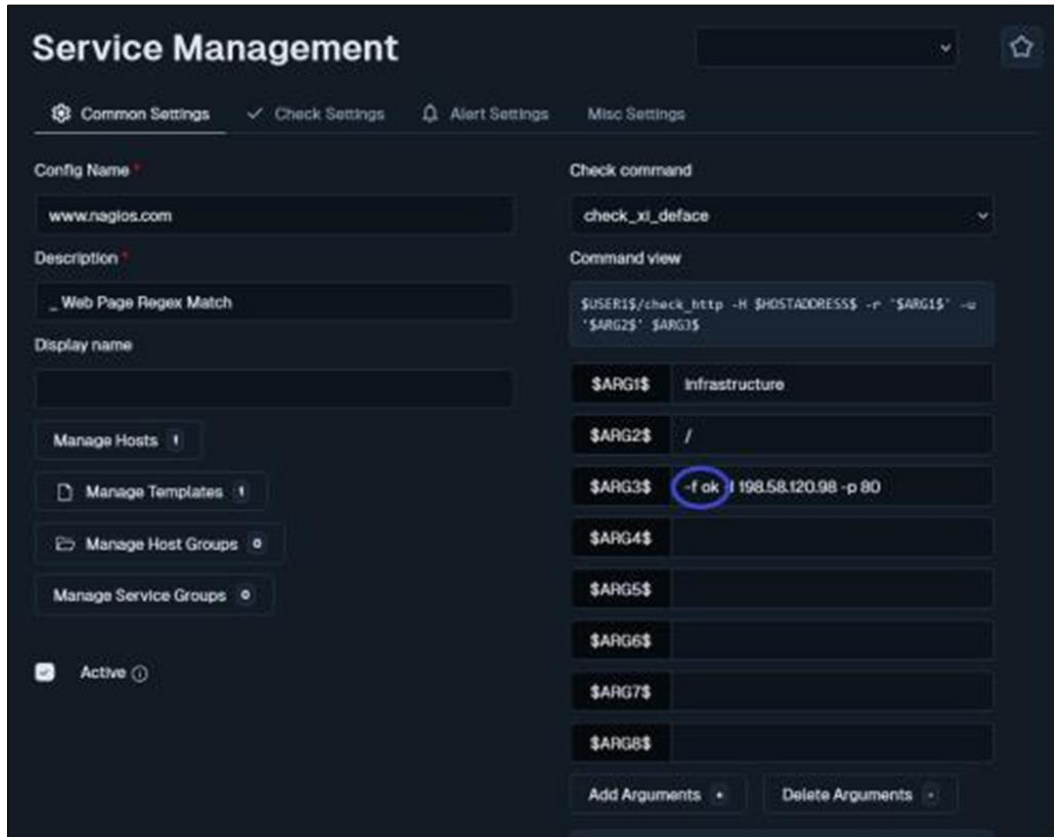


2. Click on the services in the **Service Name** column to begin editing it
In the screenshot to the right you can see that \$ARG3\$ has the value:

-f ok

3. Change **ok** to follow.

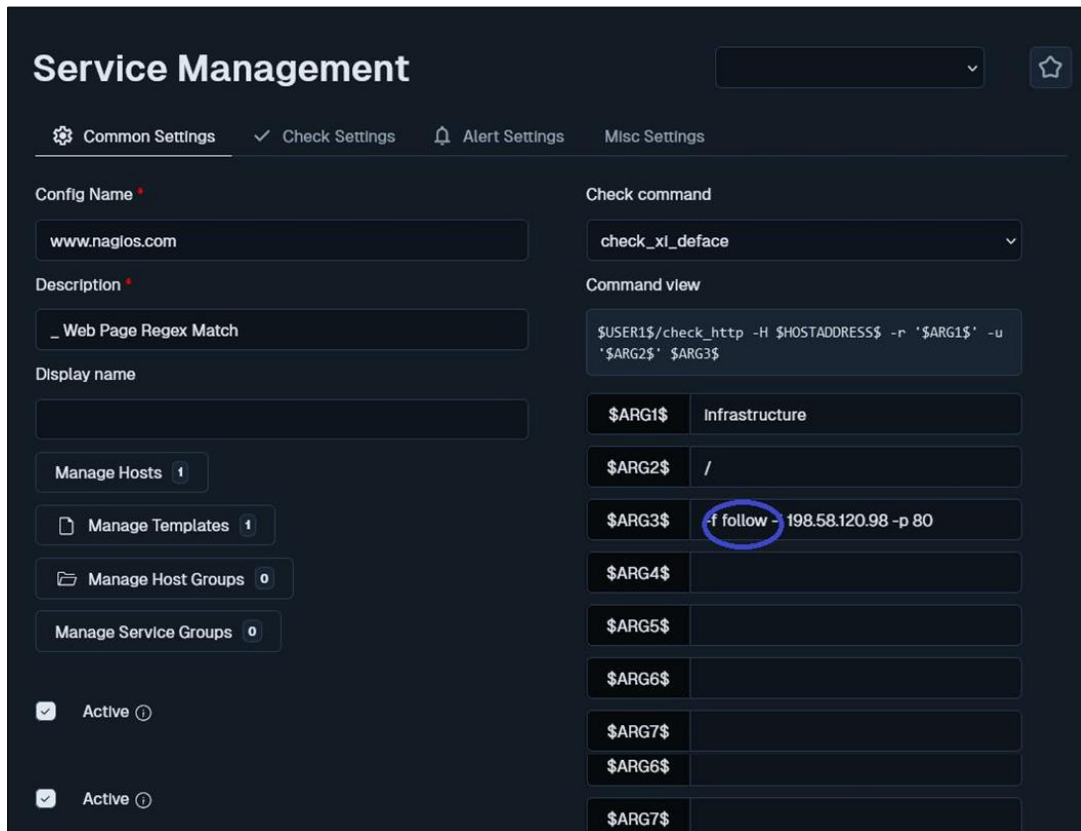
How To Monitor Website Defacement In Nagios XI 2024



In the screenshot to the right you can see that \$ARG3\$ now has value:

-f follow 198.58.120.98 -p 80

How To Monitor Website Defacement In Nagios XI 2024



4. Click **Save** to save the changes.

5. Repeat this for any other services that need updating and then click **Apply Configuration** to make the changes go into production.

Once the configuration has applied **go and view the services**. After they've performed a check with the new setting they should be working correctly.

How To Monitor Website Defacement In Nagios XI 2024

Service Status / host: www.nagios.com

Host Status Summary

- Up 1
- Down 0
- Unreachable 0
- Pending 0
- Problems 0
- Unhandled Problems 0
- All 1

Last Updated: 2024-11-29 01:22:19

Service Status Summary

- Ok 1
- Warning 0
- Unknown 0
- Critical 1
- Pending 0
- Problems 1
- Unhandled Problems 1
- All 2

Last Updated: 2024-11-29 01:22:19

Showing 1-2 of 2 total records

Page 1 / 1 15 Per Page Go Search...

Host	Service	Status	Duration	Attempt	Last Check	Status Information
www.nagios.com	_ Web Page Regex Match	Ok	3m 8s	1/5	2024-11-29 01:19:14	HTTP OK: HTTP/1.1 200 OK - 214478 bytes in 0.710 second response time
	_ Website Defacement	Critical	9m 41s	5/5	2024-11-29 01:12:41	HTTP CRITICAL: HTTP/1.1 400 Bad Request - pattern not found - 429 bytes in 0.080 second response time

Last Updated: 2024-11-29 01:22:22

Page 1 / 1 15 Per Page Go

For more information, visit the [Configuration Wizards](#) documentation.

Finishing Up

This completes the documentation on how to monitor website defacement 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](#)