vRanger Pro 4.5
&
Data Domain Integration

Best Practices

Technical Document
Knowledge Base
Date: September 27, 2010

Author: Chris Walker – Sr. Systems Engineer – USA – Eastern Region

Document Contributors:

Bernie Watson
Pete Park
Russ Sandow
Jason Mattox
Glen Porter
Mattias Sundling
Stefan Boesner
Tommy Patterson
Ray Leitz
Mark Leffler
Michael Bennett

Links to Companies referenced in this document:

vRanger Pro → www.quest.com
Data Domain → www.datadomain.com
VMware → www.vmware.com

The following abbreviations are used in this document:

DDR – Data Domain Restorer Appliance
vRanger – vRanger Pro 4.5
ESX – VMware ESX Host (Includes VMware ESX 3.x and 4.x Environments)
ESXi – VMware ESXi Host (Licensed)

Quest Software Virtualization Group Free Training Web Site:

http://training.vizioncore.com/

This document will be updated as new versions of vRanger Pro are released to the market. Please consult your Quest Software sales representative or engineer for the latest version.

Document Notes: This document demonstrates best practice recommendations for integrating vRanger Pro 4DPP and Data Domain technology in a VMware ESX environment. This document is not designed to show all the options that can be created and assumes the reader has a working knowledge of vRanger Pro 4, Data Domain Appliances and VMware. This document is not intended to replace the product operations manuals.

Date	Document Version	Author	Change Notes
08/18/09	1.0.0	Chris Walker	Initial Document Release vRanger Pro 4.0
10/26/09	1.1.0	Chris Walker	Updated for vRanger Pro 4.1
11/11/09	1.1.1	Chris Walker	Updated a few Typos and DR Section
12/07/09	1.1.2	Chris Walker	Updated for vRanger 4.2 (Notes and FAQs)
09/27/10	1.5	Chris Walker	Updated for vRanger 4.5.3

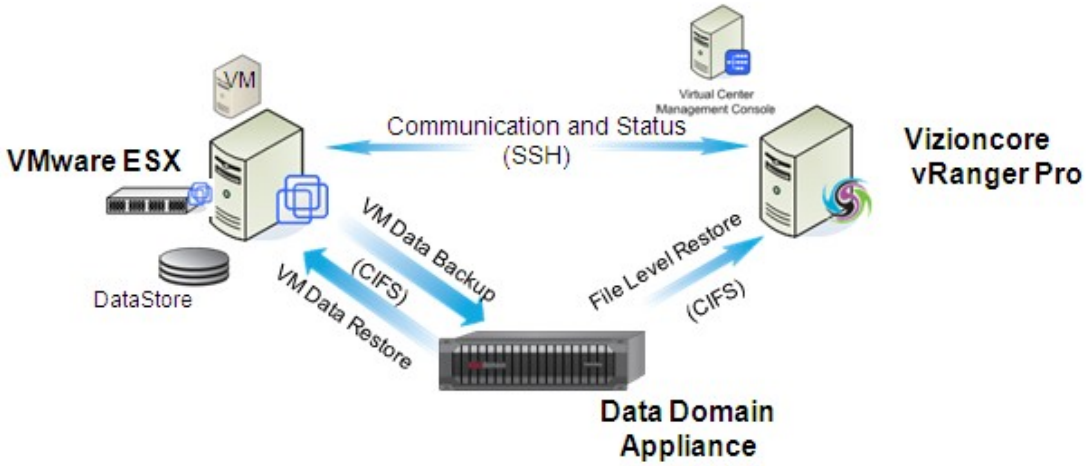
Contents

1. Architecture Overview

Quest Software vRanger Pro and Data Domain appliances provide companies with a simple and efficient method for backing up and recovering VMware environments. vRanger Pro provides significant enhancements with regard to architecture, performance and communications over traditional backup solutions. Data Domain provides superior data de-duplication capabilities. The combination of vRanger Pro and Data Domain Technology will dramatically reduce your backup and recovery time for virtual machines on VMware ESX hosts.

vRanger Pro provides a direct-to-target backup architecture, allowing for much faster backups across the entire VMware environment.

vRanger Pro 4 – Direct to Target Architecture



Note: VMware Consolidate Backup (VCB) is not used in this configuration.

1.1 Communication and Data Flow Details

1. Communication and Control
    a. vRanger → Virtual Center – Ports 443 and 902
    b. vRanger → ESX Host – Port 22 (Encrypted SSH)
2. VM Backup:
    a. vRanger injects applications for execution into ESX Host Service Console
    b. ESX Host → CIFS → Data Domain (DDR)
        i. Empty VM disk blocks are not transferred to DDR
    c. vRanger removes application from ESX Host Service Console when finished
3. VM Restore: (Full or Individual VMDK)
    a. vRanger injects applications for execution into ESX Host Service Console
    b. Data Domain (DDR) → CIFS → ESX Host
        i. Empty VM disk blocks are not transferred from the DDR
    c. vRanger removes application from ESX Host Service Console when finished
4. VM File Level Restore:
    a. Data Domain (DDR) → CIFS→ vRanger Host
    b. Image is mounted on vRanger Host
    c. File(s) can then be copied (Drag and Drop) to any host that is network connected to the vRanger Host.

2. vRanger Pro Server Preparation

vRanger Pro 4 uses a Microsoft SQL Express (Default Installation) or External Microsoft SQL database to store job configuration, event correlation and data-archiving information. The following recommendations from Quest Software are based on the Microsoft SQL Express and vRanger Pro requirements for a typical implementation of fewer than 30 ESX hosts. Actual requirements may be larger based on specific needs for each environment. Please consult the vRanger Pro Installation manual for further sizing guidance.

1. It is recommended that vRanger Pro 4 be installed in a virtual machine, as it does not move any data.
    a. It is **NOT** recommended for the vRanger Pro application to be installed on the repository. Data Domain equipment is an appliance so this note is purely informational.
        i. Reason: If the repository host gets overloaded this will result in vRanger disconnecting from the ESX host and backup failures.
    b. It is **NOT** recommended for the vRanger Pro Application to be installed on the VirtualCenter Host.
        i. Reason: Product releases for VirtualCenter and vRanger Pro are not necessarily launched during the same time frame. Since both systems utilize MS SQL, upgrades to either product may cause compatibility issues especially around MS SQL operations resulting in possible outages for one or both of the systems.
2. vRanger Pro Virtual Machine configuration (< 30 ESX Hosts)
    a. MS Windows Server (2003-2008) 32/64-bit
    b. 2 virtual CPUs for best performance
    c. 4GB RAM (2008 64 Bit may need more memory)
    d. Recommended disk configurations:
        i. C: MS Windows OS – 10GB
        ii. D: MS Windows OS Page File – 5GB (Move Page Files to this Drive)
        iii. F: vRanger Pro – 30GB
        Note: The drives are broken out to improve MS Windows and VMware performance
    e. It is also recommended to properly align the disk blocks for better performance. Quest Software vOptimizer Pro solution can be used to perform VM 64K partition alignments.
3. For environments with more than 30 ESX hosts, consult the vRanger Pro deployment guide. Such configurations may require using an external MS SQL server for the vRanger Pro database to reside on.

2.1 Installation Planning

A critical stage of any data protection system implementation is to properly plan and design the most optimal deployment configuration in order to meet the recovery objective requirements of the business. vRanger Pro gives users the ability to retain data for the same virtual machine from different time ranges, as well as to send that data to multiple repositories that may perform different purposes. In turn, using Data Domain's Replicator software capabilities, vRanger Pro repositories can be replicated to one or more other Data Domain Restorers for multiple purposes, including offsite disaster recovery and consolidated tape vaulting by a third-party backup application.

Example 1: Certain VMs are backed up to "BackupShare1" stored on Data Domain Restorer DDR1 and not replicated but backed up / vaulted to tape for long term storage by a third party backup application.

Example 2: Certain VMs are backed up to "BackupShare2" stored on Data Domain Restorer DDR1 and replicated to Data Domain Restorer DDR2 installed in a remote facility for Disaster Recovery purposes.

Example 3: Certain VMs are backed up to "BackupShare3" stored on Data Domain Restorer DDR1 and replicated to Data Domain Restorer DDR3 installed in a third facility for test/development purposes.

Utilizing the above examples it is possible to:

1. Create multiple retention policies based on the application and/or data type
    a. A virtual machine carrying higher rates of data change can backup to an isolated directory in order to accommodate more aggressive replication policies.
    b. Virtual machines with large amounts of static data can be grouped together and backed up to a directory that might use less frequent replication settings.
2. Create multiple directory replication policies on the DD System to efficiently replicate the backups to one or more DD Systems in the other locations.
3. Schedule regular restoration of virtual machines to pre-stage the Disaster Recovery environment.

Notes:

1. *It is possible for multiple "Backup Shares" to exist on one DDR and be replicated to multiple locations.*
2. *Even though vRanger Pro may be writing multiple backups of the same data to the DDR, the DDR will still de-duplicate this data across the multiple directories.*

Planning overview:

1. Planning
    a. Repository names and conventions
    b. Job naming and conventions
    c. Data classification
    d. Data retention policies
    e. Directory structure layout and CIFS Share nomenclature on DDR(s)
    f. Replication design between multiple DDRs (when applicable)
2. DDR Configuration
    a. DNS configuration (forward and reverse look up)
    b. Active directory or workgroup for user authentication
    c. CIFS Mount point creation
    d. Granting ESX host access to DDR by DNS or host entries
    e. ESX Host firewall
    f. ESX Host test for connectivity to DDR
3. vRanger Pro Installation and Repository Configuration
    a. Install/update vRanger Pro with repository information for DDR
    b. Test Backup
    c. Tuning recommendations for ESX Host

Based on the information presented above, it is highly recommend that some time be devoted to laying an optimal backup infrastructure. Key aspects to keep in mind:

a. Backup windows – full, differentials, incremental
b. Recovery requirements – applications and data
c. Repository names and conventions
d. Job naming and conventions
e. Data retention
f. Data replication with the DDR
g. Backup Network Path (Connection points between key Devices)
h. Aggregate write throughput (MB/s) and maximum stream count capabilities for a given DD System (based on model and DD OS version level)

Information regarding aggregate I/O write operation throughput and maximum stream count capabilities for a given Data Domain model and OS version level can be found on the Data Domain Support site at http://my.datadomain.com.

3. Production Environment Configuration

As described in the Overview section of this document, vRanger Pro uses the CIFS protocol to connect from a given ESX server's service console directly to the DDR. This architecture is called "Direct to Target" and does not use VMware Consolidate Backup (VCB) or the new VMware Storage API.

- vRanger Pro can utilize the new VMware vStorage API to perform LAN free (fibre) backups but it is not recommended at this time by this author for backing up to a DDR unless you have ESXi (Licensed) hosts. Reason: Utilizing the vStorage API complicates the configuration greatly requiring proxy machines to facilitate back up with fibre channel connections. This configuration is often slower than the direct to target architecture as well.

3.1 User ID/Directory Creation – Important Notes

User ID recommendations:
Example: One repository accessed with an Active Directory ID of MYCOMPANY\vranger

- The user ID used with the DDR should be the same across all Repositories (This is not required, but it does add simplicity for administration.)
- Strong passwords are recommended and, if security policies permit, the password on the DDR should **NOT** be configured to change regularly unless the environment is monitored with ongoing persistence. (Please ensure that backup failure event notifications are properly configured and monitored if password change policies are implemented in the environment.)
- If the user ID or password changes on the DDR, vRanger backups will stop until the repository password is reset in vRanger to match the password on the DDR.

Note: The vRanger Host Login ID and Repository ID can be different. vRanger Pro users do not need to have any access to the vRanger Repositories/DDR.

It is very important to create the IDs and Directories in the order displayed in this section. File level restore from vRanger Pro may not work properly if the vRanger server does not have full access to the CIFS share on the DDR. Creating the directories first using a Windows Explorer interface on the DDR will ensure that the proper rights flow down to directories and files created by vRanger/ESX hosts.

3.2 Configure the Data Domain Appliance for Access

This section describes the creation of user IDs and CIFS shares on the Data Domain Appliance that will be used by vRanger Pro.

Notes:

1. This section assumes that the DDR is on the network and remote SSH access is enabled.
2. This section assumes the CIFS protocol is active on the DDR.
3. This section assumes you have a working knowledge of the DDR OS.
4. Once vRanger Pro is configured, any valid user account can be used to log into the vRanger server. It is not required to log into the vRanger Pro server using the repository/DDR account.

Configuration Process Steps:

A. Create vRanger Pro Repository ID on DDR
B. Grant Access to the vRanger Host from the DDR (Temporary)
C. Create Repository (CIFS Share) on the DDR
D. Grant Access to vRanger Host and ESX Host to Repository (CIFS Share)

The following example will use the parameters:

vranger_repository_access = User ID that will have access to the repository
vranger_repository_directory = vRanger Repository CIFS Share
ddr_name = DNS Name of DDR
share_name = DDR Repository Share Name

Configuration Step A. Create vRanger Repository ID on DDR:

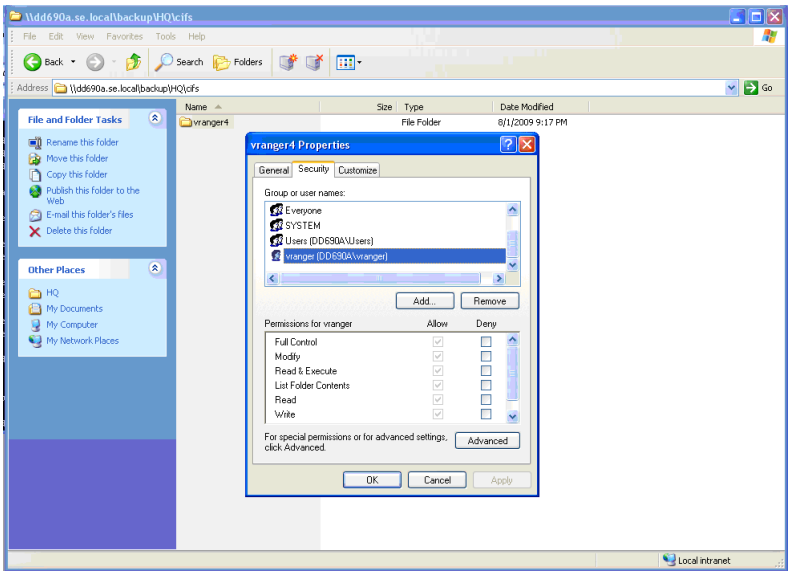
1. Connect to the DDR utilizing PuTTY or your favorite SSH Client. (ID: sysadmin)
2. Use one of the two methods outlined below, to create a new user ID on the DDR for the vRanger repository access. This ID is for vRanger to access the repository (Windows Share) on the DDR.
    a. ***DDR in Workgroup mode:***
        i. **DDR Command:**
            1. user add <vranger_repository_access> priv user
            Note: you will be prompted for the password.
    b. ***DDR in Active Directory mode:***
        i. This section assumes that the DDR is properly joined to the AD domain. If necessary, consult the DD OS users guide for more information regarding AD integration.
        ii. Create a user in AD (vranger_repository_access) that will be used to access the repositories on the DDR.
        Note: When using DDR running DDOS 4.5.x or higher, and in Active Directory mode, the Microsoft Management Console can be used to manage user access permissions on the DDR for the vRanger user to access directory shares. Consult the DDOS Users Guide, or contact Data Domain for more information on using the MMC to manage NTFS directory permissions on the DDR.
        iii. **DDR Command: (Troubleshooting only)**
            1. CIFS troubleshooting user <vranger_repository_access>
            Note: This will provide the user ID, SID, group(s), and group ID associated with the user account on the DDR from AD

Configuration Step B. Grant Access to the vRanger Host from the DDR (Temporary)

1. Connect to the DDR utilizing PuTTY or your favorite SSH Client. (ID: sysadmin)
2. Enable CIFS access for the vRanger server to connect to the DDR's /backup share:
    a. **DDR Command:**
        i. CIFS add /backup <IP of vRanger server> <FQDN of vRanger server>

Configuration Step C. Create Repository (CIFS Share) on DDR

1. Logon to the Windows vRanger Server. (RDP or Virtual Center Console)
    a. The ID used must be able to run vRanger but does not need access to the repository share
2. Using Windows Explorer on the vRanger server connect to the repository created on the DDR
    a. Start→Run: \\ddr_name\backup
        i. This should ask for an ID and Password
    b. **Important:** Make sure you connect to the share (\\ddr_name\backup) on the DDR using the workgroup or AD account created earlier (ID from above: vranger_repository_access).
3. Browse the DDR's \\ddr_name\backup" share, and create the desired directory structure for vRanger to use on the DDR
    a. Example directory structure to create on the DDR: (from Planning Session)
        i. \\ddr_name\backup\HQ\vranger\
4. Using Windows Explorer (Shown below), verify that the *vranger_repository_access* account has full control to the directory created in Section A above.
    a. Note: The repository account must have full control of the directory in order to successfully create and manage all content within the repository on the DDR.



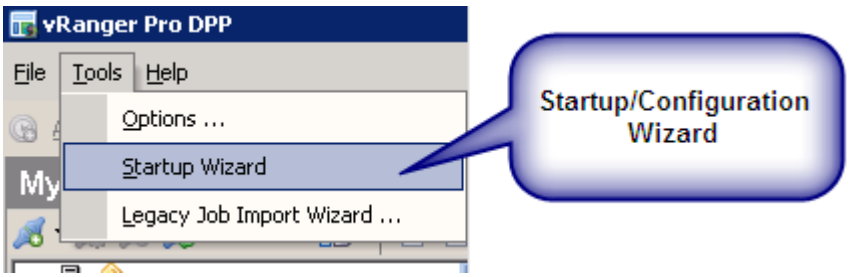
Configuration Step D. Grant Access to vRanger Host and ESX Host to Repository (CIFS Share)

1. CIFS share security can now be added on the DDR in order to further secure the directory/repository by DNS/IP Address.
2. Connect to the DDR utilizing PuTTY or your favorite SSH Client. (ID: sysadmin).
    a. Add Access for the vRanger Host and all ESX Host Service Consoles:
        i. DDR Command:
            1. CIFS share create <share_name> path /backup/<path created for vranger on DDR> clients "<IP of vRanger server>,<FQDN of vRanger server><IP of each ESX host Svc Console>,<FQDN of ESX host Svc Console>" users "<vranger_repository_access>"
        ii. Important Notes:
            1. *You must add all of the IP and FQDNs in one line. There is no "CIFS share MODIFY/ADD" command. Each time you run this command it will overwrite the previous settings.*
            2. *Best practice is to enable access to a CIFS share by listing both the IP address and the FQDN of each ESX host's and vRanger System that will be writing to the CIFS share on the DDR*
            3. *It is assumed that the Service Console of each ESX host has a valid DNS entry with both forward and reverse DNS address resolution*
            4. *For more information on the "CIFS share create" command, please refer to the Data Domain OS Users Guide.*

3.3 Adding a Repository to vRanger Pro

Adding a vRanger Pro repository can be done in two ways. The first is during installation using the “Startup Wizard” or second from the “Repository” menu screen. This section assumes that vRanger Pro is already installed and will focus on the creation of a new Repository for the DDR.

Startup Wizard Option: The Installation “Startup Wizard” can be accessed at any time from the main menu. This wizard walks through the configuration settings of vRanger including Repository creation.

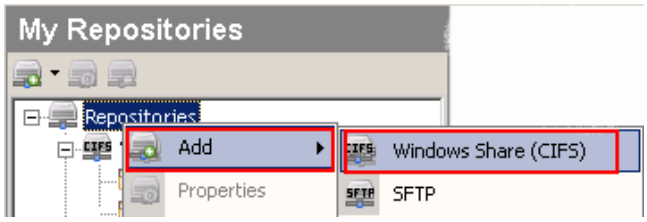


Adding a Repository from the Repository Menu

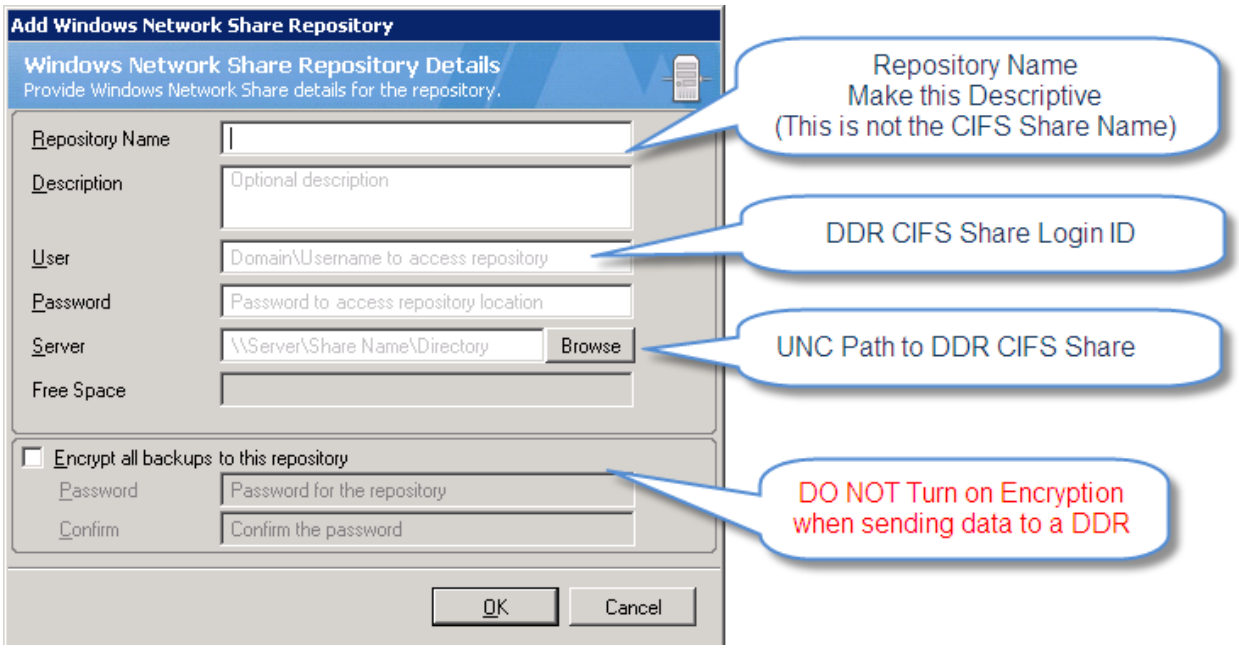
vRanger Pro Menu Navigation:

(Left Hand Menu)

Right Mouse Click on “Repositories”, Click “Add” Click Windows Share (CIFS):



The following screen will appear to show to configure the connection to the DDR (CIFS Share).



After entering all the relevant information press “OK”. This will perform a test for connectivity, and also create a “GlobalManifest.metadata” file on the CIFS share for faster indexing of data.

Notes on this Screen:

1. The “User” and “Password” fields are used by vRanger to access the Repository CIFS Share. **The User ID that logs into the vRanger Pro server does not need to have any access to the Repository Share.**
2. The ID entered here is stored in the SQL database with AES 256 Bit encryption.
3. Repository Encryption – Do **NOT** turn this feature on when sending data to a DDR. This will cause every block written to the DDR to be unique and cause the de-duplication process not to function at the full potential.

4. Disaster Recovery Environment Configuration

Data Domain has the ability to replicate data from one DDR system to another DDR system. In fact, one-to-many or many-to-one replication scenarios can be configured for maximum options for Disaster Recovery and Test purposes. Replication processes on the DDR are executed at a directory level. So proper planning is required.

The replicated data is in a “Read-Only” state unless it is modified using DDR OS commands. vRanger Pro can read this data in a “Read-Only” state and facilitate restores of the Virtual Machines. Please review Appendix D for a diagram of options on how vRanger can be used.

4.1 Adding a Replicated Repository (Read-Only)

Read-only repositories are used to access data that has been replicated to a remote repository. Generally this is done for Disaster Recovery purposes. Please see Appendix D of this document for diagrams of scenarios.

Section Terminology:

DDR-DR → Data Domain Appliance where Replicated Copy of Data Exist

Notes:

1. When using a replicated copy of the repository, nothing is written by vRanger to the DDR-DR. A temporary directory is created on the vRanger Pro host to manage metadata.

Setup:

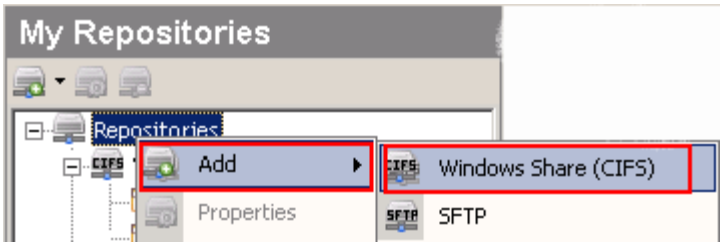
1. The vRanger Host system must be granted Read-Only access to DDR-DR replicated Share directory. (See Section 3.2.B)
2. Each ESX host that is going to receive the data needs to be added access to DDR-DR. (See Section 3.2B)

vRanger Pro Menu Navigation:

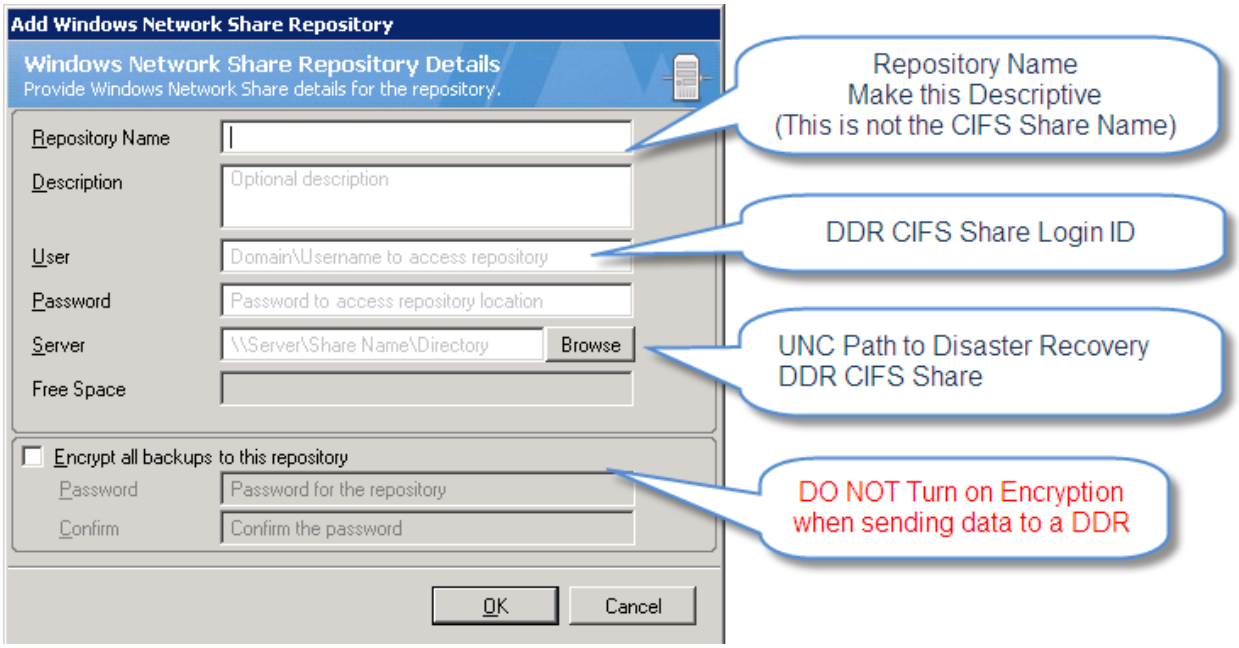
(Left Hand Menu)

→

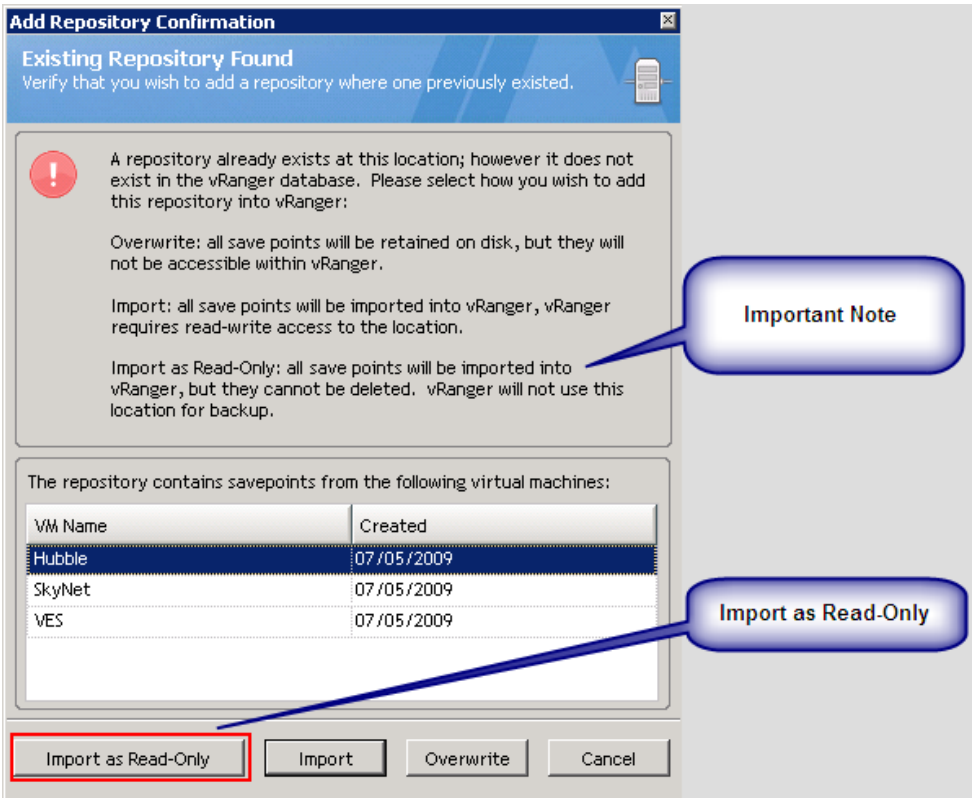
Right Mouse Click on “Repositories”, Click “Add” Click Windows Share (CIFS):



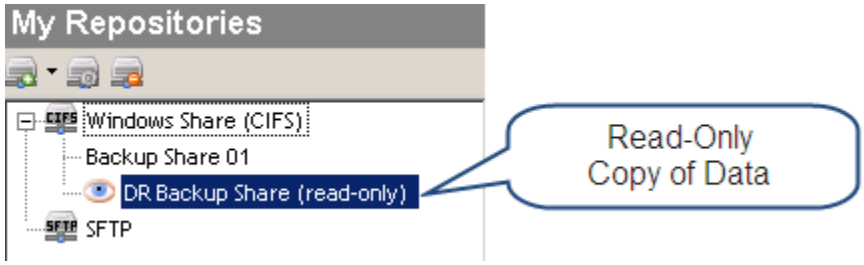
The following screen will appear to show to configure the connection to the DDR (CIFS Share).



After entering all the relevant information press “OK”. This will perform a test for connectivity, and show the following information if a “GlobalManifest.metadata” file exists.



Once configured your Repository view should look like this:



Appendix A: Troubleshooting

At the time of document creation, the following versions were field tested by Quest Software and Data Domain:

vRanger Pro Version: 4.5.3 www.vizioncore.com
Data Domain OS Version: 4.9 www.datadomain.com
VMware ESX: 3.0.2, 3.5, 4.0, 4.1 www.vmware.com

The following tests are in order based on tests that have helped to resolve issues.

1. **Verify DNS**
   a. Verify each of the following can do a simple ping of short and long(FQDN) DNS name
      i. vRanger Pro Server → Virtual Center, ESX Host Service Console, DDR
      ii. ESX Host Service Console → vRanger Pro Server, DDR
      iii. DDR → vRanger Server, ESX Host Service Console

   Note: IP address are used by vRanger but CIFS may use IP or DNS for authentication
2. **Verify Time Synchronization**
   a. It is very important that time synchronization is consistent across all systems that vRanger is communicating with. Verify that all systems have the same time and date.
3. **Test that the DDR can see the User ID for the repository login:**
   a. DDR Command: CIFS troubleshooting user <repository_username>
   Note: This will provide the user ID, SID, group(s), and group ID associated with the user account on the DDR from AD.
4. **Test that your ESX host Service Console can write to the target outside of vRanger**

Note: If your password contains special characters ($!% etc), put it in single quotes.
Test: SSH to the ESX Host that you would like to test:
*mkdir /mnt/backup (*This is a temporary place to mount the CIFS Share on ESX*)*
*esxcfg-firewall -e smbClient (*Verify ESX Firewall is open for SMB*)*
Connect the CIFS share onto your ESX host mount point.
(ESX 3)
"mount -t smbfs //RepositoryServer/Share /mnt/backup –o username=Test12,password=Password"
(ESX 4)
"mount -t cifs -o username=user,password=password //RepositoryServer /Share /mnt/backup"
If the mount times out check the DNS entries first with a simple ping.
At this point you can do a regular copy from Host to destination or touch.
Don't forget to un-mount the CIFS Share – "umount /mnt/backup"

Appendix B: Performance Tuning

There are many factors that can affect performance for backup and restore of data. vRanger can generate a very large amount of data being sent to the DDR systems. Care must be taken not to overload any one system with too many streams from vRanger and to properly load balance the Network Adaptors on the DDR. The following are some general topics and concepts that must be reviewed to ensure maximum backup speed while eliminating the risk of failures.

1. VMware Service Console Tuning
    a. Memory: Increase the amount of memory given to the service console. Different versions of VMware ESX will default to different levels. It is recommended to grant the max allowed to the service console to improve backup and restore speeds.
        i. Note: When this is changed it will require a reboot of the ESX Host to take effect.
    b. CPU: Increase the CPU to the service console. Different versions of VMware ESX will default to different levels. It is recommended that the service console is set to “Unlimited” CPU Access.
2. Switches, Routers and Firewalls
    a. When possible, minimize the number of route hops between the ESX Host Service Console and the DDR.
        i. Check hops, firewalls, proxies
        ii. High latency or even slow ping results can have huge affects on backup software that is moving large amounts of data.
3. DDR
    a. It is recommended to present each repository share on a different network adaptor that is on the same subnet as the ESX host that is being backed up. This will allow individual DDR NICs to process data faster. If you have a 10Gig NIC in your DDR this will not be necessary but should be on the same subnet as the ESX host service console.
4. vRanger Backup Streams
    a. Verify in the menu “Tools + Options” that the Repository (DDR) can accept enough backup streams. The number of backup streams accepted by a DD can be found on http://my.datadomain.com/. They vary by model.
    b. Verify that through put (MB/s) performance of your DDR model at http://my.datadomain.com/. This is also important as each model has a maximum capacity of data that it can ingest at any one time. This being said please remember that when vRanger is backing up a 100 Gig VM with only 10 Gig of data you will not need the full performance of the DDR while vRanger skips the “Blank” space in the VM.
5. vRanger Compression
    a. Make sure it is turned off on all Jobs. This is essential when writing to a de-duplication system such as Data Domain. Also this reduces the load on the ESX Host.

Appendix C: FAQs for vRanger Pro

Q: Does vRanger Pro 4.5 support VMware ESX 3.x and 4.x. (Virtual Center and vSphere)?
A: **Yes**. Please review the compatibility matrix at the following link for the latest information:
http://vizioncore.com/support/version-support

Q: Does vRanger Pro 4.5 support ESXi?
A: **Yes**, ESXi (Licensed Version) is supported.
- However this document does not cover ESXi Backup to a DDR.

Q: Do I need to turn on vRanger Data Compression?
A. **No.** This will cause the DDR to try to de-duplicate compressed data and actually cause extra overhead (storage) on the DDR and the ESX host that is not needed.

Q: Does vRanger support CIFS or NFS Protocols for the repository?
A: At this time vRanger Pro 4.5 only supports the CIFS and SFTP transport protocol from the ESX host (Direct to Target). That being said, there are many enhancements in the vRanger Pro 4 engine that allow for greater performance over the vRanger 3.x NFS backup option and also any VCB options. NFS Support is expected to be added in vRanger Pro very soon.

Q: In the future how will I convert my Data Domain Repository to NFS?
A: vRanger Pro will support NFS Repositories in the very near future. When this happens, clients will be able to disconnect the CIFS repositories and reconnect them as NFS with no data loss. Backup Job Reconfiguration may be required.

Q: Does vRanger Pro 4.x series require the setup of a Datastore on each ESX Host as did previous versions?
A: No. The vRanger Pro 4 backup engine can talk directly to the DDR via each ESX Host's Service Console.

Q: How do I access the vRanger API?
A: The vRanger Pro 4 API can be accessed from PowerShell. This will be the command line language for all vRanger 4 functions in the future. See the user manual for instructions. Examples of vRanger 4 PowerShell capabilities include (but are not limited to):
a. List all VMs in Virtual Center and compare to vRanger Backup Jobs; find Missed VMs
b. Schedule tape backup of vRanger Repositories

Q: Will a full backup be required if vMotion (Host to Host) or Storage vMotion occurs?
A: No if the VM is in the same Backup Job. vRanger Pro tracks the virtual machine (VM) in the environment and will not need to perform a new full backup for a VM that has changed host for a backup job.

Q: How much CPU is required on the ESX Host?
A: vRanger Pro 4 with Direct-to-Target Architecture uses the ESX Service Console. The Service Console (ESX 3 and 4) only uses one core of the CPU. Based on current testing, vRanger Pro 4 only uses 30-40 percent of one core in the physical ESX host during backup and restore processes. The options in vRanger Pro can be modified to perform more backups per ESX host and Datastore, so these numbers will vary based on your configuration. (Review the vRanger Menu Options – Tools, Options, MyJobs, Configuration)

Q: How much throughput should I get per ESX Host?
A: Many vRanger customers are seeing 50-80MB/Sec per ESX Host. This will vary based on your ESX Host, Network, DDR Appliance and DDR load at the time of backup.
Some clients with 10GB interfaces in their ESX Host have seen 180MB/s… Per ESX Host.
The data ingestion rate of the DDR is generally the bottle neck.

Q: How can I read/use the vRanger Repositories that have been replicated to a remote DDR?
A: vRanger Pro versions 4.1 and higher has the ability to use replicated (Read-Only) repositories.
a. See Section 4 of this document on how to add Replicated Repositories
b. See Appendix D for an overview diagram

Q: Can vRanger 4 read and restore vRanger 3.x backup Data?
A: Yes. See the vRanger Pro 4 documentation for more details.

Q: Does vRanger support Microsoft Volume Shadow Services (VSS)?
A: Yes. VMware Tools 3.5 U2 and greater has added VSS as an option. vRanger 4 can activate VSS through the VMware Tools if selected in the vRanger backup job configuration. If you need more application consistency please reviews the vRanger Pro deployment guide for the vRanger VSS 4.5 VSS Driver.
Note: If the VMware Tools were upgrade the VSS driver may not be added automatically. You need to verify that the VSS drive is installed. When VMware tools is a new install and 3.5 U2 or higher is present then the VSS driver is the default install.
A1: If a job is schedule on a VM that does not the VSS driver enabled the backup of that VM will fail. Please ensure that VSS is enabled in the VMware tools on the guest VM.

Q: Can I install vRanger on the Virtual Center host?
A: This is **NOT** recommended! Reason: Virtual Center and vRanger both use MS SQL. Product upgrades may cause outages. Also the memory and CPU required may overload a single host.

Q: Can I install vRanger on the Repository Host?
A: Yes. But **NOT** recommended! Reason: If the Repository Host gets overloaded with backup data streaming in…vRanger will lose communication to the ESX host and the backup will fail.

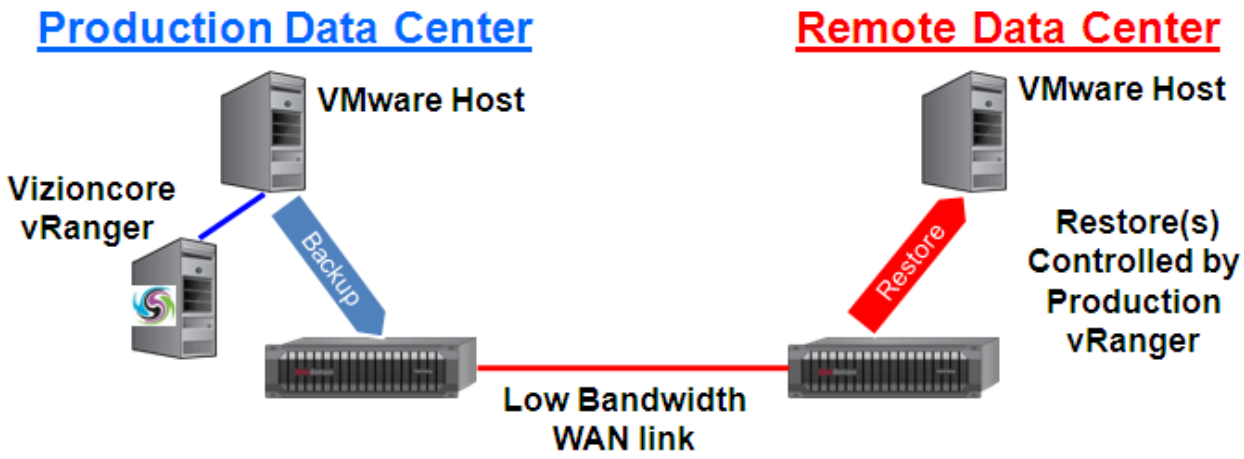
Q: Does vRanger Pro 4 support File Level Restore for both Windows and Linux Virtual Machines?
A: vRanger Pro 4.5 only supports Microsoft Windows file level restores at this time. Linux File Level restore is coming soon.

Q: Can I do a backup of a VM that has an existing snapshot?
A: **Yes.** If a Differential or Incremental is scheduled, there will be an error noted in the log files, but vRanger will perform a full backup of the VM.

Q: Where can I get training on vRanger Pro?
A: Training for all Vizioncore software Solutions are available at http://training.vizioncore.com

Appendix D.1: DR Example 1

Central Control – 1 vRanger Host

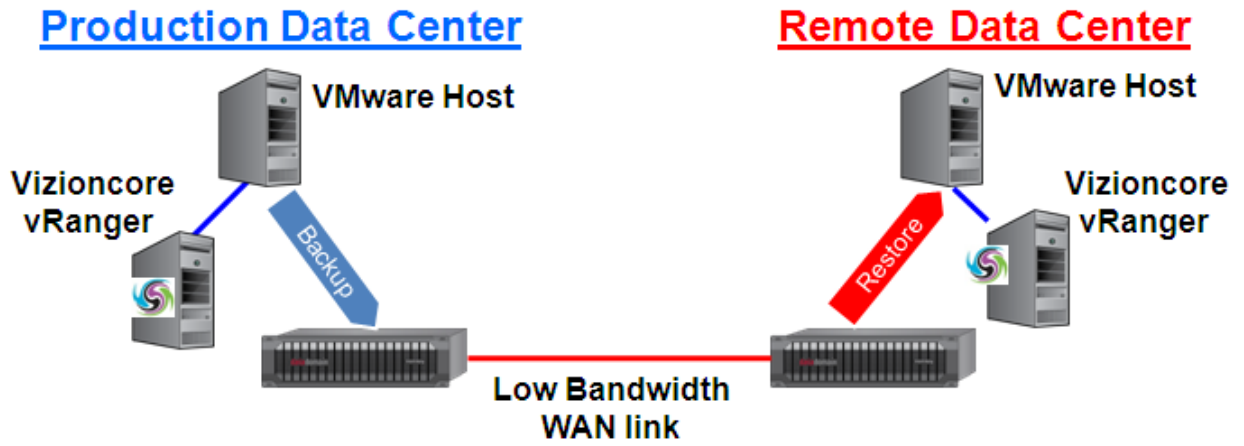


Notes:

1. See “Disaster Recovery Section” section of this document
2. vRanger only needs to be licensed for ESX Hosts that are backed up. You do not need to License ESX Hosts that are restore targets only.

Appendix D.2: DR Example 2

Distributed Control – 2 vRanger Host



Notes:

1. See “Disaster Recovery Section” section of this document
2. vRanger only needs to be licensed for ESX Hosts that are backed up. You do not need to License ESX Hosts that are restore targets only.