

I D C T E C H N O L O G Y S P O T L I G H T

Enterprise Data Recording: A New Technology for Robust Disaster Recovery

February 2010

Adapted from *Worldwide Storage Replication Software 2009–2013 Forecast: First Look as Market Evolution Provides Continued Growth* by Laura DuBois and Steven Scully, IDC #218370

Sponsored by Axxana

Introduction: Disaster Recovery Remains a Top IT Priority

Planning for disasters, whether natural or manmade, has been a key priority for IT organizations for a long time. Since the turn of the century, there has been no shortage of natural disasters such as floods, earthquakes, hurricanes, tsunamis, and forest fires as well as manmade calamities including terrorism, viruses, and power outages. IDC surveys of customers worldwide continue to show that spending on disaster recovery (DR) solutions is a top budget area for IT organizations of all sizes.

When it comes to choosing a DR solution, organizations have numerous options. These solutions are available in many shapes and sizes. They all involve certain trade-offs — capacity, performance, recovery point objectives (RPOs), recovery time objectives (RTOs), distance, and of course, cost. Traditional DR solutions involve some form of redundant hardware, special software (OS and application), and remote storage. The storage component has long been a focus of DR solutions and has evolved from tape-based to disk-based products.

For organizations that need the highest levels of protection, especially when it comes to zero data loss, the traditional choice has been one of the multiple DR solutions based on synchronous remote replication. Synchronous solutions guarantee that no data is lost by committing every write to two different disk systems before allowing the application to proceed. While effective, synchronous DR solutions have the following limitations:

- **Limited distance between the primary and remote site.** To be able to write both copies of the data near simultaneously, the typical synchronous DR solution is limited to 20 to 30 miles of separation. This is not a significant distance to protect data from regional disasters.
- **Expensive to implement.** Synchronous replication has been traditionally achieved through the use of expensive, high-end disk storage systems, coupled with specialized replication software. Professional services often are required to install and configure the solution and make sure all the components are working together.
- **Costly network resources.** Large amounts of high-priced network bandwidth need to be acquired and maintained.

Organizations that have less stringent data protection requirements and/or budget constraints have turned to asynchronous replication. These DR solutions require less expensive storage hardware and software and do not require expensive synchronous communication lines, allowing customers to

overcome the distance and cost limitations of synchronous solutions. However, asynchronous systems have their own limitations, including the following:

- Data can be lost between the time it was written at the primary site and received and written at the remote site (The farther the distance between the two sites, the greater the amount of data that is at risk.)
- Difficulties in maintaining consistency between the primary and remote sites in complex environments
- Subject to link failures (Because of the distances involved, organizations typically contract for some form of IP-based connectivity.)
- Longer recovery time

To overcome the limitations of both synchronous and asynchronous solutions, many organizations implement multihop DR solutions that rely on synchronous replication to a nearby DR site (to meet RPO requirements) and asynchronous replication to a more remote site (to meet distance requirements). These solutions can be designed to replicate simultaneously to both sites or fail over from the nearby site to the remote site.

The main drawback with multihop solutions is their tremendous cost. Customers have to buy not one DR solution (including hardware and software) but essentially two; they need two separate remote datacenters (either their own or a hosted site), they have to acquire and manage multiple separate network connections, and they typically need extensive professional services to implement.

Considering Axxana

For some IT organizations, most data (say 80%) can be adequately protected with asynchronous DR solutions. This data does not change fast enough or have the critical business value to warrant expensive DR solutions. The challenge for companies, then, is how to cost-effectively and reliably protect the data that *is* critical to the business and must be protected without any data loss. The problem that Axxana, headquartered in Tel Aviv, Israel, looked to solve was how, through virtually any disaster, to cost-effectively protect the most recent write operations that do not make it to the remote, asynchronous site. Axxana's solution was to develop a new type of storage technology.

Enterprise data recording (EDR) is a new solution for protecting and recovering data in the event of a disaster. It allows customers to achieve zero data loss without the distance limitations of traditional solutions by augmenting asynchronous DR solutions with a local synchronous copy of the most recent write operations stored in a disaster-proof device called a "Black Box," which is the core of an EDR solution.

The Black Box is a hardened vault, which is similar in concept to the black box flight data recorders used in modern aircraft to record and preserve critical flight data before a disaster. Inside the vault are all the system electronics, including a solid state disk (SSD), six-hour battery backup, and a protected cellular transmitter with multiple, redundant antennas. The vault is fully sealed, wrapped with thermal protection, and installed in a cabinet. The Black Box is designed to withstand a wide range of extreme conditions, including direct fire, prolonged heat, floods, punctures, and crushing. Specifically, the Black Box is capable of withstanding the following conditions:

- Up to 2,000F (1,093C) for an hour of direct flame
- Up to 482F (250C) for six hours
- 40G of shock

- 5,000lb (2,268kg) of weight
- 30ft of water pressure
- Pierce force of 500lb (227kg) rod with cross-section of .042 dropped from 10ft (3m) height

The Black Box works as a disaster-proof local cache for the most current write operations, and the asynchronous DR solution provides the unlimited distance capabilities. Compared with a multihop DR solution, the EDR approach offers dramatic cost savings. The asynchronous portion remains the same and provides the required long distance protection to a significantly remote site. The synchronous portion, though, is replaced by the features of EDR and the capabilities of the Black Box.

Instead of data being written synchronously to a secondary remote site, that task is accomplished onsite with a direct connection to the disaster-proof vault. This eliminates all the costs of the second regional datacenter, a second high-end storage system, synchronous replication software, and expensive synchronous communication lines.

Some of the benefits customers can expect from this approach include the following:

- A zero data loss RPO by synchronously protecting the most recent write operations
- Support for unlimited distances with zero data loss over asynchronous replication infrastructure
- Significantly lower cost, especially compared with multihop solutions and synchronous mirroring
- Ability to protect against link failures through the local copy
- Better consistency of replicated data by effectively providing synchronous replication for all data

Because an EDR solution augments existing DR infrastructures, it can be easily installed alongside the existing solution for testing and implementation. If a customer is currently using only asynchronous replication, the EDR portion can be added and will immediately begin providing local, synchronous protection. If a customer is currently using multihop replication, the EDR solution can be installed and operated in parallel until the customer is ready to retire the synchronous portion.

The Axxana Phoenix System

To deliver on the concept of EDR, Axxana has developed the Axxana Phoenix System. The Phoenix System works together with third-party asynchronous replication solutions, and the first product, the Axxana Phoenix System RP, supports EMC's RecoverPoint replication appliance. The Phoenix System consists of the following four components:

- Black Box
- Collector
- Recoverer
- Management Tool

The Black Box and the Collector are installed in the primary datacenter. The Collector continuously processes the data from the primary storage system, encrypting it and storing it synchronously to the SSD in the Black Box through a protected 2GBps Fibre Channel port. The Black Box is currently available in various capacities depending upon customer requirements.

The Recoverer is located at the remote site and orchestrates the data recovery process, when required. It reintegrates data, stored in the Black Box, with the asynchronous copy in the remote site. Extraction of the data after a disaster is accomplished with the built-in cellular capabilities of the Black Box using the highly resilient cellular network or by physically connecting the protected Ethernet port in the Black Box to a laptop running Axxana software. Using the cellular network, 2.5GB per hour can be transferred during the six hours of battery life.

For the first version of the system, the Phoenix System RP, Axxana has worked closely with EMC to deliver the value of EDR to EMC environments. Zero RPO is a key disaster recovery metric for many customer applications. This version works in conjunction with EMC's RecoverPoint remote data protection solution. RecoverPoint is a network-based solution that provides a number of capabilities from synchronous to asynchronous replication, continuous data protection (CDP), and bandwidth reduction. The Phoenix System RP targets EMC customers using CLARiiON systems, allowing utilization of replication over any distance while maintaining the ability to recover data without data loss. Integration with RecoverPoint's network splitter will allow the Phoenix System RP to support heterogeneous EMC storage solutions in the near future.

The Phoenix System RP with RecoverPoint was tested successfully for deployment with EMC's E-Lab, which maintains the industry's most rigorous interoperability testing and qualification processes. The Phoenix System is now available through the EMC Select Program.

Use Cases

The following use cases are examples of customers that have installed an Axxana EDR solution.

Use Case #1 — Protection Against Regional Disasters

Current State

Controller-based synchronous mirroring technology is used to replicate data between two datacenters located approximately 45 kilometers apart.

The company also performs monthly full backups, weekly differential backups, and daily incremental backups to tape. Tapes are stored at a secure location in another region.

To protect against regional disasters, the company maintains a disaster recovery contract with a third-party service provider in another region, where the company can restore the tape data and resume operations. The company chose the 45-kilometer datacenter distance to minimize transaction latencies associated with performing two-phase commits in transaction databases.

In the event of a single-site failure, the company is protected against data loss because all transactions are synchronously replicated to the second site. However, in the event of a catastrophic regional disaster that destroys both datacenters, the company will lose all data created since the last backup, and the time to restore the backup data from tape at the DR center will be unacceptably long.

Desired State

- Locate the second datacenter in another geographic region
- Eliminate tape backups
- Terminate the contract with the third-party DR supplier
- Continue to maintain two synchronized copies of all transaction data
- Preserve current transaction latencies

Solution

The company meets all elements of the desired state by utilizing a datacenter in another geographic region and by leveraging Axxana's EDR in conjunction with EMC RecoverPoint.

By having a second datacenter in another geographic region, the company can terminate the contract with the third-party DR supplier.

EMC RecoverPoint creates an application-consistent, mountable copy of data at the remote site, which eliminates the need for tape backups by creating multiple mountable snapshots of the data.

The Axxana EDR maintains a synchronous copy of any data created since the last snapshot. In the event of a disaster, the EDR automatically transmits the data to the remote site over a cellular network.

Use Case #2 — Link Loss: Maintaining Synchronous Replication and Eliminating Unnecessary Disaster Declarations

Current State

This company uses controller-based synchronous mirroring technology. However, link failures happen multiple times per year, during which, the company needs time to determine if it is a "real disaster" or a link failure. The company must choose between declaring a disaster, which is expensive, or turning off synchronous mirroring, which exposes the company to data loss.

Desired State

- Avoid unnecessary disaster declarations
- Eliminate data loss exposure induced by turning off synchronous replication

Solution

The company implements asynchronous mirroring with application-consistent snapshots, ensuring recoverable data, together with Axxana's EDR, which provides a three-hour buffer to diagnose the cause of a failure and determine the need to declare a datacenter disaster.

Use Case #3 — Service Provider Converting Asynch to Synch

Current State

The company is a hosting provider protecting data using asynchronous replication. The company's customers are demanding zero data loss. However, relocation of a secondary datacenter — as well as development of a third, synchronous site — is cost-prohibitive.

Desired State

- Provide zero data loss
- Avoid costs associated with datacenter relocation
- Avoid costs associated with a third datacenter

Solution

The company continues to use asynchronous mirroring with application-consistent snapshots and augments it with Axxana's EDR, which ensures that customers lose no data.

Use Case #4 — Global Bank Eliminates Need for Multisite, Multihop Replication

Current State

A global bank employs a multihop replication topology, with synchronous local and asynchronous distance replication. However, regulators and customers are demanding zero data loss. Moreover, the bank's CFO is concerned with growing datacenter costs, while shareholders are concerned about the impact on profit margins.

Desired State

- Maintain zero data loss capabilities of current solution
- Eliminate the cost of a third datacenter

Solution

The company continues to use asynchronous mirroring with application-consistent snapshots to a remote datacenter and replaces the local, synchronous datacenter with Axxana's EDR, which ensures that customers lose no data.

Market Challenges

It's especially challenging to enter the market in difficult economic times as Axxana has done. However, IT organizations facing budget constraints and resource limitations have shown surprising openness to new technologies and new vendors during these times, especially solutions that improve storage efficiencies and lower overall storage costs. As a new vendor with a new technology, Axxana will face several common challenges, including:

- Creating a new market category, which EDR represents, is never an easy task for either existing or startup (such as Axxana) vendors. It typically requires significant investment in education and promotion. The advantage for Axxana is that EDR leverages a concept many people understand — the Black Box.
- Working with established storage system vendors has two sides for Axxana. On one hand, the Phoenix System augments existing asynchronous replication offerings. Axxana must work closely with these vendors to verify system interoperability (as it has done with EMC) and then leverage those vendors to go to market. On the other hand, the Phoenix System represents yet another option for customers, creating an opportunity for confusion with the multiple data protection offerings in many storage vendors' portfolios.
- Making sure customers understand the Axxana Phoenix System is not a complete DR solution all by itself (Axxana does not represent it as such). It does require integration with third-party replication software, and Axxana is dependent on those vendor relationships to go to market. The system is designed for extreme outages with a focus on zero data loss RPO. RTO requirements are adjusted to the customer's need and might bear a slight delay over traditional synchronous replication solutions in the event of a disaster.

Conclusion

The market for disaster recovery solutions continues to grow, indicating that customers know they need DR solutions for their IT environments. IDC forecasts that between 2008 and 2013, the overall data protection and recovery market will have a compound annual growth rate (CAGR) of 4.8%. The market for storage replication solutions is also forecast to grow at a CAGR of 8.7% over the same period, especially for solutions outside traditional array-based replication.

In today's uncertain world with natural disasters and manmade calamities, organizations need the ultimate in disaster recovery solutions, either because the business value of even a couple of minutes of data loss is so great or because the regulatory requirements are so severe. For these organizations, IT managers have a new option to protect this critical data with EDR and the Axxana Phoenix System.

ABOUT THIS PUBLICATION

This publication was produced by IDC Go-to-Market Services. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Go-to-Market Services makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

COPYRIGHT AND RESTRICTIONS

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests, contact the GMS information line at 508-988-7610 or gms@idc.com. Translation and/or localization of this document requires an additional license from IDC.

For more information on IDC, visit www.idc.com. For more information on IDC GMS, visit www.idc.com/gms.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com