

OnCommand™ Plug-in 3.0 for Microsoft®

Installation and Administration Guide

NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089 USA
Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 4-NETAPP
Documentation comments: doccomments@netapp.com
Information Web: <http://www.netapp.com>
Part number: 215-05937_A0
August 2011

Contents

What you can do with OnCommand Plug-in for Microsoft	7
New features in OnCommand Plug-in for Microsoft	11
OnCommand Plug-in for Microsoft installation, upgrade, and uninstallation procedures	13
OnCommand Plug-in for Microsoft installation quick start list for System Center Operations Manager	13
Installation requirements for OnCommand Plug-in for Microsoft	15
Guidelines for installing OnCommand Plug-in for Microsoft	17
About upgrading	19
Uninstalling ApplianceWatch PRO 2.1 and 2.1.1	19
Installing and upgrading OnCommand Plug-in for Microsoft	20
Installing and upgrading OnCommand Plug-in for Microsoft in silent mode	21
Silent install and uninstall process parameters and variables	22
Feature selection for silent installation	23
Uninstalling OnCommand Plug-in for Microsoft	25
Uninstalling the plug-in with the wizard	25
Uninstalling OnCommand Plug-in 3.0 for Microsoft in silent mode	25
Importing the Opalis integration packs	27
Overview of the Opalis integration packs	27
Requirements for importing the Opalis integration packs to the integration server	27
Importing the Opalis integration packs to the integration server	28
Deploying the Opalis integration packs to the Opalis action server	29
Uninstalling the Opalis integration packs from the action server	29
Data ONTAP management pack rules	31
Finding Data ONTAP management pack rules	34
What discovery is	35
Types of discovery	35
Expediting storage discovery	36
Expediting virtualization discovery	36
Managing storage controller information	39
Adding a storage controller	39

Managing storage controller credentials	39
Removing a storage controller	40
Configuring SNMP traps	41
Modifying storage controller information using FilerView	41
Monitoring your system	43
Alert monitoring	43
Alerts View	43
Diagram View	44
Controllers View	44
Overriding monitoring rules	44
Performance monitoring	44
Performance metrics	45
Performance monitoring views	46
Checking the alignment of your Hyper-V LUNs	52
Checking the alignment of your VHDs	53
How to launch Health Explorer for a controller	53
Monitoring Operations Manager servers	54
Using OnCommand Plug-in for Microsoft PRO tips	54
Types of PRO Tips	54
Implementing PRO Tips automatically	57
Implementing PRO Tips manually	57
Events	57
Availability events	58
Configuration events	58
MetroCluster monitoring	59
Guidelines for using the MetroCluster TieBreaker Manager	59
Using the MetroCluster TieBreaker Manager	60
Reassembling a failed-over cluster	61
Reports	63
Viewing reports	64
Custom reports	65
Overview of using PowerShell cmdlets	67
Windows PowerShell execution policies and administration profiles	67
Standard optional cmdlet parameters	68
Provisioning and cloning	69
Provisioning and cloning prerequisites	69

Provisioning and cloning cmdlets	70
Disaster recovery	71
Requirements and prerequisites for disaster recovery	71
Disaster recovery cmdlets	72
The disaster recovery plan	73
The disaster recovery failover workflow	74
The disaster recovery failback workflow	75
Troubleshooting	77
Tips for solving console issues	77
Tips for solving storage controller issues	78
Performance and resource optimization (PRO) issues	78
Show Windows Installer log check box is not visible	79
Copyright information	81
Trademark information	83
How to send your comments	85
Index	87

What you can do with OnCommand Plug-in for Microsoft

OnCommand Plug-in for Microsoft includes managements packs for Microsoft SCOM 2007 R2, PowerShell cmdlets, and Opalis integration packs. With PowerShell cmdlets, you can perform provisioning, cloning, and disaster recovery for Microsoft Hyper-V virtual machines. You can also perform these same actions using Microsoft Opalis by building workflows using objects from the Opalis integration pack (OIP).

OnCommand Plug-in for Microsoft consists of the following components:

Parent Component	Sub-component	Description
System Center Operations Manager (SCOM) Management Packs	OnCommand Data ONTAP	Enables you to use your existing storage management tools to monitor all storage systems that are running Data ONTAP through one interface. OnCommand Plug-in for Microsoft enables you to view your hardware and storage layout and monitor any issues. The following features are part of Storage Monitoring and Reporting: • Data ONTAP Management Pack • Data ONTAP Reports Management Pack
	OnCommand Data ONTAP Virtualization	Enables you to monitor and report on your virtualized environment. The following features are part of Hyper-V Storage Monitoring and Reporting : • Data ONTAP Virtualization Management Pack • Data ONTAP Virtualization Reports Management Pack
	OnCommand Data ONTAP PRO	Enables you to monitor and report on those objects that are used by the PRO management pack and to receive PRO Tips with automatic remediation support within the Microsoft System Center Virtual Machine Manager console.

Parent Component	Sub-component	Description
	OnCommand Data ONTAP MetroCluster	Enables you to solve any controller disputes during MetroCluster installation and provides instruction to assist you in reassembling a cluster after the cluster has failed over.
Cmdlets	Cloning and Provisioning	You can use provisioning and cloning cmdlets to provision storage, clone virtual machines, and manage storage system credentials.
	Disaster Recovery	For disaster recovery, SnapMirror technology is used to replicate data across two sites to provide a disaster recovery (both failover and failback) solution for virtual machines running on standalone or clustered Hyper-V virtual machines that are running on dedicated, shared, or CSV LUNs.
Opalis Integration Packs	Cloning and Provisioning Integration Pack	You can use objects provided in the Opalis integration pack to create workflows to provision storage, clone virtual machines, and manage storage system credentials.
	Disaster Recovery Integration Pack	For disaster recovery, you can use Opalis objects to create disaster recovery workflows that replicate data across two sites in both failover and failback scenarios.
OnCommand Discovery Agent		You can use the OnCommand Discovery Agent which is a Windows Management Instrumentation (WMI) provider with OnCommand Plug-in for Microsoft to assist you with SCOM host discovery, provisioning, cloning, and disaster recovery cmdlet functionality.
OnCommand Plug-in Web Services		VIM Web services is the virtualization infrastructure management Web services, the Windows Communication Foundation (WCF)-based Web services that provide access to the key features of storage discovery, storage provisioning, cloning virtual machines, disaster recovery of virtual machines based on a disaster recovery plan.

Parent Component	Sub-component	Description
Documentation		The OnCommand Plug-in for Microsoft Installation and Administration Guide and the PowerShell Windows Cmdlet Reference Guide are available with the installation.

New features in OnCommand Plug-in for Microsoft

OnCommand Plug-in for Microsoft offers new features to assist you in Data ONTAP storage management.

The following new features have been added to OnCommand Plug-in for Microsoft:

- **System Center Operations Manager**
 - LUN and VHD misalignment detection including PRO Tips and reports
 - Support for virtual machines with cluster shared volumes (CSVs)
 - Full support for high availability
 - Discovery of virtual machines in CSVs
 - Alert and PRO Tips for CSV space utilization
 - Performance view and reports for CSV space utilization
 - Agentless monitoring and discovery on Hyper-V hosts
 - Support for vFiler units
 - Discovery and monitoring of vFiler units
 - View of relationship between vFiler units and their physical controllers
 - Storage efficiency statistics at volume, aggregate, and controller level in views and reports
 - Remote procedure call protocol for communicating with storage systems
 - Quality of service (QoS) monitoring
 - Volume- level and LUN-level statistics
- **Disaster recovery**
 - Crash-consistent disaster recovery (both failover and failback) of Hyper-V virtual machines that have data on Data ONTAP storage systems and are replicating data to remote sites using SnapMirror
 - The ability to perform disaster recovery across geographically dispersed sites and domains
- **Provisioning and cloning**
 - Enhanced New-OCStorage, Connect-OCStorage, Disconnect-OCStorage, and Remove-OCStorage PowerShell cmdlets to support Windows failover cluster (WFC) and CSVs
 - A new cmdlet, Resize-OCStorage, to grow or shrink the NTFS Datastore on LUNs
 - An enhanced New-OCClone cmdlet to clone an existing virtual machine that is not in a powered-on state
 - The ability to deploy virtual machines in the Windows failover cluster (WFC) and CSV environments
 - New functionality to export information on cloned virtual machines for integration with XenDesktop

- Functionality for virtual machine cloning in the following instances:
 - From a LUN (LUN A) into a LUN (LUN B) that already exists on the same host
 - From a LUN (LUN A) into a new LUN (LUN C)
 - From an existing LUN (LUN A) into the same LUN (LUN A)

This functionality supports traditional Windows LUNs or CSV LUNs within a Windows cluster.

- A new cmdlet, `New-OCCloneFile`, that creates a copy of any NTFS file within the same LUN or to another LUN that is mounted on the same storage volume

This command supports traditional Windows LUNs or CSV LUNs within a Windows cluster.

- **Opalis integration packs**

- Cloning and provisioning integration with Opalis through the Cloning and Provisioning integration pack
- Disaster recovery integration with Opalis through the Disaster Recovery integration pack
- The ability to create and customize workflows
- The ability to automate your data provisioning, cloning, and disaster recovery tasks
- The ability to test disaster recovery through a disaster recovery failover simulation
- Provisioning of Data ONTAP storage on WFCs and CSVs
- Cloning virtual machines with or without an SCVMM template on Windows LUNs or CSV LUNs and cloning NTFS files on Windows LUNs or CSV LUNs

OnCommand Plug-in for Microsoft installation, upgrade, and uninstallation procedures

Before you download and install OnCommand Plug-in for Microsoft and any additional features, your environment must meet certain Microsoft System Center Operations Manager 2007 R2, Microsoft System Center Virtual Machine Manager 2008, and Data ONTAP requirements.

OnCommand Plug-in for Microsoft installation quick start list for System Center Operations Manager

You can use the installation quick start list to assist you with the many steps involved in installing and setting up your OnCommand Plug-in for Microsoft for System Center Operations Manager (SCOM). You must complete each item in the list to ensure that OnCommand Plug-in for Microsoft is properly installed and set up on your SCOM system.

Steps

1. Install the SCOM (check the Microsoft TechNet website for installation information).
 - a. Review the SCOM Installation Guide for requirements.
 - b. Optional: During the installation, select to install the Reporting management pack, which is required for Data ONTAP reporting.
 - c. Optional: Install System Center Virtual Machine Manager (SCVMM) for Data ONTAP PRO Tips.
 - d. Make sure all installation requirements have been fulfilled and confirm proper functionality prior to proceeding with OnCommand Plug-in for Microsoft installation. Refer to the Microsoft documentation for SCOM and SCVMM for more details.

2. Download and install OnCommand Plug-in for Microsoft.

Run OnCommand Plug-in for Microsoft installation executable on the Root Management Server (RMS) SCOM server.

If the SCOM prerequisite is satisfied, the management pack and related components are selected and installed by default. Deselect any management packs from the features selection list in the SCOM installer that you do not want to install. Deselect any other components in the selection list that you do not want to install.

3. Optional: Set up SNMP.

Ensure that firewalls, proxies, or other network devices do not interfere with traffic. The required ports are SNMP, and HTTP or HTTPS.

SNMP v1 discovers all storage appliances in the environment. The following SNMP versions are supported:

- For Data ONTAP versions earlier than 7.3, SNMP 1 is supported.
 - For Data ONTAP 7.3 and later, SNMP 3 and SNMP 2C are supported.
4. Create overrides for the Data ONTAP discovery rule and the Data ONTAP virtualization discovery rule only for the management servers on which OnCommand Plug-in for Microsoft is installed.
 5. Create and save overrides to your own management pack, not the default management pack to avoid dependencies on the default management pack.
 6. Run Data ONTAP discovery to discover any network devices that are already monitored in SCOM.

This step prevents your system from monitoring duplicate controllers. To run discovery, on the Actions pane, go to **Monitoring Tab > Data ONTAP > Management Server > Data ONTAP: Run Discovery Task**.

7. Add a controller.

In the Actions pane, go to **Monitoring > Data ONTAP > Management Server**, select **Data ONTAP: Add Controller**.

8. Add the controller credentials.

In the Actions pane, select **Data ONTAP: Manage Controller Credentials**. Ensure that the appropriate roles and capabilities are assigned. The default protocol is HTTPS but VFilers can only use HTTP.

9. Run Data ONTAP discovery to discover all the controllers.

On the Actions pane, go to **Monitoring Tab > Data ONTAP > Management Server > Data ONTAP: Run Discovery Task**.

10. Run Data ONTAP virtualization discovery to discover storage on all Hyper-V hosts in SCVMM.

You must have added all of your Hyper-V hosts to SCVMM because Data ONTAP virtualization discovery only discovers those Hyper-V hosts that are on SCVMM.

11. Run Data ONTAP PRO discovery to discover Hyper-V hosts with PRO integration in SCVMM.

12. Enable PRO Tips.

Make sure all requirements have been met for SCOM and SCVMM PRO integration.

In SCVMM, go to **Administration > General > PRO Settings**.

SCVMM can take up to six hours to fully discover all the objects that are required for PRO tips. See the Microsoft TechNet website.

Installation requirements for OnCommand Plug-in for Microsoft

Your environment must meet all hardware, software, Data ONTAP, and Microsoft licensing requirements before you install and use OnCommand Plug-in for Microsoft, the various management packs, and the Opalis integration packs.

OnCommand requirements	To correctly install OnCommand Plug-in for Microsoft, any versions of ApplianceWatch must first be uninstalled. The installer will do this automatically during the installation process.
OnCommand Discovery Agent requirements	You must meet the following requirements for installation of OnCommand Discovery Agent: • Hyper-V server role is enabled • Windows Server 2008 R2 or later is installed
Data ONTAP requirements	OnCommand Plug-in for Microsoft supports the following versions of Data ONTAP: • 7.2.6 or later in the Data ONTAP 7.2 product family (System Center Operations Manager Management packs only) • 7.3 or later in the Data ONTAP 7.3 product family • 7.3.3 or later for vFiler support • Data ONTAP 8.0 7-Mode in the Data ONTAP 8.0 product family
Hardware requirements	Microsoft System Center Operations Manager 2007 R2 and Microsoft System Center Virtual Machine Manager 2008 R2 determines the hardware requirements. For more information, see the Microsoft TechNet site.
Software requirements	OnCommand Plug-in for Microsoft supports the following software versions: • .NET Framework 3.5 SP1 for all features • Microsoft System Center Operations Manager 2007 R2 for SCOM Management packs • Microsoft System Center Virtual Machine Manager 2008 R2 for cloning cmdlets • Microsoft Opalis 6.3 for Opalis integration packs For more information, see the Microsoft TechNet site.
Microsoft license requirements	OnCommand Plug-in for Microsoft requires the following Microsoft licenses: • Windows Server 2003, 2008 (32-bit or 64-bit), or 2008 R2 • Microsoft SQL Server 2005 or 2008 • Microsoft System Center Operations Manager 2007 R2

- Microsoft System Center Virtual Machine Manager 2008 R2 Enterprise and Data Center (only necessary to receive PRO Tips)

**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.2008.Library
- Microsoft.SystemCenter.VirtualMachineManager.2008.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

**System
Center
Operations
Manager
reporting
configuration
requirements**

You must configure System Center Operations Manager 2007 R2 for reporting so that the Reports management pack appears with the other management packs. To do this, you must correctly configure the SQL server data warehouse. For more information, see the Microsoft TechNet site.

**Opalis
Integration
Packs**

- You must install Opalis 6.3 and deploy the Opalis integration packs to the Opalis action 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 .NET3.5 SP1 installed in the action server host to use our integration packs in the Opalis action server.

Disaster recovery and provisioning and cloning cmdlet requirements	The installer checks for the minimum Windows configuration requirements. The installation stops if the requirements for the minimum operating system, any service pack level, or PowerShell 2.0 are not met.
Web services	The VIM Web service login account needs to have administrative privileges on the local and remote hosts or clusters across the primary and secondary sites.

Related information

Microsoft System Center - <http://technet.microsoft.com>

Guidelines for installing OnCommand Plug-in for Microsoft

You must be prepared for the installation in order for it to go smoothly. Before you install OnCommand Plug-in for Microsoft, it is useful to have all of the installation information available.

During installation, the installer automatically imports all the features that you want. If there is any missing software, a warning message informs you what you must download.

OnCommand Plug-in for Microsoft download	You must have downloaded the OnCommand Plug-in for Microsoft software from the NetApp Support Site.
Requirements	You must have met the requirements for proper installation of OnCommand Plug-in for Microsoft.
Credentials	You must have the appropriate credentials to install and run OnCommand Plug-in for Microsoft.
Installation features	You must have decided which features you want to install. You can customize your OnCommand Plug-in for Microsoft installation by choosing one or more of the following features. You can perform the installation in silent mode as well.

- **System Center Operations Manager (SCOM) Management Packs**
 - **OnCommand Data ONTAP**
Required for any use.
 - **Data ONTAP Management Pack**
 - **Data ONTAP Reports Management Pack**
 - **OnCommand Data ONTAP Virtualization**
Required for use in a virtualized environment.
 - **Data ONTAP Virtualization Management Pack**

OnCommand Web Services are installed with the Data ONTAP Virtualization management pack.

- **Data ONTAP Virtualization Reports Management Pack**
- **OnCommand Data ONTAP PRO**
- **OnCommand Data ONTAP MetroCluster**
- **Cmdlets**
 - **Cloning and Provisioning**

The cmdlets are separate from the rest of the management packs and are not dependant on them to function correctly. Provisioning and cloning functionality requires the presence of discovery agent for Hyper-V hosts with Fibre channel initiators. For iSCSI initiators only, a discovery agent is not required.

OnCommand Web Services are installed with the cmdlets.
 - **Disaster Recovery**

The cmdlets are separate from the rest of the management packs and are not dependant on them to function correctly. OnCommand Web Services are installed with the cmdlets.
- **Opalis Integration Packs**
 - **Cloning and Provisioning Integration Pack**

Provisioning and cloning functionality requires the presence of the discovery agent for Hyper-V hosts with Fibre channel initiators. For iSCSI initiators only, a discovery agent is not required.

The cloning and provisioning management pack, the disaster recovery management pack and the OnCommand Plug-in Web Services are installed by default, but if you choose to install the OIP alone, the Web services are not installed.
 - **Disaster Recovery Integration Pack**

OnCommand Plug-in Web Services are installed with the Opalis modules by default.
 - **OnCommand Plug-in Web Services**

Can be installed on a server other than an Opalis action server.
- **OnCommand Discovery Agent**

Enables the discovery of storage in environments in which LUNs are mapped using Fibre Channel.

Note: OnCommand Discovery Agent is needed only in environments in which LUNs are mapped using Fibre Channel. You can download the OnCommand Discovery Agent during installation.
- **Documentation**

Related information

<http://now.netapp.com/NOW/>

About upgrading

You can use the upgrade procedure to upgrade the cmdlets or the management packs. When you upgrade management packs, your user data and settings are preserved and it eliminates the need for you to uninstall previous management packs.

Upgrading management packs:

- When you upgrade, you must preserve your overrides when possible.
- Depending on infrastructure changes, name changes, or both, in an upgraded management pack, the overrides management pack may cause validation errors. In these cases, you should manually import the management pack that contains the overrides that are causing the problems and fix the overrides.
- To fix the overrides, you can go to **Authoring > Overrides** and find the overrides on the management pack and delete them. Then you can create and save your new overrides to a new management pack.

Uninstalling ApplianceWatch PRO 2.1 and 2.1.1

You can use the Windows Control Panel to uninstall ApplianceWatch PRO 2.1 and 2.1.1 if you no longer need it.

Steps

1. Open the **Windows Control Panel** on the appropriate management server.
2. From the **Control Panel**, run the Windows program management utility.

If...	Then...
You are using Windows 2003	Double-click Add or Remove Programs .
You are using Windows 2008	Double-click Programs and Features .

3. Select ApplianceWatch PRO 2.1.1.

If...	Then...
You are using Windows 2003	Click Remove .
You are using Windows 2008	Click Uninstall .

Installing and upgrading OnCommand Plug-in for Microsoft

Use the installation wizard to install OnCommand Plug-in for Microsoft, the management packs, the Opalis integration pack, and the Web services.

Before you begin

You must install OnCommand Plug-in for Microsoft and the associated features on every server on which the Microsoft Operations Manager 2007 R2 operations console is used. You must also have installed OnCommand Discovery Agent on all Hyper-V hosts.

About this task

The installer imports the new management packs automatically. All features are installed by default. You can deselect those features that you *do not* want to install.

Steps

1. From the NetApp Support Site, download the OnCommand Plug-in for Microsoft executable file to a directory on your hard drive.
2. Launch the OnCommand Plug-in for Microsoft executable file from a command line prompt using the path to the directory where you saved the file.

The InstallShield wizard opens.

3. Click **Next**.

The EULA Agreement dialog box opens.

4. Select **I accept the terms in the license agreement**, and click **Next**.

The Destination Folder dialog box opens.

5. Click **Next** to install to the folder that is listed or click **Change** to install to a different folder.

Click **Next** to continue with the installation.

6. In the **Custom Setup** dialog box, select the program features that you want to install.
7. Optional: If you want to view the **Custom Setup Tips** dialog box that explains the icons and their meanings, click **Help**.
8. Optional: If you want to change the location to which the files are installed, click **Change** and type in the new path.
9. Optional: If you want to view the disk space usage, click **Disk Space**.
10. After you have specified those features that you want to install, click **Next**.

The Web Services Credentials dialog box opens.

11. Type in your Web service credentials.
12. In the **Ready to Install** dialog box, click **Install** to begin the installation.
A status box opens and charts the progress of the installation. Then the InstallShield Wizard Completed box opens.
13. If the installer finds that required software is missing, a dialog box opens with information on where you can view the list of requirements and from which you can specify the installation of the missing software; the dialog box also includes a **Back** button that you can use to change your specifications, if necessary.
14. Click **Finish** to end the installation and to close the InstallShield wizard.

Installing and upgrading OnCommand Plug-in for Microsoft in silent mode

You can perform the installation or upgrade of OnCommand Plug-in for Microsoft software in silent mode, without a wizard.

Before you begin

You must install OnCommand Plug-in for Microsoft and the associated features on every server on which the Microsoft Operations Manager 2007 R2 operations console is used. You must also have installed OnCommand Discovery Agent on all Hyper-V hosts.

About this task

A silent installation means that no interface, progress bars, or error messages are displayed during the installation process. All error messages are written to a log file that is located in the temp folder.

The silent uninstall process replaces any old versions of the management packs and imports the new management packs automatically.

Steps

1. From the NetApp Support Site, download the OnCommand Plug-in for Microsoft executable file to a directory on your hard drive.
2. From a command line prompt, switch to the directory where you saved the executable file.
3. Run the command.

The installation begins and runs in the background.

Result

A log file that lists any errors that occur during the installation is saved to the temp folder after the installation finishes. Another log file is written if there is any software that the user needs to install.

Silent install and uninstall process parameters and variables

When you want to run an install or uninstall process in the background, or *silently*, you construct a command to do so using a particular set of parameters and variables.

The parameters and variables

The parameters are passed to the setup.exe in the following order: (do not leave a space between the "v" and the quotation mark.)

ocmsplugin-setup-3.0_x64_setup.exe /w /s /x /v"/qn SILENT_MODE=1"

/w Waits until the installation is complete before exiting.

If you are using the **/w** argument in a batch file, you might want to precede the entire Setup.exe command-line command with

start /WAIT

...:

start /WAIT ocmsplugin-setup-3.0_x64_setup.exe /w ...

/q Specifies silent installation with the following flags:

- b** Creates a basic user interface
- f** Displays a full user interface
- n** Does not create a user interface
- r** Displays a reduced user interface

/s Specifies silent mode.

/v Passes the arguments to the installer

/x Specifies uninstall mode.

SILENT_MODE=1 Sets the installer variable *SILENT_MODE* to 1, which indicates that the installation will run silently.

ADDLOCAL= In a custom installation, those arguments that are specified after *ADDLOCAL* indicate the features that you want to install. If there is no *ADDLOCAL* in the command, all features are installed by default.

Feature selection for silent installation

If you choose not to install all features by default, you must use specific feature names in addition to the *ADDLOCAL* parameter to construct a command that will silently run a custom installation of OnCommand Plug-in for Microsoft. Separate the feature names with a comma, but do not use spaces.

Note: *ALL* features are selected to be installed by default.

If you select to install a parent feature (like ManagementPacks) then all the child features under it will be installed also. If you select to install a child feature such as Hyper-V Storage Monitoring and Management , its parent feature (ManagementPacks) will also be installed along with any sibling features that are listed as required (such as Storage Monitoring).

In the following example, the user is performing a silent installation, during which they want to install the cmdlets and the documentation only.

```
ocmsplugin-setup-3.0_x64_setup.exe /w /s /v"/qn SILENT_MODE=1
ADDLOCAL=Cmdlets,Doc"
```

Parent Feature name in Custom Setup	Child Feature	Sub-Child Feature	Feature Name for ADDLOCAL
System Center Operations Manager (SCOM) Management Packs			ManagementPacks
	OnCommand Data ONTAP		OCPlugin
		Data ONTAP Management Pack	StorageMonitoring
		Data ONTAP Reports Management Pack	Reporting
	OnCommand Data ONTAP Virtualization		
		Data ONTAP Virtualization Management Pack	HVStorageMonitoring

Parent Feature name in Custom Setup	Child Feature	Sub-Child Feature	Feature Name for ADDLOCAL
		Data ONTAP Virtualization Reports Management Pack	HVStorageReporting
	OnCommand Data ONTAP PRO		
	OnCommand Data ONTAP MetroCluster		MetroCluster
		Data ONTAP MetroCluster Monitoring and Management Service	MetroCluster Service
Cmdlets			
	Cloning and Provisioning Cannot be installed individually.		CmdletsCP
	Disaster Recovery Cannot be installed individually.		CmdletsDR
Opalis Integration Pack			Opalis
	Cloning and Provisioning Integration Pack		OpalisCP
	Disaster Recovery Integration Pack		OpalisDR
	OnCommand Plug-in Web Services		OCWebServices
OnCommand Discovery Agent			OCAgent
Documentation			Doc

Uninstalling OnCommand Plug-in for Microsoft

You can uninstall OnCommand Plug-in for Microsoft two ways. You can use the uninstall wizard in the Control Panel or you can perform a silent uninstall to remove OnCommand Plug-in for Microsoft when you no longer need the plug-in or when you upgrade to a later version. The uninstall process only uninstalls the OnCommand Plug-in for Microsoft. It does not uninstall the management packs.

About this task

To uninstall the management packs, go to **Administration > Management Packs** and search for the management packs that you want to delete in the list. Select the management packs and then click **Delete** in the Actions pane.

Uninstalling the plug-in with the wizard

You can use the wizard to uninstall OnCommand Plug-in for Microsoft when you no longer need the plug-in or when you upgrade to a later version.

Steps

1. Open Windows Control Panel on the appropriate management server.
2. From Control Panel, run the Windows program management utility.

If...	Then...
You are using Windows 2003	Double-click Add or Remove Programs .
You are using Windows 2008	Double-click Programs and Features .

3. Select OnCommand Plug-in for Microsoft.

If...	Then...
You are using Windows 2003	Click Remove .
You are using Windows 2008	Click Uninstall .

Uninstalling the plug-in in silent mode

You can uninstall OnCommand Plug-in for Microsoft software silently, without a wizard.

About this task

There is no user interface is displayed during a silent uninstall process. There are no dialogs, progress bars, or error messages. All error messages are written to a log file that is located in the temp folder.

Steps

1. From a command line prompt, switch to the directory where you saved the executable file.
2. Run the command.

The uninstall process begins and runs in the background.

A log file that lists any errors that occur during the uninstall process is saved to the temp folder after the procedure finishes.

Importing the Opalis integration packs

To use the Opalis user interface and the Opalis objects to create workflows and automate your provisioning, cloning, and disaster recovery tasks, you must import and deploy the Opalis integration packs (OIP).

Overview of the Opalis integration packs

Opalis is one of the interfaces that you can use to perform actions through the OnCommand Plug-in for Microsoft. The Opalis integration packs (OIP) use a graphical user interface that provides objects that you can drag to create workflows for provisioning, cloning, and disaster recovery.

When you initiate the workflows, they run without user intervention. You can also create customized routines that you can save and use repeatedly.

Requirements for importing the Opalis integration packs to the integration server

You must meet all hardware, software, Data ONTAP, and Microsoft requirements before you import the Opalis integration pack to the integration (management) server.

- **Microsoft requirements:** You must have met all the requirements for Opalis 6.3. If you are not sure what the requirements are, check the Microsoft TechNet Web site.
- **Microsoft license requirements:** You must have the Opalis 6.3 license.
- **VIM Web Services requirements:** You must have installed OnCommand Plug-in VIM Web services on at least one server. This server does not need to be an Opalis integration server or action server. Web services must be installed on the local and remote hosts or clusters on both the primary and secondary sites if you want to use disaster recovery.

This procedure involves two types of servers, the action server and the integration (management) server.

The management server is the central manager of clients, action servers, policies, the policy testing console, and self-monitoring. The management server deploys integration packs to action servers and clients, deploys policies to action servers, and acts as a communication link between the clients, the action servers, and the datastore.

The action server is the engine that runs policies. Action servers communicate with the datastore. Action servers do not require a management server to be online to be able to run policies. You can deploy a single action server or multiple ones.

Importing the Opalis integration packs to the integration server

You must import the Opalis integration packs (OIPs) to the integration server before you can use the Opalis objects.

Before you begin

Opalis integration pack importation	You must have downloaded the OnCommand Plug-in for Microsoft software from the NetApp Support Site.
Requirements	You must have met the requirements for proper importation of Opalis integration packs.
Credentials	You must have the appropriate credentials to import the Opalis integration pack to the integration server.

Steps

1. Navigate to the **Opalis Integration Server Deployment Manager** by going to **Start > All Programs > Opalis Software > Opalis Integration Server > Deployment Manager**.
2. Right click **Integration Packs** in the left panel and select **Register IP with the management server**.

The Integrations Pack Registration wizard opens.

3. Click **Next**.

The Integration Pack or Hotfix Selection window opens.

4. Click **Add**.

5. Navigate to where the OnCommand Plug-in for Microsoft software is installed.

6. Select to import the OIPs. Click **Open** and close the browser window.

When you are finished adding computers, click **Next**.

The Completing Integration Pack wizard window opens.

7. Click **Finish** to close the wizard.

A green check mark appears in the Log Entries panel of the Opalis integration server window, stating that the registration (importation) of the OnCommand Plug-in for Microsoft OIPs to the integration server was successful.

After you finish

Next you must deploy the OIPs to the Opalis action server.

Deploying the Opalis integration packs to the Opalis action server

After you have imported the Opalis integration packs (OIP) to the integration server, you can deploy them to the action server.

Steps

1. Navigate to the **Opalis Integration Server Deployment Manager** by going to **Start > All Programs > Opalis Software > Opalis Integration Server > Deployment Manager**.
2. Right click **Integration Packs** in the upper right panel and select **Deploy IP to Action Server or Client**.

A green check mark appears in the Log Entries panel of the Opalis integration server window. It states that the deployment of the OnCommand Plug-in for Microsoft OIPs to the action server or client was successful.

Uninstalling the Opalis integration packs from the action server

You should use the Opalis integration server deployment manager to uninstall the Opalis integration packs from the action server. See the Microsoft TechNet Web site for details.

Data ONTAP management pack rules

OnCommand Plug-in for Microsoft includes rules and monitors so you can more effectively manage your storage resources.

Data ONTAP: Management Server rules

The following list displays all of the Data ONTAP Management Server rules:

- Data ONTAP: Aggregate Space Utilization Rule
- Data ONTAP: Aggregate State Rule
- Data ONTAP: Collect Events Rule
- Data ONTAP: Collect SnapMirror Lag Time Counter Rule
- Data ONTAP: Controller Connection Check Rule
- Data ONTAP: Controller Global Status Rule
- Data ONTAP: Controller HA Status Rule
- Data ONTAP: Controller Storage Utilization Rate of Change Rule
- Data ONTAP: Discover Recent Network Devices Rule
- Data ONTAP: Discovery Rule
- Data ONTAP: Disk State Rule
- Data ONTAP: Enclosure State Rule
- Data ONTAP: LUN Latency Rule
- Data ONTAP: LUN State Rule
- Data ONTAP: Quota Limits Rule
- Data ONTAP: Refresh Dashboard Rule
- Data ONTAP: SnapMirror Status Rule
- Data ONTAP: Storage Statistics Rule
- Data ONTAP: Trigger Controller Discovery Rule
- Data ONTAP: Trigger vFiler Discovery Rule
- Data ONTAP: Volume Space Utilization Rule
- Data ONTAP: Volume State Rule
- Data ONTAP: Volume Used Inodes Rule

Data ONTAP PRO: Hyper-V Host rules

The following list displays all of the Data ONTAP PRO Hyper-V Host rules:

- Data ONTAP PRO: Discovery Rule
- Data ONTAP PRO: Collect Hyper-V Host Events Rule
- Data ONTAP PRO: Hyper-V Replication Status PRO Tip Recovery Rule

- Data ONTAP PRO: Hyper-V Virtual Machine Thin Provisioning Volume Auto Grow PRO Tip Recovery Rule
- Data ONTAP PRO: LUN Online PRO Tip Recovery Rule
- Data ONTAP PRO: LUN Space Reservation PRO Tip Recovery Rule
- Data ONTAP PRO: Volume Deduplication Status PRO Tip Recovery Rule
- Data ONTAP PRO: Volume Online PRO Tip Recovery Rule
- Data ONTAP PRO: Volume Snapshot Auto-Delete PRO Tip Recovery Rule
- Data ONTAP PRO: Volume Space Utilization PRO Tip Recovery Rule

Data ONTAP Virtualization: Management Server rules

The following list displays all of the Data ONTAP Virtualization Management Server rules:

- Data ONTAP Virtualization: Collect Events Rule
- Data ONTAP Virtualization: Hyper-V Virtual Machine Replication Status Rule
- Data ONTAP Virtualization: Hyper-V Virtual Machine Space Utilization Rate Rule
- Data ONTAP Virtualization: Hyper-V Virtual Machine Thin Provisioning Volume Autogrow Rule
- Data ONTAP Virtualization: Hyper-V Virtual Machine Thin Provisioning Volume Snapshot Auto Delete Rule
- Data ONTAP Virtualization: LUN Alignment Rule
- Data ONTAP Virtualization: LUN Igroup Type Configuration Rule
- Data ONTAP Virtualization: LUN Online Rule
- Data ONTAP Virtualization: LUN Space Reservation Rule
- Data ONTAP Virtualization: LUN Space Utilization Rule
- Data ONTAP Virtualization: Usage Records Update Controllers Registry Rule
- Data ONTAP Virtualization: Usage Records Update Database Rule
- Data ONTAP Virtualization: VHD Alignment Rule
- Data ONTAP Virtualization: VHD Discovery Rule
- Data ONTAP Virtualization: Volume Deduplication Status Rule
- Data ONTAP Virtualization: Volume Online Rule
- Data ONTAP Virtualization: Volume Space Utilization Rule

Data ONTAP MetroCluster: Management Server rules

The following list displays all of the Data ONTAP MetroCluster Management Server rules:

- Data ONTAP MetroCluster: Aggregate Mirror Rule
- Data ONTAP MetroCluster: Cluster Status Rule
- Data ONTAP MetroCluster: Discovery Rule
- Data ONTAP MetroCluster: Disk Fabric Connection Rule
- Data ONTAP MetroCluster: Disk Ownership Rule
- Data ONTAP MetroCluster: Network Interface Ping Rule

- Data ONTAP MetroCluster: Pool Fabric Connection Rule
- Data ONTAP MetroCluster: RLM Configuration Rule
- Data ONTAP MetroCluster: RLM Interface Ping Rule
- Data ONTAP MetroCluster: Tiebreaker Configuration Rule

OnCommand Plug-in for Microsoft monitors

The following list displays all of the OnCommand Plug-in for Microsoft base management pack monitors:

- Aggregate State Monitor
- Aggregate Space Utilization Monitor
- Controller Connection Monitor
- Controller Global Status Monitor
- Controller HA Status Monitor
- Critical Trap Monitor
- Disk State Monitor
- Emergency Trap Monitor
- Enclosure State Monitor
- Fan State Monitor
- Informational Trap Monitor
- LUN State Monitor
- Power Supply State Monitor
- Processor Utilization Monitor
- Qtree Quota Monitor
- Qtree SnapMirror Monitor
- SnapMirror Status Monitor
- vFiler Monitor
- Volume Inode Utilization Monitor
- Volume Quota Monitor
- Volume SnapMirror Monitor
- Volume Space Utilization Monitor
- Volume State Monitor
- Warning Trap Monitor

OnCommand Plug-in for Microsoft PRO monitors

The following list displays all of the OnCommand Plug-in for Microsoft PRO management pack monitors:

- Data ONTAP PRO: Hyper-V Virtual Machine Replication Not Replicated Monitor
- Data ONTAP PRO: Hyper-V Virtual Machine Replication Status Monitor
- Data ONTAP PRO: Hyper-V Virtual Machine Thin Provisioning Configuration Monitor

- Data ONTAP PRO: Hyper-V Virtual Machine Used Space Rate Monitor
- Data ONTAP PRO: LUN Online Monitor
- Data ONTAP PRO: LUN Used Space Monitor
- Data ONTAP PRO: Snapshot Auto-Delete Disabled Monitor
- Data ONTAP PRO: Space Reservation Monitor
- Data ONTAP PRO: Volume ASIS Enabled Monitor
- Data ONTAP PRO: Volume ASIS Licensed Monitor
- Data ONTAP PRO: Volume Online Monitor
- Data ONTAP PRO: Volume Space Utilization Monitor

Finding Data ONTAP management pack rules

You can find the Data ONTAP management pack rules so that you can verify successful import into System Center Operations Manager or to override the rules as necessary.

Before you begin

You must have correctly imported the appropriate OnCommand Plug-in for Microsoft management packs into System Center Operations Manager.

Steps

1. From the **Authoring** pane, select **Rules**.
2. In the **Name** column, go to **Type: Management Server** and search for **Data ONTAP**.

What discovery is

OnCommand Plug-in for Microsoft utilizes rules that discover storage controllers, their associated objects, and their configurations so that you can monitor the state of each object and troubleshoot where necessary.

The main discovery rule (**Data ONTAP: Discovery Rule**) is disabled by default as Microsoft recommends. After you import the management packs, you can enable this rule on a Microsoft System Center Operations Manager management server by overriding the setting and selecting the management server that manages Data ONTAP objects.

If your storage system is running a Data ONTAP version earlier than 7.3, you must use SNMP version 1 for discovery rule support. If your storage system is running Data ONTAP 7.3 or later, SNMP versions 1, 2C, and 3 are supported for use with OnCommand Plug-in discovery rules.

OnCommand Plug-in ignores traditional volumes during the discovery process.

Types of discovery

You can use storage discovery, PRO discovery, virtualization discovery, and MetroCluster discovery to discover storage controllers and their associated objects in each type.

OnCommand Plug-in for Microsoft provides the following types of discovery:

Storage discovery	Storage discovery is accomplished when Data ONTAP storage devices are discovered as network devices by the built-in Microsoft System Center Operations Manager discovery wizard using SNMP. The controllers are recognized as Data ONTAP storage devices and, if valid credentials are set in the System Center Operations Manager database, the storage devices in these controllers are discovered.
Data ONTAP Virtualization discovery	Data ONTAP virtualization discovery finds storage on all Hyper-V hosts in SCVMM, including Hyper-V Hosts, Hyper-V LUNs, Hyper-V virtual machines, and Hyper-V virtual hard disks.
Data ONTAP PRO discovery	For PRO discovery, we create PRO targets based on the items that were discovered in virtualization discovery. Virtualization discovery logs an event to trigger off PRO discovery so that both discoveries are always done sequentially.
MetroCluster discovery	The MetroCluster management pack is an optional pack with a separate discovery process. The MetroCluster discovery process uses controller objects that were already discovered by the Data ONTAP management pack.

Expediting storage discovery

If you choose not to wait for the automated discovery process, which runs every four hours, or you have modified the storage systems being monitored, you can expedite the storage discovery process by manually running storage discovery.

Before you begin

Before you perform system discovery, the OnCommand management pack must already be installed and you must have entered valid credentials for the newly added storage systems.

Steps

1. Navigate to the Microsoft System Center Operations Manager **Monitoring** pane.
2. Select the **Management Server** view.
3. Select the management server on which discovery is enabled.
4. In the **Actions > Health Services Tasks** pane, select **Data ONTAP: Run Discovery Task**.

Expediting virtualization discovery

You can perform virtualization discovery without an agent on every Hyper-V host. You can run the Data ONTAP Virtualization: Discovery Rule to perform virtualization discovery.

About this task

Perform the following steps to invoke the Data ONTAP Virtualization: Discovery Rule manually.

Steps

1. Navigate to the **Management Server** view under the Data ONTAP node.
2. Click on the **Data ONTAP Virtualization: Run Virtualization discovery task** on the management server.

After you finish

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 you must have the OnCommand Discovery Agent installed on a Hyper-V host:

- If the Hyper-V host has LUNS with a Data ONTAP version earlier than 7.3.1.

- If the Hyper-V host has *Fibre Channel mapped LUNs*.
- If the Hyper-V host has dedicated LUNs with volume GUID and the SCOM server is not running Windows 2008 R2

Managing storage controller information

There are many tasks that you must do to maintain your storage controllers including adding, removing, and configuring storage controllers. You will also need to manage the storage controller credentials and modify that credential information. Finally, you must configure SNMP if you want to receive SNMP traps.

Adding a storage controller

You can add storage controllers so that OnCommand Plug-in for Microsoft can monitor their performance and health. Although new controllers are automatically added during scheduled discovery, you can add them manually at any time.

About this task

You cannot use this procedure to add a vFiler. To add a vFiler you must add the parent controller and the vFilers will automatically be discovered.

Steps

1. From the **Monitoring** pane, select **Diagram View**.
2. From the **Actions > Data ONTAP Controller Group Tasks** pane, select **Add Controller**.
3. From the drop-down menu, select the appropriate management server.
4. Specify the SNMP community string.
5. Specify the name or IP address of the storage controller you want to add and click **Add**.

After you finish

After adding a storage controller, you must use the **Data ONTAP: Manage Controller Credentials** action to set the credentials.

Managing storage controller credentials

You can set credentials for all of the NetApp storage controllers and vFilers that you want to monitor from either the Diagram View or the Controllers View in the Monitoring pane. You can change these credentials as necessary.

About this task

HTTPS is the default protocol that the connection uses to connect to the storage controller but you must have socket security layer (SSL) set up and enabled. If SSL is not set up and enabled, the

connection uses the HTTP protocol. If you want to connect to a vFiler, you must use the HTTP protocol.

Steps

1. From the **Monitoring > Discovered Inventory** window, change the target type to **Management Server**.
2. Go to **Actions > Health Services Tasks > Data ONTAP: Manage Controller Credentials**.
3. Enter credentials for each storage controller that you want OnCommand Plug-in for Microsoft to monitor.

You can select multiple controllers at one time and set their passwords if they use the same credentials but you should not select both vFilers and controllers when you select multiple credentials.

If you have domain credentials for the storage controller, you should type the domain name in the Domain field and type the domain user name in the **User Name** field.

4. Click **OK**.

Removing a storage controller

You can remove storage controllers and objects such as aggregates, volumes and LUNs from OnCommand Plug-in for Microsoft when you no longer need to monitor their health and performance.

About this task

If you remove a storage controller or other object from the plug-in, you also remove it from the list of network devices. When you run the discovery process, the storage controller will no longer be discovered.

Steps

1. From the **Monitoring** pane, select **Controllers**.
2. In the **Controllers** pane, select the controller that you want to remove.
3. From the **Actions > Data ONTAP Controller Tasks** pane, select **Remove Controller** and click **OK**.

Configuring SNMP traps

If you want to receive SNMP traps using OnCommand Plug-in for Microsoft, you must first configure SNMP.

Before you begin

- If you use Windows 2008, you must have installed SNMP Service and SNMP WMI Provider.
- If you use Windows 2008 SP1, you must have installed Microsoft hotfixes 958936 and 967718.
- If you use Windows Server 2008 R1, you must have installed Microsoft hotfixes 958936 and 967718.
- If you use Microsoft Operations Manager 2007 SP1, you must have installed Microsoft hotfixes 951526 and 961363.

Steps

1. Navigate to **Server Manager > Configuration > Services > SNMP Service > Properties > Security** tab.
2. Ensure that **Accepted community names** contains the names of the SNMP communities you are configuring the storage systems to use, and ensure that they have read and create privileges.
3. Select **Accept SNMP packets from any host**.
4. On each managed storage system, enable SNMP.
5. If necessary, set up the community.
6. Configure the trap destination as your Microsoft Operations Manager root management server.
The SNMP monitors are targeted at the Data ONTAP Controller class.
7. Enable the non-emergency trap monitors using monitor overrides.

Modifying storage controller information using FilerView

To use the FilerView interface to change controller configuration information, you can select the storage controllers that are monitored by OnCommand Plug-in for Microsoft and then launch FilerView.

Before you begin

You must have installed and configured OnCommand Plug-in for Microsoft.

Steps

1. From the **Monitoring** pane, select either **State View** or **Diagram View**.
2. Select a storage controller group or storage controller.
3. From the **Actions > Data ONTAP Controller Tasks** pane, select **Launch FilerView**.

Monitoring your system

There are several ways that you can monitor the performance of your system. You can monitor alerts, events, and the performance of numerous functions. There are also PRO tips to inform you when particular events occur.

Alert monitoring

You can monitor alerts to locate and isolate problems with your storage systems and storage objects. You can also customize two rules, the volume latency rule and the LUN latency rule, to meet your specific needs.

OnCommand Plug-in for Microsoft includes numerous rules that monitor the health of various discovered Data ONTAP storage objects. If the parameters of a rule are broken, OnCommand Plug-in for Microsoft generates an alert and sends it to Microsoft Operations Manager. You can use the Controller performance collection rule, which is targeted at the Data ONTAP Controller class, to override these rules as necessary.

There are two customizable rules that are available for you to modify to better meet your needs:

- | | |
|--|--|
| Data ONTAP:
Volume Latency Rule | This rule triggers an alert based on when the average volume latency exceeds a critical threshold. This rule runs by default every 30 minutes. |
| Data ONTAP: LUN
Latency Rule | This rule triggers an alert based on when the average LUN latency exceeds a critical threshold (default 500ms and 1000ms). This rule runs by default every hour. |

All other periodic monitoring rules are targeted at the Data ONTAP Management Server class.

You can find alerts, as well as locate the source of the alert, by looking at the Alerts View, Diagram View, or Controllers View windows.

Alerts View

You can view a list of every active alert found by OnCommand Plug-in for Microsoft; alternatively, you can view a list limited to the alerts specific to Data ONTAP storage. When you select an individual alert in one of these lists, you can view information about it in the Alert Details pane. You can launch Health Explorer in Microsoft Operations Manager to find the cause of the problem.

You can view active alerts by using any of the following options:

- | | |
|---|---|
| All active alerts view | You can view all alerts in the Monitoring > Active Alerts pane. |
| Data ONTAP storage
alerts view | You can view alerts specific to Data ONTAP storage in the Monitoring > Data ONTAP pane. |

Hyper-V VMs on storage alerts view

You can view alerts specific to Hyper-V virtual machine storage in the **Monitoring > Data ONTAP > Storage Systems > Alerts > Hyper-V VMs on Storage > Alerts** pane.

Alerts pane

You can view the alerts in the Alerts pane of the Dashboard.

Diagram View

You can view a pictorial representation of all of the storage and hardware currently being monitored by OnCommand Plug-in for Microsoft to enable you to isolate problems on a specific storage controller object.

You can expand the view for an individual storage controller or vFiler to display its associated objects so you can isolate problems to the exact component on which they occur. When you select a controller or associated object, you can view information about it in the Detail View window.

Controllers View

You can view a list and overall health of the storage controllers that OnCommand Plug-in for Microsoft is currently monitoring. When you select a controller, you can also view information about it in the Controllers View window. If a controller is in either a warning or critical state, you can launch the **Health Explorer** in Microsoft Operations Manager to find the root of the problem.

Overriding monitoring rules

You can adjust the frequency and timeout values of the monitoring rules as you scale your storage configuration to meet your needs.

Steps

1. In the **Authoring** window in Microsoft Operations Manager, select the rule you want to override.
2. In the **Rule Details** pane, click **View Knowledge**.
3. Click the **Override** tab and follow the directions in the tab window.

Performance monitoring

OnCommand Plug-in for Microsoft is designed to scale to large numbers of controllers. As the number of storage controllers increases, you can manage the monitoring load by changing the run frequency of the various discovery and monitoring rules.

If you run discovery and monitoring rules less frequently, you place less burden on the Microsoft Operations Manager infrastructure, but you receive less timely alert information. You should run discovery rules less frequently than monitoring rules to avoid situations where rules overlap and conflict with each other.

Performance metrics

OnCommand Plug-in for Microsoft monitors several performance metrics. You can use these metrics to monitor the state of your storage controllers and configurations, as well as to identify usage patterns.

Types of metrics include CPU utilization, space utilization, I/O operations, I/O throughput, latency, and protocols.

CPU utilization

You can use the **CPU utilization** graph to determine how much processing space you have used, how you have used it, and how much space you have left on your storage controllers.

The CPU utilization graphs display the following information:

Average processor utilization	Displays the average processor utilization percentage at specified time intervals and generates a threshold alert if two successive measurements are above the threshold specified.
CPU resource utilization	Displays the system CPU resource utilization percentage at specified time intervals.
Total processor utilization	Displays the total processor utilization percentage at specified time intervals.

Additional details are displayed in the Legend.

I/O operations

You can use the I/O operations graph to monitor the communication between your storage controllers and servers.

The I/O operations graph displays the following information:

Reads	Displays the read operations per second at specified time intervals.
Writes	Displays the write operations per second at specified time intervals.
Total reads/writes	Displays the total operations per second at specified time intervals.

Additional details are displayed in the Legend.

I/O throughput

You can use the **I/O throughput** graph to monitor the productivity of your storage controllers.

The I/O throughput graphs display the following information:

Disk data read	Displays the disk data read, in kilobytes per second, at specified time intervals.
-----------------------	--

Disk data written	Displays the disk data written, in kilobytes per second, at specified time intervals.
Network data received	Displays the network data received, in kilobytes per second, at specified time intervals.
Network data sent	Displays the network data sent, in kilobytes per second, at specified time intervals.

Additional details are displayed in the Legend.

Latency

You can use the **Latency** graph to monitor for any unusual delays among your storage controllers.

The latency graph displays the following information:

LUN latency	Displays the LUN read, write, and average latency at specified time intervals.
Read latency	Displays the average read latency, in milliseconds, at specified time intervals.
Write latency	Displays the average write latency, in milliseconds, at specified time intervals.
Total latency	Displays the average total latency, in milliseconds, at specified time intervals.
Volume latency	Displays the volume read, write, and average latency at specified time intervals.

Additional details are displayed in the Legend.

Protocols

You can use the **Protocols** graphs to determine how well the storage controllers perform based on its protocols.

The protocols graphs display the following information:

CIFS	Displays the number of CIFS operations per second at specified time intervals.
Fibre Channel	Displays the number of Fibre Channel operations per second at specified time intervals.
HTTP	Displays the number of HTTP operations per second at specified time intervals.
iSCSI	Displays the number of iSCSI operations per second at specified time intervals.
NFS	Displays the number of NFS operations per second at specified time intervals.

Additional details are displayed in the Legend.

Performance monitoring views

You can use different views in OnCommand Plug-in for Microsoft to monitor the state of your storage resources and to identify usage patterns. You can use the tasks listed in the Actions pane to perform specific tasks related to managing your storage.

Aggregates

You can view different attributes of your aggregates so that you can monitor their health and diagnose any issues at the aggregate level.

The following attributes display in the **Aggregates** view:

- State** Displays the state of the aggregate, according to System Center Operations Manager. States include Healthy, Warning, and Critical.
- Aggregate** Displays the aggregate name.
- Controller** Displays the fully qualified domain name (FQDN) of the controller to which the aggregate belongs.
- Total size** Displays the total size of the aggregate.
- RAID type** Displays the RAID type of the aggregate.
- Disk count** Displays the number of disks that belong to the aggregate.

Controllers

You can view different attributes of your storage controllers so that you can monitor their health and diagnose any issues at the controller level. OnCommand Plug-in for Microsoft displays only those storage controllers that are running supported versions of Data ONTAP.

The following attributes display in the **Controllers** view:

- State** Displays the state of the storage controller, according to System Center Operations Manager. States include Healthy, Warning, and Critical.
- Fully qualified domain name (FQDN)** Displays the fully qualified domain name of the storage controller.
- IP address** Displays the IP address of the storage system.
- Model** Displays the model type of the storage system.
- Version** Displays the version of Data ONTAP the storage system currently runs.
- Clustered** Displays whether the controller is in a High Availability (HA) pair.

Dashboard

You can use the **Dashboard** view to provide you with an overall picture of the state and health of your storage resources. This allows you to diagnose any potential issues regarding health and utilization using **Microsoft Health Explorer**.

The following attributes display in the **Dashboard** view:

Health Summary	Displays the number and state of all storage controllers and SnapMirror relationships.
Alerts	Displays the icon, name, and created date of the alerts.
Controllers	Displays information about all storage controllers that are currently monitored by OnCommand Plug-in for Microsoft.
vFilers	Displays information about all vFilers that are currently monitored by OnCommand Plug-in for Microsoft.
Storage Efficiency	Displays how efficiently the storage is currently being used by all storage controllers that are monitored by OnCommand Plug-in for Microsoft.
Storage Utilization	Displays the percentage of storage that is currently being used, broken down by aggregates, disks, spare disks, LUNs, qtrees, volumes, and deduplication volumes.

LUNs

You can view different attributes of your LUNs so that you can monitor their health and diagnose any issues at the LUN level.

The following attributes display in the **LUNs** view:

State	Displays the state of the LUN, according to System Center Operations Manager. States include Healthy, Warning, and Critical.
LUN	Displays the full path of the LUN.
Controller/vFile	Displays the fully qualified domain name of the controller or vFile to which the LUN belongs.
Total size	Displays the total size of the LUN.
Type	Displays the type of multi-protocol LUN, such as Windows or Linux.

Management Server

You can use this view for a variety of tasks including starting the manual storage discovery or PRO discovery processes, and managing the DFM servers and controller credentials.

The following attributes display in the **Management Server** view:

Name	Displays the name of the management server.
-------------	---

Qtrees

You can view different attributes of your qtrees so that you can monitor their health and diagnose any issues at the qtree level.

The following attributes display in the **Qtree** view:

State	Displays the state of the qtree, according to System Center Operations Manager. States include Healthy, Warning, and Critical.
Qtree	Displays the full name of the qtree.
Volume	Displays the name of the volume to which the qtree belongs.
Controller/vFiler	Displays the fully qualified domain name of the controller or vFiler to which the qtree belongs.
Security style	Displays the security style of the qtree. Security styles include UNIX, NTFS, or mixed.

SnapMirror status

You can view the status of all SnapMirror relationships that are monitored by OnCommand Plug-in for Microsoft.

The following attributes display in the **SnapMirror status** view:

State	Displays the state of the SnapMirror relationship, according to System Center Operations Manager. States include Healthy, Warning, and Critical.
Source	Displays the source location of the SnapMirror pair.
Destination	Displays the destination location of the SnapMirror pair.
SnapMirror State	Displays the state of the SnapMirror pair. The possible SnapMirror states include the following: • Uninitialized • SnapMirrored • Broken-Off • Quiesced • Source • Unknown
Lag	Displays the amount of time since the last SnapMirror transfer.

Storage utilization

You can use the **Storage Utilization** view to monitor how much space you have at the controller, aggregate, and volume levels. The **Storage Utilization** view tells you how much space you have used on your storage and provides you the information you need to make any necessary changes to utilize your space more efficiently.

The following attributes display in the **Storage Utilization** view:

Controller committed space	Displays the controller used-space percentage at specified time intervals.
-----------------------------------	--

Aggregate committed space	Displays the aggregate used-space percentage at specified time intervals.
Volume used space	Displays the volume used-space percentage at specified time intervals.
Legend	Displays a list of all controllers, aggregates, and volumes for which you can track space utilization.

vFilers

You can view a vFiler as an individual object with different characteristics than a physical controller. The **vFilers** view displays attributes including its storage, health roll up, and utilization.

The following attributes display in the **vFilers** view by default:

State	Displays the state of the vFiler. States include Healthy, Warning, and Critical.
FQDN	Displays the fully-qualified vFiler domain name.
Controller FQDN	Displays the fully-qualified domain name of the physical controller.
IP Address	Displays the IP address of the vFiler.
Status	Displays whether the vFiler is running.
Total Volumes	Displays the number and total size of the volumes.
Total Volume Size	Displays the number and total size of the volumes.
Total QTrees	Displays the number and total size of the QTrees.
Total LUNs	Displays the number and total size of the LUNs.
Total LUN Size	Displays the number and total size of the LUNs.

Volumes

You can view different attributes of your volumes so that you can monitor their health and diagnose any issues at the volume level.

The following attributes display in the **Volumes** view:

State	Displays the state of the volume, according to System Center Operations Manager. States include Healthy, Warning, and Critical.
Volume	Displays the volume name.
Aggregate	Displays the aggregate name.
Controller/vFiler	Displays the fully qualified domain name of the controller or vFiler to which the volume belongs.
Total size	Displays the total size of the volume.

Hyper-V Hosts

You can use the **Hyper-V Hosts** view to view all Hyper-V hosts that have monitored LUNs mapped to them.

The following attributes display in the **Hyper-V Hosts** view:

State	Displays the state of this Hyper-V host. States include Healthy, Warning, and Critical.
FQDN	Displays the fully-qualified domain name for the Hyper-V host.
Number of VMs	Displays the number of virtual machines hosted by the Hyper-V host.
Number of LUNs	Displays the number of LUNs hosted by the Hyper-V host.

Hyper-V LUNs

You can use the **Hyper-V LUNs** view to view all of the **Hyper-V LUNs** (all of the monitored LUNs that are mapped to Hyper-V hosts).

The following attributes display in the **Hyper-V LUNs** view:

State	Displays the state of the LUN. States include Healthy, Warning, and Critical.
Host	Displays the FQDN of the Hyper-V host to which LUN is mapped.
LUN path	Displays the LUN path, for example, <code>mycontroller:/vol/vol2/lun1</code> .
iGroup	Displays the iGroup name.
Controller	Displays the controller name. If there is no controller name, it displays the IP address.
Windows path	Displays the Windows drive path, mountpoint, or volume GUID. For example, <code>C:\ClusterStorage\Volume1</code> .
Cluster name	Displays the name of the cluster or N/A.
CSV path	Displays the path of the CSV or N/A.
Alignment status	Displays Aligned or unknown if the alignment cannot be determined.
Last alignment check	Displays the timestamp of the last check for misalignment.
Available space	Displays the space available on this LUN (from the host-side).
Used %	Displays the used space percentage for this LUN (from the host-side).
Total space	Displays the total space in the host-side file system.

Hyper-V VHDs

The **Hyper-V VHDs** view shows all Hyper-V virtual hard disks so that you can monitor their health and diagnose any issues at the virtual hard disk level.

The following attributes display in the **Hyper-V VHDs** view:

State	Displays the alignment of the VHDs and whether they are attached to a virtual machine. There are three possible states:
Healthy	The VHD is aligned.
Critical	The VHD is misaligned but attached to a virtual machine.
Warning	The VHD is misaligned but not attached to a virtual machine.
VHD path	Displays the path to the VHD.
Host	Displays, for an attached VHD, the name of the Hyper-V host that is hosting the virtual machine. Displays, for an unattached VHD, the name of the host where the VHD resides.
Path	Displays the VHD path key.

Hyper-V VMs

You can view different attributes of your monitored Hyper-V virtual machines so that you can monitor their health and diagnose any issues at the virtual machine level.

The following attributes display in the **Hyper-V VMs** view:

VM GUID	Displays the GUID of the virtual machine that was assigned by Hyper-V.
VM Name	Displays the name of the virtual machine.
VM FQDN	Displays the fully-qualified domain name of the virtual machine.
Host	Displays the FQDN of the Hyper-V host that is hosting the virtual machine.

Checking the alignment of your Hyper-V LUNs

To ensure the best performance of those virtual machines that are hosted on Hyper-V LUNs, it is important that the alignment check runs on a regular schedule. You can also periodically check the alignment of your Hyper-V LUNs on demand.

Steps

1. From the **Hyper-V LUNs** view, multi-select all the LUNs that you would like to check for misalignment.

2. Click **Data ONTAP Virtualization: Check LUN Alignment Status** in the **Actions** pane.

The SCOM Run Task dialog opens.

3. Click **Run** and the misalignment check process on the selected LUNs begins.

After you finish

You can dismiss the Run Task dialog box and monitor the progress of the LUN alignment check in the Task Status view to see the output of the tasks upon completion.

You can navigate to the Hyper-V LUNs view and launch the Health Explorer to view the details if any misaligned LUNs were found.

Checking the alignment of your VHDs

To ensure the best performance of those virtual machines that are hosted on VHDs, it is important that the alignment check is run on a regular schedule. You can also periodically check the alignment of the VHDs on demand.

About this task

You must have enabled Powershell remoting on all Hyper-V hosts to monitor your VHDs for alignment issues. To do this, run the `Enable-PSRemoting` cmdlet on all Hyper-V hosts. See the Microsoft TechNet website for details.

Steps

1. Navigate to the **Hyper-V VHDs** view and multi-select all the VHDs you want to check for misalignment.
2. Click **Data ONTAP Virtualization: Check VHD Alignment Status** in the **Actions** panel.

The SCOM Run Task dialog box opens.

3. Click **Run** and the check for misalignment on the selected VHDs begins.

You can dismiss the Run Task dialog box and monitor the progress of the VHD alignment check in the Task Status view to see the output of the tasks upon completion.

After you finish

You can navigate to the Hyper-V VHDs view. The State attribute displays the alignment of the VHDs.

How to launch Health Explorer for a controller

You can launch Health Explorer in Microsoft System Center Operations Manager 2007 so that you can determine the root of any NetApp storage-related issues.

Microsoft Health Explorer enables you to find information about the health of any of your storage objects. You can launch **Health Explorer** from any view.

Monitoring Operations Manager servers

Using OnCommand Plug-in for Microsoft, you can enable Microsoft System Center Operations Manager to monitor the state of NetApp Operations Manager servers.

Before you begin

You must have installed and configured OnCommand Plug-in for Microsoft.

Steps

1. From the **Monitoring** pane, select either **State View** or **Diagram View**.
2. Select a storage controller.
3. From the **Actions > Data ONTAP Controller Tasks** pane, select **Manage Data ONTAP DFM Servers**.
4. Add the NetApp Operations Manager server and click **Apply > OK**.

Using OnCommand Plug-in for Microsoft PRO tips

PRO tips are a type of alert that you can use on System Center Virtual Machine Manager (SCVMM) to notify you when storage-related problems occur in your virtual environment. If you choose, you can also enable PRO Tips to automatically repair many of those problems.

You must have an event log subscription to the SCVMM event log to receive problems related to virtual machines and CSVs. 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, you can configure PRO Tips to display in a pop-up window whenever a new tip is added.

Types of PRO Tips

OnCommand Plug-in for Microsoft has several types of PRO Tips to help you identify storage-related issues that occur between Data ONTAP LUNs, cluster-shared volumes (CSVs), and Hyper-V virtual machines. Some of the PRO Tips offer automatic remediation so that you can enable OnCommand Plug-in for Microsoft to fix the issue automatically if you choose.

The PRO Tips are generated at the host level unless the description states otherwise. The following PRO Tips are generated on the OnCommand Plug-in for Microsoft:

High LUN space utilization

This Tip is generated when space utilization on a LUN that is hosting one or more virtual machines crosses a specified threshold. The default threshold is 95 percent.

All nodes in a Hyper-V cluster must be monitored by Microsoft System Center Operations Manager. Information about the virtual cluster is collected from the active node. The LUN must be mapped to one or more drives on a host but must not be mapped to any other host.

Hyper-V protection is broken or long lag time

This Tip is generated when the volume in which a LUN resides has a broken SnapMirror relationship or a long lag time.

This Tip offers automatic remediation to perform a SnapMirror update.

Hyper-V VM space utilization rate

This Tip is generated when OnCommand Plug-in for Microsoft determines that storage space might soon be depleted on the volume on which a LUN resides.

The default threshold rate is two percent, indicating that the storage could be consumed within approximately 50 days. The default setting for displaying this Tip is once a day. A sampling rate of one day is used for the storage usage calculation.

You can configure both the threshold percentage rate and the frequency that the Tip is displayed.

There is no automatic remediation for this Tip.

Hyper-V VM not replicated

This Tip is generated when SnapMirror is licensed but is not enabled on a volume that contains LUNs that are hosting virtual machines.

LUN offline

This Tip is generated for a virtual machine if one or more storage system LUNs that serve that virtual machine is offline.

This Tip offers automatic remediation to bring the LUNs back online.

LUN-type igroup-type misconfiguration

This Tip is generated when the Hyper-V LUN type and the igroup type are mapped incorrectly between the storage system and the Hyper-V host for either Windows or non-Windows types.

If OnCommand Plug-in for Microsoft determines that the igroup type and LUN type are the incorrect Windows type, the plug-in generates a warning tip. If OnCommand Plug-in for Microsoft determines that the LUN type and igroup type are the incorrect non-Windows types, it generates a critical tip. This PRO Tip is generated only when the installed version of Data ONTAP supports Hyper-V LUN and igroup types.

Misaligned LUNs or misaligned unattached VHDs

These are two separate PRO Tips: The misaligned LUNs PRO Tip is at the host level and the misaligned VHDs PRO Tip is at the virtual machine level if the VHDs are attached or the host level if the VHDs are unattached.

Thin provisioning LUN space reservation enabled	This Tip is generated when the LUN space reservation setting is enabled on LUNs that are hosting virtual machines. To provide thinly provisioned LUNs, the LUN space reservation must be disabled. This Tip offers automatic remediation to disable LUN space reservation.
Thin provisioning Snapshot auto delete disabled	This Tip is generated when automatic deletion of Snapshot copies is not set for volumes that contain LUNs hosting virtual machines. This Tip offers automatic remediation to enable automatic Snapshot copy deletion on the volumes.
Thin provisioning volume autogrow for volumes hosting Hyper-V VMs	This Tip is generated when the volume autogrow parameter is not set for volumes that contain LUNs that are hosting virtual machines. This Tip offers automatic remediation to enable volume autogrow.
Volume deduplication not enabled	This Tip is generated for a virtual machine when deduplication is licensed but not enabled on a storage controller that hosts storage system volumes that serve two or more virtual machines. This Tip offers automatic remediation to enable deduplication on the affected volumes.
Volume deduplication not licensed	This Tip is generated for a virtual machine when deduplication is not licensed on a storage controller that hosts storage system volumes that serve two or more virtual machines. This Tip does not provide automatic remediation, but it recommends that you install a deduplication license in virtualized environments.
Volume offline	This Tip is generated for a virtual machine when one or more storage system volumes serving that virtual machine is offline. This Tip offers automatic remediation to bring the volumes back online.
Volume space utilization exceeded threshold	This Tip is generated for a virtual machine when one or more storage system volumes that serve that virtual machine is full. This Tip offers two configurable thresholds: a warning level that defaults to 95 percent and a critical level that defaults to 99 percent. This Tip offers automatic remediation to increase the volume size so that space utilization is reduced to 85 percent. The Tip also recommends that the virtual machine be paused by the SCVMM administrator to avoid running out of space.

Implementing PRO Tips automatically

To ensure that problems are resolved quickly, you can configure PRO Tips to automatically implement solutions for storage-related problems in your virtual environment.

Before you begin

Before you can implement PRO Tips, you must have installed the OnCommand Plug-in for Microsoft PRO management pack and enabled the Data ONTAP PRO discovery rule.

Steps

1. In the **Microsoft Virtual Machine Manager > Administration** pane, select **PRO Tips**.
2. In the **PRO Settings** window, select **Automatically Implement**.
3. To determine when PRO Tips are implemented, select either **Critical Only** or **Warning and Critical**.
4. Click **OK**.

Implementing PRO Tips manually

You can implement PRO Tips manually to resolve one or more storage-related problems. You can use this option to control when a solution is implemented.

Before you begin

Before you can use PRO Tips, the following requirements must be met:

- You must have installed the OnCommand Plug-in for Microsoft PRO management pack.
- You must have enabled the Data ONTAP discovery rule.
- You must have enabled PRO Tips.

Steps

1. From the SCVMM tool bar, select **PRO Tips**.
2. In the **PRO Tips** window, select one or more tips to implement.
3. Click either **Implement** or **Dismiss**.

Events

You can use the Events window to view information about the events that OnCommand Plug-in for Microsoft has logged. OnCommand Plug-in for Microsoft monitors rules and logs events based on how you have configured the rules.

Each event displays the following information:

Level	The event level either Information, Warning, or Critical
Date and Time	The date and time, in the format <i>mm/dd/yyyy hh:mm:ss tt</i>
Source	The service or originator of the event
Name	The name of the Operations Manager server on which the event occurred
User	The account the event used
Event Number	The unique number for the event type
Log Name	The name of the log to which the event was sent, either the Data ONTAP MP Log or the Data ONTAP Debug Log

The Details view in the Events window displays standard Microsoft System Center Operations Manager details that summarize the event information.

Availability events

You can view availability events that are triggered by rules that you have configured to run. A monitor sends out an event to show you the state of your storage resources.

The Availability Events view displays information for the following rules:

- LUN state rule
- Disk state rule
- Aggregate state rule
- Controller global status rule
- Volume state rule
- Shelf state rule
- Fan state rule
- Power supply state rule
- High availability state rule
- SnapMirror state rule
- SNMP trap rule

Configuration events

You can view configuration events that are triggered by rules that you have configured to run. A monitor sends out an event to show you how your storage resources are configured.

The Configuration Events view displays information for the following rules:

- Discovery rule
- Controller connection configuration rule
- High availability (HA) configuration rule
- SnapMirror configuration rule

MetroCluster monitoring

OnCommand Plug-in for Microsoft includes an optional MetroCluster management pack containing MetroCluster TieBreaker Manager and MetroCluster Recovery Assistant. These components monitor MetroCluster pairs and allow you to configure and initiate Cluster Failover on Disaster (CFOD) operations.

MetroCluster TieBreaker Manager	MetroCluster TieBreaker is a Windows service that you can install on the Microsoft System Center Operations Manager host server to monitor all discovered MetroClusters. MetroCluster TieBreaker detects failures that prevent a normal MetroCluster failover and forcibly trigger failover. You must enable this service manually after installation using the Windows Service Management utility. You can use MetroCluster TieBreaker Manager to determine which MetroCluster pairs you want to monitor and which conditions automatically trigger a failover.
MetroCluster Recovery Assistant	MetroCluster Recovery Assistant helps you reassemble a cluster after a Cluster Failover on Disaster (CFOD) event by directing you through the steps necessary to reestablish normal MetroCluster operation. After a disaster failover of a MetroCluster, you must rejoin and resynchronize the mirrored aggregates. This process can take several hours, during which MetroCluster Recovery Assistant displays the state of the cluster and the aggregate mirrors on each side as the operation progresses. You can use MetroCluster Recovery Assistant to manually initiate CFOD operations when the TieBreaker tool is not used or if it did not trigger a failover.

Guidelines for using the MetroCluster TieBreaker Manager

Before you use the MetroCluster TieBreaker Manager, you must decide on a cluster poll interval and a recovery point objective, and you must enable fencing.

Cluster poll interval	You can change the interval at which the TieBreaker service checks the health of a specific MetroCluster pair. The minimum interval is every 10 seconds, the maximum interval is every 600 seconds, and the default interval is every 30 seconds.
Recovery point objective	A predetermined set of conditions must occur in a set period of time before a disaster failover can occur. These conditions include the inability to contact a member of the MetroCluster, the degradation of the root aggregate mirror on the remaining MetroCluster member, a cluster status of Error or Waiting, and the cluster interconnect being down. The recovery point objective (RPO) is the window of time during which all of the conditions must occur. The minimum interval is every 60 seconds, the maximum interval is every four hours, and the default interval is every 600 seconds.

Incorrect setting of the RPO interval can result in inconsistent data on the primary and disaster recovery copy. An automated failover under this condition leads to presenting stale data, which could cause the application to crash.

Fencing Before bringing a failed-over storage controller back online, you need to rejoin and resynchronize the aggregate mirrors in the MetroCluster to prevent possible data corruption. To do so, you can use the fencing option to fully power-down the failed-over storage controller using the remote LAN module (RLM) interface. The storage controller must contain RLM cards to use this option. If you use the fencing parameter and it fails, the tiebreaker service does not initiate disaster failover.

Using the MetroCluster TieBreaker Manager

You can use MetroCluster TieBreaker Manager to choose which MetroCluster pairs the TieBreaker service monitors, and to configure the conditions under which the TieBreaker service initiates the Cluster Failover on Disaster operation.

Before you begin

You must have imported and installed the MetroCluster management pack.

About this task

You should install the TieBreaker Manager on a System Center Operations Manager server at a separate location from either MetroCluster site, so that it operates as an objective arbiter of MetroCluster availability.

Steps

1. From the **Monitoring** pane, select **MetroClusters > State View**.
2. From the **Actions > Data ONTAP MetroCluster Pair Tasks** pane, select **MetroCluster TieBreaker Manager**.
The MetroCluster TieBreaker Settings dialog box opens.
3. Select the MetroCluster pair for which you want to configure the tiebreaker service.
4. To enable tiebreaker features, click the **Enable TieBreaker** check box.
5. Optional: Change the value in the **Cluster poll interval** box.
6. Optional: Change the value in the **Recovery point objective** box.
7. Optional: Click the **Require Fencing** check box.
8. Enter the Remote LAN Module (RLM) user name and password for each of the cluster members.
9. Click **Apply** and then click **OK**.

Result

The parameters are saved into the Microsoft System Center Operations Manager database. The TieBreaker service reads the parameters every 15 minutes and updates operations as necessary.

Reassembling a failed-over cluster

You can use the MetroCluster Recovery Assistant to assist you in reassembling a cluster after it has failed over. You can also view the status of a MetroCluster and its mirrored aggregates or manually initiate a cluster failover on disaster event.

Before you begin

You must have imported and installed the MetroCluster management pack.

Steps

1. From the **Monitoring** pane, select **MetroClusters > State View**.
2. Select the MetroCluster you want to recover.
3. From the **Actions > Data ONTAP MetroCluster Pair Tasks** pane, select **MetroCluster Recovery Assistant**.

The MetroCluster Recovery Assistant dialog box opens.

4. Click **Help** and follow the steps to restore the MetroCluster to normal operation.

Reports

Using OnCommand Plug-in for Microsoft, you can view reports about different aspects of your storage over a specific period of time.

You can view the following reports:

**Data ONTAP
Aggregate Storage
Utilization Report**

Displays up to 50 aggregates with the highest or lowest storage utilization on all monitored controllers over a specific period of time. The report defaults to the highest aggregate storage utilization. The default time period is from the first day of the month to the current day, and the default number of aggregates is five.

**Data ONTAP
Controller Average
System Latency Report**

Displays the average I/O or network latency of the top five user-configurable storage controllers over a specific period of time. The default time period is from the first day of the month to the current day. This report assists you to determine if you can load-balance more effectively.

**Data ONTAP
Controller Rate Of
Storage Utilization
Report**

Displays the rate at which storage controller utilization changes over a specific period of time. The default time period is from the first day of the month to the current day.

**Data ONTAP
Controller Storage
Utilization Report**

Displays the amount of free space of the top five user-configurable storage controllers over a specific period of time. The default time period is from the first day of the month to the current day.

**Data ONTAP
Controllers Availability
Report**

Displays the controller availability on one or more monitored storage controllers over a specific period of time. The default time period is from the first day of the month to the current day. The report selects all monitored storage controllers if none are selected.

**Data ONTAP Group
Average System
Latency Report**

Displays the average I/O or network latency of all monitored storage controllers over a specific period of time. The default time period is from the first day of the month to the current day.

**Data ONTAP Group
Storage Utilization
Report**

Displays the storage utilization for all monitored storage controllers over a specific period of time. The default time period is from the first day of the month to the current day.

**Data ONTAP Most
Common Alerts Report**

Displays up to 50 of the most common alerts on all monitored storage controllers over a specific period of time. The default time is from the first day of the month to the current day, and the default number of alerts shown is five.

**Data ONTAP
SnapMirror Average
Lag Time Per
Controller Report
(Unit: Hours)**

Displays the average lag time, in hours, of all SnapMirror relationships per storage controller over a specific period of time. The default time period is from the first day of the month to the current day.

**Data ONTAP
SnapMirror Longest
Lag Time Report (Unit:
Hours)**

Displays the five SnapMirror relationships with the longest lag time, in hours, over a specified period of time. Both the source and destination storage controllers must be monitored.

**Data ONTAP
Virtualization LUN
Alignment Report**

Displays a summary of alignment statuses for Hyper-V LUNs over a specific period of time. The default time period is from the first day of the month to the current day.

**Data ONTAP
Virtualization VHD
Alignment Report**

Displays a summary of alignment statuses for Hyper-V VHDs over a specific period of time. The default time period is from the first day of the month to the current day.

**Data ONTAP Volume
Storage Utilization
Report**

Displays up to 50 volumes with the highest or lowest storage utilization on all monitored controllers over a specific period of time. The report defaults to the highest volume storage utilization. The default time period is from the first day of the month to the current day, and the default number of volumes is five.

Viewing reports

You can view reports generated by OnCommand Plug-in for Microsoft by using the **Reports** tab of System Center Operations Manager.

Before you begin

You must have installed and imported the Data ONTAP Reports Management Pack.

Steps

1. From the **Reporting** pane, click **Data ONTAP Reports**.
2. Right-click the report you want to view.

Custom reports

With OnCommand Plug-in for Microsoft, you can create custom reports to monitor your system.

You can create reports to monitor the LUNs, virtual machines, and cluster-shared volumes (CSVs) on your system. You can use the following statistics in addition to the numerous other statistics that OnCommand Plug-in for Microsoft monitors to create custom reports:

- Volume space utilization
- Volume latency
- LUN space utilization
- LUN latency

There are no reports that are generated specifically for CSVs; they are the same as the reports generated for other LUNs. If you want to generate reports for CSVs only, you can write a Microsoft System Center Operations Manager filter for the LUNs that you want to use in the reports or you can manually select the CSVs as objects to report on in the Reporting window.

Overview of using PowerShell cmdlets

The Windows PowerShell interface is a scripting shell that you can use to manually call cmdlets in the OnCommand Plug-in for Microsoft. The PowerShell cmdlets can be used to manage, administer, and protect your data; however you must be prepared before you begin working with them. It is important to know about the execution policies and profiles and how to add and maintain system credentials.

Windows PowerShell execution policies and administration profiles

To be able to run cmdlets automatically from Windows PowerShell, you must first set execution policies to correct levels and create administrator profiles on your local host. If you do not set the policies correctly, you might not be able to run the cmdlets securely or at all.

PowerShell Execution Policies

The following list includes the possible values for Windows PowerShell execution policies:

- | | |
|---------------------|--|
| Restricted | Restricts any scripts from being run, downloaded, or installed. |
| AllSigned | Allows scripts that have been verified with security certificates to run. |
| RemoteSigned | Allows scripts to be run, downloaded, or installed. This policy is not secure and malicious code can easily exploit and damage any PowerShell .ps1 or VB script files. |

By default, the Windows PowerShell execution policies are set to **Restricted**. To run the cmdlets securely, you should set the Windows PowerShell execution policy to **AllSigned**.

For more information about how to set Windows PowerShell execution policies, see the Microsoft TechNet site.

PowerShell Administration Profiles

You must import the SCCmdlets module into your local Windows PowerShell profile if you want them to be available from any Windows PowerShell session. This enables you to use the SCCmdlets module through PowerShell sessions from Microsoft applications, such as System Center Virtual Machine Manager and System Center Operations Manager. For more information on Windows profiles, see the *Windows PowerShell Owner's Manual* on the Microsoft TechNet site.

Related information

Microsoft System Center - <http://technet.microsoft.com>

Standard optional cmdlet parameters

You can use optional standard parameters with cmdlets to control the amount of output you want to display. You can specify if you want the cmdlet to return many screens of data or only return minimal information.

Cmdlets and parameters are not case-sensitive.

-Verbose This optional parameter provides detailed output when displaying information.

-Quiet This optional parameter stops any output from displaying.

Note: Even with the `quiet` parameter specified, failed commands still display their failure message.

-Debug Provides additional information to assist with troubleshooting and maintenance.

For more information, see the *Microsoft Technet website*.

Provisioning and cloning

You can use provisioning and cloning cmdlets with Microsoft System Center Virtual Machine Manager (SCVMM) applications to provision storage, import and export virtual machine configurations, support generic cloning and export cloned virtual machines, all of which help improve performance and space-efficiency on your Hyper-V virtual machines.

Some features of OnCommand Plug-in for Microsoft provisioning and cloning include the following functionality:

- Cloning into new multiple LUNs
- Cloning into the same source LUN
- Cloning into a new single LUN
- Cloning into an existing single LUN

Provisioning and cloning prerequisites

Before you can implement provisioning and cloning in your Hyper-V environment, you must meet requirements such as those relating to access, architecture, and available software.

You must meet the following prerequisites to use provisioning and cloning:

- For Fibre Channel, initiators must be logged in to the target port.
- For cmdlets to operate on remote hosts, the following factors must be true:
 - You must have local administrator privileges on the remote host.
 - The remote host must be in a trusted domain or the same system as that from which the cmdlet is launched.
- Microsoft Virtual Disk Service (VDS) must be installed and enabled.
- Microsoft Remote Procedure Call (RPC) Server must be enabled and started.
- Microsoft Distributed Component Object Model (DCOM) must be configured to allow VDS access from the remote computer.
- The host name must always be the FQDN (fully-qualified domain name) or a shortname that is DNS resolvable.
- The storage system name must be the FQDN, the shortname, or the IP address.
- Provisioning and cloning operations with cluster shared volumes (CSVs) can be initiated only on the CSV owner node of a particular storage resource.
- The source and destination LUNs for the cloning operation must reside in the same storage volume.
- The destination NTFS for the cloning operation must have enough space to hold the cloned virtual machine data.

- To monitor your VHDs for alignment issues, you must have enabled Powershell remoting on all Hyper-V hosts.
To do this, run the `Enable-PSRemoting` cmdlet on all Hyper-V hosts. See the Microsoft TechNet website for details.

Provisioning and cloning cmdlets

You can use the provisioning and cloning cmdlets to improve performance and space-efficiency on your Hyper-V virtual machines.

- `Add-OCStorageSystem`
- `Connect-OCStorage`
- `Disconnect-OCStorage`
- `Get-OCStorage`
- `Get-OCStorageSystem`
- `New-OCClone`
- `New-OCCloneFile`
- `New-OCStorage`
- `Remove-OCStorage`
- `Remove-OCStorageSystem`
- `Remove-OCVM`
- `Set-OCStorageSize`

Disaster recovery

Crash consistent disaster recovery uses SnapMirror to replicate data across primary and secondary sites in a disaster. When virtual machines that are running on stand-alone or clustered Hyper-V hosts on a primary site fail, you can fail over to a secondary site by initiating a PowerShell cmdlet or Opalis failover workflow that allows the virtual machines to function from a replicated or mirrored secondary site.

Requirements and prerequisites for disaster recovery

There are some important requirements and prerequisites that you must meet before you can use the disaster recovery functionality of OnCommand Plug-in for Microsoft.

Requirements

Your environment must meet the following requirements for you to use crash consistent disaster recovery:

- All disaster recovery virtual machines must be on NetApp storage.
- The secondary site must be used for the sole purpose of disaster recovery.
- Only an administration user from the host can invoke disaster recovery cmdlets.
- You can use the credentials stored in the credential file to invoke storage-side operations regardless of which user is logged in on the host.
- To monitor your VHDs for alignment issues, you must have enabled Powershell remoting on all Hyper-V hosts.
To do this, run the `Enable-PSRemoting` cmdlet on all Hyper-V hosts. See the Microsoft TechNet website for details.

Prerequisites

For replication, your system must meet the following prerequisites:

- The Data ONTAP version on the secondary storage system must be the same version or later than that on the primary storage system.
- For each volume on the primary storage system, a corresponding volume with equal or greater size must exist on the secondary storage system.
- Each source should have a unique destination.
Therefore, for each volume on the primary storage system, there must be a corresponding volume on the secondary storage system of equal or greater size.
- All replication cmdlets are invoked from the Hyper-V host rather than a source or destination storage system.

- All replication cmdlets can be used either as part of the disaster recovery plan or as stand-alone SnapMirror CLI equivalents for the following uses:
 - Microsoft PowerShell script or Opalis clients
 - Workflows or automation that uses SnapMirror only

For disaster recovery, your system must meet the following prerequisites:

- The Web services login account must have administrative privileges on the local and remote hosts or clusters on both the primary and secondary sites.
- Cross-domain trusts are required in these situations:
 - Because disaster recovery Web services and cmdlets can be invoked remotely, cross-domain trusts are required when more than one domain is participating in the disaster recovery configuration.
 - If the remote requesting host (for example, Opalis clients), primary site, and secondary site are members of more than one domain collectively, domain trusts are required.
 - Since disaster recovery Web services and cmdlets can be invoked remotely, cross-domain trust policies may be required within the primary or secondary sites when multiple clusters are present within either primary or secondary sites.

Disaster recovery cmdlets

You can use the disaster recovery cmdlets to replicate data across primary and secondary sites in a disaster and allow the virtual machines to function from the replicated or mirrored secondary site.

- Confirm-OCDRPlan
- Connect-OCDRLun
- Get-OCDRMirrorStatus
- Initialize-OCDRMirror
- Invoke-OCDRMirrorClear
- Invoke-OCDRFailback
- Invoke-OCDRFailover
- Invoke-OCDRMirrorBreak
- Invoke-OCDRMirrorQuiesce
- Invoke-OCDRMirrorResume
- Invoke-OCDRMirrorResync
- Invoke-OCDRMirrorReverseResync
- Invoke-OCDRMirrorUpdate
- New-OCDRPlan
- Reset-OCDRSite
- Restore-OCDRVM
- Start-OCDRSimulateFailover
- Stop-OCDRMirror

- Stop-OCDRSimulateFailover
- Update-OCDRPlan

The disaster recovery plan

The disaster recovery plan describes disaster recovery objects and determines how they behave during failover and failback. The plan is stored in a user-specified location as an XML file.

You create the plan on the primary site and it captures the information of the primary setup so that it can be used to replicate the configuration on the secondary site upon failover. The plan captures only the information that is required to perform failover and failback, including the following information:

- A list of the virtual machines on the primary site and the detailed virtual machine properties
- Storage information for the configuration of virtual machines, VHDs, and Snapshot data
- SnapMirror relationships for all volumes on the primary storage system on which the virtual machines are running
- The primary and secondary host- or cluster-related information

The disaster recovery plan is stored in an end-user specified path as an XML file. The naming convention pattern is `PrimaryServerOrCluster_SecondaryServerOrCluster_DRPlan.xml`.

There are three configuration cmdlets that relate to the disaster recovery plan:

New-OCDRPlan	Uses Web services to create a new disaster recovery plan
Confirm-OCDRPlan	Validates the current state of the secondary host against the data captured in the specified disaster recovery plan whenever the primary or secondary site configuration changes. The <code>Confirm-OCDRPlan</code> cmdlet checks the following factors: • Ensures that the secondary host is running a Windows 2008 R2 or later operating system and that the host type is the same as the live host • Ensures that virtual machine LUNs that are to be connected on the secondary site have valid LUN paths and SnapMirror relationships • The active SnapMirror status and the SnapMirror relationships and ensures that all the SnapMirror relationships have the <code>snapmirrored</code> status • The virtual machine cluster and configuration resources against the live virtual machine • Ensures there is no conflict with the cluster and configuration resources on the secondary host If a conflict is found in the mountpoints, the <code>Confirm-OCDRPlan</code> cmdlet checks the mountpoint that is connected in the secondary host to determine if it is connected to the required LUN on the secondary storage system • Whether the storage system credentials are configured for all the storage systems in the disaster recovery process on the secondary site

- Ensures that the Hyper-V role is enabled on the secondary host or cluster
- If the disaster recovery plan is created in the context of a cluster, it ensures that the cluster shared volume is active on the secondary cluster and that a valid cluster name and IP address resources are present and online

Update-OCDRPlan

You can use the `Update-OCDRPlan` cmdlet to update the plan.

Before you recreate the plan, you must ensure that any new storage system volumes have a corresponding volume on the secondary storage system.

The `Update-OCDRPlan` cmdlet has one parameter, `-Failback` that indicates the disaster recovery operation type. The default is `-Failover`.

The disaster recovery failover workflow

With crash consistent disaster recovery, when you experience a complete site failure of both the host and the storage, you can failover from a primary site to a secondary site with limited and reasonable downtime. The `Invoke-OCDRFailover` composite cmdlet runs several individual cmdlets to perform the failover.

Before you begin

- You must have created a disaster recovery plan, by running the `New-OCDRPlan` cmdlet on your primary site (site A), and stored it in a central location.
You can also replicate the plan to your secondary site (site B).
- You must have created new `SnapMirror` relationships from the secondary to the primary site with the `Initialize-OCDRMirror` cmdlet prior to the failover operation.
All mirror updates and initializations are asynchronous, so you must wait and ensure that the transfer is complete before you perform any additional operations. You can use the `Get-OCDRMirrorsStatus` cmdlet to check the status of the `SnapMirror` relationships.
- You must have updated the `SnapMirrors` with the `Update-OCDRMirror` cmdlet before you execute the detailed workflow.
This ensures that the latest data is transferred from the primary to the secondary site before the actual disaster recovery failover is performed.
- You must have run the `Update-OCDRPlan` cmdlet on the primary site (site A) to update the disaster recovery plan with the latest configuration information.

About this task

The `Invoke-OCDRFailover` composite cmdlet runs the following individual cmdlets to perform failover from the primary site (site A) to the secondary site (site B). No user intervention is required after the `Invoke-OCDRFailover` composite cmdlet is entered. Refer to the descriptions of the individual cmdlets in the OnCommand Plug-in 3.0 for Microsoft PowerShell Cmdlet Reference Guide for more details.

The following steps are run based on the disaster recovery plan.

Steps

1. The `Confirm-OCDRPlan` cmdlet is run to validate the secondary site (site B) before the failover begins.
2. The `Reset-OCDRSite` cmdlet is run with the `-Secondary` and `-Force` parameters specified to cleanup conflicting cluster resources and LUNs on the secondary site (site B).
3. The `Invoke-OCDRMirrorBreak` cmdlet is run to break all the `SnapMirror` relationships on the secondary site (site B).
4. The `Connect-OCDRLUN` cmdlet is run to connect all the LUNs on the secondary site (site B).
5. The `Restore-OCDRVm` cmdlet is run to restore all virtual machines on the secondary site (site B).

After you finish

After failover is complete and to prepare for failback, you must run the `Update-OCDRPlan` with the `-Failback` parameter specified to update the disaster recovery plan. Specify the `-PrimaryServer` as site B and the `-SecondaryServer` as site A.

For example,

`Update-OCDRPlan -Failback -PrimaryServer site_B -SecondaryServer site_A`

Then you must perform a failback operation to restore your original `SnapMirror` relationships from site B to site A.

The disaster recovery failback workflow

With crash consistent disaster recovery, after you failover from a primary site to a secondary site, you must perform a failback to restore the `SnapMirror` relationships from the secondary site to the primary site. The `Invoke-OCDRFailback` composite cmdlet runs several individual cmdlets to perform the failback.

Before you begin

- You must ensure that proper mirror relationships are established prior to the failback operation across your primary and secondary sites.
- If there is no data loss, you must enter the `Invoke-OCDRMirrorReverseResync` cmdlet on the secondary site (site A) to reverse all the relationships from site B to site A.
All transfers, initializations, and updates are asynchronous, so you must wait and ensure that the transfer is complete before you perform any additional operations. You can use the `Get-OCDRMirrorsStatus` cmdlet to check the status of the `SnapMirror` relationships.
- If there is data loss, you must use the `Initialize-OCDRMirror` cmdlet to create new `SnapMirror` relationships from site B to site A.

- You can update mirrors with the `Invoke-OCDRMirrorUpdate` cmdlet before you run the `Invoke-OCDRFailback` cmdlet.
This ensures that the latest data is transferred from the primary to the secondary site before the actual disaster recovery failback is performed.
- You must have run the `Update-OCDRPlan` cmdlet on the primary site (site B) to update the disaster recovery plan with the latest configuration information.

About this task

The `Invoke-OCDRFailback` composite cmdlet calls the following individual cmdlets to perform failback from the primary (site B) to the secondary site (site A). No user intervention is required after the `Invoke-OCDRFailback` composite cmdlet is entered. Refer to the descriptions of the individual cmdlets in the OnCommand Plug-in 3.0 for Microsoft PowerShell Cmdlet Reference Guide for more details.

The following steps are run based on the disaster recovery plan.

Steps

1. The `Confirm-OCDRPlan` cmdlet is run to validate the secondary site (site A) before the failback begins.
2. The `Reset-OCDRSite` cmdlet is run with the `-Force` parameter to cleanup conflicting cluster resources and LUNs on the secondary site (site A).
This activity only removes the virtual machine conflicting resources from the secondary site.
3. The `Invoke-OCDRMirrorBreak` cmdlet is run to break all the `SnapMirror` relationships on the secondary site (site A).
4. The `Connect-OCDRLUN` cmdlet is run to connect all the LUNs on the secondary site (site A).
5. The `Restore-OCDRVm` cmdlet is run to restore all virtual machines on the secondary site (site A).

After you finish

After the failback operation is complete, you should run the `Reset-OCDRSite` cmdlet with the `-full` parameter specified to clean up the previous primary site (site B). Then you should update the disaster recovery plan to ensure that it has the latest configuration information.

Troubleshooting

You can use tips to help solve common problems with consoles, storage controllers, and performance and resource optimization.

Tips for solving console issues

If you experience an issue with OnCommand Plug-in for Microsoft and the Microsoft System Center Operations Manager console, you can use tips to help find the source of the problem.

The following list provides common console issues and some tips you can use to solve them:

Console tasks do not start	Run the OnCommand Plug-in for Microsoft installer file on each computer that runs on the Microsoft System Center Operations Manager console.
Console tasks fail consistently	Ensure that you have the necessary credentials. Provide alternate credentials when prompted by the console task.
The Data ONTAP Storage Systems pane does not appear in the Microsoft Operations Manager Monitoring window	Ensure that you imported the Data ONTAP management pack.
Changes that are made to storage configuration are not reflected in the Microsoft System Center Operations Manager console	Run the Discovery rule again or wait for it to run automatically. By default, this rule runs once in a 24-hour period.
SNMP traps are not appearing in the Microsoft System Center Operations Manager console	Enable the non-emergency trap monitors globally or per storage controller. By default, they are disabled.
Alerts do not reappear after an issue reoccurs	Open Microsoft Health Explorer and select Reset Health . As a Microsoft System Center Operations Manager best practice, do not dismiss an alert without resetting its underlying monitor.
Network devices are not discovered when discovery timeout is increased	Ensure that you have done the following: • Used the correct SNMP version • Used the default timeout value of two minutes or a value less than five minutes • Run the System Center Operations Manager Discovery wizard

- Contact Microsoft for further assistance

Related information

www.microsoft.com

Tips for solving storage controller issues

If you experience an issue with OnCommand Plug-in for Microsoft and your storage controllers, you can use tips to help find the source of the problem.

Storage systems not found using the Discovery wizard

Ensure that you have enabled SNMP on the storage controllers and that the SNMP community string matches the one that you set on the storage controllers.

Storage controllers appear in the Network Device Monitoring window but not in the Data ONTAP Storage Systems pane

Enable the Data ONTAP Discovery Rule for the Microsoft Operations Manager management server and set the credentials for that server.

Storage controllers appear in the Network Device Monitoring window but not in the Data ONTAP credentials tool

Select **Show all network devices** in the **Data ONTAP Storage Systems** pane. This identifies any devices that OnCommand Plug-in for Microsoft does not support.

Storage controllers do not appear after running Data ONTAP discovery

When you use the System Center Operations Manager Discovery wizard, ensure that you have selected **Network Devices**. After discovery finishes and finds the devices that are not managed, you can select these network devices to be managed by the host proxy agent. This allows OnCommand Plug-in for Microsoft to discover your Data ONTAP storage controllers.

Storage controllers are not found using the Discovery wizard

Ensure that you have enabled SNMP on the storage controllers and that the SNMP community string matches the one that you set on the storage controllers.

Performance and resource optimization (PRO) issues

If you experience an issue with OnCommand Plug-in for Microsoft, you can use tips to help find the source of the problem.

PRO Tips do not appear Ensure that you have done the following:

- Imported the Data ONTAP management packs
- Enabled the Data ONTAP PRO Discovery Rule for the Microsoft System Center Operations Manager management server and set the credentials for that server
- Ensured that alerts appear in the Hyper-V virtual machines on the storage folder. If alerts appear, ensure that System Center Virtual Machine Manager is configured to receive PRO Tips from the System Center Operations Manager management server that runs OnCommand Plug-in for Microsoft.

Data ONTAP Virtualization: Hyper-V Host, LUN, Virtual Machine, or VHD or Data ONTAP PRO: Hyper-V Virtual Machine Storage objects are not present

- Ensure that the Data ONTAP management packs have been imported
- If your Hyper-V host does not meet the requirements for agentless monitoring, ensure that you have installed the OnCommand discovery agent on these hosts
- Ensure that your virtual machine VHD files reside on NetApp LUNs
- Ensured that your virtual machines are on and appear in Microsoft System Center Virtual Machine Manager

PRO Tip implementation fails Ensure that you have the necessary credentials.

PRO Tips do not generate

If you use Microsoft SQL Server 2008, ensure that you have installed the Microsoft SQL Server 2005 backward compatibility components, available in the Microsoft SQL Server 2008 Feature Pack. If you use Microsoft SQL Server 2005, you do not need to install the backward compatibility components. For more information, see the Microsoft Web site.

Related information

www.microsoft.com

Show Windows Installer log check box is not visible

If you use a Microsoft Windows Installer (MSI) version earlier than 4.0, you do not see the **Show the Windows Installer log** check box at the end of the installation.

If you download MSI version 4.0 or later, you can select the **Show the Windows Installer log** check box during installation to display the logs.

For more information, see the Microsoft Web site.

Related information

[*www.microsoft.com*](http://www.microsoft.com)

Copyright information

Copyright © 1994–2011 NetApp, Inc. All rights reserved. Printed in the U.S.A.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S.A. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark information

NetApp, the NetApp logo, Network Appliance, the Network Appliance logo, Akorri, ApplianceWatch, ASUP, AutoSupport, BalancePoint, BalancePoint Predictor, Bycast, Campaign Express, ComplianceClock, Cryptainer, CryptoShred, Data ONTAP, DataFabric, DataFort, Decru, Decru DataFort, DenseStak, Engenio, Engenio logo, E-Stack, FAServer, FastStak, FilerView, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexSuite, FlexVol, FPolicy, GetSuccessful, gFiler, Go further, faster, Imagine Virtually Anything, Lifetime Key Management, LockVault, Manage ONTAP, MetroCluster, MultiStore, NearStore, NetCache, NOW (NetApp on the Web), Onaro, OnCommand, ONTAPI, OpenKey, PerformanceStak, RAID-DP, ReplicatorX, SANscreen, SANshare, SANtricity, SecureAdmin, SecureShare, Select, Service Builder, Shadow Tape, Simplicity, Simulate ONTAP, SnapCopy, SnapDirector, SnapDrive, SnapFilter, SnapLock, SnapManager, SnapMigrator, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapSuite, SnapValidator, SnapVault, StorageGRID, StoreVault, the StoreVault logo, SyncMirror, Tech OnTap, The evolution of storage, Topio, vFiler, VFM, Virtual File Manager, VPolicy, WAFL, Web Filer, and XBB are trademarks or registered trademarks of NetApp, Inc. in the United States, other countries, or both.

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. A complete and current list of other IBM trademarks is available on the Web at www.ibm.com/legal/copytrade.shtml.

Apple is a registered trademark and QuickTime is a trademark of Apple, Inc. in the U.S.A. and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the U.S.A. and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the U.S.A. and/or other countries.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

NetApp, Inc. is a licensee of the CompactFlash and CF Logo trademarks.

NetApp, Inc. NetCache is certified RealSystem compatible.

How to send your comments

You can help us to improve the quality of our documentation by sending us your feedback.

Your feedback is important in helping us to provide the most accurate and high-quality information. If you have suggestions for improving this document, send us your comments by e-mail to doccomments@netapp.com. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support Telephone: +1 (888) 4-NETAPP

Index

A

- adding a storage controller 39
- administration profiles, Windows Powershell 67
- Aggregates view 47
- Alerts view 43
- alerts,
 - monitoring 43
 - PRO Tips 54
- alignment, checking 52, 53
- ApplianceWatch PRO, uninstalling 19
- availability events 58

B

- background installation 21
- background uninstallation 25

C

- cluster, reassembling 61
- cmdlets
 - overview 67
 - provisioning and cloning 70
 - standard optional parameters 68
- component descriptions 7
- configuration events 58
- configuring SNMP traps 41
- console issues, troubleshooting 77
- controller configuration information, modifying with FilerView 41
- Controllers view 44, 47
- controllers, adding 39
- CPU utilization 45
- custom reports 65

D

- Dashboard view 47
- Data ONTAP
 - reports 63
 - rules 31–33
- deploying OIPs 29
- Diagram view 44
- disaster recovery

- failback workflow 75
- failover workflow 74
- overview 71
- plan 73
- requirements and prerequisites 71
- discovery
 - expediting 36
 - rules 35
 - types 35
 - what is 35
- DRPlan 73

E

- events
 - availability 58
 - configuration 58
- Events window 57
- execution policies, Windows Powershell 67
- expediting
 - system discovery 36
 - virtualization discovery 36

F

- failback workflow 75
- failover workflow 74
- feature selection, silent installation 23
- FilerView, modifying storage controller information 41
- finding management pack rules 34

G

- guidelines
 - installing the plug-in 17
 - MetroCluster TieBreaker Manager 59

H

- Health Explorer, launching 53
- Hyper-V hosts view 51
- Hyper-V LUN alignment, checking 52
- Hyper-V LUNs view 51
- Hyper-V VHDs view 52
- Hyper-V VMs view 52

I

I/O

- operations 45

- implementing PRO Tips 57

- importing the OIP 27

installation

- guidelines 17

- quick start list 13

- requirements 15

- silent 21

- installing the plug-in 20

integration packs

- importing 28

- requirements for importing 27

interfaces

- Opalis integration packs (OIPs) 27

L

- latency 46

- launching Health Explorer 53

- list for installation, SCOM 13

- login credentials, setting 39

- LUN latency 43

- LUNs view 48

M

management pack

- monitors 31–33

- rules 31–34

- upgrading 19

- Management Server view 48

- metrics, performance 45

MetroCluster

- discovery 35

- monitoring 59

- Recovery Assistant 59, 61

- TieBreaker Manager 59, 60

- Microsoft PowerShell 71

- modifying storage controller information 41

monitoring

- alerts 43

- MetroCluster 59

- Operations Manager servers 54

- performance 44

- monitors, list of 31–33

O

- Opalis integration pack (OIP) 71

- Opalis integration packs (OIP)

- importing 27

- Opalis integration packs (OIPs)

- deploying 29

- importing 28

- interface 27

- requirements for importing 27

- uninstalling 29

- Operations Manager servers

- monitoring 54

- overrides, fixing 19

- overriding rules 44

- overview of cmdlets 67

P

- parameters, standard 68

performance metrics

- CPU utilization 45

- I/O operations 45

- I/O throughput 45

- latency 46

- protocols 46

- performance monitoring 44

- plan, disaster recovery 73

plug-in

- components 7

- installation 20

- troubleshooting 78

prerequisites

- disaster recovery 71

- provisioning and cloning 69

- PRO discovery 35

- PRO issues, troubleshooting 78

PRO tips

- implementing 57

PRO Tips

- implementing 57

- types 54

- using 54

- protocols 46

- provisioning and cloning

- prerequisites 69

- provisioning and cloning cmdlets 70

Q

- Qtrees view 48

- quick start list for installation 13

R

- removing storage controllers 40
- reports
 - custom 65
 - list of 63
 - viewing 64
- requirements
 - disaster recovery 71
 - installing the plug-in 15
- rules
 - finding 34
 - management pack 31–33
 - overriding 44
 - volume latency 43

S

- SCOM quick start list 13
- setting login credentials 39
- silent
 - installation 21
 - uninstallation 25
- SnapMirror status view 49
- SNMP traps, configuring 41
- storage controllers
 - adding 39
 - credentials 39
 - managing information 39
 - removing 40
 - troubleshooting issues 78
- storage discovery 35
- storage systems
 - Alerts view 43
 - Controllers view 44
 - Diagram view 44
- Storage Utilization view 49
- system discovery, expediting 36

T

- throughput 45
- tips
 - console issues 77
 - storage controller troubleshooting 78
- troubleshooting
 - consoles 77
 - PRO issues 78
 - storage controllers 78
 - windows installer log check box 79

U

- uninstalling
 - ApplianceWatch PRO 19
 - background 25
 - silent 25
 - the Opalis integration packs (OIPs) 29
 - the plug-in 25
- upgrading
 - the plug-in 19, 20
 - management packs 19
 - silent 21
 - the plug-in 19, 20
- using MetroCluster TieBreaker Manager 60

V

- vFilers view 50
- VHD alignment, checking 53
- views
 - Aggregates 47
 - Alerts 43
 - Controllers 44, 47
 - Dashboard 47
 - Diagram 44
 - Hyper-V hosts 51
 - Hyper-V LUNs 51
 - Hyper-V VHDs 52
 - Hyper-V VMs 52
 - LUNs 48
 - Management Server 48
 - Qtrees 48
 - SnapMirror status 49
 - Storage Utilization 49
 - vFilers 50
 - Volumes 50
- virtualization discovery 35, 36
- volume latency rule 43
- Volumes view 50

W

- what you can do with the plug-in 7
- Windows installer, show log check box 79
- Windows PowerShell
 - administration profiles 67
 - execution policies 67

