

CommVault Consulting Services

Wellness Assessment

Prepared for

${CustomerName}



Version 1.0

${ReportDate}

**Version History**

| Version Number | Revision Date | Contributor’s Name | Revision Description |
| --- | --- | --- | --- |
| 1.0 |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1 Executive Summary 4](#_Toc354652606)

[1.1 High Level Wellness Assessment Findings 4](#_Toc354652607)

[1.2 Summary of Recommendations 5](#_Toc354652608)

[2 Wellness Assessment Description 6](#_Toc354652609)

[2.1 Onsite Objectives 6](#_Toc354652610)

[2.2 Summary of Findings and Recommendations 7](#_Toc354652611)

[3 Action PLan and Roadmap 9](#_Toc354652612)

[3.1 Prioritized Action Plan 9](#_Toc354652613)

[3.2 Roadmap 10](#_Toc354652614)

[4 Detailed Findings/Analysis 11](#_Toc354652615)

[4.1 CommCell Review 11](#_Toc354652616)

[4.1.1 Product Release Level: 11](#_Toc354652617)

[4.1.2 Product Updates: 11](#_Toc354652618)

[4.1.3 DR Backup Configuration 11](#_Toc354652619)

[4.1.4 DR CommServe 12](#_Toc354652620)

[4.2 Application Review 13](#_Toc354652621)

[4.2.1 Windows File Systems: 14](#_Toc354652622)

[4.2.2 Virtual SeRver Backups: 14](#_Toc354652623)

[4.3 Storage Policy Configuration Review 14](#_Toc354652624)

[4.3.1 Shared Index Cache: 14](#_Toc354652625)

[4.3.2 DE-DUPLICATION Storage Policy Review 15](#_Toc354652626)

[4.4 Scalability Review 16](#_Toc354652627)

[4.4.1 Reporting 16](#_Toc354652628)

[4.4.2 Common Technology Engine 17](#_Toc354652629)

[4.4.3 Building Blocks 17](#_Toc354652630)

[4.4.4 Deduplication Node 20](#_Toc354652631)

[5 Remediation Plan 23](#_Toc354652632)

[5.1 VMWare Data Protection and SnapProtect 23](#_Toc354652633)

[5.2 ${CustomerName} Staffing Estimate 25](#_Toc354652634)

# Executive Summary

This report is the result of CommVault’s Wellness Assessment performed for ${CustomerName} CommVault® Singular Information Management™ environment located in ${ProductLocation}. As part of the Wellness Assessment, CommVault conducted an onsite workshop session to assist ${CustomerName} in assessing their operational performance of the CommVault solution. Each software product is examined for proper installation, operation, and performance in accordance with established CommVault Systems standards, policies, and procedures.

## High Level Wellness Assessment Findings

In general, standard Wellness Assessment parameters show that ${CustomerName} is operating within many of the best practice thresholds. However there are some specific areas that could benefit from certain modifications. The thresholds areas are summarized here:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **#PLACEHOLDER#**   |  |  |  |  | | --- | --- | --- | --- | | Parameter | Status | Outcome | Remarks | | #Parameter# | #Status# | #Outcome# | #Remarks# | |

## Summary of Recommendations

Based on the interviews and data provided by ${CustomerName}, an action plan and recommendations were created to address their specific stated issues and goals during the onsite workshop. The summary of recommendations is below by importance and suggested timeline:

|  |  |  |
| --- | --- | --- |
| **Observation** | **Impact** | **Timeline** |
| 1. ${RedObserv} | 1. ${RedImpact} | * Immediately |
| 1. ${YellowObserv} | 1. ${YellowImpact} | * Within the next 3 months |
| 1. ${GreenObserv} | 1. ${GreenImpact} | * Within the next 6 months |

Please refer to section 4 for details on each of these recommendations.

# Wellness Assessment Description

The CommVault Wellness Assessment is a current state analysis designed to ensure the CommVault solution is optimized to meet the business requirements. Performance levels, scheduling, retention requirements, and media usage are reviewed to verify an efficient design.

## Onsite Objectives

CommVault performed a CommVault Wellness Assessment at the facility located in ${ProductLocation} on ${EvaluationPeriod}. CommVault collected current-state data of the existing server and network infrastructure, applications, data distribution, and retention requirements. From this collected information, the CommVault and ${CustomerName} staff worked together to analyze the CommVault infrastructure including:

|  |  |
| --- | --- |
| Area Addressed | Explanation |
| Operational Issues Assessment | Analysis of current state performance and configuration to compare with desired business and technical goals. |
| Inventory & Compatibility Review | A review of software and firmware release levels validated against minimum CommVault and third-party requirements. |
| CommCell Review | A validation of the CommCell configuration (including ER Backup, Security, Critical Events, Logging, etc.). If required, Critical Events and persistent technical issues will be escalated. |
| Applications Review | An analysis of data protection requirements for applications in the environment to validate configuration (i.e. iDataAgents, Backup Sets, Subclients, etc.). Where needed, recommendations will be provided to achieve required business and technical goals. |
| Configuration Review | A review of Storage Policies to verify schedule configuration and media management objectives (i.e. media usage and efficiency, daily exports, etc.). Where applicable, best-practice recommendations on policy configuration, scheduling, media management and usage will be provided. |
| Operational Review | An overall review of backup/restore successes, failures, root-causes, and exceeding data protection windows (i.e. licensing, GridStor, installed components, etc.) to be able to grow the system while avoiding/eliminating serious performance degradation issues. |
| Procedural/Operational Validation | An analysis of existing and applicable reports and configuration data. Recommendations will be provided on operational monitoring processes, alerting mechanisms, and overall media management. |
| Scalability Review | A performance and load analysis of the hardware, network, and MediaAgent configuration(s). The environment is validated against CommVault Systems’ developed Scalability and Sizing Guidelines for Workgroup, Enterprise and DataCenter deployments. Review scalability and sizing requirements with respect to current state of operations and projected data and server system growth. Where applicable, proactive recommendations are provided on anticipated changes to the environment |

## Summary of Findings and Recommendations

Overall ${CustomerName}’s CommVault backup environment is providing data protection operations well. Backups are being completed successfully for ${PlatformListOne}

The total weekly amount of data backed up by CommVault is ${tweekbkdtamt} in size. The following figures show backup data details according to agent types.

**Full Backups (Total Jobs)**

**Full Backup Data Per Week(Application Size in GB)**

**Full Backup Data Percentage (6 Week Average of Application Data)**

# Action PLan and Roadmap

Based on the observations and recommendations above, CommVault has created a prioritized action plan and roadmap to allow ${CustomerName} to methodically schedule changes and improvements to the environment well in advance. This action plan and roadmap should be used as a guideline for improving and optimizing the CommVault data management software over the next ${OptimizingTime} years.

## Prioritized Action Plan

The Prioritized Action Plan listed below identifies suggestions ranked by priority which should be addressed by the ${CustomerName} team. These suggestions range from immediate ad-hoc changes to long term reconfigurations which would be changed over the course of the year.

|  |  |
| --- | --- |
| **Action Plan Summary - Configuration Recommendations** | **Priority** |
| #APSConfigRecomm# | #APSPriority# |

## Roadmap

Following the action plan, CommVault has created a roadmap to outline estimated durations and recommended start times to roll out the suggestions above. This roadmap allows the ${CustomerName} team to adequately schedule resources, procure additional hardware or augment with internal or CommVault PS staff (if needed).

# Detailed Findings/Analysis

${CustomerName} has asked for CommVault’s input on the overall health of the CommVault data management software implementation in their location. During early discussions it was discovered efficiency, simplicity, and stability would be keys to ${CustomerName}’s success. Reorganizing existing servers and applications in a more consolidated environment to be protected by the CommVault® Singular Information Management™ software suite, creating a scalable solution for the future is a must. After working with ${CustomerName},CommVault offers the following recommendations for ${CustomerName}’s use during and after the completion of this effort.

## CommCell Review

The following section provides detailed analysis and recommendations

### Product Release Level:

CommCell is utilizing ${ProductBuild}

* CommServe: **${CSID}**
* CommCell: **${CCID}**

### Product Updates:

Installed Updates: ${UpdateDetails}

Additional Updates: ${AddtnlUpdateDetails}

Needs updates: ${NeededUpdates}

|  |  |  |
| --- | --- | --- |
| **#TypeofNode#**   |  |  | | --- | --- | | #Status# | #Count# | |

It is typically best practice not to schedule automatic updates in environments that have established change control processes in place since automatic updates applies updates to CommVault services on the associated clients. The majority of larger corporate environments manually initiate updates to the CommCell environment during approved maintenance windows on high priority production systems.

### DR Backup Configuration

${LastSuccessfulDR}. The DR backup occurs in two phases. In Phase I, the backup is written in file format for ready use in case of a DR event. ${DRBkpConfig}.

### DR CommServe

It is recommended to have a DR CommServe at a remote DR site that can be used to quickly recover a DR backup set from the production CommServe. ${CustomerName} does have a DR CommServe. The DR CommServe’s services are not required to be running. However it’s required to apply the current CommVault patch level to the DR CommServe when it is used for recovery. This is to avert any issue that could occur between patch levels between the two CommServe servers.

If the DR CommServe is brought online to perform production backups for a period of time in case the primary CommServe is offline for an extended period of time, a DR backup set from the DR CommServe should be recovered on the primary CommServe in order to reverse roles back to normal.

## Application Review

The following section provides analysis of data protection requirements for applications in the environment to validate configuration (i.e. iDataAgents, BackupSets, Subclients, etc.). Actual data protection will be validated against established data protection operations. Where needed, recommendations will be provided to achieve required business and technical goals.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Backup Size of 6 weeks** | | **Percentage** | |
| **Agent** | **Average Weekly Full (GB)** | **Average Weekly Inc (GB)** | **Weekly % Change** | **% of Total Full Backups** |
| #Agent# | #AWF# | #AWI# | #PWC# | #PTFB# |

### Windows File Systems:

${WinFSReview}

### Virtual SeRver Backups:

${VSBkpReview}

## Storage Policy Configuration Review

The following section analyzes the configuration of the storage policies and provides details in support of the recommendations throughout this document.

### Shared Index Cache:

${SharedIndexCache}

### DE-DUPLICATION Storage Policy Review

${StgPolicyReviewSum}

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Storage Policy | DB Store | Storage Policy Copy | Size of Application | Size after Deduplication | Baseline Size |
| ***#SPRPolicy#*** | ***#SPRDBStore#*** | ***#SPRPolicyCpy#*** | ***#SPRSize#*** | ***#SPRSizeD#*** | ***#SPRBSize#*** |

## Scalability Review

In conversations with ${CustomerName}, the team discussed implementing a scalable architecture and ways to report and track capacity and performance. It’s imperative that you maintain and grow your software infrastructure to accommodate your rapidly growing data. Customers who do not manage their growth will eventually exceed their ability to protect and manage their data, which quickly leads to higher error rates, insufficient backup resources, and ultimately risk of data loss.

Scaling your software environment is an ongoing and necessary activity to maintain a stable growing environment. There are several tools and factors to consider when evaluating your need to increase resources which we will go into detail including:

* Available console reports and thresholds
* CommNet reporting
* CommServe Requirements
* Building Block Scaling
* Deduplication Scaling

These scalability topics will be discussed in detail with recommendations for ${CustomerName}. This section will provide ${CustomerName} the fundamental methods and approaches to track and trend the need for increasing capacity and performance, as well as outline the general principles for corrective scaling activities necessary in any growing and maintaining a healthy environment.

CommVault software modules share a common set of backend services and advanced capabilities that effortlessly “talk” to one another through the common platform. While other solutions typically consist of fragmented and expensive third-party tools, this truly unified, or “singular,” architecture performs all data management functions quickly, easily, and reliably from a single console. Data is managed and optionally content indexed into a single virtual pool that can be viewed across all applications, platforms, devices, and locations.

### Reporting

**Console Reporting**

* **DR Backup Reporting** – Reports on success of DR backups to insure the CommServe Database is protected. It is fundamental that the DR database be protected as the overall site and backup information is maintained in the CommServe Database. Failure to backup can prevent the system from being recovered in the case of a DR event.
* **Daily Job Summary** – Provides daily job details for overnight backups. Reports can be generated for specific servers or agent types so that specific application groups can have reports focused on their specific backup jobs.
* **Disk Library Alerts** – Alerts on insufficient disk or tape library capacity and can be configured to escalate alerting if the problem persists beyond a defined checkpoint. Alerting can also be configured to alert if tape or disk mount paths are offline that may need to be addressed.

**CommNet Reporting**

* **SLA (Service Level Agreement) Report** – Quickly identifies what servers are not meeting specific backup requirements. Servers that do not meet defined criteria are highlighted to identify those that need to be addressed. SLA reports also provide a success rate for the overall environment. Thresholds are configured to require a number of full and incremental backups within a number of days. The number of allowable missed backups for an individual client is permissible depending upon the nature of the client.
* **Data Growth Reporting** – Provides trend reporting over monthly and/or weekly time frames to monitor backup data growth and to identify any unexpected data growth.
* **Disk Library Performance Reporting** – Provides benchmark metrics on the amount of data being processed for each of the disk library mount paths. This data can be used to ensure data load is balanced or if there are performance bottlenecks in the system.

### Common Technology Engine

**CommServe –** Within a CommCell (logical boundary of CommVault services), the CommServe is the central host that maintains the core configuration and management for all entities. The CommServe SQL database resident on the CommCell contains all configuration information for media libraries, client configuration, schedule and storage policies, user and group security, job information, and many other details about the environment. The CommServe is the host through which users will access the CommCell GUI. This GUI can be accessed directly via Remote Desktop or via a Web Console from anywhere that has IP connectivity to the CommServe.

One CommServe can support up to 5,000 Clients, control up to 1,200 concurrent job streams, and manage up to 50 simultaneous Console GUI connections. CommServe management communication does not require fast local Ethernet connection. The Java web-based GUI could be effectively used through slower WAN communications for CommCell administration.

**CommServe Requirements**

* Windows 2008 R2
* 2-Socket Quad Core CPU
* 32GB for 5,000 clients
* 1Gb Ethernet NIC

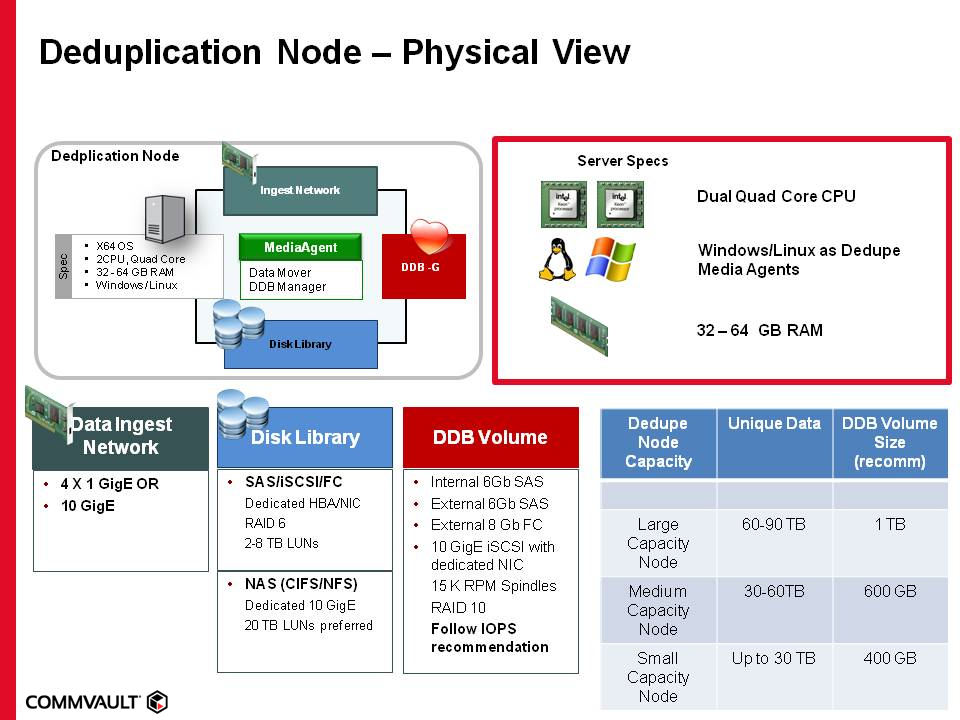
### Building Blocks

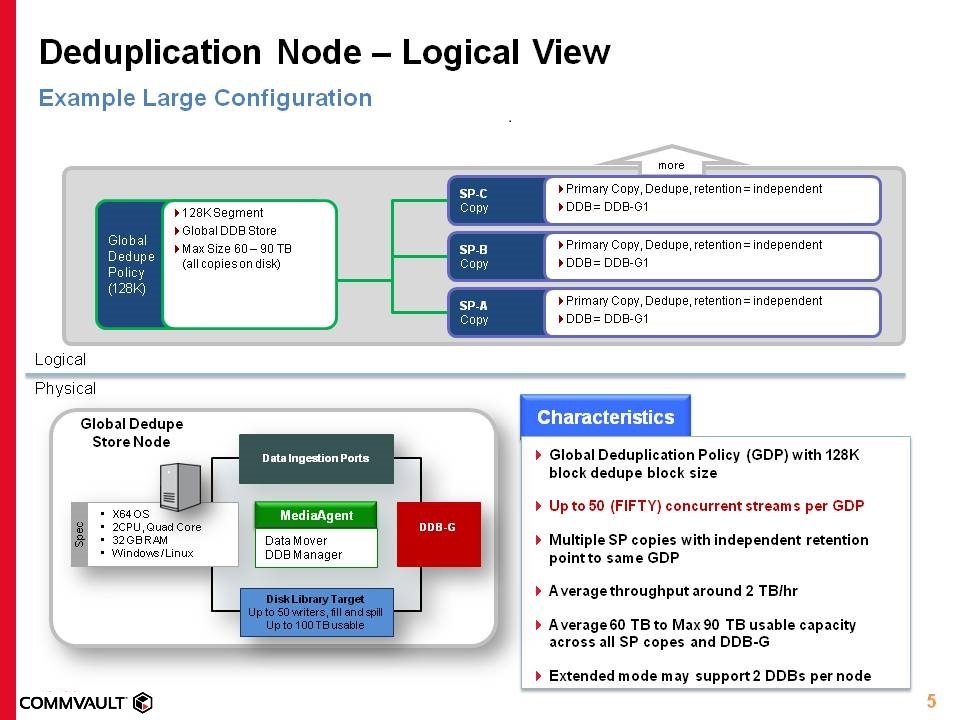
A Building Block is CommVault’s modular approach to data management. One Building Block consists of three Media Agents (Building Block Nodes) in a GridStor configuration. Each Node has an equal amount of disk storage presented to the Media Agent.

A single Building Block is capable of managing 3 deduplication stores with a single DDB per Media Agent. Each deduplication store facilitates up 90TB of backend storage. The amount of application data covered by one deduplication store depends on the type of data. Assuming a conservative deduplication ratio, 5% weekly change rate, and 1 month retention with a standard daily incremental and weekly full backup schedule, one Building Block is capable of protecting and retaining up to 210TB of front-end filesystem data, 360TB of messaging data or more than 400TB of database data and will vary depending on the level deduplication. Each Building Block also provides processing throughput over the network of approximately 6 TB/hr (2TB/hr per node).

The Building Block design is comprised of two layers; the physical layer and logical layer. The physical layer is the actual hardware specification and configuration.

The Physical Layer comprises the server(s), networking, and storage hardware of the CommVault deduplication solution. The logical layer is the CommCell configuration that overlays that hardware layer.





**Deduplication** –The deduplication engine utilizes a multi-threaded C-Tree server mode database. One DDB has a recommended maximum of 50 concurrent connections or streams. Any configuration above 50 concurrent DDB connections will have a negative impact to the Building Block performance and scalability.

Each Media Agent in a Building Block has one DDB to backup production data and may optionally host a second DDB as a target for DASH Copy data. Usually DASH Copy data traverses through slower WAN connections and generates much lower workload for the second DDB.

It is a CommVault best practice to configure Deduplication Storage Policy block sizes at a minimum of 128K. This setting represents the block size that the data stream is cut up into. Enhancements have been made to eliminate the need for Storage Policies per data type. Any block from 16 k to the configured block size will automatically be hashed and checked into the deduplication database. This eliminates the complexity of multiple storage policies per data type.

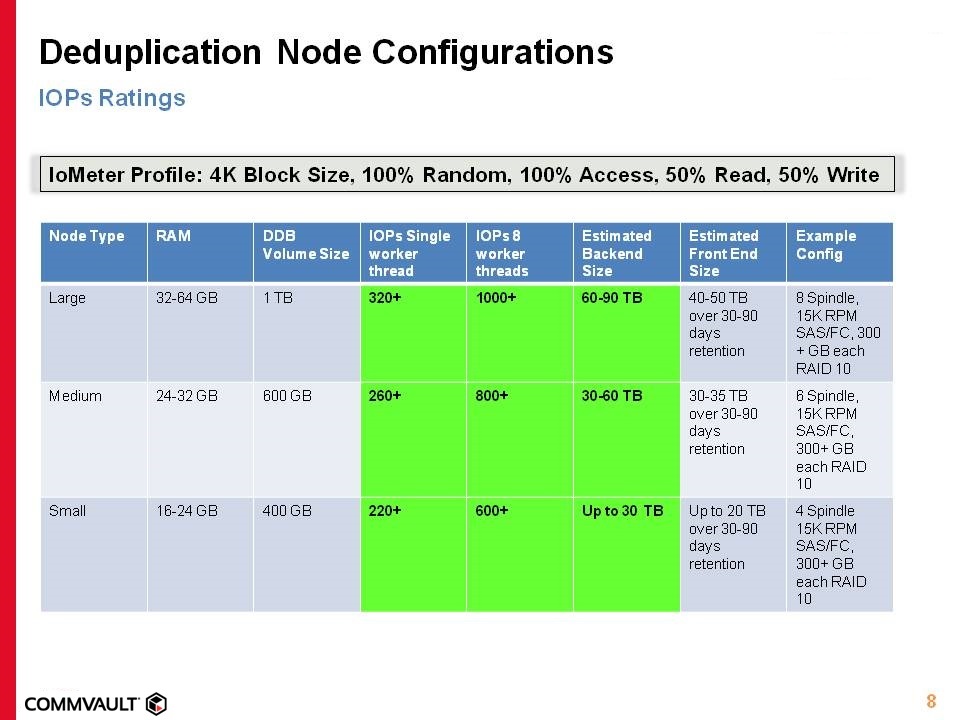
Performance of the DDB LUN is paramount and does not require RAID protection. The DDB is protected by one of two methods: a recovery point creation or a DDB backup process.

The DDB recovery point is a copy of the active DDB. This copy is used to rebuild the DDB in the event of failure. When the recovery point process is initiated all communication to the active DDB is paused. The information in memory is committed to disk to ensure the DDB is in a quiesced state. The DDB is then copied from the active location to the backup location. After a DDB has been backed up successfully the previous recovery point is deleted. All communication to the DDB is then resumed. The DDB recovery point location will require two times the size of the active DDB. This allows for the existing recovery point and the working space for the DDB recovery point in progress.

The DDB backup process uses roughly the same process to protect the DDB as the recovery point creation, but will perform the backup job to a configured Storage Policy. The job should be scheduled when there is little activity in the CommCell. In order to use DDB backup job method, a non-dedupe Storage Policy has to be created and associated with this job.

### Deduplication Node

The CommVault Media Agent Server that runs and hosts the Deduplication Engine and Store – is categorized by three capacity types to support different sized deduplication environments. Small, Medium and Large Capacity Dedupe Nodes can support up to 30 TB, 60 TB and 90 TB of ‘UNIQUE’ data – that is the data stored after Deduplication, respectively.



Each Deduplication Database (“DDB”) store has a recommended maximum of 50 concurrent backup/DASH copy streams. This is the total number of backup or DASH copy streams that concurrently access the Deduplication store.

**DDB Store** –At a minimum, 15K SAS Spindles are recommended to host the DDB store. Hardware RAID is recommended for redundancy across the dedicated LUN used to host each DDB store. All RAID configurations are supported assuming the recommended IOPs – Input Output Operations per second for the DDB can be achieved. If the DDB resides on Virtualized Storage (${VSexample}), ensure that the IOPs rating stays consistent and is not affected by the varying amounts of load on the Disk Array. The same requirement exists for SAN-based storage where a single RAID set may be accessed by multiple applications each reading from and writing to a common high speed LUN.

SSD disks are supported as long as Enterprise- class SSD disks are used in combination with RAID for redundancy.

For optimal performance, make sure a dedicated volume is configured on Media Agent for page file on Windows or swap space on Linux. This volume should be at least two times the amount of RAM on the system.

**Media Agents** –Media Agents within a CommCell are primarily responsible for all data movement. All backup, archive, and SnapProtect operations must move from a client through a Media Agent to storage. Media Agents are powerful and flexible hosts that can deployed in various ways to meet the varied needs within any modern enterprise. Media Agents can be dedicated hosts that perform nothing but CommVault related operations or they can be installed on an application server to allow for LAN-free backup operations. Media Agents can also be configured as virtual hosts in order to support data protection operations of enterprise virtual infrastructures.

***Recommendations:***

* + Each Media Agent acts as an equal partner in a Building Block.
  + Each Media Agent should have four 1Gbps interfaces connected to the client network. Four network interfaces configured as a 4Gbps aggregated link is a preferred method for Media Agent’s network connectivity.
  + Direct-attached local storage should be equally divided between all Media Agents in a Building Block. SATA spindles should be configured in RAID5 groups with not more than 7 spindles per one RAID5 group. For better performance and reliability, RAID groups should be created using spindles from different disk trays. Each RAID group should be carved into LUNs from 4 to 8 TB in size. Each LUN should be presented as one volume to the Media Agent. Each volume should have one partition with NTFS file system formatted with 64KB Block Size.
* It is recommended to use a Shared Index cache on NAS storage within ${CustomerName} environment. This has already been implemented.

**Disk Library** –A Disk Library is a logical entity representing disk storage where the backup data resides. A Disk Library consists of a number of disk mount paths combined together in one logical structure. Each mount path represents a logical disk device associated with a physical storage location. Disk devices can be local, SAN, iSCSI, or network attached storage (CIFS/NFS).

During restores and DASH copies, there is no intermediate communication between Media Agents. In direct attached, all communication must pass through the hosting Media Agent in order to service the DASH copy or restore. Backup activities are not affected by the mount path choice.

Each Media Agent should have no more than 50 writers across all the mount paths. A Media Agent with 10- 2 TB mount paths (20 TB of raw capacity) would have 5 writers per mount path. The purpose behind this is to evenly distribute the load across all mount paths and to ensure the number of concurrent connections to the DDB remains under the 50 connection limit.

Regardless of the type of disk being used, SAN or NAS, the configuration is the same. The Disk Library consists of disk devices that point to the location of the Disk Library folders. Each disk device will have a read/write path and a read only path. The read/write path is for the Media Agent controlling the mount path to perform backup. The read only path is for the alternate Media Agent to be able to read the data from the host Media Agent. This is to allow for restores or aux copy operations while the local Media Agent is busy.

**Global Deduplication** –A Global Deduplication Storage Policy (GDSP) introduces the concept of a common deduplication store that can be shared by multiple Storage Policy copies (Primary or DASH) to provide one large global deduplication store. Each Storage Policy copy defines its own retention rules. However, all participating Storage Policy copies share a common DDB, dedupe block size, and data paths.

A GDSP should be and is being used at ${CustomerName} instead of standard deduplication storage policies whenever possible. A GDSP allows for multiple standard deduplication policies to be associated to it allowing for global deduplication across all associated clients.

# Remediation Plan

In order to address the findings noted above, it is imperative to have a clear understanding of the path from current to future state. This section of the document will ensure that the transition from the current state to the future state is properly described and sufficient detailed will be provided to ensure that all parties are aware of the steps involved in the remediation effort to address all High or Medium priority items noted above. Additional information will be included regarding optional remediation steps that were listed as Low priority in the detailed findings above.

## VMWare Data Protection and SnapProtect

Traditionally, virtual guest hosts have been protected using traditional backup agents. While completely functional, this approach does not scale as well as would be expected. While agents within guest hosts may provide certain granular recovery options, it is not the most efficient method by which to protect the data contained within. The Virtual Server Agent leverages the data protection APIs available within the virtualization platform to enable a highly efficient and scalable data protection method for virtual environments. The Virtual Server Agent can be paired with SnapProtect, where appropriate, to greatly enhance the performance, scalability and flexibility of the virtual data protection scheme.

*VMware*  
VMware data protection operations are enhanced through vStorage APIs for Data Protection (VADP) which is a set of interfaces made available by VMware to allow for centralized, efficient, off-host, and LAN-free backups of vSphere virtual machines. By leveraging VADP CommVault can protect vSphere virtual machines from a central backup server or virtual machine without requiring the installation of backup agents or requiring backup processing to be done inside each virtual machine. This offloads backup processing from ESX hosts and reduces costs by allowing each ESX host to manage more virtual machines without concern for the impact of data protection operations.

CommVault, with its enhanced protection of virtual environments using our Virtual Server Agent (VSA), can greatly reduce the administrative load associated with protecting a dynamic virtual environment. With automatic discovery of virtual machines, you can be assured of complete protection across the virtual environment. Our tight integration with VMware and VADP ensures consistent protection of the individual virtual machines. Recovery operations in a virtual environment are also simplified. A virtual machine can be restored in its entirety in a single step process without the need to rebuild the client prior to performing the recovery.

CommVault leverages VADP which has the ability to use the snapshot capabilities of VMware vStorage VMFS to enable backups across the SAN without requiring downtime for virtual machines. As a result, backups can be performed non-disruptively at any time of the day thereby avoiding extended backup windows and downtime to applications and users.

In addition to VADP integration, CommVault can leverage SnapProtect to enable an even more scalable solution. SnapProtect does not perform a streaming backup at the time of job execution from the virtual machine. Instead, the Virtual Server Agent with SnapProtect integration will call vCenter or the ESX hosts directly to quiesce the virtual machines. When the virtual machines are in a consistent state, CommVault then contacts the configured array to generate a hardware-based snapshot within the storage array. During this snapshot process, all virtual machines remain online. Once the snapshot process is completed the virtual machines resumes activities as usual.

***Recommendation:***

* Virtual Server clusters will be protected using a distributed MediaAgent scheme. This will provide complete coverage while limiting access to ESX datastores from the Virtual Server Proxy hosts.
* SnapProtect should be used to protect all VMWare clients within the enterprise.
  + Validate that all hardware level snap licenses have been acquired and that all hardware arrays are listed within the CommVault Hardware Compatibility List
* VADP SAN Mode will be used to limit the amount of data that must traverse the network during protection and restore operations.
* Deduplication and Compression will be enabled on all Virtual Server Agent subclients
* DataStore affinity will be used to manage protection of VMWare clients.
* Datastores with VMWare guests can be associated with disabled subclients.
* For VM Guests that have application data contained within that cannot be protected at the ESX level, an iDataAgent will be needed within the Guest to fully protect the Virtual Guest.
* In the case of a VM Guest that experiences high IO during protection operations, which could prevent ESX from quiescing the VM Guest, an iDataAgent will need to be deployed to those VM Guests. These will be identified as rollout of the Virtual Server agent is underway. A pre-check of guest CPU metrics within VirtualCenter may be able to provide insight into which hosts are not able to be quiesced through ESX.

## ${CustomerName} Staffing Estimate

${StaffEst}