the Availability Digest

www.availabilitydigest.com

Fire Suppression Suppresses WestHost for Days

May 2010

It’s not a good idea to test a fire-suppression system by triggering it. But that’s what happened to WestHost, a major web-hosting provider headquartered in Utah. The accidental release of a blast of fire-suppressant gas severely damaged most of its servers and data stores. Hardware repair and database recovery efforts put WestHost’s customers out of commission for up to six days.

WestHost

Founded in 1998, WestHost provides shared web hosting, dedicated servers, and domain registration for businesses, organizations, and individuals. It currently hosts over 80,000 domain names. In 2008, WestHost was acquired by UK-based UK2 Group, a much larger web-hosting company that manages over a million domain names.

WestHost has been rated consistently high by web-hosting rating agencies. WestHost continually ranks in the Netcraft top 10 list of most reliable Web hosting providers, including several top 10 rankings throughout 2006, 2007, and 2008.

WestHost is collocated in an SAS 70 Type II certified data center in Utah. SAS 70 (Statement on Auditing Standards No. 70) is an internationally recognized third-party assurance audit that provides service organizations a benchmark to compare their internal controls and processes against industry best practices. SAS 70 Type II provides the highest level of SAS 70 audits and reports on each service organization’s controls and operating effectiveness over a period of time.

Among other facilities to ensure SAS 70 compliance, WestHost’s data center maintains a Tier 1 connection to the Internet, has diesel-generator power backup good for three to five days, and is equipped with an Inergen people-safe fire-suppression system.

In a review of WestHost, *The Web Hosting Doctor* said:

> “There is no doubt that WestHost provides reliable hosting solutions…. WestHost’s data center was designed to be able to handle and conquer just about any situation …. Prevention is also key in working to have a fire protection.”

It is the fire-suppression system that became the Achilles’ heel for WestHost.

Inergen

The WestHost fire-suppression system works by releasing Inergen gas. Comprising common atmospheric gases, Inergen is environmentally friendly and breathable by people; but it reduces the oxygen content of air to a level that does not support combustion.

Inergen comprises 52% nitrogen, 40% argon, and 8% carbon. Normal air is 21% oxygen and 79% nitrogen with traces of carbon dioxide and other gases. Enough Inergen in a fire-suppression system is released to create a 40% to 50% concentration in the computer room's normal air supply. This reduces the oxygen content in the computer room to about 10% to 12%, which is not enough to support combustion (about a 15% oxygen concentration is required for combustion).

However, the increased carbon dioxide level in Inergen increases a person's respiration rate (it is carbon dioxide in our blood stream that invokes the breathing response), allowing a person to function in the reduced oxygen level Therefore, Inergen is safe for humans, although they should be evacuated as quickly as possible.

In the event of a fire, Inergen is released rapidly and causes a large pressure surge that must be relieved quickly to prevent damage to the enclosed space.

The Meltdown

On Saturday, February 20, 2010, the WestHost data center underwent a standard yearly test of its Inergen fire-suppression system. Unfortunately, a third-party test technician failed to follow the published pre-test check list and did not remove one of the actuators that activates the system. At about 2:20 PM local time, when the system was re-armed following the test, the actuator fired and triggered the release of the large blast of Inergen gas designed to put a fire out.

No one seems to know for sure whether it was the pressure blast or the gas itself, but hundreds of servers and disk storage systems were severely damaged. WestHost operations immediately came to a halt, and it was days before full service was restored.

WestHost's first challenge was to get the failed servers back into operation. However, many were so severely damaged that they required the replacement of hardware components. Some servers could be repaired with onsite spares. Others had to wait for spares to be delivered from WestHost's suppliers via expedited delivery. Despite this Herculean effort, WestHost reported Monday afternoon (50 hours later) that eighteen servers had yet to be returned to service.

But this was only the beginning of the recovery effort. The repaired servers had to have their databases restored, a task that WestHost predicted would take another four days to complete. In a posted announcement, WestHost explained:

> "At present, we have restored service to all but twelve shared and six dedicated servers. … Retrieving lost data and restoring from backups can take up to 24 hours per server. This is where we are with the majority of downed servers. Our backup process restores three servers simultaneously."

The next problem then presented its ugly head. The backup drives were in the same facility as the servers, and many of the backup disks were destroyed. Some RAID drives were recoverable, and their servers were brought back into service. For others, data recovery experts were brought in and were able to restore data from failed drives. However, some data was simply deemed nonrecoverable by the data-restoration experts.

Even after servers and their databases were restored, WestHost reported that some were still experiencing file-system problems that resulted in poor performance.

The end result of all these efforts was that many shared and hosted services were down for as long as six days.

Keeping Customers Informed

Information concerning the outage and the recovery effort was slow in coming out of WestHost. Its ability to keep its customers informed did not get rave reviews, though this may be understandable due to the massiveness of the outage. Not only was WestHost swamped with customer queries, but its people were consumed by the efforts to get the data center back in business. The only source of information for many of WestHost's customers was what was posted on its Netstatus page at http://netstatus.westhost.co\m.

One important move that WestHost did make was to bring up some server capacity that its customers could use for temporary purposes. This capacity could be used to provide email services since the downed servers had taken email systems with them. It could also be used to communicate with customers to keep them informed about the outage. WestHost patched DNS addresses to reroute traffic from a customer's normal web site to the temporary web site.

WestHost said that it would also compensate its customers with one or more free months of service (the cost for business shared services ranges upwards from $12.95 per month).

Lessons Learned

The first question to ask is how a fire-suppression system could destroy so much equipment? The answer to this is still pending. If a fire-suppression system is going to cause this much damage, why have one? (Insurance costs, perhaps.)

Given that, what lessons can be learned from WestHost's experience? The blogs are full of good observations about the impact of this disastrous outage and what people should think about in the future.

- Don't depend upon data centers, even those with advanced certifications, to protect your services and data. Even their SLAs are clear that there is no protection. The degree of protection that they provide is more of a marketing statement than it is a factual guarantee. Data protection and service continuity are your responsibilities.

- Always back up your data offsite. WestHost was faulted for not having offsite data backup. Even if a data center does provide offsite backup, there is no guarantee that the backup data will be accessible if there is a major disaster such as experienced by WestHost. You should back up data on an independent hosting service, an independent backup service, or on your own servers (your own PC if you are a blogger).

- If your web site is critical (such as for an online store), be prepared to bring it up temporarily on another hosting service or on your own servers should your primary hosting service go down. This requires that your data can be restored. You will lose any data from the time of your last backup. Real-time replication of your data to an independent storage facility will minimize your lost transactions. You can easily switch all web traffic from your primary site to your backup site by simply changing the DNS pointer in your local DNS server.

- Obtain domain registration from a service other than the hosting service you are using. Otherwise, the failure of the DNS server maintained by your primary hosting service may mean that you cannot switch traffic to a temporary backup web site.

- Your email should not be provided by the same hosting service as the one that hosts your web site. It is bad enough that you lose your web site. If you also lose your email, you are really down.

- Communicate with your customers to keep them informed as to what is going on. Even if you don't plan to provide a full backup of your web site, you can provide a temporary web site to post information to your customers concerning an outage if your primary web site is unavailable. If you have this capability, all you have to do is to switch your DNS entry to point to your temporary web site.

The bottom line is that you are the only one ultimately responsible for your web services. It doesn't cost much, if anything, to make sure that you stay in business if your hosting service goes down. All it takes is a little planning.

Acknowledgements

Thanks to our subscriber, Dylan Holenstein, for bringing this to our attention.

Information from this article was taken from the following sources:

Data Center Outage Incident, *WestHost*; undated.
New York Internet and WestHost are the Most Reliable Hosting Companies in December, 2008,*Netcraft*.
WestHost Review, *The Web Hosting Doctor*; undated.
WestHost 3.0 Outage Details, *getsatisfaction.com/westhost*; February 22, 2010.
Horrendous Multi-Day Outage and ridiculous treatment of customers by WestHost, *WebHosting Talk*
Lessons Learned from the Massive WestHost Outage this Week, *Computer Tips – Tech Info*; undated.
Lessons Learned From WestHost Outage, *Larry Dearing Blog*; February 28, 2010.
WestHost, *Wikipedia.*
Inergen, *Wikipedia.*