the Availability Digest

www.availabilitydigest.com
@availabilitydig

A Look at Today's Data Center Availability

July 2015

Organizations face increasing demands for "always on" availability. How are they faring? A 2014 survey[1] by Veeam Software (http://www.veeam.com/), a provider of data center availability products, explores this topic.

The survey, performed in conjunction with Vanson Bourne, an independent market research organization, is based on interviews with 760 senior IT decision makers in ten countries. The interviewees represent companies in retail, distribution, transportation, manufacturing, financial services, and business and professional services, among others.

The survey concludes that the system and data-availability requirements for companies is ever-tightening, and that companies are struggling to keep up.

Modernizing the Data Center

IT has grown strategic for every organization, and the requirements for IT become more demanding every year. Services must be provisioned faster, security must be strengthened, and the availability of system services and the data they provide must be improved, all at reduced costs.

Currently, 81% of all companies surveyed have recently upgraded their data centers or are in the process of doing so; and 16% are planning to do so in the next two years. The primary reason for the upgrades is to reduce costs. Running a close second is the need for greater availability.

Technologies upon which companies are focused include (in order):

- Server virtualization
- Storage upgrades
- Operating system upgrades
- Data protection and disaster recovery
- Network virtualization
- Virtual desktop infrastructure
- Consolidating data centers
- Private clouds
- Public cloud Infrastructure as a Service (IaaS)
- Adding new data centers
- Public cloud Software as a Service (SaaS)
- Public cloud Disaster Recovery as a Service (DRaaS)

[1] Veeam Data Center Availability Report 2014: The Challenge of the Always-On Business.

The Increasing Availability Requirements

The demand for higher availability is being driven by several factors:

- Workers no longer bound by an 8-hour working day
- Globalization requiring businesses to operate across multiple time zones
- Customers conducting business online anytime, anywhere via their mobile devices
- Supply chain and logistics integration requiring constant access to systems and data
- The rise of the Internet of Things (IoT) with devices permanently connected and monitored

Over 90% of companies are increasing their requirements for minimizing downtime and for data access.

The Availability Gap

Even with their extensive investments in data-center modernization, companies have been unable to keep up with the increases in their SLA requirements for RTO (Recovery Time Objective) and RPO (Recovery Point Objective). This is especially true for mission-critical applications. Currently, about half of all applications are considered mission-critical.

With respect to RTO, mission-critical applications currently take an average of 2.9 hours to recover, while non-mission-critical applications require an average recovery time of 8.5 hours. These recovery times compare to average SLAs of 2.7 hours and 10.0 hours, respectively.

RPO is a function of how frequently backups are taken. Following a system failure, it is possible for all data since the last backup to be lost. Backups for mission-critical systems are taken every 4.8 hours on the average. The average backup time for non-mission-critical applications is 14.5 hours. These compare to average SLAs of 3.5 hours and 11.5 hours, respectively.

Even though compliance with respect to some SLAs is close, SLAs are getting tighter; but the technology is not changing. Some countries (Italy, Switzerland, the U.K.) are missing the RTO mark by more than a factor of 2:1. Likewise, other countries (Germany, Switzerland, Singapore) are missing the RPO mark by a similar factor.

The Financial Cost of Downtime

On the average, organizations encounter unplanned downtime in some application or another thirteen times per year. The average cost of downtime for mission-critical applications approximates USD $83,000 per hour and for non-mission-critical applications about USD $44,000 per hour.

In addition to the cost of downtime is the cost of lost data. The average cost for an hour of lost mission-critical data is about USD $71,000. For non-mission-critical data, the cost is comparable to USD $42,000. Based on the average backup intervals, a single incident can cost an organization about USD $341,000 for mission-critical data and USD $608,000 for non-mission-critical data.

Adding the costs of downtime and lost data, a single incident can cost an organization about USD $451,000 for a mission-critical system outage and close to USD $782,000 for non-mission-critical system outage. At an average of 13 incidents per year, enterprises face an average annual cost in excess of USD $10,000,000.

If RTO and RPO could be reduced to 15 minutes or less, total annual costs due to system outages could be reduced to about USD $500,000. This demonstrates the advantage of active/active systems,[2] which can have recovery times measured in seconds.

It is interesting to note that the cost of system failures due to non-mission-critical systems may be more than the cost of system failures due to mission-critical systems.

Availability Solutions and Capabilities

The inability to achieve an organization's availability goals comes down to the legacy backup solutions: without sufficient capabilities, IT departments cannot achieve the RTO and RPO SLAs that the business demands. These capabilities include:

- High-speed recovery (less than 15 minutes)
- Data-loss avoidance (less than 15 minutes)
- Verified protection (guaranteed recovery of every file and every application every time)

The primary reason why organizations cannot implement these capabilities is the cost of the new technology followed by a lack of expertise and the inability of their current products to provide these functions.

Data Backup Failures

When a backup is made, there is always a chance that it is damaged and will not recover. Organizations should therefore test their backups to ensure that they can be used effectively for data recovery. However, this is a time-consuming task; and only a fraction of backups are tested.

On average, organizations test only 5.3% of their backups every quarter. Thus, the majority of backups are not tested and can fail. The result is that approximately 16.7% of backups fail. With an unplanned downtime occurring 13 times per year, this means that there typically will be two backup failures per year, greatly increasing the cost of downtime.

Patches and application upgrades should also be thoroughly tested before they are put into production. 87% of the companies surveyed reported that they experienced more downtime than expected when they performed application patches or upgrades.

Looking Ahead

Organizations are well aware of their increasing needs to deliver improved availability for their IT services. 78% of the companies plan to change their data-protection products in the next two year.

Summary

IT departments need to be certain that recovery time is as short as possible, that data loss is minimized, and that backups will recover as expected.

Some of the statistics determined from this study can be very useful in determining where your company stands with respect to availability:

	Average Recovery Time	Average Backup Time
Mission Critical	2.9 hours	4.8 hours
Non-Mission Critical	8.5 hours	14.5 hours

[2] What Is Active/Active?, *Availability Digest*; October 2006.
http://www.availabilitydigest.com/public_articles/0101/what_is_active-active.pdf

	Average Cost of Downtime	Average Cost of Lost Data
Mission Critical	$83,000	$71,000
Non-Mission Critical	$44,000	$42,000

Average downtime incidents per year = 13

Recovery Failures per Year = 2

Acknowledgement

Our thanks to our subscriber Terry Critchley for pointing us to this topic.