

253-1001374-02
17 November 2011



Brocade Fibre Channel HBA --- Management Pack

User's Guide

Supporting Operations Manager 2007 and Virtual Machine Manager 2008

BROCADE

Copyright © 2012 Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, the B-wing symbol, BigIron, DCX, Fabric OS, FastIron, NetIron, SAN Health, ServerIron, and Turbolron are registered trademarks, and AnyIO, Brocade Assurance, Brocade NET Health, Brocade One, CloudPlex, MLX, VCS, VDX, and When the Mission Is Critical, the Network Is Brocade, are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned are or may be trademarks or service marks of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book or the computer programs that accompany it.

The product described by this document may contain “open source” software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit <http://www.brocade.com/support/oscd>.

Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters
Brocade Communications Systems, Inc.
130 Holger Way
San Jose, CA 95134
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems China HK, Ltd.
No. 1 Guanghua Road
Chao Yang District
Units 2718 and 2818
Beijing 100020, China
Tel: +8610 6588 8888
Fax: +8610 6588 9999
E-mail: china-info@brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour B - 4ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 5640
Fax: +41 22 799 5641
E-mail: emea-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems Co., Ltd. (Shenzhen WFOE)
Citic Plaza
No. 233 Tian He Road North
Unit 1308 - 13th Floor
Guangzhou, China
Tel: +8620 3891 2000
Fax: +8620 3891 2111
E-mail: china-info@brocade.com

Document History

Title	Publication number	Summary of changes	Date
<i>Brocade Management Pack User's Guide</i>	53-1001374-01	New document	April 2009
<i>Brocade Management Pack User's Guide</i>	53-1001374-02	Revised template and front matter, updated web locations, and proofed.	November 2011

Contents

About This Document

In this chapter	v
How this document is organized	v
Supported hardware and software	vi
HBA support	vi
Fabric OS and switch support	vi
Host operating system support	vi
What's new in this document	vi
Document conventions	vii
Text formatting	vii
Command syntax conventions	viii
Notes, cautions, and warnings	viii
Key terms	ix
Notice to the reader	ix
Additional information	ix
Brocade resources	ix
Other industry resources	x
Document feedback	x

Chapter 1

Introduction

In this chapter	1
Management pack overview	1
Obtaining the latest management pack and documentation	2
Supported configurations	2

Chapter 2

Getting Started

In this chapter	3
System requirements for installing management pack	3
Before you import the Management Pack	4
SCVMM and SCOM integration	4
Importing Management Packs related to SCVMM	4
Granting permission	5
Enabling PRO-Tips	6
Installing SCOM agent	7
Importing Brocade FCHBA Management Pack	10

	Creating a new management pack for overrides and other customizations	13
	Tuning performance threshold rules	14
Chapter 3	Understanding Management Pack Operations	
	In this chapter	17
	Classes	17
	Objects discovered by the management pack	19
	Oversubscribed link and deteriorated link alerts	23
	Monitors	24
	Health roll up	25
	PRO-Tip generation	27
	Setting the host unavailable for VM placement	28
Chapter 4	Troubleshooting	
	Troubleshooting PRO for Brocade HBA Management Pack	31
Chapter 5	Frequently Asked Questions	
Appendix A	Scripts	
	Port performance script	28
	Discover HBAs script	29
	Discover ports script	29
	VM migration oversubscribed link recovery task	29
	Set host unavailable recovery task	30
	VM migration deteriorated link recovery task	30
	VM migration power shell script	30
	Set host unavailable power shell script	30

About This Document

In this chapter

- [How this document is organized](#) v
- [Supported hardware and software](#)..... vi
- [What's new in this document](#)..... vi
- [Document conventions](#) vii
- [Notice to the reader](#) ix
- [Additional information](#)..... ix

How this document is organized

This document is organized to help you find the information that you want as quickly and easily as possible.

The document contains the following components:

- Chapter 1, “Introduction,” provides an overview of the Brocade Management Pack, explains how to obtain the latest management pack and documentation, and outlines supported configurations.
- Chapter 2, “Getting Started,” explains what you must know before installing the management pack, installing the SCOM agent, importing the Brocade Fibre Channel HBA Management Pack, and creating a new management pack for overrides and other customizations. Rules for tuning performance thresholds are also included.
- Chapter 3, “Understanding Management Pack Operations,” provides information on management pack service classes, discovered objects, oversubscribed link and deteriorated link alerts, health roll up, Pro-Tip generation and setting the host unavailable for VM placement.
- Chapter 4, “Troubleshooting,” provides basic troubleshooting tips for the management pack.
- Appendix A, “Scripts,” provides a table and description of scripts included with the management pack.

Supported hardware and software

This section describes HBA hardware and software support.

HBA support

The following Fibre Channel host bus adapters (HBAs) are supported in this release.

- Brocade 815. Single-port HBA with a per-port maximum of 8 Gbps using an 8 Gbps SFP+.
- Brocade 825. Dual-port HBA with a per-port maximum of 8 Gbps using an 8 Gbps SFP+.
- Brocade 415. Single-port HBA with a per-port maximum of 4 Gbps using a 4 Gbps SFP.
- Brocade 425 Dual-port HBA with a per-port maximum of 4 Gbps using a 4 Gbps SFP.

NOTE

This publication only supports the HBA models listed above and does not provide information about the Brocade 410 and 420 Fibre Channel HBAs, also known as the Brocade 400 Fibre Channel HBAs.

Fabric OS and switch support

For a current list of compatible servers, switches, storage, and applications, refer to the latest interoperability matrices on the Adapter Resources section of www.brocade.com/adapters or the Partner Network at www.mybrocade.com.

Host operating system support

For a current description of operating system support, refer to the *Brocade Adapters Installation and Reference Guide*. To access this publication, perform the following steps:

1. Visit the Adapters web page at www.brocade.com/adapters.
2. Select the link to download drivers, utilities, and documentation.

Specific operating system service pack levels, and other patch requirements are detailed in the current HBA release notes.

What's new in this document

Updated copyright page, About This Document chapter, document format, references, and Brocade web page links.

Document conventions

This section describes text formatting conventions and important notice formats used in this document.

Text formatting

The narrative-text formatting conventions that are used are as follows:

bold text	Identifies command names Identifies the names of user-manipulated GUI elements Identifies keywords and operands Identifies text to enter at the GUI or CLI
<i>italic text</i>	Provides emphasis Identifies variables Identifies paths and Internet addresses Identifies document titles
<code>code text</code>	Identifies CLI output Identifies command syntax examples

For readability, command names in the narrative portions of this guide are presented in mixed lettercase: for example, **switchShow**. In actual examples, command lettercase is often all lowercase.

Command syntax conventions

Command syntax in this manual follows these conventions:

command	Commands are printed in bold.
-- option, option	Command options are printed in bold.
- argument , arg	Arguments.
[]	Optional element.
<i>variable</i>	Variables are printed in italics. In the help pages, values are <u>underlined</u> or enclosed in angled brackets < >.
...	Repeat the previous element, for example “member[;member...]”
value	Fixed values following arguments are printed in plain font. For example, -- show WWN
	Boolean. Elements are exclusive. Example: -- show -mode egress ingress

Notes, cautions, and warnings

The following notices and statements are used in this manual. They are listed below in order of increasing severity of potential hazards.

NOTE

A note provides a tip, guidance or advice, emphasizes important information, or provides a reference to related information.

ATTENTION

An Attention statement indicates potential damage to hardware or data.



CAUTION

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.



DANGER

A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Key terms

For definitions specific to Brocade and Fibre Channel, see the technical glossaries by logging into www.mybrocade.com.

For definitions of SAN-specific terms, visit the Storage Networking Industry Association online dictionary at:

<http://www.snia.org/education/dictionary>

Notice to the reader

This document may contain references to the trademarks of the following corporations. These trademarks are the properties of their respective companies and corporations.

These references are made for informational purposes only.

Corporation	Referenced Trademarks and Products
Microsoft Corporation	Windows, Windows Server 2003, Windows Server 2008, Vista, XP, PE for Windows, Hyper V for Windows, Windows Automated Installation Kit (WAIK)

Additional information

This section lists additional Brocade and industry-specific documentation that you might find helpful.

Brocade resources

To get up-to-the-minute information, go to <http://my.brocade.com> to register at no cost for a user ID and password. A variety of resources for Brocade products is available.

Adapters

For adapter resources, such as product information, software, firmware, and documentation, visit the Brocade adapters web page at www.brocade.com/adapters and select the link to download drivers, utilities, and documentation.

FCoE Switch

For information on the Brocade FCoE Switch for connecting stand-up CNAs and Fabric Adapter ports configured in CNA mode, refer to the following publications:

- *Brocade 8000 Hardware Reference Manual*
- *Web Tools Administrator's Guide*
- *EZSwitchSetup Administrator's Guide*
- *Fabric OS Command Reference Manual*

SAN information

White papers, online demonstrations, and data sheets are available through the Brocade website at:

<http://www.brocade.com/products-solutions/products/index.page>

For additional Brocade documentation, visit the Brocade website:

<http://www.brocade.com>

Other industry resources

For additional resource information, visit the Technical Committee T11 Web site. This Web site provides interface standards for high-performance and mass storage applications for Fibre Channel, storage management, and other applications:

<http://www.t11.org>

For information about the Fibre Channel industry, visit the Fibre Channel Industry Association Web site:

<http://www.fibrechannel.org>

Document feedback

Quality is our first concern at Brocade and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. Forward your feedback to:

documentation@brocade.com

Provide the title and version number of the document and as much detail as possible about your comment, including the topic heading and page number and your suggestions for improvement.

Introduction

In this chapter

- [Management pack overview](#) 1
- [Obtaining the latest management pack and documentation](#) 2
- [Supported configurations](#) 2

Management pack overview

Brocade Management Pack v 1.0.0.0 which this document covers is Microsoft based Management pack to model Fibre Channel Host Bus Adapter (HBA) and monitor the health of HBA.

Operations Manager uses management packs to model and monitor software and hardware components. Management packs contain the models required for the software to interpret the structure of an application/device and determine the health of the application/device. This knowledge is expressed as an XML document using a pre-defined XML scheme understood by Operations Manager.

System Center Operations Manager (SCOM) 2007 Management Pack (MP) has two kinds of Models:

- **Service Model** - is where we define the classes (which are entities of our managed device/application) and define the relationships between the classes.
- **Health Model** - is where we define the discoveries for the entities and their relationships. We also write monitors and specify roll up criteria and can generate alerts.

The deployment of MP requires an SCOM agent (Health Service) to be installed on each managed host server. You can install the agent from the Root Management Server (RMS) or manually executing the agent installer on each host. This is the most scalable way to deploy in a SCOM managed environment. Please refer to [this section](#) from the *SCOM 2007 Deployment Guide* for details.

The MP is imported into Microsoft System Center Operations Manager (SCOM). It is distributed into managed Hyper-V hosts which have one or more FC HBAs. Once the host is managed, there will be Microsoft SCOM Health Service which can be deployed by SCOM automatically or manually installed. The Brocade MP will be downloaded into these managed hosts and is executed on the SCOM Health Service. The VMM agent service must be installed on the managed host for this management pack to work. This agent can be installed when the managed host is added to the SCVMM console using Add Host action or it can be installed manually.

1 Obtaining the latest management pack and documentation

The Brocade Drivers for HBAs must be installed on managed hosts with HBAs. MP relies on WMI calls through WMI service, and the Brocade Driver acts as WMI Provider servicing the WMI calls issued by MP. The driver must be installed with Administrative privilege. No additional security privileges are needed for the MP other than the OpsMgr Health Service requirement mandated by SCOM/SCVMM.

The sealed version of Management Pack is a file named Brocade.FCHBA.Monitoring.mp.

Obtaining the latest management pack and documentation

Find the Brocade FCHBA Management Pack in the [System Center Operations Manager 2007 Catalog](#).

Supported configurations

The Brocade FCHBA Management Pack for Operations Manager 2007 supports the following configurations:

- Managed host with **Windows 2008 Server** installed and **Hyper-V** role enabled.
- Managed host with VMM agent service installed. The agent can be installed when the managed host is added to SCVMM console using Add Host action or can be manually installed. The VMM agent installer is found in the installable for SCVMM.
- Also the managed host must have the Ops Manager Health Service Agent installed. This can be installed as part of adding the managed host in the SCOM console for discovery or can be installed manually. The Ops Manager Health Service agent installer can be found in the installable for SCOM.
- Managed Hyper-V host with Brocade FCHBA driver version 1.1.0.0 or later if Brocade FC HBAs are installed.
- Brocade **415, 425, 815, and 825** Fiber Channel HBAs.
- **16** dual-port **FC HBAs** on managed host.

Getting Started

In this chapter

- System requirements for installing management pack 3
- Minimum testing has been done to verify support of QLogic and Emulex FC HBAs. 4
- Before you import the Management Pack..... 4
- Installing SCOM agent..... 7
- Importing Brocade FCHBA Management Pack 10
- Creating a new management pack for overrides and other customizations 13
- Tuning performance threshold rules 14

System requirements for installing management pack

Table 1 provides the minimum hardware and software requirements for Brocade Management Pack for Microsoft System Center. Microsoft System Center Operations Manager and Virtual Machine Manager must be installed before installing the Brocade Management Pack.

TABLE 1 Management Pack system requirements

Component	Requirement
OS	Windows 2008 Server (64 bit) with Hyper-V Role Enabled. Windows 2008 Server Standard, Enterprise or Data Center Editions ¹ .
Processor	Recommended: 2 GHz or faster, 64 bit, Intel-VT or AMD-V ²
Memory	Minimum: 2 GB RAM; Recommended: 4+ GB RAM
Available Disk SpaceMinimum	10 GB
Drive	DVD-ROM drive
Display	Super-VGA (800 × 600) or higher-resolution monitor
Other	Keyboard and Microsoft Mouse or compatible pointing device

1. Windows 2008 Server Standard Edition may be sufficient for Hyper-V host, but if you need fail-over clustering service to run on the host, then only Enterprise or Data Center Edition is required.

2. [NX-Bit-compatible CPU](#) must be available and [Hardware Data Execution Prevention \(DEP\)](#) must be enabled.

Before you import the Management Pack

Before you import the Brocade FCHBA Management Pack, note the following limitations of the management pack.

Before you import the Brocade FCHBA Management Pack, note the following limitations:

- There is no support for agent-less monitoring.
- All hosts must be Hyper-V hosts. There is no support for VM-Ware ESX server hosts.
- The management pack can only work when VMM agent and Ops Manager health service agent are both installed on the managed Hyper-V host. The management pack is currently not intended to work with SCOM only and must have SCVMM manage the Hyper-V hosts.
- SCOM Agent should be present in the machine where the HBA is installed to collect the performance data.
- The version number of SCVMM library MPs that are referenced should match the version imported into (available on) SCOM for SCOM and VMM integration. The SCVMM MPs being referenced in the current version of Brocade FCHBA Management Pack is 2.0.3451.0.
- The state of the PORT, Aggregate Monitors (deteriorating link and over subscribed link) may not change immediately. It will take couple of minutes for the change to occur.
- Recalculation of the health state in the health explorer is not supported and will have no effect. This is because the custom monitor type does not support on-demand detection.
- PRO Tip will be raised only if the state of the Aggregate Monitor is changed to Critical.
- If two PRO tips (one each for deteriorating link for two HBA ports or any other combination) are received for the same HBA then the first PRO tip we implement and VMs will be migrated. Implementing the second PRO tip will not succeed as VMs are already migrated as part of the first PRO tip implementation.
- When all ports and HBAs under a host change to critical, the host changes to critical and is marked as 'Un-available for placement'. You must change the host state manually.
- Minimum testing has been done to verify support of QLogic and Emulex FC HBAs.

SCVMM and SCOM integration

Once SCOM and SCVMM are installed, following the steps in this section to integrate SCOM with SCVMM.

Importing Management Packs related to SCVMM

From Administrator pane in the Operations Console of the Operations Manager:

1. Right click **Management Packs** node and click **Import Management Pack** to import the Management Packs.
2. Browse and select the following management pack files, and click import:

- Microsoft.Windows.InternetInformationServices.CommonLibrary.MP
- Microsoft.Windows.InternetInformationServices.2008.MP
- Microsoft.Windows.Server.Library.mp
- Microsoft.Windows.Server.2008.Monitoring.mp
- Microsoft.Windows.Server.2008.Discovery.mp
- Microsoft.SystemCenter.VirtualMachineManager.2008.mp
- Microsoft.SystemCenter.VirtualMachineManager.Pro.2008.Library.mp
- Microsoft.SystemCenter.VirtualMachineManager.Pro.2008.HyperV.HostPerformance.mp
- Microsoft.SystemCenter.VirtualMachineManager.Pro.2008.VMRightSize.mp
- Microsoft.SystemCenter.VirtualMachineManager.Pro.2008.VMWare.HostPerformance.mp

Granting permission

The SCVMM server runs as the local system account of the machine on which it is installed. If the SCOM server and SCVMM server are installed on the same machine, you can skip this section. If they are installed on separate machines, you will need to grant access to the computer account of the SCVMM server to the Operations Manager Administrators user profile in SCOM. When SCOM is installed, it automatically grants the Local Administrators group Operations Manager (SCOM) Administrators rights. Thus, you can grant SCVMM server the same rights by adding its computer account to the Local Administrators group on the Operations Manager server (SCOM). After making changes, you must restart the SCOM SDK Service.

Follow these steps to configure SCOM server in SCVMM:

1. Open the VMM Administrator's Console and click the **Administration** button under the navigation pane to display the **Administration** view.
2. Select the **System Center** node in the navigation pane.
3. Right-click **Operations Manager Server** in the results pane and select **Modify**.
4. In the dialog box shown in [Figure 1](#) on page 6, enter the name of the root management server of your operations manager installation, and click **OK**.

2 SCVMM and SCOM integration

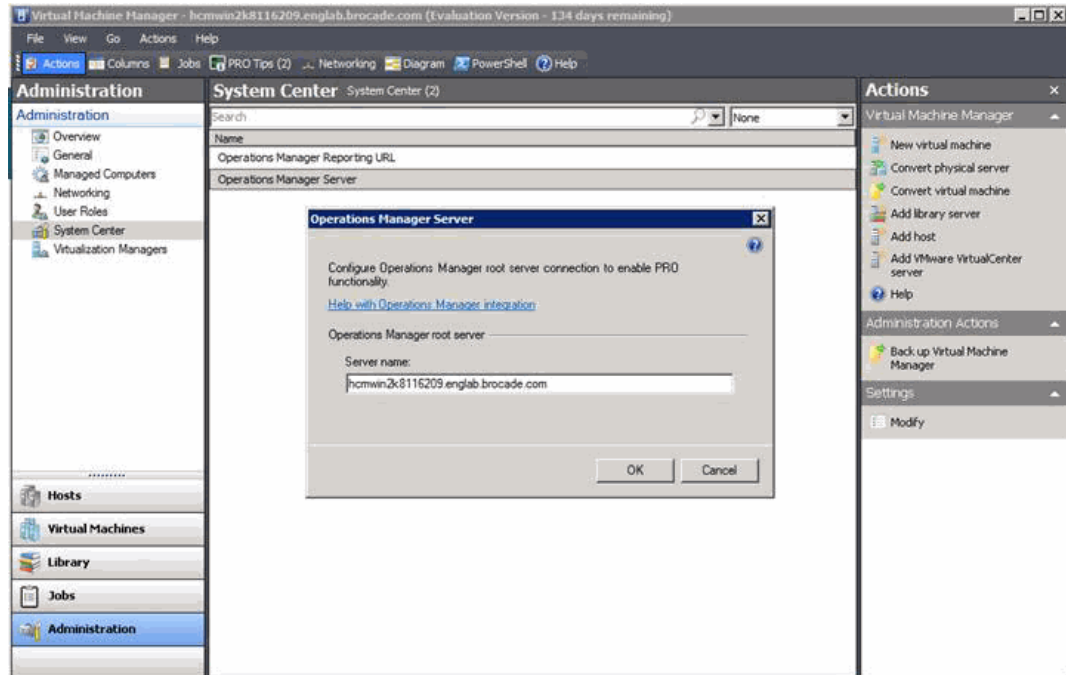


FIGURE 1 Configuring SCOM server in SCVMM

Enabling PRO-Tips

To enable PRO-Tips, use the following steps while referring to [Figure 2](#) on page 7:

1. In either the Hosts or Virtual Machines view of the VMM Administrators Console, find your cluster and open the properties.
2. On the **PRO** tab, select **Enable PRO on this host cluster**.
3. By default, the monitoring level is set to warning and critical, which means that PRO-Tips will enable all monitors and display all tips. If you would like for PRO-Tips to monitor for and display only tips with a severity level of critical, select **Critical Only**.
4. Select the option to automatically implement PRO-Tips on this host cluster check box.
5. By default, the automation level is set to **Critical Only**, which means that only PRO-Tips with a critical severity level are automatically implemented. As the oversubscribed and deteriorating link events are marked as critical, select **Critical Only** for the following options.
 - a. Enable PRO-Tip on this host cluster.
 - b. Automatically implement PRO-Tips on this host cluster.
6. Click **OK** to save your settings.

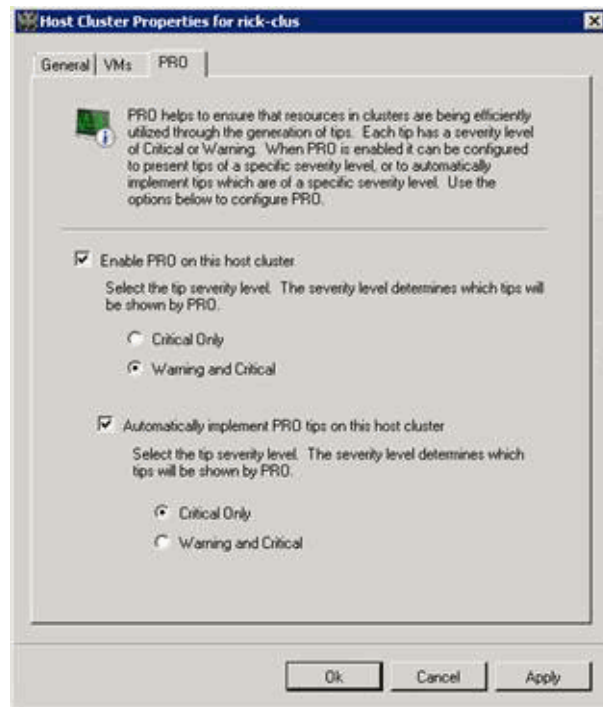


FIGURE 2 Enabling PRD in SCVMM

Installing SCOM agent

Please refer to [Using Discovery Wizard to Deploy Agents](#) for details.

To deploy the Operations Manager 2007 agent to Windows-based computers from the operations console, follow these steps.

1. Log on to the computer with an account that is a member of the operations manager administrators role for the Operations Manager 2007 Management Group.
2. In the operations console, click the **Administration** button.
3. Right-click the navigation pane and select **Discovery Wizard** (refer to [Figure 3](#) on page 8).

2 Installing SCOM agent

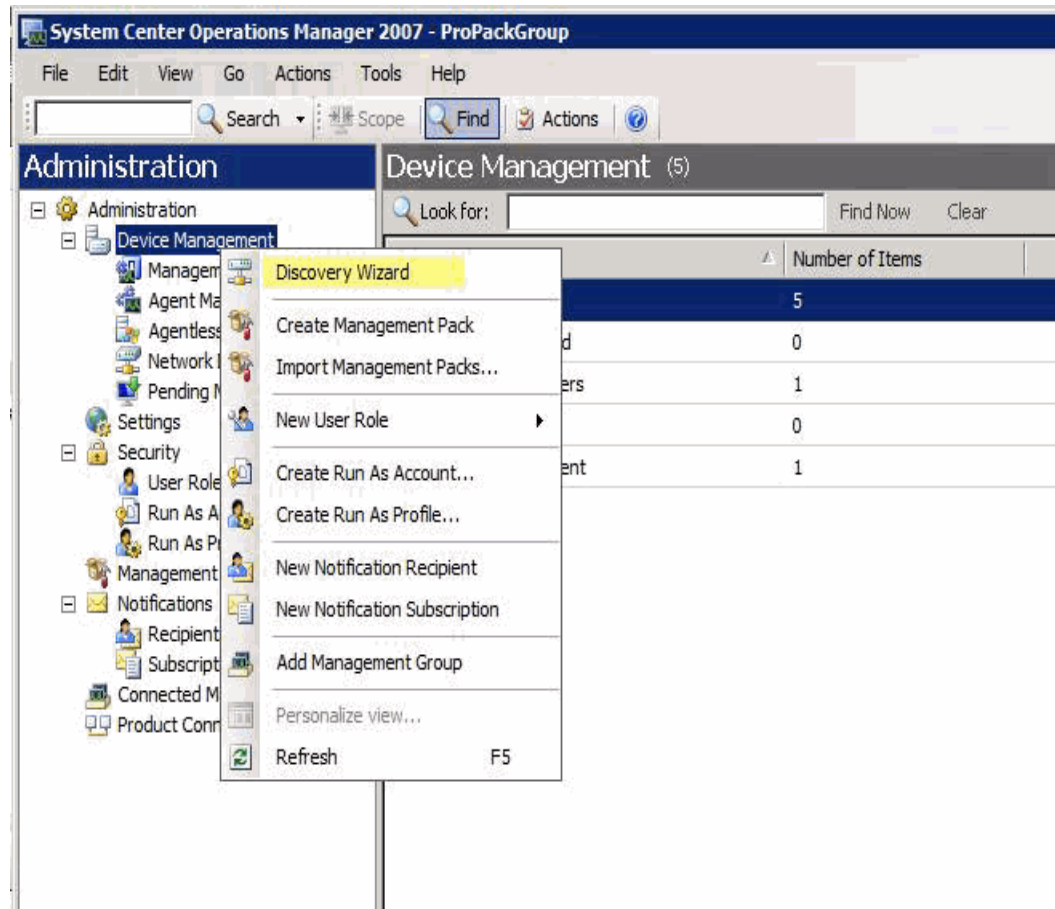


FIGURE 3 Using Discovery Wizard to add agent-managed host in SCOM

4. On the **Introduction** page, click **Next**. Note that the **Introduction** page does not appear if the Computer and Device Management Wizard have been run previously and **do not show this page again** was selected.
5. On the **Auto** or **Advanced** page, perform the following steps:
 - a. Select either **Automatic computer discovery** or **Advanced discovery**. If you select Automatic computer discovery, click **Next**, and then go to step 7. If you select **Advanced discovery**, continue with the following steps.
 - b. In the **Computer & Device Types** list, select **Servers & Clients**, **Server Only**, or **Clients Only**.
 - c. In the management server list, click the management server or gateway server to discover them. When multiple management servers are in a management group, the agents are automatically configured to use secondary management servers if their root management server is unavailable.
 - d. If you selected **Servers & Clients**, you can select the **Verify discovered computers can be contacted** check box. This may increase the success rate of agent deployment, but discovery can take longer.
 - e. Click **Next**.

6. On the **Discovery Method** page, you can locate the computers that you want to manage by either scanning or browsing **Active Directory Domain Services** or typing the computer names.
If you want to scan, do the following:
 - a. If it is not already selected, select **Scan Active Directory** and then click **Configure**.
 - b. In the **Find Computers** dialog box, type the desired criteria for discovering computers and then click **OK**.
 - c. In the **Domain** list, click the domain of the computers that you want to discover.If you want to browse active directory or type the computer names, do one of the following:
 - In the **Browse for or type-in computer names** box, click **Browse**, select the names of the computers you want to manage, and then click **OK**.
 - In the **Browse for or type-in computer names** box, type the computer names, separated by semi-colon, comma, or a new line, and then press **Enter**. You can use NetBIOS computer names or Fully Qualified Domain Names (FQDN).
7. Click **Next**, and on the **Administrator Account** page, perform the following steps:
 - a. Select **Use selected Management Server Action Account** if it is not already selected.
 - b. Select other user account, type the user name and password, and then select the domain from the list. If the user name is not a domain account, select **This is a local computer account, not a domain account**.
8. Click **Discover** to display the **Discovery Progress** page. The time it takes discovery to complete depends on many factors, such as the criteria specified and the configuration of the IT environment.
9. On the **Select Objects to Manage** page, do the following:
 - a. Select the computers you want to agent-manage.
 - b. In the **Management Mode** list, click **Agent** and then click **Next**.
10. On the 8b page, perform the following steps:
 - a. Leave the agent installation directory set to the default of %ProgramFiles%\System Center Operations Manager 2007 or type an installation path.
 - b. Leave the agent action account set to the default, **Local System**, or select **Other** and type the user name, password, and domain. The Agent Action Account is the default account the agent will use to perform actions.
 - c. Click **Finish**.
11. In the **Agent Management Task Status** dialog box, when the status for each selected computer changes from **Queued** to **Success**; the computers can be managed.
12. Click Close.

Importing Brocade FCHBA Management Pack

Use the following steps to install Management Pack in SCOM:

1. Open the SCOM - Operations Console.
2. Select the Administration tab in the left pane (refer to [Figure 4](#)).

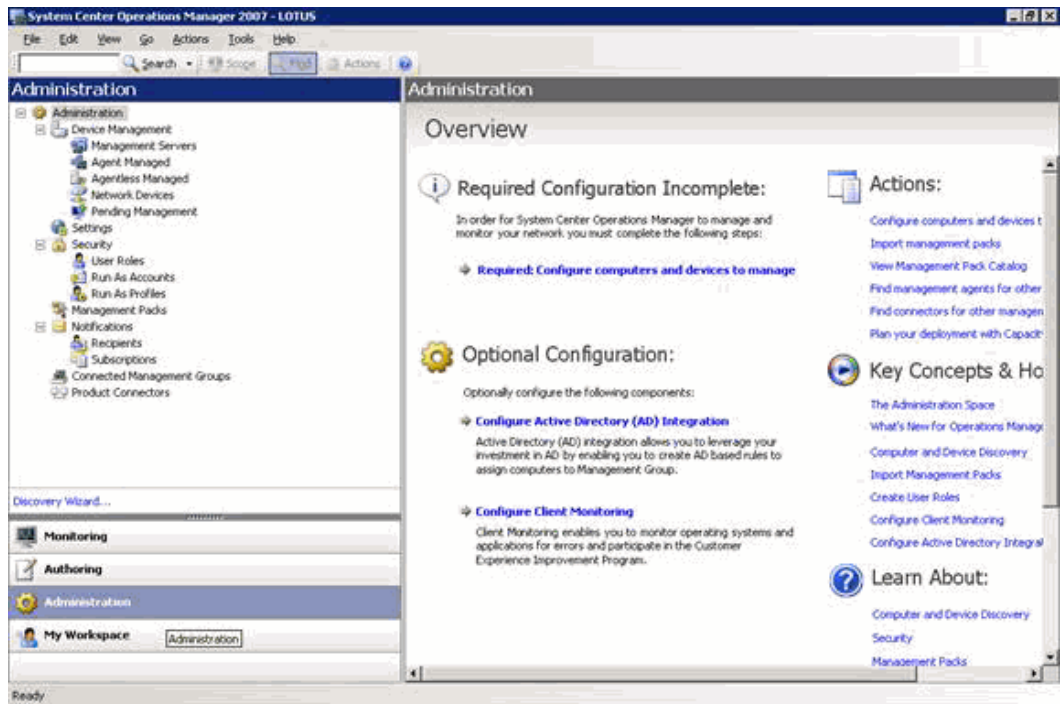


FIGURE 4 Importing Management Pack in SCOM console

3. Select the Management Packs node. Right click and select **Import Management Packs** to import the Management Packs (refer to [Figure 5](#) on page 11).

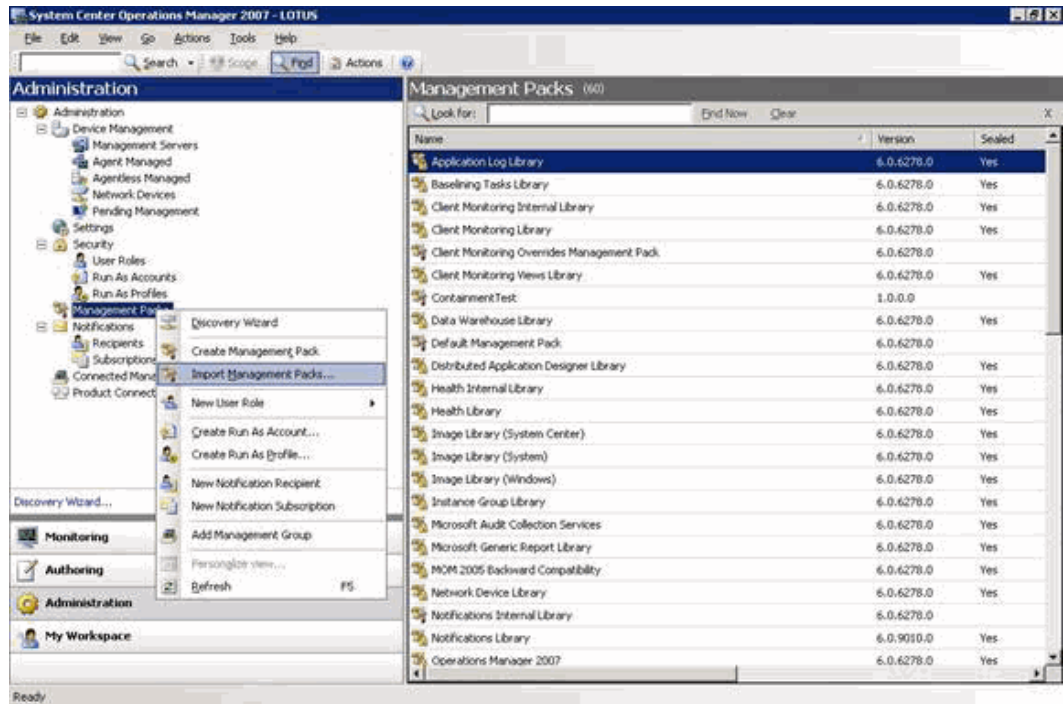


FIGURE 5 Importing Management Pack in SCOM console

4. Select the Management Pack as shown in Figure 6.

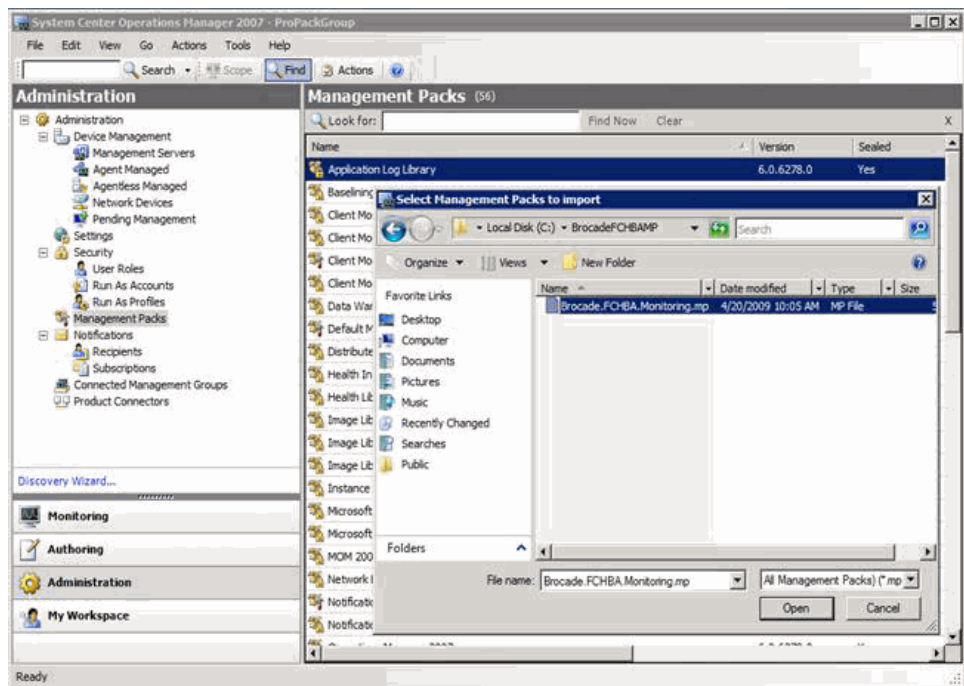


FIGURE 6 Importing Management Pack in SCOM console

2 Importing Brocade FCHBA Management Pack

5. Import the Management Pack by clicking **Import** on the screen shown in [Figure 7](#).

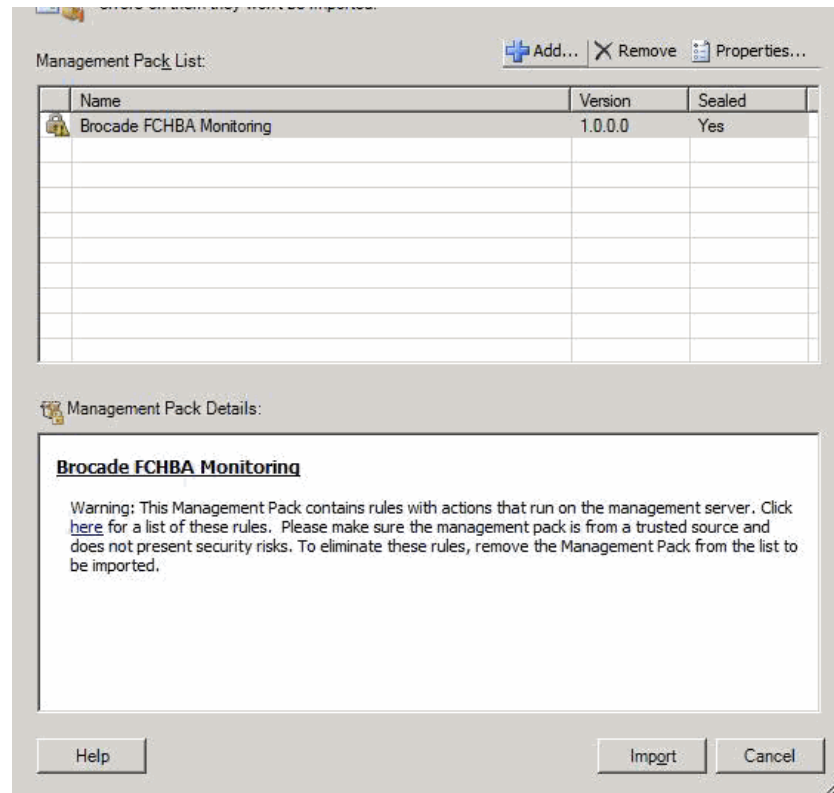


FIGURE 7 Importing Management Pack in SCOM console

6. Once the import is successful click the **Close** button.

The imported Management Pack should appear in the list of Management Packs in the Administration pane as shown in [Figure 8](#) on page 13.

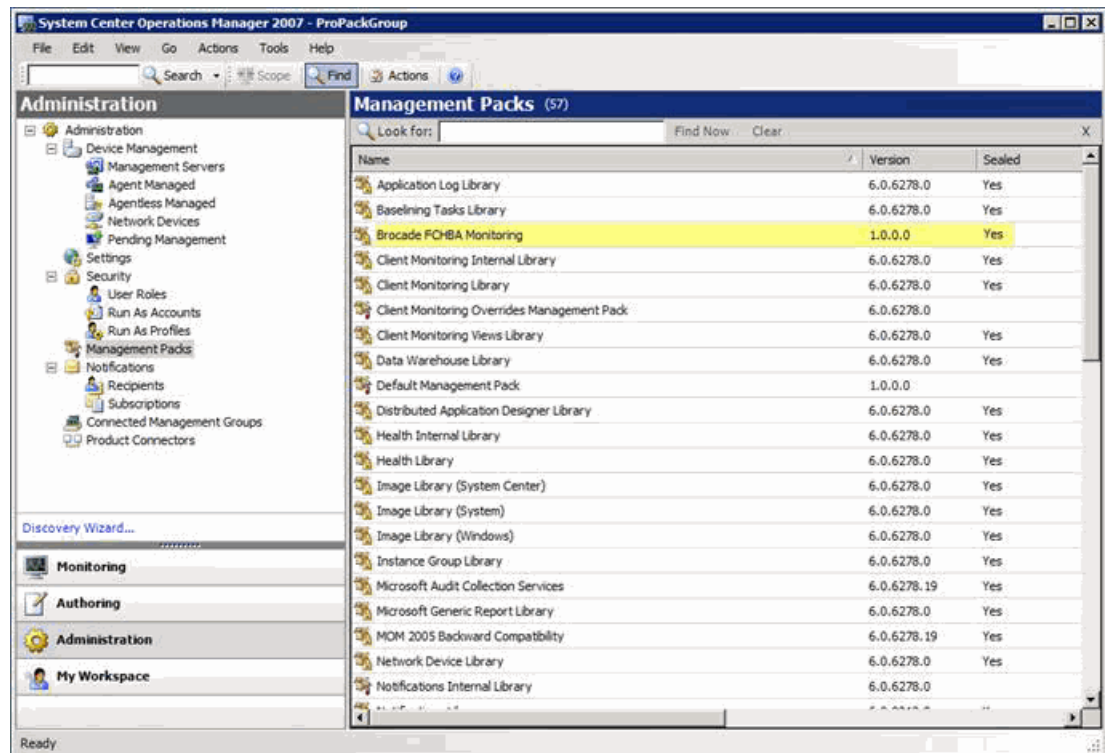


FIGURE 8 Imported Brocade FCHBA Management Pack in SCOM console

NOTE

After the Brocade FCHBA Management Pack is imported, use procedures in the following sections to finish your initial configuration.

Creating a new management pack for overrides and other customizations

Most vendor management packs are sealed so that you cannot change any of the original settings. However, you can create customizations, such as overrides or new monitoring objects, and save them to a different management pack. By default, Operations Manager 2007 saves all customizations to the default management pack. As a best practice, you should instead create a separate management pack for each sealed management pack you want to customize.

Creating a new management pack for storing overrides has the following advantages:

- It simplifies the process of exporting customizations that were created in your test and pre-production environments to your production environment. For example, instead of exporting a default management pack that contains customizations from multiple management packs, you can export just the management pack that contains customizations of a single management pack.

2 Tuning performance threshold rules

- You can delete the original management pack without first needing to delete the default management pack. A management pack that contains customizations is dependent on the original management pack. This dependency requires you to delete the management pack with customizations before you can delete the original management pack. If all of your customizations are saved to the default management pack, you must delete the default management pack before you can delete an original management pack.
- It is easier to track and update customizations to individual management packs.

Refer to [“Tuning performance threshold rules”](#) for the default Management Pack threshold values and procedures to override the default values on a per port basis or for all ports (overriding the monitor for the port type).

Tuning performance threshold rules

The following table lists performance threshold rules with default thresholds that might require additional tuning for your environment. You should evaluate these rules to determine whether the default thresholds are appropriate. If a default threshold is not appropriate, you should baseline the relevant performance counters, and then adjust the threshold by overriding them.

Counter Monitor Name	Default Interval (Seconds)	Default Threshold
DumpedFramesCustomUnitMonitor	300	50
ErrorFramesCustomUnitMonitor	300	50
InvalidCRCCustomUnitMonitor	300	1000
InvalidTxWordCustomUnitMonitor	300	1000
LinkFailureCountCustomUnitMonitor	300	25
LossOfSignalCustomUnitMonitor	300	50
LossOfSyncCountCustomUnitMonitor	300	500
NOSCountCustomUnitMonitor	300	50
PrimitiveSeqProtocolErrorCustomUnitMonitor	300	50
TxWords	300	50
RxWords	300	50

To override these default thresholds, perform the following steps:

1. Select the Authoring node in the operation console.
2. Select the **Brocade.FCHBA,Monitoring.Port** monitor and expand it,
3. Select the health entity.
4. Expand the tree and select the Performance node.
5. Right click the monitor for which you want to change the threshold

6. Select **Overrides > Override the Monitor >** for **All Objects** as shown in [Figure 9](#).

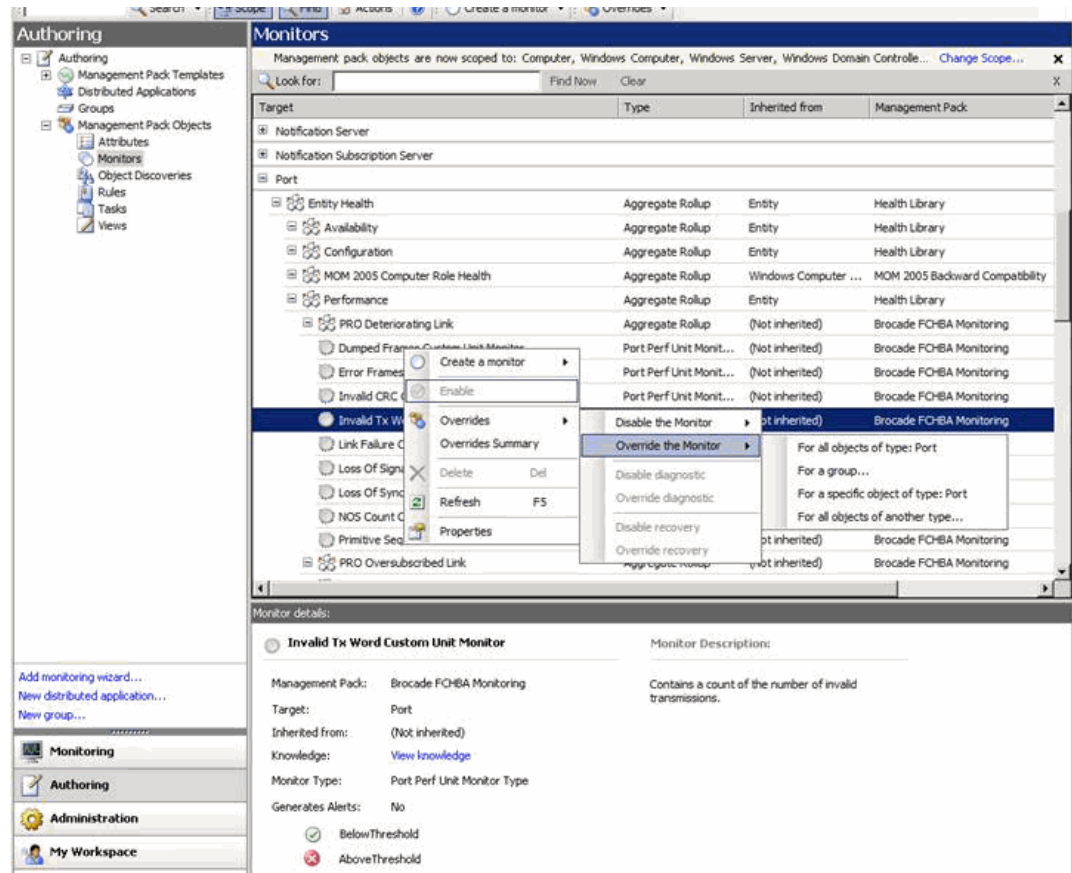


FIGURE 9 Overriding the threshold for a monitor

The **Override Properties** dialog box displays ([Figure 10](#) on page 16).

7. Select the property and provide the new value in **Override Setting** column.
8. Select **Enforced Check** box to override the default values.

2 Tuning performance threshold rules

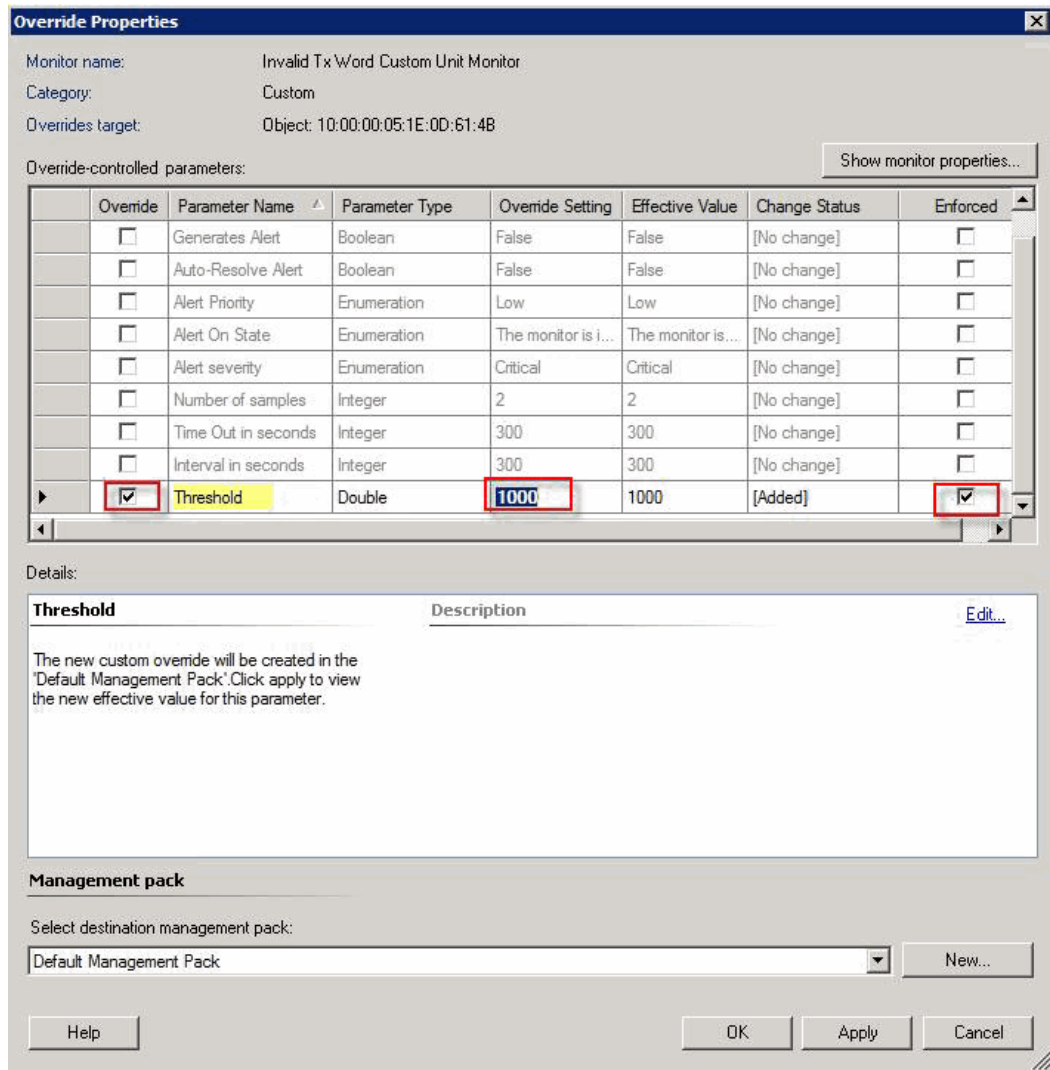


FIGURE 10 Threshold value override

Understanding Management Pack Operations

In this chapter

- [Classes](#) 17
- [Objects discovered by the management pack](#) 19
- [Oversubscribed link and deteriorated link alerts](#) 23
- [Health roll up](#) 25
- [PRO-Tip generation](#) 27
- [Setting the host unavailable for VM placement](#) 28

The Brocade FCHBA Monitoring management pack discovers Hyper-V hosts that have Brocade, QLogic, or Emulex HBA drivers installed. It also discovers the HBAs installed on the managed hosts and HBA ports.

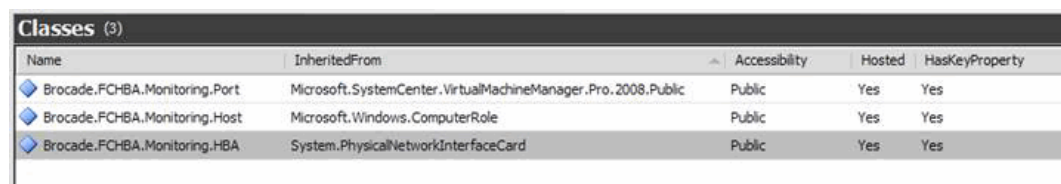
The management pack also monitors the state of the port by monitoring the port statistics counters and rolls up the port state to the HBA and then to host. It also generates PRO-Tips targeted to the port class. These display in the PRO-Tip window for the SCVMM administrator to implement or configure to auto-implement. When a PRO-Tip is implemented, one or more VMs are migrated to another host.

Classes

Three model classes are showing in the service model in [Figure 11](#) on page 17:

1. Brocade.FCHBA.Monitoring.Host - This is the Brocade driver application, which is a Microsoft.Windows.ComputerRole.
2. Brocade.FCHBA.Monitoring.HBA - This is the Host Bus Adapter class, which is a System.PhysicalNetworkInterfaceCard. This class is hosted by Brocade.FCHBA.Monitoring.Host.
3. Brocade.FCHBA.Monitoring.Port - This is the Port class, which is a Microsoft.SystemCenter.VirtualMachineManager.Pro.2008.Public. This class is contained by Brocade.FCHBA.Monitoring.HBA.

These model classes are diagrammed in [Figure 12](#) on page 18.



Name	InheritedFrom	Accessibility	Hosted	HasKeyProperty
Brocade.FCHBA.Monitoring.Port	Microsoft.SystemCenter.VirtualMachineManager.Pro.2008.Public	Public	Yes	Yes
Brocade.FCHBA.Monitoring.Host	Microsoft.Windows.ComputerRole	Public	Yes	Yes
Brocade.FCHBA.Monitoring.HBA	System.PhysicalNetworkInterfaceCard	Public	Yes	Yes

FIGURE 11 Management pack service model classes

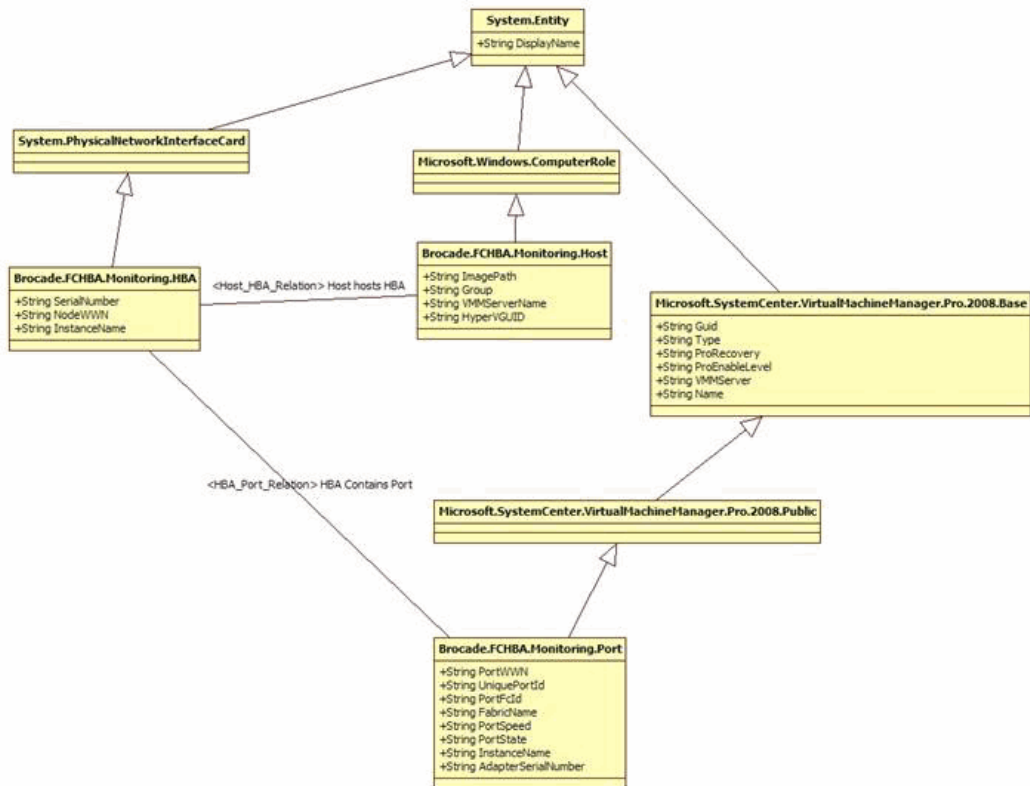


FIGURE 12 Class diagram

Brocade.FCHBA.Monitoring.Host class properties

1. ImagePath - Key property - Path of the driver - system32\DRIVERS\bfad.sys
2. Group - SCSI miniport.
3. VMMServerName - SCVMM server managing this host.
4. HyperVGUID - GUID of the hyper-v managed host.

Brocade.FCHBA.Monitoring.HBA class properties

1. SerialNumber - Key property - This is serial number of adapter.
2. NodeWWN
3. InstanceName - key property for WMI class MSFC_FCAdapterHBAAttributes.

The instance of this class is populated with WMI query to class [MSFC_FCAdapterHBAAttributes](#).

Brocade.FCHBA.Monitoring.Port class properties

1. PortWWN - Key property
2. UniquePortId - GUID for port
3. PortFcid
4. FabricName
5. PortSpeed

6. PortState
7. InstanceName - key property for WMI class [MSFC_FibrePortHBAAttributes](#).
8. AdapterSerialNumber

The instance of this class is populated with WMI query to class [MSFC_FCAdapterHBAAttributes](#).

There are 3 kinds of relationships in SCOM:

1. Hosting
2. Containment
3. Reference

Hosting is the most restrictive relationship as the hosted class instance can only exist within one and only one hosting class instance (and not multiple). Also the lifetime of the HBA class instance is same as that of the host class instance. Therefore, a HBA class instance cannot co-exist in multiple host instances. Also, because a HBA class instance has the same lifetime a host class instance, if you remove the host class instance, the hosted HBA instance goes with it.

Containment is less restrictive as the contained class instance can also exist even when containing class is removed. As an example, Windows Server Group contains Windows Server, and Windows server will still exist if Windows Group is removed.

Please refer to the [SCOM Key Concepts](#) document for details.

[Figure 13](#) shows the source and target classes of the two relationships we have defined in the Brocade HBA MP.



Relationships (2)		
Name	InheritedFrom	Source
 Brocade.FCHBA.Monitoring.Host_Hba_Rel	System.Hosting	Brocade.FCHBA.Monitoring.Host
 Brocade.FCHBA.Monitoring.HBA_PORT_Relation	System.Containment	Brocade.FCHBA.Monitoring.HBA

FIGURE 13 Management Pack service model relationships

Objects discovered by the management pack

This management Pack uses the following types of discovery processes.

- Registry based
- Script based

Registry based. This is used to find the host where the HBA is installed by searching the registry entry in the network machines. If any one of the following registry entry is available, SCOM will detect it as a host object.

- "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bfad" - for Brocade FCHBA Driver
- "SYSTEM\CurrentControlSet\Services\ql2300" - for QLogic 2300 FCHBA Driver
- "SYSTEM\CurrentControlSet\Services\Elxstor" - for Emulex FCHBA Driver

The registry entry will be created once you install the Brocade/ Qlogic/ Emulex FCHBA drivers.

3 Objects discovered by the management pack

NOTE

Very minimal testing has been done for Qlogic and Emulex FCHBAs.

Script based, This discovers the HBAs and port information through VB Script and create instances in the SCOM.

The discovered host, Brocade HBA, and ports can be viewed in the monitoring tab. Once the management pack is installed host, HBA, and port discovery may take a few minutes.

The Monitoring tab in the BrocadeMP State Views directory displays the following three items (refer to [Figure 14](#)):

- Hbas View
- Hosts View
- Ports View

Selecting BrocadeMP.HostsView will provide the host information.

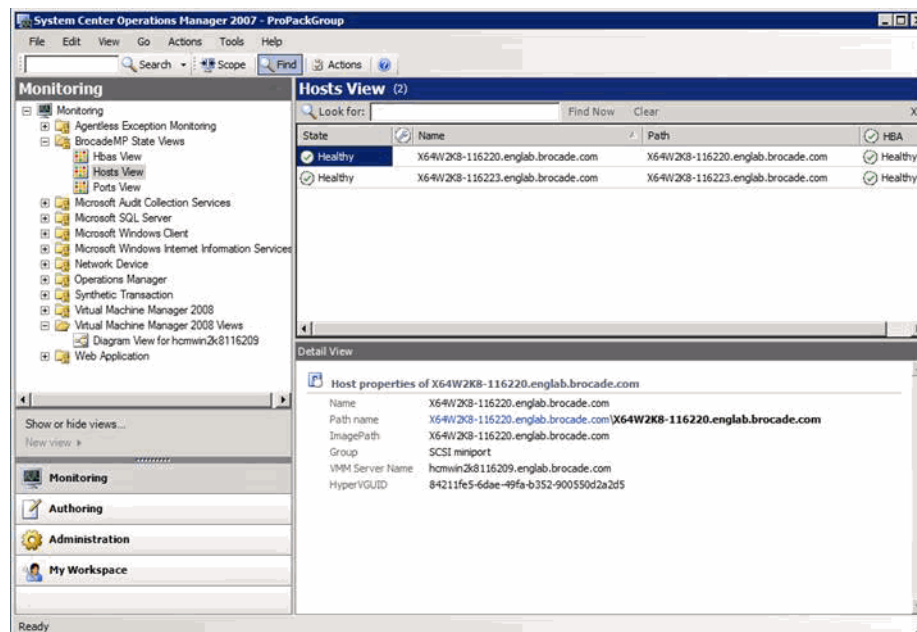


FIGURE 14 Hosts View

Select the **Hbas View** provides data on discovered HBAs as shown in [Figure 15](#) on page 21.

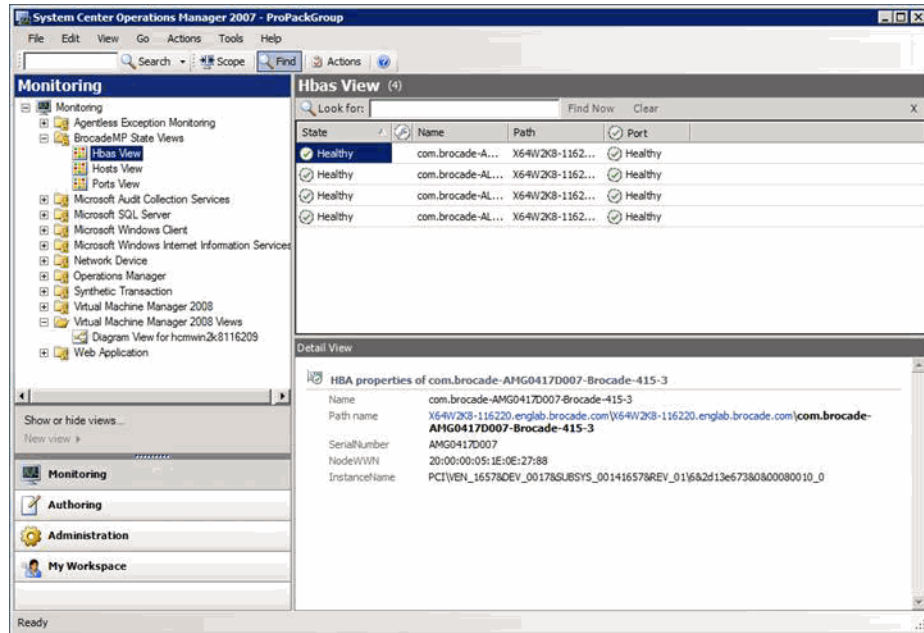


FIGURE 15 HBas View

Select the **Ports View** to display discovered HBA port information as shown in Figure 16.

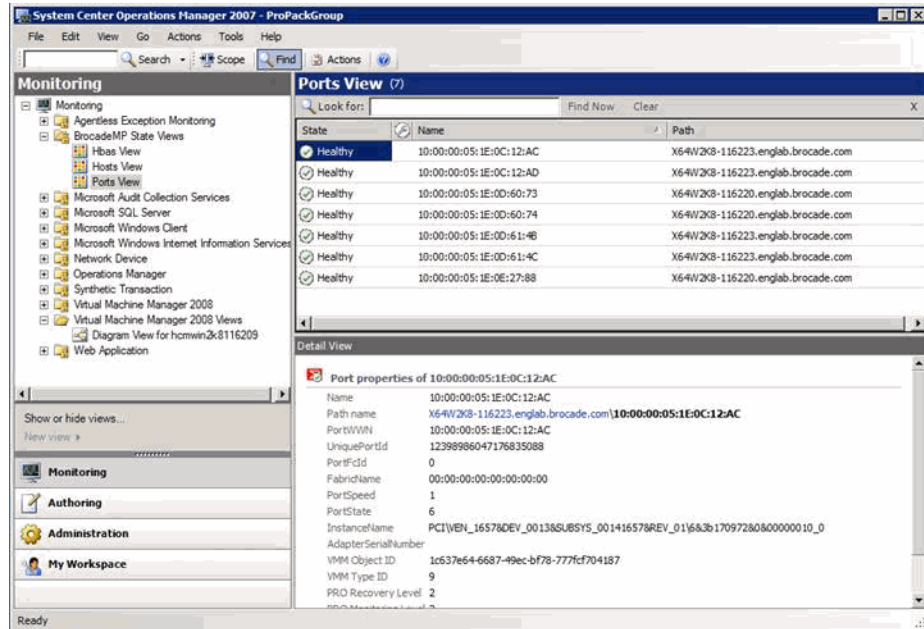


FIGURE 16 Ports View

Right-click on the host, HBA, or port and display the **Diagram View** as shown in Figure 17 on page 22.

3 Objects discovered by the management pack

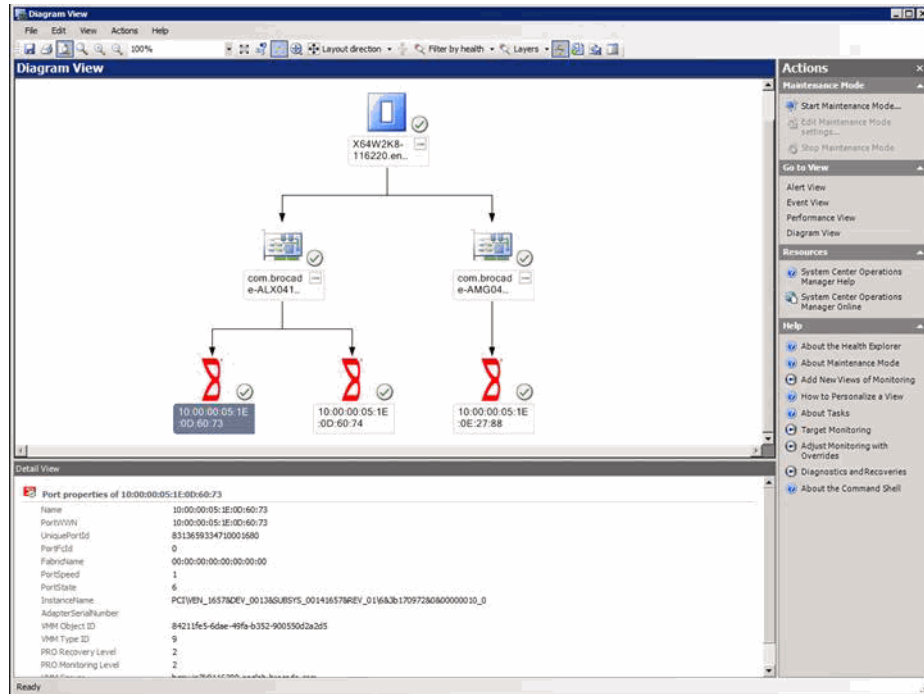


FIGURE 17 Host, HBAs and Ports seen in Host Level Diagram View

Use the following steps to view the health explorer for a host:

1. Right-click a host in the **Hosts View** and select **Open'health Explore**.

The window shown in [Figure 18](#) on page 23 will display showing the health state of the host, HBAs, and HBA ports.

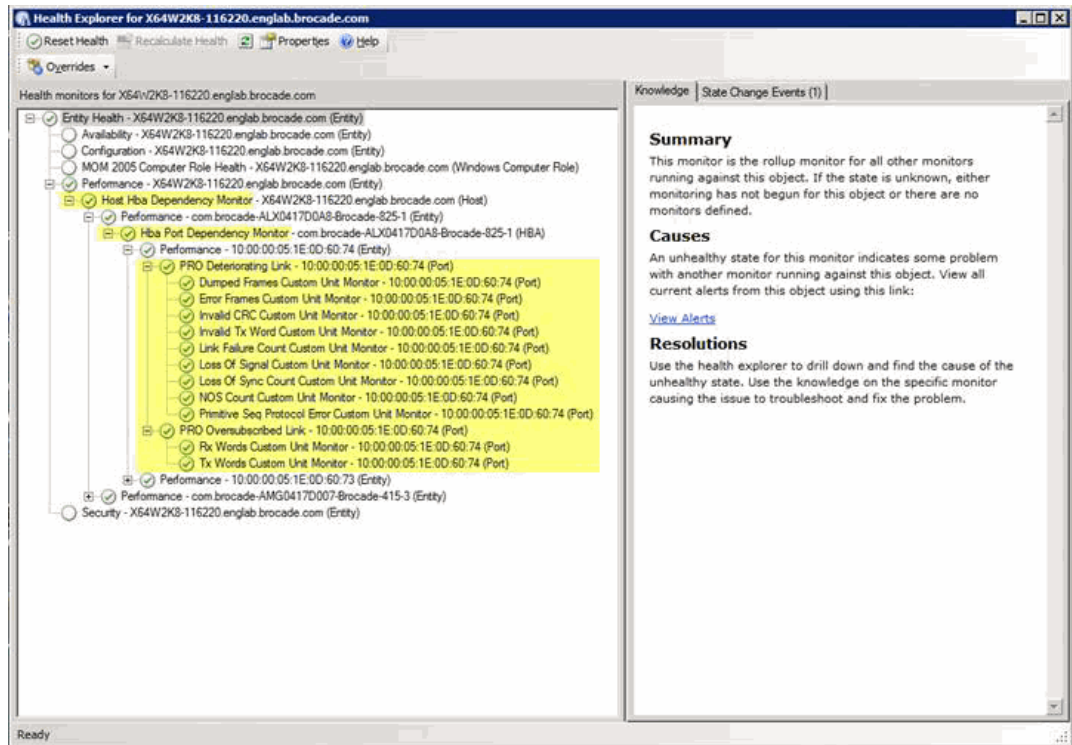


FIGURE 18 Health Explorer showing all performance monitors at Host, HBA, and port levels

Oversubscribed link and deteriorated link alerts

These events occur when values are exceeded for the deteriorated link and oversubscribed link counters.

Deteriorated link:

- Dumped Frames Count
- Error Frames Count
- Invalid CRC Count
- Invalid TxWord Count
- Link Failure Count
- Loss of Sync Count
- Loss of Signal Count
- Primitive SeqProtocolErr
- NOS Count

3 Oversubscribed link and deteriorated link alerts

Oversubscribed link:

- TXWords
- RXWords

Monitors

This section describes the monitors used to determine deteriorating links, HBA port dependency, and host dependency.

Deteriorated Link monitor (Deteriorating Link Aggregate Monitor)

Causes - Wear and tear of cables can lead to deteriorating link condition.

Resolutions - Replace the cable between HBA and switch and/or switch and storage.

This monitor is an aggregate of the following monitors. If any one of the below mentioned unit monitors cross the set threshold and goes unhealthy, then this aggregate monitor will also go unhealthy.

- Dropped Frames Count - Contains the number of frames that were lost due to a lack of host buffers available.
- Error Frames Count - Contains the number of frames that have been received in error.
- Invalid CRC Count - Contains a count of the number frames with invalid cyclic redundancy checksums.
- Invalid Tx Word Count - Contains a count of the number of invalid transmissions.
- Link Failure Count - Contains the link failure count.
- Loss of Sync Count - Contains the loss of synchronization count.
- Loss of Signal Count - Contains the loss of signal count.
- Primitive Sequence Protocol Error Count - Contains the primitive sequence protocol error count.
- NOS Count - Contains the number of nonoperational state primitive sequence (NOS) events that have occurred on the switched fabric.

Oversubscribed Link monitor. (Oversubscribed Link Aggregate Monitor)

Causes - Oversubscribed link condition indicates that either of receive or transmit traffic from the host to the storage is exceeding the set threshold.

Resolutions - Oversubscribed link conditions can be remedied by decreasing the load on the link by moving one or more VMs to bring the traffic from host to storage below the set threshold.

This monitor is an aggregate of the following monitors. If any one of the below mentioned unit monitors cross the set threshold and goes unhealthy, then this aggregate monitor will also become unhealthy.

- Tx Words Count - Contains the number of frames that were lost due to a lack of host buffers available.
- Rx Words Count - Contains the number of frames that have been received in error.

When any one of the counter value exceeded the set threshold, for the given port, that port's health state will be changed from healthy to critical. And the state can be viewed in Ports View.

HBA Port Dependency Monitor. This dependency monitor depends on the Oversubscribed link and Deteriorated link aggregate monitors. When all ports on the HBA become unhealthy then this monitor's state becomes unhealthy. The health state of this monitor rolls up to the HBA's healthy state, and the HBA also becomes unhealthy.

NOTE

Refer to [Figure 18](#) on page 23, which is the Health Explorer showing all performance monitors at host, HBA, and port levels) to see the dependency tree of monitors.

Host HBA Dependency Monitor. This is a dependency monitor that depends on the HBA Port Dependency Monitor.

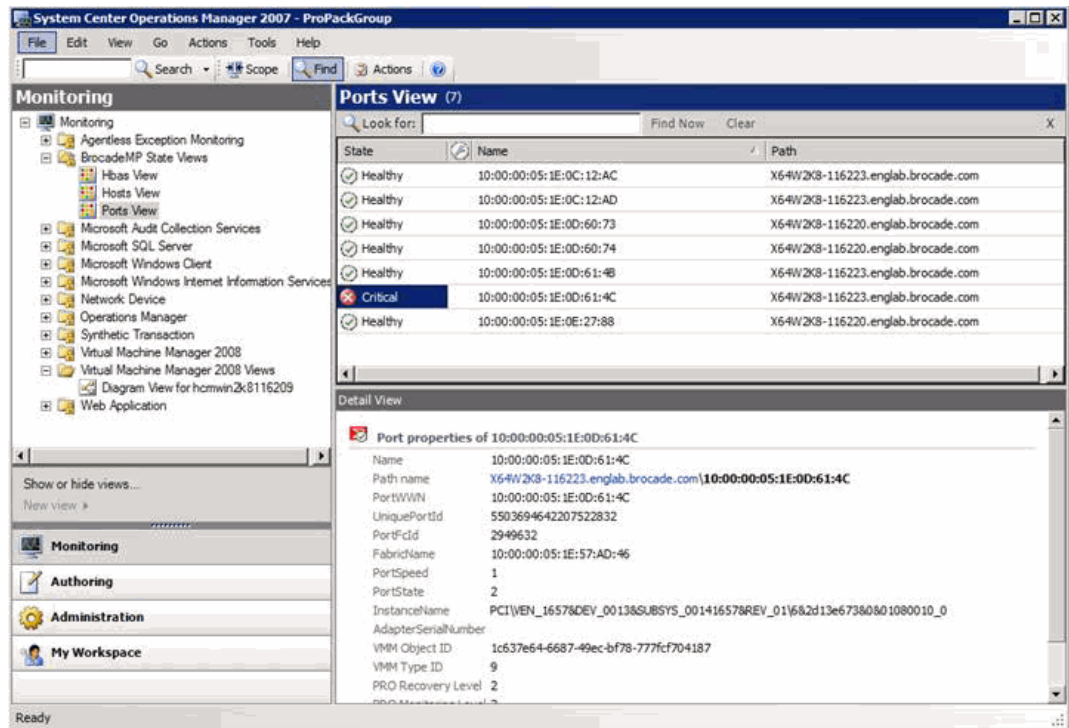


FIGURE 19 Port goes unhealthy when Rx Words monitor went unhealthy

An alert will occur in the operation manager for the event occurred.

Health roll up

When a Unit Monitor for a Port becomes unhealthy, the corresponding Aggregate Monitor (DeteriorateLinkAgMonitor or OversubscribedLinkAgMonitor) becomes unhealthy.

Then the unhealthy state rolls up to HbaPortDependencyMonitor which in turn rolls up the Unhealthy State to HostHbaDependencyMonitor. [Figure 20](#) on page 26 illustrates how when both ports on an HBA become unhealthy, the HBA also becomes unhealthy.

3 Health roll up

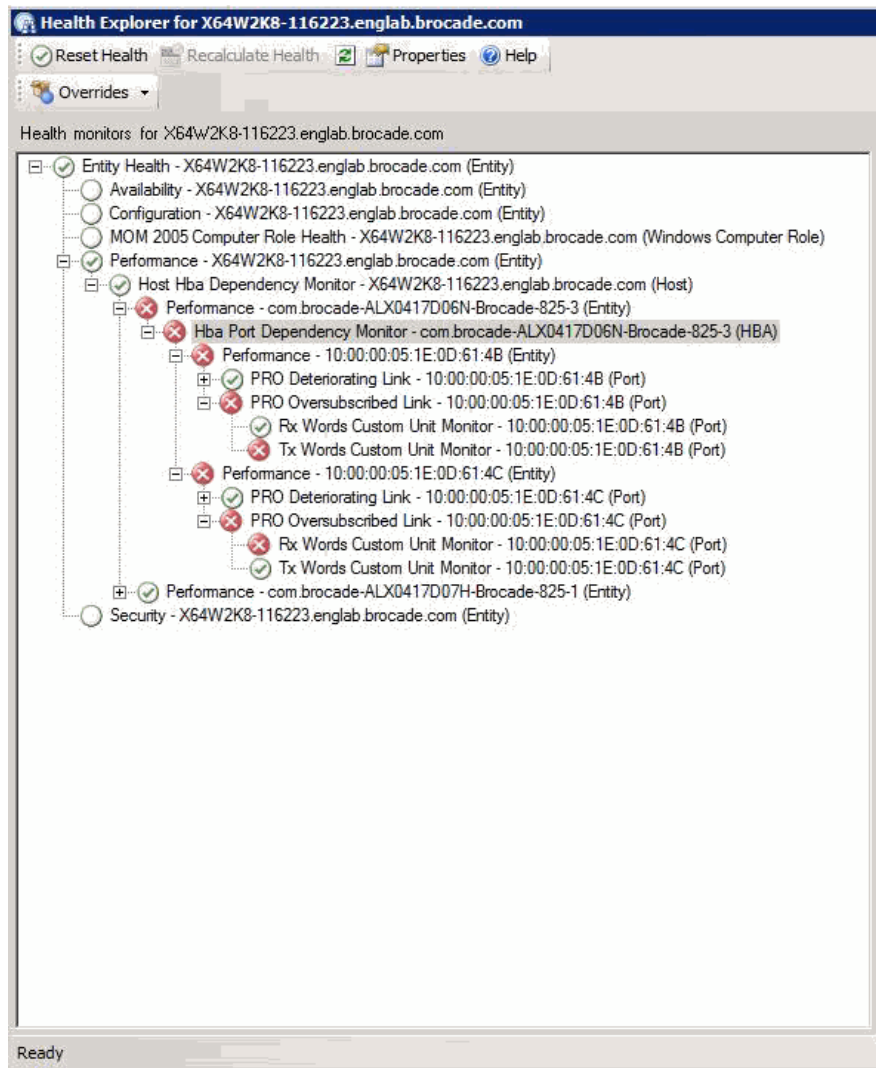


FIGURE 20 Both Ports in HBA are unhealthy, so HBA becomes unhealthy also

PRO-Tip generation

When the port state goes from Healthy to critical the Aggregate Monitor on the port object raises an Alert. This Alert will be picked as PRO-Tip and sent to the SCVMM server. [Figure 21](#) shows the Aggregate Monitor hierarchy on port object.

Target	Type	Inherited from	Management Pack	Enabled by default
Notification Server				
Notification Subscription Server				
Port				
Entity Health	Aggregate Rollup	Entity	Health Library	Yes
Availability	Aggregate Rollup	Entity	Health Library	Yes
Configuration	Aggregate Rollup	Entity	Health Library	Yes
MQM 2005 Computer Role Health	Aggregate Rollup	Windows Computer ...	MQM 2005 Backward Compatibility	Yes
Performance	Aggregate Rollup	Entity	Health Library	Yes
PRO Deteriorating Link	Aggregate Rollup	(Not inherited)	Brocade FCiBA Monitoring	Yes
Dumped Frames Custom Unit Monitor	Port Perf Unit Monitor Type	(Not inherited)	Brocade FCiBA Monitoring	No
Error Frames Custom Unit Monitor	Port Perf Unit Monitor Type	(Not inherited)	Brocade FCiBA Monitoring	No
Invalid CRC Custom Unit Monitor	Port Perf Unit Monitor Type	(Not inherited)	Brocade FCiBA Monitoring	No
Invalid Tx Word Custom Unit Monitor	Port Perf Unit Monitor Type	(Not inherited)	Brocade FCiBA Monitoring	No
Link Failure Count Custom Unit Monitor	Port Perf Unit Monitor Type	(Not inherited)	Brocade FCiBA Monitoring	No
Loss Of Signal Custom Unit Monitor	Port Perf Unit Monitor Type	(Not inherited)	Brocade FCiBA Monitoring	No
Loss Of Sync Count Custom Unit Monitor	Port Perf Unit Monitor Type	(Not inherited)	Brocade FCiBA Monitoring	No
NOS Count Custom Unit Monitor	Port Perf Unit Monitor Type	(Not inherited)	Brocade FCiBA Monitoring	No
Primitive Seq Protocol Error Custom Unit Monitor	Port Perf Unit Monitor Type	(Not inherited)	Brocade FCiBA Monitoring	No
PRO Oversubscribed Link	Aggregate Rollup	(Not inherited)	Brocade FCiBA Monitoring	Yes
Rx Words Custom Unit Monitor	Port Perf Unit Monitor Type	(Not inherited)	Brocade FCiBA Monitoring	No
Tx Words Custom Unit Monitor	Port Perf Unit Monitor Type	(Not inherited)	Brocade FCiBA Monitoring	No

FIGURE 21 Aggregate Monitor alerts get sent as PRO Tips

When PRO-Tip is received in the SCVMM server, the PRO-Tip window will open. When you click the implement button, event ID 101 will be created. The rule in SCOM will pick that event and trigger the PowerShell script written in the recovery of the monitor, and the host will be migrated. [Figure 22](#) on page 28 shows an oversubscribed link alert appearing in the **PRO-Tip** window.

3 Setting the host unavailable for VM placement

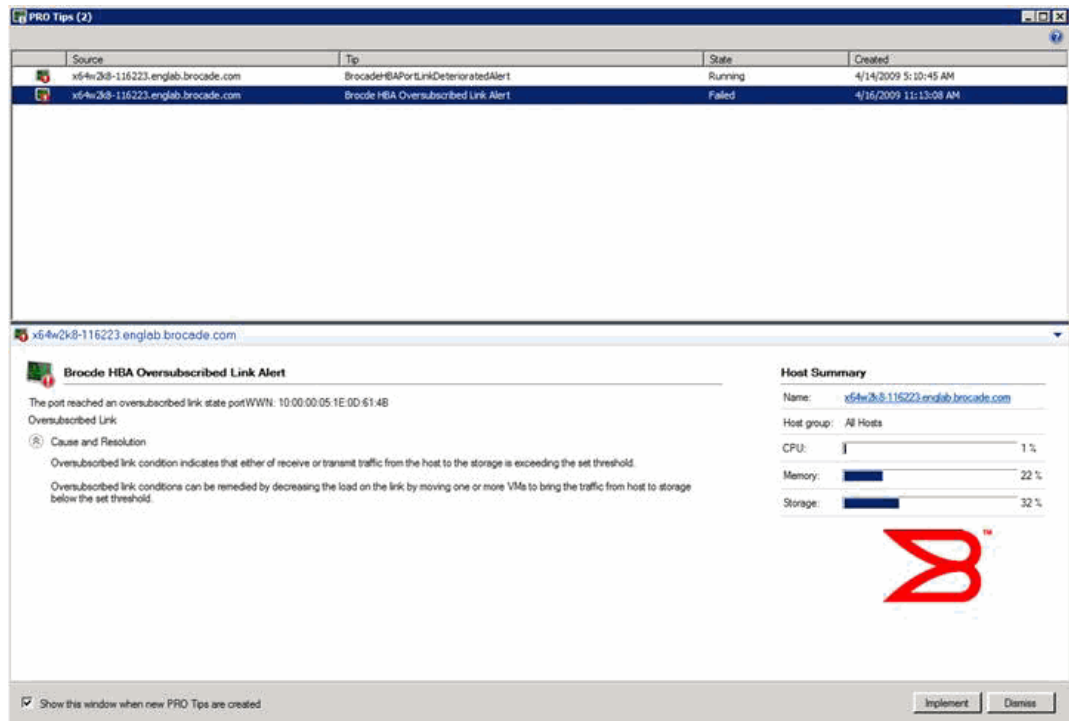


FIGURE 22 PRO Tip Window showing Oversubscribed Link Alert

Setting the host unavailable for VM placement

When all ports of one HBA are critical, health of the HBA will be set as critical. When all HBAs are critical for a host, the host object will be set as critical. Once the host object is critical, an alert will be generated, and recovery will occur and event ID 102 will write to the Windows Application event log. The corresponding Rule reads the event log and executes a power shell script to mark the host as 'Unavailable for Placement' in SCVMM." [Figure 23](#) on page 29 shows the **Host Properties** screen where **The host available for placement** is not selected.

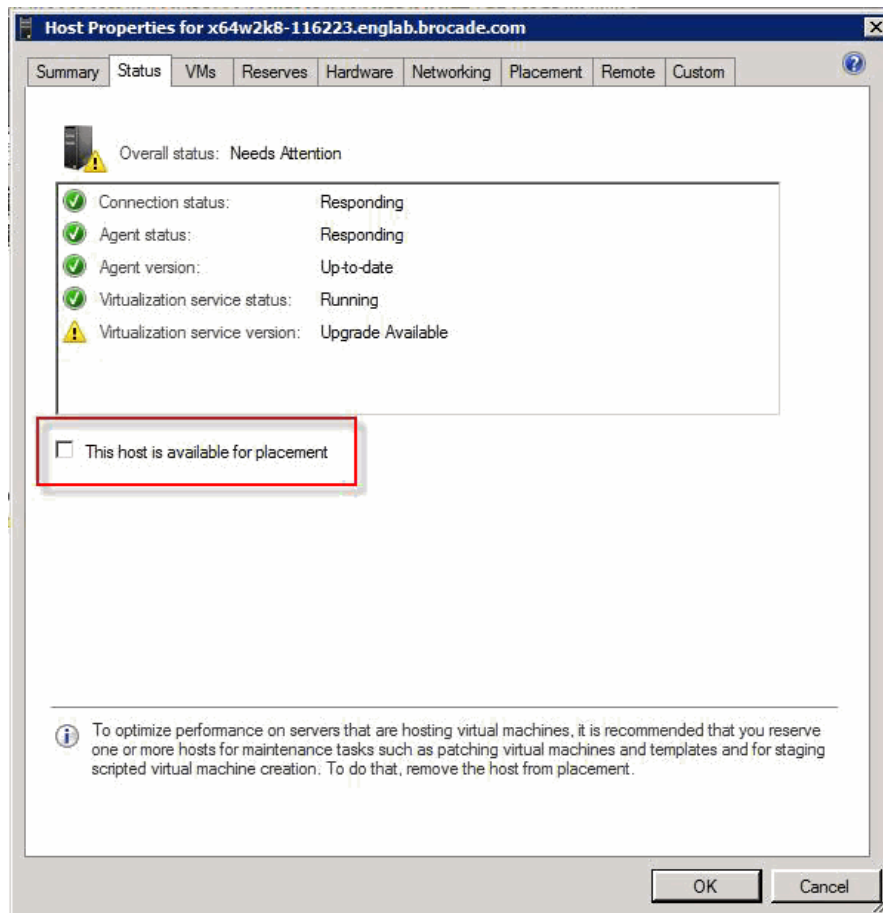


FIGURE 23 Host marked as unavailable for VM placement

3 Setting the host unavailable for VM placement

Troubleshooting

Troubleshooting PRO for Brocade HBA Management Pack

If generation or implementation of PRO is failing, check the following:

1. Verify that latest MP is imported to SCOM.
2. Verify the required registry entries are available for Host discovery.
3. If discovery of application, HBA, or port, relations is taking a long time then make sure that 'OpsMgr Health Service' is started and running on the HyperV Host machines. If they are started, try restarting this service.
4. Discovery can also be forced by executing powershell commands within VMM powershell.
 - a. `Get-VMMServer <Your VMM Server Name>`
 - b. `Set-VMMServer -OpsMgrServer <Your OpsMgr Server Name>`
5. If all PORT properties are not populated by SCVMM, try running `set-vmmserver -OpsMgrServer <SCOM Server Name>`.
6. Verify in SCVMM that VMs are available on the Host and in 'Running' status.
7. Verify that VMs are not excluded from PRO (see [Figure 24](#) on page 32).

4 Troubleshooting PRO for Brocade HBA Management Pack

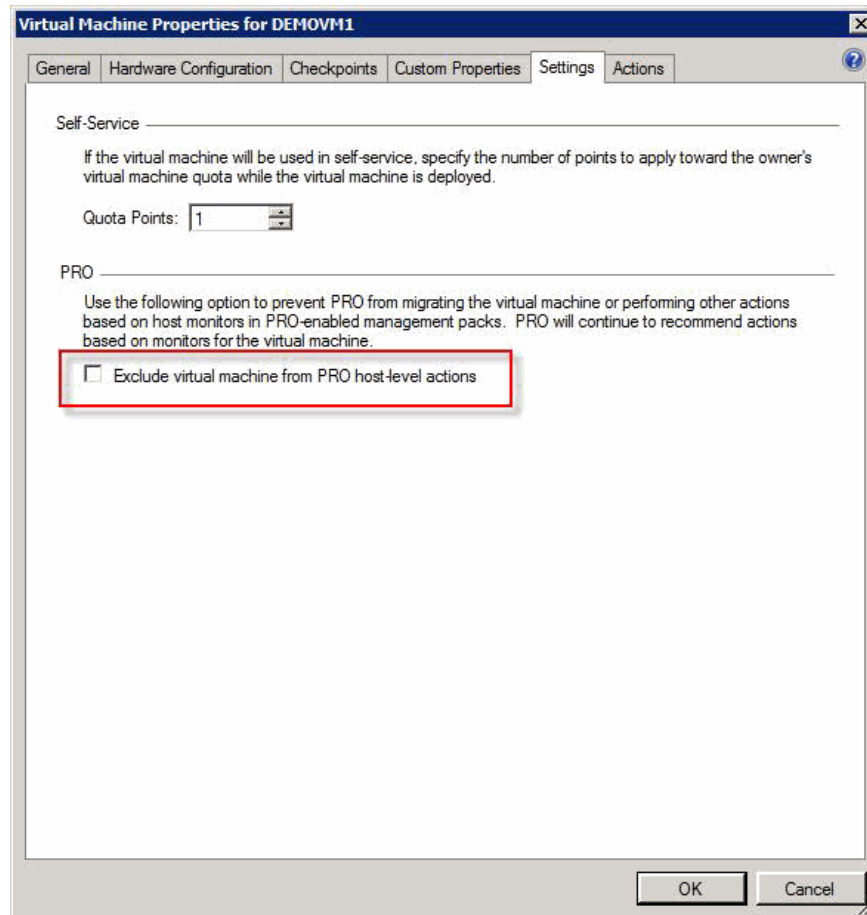


FIGURE 24 VM excluded from PRO setting

8. For execution flow specific errors, refer events with IDs of 70 or 80 in the Windows Event log (Application log).

Frequently Asked Questions

Following are frequently asked questions and answers for the Brocade HBA Management Pack.

1. Can I run SCVMM server in one PC and the SCOM in another PC?

Answer: Yes you can run SCOM and SCVMM in separate machines. But you have to grant access to SCVMM server in SCOM installed Machine by adding the SCVMM machine in a user role with administrator privilege.

2. What are the methods to push SCOM agent in remote machine?

Answer: There are two methods to push the SCOM agent to remote machine.

Manual Installation. Installing the agent setup in the remote machine.

Pushing Agent. Pushing the agent from the SCOM server to a remote machine by enabling the remote machine privilege.

3. If I already import the management pack it is it possible to import again?

Answer: If both Management Packs are different version then there is will be no problem. There will be a conflict if Management Packs with the same version are imported.

4. After importing the management pack, the SCOM doesn't discover HBA what can I do?

Answer: Restart the Operation Manager Health service on HOST and SCOM machines.

5. Do I need to install Brocade driver for discovering the HBAs through Brocade HBA Management Pack?

Answer: Yes.

5 Frequently Asked Questions

Scripts

The following table describes scripts provided with the Brocade FCHBA Management Pack.

Script	Purpose	Parameters	Default Frequency
Port Performance Script	This script provides monitoring of HBA ports statistics counters.	IntervalSeconds	300 secs (5 mins)
Discover HBAs Script	This script discovers the HBAs on a host.	ImagePath NetworkName	14400 secs (4 hrs)
Discover Ports Script	This script discovers the ports on the HBAs.	ImagePath SerialNumber DisplayName PrincipalName HyperVGUID	14400 secs (4 hrs)
VM Migration Oversubscribed Link Recovery Task	This script provides the recovery task for a PRO-Tip of oversubscribed link alert and initiates a migration of one VM at a time on the host.	<HostName>*<VMMServer>*<EventOriginId>*<PortWWN>* ONE	NA
Set Host Unavailable Recovery Task	This script provides the recovery task that marks the host as unavailable for further VM placement if all ports on that host become unhealthy	<PrincipalName>:<VMMServer>	NA
VM Migration Deteriorating Link Recovery Task	This script provides the recovery task for a PRO-Tip of deteriorated link alert and initiates the migration of all VMs on the host.	<HostName>*<VMMServer>*<EventOriginId>*<PortWWN>* ALL	NA

A Port performance script

Script	Purpose	Parameters	Default Frequency
VM Migration power shell Script	This script migrates the VMs when a PRO tip is implemented. It selectively migrates only those VMs that are on the affected port that went unhealthy. for an oversubscribed link, one VM gets migrated while for a deteriorating link, all VMs on the affected port are migrated.	EventDescription	NA
Set Host Unavailable power shell Script	This script marks the host as unavailable from further VM placement.	EventDescription	NA

Port performance script

Name: PortPerfScript.vbs

Performance Counters:

The following Port performance counters are polled by this script every IntervalSeconds:

1. TxWords
2. RxWords
3. NOSCCount
4. ErrorFrames
5. DumpedFrames
6. LinkFailureCount
7. LossOfSyncCount
8. LossOfSignalCount
9. PrimitiveSeqProtocolErrCount
10. InvalidTxWordCount
11. InvalidCRCCCount

Refer to [MSFC_FibrePortHBASStatistics](#) for details.

How the script works:

This script polls the performance counters for HBA ports every interval seconds (300 secs by default) and computes the delta value between the counter values. It then averages the number of samples.

For TxWords and RxWords counters, the rate of change is calculated based on the port speed using the following formula.

Value = (Counter / IntervalSeconds) / PortSpeed) x 100.

Where, PortSpeed is first converted to words/second with following calculation.

PortSpeed = PortSpeed * 1024*1024*1024/32

Assuming, Port Speed is in Gbps and WORD length is 32 bits.

The delta is calculated for the above values of counter and then its averaged over NumSamples.

Effective values for parameters are as follows:

- NumSamples is 2
- Threshold for each counter is defined under [“Tuning performance threshold rules”](#) on page 14.
- IntervalSeconds is 300 secs.

Discover HBAs script

This script discovers all HBAs on the host.

How the script works:

The following WMI query is executed to get the HBA attributes

```
select * From MSFC_FCAdapterHBAAttributes.
```

Discover ports script

This script discovers the Ports on all HBAs on the host.

How the script works:

The following WMI query is executed to get the port attributes.

```
select * from MSFC_FibrePortHBAAttributes.
```

VM migration oversubscribed link recovery task

This script initiates VM Migration of one VM at a time on the host as a consequence of oversubscribed link.

How the script works:

It writes an event with event ID 101 to the Windows Application event log. This event is then read by a corresponding VM Migration Rule, which executes a power shell script to cause the actual VM Migration. For an Oversubscribed link, only one VM is moved to a destination host at a time.

Timeout: 300 secs.

Set host unavailable recovery task

This script marks the host as unavailable for further VM placement.

How the script works:

Once all ports on the host become unhealthy, then the host is made unavailable for further VM placement. This recovery task initiates the marking of host as unavailable for placement by writing an event with event ID 102 in the Windows Application event log. The corresponding Set Host Unavailable Rule reads the event log once an event with ID 102 is located, it then executes a power shell script that marks the host as unavailable for placement.

VM migration deteriorated link recovery task

This script initiates VM Migration of all VMs on the host as a consequence of deteriorating link alert.

How the script works:

Writes an event with event ID 101 to the Windows Application event log. This event is then read by a corresponding VM Migration Rule which then executes a power shell script to start the actual VM Migration. For a deteriorating link, all VMs on the host are moved to a destination host.

Timeout: 300 secs.

VM migration power shell script

This script migrates the VMs when a PRO tip is implemented. It selectively migrates only those VMs that are on the affected port that went unhealthy. In case of oversubscribed link, one VM gets migrated whereas in case of deteriorating link, all VMs on the affected port are migrated.

How the script works:

Reads the event ID 101 logged by event source **BrocadeMP**. If such an event is found then it gets event description and migrates ONE or ALL VMs on the affected port.

Timeout: 300 secs.

Set host unavailable power shell script

This script marks the host as unavailable from further VM placement.

How the script works:

Reads the event ID 102 logged by event source **BrocadeMP**. If such an event is found then it gets event description and marks the identified target host as unavailable for VM placement.

Timeout: 300 secs.