NASCIO 2018 State IT Recognition Awards Nomination

AGENCY FOR STATE TECHNOLOGY

State of Florida

Enterprise Disaster Recovery

January 2016 - Ongoing

Cybersecurity Initiative

Eric Larson, Executive Director/State CIO
Eric.Larson@ast.myflorida.com
850.412.6045

Executive Summary

With over 1,350 miles of coastline, the State of Florida is always faced with the possibility of being affected by hurricanes capable of massive destruction and until recently, each state agency was responsible for Information Technology (IT) Disaster Recovery (DR) planning and execution of their respective applications. In 2014, an independent assessment was conducted to inventory, prioritize, and evaluate the disaster preparedness of all applications in the State of Florida. Approximately 950 applications were inventoried, of which 150 were deemed mission critical with very few having complete, tested disaster recovery solutions in place. The assessment discovered that 44% of the agencies had no DR capability at all and that 56% of the covered agencies used shipped tapes as their primary mode to recover with a minimum recovery point objective (RPO) of 48 hours and recover time objective (RTO) of 96 hours.

With a mission to ensure the state's critical data and applications are preserved, the Agency for State Technology (AST) began development of a centralized disaster recovery program that would be available for any customers with critical systems hosted within the State Data Center (SDC), regardless of the technology employed. Following the recommendation from the independent assessment to use a contracted data center as a DR site, the DR platform began developing solutions with two major goals:

- Protect **ALL** SDC Managed Data
- Recover **ANY** Data Center Service offsite

To achieve the goal to protect all data, AST made a series of strategic purchases during regularly planned hardware refresh cycles. One such purchase involved the introduction of a lower cost object-based storage solution. By introducing a cost effective and scalable storage solution for unstructured data, capacity was freed from the traditional (and more expensive) block-based storage. The economics of the purchase allowed AST to include peer object-based storage as a replication target for the DR site, while staying in budget. From the savings realized from this change and some other strategic standardization, AST was also able to increase capacity in the primary data center with higher speed disks and deploy companions to both the production and DR sites. Leveraging native technologies inherent in the arrays, the stage was soon set for AST to replicate all data to the DR site, providing one of the key aspect to the DR puzzle. High compression and deduplication rates further allowed AST to configure the DR targets to maintain six weeks of snapshot changes on disk. Since implementation, ALL storage is replicated to the DR site within 24 hours for all customers.

The DR platform also began implementation of advanced DR solutions for all data center services offered in the AST SDC Service Catalog that could guarantee a minimum 2-hour RPO and 24-hour RTO for any customer. All networks were stretched from the SDC to the DR data center and a low latency, high capacity, encrypted, stretch layer 2 replication circuit was implemented. Core networking and load balancing capabilities were virtualized where possible to make a shift to DR more efficient and less expensive. Mainframe services were contracted through the DR partner to provide virtual tape replication and to provide equivalent mainframe processing power at the DR site. With almost 90% of compute being virtualized at the primary data center, virtualization replication and orchestration was implemented. Near synchronous database replication solutions were implemented for Oracle and Microsoft SQL. Storage Area Network (SAN) disk-based replication technologies were implemented to maintain non-virtual systems in sync. File services were offloaded to the object storage solution which

provide near-synchronous copies of file services' data and allowed for rapid fail-over and the implementation of self-service restores of object storage data.

Implementation of most solutions were realized through service-based contracts or by moving excess capacity to the 3rd party DR site. By using this model, AST was able to implement replication of all data and provide DR solutions for all services in the service catalog that could expand as the customer need demanded.

Concept

AST supports over 30 customers - primarily state agencies, but also cities, counties, municipalities, boards and commissions throughout Florida. Although the SDC is a state-of-the-art, certified Tier III data center and is built to sustain direct hurricane force winds, Florida is uniquely exposed to catastrophic storms that could put any service offered by the State of Florida at risk. Each agency has the responsibility to ensure continuity of mission critical applications provided to citizens. With frequency and magnitude of hurricanes increasing in recent years, state leadership funded an independent assessment to inventory and evaluate business continuity of applications for all agencies in the State of Florida. The results showed that many agencies had no disaster recovery capability and others relied upon outdated, sometimes untested recovery technologies that put business continuity at serious risk.

AST was then funded to provide IT DR for eight agencies with at risk critical applications. Though the focus of the funding was for specific applications, AST sought to develop a DR offering that could be easily expanded to be used by all SDC customers. AST partnered with a private data center to begin the implementation of a multi phased approach to accomplish two major goals:

- Replicate all customer data to the DR site within 24 hours, and
- Provide a DR offering with a minimum RPO of two hours and RTO of 24 hours that could scale to include any current or future SDC workload

A primary initial goal was to ensure that a replicated copy of all customer data existed at the DR site within 24-hours, regardless of individual agency funding level. Through the efficient use of funding to standardize the 10+ backup technologies inherited by AST during legislatively directed data center consolidation, AST deployed a backup solution that was capable of housing six weeks of daily data and eighteen months of disk-based backup sets, housed both at the SDC and the DR site. Since backups of virtual machines, which represent 90% of the SDC systems, can be "live" mounted in the backup system, this provides a near instant recovery of any system that is in a degraded state. By replicating all backup data managed in the SDC at the DR site, the base level of disaster recovery is a 24-hour RPO for all customers.

To maximize efficiency of block-based storage and backup retention, AST also implemented an object-based storage solution intended to offload one petabyte of unstructured file system data. Equivalent-sized peered object storage systems were deployed at the SDC and the DR site allowing for replication of object-based data to the DR site with an RPO of two hours. A feature of the object storage platform is to allow access to previous versions of any object directly through the file system allowing customers to self-recover any previous versions.

Disk based Virtual Tape Libraries (VTL) replaced tape based backup for the mainframe environment, which allows replication to the offsite location to occur as data is committed to disk. The completed

backups are asynchronously replicated to a like-sized VTL that also exists at the DR site. By using VTL technology, all customer mainframe data is replicated to the DR site in a matter of minutes.

To accommodate the volume of data being replicated, a 10 GB encrypted, low latency, layer 2 circuit was established between the SDC and the DR site. This combination of replication technologies ensure that all customer data can be recovered in the event of a disaster with a maximum RPO of 24 hours with the costs built into the SDC offered services.

To achieve the secondary goal, the AST Disaster Recovery Platform implemented DR solutions for every major service platform offered by the SDC in its Service Catalog. All services were designed to provide a minimum RTO of 24 hours.

To support network continuity, AST established a redundant backbone network capable of failing over all primary VLANs. A core network was established at the DR site and all networks that exist in the SDC were "stretched" to the DR site, which allows for instant failover of any VLAN. Virtual routing nodes were created for each customer capable of handling the network workload for each. Application load balancers and firewalls were virtualized and replicated for each customer. Virtualization of network resources accommodates an inexpensive methodology for both easy recovery in a declared event and provides inclusive network resources for isolated testing.

For mainframe parity, AST contracted for mainframe services to be provided for all mainframe DR customers. The service is sized to run the entire production mainframe workload currently housed in the primary SDC. The service uses the replicated VTL data to quickly restore systems and customer data.

The base level of compute and storage needed for the remainder of the services was accumulated using extra capacity created through a recent refresh of both compute and storage, and through a consolidation of two primary data centers into one. Capable of supporting approximately 1000 nodes and 2 petabytes of multi-tiered block storage, this previously capitalized footprint has very small operational cost. To accommodate attrition of these resources and future capacity needs, AST integrated vendor provided, on-demand private cloud storage and compute services.

To support the large virtualized environment, virtual replication and orchestration services were established between the primary SDC and the DR site. AST works with each DR customer to rationalize applications and understand dependencies and develop recovery plans that fit the need of the customer's critical applications. The recovery plans, which can be easily initiated during a declared event, can also be initiated and redirected to isolated networks for scheduled, isolated testing. The virtual platform at the DR site is also used for always-on secondary systems like DNS and directory services.

Customer applications with critical databases are protected with similar technologies for both Oracle and Microsoft SQL. Asynchronous DR nodes are established using vendor-provided database replication technologies. Oracle databases are replicated using Oracle DataGuard. Microsoft SQL databases use AlwaysOn Availability groups to replicate to the DR node. When the availability group is established, applications are redirected to a virtual database name. Applications can be easily redirected to the DR node by executing a single script. Both vendor technologies provide and RTO/RPO of minutes.

To ensure a successful execution of the various offerings, the AST Disaster Recovery team, in cooperation with each customer, maintains an IT Disaster Recovery plan that defines the applications

protected, the components by application, the DR solution used, the person authorized to declare, a declaration process, steps to recover each solution, a description of test processes, and estimated financial responsibility. Tests of each customers protected applications are conducted at least annually. Test reports are provided to each customer and IT DR plans are updated accordingly. Agencies can also schedule additional tests beyond the routinely scheduled exercise events without incurring additional costs.

Significance

Until recently in the State of Florida Disaster Recovery was non-comprehensive and did not meet the strategic needs of the agencies or citizens of Florida. Solutions selected by the individual Agencies varied in capabilities and ability to recover. Each solution was designed to recover only in-scope data, and were segmented from interoperability with other protected and non-protected systems. The effort to recover applications for testing was often more costly than maintaining the DR solution itself and required hundreds of planning hours. For this reason, many solutions went untested. With the implementation of the AST Disaster Recovery platform and solutions, Disaster Recovery was designed as a strategic initiative with a comprehensive and integrated approach that provide complete interoperability between solutions at the primary data center and the DR site. Testing is vastly simplified, the recovery environment is persistent and predictable, and the recovery of complex, inter-related legacy systems within RTO and RPO timelines guaranteed.

Since all data managed by the SDC is now replicated to the DR site within 24 hours using replicated backups, object storage or mainframe virtual tape replication on an encrypted 10GB layer 2 replication circuit, DR customers are now able to focus on advanced protection for truly mission critical applications. Comprehensive, interconnected network capabilities between solutions ensure interoperability of applications protected for each customer. Solutions have been designed with minimal data loss and recovery time in mind and now require far less planning and specialized capabilities for testing or execution.

Remarkably, even individual applications or components can be failed over and failed back while they continue to function without risk of connectivity to dependent systems. Advanced testing capabilities allow for both live failover and/or isolated testing of all protected resources. Once isolated testing on production systems is complete, some customer Agencies use the isolated copies to perform other testing that normally is not possible against production environments. Perhaps most importantly, complete DR testing is completed annually for each protected customer with a fraction of resources previously required.

Cost savings were realized by removing the requirements for staff to travel to perform DR exercises and by minimizing the staff impacts that previous exercise events required. Additional costs were avoided as the scope has expanded, evidenced by the fact that DR scope and capacity have grown significantly without requiring additional investments. AST has increased the number of critical applications covered by those initial eight agencies, and to date has expanded the services to six additional customers with capacity to onboard more.

Impact

Based on the 2013 independent application continuity assessment only two agencies successfully protected and tested all mission critical applications. Since its creation, the AST DR platform has successfully protected and tested mission critical applications for 14 agencies. In just two years, AST has gone from the originally funded eight agencies to 14 and continues to engage additional agencies without a current need for additional funding.

By creating a centralized and dedicated Disaster Recovery group within the organization, AST has drastically improved its capability for business continuity of mission critical applications. Transitioning from a cold DR site based on a static contract with multiple time restrictions, limitations, and declaration fees to one that is dedicated with predictable equipment in a validated and flexible environment represents a huge leap forward in disaster preparedness.

Through the development of DR solutions that fully compliment the service offerings within the SDC service catalog that can provide less than 2-hour RPO and less than one-day RTO, the AST DR platform now:

- Replicates nearly 3 terabytes (TB) of critical data to the DR site daily
- Provides business continuity for 298 critical applications not previously protected
- Provides plans, tests and reports for 14 agencies annually
- Continues to engage at-risk customers with no additional funding
- Continues to integrate public and private cloud technology into disaster recovery program

Time may be the key measurement in how well any business may recover in the event of disaster. AST's ability to provide this level of disaster recovery service is an effective solution that dramatically reduces the risk to the critical services offered to the citizens by the State of Florida.