BOCADA

DATA RESILIENCY CHECKLIST

Critical Questions To Assess Backup Operations Protections

INTRODUCTION

Enterprise IT organizations are working at breakneck speeds to enact virtualization and cloud transformations to meet everyday business demands. The focus on these broader IT infrastructure evolutions often comes with a blind spot: backup operations. While assumptions may be made that new data protection technologies are “good enough” at ensuring compliance and data resiliency, verifying that this is the case can be the difference between weathering a major data loss and finding your organization under major customer, investor, and regulatory scrutiny.

IT infrastructure leaders can leverage simple yet pointed questions to identify just how effective their teams’ tools and protocols are at protecting data and ensuring that it is available for key recovery events. “Yes” or “No” answers will isolate weaknesses in day-to-day operations, audit readiness, and holistic oversight that will need to be shored up before leaders can feel confident that data is fully protected.

QUESTIONS TO ASSESS YOUR BACKUP OPERATIONS PROTECTIONS:

1. *Are All Of Our Key Resources & Assets Being Backed Up?*
2. *Are We Backing Up Data According To The Right Protocols?*
3. *Are We Regularly Meeting Our Backup Success Goals?*
4. *Can We Definitely Pass Our Next Backup Audit...And Can We Do It Efficiently?*
5. *Does Our Backup Team Fix Problems Quickly...And Can We Prove It?*

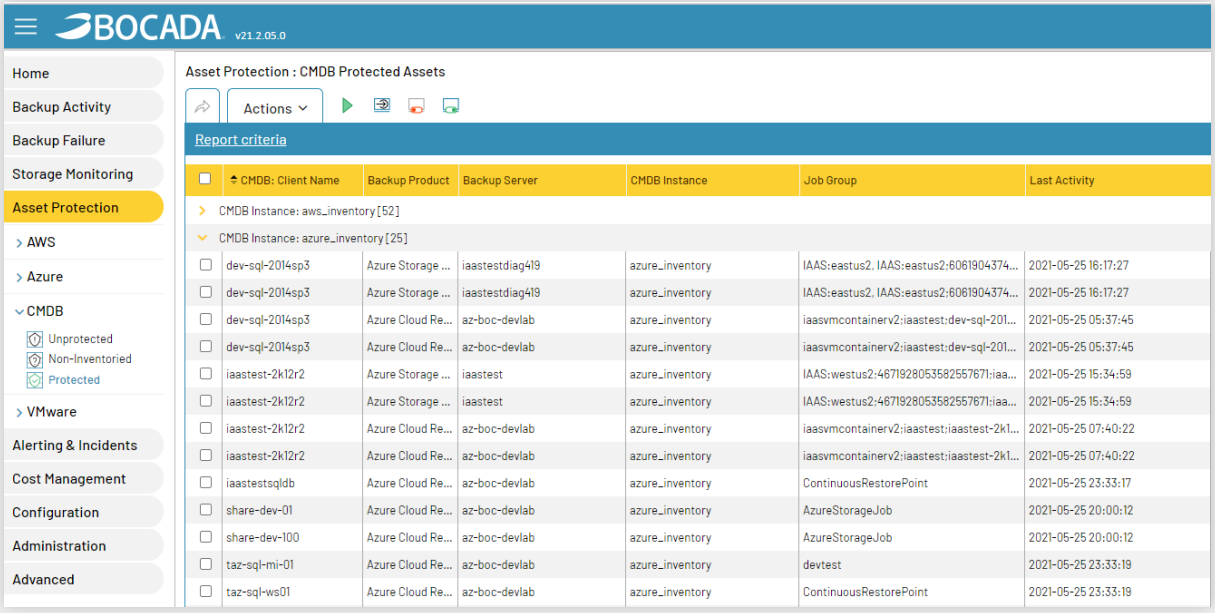
1. Are All Of Our Key Resources & Assets Being Backed Up?

How confident are you that all of your organization's resources and assets are actually being backed up? The speed with which assets are created, and the breadth of teams empowered to create those assets, can often mean that resources are left wholly unprotected.

Regardless of how asset records are kept—using asset inventory software, creating propriety in-house databases, relying on CSV files—data protection teams need a way to efficiently review backup logs, compare them against asset lists, and determine if those assets are actually being backed up.

Tackling this manually is so time intensive that teams doing this work will only do it once or twice a year. Further, the inherent human error involved in the process likely means many unprotected assets are left unidentified. However, by leveraging automated cross-referencing and reporting processes, teams can quickly, effectively, and comprehensively identify unprotected assets and develop ready-made punch lists to use for further investigation.

Unprotected Asset Report

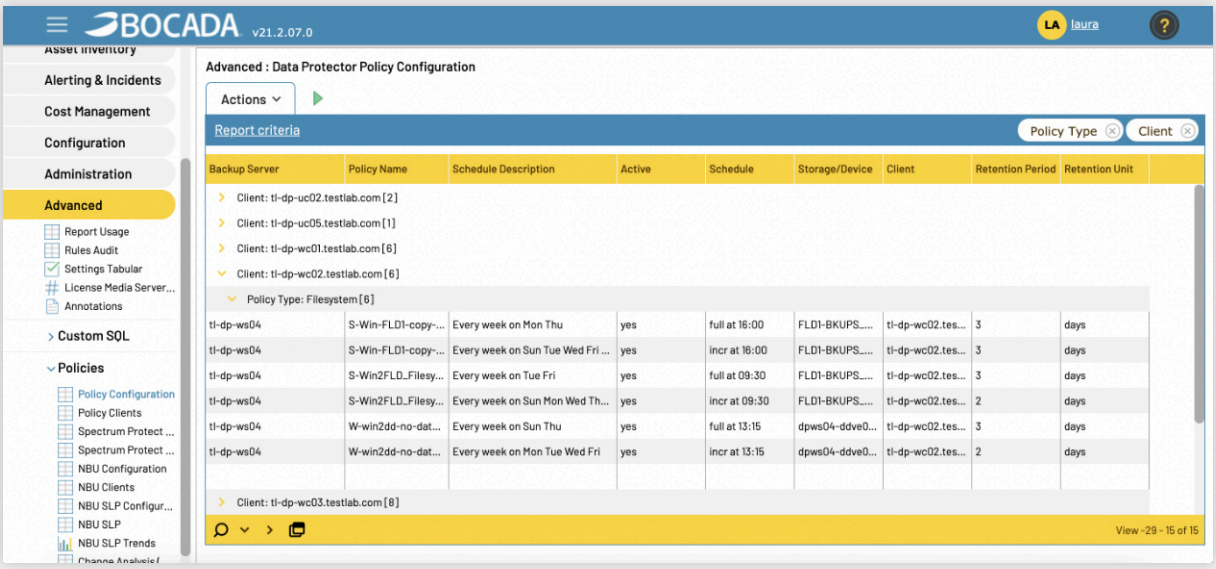


2. Are We Backing Up Data According To The Right Protocols?

There are clear cut guidelines set internally by IT security teams or externally by government regulators around what data needs to be backed up, and how often. No doubt your backup team knows this. However, with new servers and resources spun up so quickly by assorted IT teams and personnel, are you sure your backup team has had a chance to put the right protocols in place?

Checking this manually is not feasible. The sheer scale of backup clients in an enterprise environment means it's next-to-impossible to check all backup clients and their corresponding backup policies. Automating this process, however, changes the game entirely. By leveraging solutions to automatically check all backup clients and their policies, IT teams have an efficient way to confirm that backups are fully aligned with compliance regulations... or that backup policy updates are needed immediately.

Backup Policy Configuration Report



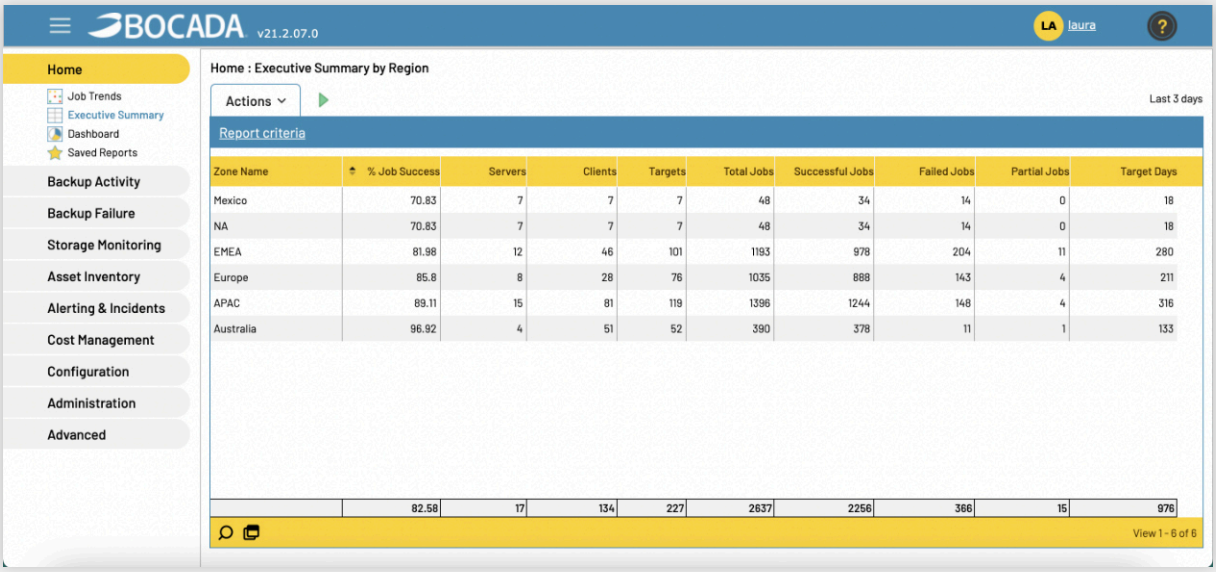
3. Are We Regularly Meeting Our Backup Success Goals?

Enterprise-scale backup environments aren't just massive in size but also unique in how different segments of the environment are managed. Can you say with confidence that each distinct part of your organization's environment—cloud vs on-prem, different business units, unique backup servers, geographic regions—is equally well protected?

Relying on piecemeal reports from different backup products or team members likely means receiving data in many different formats with a host of different metrics shown. It's scattered, inconsistent, and offers little insight into whether any teams or segments are continually underperforming.

Aggregating all of this in a normalized way via a single dashboard removes this operational uncertainty. You can quickly and easily assess backup data health, pinpoint segments that are lagging behind benchmarks, and guide data protection teams to install protocols that ensure data is fully protected and restorable.

Executive Summary Report



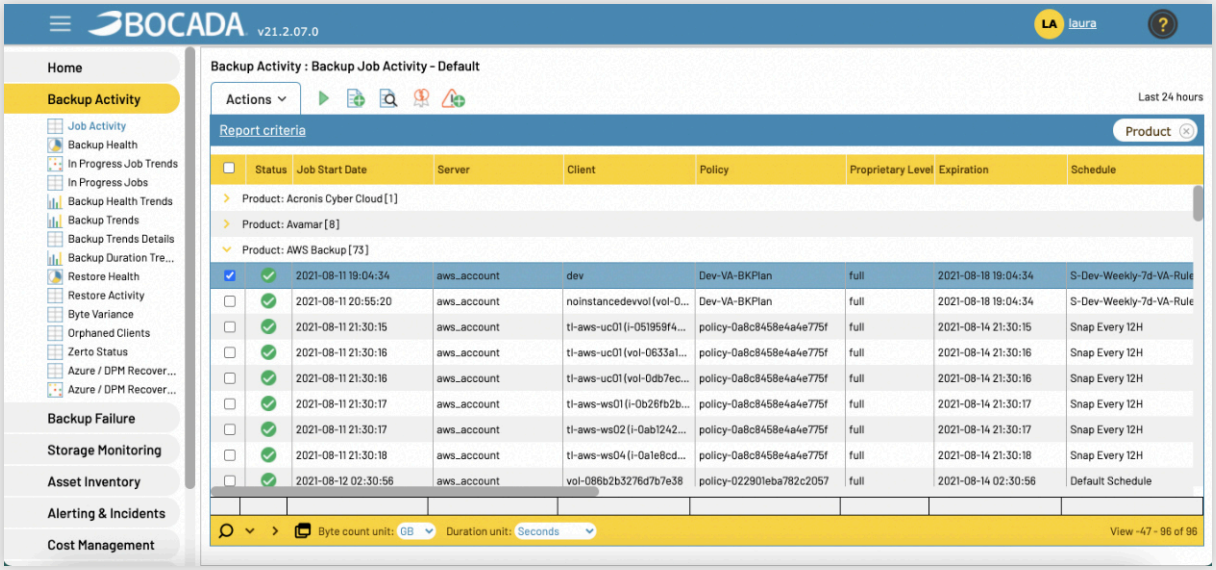
4. Can We Definitely Pass Our Next Backup Audit...And Can We Do It Efficiently?

The next time an auditor asks for the backup records from a particular server over a particular time frame, how long will it take your team to fulfill that request? And, will they be able to?

Going one by one into each backup server, extracting backup metadata, and then consolidating that data into clean, well-formatted reports is extremely time intensive. Further, it assumes the data is even available, which is often not the case given backup products' short data retention periods.

However, when teams rely on tools to automatically collect and retain backup servers' historical data on an ongoing basis, and consolidate that data under a single dashboard, they will be well-equipped to quickly and effectively respond to auditor requests. Personnel can then spend less time on audits and more time on daily operations monitoring.

Backup Job Activity Report



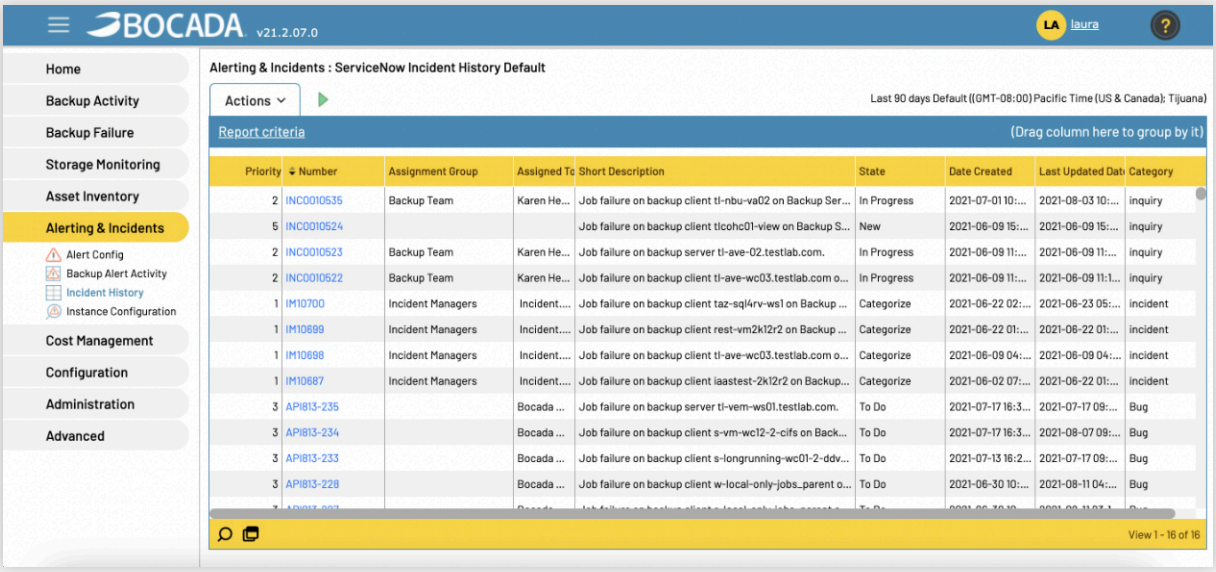
5. Does Our Backup Team Fix Problems Quickly...And Can We Prove It?

Data backups will fail at some point in time. It's an inevitable part of backup operations, but something that stands in the way of keeping data protected and restorable. Do you know how long it takes to fix those failures to ensure data resiliency?

Typical failure remediation lag times are the result of many bottlenecks inherent in the remediation process: identifying that a backup job run on a critical asset failed, populating a ticket with relevant details about that failure in a ticketing system, and monitoring the process of resolving the underlying issues.

Addressing these bottlenecks through automation greatly improves those lag time. Failures can be readily identified and tickets created in near-real time. This optimizes team labor hours around improving operations and keeping assets protected, all while shoring up the average resolution window. Further, by keeping track of typical resolution windows, teams can develop benchmarks around times to beat for fixing failure issues.

Backup Failure Ticket Monitoring



CONCLUSION

Several certainties exist in enterprise IT infrastructure operations. Bad actors will continually try to penetrate infrastructures with cyberattacks...all while auditors continually request evidence that data is secure and restorable in the event of an attack or regulatory query. These ever-present dynamics mean IT infrastructure leaders must assess just how resilient their IT operations are at safeguarding data and seek practices and tools that support comprehensive data protection.

Introducing automation, centralized monitoring, and proactive alerting and triaging addresses this reality head on. It empowers data protection teams to quickly identify issues that stand in the way of successful data restorations, business continuity, and ongoing audits, all while giving IT infrastructure leaders the assurances they need that data protection operations are secure.

About Bocada

Bocada LLC, a global IT automation leader, delivers backup reporting and monitoring solutions that give enterprises complete visibility into their backup performance. Bocada provides insight into complex backup environments, enabling IT organizations to save time, automate ongoing reporting activities, and reduce costs. With the largest installed customer base in the Fortune 500, Bocada is the world's leading provider of backup reporting automation.

For more information, visit **www.bocada.com**