NETAPP TECHNICAL REPORT

NETAPP PROTECTION MANAGER
PROTECTING YOUR DATA: POLICY-DRIVEN DATA MANAGEMENT

Jai Desai, NetApp
TR-3524-0207

ENABLING COMPREHENSIVE DATA MANAGEMENT SERVICES

This document provides an overview of how NetApp protection manager can be used to deploy an automated management policy to deliver comprehensive data management services. The NetApp protection manager applications are described, and information is provided on how the NetApp protection manager automated management differs from other solutions available today.

TABLE OF CONTENTS

1 WHAT IS NETAPP PROTECTION MANAGER?

NetApp protection manager is backup and replication management software for a NetApp disk-based data protection environment. NetApp protection manager delivers assured data protection and higher productivity by providing policy-based management, including automated data protection configuration.

NetApp protection manager provides higher data protection by eliminating the manual errors associated with configuring data protection in a dynamic environment. Automation and policy-based management reduce the possibility of user errors. This provides a higher level of assurance that the data is protected and hence available.

NetApp protection manager provides a holistic view of the NetApp disk-based data protection environment and increases the productivity of administrators by eliminating the repetitive tasks associated with backup and replication configuration setup. It also allows architects the ability to delegate the data protection tasks to backup administrators, freeing them to focus on higher value tasks.

NetApp protection manager enables users to consolidate the secondary storage resources into resource pools. These consolidated resource pools are then allocated to several data sets, thus ensuring maximum utilization of secondary storage resources.

NetApp protection manager increases scalability, efficiency, and flexibility by automated setup, scheduling, monitoring of which backups exist for a particular primary data set, and policy-based management. It reduces the time, resources, and expertise required for backup and replication tasks by reducing the many manual tasks and eliminating the complexity associated with scripting and other tasks in a large-scale and complex environment.

NetApp protection manager encapsulates the best practices recommendations by NetApp in a simple, centrally managed, policy-driven data protection tool. By seamlessly integrating the data protection features offered by NetApp, NetApp protection manager delivers a full, backup and replication solution without needing a NetApp technology expert.

2 NETAPP PROTECTION MANAGER BENEFITS

In today's business environment, two things are constant for customers:

- Growth in end-user/business data
- Dynamic nature of the business, which leads to a dynamic environment

Protecting the vast amount of growing data is a critical need to keep the business going at full steam.

Over the years, data protection infrastructures have become solid and are evolving further to meet the speed and reliability needs of the business. Individually each of these technologies is getting easier to set up and use. In this environment, some of the key data protections challenges customers mentions are:

- Guaranteeing the recoverability of the data
- Efficiently managing the data protection environment

Today, in most IT environments, the process involved in setting up the backup part for new data coming online is fairly streamlined. This process is considered essential and is an expensive part of getting the data online. The expensive nature of this process comes from the manual steps required to map the end-user data to the actual storage that needs to be backed up and the multiple independent configurations that need to be set up to get the total data protection lifecycle setup complete.

As we all know, data environments keep constantly evolving and changing. Most organizations do not have a rigid process to tie the changes in environment to the data protection process. This can lead to a situation where some current data is not getting backed up. The biggest risk in this whole process is that customers will find out the real impact only when the data is requested to be restored. This uncertainty leads to sleepless nights for backup managers who commit to SLAs.

To eliminate the sleepless nights and to deliver confidence to business, backup managers need to determine what data is getting backed up and what is not. Today, to get this picture, the backup team has to go through lots of manual inventory, scripted queries, and manual correlation to figure out where things

stand. The time it takes to accomplish this means the status gathered is out of date. Also, when one part of the data protection infrastructure has a hiccup, with today's tools, it is extremely hard for an administrator to identify what data groups are affected.

Even when the changes in data environments are identified, the process required to do the mapping and find the right kind of backup infrastructure required to get the whole backup process going fine is manual and time consuming. Customers have spent a lot of resources in optimizing their primary storage for excellent storage utilization. But, they have had very few tools to optimize their data protection infrastructure utilization. In most IT environments, the data protection resources are five to 50 times more than the storage admin that maintains primary data. Even incremental optimization would lead to tremendous amounts of savings.

The primary reasons for no optimal utilization of resources are the complex planning and manual configurations required to keep the efficiency high. With data growth exceeding IT personnel resource growth, customers are forced to take actions that create quick solutions, but not the most efficient decisions.

NetApp protection manager provides the tools that will help customers with all of the above mentioned challenges. The value propositions are as follows:

1. Dramatically simplifies addition of data protection to new and existing user/project data.
2. Enables backup organizations to determine and demonstrate data protection compliance with ease.
3. Optimizes utilization of data protection resources.
4. Automatically detects existing data protection relationships and admin can manually import them, thus making it easy to deploy in legacy environments.
5. Uses a common easy-to-use interface for disk-based backup and mirroring management, hence simplifies learning and training.
6. Policy-based management using templates enables consistent data protection SLAs to be met.
7. Automated data protection reduces the risk of human error.
8. Maximized secondary storage resources utilization reduces capital expenditures.
9. Role-based access controls enable delegation between administrators.
10. Integration with NetApp operations manager enables centralized reporting, event management and configuration management.

2.1 RESOURCE POOLS

Resource pools typically describe physical resources such as spare disks, aggregates, or storage systems that have certain attributes such as size, cost, performance, and availability. These attributes are used by the storage admin when matching physical resources with provisioning or balancing data set operations.

A typical example of a resource pool may be a set of aggregates composed of inexpensive, slow ATA drives. This pool is suitable for archival or compliance purposes but not desirable for mission critical high-performance database applications. Another resource pool may consist of all the aggregate's attached to a given set of CFO or MetroCluster systems, providing highly reliable storage. Yet another resource pool may be a set of storage systems suitable for provisioning for certain departments within an organization.

Membership in a resource pool can be both static and dynamic in nature. For example, adding a storage system to a resource pool implies that all existing aggregates and disks on the storage system are included along with any new aggregates that are created. Note that members of a resource pool need not all reside on the same storage system or cluster.

Access to a resource pool is controlled by a Role-Based Access Control (RBAC) system, so some deployments may want to group homogeneous resources together as a way of restricting access to high-performance storage. Other deployments may construct resource pools with a mix of storage attributes as a means of providing better storage utilization across an organization.

The motivation for introducing resource pools is to provide a higher level management object that describes the attributes of storage. By grouping storage together according to physical resources such as

performance, cost, physical location, or availability, administrators can treat storage that is grouped this way as a single unit for monitoring, provisioning, reporting, and access control (RBAC). This simplifies the management of these resources and allows a more flexible and efficient use of the storage.

When a resource pool contains a storage system, all aggregates and disks on the storage system are available for provisioning. Resource pools may not nest and may not overlap (that is, storage in one resource pool may not be in another resource pool). Resource pools may appear in DataFabric Manager resource groups, but cannot contain groups.

For example, if a resource pool contains backup servers in New Jersey, NetApp protection manager can help set up mirroring of a volume in New York by creating an appropriately configured volume from the New Jersey backup server resource pool.

2.2 DATA SETS

A data set is the core new abstraction introduced by NetApp protection manager. From a user's perspective, a data set is the data stored in a collection of primary storage containers, plus all of the replicas of the data in those containers. A data protection policy is applied to the data set, directing how the user wishes the data to be protected. Notice that the data set is defined in terms of the data, not in terms of the containers holding the data.

Data sets describe data that has typically been selected from a primary source to which a policy needs to be applied. A data set may also be created by populating it from legacy storage containers such as existing Data ONTAP® volumes or third-party containers such as Open System SnapVault® directories.

Note that the policy associated with a data set can be explicitly changed. The data set is not bound to any actual physical location and could move over time. The storage containers associated with a data set may become obsolete over time, which could trigger the conformance engine to re-provision secondary storage when an aggregate fills up.

Application administrators can use data sets to group storage related to particular applications (example: the “Exchange data set” might contain the three LUNs comprising the Exchange database). Backup administrators can use data sets to group storage that gets backed up in the same way (example: the “desktops data set” might contain all of the desktop PCs that get backed up via Open System SnapVault® on a particular schedule).

Each data set can have no more than one protection policy. Any component within a data set that requires a different protection setting must be moved to its own data set.

2.3 DATA PROTECTION POLICIES

Policies are used to describe the desired behavior of provisioned data, also known as data sets. The policies are predefined protection policies, and in upcoming releases we shall introduce additional kinds of policies.

Resource pools are used by administrators to group physical assets together, but there is no mechanism to describe how these assets are to be used. Policies fill that void by providing the behavior needed to describe how the storage should be used and configured. The RBAC system, described later, is used to control who has access to various operations on which resources.

The basic model is that storage is protected by using a policy, which in turn matches the desired behavior with the storage described in the available resource groups. There is now a clear separation between the data protection policy and the physical location, which is important as we optimize the use of these resources over time. Many data sets can use the same policy.

Attributes associated with policies are abstracted at the highest level possible, allowing implementations of underlying technology to change over time without adversely impacting administrators. Administrators should be shielded from the idiosyncrasies of various underlying implementations, allowing the data set to utilize newer technology as it becomes available in an automated fashion.

The attributes in the policies generally focus on software technology and configuration settings rather than hardware choices, although the choice of hardware clearly has a major impact on the performance and cost

of the storage. The physical equipment choices are driven by a simple label scheme described in more detail shortly.

For the NetApp protection manager release, protection policies are a tree graph with a single primary node, zero or more secondary nodes, and exactly one connection leading to any secondary node.

For example, a protection policy may specify that the primary data is backed up to a secondary location, and that the secondary copies are mirrored to a tertiary location. The primary storage has a particular hourly/daily/weekly/monthly Snapshot™® schedule and retention settings; the backup connection has an hourly/weekly/monthly backup schedule and transfer throttle schedule; the secondary storage has its own retention settings; finally, the mirror connection has a mirror and throttle schedule.

Protection policies are defined in an abstract sense to allow for multiple implementations. For example, a protection policy refers to “backup connections,” which may be implemented with either SnapVault®® or qtree SnapMirror®. As new data protection products are released, NetApp protection manager can be updated to use the new products to implement existing policies.

Note: The first release of NetApp protection manager support SnapVault®, qtree SnapMirror®, and asynchronous volume SnapMirror®. It does not support synchronous VSM or semi-sync VSM.

Protection policies allow no overrides. If some portion of a data set requires different policy parameters, users must move that portion into a different data set with a different policy that captures the desired parameter changes.

2.4 ROLE-BASED ACCESS CONTROL

All managed objects such as resource pools and data sets are protected by a role-based access control (RBAC) system. Roles are created that provide access rights to various operations on these managed objects. The Role Based Access Control controls the access to various resources in the system.

Role Based Access Control roles, permissions, and objects are all centrally managed. When changing the capabilities associated with a role, or objects associated with that role, it is done in one place, authenticated, and audited.

2.5 CONFORMANCE CHECKER

Central to automation is a conformance checker process that examines the policies associated with each data set (each data set has an associated policy that contains the attributes and behavior desired) and can trigger actions such as rebalancing, reprovisioning, or alert generation as needed.

Various levels of action could be envisioned by this checker such as triggering alerts when policies are in violation, providing administrators the information needed to manually optimize their storage resources, or allowing the conformance checker to automatically take the necessary steps needed to protect data in accordance with policy.

3 THE PROBLEM AND SOLUTION

From a business point of view, NetApp protection manager aims to make it so easy to manage huge SnapMirror® and SnapVault® deployments that manageability objectives are not a barrier to further sales of SnapMirror® and SnapVault® licenses.

From a customer point of view, we observe that customers often protect their data in multiple ways (example: SnapVault® to a NearStore® appliance, then SnapMirror® to another NearStore appliance); they require simpler, more coherent ways to manage these data protection relationships. Current approaches treat SnapMirror® and SnapVault® separately.

Users can group their data into data sets and their storage into resource pools to allow NetApp protection manager to automate some routine data protection tasks such as applying consistent policies to primary data, propagating future policy changes, and provisioning new volumes to accomplish data protection goals.

The data protection policies of NetApp protection manager encapsulate all the settings needed to protect the data. Policies define:

- How many physical backup nodes to use
- When to create replicas (that is, Snapshot™ copies) of primary data
- How many replicas to keep on the primary storage
- What data protection protocol (that is, SnapVault® or SnapMirror®) to use to copy replicas from one stage to the next
- When NetApp protection manager is allowed to transfer data from stage to stage (thus limiting network traffic to certain times of the day)
- How many replicas to keep on primary, secondary and tertiary nodes

Finally, users assign a data protection policy to a data set. As part of this process, the user designates which resource pools to use to hold remote replicas of the data set. NetApp protection manager provisions destination volumes and qtrees from those resource pools to receive backup copies of the data set. NetApp protection manager then creates SnapVault® and SnapMirror® relationships from each volume and qtree in the data set to the newly provisioned destination storage.

Once a data set is configured and protected, NetApp protection manager will have two ongoing activities. First, NetApp protection manager will run the data protection schedules, creating Snapshot™ copies and initiating SnapVault® and SnapMirror® transfers at the appropriate times. Second, NetApp protection manager will periodically check that the data set fully conforms to its data protection policy. If either the data set or policy changes, NetApp protection manager will attempt to bring the data set back into conformance or highlight the situation to an admin.

4 INSTALLATION

4.1 DATAFABRIC® MANAGER SERVER

There are no changes from DFM 3.4 installation. Upgrade is possible from any DFM 3.x version to v3.5. If upgrade from DFM 2.x is needed, please see the limitations in the Installation guide. Databases are upgraded automatically, and best practice recommendation is to back up the database before upgrading.

For more information on DFM installation and troubleshooting, go to:

http://now.netapp.com/NOW/knowledge/docs/DFM_win/rel35.

4.2 NETAPP HOST AGENT

There is no new version shipping with version 3.5. When you install Open System SnapVault® 2.3 it bundles NetApp Host Agent version 2.3.1. NetApp protection manager supports version 2.3.1 and later.

4.3 NETAPP MANAGEMENT CONSOLE

Installers are renamed from “DataFabric Manager Client” to “NetApp Management Console.” The default installation path on Windows® is now C:\Program Files\NetApp\Management Console. You can install NetApp management consoles that are still available from NetApp operations manager via “Tools > Download Management Console.” You can upgrade from any previous (1.x) release of DFM Client.

5 NETAPP PROTECTION MANAGER THREE-TIER ARCHITECTURE

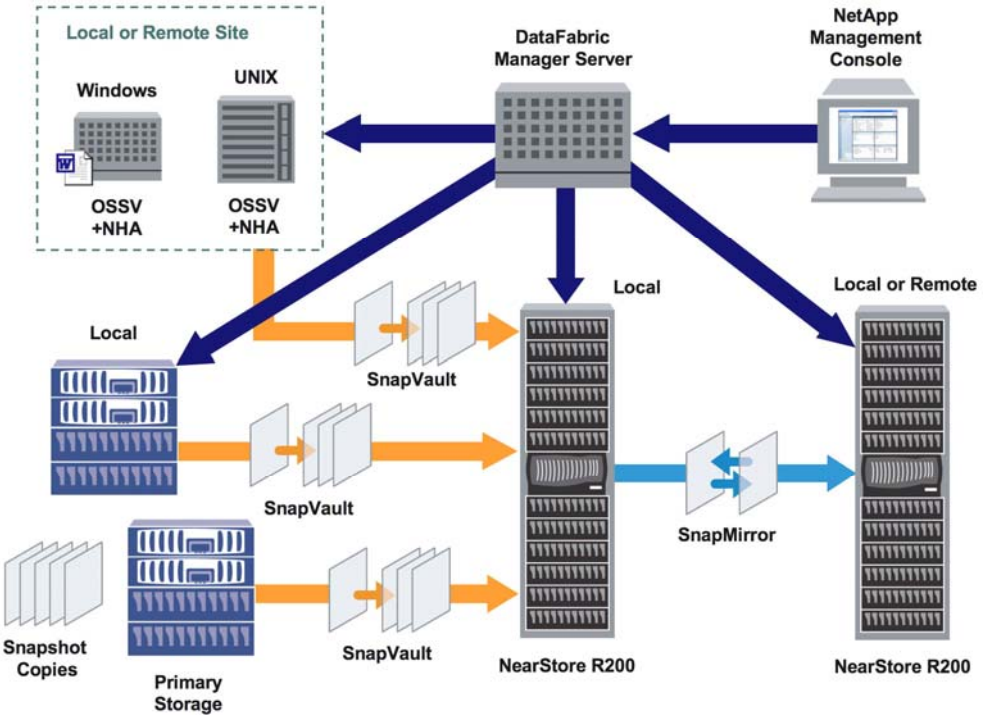


Figure 1) NetApp protection manager Three-Tier Architecture.

NetApp protection manager provides Policy-based management of SnapMirror®, SnapVault®, Open Systems SnapVault®, and Snapshot™ technologies. It also extends DataFabric Manager Server components with a new CLI and reports. It replaces the DataFabric Manager Client with NetApp Management Console which includes Performance Advisor.

6 RESTRICTIONS AND LIMITATIONS

6.1 STORAGE SYSTEMS

- Automatic provisioning via resource pools requires Data ONTAP 7.0 or later for flexible volumes and Data ONTAP 6.5 or later for traditional volumes.
- Mirroring prefers that source and destination run the same Data ONTAP version, but allows the destination to be a higher version. For best results, insure that your primary and secondary storage systems are running the same version of ONTAP.
- Backup and mirroring require Data ONTAP 6.5.6 or later.
- NetApp protection manager adds no new Data ONTAP licensing requirements: the storage systems still needs the appropriate SnapVault® and SnapMirror® licenses to enable vaulting or mirroring, respectively.
- NetApp protection manager treats Qtree SnapMirror® and SnapVault® as “backup” and treats Volume SnapMirror® as “mirror.”
- Open Systems must run Open System SnapVault® 2.2 or 2.3; Open System SnapVault® 2.3 supports additional management features (OPEN SYSTEM SNAPVAULT® Client Start and Stop) when the NetApp Host Agent is also installed.

6.2 DATAFABRIC MANAGER

- Because NetApp protection manager stores and executes schedules, we recommend configuring your DATAFABRIC MANAGER server for high availability.
    - Refer to the DataFabric Manager 3.5 NetApp operations manager Administration Guide and the DataFabric Manager 3.5 Installation and Upgrade Guide at http://now.netapp.com/NOW/knowledge/docs/DFM_win/rel35/ for details on configuring DataFabric Manager failover
- Because of additional load on DFM server, we recommend deploying a larger server hardware platform than you otherwise would.
    - Reference: DataFabric Manager Sizing Guide at www.netapp.com/library/tr/3440.pdf

7 BEST PRACTICE 3.5

BEST PRACTICE: DIAGNOSTICS

The support bundle is helpful for diagnosing whether the GUI client is behaving properly. To diagnose why backups aren't working, or why relationship creation isn't working, there are logs on the server that are more useful. From NetApp Management Console please collect the following information and send it back to NetApp when opening a support case.

- Help > About: contains platform and version information for client and server.
- Help > Create Support Bundle: packages relevant configuration data and logs into a ZIP file for sending back to NetApp.

BEST PRACTICE: SNAPMIRROR® LICENSE

If your backup schedule is going to call for backups to be made more frequently than once an hour, then a SnapMirror® license would be needed on primary and secondary as NetApp protection manager would use Qtree SnapVault® over SnapMirror® for such a case.

BEST PRACTICE: RESOURCE POOL

Resource pool Full and Nearly Full Threshold are configurable options in NetApp operations manager. Configure Nearly Full Threshold at least 10% less than Full Threshold limit to give you sufficient time to provision more space or resource pool for that data set.

Control Center -> Tools -> Options -> Default Thresholds is the location where you can set the parameters.

BEST PRACTICE: OPEN SYSTEM SNAPVAULT® DATA SET

If the data set contains Open System SnapVault® resources, neither a policy with a local backup schedule on the primary node nor a mirror connection between the primary and secondary is allowed. Enable SnapVault® license on the secondary to create a backup relationship to protect the data.

BEST PRACTICE: DATA SET

Plan and Select the policy that needs to be applied to a particular data set, as once a data set is associated with particular policy, then that primary storage object cannot become a member of any other data set. This is not the case in version 3.6.

BEST PRACTICE: ACCESS

Ensure that options SnapMirror® access and options SnapVault® access are set to “all” on destination storage systems. You can setup these options within Protection Manager in version 3.6.

BEST PRACTICE: DATAFABRIC MANAGER 3.5

Before upgrading the server please ensure to take the backup of existing database. The dfm backup CLI commands allow you to create backup copies of the working database and then restore the database from a backup. These commands can also be used to set a daily or weekly schedule for creating backups.

Creating a backup of the database:

From the command line, enter the following: `dfm backup create <backup_file_name>`

BEST PRACTICE: SCHEDULE

When importing relationships, NetApp protection manager deletes SnapMirror® schedules, but leaves Snapshot™ and SnapVault® schedules in place on the storage system. If customer wants all schedules under a central management, they need to connect to the storage system and disable all storage system resident schedules.

BEST PRACTICE: BACKUP (PRIVATE) NETWORK

The following default behavior applies to Protection Manager and Backup Manager features of DataFabric Manager (DFM):

If you set the "ndmpd.preferred_interface" option on the primary storage system, DFM tries that interface first for SnapVault data transfer. But if the secondary storage system cannot connect to that interface's IP Address, DFM uses other available IP addresses (including the primary address of the storage system) for SnapVault data transfer.

If the "ndmpd.preferred_interface" option is not set on the primary storage system, DFM first tries the primary address of the storage system for SnapVault data transfer. If the secondary storage system cannot connect to the primary IP address, DFM uses other available IP addresses for SnapVault data transfer.
`E.g.: “option ndmpd.preferred_interface e0b”`

To prevent use of the non-preferred interfaces when the preferred interface is broken, upgrade DataFabric Manager Server to a version 3.6R1 with the fix to bug 245546. When using a version with the fix to this bug, the default behavior changes so that DFM does not use any interface other than the preferred one (if ndmpd.preferred_interface is set on the primary storage system).

For SnapMirror® relationships (Qtree SnapMirror for "backup" or Volume SnapMirror for "mirror" connections), you need to set the DataFabric Manager Options "hostPreferredAddr1", and possibly "hostPreferredAddr2", on each host. When it comes time to do a transfer, the transfer job will look at these settings and find or create a DataFabric Manager DR Manager connection policy which matches the IP addresses. The net effect should be to use those interfaces, not the primary IP address of the storage system.

For the baseline transfers, these settings need to be set before creating the relationships. But these settings can be changed for subsequent transfers anytime before each transfer starts.

BEST PRACTICE: RESTORE

Restore copies data from a “backup” to an active file system, either the original location or another location. If the user wants to restore an entire volume, including its Snapshot™ copies, the user must use VSM restore from outside of NetApp protection manager.

BEST PRACTICE: SPACE RESERVATION

NetApp protection manager creates FlexVol® volumes larger than primary storage requires and tracks reservations internally; aggrNearlyFullThreshold and aggrFullThresholds are disabled on aggregates assigned to resource pools unless explicitly set, on a per aggregate basis, by the user. By default, NetApp protection manager is fairly conservative when estimating how much space is required to protect a primary qtree. To request that NetApp protection manager “thin provision” storage, increase the aggrNearlyOvercommittedThreshold.

BEST PRACTICE: CONFORMANCE

When a target volume or aggregate (if target is a FlexVol volume from a resource pool) fills up, NetApp protection manager needs to choose a new destination and rebaseline. This is not done automatically. The data set is marked as nonconformant, and the user has to request that the data set “conform now.”

BEST PRACTICE: SNAPVAULT®® VS. QSM

Customers may have SnapMirror® licenses, but still want NetApp protection manager to create SnapVault® relationships instead of Qtree SnapMirror® licenses. To change the behavior, set pmQSMBackupPreferred to “No.” And ensure SnapVault® License is enabled on storage systems.

```
“dfm option set pmQSMBackupPreferred=no”
```

BEST PRACTICE: IMPORT RELATIONSHIPS

If the customer is trying to import SnapVault® relationships coming from an Open System SnapVault® system, they should chose the “Remote backups only” policy. We will only import SnapVault® relationships to match a backup connection of a policy.

BEST PRACTICE: STEPS TO IMPORT RELATIONSHIP

1. Welcome
   Click Next
2. Associate with Data Set
   Select “Create...”
   Click Next
3. Name and Description
   Fill it in and click Next
4. Data
   Do NOT select the items you want to import.
   Always just go to pane 5 without selecting anything here.
   If you select something here and try to import it later in the wizard, then you will get the error message.
5. Protect Policy
   Select policy and click Next
6. Import Relationships
   This is the only place to select the relationship you want to import.
   Select from the Available Relationships and click Import.
   Click Next.
7. Preview
   You should not get the “already in data set” error.

8 BEST PRACTISE 3.6

All of the best practices are applied from 3.5 versions onto 3.6, except the import relationship section is completely new.

BEST PRACTICE: SUPPORT MATRIX

Please refer to the support matrix before the installation

http://now.netapp.com/NOW/knowledge/docs/olio/guides/dfm_compatibility/DFM.shtml

BEST PRACTICE: FAQ

Refer to online FAQ for any questions

http://now.netapp.com/NOW/knowledge/docs/DFM_win/rel36r1/html/faq/index.shtml

BEST PRACTICE: DATABASE MIGRATION

You can migrate the DataFabric Manager data to a different location using the “dfm datastore setup <dfm-data-dir>” command, where dfm-data-dir is the target location for the DataFabric Manager data. Besides configuring the DataFabric Manager database, this command copies the database, performance data, and script plug-in files in the specified target directory.

Do not run any dfm command while migrating the DataFabric Manager data. If some commands are run, they can interfere with the migrate operation by locking the database tables and causing the operation to fail.

BEST PRACTICE: DATA SET

The primary storage object can become member of any other data set. Even though it was associated to one dataset and a policy was applied to it already.

BEST PRACTICE: HOST AGENT

Host agent is not required to run the OSSV backup from DFM server. The host agent is required to use certain features in Protection Manager, such as stopping and starting the OSSV client, but you can backup data from an OSSV client without host agent credentials.

BEST PRACTICE: ADD HOST/STORAGE SYSTEM

Add and configure new storage system or OSSV host using Protection Manager. “Setup -> Hosts -> “Storage System/OSSV” Tab -> Add

From this single interface now you can configure Login credentials, Ndmp credentials, Add License, etc.

If the system was already added using Operations Manager, you can configure the system with Protection manager or diagnose any failures like Ndmp credentials failed, etc.

BEST PRACTICE: VOLUME FAN TOPOLOGY

This could be a very important decision point in Protection manager planning. Protection Manager will bring in these relationships via import. However, if a new volume is added to the source node of the dataset, Protection Manager will try to auto provision a new volume on the secondary. This will fail if no resource pool is associated with the secondary. Additionally, it will alter the existing topology the customer has in place.

BEST PRACTICE: IMPORT

It should be noted that existing backup versions would not be imported
The net effect is that the restore cannot be used in Protection manager for backup versions not created by Protection manager itself. Additionally, retention policies will not be applied to these backup versions (they will not be aged off).

It should be noted that existing create / transfer schedules are left untouched
After the import process is complete and verified, the existing schedules need to be disabled to prevent

duplication. Some cleanup may be necessary as well if duplicate backups have been created for some period of time.

BEST PRACTICE: AGGR SPACE

All secondary volumes would be thin provisioned (volume guarantee set to none) to aggr sizes. So, as snapvault transfers use up space, this will be charged on the aggr. (i.e. aggr used space goes up.)

In DFM, we have a concept called "overcommit" thresholds on aggregates. This indicates how much an aggregate can be thin provisioned. Nearly overcommitted threshold values are by default 95%. But, it should be set normally to more than 100% to actually overcommit an aggregate.

Over commit threshold is a way to tell Protection Manager to stop provisioning from an aggregate saying that already provisioned volumes would require remaining free space in the aggr to store backup data. So, new provisioning requests will not be honored from this aggr after overcommit threshold is breached.

Protection manager works in the following way.

1. To back up a source qtree, PM will calculate required size (projected size) for backup secondary volume.
   Formula:
   secondary Volume projected size = (max(cur_size, (max_size*SP_B_MUL)/100) * SP_A_MUL)/100;
   Where cur_size is current source volume size (used space)
   max_size is maximum source volume size.
   SP_B_MUL is default SV max size coefficient. Default value is 80
   SP_A_MUL is default SV size expansion coefficient. Default value is 150
2. It will internally store this projected size to calculate aggregate overcommit percentage.
3. But, PM will thin provision backup secondary volume to aggr size (i.e. guarantee none).
   Even though the volume size is aggr size, this will not be used for overcommit calculations.
4. Now creates a SV relationship between source qtree and destination volume.

For example,
Source volume used space is 1 TB. Max size is 2 TB. Secondary volume projected size would be (max(1, (2 * 80)/100)100) * 150)/100 = 2.4 TB. So, we look for an aggr, which has 2.4 TB free space based on overcommits thresholds.
Suppose if we find 12 TB aggr, we create secondary volume as 12 TB with guarantee none and 2.4 TB (projected size) is stored in DFM for overcommit calculations.

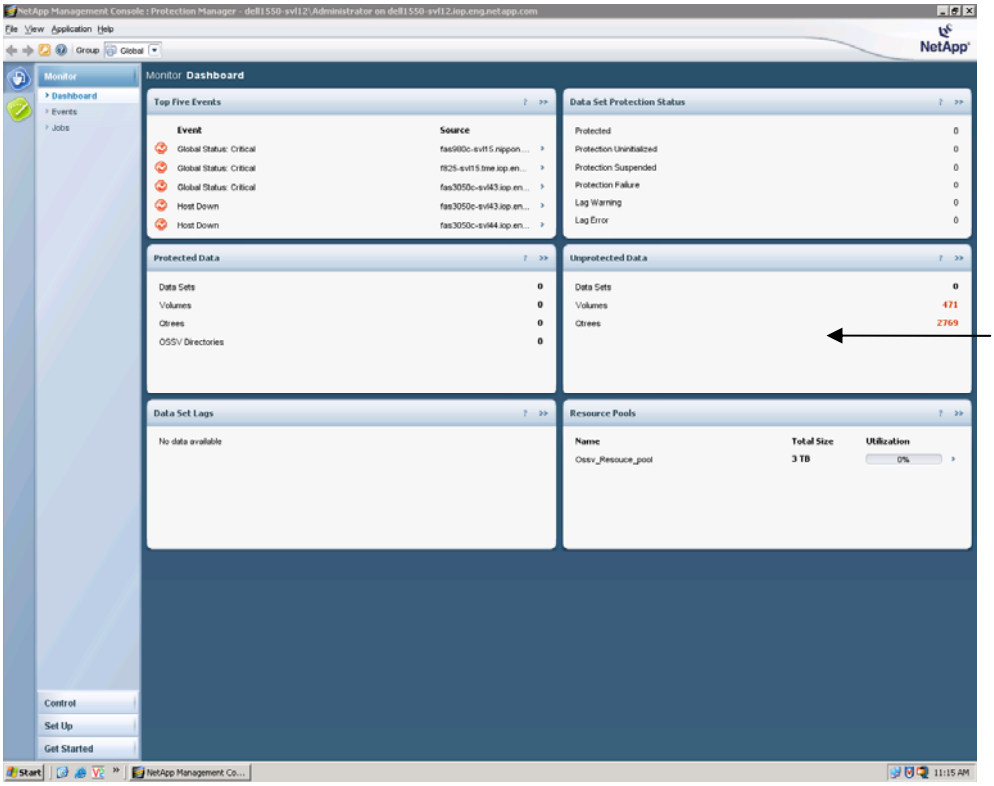
If a new volume to be created for another source volume (used space is 1 TB. Max size is 2 TB), we look at the aggr and calculate overcommit percentage from projected size. That is 2.4 TB / 12 TB = 20% which is less than default overcommit threshold (95%). So we allow provisioning from the aggr.
But after 5 provisioning requests for the same sized secondary volumes, the overcommit percentage becomes 2.4 * 5 = 12 TB. / 12 TB = 100%. So, we cannot provision from this aggr as its crossed overcommit threshold (95%)

9 EXAMPLES

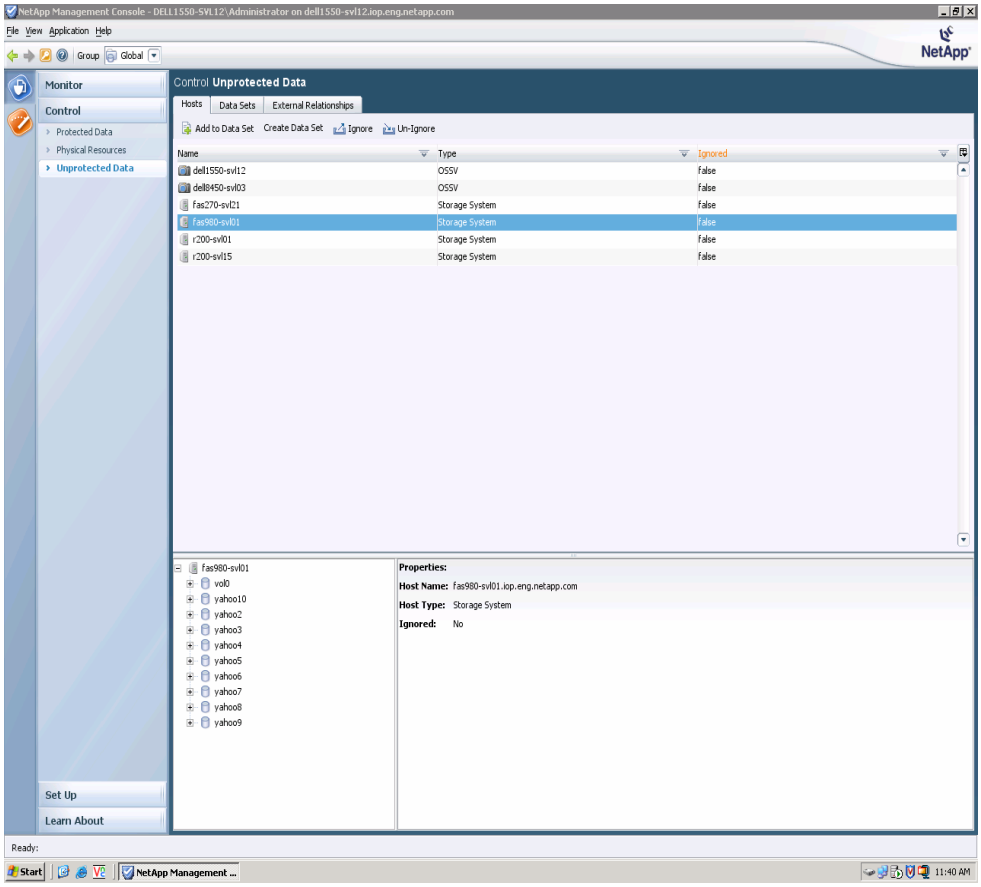
9.1 EXAMPLE 1: A BACKUP ADMIN WANTS TO FIND ALL SYSTEMS WITH QTREE AND OPEN SYSTEM SNAPVAULT® CLIENTS THAT ARE NOT CURRENTLY BACKED UP

- This means all appliances and Open System SnapVault® clients that have been discovered by DFM.
- In NetApp protection manager, in the unprotected data all the systems with qtrees and Open System SnapVault® clients that haven't been backed up will be displayed.

NETAPP PROTECTION MANAGER DASHBOARD

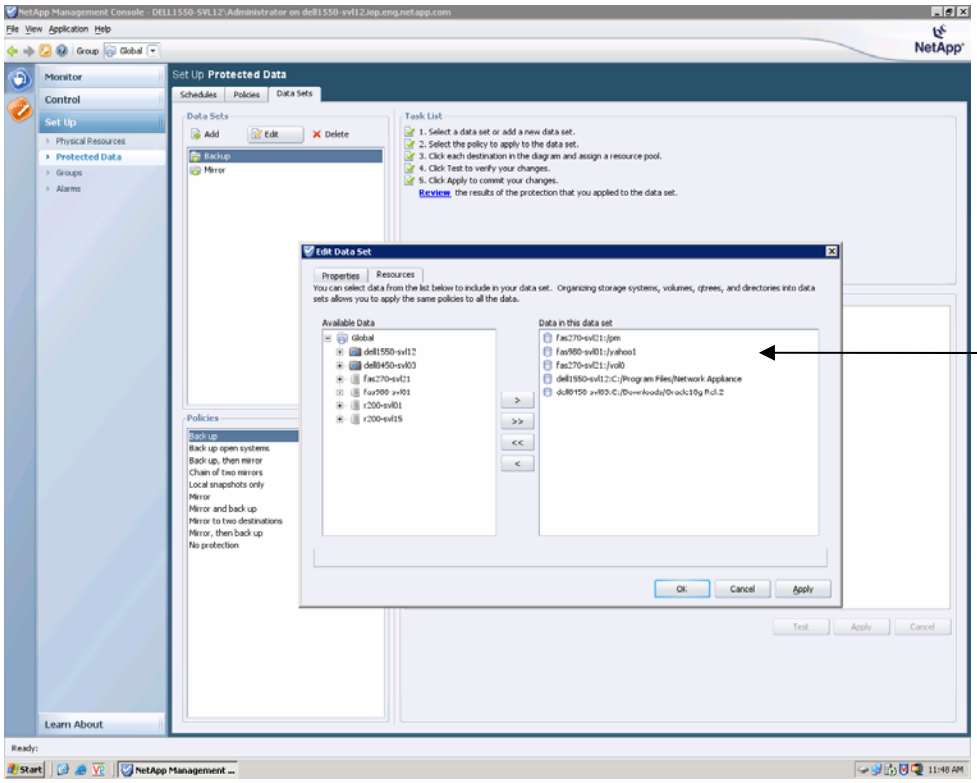


UNPROTECTED DATA (LISTING OPEN SYSTEM SNAPVAULT® CLIENTS AND VOLUMES)



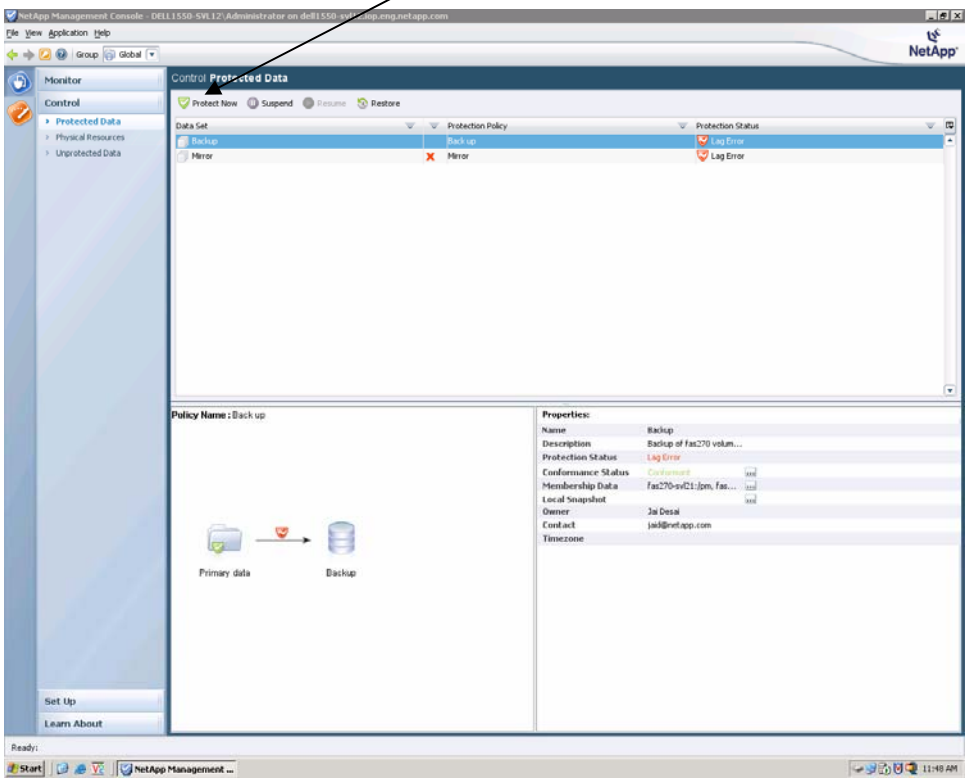
9.2 EXAMPLE 2: A BACKUP ADMIN WANTS TO CREATE POLICIES FOR BACKING UP SYSTEMS WITH QTREES AND OPEN SYSTEM SNAPVAULT® CLIENTS

- The servers can be Windows or UNIX.
- To select a secondary to use if there is a choice available; otherwise admin uses the only secondary available. This can be done while configuring the resource pool which needs to be created by admin.
- Add the Open System SnapVault® clients and qtrees in the data set.
- Select a policy, Set the schedule on the policy before you assign the policy to data set.
- To create and define a threshold for each of the backup relationships. That means for qtrees and Open System SnapVault® clients it can have two separate policies.
- Apply that policy to data sets and then wait for schedule to kick in or to kick off a backup immediately by clicking Protect Now icon.



OSSV Clients and Volumes Selected for Backup

Protect Now Button



10 USE CASES

10.1 CASE 1

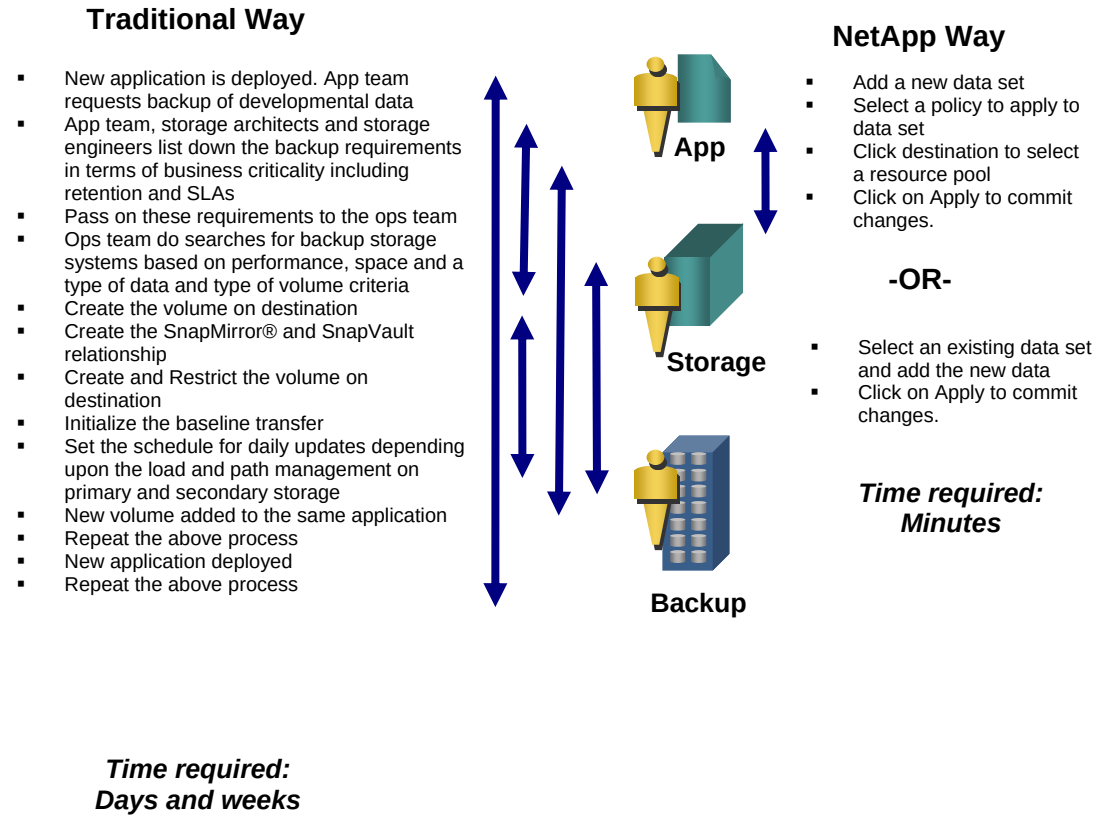


Figure 2) Steps to Protect New Data (Traditional vs. NetApp protection manager).

Assume there is new user data that needs protection (Figure 2). We show that traditional application team and storage architect would sit and list all the requirements and SLAs. Provide that information to the Operations team, who would find storage system based on certain criteria, provision the volume, create the relationship and then initialize the same. So it would be a lengthy process for each new data to be protected.

The NetApp (NetApp protection manager) way is to create a data set which would contain the data to be protected. Select a policy (Mirror, Backup or Mirror and backup policy for example) which is the rule on how you want to protect your data. Then you select a resource pool for each node. NetApp protection manager will go ahead and provision secondary storage space from the resource pool, create the right relationship for you and keep monitoring the policy to ensure that it meets the SLA that is defined; else it will trigger an event.

10.2 CASE 2

```
Source                                          Destination                                          State        Lag       Status
jamura:/vol/ora_archives_prod/em10_db_test  svlprodflr01:/vol/utility_ora_archives/em10_db_test   Broken-off
3695:30:53  Idle
svlprodflr01:e5b_p5accrlt_prod_arch01      svlbkupflr09:svlprodflr01_e5b_p5accrlt_prod_arch01    Source
06:55:49   Idle
svlprodflr01:e5b_p5accrlt_prod_oradata01   svlbkupflr09:svlprodflr01_e5b_p5accrlt_prod_oradata01  Source
06:55:49   Idle
svlprodflr01:e5b_p5infatc_prod_arch01      svlbkupflr09:svlprodflr01_e5b_p5infatc_prod_arch01    Source
06:55:49   Idle
svlprodflr01:e5b_p5tcmart_prod_arch01      svlbkupflr09:svlprodflr01_e5b_p5tcmart_prod_arch01    Source
06:55:49   Idle
svlprodflr01:e5b_p5tcmart_prod_oradata01   svlbkupflr09:svlprodflr01_e5b_p5tcmart_prod_oradata01
Source       07:55:49   Idle
svlprodflr01:e5b_p5trucmp_prod_arch01      svlbkupflr09:svlprodflr01_e5b_p5trucmp_prod_arch01    Source
07:55:49   Idle
svlprodflr01:e5b_paccrual_prod_arch02      svlbkupflr09:svlprodflr01_e5b_paccrual_prod_arch02    Source
06:55:49   Idle
svlprodflr01:e5b_paccrual_prod_oradata01   svlbkupflr09:svlprodflr01_e5b_paccrual_prod_oradata01  Source
06:55:49   Idle
svlprodflr01:e5b_pinfatc_prod_arch01       svlbkupflr09:svlprodflr01_e5b_pinfatc_prod_arch01     Source
17:25:50   Idle
svlprodflr01:e5b_ptcpmart_prod_arch02      svlbkupflr09:svlprodflr01_e5b_ptcpmart_prod_arch02    Source
17:25:50   Idle
svlprodflr01:e5b_ptcpmart_prod_oradata01   svlbkupflr09:svlprodflr01_e5b_ptcpmart_prod_oradata01  Source
17:25:50   Idle
svlprodflr01:e5b_ptrucmp_prod_arch01       svlbkupflr09:svlprodflr01_e5b_ptrucmp_prod_arch01     Source
17:25:50   Idle
svlprodflr01:e5c_arkivio_01            svlbkupflr09:svlprodflr01_e5c_arkivio_01          Source       21:25:51   Idle
svlprodflr01:e5c_fin_grp               svlbkupflr09:svlprodflr01_e5c_fin_grp             Source       03:55:49   Idle
svlprodflr01:e5c_journyx               svlbkupflr09:svlprodflr01_e5c_journyx             Source       21:25:51   Idle
svlprodflr01:e5c_kvssql_db             svlbkupflr09:svlprodflr01_e5c_kvssql_db           Source       13:55:50   Idle
svlprodflr01:e5c_prod_sabrix           svlbkupflr09:svlprodflr01_e5c_prod_sabrix         Source       17:55:50   Idle
svlprodflr01:e5d_SVLTS01               svlbkupflr09:svlprodflr01_e5d_SVLTS01             Source       20:55:49   Idle
svlprodflr01:e5d_citrixprod_xp2        svlbkupflr09:svlprodflr01_e5d_citrixprod_xp2      Source       21:55:47   Idle
svlprodflr01:e5d_citrixprod_xp3        svlbkupflr09:svlprodflr01_e5d_citrixprod_xp3      Source       21:55:47   Idle
svlprodflr01:e5d_citrixprod_xp4        svlbkupflr09:svlprodflr01_e5d_citrixprod_xp4      Source       21:55:48   Idle
svlprodflr01:e9a_dicarta_prod_admin    svlbkupflr09:svlprodflr01_e9a_dicarta_prod_admin  Source
17:25:49   Idle
svlprodflr01:e9a_dicarta_prod_arch02   svlbkupflr09:svlprodflr01_e9a_dicarta_prod_arch02  Source
17:25:49   Idle
svlprodflr01:e9a_dicarta_prod_oradata01  svlbkupflr09:svlprodflr01_e9a_dicarta_prod_oradata01  Source
17:25:50   Idle
svlprodflr01:e9a_dicarta_prod_redo_2   svlbkupflr09:svlprodflr01_e9a_dicarta_prod_redo_2   Source
17:55:50   Idle
svlprodflr01:mspatch                svlbkupflr09:svlprodflr01_mspatch                Source       18:55:50   Idle
svlprodflr01:prod_dba_tools            svlbkupflr09:svlprodflr01_prod_dba_tools          Source       334:55:39  Idle
svlprodflr01:prod_netapp_bin           svlbkupflr09:svlprodflr01_prod_netapp_bin         Source       334:52:04  Idle
```

Figure 3) Manual Data Protection Process.

Data Protection processes are complex. What kind of complexity are we talking about?

Here is a typical screen of an administrator who is involved with the Data protection task. It is cryptic, difficult to understand and the potential for creating errors that affects protection of the most important asset of your organization “The Data” is much higher. Data availability is affected because of the errors that are caused due to the complexity that administrators have to deal with.

The storage administrator goes line by line to understand the data protection status of a particular volume.

The red circle highlights that the administrator accidentally came to know that the particular data is not protected for the last 334 hours while he was checking something else.

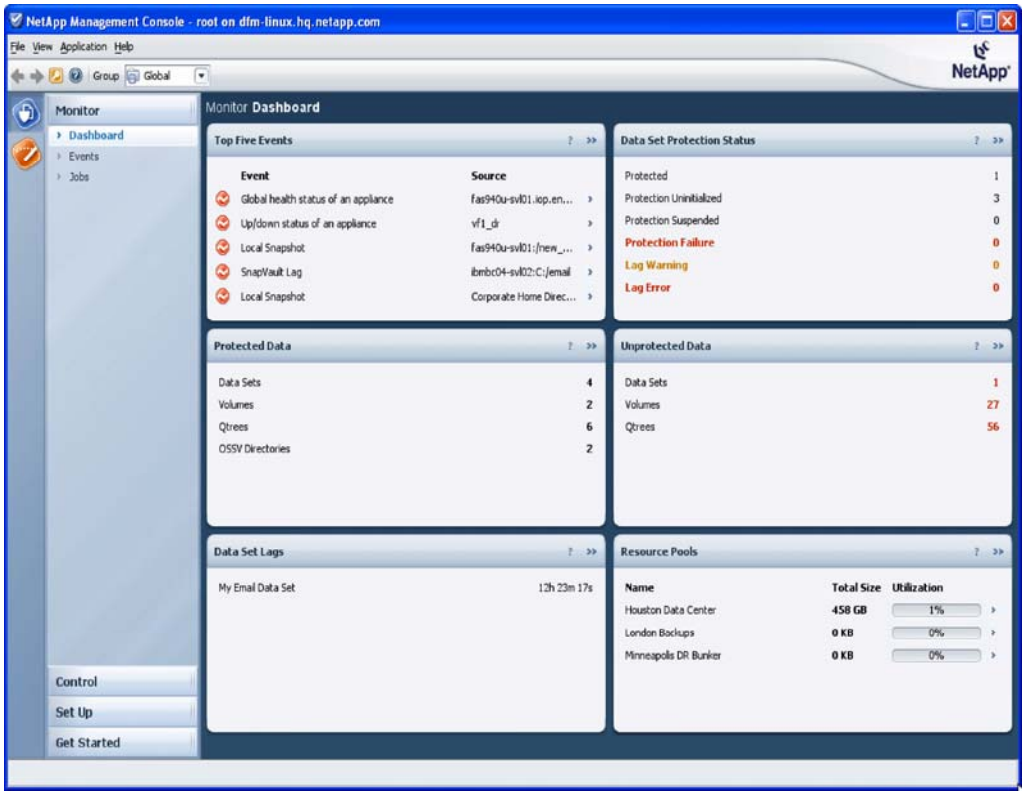
This is a highly ineffective and not a scalable way of assuring data protection.

Thus, one can safely conclude that the current data protection processes are tedious and difficult to scale. Data protection involves complex scripts and manual error-prone steps.

NetApp protection manager benefits administrators in this case because, in the figure below, you can see it provides a holistic view of the environment. It has a simplified console which improves productivity. In one single dashboard view, it provides the status of:

1. Protected data
2. Unprotected data
3. Top alerts
4. Data at risk

NETAPP PROTECTION MANAGER DASHBOARD



10.3 CASE 3

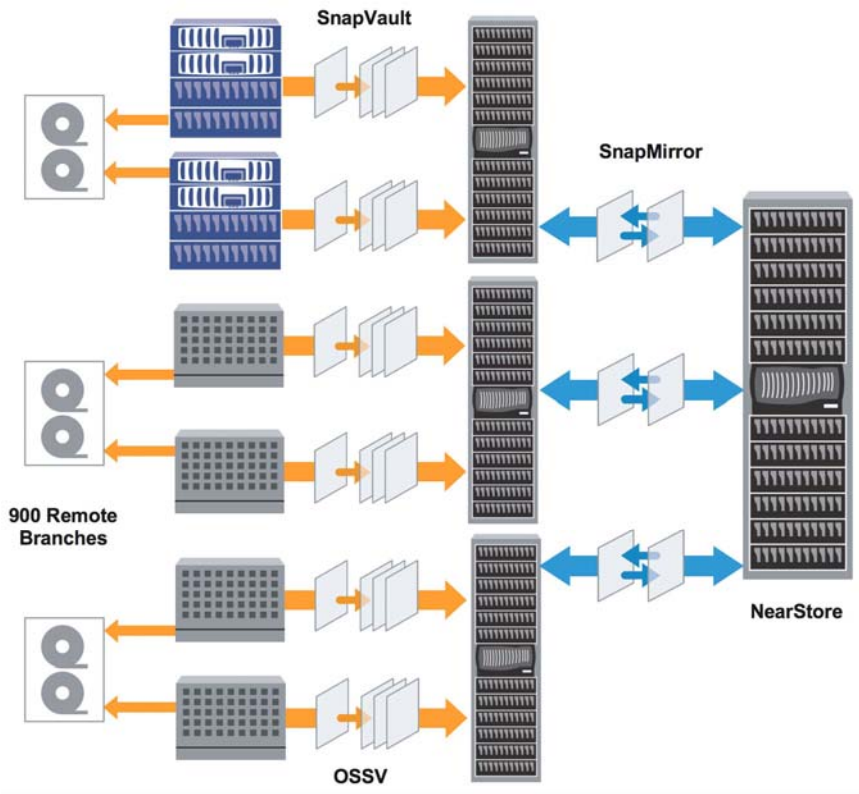


Figure 4) A Complex open system SnapVault® Environnent.

As environments get complex, managing large Open System SnapVault® environments and SnapMirror®® and SnapVault® relations become difficult and open to human error. In this case, NetApp protection manager shows how it can simplify data protection for such environments can be.

Let us assume 1000 Open System SnapVault® clients, three paths per client. To protect it you create one data set with all 1000 clients. Assign a data protection policy to the data set. NetApp protection manager builds all 3000 SnapVault® relationships. If new paths appear on the clients, NetApp protection manager automatically creates new SnapVault® relationships.

You can select a policy such that it can have a mirrored copy for additional protection.

Data sets and containment let NetApp protection manager iterate over large groups of storage containers. Resource pools let it provision (and re-provision) secondary storage. If a user changes something on the storage system; NetApp protection manager notifies the administrator it's out of compliance with the policy.

You can edit a policy and the NetApp protection manager will tell you which relationships are out of compliance or out of conformance. The NetApp protection manager will inform the user on the steps necessary to bring the data set back into conformance, if it unable to perform those steps automatically.

How NetApp protection manager provides leveraging and scaling:

1. If the backup/mirroring administrator wants to change something
2. The admin edits a policy
3. NetApp protection manager automatically updates all relationships affected by the policy

If the admin wants to see the status of all 1000 clients:

1. The admin checks the Dashboard View, which rolls up status information
2. NetApp protection manager presents data protection history of all clients

11 SUMMARY

NetApp protection manager is backup and replication management software for a NetApp disk-based data protection environment. NetApp protection manager delivers assured data protection and higher productivity by providing policy-based management, including automated data protection configuration.

With an automated policy in place, administrators can move and manage data in a logical rather than a physical way and are provided with a long-term solution to the growing problem of storage device backup and migration.

12 APPENDIX: ADDITIONAL REFERENCES

Sizing Guide

http://www.netapp.com/library/tr/3440.pdf

For more information, visit http://www.netapp.com/products/enterprise-software/manageability-software/data-suite/pm.html