DOSSarrest External Monitoring System (DEMS)

User’s Guide

- Real browser monitoring of your website
- Multi-sensor array for analysis of your CDN’s performance
- Immediate detection and reporting of outages and/or issues
- Powerful tool for your operations team for faster MTTR
- No click, single pane view to assess real-time the status of your website
- Drill down capabilities to gauge performance from 8 different sensors in 4 different geographic regions
- Aggressive 1 minute polling with auto refreshing views
- Optional 24/7 support available at your fingertips
CONTENTS

Overview .................................................. 1
Who is DEMS for? ........................................... 1
  CDN Enabled Sites ..................................... 2
  Service Provider ....................................... 2

How it Works ............................................... 3
Status ......................................................... 4
Timeline ..................................................... 5
Performance ............................................... 6
Uptime ......................................................... 6
Configuration ............................................. 7

Conclusion .................................................. 9
OVERVIEW

DOSarrest External Monitoring Service (DEMS) is at its core, a tool to monitor a customer’s website, and alert when the website goes down or suffers performance degradation. While simple enough in concept, it hasn’t been fully realized in the marketplace until now. Providing a straightforward but revealing view of the status of a website, from multiple locations, DEMS ensures instant notification of website issues and expedient failure scoping to ensure the highest possible availability.

Who is DEMS for?

At a high level, DEMS is for administrators who need to ensure 100% uptime and reachability from disparate geographical locations for one or more websites, and require instant notification when an issue arises with fast and easy to read results. Specifically, DEMS is ideal for the following types of users:

CDN enabled websites & Service Providers
**CDN Enabled Sites**

More and more customers are migrating their websites to a Content Delivery Network (CDN) for faster performance and to off load CPU usage. CDN providers (e.g. Akamai, Limelight, etc.) are able to replicate your website content and serve it from tens if not hundreds of different locations, putting it as close as possible to the end visitor. With so many servers and locations serving your content, how do you know when:

- A CDN city node is not responding to web requests, or there is degraded performance in a particular region/city
- A CDN server within a city starts to malfunction
- An incomplete DNS update resulting in inconsistent A records across various regions

With all the various issues that could arise in a CDN environment, it becomes imperative to have the ability to monitor your website performance from multiple locations, for a seamless user experience.

**Service Provider**

Service Providers (SP) typically have an operation center responsible for monitoring the server farms and network topology for their customers. To do so, there will be hundreds if not thousands of monitors and alerts set up to capture event logs, SNMP traps, etc., all to ensure that the underlying infrastructure is intact. What is typically missed, however, is how well a customer’s web presence is performing from outside of the SP environment, which is the most critical aspect for a customer.

With DEMS, an SP Operations Center can see in real time when one of their customer’s websites goes offline, and can immediately start investigating the root cause of the issue. No longer does the team have to be updated by an agitated customer that their website is not functioning properly. By leveraging DEMS, the operations team can proactively take care of the issue well before their customer notices any issues, and see immediate benefits in the areas such as:

- MTTR
- Response Time
- Accuracy of Diagnosis
- Availability
- Reduced Number of Tickets
- Reduced Number of Escalations

With an auto refresh rate of 1 minute, DEMS ensures your team is observing events in real time.
The DEMS utility is comprised of 8 sensors, deployed in strategic locations in North America, Europe, and Asia. Each sensor is housed with a separate provider and datacenter from the adjacent sensors, to ensure that there are no shared resources and/or networks.

Each sensor is responsible for monitoring a configured website by carrying out the following functions once every minute:

1. A DNS lookup of the website
2. Establishment of a TCP connection to port 80 and/or 443
3. Execute an HTTP/S request to the website and measure how long for a response back from the webserver
4. Calculate the length of time to transfer data from the first HTTP/S response to the end of the connection.

The sensors also have the capability to monitor for content changes to the website, warn if a SSL certificate is about to expire or has been changed, and do TCP checks for non HTTP/S ports (eg. Mail, DNS, etc.)

This monitoring information is then populated real time on a continuous basis, to a central database. From this centralized location, administrators can view & configure their website alerts and performance metrics via the DEMS web portal. The DEMS panel is a single pane view that provides access to the following areas:

- Status
- Timeline
- Performance
- Uptime
- Configuration

Each of these sections is accessible via the navigation section on the far left hand of the DEMS panel.

Note: The DEMS panel has been coded to provide details by simply hovering over portions of the GUI. There are also a number of shortcuts available within the GUI by simply right clicking. Don't be shy to explore these features to gain a quick appreciation of the capabilities.
The Status page is the default page when you log into the panel. The view is fairly self explanatory providing a quick summary of all configured websites and their status.

**Up Section:**
1. **ID** - a DOSarrest internal identifier for the domain
2. **Account** - main account that the site is configured for
3. **URL** - the website that is being monitored
4. **IP** - the IP that the URL is resolving to (if there are 2 or more DNS entries, the column will read “multiple”)
5. **Uptime** - how long since the last failure

**Down Section:**
1. **Account** - main account that site is configured under
2. **URL** - the website that is registering as being down
3. **Failure Reason** - detail on why the site is down, including HTTP status codes, DNS failures, TCP timeouts and excessive HTTP execution times
4. **IP** - the IP DNS was resolving to at the time of the failure
5. **LA/NY/LDN/SG** - regional breakdown of which sensors were showing the failure
6. **#** - the number of sensors out of pool of 8 that are showing the failure
7. **Downtime** - how long the site has been down

*Note:* if the DOWN section is blank, it indicates that there no events to report for that poll interval.

**Status-Navigation Section:**
1. **Update** - Click to get an immediate refresh of the status page instead of waiting for the auto refresh
2. **Auto Update** - toggle switch for enabling/disabling the auto refresh.
3. **Audio Alert** - toggle switch for enabling/disabling a sound alert for registered events
4. **Display HTTP** - toggle switch to display/remove HTTP sites
5. **Display HTTPS** - toggle switch to display/remove HTTPS sites
The Timeline section of the panel is a tool for viewing DNS changes and alerts chronologically for all websites under an account, over a specified period of time. The time intervals can range from going back 1 hour to 1 year.

On the far right hand, under the Navigation Section are a series of toggle buttons that define your Timeline view. It behaves very similar to the Navigation portion of the Status page, described previously.

With this view, you get a quick appreciation of what issues occurred, at what time, and from which location.

You’ll notice at the top of the Timeline view there are a series of drop down menus and columns. A breakdown of these areas is as follows:

1. **URL drop down** - pressing the arrow will show all available URL’s under the account.
2. **Time drop down** - selection of time intervals ranging from 1 hour to 1 year
3. **Load** - pressed once all drop down selections have values
4. **Date** - timestamp of the event
5. **Type** - shows the type of event, ranging from a failure, recovery, and DNS change.
6. **URL** - website that was selected
7. **Message** - Details on the event registered, ranging from HTTP status codes & timeouts, DNS changes, estimated downtimes, and failed TCP connections.
8. **IP** - the IP of the site during the registered event
9. **DOSarrest** - a check to confirm if the site was running through DOSarrest’s mitigation services
10. **#** - number of sensors that recorded the registered event
11. **LA/NY/LDN/SG** - regional breakdown of which sensors recorded the event
The Performance view provides a graphical view of how well a website is performing in terms of a real browser experience. Each sensor carries out a series of tests once every minute, checking for:

- **TCP**: how long it takes to create a TCP connection on port 80/443
- **HTTP execution**: how long it takes for the server to begin sending a response after an HTTP request is made
- **HTTP Transfer**: how long it takes for the server to finish transferring data to the sensor’s request

The results of these tests are charted in line graph, where the x axis denotes the time interval and the y axis denotes the time taken to execute each check. The results of each check are layered so they can be seen in a single view.

Each layer in the chart can be clicked to isolate the view to either TCP Connection, HTTP Transfer or HTTP Execution.

On the far right hand, under the Navigation section, you’ll see a legend detailing the TCP, HTTP Execution, HTTP Transfer, and Failure sections of the graph.

The Uptime section intention is to focus and chronicle only on the number of outages and duration of each incident, over a specified interval. The layout is very similar to the Timeline section, with the notable exception that it provides a summary of the total uptime of a site over the selected time interval.

With this view, the user can get a quick appreciation of how well their site has been performing for the last hour or up to one year.
Configuration

The Configuration view is an editor that can be used to customize the monitoring of the individual websites under an account. The editor has a number of preset values, and the default configuration covers most monitoring needs, so there is nothing to do here typically. For those customers who do need custom requirements, the editor is able to provide a high degree of customization, to tailor fit to their website.

Here is a list of all the tunable parameters you can employ:

1. General:
   - Enabled: Activate or disable monitoring of the site.
   - URL: The URL to be monitored
   - Timeout: The maximum amount of time the test can take
   - Test Frequency: How often a test should be run (interval range from 1 minute to 1 day)

2. Notification:
   - Send Alerts: Send notifications when an alert is triggered
   - Send Warnings: Send notifications when a warning is triggered
   - Send Notices: Send notifications when a notice is triggered
   - Email DOSarrest NOC: Send an alert to the DOSarrest NOC
   - Email Others: Send an alert to an email address or a list (comma-separated) of addresses.
   - SMS Others: Send an SMS to a phone number.

3. Alerts:
   - DNS Failure: Send an alert if the DNS lookup times out
   - TCP Failure: Send an alert if the TCP connection times out
   - SSL Failure: Send an alert if the SSL connection times out
   - HTTP Failure: Send an alert if the HTTP response times out
   - HTTP Redirect Loop: Send an alert if the site is redirecting to itself endlessly
   - HTTP Empty Response: Send an alert if the HTTP response is empty
   - MySQL Error: Send an alert if the HTTP response contains common MySQL connection errors
   - PHP Error: Send an alert if the HTTP response contains common PHP errors
   - ASP Error: Send an alert if the HTTP response contains common ASP errors
   - ColdFusion Error: Send an alert if the HTTP response contains a ColdFusion error page
   - Java Error: Send an alert if the HTTP response contains common Java errors

4. Warnings:
   - Intermittent Failures: Whether or not to record intermittent failures
   - DNS Changes: Whether or not to record DNS changes
   - Content Changes: Whether or not to record content changes
   - SSL Changes: Whether or not to record SSL changes
   - SSL Warnings: Whether or not to record SSL warnings
Configuration

5 TCP:
- IP: Use an IP address different from the DNS lookup
- Port: Use a non-standard port

6. SSL:
- Verify SSL Connection: Make sure the SSL certificates are properly verified
- SSL Protocols: Choose what protocols you want to use for verification (dropdown options of sslv2, sslv3, tlsv1, and dltsv1)

7. HTTP:
- Status Codes
- HTTP Version: What version of HTTP to use in the requests
- Follow Redirects: Whether or not to follow 301/302 redirects
- Store Cookies: Whether or not to temporarily store cookies
- Compress / Chunk Data: Whether or not to use chunked & compressed data
- Emulate Javascript: Whether or not to activate basic JavaScript emulation
- Custom User-Agent: Use a customer User-Agent string in the requests
- Response Search String: Search for a string in the response

8. Alert Thresholds:
- Simultaneous Sensors: How many sensors must fail at the same time in a row to trigger an alert
- Consecutive Failures: How many times must they fail in a row to trigger an alert
- Intermittent Failures: How many times it must fail intermittently to trigger an alert

9. Notes:
- Free form field for custom notes.
With the increased focus on e-commerce and maintaining brand recognition through your website, it’s imperative to know if and when your website is having issues from multiple vantage points. DEMS provides a fast and easy to use tool in determining the status of your website, and ensuring that your site achieves 100% uptime.

If you would like to reach our sales department for a free demo account, e-mail sales@dosarrest.com.