Backup and Recovery Best Practices with Tintri VMstore and Commvault Simpana Software

Author: Dominic Cheah (TME)

August 2015
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intended Audience</td>
<td>3</td>
</tr>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Consolidated List of Practices</td>
<td>3</td>
</tr>
<tr>
<td>Backup</td>
<td>5</td>
</tr>
<tr>
<td>Environment</td>
<td>5</td>
</tr>
<tr>
<td>Configuring Storage</td>
<td>7</td>
</tr>
<tr>
<td>Configuring Virtual Server Agent Backup</td>
<td>9</td>
</tr>
<tr>
<td>Backup</td>
<td>11</td>
</tr>
<tr>
<td>Restore</td>
<td>14</td>
</tr>
<tr>
<td>Commvault Simpana Aux Copy</td>
<td>18</td>
</tr>
<tr>
<td>Commvault Simpana DASH Full</td>
<td>19</td>
</tr>
<tr>
<td>Tintri VMstore SnapVM™, CloneVM™, and ReplicateVM™</td>
<td>19</td>
</tr>
<tr>
<td>Summary</td>
<td>21</td>
</tr>
<tr>
<td>References</td>
<td>22</td>
</tr>
</tbody>
</table>
**Intended Audience**

This Tintri Best Practices Guide for Backup and Recovery will assist individuals who are responsible for the design, deployment, and DR of Tintri VMstore™ Systems. This document will encompass vStorage APIs for Data Protection (VADP) for backups and the use of Tintri’s SnapVM™, CloneVM™ and ReplicateVM™ features to complement data protection of virtual machines and critical applications hosted on Tintri’s VMstores with Commvault Simpana v10.

**Introduction**

Deploying storage into your virtual environment should be a straightforward process. What if you didn’t have to do LUN masking on a storage array? What if you didn’t have to worry about raid levels or queue depth settings ever again? What if you could just connect a datastore to an ESXi host, discover the datastore and start deploying your virtual machines? Tintri VMstore™ is designed so that IT administrators with a working knowledge of vSphere can successfully deploy Tintri’s purpose-built VM storage with ease.

Tintri VMstore delivers extreme performance and VM density, and a wide variety of powerful features, which are seamlessly integrated with vSphere. Examples include snapshots, clones, instant bottleneck visualization, and automatic virtual disk alignment. Tintri VMstore extends and simplifies the management of virtual machines (VMs) through an intrinsic VM-awareness that reaches from the top of the computing stack, all the way down into the flash (SSD) and disk (HDD) drives.

This best practice guide highlights the following when using Commvault Simpana to protect VMs on a Tintri VMstore:

- Architectural overview of a VMware environment with Tintri VMstore and Commvault Simpana Servers.
- The simplicity of protecting VMs using VMware VADP with Commvault Simpana Software.
- The simplicity of protecting Microsoft application servers such as Microsoft Exchange 2013 DAG and Microsoft SQL 2012 servers with Commvault Simpana Software.
- The use of Tintri VMstore data protection features as a complement to Commvault Simpana Software.

**NOTE:** In this document, Simpana will be used as reference to Commvault Simpana Software.

**Consolidated List of Practices**

The table below includes the recommended practices in this document. Click the text on any of the recommendations to jump to the section that corresponds to each recommendation for additional information.

**DO:** Use the FQDN of the vCenter Host Name when configuring the vCenter Client.

**DO:** Use the OVA template that is supplied by Simpana software to create a Linux Media Agent for file recovery.

**DO:** Deploy Simpana MediaAgent hosted on Tintri VMstores with thin provision VMDKs for the O/S VMDK. In addition to the O/S VMDK, thin provision VMDKs should include the local disk library storage for the backups.

**DO:** It is Commvault’s best practice recommendation to deploy Simpana MediaAgent virtual machines deduplication database (DDB) on local ESX SSD datastores. The DDB VMDKs should be thick.
provisioned. For optimal performance, the Index Cache in the MediaAgent must also be placed on SSD datastores.

**DO:** Create additional copies of your backups and prevent against single point of failure by using Simpana’s Auxiliary Copy Feature.

**DO:** Use the Number of Data Readers for tuning the number of concurrent VMware snapshots that will be attempted, irrespective of Guest OS.

**DO NOT:** Modify the default subclient content. It is not recommended to modify the default subclient content. As a Commvault Simpana best practice recommendation, the default subclient is used for automated discovery and protection of missed VMs. It is Commvault's recommendation to create a user-defined subclient to target desired VMs.

**DO:** Create new subclients as a general practice.

**DO:** Update the VSA nExtentSize as necessary for additional performance gains. As with any performance tunable settings, the exact performance improvements depends on environmental factors. The impact of any performance tunable setting should be considered before changing the extent size. The nExtentSize performance tuning is applicable to HotAdd transport mode with Tintri VMstores.

**DO:** Use Tintri VMstore UI (Dashboard and Virtual Machines tab) to monitor latency and resource usage on a Tintri VMstore. This provides an advantage that a VM administrator can monitor resources and issues on a per VM basis or on a per virtual disk basis to determine where bottlenecks can occur.

**DO:** Deploy more than one proxy server per data center.

**DO:** Use Commvault Simpana’s virtual appliance template if Live Recovery for virtual machines is required.

**DO:** Ensure that the network connection between the ESXi server, the proxy server, and the Simpana MediaAgent is 10GigE so that NBD transport can utilize a larger network pipe for backup I/O and restore I/O.

**DO:** Ensure that the proxy server has more than one SCSI controller if HotAdd transport mode is required for every restore operation. The limit from VDDK is 4 x SCSI Controllers per HotAdd host. Use Commvault’s recommended system requirements for deploying proxy servers and MediaAgents.

**DO NOT:** Oversubscribe the number of VM disks that can be attached using HotAdd to a proxy server. Backup operations with ‘Transport mode for VMware: Auto’ will select other available transport for backup of multiple VMDKs. Restore operations will select other available transport mode for restore operations if a proxy server is oversubscribed for HotAdd transport.

**DO:** Remove the database from the SQL Availability Group before attempting a SQL database restore.

**DO:** Use DASH Copy with source side cache enabled for more efficiency.

**DO:** It is highly recommended to use Simpana Aux Copy to make additional backup copies on other storage policies on other physical MediaAgents for additional data protection.

**DO:** Protect a CommServe using Commvault’s recommended data protection solutions.

**DO:** Protect a deduplication database using Commvault’s recommended data protection solutions.

**DO:** Use Commvault Simpana Aux Copy to create multiple backup copies on other MediaAgents for data protection.

**DO:** Use Commvault Simpana replication to replicate recovery points for additional data protection.
DO NOT: Replicate a virtual machine MediaAgent offsite without the CommServe being available for recovery. Both MediaAgent and the CommServe should be replicated offsite for recovery. Use Commvault's recommended replication strategy to protect your CommServe and MediaAgent.

Backup

Environment

In this document, the referenced VMware vCenter architecture manages 3 ESXi hosts that have been configured with standard networks and distributed port groups. Simpana servers and application servers, referenced in this document, are deployed as the following:

<table>
<thead>
<tr>
<th>Server</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>CommVault Simpana CommServe/CommCell Console</td>
<td>Windows 2012 R2</td>
</tr>
<tr>
<td>CommVault Simpana Windows MediaAgent/Proxy Server A (VM)</td>
<td>Windows 2012 R2</td>
</tr>
<tr>
<td>CommVault Simpana Linux Media Agent - Physical Server</td>
<td>RHEL 6</td>
</tr>
<tr>
<td>Proxy Server B (VM)</td>
<td>Windows 2012 R2</td>
</tr>
<tr>
<td>CommVault Simpana Linux Media Agent - File Recovery Enabler for Linux</td>
<td>Windows 2012 R2</td>
</tr>
<tr>
<td>Microsoft Exchange 2013 Server A</td>
<td>Windows 2012 R2</td>
</tr>
<tr>
<td>Microsoft Exchange 2013 Server B</td>
<td>Windows 2012 R2</td>
</tr>
<tr>
<td>Microsoft SQL 2012 Server A</td>
<td>Windows 2012 R2</td>
</tr>
<tr>
<td>Microsoft SQL 2012 Server B</td>
<td>Windows 2012 R2</td>
</tr>
</tbody>
</table>

The Microsoft Exchange 2013 DAG servers and the Microsoft SQL 2012 Always on Availability Group servers, in this reference architecture, are example of Tintri VMstore supported applications. Tintri VMstores also supports other Microsoft applications that Commvault Simpana supports as virtual machines. The recommendations provided in this document apply to any other applications supported by Commvault Simpana Software that are deployed as virtual machines on Tintri VMstores.

Commvault Simpana Software version 10 was used in this reference architecture. Earlier versions of Simpana Software is also supported by Tintri VMstores as long as the Simpana Software version is licensed, supported by Commvault, and has not been end of support or end of life by Commvault.

Virtual Server Agent is required for Simpana to utilize VADP. In this example, Simpana Virtual Server Agent is installed on virtual machines:

- Proxy server A
- Proxy server B

Proxy server A is also a Commvault Simpana MediaAgent. This allows for efficient use of HotAdd transport mode to backup to and restore from MediaAgent A. Commvault MediaAgent C is a physical RHEL server. A physical MediaAgent allows auxiliary copies to be created on virtual tape library or physical tape library for extended retention. It is recommended to create copies of backups for disaster recovery purposes.

NOTE: In this example, HotAdd transport mode can also be utilized with proxy server B as long as the proxy servers are in the same data center and has access to the Tintri VMstore that the ESX/ESXi server has access to.
Configure the vCenter host from the CommCell console by providing the FQDN of the vCenter Server Name. Use the Create VMware vCenter Client window to add any new proxy servers that have been installed with the Simpana VirtualServer Agent.

DO: Use the FQDN of the vCenter Host Name when configuring the vCenter Client.

The Linux MA for File Recovery is also used for live recovery of a VM from a backup without having to wait for a full restore of a VM. Use the OVA template that is supplied by Simpana to create a VM that contains the Linux MediaAgent for file recovery.
**DO:** Use the OVA template that is supplied by Simpana software to create a Linux Media Agent for file recovery.

**DO:** Deploy Simpana MediaAgent hosted on Tintri VMstores with thin provision VMDKs for the O/S VMDK. In addition to the O/S VMDK, thin provision VMDKs should include the local disk library storage for the backups.

**DO:** It is Commvault’s best practice recommendation to deploy Simpana MediaAgent virtual machines deduplication database (DDB) on local ESX SSD datastores. The DDB VMDKs should be thick provisioned. For optimal performance, the Index Cache in the MediaAgent must also be placed on SSD datastores.

**DO:** Create additional copies of your backups and prevent against single point of failure by using Simpana’s Auxiliary Copy Feature.

In the backup set, if VMware vStorage API method for Backup is selected, VADP will be used for backing up VMs in vSphere 4.0 environments or newer for all subclients within the same backup set. By selecting Automatic in the backup set property, Commvault Simpana will determine the best mode (VCB/VADP) to use depending on the ESX version.

**Configuring Storage**

When creating a disk library, use the Mount Path Allocation Policy to set the number of writers. This determines the maximum number of concurrent operations to the disk library. Set this to Maximum Allowed Writers for the disk library.
Use the **New Storage Policy** wizard to create storage policies for your backups. Commvault Simpana supports global deduplication. If this option is selected, a global common deduplication database is shared by multiple storage policies. This option allows multiple copies to be deduplicated against each other and improves deduplication across copies. You must create a global deduplication policy before the **Use Existing Global Deduplication Policy** can be selected.

In the storage policy properties pop-up window, the block level deduplication factor is 128KB and this is Commvault’s recommended block level deduplication factor for all agent types (Commvault Simpana 10 or later) with Commvault Simpana deduplication storage. In the data path properties of the disk library, disk libraries have a default chunk size of 2GB and a default block size of 64K. These parameters can be tuned for performance at the storage policy level. Commvault recommends that the block size is set to 256K for increased performances on Disk Libraries and Tape Libraries.
Configuring Virtual Server Agent Backup

The Commvault Simpana Virtual Server Agent (VSA) for VMware is also referred to as the Virtual Server DataAgent for VMware. In the subclient properties of the backup set, the Number of Data Readers determines the parallelism of the backup for the particular subclient. By default, the value is 2. For Virtual Server Agent backups, this represents the number of VSS snapshots to be attempted in parallel for the subclient.

\[DO:\] Use the Number of Data Readers for tuning the number of concurrent VMware snapshots that will be attempted, irrespective of Guest OS.

Additionally, for resource tuning to improve performance of data transfers from the subclient properties, select the Storage Device tab and select the Data Transfer Option sub tab. The Network Agents and the
Throttle Network Bandwidth can be used to set the number of network agents for data transfer and throttling of the network traffic from the subclient.

For Virtual Server Agent backups, the VADP transport mode options is also available, auto will enable Commvault Simpana to determine the best transport mode to use for backup of VMs that are configured in the subclient policy.

When configuring the content for backups, use the Browse option to add target VMs by Hosts and Clusters, VMs and Templates or by Datastores and Datastore Clusters. Use the Add option to add target VMs by using rules.

Additional performance improvements for Backup and Restore operations with Virtual Server Agent (VSA) can be tuned in Commvault Simpana v10 or newer. To implement performance improvements, the step requires increasing the size of the extent processed by the VSA registry key. However, this will change the block boundaries, this particular performance consideration should only be implemented for new sites or where re-baseline is acceptable. The new extent size will only take effect on the next FULL backup. The additional performance improvements are applicable to SAN and HotAdd transport mode only. With Tintri VMstores, the nExtentSize performance tuning is applicable to HotAdd transport mode only.

Right click on the vCenter from the Client Computer Groups in the Commcell Console, select the Additional Settings tab and Add nExtentSize=2048. The acceptable extent size is a multiple of 512. The default nExtent size with Commvault Simpana v10 is 512. With Commvault Simpana newer than v10, the default nExtentSize will be 2048.
DO NOT: Modify the default subclient content. It is not recommended to modify the default subclient content. As a Commvault Simpana best practice recommendation, the default subclient is used for automated discovery and protection of missed VMs. It is Commvault's recommendation to create a user-defined subclient to target desired VMs.

DO: Create new subclients as a general practice.

DO: Update the VSA nExtentSize as necessary for additional performance gains. As with any performance tunable settings, the exact performance improvements depends on environmental factors. The impact of any performance tunable setting should be considered before changing the extent size. The nExtentSize performance tuning is applicable to HotAdd transport mode with Tintri VMstores.

Backup

When attempting a backup using the VirtualServer Agent, in addition to the job log, make use of the Commvault Simpana Event Details for troubleshooting. For example, the following shows a backup attempt that failed with “Unable to open the disks...”. The description of the error is always useful and provides additional checks that can be followed to complete a successful backup operation.

During a Commvault Simpana backup or any other operation of virtual machines hosted on Tintri VMstores, it is recommended to use the Tintri Dashboard and Virtual Machines view to troubleshoot
latencies or low flash hit issues. If a virtual machine experiences low I/O performance, the *Virtual Machines* view allows the data center administrator to drill down to the virtual machine level or the virtual disk level to determine the source of the I/O latency. For example, the following shows a temporary affect on the Simpana MediaAgent latency during a Commvault verify data operation. As cold data is pulled in from HDD storage for read or verify operations, there is a temporary affect on latency for the data protection operation.

**DO:** Use Tintri VMstore UI (Dashboard and Virtual Machines tab) to monitor latency and resource usage on a Tintri VMstore. This provides an advantage that a VM administrator can monitor resources and issues on a per VM basis or on a per virtual disk basis to determine where bottlenecks can occur.

**DO:** Deploy more than one proxy server per data center.

In the *Simpana Backup Job Details* window, the administrator can verify the VADP transport mode and the use of changed block tracking (CBT) on the backup jobs.

Commvault Simpana supports VMware VADP backup of application servers such as Microsoft Exchange 2013 servers, Microsoft SQL 2012 servers, etc. Application aware backup for item based recovery with truncate database logs with VMware VADP requires IntelliSnap.

Commvault Simpana also supports application server backups using Simpana installed agents. This is also a feasible alternative in protecting application servers such as Microsoft SQL servers using a traditional method that most data center administrators are already familiar with. Using application and database agent approach allows for application log truncation for supported applications and databases for backups.

This requires installing the correct application agent on the virtual machine. In this case, the backup of a virtual machine is treated as a physical server. Therefore, ensure that the network connection between the Commvault MediaAgent and the client has the network bandwidth for serving I/O and for backup. In
the Advanced Client Properties, it is also possible to define data interface pairs between the client and the MediaAgent for backup I/O. In addition to segregating backup I/O from data I/O that the application server is serving, using data interface pairs can help isolate and troubleshoot backup performance issue that could be network related.

Commvault Simpana support Microsoft Exchange DAG server backup. When configuring the Exchange DAG client, use a proxy for DAG discovery. You can specify automatic server selection in the subclient properties and allow Commvault Simpana to run backups from the next available passive server for performance purposes. Select the *Use last activation preference to select passive copy* to avoid backup jobs from running on an active Exchange server as that may slow down other database processes.

From the CommCell console, monitor the Microsoft Exchange DAG backup to completion from the Job Controller tab. Application servers that have the Simpana application agent installed allows for Commvault Simpana to perform log truncation, if selected, on the application servers.

In addition to Microsoft Exchange DAG server support, Commvault Simpana also supports backup of Microsoft SQL 2012 and SQL 2014 AlwaysOn Availability Groups.
In the SQL Management Studio’s Availability Group Properties, specify primary as the location where backups should occur. This allows incremental backup options to be available for use with Commvault Simpana.

NOTE: Tintri VMstores support HotAdd, NBD and NBDSSL transport modes. Be aware that some application servers may be paused for a long time during the snapshot removal phase in a backup process when the VM have high I/O. For these application servers that may not be able to handle long pause periods, it is recommended to ensure that the proxy server(s) has 10GigE network connectivity to the ESX/ESXi servers for the VMs that are being protected using any of the supported transport modes with Tintri VMstores. With CBT enabled, after the initial full, backups of virtual machines with NBD transport mode will only transfer change blocks and it is efficient.

It is also recommended to use CommVault Simpana’s DASH full/Incremental Forever strategy. This will help reduce the snapshot window of the VMs that are protected with Commvault Simpana Software. Review VMware’s KB for additional details on snapshot removal. Symptoms of application servers experiencing long pauses during snapshot removal includes the end user losing connectivity to the remote desktop or the end user losing connection to the application on the virtual machine.

**Restore**

Commvault Simpana provides many options for restore operations. A restore operation can be attempted at the client level by performing a *Browse and Restore* from the subclient level or by selecting View Jobs at the storage policy level.

With Virtual Server Agent restore, there are many options that are available to the data center administrator as well. One of the options is to restore a VM as a full virtual machine.

![Image](image.png)
With a full virtual machine selection, the data center administrator has the option for *in-place* restore or *out-of-place* restore. If the restore in place is unchecked, the full VM can be restored to:

- Different vCenter
- Different ESX server
- Different datastore
- Different resource pool or vApp
- Different VM name
- Restore to a VM folder.

An additional feature that is also supported by Commvault Simpana is VM restore with Changed Block Tracking (CBT). This feature efficiently restores only changed blocks to the original virtual machine. To utilize CBT for restore, set `bEnableSeekOptimization` using the registry editor on the proxy server ([Commvault Simpana Enable Seek Optimization](#)).

**NOTE:** VM restore with CBT is available on the first restore of a virtual machine to the original VM location. To utilize restore with CBT after the initial restore operation, a new backup of the VM must be executed.
Commvault Simpana also provides granular recovery from a backup that takes advantage of VADP. This provides a data center administrator options to perform restore of files or folders rather than restoring an entire virtual machine.

In addition, Commvault Simpana backup with VMware VADP provides a data center administrator the option to restore files or folders directly from a backup. The use of a Linux MA for file recovery is required but it provides a data center administrator the option to perform an instant recovery of a VM and allow the VM to be powered on from a backup without first, having to restore the entire VM. This is an efficient option that Commvault Simpana also provides to a data center administrator.

**DO: Use Commvault Simpana’s virtual appliance template if Live Recovery for virtual machines is required.**

If a restore operation is attempted from a MediaAgent that is also a VM on a Tintri VMstore, the latency and flash hit ratio will be temporarily affected as cold data could be pulled from HDD storage for read operations. This also includes data verification operations.

When performing restore operations of multiple virtual machines, ensure that the proxy server has the resources to perform restore. For example, a proxy server with a single SCSI controller allows up to 15 devices for HotAdd transport. If the restore operation requirement is to utilize HotAdd only, ensure that the proxy server has more than one SCSI controller (VMware max of 4x SCSI Controllers per HotAdd proxy server).
DO: Ensure that the network connection between the ESXi server, the proxy server, and the Simpana MediaAgent is 10GigE so that NBD transport can utilize a larger network pipe for backup I/O and restore I/O.

DO: Ensure that the proxy server has more than one SCSI controller if HotAdd transport mode is required for every restore operation. The limit from VDDK is 4 x SCSI Controllers per HotAdd host. Use Commvault’s recommended system requirements for deploying proxy servers and MediaAgents.

DO NOT: Oversubscribe the number of VM disks that can be attached using HotAdd to a proxy server. Backup operations with ‘Transport mode for VMware: Auto’ will select other available transport for backup of multiple VMDKs. Restore operations will select other available transport mode for restore operations if a proxy server is oversubscribed for HotAdd transport.

The following combination will result in very slow restore operations:

- Proxy server is oversubscribed for HotAdd.
- The network connection between the ESXi server, the proxy server and the Simpana MediaAgent is not 10GigE for NBD transport mode.

When performing restore operations on Microsoft Exchange server applications, it is good practice to restore to a recovery database (RDB) to minimize the risk of corrupting a production database. For example, with a Microsoft Exchange 2013 server, the data center administrator can restore the Microsoft Exchange database to a RDB and restore individual mailboxes without interrupting user access to the current data.

With Microsoft SQL AlwaysOn Availability Groups, it is recommended to remove the database from the Availability Group before a database restore operation. When the database can be added back into the Availability Group.
DO: Remove the database from the SQL Availability Group before attempting a SQL database restore.

Commvault Simpana Aux Copy

With Commvault Simpana, use Aux Copy to make backup copies for local and off-site extended retention. It is recommended to enable DASH Copy in the Copy Properties. This ensures that only unique blocks are used for the copy process. Commvault Simpana does not recommend using DASH copy with WAN accelerator appliances, as DASH copy is already efficient.

DO: Use DASH Copy with source side cache enabled for more efficiency.

With aux copy operations, be aware that cold backup data has to be pulled in from HDDs storage. In some cases, there is a temporary affect on the latency and flash hit ratio during the aux copy operations when a Simpana MediaAgent is hosted as a virtual machine on a Tintri VMstore. It is recommended to
aux copy to a physical server so that backup copies for extended retention can be copied onto physical tape libraries. It is also recommended to create backup copies from virtual MediaAgents onto physical MediaAgents for additional data protection purposes.

With Aux Copy, Commvault recommends enabling dynamic stream allocation when large amount of data is to be copied to a tape library. Ensure that the same MediaAgent is used for both primary and inline copy to tape media.

**Commvault Simpana DASH Full**

DASH Full utilizes Commvault’s Simpana deduplication feature to ensure that a synthetic full backup is created without requiring movement of data. When the first full backup is created, changed blocks are protected for incremental and differential backups. Rather than a traditional full where data is actually moved, DASH Full does not move data but rather update the index information and the deduplication database to create a synthetic full backup. The use of DASH Full significantly reduces the amount of time to perform additional full backups. In the schedule policy, also ensure that the synthetic full schedule is created to take advantage of Simpana’s DASH Full feature.

![New Schedule Policy](image)

**NOTE:** With MediaAgents hosted as virtual machines on Tintri VMStores, there is a temporary affect on the latency and flash hit ratios as data is read from cold storage for DASH full operations on the virtual machine MediaAgent.

**Tintri VMstore SnapVM™, CloneVM™, and ReplicateVM™**

Tintri’s SnapVM™ and CloneVM™ can be used with Commvault Simpana software for protection of virtual machines and virtual machines with application servers. In addition, SnapVM and CloneVM can also be used to protect a Simpana MediaAgent for DR purposes. For example, a Commvault Simpana MediaAgent virtual machine can be protected using Tintri’s SnapVM. In the following example, a Windows MediaAgent is protected daily with a Tintri snapshot that will be kept for no more than 2 days locally. It is recommended to keep no more than 2 days of snapshots of MediaAgents, as each snapshot could grow large. It is also a best practice to have more than 1 copy of your backups. For additional DR
purposes, always use Commvault Simpana Aux Copy to make additional copies of your backups on other physical storage with your MediaAgent.

There is no Simpana Disk Volume Reconciliation operation for deduplicated storage policy copies. This means that if a virtual machine MediaAgent is restored from a Tintri CloneVM operation, the backup jobs that were executed after the snapshot was taken and before the restore operation cannot be reconciled. This will leave orphaned volumes that cannot be reconciled with the CommServe with deduplicated storage policies.

**DO:** It is highly recommended to use Simpana Aux Copy to make additional backup copies on other storage policies on other physical MediaAgents for additional data protection.

A Tintri VMstore SnapVM and CloneVM operation for a Simpana MediaAgent is also dependent on the CommServe that it is licensed on. A restore of a Simpana MediaAgent without the corresponding CommServe is not effective if the CommServe is not available. Ensure that the CommServe and metadata on the CommServe is protected using Commvault Simpana’s recommended DR solution for protecting a CommServe and its metadata.

When a virtual machine MediaAgent is restored on a Tintri VMstore using CloneVM, set Customization: None to ensure that the virtual machine is not customized or the MediaAgent restore will be corrupted if it is customized. In addition, before continuing to use the virtual machine MediaAgent for new backup operations, it is recommended to execute *Recover Deduplication Database* and to run data verification of existing backup jobs. This will help verify that the existing backup jobs are still valid and the deduplication database is valid and no corruption was introduced with the MediaAgent restore using Tintri CloneVM.

If a global deduplication policy is utilized for some of the storage policies on the virtual machine MediaAgent, it is recommended to run *Disk Volume Reconciliation* and data verification before running new backup jobs using the storage policies on the virtual machine MediaAgent.

**DO:** Protect a CommServe using Commvault’s recommended data protection solutions.

**DO:** Protect a deduplication database using Commvault’s recommended data protection solutions.

**DO:** Use Commvault Simpana Aux Copy to create multiple backup copies on other MediaAgents for data protection.
**DO:** Use Commvault Simpana replication to replicate recovery points for additional data protection.

**DO NOT:** Replicate a virtual machine MediaAgent offsite without the CommServe being available for recovery. Both MediaAgent and the CommServe should be replicated offsite for recovery. Use Commvault's recommended replication strategy to protect your CommServe and MediaAgent.

For virtual machines that are application servers, Tintri SnapVM, CloneVM, and ReplicateVM can be used to protect critical application servers. A Microsoft Exchange DAG server and its dependencies can be protected using ReplicateVM with other Tintri VMstores. Since Tintri VMstore ReplicateVM is very efficient, only unique changed blocks are sent over LAN/WAN. This feature can reduce network bandwidth usage for replication by up to 95%. In the following example, to create VM3 that is dependent on 3 data blocks to create a full VM, only the unique data block is sent over LAN/WAN from VMstore 1 to VMstore 2 to create VM3. The other required blocks are referenced from the existing data blocks from VM2.

**Summary**

Tintri VMstores with Commvault Simpana software solution is a strong combination for providing data protection of virtual machines locally and remotely. Commvault Simpana deduplication solution is very efficient and only stores unique changed block for backups. Tintri VMstores are designed, from the ground up, for hosting virtual machines. Ensure that your virtual machines and application servers that have dependencies on other resources are protected with Commvault Simpana Software. An application
server without its dependencies cannot be brought online into a live production environment. Follow Commvault’s best practice recommendation to protect the CommServe, the deduplication database, and the backup copies for DR purposes.

References

- Tintri VMstore Overview - http://www.tintri.com/resources
- Managing VM Data with Tintri - http://www.tintri.com/resources
- Commvault Simpana Documentation - http://documentation Commvault.com/hds/