NETAPP SOLUTION DEPLOYMENT GUIDELINES

Thomson Reuters Professional – VMware on NetApp – Deployment Guidelines

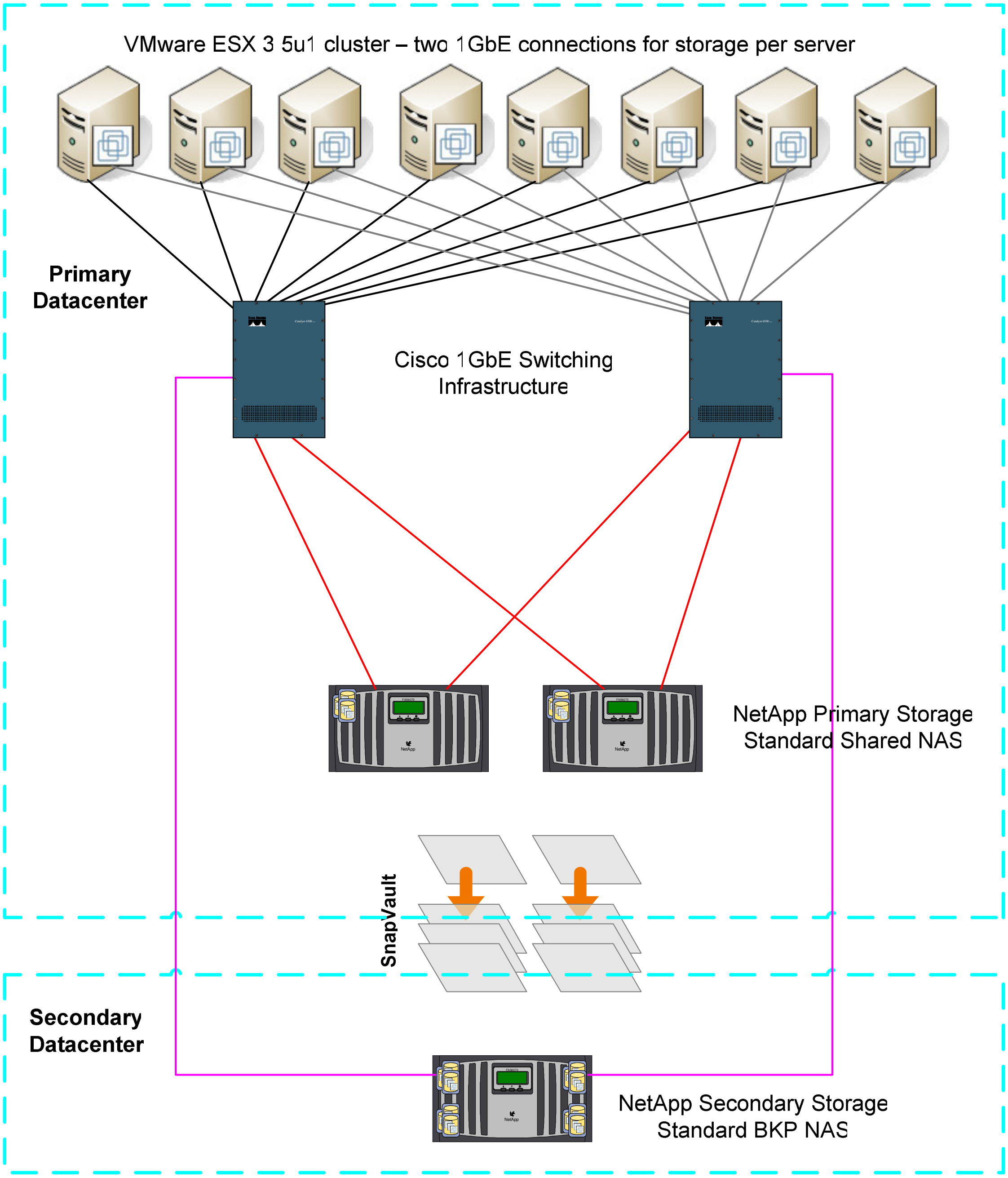
Prepared By:
Michael Arndt
arndt@netapp.com

Version 10: 2009-02-23

Table of Contents

1. Executive Summary

This document outlines the deployment guidelines for the VMware environment in Thomson Reuters Professional using NetApp storage. VMware ESX 3.5u1 will be deployed with NetApp storage to implement an improved backup and recovery architecture using NetApp SnapShot and SnapVault. Storage for the VMware environment will be accessed via the NFS protocol, and will utilize the standard shared NAS environment already in place within each datacenter at Thomson Reuters Professional. The high level logical architecture drawing below outlines the configuration and the remainder of this document will provide the details surrounding each component of the solution as it relates to storage and backup / recovery of the VMware environment.


VMware ESX 3 5u1 cluster – two 1GbE connections for storage per server
Primary Datacenter
Cisco 1GbE Switching Infrastructure
NetApp Primary Storage Standard Shared NAS
SnapVault
Secondary Datacenter
NetApp Secondary Storage Standard BKP NAS

2. VMware ESX Server Configuration

2.1 Datastore configuration

The VMware ESX servers will be using NFS datastores. NFS datastores can be provisioned from the Virtual Center management interface. Every NFS datastore provisioned for a VMware ESX cluster must be connected to each node in the cluster. NetApp recommends creating the following datastores on each VMware ESX cluster:

Datastore Description	Datastore Name	NFS Storage Path
VMs that do not require backup	<vmware_cluster>_vms_nosnap	<filer>:/vol/infra_<vmware_cluster>_vms_nosnap
VMs with 7 days of backup	<vmware_cluster>_vms_snap07	<filer>:/vol/infra_<vmware_cluster>_vms_snap07
VMs with 14 days of backup	<vmware_cluster>_vms_snap14	<filer>:/vol/infra_<vmware_cluster>_vms_snap14
VMs with 45 days of backup	<vmware_cluster>_vms_snap45	<filer>:/vol/infra_<vmware_cluster>_vms_snap45
VMware ESX virtual swap files	<vmware_cluster>_vmw_nosnap	<filer>:/vol/infra_<vmware_cluster>_vmw_nosnap

In the above table, the <vmware_cluster> specification will be the cluster portion of the virtual host naming convention as defined by Thomson Reuters. This string will be provided by the VMware team when they make a request for storage to the Thomson storage team.

2.2 ESX NFS Datastore heartbeat settings

The NFS client in VMware ESX has timeout settings that dictate when it considers a NFS datastore to be offline. These settings should be modified from their default in order to accommodate the amount of time it takes to perform a cluster failover event on a NetApp storage system. The following steps should be followed on every ESX 3.5 server in the cluster in order to set the appropriate NFS timeout values:

1. Open VirtualCenter.
2. Select an ESX host.
3. In the right pane, select the Configuration tab.
4. In the Software box, select Advanced Configuration.
5. In the pop-up window, left pane, select NFS.
6. Change the value of NFS.HeartbeatFrequency to 12.
7. Change the value of NFS.HeartbeatMaxFailures to 10.
8. Repeat for each ESX Server.

2.3 ESX virtual swap location

VMware ESX server requires virtual swap space for each virtual machine, equal in size to the memory allocated to the virtual machine. This virtual swap space is required to be on storage that is shared across the VMware cluster in order to facilitate VMware features such as VMotion. The storage used for virtual swap does not require backup, as it is re-initialized every time a virtual machine is booted. Because the data in the virtual swap space does not require backup, a separate NFS datastore is to be provisioned for it in each VMware cluster. The following process details how to move the virtual swap space for a virtual machine to a separate datastore than the one used for the actual virtual machine data.

1. In VirtualCenter right-click the ESX cluster and select Edit Settings. Click Swapfile Location and choose the option “Store the swapfile in the datastore specified by the host.” Click OK.
2. In the VirtualCenter configuration tab for **each** ESX host in the cluster, click the Virtual Machine Swapfile Location link.
3. Click the Edit link and select the shared datastore for this cluster that has been allocated for virtual swap space.

2.4 Guest Operating System (GOS) virtual disk alignment

The starting partition offset on each GOS virtual disk should be such that each 4k, or multiple of 4k, I/O from the GOS is performed within a single 4k, or multiple of 4k, block on the storage array. If this is not performed, for example, a 4k I/O from the GOS may require two 4k I/Os to be performed on the storage array, and performance of the storage array will suffer as the number of virtual machines performing I/O increases.

2.4.1 GOS virtual disk alignment on Windows virtual machine templates

When deploying Windows virtual machines via a template, the partition(s) on the VMDK(s) should be configured such that the starting offsets are a multiple of 4096. This can be done by connecting the VMDK file for your template to a running Windows virtual machine and using the “diskpart” utility to create the partition(s) prior to actually installing Windows. Be aware that using the diskpart utility to create partitions would destroy any previously existing data on a VMDK, so this should only be used as part of the process when creating new virtual machines that will be used as templates. Once you have a properly aligned template, all virtual machines deployed from the template will also be properly aligned.

The following is an example of creating a properly aligned partition on disk 1 using diskpart:

```
C:\>diskpart
DISKPART> list disk
DISKPART> select disk 1
Disk 1 is now the selected disk.
DISKPART> create partition primary align=32
```

Correct alignment of Windows virtual machines can be verified using the “msinfo32” utility. Using ms32info, navigate to System Summary -> Components -> Storage -> Disks and look at the Partition Starting Offset. The Partition Starting Offset will be evenly divisible by 4096 if it is properly aligned.

2.4.2 GOS virtual disk alignment on Windows virtual disks created via P2V

Since the data on virtual disks created as part of the P2V process needs to be retained, we can not use diskpart to correct the alignment on virtual machines that have been created in this manner. Instead, NetApp provides a tool call “mbralign” that can be run from the ESX 3.5 service console in order to correct the alignment on a Windows virtual disk while maintaining the contents of the virtual disk. To use mbralign, simply run “mbralign /path/to/virtual_machine.vmdk” from the ESX service console. Since the mbralign tool can only work on virtual disks for virtual machines that are not running, the ideal time to run mbralign will be after the initial P2V process, as that process already involves downtime for the virtual machine.

2.4.3 GOS virtual disk alignment on Linux virtual machine templates

For non-boot virtual disks, the entire device can be used for the filesystem if desired. For example, running “mkfs –t ext3 /dev/sdb” would create a filesystem on the entire virtual disk backed by /dev/sdb, and I/O using this virtual disk would be properly aligned.

For boot virtual disks, or virtual disks with multiple partitions, use the “fdisk” command as follows:

1. Run the **fdisk** command on your new virtual disk after attaching it to a different temporary Linux VM.
2. Type **n**, and create new primary partitions as desired for your disk layout.
3. Type **t** to se the partition system IDs. Type **82** for swap, type **83** for ext3, and type **8e** for LVM partitions.
4. Type **x** to go into expert mode.
5. Type **b** to set the starting block number for each partition. The starting block number should be increased slightly from the original value, so that it is evenly divisible by 8. For example, if the starting block number is **63**, change it to **64**.
6. Type **w** to write label and partition information to disk.

As with the use of diskpart for Windows virtual disks, the use of fdisk to create a properly aligned partition assumes that all other data on the virtual disk will be destroyed. As such, this should only be used to create a template so that virtual machines deployed from the template are properly aligned. Once the new virtual disk has properly aligned partitions on it, you can disconnect it from the temporary VM and install Linux on the new VM.

2.4.4 GOS virtual disk alignment on Linux virtual disks created via P2V

NetApp does not currently offer a tool to automate the process of properly aligning Linux virtual disks. However, as of the writing of this document, all Linux virtual machine deployments at Thomson Reuters Professional are planned to be performed based off a template. Since the P2V process is not currently in use for Linux virtual machines, this is not an issue for Thomson Reuters Professional. If Linux virtual machines are created via the P2V process in the future, the topic of properly alignment these virtual disks should be revisited.

2.5 Guest Operating System (GOS) disk timeout settings

GOS should be configured such that they will not timeout during a cluster failover event on a NetApp storage cluster. Typical cluster failover events complete within 30-60 seconds on NetApp storage clusters, but best practice is to configure the GOS to withstand a longer delay in I/O to accommodate rare instances of longer failover events.

2.5.1 GOS disk timeout settings on Windows virtual machines

Change the Registry Parameter DiskTimeOutValue in Windows Guest Operating System under *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Disk\TimeOutValue* to *190* (Decimal).

2.5.2 GOS disk timeout settings on Linux virtual machines

Follow the instructions in the following NetApp knowledgebase article to properly set the disk timeouts on Linux virtual machines:

https://now.netapp.com/Knowledgebase/solutionarea.asp?id=kb41511

This knowledge base article contains links to scripts from NetApp engineering that will automatically set the correct disk timeouts for various Linux distributions.

3. NetApp storage system configuration

3.1 Storage system requirements

Storage for VMware ESX servers should be deployed on the latest standard high tier shared NAS environment at Thomson Reuters Professional. As of the writing of this document, that consists of a FAS6080 storage cluster with 300GB 15k RPM drives, running Data ONTAP 7.2.4 at a minimum, with 7.2.5.1 or higher preferred. The old high tier shared NAS environment, consisting of FAS980 storage clusters with 144GB 10k RPM drives, running Data ONTAP 7.2.3, is not recommended because it does not support NetApp data de-duplication.

3.2 Aggregate configuration

The following considerations should be kept in mind in terms of aggregate configuration:

- The aggregate should be named *aggrX_thin_vm*, where *X* is the aggregate number.
- The starting aggregate size to provide storage for VMware ESX clusters should be at least one full raid group of 17 15k RPM 300GB FC drives, which would provide about 3400GB of usable disk space.

- A standard size (and fully populated) VMware ESX cluster would consist of 6 nodes with 30 VMs per nodes, or 180 VMs in total. Assuming 50GB of space for each VM, this would require 9TB of storage prior to performing data deduplication.
- Provision one standard size VMware ESX cluster per aggregate if data deduplication is not in use.
- Provision two standard size VMware ESX clusters per aggregate if data deduplication is being used.
- More than two VMware ESX clusters can be provisioned per aggregate if the VMware ESX clusters are not planned to grow to the full configuration of 180 VMs. In this instance, capacity and performance resources must be monitored in order to determine how many VMware ESX clusters to provision per aggregate.

3.3 Volume configuration

Each VMware ESX server deployment will require the following flexvols configured on a NetApp primary storage system in the standard high tier shared NAS environment at Thomson Reuters Professional. All flexvols will be thin provisioned to the full size of at least one raid group on the containing aggregate, and space management will be performed at the aggregate level. In the example below, we assume 3400GB is to be provisioned, so all volumes for the cluster are set to this size. If more space is required, size each volume to the amount of space required for the ESX cluster.

Volume Name	Vol Size	Snap Reserve	SnapVault?
infra_<vmware_cluster>_vms_nosnap	3400GB	0%	No
infra_<vmware_cluster>_vms_snap07	3400GB	10%	Yes
infra_<vmware_cluster>_vms_snap14	3400GB	10%	Yes
infra_<vmware_cluster>_vms_snap45	3400GB	10%	Yes
infra_<vmware_cluster>_vmw_nosnap	3400GB	0%	No

In the above table, the <vmware_cluster> specification will be the cluster portion of the virtual host naming convention as defined by Thomson Reuters. This string will be provided by the VMware team when they make a request for storage to the Thomson storage team.

The follow configuration settings apply for each volume:

- Set the volume guarantee to “none”.
- Set the “try_first” volume option to “snap_delete”.
- Each volume will need to be exported via NFS, with r/w and root privileges, to all nodes in the VMware ESX cluster that it is being provisioned for. Note that NFS exports need to be configured for access from the VMkernel interface on the VMware ESX servers, not the service console interface.
- Each volume that will use snapshots will need the following volume options set in order to allow access to the directories via CIFS on the SnapVault secondary systems for single file recovery:
    - vol options <volname> create_ucode on
    - vol options <volname> convert_ucode on

3.4 SnapShot backup configuration on primary storage

SnapShot creation on primary storage will be configured just like any normal (non-database) flexvol that requires SnapVault backups in the standard high tier shared NAS environment at Thomson Reuters Professional. The “snapvault snap sched” method for configuring the backup schedule will be used on primary and secondary storage. Snapshots will be taken once per day on primary storage, and the retention will be set for 7 days on the primary system. Snap autodelete functionality will be configured to remove snapshots if required before the 7 day retention period has elapsed. The snap autodelete settings should be configured as follows:

```
state                            : on
commitment                       : try
trigger                          : snap_reserve
target_free_space                : 20%
delete_order                     : oldest_first
defer_delete                     : user_created
prefix                           : (not specified)
```

3.5 SnapVault backup configuration on secondary storage

SnapVault update schedules will be configured on the secondary storage system just as they would for any other (non-database) backups in the standard high tier shared NAS environment at Thomson Reuters Professional. Retention schedules will be set accordingly for the 7, 14, and 45 day backup requirements on the respective volumes.

3.6 Data deduplication configuration on primary storage

NetApp data deduplication will be configured on all primary storage volumes used for VMware datastores. Since we do not expect the virtual machine data to change on a regular basis, the actual deduplication of the data will be run only once per week. The following commands detail how to configure NetApp data deduplication on the primary storage volumes:

1. Run "sis on </vol/volume_name>" and "sis start –s </vol/volume_name>" for all volumes holding VMware data.
2. Run "sis config –s sat@2 </vol/volume_name>" for all volumes holding VMware data to schedule deduplication to run weekly at 2am every Saturday morning.
3. Use the "sis status –l" and "df –s" command to monitor the status of deduplication processes and measure the space savings obtained by deduplication.

Note: Only volumes containing virtual machines that are properly aligned (per section 2.4 of this document) should be deduplicated. If a volume contains virtual machines that have not been aligned, it is recommended to not use deduplication until alignment can be completed.

3.7 Data deduplication configuration on secondary storage

NetApp data deduplication will be configured on all SnapVault secondary storage volumes used for backups of VMware datastores. The following commands detail how to configure NetApp data deduplication on the SnapVault secondary storage volumes:

1. Run "sis on </vol/volume_name>" and "sis start –s </vol/volume_name>" for all volumes that are backing up VMware datastores.
2. Use the "sis status –l" and "df –s" command to monitor the status of deduplication processes and measure the space savings obtained by deduplication.

Note that there is no need to set a schedule for deduplication on a SnapVault secondary storage system. The deduplication process runs automatically on SnapVault secondary storage systems after more than 20% of the data in the volume has changed.

3.8 Secondary storage configuration for single file restores

While primary storage systems need to only be exported via NFS to the VMkernel interfaces on each node in the VMware ESX cluster, the SnapVault secondary storage systems need to also accommodate clients that will be performing single file recovery from the virtual disk files that have been backed up. To accommodate single file recovery from Windows virtual disks, the following must be true:

1. A CIFS share should be created for each SnapVault secondary volume. This share can be created by the Microsoft Windows Administration team within Thomson Reuters Professional.
2. The users performing single file recovery must be part of an AD group that is in the local administrators group of the SnapVault secondary storage system.
3. The "wafl.nt_admin_priv_map_to_root" option must be on for the SnapVault secondary storage system.

4. Virtual machine backup and recovery

4.1 Datastore backups

Backups of each VMware datastore will be performed each night when NetApp SnapShots of the datastores are created. In addition, these SnapShots will be transferred to secondary storage systems on a nightly basis using NetApp SnapVault technology. No configuration is required on the VMware ESX servers or the VMware Virtual Center server to accommodate these SnapShot backups. This method of backing up the datastores is known as a hot backup, or a crash consistent backup.

4.2 Performing restores

4.2.1 Restoring an entire datastore from Primary SnapShot backups

Restoring an entire datastore from SnapShot backups on primary storage can be accomplished via two methods:

1. Restore each individual virtual machine on the datastore, one at a time, using the method documented in section 4.2.2. This method will take more time, and cause additional SnapShot space utilization on the volume, but has the benefit of not removing any SnapShot backups from the primary storage system. If this method is used, keep one restore running on each physical ESX node in the cluster (i.e. 6 restores running in parallel on a 6 node ESX cluster), in order to reduce the amount of time required to complete the overall restore of all virtual machines in the datastore.
2. Restore the entire primary volume back to a previous SnapShot backup using a volume SnapRestore. This method will be very fast, however the following caveats apply:
    a. This will restore **all** Virtual Machines within the volume back to the point in time SnapShot.
    b. Any SnapShot backups taken after the restore point will be lost.
    c. If the restore is performed to a SnapShot backup that was taken prior to the most recent SnapVault backup SnapShot, the SnapVault relationship will need a new level 0 transfer.

If the volume SnapRestore method is chosen, extreme caution should be taken to understand the caveats described above. The steps for performing a datastore recovery using the volume SnapRestore method are:

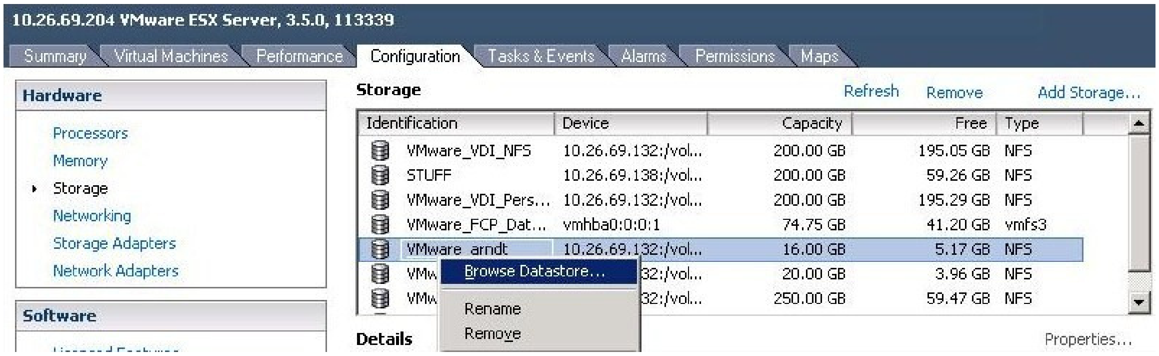
1. Make sure that all virtual machines that use the datastore are powered off.
2. Run the following command on the NetApp primary storage system to revert the NetApp volume for the associated datastore back to a SnapShot backup.
   ```
   > snap restore –t vol -s <snapshot_backup_name> <volume_name>
   ```
3. Power on all virtual machines that use the datastore.

4.2.2 Restoring individual virtual machines from Primary SnapShot backups

To restore an individual virtual machine from a SnapShot backup on the primary storage system, use the VMware Virtual Infrastructure Client to perform the following steps:

1. Power off the virtual machine to be restored. If the virtual machine is not powered off, the restore operation will fail.

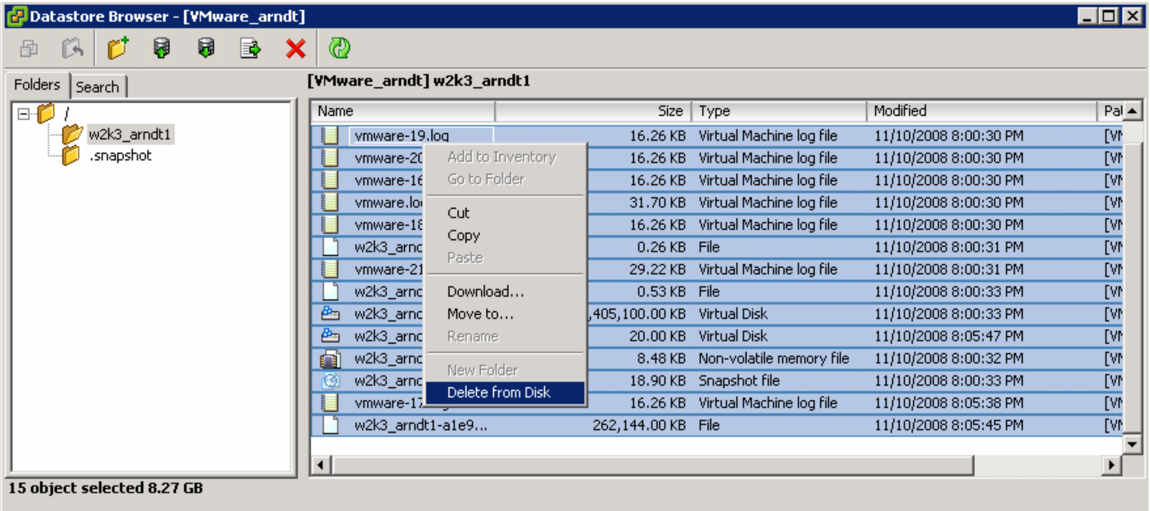
2. Browse the datastore which contains the virtual machine that you would like to restore.



Storage

Identification	Device	Capacity	Free	Type
VMware_VDI_NFS	10.26.69.132:/vol...	200.00 GB	195.05 GB	NFS
STUFF	10.26.69.138:/vol...	200.00 GB	59.26 GB	NFS
VMware_VDI_Pers...	10.26.69.132:/vol...	200.00 GB	195.29 GB	NFS
VMware_FCP_Dat...	vmhba0:0:0:1	74.75 GB	41.20 GB	vmfs3
VMware_arndt	10.26.69.132:/vol...	16.00 GB	5.17 GB	NFS
VMw	32:/vol...	20.00 GB	3.96 GB	NFS
VMw	32:/vol...	250.00 GB	59.47 GB	NFS

3. Select all the files in the virtual machine directory, right click and choose “Delete from Disk”:

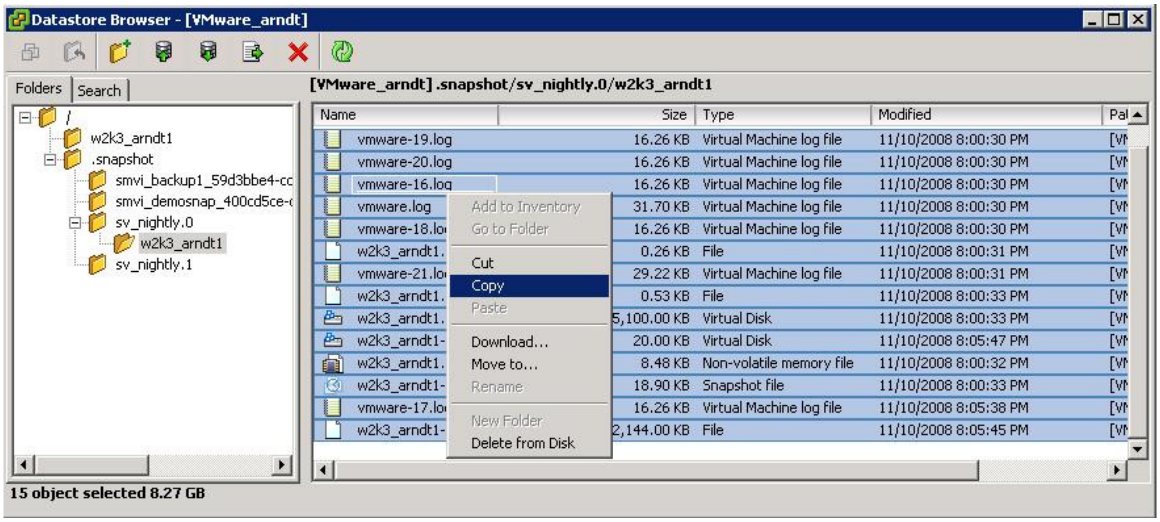


[VMware_arndt] w2k3_arndt1

Name	Size	Type	Modified	Pat
vmware-19.log	16.26 KB	Virtual Machine log file	11/10/2008 8:00:30 PM	[VM
vmware-20	16.26 KB	Virtual Machine log file	11/10/2008 8:00:30 PM	[VM
vmware-16	16.26 KB	Virtual Machine log file	11/10/2008 8:00:30 PM	[VM
vmware.lo	31.70 KB	Virtual Machine log file	11/10/2008 8:00:30 PM	[VM
vmware-18	16.26 KB	Virtual Machine log file	11/10/2008 8:00:30 PM	[VM
w2k3_arnc	0.26 KB	File	11/10/2008 8:00:31 PM	[VM
vmware-21	29.22 KB	Virtual Machine log file	11/10/2008 8:00:31 PM	[VM
w2k3_arnc	0.53 KB	File	11/10/2008 8:00:33 PM	[VM
w2k3_arnc	,405,100.00 KB	Virtual Disk	11/10/2008 8:00:33 PM	[VM
w2k3_arnc	20.00 KB	Virtual Disk	11/10/2008 8:05:47 PM	[VM
w2k3_arnc	8.48 KB	Non-volatile memory file	11/10/2008 8:00:32 PM	[VM
w2k3_arnc	18.90 KB	Snapshot file	11/10/2008 8:00:33 PM	[VM
vmware-17	16.26 KB	Virtual Machine log file	11/10/2008 8:05:38 PM	[VM
w2k3_arndt1-a1e9...	262,144.00 KB	File	11/10/2008 8:05:45 PM	[VM

15 object selected 8.27 GB

4. Browse to the .snapshot directory of the datastore, select the snapshot that you would like to restore from, and then navigate to the directory within that snapshot of the virtual machine to be restored. Select all the files in the snapshot copy of the virtual machine directory, right click, and select “copy”.

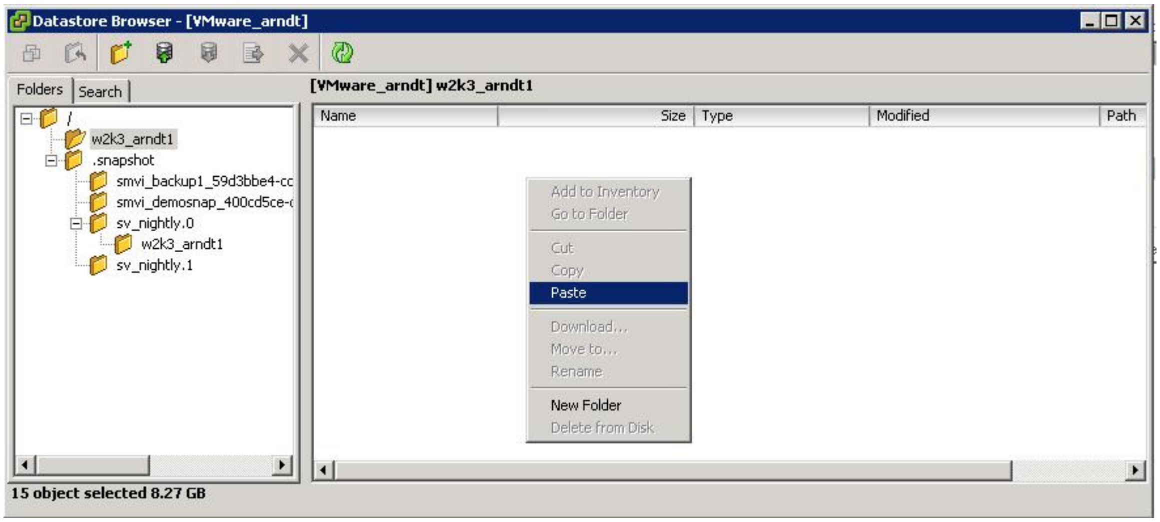


[VMware_arndt] .snapshot/sv_nightly.0/w2k3_arndt1

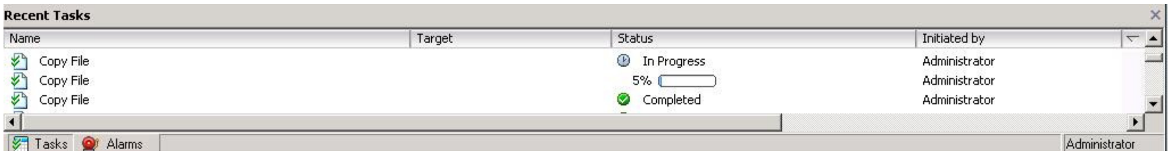
Name	Size	Type	Modified	Pat
vmware-19.log	16.26 KB	Virtual Machine log file	11/10/2008 8:00:30 PM	[VM
vmware-20.log	16.26 KB	Virtual Machine log file	11/10/2008 8:00:30 PM	[VM
vmware-16.log	16.26 KB	Virtual Machine log file	11/10/2008 8:00:30 PM	[VM
vmware.log	31.70 KB	Virtual Machine log file	11/10/2008 8:00:30 PM	[VM
vmware-18.lo	16.26 KB	Virtual Machine log file	11/10/2008 8:00:30 PM	[VM
w2k3_arndt1.	0.26 KB	File	11/10/2008 8:00:31 PM	[VM
vmware-21.lo	29.22 KB	Virtual Machine log file	11/10/2008 8:00:31 PM	[VM
w2k3_arndt1.	0.53 KB	File	11/10/2008 8:00:33 PM	[VM
w2k3_arndt1.	5,100.00 KB	Virtual Disk	11/10/2008 8:00:33 PM	[VM
w2k3_arndt1-	20.00 KB	Virtual Disk	11/10/2008 8:05:47 PM	[VM
w2k3_arndt1.	8.48 KB	Non-volatile memory file	11/10/2008 8:00:32 PM	[VM
w2k3_arndt1-	18.90 KB	Snapshot file	11/10/2008 8:00:33 PM	[VM
vmware-17.lo	16.26 KB	Virtual Machine log file	11/10/2008 8:05:38 PM	[VM
w2k3_arndt1-	2,144.00 KB	File	11/10/2008 8:05:45 PM	[VM

15 object selected 8.27 GB

5. Browse back to the root of the datastore and navigate back to the now empty directory of the virtual machine to be restored. Right click and select “paste” to copy the files from the snapshot copy of the virtual machine back to the active datastore directory for the virtual machine.



6. Use the status log of the VMware Virtual Infrastructure Client to monitor the progress of the file restores:



Name	Target	Status	Initiated by
Copy File		In Progress	Administrator
Copy File		5%	Administrator
Copy File		Completed	Administrator

7. When the restores are complete, power on the virtual machine.

4.2.3 Restoring an entire datastore from Secondary SnapShot backups

To restore the contents of an entire datastore from a SnapVault Secondary storage system to the primary storage system, use the ndmpcopy command to transfer the contents of the SnapShot backup from the SnapVault Secondary storage system back to the primary storage system. The steps to perform this restore would be as follows:

1. Make sure that all virtual machines that use the datastore are powered off.
2. Make sure you have enough free space on the primary storage volume to overwrite all virtual machines.
3. Re-create the qtree on the primary NetApp storage system, if required.
4. Run the following command on the NetApp secondary storage system virtual filer to copy the datastore contents back to the primary storage system for the associated datastore.

```
> ndmpcopy –da <user:password> /vol/<volname>/1/.snapshot/<snapshot_name>/<qtreename>
source_filer:/vol/<volname>/<qtreename>
```

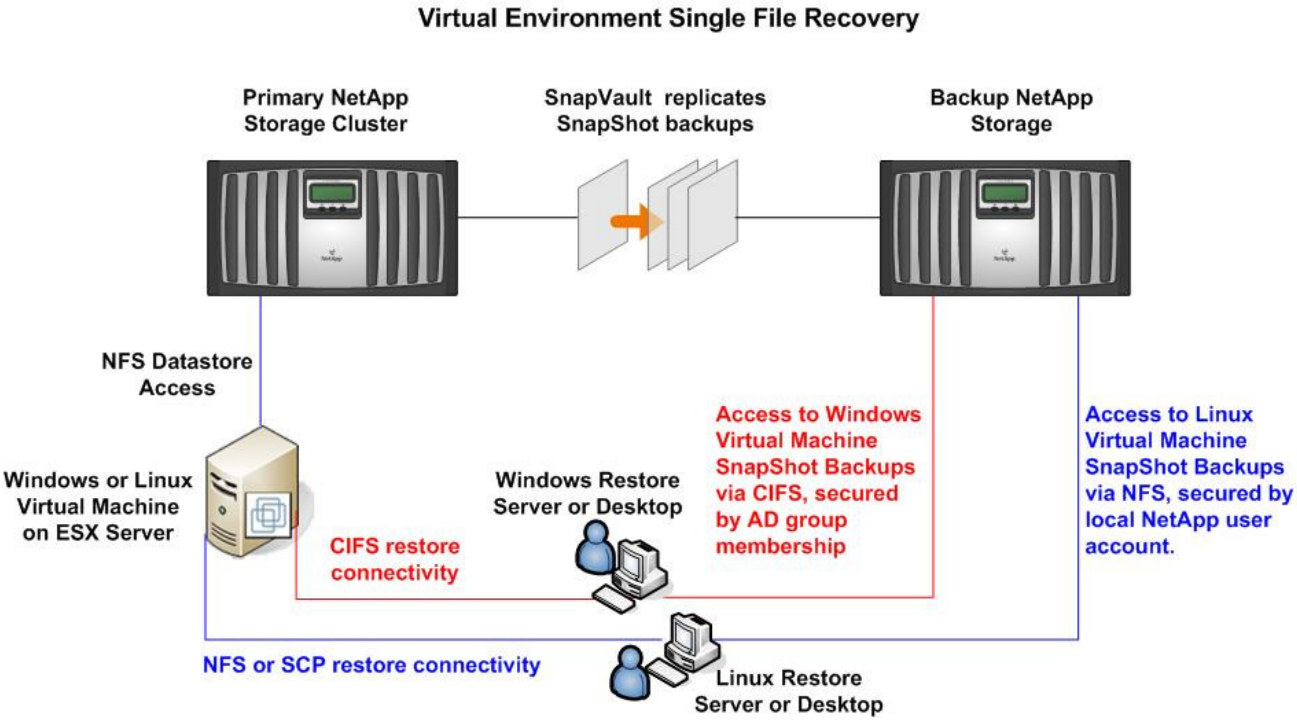
5. Once the ndmpcopy job finishes, you may power on all virtual machines that use the datastore.

4.2.4 Restoring individual virtual machines from Secondary SnapShot backups

To restore an individual virtual machine from a SnapVault Secondary storage system to the primary storage system, simply mount the SnapVault Secondary storage location as a NFS datastores on a node in the VMware cluster. The VMware administrator can then perform a copy and paste restore using the Virtual Infrastructure client in exactly the same manner as documented in section 4.2.2. Once the restore is complete, make sure to disconnect the SnapVault Secondary storage location as a datatastore from the VMware node on which it was connected.

4.2.5 Single file recovery architecture

The following diagram depicts the architecture for performing single file recovery from NetApp SnapShot backups of virtual machines.


Virtual Environment Single File Recovery
Primary NetApp Storage Cluster
SnapVault replicates SnapShot backups
Backup NetApp Storage
NFS Datastore Access
Windows or Linux Virtual Machine on ESX Server
Windows Restore Server or Desktop
Access to Windows Virtual Machine SnapShot Backups via CIFS, secured by AD group membership
Access to Linux Virtual Machine SnapShot Backups via NFS, secured by local NetApp user account.
CIFS restore connectivity
NFS or SCP restore connectivity
Linux Restore Server or Desktop

4.2.6 Restoring single files from a SnapShot backup of a Windows virtual machine

Use the vmware-mount.exe utility from VMware to connect to a virtual disk file directly from a SnapShot via a UNC path to the SnapVault secondary storage system. For example:

```
C:\> vmware-mount.exe z: \\filer\share\~snapshot\snapshot_name\virtual_machine\virtual_machine.vmdk /m:n
```

The command above would connect partition 1 of the Windows (NTFS formatted) VMDK to the Z:\ drive on the system that the command was run from. Once data has been restored from the Z:\ drive, it can be disconnected using the following command:

```
C:\> vmware-mount.exe z: /d
```

The above commands are an example of using the CLI to access files from a SnapShot copy of a VMDK. The actual procedures used by the Thomson Reuters Professional Windows Administration team, as documented by Matt Dronen, are located in the document titled ***Thomson Reuters EAGAN File Restore Procedures for VM instances located on NAS Storage.doc*****.**

4.2.7 Restoring single files from a SnapShot backup of a Linux virtual machine

Use the vmdkmounter.pl script from NetApp to connect to a virtual disk file in a SnapShot. This script will automate the task of creating a FlexClone based off the given SnapShot so that the Linux virtual disk can be mounted via a loopback filesystem from any Linux based operating system. For example:

```
# vmdkmounter.pl –o connect –h <filer> -u <user> -f </vol/volname/path/to/vm/vm-flat.vmdk> -s <snapshot> -m <mountpoint>
```

The command above would connect all partitions and logical volumes found on the virtual disk onto mountpoints underneath the <mountpoint> directory. Once the data has been restored, the mountpoint can be disconnected and the FlexClone destroyed using the following command:

```
# vmdkmounter.pl –o disconnect –h <filer> -u <user> -m <mountpoint>
```

5. Storage system monitoring and alerting

5.1 Aggregate capacity alerting

Since we are using thin provisioned volumes, and managing space at the aggregate level, we must use different capacity alerting metrics than fully provisioned volumes would use. NetApp Operations Manager should be configured to set the Aggregate Full Threshold to 70% and the Aggregate Nearly Full Threshold to 60% for aggregates used for VMware datastores. These settings can be overridden from the global default values by navigating to **Global -> Member Details -> Aggregates -> <aggr name> -> Aggregate Tools Edit Settings** in the Operations Manager web interface. Operations Manager alarms should then be configured to notify appropriate personnel when these thresholds are breached.

5.2 Performance alerting

The Performance Advisor functionality of Operations Manager should be used to configure alerts for NFS read latency over 30ms and NFS write latency over 10ms, for a period of 180 seconds, on storage systems that hold aggregates for VMware datastores.

Appendix A: Resources and Whitepapers

- NetApp and VMware Virtual Infrastructure 3 Storage Best Practices:
  - http://media.netapp.com/documents/tr-3428.pdf
- Recommendations for Aligning VMFS Partitions:
  - http://www.vmware.com/pdf/esx3_partition_align.pdf
- Disk timeout settings for GOS on NFS datastores:
  - https://now.netapp.com/Knowledgebase/solutionarea.asp?id=kb37986
- NetApp Deduplication for FAS Deployment and Implementation Guide:
  - http://media.netapp.com/documents/tr-3505.pdf
- VMware Site Recovery Manager in a NetApp Environment:
  - http://media.netapp.com/documents/tr-3671.pdf
- VMware Virtual Disk Development Kit (containing vmware-mount.exe):
  - http://www.vmware.com/support/developer/vddk/