Achieving Predictive Business Continuity

A proactive approach to infrastructure optimization and protection to mitigate the risk of business disruption

By Bennett Klein, Product Marketing Manager, Quest® Software

Smack in the middle of digital transformation, you're expected to deliver faster and better service to all departments. At the same time, you're trying to control IT budgets and avoid data loss and downtime despite the ever-increasing risk from unplanned outages, natural disasters and cybercriminals.

It's no surprise that almost two-thirds of technology professionals say maintaining current systems while simultaneously developing or incorporating new digital services is a major roadblock to digital transformation for them.[1] Business downtime puts companies at risk for both financial and reputational damage.

But what if you could remove the complexity and cost from your existing environment and unlock budget and staff time to fully embrace the digital transformation? What if you could automatically optimize and protect your systems, had complete insight into your hybrid IT environment and could proactively avoid problems before they happen?

A data protection strategy is good. A data protection strategy combined with a strategy for keeping IT infrastructure optimized is better.

Predictive business continuity is knowing your systems, applications and data are protected from unplanned system downtime and data loss, as well as ensuring your system resources are optimized to help mitigate the risk of system outages in the first place.

This paper explores that rare combination of infrastructure optimization and data protection. Beyond the scope of traditional business continuity (data protection, disaster recovery, system and application availability), readers will see the value in achieving predictive business continuity, which blends data protection with technology to manage, monitor and optimize IT infrastructure automatically. The result is lower risk of business disruption from system outages, data loss and disasters that administrators prepare for.

[1]Cited by Jake Hird, "101 Digital Transformation Statistics (2016)," TechValidate, 2016, https://image.slidesharecdn.com/digital-transformation-statistics-2016-160524053030/95/101-digital-transformation-statistics-2016-61-638.jpg

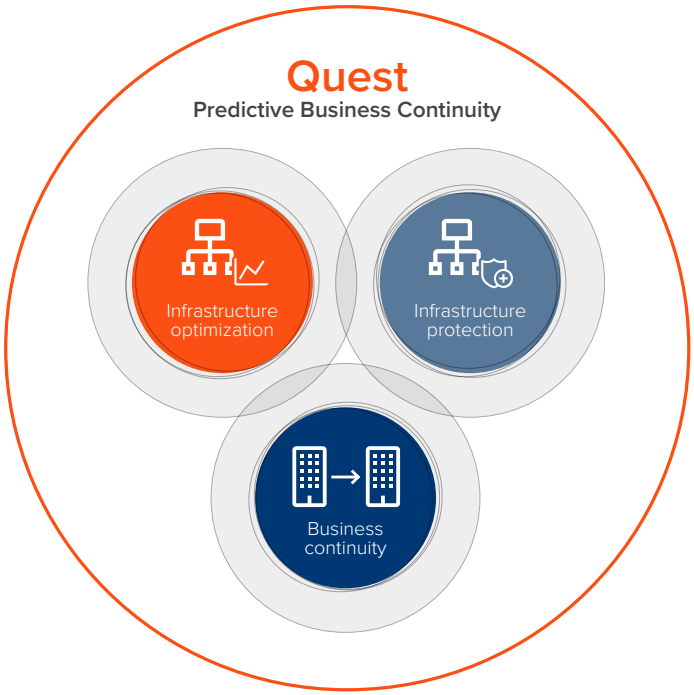

Figure 1: Predictive business continuity combines monitoring, management and optimization with protection and recovery

When something goes wrong and business is disrupted, IT is thrust into the spotlight to control damage to both finances and the company's reputation.

IT REALITIES ON THE PATH TO OPTIMIZING AND PROTECTING INFRASTRUCTURE

While IT executives want their department to become a true business enabler, the fact is that their staff rarely has the time or budget to deliver that vision. IT staff spend most of their resources managing the infrastructure. But the business demands that IT help support initiatives like digital transformation, and it just expects that systems and data are always available for customers and staff alike.

Typically, IT staff focus on their daily tasks, such as backup, network administration, hardware upgrades, software configuration, infrastructure expansion and user support; in other words, solving problems reactively. They dream about spending more time and resources on new technologies that enable business growth.

When something goes wrong and business is disrupted, disaster recovery and business continuity suddenly intersect. IT is thrust into the spotlight to control damage to both finances and the company's reputation.

IT organizations need a proactive approach that both optimizes the infrastructure and protects data, to mitigate the risk of business disruption. That is the essence of predictive business continuity.

Optimizing infrastructure

To help proactively avoid the most common IT issues and outages, systems need to be right-sized. Many organizations have built up complex infrastructure that makes IT management difficult. With the wide acceptance of virtualization, IT staff face uncontrolled sprawl of virtual machines (VMs); however, many VMs are over- or underutilized, wasting critical resources. Add cloud utilization to the mix and IT management can become daunting.

The goal of monitoring, managing and optimizing infrastructure is to ensure that available resources (CPU, memory, storage and network) are always on par with demand. That requirement applies regardless of the platform on which they reside (on-premises, remote, or cloud).

Overloaded systems are more prone to crash than stable, adequately managed systems. That applies regardless of platform—on-premises data center, private

cloud or public cloud. It also applies under ordinary circumstances, let alone in a disaster. Correctly allocating resources like memory, storage and compute (CPU) to meet business needs for performance and utilization is likely to reduce the risk of system downtime.

Also, since "optimizing" means "not too little and not too much," the other edge of the IT sword is to guard against over-provision as much as under-provision. Mitigating the risk of an outage should not be an exercise in building storage or memory far beyond foreseeable needs.

Both under-provisioning and over-provisioning affect OpEx and CapEx. There are measurable fixed and variable costs associated with new hardware and licenses for the hypervisors, operating systems and platform space for each VM, plus the software tools IT uses to monitor the environment.

By optimizing infrastructure, IT ensures that the environment is right-sized for the organization's workloads and that the risk of data loss due to an outage is minimal.

System and Data Protection

IT organizations face day-to-day disruptive events such as accidental data loss, deliberate cyberattacks and server, storage or application crashes. Beyond these mundane occurrences, IT organizations must have disaster recovery plans to address natural disasters, such as wildfires, floods, hurricanes, tornadoes, storms and earthquakes, that destroy IT assets or render them useless. Then come unplanned, man-made disasters like fires and power outages.

In fact, there are as many sources of internal disasters as of external ones. The role of IT is to protect the systems and data from all disasters as much as possible and then, when events overtake protection, to recover and get the business back to work as quickly as possible.

Finally, it is the role of IT to negotiate, set and adhere to service-level agreements (SLAs). Those include recovery point objectives (RPOs) and recovery time objectives (RTOs). System availability SLAs extend to outage duration and frequency, loss of productivity, and degradation of particularly sensitive services like email.

Industry statistics

Recent trends in IT provide the answers to several thorny questions about business continuity.

Regarding the role of business continuity in the organization, a survey of IT administrators in 180 global companies found increased focus on bringing teams outside of IT into the business continuity effort, climbing from two percent of respondents in 2017 to six percent in 2018. However, 13 percent of them believe they will lack the time for business continuity tasks in 2018, a jump from 2.5 percent in 2017.[2]

Another combination of surveys of over 5,500 IT professionals worldwide indicates that, in general, disaster recovery plans are weak. About half of the organizations surveyed had endured at least one failure requiring disaster recovery or high availability, with almost one third resulting in a day or more of downtime. Worse yet, more than four out of five respondents reported they did not have 100-percent confidence in their recovery plan, if they even had a plan.[3]

While the average cost of recovering from an outage jumped from about $500,000 in 2010 to more than $740,000 in 2016,[4] IT professionals are turning to cloud infrastructure as a cost-effective disaster recovery target worth spending money on.[5]

Thus, assuring the organization of business continuity is becoming a minefield. IT is unable to innovate fast enough to stay comfortably far ahead of disasters, OpEx and CapEx are rising, and the risk and cost of business disruption from disasters are increasing.

Which technologies can help IT navigate that minefield?

More than four out of five respondents reported they did not have 100-percent confidence in their recovery plan, if they even had a plan.

[2] "Business continuity trends and challenges, 2018," ContinuityCentral.com, January 3, 2018, http://www.continuitycentral.com/index.php/news/business-continuity-news/2563-business-continuity-trends-and-challenges-2018
[3] "2018 State of Resilience," Syncsort, January 10, 2018, http://www.syncsort.com/en/About/News-Center/Press-Release/Syncsort-State-of-Resilience-Report
[4] "Cost of Data Center Outages," Emerson Network Power/Ponemon Institute, January 2016, https://www.storagecraft.com/blog/wp-content/uploads/2016/06/2016-Cost-of-Data-Center-Outages-FINAL-2-1.pdf
[5] Bill Lundell, "2017 IT Spending Intentions Survey," cited in "Midyear Check-in on Data Protection Initiatives in 2017," Enterprise Strategy Group, July 17, 2017, http://www.esg-global.com/blog/midyear-check-in-on-data-protection-initiatives-in-2017

When overprovisioned resources are returned to the resource pool, IT can save on license fees, disk space, server utilization, administrative time, floor space and electricity costs.

TECHNOLOGIES FOR SUPPORTING PREDICTIVE BUSINESS CONTINUITY

The ideal tools for combining infrastructure optimization and data protection encompass the top features of both sets.

Infrastructure optimization — Monitoring, management and optimization

- **Measurement of performance and utilization** — Keeping physical and virtual infrastructure running smoothly requires finding and optimizing poorly performing user sessions quickly. It also requires promptly removing powered-off VMs, obsolete snapshots and zombie VMs to reduce waste in the resource budget.
- **System monitoring** — Processes that use resources (memory, storage and CPU) inefficiently can affect performance, so good tools set a baseline with thresholds and spot small bottlenecks before they become big ones. The best tools help predict where problems are likely to arise.
- **Optimization and management of resources** — When overprovisioned resources are returned to the resource pool, IT can save on license fees, disk space, server utilization administrative time, floor space and electricity costs. The right tool uses analysis and automation to take the guesswork out of capacity management and workload allocation.
- **Analytics** — What-if analysis helps administrators evaluate changes before they make them, and audit trails allow deep discovery of modifications and who made them. When paired with roll-back functions, analytics can go one step further by helping undo changes that lower performance.

Data protection

- **Backup and recovery** — Every product that protects data must be able to back up properly and recover quickly, as well as test and verify backup copies against the day when they are restored to original systems after an outage.
- **Hardware and software snapshots** — Frequent snapshots (as often as every five minutes) keep RPOs and RTOs as short as practical by capturing entire servers and applications in their most recent state.
- **Local and remote replication** — One copy of a backup makes for safety; multiple copies make for security. The best tools allow replication to both local and remote/cloud hosts.
- **Live recovery and bare-metal recovery** — Live recovery processes resume physical/virtual machines directly from backup to get users up and working within minutes after an outage. Bare-metal recovery (BMR) restores the full software configuration for a specific system by reformatting the hard drive and restoring its contents.
- **Public and private cloud** — Three use cases apply. Cloud archive is low-cost, long-term storage to comply with requirements for data retention. Disaster recovery as a service (DRaaS) features off-site replication for secure storage and recovery. Software as a service (SaaS) is the execution of business applications on virtual servers in the cloud.
- **Backup-related software-defined storage (SDS)** — These products help virtualize the backup target storage pool. Advanced features often include direct-to-disk backup, deduplication, compression and wide support for backup protocols. Results are faster performance, improved scalability and lower storage costs.

For mission-critical systems, applications and data, there are a number of more costly technologies such as continuous data protection (CDP), mirrored/duplexed systems and high-availability software with synchronous replication and failover.

PREDICTIVE BUSINESS CONTINUITY – COMBINING MONITORING, MANAGEMENT, OPTIMIZATION AND DATA PROTECTION

The problem is that generally, the vendors of infrastructure monitoring products don't offer solid data protection and, conversely, data protection vendors don't offer robust features for infrastructure management, monitoring and optimization. Obtaining a solution that integrates both is the holy grail.

Truly predictive business continuity solutions give IT what it needs to work proactively rather than reactively. Even across hybrid environments with multiple hypervisors, all infrastructure is visible for full backup and disaster recovery. Automation detects and protects new VMs in growing virtual environments, then balances workloads across resources.

On the operational level, predictive business continuity includes applying snapshot technology to eliminate backup

windows and connecting to public clouds for archiving, backup, replication and failover. Deduplication, compression and WAN acceleration reduce the burden on the network. When data protection is nearly continuous and recovery is almost instantaneous, IT can be confident in the high probability of system and data recovery and the low risk of data loss and business downtime.

The solution also allows IT to work predictively and keep costs low by identifying underutilized resources and modeling planned changes. Data on performance trends contributes to forecasts of future costs, facilitates decisions about migrating to the cloud and highlights potential issues in the virtual environment before they become problems.

When IT staff can see where to reclaim underused resources and maximize the performance of existing systems, they can estimate costs more accurately. And when they can anticipate bottlenecks and outages before they happen, they can take steps to maximize system uptime and availability.

When infrastructure monitoring and data protection combine in a single solution, the result is predictive business continuity: complete insight into the IT environment, with automatic optimization and protection to mitigate the risk of system downtime and data loss.

Results

The potential benefits from implementing predictive business continuity include many of IT's most keenly pursued objectives.

First, infrastructure optimization improves IT's ability to mitigate risk and respond with improved backup and restore speeds. The entire business benefits from backup windows and recovery times that are shortened from dozens of hours to dozens of minutes. Then, accurate forecasting of resource requirements leads to thousands of dollars in reduced CapEx and OpEx through reclaimed, underutilized resources and lower storage costs. Finally, when the environment is both right-sized and protected, productivity increases. Users enjoy improved availability of their applications and IT reduces administration time so it can focus on strategic contributions to the business.

CONCLUSION

Optimizing infrastructure and protecting data are two of IT's biggest contributions to business continuity in any company. When IT organizations can automate processes and remove complexity from the environment, they free up staff time for innovation.

IT organizations offer more value to the business when they plan for predictive business continuity: the combination of infrastructure optimization and data protection. Predictive business continuity includes not only the ability to recover from business disruptions, whether due to man-made, accidental or natural disasters, but also the foresight to avoid resource shortages (CPU, memory, storage and network) and mitigate the risk of business disruption.

Once on the path to predictive business continuity, IT teams can free up staff time and budget for innovation like digital transformation, reduce their CapEx and OpEx, accurately predict future costs and prevent problems before they arise.

Visit Quest.com for more information about disaster recovery and predictive business continuity.

IT organizations offer more value to the business when they plan for predictive business continuity.

ABOUT THE AUTHOR

Bennett Klein has more than 20 years' software, SaaS and Cloud product marketing experience, including 12 years focused on storage and data protection. He has worked for fast-paced, global software companies with direct and indirect sales channels.

ABOUT QUEST

At Quest, our purpose is to solve complex problems with simple solutions. We accomplish this with a philosophy focused on great products, great service and an overall goal of being simple to do business with. Our vision is to deliver technology that eliminates the need to choose between efficiency and effectiveness, which means you and your organization can spend less time on IT administration and more time on business innovation.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (www.quest.com) for regional and international office information.