

The Industry Standard in IT Infrastructure Monitoring

Purpose

This document describes how to monitor websites effectively with Nagios XI.

Target Audience

This document is intended for use by both Nagios administrators and end-users.

Considerations

When monitoring websites, it is often recommended to check the operational status of several key metrics, including:

- HTTP response validity and load time
- DNS resolution and IP address match
- Website content
- SSL certificates
- Web transaction success and run time

Your monitoring needs will vary depending on the complexity of your website, its purpose, and its intended end-user.

Getting Started

Monitoring websites is made simple through the use of configuration wizards shipped with Nagios XI. There are two different ones for this category, with one checking more steady-state aspects of a web site and another for testing transactions and other interactive, dynamic activities on your site, named the *Website* and *Web Transaction* configuration wizards, respectively.

The Website wizard

This is the wizard you will use for most types of sites, where what you are checking are common server / site metrics. The best way to understand its capabilities is to see them, so a walkthrough of using this wizard follows. Begin by visiting the configuration wizards page, and selecting the **Website** option.

Monitoring Wizard - Step 1

Monitoring wizards guide you through the process of monitoring devices, servers, applications, services, and more. Select the appropriate wizard below to get started. Need a custom configuration wizard created for your organization? No problem! [Contact us](#) for pricing information.

- Generic Network Device**
Monitor a generic IP network device.
 - Printer**
Monitor an HP JetDirect compatible network printer.
 - SNMP**
Monitor a device, service, or application using SNMP.
 - Network Switch**
Monitor a network switch.
 - TCP/UDP Port**
Monitor common and custom TCP/UDP ports.
 - Website**
Monitor a website.
 - Web Transaction**
Monitor a synthetic web transaction.
 - Windows Desktop**
Monitor a Microsoft® Windows XP, Windows Vista, or Windows 7 desktop.
 - Windows Server**
Monitor a Microsoft® Windows 2000, 2003, or 2008 server.
-

Website Monitoring Wizard - Step 2



Website Information

Website URL:

The full URL of the website you'd like to monitor.

Next enter the URL to your website, which can either be to the front page of the domain or any subpage. The latter will only have an effect for checking of existence of that page and content monitoring on it.

The next step is where most of your options will be set. Here you can define which services you want to add for this site, including whether:

- to use SSL (HTTPS) and what port that listens on,
- it returns a valid HTTP OK message,
- responds to ping,
- DNS resolution appears to be working,
- the DNS response matches what you had while running the wizard,
- a particular string is found on the page (either literally or as a regular expression),
- and the SSL certificate's expiry date is sufficiently far away.

The **Use SSL** option and **SSL Certificate** check will be enabled if the URL you gave in Step 2 began with `https://`, and will not for other URLs. It is also possible to specify authentication credentials for if the page you are checking is protected by Basic authentication.

Website Monitoring Wizard - Step 3



Website Details

Website URL:

Host Name:
The name you'd like to have associated with this website.

IP Address:
The IP address associated with the website fully qualified domain name (FQDN).

Website Options

Use SSL:
Monitor the website using SSL/HTTPS.

Port:
The port to use when contacting the website.

Credentials: Username: Password:
The username and password to use to authenticate to the website (optional). If specified, basic authentication is used.

Website Services

Specify which services you'd like to monitor for the website.

- HTTP**
Includes basic monitoring of the website to ensure the web server responds with a valid HTTP response.
- Ping**
Monitors the website server with an ICMP "ping". Useful for watching network latency and general uptime of your web server. Not all web servers support this.
- DNS Resolution**
Monitors the website DNS name to ensure it resolves to a valid IP address.
- DNS IP Match**
Monitors the website DNS name to ensure it resolves to the current known IP address. Helps ensure your DNS doesn't change unexpectedly, which may mean a security breach has occurred.
- Web Page Content**
Monitors the website to ensure the specified string 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.
Content String To Expect:
- 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.
Regular Expression To Expect:
- SSL Certificate**
Monitors the expiration date of the website's SSL certificate and alerts you if it expires within the specified number of days. Helps ensure that SSL certificates don't inadvertently go un-renewed.
Days To Expiration:

The remaining steps are all similar to the other wizards, and define the usual monitoring and notifications settings. You will want to keep in mind that each of the service checks is a hit on your web server, and you may not want to have those checks run too frequently if there is a risk of interfering with normal traffic. The defaults are likely fine for most situations though.

Website Monitoring Wizard - Step 4



Monitoring Settings

Define basic parameters that determine how the host and service(s) should be monitored.

Under normal circumstances...

Monitor the host and service(s) every minutes.

When a potential problem is first detected...

Re-check the host and service(s) every minutes up to times before generating an alert.

Website Monitoring Wizard - Step 5



Notification Settings

Define basic parameters that determine how notifications should be sent for the host and service(s).

When a problem is detected...

- Don't send any notifications
- Send a notification immediately
- Wait minutes before sending a notification

If problems persist...

Send a notification every minutes until the problem is resolved.

Send alert notifications to...

- Myself (Adjust settings)
- Other individual contacts
 - Default Contact (xi_default_contact)
- Specific contact groups
 - Nagios Administrators
 - All Contacts

Website Monitoring Wizard - Final Step



Final Settings

Click **Apply** to add your new configuration.

Once these are completed and the checks have run, you should see output similar to this:

Host	Service	Status	Duration	Attempt	Last Check	Status Information
www.linode.com	DNS IP Match	Critical	32m 45s	5/5	2010-05-26 16:06:21	DNS CRITICAL - expected '72.14.191.202' but got '69.164.200.202,72.14.180.202,72.14.191.202'
	DNS Resolution	Ok	31m 19s	1/5	2010-05-26 16:08:47	DNS OK: 0.057 seconds response time. www.linode.com returns 69.164.200.202,72.14.180.202,72.14.191.202
	HTTP	Ok	29m 54s	1/5	2010-05-26 16:05:12	HTTP OK HTTP/1.1 200 OK - 6016 bytes in 0.271 seconds
	Ping	Ok	33m 49s	1/5	2010-05-26 16:06:17	OK - www.linode.com: rta 57.031ms, lost 0%
	SSL Certificate	Ok	32m 24s	1/5	2010-05-26 16:07:42	OK - Certificate will expire on 07/04/2013 22:58.
	Web Page Content	Ok	30m 58s	1/5	2010-05-26 16:09:08	HTTP OK HTTP/1.1 200 OK - 0.325 second response time

Page 1 of 1 15 Per Page Go

The Web Transactions wizard

A more complex use case of website monitoring would be if you expect the content to be dynamic with user input and actions, and want to test that those actions complete as expected. For instance, you might test that a search box works (and what the results returned are), whether the purchase and checkout process of your web store is behaving properly, or that a user can log in successfully. The **Web Transaction** wizard can be used for these types of checks. Additionally, it allows for checking all three of those in succession, and other multi-step procedures where each stage may be dependent on the previous one.

This wizard relies on a tool called *WebInject*, which handles the transition logic between stages of the transaction. Therefore you will need to understand how to write the configuration XML in the WebInject syntax to configure these kinds of checks. Some examples are given below, and the WebInject manual can be found online at <http://www.webinject.org/manual.html>. Note that certain special characters need to be escaped. For instance, the < should be replaced with \x3C so as not to interfere with the XML, and within POST data URL escapes are used, so for instance @ becomes %40.

This syntax will go into the large **Test Case Data** input box in Step 3 of the wizard.

Example #1: Searching a forum

```
<testcases repeat="1">
<case
  id="1"
  url="http://support.nagios.com/forum/"
/>
<case
  id="2"
  method="post"
  url="http://support.nagios.com/forum/./search.php"
  postbody="keywords=foobar&submit=Search"
  verifypositive="\x3Cp>No posts were found because the word \x3Cstrong>foobar\x3C/strong> is
not contained in any post\.\x3C/p>"
/>
</testcases>
```

In this example, first the main forum page is loaded, which will make sure it appears to be present and working. The second step submits a search for the word “foobar”, and checks to make sure that the results say that no posts exist using that phrase. Instead of “foobar” you might use something like “Internet Explorer”, such that you could alert your CSS guru when someone reported something that was broken.

Web Transaction Monitoring Wizard - Step 2



Web Information

Monitoring a synthetic web transaction is a process which may involve several steps, including the submission and processing of data. Transaction logic is handled using *WebInject*, so you must be familiar with its syntax before monitoring a transaction.

Transaction Name:
 The name you'd like to have associated with this synthetic transaction test.

Primary URL:
 The primary URL that this transaction is associated with.

Web Transaction Monitoring Wizard - Step 3



Transaction Host Details

Primary URL:
 The primary URL that this transaction is associated with.

Host Name:
 The name you'd like to have associated with the primary URL.

IP Address:
 The IP address associated with the primary URL's fully qualified domain name (FQDN).

Transaction Details

Specify the details of how the transaction should be monitored.

Transaction Name:
 The name you'd like to have associated with this synthetic transaction test.

Test Case Data:

Timeout: seconds
 The response timeout for each test case.

Global Timeout: seconds
 A global timeout for running all tests. A warning message will be returned if total execution time exceeds this value.

Example #2: Using an Online Store

```

<testcases repeat="1">
  <testvar varname="USER">YourEmailAddressHere</testvar>
  <testvar varname="PASS">YourPasswordHere</testvar>

  <case
    id="1"
    description1="Login page"
    url="https://members.oreilly.com/account/login"
    parseresponse='_authentication_token' type="hidden" value="|" |escape'
    verifypositive="Sign in"
  />
  <case
    id="2"
    description1="Sign in"
    url="https://members.oreilly.com/account/login"
    method="post"
    postbody="email=${USER}&password=${PASS}&_authentication_token={PARSEDRESULT}"
    verifypositive="https://members.oreilly.com/account/benefits"
    parseresponse="found at |;"
  />
  <case
    id="3"
    description1="Members page"
    url="{PARSEDRESULT}"
    verifypositive="view or edit your account information"
  />
  <case
    id="4"
    description1="Book price"
    url="http://oreilly.com/catalog/9781593271794/"
    verifypositive="59.95"
  />
  <case
    id="5"
    description1="Book added to cart"
    url="https://epoch.oreilly.com/shop/cart.orm?prod=9781593271794.BOOK"
    verifypositive="Nagios, 2Ed"
  />
  <case
    id="6"
    description1="Book still in cart"
    url="https://epoch.oreilly.com/shop/cart.orm"
    verifypositive="Nagios, 2Ed"
    verifynegative="Backorder"
  />
  <case
    id="7"
    description1="Logout"
    url="https://members.oreilly.com/account/logout"
    verifypositive="http://oreilly.com/"
    parseresponse="found at |;"
  />
  <case
    id="8"
    description1="Main page"
    url="{PARSEDRESULT}"
    verifypositive="News & Commentary"
  />
</testcases>

```

This obviously more complicated example begins to show the power WebInject offers, using O'Reilly Media's web site. The first step confirms that the login page loads. The second provides your authentication credentials and then checks that they were accepted, and follows the redirect to the members page in step 3. Step 4 checks the price on "[Nagios, Second Edition \(by Wolfgang Barth\)](#)", and step 5 adds it to your shopping cart, with step 6 confirming it remains in your cart properly after that and appears to be in stock. Finally, the last two steps log you out and check that the home page loads. By carefully crafting the different steps and plenty of sufficiently specific verifypositive and verifynegative parameters, a great deal of information can be confirmed through this single Nagios service.

The Result

Once you have gone through all of that, Nagios XI will show two nice little summaries encompassing everything about those two web processes like this:

oreilly.com	 Web Transaction	 OK	11m 18s	1/5	2010-05-27 13:19:05	WebInject OK - All tests passed successfully in 6.931 seconds
support.nagios.com	 Web Transaction	 OK	15m 25s	1/5	2010-05-27 13:19:58	WebInject OK - All tests passed successfully in 0.897 seconds