vmPRO 3.x Best Practices Guide

This document contains the following topics:

6-67729-02 Rev A, August 2015

vmPRO 3.x Best Practices Guide Introduction

Disclaimer

The information contained in this publication is subject to change without notice. Quantum Corporation makes no warranty of any kind with regard to this manual,including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Quantum Corporation shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual.

The instructions provided in this document by Quantum Corporation are for customer convenience and are not warranted or supported by Quantum Corporation. Quantum Corporation expects users to integrate third-party software as needed, but Quantum Corporation is not responsible for the usability of the third-party software after installation.

The vmPRO 3.x Best Practices Guide provides best practice recommendations for Quantum's vmPRO 3.x virtual appliance. 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 Helpful Resources. The vmPRO virtual appliance (hereafter referred to as "the appliance") consists of a Linux virtual server running vmPRO software.

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 in this document apply to both trial copies and licensed copies of vmPRO. See Helpful Resources for information on how to download a trial copy.

Deploy your appliance from an OVF template into a compatible customer-provided VMware vSphere ESX or ESXi environment.

vmPRO Components

vmPRO technology consists of three main components.

SmartView™

This feature 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™

This feature 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™

This feature 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.

Note: 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.

vSphere Host System Requirements

The vSphere Host System's requirements include the following:

Component	Requirements
Virtual Server	Licensed installation of VMware vSphere ESX or ESXi 4.x, 5.x or 6.x **Note:** The free license for ESXi is not supported, as it does not include the vStorage API for Data Protection (VADP). **Note:** A vCenter Server is recommended for ease of management to allow for automatic discovery of all ESX hosts, but it is not required.
Hardware per appliance	• 12 GB of free disk space • 1280 MB of vRAM • 1 vCPU
CBT Differential Backup Functionality	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

Review the following recommendations:

Appliance Deployment Numbers

Deploy at least one appliance per VMware vCenter instance. If required, scale out backup capacity across larger environments by deploying additional appliances on additional ESX hosts, using vmPRO Group Mode.

ESX Hosts

Seek out target ESX hosts for appliance deployment that have the highest-performing uplinks to the target storage device (DXi or other NAS share). Avoid hosts that are potentially oversubscribed or are triggering resource alerts in vCenter.

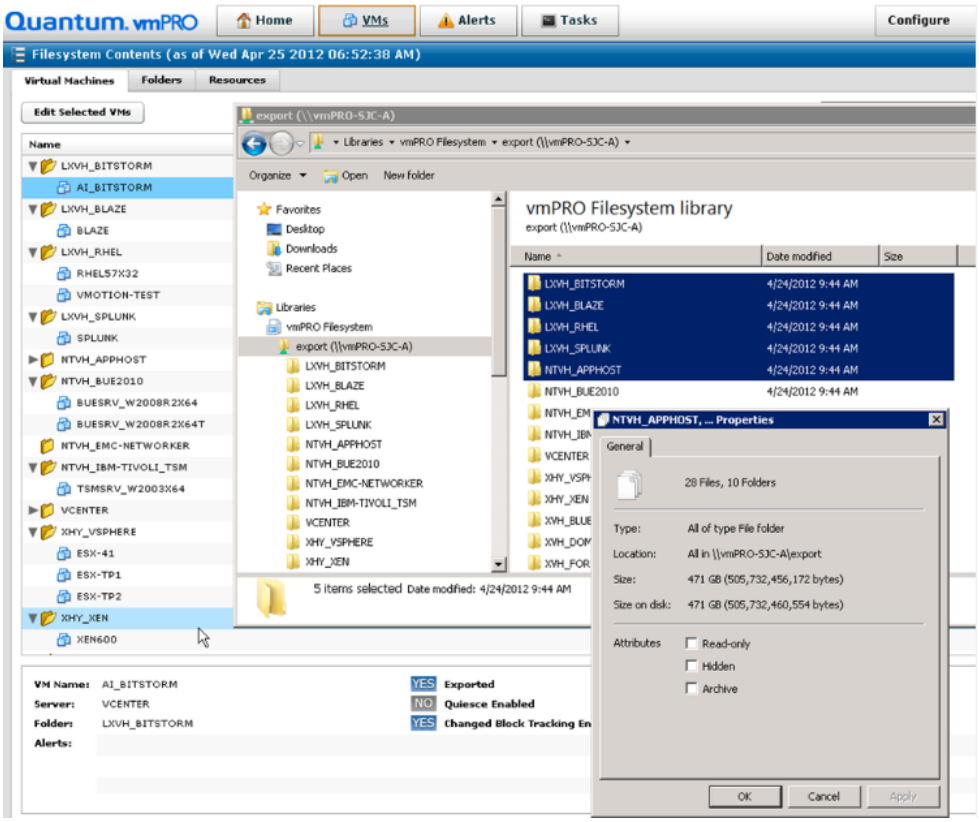
VMware Resource Groups

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

VM Aggregate Size

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.

Figure 1: vmPRO Export Directory – NAS Share



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. 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.

Considerations

When configuring Datastores, keep the following in mind:

Supported Datastore Types

VSAN, FC, iSCSI, DAS, and NFS are supported as Datastore types.

Unsupported SCSI Volumes

SCSI 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 remapped to the VM using a Virtual Mode Raw Device Mapping (RDM).

Note: VMware uses the acronyms as pRDM and vRDM when referring to Raw Device Mapping.

Additional Resources

VMware vSphere Blog: Migrating RDMs, and a question for RDM Users

VMware Knowledge Base (1006599)

Network Mapped Drives

Network mapped drives inside the guest, regardless of protocol (such as CIFS, NFS, and SMB) will not be included in the backup. They are not visible to the VMware Storage API.

Supported Raw LUNs

Raw LUNs may be supported, depending on how they are attached. VMware provides two modes:

Virtual Mode RDM (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 62 TB size limit.

Physical Mode RDM (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 up to 64 TB.

pRDM disks may easily be remapped to the VM as vRDM, provided they are equal to or smaller than 62 TB.

Progressive Optimization

SmartRead's progressive optimization functionality is supported for NTFS, EXT2, EXT3, and EXT4 guest file systems only.

Other File Systems

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

Image-level recovery is available for other file system types, but direct file-level recovery is only available for the file systems listed. Indirect file level recovery is available for any file system type by using the vmPRO iSCSI target functionality.

Unsupported Disks

HA (High Availability) and FT (Fault Tolerant) disks are not supported for backup, as the disk data is not available from the VMware API.

Additional Resource

VMware Knowledge Base (1016619)

Multiple Guest VMDKs

When possible, avoid striping volumes across multiple guest VM disks. A file system spanning more than one VMDK disk cannot be used for direct 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.

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 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

The following topic presents best practice considerations for configuring protocol types.

Considerations

Keep in mind the following when configuring protocol types:

Supported NFS Protocol Datastore

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.

NAS Target Device

NAS target devices vary on how well they support NFS or CIFS protocols. Test a backup workload with each protocol type to determine the best protocol to use with the NAS target device.

Ethernet Networking Considerations

The following topic presents best practice considerations when configuring Ethernet networking.

Considerations

Keep in mind the following when configuring Ethernet networking:

Appliance Backup Traffic

The appliance backup traffic is directed to each ESX host at the Management IP address used to register that host in vCenter.

If your ESX hosts have multiple Management interfaces on different subnets, you can force the vmPRO appliance to use a different Management interface by moving it to the target subnet. Routing on the ESX host then directs the vmPRO appliance's backup traffic to that network.

Secondary Network Interface

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.

Firewall Protection

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

vmPRO Appliance Configuration Notes and Best Practices

This section presents considerations and best practices for configuring vmPRO appliances. Review the following topics for more information:

vCenter Versus ESX-Based VM Inventory Discovery

When configuring the appliance, you have **one** of the following options:

- Specify a single vCenter server hostname for VM discovery
- Specify one or more standalone ESX hosts.

Caution: You cannot use both types of servers simultaneously.

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

Auto-Export

By default, the Auto-Export feature is set to **active** when you deploy a new appliance. This setting automatically enables SmartView and SmartMotion capabilities for any new VM discovered in the vCenter inventory. This is convenient for unattended backup of remote, isolated, or fully automated vSphere environments, or anywhere that new VMs are frequently created. When set to **active**, new VMs are automatically protected.

Considerations

Keep the following in mind when using Auto-Export:

Excessive VM Additions

- Auto-Export must be used with caution, since excessive additions of VMs to a backup job may cause it to run longer than anticipated.
- Account for any new VMs that may become Auto-Exported due to a vMotion/DRS operation that would relocate them onto a vSphere host being managed by vmPRO. Plan for available capacity in your backup target.

Storage Requirements

- Use caution when enabling Auto-Export in large environments.
- Be mindful that "automatic" does not mean "set and forget." Each VM that is protected consumes space on the target storage device. As the population of VMs grow, so does the storage requirement.

Storage Target Capacity

- Be mindful of the capacity and utilization of the storage target when using Auto-Export. Too many new VMs may overburden the target.
- 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 from the **VMs > Virtual Machines** page by selecting or deselecting the **Automatically export new VMs** check box.

Figure 2: Virtual Machines Page – Enable Auto-Export

CBT 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.

Considerations

Keep the following in mind when using CBT-based backups:

Reduced Network I/O and Time

CBT-based backups reduce the amount of network I/O and time required for daily backups.

Turning CBT On and Off

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 trigger is required by the VMware API.

Scheduling CBT Resets

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.

CBT Backup Files

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, **/import** share, or **/recover/images** share before being usable to ESX.

Folder Organization

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.

Considerations

Keep in mind the following when configuring and using folders:

Multiple Backup Policies

Add folders and divide your VMs among them to enable multiple backup rotation policies.

Organization Needs
Define folders that reflect your organization's needs.

Example

Name folders and group VMs according to backup schedules or classes of VMs, such as Prod, QA, and Dev.

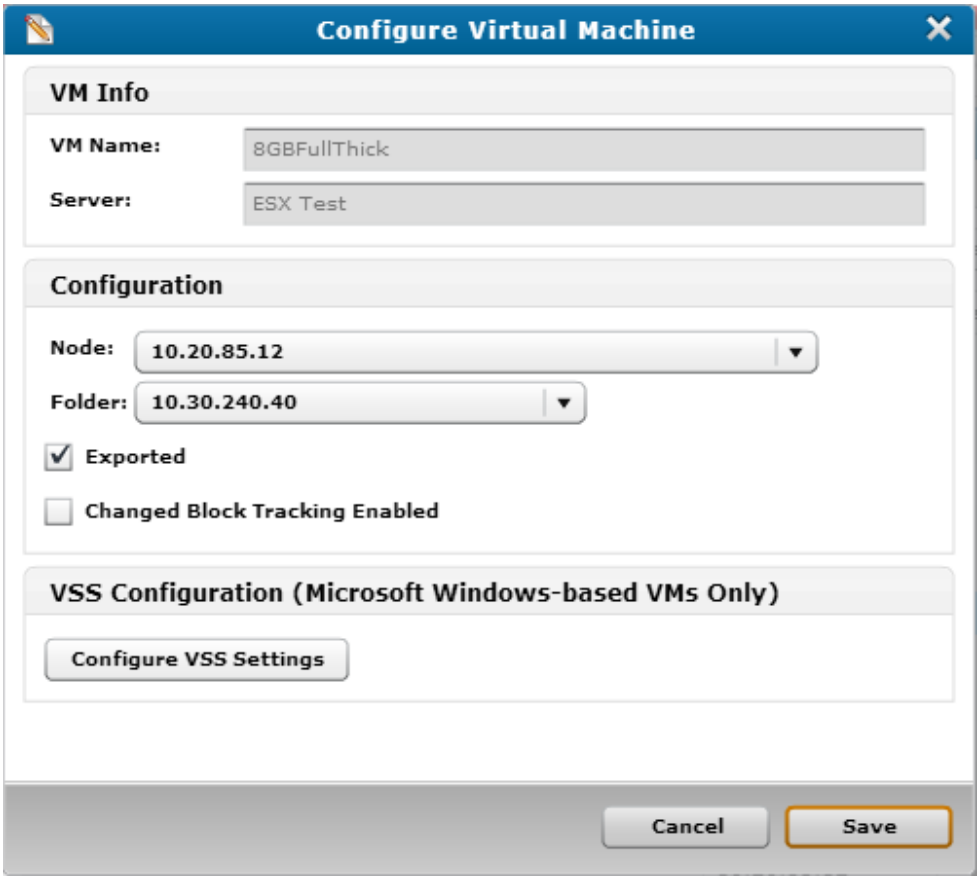
Shorten Backup Times

Stagger full backups across different weeks to shorten long full backup windows.

Group Configuration

To distribute the backup load, assign folders and VMs to be managed by the different appliance nodes in a group on the Configure Virtual Machine dialog box.

Figure 3: Configure Virtual Machine Dialog Box



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.

Considerations

Keep the following considerations in mind when using Group Mode:

Network Connectivity and DNS Resolution

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

DNS resolution failures or IP routing issues in the group deployment may cause backup jobs to fail for VMs assigned to misconfigured nodes.

Appliance Upgrades

Verify that all group members/nodes have been upgraded to the same release version of the appliance, such as 3.3.

Folder Creation

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.

Configure Group Mode Licensing

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

http://forumv.co/page/resources-1

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.

   http://downloads.quantum.com/quantum_vmPRO_software/3.3.0/6-67535-06_RevA_vmPRO_3.3_Users_Guide.pdf

   http://forumv.co/page/resources-1

3. Configure the vmPRO as the Master.
4. Install all the vmPRO appliances that you want to be nodes (appliances managed by this Master).
5. Configure each node (add it to the group managed by this master).

Note: For detailed instructions on configuring Group Mode Licensing, see the **vmPRO Group Configuration** book of the vmPRO 3.3 Online Help.

Appliance Network Interface Settings

By default, the appliance is configured with a VMXNET3-type network interface, as defined in the VM's settings stored in the vmx configuration file. This adapter usually offers superior performance, but you may get better performance by switching to the Intel E1000 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.

Considerations

Consider the following before switching adapters:

Existing Network Removal

If you remove the existing Network Interface through vSphere Client, make sure to take note of the vSwitch to which the adapter was connected.

Network Reset

After switching the adapter type, it may be necessary to perform a Network Reset in the appliance console.

Figure 4: Network Type Dialog Box

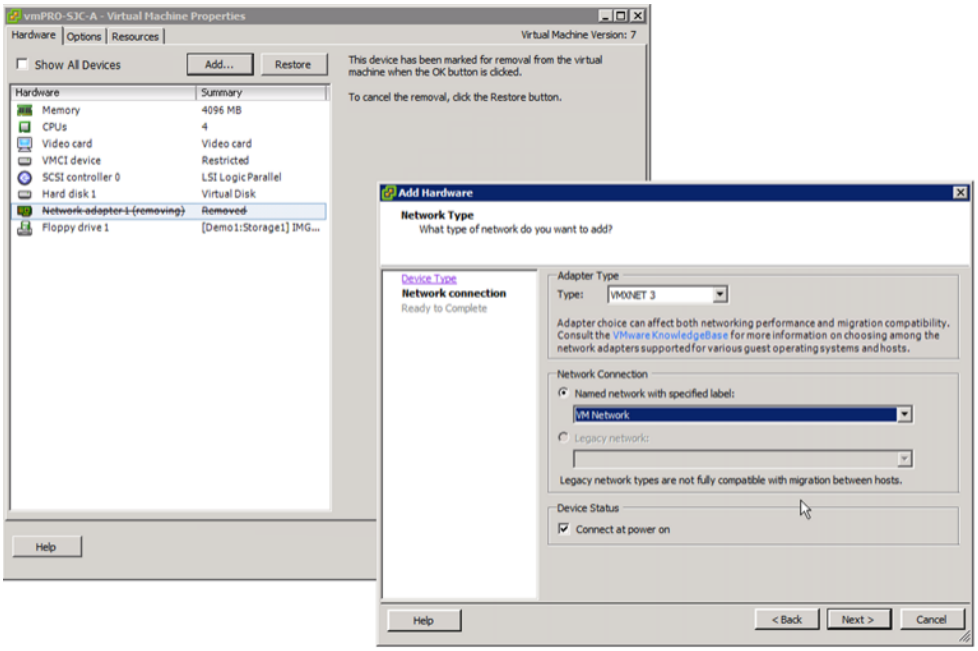
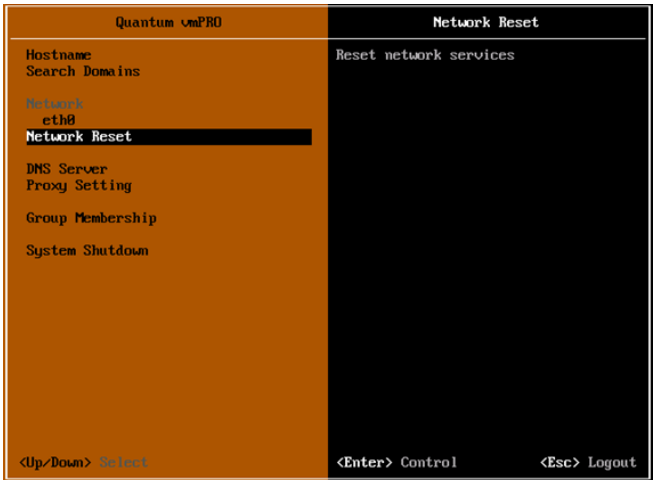


Figure 5: Client Console – Network Reset



Appliance RAM and vCPU Settings

In general, we recommend 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.

Increasing the Number of CPUs

Under certain circumstances, increasing the number of CPUs in a VM can improve performance. You should only increase the number of CPUs 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.

Keep in mind that It is not necessary to adjust or increase these values. If you have altered them, 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.

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.
- The number of active backup policies/tasks may be modified using the command

  `reg set smartmotion.max_tasks = n`

  Where **n** equals the maximum number of simultaneous tasks in the appliance/group.

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

Consider the following best practices for performance enhancements:

Areas effecting 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 target device
- ESX overall load level
- ESX overall network usage

Sharing backup load

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

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, and so it is important to understand their intended uses. Refer to the following table, as needed.

Share Name	Purpose	Relative Performance
/import (r/w)	VMs to be restored are transferred into this directory	Medium
/export (read-only)	Source for SmartView and SmartMotion backup data	Medium, dependent on ESX
NAS backup target (/<backup>) (r/w)	External target for SmartMotion backups and VM restores	Fast, direct from NAS (DXi)
/recover/files (read-only)	Sythetic file-level view of backups / file level restores	Slow, high overhead
/recover/images (read-only)	Synethic full disk image view of backups / image level restore	Medium

Share Name	Purpose	Relative Performance
/files (read-only)	Source for file level backups / live view of VM data	Slow, high overhead

Considerations

Consider the following when using mount points:

/backup Share

All shares listed above live on the appliance, except for the NAS backup target (**/<backup>**) share, which is the share created on the DXi or other storage target to serve as a destination for SmartMotion.

Note: The name **/backup** is an example. You can give the share a different name.

/files Share

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

This following sections address considerations and best practices for backups.

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 virtual machine (VM) guests. In general, it is best to start with a lower number of backups retained, until the capacity growth rate can be observed, typically between 7 to 14 days.

Note: 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.

Considerations

Consider the following when performing backups:

Deduplication-Enabled Target

DXi systems, and other deduplicating NAS targets, will generally achieve 10:1 to 20:1 or beyond 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.

MS SQL Server Backup

vmPRO does not support automated Microsoft SQL Server log file truncation with the included Quantum VSS agent. The **Log Truncation Enabled** option on the **Configure VSS Login** dialog box currently applies to the Microsoft Exchange Server only.

If you enable VSS integration for a Microsoft SQL Server VM and you have the Quantum VSS agent installed, we highly recommend that you enable a SQL Server management policy to manage truncation of the SQL Server database logs.

References

Refer to the following articles for additional information on implementing automation to manage SQL Server log files.

If you choose not to implement a SQL Server transaction log maintenance plan, make sure to monitor the available disk space on any volume where you have a SQL database present. If a transaction log is left unchecked for a long enough period of time, it may fill the disk and potentially interfere with SQL server operations and successful VM backups.

MS TechNet Articles

- MS189085 Transaction Log Truncation:

  https://technet.microsoft.com/en-us/library/ms189085(v=sql.105)

- MS178037 Shrinking the Transaction Log:

  https://technet.microsoft.com/en-us/library/ms178037(v=sql.105)

- MS189826 Using Transact-SQL:
  http://technet.microsoft.com/en-us/library/ms189826(v=sql.90)
- MS170572 Using the sqlcmd utility:
  http://technet.microsoft.com/en-us/library/ms170572(SQL.90).aspx
- MS170572 Using the sqlcmd utility:
  http://technet.microsoft.com/en-us/library/ms170572(SQL.90).aspx

Recovery Notes and Best Practices

For the fastest access to File Level Recovery, use the vmPRO **Recover Virtual Machines Wizard** to recover virtual machines (VMs) backed up with a third-party application. This wizard provides file-level access to the backups at the **\\vmPRO\recover\files** CIFS share.

For information regarding data recovery of VMs, see the **vmPRO Data Recovery** book in the vmPRO 3.3 Online Help.

Helpful Resources

Use the following resources for further assistance.

Request a trial copy of vmPRO Virtual Appliance

You can request a trial copy of the vmPRO Virtual Appliance on the Quantum Website. Please allow 48 hours for processing.

Use the following link: http://www.quantum.com/products/software/vmPROTrial/index.aspx

Access the complete documentation set and software downloads

You can access the complete vmPRO Virtual Appliance documentation set, software downloads, and knowledge base articles at the following links.

- Mosaic Web Siste (https://mosaic.quantum.com/)
- Quantum Web Site (www.quantum.com)

Access additional information

You can access additional documents, references, and information regarding specific activities and products at the following links:

- Quantum Web Site (http://www.quantum.com)
- Quantum Service Web Site (http://www.quantum.com/serviceandsupport/index.aspx)

Call Center Americas

You can contact Quantum's world-class support representatives at the following:

- Telephone (toll free): 800-284-5101
- Telephone (local, not toll-free): 949-725-2100

Call Center Americas hours of operation follow. Note that these hours are subject to change without notice.

- 7 days a week, 24 hours a day with valid contract
- 7x24x4 or 7x24x2 coverage available

Note: Users with all other contracts can contact Quantum during normal business days from 5 AM to 5 PM US Pacific Time.

Quantum's Service-Level Objective

You can view Quantum's service-level objective on the Quantum Website.

Use the following link: http://www.quantum.com/ServiceandSupport/ServiceLevelAgreement/Index.aspx