the Availability Digest

www.availabilitydigest.com

# Commerzbank Survives 9/11 with OpenVMS Clusters

July 2009

On September 11, 2001, the World Trade Center was destroyed when two airliners piloted by terrorists crashed into the twin towers. The New York offices of Commerzbank, a major German bank, were only 100 yards away on the 31st to 34th floors of 2 World Financial Center. Though the bank's data center physically survived the terrorist attack, the intense dust and heat caused most of its systems to crash. To complicate matters, all communication with the outside world was lost, potentially bringing its U.S. business to a halt.

However, Commerzbank had the foresight to distribute its processing with an OpenVMS Active/Active Split-Site Cluster. Its processing services continued uninterrupted in its alternate location thirty miles away, allowing it to continue to provide seamless service following the terrorist attack.

## Commerzbank

Commerzbank (www.commerzbank.com) has a long and varied history. It was established in 1870 in Hamburg, Germany, to facilitate overseas trade for Hamburg. It survived World War I and continued to grow by merger and acquisition during the inflation years triggered by the Versailles treaty, which laid the groundwork for the growth and eventual takeover of German life by the National Socialist Party.

Commerz- und Privat-Bank Aktiengesellschaft
HAMBURG.
Depositenkasse St. Georg.
1,000,000 Mark
in 10 Stück zu 100,000 Mark.
Ohne Gewähr, daher beim Empfang zu zählen!
Nachträgliche Beanstandungen können nicht berücksichtigt werden.

**Bank-note band from the inflation years, circa 1922**

Following World War II, Commerzbank lost the 45% of its locations that were in the Soviet zone. However, it continued to build a national network of branches and began its international expansion. It opened its first New York branch in 1971 – the first German bank branch in the United States. Opening further U.S. branches in Los Angeles, Chicago, and Atlanta, its U.S. branches focused on commercial and investment banking. Today, Commerzbank North America is a wholesale bank that serves approximately 500 customers, many of whom are Fortune 500 companies. Commerzbank now has branches in major business and financial centers in over forty countries.

Commerzbank has grown to be Germany's second largest bank. With headquarters now in Frankfurt, It has 36,000 employees, 8,000 of whom are outside of Germany. It provides in-branch, telephone, and online financial services to individuals, small to medium-sized businesses, and large multinational companies. With 1,200 branches, it services 5.7 million retail clients and has a stated objective to establish itself as the number one bank for Germany's small to medium-sized businesses. Through a subsidiary, it is now Germany's largest online broker. True to its roots, it finances 16% of Germany's foreign trade.

## Commerzbank's Quest for Zero Downtime

While most large organizations today have plans for disaster recovery and in many cases for disaster tolerance (i.e., users will be unaware of a site disaster), few have had to put these plans to a real-life test. But on September 11, 2001, Commerzbank's critical processing systems were tested when its primary North-American data center near the World Trade Center was put out of commission after the twin towers collapsed following a terrorist attack. Because of astute foresight, Commerzbank was able to continue its North American operations in its data center thirty miles away.

Commerzbank's stated goal is for zero downtime in any of its critical IT production systems. This imperative means that there must be redundancy of data and processing at more than one location and with rapid failover.

To achieve this goal, the bank runs its critical systems on HP's OpenVMS Split-Site Cluster. Commerzbank uses OpenVMS servers in a cluster configuration at two locations – 2 World Financial Center across the West Side Highway from the World Trade Center in New York City (its primary data center) and in Rye, New York, thirty miles away (its remote data center). The remote data center in Rye is the contingency site for disaster tolerance and is used during normal times for development, testing, and training. Its databases are kept in real-time synchronization with those at the primary site so that it is immediately available to take over processing with no loss of data in the event of a primary site failure.

OpenVMS Clusters[1] are active/active systems that allow applications to run simultaneously on multiple nodes. The geographically-distributed databases (shadow sets) at the various nodes are kept synchronized via synchronous replication using distributed lock and cache management (a technology called Host-Based Volume Shadowing, or HBVS). Should a node in a data center fail, or should an entire data center be taken down, user requests are simply rerouted to a surviving node or data center. Failover can be accomplished in seconds.

Critical applications entrusted to the OpenVMS clusters include a money-transfer system responsible for the bank's connection to the Federal Reserve and the New York Clearing House, a trading system, a banking system that handles international banking requirements, a letter-of-credit system, and a futures and options system.

## The OpenVMS Cluster Configuration - 2001

To ensure constant uptime, the bank at the time of the 9/11 attacks ran one AlphaServer GS160 system at its primary site in downtown Manhattan and one such server in its remote location in Rye. Storage was provided via StorageWorks systems to store two terabytes of data utilizing RAID 0, RAID 1, and RAID 5 technologies in a SAN (storage-area network) environment.

At the remote site was a pair of AlphaServer 4100 servers that were logically part of the primary cluster. Their role was to connect the remote drives to the primary cluster node using fibre-channel links. All disk drives at both the primary site and the remote site were volume shadowed so that changes made to any database at the primary site were synchronously replicated to the remote site.

As a result of this wide-area clustering, the application databases were always available and were updated in real time.

[1] OpenVMS Active/Active Split-Site Clusters, *Availability Digest*; June 2008.

## Surviving the Meltdown[2]

When the first jet hit, Commerzbank's World Financial Center facility lost its communications with the Federal Reserve and the New York Clearing House. A staff member switched the links to the remote site, and connection between the primary site and these organizations was restored.

Operations proceeded normally until the second jet hit. At this point, the 400 employees at the primary site evacuated the building.

The primary site was heavily protected with environmental contingency, including its own generator, fuel tank, cooling tower, uninterrupted power supply, battery-backup system, fire suppression, as well as extra CPUs and disk drives. As a result, when the World Trade Center lost power, the generator and cooling system kicked in so that all systems continued in operation initially. However, dust and debris from the collapse of the towers caused the air-conditioning units to fail; and temperatures rose dramatically.

Because of the intense heat in the building, which climbed to 104º F, all of the systems in the data center crashed except for the clustered AlphaServer, which managed to keep running all of its partitions but one. The disk SANs crashed, but the primary AlphaServer used the fibre-connected SANs at the remote site. The critical money-transfer system never went down and continued to operate at the primary site for the rest of the day.

Commerzbank's main challenge at this point was to get its employees to the remote data center in Rye. This was in the face of the closure of the New York City subways, trains, and bridges. However, though there were 400 employees stationed in the primary data center, Commerzbank's contingency plan allowed the remote site to be temporarily operated for two days with only ten people. It was able to get sixteen people to Rye the first day, and the remainder of the employees arrived over the next few days as transportation became available.

Compaq (now HP) offered whatever help Commerzbank needed, including emergency extra hardware. But because of its remote site, Commerzbank needed no such help.

For the next eight months, about two-thirds of the bank's employees worked in Rye; and the remainder worked at a subsidiary in Midtown Manhattan. The primary facility was available for reoccupancy in mid-May, 2002.

## The Power of a Contingency Plan

Commerzbank's experience during this disaster clearly reflects the power of proper contingency planning. The bank's disaster tolerance environment is only part of a much larger business-continuity plan. Not only does the bank test its contingency procedures with business users on a regular basis, but it has a call tree to make sure that everyone is on board with the situation during an emergency.

Frequent testing of its contingency procedures is possible because of the active/active capability of the OpenVMS Cluster. Users can be switched rapidly and reliably to the backup system with little concern about experiencing a failover fault.

[2] Material for this case study was taken from the OpenVMS case study, HP AlphaServer technology helps Commerzbank tolerate disaster on September 11, http://h71000.www7.hp.com/openvms/brochures/commerzbank.

## Summary

Commerzbank’s continued operation in the face of the 9/11 disaster is a testament to the power of active/active systems. Though in its case, only the disk systems were run in an active/active mode, the provision of a synchronized remote database allowed the bank to rapidly switch users from the failed primary data center to the remote data center.

This same capability allowed the bank to frequently test its disaster-tolerance contingency plan. Too often, companies avoid testing failover to a redundant system because of the extended downtime imposed on users during failover and the risk of a failover fault because the backup system’s environment does not match that of the primary system.

With active/active configurations, failover can be done in seconds. Furthermore, it is always known that all nodes are operational because they are in service (even if one is idle in contingency mode). Testing can be done frequently and with little risk to ensure that when a disaster happens, contingency works.