FUTUREWEI
Technologies

Whitepaper

Data Backup Rules

Enter the Era Beyond Conventional Rules

Trademarks and Permissions

Notice

The purchased products, services, and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services, and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees, or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

FUTUREWEI® TECHNOLOGIES, INC.

Boston Research Center

Address: 111 Speen Street, Suite 114
Framingham, MA 01701
United States of America

Website: http://www.futurewei.com/

Table Of Contents

Executive Summary

- Ensuring secure data backups is a critical responsibility for IT professionals, as they must safeguard their company's information from loss or corruption by maintaining a secure data center infrastructure.

- Experts commonly recommended the 3-2-1 strategy for data loss prevention. However, due to the escalating threat of ransomware attacks, businesses increasingly favor backup rules such as 4-3-2, 3-2-1-1-1, and 3-2-1-1-0 for enhanced protection against data breaches.

- Neglecting backup frequency and speed is simply not viable in today's digital landscape. Therefore, the current backup rule, 3-2-1-1-0 need to be enhanced to **3-2-1-1-0-x-c** to adapt to the evolving data security paradigm and ensure robust protection measures.

Introduction

Data backup is an essential practice involving the replication of system, configuration, or application data, stored separately from the original source. It serves as a safeguard against various unforeseen events, such as natural disasters, human errors, security breaches, or system malfunctions, which could lead to either partial or complete data loss. By maintaining backups, organizations mitigate the risks associated with such incidents, ensuring the capability to restore systems and applications to predefined states.

Although organizations aspire for seamless system functionality, the reality is that individual components can malfunction, and in rare cases, entire systems may fail. Data backup encompasses the infrastructure, technologies, and procedures designed to duplicate organizational data, facilitating restoration in the event of failures. This includes comprehensive disaster recovery plans, alongside tailored backup strategies and solutions.

As data volumes grow and cyber threats evolve, effective backup planning has become indispensable for organizations of all sizes. The proliferation of remote work, coupled with stringent compliance frameworks, underscores the importance of regular and reliable backups, posing a significant challenge for cybersecurity practitioners.

This paper aims to explore prevalent backup protocols within the industry and advocate for their enhancement to counter ransomware threats and bolster data protection in contemporary times. By delving into modern backup strategies, we seek to address evolving cybersecurity challenges and promote proactive measures for safeguarding organizational data integrity.

What makes up the Backup Rule?

In contemporary digital age, safeguarding data is paramount, with backup rules serving as a critical component. Thus, the metrics comprising backup rules must possess sound reasoning and deliver tangible value. IT budgets form a significant portion of operational expenses, prompting organizations to seek optimization strategies. Consequently, organizations adopt various backup approaches tailored to their specific needs and capabilities, aligning with their contributions to IT budget management. By ensuring that backup strategies are not only effective but also cost-efficient, organizations can strike a balance between safeguarding their data and optimizing their financial resources. This synergy between data protection and budgetary considerations underscores the importance of implementing backup rules that are both rational and economically viable in today's dynamic digital landscape.

Here are the key considerations that are used to make up today’s backup rule.

Number Of

Data Copies

To start, having multiple copies of any data is the foundation of this strategy This number indicates the existence of three copies of your data. You should have three separate copies of your data stored in different locations to ensure redundancy and resilience against data loss. This redundancy helps protect against various scenarios such as hardware failures, data corruption, or accidental deletions.

Type Of
Media

The number two stands for two different types of media used for backups. It suggests diversifying the backup storage media to reduce the risk of data loss due to a single type of failure. For instance, one might use a combination of HDD, SSD , NVMe, tapes, or cloud storage for the backups.

Number Of
Offsite copy

This number signifies that at least one copy of your data should be stored off-site or off-network. Storing a backup off-site provides protection against disasters that might affect the primary location, such as fire, flood, or theft. It ensures that even if the primary site is compromised, one can still recover the data from a separate location.

Number Of
Offline Copy

This represents having number of copies of the data in a format that is not directly accessible. This could mean storing backups in an offline or immutable format, such as write-once optical disks or tape archives. This provides an extra layer of protection against ransomware attacks or accidental deletions because the backups cannot be altered or deleted easily.

Number Of
Errors

This implies number of errors or failures in the backup and recovery process. While achieving perfection might be aspirational, it emphasizes the importance of regularly testing and validating your backup systems and processes to ensure they are functioning correctly. Regular testing helps identify and rectify any issues before they become critical during a real data loss event.

Number Of

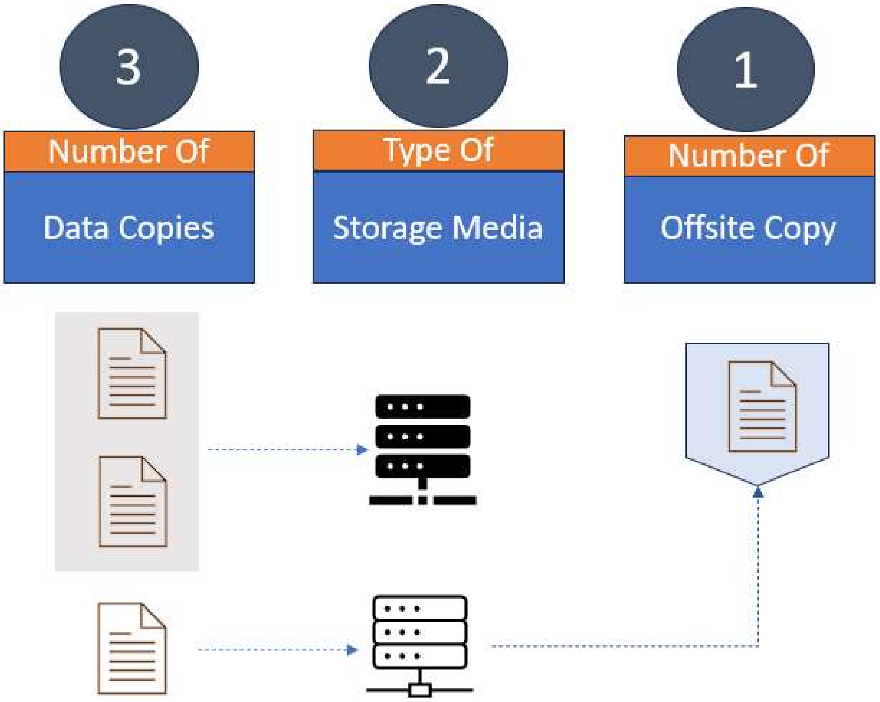
Location

This represents having separate copies of the data stored in different locations. Storing copies of data in different locations helps protect against various scenarios such as disasters (e.g., fire, flood), theft, or localized infrastructure failures. It ensures that even if one location is compromised, one can still recover the data from another location.

Most Common Backup Rules

3-2-1 Backup Rule

The 3-2-1 backup rule, was long hailed as a cornerstone of data protection strategies, faced challenges in the modern landscape, particularly for small and medium businesses reliant on SaaS solutions. Technological advancements, burgeoning data volumes, and evolving cyber threats necessitate a critical examination of its efficacy. A lot of limitations became apparent.

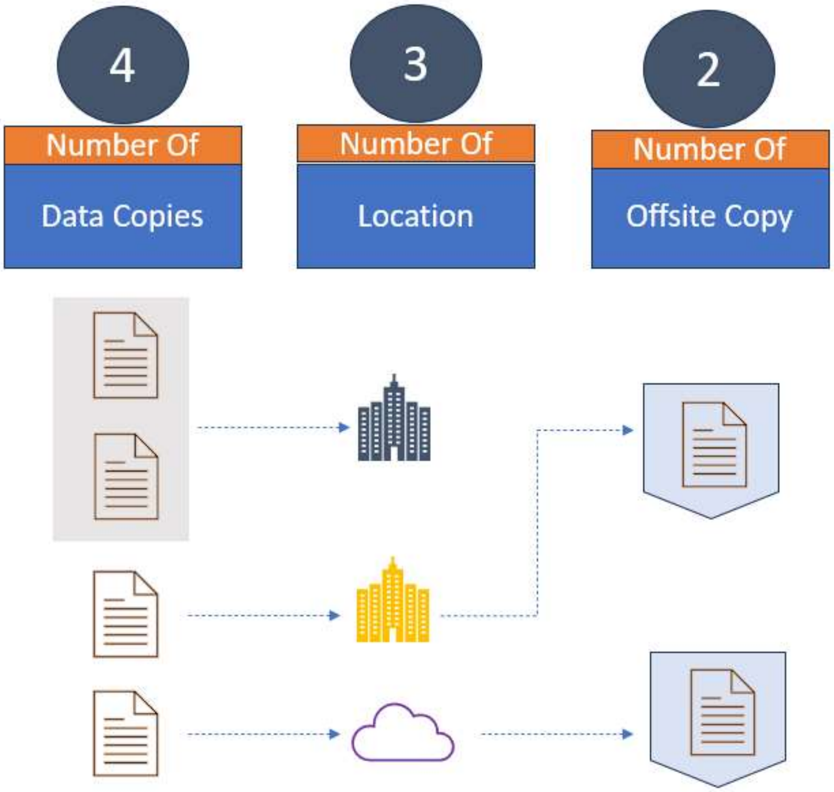


Firstly, the exponential data growth surpasses the rule's capability to safeguard information adequately with only three copies. Secondly, the proliferation of devices complicates comprehensive backup coverage across diverse platforms. Moreover, the escalating sophistication of cyber threats, notably ransomware, presented a formidable challenge to data integrity, surpassing the rule's capabilities alone.

Furthermore, the escalating costs of data loss, including financial, reputational, and legal ramifications, emphasize the necessity for robust data protection measures that align with Recovery Point Objective and Recovery Time Objective metrics. Consequently, businesses had to explore more nuanced and adaptive backup strategies to mitigate risks effectively in today's dynamic digital landscape.

4-3-2 Backup Rule

The 4-3-2 backup strategy, akin to the 3-2-1 backup rule, was crafted to ensure data redundancy and resilience against potential loss. However, a key distinction lied in the 4-3-2's provision of an additional data copy and designated storage location. Here, organizations uphold four data copies dispersed across three distinct locations, with two copies stored off-site.



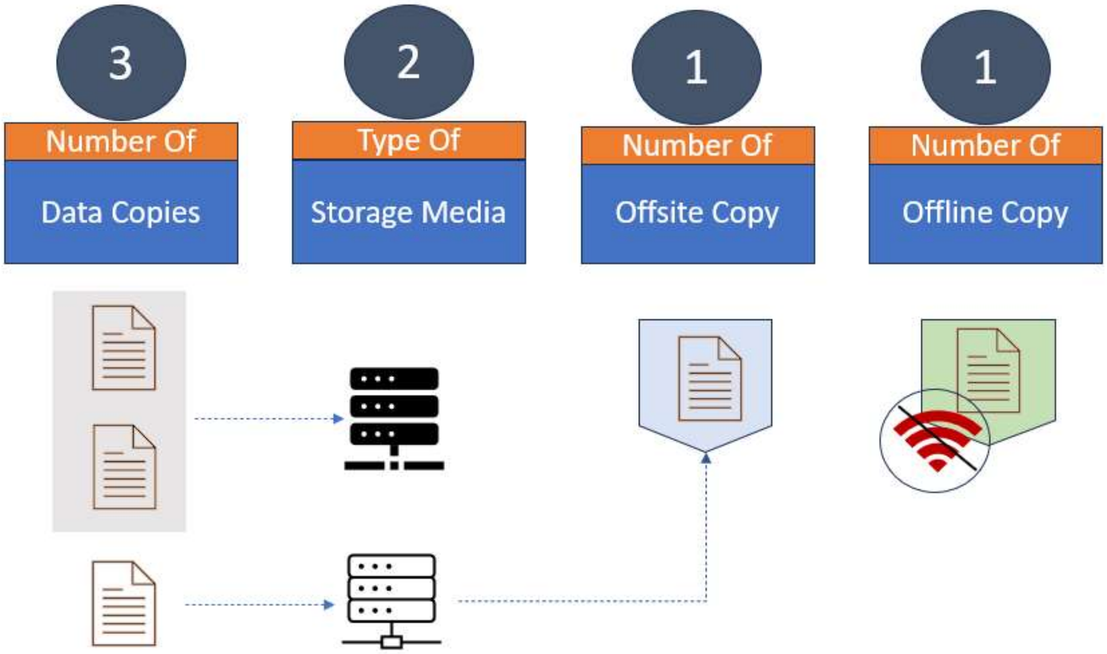
Yet, the 4-3-2 rule exhibits notable limitations. It lacks specifications regarding the use of varied storage media, which is crucial for mitigating data loss risks associated with specific storage technologies. Furthermore, while advocating for two off-site data copies, it overlooks the critical emphasis on off-site backups' importance in shielding against calamities such as fires or theft.

Moreover, the rule fails to address the necessity for immutable or offline backups, crucial for combatting ransomware attacks and accidental deletions. Immutable backups, impervious to alterations or deletions, offer an additional layer of safeguarding against data loss.

Lastly, the rule's focus on data replication neglects adequate prioritization of testing and validation procedures. Regular testing ensures backup viability and successful restoration when required, an aspect pivotal in a robust data protection strategy. Thus, while the 4-3-2 rule offers a foundation for data resilience, addressing these limitations is imperative for comprehensive protection against contemporary threats.

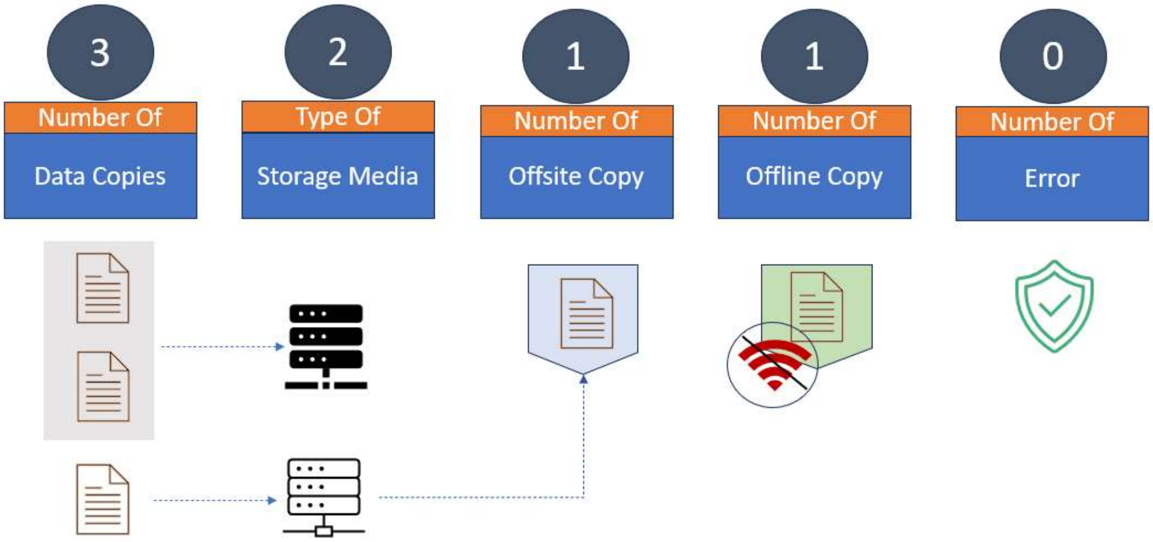
3-2-1-1 Backup Rule

Amid a surge in ransomware attacks, a crucial lesson emerged: maintaining offline backups is imperative. Hackers now target backups, realizing their importance in recovery. Breaching primary data or backups grants hackers the ability to expand their attack, underscoring the necessity for secure offline storage.



3-2-1-1-0 Backup Rule

Industry leaders remained skeptical about the effectiveness of the 3-2-1-1 data protection strategy, prompting further enhancements. This skepticism culminated in the development of the 3-2-1-1-0 rule.



Other Factors Worthy Of Consideration

Developing a data backup strategy should always involve careful consideration of backup frequency and speed. Deciding on the optimal backup frequency and speed is not a one-size-fits-all solution, as diverse data types and business contexts have varying requirements. By following specific guidelines, individuals can navigate this decision-making process effectively. The key objective is to strike a balance between data availability, security, and cost to ensure comprehensive data protection.

Consideration For frequency Of Data Backup

Consider these essential factors when establishing the frequency of data backups.

Data Change Rate: The frequency of data backup should align with the rate at which data changes within your organization. Data that undergoes frequent changes may require more frequent backups to minimize the risk of data loss.

Recovery Point Objective (RPO): RPO defines the maximum acceptable amount of data loss in the event of a disruption. The backup frequency should be set to ensure that RPO targets are met. For example, if the RPO is one hour, backups should occur at least every hour to minimize potential data loss.

Criticality of Data: The importance of the data to your organization's operations will influence the backup frequency. Critical data that is essential for business continuity may require more frequent backups compared to less critical data.

Operational Requirements: Consider operational requirements and workflows when determining backup frequency. For example, if certain processes rely on up-to-date data, more frequent backups may be necessary to support those operations effectively.

Storage Capacity and Resources: The availability of storage capacity and backup resources will impact backup frequency. Balancing backup frequency with available resources ensures that backups can be completed within acceptable timeframes without causing undue strain on infrastructure.

Regulatory and Compliance Requirements: Some industries have specific regulatory or compliance requirements that dictate backup frequency. Ensure that backup practices align with relevant regulations and standards applicable to your organization.

Recovery Time Objective (RTO): RTO specifies the maximum acceptable downtime for restoring data and systems after an incident. Backup frequency should be set to support RTO objectives by ensuring that data can be restored within the required timeframe.

Risk Management Considerations: Assess risks associated with data loss and weigh them against the cost and effort of implementing backup solutions. Higher risks may warrant more frequent backups to mitigate potential impacts.

Consideration For Data Backup Speed

The speed of data backup should be based on various parameters to ensure efficient and timely protection of data while considering factors such as the size of the data, available resources, and operational requirements. Here are some key parameters to consider when determining data backup speed:

Data Volume: The amount of data being backed up directly impacts backup speed. Larger volumes of data will generally take longer to back up compared to smaller datasets. Backup speed should be sufficient to complete the backup within the desired timeframe, considering data growth over time.

Network Bandwidth: Backup speed can be constrained by the available network bandwidth, especially in environments where data is being transferred over a network to remote backup locations or cloud storage. Optimizing network infrastructure and bandwidth allocation can help improve backup speeds.

Backup Infrastructure: The performance of backup infrastructure components such as backup servers, storage systems, and backup software can affect backup speed. Utilizing high-performance hardware and efficient backup solutions can help accelerate the backup process.

Backup Methodology: The backup method employed can impact backup speed. Different backup methods, such as full backups, incremental backups, or differential backups, have varying impacts on backup speed and efficiency. Choosing the most appropriate backup method based on data change rates and recovery requirements can optimize backup speed.

Concurrency: Parallelizing backup operations by backing up multiple datasets simultaneously can help improve backup speed, especially in environments with large volumes of data. However, resource contention should be carefully managed to avoid performance degradation.

Backup Window: Backup speed should be aligned with the available backup window, which is the period during which backups can be performed without impacting normal business operations. Efficient utilization of the backup window ensures that backups are completed within acceptable timeframes.

Recovery Time Objective (RTO): Backup speed should support the organization's recovery time objectives by ensuring that data can be restored within the required timeframe. Faster backup speeds contribute to shorter recovery times in the event of data loss or system failures.

Cost Considerations: Faster backup solutions may incur higher costs due to the need for more advanced infrastructure or software licenses. Balancing backup speed with cost considerations is important to ensure cost-effective backup solutions.

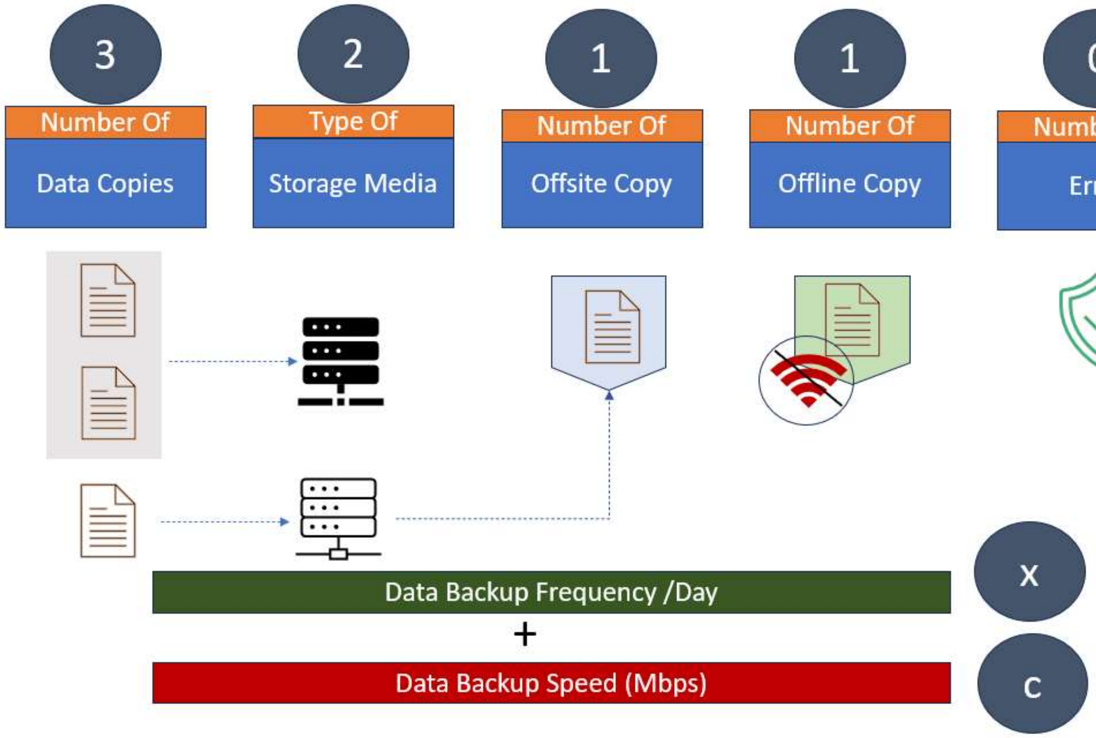
Proposed Enhancement To Existing Backup Rule

As stated, any data backup strategy necessitates deliberation on backup frequency and speed. Therefore, it is prudent and strongly recommended to incorporate these aspects into the current gold standard of backups, known as the 3-2-1-1-0 rule.

The proposed enhanced Backup Rule is defined as **3-2-1-1-0-x-c**, where:

"x" represents the data backup frequency per day,

"c" signifies the minimum backup speed measured in Mbps.



Conclusion

In today's digital era, ransomware attacks are becoming more intricate as data volumes rapidly expand. Organizations must prioritize robust data protection protocols to combat these evolving threats effectively. Recognizing the heightened risks and complexities involved, embracing the newly proposed backup rule of 3-2-1-1-0-x-c represents a significant step toward bolstering data security. This rule emphasizes maintaining three data copies stored across two different mediums, with at least one copy stored offsite, one immutable copy, and zero errors. Additionally, it emphasizes backup frequency to minimize data loss and ensures backup speed aligns with infrastructure capabilities for timely backups. By adhering to this comprehensive backup strategy, organizations can strengthen their defenses against ransomware, safeguarding critical data integrity and availability while mitigating potential cyberattack consequences.

References

https://www.backblaze.com/blog/whats-the-diff-3-2-1-vs-3-2-1-1-0-vs-4-3-2/

https://www.nakivo.com/blog/3-2-1-backup-rule-efficient-data-protection-strategy/

https://www.backblaze.com/blog/the-3-2-1-backup-strategy/

https://aws.amazon.com/what-is/data-backup/

https://www.mimecast.com/content/backup-planning-and-strategy/

https://community.veeam.com/blogs-and-podcasts-57/3-2-1-1-0-golden-backup-rule-569

https://www.techtarget.com/searchdatabackup/definition/3-2-1-Backup-Strategy

https://www.scalepad.com/blog/321-backup-rule/

https://xopero.com/blog/en/the-evolution-of-data-backup-is-the-3-2-1-backup-rule-a-thing-of-the-past/

https://stonefly.com/blog/3-2-1-vs-3-2-1-1-0-vs-4-3-2-backup-strategies/