Technical Report

OnCommand Plug-In 3.1 for Microsoft: Best Practices Guide

Sadhana B, Alex Jauch, NetApp

July 2012 | TR-4091

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Introduction

The NetApp® OnCommand® Plug-In 3.1 for Microsoft® (OCPM) is an enterprise-class storage monitoring application that provides integration with Microsoft System Center Operations Manager (SCOM) and System Center Virtual Machine Manager (SCVMM) 2012. It enables system administrators to monitor, manage, and report NetApp storage.

The key features of this release are as follows:

- Management packs (MPs) for SCOM 2012.
- Rapid provisioning with SCVMM 2012.
- Integration packs for System Center Orchestrator 2012.
- The root management server machine is removed and replaced with a root management server (RMS) (emulator) role. There is a dependency that the SCVMM server needs to connect to this RMS emulator node for receiving PRO tips.
- Limited support for SCOM high availability; Network Load Balancing (NLB) is the only supported configuration.
- Additional cmdlets for managing controllers.
- Deprecated support for SCVMM SSP 2.0 and MetroCluster™.

1.1 Common Terminology

Table 1 lists acronyms and abbreviations commonly used throughout the documentation.

Table 1) Acronyms and abbreviations.

Acronyms or Abbreviations	Definition
OCPM	NetApp OnCommand Plug-In 3.1 for Microsoft.
SC	Microsoft System Center solutions are a set of management products that help IT pros manage 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 installation 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 installation of SCOM where the SCOM SDKs and connectors are installed on a system that has not been installed with SCOM console. This installation does not have the user interface (UI), and it is intended for systems that must communicate monitoring and other information to the SCOM server. This agent can be installed remotely on systems using SCOM console on the SCOM server.

Acronyms or Abbreviations	Definition
SCVMM	A member of the SC family, System Center Virtual Machine Manager is for IT professionals responsible for managing virtual infrastructures. SCVMM provides solutions for the following: • 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 • Rapid provisioning of new virtual machines by leveraging the expertise and investments in Microsoft Windows Server® technology
PRO	Performance and resource optimization (PRO), a feature of System Center Suite that in SC 2012 can be implemented in both SCOM and SCVMM and ties specific alerts from System Center Operations Manager (SCOM) 2012 to remediation actions in SCVMM. Management packs that allow using this SCVMM PRO feature are referred to as Data ONTAP® PRO management packs.
MP	Management pack defines the author's definition of healthy state for application, services, or hardware that SCOM monitors.
SCO	System Center Orchestrator 2012 is a workflow management solution for the data center. Orchestrator lets you automate the creation, monitor, and deploy resources in your environment.
Controller	A NetApp storage element that serves data.
MultiStore®	MultiStore is an abstraction in Data ONTAP that allows a controller to be partitioned into a set of relatively independent "virtual" controllers (vFiler® units). MultiStore needs to be licensed on the controller.

1.2   Target Audience

This guide is intended for NetApp storage and Windows Server administrators who manage NetApp storage systems using OCPM. OCPM provides integration with System Center Operations Manager to give Windows IT administrators a central interface to monitor NetApp storage systems using System Center Operation Manager. OCPM also includes System Center Orchestrator integration pack (OIP), PRO-enabled management packs, and rapid provisioning cmdlets.

A good understanding of Windows® administration, SCOM, SCVMM, and SCO is necessary, as well as an understanding of NetApp storage concepts. The recommendations found in this document are guidelines to assist with configuration of OnCommand Plug-In 3.1 for Microsoft. NetApp recommends that you refer to the following guides before using this guide:

• OnCommand Plug-In 3.1 for Microsoft Installation and Administration Guide
• OnCommand Plug-In 3.1 for Microsoft Release Notes
• OnCommand Plug-In 3.1 for Microsoft Cmdlet Reference Guide

2   Installation and Basic Configuration

This section provides information on the installation and basic configuration.

2.1   System Requirements

Table 2 lists the installation requirements to successfully run OnCommand Plug-In 3.1 for Microsoft.

Table 2) OCPM installation requirements.

Category	Requirements
Hardware requirement	Microsoft System Center Operations Manager 2012 (SCOM) and Microsoft System Center Virtual Machine Manager 2012 (SCVMM) determine the hardware requirements. For more information, visit: http://technet.microsoft.com/en-us/library/hh205987.aspx.

Data ONTAP requirements	• Data ONTAP 7 product family, operating in 7-Mode:
	  − 7.3 or later
	  − 7.3.3 or later for MultiStore support
	• Data ONTAP 8 product family operating in 7-Mode:
	  − 8.0.1, 8.0.2, and 8.0.3
	  − 8.1.0 and 8.1.1

Software requirements	• .NET Framework 3.5 SP1 and .Net 4 • Microsoft System Center Operations Manager 2012 (SCOM) for management packs • Microsoft System Center Virtual Machine Manager 2012 (SCVMM) for cloning cmdlets • Microsoft System Center Orchestrator 2012 (SCO) for SCO integration packs For more information, see the Microsoft TechNet site.
System Center Operations Manager configuration	You must configure Microsoft System Center Operations Manager 2012 (SCOM) for reporting so that the reporting management pack appears with the other management packs. To do this, you need to correctly configure SQL Server® reporting services. For more information, see the Microsoft TechNet site.
System Center Operations Manager library requirements	The following System Center Operations Manager libraries are required for OnCommand discovery agent functionality: • 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 • Microsoft.SystemCenter.VirtualMachineManager.Pro.Library • Microsoft.SystemCenter.VirtualMachineManager.Library The following System Center Operations Manager libraries are required for reporting functionality: • Microsoft.SystemCenter.DataWarehouse.Report.Library • Microsoft ODR Report Library • Microsoft.SystemCenter.DataWarehouse.ServiceLevel.Report.Library
Microsoft licenses	• Windows Server 2008 R2 SP1 • Microsoft SQL Server 2008 SP1, 2008 R2, or 2008 R2 SP1 • Microsoft System Center Operations Manager 2012

Category	Requirements
	• Microsoft System Center Virtual Machine Manager 2012
OCPM requirement	To correctly install OnCommand Plug-In 3.1 for Microsoft, you must first uninstall any earlier versions of OCPM. The installer will prompt during installation and exit if older versions are found. Also, make sure that firewalls, proxies, or other network devices do not interfere with traffic. The required ports are SNMP, and HTTP or HTTPS. Remote operations also require that Windows Web services be enabled. This uses port 808 by default.
OnCommand discovery agent requirements	• Hyper-V™ server role is enabled • Windows Server 2008 R2 or later is installed
Orchestrator integration packs	• You must install System Center Orchestrator and deploy the integration packs to the runbook server. • To enable the cloning, provisioning, and disaster recovery functionality, OnCommand Plug-In VIM Web services must be installed in a Windows Server 2008 R2 host. • You must have .NET 4 installed on SCO runbook server.

2.2 OCPM Preinstallation Requirements

After Microsoft SCOM and SCVMM have been installed and properly configured, the administrator can continue with the OnCommand Plug-In 3.1 for Microsoft installation. SCOM and SCVMM must be properly integrated for virtual machine-based alerts and functionality. Hyper-V hosts must also be added to both SCOM and SCVMM server to enable PRO functionality.

The following procedures can help administrators determine if SCVMM has been properly integrated with SCOM.

1. To confirm SCVMM is configured with SCOM:

    From SCVMM console:

    a. Go to Administration.

    b. Select System Center.

    c. Right-click Operations Manager Server and type in the 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 2012 Views.

    c. Select Diagram View and make sure Hyper-V VMs are visible.

Refer to the Microsoft System Center documentation to make sure of proper installation and configuration. For more information, refer to http://technet.microsoft.com/en-us/library/bb309428.aspx.

Refer to the NetApp Installation and Administration Guide and the Release Notes for OCPM to make sure of proper installation and configuration.

- [OnCommand Plug-In 3.1 for Microsoft Installation and Administration Guide](#)
- [OnCommand Plug-In 3.1 for Microsoft Release Notes](#)
- [OnCommand Plug-In 3.1 for Microsoft Cmdlet Reference Guide](#)

For more information, visit:
http://support.netapp.com/documentation/productlibrary/index.html?productID=60314.

2.3   NetApp Storage Minimal Access Control

In some IT environments, a detailed assignment of the minimal permissions is required. Table 3 describes the permissions that are needed to connect to the storage system from OnCommand Plug-In for Microsoft and gather monitoring data by using a local account on the storage system. This set of permissions is purely for monitoring of the OnCommand Plug-In for Microsoft basic functions and does not include any of the advanced features.

This local Data ONTAP account is a customized role and contains the permissions listed in Table 3.

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

Table 3) NetApp storage permissions for basic monitoring.

NetApp Storage Permissions
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

NetApp Storage Permissions
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
api-quota-report-iter-end

Example: 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
```

Sample Windows PowerShell™ command using the Data ONTAP Windows PowerShell toolkit to add a new role with the preceding capabilities:

```
New-NaRole -Role scom-user-roles -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
```

2.4   Configuring Default Action Account in SCOM

All OCPM rules and tasks run under the SCOM default action account for the management server on which OCPM is installed. OCPM requires that the default action account on this management server be correctly configured with sufficient privileges to communicate with the storage controllers using HTTP or HTTPS.

Customers should verify the default action account by navigating to Administration > Run As Configuration > Profiles and selecting Default Action Account and click Properties. In the Run As Configurations section, all Run As accounts are listed. Scan the list for the entry with Path being the name of the management server on which OCPM is installed. Verify the account name for this action account.

Figure 1 shows the profiles.

Figure 1) Profiles.
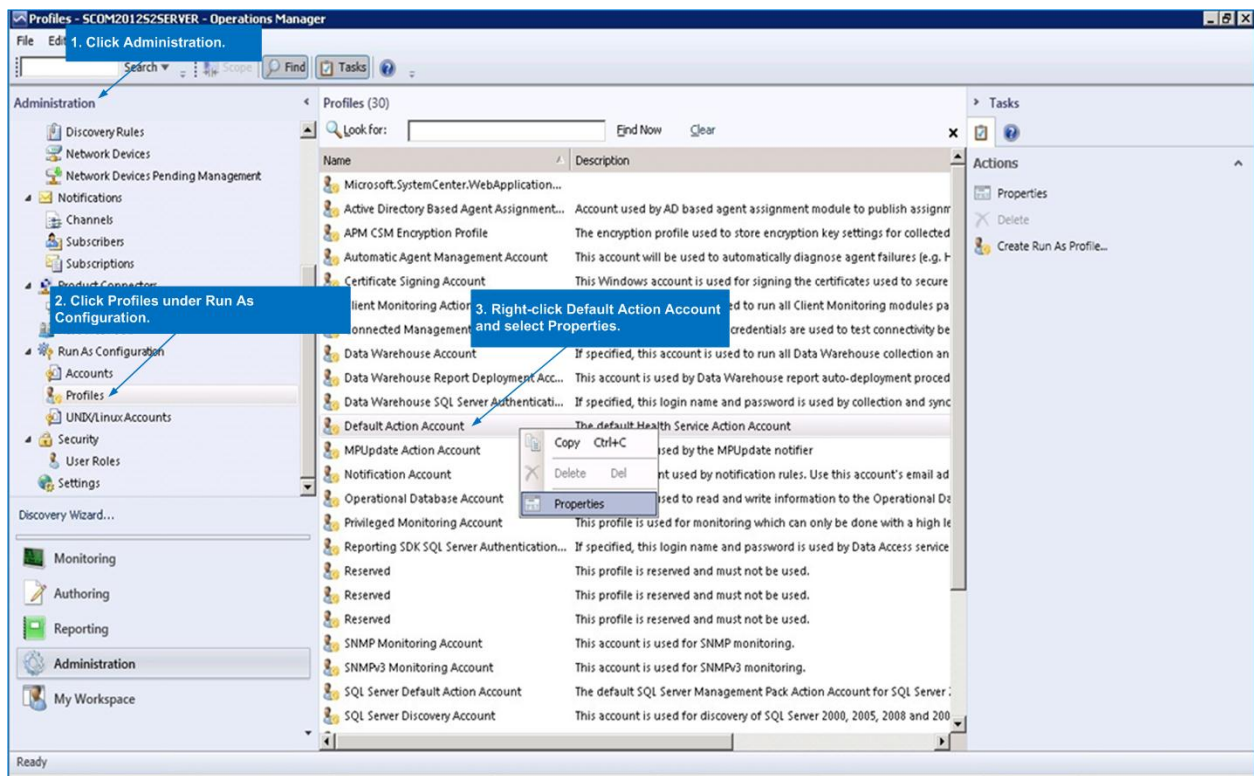
To verify this action account, click Accounts under Run As Configuration and find the corresponding action account entry. Click Properties and then make sure that proper credentials are entered.

Note: SCOM does *not* automatically update these credentials if they have been changed in the AD. Users must be sure to update the credentials themselves in SCOM.

Figure 2 shows the accounts.

Figure 2) Accounts.

2.5 OnCommand Plug-In 3.1 for Microsoft Installation

Administrators have the option of installing the entire OnCommand Plug-In 3.1 for Microsoft package or to select specific components with the custom install option.
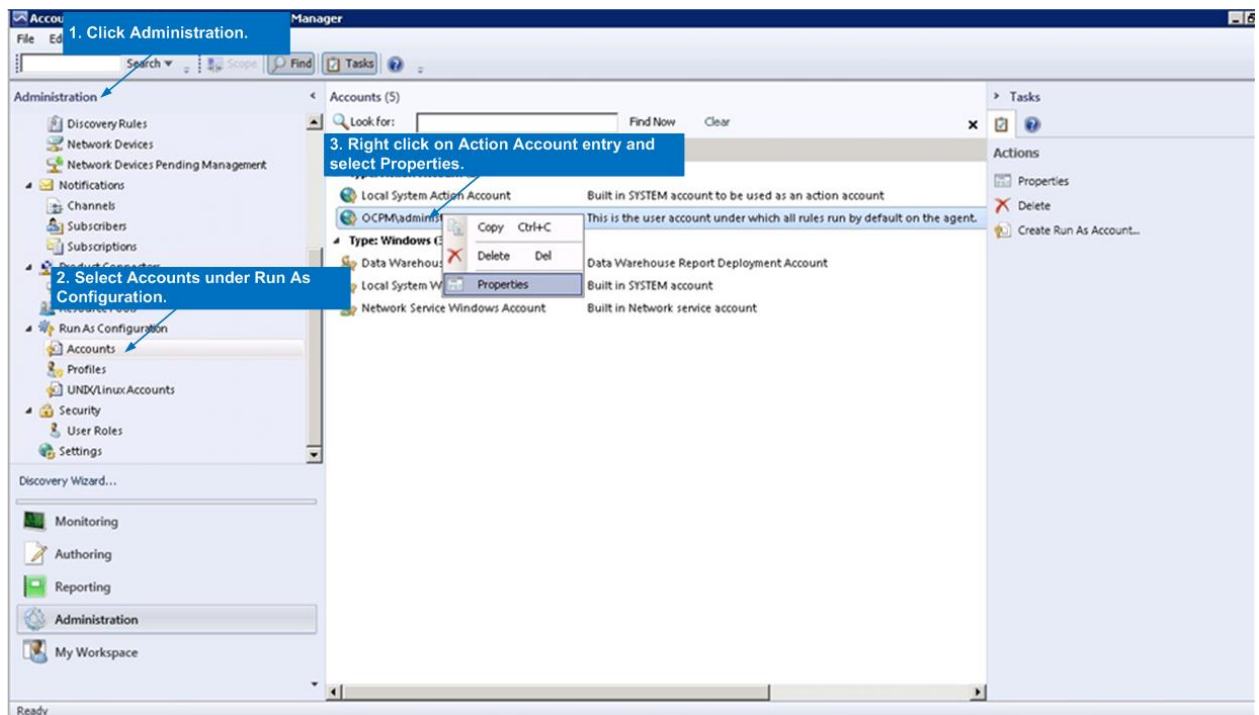
Refer to the OnCommand Plug-In 3.1 for Microsoft Installation and Administration Guide for a detailed description of the components available for installation.

During install, the installer will:

- Automatically uncheck SCOM management packs feature from feature tree if SCOM 2012 installation is not detected on system.
- Check for any missing management pack requirements and provide a list to the user. Refer to section 2.6, "Management Pack Dependencies ," for management pack dependencies.
- Automatically import management packs (management packs that have met all the requirements) into SCOM.

2.6 Management Pack Dependencies

This section lists the management pack dependencies for OCPM. Most of the Microsoft management packs can be found within the SCOM installation, and others might need to be downloaded.

For missing MPs, visit the following link to check the Microsoft management pack catalog:

http://pinpoint.microsoft.com/en-US/systemcenter/managementpackcatalog

The dependencies for OCPM management packs are:

- Data warehouse library
- Health library
- Microsoft generic report library
- Instance group library

- Network device library
- Performance library
- SNMP library
- System Center core library
- System Center Virtual Machine Manager 2008 R2 PRO library
- Windows core library

2.7   OCPM 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 must be saved in a management pack. Saving any overrides in the default management pack will cause issues with upgrades and uninstallation of OCPM. To mitigate any problems in the future, create a new management pack and save the OCPM overrides to the newly created management pack prior to enabling any overrides for OnCommand Plug-In 3.1 for Microsoft. Also, make sure that "Management Server" is the target. If Management Server does not appear, click "Change Target Type" in the Actions pane on the right.

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 than 4 hours and as a best practice recommends that this be kept at the 24-hour default.

Figure 3 shows the Data ONTAP discovery rule overrides.

Figure 3) Data ONTAP discovery rule overrides.
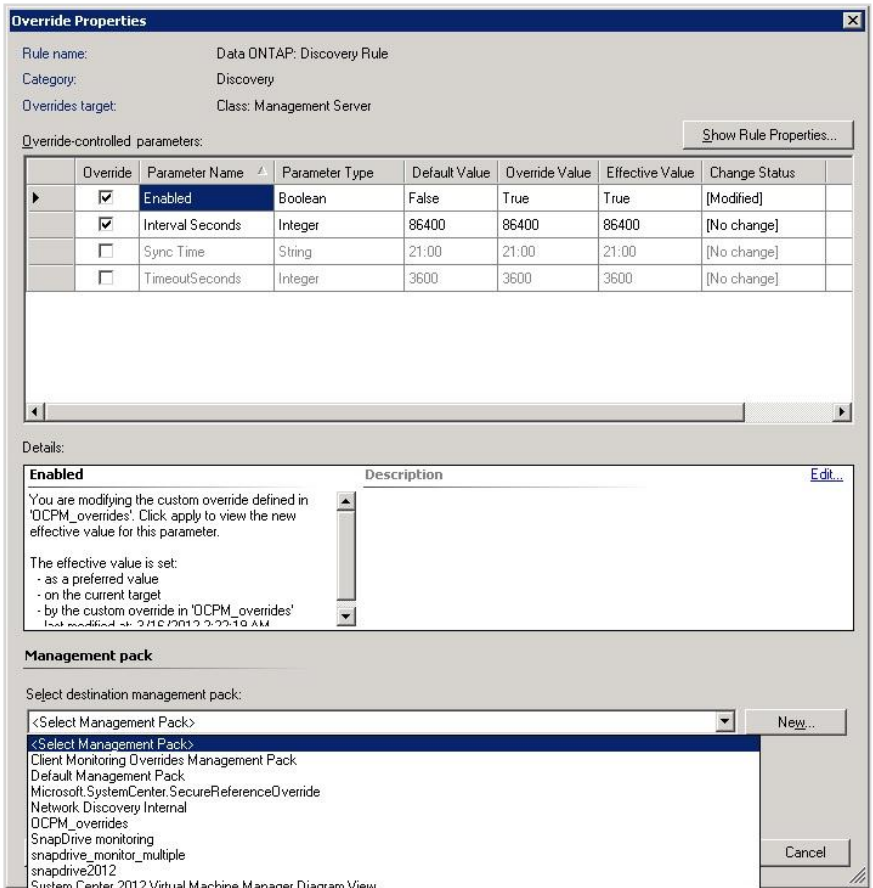
2.8 OCPM Quick Start Guide

Many steps are required when configuring SCOM and SCVMM to work with OCPM. OCPM also requires a number of steps after installing SCOM and SCVMM to function correctly. The following list shows general steps required for getting OCPM to function properly. For more specific details, refer to the OnCommand Plug-In 3.1 for Microsoft Installation and Administration Guide.

1. SCOM Installation:

   a. Review SCOM Installation Guide for requirements: http://technet.microsoft.com/en-us/library/hh205987.aspx.

   b. SCOM reporting: SCOM reporting module installation required.

   c. SCVMM: SCVMM Installation and PRO integration required between SCOM and SCVMM.

2. Make sure all installation requirements are met. Confirm proper functionality prior to proceeding with OCPM installation. For more details, refer to the Microsoft documentation for SCOM, SCVMM, or reporting at http://technet.microsoft.com/en-us/library/hh205987.aspx.

3. OnCommand Plug-In 3.1 for Microsoft Installation: Download from NetApp Support (formerly NOW®) site.

   a. Install OnCommand Plug-In 3.1 for Microsoft.

   b. Run OnCommand Plug-In 3.1 for Microsoft executable on SCOM server.

   c. Discover network devices:

   – Open SCOM, Administration, click Discovery wizard, and discover network devices.

   – Make sure SNMP is set up appropriately on SCOM server and NetApp storage prior to running network device discovery.

   – Refer to OnCommand Plug-In 3.1 for Microsoft Installation and Administration Guide for configuring SNMP.

Note: SNMP version support:

   - For Data ONTAP versions earlier than 7.3, only SNMP V1 will be supported.

   - For Data ONTAP version 7.3 and later, SNMP V3, SNMP V2C, and SNMP V1 will be supported.

   d. Add NetApp storage controller:

   – After network device discovery is complete, go to Monitoring > Discovered Inventory (make sure Discovered Inventory scope is set to Management Server), and select Data ONTAP: Add Controller.

   e. Add NetApp storage credentials:

   – Select Data ONTAP: Manage Controller Credentials (make sure user credentials has appropriate roles and capabilities assigned; see section 2.3, "NetApp Storage Minimal Access Control" for minimum roles and capabilities).

   f. Enable discovery:

   – Go to Authoring > Rules > Filter and look for Data ONTAP: Discovery Rule under Management Server (not Data ONTAP Management server). Enable PRO if installed and configured.

   – 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. Repeat both these steps. For Data ONTAP: Virtualization Discovery Rule. Follow the best practice for overrides in section 2.6 and save all OnCommand Plug-In 3.1 for Microsoft overrides to a new management pack.

   g. PRO environments:

   – Install OnCommand Plug-In 3.1 for Microsoft agent on all Hyper-V parent nodes managed by SCVMM if monitoring is required by OnCommand Plug-In 3.1 for Microsoft. Note that this is needed only if Hyper-V host has LUNs mapped with FCP.

h. Enable PRO tips:

– From SCVMM console, click Administration > General > PRO Settings > Enable PRO Tips.

## 2.9 Manual Discovery of NetApp Storage Systems

After installing OnCommand Plug-In 3.1 for Microsoft and all of the required MPs, a discovery process is required to capture all of the data to populate the SCOM console with the NetApp information. The manual process can be started by launching the Data ONTAP run discovery task. Make sure that you have followed the 2.8 "OCPM Quick Start Guide" or the OnCommand Plug-In 3.1 for Microsoft Installation and Administration Guide for proper setup of the environment prior to running manual discovery.

To manually run a discovery task:

1. Select Management Server view under Data ONTAP folder.

2. Click the Data ONTAP: Run Discovery Task to initiate the manual discovery process.

Figure 4 shows the manual discovery task.

Figure 4) Manual discovery task.
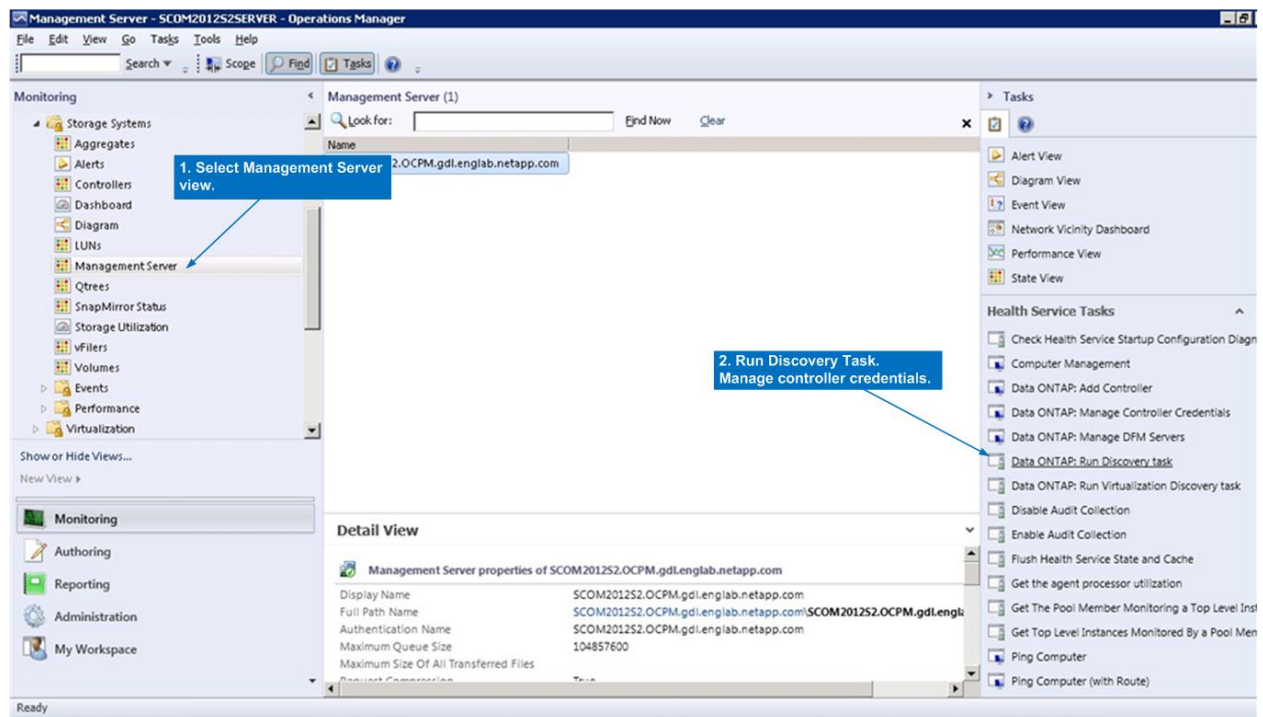
2.10 MultiStore Units (vFiler Units)

MultiStore units, also known as vFiler units, are monitored as individual objects in OCPM 3.1, including their storage, health roll-up, and utilization. vFiler unit discovery is part of the Data ONTAP discovery action. During the discovery, vFiler unit information such as volume info, qtree info, and LUN info is also gathered. Since vFiler unit's volume, qtree, and LUN path are also in the physical storage system's path, these are mapped to the corresponding aggregates.

HTTPS is the default protocol used to connect to the storage controller, but you must have Secure Sockets Layer (SSL) enabled on the controller. If SSL is not enabled, then HTTP is used to connect to the storage. If you want to connect to a vFiler unit, you must use HTTP. This option is available in the Manage Controller Credentials action.

Figure 5 shows the list of controllers and MultiStore units (vFiler units) in Credential Manager window.

Figure 5) List of controllers and MultiStore units (vFiler units) in Credential Manager window.
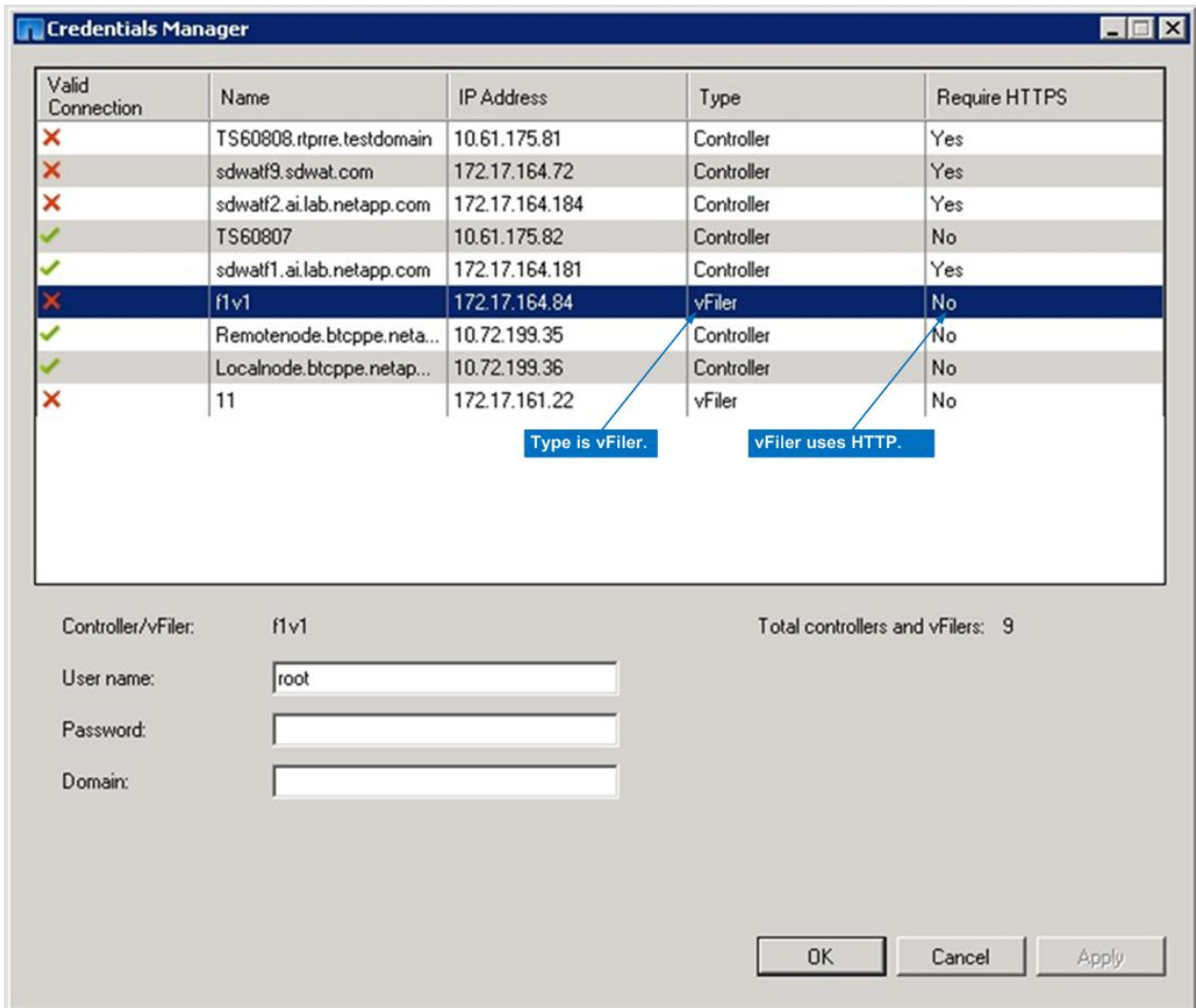
2.11 Installing Orchestrator Components

When installing and using Orchestrator components, it is important to note that the Orchestrator integration packs (OIPs) run on both the management server and all action servers. The deployment of the OIPs is managed by the Orchestrator Deployment Manager tool, but the administrator needs to be aware that the OIPs will attempt to contact the Hyper-V server designated in the runbook through Web services. This implies that there is IP connectivity on the designated port between the action servers and the Hyper-V servers you are attempting to manage.

Figure 6) OCPM-SCO integration.
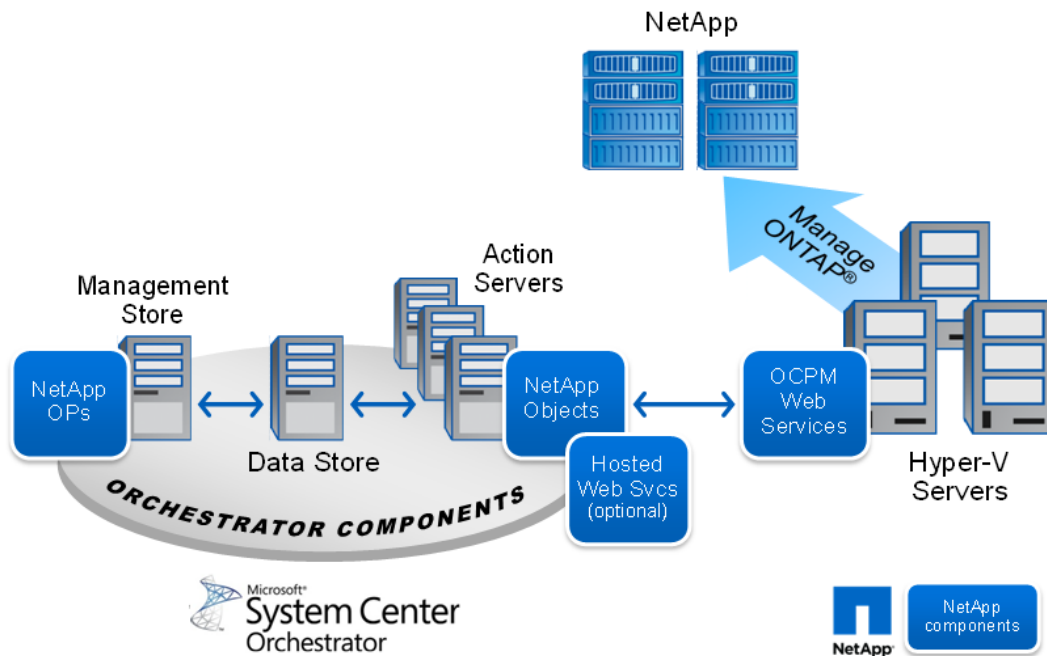
Best Practice
As a best practice, it is recommended that the OCPM VIM service be installed on all of the Hyper-V servers in your environment that you are planning to manage. This makes sure that runbooks will work consistently.
In addition, OCPM maintains a credential cache on each Hyper-V server. You will need to populate correct administrator credentials for each FAS controller that will be managed as part of your runbooks. Note that this cache is local to the Windows Server and must be updated individually. This task can be automated using the included OIPs.

2.12 Uninstalling OCPM

Custom configurations set during OnCommand Plug-In 3.1 for Microsoft setup can cause the uninstall process of OnCommand Plug-In 3.1 for Microsoft to react differently. The following steps introduce the user on how to completely uninstall OnCommand Plug-In 3.1 for Microsoft and get the SCOM environment back to its original state. To uninstall OnCommand Plug-In 3.1 for Microsoft, follow these steps:

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

| Warning |
|---|
| When trying to delete the OCPM management packs (MPs), 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 Data ONTAP stored in the default MP prior to uninstalling OnCommand Plug-In 3.1 for Microsoft. |

4. To check for Data ONTAP override values > Authoring tab > Overrides > Target where overrides were saved, and delete the Data ONTAP overrides.

Figure 7 shows the override values under the Authoring tab.

Figure 7) Override values under Authoring tab.
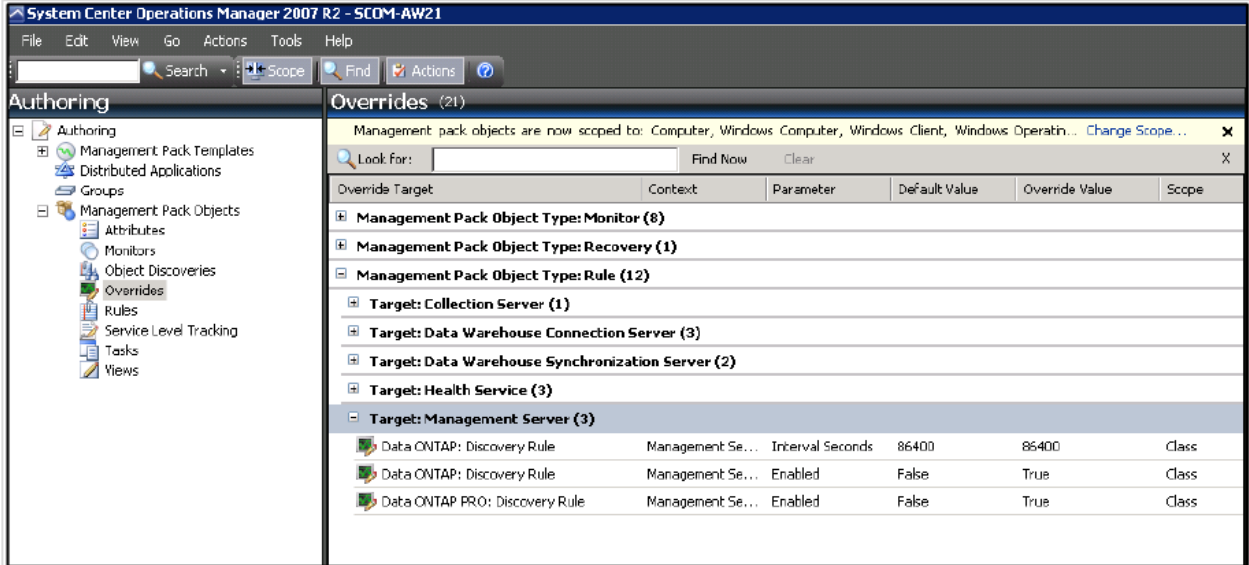
5. Delete OCPM management packs.
6. Uninstall OnCommand Plug-In 3.1 for Microsoft application from Windows control panel and reboot.

For specific steps and details, refer to:

- [OnCommand Plug-In 3.1 for Microsoft Installation and Administration Guide](#)
- [OnCommand Plug-In 3.1 for Microsoft Release Notes](#)

3 OnCommand Plug-In 3.1 Microsoft Alerts, Monitoring, and Views

OnCommand Plug-In 3.1 for Microsoft offers various alerts, monitoring options, and views for your NetApp storage array. After installing and discovering all objects within the environment, information on LUNs, qtrees, volumes, aggregates, and other detailed views is displayed. These various tools allow you to efficiently manage your NetApp storage systems.

3.1 Alerts

The alerts view allows administrators to instantly view and report problems within their NetApp environment.

Figure 8 shows the locations of the important details of each alert.

Figure 8) Alerts window.
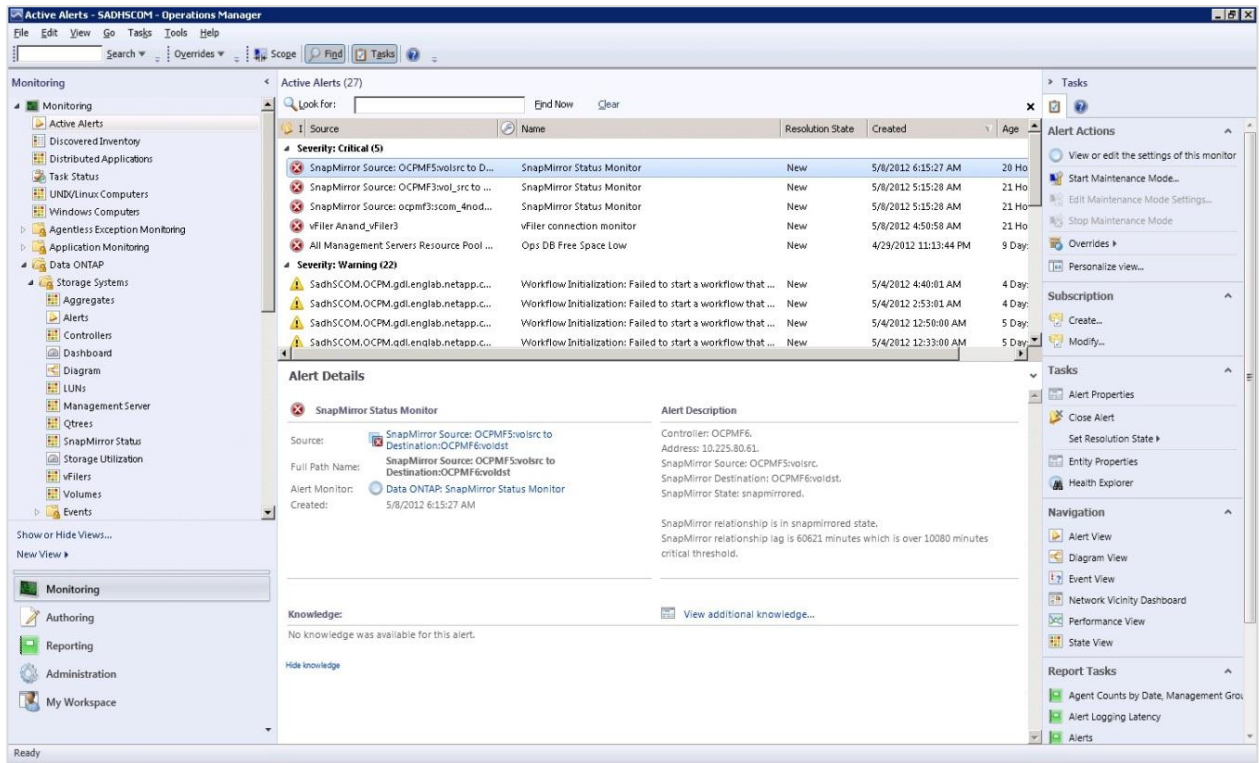
3.2 Tuning, Monitoring, and Alerting

In larger deployments where OCPM monitors more than 10 controllers, NetApp recommends that the user tune OCPM monitoring rules for performance reasons. Users might intend to reduce the frequency of specific rules depending on the requirements of their environments by setting the appropriate overrides. Users might also want to turn off specific rules if they do not want to receive alerts for those objects. In large deployments, it is recommended to turn off disk monitoring rules. Disk-related alerts will still be collected at the aggregate level.

4 Data ONTAP Virtualization Management Pack

The OCPM 3.1 includes a Data ONTAP virtualization management pack with all virtualization objects and their related storage discovered and monitored. This includes the Hyper-V host, Hyper-V LUN, and Hyper-V VHD objects.

Table 4 lists all the Data ONTAP virtualization management pack objects.

Table 4) Data ONTAP virtualization management pack objects.

Data ONTAP Virtualization Objects	Description
Hyper-V host	This object represents any Hyper-V host in SCVMM that has at least one NetApp LUN (monitored by SCOM) mapped to it whether the mapped LUN(s) has VHDs or not.
Hyper-V LUN	This object represents a NetApp LUN that is mapped to a Hyper-V host object as a Windows disk or CSV. In the case of CSVs, there will be one Hyper-V LUN object for each host that maps

Data ONTAP Virtualization Objects	Description
	to this LUN. If the LUN is not a CSV, the cluster name and CSV name properties are displayed as "N/A."
Hyper-V virtual machine (VM)	This object represents all the virtual machines that are associated with VHDs on a NetApp LUN.
Hyper-V virtual hard disk (VHD)	This object represents a virtual hard disk (VHD) that resides on a NetApp LUN. During virtualization discovery all VHDs, whether attached to a VM or not, will be discovered as Data ONTAP virtualization: Hyper-V virtual hard disk instances.

4.1 Virtualization Discovery

Data ONTAP virtualization discovery finds NetApp storage mapped to all of the Hyper-V hosts listed in SCVMM, including Hyper-V hosts and NetApp LUNs mapped to them, Hyper-V virtual machines, and Hyper-V virtual hard disks. In some cases, the Data ONTAP virtualization discovery requires the OnCommand discovery agent on the Hyper-V host.

Perform the following steps to invoke the Data ONTAP virtualization: discovery rule manually.

1. Navigate to the Management Server view under the Data ONTAP node.

2. Click the Data ONTAP Virtualization: Run Virtualization discovery task on the management server.

This rule targets the management server and has a default interval of four hours and a default timeout of one hour.

The following situations determine if the OnCommand discovery agent is required to be installed on a Hyper-V host:

* The Hyper-V host is mapped to LUNs residing on a NetApp controller running any version of Data ONTAP earlier than 7.3.1.

* The Hyper-V host has Fibre Channel mapped LUNs.

* The Hyper-V host has dedicated LUNs mounted using volume GUID and the SCOM server is not running Windows 2008 R2.

4.2 Detecting LUN and VHD Misalignments

LUN and VHD misalignments can degrade the storage controller's performance. It is crucial to detect and correct LUN and VHD misalignments to improve storage performance. In most cases, a file system is installed in a partition in a VHD file. The partition should align with the LUN to achieve maximum read and write performance. There are fixed VHDs, dynamic VHDs, and differencing VHDs. The partition can be MBR or GPT partition. The GPT partition is also checked for misalignment. In case of GPT, however, only the first four primary partitions of GPT are checked for misalignment issues since it is very uncommon for customers to have VHD with more than a couple of primary partitions. If any partition is misaligned, the VHD is marked as misaligned. However, only primary partitions are checked for misalignment issues. The system or reserved partitions in a VHD are not checked for misalignment. NetApp LUNs should be partitioned with a single primary partition.

For dynamic or differencing disks, NetApp cannot guarantee alignment, and so these are not checked for misaligned partitions. However, a warning is generated to indicate the type of disks detected.

The misalignment detection does not require a VM to be shut down. Detection is seamless to the Hyper-V VMs.

For VHD alignment checking:

- Remote Windows PowerShell needs to be enabled on these hosts.

Visit http://technet.microsoft.com/en-us/library/dd819498.aspx for instructions on how to enable these on remote Hyper-V hosts.

It is important to note that:

- VHD alignment checking for VHDs on LUNs mounted with volume GUIDs is not supported.
- For VHD for which no partition information is available, the alignment status is marked as unknown.
- The misalignment check cannot automatically fix misalignment issues.

The misalignment check can be invoked as follows:

- A rule to run on a schedule.
- Tasks on virtualization LUN view and host view can invoke misalignment detection on LUN level and on Hyper-V host level.

Figure 9 shows a VHD misalignment alert in the SCOM console.

Figure 9) VHD misalignment alert.
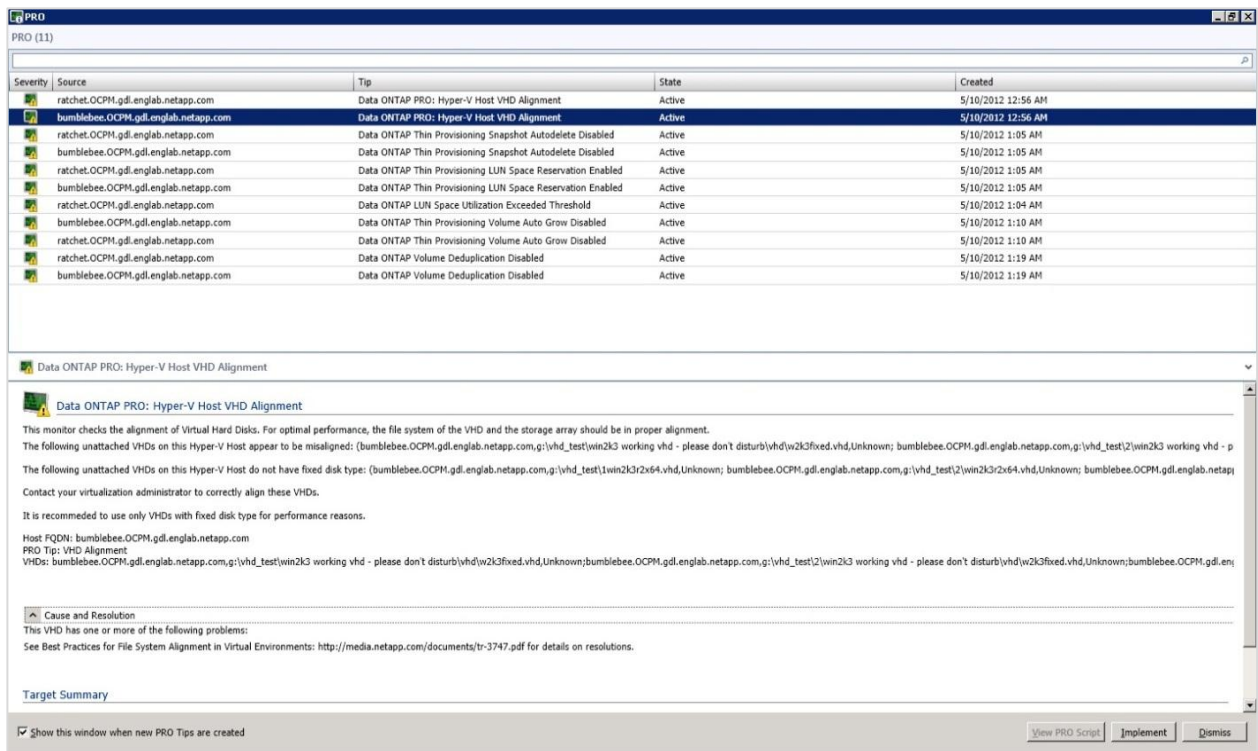
5 OnCommand Plug-In 3.1 for Microsoft Reporting

OnCommand Plug-In 3.1 for Microsoft includes a reporting management pack so you can view reports on various aspects of your NetApp storage. You must configure System Center Operations Manager 2012 for reporting to use Data ONTAP reports management pack.

For more information on setting up reporting for SCOM, visit Microsoft TechNet.

5.1 Custom Reporting

The Data ONTAP reporting management pack in OCPM includes various prepackaged reports. You can also create custom reports for specific NetApp objects by performing the following steps.

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 `ontap` as keyword for available report options.

Figure 10 shows the custom reporting option.
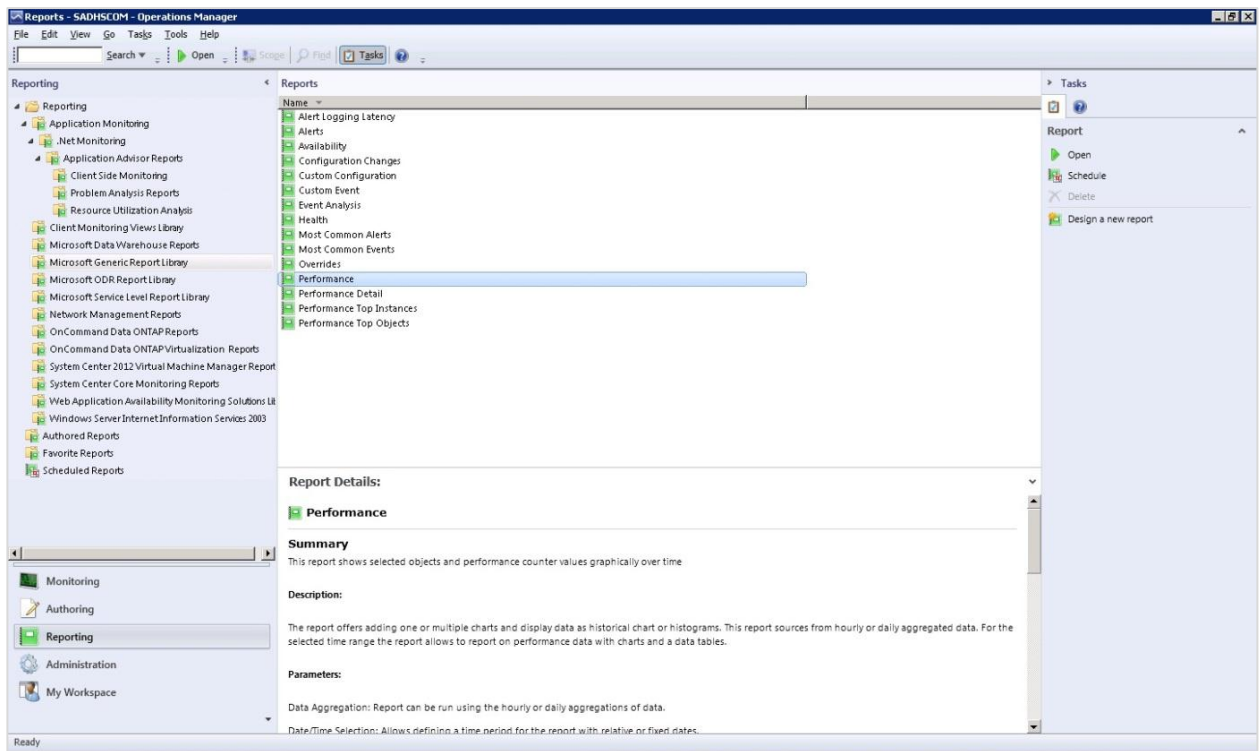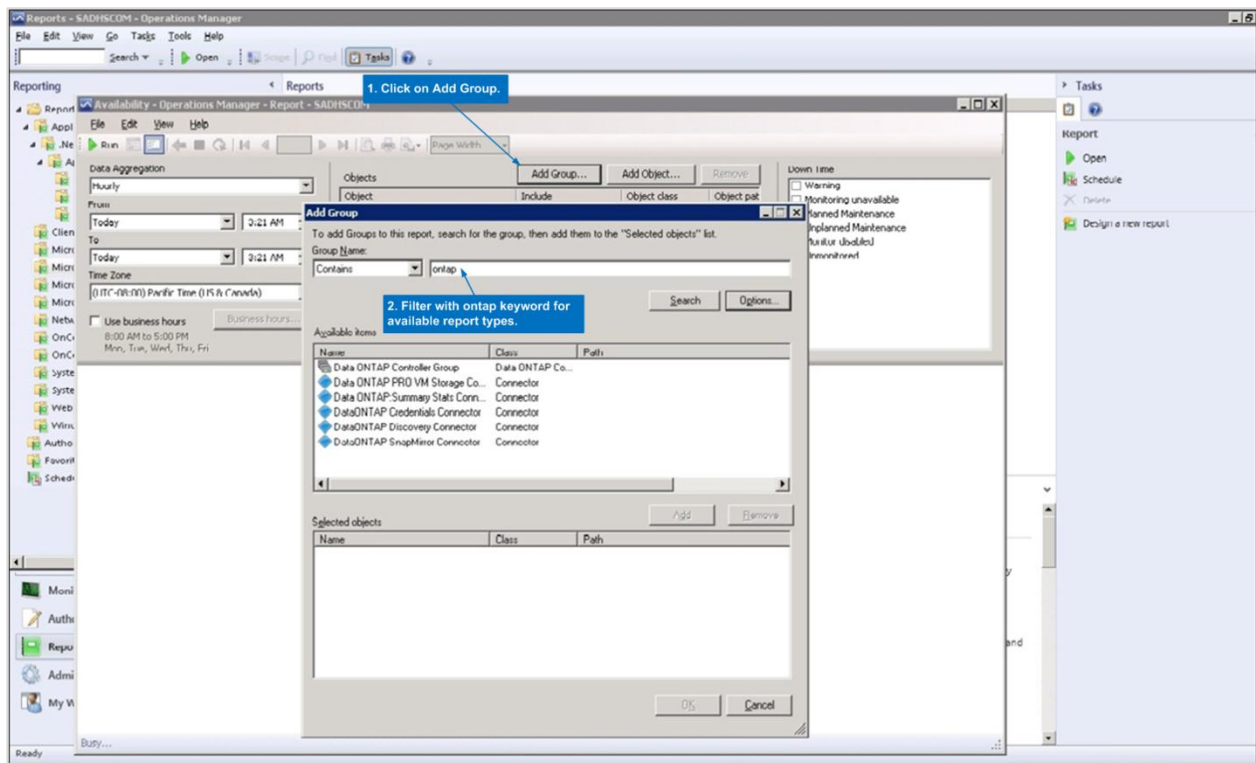
Figure 10) Custom reporting.

Figure 11 shows how to create custom reports for Data ONTAP inventory.

Figure 11) Creating custom reports for Data ONTAP inventory.

6 OnCommand Plug-In 3.1 for Microsoft PRO Tips

PRO tips are a type of alert that you can use with System Center Virtual Machine Manager (SCVMM) to notify when storage-related problems occur in your virtual environment. They can also be enabled to automatically fix many of those problems. You must have an event log subscription to the SCVMM event log to receive problems related to virtual machines. When OnCommand Plug-In for Microsoft receives these events, PRO rules are triggered in the management pack to immediately generate PRO tips.

PRO tips are part of the OnCommand Plug-In for Microsoft management pack. The PRO tips button in the SCVMM toolbar displays the number of tips that are currently available. Optionally, PRO tips can also be configured to display in a pop-up window whenever a new tip is added.

In the case of a highly available SCOM setup, make sure that the SCVMM server is connected to the SCOM server that has the RMS emulator enabled to receive the PRO tips on the SCVMM pane. Use `powershell cmdlet Set-SCOMRMSEmulator` to move the RMS emulator to the specified management server.

6.1 Volume Space Utilization PRO Tip

When implemented, this PRO tip will increase the size of a volume. There are cases when the size of a volume cannot be automatically increased: for example, when the aggregate does not have sufficient free space or because the volume is the source of a SnapMirror® relationship (growing the source volume larger than the destination volume would inhibit replication updates). Clicking the implement button for these situations will not change the size of the volume.

Figure 12 shows the volume space utilization PRO tip.

Figure 12) Volume space utilization PRO tip.
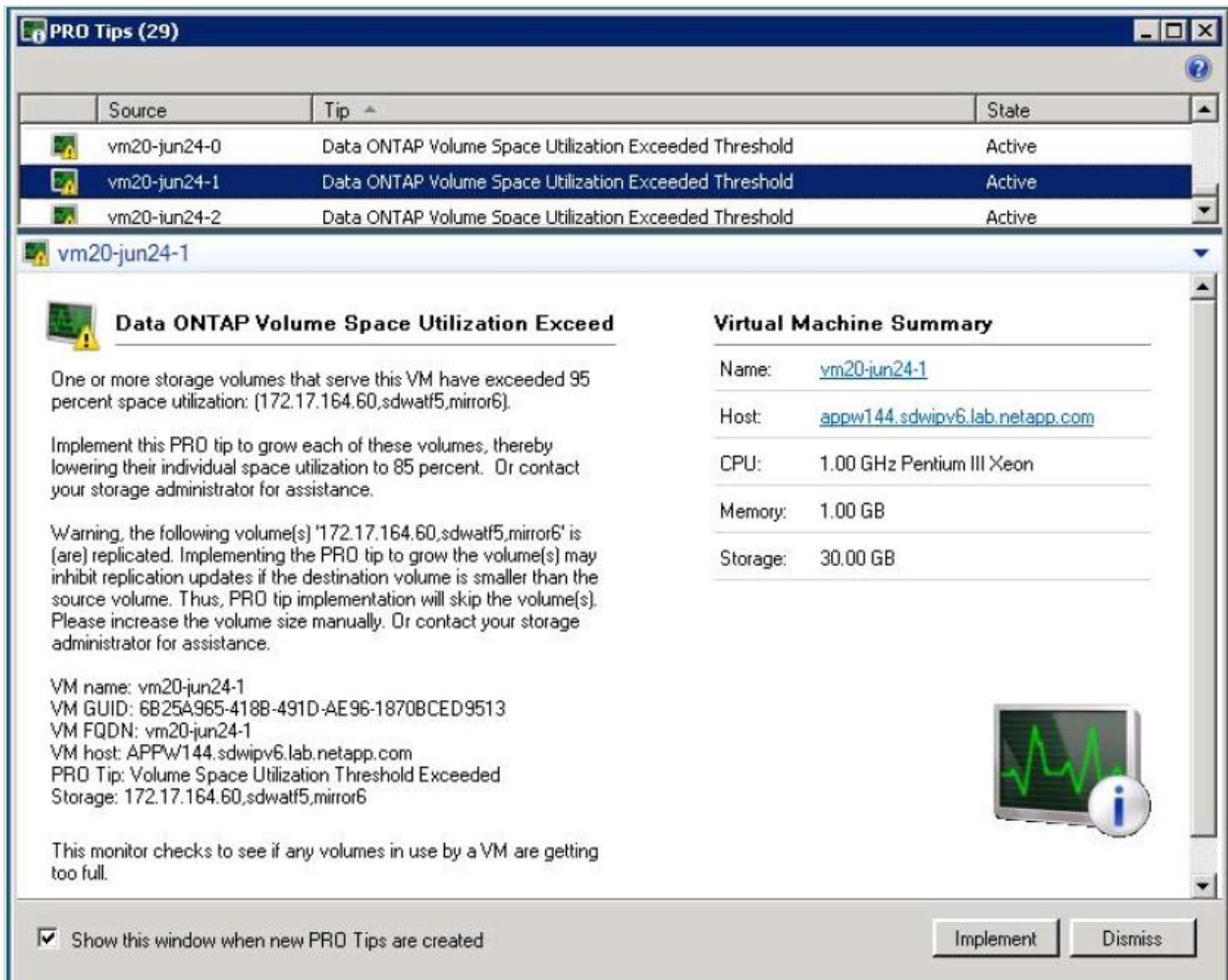
6.2 Best Practices for Snapshot Autodelete PRO Tip

The thin-provisioning Snapshot™ autodelete PRO tip checks if Snapshot autodelete is 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 or SnapManager® for Hyper-V. Enabling Snapshot autodelete on these volumes might disrupt the other protection mechanisms and cause issues with consistency.

Figure 13 shows the Snapshot autodelete PRO tip.

Figure 13) Snapshot autodelete PRO tip.
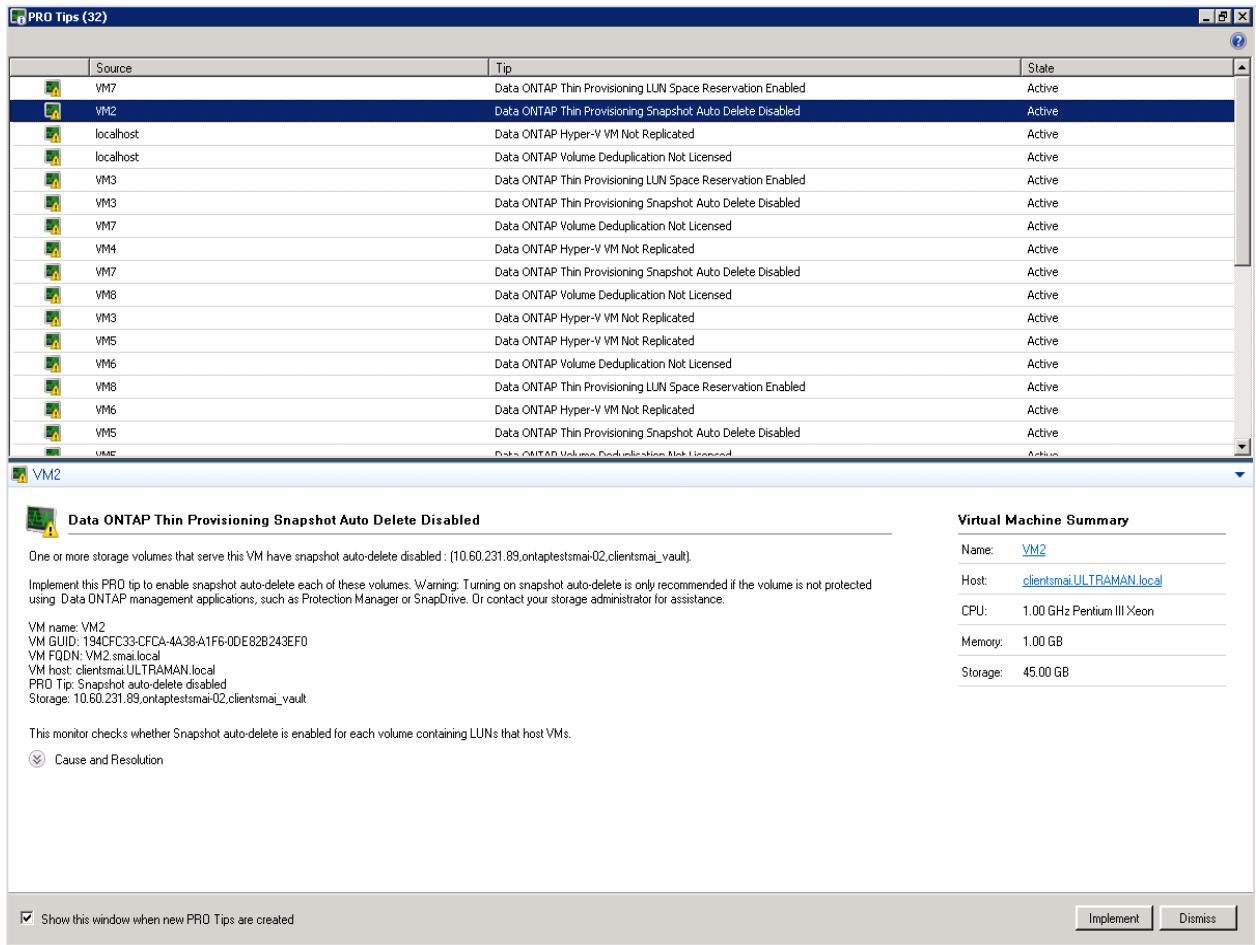
6.3 Best Practices for LUN and VHD Alignment PRO Tip

PRO tips are generated at the Hyper-V host level for misaligned LUNs or misaligned unattached VHDs. For attached misaligned VHDs, the PRO tips are generated at the Hyper-V VM level. These PRO tips cannot automatically fix misalignment issues. Instead, the PRO tips include references to methods for fixing them.

Figure 14 shows the VHM misalignment PRO tip.

Figure 14) VHD misalignment PRO tip.

7 OnCommand Plug-In 3.1 for Microsoft Rapid Provisioning and Cloning

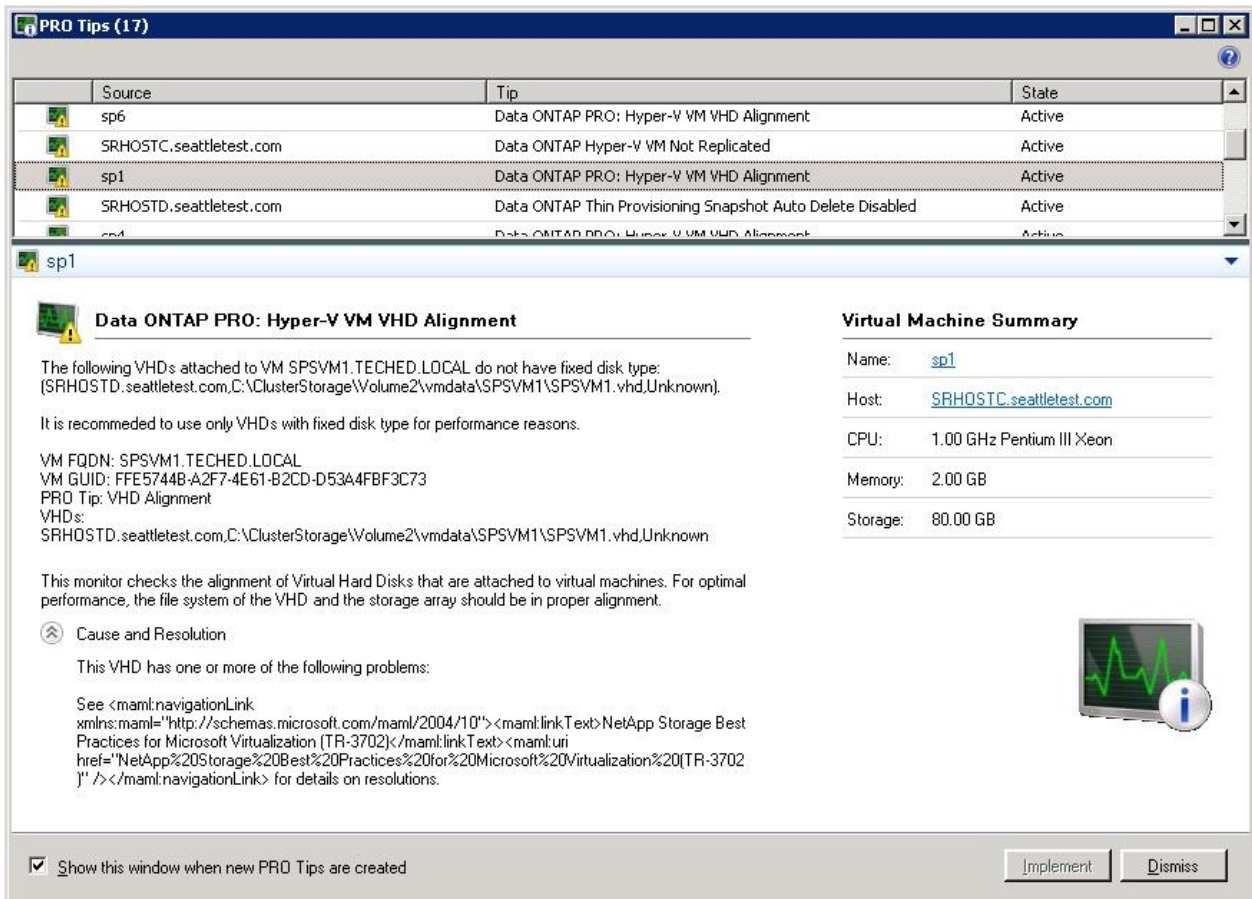The rapid provisioning and cloning cmdlets install separately from the core management packs and have no dependency on them. The cmdlets and associated Orchestrator integration packs (OIPs) allow for basic provisioning tasks (create storage, present storage, remove storage, and so on) and cloning operations (clone VM, clone file, and so on). In addition, the rapid provisioning and cloning cmdlets are used with Microsoft System Center Virtual Machine Manager (SCVMM) to dramatically speed up provisioning of Hyper-V virtual machines and minimize storage requirements. For more information on the provisioning and cloning cmdlets, see the OnCommand Plug-In 3.1 for Microsoft Windows PowerShell Cmdlet and Orchestrator Activity Reference Guide.

7.1 Cmdlets and User Access Control

For systems with UAC enabled, Windows PowerShell will not be able to correctly load and execute the OCPM cmdlets unless you manually raise your permissions level using the Run as Administrator option. Either disable UAC or open the cmdlet window using Run As Administrator.

Similar to any Windows PowerShell cmdlet, the OCPM cmdlets provide help using the Get-Help cmdlet. Full or partial help is available as normal in Windows PowerShell. Additional help can be found in the OCPM command reference guide that is shipped with the OCPM installer.

7.2   Sub-LUN Cloning Features and Limitations

OCPM provides several methods for accessing sub-LUN cloning. This function is called as part of the New-OCClone cmdlet and can be accessed directly using the New-OCCloneFile cmdlet. These same features can be accessed using the Orchestrator rapid provisioning OIP. In any of these cases, the same limitations and capabilities apply.

Sub-LUN cloning refers to the ability of a FAS series controller to "clone" a single file within a mounted LUN on a Windows host or guest. This operation is performed by the OCPM VIM service and requires that the source and destination LUN be mounted on the local host. When using the New-OCClone cmdlet, the new LUN is managed automatically. However, when using the New-OCCloneFile cmdlet (or associated clone NTFS file OIP), the source and target files must both reside on NetApp LUNs from the same volume that are mounted on the same Windows host or guest.

While this technology is truly revolutionary, it does come with some caveats. When using these features, make sure that you keep these restrictions in mind. Sub-LUN cloning utilizes the same block reference count feature as deduplication. If the Data ONTAP block reference count limit has been exceeded due to deduplication, this will cause Data ONTAP to *copy* the affected block rather than *clone* the block. For all versions of Data ONTAP earlier than 8.1, this maximum is 255. For large fixed sized VHDs, this could involve copying tens of thousands of blocks and result in cloning delays of up to an hour. When deploying OCPM's rapid provisioning features, be sure to check to see if the source volume has exceeded its maximum reference count or use a volume that is not deduplicated as a clone source. (Use priv set diag; sis stat -lv /vol/test to view current reference counts.) NetApp recommends upgrading your FAS controllers to Data ONTAP 8.1 or higher if at all possible for best possible cloning performance.

In OCPM, MBR partitions are not supported. GPT is the default partition type for Windows Server 2008 R2, but systems that have been upgraded from older Windows versions might still have MBR partitions.

In OCPM, only fixed VHDs are supported as the source VHD for cloning. Dynamic and/or differencing VHDs cannot be cloned. This is consistent with the [NetApp Hyper-V Best Practice Guide](#) and with Microsoft best practice to utilize only fixed VHDs for production VMs (http://technet.microsoft.com/en-us/library/dd440865(WS.10).aspx#fixed).

Because only the controller node for a CSV has actual ownership of the underlying LUN, you can only perform clone operations from the controller node of a cluster. You can check for CSV ownership in Windows PowerShell by using the following command:

```
Get-ClusterSharedVolume
```

7.3   Best Practices for the New-Clone Cmdlet

The New-OCClone cmdlet operates in one of two modes. Either it can clone a single VM on a Hyper-V host, or it can create a new VM from an SCVMM template. In either case, New-OCClone will perform a sub-LUN clone operation of the VM's VHD file first and then create a new VM using this cloned file.

In the case of SCVMM templates, it is very important that the template be configured correctly. The cmdlet should be executed on the host, which has the VHD share. The target machines should be managed by the SCVMM server. In local template cloning the VHD share should be on the target machine (local). HA VM will be created in a clustered disk in a clustered environment. Note that if server switch is not specified by default, it takes the local cluster name.

Table 5 lists the supported configuration for a clustered environment.

Table 5) Supported configuration for a clustered environment.

lNew Shared	Mount point is specified	nc=1	Create a shared disk on the mount point specified and clone into it	Supported
	No mount point is specified	nc>1	Multiple copy of template cloning into multiple new different shared disks	Supported
	New mount point/all in single LUN is specified	nc>1	Multiple copy of template cloning into a single shared disk	Not supported
Existing Shared	Existing mount point is specified	nc=1	Template cloning into a single shared disk	Not supported
	Existing mount point is specified	nc>1	Multiple copy of template cloning into a single shared disk	Not supported
New CSV	CSV is specified	nc=1	Creates a CSV disk and clone into it	Supported
	CSV and all in single LUN are specified	nc>1	Multiple copy of template cloning into a single CSV disk	Supported
	CSV is specified and all in single LUN is not specified	nc>1	Multiple copy of template cloning into multiple new different CSV disks	Not supported
Existing CSV	Existing mount point is specified	nc=1	Clone into the specified CSV	Supported
	Existing mount point is specified	nc>1	Multiple copy of template cloning into a specified CSV disk	Supported

In case of a dedicated environment, non-HA VM will be created in a dedicated disk. If server is not specified, it assumes the local host name.

Table 6 lists the supported and unsupported configurations for a dedicated environment.

Table 6) Supported and unsupported configurations for a dedicated environment.

New Dedicated	New mount point/no mount point with all in single LUN	nc=1	Creates a dedicated disk and clone onto it	Supported
	New mount point/no mount point with all in single LUN	nc>1	Multiple copy of template cloning into a single dedicated disk	Supported
Existing Dedicated	Existing mount point is specified	nc=1	Clones into the specified dedicated disk	Supported
	Existing mount point is specified	nc>1	Multiple copy of template cloning into a single dedicated disk	Supported

In remote template cloning, the VHD share can be on any node. It is not mandatory to place the VHD share on the target machines. Remote template cloning on an existing clustered/dedicated disk is not supported.

Table 7 lists the supported and unsupported configurations for remote cloning.

Table 7) Supported and unsupported configurations for remote cloning.

New Shared	Mount point is specified	nc=1	Create a shared disk on the mount point specified and clone into it	Supported
	No mount point is specified	nc>1	Multiple copy of template cloning into multiple new different Shared disks	Supported
	New mount point/all in single LUN is specified	nc>1	Multiple copy of template cloning into a single shared disk	Not supported
New CSV	CSV is specified	nc=1	Creates a CSV disk and clones into it	Supported
	CSV is specified	nc>1	Multiple copy of template cloning into multiple new different CSV disks	Not supported
	CSV and all in single LUN are specified	nc>1	Multiple copy of template cloning into a single CSV disk	Not supported
New Dedicated	New mount point/no mount point with all in single LUN	nc=1	Creates a dedicated disk and clone into it	Supported
	New mount point/no mount point with all in single LUN	nc>1	Multiple copy of template cloning into a single dedicated disk	Supported

In the case of Hyper-V VMs, the source VM must be turned off for the clone operation to complete. This is because the metadata describing the VM is not available to the New-OCClone cmdlet when it is running and we cannot clone a file that is currently opened by Hyper-V manager.

Depending on the options chosen in the command, the new VHD will be placed on a new LUN or be added to an existing LUN. In either case, the target Hyper-V host must already have connectivity to the storage controller that owns the source LUN. If a new LUN is created as part of this operation, it will automatically be connected to the Hyper-V host.

7.4 Best Practices for Using "Create LUN by Size" Object in SCO 2012

"Create LUN by size" object allows creating LUNs of different OS type.

Following is the configuration that supports each LUN type:

- **Image.** When the host OS is not specified in the list but if it is listed as a supported OS, then use as "image"
- **Windows_gpt.** Windows Server 2008 > physical server > without Hyper-V with SnapDrive® installed
- **Hyper_v.** Windows Server 2008 > Hyper-V server > physical disk with SnapDrive installed
- **Windows_2008.** Windows Server 2008 > physical server > without Hyper-V without SnapDrive installed

    Windows Server 2008 > Hyper-V server > physical disk without SnapDrive installed

Refer to the LUN type table after visiting the following link:

http://www.netapp.com/us/communities/tech-ontap/tot-hyperv-best-practices-0911.html

7.5 Best Practices for Rapid Deployment

When configuring rapid deployment, you need to consider both your business requirements and the underlying technical restrictions of the cloning technology in Data ONTAP. Since you can only clone within a single FlexVol® volume and you must have both the source and destination mapped to a single

Windows Server instance, the optimal use case is to have every CSV preprovisioned with your template VHDs prior to provisioning VMs.

In this case, the best practice is to create a single, gold master CSV. This CSV will contain your gold master template VHD files. When you provision a new CSV, you should always use a FlexClone® volume of this gold master. This makes sure that all CSVs will always have the required templates local to the CSV. It also makes sure that both source and destination will always remain within a single FlexVol volume. If you have a large number of templates, you can create multiple CSVs within a single FlexVol volume. In this case, the additional template VHDs will be deduplicated automatically if you have dedupe enabled on the volume.

In this way, you can have both the advantage of "local" templates without taking up additional space for repetitive template VHDs.

You can create the clone in Windows PowerShell using a script similar to the following:

```
New-NaLunClone -ClonePath <path> -ParentPath <path> -Unreserved -ParentSnapshot <snapshot>
Set-NaLunSignature -GenerateRandom –Path <path>
Set-NaLun -Path <path> -Online
Connect-OCStorage -StoragePath <path> -ClusterSharedVolume
```

Note that in the preceding script, we create a new disk signature before presenting the LUN to the cluster. This is required because Windows failover cluster will not allow you to mount two disks with identical disk signatures to the same cluster.

After the CSV is created and mounted, you can begin to provision VHDs. Note that the standard OCPM new-OCClone cmdlet assumes that the SCVMM library is local to the Hyper-V server. If this is not the case, you can manually create the clone, then call SCVMM to create the VM.

The following Windows PowerShell script is a sample using SCVMM cmdlets, and you can create a similar script using the following OCPM cmdlets.

```
$SCVMMHost = <<VMM SERVER NAME>>
$VMMServer = Get-VMMServer $SCVMMHost;
$CPath = <<TARGET VHD>>
$TPath = <<TEMPLATE VHD>>
$TargetHost = <<Target Host>>
$TemplateName = <<VMM Template Name>>
$JobGroupID = [guid]::NewGuid()
New-OcCloneFile $TPath $CPath

Move-VirtualHardDisk -IDE -BUS 0 -LUN 0 -Path $CPath -JobGroup $JobGroupID

$JName = <<Name for Job and new VM>>
$VMPath = <<Path for VM>>

new-vm -name $JName -Path $VMPath -Template $TemplateName -VMHost $TargetHost -
UseLocalVirtualHardDisks -JobGroup $JobGroupID -StartVM -ComputerName $JName -RunAsynchronously
```

8 Disaster Recovery

OCPM provides the capability to move virtual machines from one Hyper-V cluster to another for disaster recovery. This feature is heavily dependent on NetApp SnapMirror capability. For more information about SnapMirror, see TR-3326 SnapMirror Sync and SnapMirror Semi-Sync Overview and Design Considerations. For more information on OCPM disaster recovery feature, refer to the following documents:

- OnCommand Plug-In 3.1 for Microsoft Installation and Administration Guide
- OnCommand Plug-In 3.1 for Microsoft Release Notes
- OnCommand Plug-In 3.1 for Microsoft Cmdlet Reference Guide

8.1 Configuring OCPM Disaster Recovery

Prior to failing workloads over to your secondary site, the disaster recovery process must be configured, and the underlying storage must be configured correctly. When designing your Hyper-V deployment, care should be given to identify what VMs need to be replicated to the secondary site. As a best practice, NetApp recommends segregating workloads into multiple classes of service. Service levels are often expressed in tiers. In the following example, the service levels are expressed as gold, silver, and bronze service tiers. Each tier will be associated with RPO and RTOs and the associated storage features to achieve these RPO and RTOs.

Table 8 lists sample service levels.

Table 8) Sample service levels.

Service Tier	RPO	RTO	Redundancy	Backup
Bronze	24 hours on site	1 hour on site	Single site only, no DR site	Daily Snapshot copy, 1-week retention
Silver	1 hour on site, 24 hours DR	10 minutes on site, 1 hour DR	DR with daily replication	Hourly Snapshot copy, 30-day retention
Gold	0 on site, 10 seconds DR	0 on site, 10 minutes DR	DR with semi-sync replication	Hourly Snapshot copy, 30-day retention

Table 8 is a sample only. Each organization will need to discuss internal and external SLOs so that the service tiers established in the system reflect actual business requirements. Once service tiers are established, storage infrastructure can be aligned. In our case, this implies a volume-level configuration and mapping. Because operations such as SnapMirror and dedupe are performed at the volume level, it is recommended that each volume be assigned a service tier, and then LUNs and VMs can be provisioned against volumes in the correct service tier.

After finalizing your Hyper-V design, establish SnapMirror relationships and schedules that align to your RPO agreements. These relationships will determine the amount of data that is replicated and the replication frequency. OCPM does not manage these relationships for you.

Once these relationships are established, begin to provision Hyper-V VMs into your cluster. After the VMs have been provisioned, but *before* they are put into production, you can use the New-OCDRPlan cmdlet to generate your DR plan. A DR plan is an XML file that specifies the VM configuration and layout that will be created on the secondary site when you attempt to use the Invoke-OCDRFailover cmdlet or associated cmdlets.

By default, this file is placed into C:\ProgramData\OnCommand\MS_Plugin. This directory is also shared as MS_Plugin by the OCPM installer for ease of use. This xml file must be copied or replicated to the secondary site at configuration time. Without it, restoration cannot be performed. The simplest way to do this is to place it into a container (such as a CIFS share) that exists on the primary that will be replicated to the secondary.

Note that the VMs on the cluster must be offline before running the New-OCDRPlan cmdlet. For this reason, we recommend running the cmdlet *before* the VMs are placed into production. This will prevent you from having to schedule an outage to create the DR plan.

In OCPM 3.1, mixed mode Hyper-V hosts are not supported. This means a primary setup containing both dedicated and cluster VMs is not supported. You can confirm this by comparing Hyper-V Manager to Cluster Manager. If any VMs are listed in Hyper-V Manager that are not listed in Cluster Manager, the New-OCDRPlan cmdlet will fail.

8.2   Best Practices for Disaster Recovery

The best practice for disaster recovery is:

Best Practice
When implementing a planned failover, it is recommended that you gracefully shut down the VMs on the primary site before failing over to the secondary site. This will make sure that the guest operating systems come up correctly and will eliminate any problems with open files or corrupt application databases.

Once machines are shut down, it is very important to *update* the SnapMirror relationship prior to running the restore process. This will make sure that the final changes to the VHDs are committed to the secondary site before you attempt to restore them. Again, this will eliminate any issues with open files or corrupt application databases. Once the update is complete, you need to quiesce the link to make sure that no additional transactions are committed.

Following are the Windows PowerShell commands that need to be used:

```
Invoke-OCDRMirrorUpdate
Get-OCDRMirrorStatus
Invoke-OCDRMirrorQuiesce
```

Note: The Invoke-OCDRMirrorUpdate command is asynchronous. This means that the command might still be running in the background. You must wait until the update is complete before running the Invoke-OCDRMirrorQuiesce cmdlet. You might need to run Get-OCDRMirrorStatus several times before the status returns to idle.

In the case of an unplanned failover, it is not possible to update the mirror or gracefully shut down the VMs, and additional application recovery steps might need to be taken. For database-driven applications, such as SQL Server or Exchange Server, it is recommended that additional application-specific backups be performed with tools such as SnapManager for Exchange or SnapManager for SQL Server. Once the data volumes are restored to the secondary site, the applications can be restored from Snapshot as would normally be done. SnapMirror replicates all volume Snapshot data along with all other data contained in the volume as part of its normal replication. In most cases, the virtual machine will simply restart with no corrective action, but a second layer of protection is recommended to protect against database corruption.

9   OnCommand Plug-In 3.1 for Microsoft Troubleshooting

Refer to the troubleshooting section in OnCommand Plug-In 3.1 for Microsoft Installation and Administration Guide for basic troubleshooting guidelines.

9.1   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   Reinstalling OnCommand Plug-In 3.1 for Microsoft and Discovery

There might be times when a reinstallation of OnCommand Plug-In 3.1 for Microsoft is required. After following the instructions within the OnCommand Plug-In 3.1 for Microsoft Installation and Administration Guide, discovery will need to be reinitiated even if it was executed in the previous installation. To rediscover after reinstallation:

1. Set up credentials using Data ONTAP Manage Controller Credentials in Actions pane.
2. Click Data ONTAP: Run discovery task.

Refer to best practice in section 2.9, "Manual Discovery of NetApp Storage Systems."

9.3   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.

If the SQL Server database is simply full, but there is space remaining on the drive where it resides, you might choose to simply allow the database to autogrow. This means that SQL Server will continue to increase the size of the SQL Server database until the drive is completely full. Alternatively, you might need to work with your SQL Server DBA to determine how to support SCOM data growth.

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. In the column Autogrowth, double-click the button on the right showing "…"
6. Adjust the setting to allow the database to use the autogrowth.

Alternatively, 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   Discovery Troubleshooting

Open a console window to the NetApp storage array to troubleshoot any OnCommand Plug-In 3.1 for Microsoft 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 OnCommand 3.1.0.0: (100) OnCommand plug-in For
Microsoft: DataONTAP MP discovery rule
```

9.5   SNMP Versions

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

- For Data ONTAP versions earlier than 7.3, only SNMP V1 will be supported.
- For Data ONTAP version 7.3 and higher, SNMP V3 and SNMP V2C will be supported.

If the storage environment contains multiple different types of Data ONTAP, use SNMP V1 to discover all storage arrays with OnCommand Plug-In 3.1 for Microsoft.

9.6 Event Viewer Logs

Use the Windows event viewer to review the OCPM-specific logs for further information on any issues. Users will find an OCPM-specific event log under Applications and Services Logs in event viewer. In addition to the OCPM-specific logs, users will find important information in the application logs and the Operations Manager logs. Utilize these logs to find specific issues with OCPM discovery or any other issues.

Figure 15 shows the event viewer.

Figure 15) Event viewer.
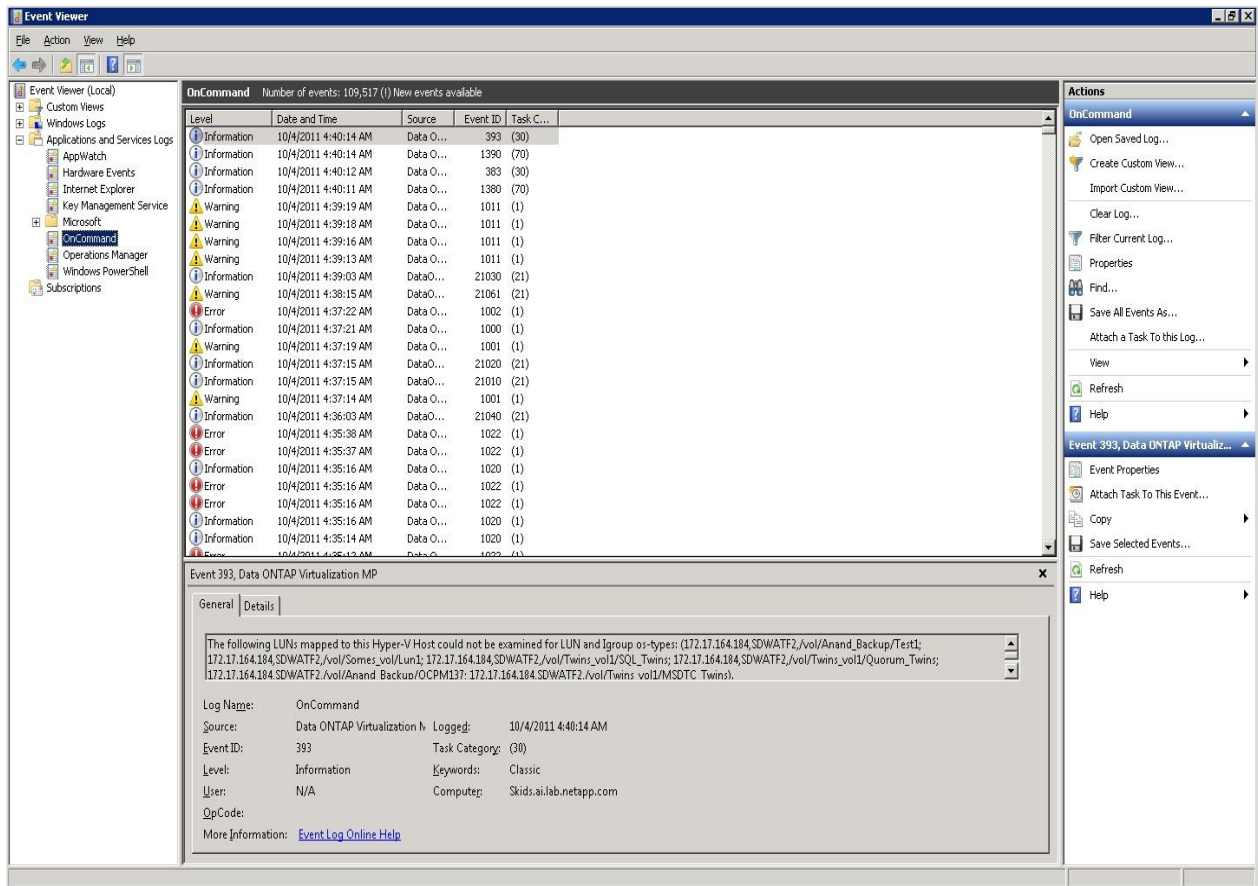
9.7 Debugging

To enable debug logging for OCPM, you will need to set the DEBUG value within the OC.Common.Library.LogSettings.xml. The LogSettings.xml is located within the OCPM install directory, and the default location is:

'C:\Program Files\NetApp\OnCommand\MS_Plugin\OC.Common.Library.LogSettings.xml'

To enable OCPM debugging:

1. 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 OCPM Debugging-->
<appender-ref ref="EventLogAppender" />
</root>
```

9.8 Advanced Troubleshooting

When basic troubleshooting does not resolve any issues with OnCommand Plug-In 3.1 for Microsoft, use one of the many support features provided to NetApp customers.

1. [NetApp Community](#)

   A public forum where customers can discuss topics with other NetApp experts about specific technologies. For questions and topics specific to the OnCommand Plug-In 3.0 for Microsoft, visit http://communities.netapp.com/community/products_and_solutions/storage_management_software.

2. [NetApp Support Community](#)

   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.

Go further, faster®

NetApp®

www.netapp.com