CONTINUITY SOFTWARE

FORTUNE 1000 COMPANY ENSURES PRIVATE CLOUD RESILIENCE

THE CHALLENGE

THIS FORTUNE 1000 FINANCIAL SERVICES COMPANY ENCOUNTERED RESILIENCY CHALLENGES WHILE TRANSITIONING MISSION-CRITICAL SYSTEMS TO A VMWARE VIRTUALIZED PRIVATE CLOUD ENVIRONMENT.

Meeting Stability and Availability Expectations

Two years into the process, the team has realized that despite their efforts, stability and availability in the virtualized environment were not up to par with expectations.

Introducing New Technologies to the Environment

The IT team lacked the knowledge and tools to successfully implement all the newly-deployed technologies involved without introducing any
new vulnerabilities.

THE SOLUTION

Using Continuity Software's Cloud HealthCheck tool, the IT team received – within less than 24 hours – a detailed report pinpointing critical issues in multiple areas of their VMware infrastructure.

Following this quick success in detecting and fixing hidden issues, the IT team decided to implement Continuity Software's AvailabilityGuard as their entire IT infrastructure stack risk detection and resiliency assurance solution.

Proactive availability risk detection

Integration with ITSM & CMDB

BACKGROUND:

Transitioning to the Cloud

LIKE MOST ENTERPRISES TODAY, THIS FORTUNE 1000 COMPANY HAS BEEN IN THE PROCESS OF MIGRATING INCREASING PORTIONS OF ITS MISSION CRITICAL SYSTEMS FROM TRADITIONAL DATACENTERS TO A VIRTUALIZED PRIVATE CLOUD ENVIRONMENT. NOT UNLIKE OTHER LARGE ENTERPRISES, THE TECHNOLOGY OF CHOICE FOR THEIR VIRTUAL INFRASTRUCTURE WAS PROVIDED BY MARKET LEADER VMWARE.

TO ENSURE RESILIENCY IN THE NEWLY CREATED VIRTUAL ENVIRONMENT, THE IT INFRASTRUCTURE TEAM HAS BEEN IMPLEMENTING AN ACTIVE-ACTIVE CONFIGURATION – CONCURRENTLY RUNNING BUSINESS APPLICATIONS ON MULTIPLE AVAILABILITY ZONES. HOWEVER, ALMOST TWO YEARS INTO THE PROCESS, THE TEAM HAS REALIZED THAT DESPITE THEIR EFFORTS, STABILITY AND AVAILABILITY IN THE VIRTUALIZED ENVIRONMENT WERE NOT UP TO PAR WITH EXPECTATIONS.

CHALLENGES:

Ensuring Resiliency in the Virtualized Environment

Caught in the desire to quickly take advantage of all the benefits afforded by the virtual infrastructure, the IT team was struggling to build up the knowledge required to safely implement all the newly-deployed technologies while adjusting to the constantly evolving technology.

Some of the specific challenges encountered by the team included corrupted virtual machines (VMs), unexplained performance issues, as well as hundreds of VMs that wouldn't demonstrate following a server upgrade.

Faced by a stream of outages following migration of workloads to newly-defined hardware, the IT team found itself in a constant state of firefighting, reacting to one crisis after the other with no idea where the next issue was going to pop up. As new technologies such as VPLEX and vMSC were becoming available, they wanted to make sure these technologies could be deployed without introducing any new vulnerabilities to the cloud environment.

The need to create best practices and processes that would ensure safe migration to the virtualized environment became apparent to the team leaders.

THE SOLUTION:

AvailabilityGuard

The IT infrastructure team decided to engage with Continuity Software by using the Cloud Health Check tool. Within less than 24 hours, they received a detailed report pinpointing a number of critical issues in multiple areas of their VMware cloud infrastructure. In addition, the report provided suggestions that could be immediately put to action to fix these problems.

Following the success of this limited implementation, the IT team decided to standardize on Continuity Software's AvailabilityGuard as the tool of choice for risk detection and resiliency assurance for the company's IT infrastructure.
Reflecting on the decision, one of the IT leaders said:

> *"We could have attempted to script some of these checks ourselves but it wouldn't make sense. AvailabilityGuard already has over 6,000 scenarios documented, it would take us years to get to that level of coverage."*

CONTINUITY SOFTWARE

USING AVAILABILITYGUARD TO ENSURE IT RESILIENCE

AvailabilityGuard is used across all layers of the company's IT infrastructure and throughout all stages of IT system deployment and operations.

AvailabilityGuard is integrated with the company's Configuration Management Database (CMDB), ensuring that every system is automatically scanned for risk analysis as soon as it is added to the CMDB.

The validation process begins when a system is in pre-production, allowing the IT team to verify that all configuration is up to standards before the system goes into production mode. In addition, AvailabilityGuard allows the team to compare the configuration of pre-production servers to those that are already in production.

Any differences in configuration could spell potential problems, but those can now be addressed ahead of time thanks to AvailabilityGuard.

Once the system goes into production, scanning and analysis of data loss and availability risks is done on a daily basis. Any single-point-of-failure or deviation from vendor recommendations are immediately flagged and directed to the appropriate team for review and corrective action.

AvailabilityGuard is tightly integrated with ServiceNow, used by the IT organization as a company-wide incident management system. Each risk detected by AvailabilityGuard automatically generates a ticket in ServiceNow and routed to the relevant team, ensuring a closed-loop process that assigns the issue to right department or team member.

CONTINUITY SOFTWARE

ENSURING RESILIENCY IN THE VMWARE ENVIRONMENT

As additional systems are transitioned and rolled out to the VMware environment, AvailabilityGuard plays an integral role in the Physical-to-Virtual (P2V) transition process.

Even before the VMs are created, AvailabilityGuard scans the virtual infrastructure to ensure the cluster, network, and storage layers are configured correctly and in compliance with all vendor recommendations and company standards.

Once the VMs are provisioned, AvailabilityGuard verifies that the configuration is fully resilient – ensuring loads are distributed correctly between sites, that SAN IO configuration is optimized for performance, and that all HA-related configuration is correctly implemented, among others. Since the IT team also relies on VMware Site Recovery Manager (SRM) for recovery of tier-2 applications, AvailabilityGuard verifies the protected and recovery infrastructure is well aligned and that all recovery plans are correctly configured.

RESULTS

With AvailabilityGuard in place for over a year now, the IT team is seeing a noticeable improvement in productivity.

With fewer incidents and emergency drills to deal with, the team is able to deploy new technologies in about a third of the time it used to take prior to implementing AvailabilityGuard.

Management has better visibility and greater confidence in the stability of the private cloud, allowing the transition to the virtualized environment to move forward at an accelerated pace.

Most important, the IT team has been able to prevent several incidents in various areas of the IT infrastructure – and in particular in the private cloud environment – that would have likely resulted in downtime and service disruption if not addressed in time.