Rocket

EBOOK

The Top 5 Reasons Your Backups are Failing

(and How to Address Them)

Contents

Rocket

Introduction

Regardless of what software you use to backup and restore your systems, failures are a fact of life for backup administrators. With every failure there's the potential for data loss that would require vast expenditures of resources to correct and assure business continuity. In order to learn more about this challenge, we consulted dozens of backup and storage administrators, implementation experts, and industry consultants to learn about the most common reasons that backups fail—and how to prevent them.

We worked with top-performing companies that have backup success rates of 98% or higher to provide information you can apply to your own data protection systems and processes.

The Myth of Five Nines

Why can't you have a 99.999% success rate or higher? It's a reasonable question, and one with a practical answer. As environments get larger, it's difficult to exceed a 98% success rate due to factors outside of the IT team's control. Power failures and network problems are the most common culprits, followed closely by human error. Older servers that maintain static data and storage devices scheduled for decommissioning also contribute to an increase of backup failures, and keep backup success rates well below even a much more achievable rate of 98%.

Many companies struggle to get their backup success rates to 80%, and some of those that report higher success rates even "cheat" by looking at a single point in time or even adjusting their backup data to factor out anomalies. While it may be reasonable to remove some data points caused by extenuating circumstances, it's far better to standardize on a reputable, consistent reporting system rather than get caught in an awkward situation when it's time to review the effectiveness of your business continuity efforts.

Improving Your Backup Performance

The tips on the following pages come from data protection professionals who have successfully optimized their backup systems to minimize failures. What follows are the top challenges for backup professionals every day-and their solutions. Addressing these problems in your own system is a great way to get closer to that 98% success rate.

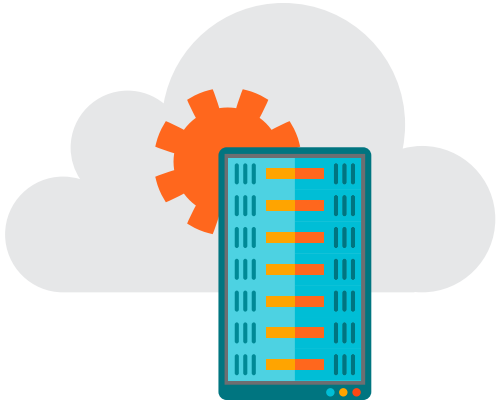
REASON 1

Data Protection Responsibilities are Distributed

In many cases, organizations are reducing central data protection costs by pushing the responsibility for backup processes out to content and application owners for second tier systems. A mandate for backing up the systems remains in place, but the burden falls to non-administrators making individual decisions about how to achieve the task. In many cases, it's not safe to assume that backups will continue to take place. Recreating data (even for secondary systems) can be costly, and ultimately the entire company suffers if data is lost. And don't forget, data that's permanently lost often equates to money or opportunity (or both) that are also permanently lost.

Solution

Using a backup monitoring solution that provides oversight for many different systems-including cloud storage-can provide peace of mind and assurance that company assets are being protected. You should also consider using a solution that has been designed for use by any team member with any level of expertise, not just backup administrators.



REASON 2

Insufficient Monitoring Processes

While poor monitoring doesn't cause backup failures, it can prevent backup failures from being seen and corrected. Poor monitoring protocols can trigger a domino effect that leads to future failures, and result in wasted time when the backup administrator is forced to use multiple spreadsheets full of irrelevant log data to diagnose problems manually.

Many backup systems have been in place for an extended period of time and were originally designed to monitor a relatively small number of servers. As the environments they were monitoring grew and became geographically dispersed, the backup systems became ineffective. An effective management strategy requires an integrated monitoring system that collects information from all of the storage devices and provides a holistic view of the backup and storage environment. Without this capability, the management process becomes time consuming thanks to a manual process on a per-system basis. Controlling these monitoring conflicts requires setting up alerts and connecting them with an SNMP-based management system.

With this type of solution, information from each backup is sent to a database, which is searched and reviewed by an administrator, then aggregated to identify problems. The alert system must be configured to deliver the message to each server's respective administrator. Administrators can then query this database while the clients are responsible for responding to the email alert from their SNMP monitoring system.

Any IT department would be challenged to put these database aggregation and query processes into place with a custom solution, especially when it comes to legacy backup systems that often can't be included in this larger monitored environment. These challenges increase when faced with the problem of monitoring and integrating backup systems from multiple vendors. Most IT environments include technologies from multiple backup vendors (on average three or more), forcing separate command and control centers for each backup application, which minimizes the ability to leverage resources and enforce consistent policies across data protection environments.

Solution

The best way to improve your monitoring protocol is to implement a monitoring system that automates the aggregation of data and provides a graphical user interface to look at the overall environment, as well as individual servers and clients. This system should also work across multi-vendor backup applications and provide a comprehensive monitoring system for backups across the enterprise, with dashboarding to make the data easy to understand.

REASON 3

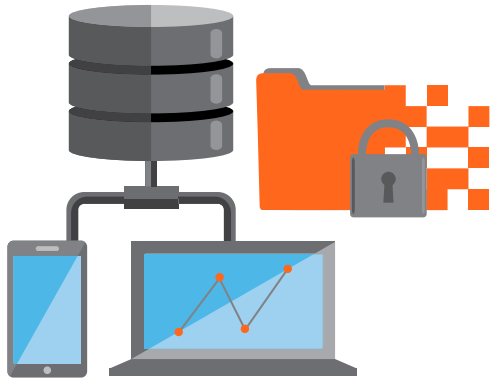
Missed Alerts

Most backup systems issue alerts when data in a client is not being adequately protected. The alert typically comes in the form of an email message sent to the administrator responsible for managing that client.

While this can work well when the environment is first setup, it takes discipline to keep up with the changes in people, applications, servers, and backup devices that happen over time. The alerting system needs to make it easy to update alerting processes to account for such changes as they happen, minimizing scenarios in which alerts can go unseen. It is vital that when an alert is issued, the right administrator gets the message promptly so he or she can search the database and determine the root cause of the failure.

Solution

This problem can be addressed by implementing data protection solutions that allow real-time alerts to be set up and sent to a command console where they can be brought to the attention of a team of administrators and managers via email, SNMP integration, and SMS. This allows the right admin to respond directly to a backup error using detailed information that is immediately accessible.



REASON 4

Insufficient Planning and Reporting

Many backup administrators only pay attention to single reporting system, which sends a regularly scheduled alert after each backup process completes, or fails to. While it's important to identify which servers are most vulnerable, this is only one aspect of keeping a data protection environment running smoothly. Admins who don't create alert reports, trending reports, forecasting reports, or other custom reports optimized for various departments are not following best practices.

There can also be challenges when alerts and monitoring data stored in distributed or secondary backup servers are transferred to their primary backup server. Secondary server data is commonly flushed after transfer, to make room for new data. The aggregated data collected on the primary server is often saved via a default setting, and only available for 14 days. Should the need arise to query this data or research problems after the 14-day window has passed, the key to understanding these failed backups may only exist on the secondary server. If the data have been flushed and are no longer available, it will take much longer to find the answers needed, and in the case where a critical issue is being examined, it may prove impossible to prevent similar occurrences in the near-term.

Solution

Collect data from both primary and distributed backup servers in a separate database so as not to affect day-to-day backup operations. This keeps the data available for analysis and troubleshooting at any time so it can be used in trending and forecasting reports that are relevant to the unique needs of your IT department and your entire data protection environment.

REASON 5

Misconfiguration

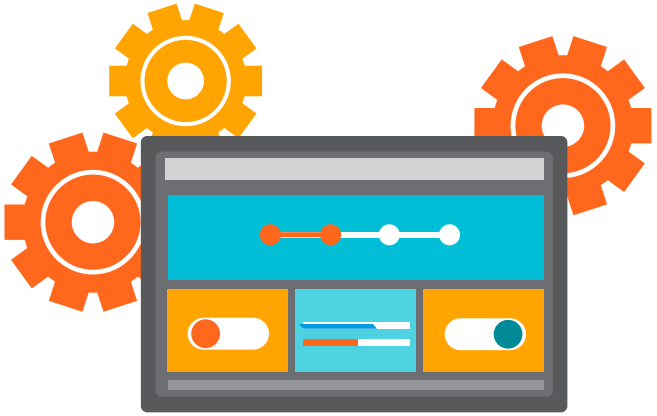
Because they are used in most IT departments, backup and recovery systems are generally thought to be well understood. But if misconfigured, they can create operational challenges. Misconfigurations of the data protection environment can occur at startup if any given parameter is improperly set, but in most cases problems creep in as the environment changes due to data and server growth, which can render the initial settings obsolete. Typical challenges include:

- **Improper sizing of recovery logs**
  Backup information is written to a recovery log, and that information is then written to a database. When the database is backed up, the recovery log is flushed to accept new information. If the recovery log reaches capacity before the database is backed up, transactions are no longer recorded. The recovery log file space must be manually expanded and restarted before the recovery log is available. If a failure occurs before the recovery log becomes available, again, an unnecessary emergency is created—potentially one from which you can't recover.

- **Disk-to-tape mismatch**
  In IT departments where tapes are used, most backups are written to disks, and then copied from disk to tape. If the disk pool is too small to accept new data before the process of writing the previous backup to tapes has finished, it can cause backup delays and missed backup windows. Backup software is typically able to write multiple threads to a disk pool, but only a single thread from a disk pool to a tape device. If the

tape devices don't support the speeds necessary for data to be written from the disk pool, the disk pool can no longer accept backup data.

- **Too many concurrent backup sessions**
  In new data protection environments, or as new backup clients are added to expanding data environments, the maximum number of clients that the backup system can support can easily be exceeded, and the backup window missed.



Solution

Because mistakes are (to some extent) inevitable, using expanded monitoring systems to keep an eye on your backup environment is a must. This allows you to quickly identify when an error has been made, or if the data protection environment has changed to the point where old operating procedures or systems no longer support your backup needs. While properly-implemented backup software may meet all of your backup needs today, it's unlikely your data protection environment will stay static, your data won't grow, or your servers won't change. There's no possible "set it and forget it" configuration, so best practices call for a monitoring system that works in concert with the backup system to allow you to follow trends and forecast when parameters in your backup environment may go out of alignment.

Art or Science?

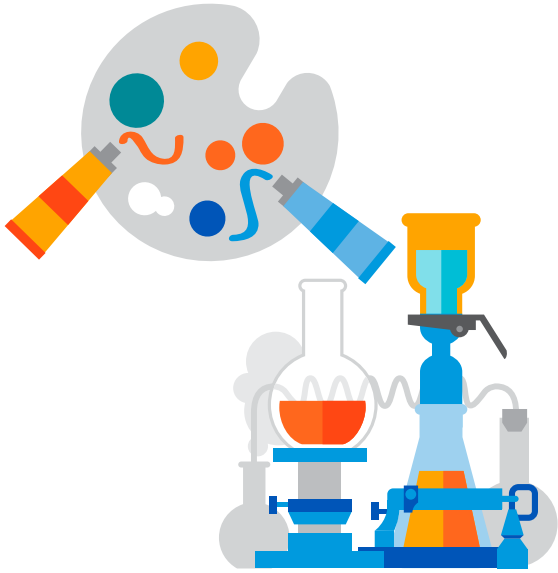
There's little doubt that proper operation of a backup environment is a precision science, with success shaped by failure rates, capacity, speed, and timing. The best-implemented software only operates at peak efficiency and value when properly configured for it's assigned task. This is when the real art of backup administration has its value.

To effectively operate a data protection environment, administrators need tools that help them follow trends and forecast future challenges. In some cases, this can be handled simply by keeping a watchful eye over thresholds. There are environments, that can maintain a 98% backup success rate this way, however, admins pay for that success rate with countless hours of time spent probing, collecting, analyzing, and reporting on the environment.

The admins managing some of the best-run data protection environments have traded in their spreadsheets and slide sets for monitoring, dashboarding, and reporting tools that can work in tandem with their backup software. They provide a GUI, real-time alerts, monitoring tools, trending tools, and customizable dashboards needed to operate the backup systems with maximum efficiency.

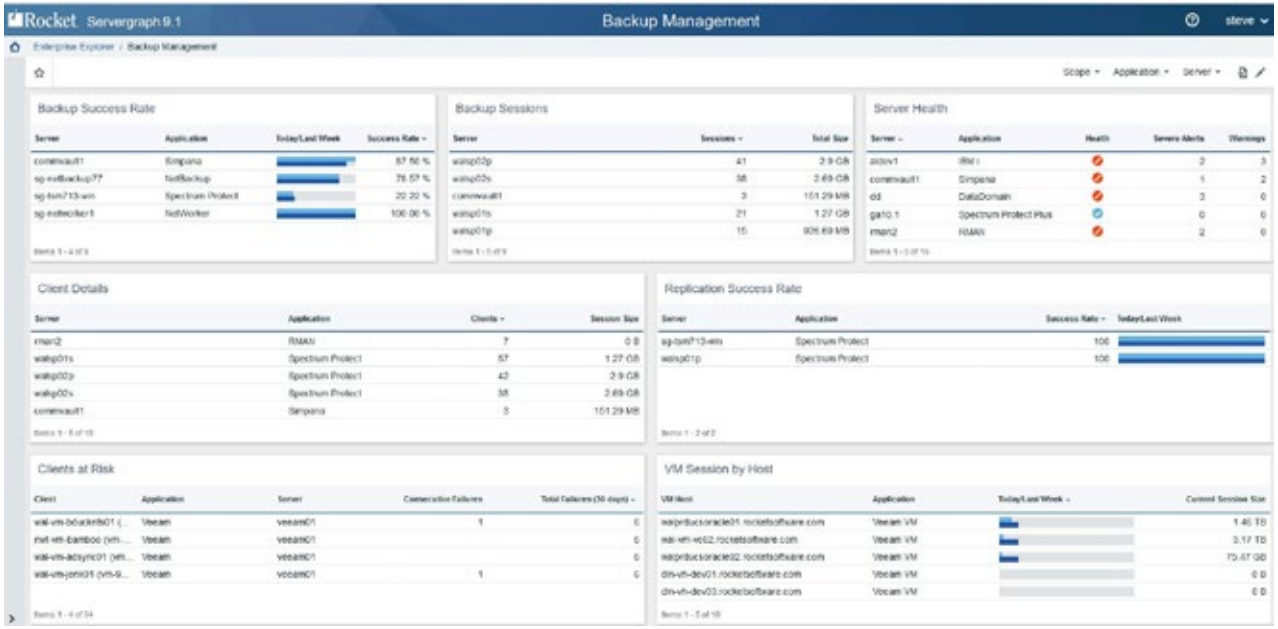
For these professionals, a 98% backup success rate is achievable with their standard operating procedure. Time that was once spent monitoring systems manually can be spent on higher-value tasks such as increased testing of critical systems, expansion of new data types and sources, and better utilizing technology to further the business success and continuity of the organization.

Top-performing organizations also tend to use backup software from multiple vendors, where servers and storage are managed and backed up with tools specific to their systems. In these multi-vendor environments, backup monitoring and reporting systems are even more advantageous. These systems allow common practices for backup management to be readily applied to these different environments. By utilizing similar monitoring and reporting techniques across multiple backup applications, this software can keep all the backup environments performing at high levels of completion and restore reliability.



Archive & Backup Management

Rocket® Servergraph® makes it easy to understand what's happening in your entire backup environment. You can automate daily backups, get prioritized real-time alerts, and gain insight into complex, multi-vendor backup environments from a single view.



Find out more by calling us at: +1-855-577-4323 or visiting our website:

Learn More about
Rocket Servergraph

Rocket

rocketsoftware.com
info@rocketsoftware.com
US: 1 855 577 4323
EMEA: 0800 520 0439
APAC: 612 9412 5400
twitter.com/rocket
www.linkedin.com/company/rocket-software
www.facebook.com/RocketSoftwareInc
blog.rocketsoftware.com