

Did You Know?

SolarWinds Pingdom uptime monitoring is more than meets the eye!

Uptime monitoring is a main and essential part of any website monitoring tool. Having your website up and running is critical for your business. [SolarWinds® Pingdom®](#) uptime checks can solve multiple problems. It can make you aware if your website is down, or if you want to check the availability of critical pages on your website, like your shopping cart or pricing page. But that's not all—there's much more you can do with Pingdom uptime monitoring. You can also monitor other critical elements to your web applications and services like APIs, networks, email systems, and more.

Availability Checks

1. API Monitoring. In a modern microservices, distributed, containerized environment, APIs play a crucial role in application performance. Traditional website monitoring doesn't always capture API fails, so your service can be down without you knowing about it. You can easily create automatic availability checks to help ensure your APIs are available and responding to requests. Monitor your in-house APIs to ensure excellent application performance, including all critical business transactions. Many companies use third-party APIs for their critical business services (user authentication, payments, location, financial services), so these APIs should be monitored as well for the same reason.

2. SaaS Monitoring. Making sure all your internal software systems are performing well is very important; their poor performance can negatively influence the productivity and efficiency of your employees, making them lose valuable time. Two popular examples of SaaS monitoring by Pingdom include making sure your Salesforce and Microsoft Office 365 accounts are accessible from anywhere.

3. Email Monitoring. Pingdom checks to see if your email server is up and running. These types of checks monitor your mail server for a response. A 220 for POP is the default, but you can change it in the optional settings. The primary use case for SMTP, POP3, and IMAP checks is to make sure your email server is up and able to send out and receive emails. SMTP stands for Simple Mail Transfer Protocol and is used for sending emails out. Mail Transfer Protocol POP3(S) and IMAP(S) are for receiving emails. POP3 stands for Post Office Protocol, and IMAP stands for Internet Message Access Protocol.

4. Custom Monitoring. The HTTP custom check allows you to monitor a wide variety of things, many of them not supported by the regular uptime check.

- Broadband connection
- Custom status page
- The amount of free RAM or HD space on your server
- The CPU load on your server
- The number of active connections to your web server
- And more...

With the custom checks, you can run your own check scripts and let Pingdom get the status and response time. Just put your check script on a web server and enter the URL to the XML script. Any status other than OK will make the check count as down.

Network Checks

A network check is an essential part of website/application monitoring, helping ensure the data is transferred without interruptions; it will help you prevent outages, and, in case it occurs, troubleshoot it as quickly as possible.

1. DNS Monitoring. A check specific for making sure your DNS servers are working—one check for every DNS server is required. DNS is a “face” of your company, so it is extremely important to keep an eye on it; from a security perspective, DNS is often a primary target for malicious attacks. Set up a DNS check to be the first to catch suspicious activities and prevent potential damage to your brand. Also, DNS servers should be monitored for availability to ensure an excellent end-user experience.

2. TCP/UDP Monitoring. TCP stands for Transmission Control Protocol. It is the most commonly used protocol on the Internet. When you load a webpage, your computer sends TCP packets to the web server’s address, asking it to send the page to you. The web server responds by sending a stream of TCP packets, which your browser stitches together to form the web page and display it to you. When you click a link, sign in, post a comment, or do anything else, your browser sends TCP packets to the server, and the server sends TCP packets back. TCP is not just a one-way communication; the remote system sends packets back to acknowledge it has received your packets.

UDP stands for User Datagram Protocol—a datagram is the same thing as a packet of information. The UDP protocol works similarly to TCP, but it throws all the error-checking stuff out. All the back-and-forth communication and deliverability guarantees slow things down. When using UDP, packets are sent one way, to the recipient. The sender will not wait to make sure the recipient received the packet—it will continue sending the next packets.

Connect to a specific TCP/UDP port to make sure it’s responding. Optionally, a string to send and to expect can be entered. The specific string will have to be found from the documentation of the service you’re monitoring through.

Start leveraging the full power of Pingdom now. Sign up for a [14-day free trial](#).