



# FlexPod Datacenter with SnapProtect Implementation Guide

Shawn Preissner, NetApp  
August 2013 | TR-4213

## Acknowledgements

Sunder Parameswaran, Product Manager, NetApp

Don Clough, Program Manager, NetApp

Will Stowe, Consulting Systems Engineer, Microsoft Solutions, NetApp

James Raffield, Product Manager, CommVault

Glenn Speer, Partner Alliance Manager, CommVault

Kevin Schemery, Consulting Systems Engineer, Cisco

## TABLE OF CONTENTS

<b>1</b>	<b>Target Audience.....</b>	<b>4</b>
<b>2</b>	<b>SnapProtect Solution Overview .....</b>	<b>4</b>
2.1	SnapProtect NAS.....	5
2.2	SnapProtect VMware .....	5
<b>3</b>	<b>FlexPod Solution Overview .....</b>	<b>6</b>
3.1	Problem Statement .....	7
3.2	FlexPod Technology .....	8
3.3	Physical Infrastructure .....	9
<b>4</b>	<b>Use Cases Validated.....</b>	<b>11</b>
4.1	Use Case 1 .....	11
4.2	Use Case 2 .....	13
<b>5</b>	<b>Configuration Procedure .....</b>	<b>15</b>
5.1	Array Management .....	15
5.2	Backing Up an Exchange DAG Client.....	15
5.3	Copy Precedence .....	21
5.4	Scheduled Policies.....	22
5.5	VMware Backup.....	23
5.6	Auxiliary Copy .....	24
5.7	VMware Restore .....	25
<b>6</b>	<b>Testing .....</b>	<b>26</b>
<b>7</b>	<b>Conclusion .....</b>	<b>27</b>
	<b>Appendix.....</b>	<b>27</b>
	Supporting Documents .....	27
	Glossary .....	28

## LIST OF FIGURES

Figure 1)	Example of SnapProtect workflow.....	4
Figure 2)	FlexPod infrastructure. ....	7
Figure 3)	FlexPod physical topology (example).....	9
Figure 4)	CIFS access topology. ....	12

Figure 4) NFS access topology. ....	12
Figure 5) NAS and VMware topology. ....	14
Figure 6) Exchange DAG. ....	14

## 1 Target Audience

This document describes the architecture and deployment procedures of an infrastructure composed of Cisco®, NetApp®, and VMware® virtualization that uses storage serving NAS and SAN protocols. The intended audience for this document includes, but is not limited to, sales engineers, field consultants, professional services, IT managers, partner engineering, and customers who want to deploy NetApp SnapProtect® on a FlexPod® architecture.

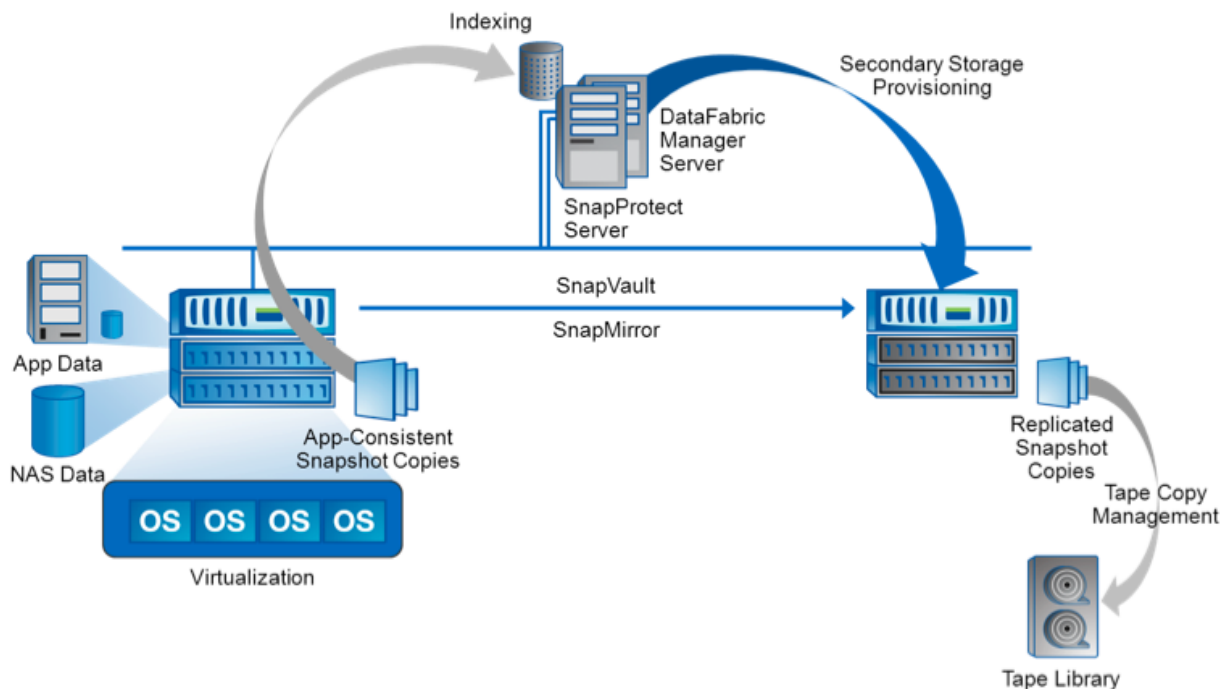
## 2 SnapProtect Solution Overview

NetApp is an industry leader in array-based data protection. The efficiencies of NetApp Snapshot™ technology and data replication have changed the way we look at backup and recovery and disaster recovery (DR) strategies. The need to achieve higher service-level agreements (SLAs) and to meet backup windows is a constant challenge, given the proliferation of data with which enterprises are dealing today. Data center consolidation through virtualization has also created challenges around data protection. Disk-to-disk data protection solutions are becoming more widely accepted for both backup and recovery and DR strategies. NetApp data protection solutions offer speed and flexibility while reducing storage capacity requirements by using efficient array-based technologies. The result is a simplified approach that reduces costs and administrative effort.

NetApp SnapProtect management software offers enterprise-class management for backup and recovery in the data center. The SnapProtect software manages Snapshot copies on NetApp primary storage and replication to secondary and tertiary storage, as well as tape creation. Regardless of whether you are protecting NetApp application data, file data for network-attached storage (NAS), file data in logical unit numbers (LUNs), or data in virtualized environments, the SnapProtect solution provides the management, storage provisioning, cataloging, and granular recoverability required for seamless operation.

Use SnapProtect solution to protect the following applications hosted on NetApp: Microsoft® Exchange Server, SQL Server®, SharePoint®, Oracle®, DB2, Lotus Notes, and SAP® for Oracle.

Figure 1) Example of SnapProtect workflow.



## 2.1 SnapProtect NAS

One of the most basic functions that SnapProtect manages is the backup and recovery of NAS data in NetApp storage systems. When a backup is performed, SnapProtect creates a Snapshot copy of the volumes associated with the data being protected. After the Snapshot copy is created, SnapProtect generates an index of the backup and writes that metadata to an associated disk library.

The NetApp NAS NDMP iDataAgent (iDA) manages NAS data backups for the NetApp primary array. The NetApp primary array is the client in this case, and the subclients are configured to determine the data that will be protected.

Use SnapVault® and/or volume SnapMirror® to replicate a SnapProtect backup. Each suits a different backup and recovery need; SnapMirror is a 1:1 data (mirroring) workflow commonly used for disaster recovery purposes, whereas SnapVault allows you to replicate data to different storage with different retention settings and number of copies. The OnCommand® Unified Manager (formerly DataFabric® Manager) manages the replication and provisioning components, while SnapProtect initiates all replication jobs. It is important to understand how SnapProtect subclients integrate with OnCommand datasets.

For example, if a single NetApp primary system is configured as a NAS client, all of the NAS volumes on that primary system can be grouped together by a single subclient. This results in a single dataset in OnCommand. If the storage policy in the SnapProtect software calls for mirroring this subclient, then the dataset creates mirror relationships for each of the volumes in the subclient.

Vaulting NAS data is slightly different because a vault can be more granular in scope. In addition to the entire volume, individual qtrees in a primary volume can be selected for vaulting purposes.

Consider several factors when determining the data to group together into a subclient because each grouping method offers a different set of advantages. For example, placing more volumes and qtrees in a single subclient makes it easier to manage and schedule backups because only one object must be managed for the group of volumes. Having several qtrees in the same subclient also allows for fan-in. The advantage of having fewer volumes and qtrees in one subclient is that, when backups must be expired (for example, to recover space), then only one set of data must be expired. In other words, having fewer volumes in a subclient offers more granularity for managing the storage.

## 2.2 SnapProtect VMware

A key feature of SnapProtect management software is the ability to protect many virtual machines (VMs) very quickly. In addition, it can index the contents of Windows® VMs, and it allows different levels of recoverability, including single file recovery.

SnapProtect software is flexible and allows discovery rules to be established so that new VMs can be automatically added to a subclient and protected. For example, using a discovery rule of datastore affinity automatically protects new VMs on specific datastores.

SnapProtect software uses the virtual server agent (VSA) to perform the data protection operations for virtual environments. The VSA is installed on a system configured as a media agent. Within the VSA, instances are created that define the type of virtualization solution being used. In a VMware environment, a VMware instance would be created under the VSA. Within the instance, a backup set contains the subclients.

**Note:** Because of the advantages of the VMware HotAdd transport mode during restores, NetApp recommends installing the VSA on a virtualized media agent. This virtualized media agent should run on an ESX® host that has access to the production datastores, such as an ESX proxy host.

When SnapProtect backs up a VM, it creates a Snapshot copy for the NetApp volume associated with the datastore that contains that VM. This is an important consideration when configuring policies to protect the virtual environment. Because a NetApp Snapshot copy is created at the volume level, it makes sense

to group VMs with the same protection requirements into the same datastores. In Virtual Machine File System (VMFS) environments, it is helpful to limit datastores to one per volume.

Multiple subclients can be used to stagger backup jobs and separate policies that have different scheduling and retention requirements.

Backup settings allow different granularity for restore operations. During restore operations, data for the VMs can be browsed and recovered based on the recovery type selected. A container restore can be performed to recover an entire VM. Individual files can also be restored for Windows VMs.

## VMware and Exchange/Applications

When run inside a VM, Microsoft Exchange and SQL Server have integration with Volume Shadow Copy Service (VSS) to allow database consistency during the backup of the VM. To get this functionality, the file system iDA and the SnapProtect VSS provider must be installed on the guest operating system, and the database must reside in virtual machine disks (VMDKs). To enable these application-consistent backups, make sure that the Application Aware Backup for Granular Recovery checkbox is selected under the SnapProtect Operations tab for the subclient. Exchange backups offer the additional option to perform log truncation as part of the backup operation (select Truncate ExDB Logs).

Consistent out-of-place restores of SQL Server and Exchange databases can be performed by restoring the flat database files. The Exchange Offline Mining tool is a standalone utility that allows individual message restores from a backup copy of the Exchange database.

For applications that reside on raw device mappings (RDMs), the appropriate iDA must be used from within the VM.

## 3 FlexPod Solution Overview

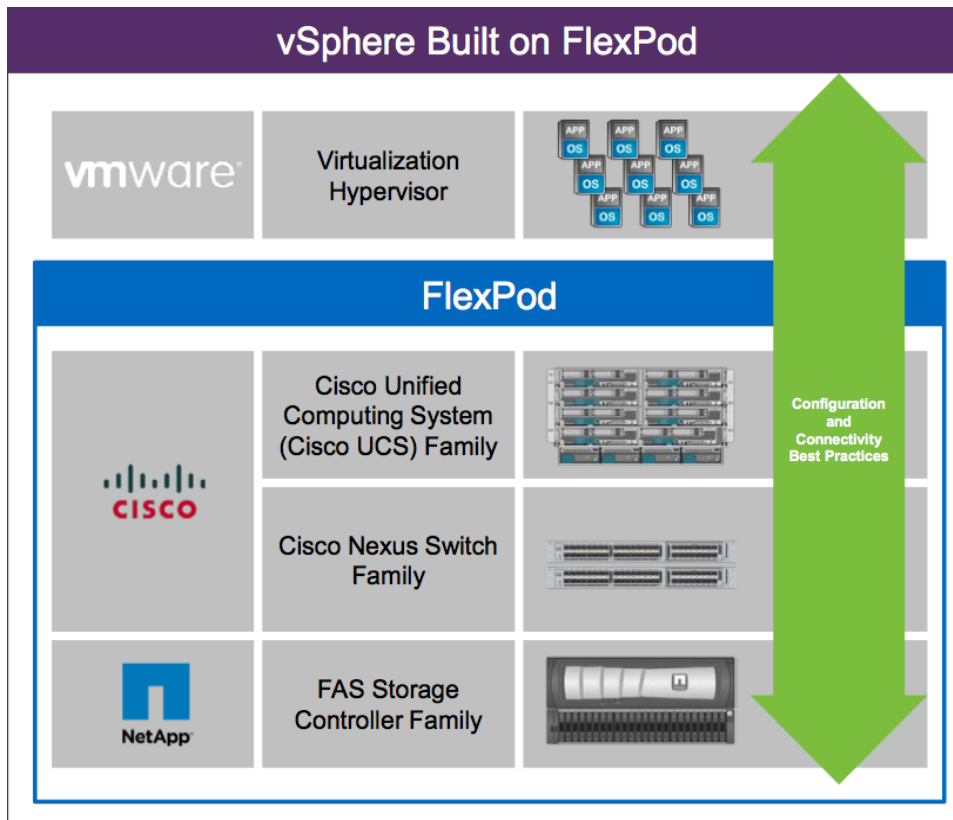
Industry trends indicate a vast data center transformation toward shared infrastructure and cloud computing. Enterprise customers are moving away from silos of IT operation toward more cost-effective virtualized environments, leading eventually to cloud computing to increase agility and reduce costs. This transformation appears daunting and complex because companies must address resistance to change in both their organizational and technical IT models. To accelerate this process and simplify the evolution to shared cloud infrastructure, Cisco and NetApp have developed the FlexPod data center solution.

FlexPod is a predesigned, best practice data center architecture that is built on the Cisco Unified Computing System™ (Cisco UCS®), Cisco Nexus® switches, and NetApp fabric-attached storage (FAS) systems. FlexPod is an ideal platform for running a variety of enterprise workloads. FlexPod can scale up for greater performance and capacity (adding compute, network, or storage resources individually as needed), or it can scale out for environments that need multiple consistent deployments (rolling out additional FlexPod stacks). FlexPod delivers a baseline configuration, but also the flexibility to be sized and optimized to accommodate many different use cases.

This document focuses on the SnapProtect implementation on a FlexPod infrastructure, rather than the deployment and configuration of FlexPod itself. For collateral that speaks to the configuration and setup of the core FlexPod implementation, along with VMware, see the following hyperlinks. Figure 2 also helps illustrate the hardware families that define a FlexPod configuration.

- [FlexPod Deployment Guide](#)
- [VMware Built on FlexPod Deployment Guide](#)

Figure 2) FlexPod infrastructure.



### 3.1 Problem Statement

Customers face several questions as they transition toward shared infrastructure, or cloud computing, such as:

- What will be my return on investment?
- How do I build a future-proof infrastructure?
- How do I transition from my current infrastructure cost-effectively?
- Will my applications run properly in a shared infrastructure?

The FlexPod architecture is designed to help customers answer these questions with proven guidance and measurable value. FlexPod helps customers mitigate the risk and uncertainty involved with planning, designing, and implementing a new data center infrastructure.

### How Does FlexPod Add Value?

Cisco and NetApp have thoroughly tested and verified the FlexPod solution architecture and its many use cases while creating a portfolio of detailed documentation, information, and references to assist customers in transforming their data centers to this shared infrastructure model. This portfolio includes but is not limited to:

- Best practice architectural design
- Workload sizing and scaling guidance
- Implementation and deployment instructions
- Bills of materials and technical specifications
- Frequently asked questions (FAQs)

Cisco and NetApp have built a robust and experienced support team focused on FlexPod solutions, from customer account and technical sales representatives to professional services and technical support engineers. This foundation is further strengthened by a rich ecosystem of FlexPod delivery and solution partners.

The unprecedented experience, technology, and value delivered by Cisco and NetApp and the FlexPod ecosystem converge to help customers minimize risk and maximize their IT potential, shifting the focus from IT concerns back to the core business.

## How Does SnapProtect Add Value?

NetApp SnapProtect is a complete D2D2T backup and recovery solution for Data ONTAP® that seamlessly brings together NetApp's unique storage strengths such as:

- Storage efficiency
- Zero-impact Snapshot copies and clones
- Thin replication
- Array-based restores
- Modernized backup and recovery management and ease of use
- SPOG management for end-to-end backup and recovery
- Application-consistent Snapshot backups
- Seamless policy-based D2D2T data movement
- File and application catalog for Snapshot copies and tape backups
- Granular file-level recovery
- Automated inline secondary storage provisioning
- Native backup copies for other uses such as development, testing, and analytics
- Monitoring and reporting

## 3.2 FlexPod Technology

FlexPod is a predesigned and validated base configuration that includes:

- Cisco UCS and Cisco UCS Manager
- Cisco Nexus data center switches
- NetApp FAS systems

FlexPod includes all of the infrastructure elements that serve as the foundation for layering a broad range of workload solutions. Many customers require the ability to support a variety of operating systems. To satisfy this demand, FlexPod can be deployed as a virtualized, physical platform or hybrid environment.

As a general example, a VMware vSphere® built on FlexPod solution illustrates a fully virtualized environment, the Red Hat Enterprise Linux® built on FlexPod solution exemplifies a physical platform environment, and the SAP applications built on FlexPod solution demonstrates a hybrid approach.

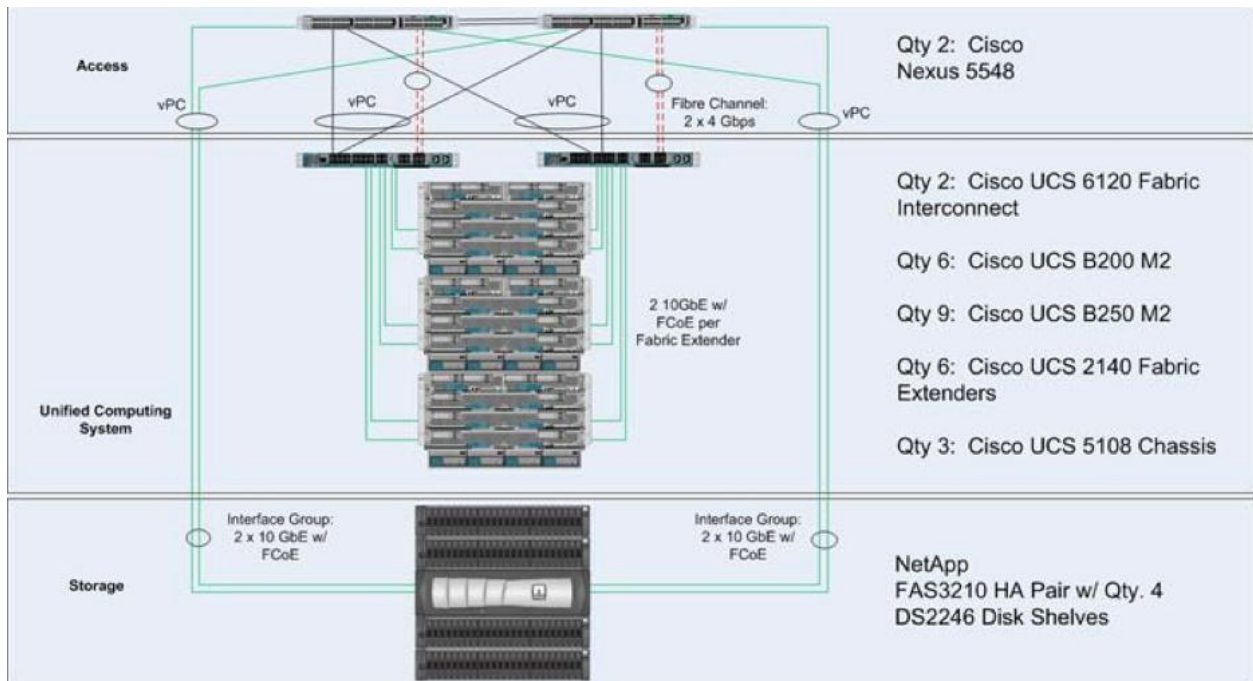
FlexPod has the flexibility to be sized and optimized to accommodate many different use cases or any combination of cases. For example, a customer who needs a FlexPod configuration to satisfy virtual desktop infrastructure (VDI) requirements might require higher capacity server and optimized NetApp Flash Cache™ technologies. For a development and test environment, a customer might require more compute resources but less storage because of the extreme efficiencies of NetApp storage. In contrast, for a data protection and backup environment, a customer might require less computing and more storage capacity.

The flexibility of the FlexPod shared infrastructure makes it a great foundation for many different use cases. Customers can begin with a small, simple FlexPod configuration and scale up or out as the needs



of the business grow. Figure 3 illustrates one example of a VMware vSphere interface built on FlexPod connectivity topology. Because of the inherent flexibility in supported configurations, FlexPod component details and connectivity can vary.

Figure 3) FlexPod physical topology (example).



### 3.3 Physical Infrastructure

#### 3.3.1 What We Validated On

Storage:

- NetApp FAS3270 controllers
- SnapProtect V9SP8
- OnCommand Core 5.1
- Data ONTAP 8.0.2P4 7-Mode
- 10Gb FCoE connected to Cisco Nexus 5000

Compute:

- Cisco UCS B-Series B200-M2 Blade Servers
- Cisco UCS 6100 Fabric Interconnects
- Cisco UCS Manager 2.0
- Cisco UCSM 2104 IOM modules

Network:

- Cisco Nexus 5000
- 10Gb FCoE
- 10Gb Ethernet
- Virtual PortChannels (vPCs) 10GbE connections to Cisco UCS and NetApp

Virtualization:

- VMware ESXi™ 5.0 Update 1
- Windows 2008 R2
- Red Hat Enterprise Linux 6.2

## **Cisco Nexus 5000 Series Switch Family**

The networking foundation for any FlexPod deployment is the Cisco Nexus 5000 series family of switches. The Cisco Nexus 5000 series switch enables any transport over Ethernet, including Layer 2 and Layer 3 traffic and storage traffic, on one common data center–class platform. Cisco Nexus 5000 series switches help transform data centers with a standards-based, multipurpose, multiprotocol, Ethernet-based fabric.

Cisco Nexus 5000 series switches are ideal for enterprise-class data center server access layer and smaller scale, midmarket data center aggregation layer deployments. These multipurpose, multilayer switches can be deployed across a diverse set of traditional, virtualized, unified, and high-performance computing (HPC) environments.

## **Cisco UCS Fabric Interconnects**

The Cisco UCS Fabric Interconnects are a core part of the Cisco UCS platform, providing both network connectivity and management capabilities for the system. The Cisco UCS Fabric Interconnects offer line-rate, low-latency, lossless 10GbE and Fibre Channel over Ethernet (FCoE) functions.

The Cisco UCS Fabric Interconnects provide the management and communication backbone for the Cisco UCS B-Series Blades and C-Series rackmount servers. All Cisco UCS blade and rackmount servers attached to the Cisco UCS Fabric Interconnects become part of a single highly available management domain. In addition, by supporting unified fabric, the Cisco UCS Fabric Interconnects provide both the LAN and the storage area network (SAN) connectivity for all blades within their domain. The VMware vSphere deployment described in this document is based on B-Series blade servers.

## **Cisco UCS B-Series Blades and Blade Server Chassis**

The Cisco UCS 5100 Series Blade Server Chassis is a crucial building block of the Cisco UCS system, delivering a scalable and flexible blade server chassis for today's and tomorrow's data center while helping reduce total cost of ownership (TCO).

Cisco's first blade server chassis offering, the Cisco UCS 5108 Blade Server Chassis, is six rack units (6RU) high and can mount in an industry-standard 19-inch rack. A chassis can house up to eight half-width Cisco UCS B-Series Blade Servers and can accommodate both half- and full-width blade form factors.

## **NetApp Fabric-Attached Controllers**

The NetApp Unified Storage Architecture provides customers with an agile and scalable storage platform. All NetApp FAS storage systems use the NetApp Data ONTAP operating system to provide SAN (FCoE, FC, iSCSI), NAS (CIFS, Network File System [NFS]), and primary and secondary storage within a single unified platform so that all data resources can be hosted within the same storage array. A unified storage platform for activities such as installation, provisioning, mirroring, backup, and upgrading is used throughout the entire NetApp FAS product line, from the entry level to enterprise-class controllers. NetApp unified storage delivers unprecedented simplicity and efficiency to even the most complex enterprise data management challenges, enabling customers to achieve measurable business value, such as:

- Reducing the complexity of data ownership
- Enabling companies to adapt to their changing business needs without interruption

- Reducing TCO

## 4 Use Cases Validated

### 4.1 Use Case 1

#### High-Level Description

Backup and recovery solution based on NetApp SnapProtect for customers deploying NAS shares to be accessed through NFS and/or CIFS on a FAS system in a FlexPod configuration accessed by Windows and Linux virtual machines running on VMware ESX server.

#### Layout and Requirements

- Type: NAS volumes
- Number of volumes: 20
- Files per volume: ~ 2M
- Average file size: 200KB
- Access method: NFS 50%, CIFS 50%
- Number of Windows VMs: 10
- Number of Linux VMs: 10
- Average VM size: ~ 40GB

#### Backup and Recovery Requirements

##### NAS Shares

- NAS Snapshot copies: 6 per day (every 4 hours)
- File indexing for NAS Snapshot copies: 1 per day (last Snapshot copy)
- Indexing level: initial full followed by daily incremental
- Snapshot retention on primary FAS: 1 week
- Snapshot retention in secondary SnapVault destination: 6 months
- Tape backup from SnapVault: once a month
- Tape retention: 5 years
- File-level restore capability from all backup copies: only indexed backups for this use case
- Volume-level restore from Snapshot copy: yes

##### Virtual Machines

- Virtual machine Snapshot copies: 6 a day (every 4 hours)
- Virtual machine file indexing (Windows VM only): 1 a day
- Indexing level
- Snapshot retention on primary FAS: 1 week
- Snapshot retention in secondary FAS SnapVault: 6 months: one Snapshot copy taken at a weekly frequency, retained for up to 6 months
- File-level restore capability from all backup copies: yes (excluding Linux VM file-level restore from Snapshot copy)
- Single VM restore from Snapshot copy: yes
- Datastore-level restore from Snapshot copy: yes

## Primary Replication Requirements

- All VMs and NAS shares are replicated to secondary FAS every two hours through SnapMirror (this is common DR practice)

Figure 4) CIFS access topology.

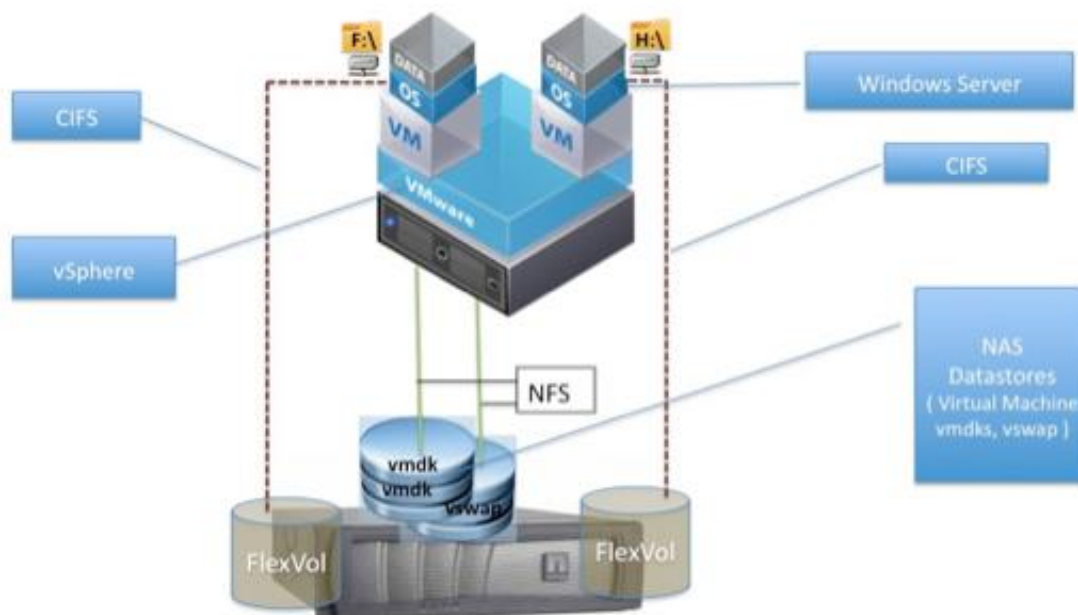
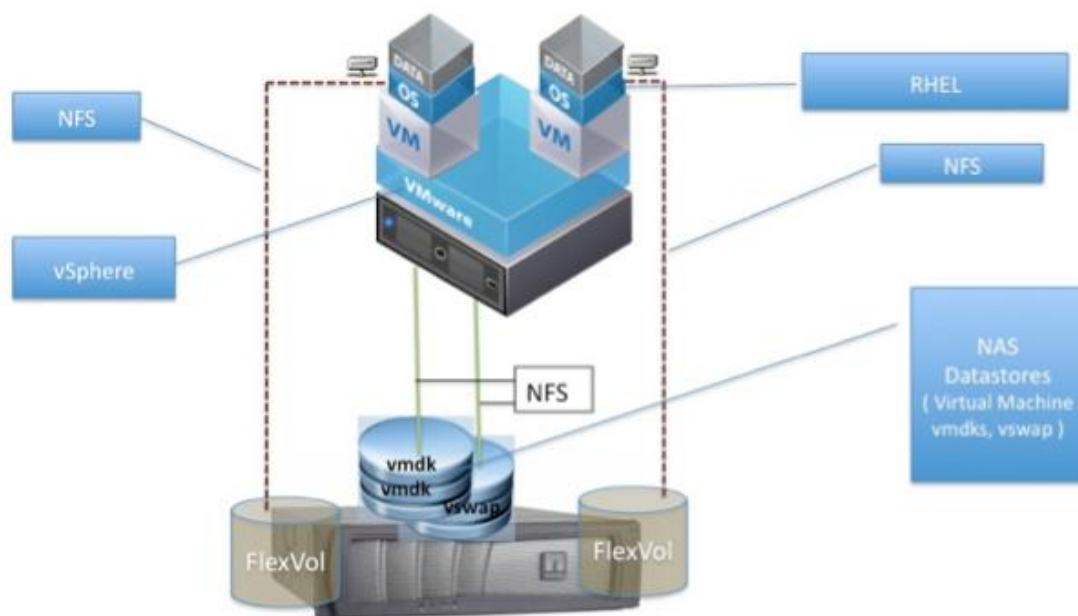


Figure 5) NFS access topology.



## 4.2 Use Case 2

### High-Level Description

Backup and recovery solution based on NetApp SnapProtect for customers deploying Microsoft Exchange Server 2010 in a FlexPod configuration.

### Layout and Requirements

Per requirements and configuration for “small DC” environment described in the Microsoft Exchange CVD (see section [References](#)).

### Backup and Recovery Requirements

- Exchange DB backup: 6 a day (every 4 hours)
- Transaction log backup: hourly
- Transaction log retention: 1 day
- Snapshot retention on primary FAS: 1 week
- Snapshot retention in secondary FAS: 6 months of weeklies
- Tape backup from SnapVault: once a month
- Tape retention: 5 years
- Mailbox-level restore capability from all backup copies: yes
- Database restore from Snapshot: yes
- Point in time recovery from logs: yes

### Virtual Machines

- Exchange environments virtual machine Snapshot copies: once a day
- Virtual machine file indexing (Windows VM only): once a day
- VM file-level indexing: initial full followed by daily incremental
- Snapshot copy retention on primary FAS: 1 week
- Snapshot copy retention in secondary FAS SnapVault: 6 months, weekly only
- File-level restore capability from all backup copies: yes
- Image-level restore from Snapshot copy: yes

### Disaster Recovery Requirements

- All Exchange VMs and DB LUNs replicated to secondary FAS every one hour

Figure 6) NAS and VMware topology.

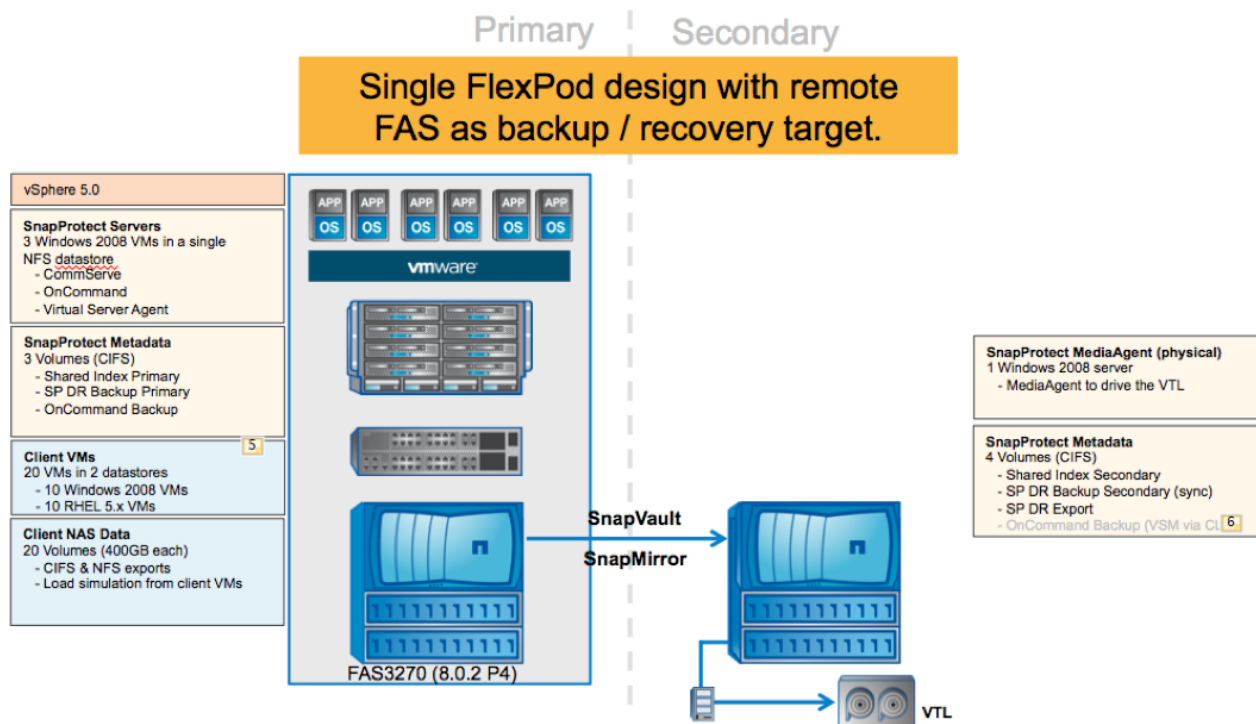
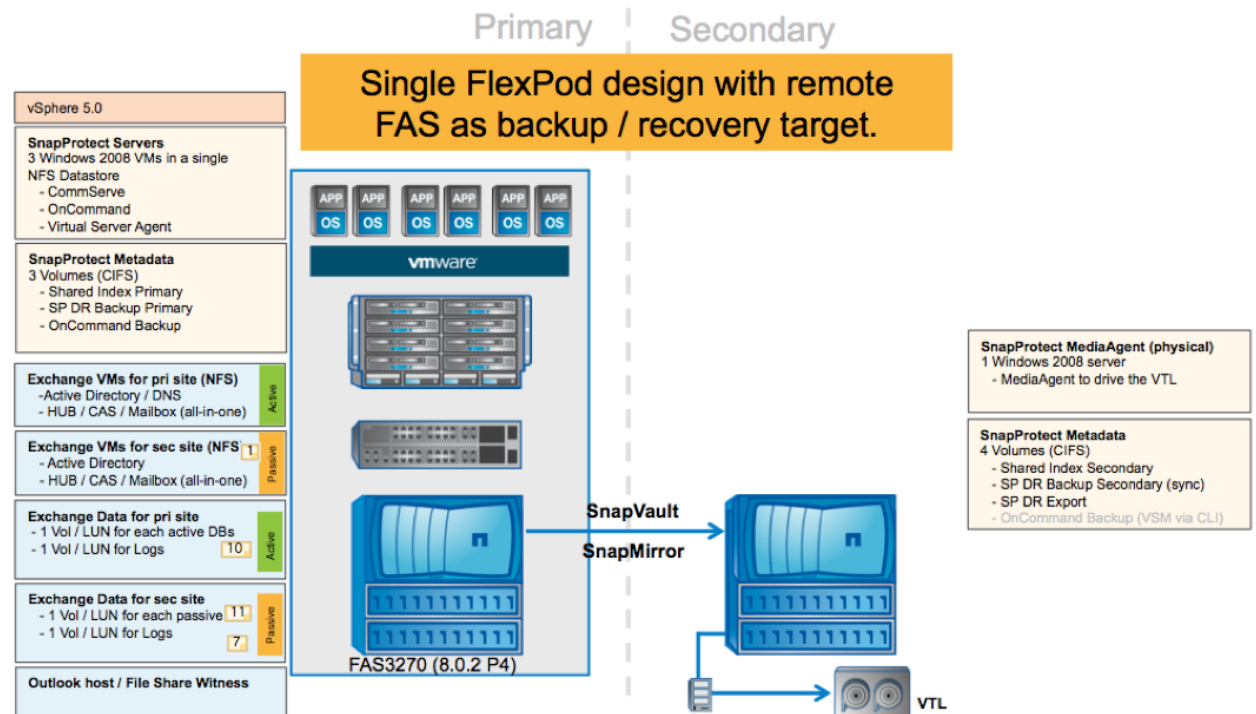


Figure 7) Exchange DAG.



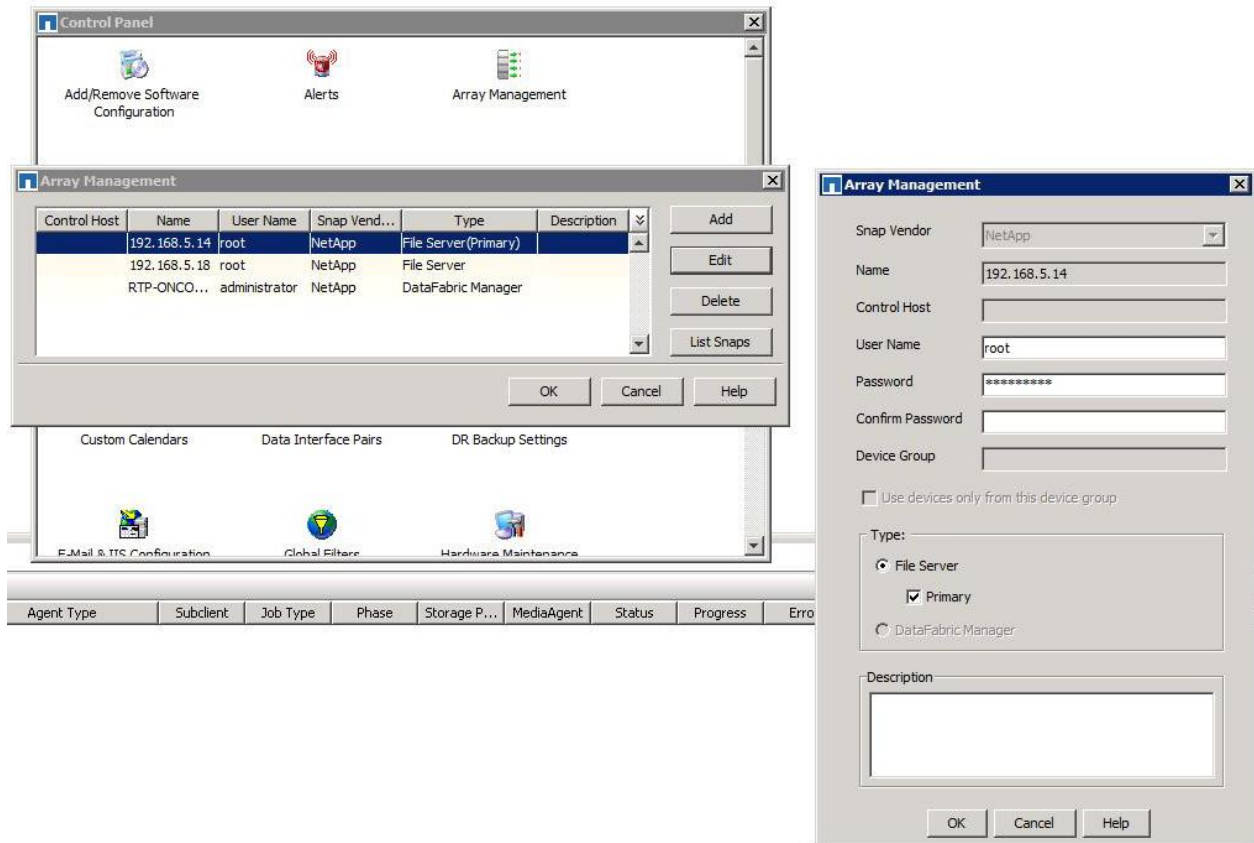


## 5 Configuration Procedure

For assistance with general SnapProtect deployment, leverage the [SnapProtect POC Cookbook](#), which is located in the [Field Portal](#). Reach out to your local SE to find an alternative solution if you're not authorized to access this link.

### 5.1 Array Management

To view the configured controllers and servers that SnapProtect will access and use (transparent to the end user) to perform backups and recovery in the SnapProtect GUI, click Control Panel > Array Management.



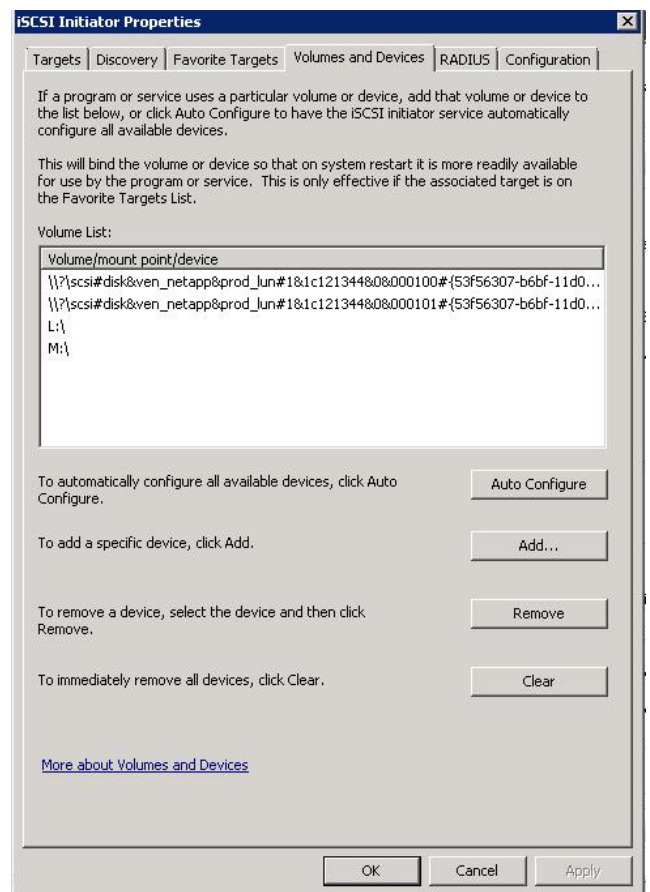
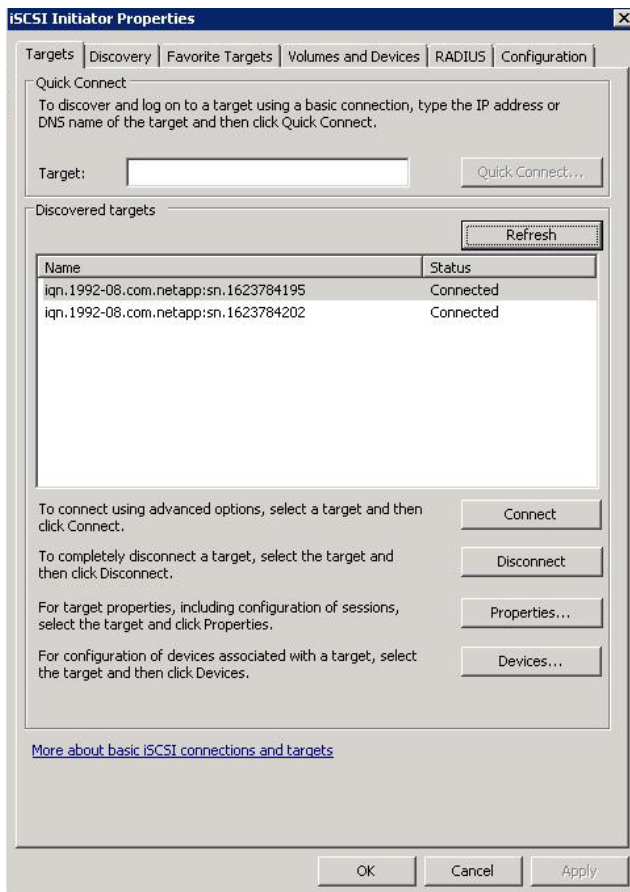
In our setup, the Array Management dialog box displays three storage controllers:

- The FAS in Raleigh with its IP ending with .14
- The secondary site located in San Jose with the IP ending in .18
- The OnCommand server (DFM) for provisioning and replication under the covers

To set the primary site, highlight the desired storage controller; click Edit. Select the Primary checkbox.

### 5.2 Backing Up an Exchange DAG Client

1. In the iSCSI Initiator Properties while logged into Exchange hosts (Raleigh's and San Jose's host) you can verify that Exchange DAG servers at both sites are configured and in a healthy state, verify that iSCSI ports are properly communicating, and view volumes (DB and logs).

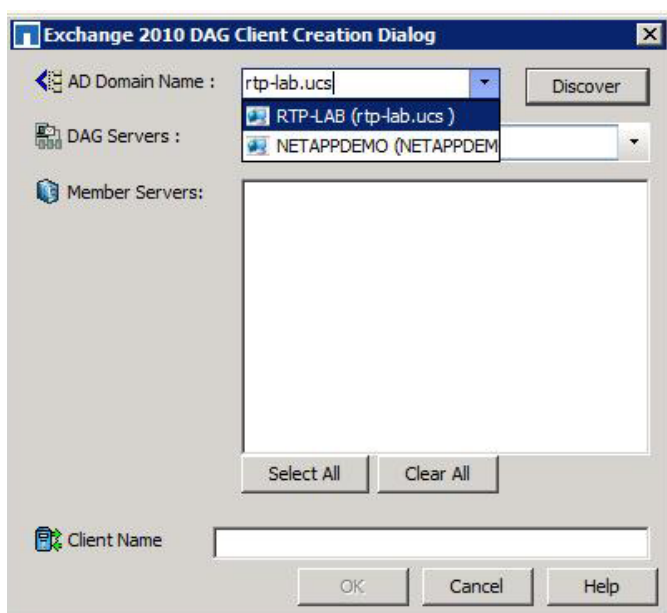


2. To add a new client, in the SnapProtect GUI, right-click Client Computers, and select Add New Client. From Select Client drop-down menu, select Exchange 2010 DAG client.

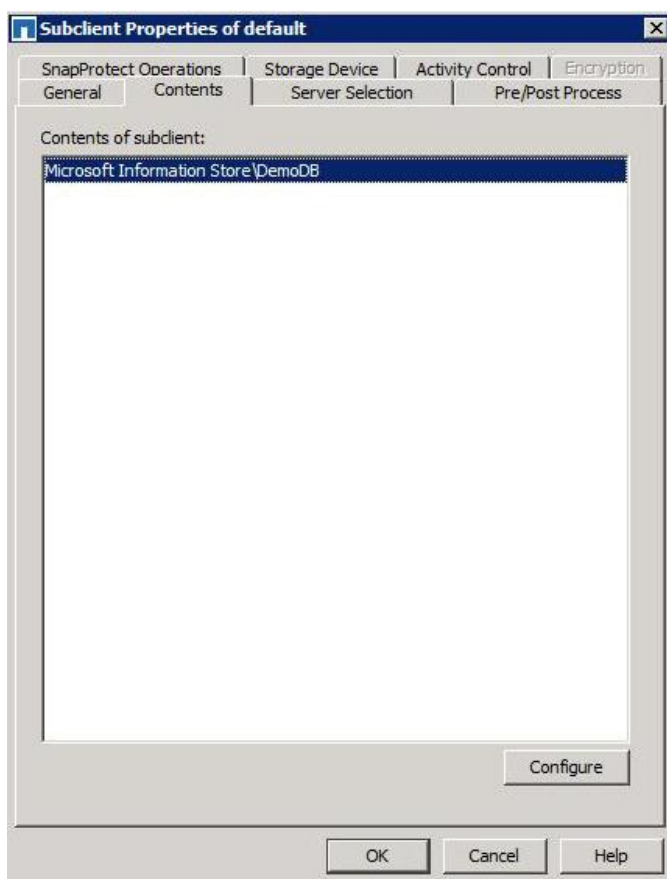




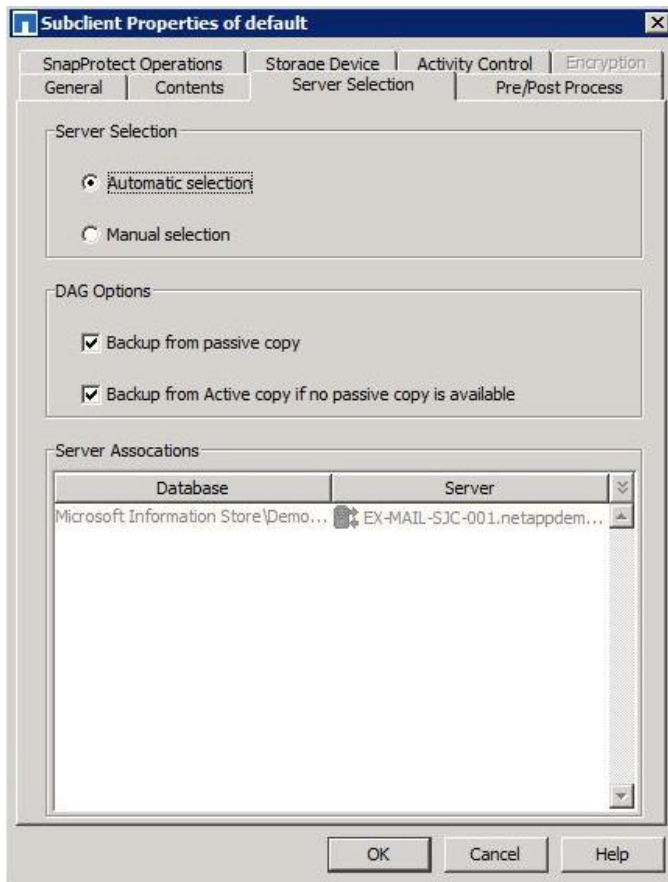
3. Choose appropriate domain and enter the AD server credentials if prompted.



4. The subclient configuration captures the content that will be backed up in the dataset. To configure the subclient, select the subclient, and click Configure.



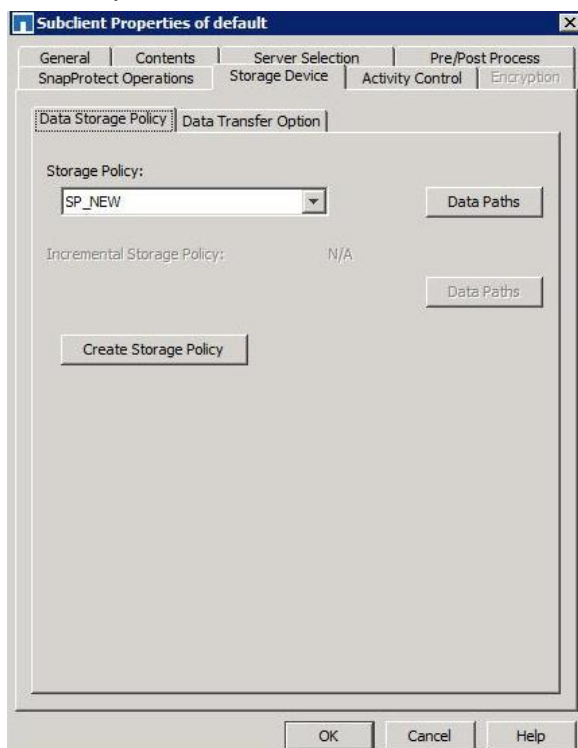
5. Select the “Automatic selection” option. Select the “Backup from passive copy” and “Backup from Active copy if no passive copy is available” checkboxes. In the Server Associations box, verify the database to server association.



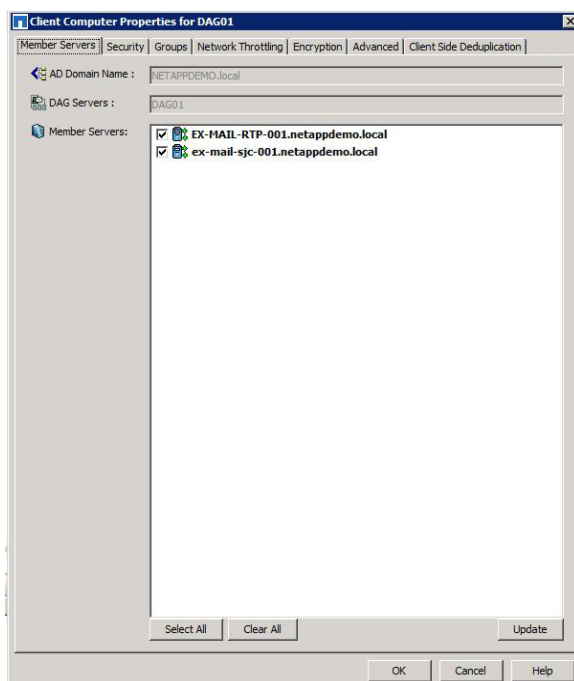
6. Click the SnapProtect Operations tab. Select your proxy servers, As shown in our example setup, ex-mail-rtp-001 and ex-mail-sjc-001 were selected as virtual proxy servers.



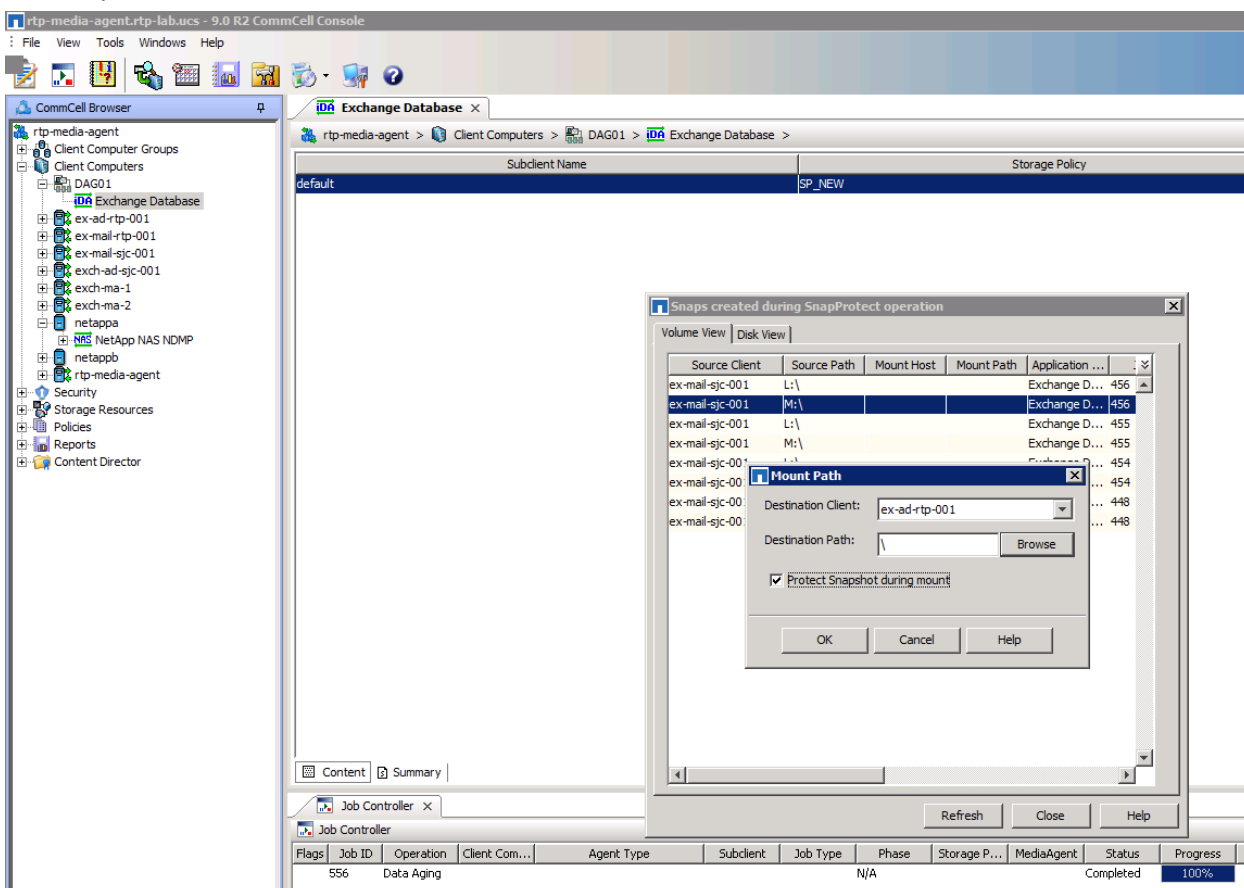
7. Click the Storage Device tab and then click the Data Storage Policy tab. Select the preferred Storage Policy to associate. You can also create a new storage policy by clicking Create Storage Policy.

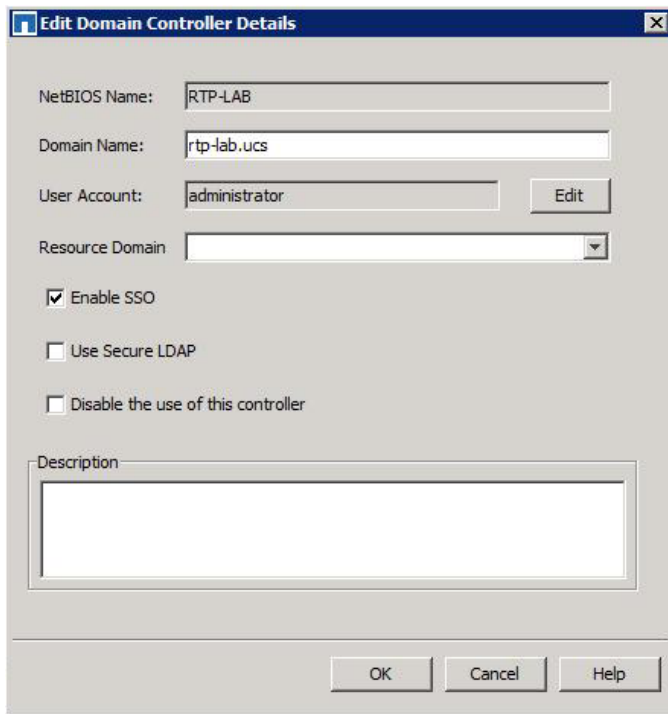


8. You can view both sites in the Member Servers tab.



9. To recover an Exchange DAG client, in the CommCell Browser navigation page, select DAG01 > List Snaps > Mount.

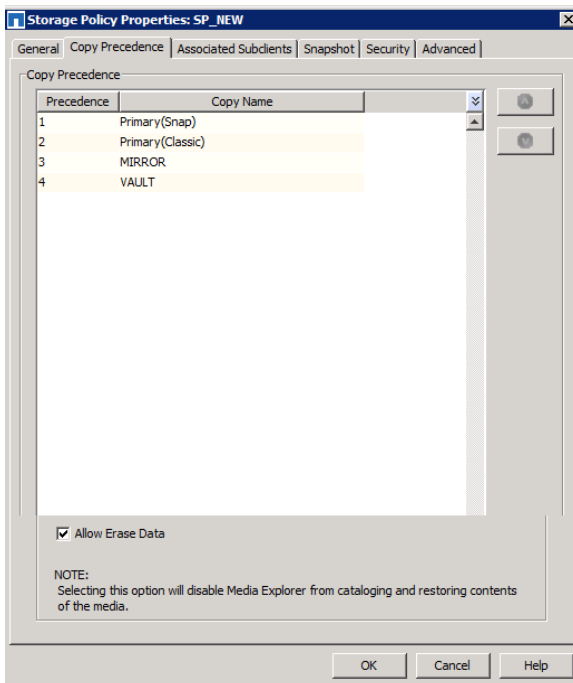




10. We created a name server (under Security category) to leverage for host name resolution.

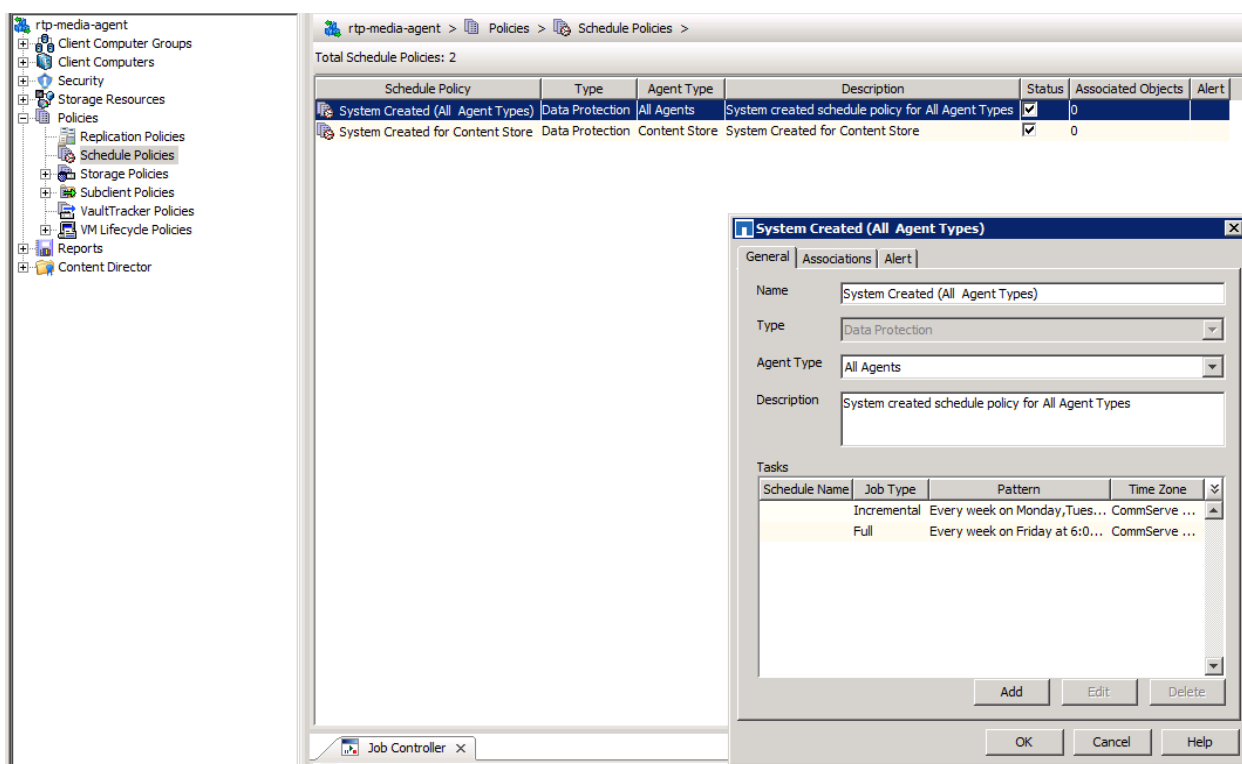
### 5.3 Copy Precedence

Using the copy precedence settings, you can specify the storage policy copy (1–4 in this example) from which you want data to be restored through the restore options of the individual agents.

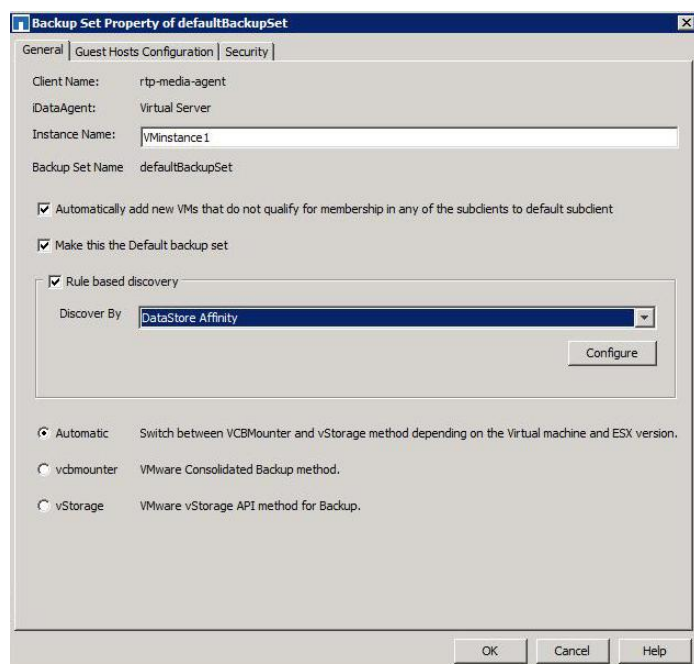


## 5.4 Scheduled Policies

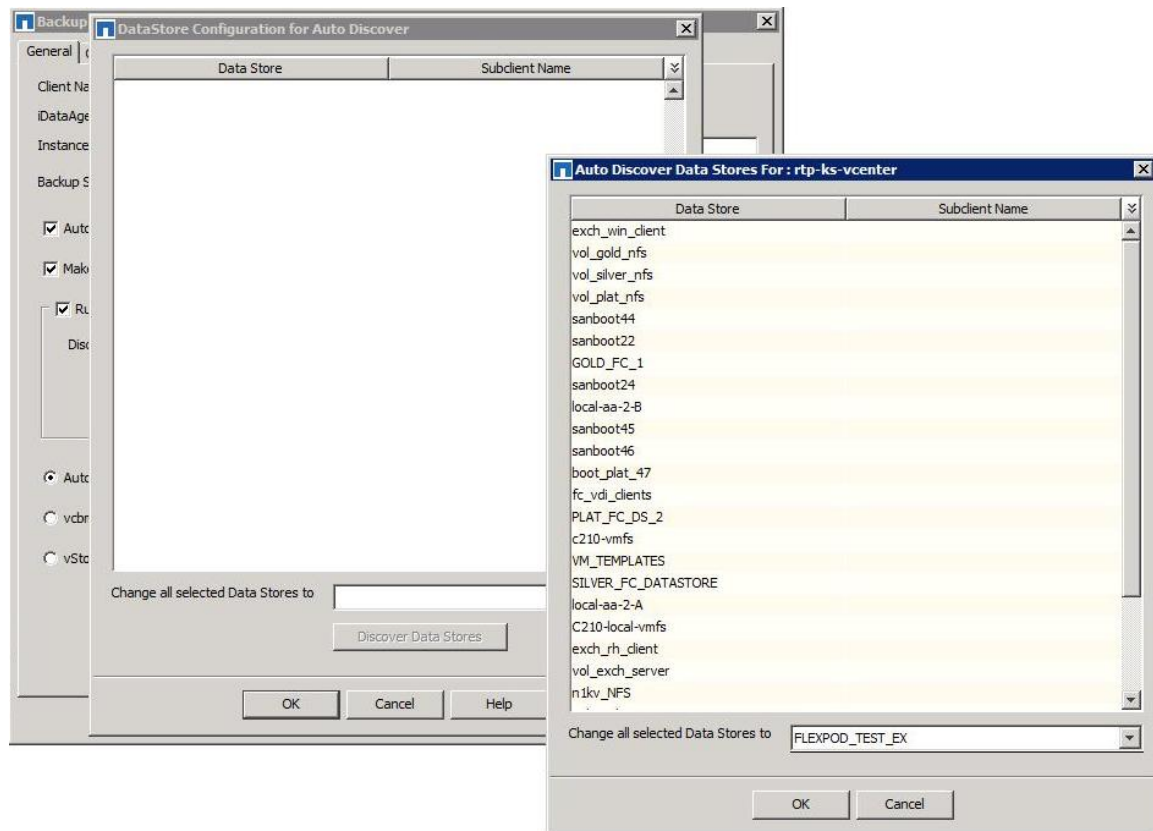
By scheduling policies, you can automate backup, recovery, and push install jobs. This is very useful in eliminating the need for manual onsite intervention during off-peak hours and maintenance windows.



Enabling the VMware datastore affinity rule will automatically find any newly created VMs within a datastore and include them in the backup set. This helps mitigate administration risk and prevent oversights in large, ever changing virtual environments.

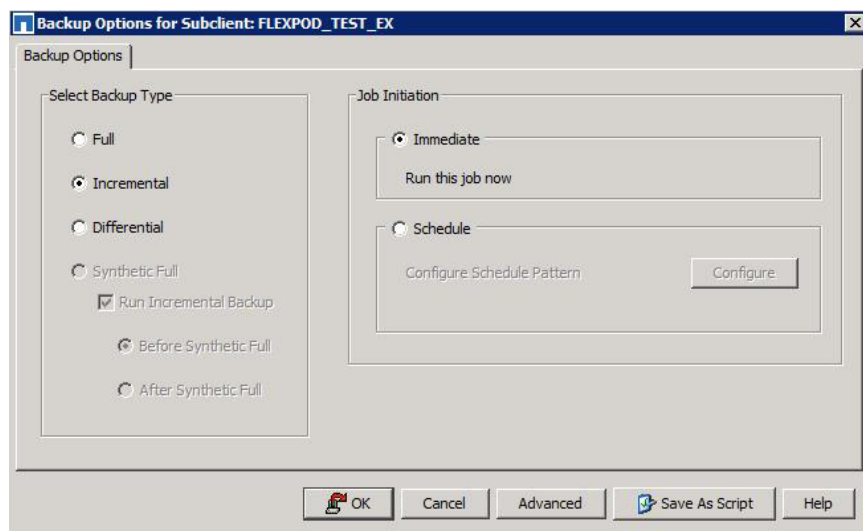


The datastore configuration for autodiscover feature is tightly integrated with VMware vCenter™. Clicking Discover Data Stores will open a list of datastores.



## 5.5 VMware Backup

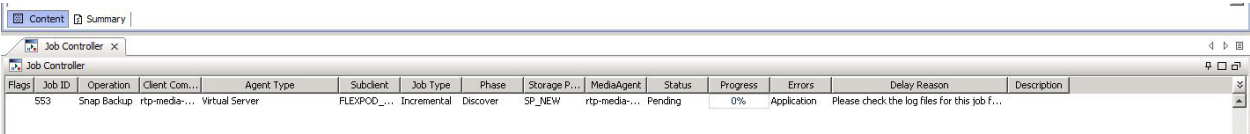
A full or incremental restore makes no difference here aside from for indexing/cataloging purposes. NetApp Snapshot technology always represents a full backup of your data.



You can view the progress of the backup job in the Job Controller window at the bottom of the screen.

The backup job will discover and communicate with vCenter to quiesce and create the VMware snapshot and then pass control back to storage array to create the NetApp Snapshot copy.

Indexing then occurs and is added to the catalog of the backup. All is completed and transparent to the user by leveraging OnCommand.

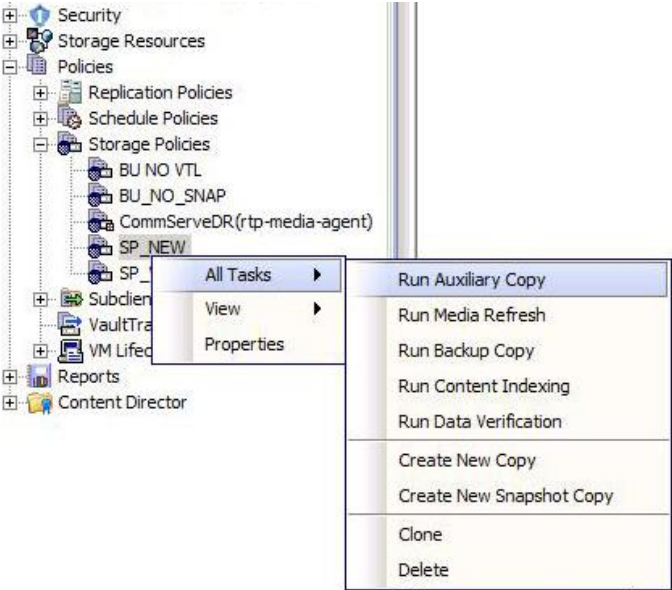


Flags	Job ID	Operation	Client Com...	Agent Type	Subclient	Job Type	Phase	Storage P...	MediaAgent	Status	Progress	Errors	Delay Reason	Description
	553	Snap Backup	rtp-media...	Virtual Server	FLEXPOD...	Incremental	Discover	SP_NEW	rtp-media...	Pending	0%	Application	Please check the log files for this job f...	

5.6 Auxiliary Copy

After creating the primary Snapshot copy, you can then replicate it by using SnapVault, SnapMirror, NDMP, or SMTape to secondary or tertiary sites for further retention. An auxiliary copy is any replication off of the primary site, whether it be to a secondary, tertiary, or other site.

To run auxiliary copy, right-click the appropriate storage policy and select All Tasks > Run Auxiliary Copy.



The auxiliary copies are retained based on the retention policy. The Retain For column displays the policies that were defined based on the RPO/RTO requirements set in our use cases mentioned previously.

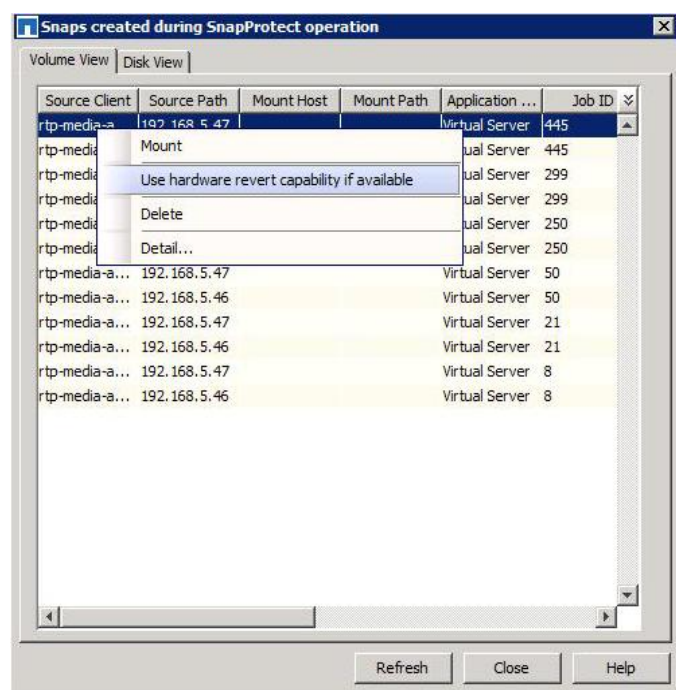
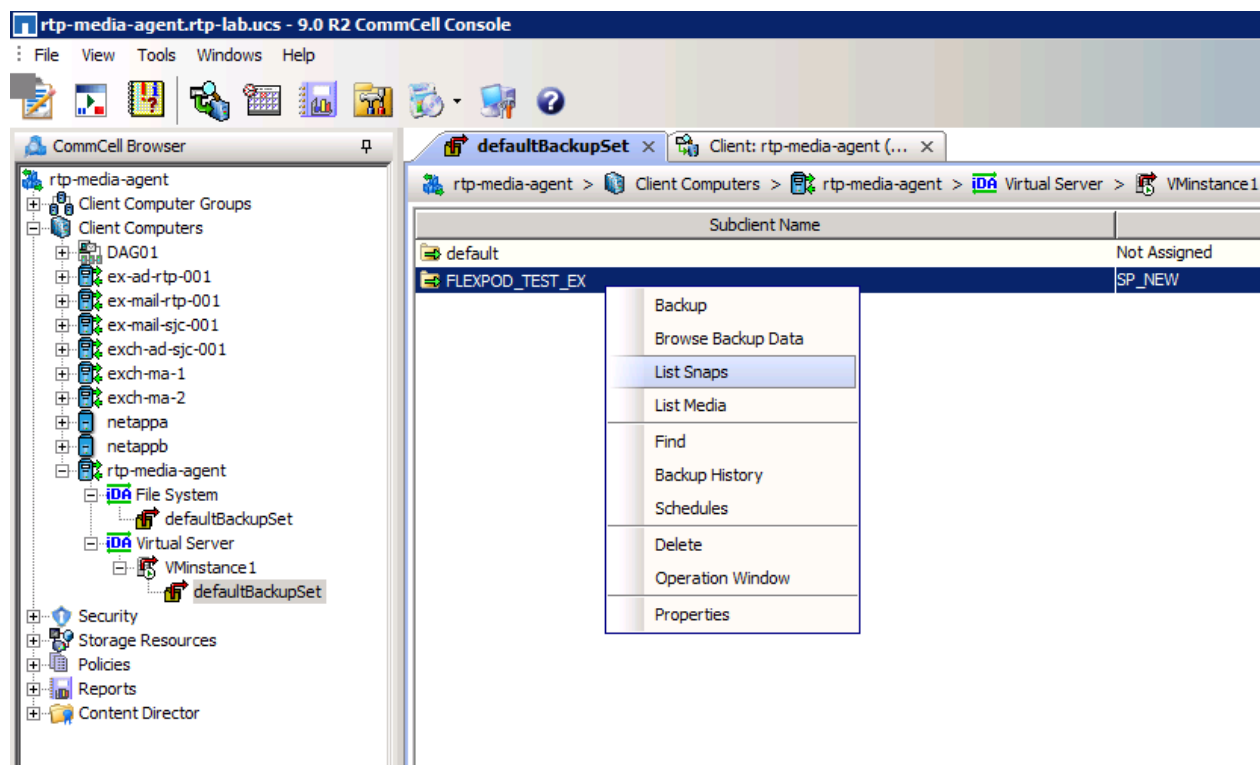
Copy	Copy Type	Default Library	MediaAgent	Default Drive Pool	Scratch Pool	Retain For	Archiver data Ret.	Retain by Jobs	Hardware Compression	Source Copy
MIRROR	Snap Mirror	NETAPP VTL 1	rtp-media-agent	DrivePool(tp-media-ag... Default Scratch		Not Applicable	Not Applicable	24	✓	Primary(Snap)
Primary(Classic)	Primary	NETAPP VTL 1	rtp-media-agent	DrivePool(tp-media-ag... Default Scratch		28 days, 2 cycles	Infinite	Not Applicable	✓	
Primary(Snap)	Snap Primary	NETAPP VTL 1	rtp-media-agent	DrivePool(tp-media-ag... Default Scratch		Not Applicable	Not Applicable	24	✓	
VAULT	Snap Vault	NETAPP VTL 1	rtp-media-agent	DrivePool(tp-media-ag... Default Scratch		7 days, 0 cycles	Not Applicable	Not Applicable	✓	Primary(Snap)



## 5.7 VMware Restore

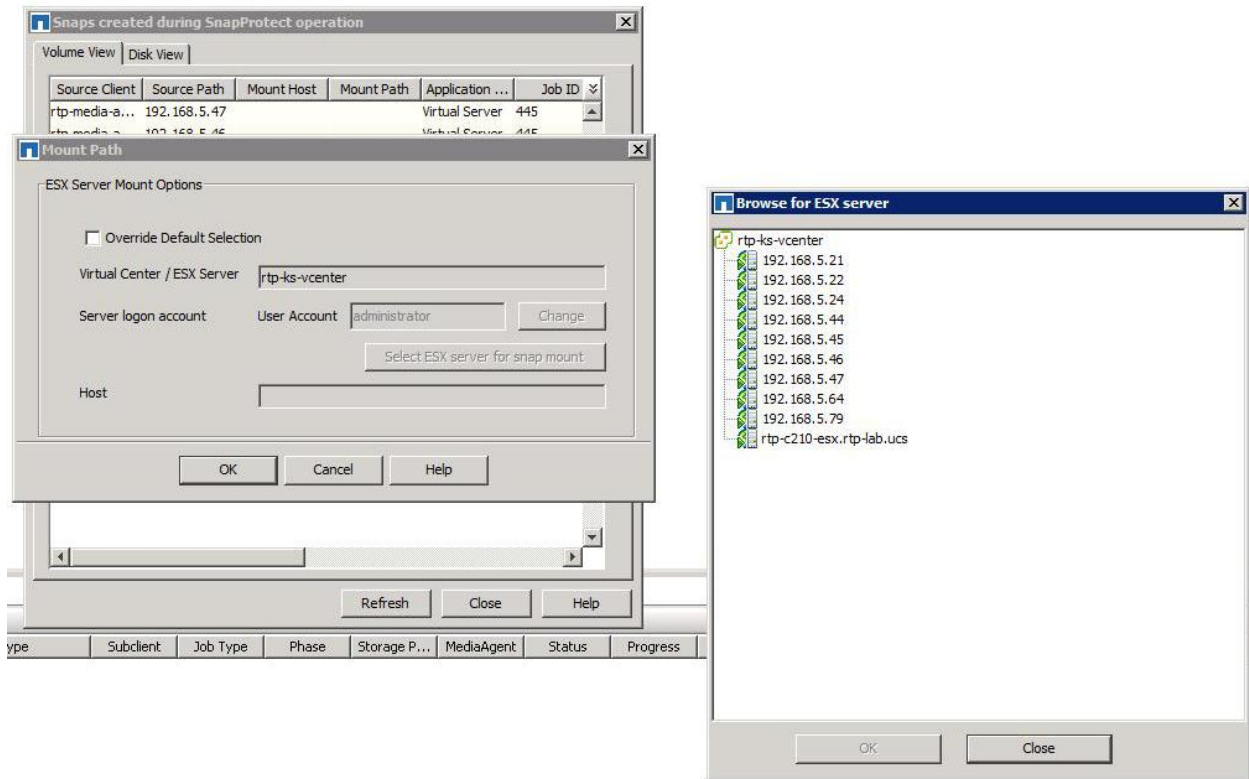
### Option 1

This hardware revert option, also known as single-file SnapRestore® (SFSR), provides very fast array-based (flipping bits versus streaming data) restores of Windows VMs. The Snapshot copy has to be located on the primary on which the restore is occurring.



## Option 2

The other option to perform a revert is to right-click the default backup set created previously and select “Mount.” Select the specific ESX server that you want to use.



## 6 Testing

1. Run backup.
  - a. Right-click the subclient and select Backup.
  - b. Select Full Backup.
  - c. Under Advanced Options, clear the selection for Skip Catalog Phase for SnapProtect (for NAS).
  - d. For VMware, under Advanced Options, select the Enable Granular Recovery checkbox.
  - e. Click OK and then click OK again.
  - f. Monitor the job controller for job status.
2. Run auxiliary copy.
  - a. Right-click the appropriate storage policy and select All Tasks > Run Auxiliary Copy.
  - b. Click OK.
  - c. Monitor the job controller for job status.
3. Restore the data.
  - a. Right-click the appropriate subclient and select Browse Backup Data.
  - b. Click OK.
  - c. Expand the backup set and the volume (or VM to restore).
  - d. Select the data to be restored.

- e. Click Recover All Selected.
  - f. For VMware, clear the selection for the Restore in Place checkbox and rename the VM.
  - g. Click OK to restore to the same folder or provide an alternate destination path and then click OK.
  - h. Monitor the job controller for job status.
4. Restore single file from VMware backup (single mail from Exchange follows similarly).
    - a. Right-click the VMware subclient and select Browse Backup Data.
    - b. Select Individual Files/Folders.
    - c. Click OK.
    - d. Expand Backup Set.
    - e. Expand the VM and select a file or directory to restore.
    - f. Click Recover All Selected.
    - g. Specify a staging path on the media agent. The file will be restored to this location.
    - h. Click OK.
    - i. Monitor the job controller for job status.

## 7 Conclusion

FlexPod is the optimal shared infrastructure foundation on which to deploy a variety of IT workloads. Cisco and NetApp have created a platform that is both flexible and scalable for various use cases and applications. SnapProtect revolutionizes the way you think about backups. With ability to leverage Snapshot backup and recovery and index/catalog, along with the ability to manage your entire D2D2T environment from a SPOG, the value is clear. The flexibility and scalability of FlexPod also enable customers to start out with a right-sized infrastructure that can ultimately grow with and adapt to their evolving business requirements with the cost-effective controller-based licensing model of SnapProtect.

## Appendix

### Supporting Documents

- System requirements can be found at:  
[https://support.netapp.com/NOW/knowledge/docs/snapprotect/relsnap\\_protect90sp8/215-07337\\_A0\\_books\\_online\\_90sp8/books\\_online\\_1/default.htm](https://support.netapp.com/NOW/knowledge/docs/snapprotect/relsnap_protect90sp8/215-07337_A0_books_online_90sp8/books_online_1/default.htm)
- The hardware compatibility matrix lists supported devices  
[http://support.netapp.com/NOW/knowledge/docs/olio/guides/snapprotect/hardware\\_compatibility\\_matrix.shtml](http://support.netapp.com/NOW/knowledge/docs/olio/guides/snapprotect/hardware_compatibility_matrix.shtml)
- SnapProtect Sizing Guide  
<https://fieldportal.netapp.com/viewcontent.asp?qv=1&docid=39673>
- TR-3920: NetApp SnapProtect Management Software: Overview and Design Considerations  
<http://www.netapp.com/us/library/technical-reports/tr-3920.html>
- SnapProtect SE Presentation  
<https://fieldportal.netapp.com/viewcontent.asp?qv=1&docid=33211>
- VMware vSphere Built on FlexPod with IP-Based Shared Storage  
[http://www.cisco.com/en/US/docs/unified\\_computing/ucs/UCS\\_CVDs/cisco\\_ucs\\_vmware\\_ethernet\\_flexpod.html](http://www.cisco.com/en/US/docs/unified_computing/ucs/UCS_CVDs/cisco_ucs_vmware_ethernet_flexpod.html)
- Red Hat Enterprise Linux Built on FlexPod Deployment Guide  
[http://www.cisco.com/en/US/docs/solutions/Enterprise/Data\\_Center/Virtualization/flexpod\\_rhel.html](http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/Virtualization/flexpod_rhel.html)

- Microsoft Exchange 2010 with VMware VSphere on Cisco Unified Computing System with NetApp Storage  
[http://www.cisco.com/en/US/docs/solutions/Enterprise/Data\\_Center/App\\_Networking/Exchange\\_VSphere\\_UCS\\_NetApp.html#wp343440](http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/App_Networking/Exchange_VSphere_UCS_NetApp.html#wp343440)
- SnapProtect V9 SP8 Books Online  
[https://support.netapp.com/NOW/knowledge/docs/snapprotect/relnap\\_protect90sp8/](https://support.netapp.com/NOW/knowledge/docs/snapprotect/relnap_protect90sp8/)

## Glossary

Table 1) Terms used.

Component	Description
CommCell	A single instance of a SnapProtect environment.
CommServe	The master server in a SnapProtect environment. This server uses a Microsoft SQL Server database and therefore must be a Microsoft Windows system (Windows Server 2003 or 2008).
Media agent	A media server in a SnapProtect environment. Media agents have broad operating system support, including Windows, Linux, and UNIX options.
CommCell console	The SnapProtect management interface.
iDataAgent (iDA)	The agents that control data consistency during backup operations.
Clients	Hosts running iDAs for which data is protected.
Backup set	A layer of management within iDAs for grouping subclients.
Subclient	A layer of management within a backup set. A client can have multiple subclients, each of which can be associated with different source data.
Disk library	A storage resource with an associated mount path that is used in the SnapProtect solution to store index information backups.
Storage policy	A logical object through which a subclient is protected. The storage policy defines how data is backed up and replicated; it also defines the retention requirements.
OnCommand server	A server running NetApp OnCommand server software. The OnCommand server and the CommServe server should typically be separate systems.
NetApp Management Console (NMC)	The NMC is an interface used for creating resource pools and provisioning policies within the OnCommand framework. The NMC should be installed on a separate system from the OnCommand server.
NetApp primary	The production NetApp storage array.
NetApp secondary	The secondary NetApp storage array used as a destination for replication.
NetApp tertiary	A third NetApp storage array used for replicating previously replicated data.
Snapshot copy	A NetApp array-based point-in-time copy used for recovering data.
SnapVault	A NetApp replication technology used for backup and recovery. In the SnapProtect solution, a vault copy uses SnapVault.
SnapMirror	A NetApp replication technology used for DR. In the SnapProtect solution, a mirror copy uses SnapMirror.

Refer to the [Interoperability Matrix Tool \(IMT\)](#) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

NetApp provides no representations or warranties regarding the accuracy, reliability, or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer's responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.

[Go further, faster®](#)