Buyer Case Study

El Al Uses Continuity Software's AvailabilityGuard to Proactively Identify Service Availability Risks

Dan Yachin
Sponsored by: Continuity Software

IDC OPINION

In the digital transformation era, data is the lifeblood of the business. The ability to capture and analyze huge amounts of historical and real-time data from multiple internal and external sources and in various content types for better and faster decision making has become paramount for business growth. As organizations of all sizes continue to embrace the digital enterprise and the always-on world in which they serve their customers, they are dependent on the constant availability of their IT systems to support revenue-generating, data-driven services. However, as IT environments continue to grow in scale and diversity with multiple interdependencies between systems, technologies, processes, and users, it is becoming increasingly difficult to proactively identify and prevent possible risks that may compromise the resiliency of critical systems. Whether due to human error, system failure, or ineffective (or lack of) redundancy, in complex IT environments more things can go wrong. Without proper visibility, organizations may only become aware of such risks after the fact.

El Al, Israel's national airline, was facing this kind of challenge. After embarking on large-scale digital transformation initiatives to improve operational efficiencies and increase productivity, the company had to maintain the continuous availability of critical business processes and operations while dealing with an IT environment that is highly heterogenous and complex. To ensure that the disaster recovery (DR) and high availability (HA) plan was working as intended, El Al deployed Continuity Software's AvailabilityGuard to validate the configuration of the production and DR environments, and proactively detect misconfigurations and potential risks.

IN THIS BUYER CASE STUDY

This IDC case study discusses the use of Continuity Software's AvailabilityGuard by commercial airline El Al. It analyzes the company's challenges in meeting DR and HA goals due to the growing complexity of its IT infrastructure, and how AvailabilityGuard was used to tackle them.

SITUATION OVERVIEW

El Al Organization Overview

Founded in 1948, El Al is the national airline of Israel. The company currently operates direct flights to 35 destinations around the world, carrying around 5.5 million passengers a year, with a team of 6,000 employees. In 2016, El Al recorded revenues amounting to nearly $2.04 billion.

As a large commercial airline, El Al operates a vast IT infrastructure with hundreds of servers in the company's datacenter and backup site supporting various business services, including multiple VMs in production and test environments. To maintain the high availability and business continuity of this infrastructure, El Al uses different data protection and recovery technologies. The

company's VMware servers and array-based virtualization software support an active-active storage topology and are replicated using EMC's VPLEX. UNIX systems and physical Windows servers are replicated to the company's backup site using continuous data protection (EMC's RecoverPoint) with recovery to predefined timeframes.

Challenges and Solution

Over the last few years, El Al has carried out a number of digital transformation projects, including the creation of new online business services and a digital workspace. In support of these initiatives, the company made significant investments to enhance its IT infrastructure, utilizing virtualization, cloud technologies, and mobile technologies, as well as management and security solutions.

One of the implications of the growing scale and diversity of El Al's IT environment was the difficulty in maintaining and validating its resiliency and DR readiness. To address this challenge, the company was looking for a solution with the ability to continuously scan the IT infrastructure to proactively detect misconfigurations and potential risks in its Continuous Availability strategy that may lead to downtime and data loss. Another key requirement was that the solution could continuously ensure that servers are fully and properly replicated and ready to be brought online from the backup site in the event of a primary site failure.

After reviewing different solutions, Continuity Software's AvailabilityGuard was chosen by El Al to provide end-to-end validation of the IT infrastructure configuration and ensure that the company's service availability and DR goals are consistently met. AvailabilityGuard is an IT operations analytics solution that performs cross-domain routine scans of IT infrastructure configurations, covering virtual machines, operating systems, hypervisors, physical servers, storage arrays, databases, and application servers, and calculates the dependencies and relationships between them. The configuration data is collected from the pre-production, production, and DR environments in a nonintrusive manner using read-only commands with no agents installed on systems. AvailabilityGuard analyzes the data against a knowledge base of thousands of gaps and vulnerabilities to detect configuration drifts and deviations from best practices and vendor recommendations. When potential data protection, availability, or DR risks are detected, a ticket containing the details regarding the severity of the problem and its business impact can be automatically issued to the appropriate team, along with a suggested resolution.

AvailabilityGuard was implemented by El Al to scan the IT environment, including VMware vCenter servers, physical servers, storage systems, operating systems, and databases. The product is currently being extended to provide complete monitoring of the entire primary and backup sites, covering a total storage capacity of around 0.5 petabyte in each site.

According to Galit Cohen, head of storage at El Al and system resilience optimization project leader: "AvailabilityGuard is used to perform daily scans of hundreds of servers supporting business-critical applications such as flight planning, crew placement, operational control center, cargo system, CRM applications, passenger information systems, billing, HR software, and IT infrastructure management software. In each scan, the product looks for misconfigurations and points of failure that may compromise the availability and stability of systems and services and lead to data loss. Identified risks and related details are presented on the system and reported to designated teams in time frames defined by El Al. In the following scan, AvailabilityGuard performs checks to ensure that the risk is mitigated. This closed tight feedback loop helps deploy new technologies much more quickly, with better results."

Results

AvailabilityGuard was successfully deployed across El Al's primary and backup sites. After completing the implementation, the company developed internal workflows for the handling of

alerts generated by AvailabilityGuard, streamlining the processes of reviewing, investigating, fixing, and reporting issues by designated technical teams. Based on these processes, El Al is now able to continually measure its readiness, utilizing dashboard views and data feeds provided by AvailabilityGuard to understand the risk posture at any given moment, and take proactive, corrective actions accordingly. In addition, AvailabilityGuard is used by El Al for measuring compliance with the company's predefined resiliency standards.

The successful implementation of AvailabilityGuard and the establishment of internal workflows enabled El Al to discover previously unknown service availability and DR risks, identify infrastructure optimization opportunities, and achieve operational improvements across various functional areas. Another key benefit gained from the use of AvailabilityGuard is the ability to automatically generate customized reports on various operational matters, including the mapping of server versions and updates, a comparison of updates between different systems or cluster members, and a listing of non-replicated LUNs on replicated servers.

ESSENTIAL GUIDANCE

Major international airlines have recently experienced significant outages due to large-scale computer system failures. Early in 2017, two of the largest U.S. flight carriers, United Airlines and Delta, suffered major IT problems that resulted in hundreds of flight delays and cancellations. Prior to that, in August 2016, Delta experienced an even larger outage that lasted for several days. A month earlier, a faulty router caused a system-wide outage at Southwest Airlines that led to the cancellation of 2,300 flights.

These recent outages illustrate the impact of downtime on organizations that are highly dependent on their IT infrastructure to conduct day-to-day operations. While the need to ensure continuous availability and access in the event of unplanned outages is a challenge for all businesses, it is particularly apparent in industries such as aviation, where computing systems have been in use for decades to streamline critical operations. Ensuring that older generations of computing systems can be seamlessly integrated with new technologies is therefore a major concern for companies in these industries — especially as many of them are currently engaging in digital transformation initiatives that introduce even more complexity into their IT environments, resulting in increased potential for IT outages.

Consistent with this, IDC's 2016 Enterprise Datacenter Survey found that the primary cause of unplanned downtime in respondents' datacenters was system failure. This represents a noticeable change from previous years, when human error was consistently the leading cause of unplanned downtime. IDC believes that the shift in primary causes of downtime is due to increased automation in the datacenter, with less need for human interference. To address this challenge, automation must also be applied to enterprises' data protection and recovery strategies to meet increasingly demanding objectives, such as shortening restore times to minutes rather than hours, and improving backup performance to reduce backup windows.

This case study shows that as IT environments become increasingly complex and heterogeneous, organizations should improve their testing processes and focus on measuring and continually improving IT resilience, and consider the use of automated solutions to proactively detect risks. Automated test tools can also contribute to cyber resilience, which represents an emerging risk-based approach to ensuring the ability of systems and organizations to survive and quickly recover from attacks and accidents, measured by the combination of mean time to failure and mean time to recovery. Built on the convergence of risk management, information security, business continuity, and other adjacent domains, cyber-resilience is gaining traction as a long-term strategy for preparing, preventing, and responding to disasters and other emergencies.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com
