Assessment and Recommendations

Prepared for:

Merit Systems Protection Board

Prepared by
Kelyn Professional Services
May 17, 2016

Version 1.0

Version History

Version Number	Revision Date	Contributor's Name	Revision Description
1.0	8/3/2015	(b) (6)	First Draft
1.1	8/12/2015	(b) (6)	Minor revision

Prepared by Kelyn Professional Services

Table of Contents

Introduction

In June 2015, MSPB experienced a catastrophic failure of its VMWare virtual environment. Most of the virtual servers were successfully rebuilt, but one particularly critical virtual server had not had a successful backup, and critical data was lost in this failure. MSPB has requested Kelyn technologies to perform an assessment, assist with configuration and troubleshooting, and recommend changes and improvements to the CommVault environment that will reduce the likelihood of future data loss.

This document records some of the key configuration changes made during the on-site visit. It is also a current state analysis of MSPB's CommVault backup environment, and makes recommendations in accordance with CommVault best practices that will make the backups more robust and increase the likelihood of being able to restore data going forward. This analysis was researched at the MSPB offices Washington DC.

While on site, the Kelyn engineer also assisted the customer in attempting to locate and retrieve lost data that had had expired from backups, but had potentially not been overwritten on tape. Unfortunately, the specific data in question was not in the backup sets that were on tape.

Recommendations and Improvements

Summary of Configuration Changes

While the Kelyn engineer was on-site, certain key configurations were changed. Among them are the following:

Automatic discovery of VMs. The default subclient was configured to automatically discover VMs as they are created and back them up. This will require continual monitoring and removal of VMs where backup is not required.

Modified the schedule for Oracle backups. There was a conflict in the schedule for Oracle backups that was causing a backup job to fail, which in turn was causing data to be retained too long on tapes, so that there were no longer tapes available, and aux copy jobs were not able to run.

According to CommVault best practices, storage policies should be kept to a minimum number, which is determined by retention requirements and location of the libraries. At the start of the engagement, there were seven storage policies. We were able to remove three storage policies that were obsolete, and establish a plan for consolidating the remaining policies into a single policy.

Recommendations for Architectural Improvements

Define requirements for frequency of backups and retention. A business impact analysis (BIA) that includes definition of Recovery Point Objective (RPO) and Recovery Time Objectives (RTO) should be performed to assess the relative importance of data and determine schedule and retention requirements based on RPO and RTO.

Definitions:
RPO - the maximum targeted period in which data might be lost from an IT service due to an incident

RTO - the targeted duration of time within which a business process must be restored after a disruption of service

Based on the RPO and RTO that is established by management retention policy and schedule may need to be adjusted

Retention policy: While the Kelyn engineer was on site, management instructed the backup administrator to change the primary and secondary copies from 4 days 2 cycles to a 14 day and 1 cycle retention. A monthly full backup is retained on tape for 6 months. The primary retention is a much shorter than what is typically seen in backup environments, and restores from more than 14 days may require tapes to be retrieved from offsite. Kelyn recommends that the backup environment be designed so that it most cases short of a disaster, recoveries can be performed from the primary (onsite) copy.

Based on the RPO established by management, the backup schedule could be adjusted from one backup per day for all data, to schedules where backups can be performed multiple times per day for critical servers.

In order to enable quick recovery of data, it is advisable that retention on local disk be adequate in duration that nearly all restore operations can be performed from local disk. Offsite backups should generally be considered an option of last resort in case of a major disaster. Additional data retention will require significant increases in the amount of disk space needed in the disk library unless deduplication is implemented.

Use disks at an offsite data center or a cloud provider for secondary copy instead of using tapes. Tape management and handling is a very time consuming task for backup administrators and adds additional risks to the backup process than can be avoided by performing data replication electronically to an offsite center or a cloud provider. Tapes are notoriously unreliable and fail at a much higher rate than disks. This, coupled with the handling of tapes, moving them in and out of the tape library, moving them to the offsite location, exposes the data to significant risks including loss of data, interception of data, and human error.

Implement CommVault deduplication: Deduplication will drastically decrease the amount of time that it takes to perform backups, reduce the amount of data transferred over and allow storage of multiple backups of a single host while using a significantly reduced of disk space over non-deduplicated

backups. It is a foundation technology that serves as the base for other recommendations: Increase retention on local media agent, and transfer offsite backups to offsite disks or a cloud provider.

The primary backup copy is being written to the same Nutanix hardware as the primary storage for the virtual servers. There is redundancy and replication built into the storage, but in general, separate hardware for the CommVault backup libraries is recommended. This architecture should be reviewed to determine if this single point of failure is putting data at risk.

CommCell Environment Evaluation

Product Release Level

CommCell Service Level: Simpana® V10R2SP11
CommServe: (b) (7)(E)
CommCell: (b) (7)(E)
Observations:
All CommVault components are up-to-date, or at the latest release supported for the operating system.
Remediation:

- **None**

Product Updates

Installed Updates: Service Pack 11
Additional Updates: none
Needed Updates: none
Observations:

- **Up to date**

Remediation:

- **None**

Disaster Recovery Backup Configuration

The Disaster Recovery backup is the crucial element of restoring the CommVault backup environment in case of a failure of CommVault. It backs up the CommVault SQL database that resides on the Commserve server.
Observations:

- **DR backups are written on the commserve server, (b) (7)(E) . Configured to retain the last seven backups**
- **Two additional copies are written to tape using the CommServeDR storage policy**
- **DR backup copies on tape have an infinite retention**

Remediation:

- **DR backups have a short useful life, making the infinite retention unnecessary. The tape copy retention can be reduced and free up most of the tapes that contain DR backups**
- **Confirm that the most recent DR backup tapes are being removed from the tape library and taken offsite weekly.**

Index Cache

Observations:

- Each media agent has an index cache that is located at the following locations:
  (b) (7)(E)
  (b) (7)(E)
  (b) (7)(E)
  (b) (7)(E)

Remediation:

- None

Storage Policy

Observations:

- According to best practices, storage policies should be kept to the minimum number to meet retention requirements. At the beginning of the engagement, there were seven storage policies, we were able to remove three, and advised the backup administrator to consolidate the four remaining storage policy into a single storage policy.

Remediation:

- Reduce storage policies to the minimum to meet retention requirements. Since all backups require the same number of days of retention, all of the hosts that are backing up should be configured to use the same storage policy. Two of the storage policies, one for full backups, and one for incrementals were recently created using new disk, while two of the storage policies are using the older disk. All subclients should be changed so that they are associated (both full and incremental backups) with one of the new storage policies. The storage policy can then be renamed to accurately describe its purpose.

Observations:

- **Subclients are set up to contain servers according to their business function.**
- **Automatic discovery of new virtual servers was enabled during the course of this assessment.**

Remediation:

- Continue to monitor automatic discovery of VMs

CommVault Customer Support Hotline

For a list of all Global Technical Support Hotline numbers please click on the following link:

CommVault Support	Telephone Support – phone 1-877-780-3077 In order to open a case with support, you will need to provide your commcell ID: (b) (7)(E)

CommVault Web Support

Access the Maintenance Advantage Customer Support Portal at the following link:

Maintenance Advantage	http://ma.commvault.com
Documentation	http://documentation.commvault.com

Please be aware that critical calls cannot be opened on the Web and will need to be called in to the Support Hotline. To increase the severity of an incident contact the Customer Support Hotline.

