Extended journaling

Getting the most out of your recovery point objective and disaster recovery test

ABSTRACT: (insert)

Table of contents

Introduction

As AI, IoT and billions of mobile devices become more complex, so too does the job of protecting your data and infrastructure. Gone are the days when simple backups sufficed; these backups are slow and labor-intensive by today's standards. Instead, companies rely on more dynamic solutions, like disaster-recovery-as-a-service (DRaaS). But what happens when a basic DRaaS solution falls short?

While malware, breaches, phishing and other cyberattacks have been on the rise for years, the dramatic explosion in ransomware attacks is shaking the IT security landscape. Recent research by Cybersecurity Ventures predicts that ransomware attacks on businesses will occur every 14 seconds by the end of 2019, and every 11 seconds by 2021. This statistic is particularly alarming given ransomware's ability to quietly encrypt data, potentially undetected, for days. This drastic rise in attacks highlights the vulnerability of companies whose recovery windows are limited to mere hours; this failback period may not be enough to restore files and minimize data loss associated with a well-concealed ransomware attack.

This looming threats presents a disturbing scenario and liability for any business and begs the question, *How can a business ensure the rapid and accurate recovery of its files without extensive data loss*? A DRaaS solution that replicates days' worth of data, rather than hours, is a powerful first step.

<insert below text as a sidebar>

Ransomware attacks on businesses will occur every 11 seconds by the end of 2021.Cybersecurity Ventures

The threats in our midst

It's well-storied that data is the lifeblood of most businesses, but with the growing threats of malware, phishing, human error and natural disasters, How can a business ensure business continuity?

While perpetual data protection is an integral part of the solutions, the period of time for which the data is retained is perhaps the greatest driver of outcomes. Data is commonly retained for a period of hours. While this may be a wide enough span for a "run-of-the-mill" power outage that is immediately identified, there are an increasing number of situations in which rolling back for more than a few hours is necessary to recover operations.

Consider, for example, the company that chooses not to monitor its IT environment outside of regular business hours. The IT staff could leave at the end of the day only to return the next morning to an outage that occurred overnight, leaving the company with eight or more hours of lost data. Will the company have a replication history long enough to restore the environment and minimize the amount of lost data? Probably not.

An even more concerning situation involves malware — in particular, ransomware. Ransomware's ability to quietly encrypt data for days leaves businesses in a vulnerable position: either pay the ransom or lose the data. Often, even when the ransom is paid, the data is never returned — truly, a lose-lose situation. Ransomware is a scenario in which a backup window of hours vs. days is insufficient.

To better protect data and optimize business continuity in the face of a man-made or natural disaster, businesses must retain data for a long enough period of time that they can return to the replication point just before the incident occurred. To achieve this, businesses need to consider failback in terms of days, not mere hours.

<insert below text as a sidebar>

Businesses need to consider failback in terms of days, not mere hours.

Today more than ever, businesses demand value from a DRaaS solution. This means having a flexible failback window that can roll back days to maximize not only recovery capabilities, but also the testing environment. Being limited to hours of recovered data makes a company extremely susceptible to data loss.

U.S. businesses and consumers have historically been more prone to ransomware attacks than other countries based on willingness to pay the demanded ransom. According to TechRepublic, some 45% of US companies hit with ransomware last year

paid at least one ransom, according to the report. However, only 26% of those actually had their files unlocked afterwards. Further, organizations that paid the ransom were targeted and attacked again 73% of the time.

The most vulnerable targets include companies with a high cost of downtime, a high risk of incidents, or high-stakes compliance requirements. The financial and healthcare industries fall right into this mix. With extensive regulations dictating both the security and management of their data, these industries face steep fines and perilous business consequences for being ill-prepared to handle threats to applications availability.

Not surprisingly, a company's ability to retrieve an extended log of data can boost its confidence; in fact, companies with stronger disaster recovery capabilities are less likely to pay a ransom for their data. Having the ability to effectively restore their files with minimal data loss renders the ransom threat null and void.

The benefits of a failback of days vs. hours go beyond recovery; a longer failback period enables companies to conduct longer, more interactive and complete testing to be conducted. A sandbox environment that has a more enduring period of time enables an organization to implement better testing through testing patches, to test-drive enhancements and gain greater insight into the performance of their disaster recovery environments —all without impacting the production environment.

Given the growing number and forms of potentially business-crippling events in today's data landscape, how can your organization protect its data and business continuity? The answer is found in extended journaling.

Extended journaling

Extended journaling is a feature of the Flexential DRaaS solution, the *Recovery Cloud.* Recovery Cloud is offered in three tiers — Essentials, Prime and Premium — to provide customers with scalable, *tailored* disaster recovery programs that ensure rapid recovery of mission-critical applications and minimal data loss in the event of a failure. Designed to offer optimum flexibility, the Flexential Prime and Premium tiers deliver up to 30 days of data replication history to protect critical assets, while the Essentials tier provides for 14 days of replication. Backed by the redundancy of the company's geographically diverse data center locations and the resiliency of Flexential interconnection services, extended journaling enables a company to protect its data, enrich its testing capabilities and improve its overall level of preparedness.

By delivering a deeper retention period, extended journaling improves continuous data protection and offers greater flexibility in recovering business applications to a specific period of time.

<insert below text as a sidebar>

Extended journaling enables a company to protect its data, enrich its testing capabilities and improve its overall level of preparedness.

Up to 30 days of data replication history

Flexential extended journaling offers up to 30 days of replication history, enabling the cost-effective recovery and testing of servers protected in the Recovery Cloud. With multiple checkpoints every hour, the service offers thousands of recovery points to deliver a granular level of restoration and enable a business to pinpoint precisely the recovery point – and effectively balance the need to restore the data against the amount of data that will be lost.

Extended journaling enables this level of data protection by allowing a customer to choose the default journal length that best suits its unique needs. Regardless of the length of the journal setting, customers receive an unlimited journal size for every virtual machine within a virtual protection group. Further, the length of this journaling history does not impede recovery speed, which allows businesses to maintain their expected RTOs for each virtual protection group.

Self-service for ease of use and ultimate flexibility

Designed as an easy-to-use, self-service product with intense flexibility, extended journaling offers customers real-time visibility into their DRaaS environments. Individual virtual protection groups can be easily monitored and managed through the customer portal, which provides direct access to the operations driving the replication process.

<insert graphic>

The Flexential customer portal has a user-friendly dashboard that allows the customer to manipulate its settings for greater control over its DR environment. Using the self-service dashboard, a business can monitor the status of:

- the Recovery Cloud
- the total amount of recovery data in its DR environment
- the recovery and test history of its virtual protection groups

This level of autonomy puts control of a customer's virtual protection group solution directly into its own hands.

For further flexibility, virtual machines can be managed with an interface tool to tune the journaling length of each or all virtual machines to meet current and evolving needs. This failback window can also be set across all virtual protection groups or individually for each virtual protection group protected in the Recovery Cloud to support any disaster recovery or testing need, offering optimized financial spend, efficiency and application rollback.

While extended journaling is designed to be self-service, Flexential still delivers the resources and expertise across other DRaaS functions to ensure successful implementation and declaration. From our consultative approach to feedback loops to assisted disaster declarations, we provide more than just a technology solution. And Flexential experts are available to customers 24/7/365 to ensure they get the most out of their disaster recovery and testing plans.

Addressing a broader spectrum of disaster conditions

Threats are an unfortunate, inevitable part of business. How you prepare for and handle them makes all the difference when it comes successful business continuity and compliance.

<insert below text as a sidebar>

50% of a surveyed 582 cybersecurity professionals do not believe their organization is prepared to repel a ransomware attack.

According to a report published by Ponemon Institute, 66% of survey respondents view the threat of a ransomware attack as very serious while only 13% rate their companies' preparedness to prevent ransomware as high. This means companies need a reliable solution to restore data compromised by ransomware or any other disruptive event.

Given the security and redundancy built into the Flexential Recovery Cloud, supplementing your DRaaS solution with extended journaling is an excellent step toward protecting your business data. Extended journaling pushes competences further to decrease the potential for significant data exposure. Its 30-day replication journal can effectively and confidently handle the threat of corrupted or lost data associated with any form of malware, cyberattacks, outages and good old-fashioned natural disasters.

More complete testing for improved performance

An extended replication window offers tremendous testing benefits. When testing is limited to a set number of hours, businesses will likely only have time to handle their most compulsory needs, leaving other initiatives underutilized or untouched.

Testing within a less restrictive environment enables more complete, interactive testing, allowing end users to be more involved in the testing process. With the ability to conduct more business-enabling analyses, companies can:

- assess new features and applications
- better understand their capabilities during and after a disaster
- conduct any other strategic initiatives without disrupting the production environment

This improved testing environment increases the level of preparedness to drive even greater value from the disaster recovery solution.

Flexential also offers on-demand, self-service DR testing through our secure portal. Self-service testing allows organizations to get immediate feedback on the health of their disaster recovery plans without impacting production, and extended journaling gives customers the option to self-test for up to 48 hours.

Conclusion

As threats continue to evolve, businesses must keep pace with the services and capabilities that protect their workloads and enhance their operations. A DRaaS solution that delivers day of replication – not just hours – empowers today's businesses to get the most from their recovery solutions. An extended replication history of days vs. hours arms companies with the confidence that they can recover from a disaster with minimal data loss. Further, an extended replication window provides a more comprehensive testing environment that drives both business direction and acumen.

(Note: Format bibliography per AP)

REFERENCES: USE AP STYLE
https://owl.purdue.edu/owl/research_and_citation/apa_style/apa_formatting_and_style_guide/in_text_citations_the_basics.html

- Cybersecurity Ventures -
- https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

- nearly 40 percent of ransomware victims pay the ransom.
- https://go.malwarebytes.com/OstermanRansomwareSurvey.html

- https://www.techrepublic.com/article/only-26-of-us-companies-that-paid-ransomware-attackers-had-files-unlocked/
- % of companies that paid the ransomware vs. how many got their data back.

- Ponemon – Jan. 2017
- https://www.ponemon.org/local/upload/file/Ransomware%20Report%20Final%201.pdf