Technical Report

ApplianceWatch PRO 2.1.1 Best Practices Guide

Author: Allan Watanabe, NetApp
January 2011 | TR-3893

Status: FINAL

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

ApplianceWatch™ PRO 2.1.1 is an enterprise-class storage monitoring application that simplifies storage management and increases tools available to SCOM administrators for NetApp® storage controllers.

Following are the key features of ApplianceWatch PRO 2.1.1:

- Easy storage management for Windows® and NetApp storage administrators
- Monitor all elements of IT infrastructure (single pane of glass from MMC)
- Simplify distributed NetApp storage system monitoring
- Isolate problems quickly using alerts
- Troubleshoot performance issues using performance views
- Minimize downtime, shorten time to resolution, and provide autorecovery tools in a virtualized environment
- Rapidly provision and clone VMs using the cmdlets

1.1 COMMON TERMINOLOGY

Table 1 is a list of acronyms commonly used throughout the documentation.

Table 1) Acronym definition.

Acronym	Definition
SC	Microsoft® System Center solutions are a set of management products that help IT pros manage the physical and virtual IT environments.
SCOM	A member of the SC family, System Center Operations Manager is the end-to-end service management product that works with Microsoft software and applications, helping organizations increase efficiency while enabling greater control of the IT environment.
SCOM console/server	SCOM console refers to the software install of SCOM, which allows the user to launch the console GUI to view managed objects and perform administrative SCOM tasks. SCOM Server refers to the computer that has SCOM console installed.
SCOM agent	SCOM agent refers to the software install of SCOM where the SCOM SDKs and connectors and installed on a system that does not have the SCOM Console installed. There is no UI: this install is intended for systems that need to communicate monitoring and other information to the SCOM Server. This agent can be installed remotely on systems using SCOM console on the SCOM Server.
SCVMM	A member of the SC family, System Center Virtual Machine Manager is for IT professionals responsible for managing virtual infrastructures, provides solution for unified management of physical and virtual machines, performance and resource optimization (PRO) for dynamic and responsive management of virtual infrastructure, consolidation of underutilized physical servers, and rapid provisioning of new virtual machines by leveraging the expertise and investments in Microsoft Windows Server technology.

Acronym	Definition
PRO	Performance and resource optimization (PRO), a feature of System Center Virtual Machine Manager (SCVMM), ties specific alerts from System Center Operations Manager (SCOM) 2007 to remediation actions in SCVMM. Management packs that allow use of this SCVMM PRO feature are referred to as PRO management packs. We will be providing one such management pack called "Data ONTAP PRO MP."
MP	Management pack: It defines the author's definition of a healthy state for application, services, or hardware that SCOM is monitoring.
Controller	A NetApp storage element that serves data.
MCTB	MetroCluster™ Tiebreaker is an algorithm used to prevent split-brain scenarios in MetroCluster installations.

1.2 TARGET AUDIENCE

This guide is intended for NetApp storage and Windows server administrators managing NetApp storage systems using the SCOM solution. The information contained in this best practices document is intended for ApplianceWatch PRO 2.1.1. ApplianceWatch PRO 2.1.1 for SCOM is designed to be installed on the SCOM 2007 server to give Windows IT administrators a central interface to monitor NetApp storage systems. ApplianceWatch PRO discovers hardware and storage layouts of your NetApp storage systems and provides alerts, health views, and various performance views. Customers can also dynamically manage their virtualized environment with the addition of performance and resource optimization (PRO). PRO is a feature of System Center Virtual Machine Manager 2008 that enables dynamic management of virtualized infrastructure. PRO provides an open and extensible framework for the creation of management packs for virtualized applications or associated hardware.

A good understanding of Windows SCOM administration is necessary, as well as an understanding of NetApp storage concepts. The recommendations found in this document are guidelines to assist with configuration of ApplianceWatch PRO 2.1.1. NetApp recommends that users refer to the following guides before using this guide:

- *ApplianceWatch PRO 2.1.1 Installation and Administration Guide*
- *ApplianceWatch PRO 2.1.1 Release Notes*
- *Rapid Provisioning and Cloning Command Reference Guide*

2 INSTALLATION AND BASIC CONFIGURATION

2.1 SYSTEM REQUIREMENTS

The following table outlines the installation requirements to successfully run ApplianceWatch PRO 2.1.1.

Table 2) Installation requirements.

Requirements	Requirements for Installing ApplianceWatch PRO 2.1.1
Hardware requirements	Microsoft System Center Operations Manager 2007 R2 (SCOM) determines the hardware requirements. For more information on Operations Manager 2007 R2, visit *www.microsoft.com/systemcenter/en/us/default.aspx*.
Software requirements	Microsoft System Center Operations Manager 2007 R2 (SCOM) and Virtual Machine Manager 2008 R2 (SCVMM) determine the software requirements. Microsoft .NET Framework 3.5 is also required. For more information, see the Microsoft TechNet site.
ApplianceWatch PRO requirements	To correctly install ApplianceWatch PRO 2.1.1, you must first uninstall any earlier versions of ApplianceWatch.
System Center Operations Manager configuration	You must configure Microsoft System Center Operations Manager 2007 R2 (SCOM) for reporting so that the Reporting management pack appears with the other management packs. To do this, you need to correctly configure the SQL Server® data warehouse. For more information, see the Microsoft TechNet site.
Data ONTAP® requirements	ApplianceWatch PRO supports the following versions of Data ONTAP: • 7.2.6 or later in the Data ONTAP 7.2 product family • 7.3 or later in the Data ONTAP 7.3 product family • Data ONTAP 8.0 7-Mode in the Data ONTAP 8.0 product family
Microsoft licenses	ApplianceWatch PRO requires the following Microsoft licenses: • Windows Server 2003, 2008 (32-bit or 64-bit), or 2008 R2 • Microsoft System Center Operations Manager 2007 R2 (SCOM) • Microsoft System Center Virtual Machine Manager 2008 R2 (SCVMM) - Required for ApplianceWatch PRO tips and rapid provisioning and cloning.

2.2 BEST PRACTICES FOR MICROSOFT SYSTEM CENTER PREINSTALLATION

The following software applications are required prior to installing ApplianceWatch PRO 2.1.1:

- Microsoft System Center Operations Manager (SCOM) – required for basic ApplianceWatch PRO monitoring.
- Microsoft System Center Virtual Machine Manager (SCVMM) – required for PRO based alerts, automation, and rapid provisioning and cloning cmdlets.

SCOM and SCVMM must be properly integrated for virtual machine-based alerts and functionality. Always refer to the Microsoft documentation and best practices for install and setup of the applications listed.

For more information visit Microsoft, *www.microsoft.com/systemcenter/en/us/default.aspx*.

2.3 BEST PRACTICES FOR APPLIANCEWATCH PRO PREINSTALLATION

After Microsoft SCOM and/or SCVMM has been installed and properly configured, the administrator can continue with the ApplianceWatch PRO installation. SCOM and SCVMM must be properly integrated for virtual machine based alerts and functionality. Hyper-V™ host must also be added to both SCOM and SCVMM server in order for PRO functionality. The following procedures can help administrators distinguish if SCVMM has been properly integrated with SCOM.

To confirm SCVMM is configured with SCOM:

1. From SCVMM console:
    a. Go to Administration.
    b. Select “System Center.”
    c. Right-click Operations Manager Server and confirm SCOM server name.
2. Confirm Hyper-V nodes are added to SCVMM:
    a. Go to Administration tab.
    b. Select “Managed Computers.”
    c. Confirm Hyper-V hosts are listed.
    d. Use the “Add Host” action to provide Hyper-V host and credential information.
3. From SCOM console:
    a. Go to Monitoring tab.
    b. Select “Virtual Machine Manager 2008 Views.”
    c. Select Diagram View and make sure Hyper-V VMs are visible.

Always refer to the Microsoft System Center documentation to make sure of proper installation and configuration. Visit *www.microsoft.com/systemcenter/en/us/default.aspx* for more details.

Always refer to the NetApp Installation and Administration Guide and the Release Notes for ApplianceWatch PRO to make sure of proper installation and configuration.

- *ApplianceWatch PRO 2.1.1 Installation and Administration Guide*
- *ApplianceWatch PRO 2.1.1 Release Notes*
- *Rapid Provisioning and Cloning Command Reference Guide*

For more information, visit
http://now.netapp.com/NOW/knowledge/docs/AppWatch/2.1.1/relaw21/html/index.shtml.

2.4 BEST PRACTICES FOR NETAPP STORAGE MINIMAL ACCESS CONTROL

In some IT environments, a detailed assignment of the minimal permissions is required. Table 3 describes the capabilities that are needed to connect to the storage system from ApplianceWatch PRO and gather monitoring data by using a local account on the storage system. This set of capabilities is purely for monitoring of the ApplianceWatch PRO basic functions and does not include any of the advanced features. This local Data ONTAP account will need to be assigned a customized role and contain the following capabilities.

Note: These are the minimum requirements for basic monitoring only and do not contain any active management, cmdlets, or SCVMM PRO functionality.

Table 3) Minimum capabilities for NetApp storage users for monitoring with ApplianceWatch PRO.

NetApp Storage Capabilities
login-http-admin
api-system-get-version
api-system-get-info
api-system-get-vendor-info
api-cf-status
api-system-get-ontapi-version
api-vfiler-list-info
api-ems-autosupport-log
api-aggr-list-info
api-volume-list-info
api-lun-list-info
api-disk-list-info
api-storage-shelf-list-info
api-license-list-info
api-lun-map-list-info
api-volume-autosize-get
api-aggr-options-list-info
api-qtree-list,api-storage-shelf-environment-list-info
api-lun-get-space-reservation-info
api-volume-options-list-info
api-perf-object-get-instances
api-snmp-get
api-snapmirror-get-status
api-quota-report-iter-start
api-quota-report-iter-next

Ex. Sample command to add/modify a custom role.

useradmin role modify scom-user-roles -a login-http-admin,api-system-get-version,api-system-get-info,api-system-get-vendor-info,api-cf-status,api-system-get-ontapi-version,api-vfiler-list-info,api-ems-autosupport-log,api-aggr-list-info,api-volume-list-info,api-lun-list-info,api-disk-list-info,api-storage-shelf-list-info,api-license-list-info,api-lun-map-list-info,api-volume-autosize-get,api-aggr-options-list-info,api-qtree-list,api-storage-shelf-environment-list-info,api-lun-get-space-reservation-info,api-volume-options-list-info,api-perf-object-get-instances,api-snmp-get,api-snapmirror-get-status, api-quota-report-iter-start, api-quota-report-iter-next

2.5 BEST PRACTICES FOR APPLIANCEWATCH PRO INSTALLATION

Administrators have the option of installing the entire ApplianceWatch PRO package or to select specific components with the custom install option. The following list describes the available installation packages when the custom install option is selected.

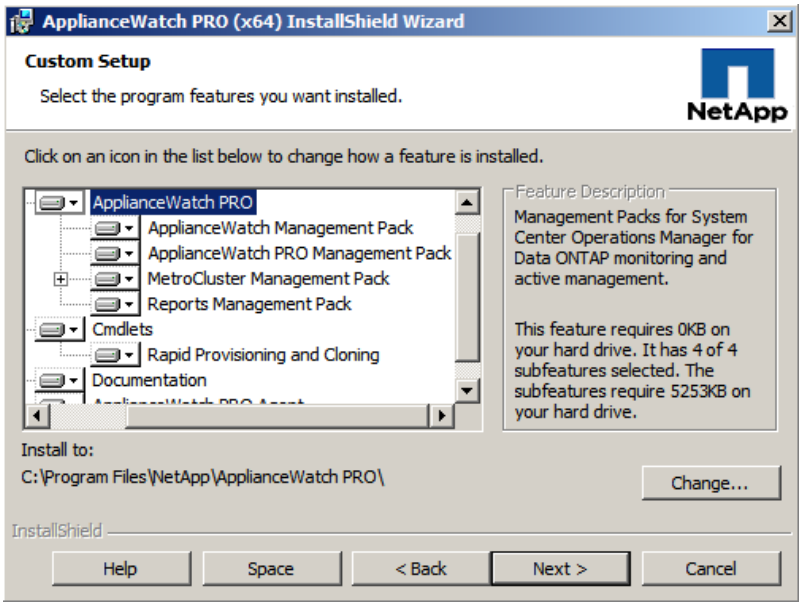

Figure 1) ApplianceWatch PRO custom installation option.

Table 4) ApplianceWatch PRO management pack installation.

Management Pack	Description
ApplianceWatch management pack	ApplianceWatch MP enables basic features such as alerts, monitoring, and views. (This MP must be installed for basic ApplianceWatch functionality.)
ApplianceWatch PRO management pack	ApplianceWatch PRO MP enables PRO generated tips for SCVMM which provide autorecovery tools in virtualized environments.
MetroCluster management pack	MetroCluster MP installs the ApplianceWatch MetroCluster Tiebreaker tool for MetroCluster environments.
Reports management pack	Reports MP enables the ability to generate historic reports on NetApp storage controllers monitored by ApplianceWatch PRO. (SCOM Reporting component must be installed prior to ApplianceWatch PRO install. Please refer to the Microsoft documentation for installation procedures and best practices.) For more information visit Microsoft, *www.microsoft.com/systemcenter/en/us/default.aspx*.
Cmdlets: rapid provisioning and cloning	Cmdlets enable rapid provisioning and cloning of Hyper-V VM guest machines. Cmdlets also provide functionality to create or connect NetApp LUNs on Hyper-V parents. SCVMM is required for cmdlets and rapid provisioning and cloning. For more information visit Microsoft, *www.microsoft.com/systemcenter/en/us/default.aspx*.
ApplianceWatch PRO Agent	ApplianceWatch PRO 2.1.1 Agent must be installed on Hyper-V host(s) for ApplianceWatch PRO to discover and monitor virtual machines.

2.6 BEST PRACTICES FOR MANAGEMENT PACK DEPENDENCIES

The following lists the management pack dependencies for ApplianceWatch PRO MPs to function appropriately. Most of the Microsoft Management packs can be found within the SCOM installation and others might need to be downloaded. Please check the Microsoft Management Pack Catalog for missing MPs. *http://pinpoint.microsoft.com/en-US/systemcenter/managementpackcatalog*

Table 5) ApplianceWatch PRO management pack dependencies.

ApplianceWatch PRO Management Packs	Microsoft System Center Operations Manager Management Pack Requirements
ApplianceWatch management pack	• Microsoft.SystemCenter.DataWarehouse.Library • Microsoft.SystemCenter.Library • Microsoft.SystemCenter.InstanceGroup.Library • Microsoft.SystemCenter.NetworkDevice.Library • Microsoft.Windows.Library • System.Health.Library • System.Library • System.Performance.Library • System.Snmp.Library
ApplianceWatch PRO management pack	• Data ONTAP ApplianceWatch management pack • Microsoft.SystemCenter.DataWarehouse.Library • Microsoft.SystemCenter.VirtualMachineManager.2008 • Microsoft.SystemCenter.VirtualMachineManager.Pro.2008.Library • Microsoft.SystemCenter.Library • Microsoft.Windows.Library • System.Health.Library • System.Library
MetroCluster management pack	• Data ONTAP ApplianceWatch management pack • Microsoft.SystemCenter.Library • Microsoft.SystemCenter.InstanceGroup.Library • Microsoft.Windows.Library • System.Health.Library • System.Library
Reports management pack	• Data ONTAP ApplianceWatch management pack • Microsoft.SystemCenter.DataWarehouse.Reports • Microsoft.SystemCenter.DataWarehouse.Report.Library • Microsoft.SystemCenter.DataWarehouse.ServiceLevel.Report.Library • Microsoft.SystemCenter.Library • Microsoft ODR Report Library • Microsoft.Windows.Library • System.Health.Library • System.Library • System.Performance.Library

2.7 BEST PRACTICES FOR APPLIANCEWATCH PRO OVERRIDES AND DEFAULTS

Administrators will be asked to enable specific rules such as the Discovery Rule to start the discovery process. The changes to these rules are called “Overrides” and the overrides will need to be saved in a management pack, which by default is the “Default management pack." Saving any overrides in the Default management pack will cause issues with upgrades and uninstallation of ApplianceWatch PRO. To mitigate any problems in the future, create a New management pack and save the ApplianceWatch PRO overrides to the newly created management pack prior to enabling any overrides for ApplianceWatch PRO.

Discovery interval is 24 hours by default, and in most cases this should not be changed as this might disrupt the SCOM environment if the Discovery interval is set too short, causing a shortage in resources such as CPU, memory, and network. NetApp does not recommend setting the interval any lower then 4 hours and as a best practice recommends that this be kept at the 24-hour default.

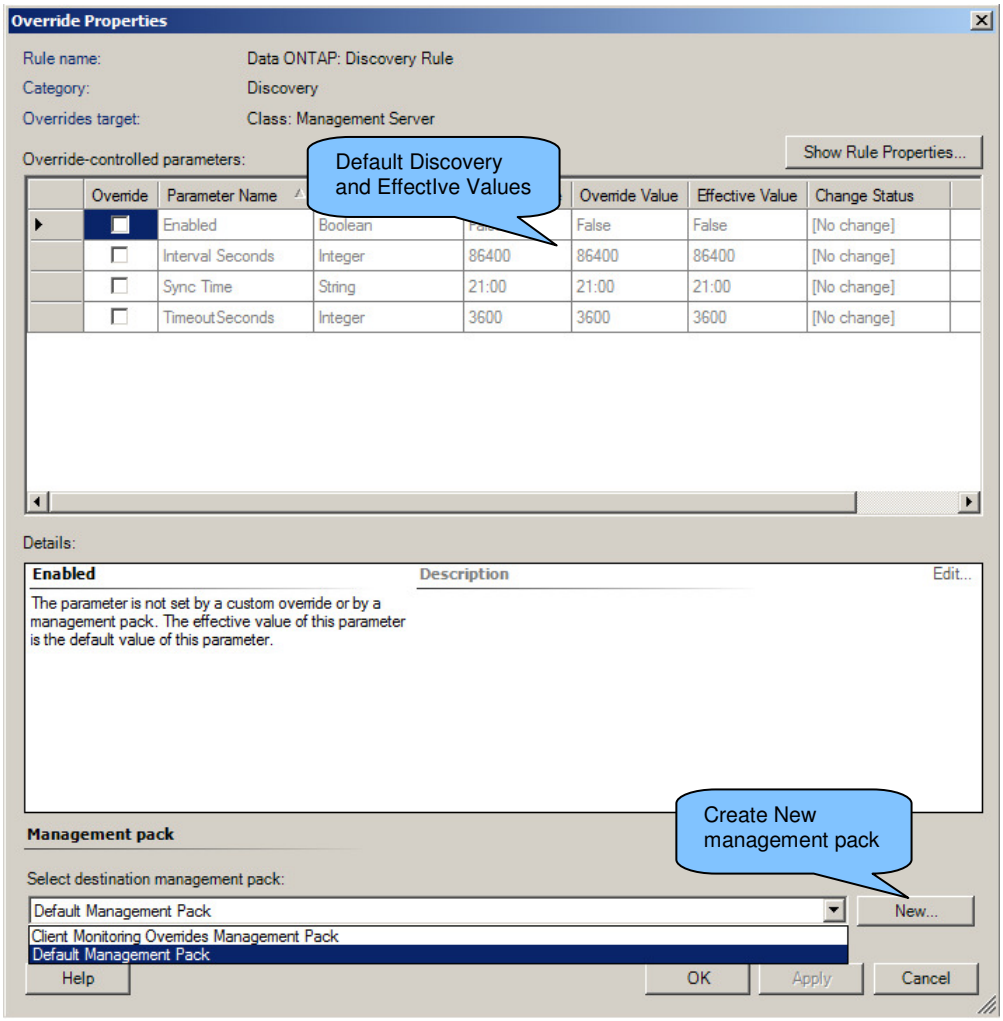

Figure 2) Discovery rule overrides.

2.8 BEST PRACTICES FOR APPLIANCEWATCH PRO QUICK START

There are many steps required when configuring SCOM and SCVMM to work appropriately with ApplianceWatch PRO. ApplianceWatch PRO also requires a number of steps after installing SCOM and SCVMM to function correctly. The following list shows a list of general steps required for getting ApplianceWatch PRO to function properly. For more specific details, please refer to the *ApplianceWatch PRO 2.1.1 Installation and Administration Guide*.

ApplianceWatch PRO Quick Start Guide:

1. SCOM Installation:
   a. Review SCOM Installation Guide for requirements.
      http://technet.microsoft.com/en-us/library/bb309428.aspx
   b. SCOM Reporting – SCOM Reporting Module Installation Required.
   c. SCVMM – SCVMM Installation and PRO Integration Required between SCOM and SCVMM.
   d. Make sure all installation requirements have been fulfilled and confirm proper functionality prior to proceeding with ApplianceWatch PRO installation. Refer to the Microsoft documentation for SCOM, SCVMM, or Reporting for more details.
      www.microsoft.com/systemcenter/en/us/default.aspx
2. ApplianceWatch PRO Installation - *Download from NOW*™
   a. Install ApplianceWatch PRO:
      i. Run ApplianceWatch PRO executable on SCOM server.
   b. Discover Network Devices:
      i. Open SCOM, Administration, click “Discovery wizard” and discover Network devices.
      ii. Make sure SNMP is set up appropriately on SCOM and NetApp storage prior to running Network Device Discovery.

NOTE: SNMP Version Support
For Data ONTAP versions below 7.3, only SNMP V1 will be supported.
For Data ONTAP version 7.3 and above - SNMP V3 and SNMP V2C will be supported.
Using SNMP Version V1 will discover all storage appliances in the environment.

   c. Add NetApp storage controller:
      i. After Network Device Discovery is complete, go to Monitoring, Discovered Inventory (make sure Discovered Inventory scope is set to Management Server), select “Data ONTAP: Add Controller.”
   d. Add NetApp storage credentials:
      i. Select “Data ONTAP: Manage Controller Credentials” (make sure user credentials has appropriate roles and capabilities assigned, see Section 2.4 for minimum roles and capabilities).
   e. Enable Discovery:
      i. Go to Authoring, Rules, Filter & Look For: “Data ONTAP: Discovery Rule” under Management Server (not Data ONTAP Management server). Enable PRO and MetroCluster discovery if installed and configured.
      ii. Right click rule, select Overrides, Override the Rule, For all objects of class: Management Server, select Override for “Enabled” and set Override Value to “True." Follow the Best Practice for Overrides in Section 2.7 and save all ApplianceWatch PRO overrides to a new management pack.
   f. PRO Environments:
      i. Install ApplianceWatch PRO Agent on all Hyper-V Parent Nodes managed by SCVMM if monitoring is required by ApplianceWatch PRO.
   g. Enable PRO tips:
      i. From SCVMM, Administration, General, PRO Settings, Enable PRO Tips.

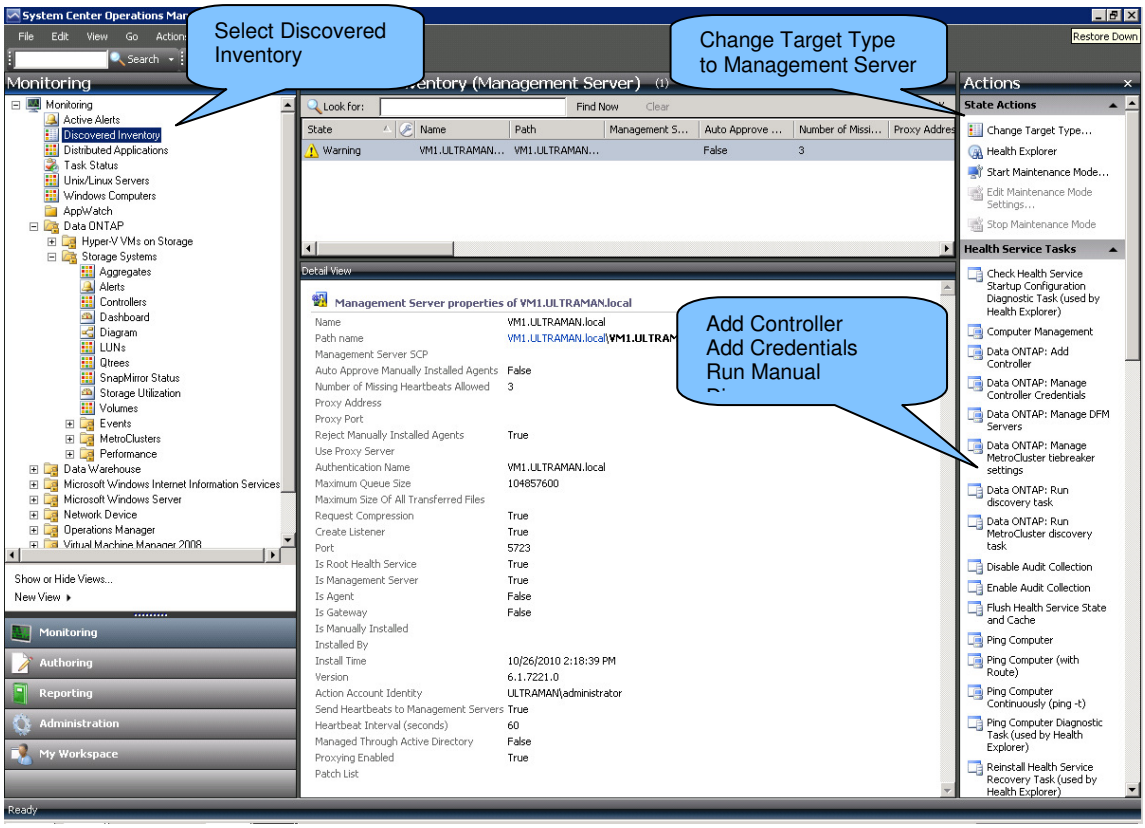

Figure 3) Quick Start Guide.

2.9 BEST PRACTICES FOR MANUAL DISCOVERY

After installing ApplianceWatch PRO and all of the required MPs a discovery process is required to capture all of the data to populate the SCOM UI with NetApp information. The manual process can be started by launching the Data ONTAP Run discovery task. Make sure that you have followed the Quick Start Best Practice in Section 2.8 or the *ApplianceWatch PRO 2.1.1 Installation and Administration Guide* for proper setup of the environment prior to running manual discovery.

To manually run a discovery task:

1. Go to Monitoring and click Discovered Inventory.
2. Make sure that the Discovery Inventory type is the Management Server.
3. If Management Server is not shown, click “Change Target Type” in Actions Pane on right.
4. Then find and select Management Server. Data ONTAP Management Server should not be mistaken for Management Server.
5. After completing the above steps, users should now see a number of Data ONTAP actions and use Data ONTAP: Run Discovery Task to initiate the manual discovery process.

2.10 BEST PRACTICES FOR UNINSTALLATION

Custom configurations set during ApplianceWatch PRO setup can cause the uninstall process of ApplianceWatch PRO to react differently. The following steps introduce how to completely uninstall ApplianceWatch PRO and get the SCOM environment back to its original state.

To uninstall ApplianceWatch PRO, follow these steps:

1. Navigate to the “Administration tab” within SCOM.
2. Select the ApplianceWatch management packs that were installed.
3. Delete Data ONTAP ApplianceWatch management pack and all other Data ONTAP management packs that have been installed.

WARNING: When trying to delete the ApplianceWatch PRO management packs (MP), SCOM might prompt you to remove the Microsoft Default MP dependency. This message occurs if you save any override MP values to the default MP. You will lose all override settings stored in the Default MP. To eliminate any loss of settings, remove the override settings for ApplianceWatch stored in the Default MP prior to uninstalling ApplianceWatch PRO

4. To check for ApplianceWatch override values, go to “Authoring” tab, “Overrides," go to Target where overrides were saved, and delete the Data ONTAP overrides.

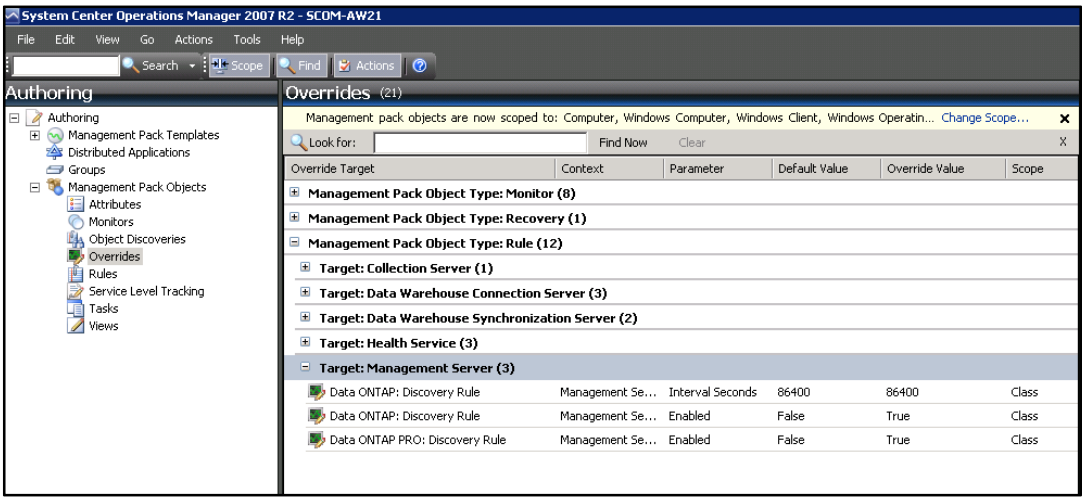

Figure 4) Checking overrides.

5. Delete ApplianceWatch management packs.
6. Uninstall ApplianceWatch PRO application from Windows control panel and reboot.

*Always refer to the ApplianceWatch PRO documentation for exact steps and details.

ApplianceWatch PRO 2.1.1 Installation and Administration Guide

ApplianceWatch PRO 2.1.1 Release Notes

3 APPLIANCEWATCH PRO 2.1.1 ALERTS, MONITORING, AND VIEWS

ApplianceWatch PRO offers various alerts, monitoring options, and views for your NetApp storage array. After installing and discovering all objects within the environment, administrators should successfully see information on LUNs, qtrees, volumes, aggregates, and other detailed views. These various tools allow administrators to efficiently manage their NetApp storage arrays.

3.1 BEST PRACTICES FOR ALERTS

The alerts view allows administrators to instantly view and report any problems within their NetApp environment. There are numerous ways to view the alerts, and the following image notes the locations of the important details of each alert.

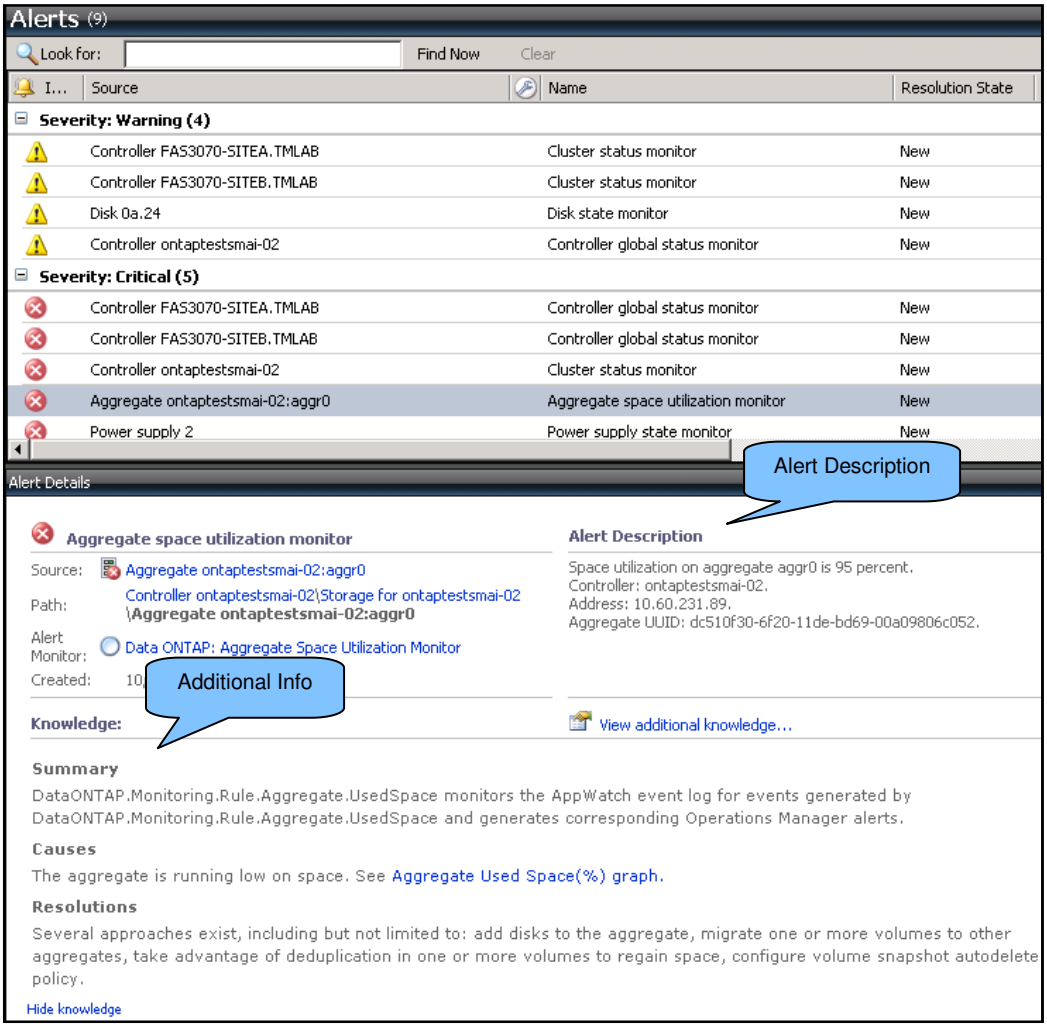

Figure 5) Alerts.

3.2 BEST PRACTICES FOR ALERT NOTIFICATIONS

Use of alert subscriptions can enable administrators to be notified immediately via email on specific events.

To create a custom alert subscription:

1. Right click the specific alert.
2. Select “Notification subscription.”
3. Select “New” to start the Notification Subscription Wizard.

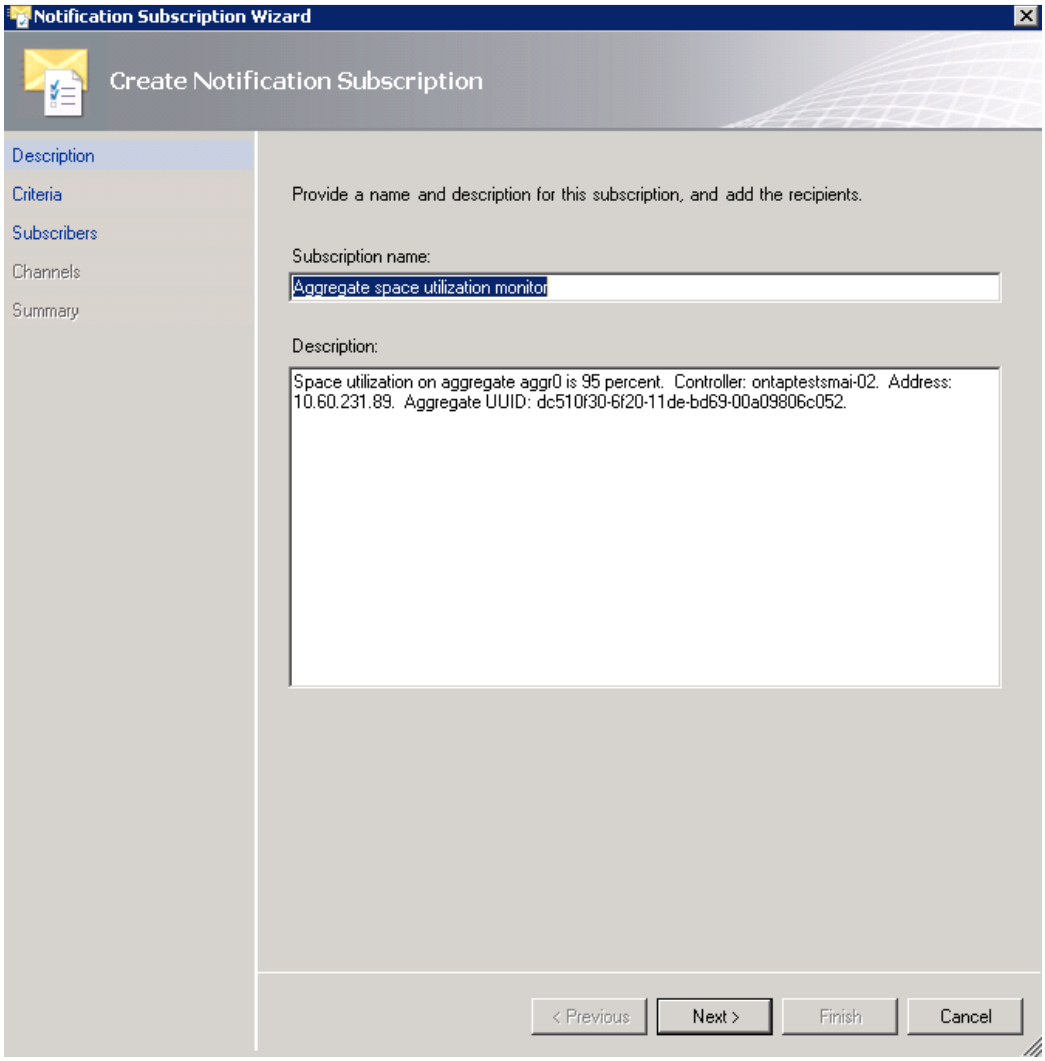

Figure 6) Custom notifications.

3.3 BEST PRACTICES FOR MONITORING

The SCOM GUI interface comes with a number of different types of views that administrators can use to monitor and manage their environment. Aside from the various views, there is a specific view called the “Health Explorer” that allows administrators to view the entire object and pinpoint locations where exact problems are occurring.

To access the Health Explorer View:

1. Right-click any object within SCOM for popup menu.
2. Select Health Explorer.

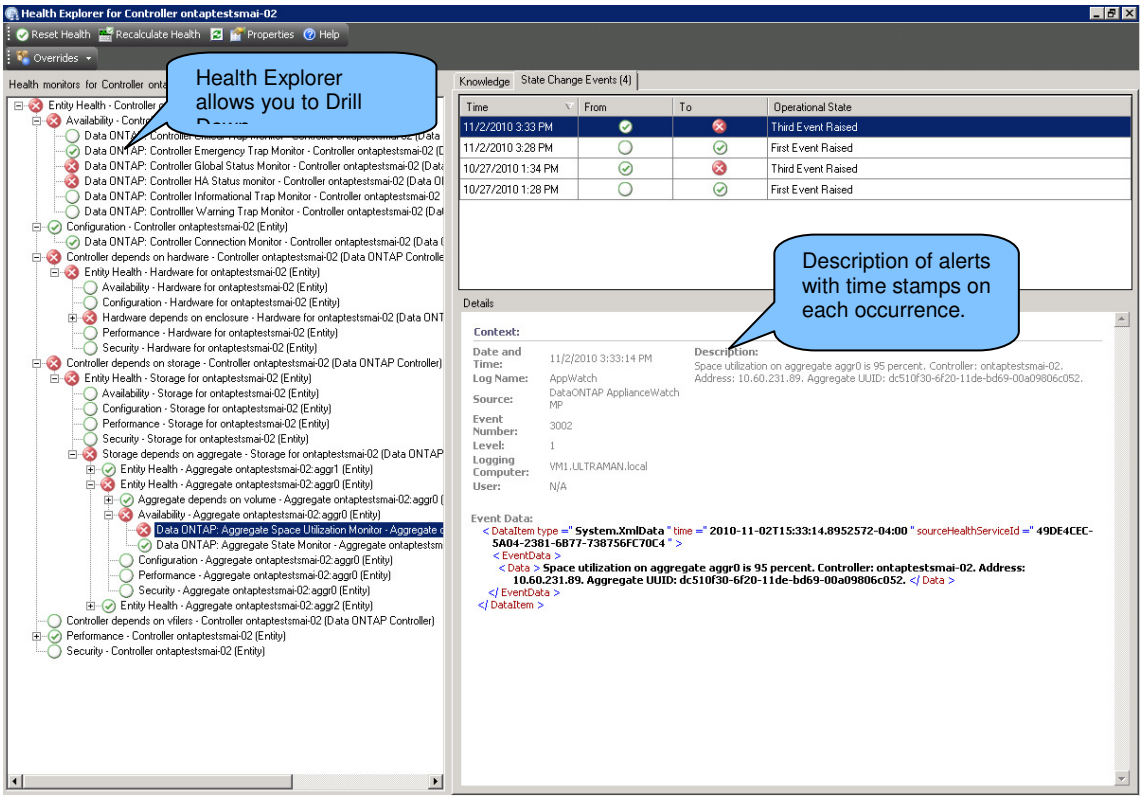

Figure 7) Health Explorer.

3.4 BEST PRACTICES FOR VIEWS

Each view within SCOM has a particular set of default data points that are shown with the ApplianceWatch MPs. The views can be modified to show more or less data and can be “personalized” for the administrator's convenience. There might also be times when the administrator has made various changes to the different views and would like to revert back to default or would like to clear any cached views to make sure fresh data is being presented.

To modify the views:

1. Right click inside of the view.
2. Select “Personalize View.”
3. Then click “Reset to Default.”

To reset the view back to its original state:

1. Right click inside of the view.
2. Select “Personalize View.”
3. Then click “Reset to Default.”

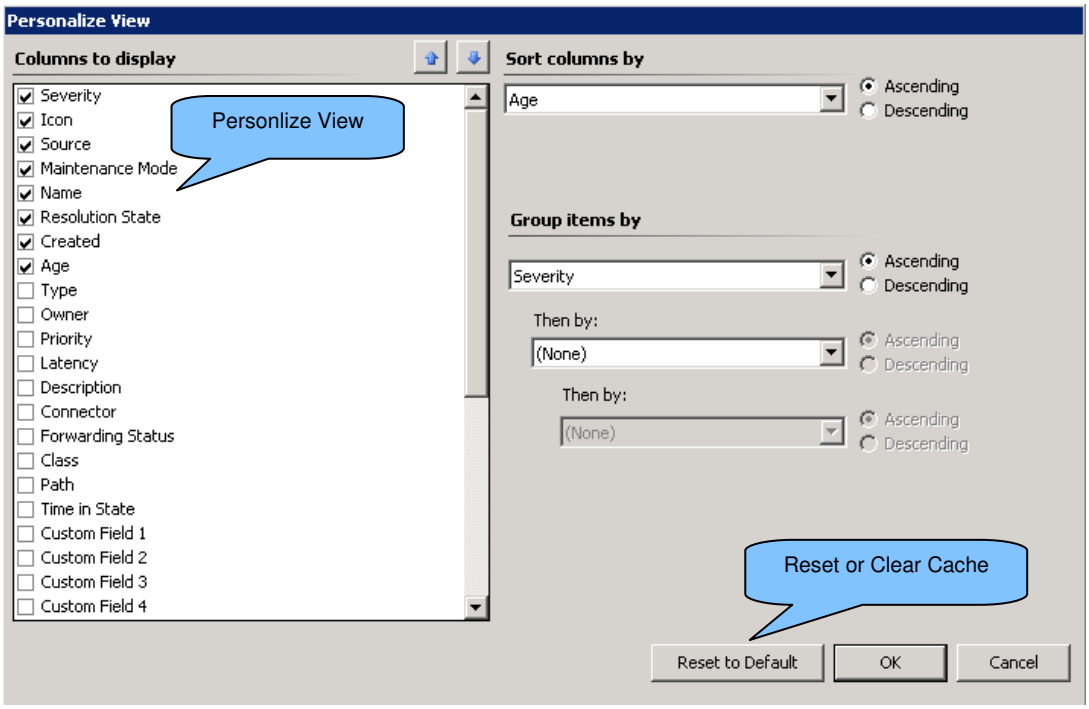

Figure 8) Personalize view.

4 APPLIANCEWATCH PRO 2.1.1 PRO REPORTING

ApplianceWatch PRO 2.1.1 comes with a Reporting management pack so you can view reports on various aspects of your NetApp storage. You must configure System Center Operations Manager 2007 R2 for reporting so that the Data ONTAP Reports management pack appears with the other management packs. For more information on setting up reporting for SCOM, please visit Microsoft.
www.microsoft.com/systemcenter/en/us/default.aspx

4.1 BEST PRACTICES FOR CUSTOM REPORTING

The Reporting management pack within ApplianceWatch PRO 2.1.1 comes with various prepackaged reports. Administrators can also create custom reports for specific NetApp objects by following these procedures.

To create a custom report:

1. Click the Reporting tab.
2. Select Microsoft Generic Report Library.
3. Double click the specific report type for the custom report.
4. Select “Add Group.”
5. Filter with “Ontap” keyword for available report options.

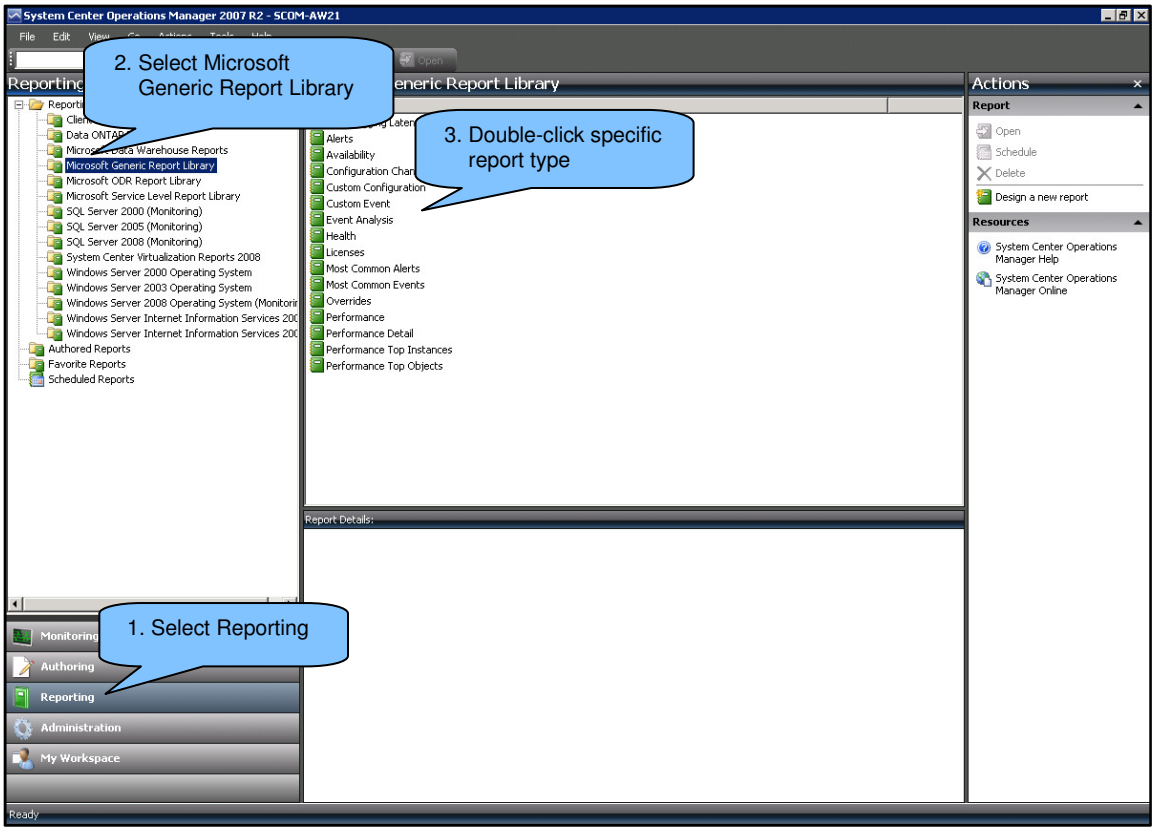

Figure 9) Custom reports.

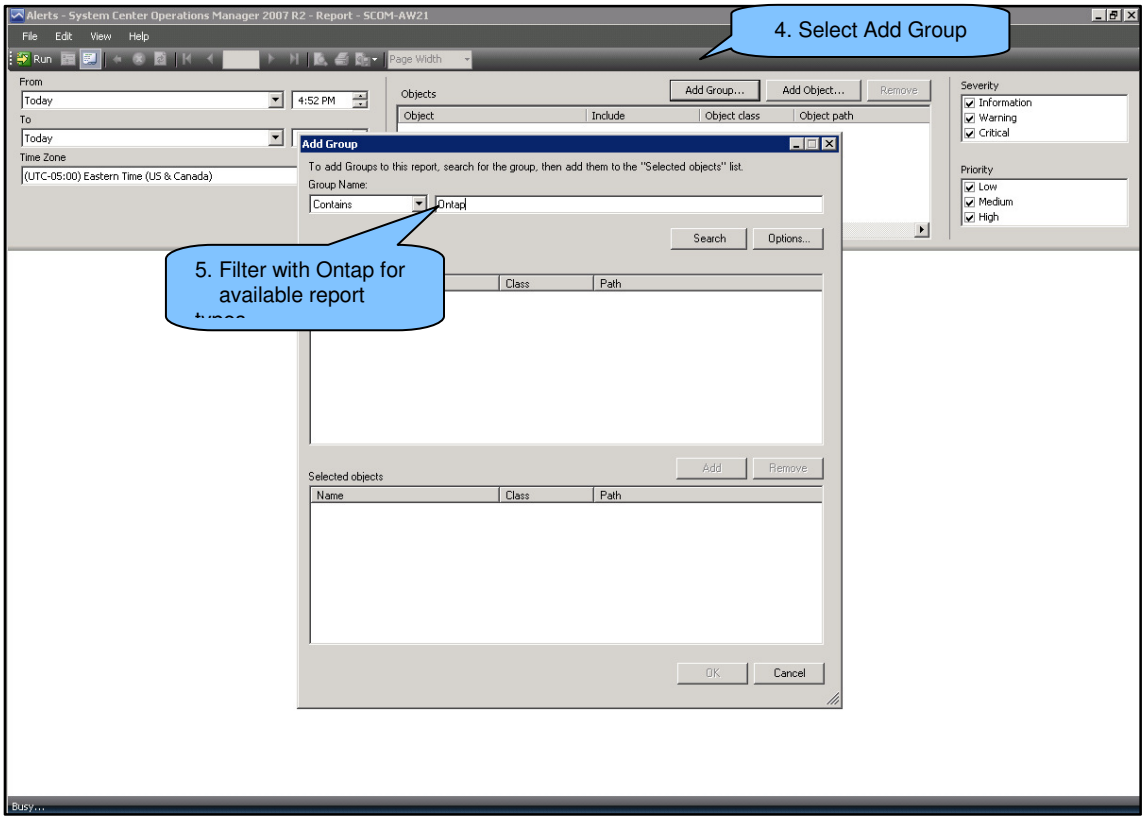

Figure 10) Custom report object selection.

5 APPLIANCEWATCH PRO 2.1.1 PRO TIPS

ApplianceWatch PRO offers the usage of PRO tips, which can be enabled by proper setup and integration of SCOM and SCVMM. Once SCOM and SCVMM have been integrated, the administrator can install the ApplianceWatch PRO and use the Discovery feature to find Virtual Machines that exist on Data ONTAP storage. Same as storage Discovery, this rule is disabled by default and must be enabled by the administrator prior to receiving any PRO tips. As a best practice, always read the description of the PRO tip in full prior to implementing any changes to the environment.

5.1 BEST PRACTICES FOR VOLUME SPACE UTILIZATION PRO TIP

When implemented, this PRO TIP will add storage to a volume. There are cases when the volume space cannot be automatically increased due to conditions such as not having enough space in the aggregate or because the volume is the source of a SnapMirror® relationship, and growing the source volume larger than the destination volume will inhibit replication updates. Applying the implement button for these situations will not enlarge the volume.

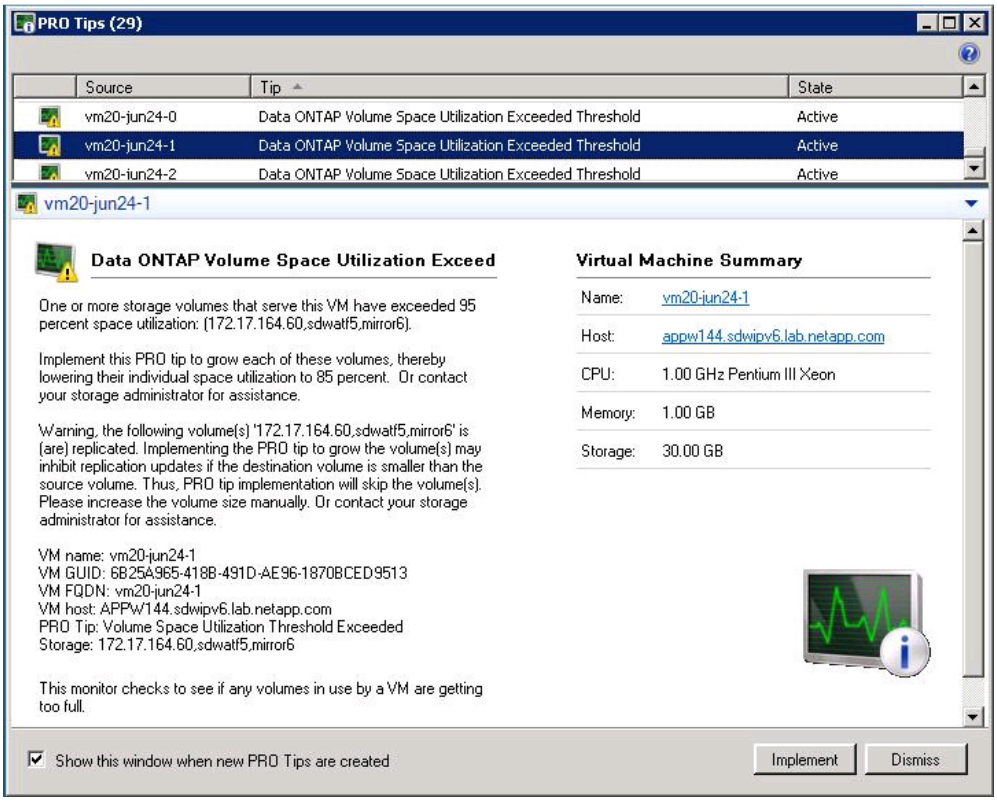

Figure 11) Volume space utilization PRO tip.

5.2 BEST PRACTICES FOR SNAPSHOT AUTODELETE PRO TIP

The thin-provisioning Snapshot® autodelete PRO tip checks for Snapshot autodelete turned off for volumes hosting Hyper-V VMs. If implemented, the PRO tip will enable Snapshot autodelete for the volume.

WARNING: Do not enable Snapshot autodelete for volumes that are currently protected by other NetApp management applications such as System Manager, SnapManager® for Hyper-V, and so on. Enabling Snapshot autodelete on these volumes might disrupt the other protection mechanisms and cause issues with consistency.

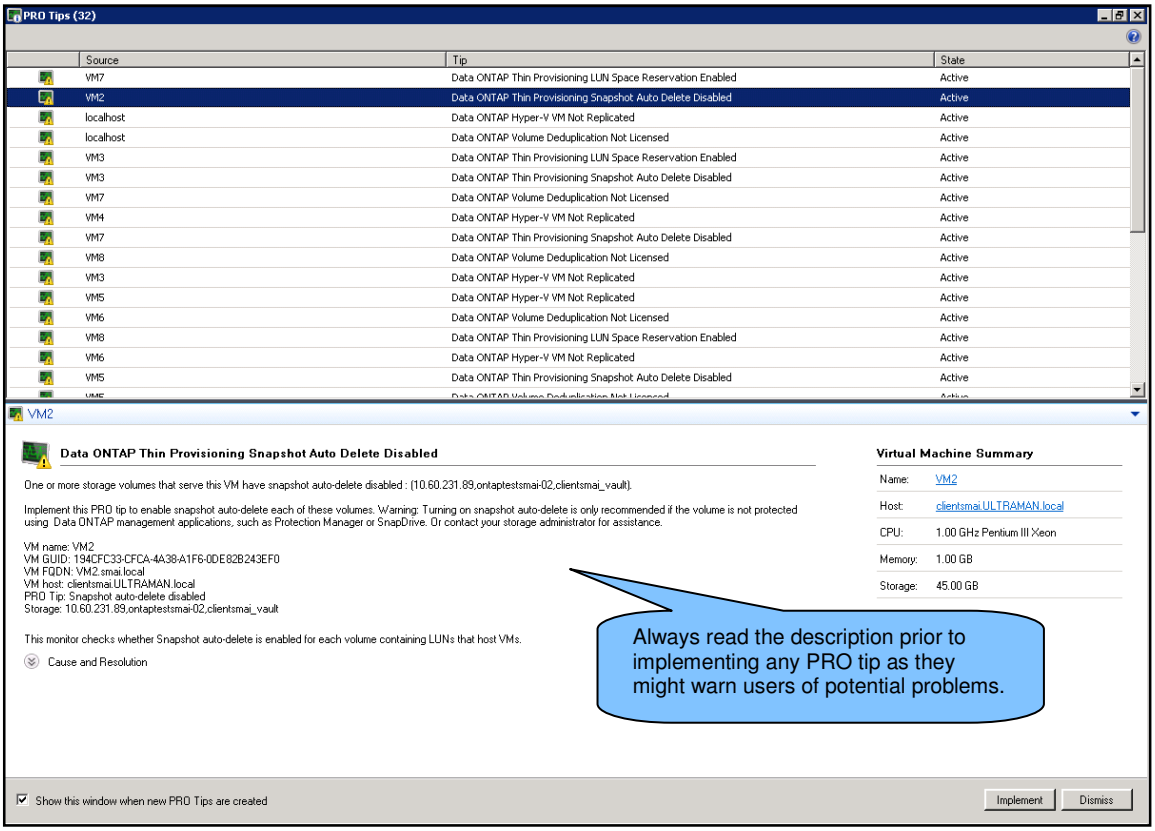

Figure 12) SCVMM PRO tip.

6 APPLIANCEWATCH PRO 2.1.1 RAPID PROVISIONING AND CLONING

The rapid provisioning and cloning cmdlets are a separate install from the core management packs and are not dependant on them to function. By using rapid provisioning and cloning cmdlets with Microsoft System Center Virtual Machine Manager (SCVMM) applications, you can utilize your existing NetApp storage resources to perform faster and more space-efficient provisioning and cloning of Hyper-V virtual machines. For more information on the provisioning and cloning cmdlets, see the *Rapid Provisioning and Cloning Command Reference Guide.*

6.1 BEST PRACTICES FOR USING CMDLETS AND USER ACCESS CONTROL

Cmdlets included with the ApplianceWatch PRO rapid provisioning and cloning cmdlets fail if user access control is enabled within the Windows operating system and if the terminal is not opened using "Run As Administrator." Either disable UAC or open cmdlet using “Run As Administrator."

6.2 BEST PRACTICES FOR THE NEW-CLONE CMDLET

The New-Clone cmdlet clones from a Microsoft System Center Virtual Machine Manager template to a virtual machine that is currently shut down. You must execute the New-Clone cmdlet on the host on which the System Center Virtual Machine Manager template library share exists.

When using the [-server] flag with the New-Clone cmdlet, the remote server must have a NetApp storage path already present to the storage containing the VHD. The VHD needs to be on a NetApp LUN that is mapped to the host executing New-Clone. The LUN should not be mapped to the remote host (the –Server host), but the remote host should be connected to the storage array via FCP or iSCSI.

6.3 BEST PRACTICES FOR GENERAL HELP WITH CMDLETS

Use the “get-help” command to find cmdlets and also to show specific details for the particular cmdlet.

To use the Get-help command:

1. Double click the rapid provisioning and cloning shortcut created on your desktop during ApplianceWatch PRO installation.
2. In the command prompt enter, [get-help *] to get a list of available cmdlets.

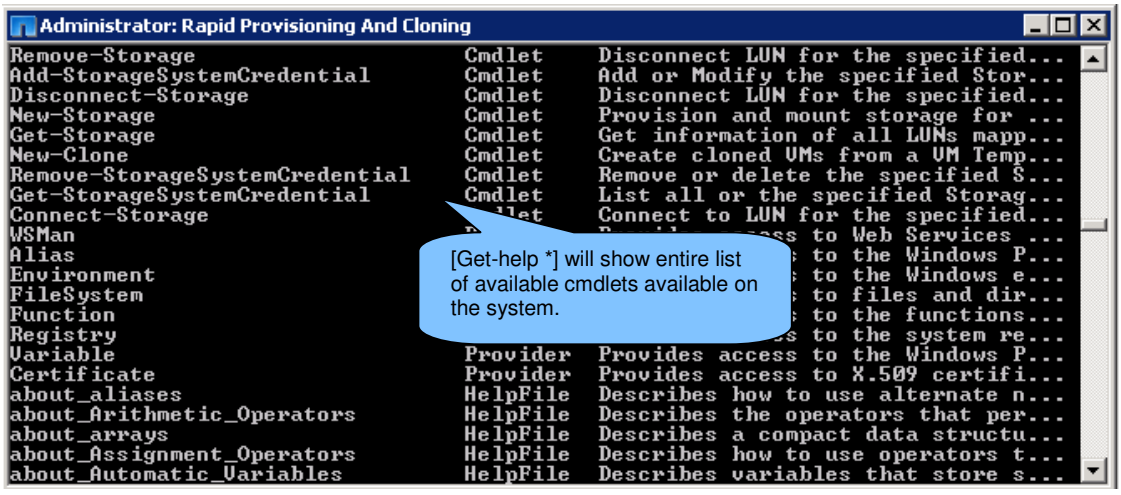

Figure 13) Cmdlets.

To get specific details of a cmdlet:

1. In the command prompt enter [get-help “cmdlet name”] to get full details of the cmdlet.

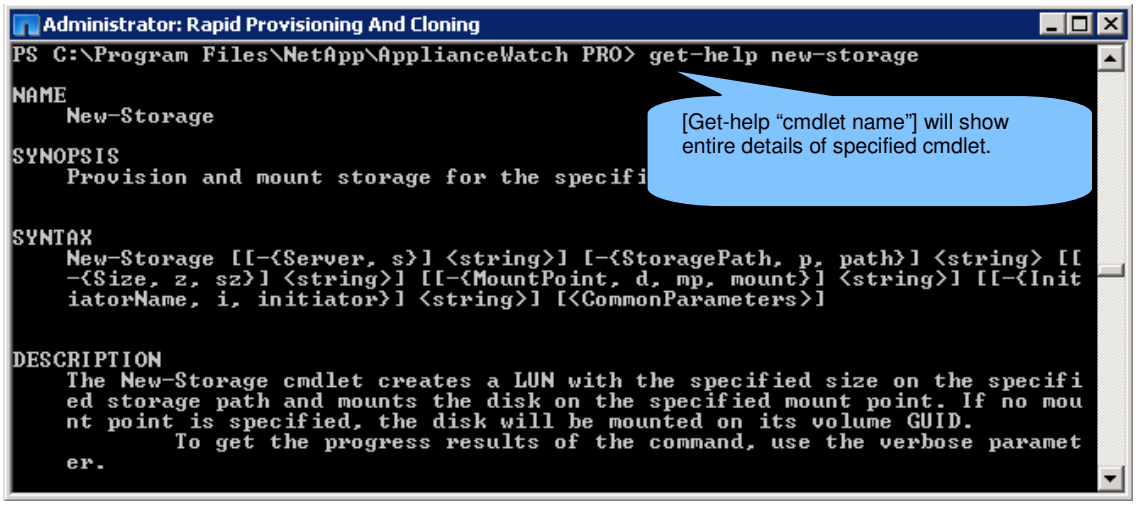

Figure 14) Get-help cmdlet.

7 APPLIANCEWATCH PRO 2.1.1 SSP INTEGRATION

As described above, ApplianceWatch Pro 2.1.1 contains a set of powershell cmdlets for cloning Hyper-V VMs from templates. These same cmdlets and two powershell scripts can be used to enable rapid VM provisioning from Microsoft System Center Virtual Machine Manager (SCVMM) Self Service Portal 2.0. SSP provides a Web portal for data center admins to allow users to create Hyper-V VM requests and allows users to rapidly provision VMs from templates to the most suitable Hyper-V parent on demand.

7.1 BEST PRACTICES FOR INSTALLATION OF CMDLETS WITH SSP

Installing the rapid provisioning and cloning cmdlets after the Self Service Portal service requires restart of the SSP service.

7.2 BEST PRACTICES FOR SELF SERVICE PORTAL SETUP

Make sure the Self Service Role has been created in SCVMM to allow proper functionality.

1. Go to SCVMM.
2. Select Administration tab.
3. Select “User Roles.”
4. Make sure Self-Service User is created.
5. Verify the user has appropriate permissions within the following tabs:
   a. Members, make sure user has correct roles.
   b. VM Permissions, make sure user has correct permissions.
   c. Create VM, make sure user has appropriate templates.

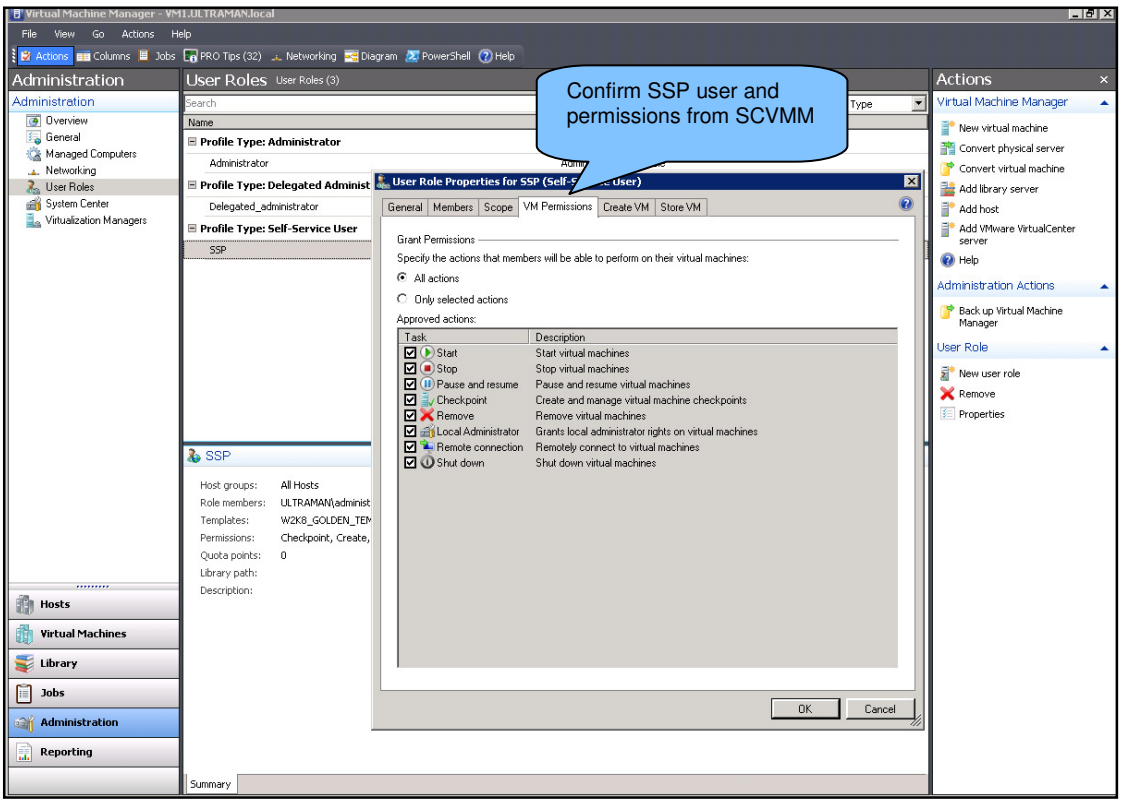

Figure 15) Self Service Portal.

8 APPLIANCEWATCH PRO 2.1.1 METROCLUSTER

Environments using NetApp MetroCluster will find the ApplianceWatch PRO 2.1.1 MetroCluster management pack to offer many added benefits. The MetroCluster management pack includes the ability to monitor, act as a tiebreaker, and failback. The Tiebreaker function is a Windows service that continually monitors MetroCluster pairs and forces a cluster failover in the event of a disaster.

The monitoring provided for MetroCluster pairs includes the following:

- Cluster status (adds detection of interconnect degradation)
- Aggregate mirror status
- Network reachability
- RLM reachability
- Aggregate mirror configuration
- Disk ownership
- Fabric connection (fabric MC only)
- RLM configuration
- Tiebreaker service
- Tiebreaker configuration
- Recovery Assistant (failback)

8.1 BEST PRACTICES FOR METROCLUSTER TIEBREAKER

The Tiebreaker service should be installed on an SCOM management server that is not colocated with either side of a MetroCluster pair to avoid any problems with complete site outages.

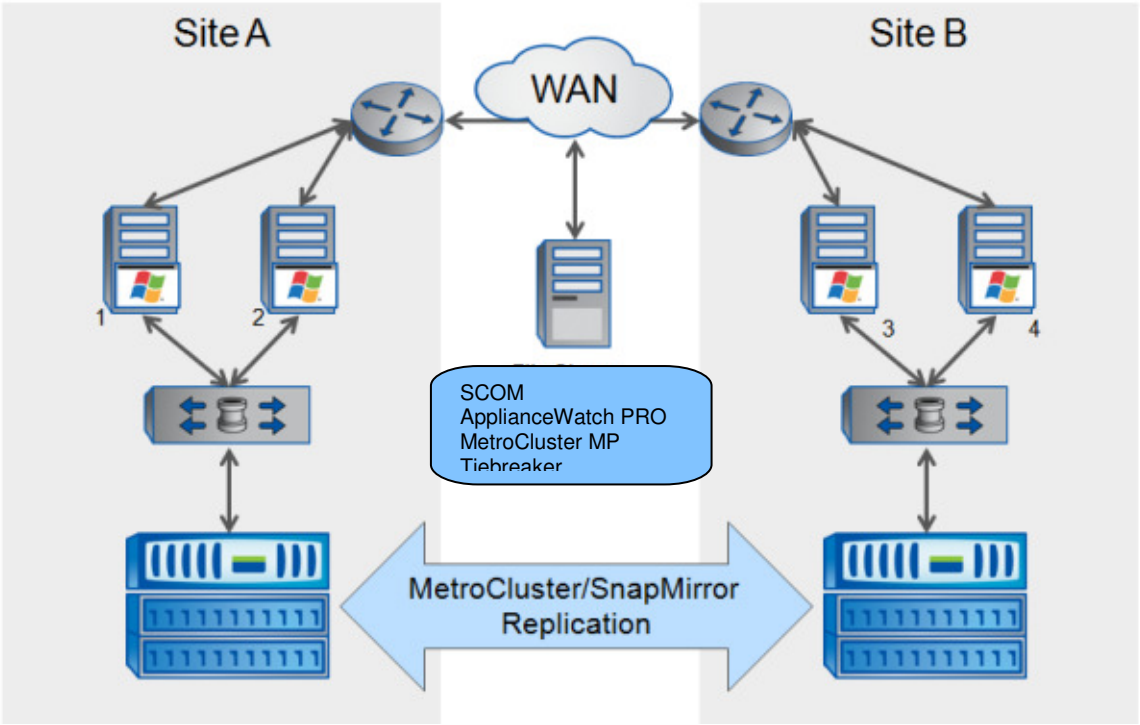

Figure 16) MetroCluster Tiebreaker.

8.2 BEST PRACTICES FOR METROCLUSTER RECOVERY ASSISTANT

Set the RLM credentials for both of the controllers using the Data ONTAP ‘MetroCluster Tiebreaker settings in order to identify the controllers as ApplianceWatch PRO requires login on the storage. Proper RLM settings also make sure of proper use of the power controller on/off menu and fencing functionality. If aggregate information shown in the Recovery Assistant is not consistent with the actual**[[NOTE: Incomplete sentence?]]**.

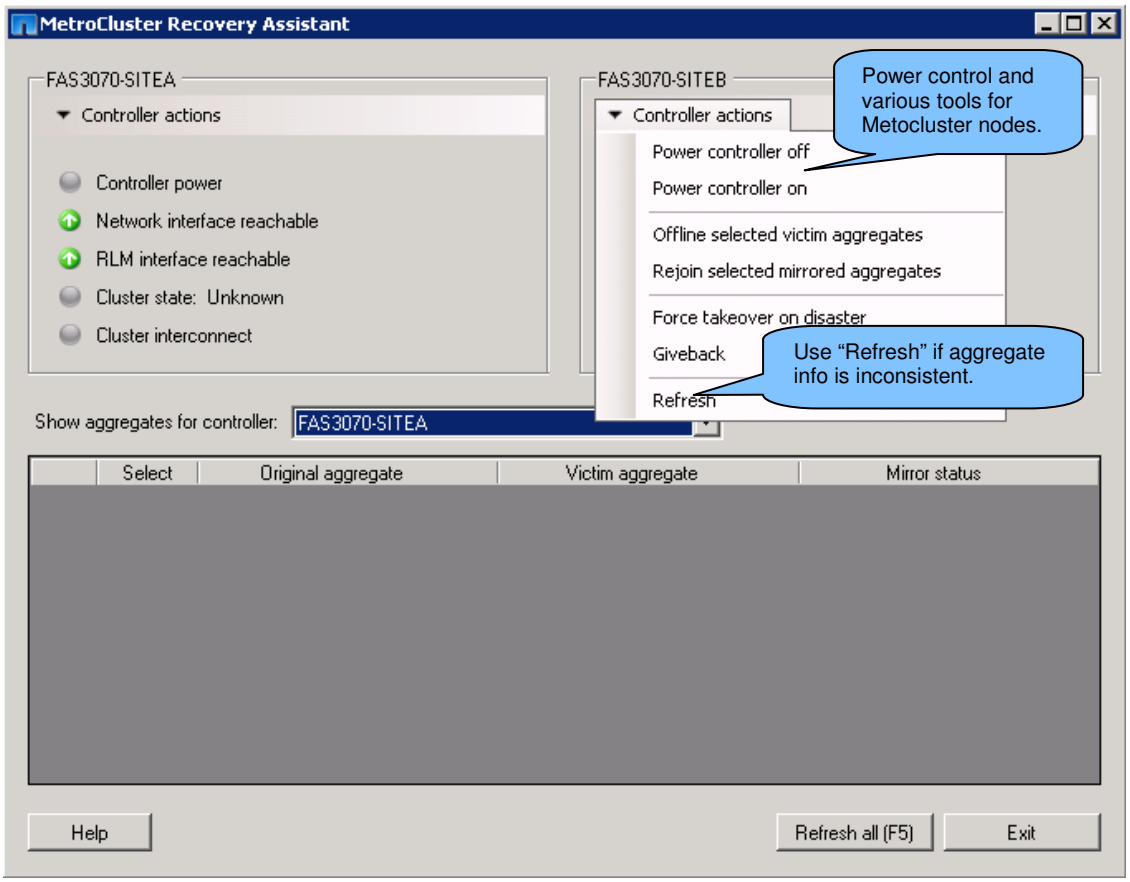

Figure 17) MetroCluster Recovery Assistant.

9 APPLIANCEWATCH PRO 2.1.1 TROUBLESHOOTING

9.1 BEST PRACTICES FOR CLEARING SCOM RELATED CACHE ISSUES

In some situations there might be times when the cached UI view within SCOM needs to be cleared to troubleshoot the environment.

Run the following command to launch a new instance of SCOM console with cleared UI cache:

Microsoft.MOM.UI.Console.exe /ClearCache

9.2 BEST PRACTICES FOR REINSTALLING APPLIANCEWATCH PRO AND DISCOVERY

There might be times when a reinstallation of ApplianceWatch PRO is required. After following the instructions within the Installation and Administration Guide for ApplianceWatch PRO, discovery will need to be reinitiated even if it was executed in the previous installation.

To rediscover after reinstallation:

1. Go to Discovered Inventory, Actions -> State Actions -> Change Target Type to change to "Management Server."
2. Set up credentials using Data ONTAP Manage Controller Credentials in Actions pane.
3. Click Data ONTAP: Run discovery task.

Refer to Section 2.8 for Best Practice for Manual Discovery.

9.3 BEST PRACTICES FOR SCOM DATABASE

When viewing host, controllers, or entities within the controllers in the Monitoring view, and the critical / warning / healthy icons are grayed-out instead of colored, the problem indicates that the database updates are hindered or that the database is full.

To resolve this problem with database autogrow:

1. Go to SQL Server Management Studio.
2. Connect to the SCOM MS-SQL Server database server.
3. Under Databases, select the Operations Manager database.
4. Right click, select Properties, and select Files.
5. Two rows in the table should be displayed with logical names MOM_DATA and MOM_LOG.
6. In the column Autogrowth, double click the button on the right showing “…”
7. Adjust the setting to allow the database to use the Autogrowth.

To resolve this problem by allowing the MOM_DATA file in the Operations Manager database to grow to a reasonable size, run the following SQL Server script:

```
alter database OperationsManager
{
MODIFY FILE(NAME = MOM_DATA, Filegrowth = 10MB);
}
```

9.4 BEST PRACTICES FOR DISCOVERY TROUBLESHOOTING

Open a console window to the NetApp storage array to troubleshoot any ApplianceWatch PRO discovery issues.

If access is denied or if there are issues with user permissions the following will be logged:

[NetAppStorage01:useradmin.unauthorized.user:warning]: User 'scom' denied access

If access and discovery complete successfully the following will be logged:

[*NetAppStorage01: app.log.info:info]: VM1.local: ApplianceWatch 2.1.1.0.0: (100) ApplianceWatch: Data ONTAP MP discovery rule*

9.5 BEST PRACTICES FOR SNMP VERSIONS

Different versions of Data ONTAP will determine the supported SNMP version for ApplianceWatch.

For Data ONTAP versions below 7.3, only SNMP V1 will be supported.

For Data ONTAP version 7.3 and above - SNMP V3 and SNMP V2C will be supported.

If storage environment contains multiple different types of Data ONTAP, use SNMP V1 to discover all storage arrays with ApplianceWatch PRO.

9.6 BEST PRACTICES FOR EVENT VIEWER LOGS

Use the Windows Event viewer to review the AppWatch specific logs for further information on any issues. Users will find a AppWatch specific event log under “Applications and Services Logs” in Event Viewer. In addition to the AppWatch specific logs, users will find important information in the Application Logs and the Operations Manager Logs. Utilize these logs to find specific issues with ApplianceWatch discovery or any other issues.

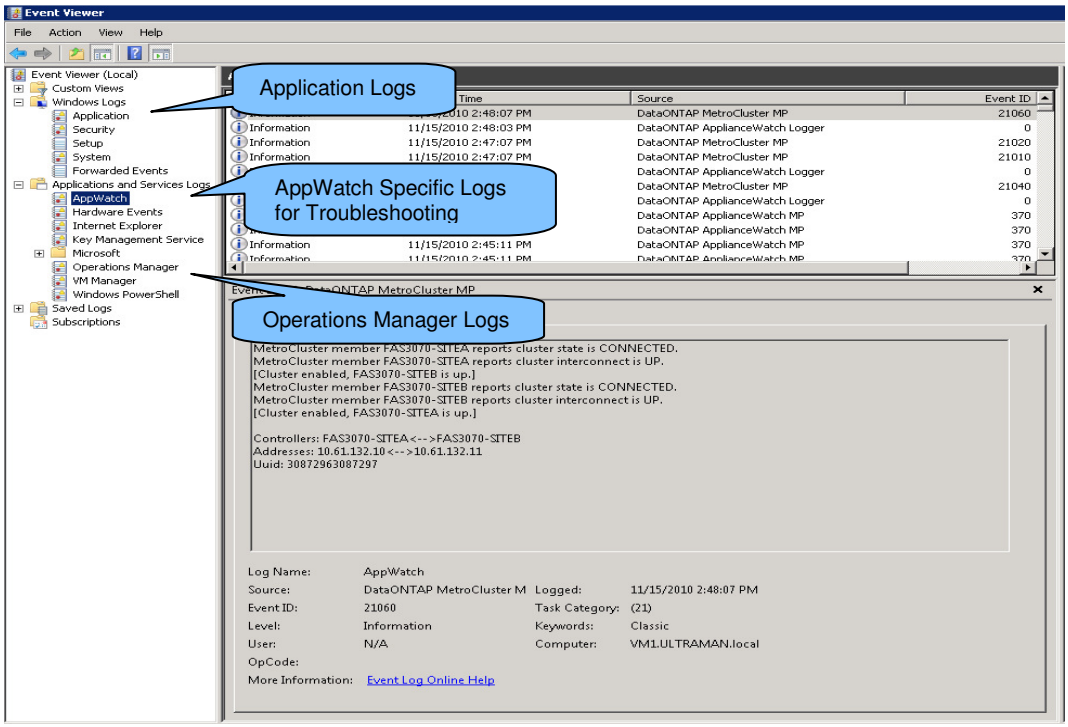

Figure 18) Event Viewer Logs.

9.7 BEST PRACTICES FOR DEBUGGING

To enable debug logging for ApplianceWatch you'll need to set the DEBUG value within the LogSettings.xml. The LogSettings.xml is located within the ApplianceWatch install directory and the default location is C:\Program Files\NetApp\ApplianceWatch PRO.

To enable ApplianceWatch PRO Debugging:

Change the INFO to DEBUG value within the root logger section of the LogSettings.xml file:

<!-- Set root logger level -->

<root>

<level value="INFO" /> <!-- Change Info to DEBUG for ApplianceWatch Debugging-->

<appender-ref ref="EventLogAppender" />

</root>

9.8 BEST PRACTICES FOR ADVANCED TROUBLESHOOTING

When basic troubleshooting does not resolve any issues with ApplianceWatch PRO, please use one of the many support features provided to NetApp customers.

1. NetApp Community - *http://communities.netapp.com/index.jspa*
   A public forum where customers can discuss with other NetApp experts about specific technologies. For ApplianceWatch PRO specific questions and topics, *http://communities.netapp.com/community/products_and_solutions/storage_management_software*
2. NetApp Support Community - *https://forums.netapp.com/index.jspa*
   Support forum for customers with specific NetApp technology questions.
3. NetApp customers with support contracts can call our NetApp Global Support (NGS) Center 24x7 for immediate support issues.