vmPRO Best Practices Guide

6-67729-01 Rev A, July 2012

Introduction

This guide provides best practice recommendations for Quantum's vmPRO v3.0 virtual appliance and vmPRO 4000 series appliance bundle. It contains information supplementary to the base vmPRO user documentation, and in some cases refers to other documents for operating system or ISV application-specific topics.

Information on how to obtain the vmPRO documentation set and software download links are contained in the Resources section at the end of this document.

The vmPRO virtual appliance (hereafter referred to as "the appliance") consists of a Linux virtual server running vmPRO software. It is deployed from an OVF template into a compatible customer-provided VMware vSphere ESX or ESXi environment.

The vmPRO 4000 series bundle includes an appliance, and a Quantum DXi disk-based backup system, which serves as the backup target. The appliance is identical in both versions of the product. The recommendations that follow apply universally.

vmPRO technology consists of three main components:

- **SmartView**™ presents the ESX environment as a virtual NAS file system (an NFS or CIFS share). This provides a simple integration point for third-party applications.
- **SmartRead**™ is automatically invoked whenever a read is performed of the virtual file system. It performs progressive optimization of the **vmdk** files, leaving out whitespace and deleted and unused blocks, and organizing the data stream for efficiency.
- **SmartMotion**™ optionally provides simple backup services by initiating a scheduled *push* of specified **vmdk** files (leveraging SmartRead) to any specified NAS mount point. The mount point may be resident on plain NAS storage, or may be on a deduplication system such as the Quantum DXi.

SmartView and SmartMotion have different characteristics with respect to backup window, file level recovery, and DR functionality, as outlined in later sections. Your requirements will dictate the most appropriate deployment method.

During the 30-day trial period, full access to all features of the product is available, and trial copies are easily promoted to production by applying a purchased license key. At the end of the trial period, the appliance will return to a failsafe 30-day grace period before its functionality is disabled.

The recommendations presented below apply to both trial copies and licensed copies of vmPRO. See the Resources section at the end of this document for information on how to download a trial copy.

vSphere Host System Requirements

Host requirements include:

- Licensed installation of VMware vSphere ESX or ESXi 4.x or 5.x
  - The free license for ESXi is not supported, as it does not include the vStorage API for Data Protection (VADP).
  - 1280 MB vRAM, 1 vCPU, 12 GB disk space per appliance.
- A vCenter Server is recommended for ease of management to allow for automatic discovery of all ESX hosts, but it is not required.
- CBT change block differential backup functionality requires VM virtual hardware version 7 or later.

Architecture and Sizing

Before you select a deployment host for the appliance, first survey the VMware vSphere infrastructure and assess the resources available to the ESX hosts and their utilization levels. The workloads active on these ESX hosts and clusters will have an impact on backup performance that is proportional to the size of the existing vSphere/ESX host load levels.

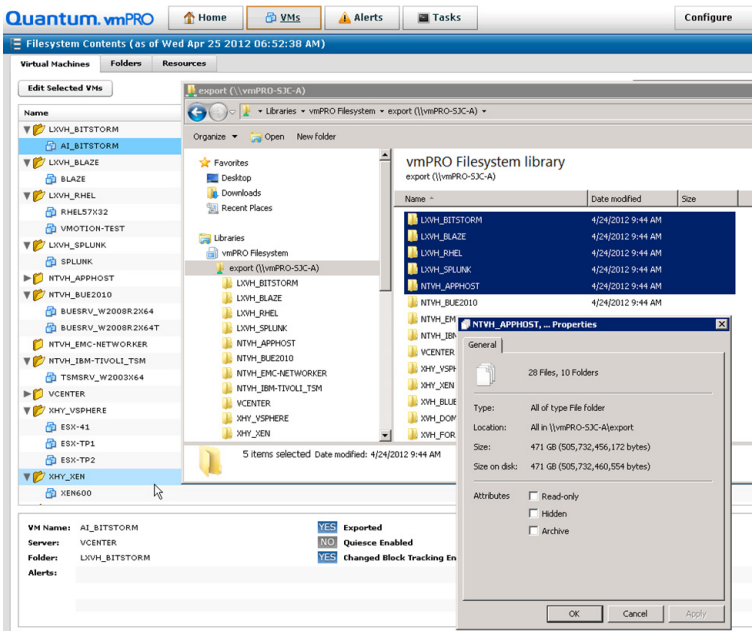
The specification of the ESX hosts and their underlying processing, network, and storage platforms will determine backup throughput performance maximums, in conjunction with VMware limits.

Recommendations:

- Deploy at least one appliance per VMware vCenter instance. If required, scale out backup capacity across larger environments by deploying additional appliances on the same or additional ESX hosts.
- Seek out target ESX hosts for appliance deployment that have the highest-performing vSwitch uplinks to the target storage device (DXi or other NAS share).

  Avoid hosts that are potentially oversubscribed or are triggering resource alerts in vCenter.
- Assess the aggregate size of the VMs to be protected by surveying the Datastore inventory in the environment. After deployment, the you can use the appliance's SmartView filesystem to gain insight on backup size by viewing the properties of the VMs and folders visible in the **\\vmPRO\export NAS** share (see Figure 1).

Figure 1 vmPRO NAS Share



vSphere ESX Host Notes and Best Practices

This section offers advice, considerations, and best practices for vSphere ESX hosts.

Datastore and Storage Considerations

Datastore performance and available network bandwidth on the ESX host vSwitches will determine the rate at which the appliance can read data from the environment during backup.

Storage capacity utilization should ideally be below 80% on any Datastore being backed up prior to performing backups. The appliance relies on VMware snapshots to function, and overhead space of between 5% and 15% of the total allocated VM size will be used on each Datastore for snapshot data during the backup.

Anything that inhibits VMware visibility to the storage, or that otherwise prevents VMware snapshot functionality from operating, will prevent the appliance from protecting VMs on those Datastores.

Keep the following considerations in mind.

- FC, iSCSI, DAS, and NFS are supported as Datastore types
- iSCSI volumes connected via guest-based iSCSI initiators are not supported, and cannot be backed up by the appliance. Communication to and from iSCSI storage connected in-guest appears to VMware as standard network activity and is not distinguishable as storage traffic. Therefore, VMware snapshots are not possible.

- Volumes using in-guest initiators can typically be re-mapped to the VM using a Virtual Mode Raw Device Mapping (RDM), as long as they are 2 TB or less.

  Note: VMware uses the acronyms as pRDM and vRDM when referring to Raw Device Mapping. For more information regarding Raw Device Mapping, see http://blogs.vmware.com/vsphere/2012/02/migrating-rdms-and-a-question-for-rdm-users.html.

  - For information, see http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1006599.

- Network mapped drives inside the guest, regardless of protocol (such as CIFS, NFS, and SMB) will not be included in the backup, because they are not visible to the VMware Storage API.
- Raw LUNs may be supported, depending on how they are attached. VMware provides two modes - Virtual Mode RDM (vRDM) and Physical Mode RDM (pRDM).
  - For vRDM, VMware uses a software shim layer between the VM and the LUN to abstract the physical characteristics of the SAN. This allows VMware snapshots to occur as normal, enabling vmPRO support for these volumes. vRDM LUNs have a 2TB size limit.
  - With pRDM, the VM is directly connected to the disk bus, and VMware snapshots are not possible. Therefore, vmPRO cannot protect volumes connected via pRDM.pRDM LUNs can be larger than 2TB.
  - pRDM disks may easily be re-mapped to the VM as vRDM, provided they are smaller than 2TB.
- SmartRead's progressive optimization functionality is supported for NTFS, EXT2, EXT3, and EXT4 guest file systems only.
  - Other file systems may be used, but they will not incur the benefit of progressive optimization. All data in the **vmdk** file will be transferred as-is, including whitespace and unused blocks.
  - Image-level recovery is available for other file system types, but file-level recovery is only available for the file systems listed.
- HA (High Availability) and FT (Fault Tolerant) disks are not supported, as the disk data is not available from the VMware API.
  - For more information, see http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1016619.
- Keep guest VM file systems to 2 TB or smaller.
- When possible, avoid striping volumes across multiple guest VM disks. A file system spanning more than one VMDK disk cannot be used for file-level recovery.

SmartMotion NAS Target Protocol Selection

Depending on the makeup of the VM guests populating your vSphere environment, their applications, and the data within them, you may choose between the CIFS and NFS protocols for sending backup data, based on which is a best fit.

For example, if you would like the SmartMotion backup files on the DXi or other NAS to be directly available to Windows systems, you may prefer to use the CIFS protocol. When UNIX/Linux/vSphere host integration is a priority, you may determine NFS to be more appropriate.

Additionally, depending on the contents of the data inside the VM disks, you may observe substantially different performance characteristics during backup and recovery between the two protocols.

Since no two vSphere environments are entirely alike, best practice is to conduct a test backup and recovery with at least 40 GB worth of data over each protocol to observe the throughput and job completion time characteristics. This will allow you to choose the protocol best suited to your operations.

Protocol Considerations

Some protocol considerations to keep in mind include:

- The NFS protocol type is supported as a Datastore type by vSphere.

  VMware vSphere ESX hosts can mount a SmartMotion NAS backup target to allow for direct recovery of the backup images when using the NFS protocol to send backup data.

- The appliance supports using a sparse writing approach when sending backup images using the NFS protocol, reducing the I/O overhead and time required for a backup job. (For more information on sparse writing, see sparse writes in the Performance Recommendations section on page 13.

Ethernet Networking Considerations

Some considerations for Ethernet networking include:

- The appliance backup traffic is directed to each ESX host at the Service Console IP address that is used to register that host in vCenter.
- Add a secondary Network Interface (eth1) to the appliance if additional connectivity is required to reach either the vSphere hosts or the NFS DXi storage target.

  You can do this by editing the appliance VM settings in vSphere Client and adding an additional network interface.

- If you are operating in a restricted or strongly firewalled networking environment, check the appliance log files for assistance in diagnosing possible connectivity problems related to backup failures.

Resource Groups

Be mindful if placing appliances into VMware Resource Groups. Reduced priority and resources assigned to the appliance may artificially constrain backup performance.

vmPRO Appliance Configuration Notes and Best Practices

Some considerations and best practices for vmPRO appliance configuration include:

vCenter vs. ESX-based VM inventory discovery

When configuring the appliance, you have the option of specifying either a single vCenter server hostname for VM discovery, OR one or more standalone ESX hosts, but not both simultaneously.

If you have the option of using a vCenter server, it is recommended that you use this option, for ease of use and reduced management overhead by auto discovering all ESX hosts.

Auto-Export

By default, when you deploy a new appliance, the "Auto-Export" feature is set to "active." This setting automatically enables SmartView and SmartMotion capabilities for any new VM discovered in the vCenter inventory.

This is convenient for un-attended backup of remote, isolated, or fully automated vSphere environments, or anywhere that new VMs are frequently created. When set "active," new VMs are automatically protected.

Please note the following:

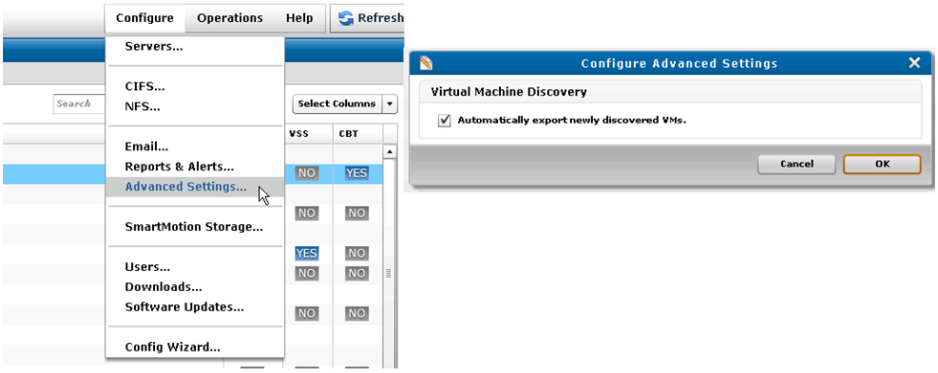
- Auto-Export must be used with caution, since excessive addition of VMs to a backup job may cause it to run longer than anticipated.
- Be mindful of the capacity and utilization of the target storage when using Auto-Export, since too many new VMs may overburden the target.
- Use caution when enabling Auto-Export in large environments. See the sizing guidelines below for recommendations regarding the volume of VMs to assign to each vmPRO.
- Account for any new VMs that may become Auto-Exported due to a vMotion/DRS operation relocating them onto a vSphere host being managed by vmPRO, and plan for available capacity in your backup target.

Be aware also that "automatic" does not mean "set and forget." Each VM that is protected consumes space on the target storage device, so as the population of VMs grows, so does the storage requirement.

When the target storage capacity exceeds 80% utilization, the appliance will generate an alert to warn the administrator that the storage device is nearing full capacity.

You can enable or disable Auto-Export in the **Configure > Advanced Settings** menu (see Figure 2).

Figure 2 Enable or Disable Auto-Export



Changed Block Tracking and Differential / Partial Backups

The appliance's SmartRead and SmartMotion capabilities can leverage VMware's Changed Block Tracking feature to identify the virtual disk blocks that have changed, allowing backup and storage processes to avoid unnecessary reads. This provides the basis for the appliance's differential backup capability.

Please keep the following in mind:

- CBT-based backups reduce the amount of network I/O and time required for daily backups.
- Be mindful that activating or deactivating the CBT feature will trigger the immediate creation and removal of an ESX snapshot for each VM activated; this is required by the VMware API.
- Do not schedule CBT resets to occur at the same time as backups. CBT resets should be scheduled a few hours before backups, to ensure that all CBT-enabled VMs have been reset before backups begin.
- Differential CBT backup files are designated with the **-pancbt.vmdk** suffix. Unlike a Full backup, these files are not complete. VMware expects **.vmdk** files to be complete images, thus CBT-based backups require recovery through the vmPRO Recovery Wizard before being usable to ESX.

Folders: Organizing VMs and Rotating Full Backups

By default, the appliance's virtual file system organizes your VMs in folders named for their respective vSphere ESX hosts. These folders are separate from your existing folder structures inside vSphere. They are used in the appliance to allow you to refine and optimize backup loads across your appliances.

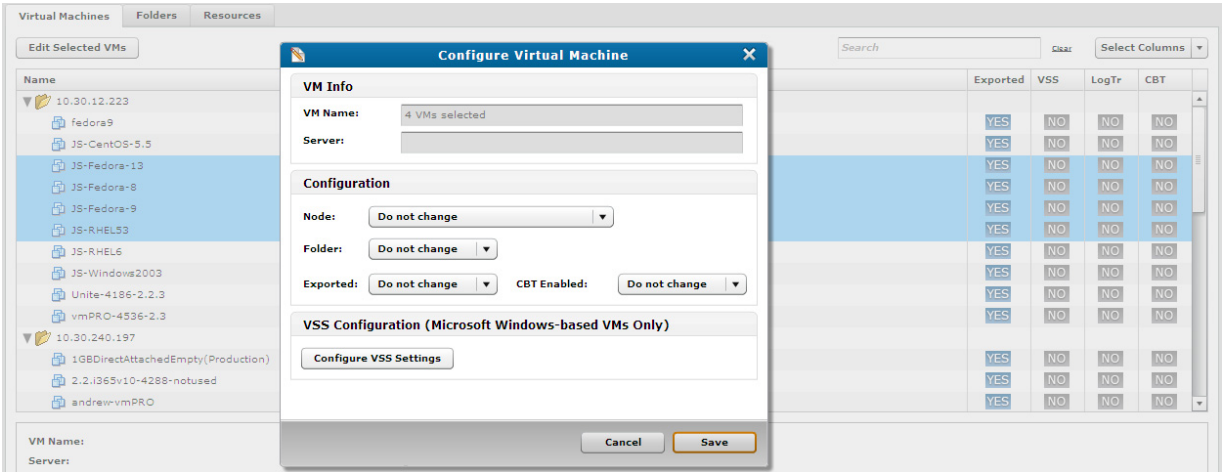
If you add a vCenter server, your VMs will all appear in a single initial folder with the name of that vCenter server. Alternately, if you add one or more ESX servers, your VMs will appear in folders whose names correspond to the ESX host on which they reside.

Folders are a powerful construct within the appliance. They enable you not only to organize your VMs visually, but also to manage multiple Differential CBT backup rotation schedules, and the distribution of backup jobs across multiple appliance nodes. If you are using Group Mode, all folders that you create on the master appliance will appear on all node appliances.

Keep in mind the following information about folders:

- Add folders and divide your VMs among them to enable multiple backup rotation policies.
- Define folders that reflect your organization's needs. For example, name folders and group VMs according to backup schedules, or classes of VMs, such as Prod, QA, and Dev.
- Stagger full backups across different weeks to shorten long full backup windows.
- To distribute the backup load, assign folders and VMs to be managed by the different appliance nodes in a group (see Figure 3).

Figure 3 Assign Folders and VMs to Nodes in a Group



Group Mode

If a single appliance does not provide enough throughput to complete backups in the desired window, additional appliances may be deployed in the environment.

Group Mode streamlines management of multiple appliances. When you configure Group Mode, one appliance is selected as the master. All configuration is then performed from the master.

Keep the following considerations in mind:

- Before deploying multiple appliances in Group Mode, confirm that each appliance has network connectivity and DNS resolution. Use the **net ping** command in the CLI to verify that each appliance can ping the other appliances that will be part of the group (by name if using DNS). Perform this test before creating the group, to ensure proper functioning of the group deployment.
- DNS resolution failures or IP routing issues in the group deployment may cause backup jobs to fail for VMs assigned to misconfigured nodes.
- Verify that all group members/nodes have been upgraded to the same release version of the appliance, for example 2.3.1.
- Create your folders on the master appliance. They will then appear on all nodes.

Group Mode Licensing

If you find that you need to increase the performance of a vmPRO, you can do so by distributing backups across other vmPRO nodes using a single capacity based license. Once installed, the single license is shared by the group and the capacity of the entire group is managed by the one capacity license.

To take advantage of **Group Mode Licensing**, you must install multiple vmPRO appliances, designate one as the Master, and then add the other vmPRO appliances as nodes of the Master. To accomplish this, do the following:

1. Install a vmPRO (the one you want to use as the Master). Follow the instructions presented in the Installation Guide. (https://mosaic.quantum.com/docs/InstallGuide)

   Note: You will need a valid e-mail address and password to access the vmPRO Installation Guide.

2. Install the capacity license that you have purchased. Follow the instructions presented by the **Licenses Wizard**. To access the **Licenses Wizard**, see the **Configure** section, Chapter 1, of the vmPRO User's Guide. (https://mosaic.quantum.com/docs/vmPROUserGuide)
3. Configure the vmPRO as the Master. Follow the instructions presented in the **Set Up Groups** > **Create the Group's Master** section, Chapter 3, of the vmPRO User's Guide.
4. Install all the vmPRO appliances that you want to be nodes (appliances managed by this Master) by following the instructions presented in **Step 1** of this procedure.
5. Configure each node (add it to the group managed by this master) by following the instructions presented in the **Set Up Groups** > **Add Quantum vmPRO Appliances to a Group** section, Chapter 3, of the vmPRO User's Guide.

Appliance Network Interface Settings

By default, the appliance is configured with a VMXNET-type network interface, as defined in the VM's settings stored in the vmx configuration file. This adapter is offered for legacy compatibility, but you will often get better performance by switching to either the Intel E1000 or VMXNET3 type of adapter. This can be done by shutting down the appliance and editing its settings, either through vSphere Client, or by editing the **.vmx** file on the Datastore.

Some considerations:

- If you remove the existing Network Interface through vSphere Client, make sure to take note of the vSwitch to which the adapter was connected.
- After switching the adapter type, it may be necessary to perform a Network Reset in the appliance console (see Figure 4 and Figure 5).

Figure 4 Network Type

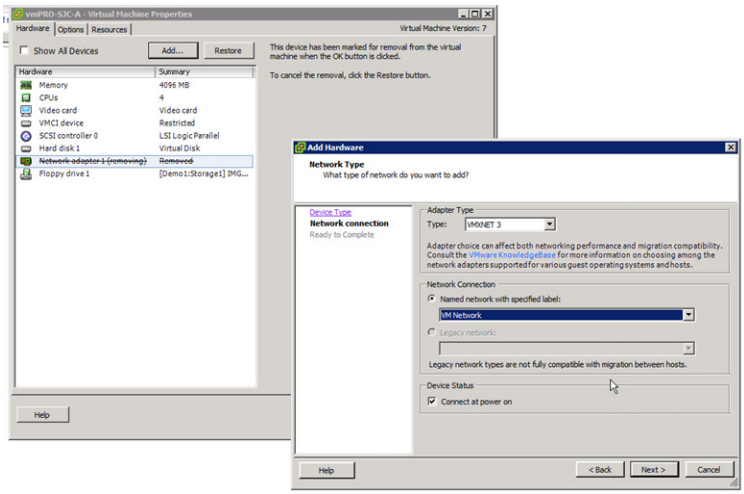
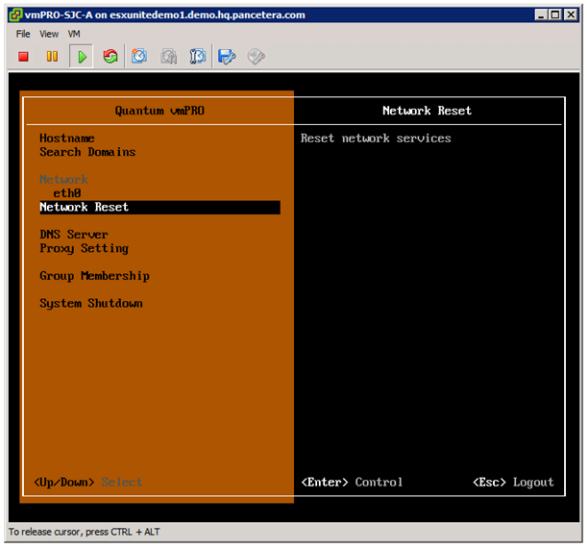


Figure 5 Network Reset



Appliance vRAM and vCPU settings

In general, Quantum recommends that the RAM and CPU allocations for the appliance remain as set in the default settings contained in the .OVF deployment template: 1 vCPU and 1,280 MB vRAM. Under certain circumstances increasing the number of CPUs in a VM can improve performance; however, this should only be attempted after discussing your unique requirements with Quantum Support.

Adding additional resources, or altering this configuration, can have unexpected and undesired consequences, due to the way vmPRO is tuned to operate internally.

It is not necessary to adjust or increase these values. If you have altered them, please consider returning them to the defaults, or re-deploying the appliance from the .OVF image.

Scaling vmPRO Performance

Each appliance can move between 100 MB and 300 MB of data per second (360 GB to 1,080 GB per hour), depending on the factors that affect throughput in your environment.

- For example, if you need to move 1200 GB per hour, you will need to install between 2 and 4 appliances.
- A maximum of eight data streams per appliance is recommended. Four streams is the default. The number of streams may be modified at the appliance command line by using the command

  reg set smartmotion.max_streams = n

where **n** equals the maximum number of concurrent streams for that appliance.

- Transfer buffer space and connection limitations within the VMware Network File Copy (NFC) protocol may limit the maximum number of streams per appliance. The maximum number of concurrent configured streams will only be active if sufficient NFC resources are available. This is a VMware limitation.
- If you require more data streams for better load balancing, or to accommodate more backup policies, deploy additional appliances on other ESX hosts.

Performance Recommendations

Some considerations and best practices for performance enhancements include:

- It is important to remember there can be several areas that can affect backup performance:
  - Datastore disk speed
  - Number of datastores residing on the same disk
  - ESX CPU speed (GHz)
  - Connectivity to the backup storage device (1 GbE, 10 GbE, …)
  - Performance of backup storage device
  - ESX overall load level
  - ESX overall network usage
- Sharing the backup load evenly across multiple vmPRO instances on a ESX server (vmPRO Group Mode) will improve performance more than any other recommendation given the same hardware. The backup NAS storage device and network can become a bottleneck when using multiple vmPRO instances. It is important to remember that backup data traffic may be shared with other concurrent network traffic depending on how the external network is configured. The following is a rough guide for network connection to vmpro instances:
  - 1 x 1 GbE connection to NAS storage: 1 vmPRO instance
  - 2 x 1 GbE connections: 2 vmPRO instances
  - 1 x 10 GbE connection: 3 vmPRO instances

- NFS connected backup storage device will have better performance than CIFS using *sparse writes*. When zero's are encountered in the backup data stream, NFS has the ability to not transfer every zero, but rather send the number of zeros. This is seen on the DXi with no traffic on Ethernet (see Figure 6), but the "Before Reduction" tally increasing (see Figure 7).

Note: Both charts are of the same time period.

Figure 6 No Ethernet Traffic

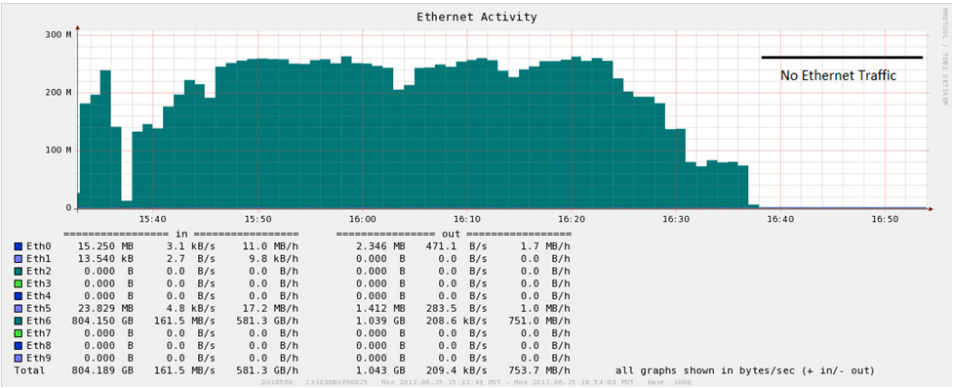
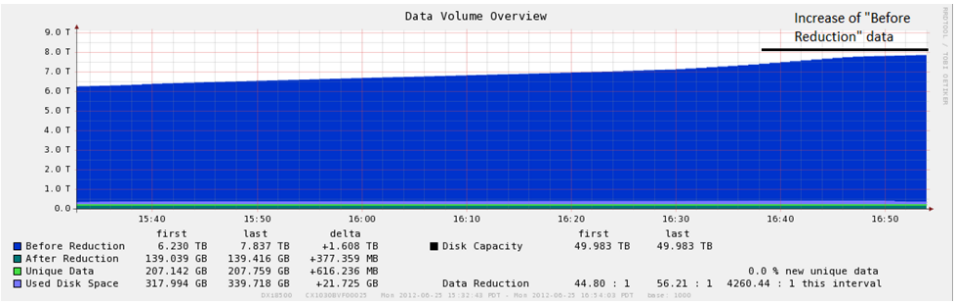


Figure 7 Before Reduction



- In regards to Increasing the number of CPUs, see Appliance vRAM and vCPU settings on page 12.

Appliance Folders and Mount Points

Each appliance presents several mount points and folders for various uses. Different folders and mount points have different functions and performance characteristics, so it is important to understand their intended uses. The following table should be useful.

Table 1 Folder and Mount Points

Share	Purpose	RELATIVE Performance
/import	VMs to be restored are transferred into this directory.	Medium
/export (read-only)	Source for SmartMotion backups – SmartMotion reads from here and pushes to specified target.	Medium, dependent on ESX
<backup target>/backup	External target for SmartMotion backups and *VM* restores.	Fast, direct from DXi
/recover/files (read-only)	Synthetic file-level view of backups – source for individual file restores.	Slower, high overhead
/recover/images (read-only)	Synthetic full disk image view of backups – source for image-level restores.	Medium
/files (read-only)	Source for file level backups – current live view of VM files.	Slower, high overhead

Please note that:

- All shares listed above live on the appliance, except for **/backup**, which is the share created on the DXi or other storage target to serve as a destination for SmartMotion. The name **/backup** is an example; you may name the share as you wish.
- Avoid using **/files** for large backups, because reading individual files is slower than reading images, due to higher processing overhead. You do not have to back up **/files** to be able to perform individual file-level restores - file-level restores are possible from image-level backups.

Backup Notes and Best Practices

Some considerations and best practices for backups include:

SmartMotion Scheduling

Each vmPRO appliance can have multiple backup policies and each policy will have its own schedule; however, a specific policy can only be run once per day.

If you are executing backup polices in a group configuration, only one policy can run at a time on a particular node, but all nodes can be running a policy. In other words, the master node can be running a unique backup policy and each member node in the group configuration can be running a unique backup policy.

Retention

The number of backups it is possible to retain is highly dependent on the characteristics of the target NAS storage device. The rate of storage utilization depends on a number of factors, such as deduplication, and the rate of unique block creation in the VM guests. In general, it is best to start with a lower number of backups retained, until the capacity growth rate can be observed, for example between 7 to 14 days

- Deduplication-Enabled Target—DXi systems, and other deduplicating NAS targets, will generally achieve 10:1 to 20:1 reduction in aggregate backup volume, enabling greater retention periods than with comparably sized non-deduplicating storage devices. Full and Differential/CBT backups will have approximately the same storage utilization impact on targets that perform deduplication.
- Non-Deduplicating Target—Non-deduplicating NAS targets will consume disk more rapidly. Here, full and differential/CBT backups will have different impacts, with CBT-based backups generally being approximately 15% to 30% the size of a full backup, depending on your environment.
- Regardless of the type of storage target in use, the biggest factor affecting the rate of storage utilization is the rate at which unique data blocks are generated by guest VMs.

Recovery Notes and Best Practices

Some considerations and best practices for recovery include:

- For the fastest access to File Level Recovery, configure the Recovery Mount setting on the appliance to point directly to the location of the SmartMotion backups. This setting is preserved through reboots of the appliance and provides file-level access to the backups at the **\\vmPRO\recover\files** CIFS share.
- For information regarding the recovery of VMs, see the **Back Up, Store, and Recover Data > Recovering VMs** section, Chapter 3, of the vmPRO User's Guide. (https://mosaic.quantum.com/docs/vmPROUserGuide)
- For information regarding file level recovery, see the **Back Up, Store, and Recover Data > Recovering Individual Files** section, Chapter 3, of the vmPRO User's Guide.

Resources

If you wish to request a trial copy of vmPRO Virtual Appliance, use the following link. Please allow 48 hours for processing: http://www.quantum.com/products/software/vmPROTrial/index.aspx

The complete vmPRO Virtual Appliance documentation set, software downloads, and knowledgebase articles are available here: http://mosaic.quantum.com/