

Bocada White Paper Series: Improving Backup and Recovery Success with Bocada Enterprise

Benefits of Backup Policy Management

Why Policy Management Matters3

Data Protection Service Management: An Overview3

Policy Management’s Role in Effective Data Protection Service Delivery4

Best Practices in Policy Management.....5

Effective Policy Management Drives SLA Success6

Reducing Risk through Continuous Policy Review8

Cost Benefits of Continuous Policy Management8

Summary..... 10

Why Policy Management Matters

Ensuring successful backups across the data protection environment is a goal that all IT administrators strive to achieve. Yet most experienced administrators understand that a backup success only tells part of the story. Take Michael, the eager backup administrator who reviews and remediates all his environments' backups to ensure 99% success rates. When tasked with restoring the CEO's email from a month ago, he is confident that his hard work of resolving missed and failed backups on a daily basis will ensure a quick recovery. However, much to his dismay, he discovers that the mail server he hopes to restore had been mistakenly assigned to a legacy data retention policy which only stores one week worth of backup data.

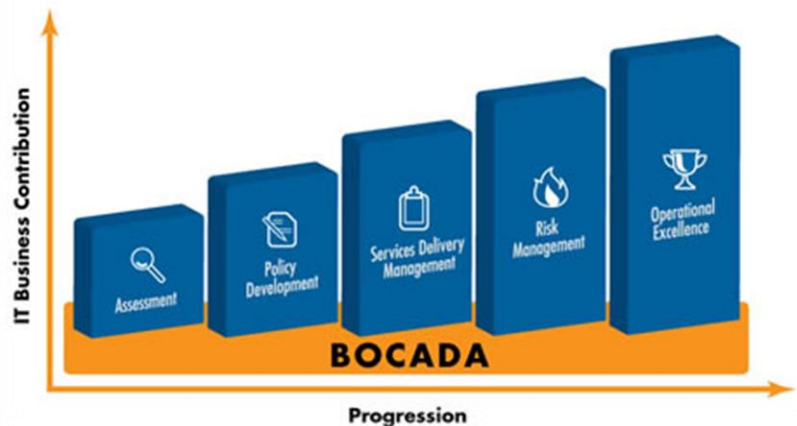
Everyday more and more organizations face similar challenges when attempting to ensure recoverability of their electronic assets. These challenges, in addition to increasing regulatory mandates demanded from storage teams, require a better view into the health of data protection processes and require control of retention policies. Backup administrators need to quickly and easily be able to view all of the existing backup schedules and retention policies in order to not only ensure backups complete, but that the data is recoverable and retained according to business requirements.

Data Protection Service Management: An Overview

Preventative and proactive management of the data protection environment is essential for meeting these challenges. However, proactively managing and troubleshooting a backup environment entails much more than just monitoring job success and failure rates. As in the above example, monitoring success and failures can help ensure recoverability, to a point. There are many other aspects of the backup operation that must be monitored and managed to ensure all data is recoverable.

Many IT organizations are familiar with IT Service Management (ITSM), the process based practice of aligning the delivery of IT services with the needs of the business, with a particular focus on customer benefits. Aligning with this concept, Bocada together with leading enterprise customers and service providers has developed the Data Protection Service Management (DPSM) delivery model (Figure 1). The model is an actionable methodology targeted at enhancing

the delivery of data protection services to internal or external customers. The model outlines a multi-phased approach to assess the overall data protection delivery infrastructure and effectiveness, improve the ability to deliver quality data protection and recovery services, publish the results to customers and continuously advance the effectiveness of data protection operations while lowering costs.



The DPSM Model leverages the collective experience of Bocada Enterprise customers over the past eight years, drawing upon their best practices using the Bocada Enterprise solution. The phases of the model include:

- Phase 1 Initial Assessment
 - This health check helps reveal the effectiveness of an organization's data protection environment, pinpoints and eliminates trouble spots and identifies opportunities for improvement.
- Phase 2 Policy Management
 - Policies and processes are modified to better ensure success, recoverability and IT business alignment.
- Phase 3 Services Delivery Management
 - After completing phases 1 & 2, organizations can confidently create and publish a data protection service catalog. Managing SLAs enables organizations to effectively measure adherence and success rates and publish results to customers.
- Phase 4 Risk & Problem Management
 - Utilize information to expose risk areas, eliminate problem areas, track problem resolution, identify unprotected assets and confidently deliver against published SLAs.
- Phase 5 Operational Excellence
 - Standardizing on the processes developed in previous phases enables streamlined operations, reduced TCO and increased IT business contribution and customer retention.

The focus of this paper is the Policy Management phase and the benefits of effectively and continuously reviewing and modifying policies in order to meet business goals as they related to data protection, retention and recoverability.

Policy Management's Role in Effective Data Protection Service Delivery

Ongoing policy review is a critical piece of the data protection service management process. Customers need to ensure that their policies are effectively supporting the business goals of the company as it relates to recoverability, compliance, SLA adherence and capacity management. An automated reporting solution that can regularly mine policy configuration provides the visibility required for customers to quickly and easily review policies and determine if changes need to be made to meet those goals.

Since policies dictate how data is being protected, it is critical to monitor them closely and ensure that they are configured as expected. As storage teams grow, or in cases where team members are in multiple geographic locations, the number of people who could accidentally make changes to policy setup increases, potentially compromising data protection efforts. This alone increases the importance of having a straightforward process for monitoring policy configurations. In addition, retention standards change over time due to organizational requirements or due to regulatory mandates relating to certain types of data. When these changes occur, it is important to understand the current policy definitions and how those need to change to reflect new mandates to avoid the risk of not being able to recover older data.

In order to drive a service management approach to data protection, storage teams need to develop standard offerings based on the various needs of the business. With standardized policies and processes in place, storage teams will be able to effectively communicate how data is being protected and set expectations with end users on how different levels of data protection impact overall costs.

Best Practices in Policy Management

The Bocada DPSM model recommends that users initially review all policies in place to ensure they are supporting the business requirements of the organization. Once the review is complete, the following best practices should be put in place:

- Define limited number of policies/processes
 - Processes should align with what infrastructure can support
 - Ensure policies are consistent across data and/or application types (ex: all Exchange servers have similar policies in place)
- Ensure all clients are on the latest backup application version (not doing so can cause failures)
- Ensure retention policies are supporting recovery point objectives
 - Initialize communication with business owners on their application priorities and what policies will support their needs
- Publish a services catalog to customers to standardize offerings.

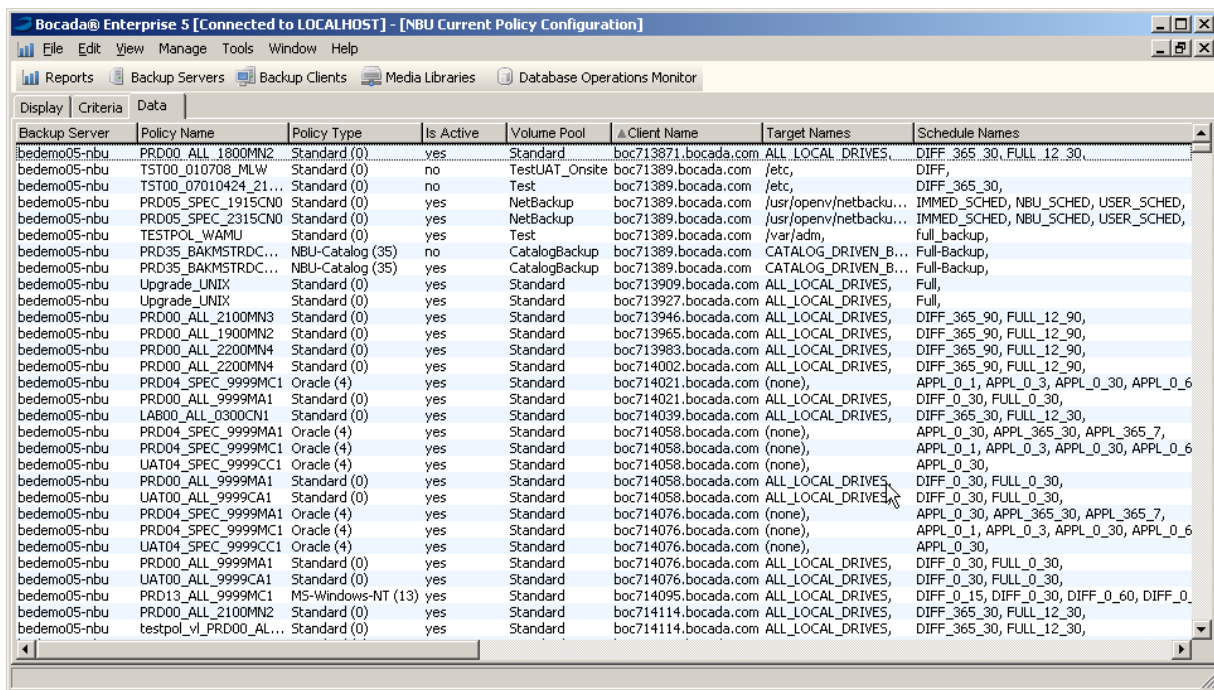
The Policy and Configuration reports in Bocada Enterprise provide a quick view into currently defined data server and client policies. The Current Policy Configuration report (Figure 2) gives a detailed tabular view into policies across an entire customer environment. Organizations can quickly see the various policies that have been created on all of their master servers and also display the clients that are assigned to the policies listed in the report. Advanced selection criteria also

Policy Reports Aid in Success

Bocada can assist in these efforts with the Policy and Client Configuration reporting available in Bocada Enterprise. Bocada provides visibility into policy configuration to address many data protection challenges in order to meet the following goals:

- Improve recoverability
 - Ensure retention rates meet RPO goals
 - Identify unintentional “inactive” policies
- Help meet SLA goals
 - Determine if policies support business requirements
 - Facilitates consistent SLA offerings
- Enhance communication with internal/external customers
 - Review policies as part of service catalog/SLA negotiations
 - Publish policies with SLA results
- Provide audit trails for compliance & change management
 - Track historical records of changes
- Reduce overall costs
 - Identify “over-protected” clients consuming excess capacity
 - Free up administrative hours

exist to allow customers to only select sets of clients that they may be interested in analyzing, such as Email servers or any other policy dependent applications in the organization. Bocada's native zoning feature allows for easy definition of these groupings, ensuring mission critical servers have properly defined policies. These reports allow organizations to ensure consistency across policy settings and attributes.



Backup Server	Policy Name	Policy Type	Is Active	Volume Pool	Client Name	Target Names	Schedule Names
bedemo05-nbu	PRD00_ALL_1800MN2	Standard (0)	yes	Standard	boc713871.bocada.com	ALL_LOCAL_DRIVES,	DIFF_365_30,FULL_12_30,
bedemo05-nbu	TST00_010708_MLW	Standard (0)	no	TestUAT_Onsite	boc71389.bocada.com	/etc,	DIFF,
bedemo05-nbu	TST00_07010424_21...	Standard (0)	no	Test	boc71389.bocada.com	/etc,	DIFF_365_30,
bedemo05-nbu	PRD05_SPEC_1915CNO	Standard (0)	yes	NetBackup	boc71389.bocada.com	/usr/opensv/netbacku...	IMMED_SCHEDULED,NBU_SCHEDULED,USER_SCHEDULED,
bedemo05-nbu	PRD05_SPEC_2315CNO	Standard (0)	yes	NetBackup	boc71389.bocada.com	/usr/opensv/netbacku...	IMMED_SCHEDULED,NBU_SCHEDULED,USER_SCHEDULED,
bedemo05-nbu	TESTPOL_WAMU	Standard (0)	yes	Test	boc71389.bocada.com	/var/adm,	full_backup,
bedemo05-nbu	PRD35_BAKMSTRDC...	NBU-Catalog (35)	no	CatalogBackup	boc71389.bocada.com	CATALOG_DRIVEN_B...	Full-Backup,
bedemo05-nbu	PRD35_BAKMSTRDC...	NBU-Catalog (35)	yes	CatalogBackup	boc71389.bocada.com	CATALOG_DRIVEN_B...	Full-Backup,
bedemo05-nbu	Upgrade_UNIX	Standard (0)	yes	Standard	boc713909.bocada.com	ALL_LOCAL_DRIVES,	Full,
bedemo05-nbu	Upgrade_UNIX	Standard (0)	yes	Standard	boc713927.bocada.com	ALL_LOCAL_DRIVES,	Full,
bedemo05-nbu	PRD00_ALL_2100MN3	Standard (0)	yes	Standard	boc713946.bocada.com	ALL_LOCAL_DRIVES,	DIFF_365_90,FULL_12_90,
bedemo05-nbu	PRD00_ALL_1900MN2	Standard (0)	yes	Standard	boc713965.bocada.com	ALL_LOCAL_DRIVES,	DIFF_365_90,FULL_12_90,
bedemo05-nbu	PRD00_ALL_2200MN4	Standard (0)	yes	Standard	boc713983.bocada.com	ALL_LOCAL_DRIVES,	DIFF_365_90,FULL_12_90,
bedemo05-nbu	PRD00_ALL_2200MN4	Standard (0)	yes	Standard	boc714002.bocada.com	ALL_LOCAL_DRIVES,	DIFF_365_90,FULL_12_90,
bedemo05-nbu	PRD04_SPEC_9999MC1	Oracle (4)	yes	Standard	boc714021.bocada.com	(none),	APPL_0_1,APPL_0_3,APPL_0_30,APPL_0_6
bedemo05-nbu	PRD00_ALL_9999MA1	Standard (0)	yes	Standard	boc714021.bocada.com	ALL_LOCAL_DRIVES,	DIFF_0_30,FULL_0_30,
bedemo05-nbu	LAB00_ALL_0300CN1	Standard (0)	yes	Standard	boc714039.bocada.com	ALL_LOCAL_DRIVES,	DIFF_365_30,FULL_12_30,
bedemo05-nbu	PRD04_SPEC_9999MA1	Oracle (4)	yes	Standard	boc714058.bocada.com	(none),	APPL_0_30,APPL_365_30,APPL_365_7,
bedemo05-nbu	PRD04_SPEC_9999MC1	Oracle (4)	yes	Standard	boc714058.bocada.com	(none),	APPL_0_1,APPL_0_3,APPL_0_30,APPL_0_6
bedemo05-nbu	UAT04_SPEC_9999CC1	Oracle (4)	yes	Standard	boc714058.bocada.com	(none),	APPL_0_30,
bedemo05-nbu	PRD00_ALL_9999MA1	Standard (0)	yes	Standard	boc714058.bocada.com	ALL_LOCAL_DRIVES,	DIFF_0_30,FULL_0_30,
bedemo05-nbu	UAT00_ALL_9999CA1	Standard (0)	yes	Standard	boc714058.bocada.com	ALL_LOCAL_DRIVES,	DIFF_0_30,FULL_0_30,
bedemo05-nbu	PRD04_SPEC_9999MA1	Oracle (4)	yes	Standard	boc714076.bocada.com	(none),	APPL_0_30,APPL_365_30,APPL_365_7,
bedemo05-nbu	PRD04_SPEC_9999MC1	Oracle (4)	yes	Standard	boc714076.bocada.com	(none),	APPL_0_1,APPL_0_3,APPL_0_30,APPL_0_6
bedemo05-nbu	UAT04_SPEC_9999CC1	Oracle (4)	yes	Standard	boc714076.bocada.com	(none),	APPL_0_30,
bedemo05-nbu	PRD00_ALL_9999MA1	Standard (0)	yes	Standard	boc714076.bocada.com	ALL_LOCAL_DRIVES,	DIFF_0_30,FULL_0_30,
bedemo05-nbu	UAT00_ALL_9999CA1	Standard (0)	yes	Standard	boc714076.bocada.com	ALL_LOCAL_DRIVES,	DIFF_0_30,FULL_0_30,
bedemo05-nbu	PRD13_ALL_9999MC1	MS-Windows-NT (13)	yes	Standard	boc714095.bocada.com	ALL_LOCAL_DRIVES,	DIFF_0_15,DIFF_0_30,DIFF_0_60,DIFF_0
bedemo05-nbu	PRD00_ALL_2100MN2	Standard (0)	yes	Standard	boc714114.bocada.com	ALL_LOCAL_DRIVES,	DIFF_365_30,FULL_12_30,
bedemo05-nbu	testpol_vl_PRD00_AL...	Standard (0)	yes	Standard	boc714114.bocada.com	ALL_LOCAL_DRIVES,	DIFF_365_30,FULL_12_30,

Figure 2: Current Policy Configuration report. A centralized view of policy attributes can be immediately highlighted. In this example there are a few inactive policies that should be investigated.

Effective Policy Management Drives SLA Success

The DPSM model is focused on ensuring organizations can effectively deliver on SLAs to either internal or external customers. The process starts with an overall assessment of the backup environment, with the goal of understanding exactly what level of success rates and recoverability objectives the infrastructure can support. Once this is reviewed, a standard set of policies should then be put in place for different data sets and/or applications. Standardization is a critical piece of being able to publish a Service Catalog to customer with an assurance that the agreed to SLAs can be met.

Standardization across clients in a backup environment is critical to ensure proper recovery can take place in the event of a disaster. The Client Configuration report (Figure 3) allows customers to report on the current configuration settings across their entire environment and helps them easily see clients that need attention, such as outdated operating systems that are in need of upgrades. Hardware, Operating Systems and even backup client versions can be displayed. Legacy clients (clients that are using outdated backup agents) can be singled out in the client configuration report and emailed to administrators for further review. This list of clients should have their backup software updated to match the rest of the organization, making it easier to manage problems and standardize on remediation techniques.

Backup Server	Node Name	Node Type	Platform Name	OS Version	Domain Name	Option Set	Compression	Client Version	Backup Delete Allowed
bedemo01-tsm	CSOL1	CLIENT	WinNT	5.01	TEST	TEST3	CLIENT	5.3.5	NO
bedemo01-tsm	T1-TSMHOST04	CLIENT	WinNT	5.02	STANDARD	TEST3	CLIENT	5.5.0	NO
bedemo01-tsm	T1-VM64-CLIENT	CLIENT	WinNT	5.02	STANDARD		CLIENT	5.5.0	NO
bedemo01-tsm	T1-VM64-CLIENT2	CLIENT	WinNT	5.02	NASDOMAIN		CLIENT	5.5.0	NO
bedemo01-tsm	T1-VM64-CLIENT3	CLIENT	WinNT	5.02	STANDARD		CLIENT	5.5.0	NO
t1-tsmhost04.testlab1.com	CSOL1	CLIENT	WinNT	5.01	TEST	TEST3	CLIENT	5.3.5	NO
t1-tsmhost04.testlab1.com	T1-TSMHOST04	CLIENT	WinNT	5.02	STANDARD	TEST3	CLIENT	5.5.0	NO
t1-tsmhost04.testlab1.com	T1-VM64-CLIENT	CLIENT	WinNT	5.02	STANDARD		CLIENT	5.5.0	NO
t1-tsmhost04.testlab1.com	T1-VM64-CLIENT2	CLIENT	WinNT	5.02	NASDOMAIN		CLIENT	5.5.0	NO
t1-tsmhost04.testlab1.com	T1-VM64-CLIENT3	CLIENT	WinNT	5.02	STANDARD		CLIENT	5.5.0	NO

Figure 3: Client Configuration reports Keep track of out of date versions and other client settings to drive more consistent configurations in the environment. In this example, notice that two of the clients are running older client versions of the backup software.

By consistently monitoring SLA success rates with Bocada Enterprise (Figure 4), and reviewing if the policies in place are supporting the optimal SLA outcomes, organizations can improve service delivery, increase customer satisfaction and more easily charge for backup services.

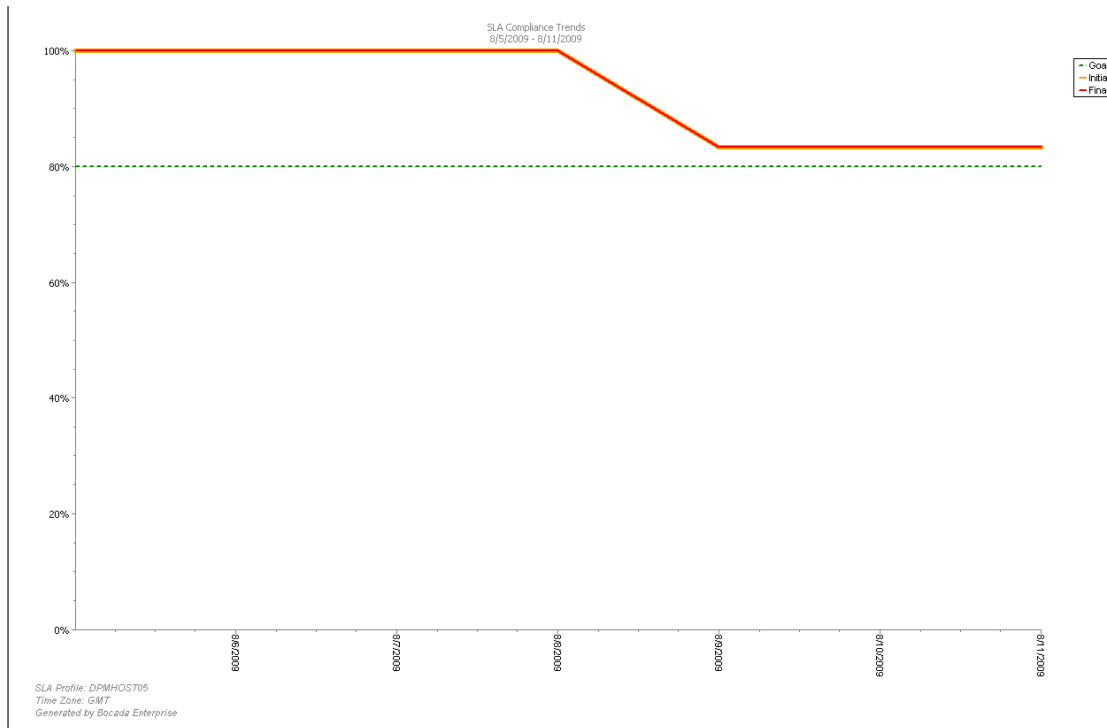


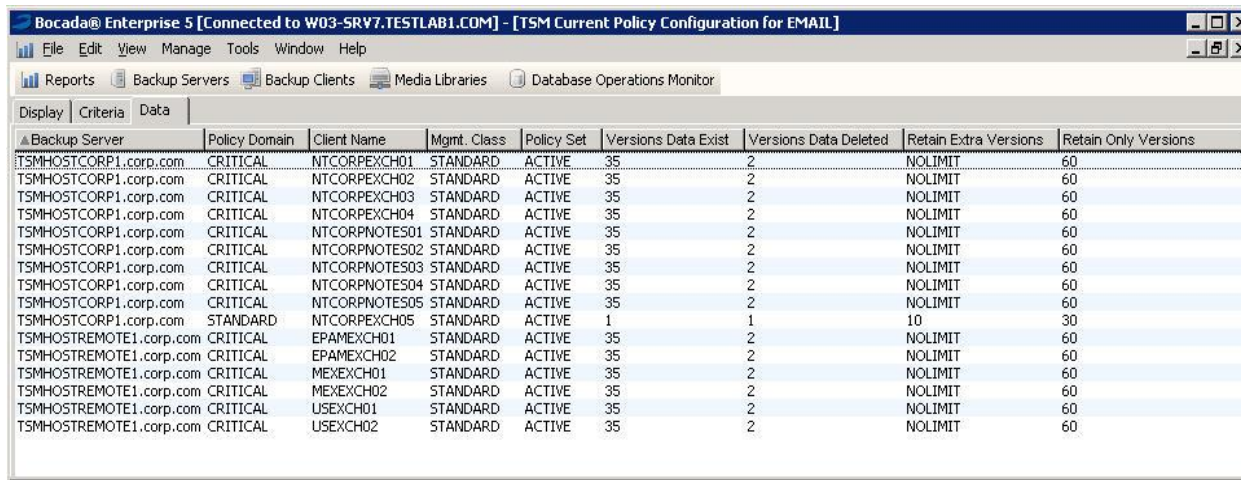
Figure 4: SLA Reports. The Bocada Enterprise SLA Trends Report measures performance against agreed to service level agreements, allowing storage teams to track progress over time. More detailed reports are also available to diagnose missed or low SLAs that indicate at-risk clients.

Reducing Risk through Continuous Policy Review

The best way to reduce the risk of unplanned downtime and ensure compliance is to ensure the proper policies are in place to guarantee data is protected and recoverable. Data retention policy control is an important foundation for the continuous advancement in the effectiveness of data protection operations.

Acceptable retention settings defined in policies, combined with successful backups of corporation’s increasingly growing data streams are critical in ensuring that an organization’s not only compliant with legislative requirements and industry regulations, but also makes certain that adequate data backups exist to prevent loss of data during catastrophes. The lack of strong data retention policies may put organizations in a position that make it impossible to continue normal business operations immediately following a disaster.

Retention policies will vary in every organization, even in individual departments; there is no “one size fits all” recommendation for how long data is retained for recovery purposes. While a single retention policy may be easiest to implement, that practice would likely result in a waste of storage resources when non-essential data is retained for too long. On the other hand, it is not feasible to manage hundreds of retention policies in an organization. The DPSM model recommends that retention rates are first determined based on the business importance of the clients and/or data being protected, and policies are consistently set against each “grouping” (for example all Exchange servers have the full, incremental schedule and retention settings (Figure 5)).



Backup Server	Policy Domain	Client Name	Mgmt. Class	Policy Set	Versions Data Exist	Versions Data Deleted	Retain Extra Versions	Retain Only Versions
TSMHOSTCORP1.corp.com	CRITICAL	NTCORPEXCH01	STANDARD	ACTIVE	35	2	NOLIMIT	60
TSMHOSTCORP1.corp.com	CRITICAL	NTCORPEXCH02	STANDARD	ACTIVE	35	2	NOLIMIT	60
TSMHOSTCORP1.corp.com	CRITICAL	NTCORPEXCH03	STANDARD	ACTIVE	35	2	NOLIMIT	60
TSMHOSTCORP1.corp.com	CRITICAL	NTCORPEXCH04	STANDARD	ACTIVE	35	2	NOLIMIT	60
TSMHOSTCORP1.corp.com	CRITICAL	NTCORPNOTES01	STANDARD	ACTIVE	35	2	NOLIMIT	60
TSMHOSTCORP1.corp.com	CRITICAL	NTCORPNOTES02	STANDARD	ACTIVE	35	2	NOLIMIT	60
TSMHOSTCORP1.corp.com	CRITICAL	NTCORPNOTES03	STANDARD	ACTIVE	35	2	NOLIMIT	60
TSMHOSTCORP1.corp.com	CRITICAL	NTCORPNOTES04	STANDARD	ACTIVE	35	2	NOLIMIT	60
TSMHOSTCORP1.corp.com	CRITICAL	NTCORPNOTES05	STANDARD	ACTIVE	35	2	NOLIMIT	60
TSMHOSTCORP1.corp.com	STANDARD	NTCORPEXCH05	STANDARD	ACTIVE	1	1	10	30
TSMHOSTREMOTE1.corp.com	CRITICAL	EPAMEXCH01	STANDARD	ACTIVE	35	2	NOLIMIT	60
TSMHOSTREMOTE1.corp.com	CRITICAL	EPAMEXCH02	STANDARD	ACTIVE	35	2	NOLIMIT	60
TSMHOSTREMOTE1.corp.com	CRITICAL	MEXEXCH01	STANDARD	ACTIVE	35	2	NOLIMIT	60
TSMHOSTREMOTE1.corp.com	CRITICAL	MEXEXCH02	STANDARD	ACTIVE	35	2	NOLIMIT	60
TSMHOSTREMOTE1.corp.com	CRITICAL	USEXCH01	STANDARD	ACTIVE	35	2	NOLIMIT	60
TSMHOSTREMOTE1.corp.com	CRITICAL	USEXCH02	STANDARD	ACTIVE	35	2	NOLIMIT	60

Figure 5: Zoned Policy Reports. In this example, one of the policies is defined to only retain one version of the data – if a restore request for a previous version is submitted, the backup team will fail to meet this request, even if backup activity is successful on a nightly basis.

Cost Benefits of Continuous Policy Management

Continuous review and updating on data protection policies can help reduce administrative and capital costs and potentially reduce any costs associated with unplanned downtime due to servers and data being unrecoverable.

Logging on to each backup server to manually verify that policies are configured correctly can be a time consuming effort. With an automated reporting solution policies can be mined on a regular basis for review, and additional reports such as Backup Success and Failure, historical trending, performance and capacity reports can indicate if current policies support the organizations data protection goals. This centralized view and automated collection of critical information helps save administrative time, contributes to better resource management and helps lower overall operational costs.

As storage environments and teams grow the risk of overprotecting assets increases. Clients that are inadvertently included in multiple policies unnecessarily use up network bandwidth and storage media. With centralized visibility across multiple backup servers, clients associated with multiple policies can be quickly identified. Policy reporting can also give visibility into configuration of non-vital clients (such as workstations) easily identifying if their data is being kept longer than necessary taking up valuable storage resources.

Bocada's Occupancy Trending reports (Figure 6) provide unique insight into the total data stored on media and uncovers costly backup policies. Bocada Enterprise occupancy reporting provides a previously very difficult-to-obtain view of how total storage is changing over time. By tracking overall occupancy over time, organizations can measure the impacts of the major cost drivers in backup and storage operations.

These reports enable cost analysis and reduction:

- Identify the most costly backup clients or backup policies in the environment (shown by total data on media)
- Accurately predict the cost of changes to backup configuration, such as increased retention periods
- View trends over time and see the immediate effects of policy changes
- Plan for future growth by viewing changes in storage requirements over time
- Enable accurate use based charge-back models

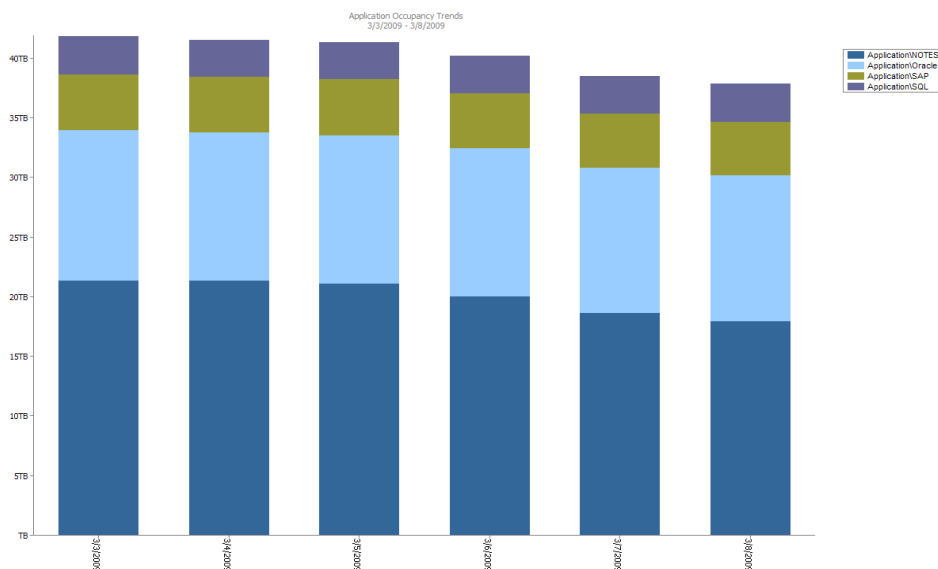


Figure 6: With Occupancy Reporting in Bocada Enterprise, users can quickly determine whether total data storage amounts are trending within expectations, making adjustments to policies for those that are growing unexpectedly.

Summary

An automated reporting solution that can regularly mine policy configuration provides the visibility required for customers to quickly and easily review policies and determine if changes need to be made to meet business goals. Overtime, standardization and diligent policy management can significantly improve on backup SLA success, drive down costs and improve overall data protection results.

Bocada Enterprise provides automated insight and visibility into data protection processes, enabling IT organizations to confidently analyze data recoverability, predict risk vulnerability and identify opportunities for cost reduction. Based on patented, agent-less technology, Bocada solutions deploy rapidly and scale to meet the demands of the largest multi-vendor data protection environments.