



DISASTER RECOVERY

Omniture Disaster Plan

June 2, 2008

Version 2.0



1 Disaster Recovery Plan Overview

In the event that one of our data collection environments are unavailable due to an event, whether a problem at the facility, a local situation, or a regional disaster, the following process will be followed to allow for continuation of data collection, and ensure an effective and accurate recovery.

1.1.1 Failover Process

When it has been determined that an event will result in long term disruption in data collection, Omniture will reconfigure DNS to send data collection requests to a secondary location not affected by the disaster. Omniture will also manually place a hold on data processing in the primary environment to preserve the chronological order of page views, which is necessary for the recovery process to work successfully. DNS record TTL (time to live) is set to allow this switch to the secondary location to happen quickly.

While data collection is in a failover mode, customers are notified of the ongoing situation with regular status updates from their account manager. If it is expected that the primary data collection location will be back online within five business days, no historical data will be transferred to, or data collection processed at, the secondary location. If the disaster at the primary data collection location is serious enough to have destroyed or make historical data there unavailable, Omniture will restore that data from backup tape stored at off-site locations.

1.1.2 Recovery Process

When the primary data collection location is available and stable again, the failover process will be reversed. All traffic collected at the secondary location will be merged with data in the primary location, DNS records will be restored, and page views will be processed sequentially in time order. During page view processing, SiteCatalyst will be available, but reports will not be real-time until page view processing is complete. Page view processing will take approximately one day for every four hours the failover process was active. Time required to recover historical data from tape may take up to an additional ten days.

2 Disaster Prevention Strategy

Omniture has implemented multiple levels of protection to prevent single, and even many multiple, failures from turning into a disaster. This section reviews many of the strategies employed to keep our service available and reliable.

2.1 Data Center Facilities

Omniture takes our choice of co-location facilities seriously and requires all facilities to meet the following basic requirements:

2.1.1 Power

The facility maintains multiple levels of backup power to prevent any power loss for customers. Each Omniture rack is fed by multiple primary and secondary circuits that are delivered from different PDUs and are connected to different generator banks. The facility can provide 100% of the power necessary to run independently of any other power supply. Transition from primary power to backup power must be fully automatic and occur without interruption of service.

2.1.2 Fire

The facility must employ VESDA (Very Early Smoke Detection) system that alerts facility personnel at the first sign of a fire, and pre-action, dry-pipe sprinkler systems with double interlock to ensure no water is released into a server area without the activation of a smoke detector and the presence of heat.

2.1.3 Security

The facility has 24-hour on-site personnel who require credentials to gain admittance to the facility. Use of biometric scanners to authorize data center access is also required. Remotely monitored video cameras provide continuous surveillance. All access to the facility is logged.

In the event of a disaster or at any time, Omniture can quickly deploy equipment to alternate locations and scale these sites to be full data collection locations, if necessary. Omniture is also currently evaluating additional facilities to bring online and deploy equipment to serve as failover sites.

2.2 Network Infrastructure

Omniture takes great care to ensure site availability and top notch performance for its customers. InterNAP provides Omniture with a uniquely built connection that puts the leading network providers of the Internet at Omniture's disposal. InterNAP manages Omniture's connectivity to the Internet, providing multiple redundant network carriers and offering advanced BGP management. This ensures not only top notch performance, but supreme redundancy. Network providers in use currently include: AT&T, Cable & Wireless, Global Crossing, UUNet, Genuity, Qwest, and Verio.

A failure or slowdown by any of these network providers is easily managed by InterNAP and traffic is automatically rerouted via alternate network paths. Key components, such as front end switches, load balancers, and firewalls, have standby equipment in place and will fail over automatically in the event of a device failure.

2.3 System Monitoring

Omniture takes great care to ensure site availability and top notch performance for all customers. To do so, we have developed application specific tools for monitoring the availability and performance of our services, providing a much greater detail and customization, that no commercial product could provide.

Omniture's Network Operations Center (NOC) is staffed 24/7 to monitor the status of the network and servers. Also, members of Omniture Network Operations are on-call 24/7/365 to answer and deal with any issues that cannot be handled by the NOC. Additionally, there is an automatic escalation process, if the NOC or on-call person does not respond to the monitoring system notification within 30 minutes. Every 15 minutes after this, additional personnel are notified until the problem is acknowledged or resolved.

We monitor a great deal of information about each piece of hardware, at each data center. For instance, all database servers are checked according to a strict monitoring schedule for system load, memory usage, disk space utilization, process status, correct time, and more.

System monitoring agents are in place at all data centers and our corporate office, and provide cross-monitoring. Should any monitoring agent fail, Omniture could deploy a new agent to a standby server within a matter of hours.

In addition our own tools, contracts have been arranged with system monitoring companies. These third-parties and the exact services they provide change from time to time, but the goal is to also have an external view on the performance and availability of our services.

2.4 Data Collection Servers

Every Omniture service is load balanced across multiple data collection servers. In the event of equipment or network failure, the load balancer detects the problematic server, removes it from rotation, and redistributes its connections amongst the remaining servers in the cluster. No disruption of service is experienced during a data collection server failure.

The on-call NetOps employee is then paged by the network monitoring server to further diagnose the issue. On-site data center technicians are available 24/7/365 to assist.

In the case of data collection server data loss, daily backups compile vital configuration files and can typically be recovered in a matter of minutes. This information is backed up to tape nightly. All data collection server data is simply a copy of data from our primary 'upload' server, so there is no data loss in the event of a complete data collection server crash.

2.5 Data Processing Servers

Utilized by Omniture data collection servers to process users' statistics, data processing servers function as an application layer to the data storage servers. When one of these data processing machines fails, the data collector stores the information it would normally transfer to the data collection server on disk. A standby data processing server checks each data collection server frequently for any stored hits. If it finds any, it retrieves and processes them.

When the failed data processing server is restored (or a backup activated) to working condition, the data collection server begins sending the hit information to it again. While a data processing server is down, a user's statistics may not be tracked in real-time, but all data collection continues uninterrupted. This remains the case until the server's assigned users are diverted to a spare data processing server.

2.6 Data Storage Servers

Omniture statistics are stored on database servers called data storage servers. When one of these machines experiences hardware failure, the data processing server continues to process statistics, but holds the data until the data storage server recovers. There is no impact on customer traffic recording during this time. The only customer impact is the brief inability to view stats during a data storage server outage.

If a data storage server becomes unstable, but returns to good health upon reboot, its logs are inspected for any information that yields insight into the crash. Any suspicious databases are checked for data corruption and repaired by a system administrator. If the server continues to be problematic, its information is redistributed to other servers.

Daily backups are made for each data storage server. If a server's databases are lost for any reason, they can be restored from the backup server. Data storage server data is stored on the highest quality SCSI drives in a RAID array with a hot spare. Once a drive failure is detected (check are made every five minutes), replacement of the failed drive is scheduled.

If data must be restored from a backup, the process must be initiated by a system administrator and can vary depending on the amount of data to be restored. Any data collected between the time of the last backup and the time of the crash may be lost.

The users assigned to a failed data storage server cannot view their Omniture reports until the server has been restored, or its database contents moved to another server. During this time, they are greeted by a page informing them of system maintenance.

2.7 Service Databases

Service database servers are a single point of failure. If they not available, the service is unusable. These machines are backed up twice daily and in the event of a catastrophic hardware failure, the most recent backup would be restored to a standby machine. In such a case, the maximum window of data loss is 12 hours.

2.7.1 Report Servers

Omniture report service is load balanced across multiple servers. In the event of equipment or network failure, the load balancer detects the problematic server, removes it from rotation, and redistributes its connections amongst the remaining servers. No disruption of service is experienced during a report server failure.

2.7.2 Backup System

System data is downloaded nightly and archived onto a number of massive and redundant disk arrays. Backups are kept locally on disk for several days. This allows for quick retrieval in case of emergency, without going to tape. Backups are made across multiple servers and consolidated to central backup master servers each day. Then, backups are made to directly attached tape storage libraries. Tapes are rotated each week by data center technicians.

Backup tapes are immediately available throughout a calendar month. Tapes are moved to an off-site storage facility each week, where they are archived for up to one year. There they are stored securely. Backups from off-site storage can be initiated within a matter of hours.

2.7.3 Staffing

Omniture employs a highly-training and very skilled group of employees for network management and software development. All members of the network operations team are cross-trained in each area, so they will be able to resolve any potential problem.

In the event that the situation arises where it becomes necessary to replace these employees in an emergency, several other employees at Omniture, especially in software development, are well-suited to take over because they have a general understanding of the system's design and function.

2.7.4 Equipment Procurement

Omniture maintains relationships with multiple vendors, including national companies and local companies. Effort is made to keep all of these channels open so that we can immediately order and schedule emergency delivery of any needed equipment.



Should it become necessary, Omniture will work with these local and national vendors to rebuild any critical components affected by an event. We also maintain an in-house inventory of components that have a higher failure rate or need replacement in the event they become unavailable in the current marketplace.



CALL 1.877.722.7088
1.801.722.0139

www.omniture.com
info@omniture.com

550 East Timpanogos Circle
Orem, Utah 84097

