

OnCommand® Plug-in 3.1 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) 463-8277
Web: www.netapp.com
Feedback: doccomments@netapp.com
Part number: 215-06928_A0

Contents

OnCommand Plug-in for Microsoft components	9
Windows PowerShell execution policies and administration profiles	11
Common cmdlet parameters	12
What OIPs are	14
Preparation to use OnCommand Plug-in for Microsoft	15
Installation checklist for SCOM and OnCommand Plug-in for Microsoft	15
Installation requirements for OnCommand Plug-in for Microsoft	16
Guidelines for installing OnCommand Plug-in for Microsoft	18
Upgrade requirements	20
Uninstalling ApplianceWatch PRO 2.1 and 2.1.1 and OnCommand Plug-in for Microsoft 3.1	20
Installing and upgrading OnCommand Plug-in for Microsoft	20
Installing OnCommand Plug-in for Microsoft in silent mode	22
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 by using the wizard	25
Uninstalling OnCommand Plug-in 3.0 for Microsoft in silent mode	25
Importing and deploying the OIPs	27
Guidelines for using OnCommand virtual infrastructure management web service	27
Importing the OIPs to the integration server	27
Deploying Orchestrator integration packs to the Orchestrator runbook designer and server	28
Uninstalling and unregistering the OIPs from the runbook server	29
Configuring the plug-in	30
Adding controllers	30
Adding controller credentials	30
What storage discovery is	31
Enabling discovery	31
Running discovery	31
Expediting discovery	31

Locating Data ONTAP management pack rules	33
Lists of Data ONTAP management pack rules	34
Multiple management server environment	36
Configuring SNMP traps	36
Managing storage controllers	37
Managing storage controller credentials	37
Launching System Manager from the plug-in	38
Removing a storage controller	38
Monitoring your system	40
List of OnCommand Plug-in for Microsoft monitors	40
List of OnCommand Plug-in for Microsoft PRO monitors	41
Overriding monitoring rules	41
Alert monitoring	42
Alerts View	42
Diagram View	43
Controllers View	43
Performance monitoring	43
Performance metrics	43
Performance monitoring views	45
Monitoring Operations Manager servers	51
Using PRO tips	51
Types of PRO tips	51
Enabling PRO tips	54
Implementing PRO tips automatically	55
Implementing PRO tips manually	55
Events	56
Availability events	56
Configuration events	57
Reports	57
Viewing reports	59
Custom reports	59
Checking the alignment of your VHDs	60
Checking the alignment of your Hyper-V LUNs	60
How to launch Health Explorer for a controller	61
What Data ONTAP Toolkit Integration Pack activities are	62
Storage System cache credentials	63

Provisioning storage	64
Requirements for provisioning	64
The Connect Storage activity vs. the Provision Storage activity	65
Cloning storage	66
Requirements for cloning	66
What Sub-LUN cloning is	67
Activities for creating clones	67
File cloning	67
Virtual machine cloning	67
Clone a virtual machine from an SCVMM template	68
Situations for using the Clone VM activity	68
Situation 1: Creating clones from a LUN into a new LUN	68
Situation 2: Creating clones from a LUN into the same LUN	69
Situation 3: Creating a clone of a LUN into an existing CSV on a LUN	69
Disaster recovery cmdlets and activities	71
Requirements for disaster recovery	71
What the disaster recovery plan is	72
Requirements for creating and updating disaster recovery plans with cmdlets	72
Disaster recovery plan guidelines	73
Cmdlets and activities used with the disaster recovery plan	73
Granular vs. composite workflows	74
Failover and failback requirements	74
Failover workflow breakdown	75
The disaster recovery failover workflow	78
Disaster recovery failback workflow	79
The consecutive failover workflow	80
What the Start Test DR Failover activity does	82
Usage tips	84
Tips for solving SCOM console issues	84
Tips for solving storage controller issues	85
Troubleshooting	86
The specified destination server is not managed by an SCVMM server	86
Troubleshooting Orchestrator	86
Troubleshooting cloning	87
Troubleshooting disaster recovery	88

Known issues	90
System Center Operations Manager issues	90
Performance and resource optimization issues	90
Show Windows Installer log check box is not visible	91
View PRO Script is not visible for PRO Tips	91
The alignment of some VHDs is not checked when selecting a large number of VHDs in SCOM for VHD alignment checking	91
The specified source and destination LUNs reside in different storage systems	92
The installation of OnCommand Plug-in for Microsoft results in error 1158	92
The path to the executable file is missing	92
Data ONTAP: Add Controller reports a success message for invalid entries	92
Virtualization discovery does not return any values for Hyper-V host after ApplianceWatch PRO 2.1 or 2.1.1 is uninstalled	93
System Center Operation Manager might crash when Data ONTAP Discovery task is run	93
OC.SCOM.log rolls over into multiple logs	93
Calculation for projected savings can actually be less than the current savings	93
A controller might be displayed more than once in the Manage Controller Credentials view	94
OnCommand Virtual Infrastructure Management Service (VIM_Service) on the local computer started and then stopped	94
vFiler unit credentials are not removed if the physical filer is removed	94
Hyper-V hosts might take three to four hours to appear in SCOM	94
Provisioning issues	95
Using Volume GUID as a mount point for virtual machine configuration ...	95
Map LUNs to igroups with type Hyper_V only	95
A PowerShell execution policy set to Allsigned causes New-OCClone cmdlet to fail	95
Virtual machine cloning into an existing CSV with the same base name fails	96
XenDesktop import failure - host names of virtual machines are not changed from the source virtual machine name	96

You must add a string of MSvSCVMM as a connection name when you add an SCVMM host to Citrix Desktop Studio	96
Running provisioning and cloning cmdlets as a user other than the Windows administrator	97
If the system clock is out of sync, the node loses connectivity	97
Error when you use the volume GUID as a mount point for virtual machine configuration	97
Resizing dedicated disks could take longer than expected	98
The storage path of FC connected disks owned by adjacent nodes in a cluster cannot be discovered	98
Virtual Machine Manager encountered an error and exited the process	98
The default settings and timeouts in SCVMM SSP 2.0 might limit the number of simultaneous CreateVM requests	98
Creating a virtual machine request from SCVMM Self-Service Portal fails	99
WMI warnings appear in the event logs	99
Two HA virtual machines with the same name	99
Cloning Issues	100
New-OCClone cmdlet fails because the VHD path information already exists	100
New-OCClone might result in excess free space	101
The New-OCClone cmdlet fails on vFiler units that use Data ONTAP versions earlier than 7.3.3	101
Cloning into an existing LUN on a remote system is not supported	101
Cannot clone a virtual machine from a System Center Virtual Machine Manager (SCVMM) template into a CSV	101
Neither source VHD nor clone destination is on a LUN	102
The specified destination server is not managed by an SCVMM server	102
Disaster recovery issues	102
Partial restore operations for virtual machines	102
Disaster recovery failover fails on the secondary site	103
After a disaster recovery restore, the restored virtual machine fails to start	103
The -Force parameter is required to perform some disaster recovery failover procedures	103

The disaster recovery plan folder does not contain all the virtual machine configuration files	103
A failure occurs when you try to create a disaster recovery plan across domains	104
The disaster recovery Invoke-OCDRMirrorReverseResync cmdlet fails because of an incorrect storage system name	104
Reset-OCDRSite does not delete virtual machine resource groups	104
The Reverse Resync SnapMirror object call fails	104
The specified source and destination LUNs reside in different storage systems	105
The Reverse Resync SnapMirror object call fails	105
Copyright information	106
Trademark information	107
How to send your comments	108
Index	109

OnCommand Plug-in for Microsoft components

OnCommand Plug-in for Microsoft is a tool that you can use to configure, monitor, and maintain your storage. The plug-in includes management packs for Microsoft System Center Operations Manager (SCOM) 2012, PowerShell cmdlets, and System Center Orchestrator integration packs (OIPs) that you use to perform a variety of tasks, including provisioning, cloning, and disaster recovery for Microsoft Hyper-V virtual machines.

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

Parent component	Subcomponent	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 (SCVMM) console: • Data ONTAP PRO Management Pack
Cmdlets	Provisioning	You can use provisioning cmdlets to provision storage and manage storage system credentials.

Parent component	Subcomponent	Description
	Cloning	You can use cloning cmdlets to clone virtual machines, LUNs, aggregates, and volumes.
	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.
Orchestrator Integration Packs	Data ONTAP Toolkit Integration Pack	You can use the activities provided in the Data ONTAP toolkit to perform many of the most common tasks in the plug-in.
	Cloning and Provisioning Integration Pack	You can use the activities provided in the Orchestrator 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 Orchestrator activities 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	Subcomponent	Description
Documentation		The <i>OnCommand Plug-in for Microsoft Installation and Administration Guide</i> and the <i>OnCommand Plug-in for Microsoft Windows PowerShell Cmdlet and Orchestrator Activity Reference Guide</i> are available at C:\Program Files\NetApp\OnCommand\MS_PLUGIN\ after the installation.

Windows PowerShell execution policies and administration profiles

The Windows PowerShell interface is a scripting shell that you can use to manually call cmdlets in the plug-in to manage, administer, and protect your data. 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**.

PowerShell Administration Profiles

You must import the SCCmdlets module into your local Windows PowerShell profile if you want the cmdlets 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 (SCVMM) and System Center Operations Manager (SCOM).

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

Related information*[Microsoft TechNet web site](#)*

Common cmdlet parameters

The Windows PowerShell cmdlets include both common cmdlet parameters and risk-mitigation parameters that you can use to customize the operation that the cmdlet performs.

Cmdlet parameters**[-Verbose {True | False}]**

Displays expanded information about the operation.

[-Debug {True | False}]

Displays technical information about the operation.

[-WarningAction {SilentlyContinue | Continue | Inquire | Stop}]

Determines how the cmdlet responds to a warning when performing the operation. The following list describes what each value means:

SilentlyContinue	Suppresses the warning message and continues with the operation.
Continue	Displays the warning message and continues with the operation. This is the default value for this parameter.
Inquire	Displays the warning message and asks if you want to continue.
Stop	Displays the warning message and stops the operation.

-WarningVariable | *Variable_name*

Stores warnings about the cmdlet in the specified variable.

[-ErrorAction {SilentlyContinue | Continue | Inquire | Stop}]

Determines how the cmdlet responds to a warning when performing the operation. The following list describes what each value means:

SilentlyContinue	Suppresses the warning message and continues with the operation.
Continue	Displays the warning message and continues with the operation. This is the default value for this parameter.

Inquire	Displays the warning message and asks if you want to continue with the operation.
Stop	Displays the warning message and stops the operation.

-ErrorVariable | *Variable_name*

Stores errors about the cmdlet in the specified variable.

-OutVariable | *Variable_name*

Displays objects output by the cmdlet and then stores them in the specified variable.

-OutBuffer | *Object_number*

Determines the number of objects that can reside in the buffer before they are sent.

Risk mitigation parameters**[-WhatIf {True | False}]**

Displays a message about the outcome of the cmdlet instead of executing the operation.

[-Confirm {True | False}]

Prompts you for input before executing the operation.

What OIPs are

In a Microsoft System Center Orchestrator (SCO) environment, you can import and deploy Orchestrator integration packs (OIPs), which contain activities that you can use to create workflows to automate complex processes. There is an OIP for provisioning and cloning, one for disaster recovery, and another for commonly used data storage operations.

To use the Orchestrator integration packs, you must have an Orchestrator installation configured to Microsoft's specifications.

Related information

[Microsoft TechNet web site](#)

Preparation to use OnCommand Plug-in for Microsoft

Before you download and install OnCommand Plug-in for Microsoft and any additional features, your environment must meet certain Microsoft System Center Operations Manager 2012, Microsoft System Center Virtual Machine Manager 2012, and Data ONTAP requirements.

Installation checklist for SCOM and OnCommand Plug-in for Microsoft

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

Before you begin

All installation requirements should have been fulfilled and proper functionality confirmed prior to proceeding with the plug-in installation. Review your SCOM installation information for requirements.

Steps

1. Download and install OnCommand Plug-in for Microsoft.
2. Optional: Set up SNMP.
3. 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.
4. Create and save overrides to your own management pack, not the default management pack to avoid dependencies on the default management pack.
5. Run Data ONTAP discovery to discover any network devices that are already monitored in SCOM.

This step prevents your system from monitoring duplicate controllers.

Related tasks

[*Completing the configuration of your plug-in*](#) on page 0

[*Importing the OIPs to the integration server*](#) on page 27

Related information

[*Microsoft TechNet web site*](#)

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 the plug-in, any versions of ApplianceWatch and OnCommand Plug-in 3.0 for Microsoft must first be uninstalled.

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 SP1 is installed

Data ONTAP requirements OnCommand Plug-in for Microsoft supports the following versions of Data ONTAP:

- 7.3 or later in the Data ONTAP 7.3 product family
- 7.3.3 or later for vFiler support
- Data ONTAP 8.0, 8.1 and 8.1.1 7-Mode

Hardware requirements Microsoft System Center Operations Manager (SCOM) 2012 and Microsoft System Center Virtual Machine Manager (SCVMM) 2012 determines the hardware requirements. For more information about the requirements for these Microsoft products, refer to the Microsoft TechNet site.

Software requirements OnCommand Plug-in for Microsoft requires the following software versions:

- .NET Framework 3.5 SP1 for all features
- Microsoft System Center Operations Manager (SCOM) 2012 for SCOM Management packs
- Microsoft System Center Virtual Machine Manager (SCVMM) 2012 for cloning cmdlets
- Microsoft System Center Orchestrator 2012 for Orchestrator integration packs

Microsoft license requirements OnCommand Plug-in for Microsoft requires the following Microsoft licenses:

- Windows Server 2008 R2 SP1
- Microsoft SQL Server 2008
- Microsoft System Center Operations Manager 2012

- Microsoft System Center Virtual Machine Manager 2012 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
requirements**

- To monitor your VHDs for alignment issues, you must have enabled PowerShell remoting on all Hyper-V hosts.
- You must configure System Center Operations Manager 2012 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 about configuring the SQL server data warehouse, refer to the Microsoft TechNet site.

**Orchestrator
Integration
Packs**

- You must install System Center Orchestrator 2012 and deploy the Orchestrator integration packs to the Orchestrator runbook server.
- To enable the cloning, provisioning, PowerShell toolkit, and disaster recovery functionality, OnCommand Plug-in VIM web services must be installed in a Windows Server 2012 host.
- You must have .NET3.5 SP1 installed in the runbook server host to use integration packs in the Orchestrator runbook server.

Disaster recovery, 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.
- To use cloning to monitor your VHDs for alignment issues, you must have enabled PowerShell remoting on all Hyper-V hosts.

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 TechNet web site*](#)

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**
- **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.
- **Orchestrator 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 Orchestrator modules by default.
 - **OnCommand Plug-in Web Services**
Can be installed on a server other than an Orchestrator runbook 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://support.netapp.com/>

Upgrade requirements

You cannot upgrade automatically from OnCommand Plug-in 3.0 for Microsoft to OnCommand Plug-in 3.1 for Microsoft. To upgrade to the 3.1 version of the plug-in, you must first uninstall the prior version of the plug-in and then install the 3.1 version.

Uninstalling ApplianceWatch PRO 2.1 and 2.1.1 and OnCommand Plug-in for Microsoft 3.1

You can use the Windows Control Panel to uninstall ApplianceWatch PRO 2.1 and 2.1.1 as well as OnCommand Plug-in for Microsoft 3.1 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

You can use the installation wizard to install OnCommand Plug-in for Microsoft, the management packs, the Orchestrator integration pack, and the Web services.

About this task

You cannot upgrade automatically from ApplianceWatch PRO or OnCommand Plug-in for Microsoft versions prior to 3.1 to OnCommand Plug-in 3.1 for Microsoft. To upgrade to the 3.1 version of the

plug-in, you must first uninstall the 3.0 or earlier version of the plug-in and then install the 3.1 version.

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 Destination Folder dialog box opens.
4. Click **Next** to install to the folder that is listed or click **Change** to install to a different folder.
5. Click **Next** to continue with the installation.
6. In the **Feature Selection** 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 OnCommand Plug-in for Microsoft in silent mode

You can install OnCommand Plug-in for Microsoft software in silent mode, without a wizard. Silent installation requires less intervention and is a less intrusive process than installing using the wizard.

About this task

During silent installation, no interface, progress bars, or error messages are displayed. Error messages, if there are any, are written to a log file that is located in the Temp folder after the installation finishes if you do not provide a log file path in the silent install command line. Another log file is written if there is any software that the user needs 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. From a command line prompt, switch to the directory where you saved the executable file.
3. Run the executable.

```
OnCommand-PlugIn-Microsoft_3.1_x64_NetApp.exe /s /v"/qn /L*v C:\
\OCPMInstall_NetApp.log ADDLOCAL=ALL SVCUSERNAME=<Domain user>
SRV_PASSWORD=<passwd> SRV_CONFIRMUSERPASSWORD=<passwd>"
```

The installation begins and runs in the background.

Related concepts

[Installation requirements for OnCommand Plug-in for Microsoft](#) on page 16

[Guidelines for installing OnCommand Plug-in for Microsoft](#) on page 18

Related tasks

[Managing storage controller credentials](#) on page 37

Related references

[Feature selection for silent installation](#) on page 23

[Silent install and uninstall process parameters and variables](#) on page 22

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

```
OnCommand-PlugIn-Microsoft_3.1X12_x64_NetApp.exe /s /v"/qn /L*v
SVCUSERNAME=<domain user> SRV_PASSWORD=<passwd>
SRV_CONFIRMUSERPASSWORD=<passwd>
```

/w (Optional) Waits until the installation is complete before exiting

If you are using the **/w** argument in a batch file, you should precede the entire `setup.exe` command line with **start /WAIT...**:

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

/q Specifies silent installation with which you can use 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

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* element in the command, all features are installed by default.

Feature selection for silent installation

If you do not want to use the default OnCommand Plug-in for Microsoft installation (which includes all plug-in features), you must select the names of the features that you do want and use the *ADDLOCAL* parameter to construct a command that silently runs a custom installation.

If you select to install a parent feature (such as ManagementPacks), then all of its child features are installed also. If you select to install a child feature such as Hyper-V Storage Monitoring and Management, its parent feature (in this case, ManagementPacks) is also installed, along with any required sibling features (such as, in this case, Storage Monitoring).

In the following example, the user is performing a customized 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"
```

Feature names for use in silent installation cmdlets

You can use the feature names for *ADDLOCAL* that are listed in the table when you want to perform a silent installation.

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
		Data ONTAP Virtualization Reports Management Pack	HVStorageReporting
	OnCommand Data ONTAP PRO		
Cmdlets			
	Cloning and Provisioning Cannot be installed individually.		CmdletsCP
	Disaster Recovery Cannot be installed individually.		CmdletsDR
Orchestrator Integration Pack			Orchestrator
	Cloning and Provisioning Integration Pack		OrchestratorCP
	Disaster Recovery Integration Pack		OrchestratorDR

Parent feature name in custom setup	Child feature	Sub-child feature	Feature name for ADDLOCAL
	OnCommand Plug-in Web Services		OCWebServices
OnCommand Discovery Agent			OCAgent
Documentation			Doc

Uninstalling OnCommand Plug-in for Microsoft

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

Uninstalling the plug-in by using 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**, double-click **Programs and Features**.
3. Select OnCommand Plug-in for Microsoft.
4. Click **Uninstall**.

Uninstalling the plug-in by using silent mode

You can uninstall OnCommand Plug-in for Microsoft software silently, without a wizard when you no longer need the plug-in or when you upgrade to a later version.

About this task

During a silent uninstall process, no interface, progress bars, or error messages are displayed.

Steps

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

```
MsiExec.exe /x{8B77D13A-B265-4A01-A8BB-DD4FB96FB912} /L*v  
C:your_log_file.log /q
```

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 and deploying the OIPs

Before you can use the Orchestrator user interface and the Orchestrator activities to create workflows and automate tasks, you must install the Virtual Infrastructure Management (VIM) web service and import and deploy the Orchestrator integration packs (OIPs) for disaster recovery and provisioning and cloning. Other important OIP tasks include managing the controller credentials, meeting the OIP requirements, and uninstalling the OIPs.

Guidelines for using OnCommand virtual infrastructure management web service

OnCommand virtual infrastructure management (VIM) web service is required for the Orchestrator integration packs to communicate remotely with your Hyper-V hosts. You must follow certain guidelines when you install the web service, configure the TCP port, and manage controller credentials.

The following list includes guidelines for using the VIM web service:

- It must be installed on Microsoft Windows Server 2008 .
- .NET3.5 SP1 must be installed on all Orchestrator servers on which OnCommand Plug-in for Microsoft IPs runs.
- Port 808 must be the default TCP port for the VIM web service.
You can change the default web service port, but if you use a port other than 808, you must specify that port in the object in your workflow. You must configure all firewalls on all Orchestrator and Hyper-V servers to enable communications on this port.
- Each Hyper-V server must be configured with the appropriate credentials for all the controllers that you want to connect to, before you run any workflows.
You can do this by using the OIPs or the PowerShell interface directly on each Hyper-V host.

Importing the OIPs to the integration server

You must import the Orchestrator integration packs to the integration server before you can use the Orchestrator activities.

Before you begin

You must have met the following requirements:

- You must have downloaded the OnCommand Plug-in for Microsoft software.
- You must have the System Center Orchestrator 2012 license and have met all of the requirements for Orchestrator 2012.

If you are not sure what the requirements are, refer to the Microsoft TechNet Web site.

- You must have an integration (management) server to which to import the integration packs and an action server on which to deploy the integration packs.

Steps

1. Navigate to **Orchestrator Integration Server Deployment Manager** by clicking **Start > All Programs > Microsoft System Center 2012 > Orchestrator > Deployment Manager**.
2. Right-click **Integration Packs** in the left panel and select **Register IP with the Orchestrator management server**.
3. In the **Integrations Pack Registration** wizard, click **Next**.
4. Complete the steps in the wizard.

You can register multiple integration packs using the wizard once, by adding multiple integration packs when prompted.

Result

A green check mark appears in the Log Entries panel of the Orchestrator integration server window, indicating 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 Orchestrator Runbook designer.

Related information

[*Microsoft TechNet web site*](#)

Deploying Orchestrator integration packs to the Orchestrator runbook designer and server

You must deploy OIPs to the runbook designer or the runbook server before you can run activities.

Before you begin

The OIPs must have been registered on the integration server.

Steps

1. Navigate to **Orchestrator Integration Server Deployment Manager** by going to **Start > All Programs > Microsoft System Center 2012 > Orchestrator > Deployment Manager**.

2. Right-click **Integration Packs** in the upper right panel and select **Deploy IP to Runbook Designer**.
3. Complete the steps of the wizard.

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

After you finish

You must install the Virtual Infrastructure Management (VIM) web service to use the Orchestrator activities.

Uninstalling and unregistering the OIPs from the runbook server

When you no longer need the Data ONTAP Toolkit, disaster recovery or provisioning and cloning integration packs, you can use the Orchestrator integration server deployment manager to uninstall the Orchestrator integration packs (OIPs) from the runbook server. In the integration server, you unregister OIPs. When you uninstall and unregister the OIPs, the processes remove the OIPs on the server. Refer to the Microsoft web site for details.

Related information

[Microsoft TechNet web site](#)

Configuring the plug-in

You must perform several tasks to prepare the plug-in for use. These tasks include such things as adding controllers, discovering and configuring the controllers and tasks with the management pack rules. These tasks are required before you can begin to monitor your storage.

Adding controllers

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.

Steps

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

The **Add Controller** window opens.

2. Enter the SNMP string and the Controller name or IP address of the controller that you want to add.
3. Click **OK**
4. Go to **Actions > Data ONTAP: Manage Controller Credentials** to validate that the controller was added.

After you finish

After you have added a storage controller, you can use **Data ONTAP: Manage Controller Credentials** to set the credentials.

Adding controller credentials

After you have added controllers to the plug-in, you must add credentials to those controllers to enforce the security of your data.

About this task

The default protocol is HTTPS but vFilers can only use HTTP.

Steps

1. In the **Actions** pane, select **Data ONTAP: Manage Controller Credentials**.
2. Ensure that the appropriate roles and capabilities are assigned.

What storage discovery is

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

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 plug-in discovery rules.

The plug-in ignores traditional volumes during the discovery process.

Enabling discovery

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

Running discovery

There are three types of discovery that you must run to discover all of your storage. Discovery is required for the plug-in to recognize your controllers and begin the management of your storage.

About this task

You can 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.

You can run Data ONTAP PRO discovery to discover Hyper-V hosts with PRO integration in SCVMM.

Step

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

Expediting 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 discovery process by manually running also known as expediting discovery. The plug-in utilizes rules that discover

storage, virtualization and PRO objects 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 for Microsoft discovery rules.

The plug-in ignores traditional volumes during the discovery process.

Types of discovery

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

Related concepts

[*Expediting discovery*](#) on page 31

Related tasks

[*Enabling discovery*](#) on page 31

[*Expediting virtualization discovery*](#) on page 33

[*Expediting storage discovery*](#) on page 32

Expediting 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 (SCOM) database, the storage devices in these controllers are discovered.

Before you begin

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 SCOM **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

Data ONTAP virtualization discovery finds storage on all Hyper-V hosts in System Center Virtual Machine Manager (SCVMM), including Hyper-V hosts, Hyper-V LUNs, Hyper-V virtual machines, and Hyper-V virtual hard disks. You can perform virtualization discovery manually, without an agent on every Hyper-V host by using the Data ONTAP Virtualization: Discovery Rule.

Before you begin

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

Steps

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

Locating 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 (SCOM) or to override the rules as necessary.

Before you begin

You must have correctly imported the OnCommand Plug-in for Microsoft management packs that you installed into SCOM.

Steps

1. From the **Authoring** pane, select **Rules**.
2. In the **Name** column, go to **Type: Management Server** and search for **Data ONTAP**.
3. Then from the list of rules, right click any rule and set the overrides to the entire group.

4. Save the changes to the rule.

These changes can be either saved to the SCOM standard default management pack or to a new management pack which you create.

Related tasks

[Overriding monitoring rules](#) on page 41

Lists of Data ONTAP management pack rules

OnCommand Plug-in for Microsoft includes rules that enable you to more effectively manage your storage resources. The lists include Data ONTAP: Management Server rules, Data ONTAP PRO: Hyper-V Host rules, Data ONTAP Virtualization: Management Server rules, Data ONTAP MetroCluster: Management Server rules.

Data ONTAP: Management Server rules

The following list names 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 names 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 names 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

Related tasks

Locating Data ONTAP management pack rules on page 33

Multiple management server environment

In System Center Operations Manager (SCOM) 2012, a multiple management server environment consists of management servers that have peer-to-peer relationships. Each management server can communicate directly with the SDK service and database of the other servers, on the condition that all servers in the environment are running OnCommand Plug-in for Microsoft 3.1 or later.

The SCOM environment is protected if a single node goes down. In fact, some of the workload of the inoperative management server is failed-over to another management server. Although you can have the plug-in installed on more than one management server in your multiple-server environment, SCOM discovery operates on only one management server.

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.

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 that 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.

For further instructions on how to enable SNMP, refer to the *Data ONTAP Installation and Administration Guide* for your version of DATA ONTAP.

5. If necessary, set up the community.
6. Configure the trap destination as your System Center Operations Manager server on which you installed the plug-in.

The SNMP monitors are targeted at the Data ONTAP Controller class.

7. Enable the non-emergency trap monitors using monitor overrides.

Managing storage controllers

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.

Managing storage controller credentials

You can set credentials for all of the controllers and vFiler units 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 unit, 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 vFiler units 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**.

Related tasks

[*Completing the configuration of your plug-in*](#) on page 0

Launching System Manager from the plug-in

To use the System Manager interface to change controller configuration information, you can select the storage controllers that are monitored by OnCommand Plug-in for Microsoft and then launch Data ONTAP: Launch NetApp System Manager.

Before you begin

You must have installed and configured OnCommand Plug-in for Microsoft. You also must have System Manager installed on the System Center Operations Manager server on which the plug-in is installed.

It is strongly recommended that you have System Manager installed to perform active management tasks on your system.

Steps

1. Navigate to the **Controllers** view or the **Diagram** view.
2. Select a storage controller group or storage controller.
3. From the **Actions** pane, go to **Data ONTAP Controller Tasks** pane.
4. Select **Data ONTAP: Launch NetApp System Manager**.

After you finish

Refer to your System Manager documentation for more information about System Manager tasks.

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**.

Related tasks

Completing the configuration of your plug-in on page 0

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.

List of OnCommand Plug-in for Microsoft monitors

The Data ONTAP PRO management packs are used to monitor and report alerts and events on the functions of the Storage Controllers and all virtualization objects that are provided from System Center Virtual Machine Manager (SCVMM). These alerts are sent to the SCVMM Console as PRO Tips, which pop up in their specific window in SCVMM. The user can chose to implement or dismiss a PRO tip.

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

List of OnCommand Plug-in for Microsoft PRO monitors

The PRO management pack are used to monitor the functions of the volumes, virtual machines and LUNs.

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

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.

Related tasks

[*Locating Data ONTAP management pack rules*](#) on page 33

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 System Center 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.

You can modify two customizable rules 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 (the default is 500 ms and 1000 ms). 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.

Related concepts

Types of PRO tips on page 51

Alerts View

The Alerts view displays a list of every active alert found by OnCommand Plug-in for Microsoft, but you can filter the view to display a list limited to the alerts specific to Data ONTAP storage. You can view information about an individual alert in the Alert Details pane, and you can view the cause of the problem in Health Explorer in System Center Operations Manager (SCOM).

You can view active alerts from any of the following interface locations:

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 isolate problems with a specific storage controller object.

You can expand this view to display associated objects as well, so that 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 System Center Operations Manager to find the root of the problem.

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 (SCOM) 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.

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 view

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 view

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 view

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 the plug-in.
vFilers	Displays information about all vFiler units that are currently monitored by the plug-in.
Storage Efficiency	Displays how efficiently the storage is currently being used by all storage controllers that are monitored by the plug-in.
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 view

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/vFiler	Displays the fully qualified domain name of the controller or vFiler unit 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 view

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

The following attribute displays in the **Management Server** view:

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

Qtrees view

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 **Qtrees** 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 view

You can view the status of all SnapMirror relationships that are monitored by the plug-in.

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: • Initialized • SnapMirrored • Broken-Off • Quiesced • Source

- Unknown

Lag Displays the amount of time since the last SnapMirror transfer.

Storage utilization view

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.

vFiler units

You can view a vFiler unit 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 unit. 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 unit.
Status	Displays whether the vFiler unit 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 view

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 unit to which the volume belongs.
Total size	Displays the total size of the volume.

Hyper-V Hosts view

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 view

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, C:\ClusterStorage\Volume1.
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 view

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 view

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 fully qualified domain name (FQDN) of the Hyper-V host that is hosting the virtual machine.

Monitoring Operations Manager servers

Using OnCommand Plug-in for Microsoft, you can enable Microsoft System Center Operations Manager (SCOM) to monitor the state of the Microsoft 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 Operations Manager server and click **Apply > OK**.

Using PRO tips

OnCommand Plug-in for Microsoft 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 LUN 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 the plug-in 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.

Related concepts

Alert monitoring on page 42

Related tasks

Implementing PRO tips automatically on page 55

Implementing PRO tips manually on page 55

Related references

Performance and resource optimization issues on page 90

Enabling PRO tips

You should enable PRO tips in order to discover all the objects that are required to use PRO tips. When you enable PRO tips, the PRO tips automatically repair storage-related problems that occur in your virtual environment.

Before you begin

All requirements should have been met for SCOM and SCVMM PRO integration.

About this task

SCVMM can take up to six hours to enable PRO tips.

Steps

1. In SCVMM, display the **Properties** dialog box in Operations Manager server.
The Properties dialog box displays the Add Operations Manager Introduction window.
2. Click **Next**.
3. On the **Connection to Operations Manager** page, enter the server name.
The server name should be the name of the Root Management Server (RMS) emulator.
4. Check **Enable Performance and Resource Optimization (PRO)** check box.
5. On the **Connection to VMM** page, enter the user name and password.
6. Click **Next** to confirm the settings.
7. Click **Finish** to launch a jobs window and create a PRO connection.
8. You can track the progress of this process from **PRO Diagnostics**.
9. You must click **Test PRO** in the **Properties** window to verify the status of the operation.

Related information

[Microsoft TechNet web site](#)

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

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

Steps

1. Navigate to the **SCVMM Console** and select the **Fabric**.
2. Select **Servers** from the left pane of the **SCVMM Console** and select the **All Hosts** menu.
3. Click **All Hosts** and select **Properties**.
4. Select **PRO Configuration**.
5. Select **Remediate** for the appropriate PRO tip.
6. Click **OK**.

Related concepts

[Types of PRO tips](#) on page 51

Related tasks

[Implementing PRO tips manually](#) on page 55

Related references

[Performance and resource optimization issues](#) on page 90

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

You must have met the following requirements:

- 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**.

Related concepts

Types of PRO tips on page 51

Related tasks

Implementing PRO tips automatically on page 55

Related references

Performance and resource optimization issues on page 90

Events

You can use the Events window to view information about the events that OnCommand Plug-in for Microsoft has logged. The plug-in 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 events triggered by 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

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.

Related concepts

[Custom reports](#) on page 59

Related tasks

[Viewing reports](#) on page 59

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 the plug-in 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.

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. Refer to the Microsoft TechNet website for details.

Steps

1. Navigate to the **Hyper-V VHDs** view and select the names of all of the VHDs that 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** to begin the misalignment check on the selected VHDs.

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, in which the **State** attribute displays the alignment of the VHDs.

Related information

[Microsoft TechNet web site](#)

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, select the names of all of 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 box opens.

3. Click **Run** to begin the misalignment check on the selected LUNs.

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.

How to launch Health Explorer for a controller

You can launch Health Explorer in Microsoft System Center Operations Manager so that you can determine the root of any 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.

What Data ONTAP Toolkit Integration Pack activities are

The Data ONTAP Toolkit activities enable you to invoke Data ONTAP commands from System Center Orchestrator. You can also use the activities individually as an alternative to using the Data ONTAP command-line interface and PowerShell scripting workflows.

For more information about the Data ONTAP Toolkit activities, see the *OnCommand Plug-in 3.1 for Microsoft Windows PowerShell Cmdlet and Orchestrator Activity Reference Guide*.

Storage System cache credentials

You use the Storage System cache credential cmdlets and activities to add storage systems to storage systems cache. These cmdlets and activities add, retrieve or remove user credentials from a local repository so that you can use other cmdlets without entering credential information.

For more information about the Storage System cache credentials, refer to the *OnCommand Plug-in 3.1 for Microsoft Windows PowerShell Cmdlet and Orchestrator Activity Reference Guide*.

Provisioning storage

By using provisioning cmdlets with Microsoft System Center Virtual Machine Manager (SCVMM) applications, you can use your existing storage resources to perform faster and more space-efficient provisioning of Hyper-V virtual machines.

For more information about the cmdlets and activities used to clone storage, refer to *OnCommand Plug-in for Microsoft 3.1 Windows PowerShell Cmdlet and Orchestrator Activity Reference Guide*.

Requirements for provisioning

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:

- 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 short name that is DNS resolvable.
- The storage system name must be the FQDN, the short name, or the IP address.
- Provisioning operations with cluster shared volumes (CSVs) can be initiated only on the CSV owner node of a particular storage resource.

The plug-in is not able to create software initiators if the computer name contains invalid characters.

DNS host names cannot contain the following characters:

- comma (,)
- tilde (~)
- colon (:)
- exclamation point (!)
- at sign (@)
- number sign (#)
- dollar sign (\$)

- percent (%)
- caret (^)
- ampersand (&)
- apostrophe (')
- period (.)
- parentheses (())
- braces ({})
- underscore (_)

Related information

[Microsoft TechNet website](#)

The Connect Storage activity vs. the Provision Storage activity

Although the **Connect Storage** activity connects storage and the **Provision Storage** activity also connects storage, they are quite different activities. It is important to know when to use each activity and what the activity does beyond just connecting your storage.

There are two primary differences in the use of these activities.

1. The **Provision Storage** activity creates the storage and connects it to the host.
The **Connect Storage** activity does not create the storage.
2. Only LUNs that were previously mounted on the host can be connected with the **Connect Storage** activity.

Cloning storage

By using cloning cmdlets with Microsoft System Center Virtual Machine Manager (SCVMM) applications, you can use your existing storage resources to perform faster and more efficient use of the space on your Hyper-V virtual machines.

For more information about the cmdlets and activities used to clone storage, refer to *OnCommand Plug-in for Microsoft 3.1 Windows PowerShell Cmdlet and Orchestrator Activity reference Guide*.

Requirements for cloning

Before you can implement 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 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 domain 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 short name that is DNS resolvable.
- The storage system name must be the FQDN, the short name, or the IP address.
- 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. Refer to the Microsoft TechNet website for details.

Related information

[Microsoft TechNet web site](#)

What Sub-LUN cloning is

Sub-LUN cloning is a process by which you can create clones of one file or a few files that are stored on a LUN. Sub-LUN cloning enables you to create exact duplicates of existing files without copying. Within the controller, Data ONTAP uses pointers to the individual files thereby representing multiple files to Windows while keeping only one copy of the duplicates on the storage in the controller.

Activities for creating clones

There are three activities that you can use in Orchestrator to create clones: the **Clone NTFS File** activity, the **Clone VM** activity, and the **Clone VM from SCVMM** activity. It is important to understand the differences in these three activities and the guidelines for the use of each one.

File cloning

The New-OCCloneFile cmdlet (**Clone NTFS File**) clones any file on a mounted NTFS or cluster-shared volume (CSV) on a LUN to a specified path within another mounted NTFS or CSV. This object supports Windows LUNs or CSV LUNs within a Windows cluster.

Note: The names of equivalent activities are given in parentheses after the cmdlet names for those who are using Microsoft System Center Orchestrator.

To use the New-OCCloneFile cmdlet (**Clone NTFS File**), your environment must meet the following requirements:

- Both the source and destination LUNs must reside in the same storage volume on a storage system.
- Both the source and destination NTFS or CSV must be mounted on the same host.
- If the source or destination path is on a CSV, the CSV must be owned by the node from which the command is run.
- The directory of the destination path must exist.
- The existing NTFS or CSV must have enough space to hold the new cloned file.

Virtual machine cloning

The New-OCClone cmdlet (the **Clone VM** activity in Microsoft System Center Orchestrator) clones a file from an existing Hyper-V virtual machine that is currently in an off state. The cloned virtual machines can be deployed on the same host or on a parent cluster of the host where you run the object.

To clone an existing virtual machine with the New-OCClone cmdlet (or **Clone VM** activity), you must observe the following requirements:

- You must enter either a virtual machine name or the GUID of an existing virtual machine in the object properties.
- The virtual machine must exist on the host where you run the object.

The New-OCCLone cmdlet (or **Clone VM** activity) performs a sub-LUN clone operation first and then uses the cloned file to create the virtual machine.

Clone a virtual machine from an SCVMM template

The New-OCCLone cmdlet (**Clone VM from SCVMM Template**) clones a virtual machine from an SCVMM virtual machine template.

Note: The names of equivalent activities are given in parentheses after the cmdlet names for those who are using Microsoft System Center Orchestrator.

To clone from a template with the New-OCCLone cmdlet (**Clone VM from SCVMM Template**), you must observe the following requirements:

- You must enter an SCVMM server name and template name in the activity properties.
- The template must be configured correctly.

The cloned virtual machines can be deployed on the same host where the activity is run or to a different host or host cluster.

The New-OCCLone cmdlet (**Clone VM from SCVMM Template**) performs a sub-LUN clone operation first and uses the cloned file to create the virtual machine.

Situations for using the Clone VM activity

There are several situations in which you can use the **Clone VM** activity to clone a virtual machine. These situations include cloning into the same source LUN, cloning into a new single LUN, and cloning into an existing CSV on a LUN.

Situation 1: Creating clones from a LUN into a new LUN

You can use the **Clone VM** activity to create clones of a virtual machine in an off state from a LUN into a new LUN and then start the cloned virtual machines on a specified Hyper-V host.

Before you begin

Web service must be installed in the same location as the virtual machine and **Clone VM** activity must be configured with the name of the Web service server.

Steps

1. To run the **Clone VM** activity, in the activity properties, specify the following information.
 - The virtual machine name

- The number of clones
- The virtual machine clone name prefix
- The Hyper-V host name

2. Run the **Clone VM** activity.

Storage for the virtual machine is cloned on the storage array and the cloned virtual machines are started.

Situation 2: Creating clones from a LUN into the same LUN

You can use the **Clone VM** activity to create clones of a virtual machine in an off state from a LUN into the same LUN and then start the cloned virtual machines on the same Hyper-V host or on another Hyper-V host that is sharing that LUN.

Before you begin

The `AllinSingleLUN` or the `AllinSourceLUN` property must be used to create clones in the same LUN.

Steps

1. Specify the following information in the activity properties.

- The virtual machine name
- The number of clones
- The virtual machine clone name prefix
- The Hyper-V host name

2. Run the **Clone VM** activity.

Storage for the virtual machines is cloned on the storage array and the cloned virtual machines are started on the same Hyper-V host.

Situation 3: Creating a clone of a LUN into an existing CSV on a LUN

You can use the **Clone VM** activity to create clones of a virtual machine from a LUN into another existing cluster-shared volume (CSV) on a LUN and start the cloned virtual machines on the same Hyper-V host. If the clones are created in a CSV, those virtual machines can be started on another Hyper-V host that shares that destination CSV.

Steps

1. To run the **Clone VM** activity, in the activity properties, specify the following information.

- The virtual machine name
- The number of clones
- The virtual machine clone name prefix
- The Hyper-V host name

- Mount point

2. Run the **Clone VM** activity.

Storage for the virtual machine is cloned on the storage array in another existing LUN. The cloned virtual machines are started on the same Hyper-V host or another Hyper-V node that is sharing the same CSV.

Disaster recovery cmdlets and activities

Crash-consistent disaster recovery uses the SnapMirror feature to replicate data across primary and secondary sites following a disaster. To properly use disaster recovery, you must be familiar with the SnapMirror feature and the requirements for disaster recovery. There are several disaster recovery cmdlets and activities, including composite cmdlets and automated activities and their properties.

Related concepts

[Requirements for disaster recovery](#) on page 71

[What the disaster recovery plan is](#) on page 72

Requirements for disaster recovery

Your environment must meet some important requirements to enable you to use the crash-consistent disaster recovery activities.

- All disaster recovery virtual machines must be on NetApp storage.
- The secondary site must be used for the sole purpose of disaster recovery.
- Only a host administrator from the host can invoke disaster recovery objects.
- 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 of equal or greater size must exist on the secondary storage system.
- All replication objects must be invoked from the Hyper-V host rather than a source or destination storage system.
- The web service login account must have administrative privileges on the local and remote hosts or clusters on both the primary and secondary sites.
- If you are using Orchestrator to perform the disaster recovery tasks, the Orchestrator server must have administrative rights on the hosts and clusters on which you want to perform any restore operations.
- Access to the disaster recovery plans requires that the proper permissions are provided for the ACL and NTFS folders.
- All virtual machines must be in the off state before you create or update your disaster recovery plans.
- SnapMirror on the NetApp storage system side should be configured using the host short name, on both the source and destination storage systems.
- Remote access across the source and destination filers or the source and destination volumes must be enabled for SnapMirror to function properly.
- SnapMirror relationships must be identified by the system short names instead of IP addresses in their mirror relationships.

- Disaster recovery cmdlets must be invoked on the primary and secondary site nodes where the web service is installed.
- Invoking disaster recovery cmdlets or operations remotely is not supported.
- The storage system credentials on both the primary and the secondary sites must be configured on all storage appliances and must be present on the nodes where the plug-in is installed and disaster recovery cmdlets are invoked.
- All DNS, nslookup, ping, and forward and reverse lookups must be configured properly for disaster recovery and for live or quick migration of Hyper-V virtual machines in a Windows failover cluster setup.
- Two way cross-domain trust policies must be properly established across the primary and the secondary sites.
- You must ensure that firewalls do not interfere with disaster recovery operations.

Refer to your SnapMirror documentation for more details.

Related information

[*Microsoft TechNet website*](#)

What the disaster recovery plan is

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 and can be replicated to your secondary site. The naming convention pattern is `PrimaryServerOrCluster_SecondaryServerOrCluster_DRPlan.xml`.

You create the plan on the primary site and it captures information about 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
- 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-related or cluster-related information

Requirements for creating and updating disaster recovery plans with cmdlets

To update the disaster recovery plan with cmdlets you must follow some specific guidelines.

1. Ensure all virtual machines are turned off.
2. Ensure all virtual machines are moved to the local node where OnCommand Plug-in for Microsoft web service is installed.

3. In case of shared cluster configurations, ensure that the local node where you are running the cmdlet is also the owner of the cluster group resource. The available storage can be owned by other nodes.
4. You must run the disaster recovery plan tasks on the sites, Site A or Site B, as specified in the following list.
 - New-OCDRPlan on Site A
 - Update-OCDRPlan on Site A
 - Update-OCDRPlan -Failback on Site B

Disaster recovery plan guidelines

You must follow several guidelines when you update or create a new disaster recovery plan because the disaster recovery plan plays a vital role in the failover or failback of your storage system.

Ensure that you have performed all of the following guidelines when you create or update a disaster recovery plan:

- Turned off all virtual machines.
- Moved all virtual machines to the local node where web services is installed.
- For cluster shared volume configurations, ensure that the local node where you are running the cmdlet is also the owner of the cluster group resource.

The available storage can be owned by other nodes.

It is important to run the disaster recovery plan on the appropriate sites (Site A or Site B). The following list outlines the disaster recovery plan create and update configurations that are supported on the plug-in:

- Run the New-DRPlan cmdlet or the **Create DR Plan** activity on Site A.
- Run the Update-OCDRPlan or the **Update a DR Plan** activity on Site A.
- Run the Update Update-OCDRPlan -Failback or the **Update a DR Plan** activity with Failback as the operation direction on Site B.

Cmdlets and activities used with the disaster recovery plan

There are three configuration cmdlets and three configuration activities that you can use to help you create, validate, and update your disaster recovery plan.

New-OCDRPlan cmdlet and Create DR Plan activity:

Use web services to create a new disaster recovery plan

Confirm-OCDRPlan cmdlet and Validate DR Plan activity:

Validate 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 Confirm-

OCDRPlan cmdlet and the Validate DR Plan activity confirm the following factors in the disaster recovery plan:

- Ensure 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
- Ensure that virtual machine LUNs that are to be connected on the secondary site have valid LUN paths and SnapMirror relationships
- Confirm active SnapMirror status and the SnapMirror relationships and ensures that all the SnapMirror relationships have the snapmirrored status
- Validate the virtual machine cluster and configuration resources against the live virtual machine
- Ensure there is no conflict with the cluster and configuration resources on the secondary host
If a conflict is found in the mount points, the Confirm-OCDRPlan cmdlet checks the mount point that is connected in the secondary host to determine if it is connected to the required LUN on the secondary storage system.
- Verify whether the storage system credentials are configured for all the storage systems in the disaster recovery process on the secondary site
- Ensure that the Hyper-V role is enabled on the secondary host or cluster
- Ensure 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 if the disaster recovery plan is created in the context of a cluster

Update-OCDRPlan cmdlet and Update DR Plan activity:

Before you re-create the plan, you must ensure that any new storage system volumes have a corresponding volume on the secondary storage system. You must run this cmdlet or activity after any addition or deletion of resources.

You can use the Update-OCDRPlan cmdlet and the Update DR Plan activity to update the plan.

The Update-OCDRPlan cmdlet has one parameter, -Failback, that indicates the disaster recovery operation that the plan is being configured for. The default is -Failover.

Granular vs. composite workflows

You can use the disaster recovery cmdlets and the Orchestrator automated activities to call several individual activities to automate a workflow, such as controlling failover and failback procedures, making changes to the disaster recovery plan, and controlling the SnapMirror relationships. Composite cmdlets and Orchestrator automated activities are created from a group of regular cmdlets or activities that are performed together, in a preset order.

Failover and failback requirements

With crash-consistent disaster recovery, when you experience a complete site failure of both the host and the storage, you can fail over from a primary site to a secondary site. After you fail over from a primary site to a secondary site, you must perform a failback to restore the SnapMirror relationships.

There are different requirements depending on whether you want to perform a failover operation or a failback operation.

Failover requirements

You must have performed the following tasks on your system prior to a failover operation:

- Created a disaster recovery plan and stored it in a central location.
You can also replicate the plan to your secondary site.
- Established SnapMirror relationships from the primary to the secondary site.
- Updated the SnapMirror relationships.
This ensures that the latest data is transferred from the primary to the secondary site before the actual disaster recovery failover is performed.
- Run the `Update-OCDRPlan` cmdlet or the **Update DR Plan** activity on the primary site (site A).

Failback requirements

You must have performed the following tasks on your system after a failover operation has finished and prior to initiating a failback operation:

- Ensured that proper mirror relationships are established across your primary and secondary sites.
- Run the `Update-OCDRPlan` cmdlet or the **Update DR Plan** activity indicating failback as the operational direction on the primary site (Site B) to update the disaster recovery plan with the latest configuration information.
- If there is no data loss, you must have used the `Invoke-OCDRMirrorReverseResync` cmdlet or the **Reverse Resync SnapMirror** activity on the secondary site (Site A) to reverse all of the relationships from Site B to Site A.
- If there is data loss, you must have used the `Initialize-OCDRMirror` cmdlet or the **Initialize SnapMirror** activity to create new SnapMirror relationships from Site B to Site A.
- Updated mirror relationships.

Note: All transfers, initializations, and updates to your system are performed asynchronously, so you must wait and ensure that an operation is complete before you perform any additional operations.

Related concepts

[What the disaster recovery plan is](#) on page 72

Failover workflow breakdown

There are several ways that you can perform a failover operation from a primary site to a secondary site. The workflow breakdown provides information about the various cmdlets that you can use to do

this, and their options; where to use the cmdlet; the role of those sites at that stage of the task; and any additional information that you need about that stage.

Preparation for failover

Cmdlet	Site	Role	Notes
Initialize-OCDRMirror -sourceloc filerA:sourcevol -destloc filerB:destvol -verbose	Any site		The Initialize-OCDRMirror cmdlet can be used for failback in the event of loss of Site A.
New-OCDRPlan -drf\\sunny\cher -drn p1.xml -prisvr <siteA> -secsvr <siteB> -ver	Site A	Primary	
Confirm-OCDRPlan -drp\\sunny\cher\p1.xml -ver	Any site		

The failover operation

Cmdlet	Site	Role	Notes
Invoke-OCDRFailover	Site B	Secondary	

Following the failover

After the failover operation, perform a failback and then a 2nd failover operation.

Cmdlet	Site	Role	Notes
Update-OCDRPlan -Failback -prisvr <siteB> -secsvr <siteA>	Site B	Secondary > Primary	

Invoke - OCDRMirrorReverseResync	Site A	Secondary	This cmdlet establishes Site B as the mirror source, and takes the LUNs offline on Site A.
Reset -OCDRSite -force	Site A	Secondary	This step is optional and is part of composite failback cmdlet. It removes the VMs and leaves the LUNs on Site A.
Confirm-OCDRPlan	Any site		This step is for failback and it reports conflicts because Site A contains the VMs and LUNs.
Invoke-OCDRFailback -force	Site A	Secondary	The Site B to Site A failback was executed. The -Force option is needed because the -Full option was not used in the preceding Reset -OCDRSite cmdlet.
Update-OCDRPlan	Site A	Secondary > Primary	Site A is staged to fail over to Site B.
Reset -OCDRSite -force -full	Site B	Secondary	This cmdlet removes all VMs and LUNs in the disaster recovery plan on Site B.
Invoke-OCDRMirrorResync	Site B	Secondary	Site A is set as the mirror source.
Confirm-OCDRPlan	Any site		This step validates the Site A to Site B failover. It does not report conflicts.

Invoke-OCDRFailover	Site B	Secondary	The Site A to Site B failover is executed.
---------------------	--------	-----------	--

Performing consecutive failover operations

Cmdlet	Site	Role	Notes
Confirm-OCDRPlan	Any site		Success confirms that the mirrors are synchronized.
Start-OCDRSimulateFailover	Site B	Secondary	This cmdlet gives the same result as Invoke-OCDRFailover.
Update-OCDRPlan	Site A	Primary	
Stop-OCDRSimulateFailover -force	Site B	Secondary	Conflicting virtual machines and LUNs are removed from Site B.
Update-OCDRPlan	Site A	Primary	
Start-OCDRSimulateFailover -force	Site B	Secondary	The -Force option is needed to successfully fail over because conflicting LUNs remain on the secondary site.
Update-OCDRPlan	Site A	Primary	
Stop-OCDRSimulateFailover -force	Site B	Secondary	Conflicting virtual machines and LUNs are removed from Site B.

The disaster recovery failover workflow

The Invoke-OCDRFailover composite cmdlet (**DR Failover**) run an automated workflow to perform the failover of virtual machines from a primary site to a secondary site. With crash-consistent disaster recovery, when you experience a complete site failure of both the host and the

storage, you can fail over from a primary site to a secondary site with limited and reasonable downtime.

About this task

Note: The names of equivalent activities are given in parentheses after the cmdlet names for those who are using Microsoft System Center Orchestrator.

The `Invoke-OCDRFailover` composite cmdlet (**DR Failover**) runs several individual objects to perform the failover.

The `Invoke-OCDRFailover` composite cmdlet (**DR Failover**) perform failover from the primary site (site A) to the secondary site (site B). It must be run with the `-Force` parameter or property if any of the entities to be failed over already exist.

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

Refer to the descriptions of the individual cmdlets or the activities in the *OnCommand Plug-in 3.1 for Microsoft Windows PowerShell Cmdlet and Orchestrator Activity Reference Guide* for more details.

Steps

1. The `Confirm-OCDRPlan` cmdlet (**Validate DR Plan**) is run to validate the secondary site (site B) before the failover begins.
2. The `Reset-OCDRSite` cmdlet (**Clean-up a DR Site**) is run with the `-Force` parameter specified to cleanup conflicting cluster resources and LUNs on the secondary site (site B).
3. The `Invoke-OCDRMirrorBreak` cmdlet (**Release SnapMirror**) is run to break all the `SnapMirror` relationships on the secondary site (site B).
4. The `Connect-OCDRLUN` cmdlet (**Connect DR Storage**) is run with the `-Force` parameter specified to connect all the LUNs on the secondary site (site B).
5. The `Restore-OCDRVm` cmdlet (**Restore VMs activity**) 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` cmdlet (**Update DR Plan**) with the `-Failback` parameter specified to update the disaster recovery plan. Specify the primary server as site B and the secondary server as site A.

For example, with cmdlets you would input the following:

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.

Disaster recovery failback workflow

With crash-consistent disaster recovery, after you fail over from a primary site to a secondary site, you must perform an `Update-OCDRPlan -Failback` on Site B and an `Invoke-`

OCDRMirrorReverseResync on Site A to restore the SnapMirror relationships from the secondary site to the primary site. The Invoke-OCDRFailback composite cmdlet (**DR Failback**) run several individual activities to perform the failback.

About this task

Note: The names of equivalent activities are given in parentheses after the cmdlet names for those who are using Microsoft System Center Orchestrator.

The Invoke-OCDRFailback composite cmdlet (**DR Failback**) must be run with the -Force parameter to perform failback from the primary site (Site B) to the secondary site (Site A).

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

See the descriptions of the individual cmdlets in the *OnCommand Plug-in 3.1 for Microsoft Windows PowerShell Cmdlet and Orchestrator Activity Reference Guide* for more details.

Steps

1. The Confirm-OCDRPlan cmdlet (**Validate DR Plan**) is run to validate the current state of the secondary host against the data captured in the specified disaster recovery plan file before the failback begins.
2. The Reset-OCDRSite cmdlet (**Clean-up DR Plan**) is run with the -Force parameter to clean up conflicting cluster resources and LUNs on the secondary site (Site A).
This activity removes only the virtual machine conflicting resources from the secondary site.
3. The Invoke-OCDRMirrorBreak cmdlet (**Break SnapMirror**) is run to break all the SnapMirror relationships on the secondary site (Site A).
4. The Connect-OCDSLUN cmdlet (**Connect DR Storage**) or is run with the -Force parameter to connect all the LUNs on the secondary site (Site A).
5. The Restore-OCDRVMD cmdlet (**Restore VMs**) is run to restore all virtual machines on the secondary site (Site A).

After you finish

After the failback operation is complete, you should update the disaster recovery plan for the next failover from Site A. Then you could run the Reset-OCDRSite cmdlet (**Clean-up a DR Site**) with the -Force and -Full options specified on Site B to clean up the secondary site.

The consecutive failover workflow

With crash-consistent disaster recovery, following a failback operation, you should run a second failover operation called the consecutive failover. After you have run a failback operation to restore the data to Site A, you must reestablish the SnapMirror relationships which changes the primary and secondary sites and prepares your system for a future forward failover from Site A to Site B.

Preparing to run the DR Failover activity for a consecutive failover

Although the consecutive failover workflow is automated, you must ensure that you have SnapMirror relationships from Site A to Site B.

Steps

1. Ensure that proper mirror relationships are established.
2. Perform the appropriate step, based on your circumstances:
 - If there is no data loss, use the **Resync SnapMirror** activity on the secondary site (Site B) to resync the relationships from Site A to Site B.
 - If there is data loss, use the **Initialize SnapMirror** activity to create new SnapMirror relationships from Site A to Site B.

After you finish

You can now run the **DR Failover** activity for a consecutive failover.

Running the consecutive failover

It is important to run the consecutive failover workflow following a disaster recovery failback workflow because it validates the disaster recovery plan, removes conflicting resources and LUNs, resets the SnapMirror relationships, and then restores the virtual machines.

Before you begin

Ensure that you have performed all the tasks to prepare to run the **DR Failover** activity with the - Force property for the consecutive failover.

Steps

1. The **Validate DR Plan** activity is run to validate the secondary site (Site B) before the failover begins.
2. The **Clean-up a DR Site** activity is run with the Secondary and Force properties specified to remove conflicting cluster resources and LUNs on the secondary site (Site B).
3. The **Break SnapMirror** activity is run to break all the SnapMirror relationships on the secondary site (Site B).
4. The **Connect DR Storage** activity is run to connect all the LUNs on the secondary site (Site B).
5. The **Restore VMs** activity is run to restore all virtual machines on the secondary site (Site B).

Result

After the consecutive failover operation completes, the SnapMirror relationships are broken, but can be reestablished with a resync operation so that the system is prepared to recover from another failure.

What the Start Test DR Failover activity does

You can use a simulated workflow activity to run a simulation of an automated workflow to perform the failover of virtual machines from a primary site to a secondary site.

The **Start Test DR Failover** activity is a composite activity that runs several individual activities to perform the failover simulation. For more information about the simulated failover workflow, see the *OnCommand Plug-in 3.1 for Microsoft Windows PowerShell Cmdlet and Orchestrator Activity Reference Guide*.

Running the Start Test DR Failover activity

The **Start Test DR Failover** activity performs the steps necessary to complete a simulation of a failover operation from the primary site (Site A) to the secondary site (Site B). No user intervention is required after the **Start Test DR Failover** activity is entered. Refer to the descriptions of the individual objects for more details.

Steps

1. The **Validate DR Plan** activity is run to validate the secondary site (Site B) before the failover begins.
2. The **Clean-up a DR Site** activity is run with the Force properties specified to remove conflicting cluster resources and LUNs on the secondary site (Site B).
3. The **Break SnapMirror** activity is run to break all the SnapMirror relationships on the secondary site (Site B).
4. The **Connect DR Storage** activity is run to connect all the LUNs on the secondary site (Site B).
5. The **Restore VMs** activity is run to restore all virtual machines on the secondary site (Site B).
6. The **Stop Test DR Failover** activity is run to reset the test environment in preparation to run the **Start Test DR Failover** activity again.

The **Start Test DR Failover** activity resets the secondary site and performs a reverse resynchronization.

Preparing to simulate failover

Although the simulate failover workflow is automated, you must ensure that your disaster recovery plan and SnapMirror relationships are updated.

Steps

1. Run the **Create DR Plan** object on the primary site (Site A) to create a disaster recovery plan and store it in a central location; the default folder location is C:\ProgramData\OnCommand\MS_Plugin.

You can replicate the disaster recovery plan to the secondary site (Site B).

2. Create new SnapMirror relationships from the primary site to the secondary site with the **Initialize SnapMirror** object prior to the failover operation.
3. Update the SnapMirror relationships with the **Update SnapMirror** object 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.

4. Run the **Update DR Plan** object on the primary site (Site A) to update the disaster recovery plan with the latest configuration information.

After you finish

You can now run the **Start Test DR Failover** object.

Usage tips

The following tips are intended to assist you with challenging issues related to your use of the plug-in and the associated systems.

Tips for solving SCOM console issues

If you experience an issue with OnCommand Plug-in for Microsoft and the Microsoft System Center Operations Manager (SCOM) console, there are some tips to help you find the source of the problem and solve it.

Console tasks fail consistently

The Data ONTAP Storage Systems pane does not appear in the SCOM Monitoring window

Ensure that you imported all the Data ONTAP management packs.

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

[*Microsoft TechNet web site*](#)

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 and resolve it.

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.

Troubleshooting

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

The specified destination server is not managed by an SCVMM server

Issue

When you try to create a clone from an SCVMM template and the specified destination server is not managed by an SCVMM server, you receive an error.

Corrective action

Add the clone destination server to the SCVMM server.

Troubleshooting Orchestrator

You can use the troubleshooting information to research an issue, view any error messages, determine the cause of that issue, and what the resolution or workaround for that issue is.

The published data is not visible even though you subscribed

Issue

The published data is not visible even though you subscribed to it in the user interface.

Corrective action

1. Double-click on the Orchestrator activity for which you want to receive published data.
2. In the properties window, go to the **Run Behavior** tab, click on the **Flatten** check box, then click **Finish**.
3. Link the activity to another activity such as the **Append Line** activity
4. Right-click in one of the text boxes in the properties window, select **Subscribe > Published Data**. The Published Data window opens with the published data listed.
5. You can go back to uncheck the **Flatten** check box. The properties remain.

You cannot run the Delete VM activity on a remote host

Message The specified Virtual machine <VM Name> is not found on your local host <localhost>. Remote VM delete operations are not supported. Please try the operation on the host where VM is present.

Corrective Action When you build the **Delete VM** workflow, the VIM web service server used in the input field must be the server on which the virtual machine resides and the VIM web service is installed.

Create clone request is invalid

Description The error occurs only for requests to clone a virtual machine with an System Center Virtual Machine Manager (SCVMM) template.

Message The create clone request is invalid. Reason : Error: - SCVMM Administrator console not installed on the local host.
Exception: FaultException`1 Target site: RealProxy.HandleReturnMessage Stack trace: ...

Corrective action

- Make sure the correct Web service server is specified in the activity properties where the template is located and the Web service is installed.
- The SCVMM Administrator console must be installed on the same server on which the template resides if it is not an SCVMM server.

VIM web service does not restart

Issue VIM web service does not restart.

Corrective action Perform the following procedure:

1. Go to **Administrative Tools > Services**
2. From **Virtual Disk service**, restart the VDS service.
3. Restart the VIM web service again.

Troubleshooting cloning

Invalid mount point

Message ValidateCreateCloneRequest: Invalid mount point for create clone request.

Description	Either the specified mount point format is invalid or that mount point is in use on the clone destination server.
Corrective action	Use another mount point or correct the mount point format.

Unsupported OSType

Message	<code>ValidateLunOsType</code> failed.
Cause	A LUN that contains the source virtual machine or template VHD is created with an unsupported <code>OsType</code> . The supported <code>OsTypes</code> are <code>windows_2008</code> and <code>hyperv_v</code> .
Corrective action	Create a new LUN with the proper <code>OsType</code> and create a source virtual machine or template on it.

Misaligned VHD path

Message	<code>"VHDPATH"</code> is not aligned to 4K boundary.
Cause	The partition inside one of the VHDs of the source virtual machine or template is not aligned to a 4K boundary.
Corrective action	Create the VHD with partitions that are 4k aligned. If the VHD has MBR partitions, run the <code>MBRAAlign</code> tool.

Cloning a template fails

Message	VMM is unable to complete the request. The connection to the agent on machine has been lost.
Cause	There was a connection problem from the SCVMM server to the Hyper-V server where the virtual machine was being deployed.
Corrective action	Check the network access from the SCVMM server to the Hyper-V server. Check that the DNS name resolves to the proper I/O address for the SCVMM server and the Hyper-V server.

Troubleshooting disaster recovery

Creating a disaster recovery plan across domains fails

Description	When you run the Create DR Plan object to create a disaster recovery plan across two different domains, it fails.
--------------------	--

Message	An Error occurred while retrieving the GetHostData data.
Corrective action	You need to ensure that the following factors are true: • The domain trusts are working in directions. • If the two domains are from two different forests, you need to check for access rights. To add user access rights, go to Computer Management > Local Users and Groups > Groups. Add the user from the other domain to the administrators group.

The Update DR Plan activity returns a generic failure

Message	Update DR Plan returned a generic failure.
Description	The error occurred because an invalid mount point D:\ was used. Since the D: drive is a DVD drive, the check for conflicting mount points causes the DR Failover process to fail.
Corrective action	Do not use a mount point that uses the local CD/DVD drives on both the primary and secondary sites for virtual machines.

The restored virtual machine fails to start

Issue	After a successful disaster recovery failover and failback operation, the restored virtual machine fails to start.
Description	After a restore of the virtual machine, the virtual machine incorrectly enters the Saved state and then fails to start.
Corrective action	You must delete the saved state file from the virtual machine and then start the virtual machine. In the Hyper-V Manager interface, right-click the restored virtual machine and select Delete Saved State .

Known issues

The description of the known issues in the 3.1 release of OnCommand Plug-in for Microsoft can help you to recognize issues that have been encountered in the various areas if the plug-in.

System Center Operations Manager issues

This section contains issues related to the System Center Operations Manager (SCOM).

Performance and resource optimization issues

If you experience an issue with OnCommand Plug-in for Microsoft performance and resource optimization (PRO) tips, you can use tips to help find the source of the problem and resolve it.

PRO Tips do not appear

If you are experiencing problems viewing PRO Tips, you can perform the following steps:

1. Import the Data ONTAP management packs.
2. Enable the Data ONTAP PRO Discovery Rule for the Microsoft System Center Operations Manager management server and set the credentials for that server.
3. Ensure 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.

In MultiNode and NLB SCOM Server deployments, ensure SCVMM server is connected to the SCOM Server having the Root Management Server (RMS) Emulator set to Yes.

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 you have done the following:

- 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. For more information, see the Microsoft Web site.

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 concepts

[Preparation to use OnCommand Plug-in for Microsoft](#) on page 15

Related information

[Microsoft TechNet web site](#)

View PRO Script is not visible for PRO Tips

View PRO script is visible only if you use the built-in Microsoft PRO module. In SCVMM 2012, this module runs on the SCVMM server so that **View PRO script** is not visible.

The alignment of some VHDs is not checked when selecting a large number of VHDs in SCOM for VHD alignment checking

If you select a large number of VHDs when you run the "Data ONTAP Virtualization: Check VHD Alignment Status" task, some of the VHDs might not be examined for alignment. You should run the "Data ONTAP Virtualization: Check Host VHD Alignment Status" for Hyper-V Hosts which examines all VHDs on all selected hosts. Another alternative is that you can wait for the VHD alignment checking rule to run.

This issue is due to a Microsoft limitation on the number of PowerShell calls that can be made.

The specified source and destination LUNs reside in different storage systems

Description

When you use any cloning object to create a clone and the LUN that contains the source virtual machine or VHD and the specified clone data destination LUN are on different storage systems, you receive an error.

Corrective action

Specify an NTFS that is mounted on the LUN that is on the same storage system and same storage volume as that of the LUN that contains the source VHDs.

The installation of OnCommand Plug-in for Microsoft results in error 1158

When you start the installation of OnCommand Plug-in for Microsoft from the executable file, an error message might appear with the error number 1158. You can try the installation again.

If the problem persists, close any unnecessary windows that are open on the desktop. Go to **Control Panel > Uninstall** and refresh the list of programs, then try the installation again.

The path to the executable file is missing

After you install or upgrade OnCommand Plug-in for Microsoft, when you execute tasks such as discovery, adding and removing controllers, or managing controller credentials, your system might fail with the following error: %OCSCOMPAT%/executable.exe not found. The error is caused because the installer path environment variable has not taken effect in System Center Operations Manager (SCOM) and the path to the executable file is missing.

Workarounds:

- During installation, keep the SCOM console closed.
If the console was open during the installation, after installation has finished, close the SCOM console and reopen it.
- Run the SCOM console with the clear cache command:
Microsoft.MOM.UI.Console.exe/ClearCache
- Log off and then log on to the system and reopen SCOM.

Data ONTAP: Add Controller reports a success message for invalid entries

When you try to add a controller using **Data ONTAP: Add Controller**, the plug-in tries to contact the controller using SNMP first, which is registered as a Reserved task in the System Center Operations Manager (SCOM) tasks view. If SNMP is successful, the plug-in then proceeds to contact the controller using HTTP or HTTPS.

When a controller can be reached by SNMP and not by HTTP or HTTPS, the Reserved task in SCOM presents a successful status.

Virtualization discovery does not return any values for Hyper-V host after ApplianceWatch PRO 2.1 or 2.1.1 is uninstalled

The virtualization discovery Web service from the System Center Operations Manager (SCOM) host to the Hyper-V host completes successfully but there are no values in the virtualization folder in SCOM after an upgrade.

Workaround:

Perform the following procedure after you uninstall ApplianceWatch PRO 2.1 or 2.1.1.

1. Install the OnCommand Plug-in for Microsoft 3.0 discovery agent on the Hyper-V host.
2. Optional: Uninstall OnCommand Plug-in for Microsoft 3.0 discovery agent if you do not need it. Installing and then uninstalling the discovery agent ensures that the root\dataontap namespace is properly cleaned up.

Contact Microsoft for SCOM updates to address this issue.

System Center Operation Manager might crash when Data ONTAP Discovery task is run

System Center Operation Manager (SCOM) might crash when the Data ONTAP Discovery task is run due to an incompatibility with Internet Explorer 9.

Workaround:

Uninstall Internet Explorer 9.

OC.SC.COM.log rolls over into multiple logs

OC.SC.COM.log is normally created when it has logged processes that total 10 MB in size. When a log reaches 10 MB, another log file is created to collect the next 10 MB of events: for example OC.SC.COM.log.1, OC.SC.COM.log.2, and so on. The log file often does not reach 10 MB in size when multiple processes are sending events to the OC.SC.COM.log file at the same time. Instead, the log file might roll over multiple times and create a new log file that is very small.

Calculation for projected savings can actually be less than the current savings

In certain cases, the calculation for projected savings can actually be less than the current savings.

For clarification, the three savings metrics are defined as follows:

Current Savings	An estimate of how much space is being saved due to deduplication and cloning.
Projected Savings	An estimate of how much space will be saved in the future due to deduplication, while taking into account overhead for space reserves. Note that this can be less than your current savings in some cases.

**Storage
Efficiency**

An estimate of how efficiently space is saved, based on your current and projected savings.

A controller might be displayed more than once in the Manage Controller Credentials view

If you click **Add Controller** from the Tasks pane to add a controller with an IP address and then later use **Add Controller** to add the same controller using a different IP address, the controller is displayed twice in the Manage Controller Credentials view.

To avoid adding controllers that are already monitored by System Center Operations Manager (SCOM), during an upgrade, you must first run the discovery task to discover all controllers and network devices that are being monitored; then you can add any new controllers.

OnCommand Virtual Infrastructure Management Service (VIM_Service) on the local computer started and then stopped

The following error is returned if you used Ctrl + Break to end a PowerShell session while a cmdlet was still running:

The Virtual Infrastructure Management Service on Local Computer started and then stopped. Some services stop automatically if they are not in use by other services or programs.

In this case, OnCommand Virtual Infrastructure Management Service (VIM_Service) might not start. If, before you ended the session, the cmdlet had sent any requests to Microsoft Virtual Disk Service (VDS), that service might be left in a state that would prevent restarting.

Workaround:

Restart the VDS service and then restart VIM_Service.

vFiler unit credentials are not removed if the physical filer is removed

vFiler unit credentials are encrypted and saved in the System Center Operations Manager (SCOM) database. If the parent controller is removed from SCOM and then added back into SCOM, the vFiler unit credentials that were entered previously remain in the SCOM database and are used to monitor the vFiler unit again.

Therefore, the vFiler unit is automatically authenticated which is a security issue.

Hyper-V hosts might take three to four hours to appear in SCOM

Hyper-V hosts that are managed by the System Center Virtual Machine Manager (SCVMM) server and have Hyper-V Snapshot copies associated with them might take three to four hours to appear in System Center Operations Manager (SCOM).

Provisioning issues

This section contains issues related to provisioning.

Using Volume GUID as a mount point for virtual machine configuration

Description When a virtual machine is hosted on a LUN that uses the volume GUID as the mount point on the primary site, you can create a new disaster recovery plan successfully. When you perform a disaster recovery failover to the secondary site, the LUN is connected successfully. And then the operation fails with an error.

Message Copy virtual machine export data failed for VM = *VM_name*, VMGUID = *VM_GUID_number*, Reason = Illegal characters in path.

Corrective action There is no workaround for this issue. Using a volume GUID for virtual machine configuration is not supported in this release.

Map LUNs to igroups with type Hyper_V only

If you use the `New-OCStorage`, `Connect-OCStorage`, or `New-OCClone` cmdlets to map LUNs to igroups that contain host initiators with a type other than `Hyper_V`, an error is returned.

To successfully run a LUN to the host initiator task, you must change the igroup type to `Hyper_V`.

If you have mapped any other LUNs to igroups with a type other than `Hyper_V`, you must first delete the mappings and then change the type to `Hyper_V`.

If you have not mapped any LUNs to igroups with a type other than `Hyper_V`, you can delete the igroup and try the operation again.

A PowerShell execution policy set to Allsigned causes New-OCClone cmdlet to fail

If you use the PowerShell Allsigned execution policy with the `New-OCClone` cmdlet, the operation fails. You can import the Microsoft System Center Virtual Machine Manager (SCVMM) certificate as a Trusted Publisher to avoid this error.

For more information on importing a certificate, see the Microsoft TechNet Web site.

Related information

[Microsoft TechNet website](#)

Virtual machine cloning into an existing CSV with the same base name fails

The path for a cloned VHD is generated by using the name of the source VHD and appending `_clone_BaseVMName` to it. If the `New-OCCLone` cmdlet fails because the VHD path information already exists, the system returns the following error:
Failed to create file <VHD File Path>. The file exists.

Workaround:

Retry the command and change the `-BaseVMName` parameter to ensure a unique new path that does not conflict with any existing VHD path.

XenDesktop import failure - host names of virtual machines are not changed from the source virtual machine name

Clones must have unique names in the Hyper-V Manager. If the host name of a newly cloned server is the same as the name of the source virtual machine, the server name is not changed and therefore not unique, which causes the XenDesktop import to fail.

You can use the tool that is indicated for your operating system to change the host name:

- For Windows 2003, Windows XP, and older operating systems, you can use `sysprep.exe` to run the Sysprep tool on your VHDs.
- For Windows Vista and newer operating systems, you can use Windows Automated Installation Kit (WAIK) to create an answer file and then run the Sysprep tool on your VHDs.

The source VHD and source virtual machine configuration must be on a LUN from Data ONTAP storage.

Run Sysprep on the VHD that is attached to the virtual machine. The virtual machine is in an off state after you attach the VHDs on which Sysprep has been run.

For detailed information on how to run Sysprep in Windows XP and Windows 7, see the Microsoft TechNet site.

Related information

[*Microsoft TechNet website*](#)

You must add a string of MSvSCVMM as a connection name when you add an SCVMM host to Citrix Desktop Studio

When you use the Add Host Wizard during the initial configuration of Citrix Desktop Studio to add the SCVMM host, a connection name is requested. You must enter a specific string of MSvSCVMM in this field for the import to succeed.

Running provisioning and cloning cmdlets as a user other than the Windows administrator

You can avoid running the provisioning and cloning cmdlets as the built-in Windows administrator and run them as a user in the Administrators group.

Before you begin

You must have installed the provisioning and cloning cmdlets.

Steps

1. Open the Windows **Start** menu.
2. Select **Run**, type `secpol.msc`, and click **OK**.
3. From the **Local Security Settings** window, click **Local Policies** and then **Security Options**.
4. Double-click **User Account Control: Run all administrators in Admin Approve Mode**.
5. Select **Disabled** and click **OK**.
6. Close the **Local Security Settings** window.
7. Restart the Windows host.

Result

After you restart the Windows 2008 R2 server, you can run the provisioning and cloning cmdlets without being the Windows built-in administrator.

If the system clock is out of sync, the node loses connectivity

If the system clock on any node is more than five minutes out of sync with the clock on the storage controller, the node loses connectivity to the storage controller. You should also ensure that the time difference is less than five minutes between the host machine and the domain controller time clocks and the storage system.

If the clock is out of sync on one of the nodes in a cluster and you run the `New-OCStorage` cmdlet with the `-CSV` parameter, it should create a LUN that is connected to all the nodes of the cluster. But it actually results in creating a dedicated LUN that is connected to only one host.

Error when you use the volume GUID as a mount point for virtual machine configuration

When a virtual machine is hosted on a LUN that uses the volume GUID as the mount point on the primary site and you perform a disaster recovery failover to the secondary site, the LUN is connected successfully. But then the operation fails with the following error:

Copy virtual machine export data failed for VM = Clus-01-vm02, VMGUID = 4B786875-64BD-4AEA-ACDE-1CD286FFD09C, Reason = Illegal characters in path

The 3.1 version of OnCommand Plug-in for Microsoft does not support the virtual machines that use the volume GUID for configuration in disaster recovery operations.

Resizing dedicated disks could take longer than expected

The time that is required to expand or shrink a shared LUN varies based on the size of the LUN and could take longer than expected. For example, to resize a shared LUN that is 100 GB in size can take as long as six minutes to complete.

The storage path of FC connected disks owned by adjacent nodes in a cluster cannot be discovered

The storage path of FC connected disks owned by adjacent nodes in a cluster cannot be discovered. Therefore, when you run cmdlets remotely on adjacent nodes of a cluster, the Set-OCStorageSize, Remove-OCStorage, and Disconnect-OCStorage cmdlets might fail.

Workaround:

Ensure that you have the discovery agent installed in order to discovery FC LUNs. You do not need to do anything further to discover iSCSI LUNs.

Virtual Machine Manager encountered an error and exited the process

Virtual Machine Manager encountered an error and needed to exit the process. The crash occurs when SCVMM encounters incorrect or incomplete HA virtual machine configurations.

To recover from this problem, you should restart the service after cleaning up and removing any virtual machines on the host or cluster that do not have the complete virtual machine configuration.

This error can happen when you use the Remove-OCVM cmdlet on an HA virtual machine because the resource group for the virtual machine is not deleted from the Windows failover cluster (WFC).

If you use the Remove-OCVM cmdlet, you should delete the resource group that was left behind in the WFC. To correctly remove the HA virtual machines, use the SCVMM Remove-VM cmdlet.

The default settings and timeouts in SCVMM SSP 2.0 might limit the number of simultaneous CreateVM requests

The service and portal timeout settings for Microsoft System Center Virtual Machine Manager Self-Service Portal 2.0 are different, which might affect the success of a large number of CreateVM requests.

You can use the following settings to successfully create large numbers of CreateVM requests:

- Portal setting - sessionState timeout
- Service setting - maxSimultaneousWorkflows
- Service setting - maxVMHostCapacity

To change the settings, see the following Microsoft documentation:

- *Virtual Machine Manager Self-Service Portal Operations Guide*
- *Virtual Machine Manager Self-Service Portal Administration Guide*
- *Virtual Machine Manager Self-Service Portal Deployment Guide*
- *Virtual Machine Manager Self-Service Portal Extensibility Guide*

After changing the settings, you should restart the Self-Service Portal.

Related information

[*Microsoft TechNet web site*](#)

Creating a virtual machine request from SCVMM Self-Service Portal fails

Creating a virtual machine request from the SCVMM Self-Service Portal fails to deploy cloned virtual machines into a server that is a member of the Windows failover cluster. Only HA virtual machines can be created from an SCVMM template on a cluster node.

The following error message is returned:

Virtual Machine Clone operation failed to execute.

Workaround:

Join the NetApp community for OnCommand Plug-in for Microsoft on the NetApp Community Web page and request the updated scripts.

WMI warnings appear in the event logs

When WMI warnings are seen in the event log, you should check the administration events in the Hyper-V VMMS event log for more information.

If the WMI warnings contain the Microsoft synthetic Ethernet port error, you should check and reconfigure the virtual machine network configurations for those cloned virtual machines that produced the warnings.

Because you do not know what other WMI warnings, issues, or errors Microsoft WMI might produce, you should always be vigilant of Microsoft administration events in the Hyper-V Virtual Machine Management Service (VMMS) event log and look in the Microsoft event log for more information.

Two HA virtual machines with the same name

Issue

If there is an existing HA virtual machine on the secondary site that has the same name as an HA virtual machine on the primary site (with a different GUID), the disaster recovery failover requires the Force property.

Description

After you issue a disaster recovery failover with the Force property, the disaster recovery failover removes the existing cluster resource with the same name from the secondary site, moves the

resource disk to the available storage group, and leaves the existing virtual machine configuration unchanged.

Then the disaster recovery failover creates the same cluster resource group and the HA virtual machine. After the disaster recovery failover operation completes, there are two virtual machines with the same name in the Hyper-V Manager. The disaster recovery failover does not remove the virtual machine with same name in the Hyper-V Manager since this virtual machines have a different GUIDs.

Corrective action

Because the disaster recovery failover does not delete the existing virtual machine that has the same name as the Hyper-V Manager, there are two resolutions:

1. Manually delete the duplicate virtual machine name from the Hyper-V Manager
2. If you want to recover this existing virtual machine, you can run it as a non-HA virtual machine or go back to the cluster and add this virtual machine back for HA. In this case, the new virtual machine resource group has the same name as the one created by the disaster recovery failover.

Cloning Issues

This section contains issues related to cloning.

New-OCClone cmdlet fails because the VHD path information already exists

If the New-OCClone cmdlet is run with the JustCloneVHD parameter and then run again using the same base name but without the JustCloneVHD parameter, the second New-OCClone cmdlet fails because the VHD path information already exists.

The system returns the following error:

```
Failed to create file <VHD File Path>. The file exists.
```

The path for a cloned VHD is generated by using the name of the source VHD and appending `_clone_BaseVMName` to it. Changing the `-BaseVMName` parameter ensures a unique new path that does not conflict with any existing VHD path.

Workaround:

Retry the command and change the `-BaseVMName` parameter to ensure a unique new path that does not conflict with any existing VHD path.

New-OCClone might result in excess free space

The New-OCClone cmdlet might leave free space when you create or clone a new LUN for a virtual machine. If the free space is larger than 8 MB, it shows up in the Disk Management view.

When you create or clone the LUN, the full space is not used in the partitioning and formatting of the LUN. You can leave the space as it is, and all the applications on the system that use formatted NTFS on the LUN still perform correctly.

The New-OCClone cmdlet fails on vFiler units that use Data ONTAP versions earlier than 7.3.3

The use of vFiler units is only supported when you use Data ONTAP version 7.3.3 and later.

Cloning into an existing LUN on a remote system is not supported

Issue

Cloning into an existing LUN on a remote system is not supported.

Description

The clone target is a remote system or cluster and the mountpoint is in use by a mounted NTFS.

Corrective action

Use a mountpoint that is not used by a mounted NTFS so that a new LUN is created with the cloned data and mounted at the specified mountpoint.

Cannot clone a virtual machine from a System Center Virtual Machine Manager (SCVMM) template into a CSV

Cloning virtual machines from an System Center Virtual Machine Manager (SCVMM) template to put each virtual machine into a newly created cluster shared volume (CSV) is not supported due to SCVMM limitations. If you want to clone a virtual machine into a CSV, you must perform the following steps.

Steps

1. Use the New-OCStorage cmdlet to create a CSV of the size that is large enough to hold the specified number of virtual machines that you want to create:

```
New-OCStorage -StoragePath lun_path_on_storage -s clustername -csv -size required_size_gb/mb
```

2. Use the Refresh-VMHostCluster cmdlet or use the SCVMM GUI to refresh an SCVMM host or cluster:

```
Refresh-VMHostCluster -VMHostCluster VMHostCluster
```

3. Use the New-OCCLone cmdlet to clone virtual machines into the existing CSV:

```
New-OCCLone -vmms $SCVMM server-template $Template_Name -s $cluster_name-mp  
existing_csv_reparsepoint
```

Neither source VHD nor clone destination is on a LUN

Issue

Neither the mounted NTFS that contains the source VHD nor the specified mount point of an existing NTFS to be used as the clone destination is on a LUN.

Corrective action

The source VHDs must be mounted on a LUN and the clone destination must be a LUN.

The specified destination server is not managed by an SCVMM server

Issue

When you try to create a clone from an SCVMM template and the specified destination server is not managed by an SCVMM server, you receive an error.

Corrective action

Add the clone destination server to the SCVMM server.

Disaster recovery issues

This section contains issues related to disaster recovery.

Partial restore operations for virtual machines

Occasionally, a failover or failback operation does not restore all the virtual machines that reside at a site.

During failover, the system attempts to restore all of the virtual machines that it can, even if one or more virtual machines cannot be restored. As a result, it might restore only a subset of the total number of virtual machines to the secondary site. During a failback operation, a subset of virtual machines might be restored to the primary site while the remaining virtual machines remain on the secondary site.

You can determine the reasons for the partial restore operation in the event log. When you experience a partial restore, the administrator must ensure that the setup is reset before you attempt another failover or failback operation.

For more information about restoring virtual machines, see the *OnCommand Plug-in 3.1 for Microsoft Windows PowerShell Cmdlet and Orchestrator Activity Reference Guide*.

Related concepts

[Failover and failback requirements](#) on page 74

[Events](#) on page 56

Disaster recovery failover fails on the secondary site

Disaster recovery failover fails on the secondary site and returns the following error:
UpdateDRPlan returned a generic failure

To avoid this conflict, you must ensure the following:

- An identical hardware configuration exists on both the primary and the secondary sites.
- Local CD or DVD drives or devices are used as mountpoints for virtual machine configurations.

After a disaster recovery restore, the restored virtual machine fails to start

After a disaster recovery restore operation, the virtual machine that has been restored enters the saved state and fails to start.

Perform the following steps to delete the saved state file for the virtual machine and then restart the system:

1. In the Hyper-V Manager interface, right-click the restored virtual machine.
2. Select **Delete Saved State**.
3. Start the virtual machine.

The -Force parameter is required to perform some disaster recovery failover procedures

If there is a high availability virtual machine on the primary site and another high availability virtual machine with the same name but a different GUID on the secondary site, you must use the `-Force` parameter to perform a disaster recovery failover.

After you issue the `Invoke-OCDRFailover` cmdlet with the `-Force` parameter, the disaster recovery failover removes the existing cluster resource with the duplicated name from the secondary site, moves the resource disk to the available storage group, and leaves the existing virtual machine configuration untouched on the Hyper-V Manager. Then the disaster recovery failover creates the same cluster resource group on the HA virtual machine.

After the disaster recovery failover operation completes, there are two virtual machines with the same name in the Hyper-V Manager. The disaster recovery failover does not remove the virtual machine with the duplicated name in the Hyper-V Manager since this virtual machine has a different GUID.

The disaster recovery plan folder does not contain all the virtual machine configuration files

When virtual machines are hosted on more than one node and you run the `New-DRPlan` cmdlet, the virtual machines are only exported locally. The result is that the virtual machine configuration files

only exist on the node that the virtual machines are currently on but not on the node where the New-DRPlan cmdlet was run.

A failure occurs when you try to create a disaster recovery plan across domains

A failure occurs when you try to create a disaster recovery plan across domains. The following error is returned:

An Error occurred while retrieving the GetHostData data.

If the two domains are from two different forests, you must ensure the following:

- The domain trusts are working in both directions.
- If the two domains are from two different forests, you must check for access rights.

To add user access rights, go to **Computer Management > Local Users and Groups > Groups** and add the user to the Administrators group.

The disaster recovery Invoke-OCDRMirrorReverseResync cmdlet fails because of an incorrect storage system name

Storage system names are case sensitive. The disaster recovery Invoke-OCDRMirrorReverseResync cmdlet fails if the storage system name does not match exactly the name as listed in the disaster recovery plan.

If the cmdlet fails due to a storage system name mismatch, remove the SnapMirror relationships that are involved, reestablish the relationships with the proper short names, and try the cmdlet again.

Reset-OCDRSite does not delete virtual machine resource groups

After the Reset-OCDRSite cmdlet is run successfully on the secondary site, the virtual machine cluster resource disk is removed properly but the virtual machine resource group is still present.

Workaround:

After you run the Reset-OCDRSite cmdlet, perform the following steps:

1. Go to the Failover Cluster Manager.
2. In Services and Applications, manually delete the remaining virtual machine resource groups.

The Reverse Resync SnapMirror object call fails

Issue

The **Reverse Resync SnapMirror** object call fails because of a case-sensitive issue in the SnapMirror relationship name.

Corrective action

Create or establish the SnapMirror relationship with a correct case-sensitive storage system name or use the **Initialize SnapMirror** object. The Storage System name that is used to establish the mirror relationship must match the short storage system name.

The specified source and destination LUNs reside in different storage systems**Description**

When you use any cloning object to create a clone and the LUN that contains the source virtual machine or VHD and the specified clone data destination LUN are on different storage systems, you receive an error.

Corrective action

Specify an NTFS that is mounted on the LUN that is on the same storage system and same storage volume as that of the LUN that contains the source VHDs.

The Reverse Resync SnapMirror object call fails**Issue**

The **Reverse Resync SnapMirror** object call fails because of a case-sensitive issue in the SnapMirror relationship name.

Corrective action

Create or establish the SnapMirror relationship with a correct case-sensitive storage system name or use the **Initialize SnapMirror** object. The Storage System name that is used to establish the mirror relationship must match the short storage system name.

Copyright information

Copyright © 1994–2012 NetApp, Inc. All rights reserved. Printed in the U.S.

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. 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 United States and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the United States 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 United States 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 email 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 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

Index

A

- activities
 - automated 74
 - Connect Storage 65
 - Data ONTAP Toolkit 62
 - Provision Storage 65
- Add Controller 92
- administration profiles, Windows Powershell 11
- Administrators group 104
- Aggregates view 45
- Alert Details pane 42
- alerts
 - PRO tips 51
- Alerts view 42
- alerts,
 - monitoring 42
- alignment
 - checking 60
- alignment checking 60, 91
- Allsigned execution policy 95
- ApplianceWatch PRO, uninstalling 20
- attributes 47
- automated workflow activity 81
- automated workflow objects 81
- availability events 56

B

- background installation 22
- background uninstallation 25

C

- cache credentials
 - storage system 63
- Check VHD Alignment Status 91
- checklist for plug-in installation 15
- child features
 - silent installation 23
- Clone NTFS File activity 67
- Clone VM activity 67
- Clone VM from SCVMM Template activity 67
- cloning
 - into a new LUN 68
 - file 67

- into an existing CSV 69
 - into the same LUN 69
 - prerequisites 66
 - virtual machines 68
- cloning cmdlets 66
- cloning issues 100
- cloning virtual machines 67
- cmdlet
 - New-OCClone 95
- cmdlet requirements
 - cloning 66
 - provisioning 64
- cmdlets
 - cloning 66
 - common parameters 12, 13
 - New-OCClone 101
 - provisioning 64
- component descriptions 9
- composite cmdlets 74
- configuration 30
- configuration events 57
- Connect Storage activity 65
- consecutive failover
 - preparation 81
 - workflow 80
- console issues, troubleshooting 84
- controller configuration information
 - modifying with System Manager 38
- controller credentials
 - adding 30
- controllers
 - monitoring 43
- Controllers view 43, 45
- controllers, adding 30
- CPU utilization 43
- crash-consistent disaster recovery 71
- create DRPlan
 - requirements 72
- CreateVM request limitation 98
- credentials
 - adding to controllers 30
- custom reports 59

D

- Dashboard view 46

Data ONTAP

- Discovery Rule 31
- reports 57
- rules 34, 35

Data ONTAP management server object 36

Data ONTAP objects 31

Data ONTAP Toolkit

- activities 62

Data ONTAP:Add Controller

- messages 92

deploying OIPs 28

Diagram view 43

disaster recovery

- failback workflow 79
- failover workflow 78
- overview 71
- plan 72
- requirements 71

disaster recovery issues 102

disaster recovery plan

- activities 73, 74
- cmdlets 73, 74
- guidelines 73

discovery

- adding controllers 30
- enabling 31
- expediting 32, 33
- rules 31
- running 31
- types 32
- what is 31

discovery task 93

DR Failover object 81

DRPlan

- activities used with 73, 74
- cmdlets used with 73, 74
- See also* disaster recovery plan

DRPlan requirements 72

E

Enable-PSRemoting cmdlet 60

event logs 99

events

- availability 56
- configuration 57

Events window 56

execution policies, Windows Powershell 11

expediting system discovery 32

expediting virtualization discovery 33

F**failback**

- requirements 74, 75

failback workflow 79

failover and failback, requirements 74, 75

failover workflow 78

failover workflow steps 75, 76, 78

feature selection, silent installation 23

file cloning 67

G

GetHostData 104

granular cmdlets 74

guidelines

- disaster recovery plan 73
- installing the plug-in 18

guidelines, VIM Web service 27

H

HA virtual machine configurations

- incorrect or incomplete 98

Health Explorer 42

Health Explorer, launching 61

Hyper-V hosts 94

Hyper-V hosts view 49

Hyper-V LUN alignment

- checking 60

Hyper-V LUNs view 49

Hyper-V Snapshot copies 94

Hyper-V VHDs view 50

Hyper-V VMs view 50

I**I/O**

- operations 44

implementing PRO tips 55

incorrect HA virtual machine configurations 98

installation

- checklist 15
- guidelines 18
- requirements 16
- silent 22

installing the plug-in 20

integration packs, importing 27

invalid entries

- Data ONTAP: Add Controller 92
- Invoke-OCDRFailback composite cmdlet 79
- issues
 - cloning 100
 - disaster recovery 102
 - provisioning 95

L

- latency 44
- launching Health Explorer 61
- limitation on number of CreateVM requests 98
- locating management pack rules 33
- login credentials, setting 37
- LUN latency 42
- LUNs view 46

M

- management of storage controllers 37
- management pack
 - monitors 34, 35
 - rules 33–35
 - upgrading 20
- management packs
 - uninstalling 25
- Management Server view 47
- metrics, performance 43
- Microsoft PRO module 91
- monitoring
 - alerts 42
 - Operations Manager servers 51
 - performance 43
- monitors
 - plug-in 40
 - PRO 41
- monitors, list of 34, 35
- mount point 97
- multiple management server environment 36

N

- New-OCClone cmdlet 101
- New-OCClone cmdlet fails 95

O

- OIPs
 - Data ONTAP Toolkit 62

- deploying 27, 28
 - importing 27
- OIPs)
 - importing 27
- OnCommand Plug-in 3.0 for Microsoft uninstalling 20
- Operations Manager servers
 - monitoring 51
- Orchestrator
 - installation 14
 - integration packs (OIPs) 14
- Orchestrator integration packs (OIPs)
 - deploying 28
 - importing 27
 - uninstalling 29
- overrides, fixing 20
- overriding rules 41

P

- parameters
 - common cmdlet parameters 12, 13
- parent features
 - silent installation 23
- partial failover or failback operation 102
- performance metrics
 - CPU utilization 43
 - I/O operations 44
 - I/O throughput 44
 - latency 44
- performance monitoring 43
- performance monitoring views 45
- plan
 - disaster recovery 72
- plug-in
 - components 9
 - installation 20
 - monitoring 40
 - troubleshooting 90, 91
 - uninstalling 25
- plug-in components 9
- plug-in configuration
 - with multiple management servers 36
- plug-in monitors 40
- plug-in usage and functionality 9
- PowerShell execution policy 95
- preparation
 - for consecutive failover 81
 - to simulate failover 83
- prerequisites
 - cloning 66

- provisioning 64
- prerequisites, disaster recovery 71
- PRO discovery 31
- PRO issues, troubleshooting 90, 91
- PRO monitors 41
- PRO tips
 - enabling 54
 - implementing 55
 - types 51
 - using 51
- Provision Storage activity 65
- provisioning
 - prerequisites 64
- provisioning cmdlets 64
- provisioning issues 95

Q

- Qtrees view 47

R

- relationship state 47
- removing storage controllers 38
- reports
 - custom 59
 - list of 57
 - viewing 59
- requirements
 - for DRPlan 72
 - for failover and failback 74, 75
 - installing the plug-in 16
- requirements, disaster recovery 71
- restore operations for virtual machines 102
- rules
 - availability events 56
 - locating 33
 - management pack 34, 35
 - overriding 41
 - volume latency 42
- runbook designer and server 28

S

- scheduled discovery 30
- SCOM checklist for installation 15
- SCVMM certificate 95
- SCVMM PRO integration 54
- SCVMM Self-Service Portal 98
- setting login credentials 37

- silent
 - installation 22
 - uninstallation 25
- silent installation
 - feature names 23
- simulate failover
 - preparation 83
 - workflows 82
- situations for cloning VMs 68
- SnapMirror
 - status view 47
 - relationship state 47
 - using for disaster recovery 71
- SnapMirror pairs
 - source location 47
- SnapMirror relationships
 - restoring 80
- SNMP communities 36
- SNMP traps
 - configuring 36
- Start Test DR Failover activity 82
- steps to failover 75, 76, 78
- storage cloning 66
- storage controllers
 - adding 30
 - credentials 37
 - managing 37
 - removing 38
 - troubleshooting issues 85
- storage discovery 32
- storage resources
 - monitoring 45, 56
- storage system cache credentials 63
- storage systems
 - Alerts view 42
 - Controllers view 43
 - Diagram view 43
 - Storage Utilization view 48
- sub-component descriptions 9
- sub-LUN clones 67
- sysprep 96
- system
 - monitoring 40
- system discovery, expediting 32
- System Manager
 - modifying storage controller information 38

T

- template

- cloning 68
- throughput 44
- timeout settings 98
- tips
 - console issues 84
 - storage controller troubleshooting 85
- tips for use of the plug-in 84
- troubleshooting
 - consoles 84
 - PRO issues 90, 91
 - storage controllers 85
 - windows installer log check box 91

U

- uninstall wizard 25
- uninstalling
 - ApplianceWatch PRO 20
 - background 25
 - OnCommand Plug-in 3.0 for Microsoft 20
 - silent 25
 - the plug-in 25
- uninstalling the Orchestrator integration packs (OIPs) 29
- update DRPlan
 - requirements 72
- upgrade
 - silent 22
- upgrading
 - the plug-in 20
 - management packs 20
 - the plug-in 20
- usage patterns
 - identifying 43, 45
- usage tips 84
- user access rights 104

V

- vFiler unit credentials 94
- vFilers view 48
- VHD alignment checking rule 91
- VHD alignment, checking 60
- VHDs
 - alignment checking 91
- View PRO Script 91
- views
 - Aggregates 45
 - Alerts 42
 - Controllers 43, 45
 - Dashboard 46

- Diagram 43
- Hyper-V hosts 49
- Hyper-V LUNs 49
- Hyper-V VHDs 50
- Hyper-V VMs 50
- LUNs 46
- Management Server 47
- performance monitoring 45
- Qtrees 47
- SnapMirror status 47
- Storage Utilization 48
- vFilers 48
- Volumes 49
- virtual infrastructure management (VIM) web service,
 - guidelines for using 27
- Virtual Infrastructure Management web service 27
 - See also* VIM web service
- virtual machine
 - cloning from a template 68
- virtual machine cloning 67
- virtual machine configuration 95, 97
- virtual machine host names 96
- Virtual Machine Manager
 - error 98
- virtual machines
 - partial restore 102
- virtual machines, cloning 68
- virtualization discovery 31–33
- volume GUID 97
- Volume GUID as mount point 95
- volume latency rule 42
- Volumes view 49

W

- Windows installer, show log check box 91
- Windows PowerShell
 - administration profiles 11
 - execution policies 11
- WMI warnings 99
- workflow
 - disaster recovery failback 79
- workflows
 - automated 74
 - consecutive failover 80
 - granular and composite 74
 - simulate failover 82

X

XenDesktop

import failure 96