



WHITE PAPER



OMNITURE MONITORING

Ensuring the Security and Availability of Customer Data

June 16, 2008

Version 2.0



1 Omniture Monitoring

The Omniture Network Operations (NetOps) team has built a highly customized monitoring and notification system to proactively and reactively determine the health of Omniture's systems. Omniture NetOps has deployed a customized version of the open-source utility Nagios as our primary tool to monitor and alert the Omniture NetOps Staff 24 hours a day. In addition, Omniture has developed a customized Knowledge Base and ticket tracking system, including escalation, which ensures Omniture NetOps will be aware of any and all types of issues that may arise. The following sections outline the system checks, the frequency of these checks, as well as other procedures and systems related to Omniture monitoring.

1.1 Notification Procedures

Omniture's Network Operations Center (NOC) is staffed 24 hours a day by technicians and system administrators who monitor the network environment and the status of Omniture products. The NOC is prepared to receive and respond to a "hard" failure state (or alarm). Each time a hard failure occurs, an alarm is generated and sent to NOC. A ticket is also created in Omniture's problem tracking system (PTS) and an email is sent to all Omniture NetOps Staff members. The NOC has a fixed amount of time to acknowledge the alarm and start working on the issue.

If the NOC is unable to resolve an issue they will escalate to a rotating member of the Omniture NetOps Staff who carries a pager 24 hours a day. If after the allotted time, the NOC or a staff member has not either a) acknowledged that the issue is being worked on, or b) resolved the issue, another staff member carrying an "escalation" pager is notified. This alternate pager operates via a different pager network from the primary pager, for added redundancy in order to ensure that an issue is brought to the attention of the NetOps team in a timely manner. Both the primary and secondary contacts are then notified continuously until the problem is resolved.

1.2 Monitoring Descriptions

1.2.1 Servers

All Omniture servers have a set of standard checks performed on them, including all Linux and Solaris systems. These checks are listed as follows.

Check	Description
Ping	Ping checks are performed on an as-needed basis. If any of the monitoring checks fail, the system will perform a ping check to see if the server is responding and alert accordingly.
Current Time	If the system time varies by more than six seconds from Omniture time servers, an alarm is generated.
Disk Space	Each drive partition on each server is checked for free space. Depending on the server type, alerts will be sent out according to the amount of free space remaining.
Hardware Checks	Hardware failures generate warning or critical alerts, depending on the platform type and whether or not the failed item has redundancy. Hardware checks include items like CPUs, memory, power supplies, fans, hard drives and RAID arrays.

1.2.2 Services and applications

In addition to the standard set of server checks, servers also receive checks based on the services they provide. Monitored services include standard solutions such as database and web servers and customized solutions such as modified process or Omniture-specific services. These checks are performed to ensure that Omniture’s applications are functioning properly.

1.2.3 Web Servers

In addition to the standard set of checks, web servers receive some additional checks. Web servers receive additional checks for the following.

Check Item	Description
DNS	Each web server that uses DNS to perform reverse DNS lookups is checked to verify DNS is responding in a timely manner.
HTTP Service	The http/web service on each web server is checked for responsiveness and to ensure it is returning correct data.
HTTPS Service	Those web servers that provide SSL traffic receive additional checks on their HTTPS services. These work similar to the HTTP service checks, but also check for SSL encryption, functionality, and responsiveness, as well as the validity of the SSL certificate.

1.2.4 Network Devices

All switches, load balancers, and firewalls are checked at least every five minutes. Each device is checked via ICMP and TCP to ensure it is up and responsive. In addition, these devices are monitored via SNMP for items such as CPU utilization, failover state and power supply status. SNMP logs are monitored and critical events are reviewed by the NetOps staff.

1.2.5 Traffic Monitoring

Network devices are also polled via SNMP for traffic levels and connection counts, which we gather and graph via MRTG/RRD. Additionally, Omniture has systems in place to monitor all Omniture traffic for security issues. This information assists in the detection and diagnosis of problems.

1.2.6 Network and Other Specialized Servers

In addition to the standard Web, database, and network devices, Omniture has numerous other servers that provide supporting roles to the system, including servers that provide DNS, email, monitoring, and backup services.

Supporting Role	Description
DNS	We perform numerous checks on the availability of DNS, against both our primary and secondary DNS servers, from multiple locations. We monitor for responsiveness and the ability of the service to return accurate data.
Email	Email services are monitored from multiple locations, including our primary site, our secondary site, and our office locations. Receiving email communication from our servers is important to the management of our system and thus the ability for email to be processed correctly is very important. Both public and private network

	connections are in place to route email, should there be an Internet related email delivery problem.
Monitoring	Omniture's monitoring agents are deployed to multiple physical and network locations. In addition to monitoring hosts and services at its location, each agent monitors remote agents to verify that is 100% functional and correctly monitoring its designated devices and services.
Backups	We monitor the size of backups each day, as well as the completion rate and any errors, in order to verify all backups completed successfully. Additionally, we perform a battery of specialized checks on the hardware and software of the backup servers. Periodic test restores are performed to verify the integrity of backups.
Environmental Monitors	We monitor the temperature and humidity throughout our data center space, to ensure that all servers are operating in an ideal operating environment. Each environmental monitor is measured several times per hour, and any abnormalities are addressed by the Network Operations team.

1.3 Miscellaneous Checks

In addition to all of the server and device checks, we monitor many other aspects of our system, including, but not limited to the following.

Monitoring Type	Description
Web Site Responsiveness	Each web site we manage is checked via Nagios to make sure it is up and responsive. This allows us to independently detect application or software errors affecting a web site, which may not be detected by the previously defined system checks.
Application Monitoring	<ul style="list-style-type: none"> ▪ Numerous checks are performed on each system. A few examples of this monitoring are listed below. <ul style="list-style-type: none"> ○ Application state and performance on each Web and application server ○ Completion of nightly batch jobs ○ Number of emails being sent to customers ○ Minute by minute traffic levels <p>Dozens of services and areas of our system are checked every few minutes to make sure the applications are working normally and users can access their contracted services.</p>
First-party SSL Certificates	Omniture monitors client first-party SSL certificate implementations to ensure that the client's certificate is valid and has not expired

1.4 Network Availability & Performance

Omniture monitors the network availability and performance via numerous internal and external agents. Omniture uses multiple NSP's (Network Service Providers) and each NSP is monitored via multiple agents to ensure that Omniture's data collection agents and reports are available at all times.

Omniture has the ability to review network performance from more than 50 distinct Internet locations, both in the U.S. and abroad. Active monitoring runs at all times from approximately 20 independent locations connected to every

major NSP. Three independent monitoring providers have contracted with Omniture to provide minute by minute monitoring of network availability and performance. Alarms due to Internet connectivity are sent directly to Omniture's NetOps team for review and action.

1.5 Additional External Monitoring

Omniture also has contracted with several third-party monitoring providers to measure the availability of our systems and alert the NOC of any degradation in availability or response time.

1.5.1 Third-Party HTTP Monitoring

Multiple Vendors are engaged to monitor various components of Omniture services and reporting, as well as related services such as DNS. This occurs with varying frequency, but usually between one and three minutes for each vendor. Service failures are logged and sent to the Omniture NOC.

1.5.2 Keynote

Keynote timing and availability monitoring services are used to make sure our site is up and responsive from numerous locations around the country and world. Keynote also monitors the performance of our services in relation to how our competitors perform. Additionally, we have set response time thresholds for each test. Anything outside those thresholds generates an alert to the Omniture NOC.

1.5.3 Gomez

Omniture uses Gomez to monitoring our site availability and to verify the availability of Omniture services and reporting. Several times each hour, Gomez logs in and views multiple reports, simulating a user. Gomez generates alarms when the site is unavailable, the pages take too long to load, the entire process takes longer than set thresholds, or an unexpected error occurs. In addition, Gomez monitors the performance of data collection by checking performance from a variety of U.S. and International monitoring agents.

Omniture also uses Gomez private agents to measure response time from within our data centers without any impact from traversing the Internet. This provides the ability to identify the source of any performance degradation and better measure any variance in site performance due to internal factors.

1.5.4 WebSitePulse (WSP)

WSP monitors the performance and availability of several of Omniture products and services. WSP monitors multiple DNS servers, as well as both HTTP and HTTPS services for Omniture. These checks are performed every one to three minutes, depending on the configuration. Performance thresholds are in place on all measurements and WSP will contact Omniture NOC via email and pager, should any measurement exceed its limits or any other problems be detected.

1.5.5 External Nagios Deployments

Using the same Nagios monitoring technology that monitors our site locally, we run additional instances of Nagios at remote locations so that each site is monitored by at least one remote location. Each remote Nagios installation checks the other Nagios locations to verify the systems can be contacted and are fully functional, as well as performing other checks on Omniture products and services.

1.5.6 System Monitoring Uptime Reference Framework

Omniture has developed and deployed an internal tool that allows us to verify the availability and response time of data collection nodes every five seconds. This tool allows us to truly measure and verify uptimes exceeding 99.999% [5 nines] as measured from within our data center.

1.6 Summary

Omniture's Management and Network Operations staff takes the performance, availability, and scalability of our Web sites and services very seriously. We believe that the monitoring system in place is robust and thorough, resulting in more than a 700,000 checks per hour against our systems, hardware, software, and services. However, we continue to look for new and innovative ways to monitor our system and proactively detect potential problems before they arise.



CALL 1.877.722.7088
1.801.722.0139

www.omniture.com
info@omniture.com

550 East Timpanogos Circle
Orem, Utah 84097

