As cloud adoption continues to rise, so has the demand from Service Providers for software products that support their multi-tenant business model. However, multi-tenancy is a broad concept that may have different meanings depending on the practitioner and his/her particular use case.

COMMVAULT CLOUD SOLUTIONS GROUP
Wednesday, October 22, 2014
## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>COMMVAULT SIMPANA® SOFTWARE BENEFITS FOR SERVICE PROVIDERS</td>
<td>1</td>
</tr>
<tr>
<td>MANAGEMENT SERVER</td>
<td>2</td>
</tr>
<tr>
<td>USER MANAGEMENT</td>
<td>2</td>
</tr>
<tr>
<td>Clients</td>
<td>3</td>
</tr>
<tr>
<td>Client Computer Groups</td>
<td>3</td>
</tr>
<tr>
<td>POLICIES</td>
<td>4</td>
</tr>
<tr>
<td>Storage Policy</td>
<td>4</td>
</tr>
<tr>
<td>Schedule Policy</td>
<td>4</td>
</tr>
<tr>
<td>DATA MOVER</td>
<td>5</td>
</tr>
<tr>
<td>NETWORKING</td>
<td>6</td>
</tr>
<tr>
<td>Proxies</td>
<td>6</td>
</tr>
<tr>
<td>Firewalls</td>
<td>7</td>
</tr>
<tr>
<td>Network Bandwidth</td>
<td>7</td>
</tr>
<tr>
<td>Encryption</td>
<td>7</td>
</tr>
<tr>
<td>REPORTING</td>
<td>8</td>
</tr>
<tr>
<td>GRAPHICAL USER INTERFACE (GUI)</td>
<td>8</td>
</tr>
<tr>
<td>SECURITY</td>
<td>9</td>
</tr>
<tr>
<td>Client Owner</td>
<td>9</td>
</tr>
<tr>
<td>Enabling Privacy</td>
<td>9</td>
</tr>
<tr>
<td>Data Level Security</td>
<td>9</td>
</tr>
<tr>
<td>APPENDIX: TERMINOLOGY</td>
<td>11</td>
</tr>
</tbody>
</table>
INTRODUCTION

As cloud adoption continues to rise, so has the demand from Service Providers for software products that support their multi-tenant business model. However, multi-tenancy is a broad concept that may have different meanings depending on the practitioner and his/her particular use case. Today, multi-tenancy is not a simple yes or no checkbox item. At CommVault, we believe multi-tenancy is a deep technical topic worthy of a detailed conversation. This whitepaper will discuss multi-tenancy taxonomy for data management and its implementation. In addition it will cover the following topics:

- Management Server
- User Management
- Policies
- Data Mover
- Network (Proxies, Firewall, & Bandwidth)
- Security
- Reporting
- Graphical User Interface (GUI)

CommVault provides a robust and feature-rich data management solution which enables multi-tenancy through a single software platform, enhanced through many years of direct feedback from our Service Provider customers.

COMMVAULT SIMPANA® SOFTWARE BENEFITS FOR SERVICE PROVIDERS

- **Lower Infrastructure Costs** – Simpana® software’s singular platform shares heterogeneous storage infrastructure across backup, archive and replication managed from a single console.

- **Add New Revenue Streams** – Simpana® software’s modular product offering allows you to implement your backup solution first, then add functionality to address disaster recovery, archiving and e-Discovery over time, scaling up to thousands of servers, without having to deploy additional software products.

- **Improve Operational Efficiency** – Enterprise-class, multi-tenant architecture offers built-in data compression and deduplication across backup and archive data copies, to increase performance and infrastructure efficiency.

- **Rapidly Scale** – Simpana® software grows with your business. With Simpana software, a solution can start small, then scale out to match your growth without major re-design.

- **Increase Productivity** – Workflow automation, reporting tools, and self-service features reduce staff time spent on manual tasks, while increasing visibility into operations.

- **Flexible Commercial Models** – Single monthly payment for software, maintenance and customer support based on usage or traditional purchase models available.
TAXONOMY

When speaking with Service Providers, multi-tenancy is an extremely high priority feature. However, we found most providers do not all have a consistent definition of multi-tenancy. Simply put, CommVault defines multi-tenancy as the secure separation and management of shared resources between defined entities. When dissecting multi-tenancy for data management, CommVault believes there are eight areas that make a solution multi-tenant:

- Management Server
- User Management
- Policies
- Data Mover
- Network (Proxies, Firewall, & Bandwidth)
- Security
- Reporting
- Graphical User Interface (GUI)

CommVault Simpana® software is a top data management software that provides multi-tenancy for each area in a single platform. The following sections within the whitepaper will describe in detail Simpana software’s multi-tenancy features specific for Service Providers.

MANAGEMENT SERVER

In the deployment of CommVault Simpana® software, the CommServe® is the central management server. Simpana software can isolate and logically manage tenants separately within the same CommServe regardless of whether the configuration of underlying components are shared or dedicated. For example, some tenants may require having dedicated data movers (known as MediaAgents) or storage, whereas other tenants may utilize a shared environment. Simpana software can manage any of the examples referenced above within a single CommServe. For a Service Provider, that means not having to deploy and manage multiple CommServes to satisfy most tenants’ needs. Service Providers only need to install multiple CommServes if the tenant requires a completely physically isolated data management instance or has to manage more than 20,000 clients.

USER MANAGEMENT

At Simpana software’s core, multi-tenancy is enabled through its robust implementation of Role Based Access Control (RBAC) as part of its overall security framework. Simply put, multiple users can access the platform without any knowledge of each other or access to each others’ data. Managing individual user permissions may be acceptable for some individual enterprises. However, for Service Providers, this would quickly become unmanageable. Therefore, Simpana software
has created the concept of roles with a common set of attributes and permissions. Service Providers can create two categories of roles which are described as follows:

- **Service Provider roles** – reserved for service provider administrative staff and created to manage the overall service across all customers.
- **Customer or Entity roles** – designated to consumers of the service with common local data permission, however restricted to their own data.

Typical roles restrict functional tasks such as backup and restore (including locations), as well as access to reporting or deletion of protected data. For a full list of capabilities and permitted actions (otherwise known as permissions) descriptions, refer to:

CommVault Simpana® Software User Capabilities and Permitted Actions: [documentation.commvault.com](http://documentation.commvault.com)

CommVault Simpana® Software Capabilities and Permitted Actions by Feature: [documentation.commvault.com](http://documentation.commvault.com)

**Clients**
The end-user controlled laptops, servers, or virtual machines that require protection are designated as clients within Simpana software. Agents are modules installed on clients to protect a specific type of data such as the file system, database, or application. During agent installation, each agent is issued a SSL certificate by the CommServe. Using certificate based authentication is believed to be more secure than username-password based authentication (used by most of CommVault’s competitors), which is subject to “spoofing” and potential data breaches.

**Client Computer Groups**
The power of Client Computer Groups provides the Service Provider administrator the flexibility to group resources by a multitude of parameters. Groups can be automatically updated with new or existing clients meeting the designated criteria, known as Smart Client Computer Groups. The use of Smart Client Computer Groups can reduce administration tasks for Service Providers by automating these assignments using pre-defined rules. Typical Client Computer Group use cases for Service Providers are:

- Customers
- Service plan
- Waiting room for new, but unauthorized client
- Hostname
- Operating system
- Network configuration (IP address or firewall rules)
- Installed application or agent

To view a full listing of rules that can be set for Smart Computer Group, refer to: [documentation.commvault.com](http://documentation.commvault.com)
POLICIES

For Service Providers, performing data management tasks for the entire environment at an individual user or single tenant level would quickly become unmanageable. Therefore using an automated, policy-based approach is critical for efficient operations. Simpana software has two types of policies that can be applied with detailed granularity, or applied broadly for rapid changes:

- **Storage Policy** – defines where backup or archive data will reside, number of copies of data, and how long data should be retained
- **Schedule Policy** – defines when data management tasks should be protected

**Storage Policy**

Storage Policy directs data and its secondary copies to a specified storage target, sets the level of protection, and defines the retention period. Storage Policies can segment data into public or private categories, which provides flexible deployment options for service offerings to the service provider. Through the use of Storage Policies, storage targets can be shared across some tenants in order to reduce service costs, whereas dedicated storage can be deployed for some tenants due to privacy or other requirements. Both examples can be provided within a single instance of the Simpana software platform. CommVault’s multi-tenancy features are further differentiated by the granularity with which Storage Policies can be associated, such as by:

- Tenant
- Sub-tenant
- Service plan
- Application group
- Data type

Each of the Storage Policy association examples can be specified and applied at the Client Computer level (usually a tenant), which reduces the overall administration burden. Storage Policies can even be associated to a sub-client (more commonly known as a partial set of data) to address specific customer requests.

**Schedule Policy**

Maximizing resource utilization is important to Service Providers, and Simpana software can intelligently schedule jobs to keep resources at top utilization while achieving data protection objectives. CommVault provides the ability to set the timing of a job to start, which in most cases is a data protection job (such as backup or archiving).
Some common examples of Schedule Policies include:

- **Time Slot** – a specified window of time when a job must start
- **Start Time** – an exact time for the job to begin

Commonly, tenants will request a specific start time (or window) when jobs should start. Schedule Policies enable Service Providers to offer these as options to their tenants, often as a service enhancement or upsell feature.

Similar to Storage Policies, Schedule Policies can be associated at a very granular level depending on the Service Provider’s offerings and tenants’ demands:

- Tenant
- Sub-tenant
- Service plan
- Application group
- Data type

**DATA MOVER**

In Simpana® software, Clients send the data, while the MediaAgent moves the data to the storage target. Storage Policies direct the MediaAgent to which storage target should be utilized per job, which can be shared among many tenants or dedicated to a single tenant. To provide the Service Provider with the highest levels of granularity and flexibility, MediaAgents can have multiple Storage Policies running simultaneously with a wide variety of configurations. While MediaAgents can be configured many ways for multi-tenancy, the following are the most common:

- **Private** – dedicated hardware with the MediaAgent dedicated to a single tenant, which can have a dedicated or shared CommServe server managing it
- **Multi-Instance** – single physical hardware with multiple images of the MediaAgent software running at once. Useful for Service Providers to satisfy privacy requirements and optimize hardware utilization
- **Public** – shared among multiple tenants

Note: Simpana software’s deduplication database (DDB) can be isolated to a single tenant or can be shared among multiple tenants in a Public configuration.
NETWORKING

Simpana software has extensive networking configuration options to help meet a Service Provider’s needs. The diagram below provides an overview of these options.

First, from a security perspective Simpana® software utilizes certificate based authentication between Simpana® components and client computers. This protects against a variety of networking attacks such as “spoofing”. Secondly, Simpana® software provides the ability to have dedicated interfaces or shared networking interfaces among networking configurations with Data Interface Pairs (DIP).

For more information regarding CommVault Simpana® Software Data Interface Pairs, refer to: documentation.commvault.com

Proxies

Proxies are an important component of Service Provider datacenter network security configurations, to reduce the number of ports opened and provide secure data transfer between provider and tenant. Simpana software offers two proxy configurations. Within a single CommCell deployment, both configurations can be utilized:

**Private**
- Dedicated proxy to the tenant
- Located at the customer or service provider’s site
- Prevents the tenant’s infrastructure from being internet facing
- CommServe and MediaAgent are internet facing
Shared Proxy
- Single proxy with multiple tenants pooled together
- Located in the service provider’s DMZ
- Prevents the service provider’s infrastructure from being internet facing

Firewalls
Simpana software can enable providers to insert firewall rules per client, enabling tenant segregation and custom network configuration. This firewall feature provides the ability to offer multiple network configurations per CommCell instance. The firewall service is not restricted by a specific network configuration and can be tuned at several levels -- for example, per:
- Tenant
- Sub-tenant
- Client

For more information on CommVault Simpana software firewall configurations, refer to: documentation.commvault.com

Network Bandwidth
Oversubscription of network resources is a common challenge in service provider datacenter environments, and the ability to throttle is crucial for network management. Simpana software has two available options to perform network throttling:
- Relative – % of available send or receive
- Absolute – fixed amount send or receive

More interesting for Service Providers is the ability to assign or even schedule network throttling through a policy based approach:
- Tenant
- Client or Client Group
- MediaAgent
- Copy jobs local or remote
- Based on IP range

For more on Network Bandwidth information, refer to: documentation.commvault.com

Encryption
From a networking perspective, data can be encrypted from end-to-end, at the source as well as in-transit. Simpana software allows service providers to define encryption keys per tenant, which is discussed in more detail in the Data Level Security section.

For more information regarding encryption configuration options, refer to: documentation.commvault.com
REPORTING

Simpana® software has robust reporting functionality, to show real-time and historical trending data depending on the service provider and tenant needs. Simpana software extends user and group attributes to reporting by embedding filtering by permission set. For example, a tenant could run a capacity report, however the report view would be limited to resources assigned to that tenant. Assigning and grouping tenant resources can be accomplished in many ways and for more information refer to the user management section of this report.

Service Providers can assign permissions at a report level basis. For example, a Service Provider could have a whole portfolio of reports and only publish certain reports subscribed to by tenants or even users.

CommVault has a service to build custom reports that are multi-tenant enabled through a Personalization Service.

For more information on the Personalization Service, refer to: commvault.com®

GRAPHICAL USER INTERFACE (GUI)

Simpana software offers two distinctly different types of GUI from a Service Provider perspective:

- **Administration** – for creating policies, assigning duties user/groups, associating permissions, and other tasks
- **Consumption** – for viewing and executing tasks that have been delegated to a user, group, or tenant

The two GUI’s available in Simpana software are:

**CommCell Console**
- Advanced administration
- Advanced recovery requirements

**Web Console**
- View only what you own (client owner)
- View only what has been assigned (group privileges)
- End-user self-service for basic recovery options
SECURITY

CommVault Simpana software has many embedded security features which have been continually refined with each generation of the product. While several security related topics have been covered so far in this document, three specific security features to highlight relating to multi-tenancy which have not yet been discussed include:

- **Client Owner** – special permission set enabling administrator-like privileges restricted to a specific client object
- **Enabling Privacy (Client side)** – restricts the administrator’s abilities to perform tasks on a specific client without a passphrase
- **Data Level Security** – various levels of data security from client, target, and in-transit

**Client Owner**

Client owner provides special permission to a user limited to a particular object – usually a single or group of clients. For example, a tenant that has been assigned Client Owner permissions to a server where the tenant would have administrator-like privileges could be limited in scope to that server. Included in the Client Owner permissions is access to the Web Console GUI, where the tenant would only view resources where Client Owner was assigned.

**Enabling Privacy**

Some tenants may require additional security and assurances that their privacy is being appropriately controlled in a multi-tenant environment. Simpana software has an additional privacy feature that can be enabled where a password will be required to perform certain tasks such as:

- Viewing or browsing data
- Restoring data

The tenant would create and manage the password, which would essentially lock-out the Service Provider from performing certain tasks. This feature is not enabled by default in Simpana software and the Service Provider would have to configure the options before making this feature available to tenants.

For more information on Enabling Privacy refer to: documentation.commvault.com

**Data Level Security**

As described in the Clients section (under Management Server), the CommServe generates an SSL certificate when new clients join the environment to provide an extra level of security against “spoofing” or unauthorized access to data. Simpana software provides three levels of encryption:

- **Source side** – encrypt at the agent
- **Target side** – encrypt it before you write it to storage (i.e. media agent)
- **In-Transit** – encrypt at source, decrypts before written to storage
Service providers can enable or disable the three types of encryption at:

- Tenant
- Client
- Storage policy
- Storage array
- Off-site copy

For more information on the Simpana software standard ciphers and FIPS certifications, refer to: documentation.commvault.com
**APPENDIX: TERMINOLOGY**

This table provides a listing of common industry terminology, and the corresponding CommVault specific terminology.

<table>
<thead>
<tr>
<th>Industry Term</th>
<th>CommVault Specific Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group and User Permission</td>
<td>Capabilities &amp; User Actions</td>
</tr>
<tr>
<td>Agent</td>
<td>iDataAgent</td>
</tr>
<tr>
<td>Backup Server</td>
<td>MediaAgent</td>
</tr>
<tr>
<td>Desktop &amp; Laptops</td>
<td>Edge Devices</td>
</tr>
<tr>
<td>Management Server</td>
<td>CommServe</td>
</tr>
<tr>
<td>Backup Environment</td>
<td>CommCell</td>
</tr>
<tr>
<td>Laptop, Server, and/or Virtual Machine containing 1 or more Agents</td>
<td>Client or Client Computer</td>
</tr>
<tr>
<td>Selection of data on a Client to be managed uniquely</td>
<td>Sub-client</td>
</tr>
<tr>
<td>Secure network routing</td>
<td>Firewall Configuration</td>
</tr>
<tr>
<td></td>
<td>• Direct Connections using port tunnels</td>
</tr>
<tr>
<td></td>
<td>• Port-forwarding gateways</td>
</tr>
<tr>
<td></td>
<td>• The perimeter network (also known as a DMZ) using a Simpana® proxy</td>
</tr>
<tr>
<td></td>
<td>• HTTP proxies (including WiFi connections)</td>
</tr>
<tr>
<td></td>
<td>Combinations of these</td>
</tr>
<tr>
<td>Collection of settings</td>
<td>Storage Policy</td>
</tr>
<tr>
<td></td>
<td>• Retention</td>
</tr>
<tr>
<td></td>
<td>• Storage logical target</td>
</tr>
<tr>
<td></td>
<td>• Number of data copies</td>
</tr>
<tr>
<td>Storage lifecycle policy</td>
<td></td>
</tr>
<tr>
<td>Storage configuration</td>
<td></td>
</tr>
</tbody>
</table>
Resources

1 documentation.commvault.com/commvault/v10/article?p=features/user_admin/capabilities_and_actions.htm
2 documentation.commvault.com/commvault/v10/article?p=features/user_admin/capabilities_and_actions_by_feature.htm
3 documentation.commvault.com/commvault/v10/article?p=features/client_group/smart_client_group.htm
4 documentation.commvault.com/commvault/v10/article?p=features/data_interface_pairs/data_interface_pairs.htm
5 documentation.commvault.com/commvault/v10/article?p=features/firewall/firewall_new.htm
7 documentation.commvault.com/commvault/v10/article?p=features/data_encryption/data_encryption.htm
8 commvault.com/services-and-support/professional-services/simpana-software-personalization
9 documentation.commvault.com/commvault/v10/article?p=products/web_console/config_adv.htm
10 documentation.commvault.com/commvault/v10/article?p=features/data_encryption/data_encryption.htm