Brocade FCHBA Management PRO Pack Guide for Operations Manager 2012 and Virtual Machine Manager 2012

Published: 12/*10/2012*

Table of Contents

Table of Figures

Table 1: Revision History Table

Revision	Date	Author(s)	Description of changes
0.01	06/07/12	Watsh Rajneesh	Updated the document for TR000385681 (info about FC port speed).
0.02	12/10/12	Dhanuskodi & Watsh	Updated documentation for SC 2012 support.

1 Introduction

Brocade FCHBA Monitoring Management Pack (MP) is based on the Microsoft System Center Operations Manager (SCOM) Management pack that models Fibre Channel Host Bus Adapters (HBA) and monitors the health of Brocade FC HBAs.

The 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 or device and determine the health of the application or device. This information is output as an XML document using a pre-defined XML scheme understood by Operations Manager.

System Center Operations Manager (**SCOM**) Management Pack includes two types of models:

1. **Service Model** – Defines the classes (which are entities of our managed device or application) and the relationships between the classes.
2. **Health Model** – Defines the discoveries for the entities and their relationships. This also provides monitors, specifies roll-up criteria, and generates alerts.

The MP also includes a custom monitor type definition and the presentation state views definitions.

MP deployment requires that SCOM agent (**Health Service**) and SCVMM agent be installed on each managed Windows Hyper-v server. SCOM agent installation can be done from within the Management Server and SCVMM agent installation can be done from within the VMM Server. Please refer to the SCOM 2012 Deployment Guide and SCVMM 2012 Deployment Guide for more details.

The MP is imported into SCOM. It is distributed into managed Hyper-V hosts containing one or more FC HBAs. Once the host is managed the Microsoft SCOM Health Service will be deployed by SCOM automatically or you can manually install it. The Brocade MP will be downloaded into these managed hosts and executed on the SCOM Health Service. The VMM agent service must be installed on the managed host. Install the agent when the managed host is added to SCVMM administrator console using an Add Host entry or manually install it.

Brocade HBA drivers must be installed as prerequisite in managed hosts with Brocade HBAs installed. Management Pack relies on WMI calls through WMI service, and the Brocade driver acts as a WMI Provider servicing the WMI calls issued by the Management Pack. Install the driver with Administrative privilege. No additional security privileges are needed other than the OpsMgr Health Service mandated by SCOM and SCVMM.

The **sealed** version of Management Pack is a file named **Brocade.FCHBA.Monitoring.2012.mp**, which is compatible with System Center 2012 and a file named Brocade.FCHBA.Monitoring.2007.mp, which is compatible with SCOM 2007 and SCVMM 2008

2 Obtaining the Latest Management Pack and Documentation

Find the Brocade FCHBA MP on http://www.brocade.com.

3 Supported Configurations

Following are requirements for the Brocade FCHBA Management Pack for Operations Manager:

- Each managed host be a **Windows 2008 R2 Server** host with **Hyper-V** role enabled.
- The managed host must have Virtual Machine Manager (**VMM) agent service** installed. This agent can be installed when the managed host is added to SCVMM console using an *Add Host* action or can be installed manually. The VMM agent is in the SCVMM installable.
- The managed host must have the **Ops Manager Health Service Agent** installed. This can be installed when adding the managed host in the SCOM console for discovery or can be installed manually. The Ops Manager Health Service agent installer is in the SCOM installable.
- **Brocade FC HBA driver version 1.1.0.0** or later must be installed if a Brocade FC HBA is installed on the managed Hyper-V host.
- Brocade Fiber Channel HBA series **415, 425, 815, 825, 1860 (in FC HBA mode only)** are supported. The supported FC port speeds are 1 Gbps, 2 Gbps and 4 Gbps only. For any other FC port speeds, the PRO features of MP will not work, but HBA and port discoveries still function.

- The MP supports up to **16** dual port **FC HBAs** on a managed host.

4 Getting Started

4.1 System Requirements: Installing Management Pack

Below are the minimum hardware and software requirements for Brocade FCHBA Management Pack (MP) for Microsoft System Center. Refer to the "Supported Configurations" section for additional information.

Component	Requirement
OS	Windows 2008 R2 Server (64 bit) with Hyper-V Role enabled. Windows 2008 R2 Server Standard, Enterprise or Data Center Editions. (*)
Processor	Recommended: 2 GHz or faster, 64 bit, Intel-VT or AMD-V (**)
Memory	Minimum: 2 GB RAM; Recommended: 4+ GB RAM
Available Disk Space	Minimum: 10 GB
Drive	DVD-ROM drive
Display	Super-VGA (800 × 600) or higher-resolution monitor
Other	Keyboard and Microsoft mouse or compatible pointing device

Note:
* Windows 2008 R2 Server Standard Edition may be sufficient for a Hyper-V host, but if you need fail-over clustering service to run on the host then only Enterprise or Data Center Edition are required.

** NX bit-compatible CPU must be available and Hardware Data Execution Prevention (DEP) must be enabled.

4.2 Before You Import the Management Pack

Before you import the Brocade FCHBA MP, 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 MP can only work when VMM agent and Ops Manager health service agent are both installed on the managed Hyper-V host. The MP is currently not intended to work with SCOM only and must have SCVMM to manage the Hyper-V hosts.
- SCOM Agent should be present in the host where the HBA is installed to collect the performance data.
- The version number of SCVMM library MPs that are referenced should match with those imported into (available on) SCOM for SCOM and VMM integration. The SCVMM MPs being referenced in the Brocade FCHBA MP for SC2012 are **3.0.6005.0**. The SCVMM MPs being referenced in the Brocade FCHBA MP for SC 2012 are **2.0.3451.0**.
- The state of the port and Aggregate Monitors (deteriorating link and oversubscribed link) may not change for a couple minutes.
- **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 on two-port HBAs or any other combination) are received for the same HBA, then the first PRO tip implemented and VMs will be migrated. When we implement the second PRO tip, then the implementation 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 then change the host state manually.
- Minimal testing has been done to verify support of QLogic and Emulex FC HBAs.

4.2.1 SCVMM and SCOM integration

Once SCOM and SCVMM are installed, use the following steps need to be followed to integrate SCOM with SCVMM.

1. Importing Management Packs related to SCVMM

1. From the Administrator pane in the Operations Console of the Operations Manager, right click the “Management Packs” node and click Import Management Pack to import the Management Packs.
2. **For SCOM 2007/SCVMM 2008**, import the following SCVMM related management packs into SCOM:
   - 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
3. **For SC 2012**, import the following SCVMM related management packs into SCOM:
   - Microsoft.SystemCenter.VirtualMachineManager.2012.Monitoring.mp
   - Microsoft.SystemCenter.VirtualMachineManager.PRO.2012.Diagnostics.mp
   - Microsoft.SystemCenter.VirtualMachineManager.2012.Discovery.mp
   - Microsoft.SystemCenter.VirtualMachineManager.2012.DiagramViews.mp
   - Microsoft.SystemCenter.VirtualMachineManager.2012.Reports.mp
   - Microsoft.SystemCenter.VirtualMachineManager.Library.mp
   - Microsoft.SystemCenter.VirtualMachineManager.Override.mp
   - Microsoft.SystemCenter.VirtualMachineManager.Pro.2008.Library.mp
   - Microsoft.SystemCenter.VirtualMachineManager.PRO.Library.mp
   - Microsoft.SystemCenter.VirtualMachineManager.PRO.V2.HyperV.HostPerformance.mp
   - Microsoft.SystemCenter.VirtualMachineManager.PRO.V2.Library.mp

2. Granting Permission

The SCVMM server runs as the Local System account of the host on which it is installed. If the SCOM server and SCVMM server are installed on the same host, you can skip this section. If they are installed on separate hosts, 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) Administrator 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 you make that change, you must restart the SCOM SDK Service.

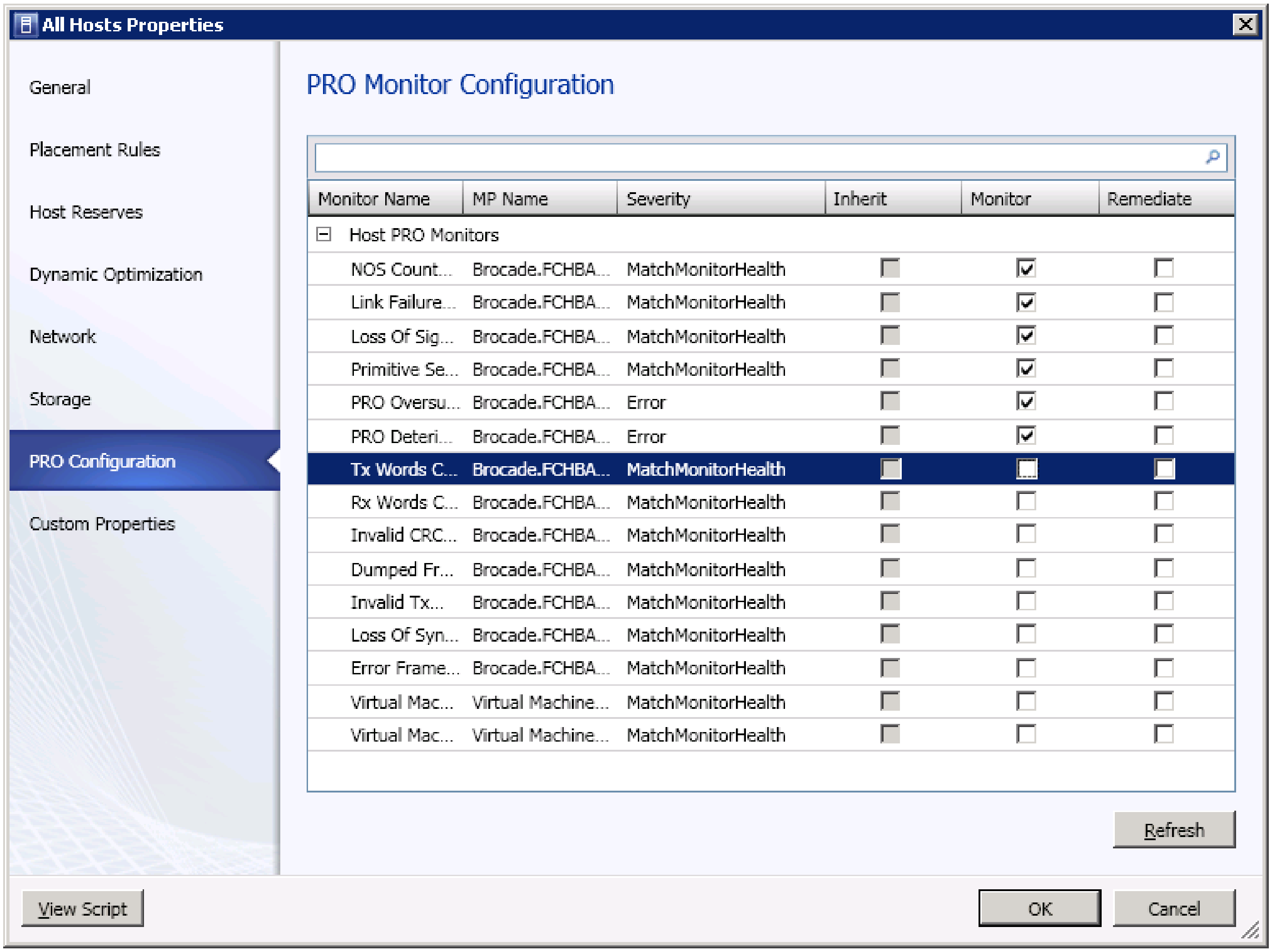
3. Configuring SCOM server in SCVMM

- Please refer to How to Connect VMM with Operations Manager 2012 or Configuring Operations Manager Integration in VMM 2008/2008R2 for details

4. PRO Configuration

In the previous releases of VMM (2008, 2008 R2 and 2008 R2 SP1), you could only enable or disable PRO Tips for a specific host group, cluster, or the VMM server itself. The net effect was that all the monitors that targeted PRO objects within the host group, cluster, or VMM server were either enabled or disabled. SCVMM 2012 introduced the concept of a PRO monitor configuration to give users fine-grained control over the PRO monitors and resulting PRO Tips. Using the PRO monitor configuration, you can choose to enable or disable individual PRO monitors and auto-remediation for specific objects such as Host Group, Host Cluster, Cloud, Service instance, or specific Virtual Machines.

1. Open the VMM Administrator's Console and click the **Fabric** workspace under the navigation pane to display the Fabric view.
2. Select the **Server** - > **All Hosts** in the navigation pane.
3. Right-click on **All Hosts** and select Properties.



PRO Monitor Configuration

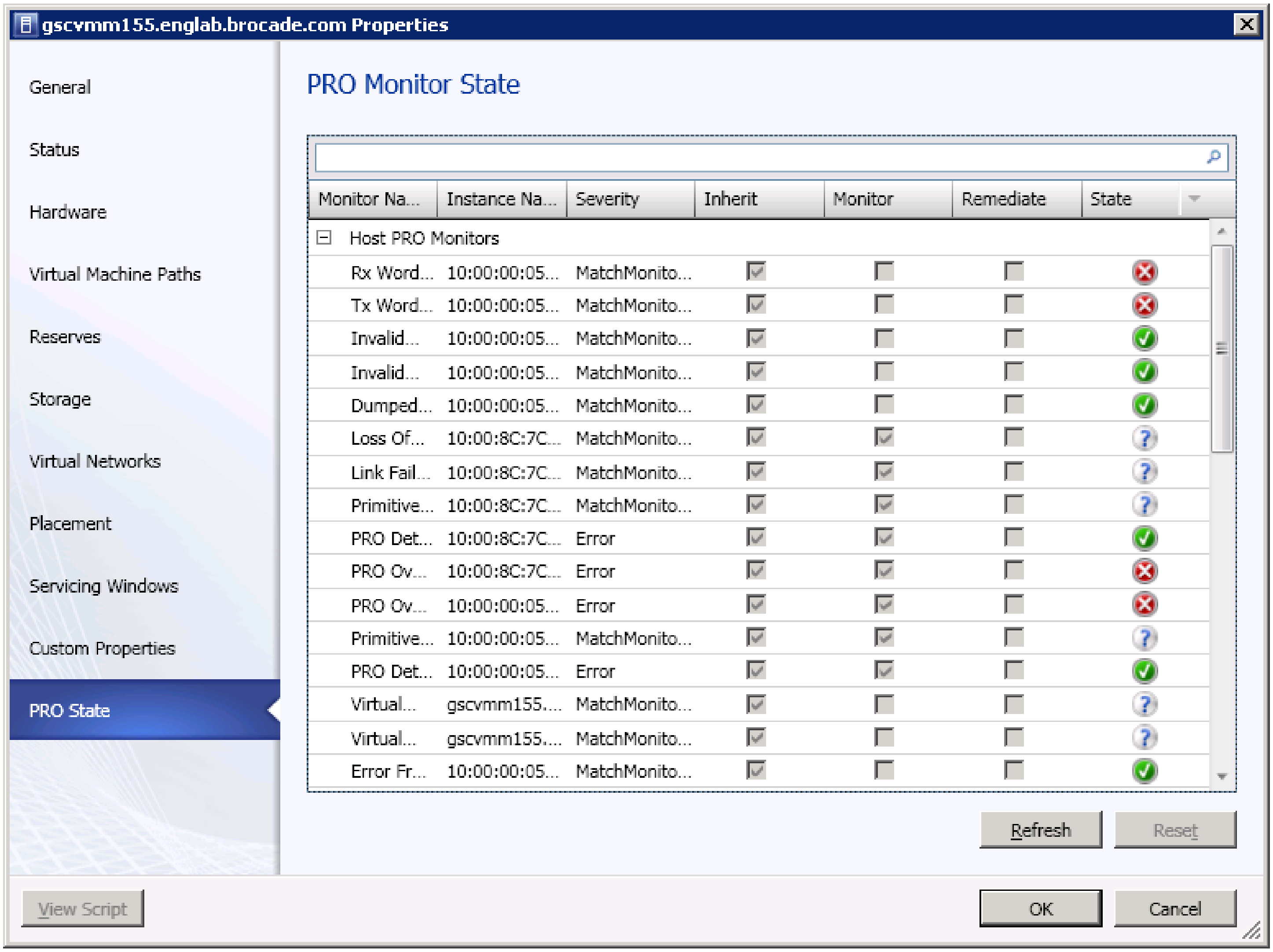
Monitor Name	MP Name	Severity	Inherit	Monitor	Remediate
⊟ Host PRO Monitors					
NOS Count...	Brocade.FCHBA...	MatchMonitorHealth	□	☑	□
Link Failure...	Brocade.FCHBA...	MatchMonitorHealth	□	☑	□
Loss Of Sig...	Brocade.FCHBA...	MatchMonitorHealth	□	☑	□
Primitive Se...	Brocade.FCHBA...	MatchMonitorHealth	□	☑	□
PRO Oversu...	Brocade.FCHBA...	Error	□	☑	□
PRO Deteri...	Brocade.FCHBA...	Error	□	☑	□
Tx Words C...	Brocade.FCHBA...	MatchMonitorHealth	□	□	□
Rx Words C...	Brocade.FCHBA...	MatchMonitorHealth	□	□	□
Invalid CRC...	Brocade.FCHBA...	MatchMonitorHealth	□	□	□
Dumped Fr...	Brocade.FCHBA...	MatchMonitorHealth	□	□	□
Invalid Tx...	Brocade.FCHBA...	MatchMonitorHealth	□	□	□
Loss Of Syn...	Brocade.FCHBA...	MatchMonitorHealth	□	□	□
Error Frame...	Brocade.FCHBA...	MatchMonitorHealth	□	□	□
Virtual Mac...	Virtual Machine...	MatchMonitorHealth	□	□	□
Virtual Mac...	Virtual Machine...	MatchMonitorHealth	□	□	□

Figure 1 – Configuring PRO in SCVMM

If a specific monitor is enabled in VMM, an override for that monitor is created in Operations Manager for the specific scope. The override is stored in a separate Management Pack (called the working MP) that has the name of the PRO Pack followed by the word “Working”. The “Remediate” checkbox creates an override to enable auto-remediate. If the remediate option is unchecked, you will have the option to manually implement the PRO Tip, should one be generated.

VMM 2012 enhanced the PRO feature to report the health state of individual PRO monitors. The health state reflects the current health state (Warning, Healthy, Critical, or Uninitialized) of the monitor in Operations Manager for the specific object of interest (Host, VM, Cloud, Service Instance, etc). Along with the health state, the current configuration of each monitor is displayed:

1. Open the VMM Administrator’s Console and click the **Fabric** workspace under the navigation pane to display Fabric view.
2. Select the **Server** - > **All Hosts** in the navigation pane.
3. Select any discovered host, right-click the **Host**, and select **Properties**.



PRO Monitor State

Monitor Na...	Instance Na...	Severity	Inherit	Monitor	Remediate	State
⊟ Host PRO Monitors						
Rx Word...	10:00:00:05...	MatchMonito...	☑	☐	☐	✗
Tx Word...	10:00:00:05...	MatchMonito...	☑	☐	☐	✗
Invalid...	10:00:00:05...	MatchMonito...	☑	☐	☐	✓
Invalid...	10:00:00:05...	MatchMonito...	☑	☐	☐	✓
Dumped...	10:00:00:05...	MatchMonito...	☑	☐	☐	✓
Loss Of...	10:00:8C:7C...	MatchMonito...	☑	☑	☐	?
Link Fail...	10:00:8C:7C...	MatchMonito...	☑	☑	☐	?
Primitive...	10:00:8C:7C...	MatchMonito...	☑	☑	☐	?
PRO Det...	10:00:8C:7C...	Error	☑	☑	☐	✓
PRO Ov...	10:00:8C:7C...	Error	☑	☑	☐	✗
PRO Ov...	10:00:00:05...	Error	☑	☑	☐	✗
Primitive...	10:00:00:05...	MatchMonito...	☑	☑	☐	?
PRO Det...	10:00:00:05...	Error	☑	☑	☐	✓
Virtual...	gscvmm155....	MatchMonito...	☑	☐	☐	?
Virtual...	gscvmm155....	MatchMonito...	☑	☐	☐	?
Error Fr...	10:00:00:05...	MatchMonito...	☑	☐	☐	✓

Figure 2 – PRO State in SCVMM

4.2.2 Installing SCVMM agent

To deploy the Virtual Machine Manager 2012 agent to Windows-based computers from a VMM console, the following steps must be followed to configure SCOM Server to SCVMM.

1. Open the VMM Administrator’s Console and click the **Fabric** workspace under the navigation pane to display the Fabric view.
2. Select the **Server** in the navigation pane. On the **Home** tab, in the **Add** group, click **Add Resources**, and then click Hyper-V Hosts and Clusters. The Add Resource Wizard starts.
3. Follow the interaction shown in the dialog box (depicted below). Please refer [Adding and Managing Hyper-V Hosts and Host Clusters in VMM] for details.

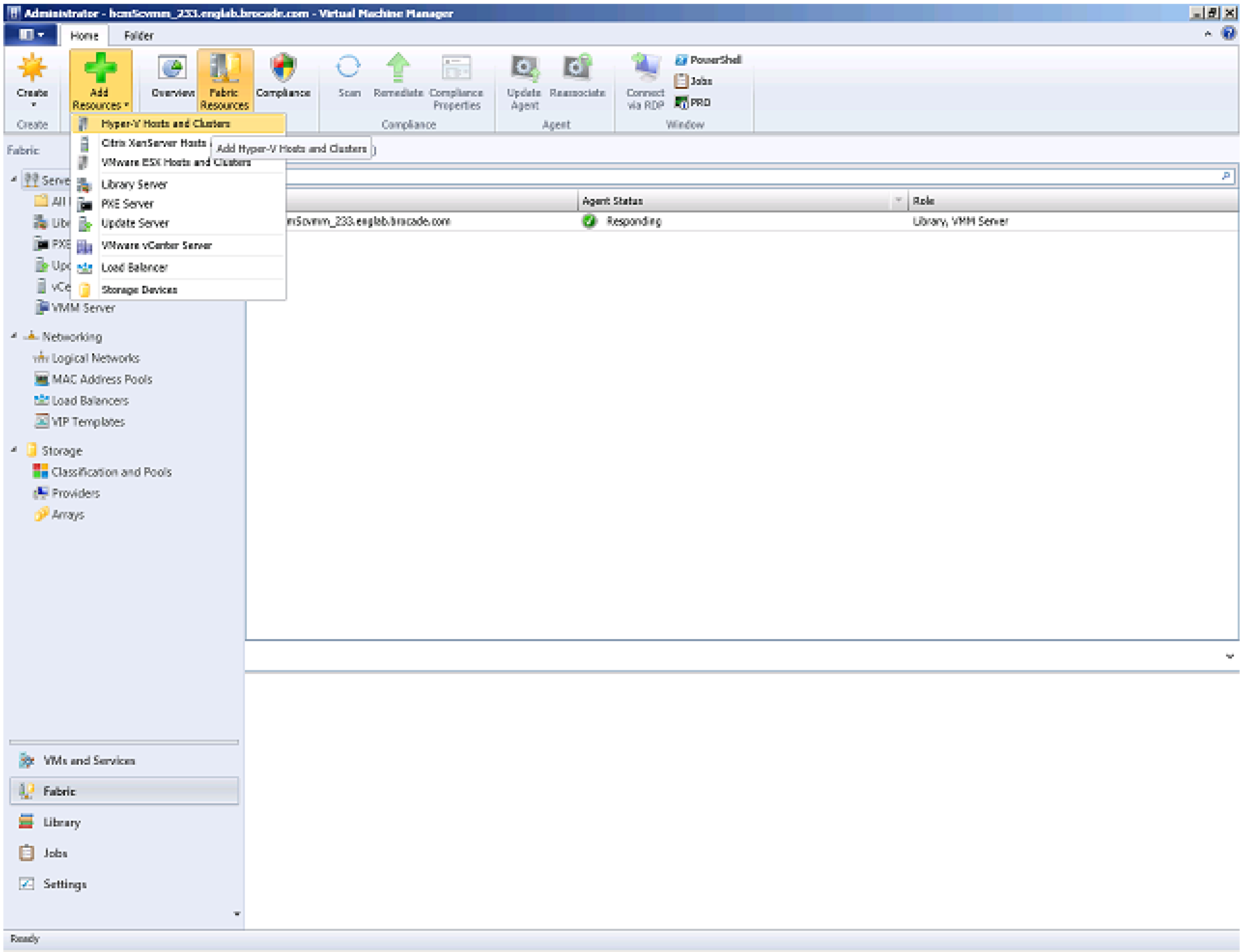
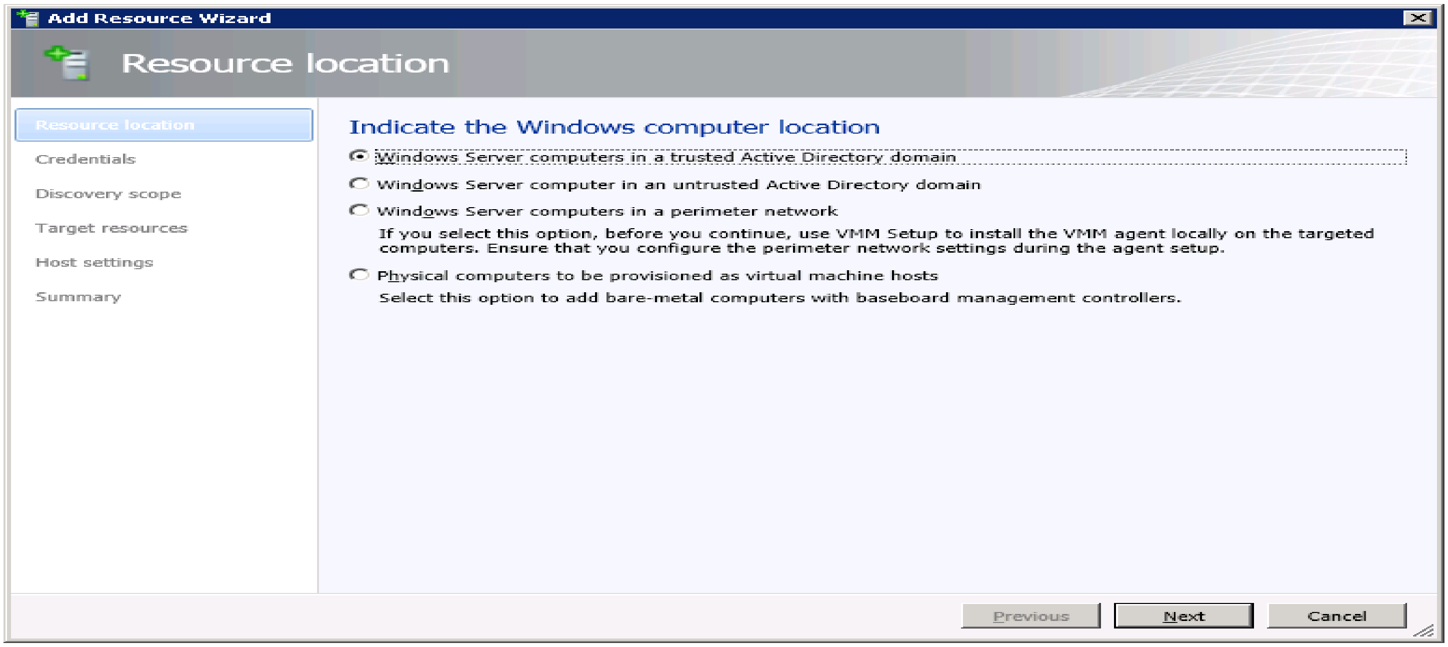


Figure 3 – Installing SCVMM agent – Add Host Menu

4. On the **Resource location** page, click **Windows Server computers in a trusted Active Directory domain**, and then click **next**.



Indicate the Windows computer location

● Windows Server computers in a trusted Active Directory domain

○ Windows Server computer in an untrusted Active Directory domain

○ Windows Server computers in a perimeter network

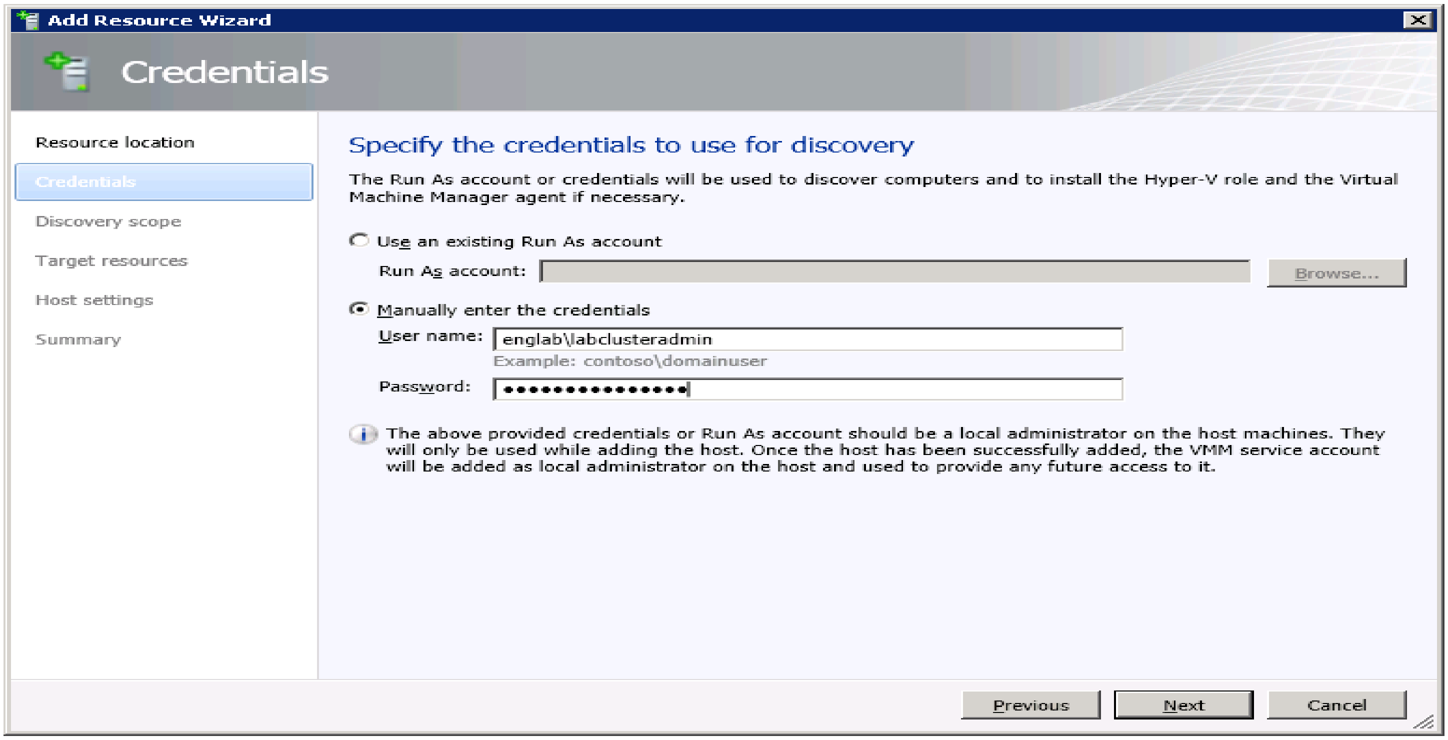
If you select this option, before you continue, use VMM Setup to install the VMM agent locally on the targeted computers. Ensure that you configure the perimeter network settings during the agent setup.

○ Physical computers to be provisioned as virtual machine hosts

Select this option to add bare-metal computers with baseboard management controllers.

Figure 4 – Installing SCVMM agent – Resource location

5. On the Credentials page, enter the credentials for a domain account that has administrative permissions on all hosts that you want to add, and then click **Next.**



Specify the credentials to use for discovery

The Run As account or credentials will be used to discover computers and to install the Hyper-V role and the Virtual Machine Manager agent if necessary.

○ Use an existing Run As account

Run As account:

● Manually enter the credentials

User name: englab\labclusteradmin

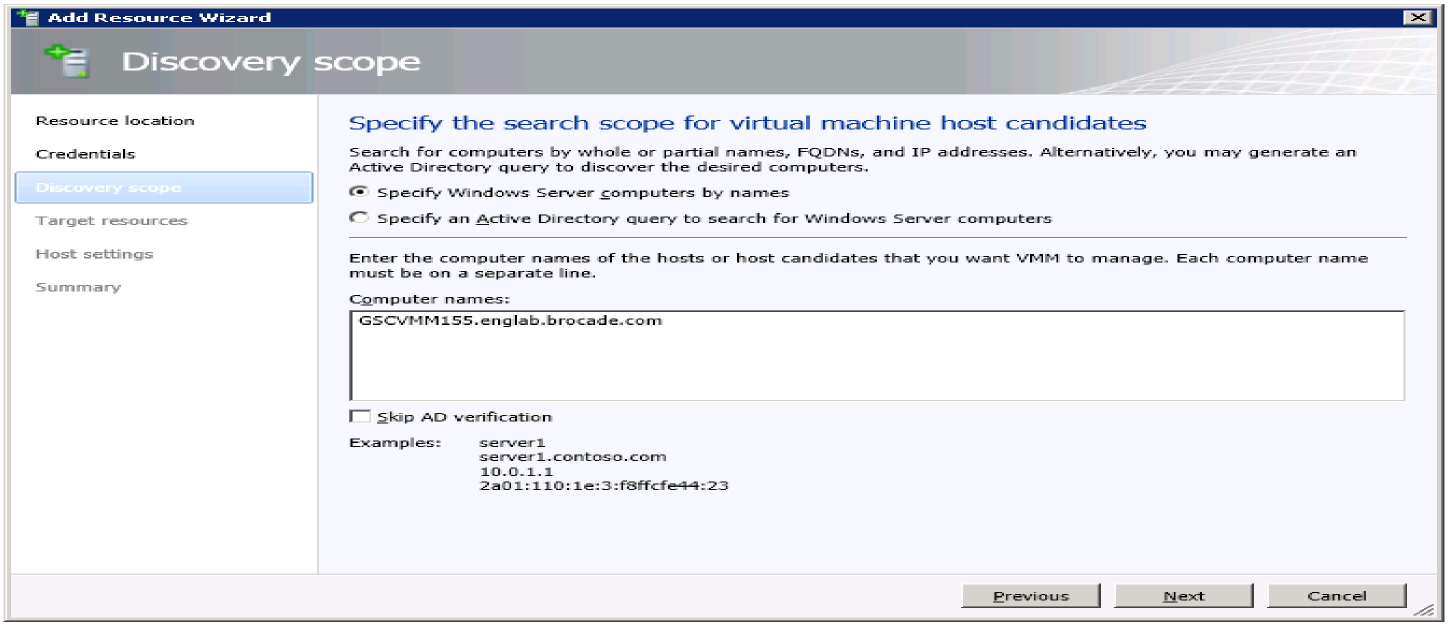
Example: contoso\domainuser

Password: ●●●●●●●●●●●●●●●

The above provided credentials or Run As account should be a local administrator on the host machines. They will only be used while adding the host. Once the host has been successfully added, the VMM service account will be added as local administrator on the host and used to provide any future access to it.

Figure 5 – Installing SCVMM agent – Credentials

6. On the Discovery scope page, click “Specify Windows Server computers by names”. In the Computer names box, enter the computers that you want to add, with each computer name or IP address on a new line.



Specify the search scope for virtual machine host candidates

Search for computers by whole or partial names, FQDNs, and IP addresses. Alternatively, you may generate an Active Directory query to discover the desired computers.

● Specify Windows Server computers by names

○ Specify an Active Directory query to search for Windows Server computers

Enter the computer names of the hosts or host candidates that you want VMM to manage. Each computer name must be on a separate line.

Computer names:

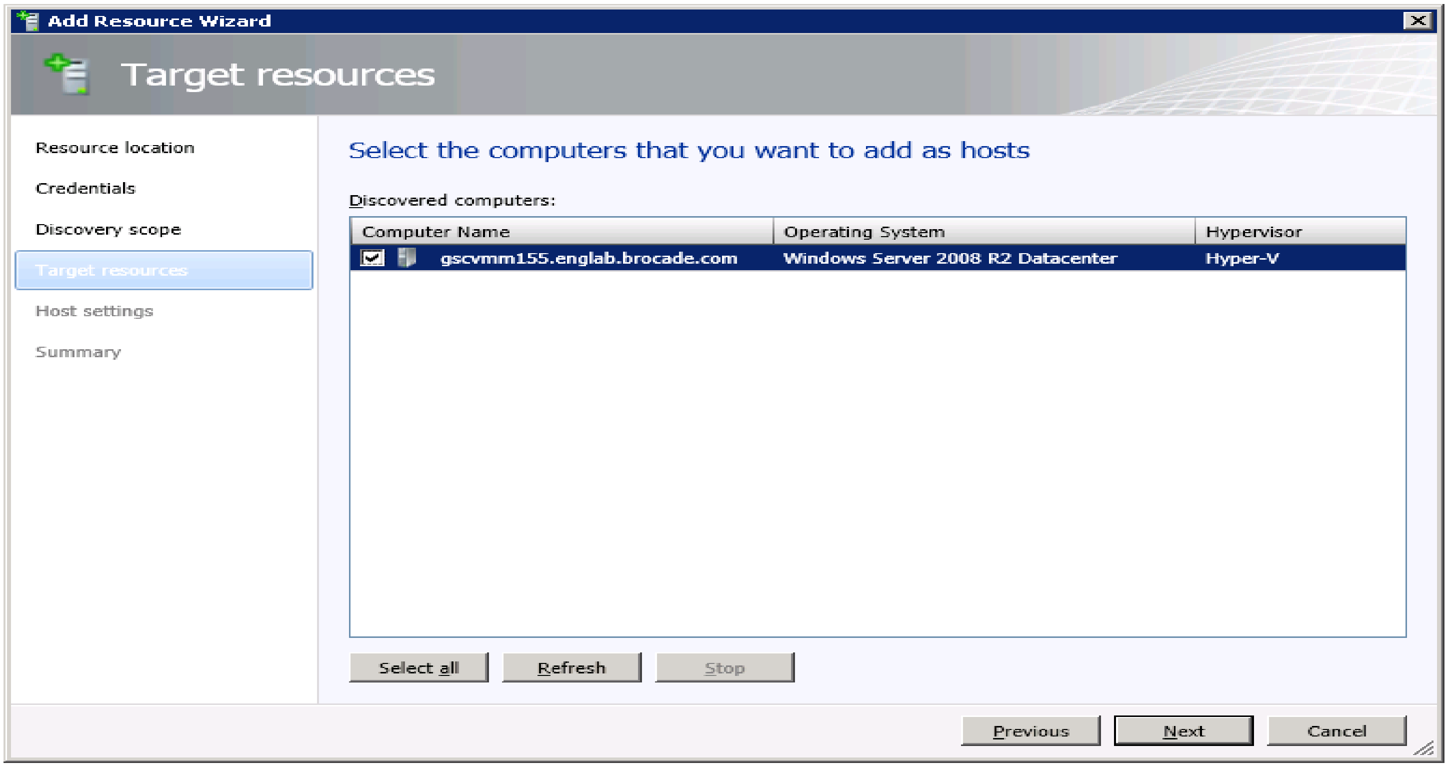
```
GSCVMM155.englab.brocade.com
```

□ Skip AD verification

```
Examples:     server1
              server1.contoso.com
              10.0.1.1
              2a01:110:1e:3:f8ffcfe44:23
```

Figure 6 – Installing SCVMM agent – Discovery Scope

7. On the **Target resources** page, select the check box next to each computer that you want to add, and then click **next**.



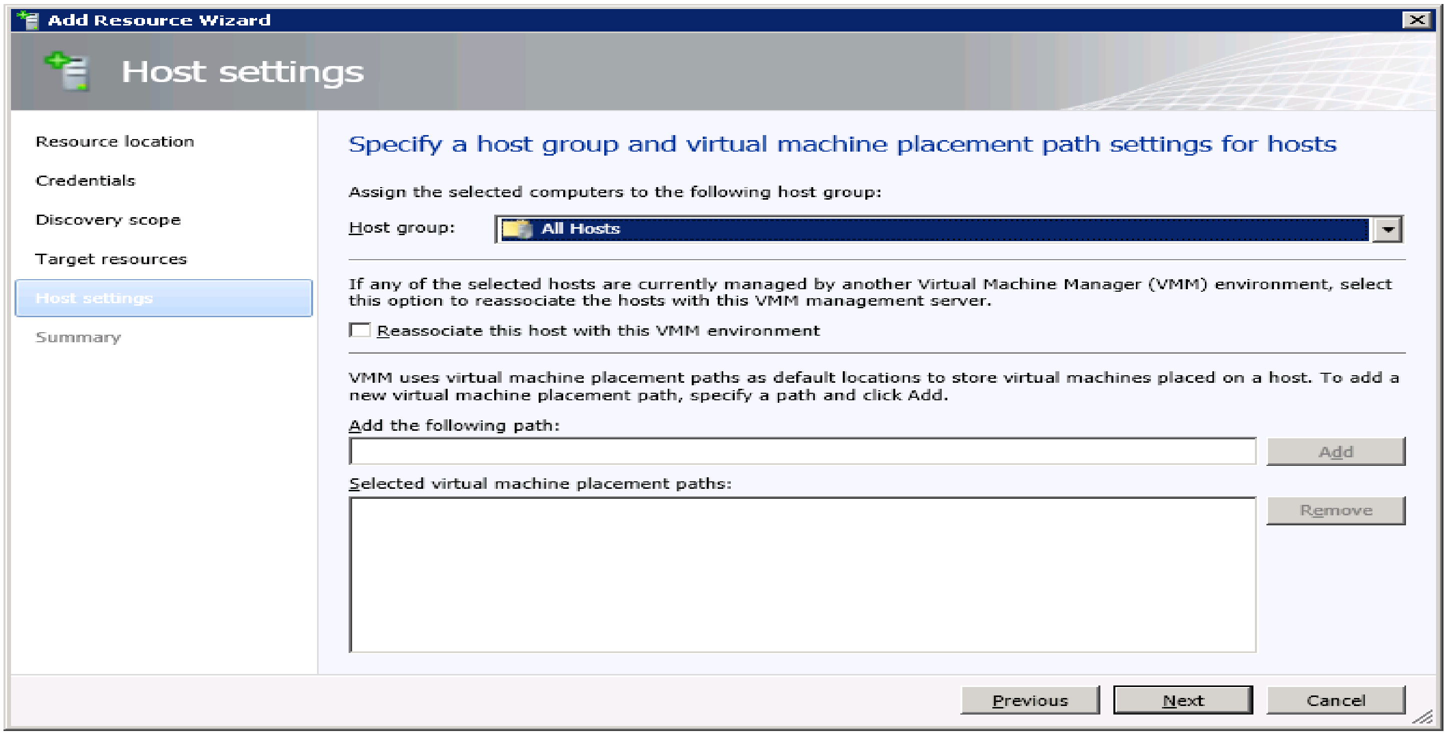
Select the computers that you want to add as hosts

Discovered computers:

Computer Name	Operating System	Hypervisor
☑ gscvmm155.englab.brocade.com	Windows Server 2008 R2 Datacenter	Hyper-V

Figure 7 – Installing SCVMM agent – Target resources

8. On the **Host settings** page, In the **Host group** list, click the host group to which you want to assign the host or host cluster.



Specify a host group and virtual machine placement path settings for hosts

Assign the selected computers to the following host group:

Host group: All Hosts

If any of the selected hosts are currently managed by another Virtual Machine Manager (VMM) environment, select this option to reassociate the hosts with this VMM management server.

□ Reassociate this host with this VMM environment

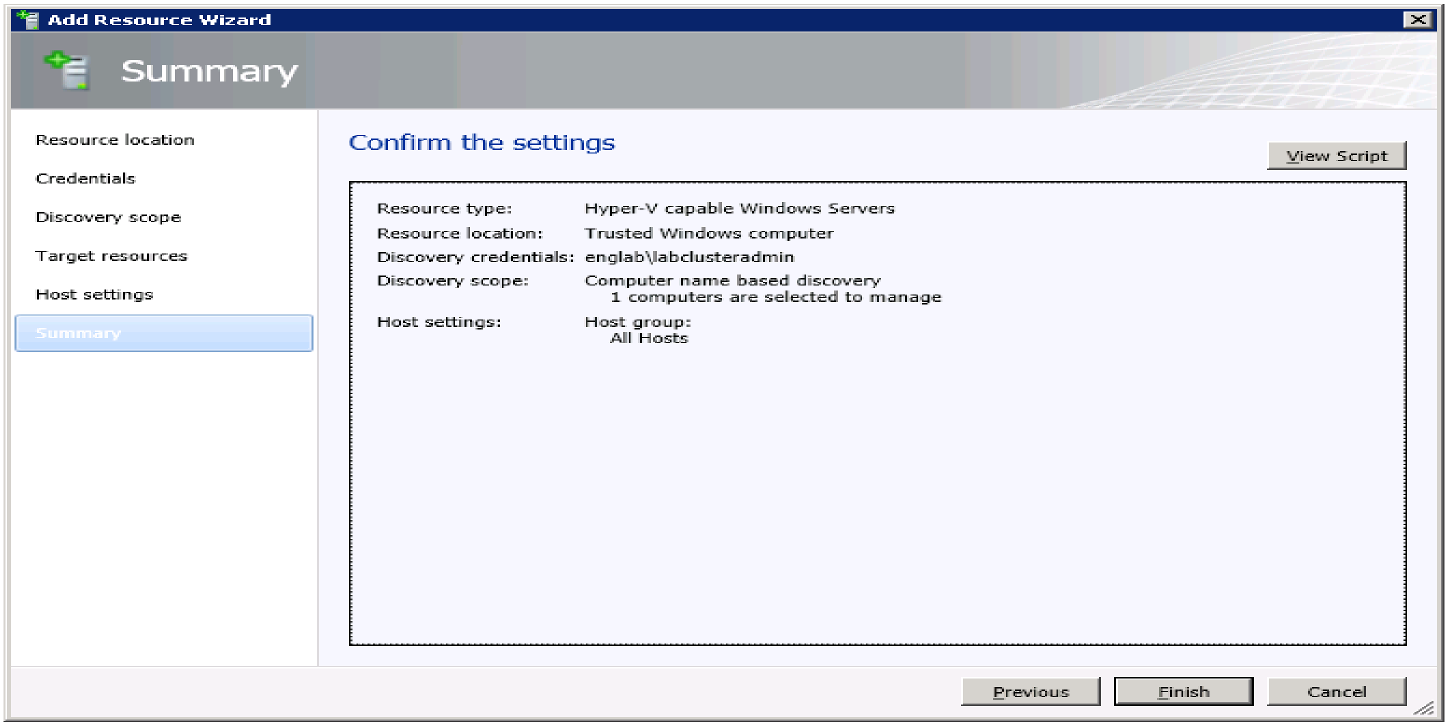
VMM uses virtual machine placement paths as default locations to store virtual machines placed on a host. To add a new virtual machine placement path, specify a path and click Add.

Add the following path:

Selected virtual machine placement paths:

Figure 8 – Installing SCVMM agent – Host Settings

9. On the **Summary** page, confirm the settings, and then click **Finish**.

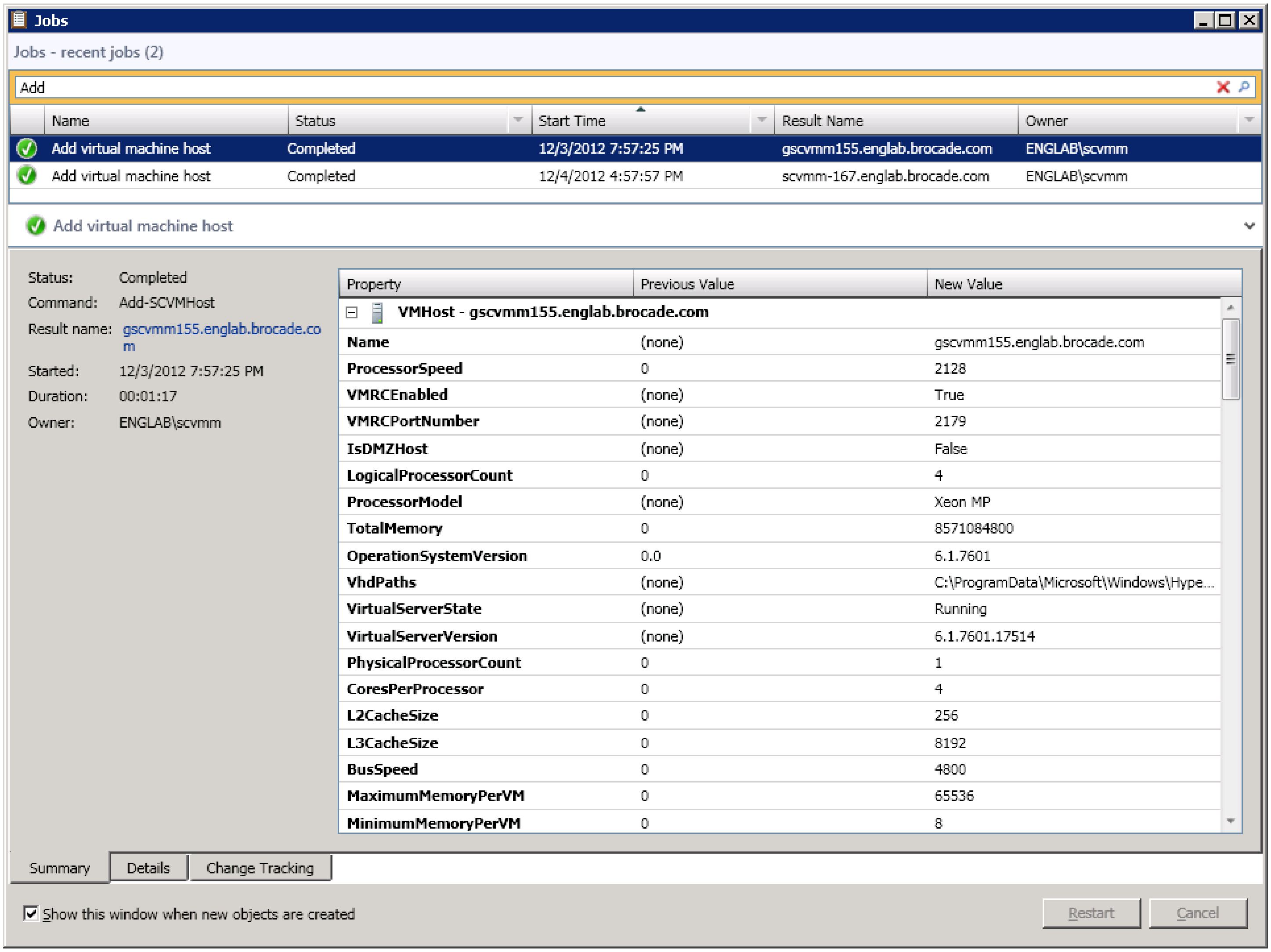


Confirm the settings

Resource type:	Hyper-V capable Windows Servers
Resource location:	Trusted Windows computer
Discovery credentials:	englab\labclusteradmin
Discovery scope:	Computer name based discovery 1 computers are selected to manage
Host settings:	Host group: All Hosts

Figure 9 – Installing SCVMM agent – Summary

10. When the **Jobs** dialog box appears to show the job status, make sure that the job has a status of **Completed**, and then close the dialog box.



Name	Status	Start Time	Result Name	Owner
Add virtual machine host	Completed	12/3/2012 7:57:25 PM	gscvmm155.englab.brocade.com	ENGLAB\scvmm
Add virtual machine host	Completed	12/4/2012 4:57:57 PM	scvmm-167.englab.brocade.com	ENGLAB\scvmm

Add virtual machine host

Status: Completed
Command: Add-SCVMHost
Result name: gscvmm155.englab.brocade.com
Started: 12/3/2012 7:57:25 PM
Duration: 00:01:17
Owner: ENGLAB\scvmm

Property	Previous Value	New Value
VMHost - gscvmm155.englab.brocade.com		
Name	(none)	gscvmm155.englab.brocade.com
ProcessorSpeed	0	2128
VMRCEnabled	(none)	True
VMRCPortNumber	(none)	2179
IsDMZHost	(none)	False
LogicalProcessorCount	0	4
ProcessorModel	(none)	Xeon MP
TotalMemory	0	8571084800
OperationSystemVersion	0.0	6.1.7601
VhdPaths	(none)	C:\ProgramData\Microsoft\Windows\Hype...
VirtualServerState	(none)	Running
VirtualServerVersion	(none)	6.1.7601.17514
PhysicalProcessorCount	0	1
CoresPerProcessor	0	4
L2CacheSize	0	256
L3CacheSize	0	8192
BusSpeed	0	4800
MaximumMemoryPerVM	0	65536
MinimumMemoryPerVM	0	8

☑ Show this window when new objects are created

Figure 10 – Installing SCVMM agent – Jobs

Please refer to “Adding Hosts” for details on adding a Hyper-v host to SCVM M 2008/2008 R2.

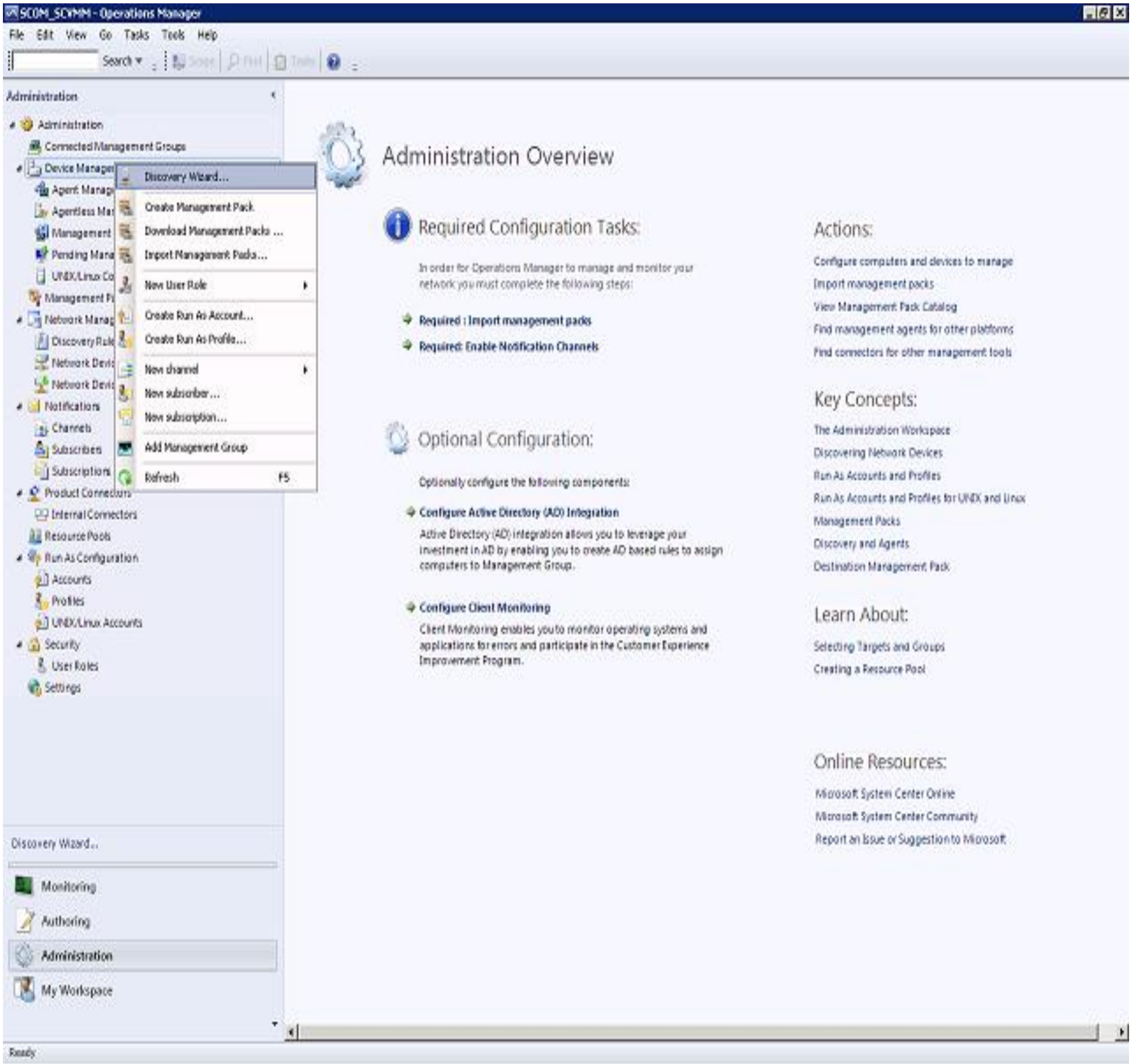
4.2.3 Installing SCOM agent

Please refer to Operations Manager Agent Installation Methods for details.

Use the following steps to deploy the Operations Manager 2012 agent to Windows-based computers from the Operations console:

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager 2012 Management Group.
2. In the Operations Console, click the Administration button.

3. At the bottom of the navigation pane, click Discovery Wizard.



Administration Overview

Required Configuration Tasks:

In order for Operations Manager to manage and monitor your network you must complete the following steps:

- Required : Import management packs
- Required: Enable Notification Channels

Optional Configuration:

Optionally configure the following components:

- Configure Active Directory (AD) Integration

  Active Directory (AD) integration allows you to leverage your investment in AD by enabling you to create AD based rules to assign computers to Management Group.

- Configure Client Monitoring

  Client Monitoring enables you to monitor operating systems and applications for errors and participate in the Customer Experience Improvement Program.

Actions:

Configure computers and devices to manage
Import management packs
View Management Pack Catalog
Find management agents for other platforms
Find connectors for other management tools

Key Concepts:

The Administration Workspace
Discovering Network Devices
Run As Accounts and Profiles
Run As Accounts and Profiles for UNIX and Linux
Management Packs
Discovery and Agents
Destination Management Pack

Learn About:

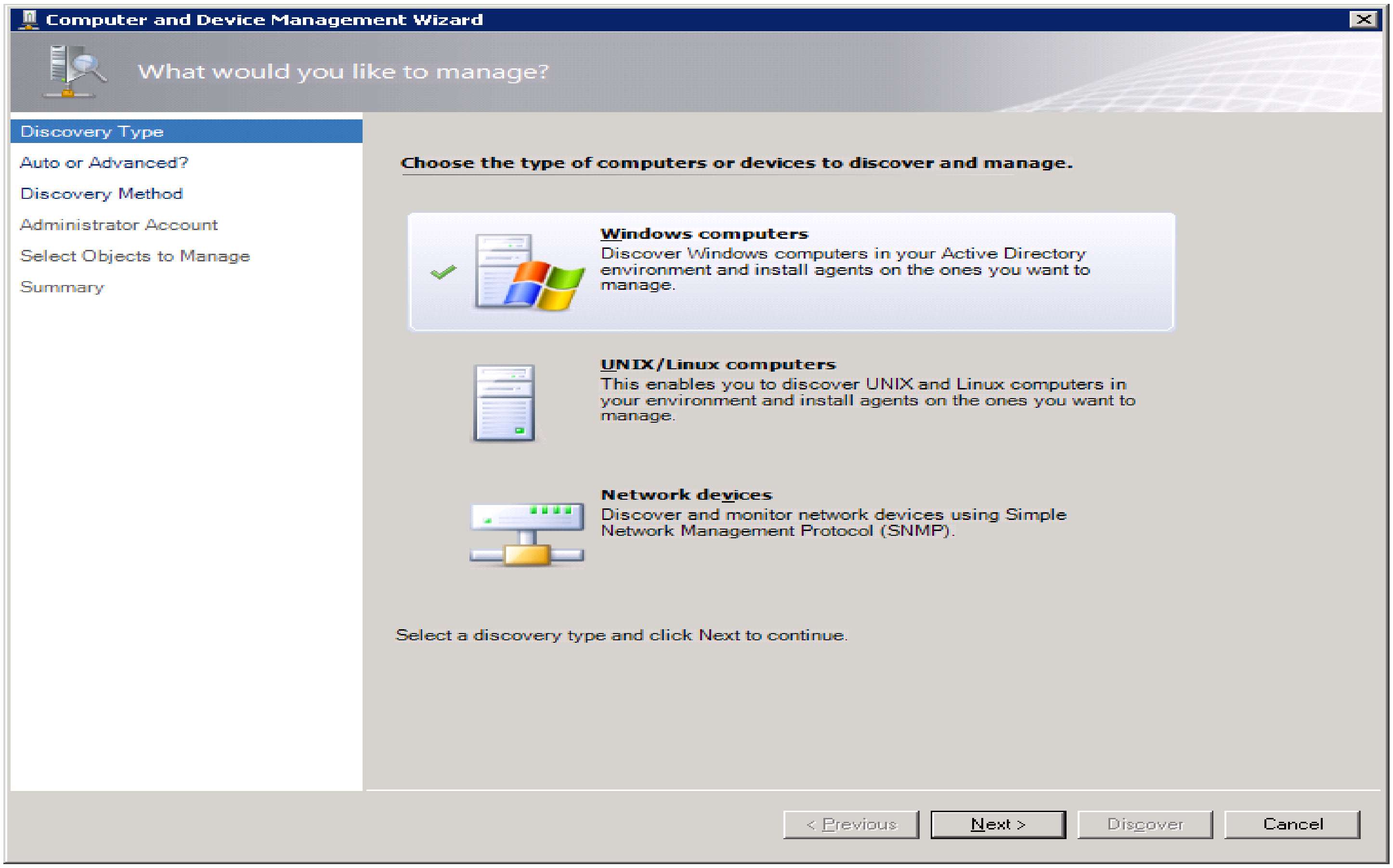
Selecting Targets and Groups
Creating a Resource Pool

Online Resources:

Microsoft System Center Online
Microsoft System Center Community
Report an Issue or Suggestion to Microsoft

Figure 11 – Installing SCVMM agent-managed host in SCOM

4. On the **Discovery Type** page, click **Windows computers**.



Choose the type of computers or devices to discover and manage.

Windows computers
Discover Windows computers in your Active Directory environment and install agents on the ones you want to manage.

UNIX/Linux computers
This enables you to discover UNIX and Linux computers in your environment and install agents on the ones you want to manage.

Network devices
Discover and monitor network devices using Simple Network Management Protocol (SNMP).

Select a discovery type and click Next to continue.

Figure 12 – Installing SCVMM agent –Discovery Type

5. On the Auto or Advanced page, perform the following steps:

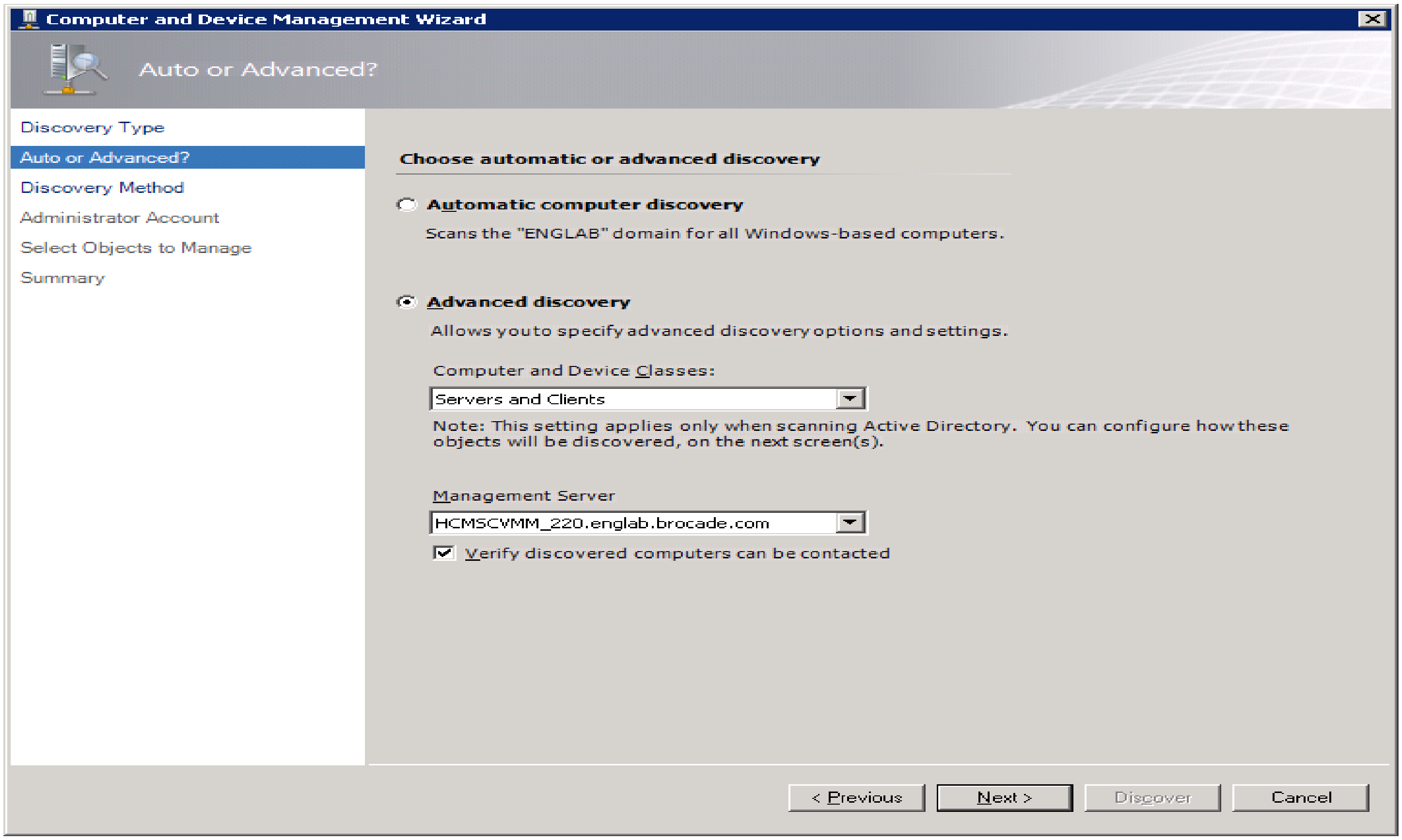
    1. Select either Automatic computer discovery or Advanced discovery. If you select Automatic computer discovery, click **Next**, and then go to step 7. If you select Advanced discovery, continue with the following steps.

    2. In the Computer & Device Types list, select **Servers & Clients**, **Server Only**, or **Clients Only**.

    3. In the Management Server list, click the Management Server or gateway server to discover the computers. 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.

    4. If you selected **Servers & Clients**, you can select the “Verify discovered computers can be contacted” check box. This is likely to increase the success rate of agent deployment, but discovery can take longer.

    5. Click **Next**.



Choose automatic or advanced discovery

○ Automatic computer discovery

Scans the "ENGLAB" domain for all Windows-based computers.

● Advanced discovery

Allows youto specify advanced discovery options and settings.

Computer and Device Classes: Servers and Clients

Note: This setting applies only when scanning Active Directory. You can configure how these objects will be discovered, on the next screen(s).

Management Server: HCMSCVMM_220.englab.brocade.com

☑ Verify discovered computers can be contacted

Figure 13 – Installation of SCVMM agent –Auto or Advanced

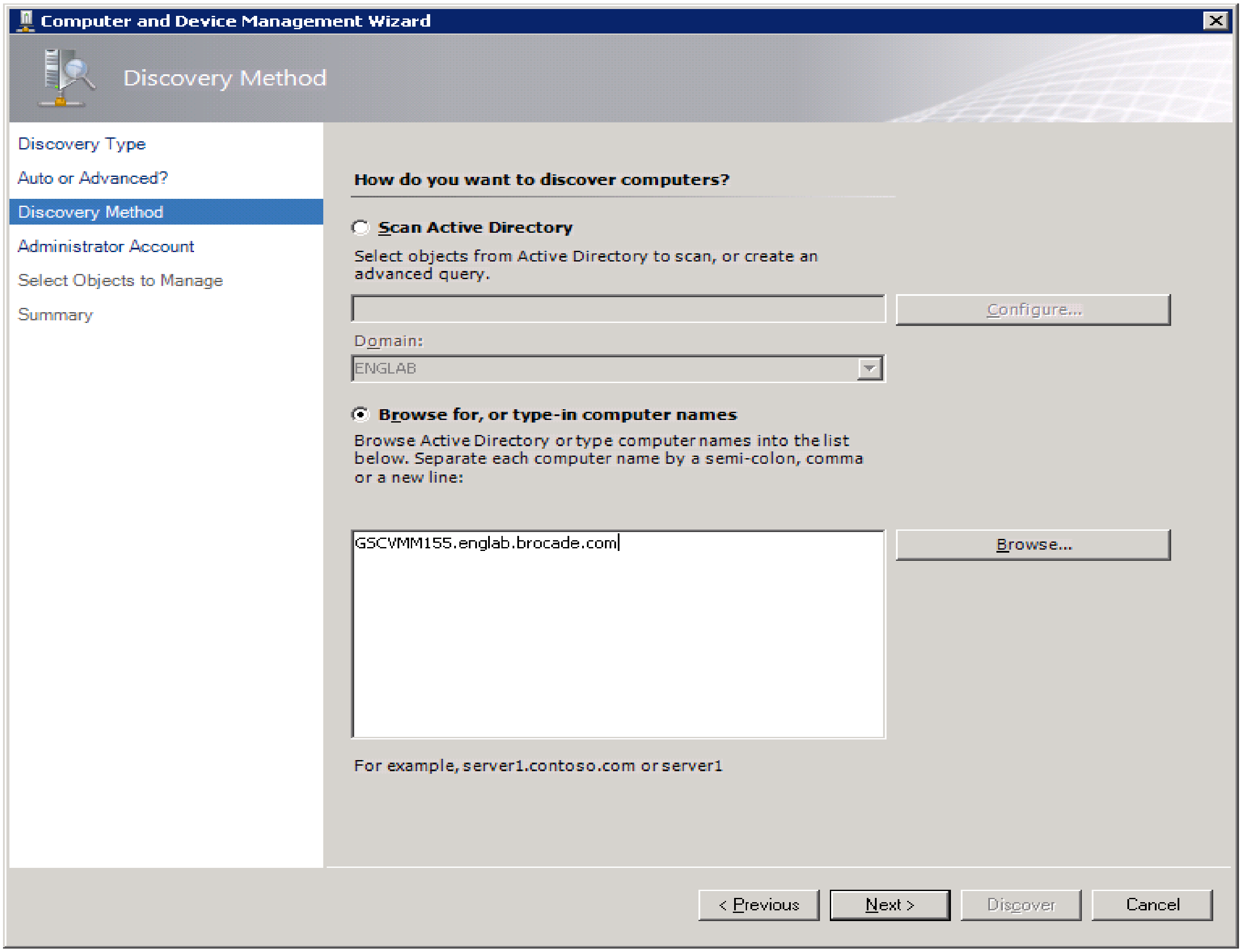
6. On the Discovery Method page, locate the computers that you want to manage by either scanning or browsing Active Directory Domain Services or typing the computer names.

   If you want to scan, perform the following steps:

   1. If it is not already selected, select **Scan Active Directory**, and then click **Configure**.
   2. In the **Find Computers** dialog box, type the desired criteria for discovering computers, and then click **OK**.
   3. 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, perform the following steps:

   - Select “Browse for”, or “type-in computernames” and specify the names of the computers you want to manage. 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 [ENTER]. You can use NetBIOS computer names or Fully Qualified Domain Names (FQDN).



How do you want to discover computers?

○ Scan Active Directory

Select objects from Active Directory to scan, or create an advanced query.

Domain: ENGLAB

● Browse for, or type-in computer names

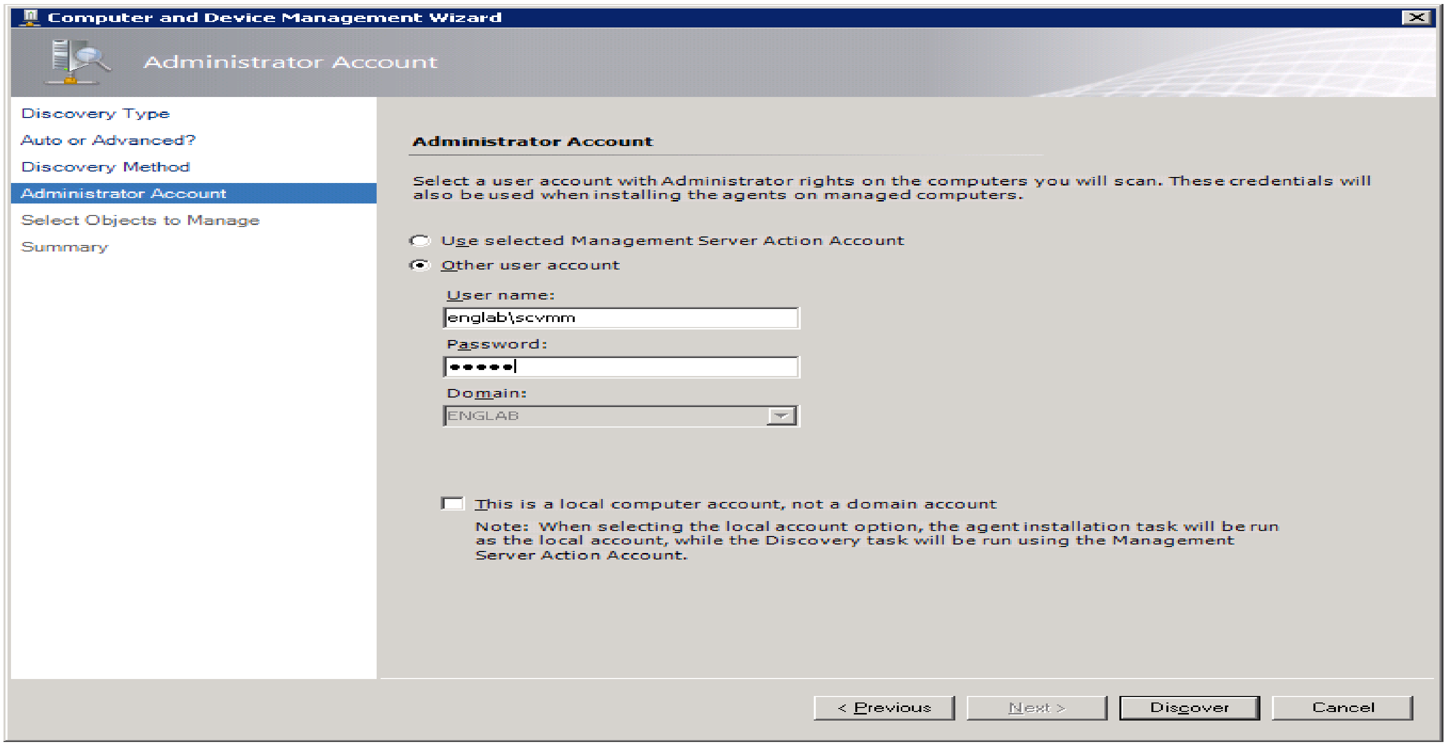
Browse Active Directory or type computer names into the list below. Separate each computer name by a semi-colon, comma or a new line:

GSCVMM155.englab.brocade.com

For example, server1.contoso.com or server1

Figure 14 – Installing SCVMM agent –Discovery Method

7. Click **Next**, and on the Administrator Account page, perform one of the following steps:
   - Select Use selected Management Server Action Account if it is not already selected.
   - Select another 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”.



Administrator Account

Select a user account with Administrator rights on the computers you will scan. These credentials will also be used when installing the agents on managed computers.

○ Use selected Management Server Action Account

● Other user account

User name: englab\scvmm

Password: •••••

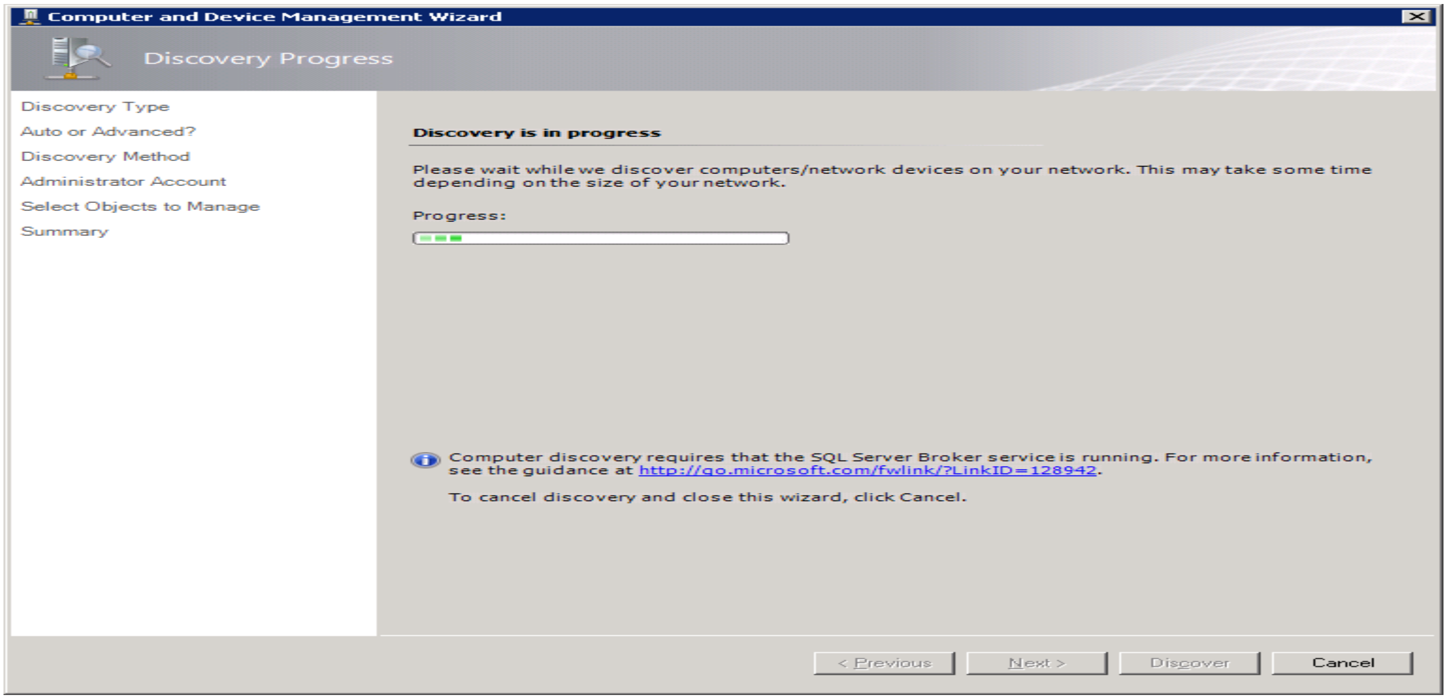
Domain: ENGLAB

□ This is a local computer account, not a domain account

Note: When selecting the local account option, the agent installation task will be run as the local account, while the Discovery task will be run using the Management Server Action Account.

Figure 15 – Installing SCVMM agent –Administrator Account

8. Click **Discover** to display the **Discovery Progress** page. The time for discovery to complete depends on many factors, such as the criteria specified and the configuration of the IT environment.



Discovery is in progress

Please wait while we discover computers/network devices on your network. This may take some time depending on the size of your network.

Progress:

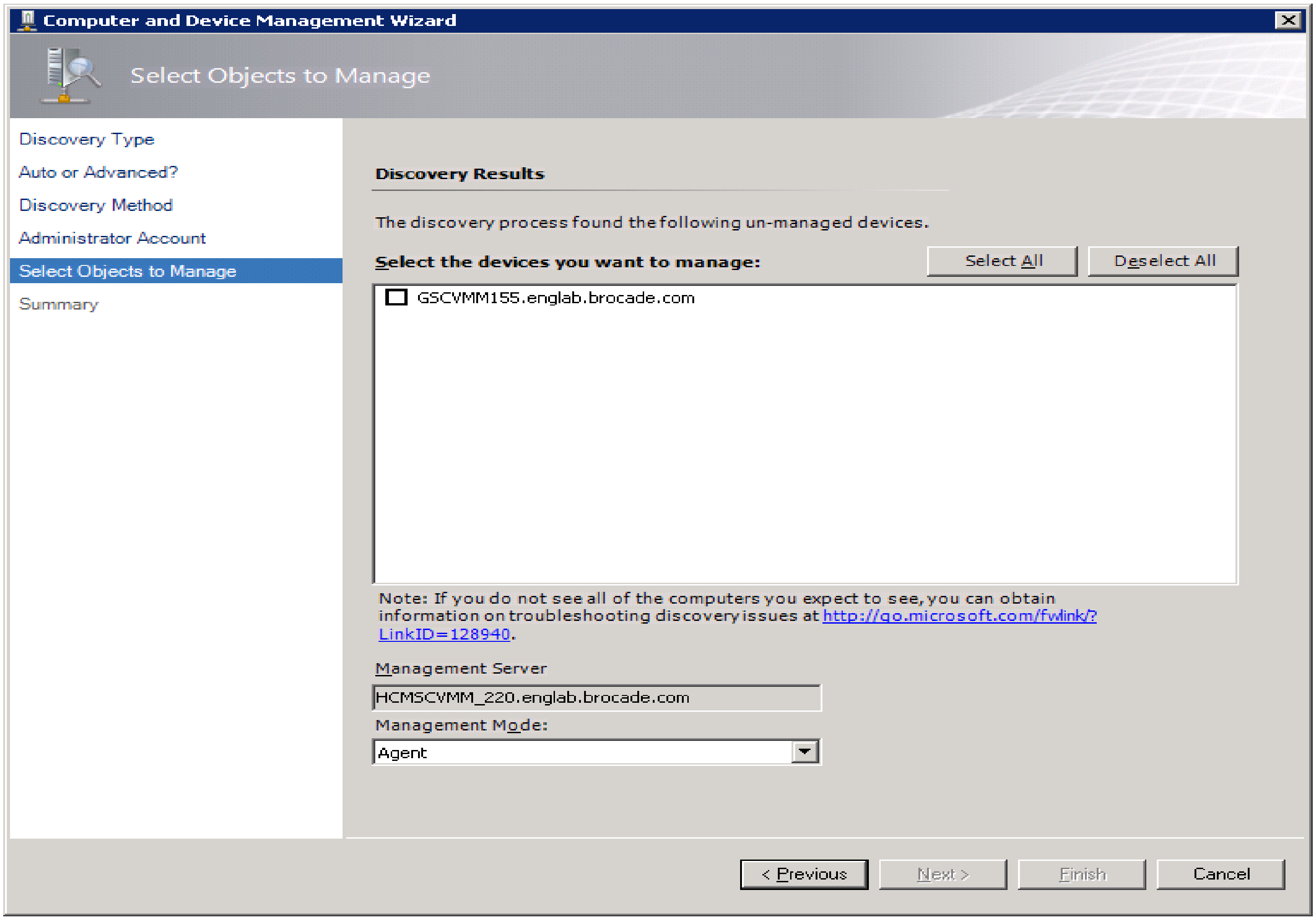
Computer discovery requires that the SQL Server Broker service is running. For more information, see the guidance at http://go.microsoft.com/fwlink/?LinkID=128942.

To cancel discovery and close this wizard, click Cancel.

Figure 16 – Installing SCVMM agent –Discovery is in progress

9. On the **Select Objects to Manage** page, perform the following steps:

- Select the computers that you want to agent-manage.
- In the Management Mode list, click **Agent**, and then click **next**.



Computer and Device Management Wizard

Select Objects to Manage

Discovery Results

The discovery process found the following un-managed devices.

Select the devices you want to manage:

□ GSCVMM155.englab.brocade.com

Note: If you do not see all of the computers you expect to see, you can obtain information on troubleshooting discovery issues at http://go.microsoft.com/fwlink/?LinkID=128940.

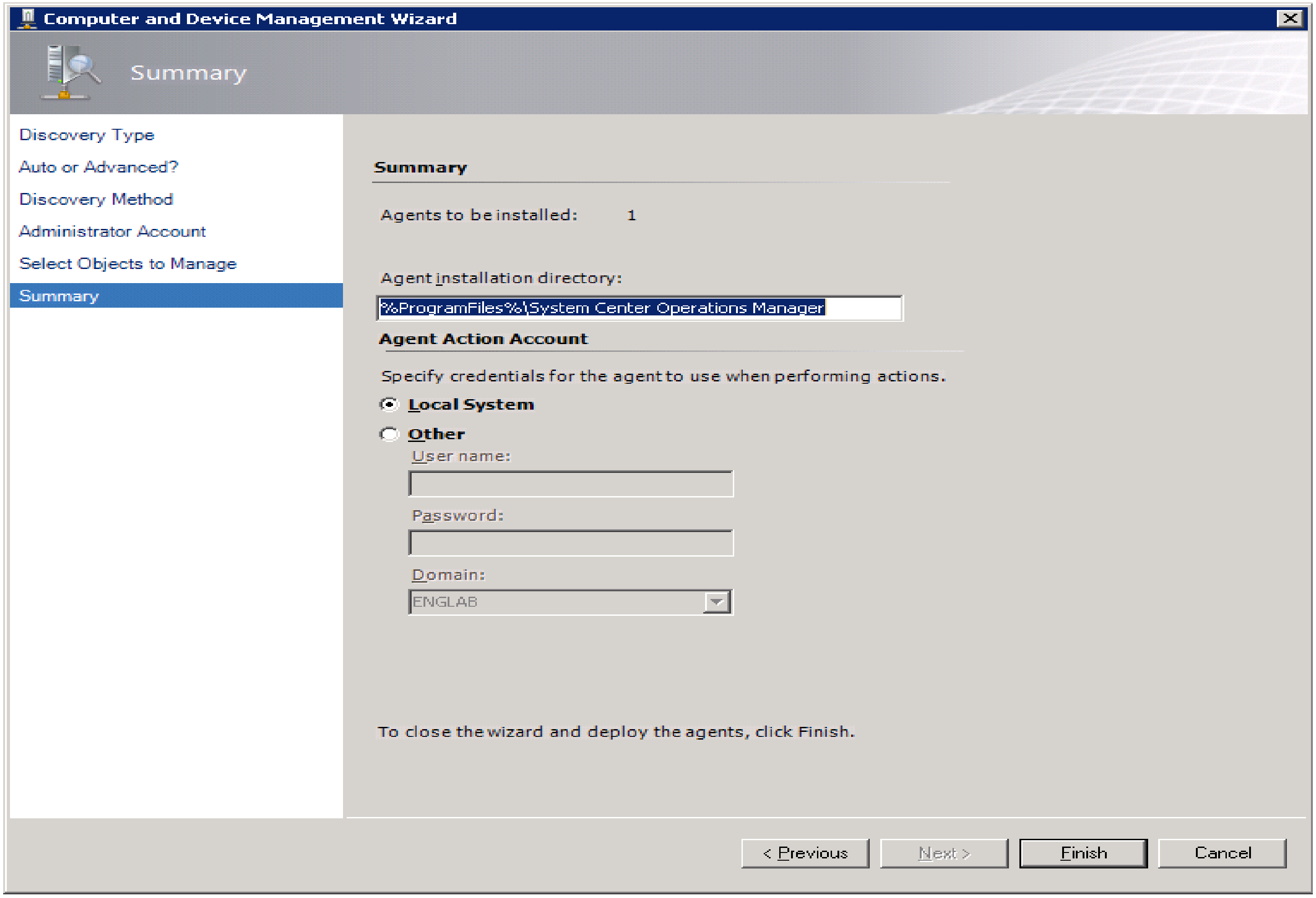
Management Server: HCMSCVMM_220.englab.brocade.com

Management Mode: Agent

Figure 17 – Installing SCVMM agent –Select Object to Manage

10. On the Summary page, perform the following steps:

- Leave the agent installation directory set to the default of %ProgramFiles%\System Center Operations Manager or type an installation path.
- Leave **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.
- Click **Finish**.



Summary

Agents to be installed: 1

Agent installation directory: %ProgramFiles%\System Center Operations Manager

Agent Action Account

Specify credentials for the agent to use when performing actions.

● Local System

○ Other

User name:

Password:

Domain: ENGLAB

To close the wizard and deploy the agents, click Finish.

Figure 18 – Installing SCVMM agent –Summary

In the **Agent Management Task Status** dialog box, when the Status for each selected computer changes from Queued to Success, the computers are ready to be managed.

For SCOM 2007/2007 R2, please refer to "Use the Discovery Wizard to Deploy agents".

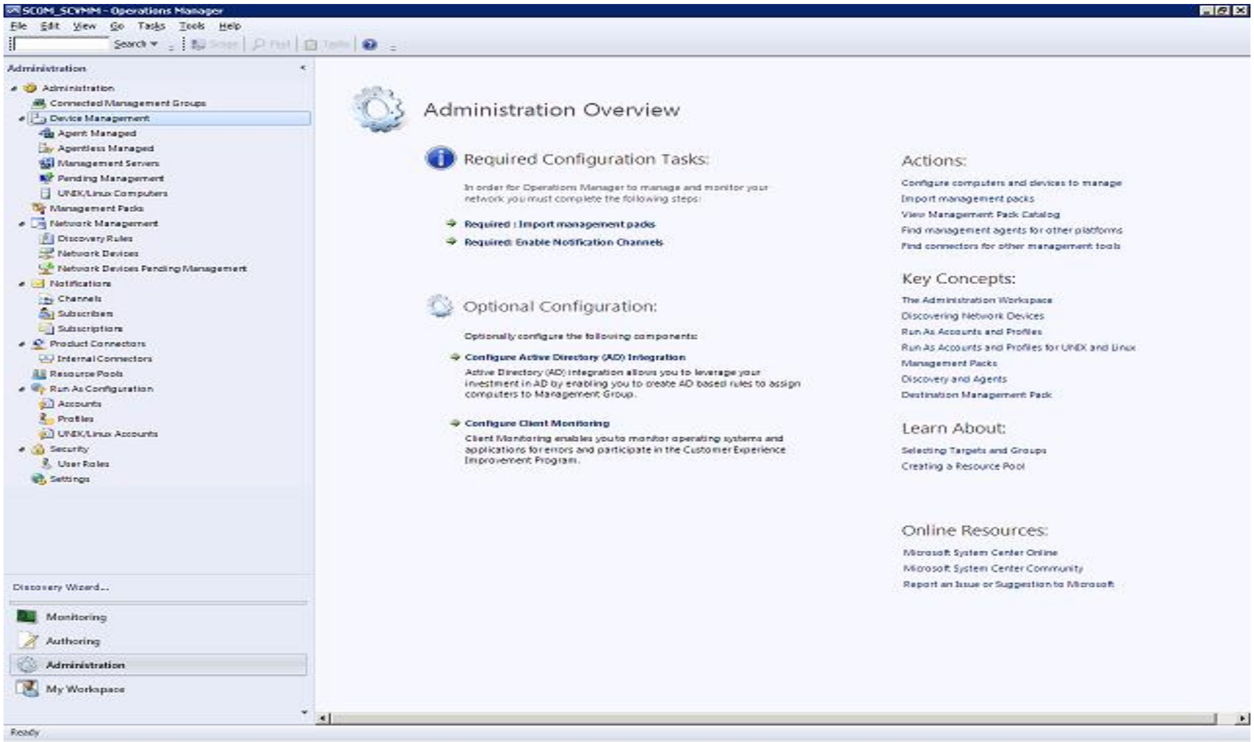
4.2.4 Importing Brocade FCHBA Management Pack

For instructions about importing a management pack, see How to Import an Operations Manager Management Pack in SCOM 2012 (http://technet.microsoft.com/en-us/library/hh212691.aspx).

For SCOM 2007/ 2007 R2, refer to the document "How to Import a Management Pack in Operations Manager 2007" (http://technet.microsoft.com/en-us/library/cc974494.aspx).

Use the following steps to install Management Pack in SCOM 2012:

1. Open the SCOM – Operations Console, and then select **Administration** in the left pane.



Administration Overview

Required Configuration Tasks:

In order for Operations Manager to manage and monitor your network you must complete the following steps:

- Required : Import management packs
- Required: Enable Notification Channels

Optional Configuration:

Optionally configure the following components:

- Configure Active Directory (AD) Integration

  Active Directory (AD) integration allows you to leverage your investment in AD by enabling you to create AD based rules to assign computers to Management Group.

- Configure Client Monitoring

  Client Monitoring enables you to monitor operating systems and applications for errors and participate in the Customer Experience Improvement Program.

Actions:

Configure computers and devices to manage
Import management packs
View Management Pack Catalog
Find management agents for other platforms
Find connectors for other management tools

Key Concepts:

The Administration Workspace
Discovering Network Devices
Run As Accounts and Profiles
Run As Accounts and Profiles for UNIX and Linux
Management Packs
Discovery and Agents
Destination Management Pack

Learn About:

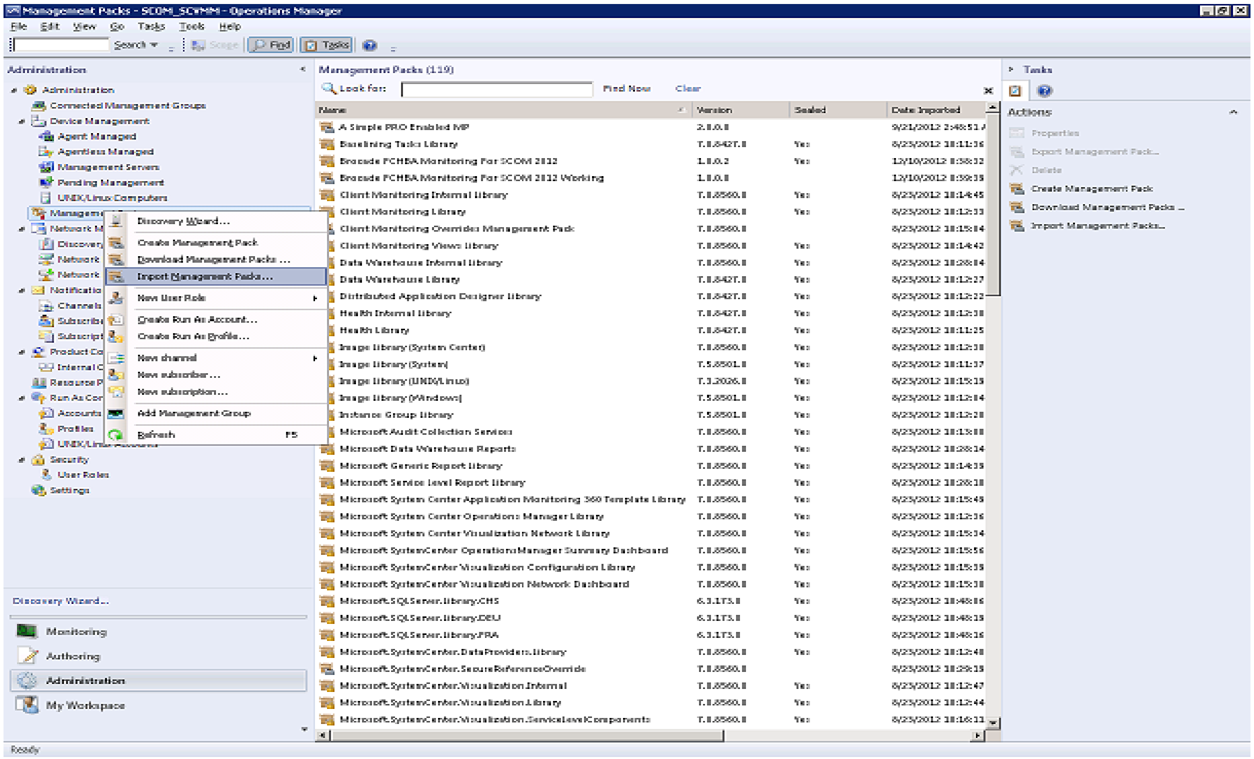
Selecting Targets and Groups
Creating a Resource Pool

Online Resources:

Microsoft System Center Online
Microsoft System Center Community
Report an Issue or Suggestion to Microsoft

Figure 19 – Importing Management Pack in SCOM Console – Step 1

2. Right-click the Management Pack's node, and then select "Import Management Packs" to import the Management Packs.

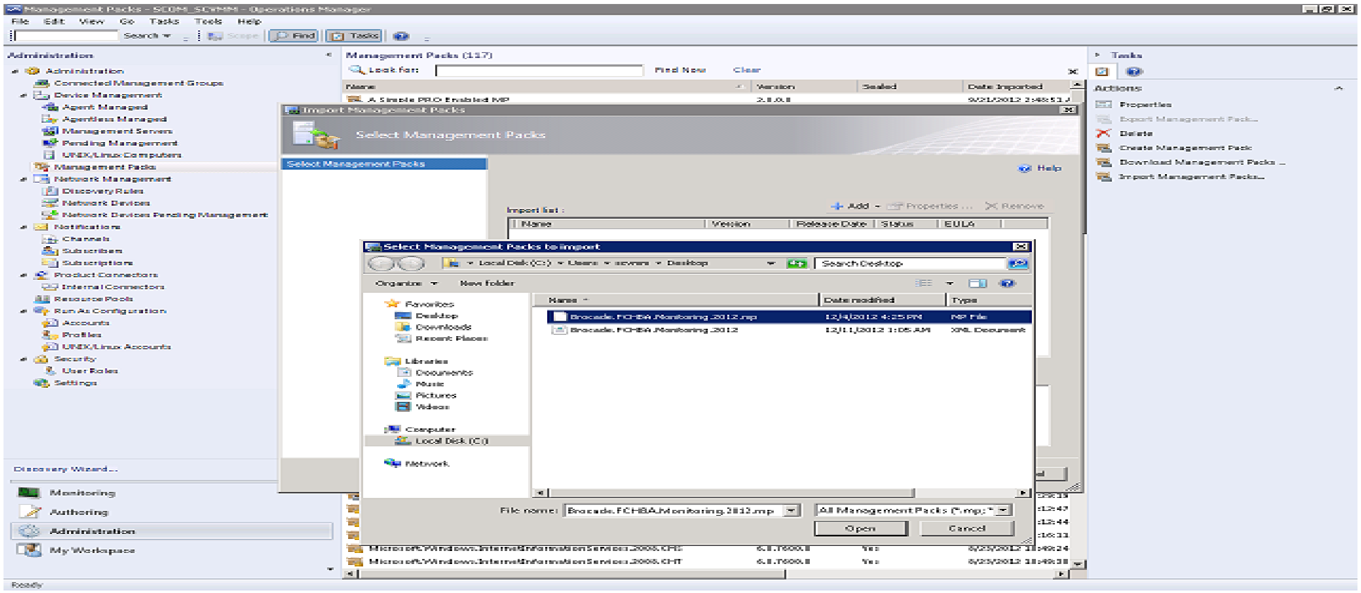


Management Packs (119)

Name	Version	Sealed	Date Imported
A Simple PRO Enabled MP	2.0.0.0		9/21/2012 2:48:51 A
Baselining Tasks Library	7.0.8427.0	Yes	8/23/2012 10:11:36
Brocade FCHBA Monitoring For SCOM 2012	1.0.0.2	Yes	12/10/2012 8:58:32
Brocade FCHBA Monitoring For SCOM 2012 Working	1.0.0.0		12/10/2012 8:59:35
Client Monitoring Internal Library	7.0.8560.0	Yes	8/23/2012 10:14:45
Client Monitoring Library	7.0.8560.0	Yes	8/23/2012 10:12:33
Client Monitoring Overrides Management Pack	7.0.8560.0		8/23/2012 10:15:04
Client Monitoring Views Library	7.0.8560.0	Yes	8/23/2012 10:14:42
Data Warehouse Internal Library	7.0.8560.0	Yes	8/23/2012 10:28:04
Data Warehouse Library	7.0.8427.0	Yes	8/23/2012 10:12:27
Distributed Application Designer Library	7.0.8427.0	Yes	8/23/2012 10:12:22
Health Internal Library	7.0.8427.0	Yes	8/23/2012 10:12:38
Health Library	7.0.8427.0	Yes	8/23/2012 10:11:25
Image Library (System Center)	7.0.8560.0	Yes	8/23/2012 10:12:38
Image Library (System)	7.5.8501.0	Yes	8/23/2012 10:11:37
Image Library (UNIX/Linux)	7.3.2026.0	Yes	8/23/2012 10:15:15
Image Library (Windows)	7.5.8501.0	Yes	8/23/2012 10:12:04
Instance Group Library	7.5.8501.0	Yes	8/23/2012 10:12:28
Microsoft Audit Collection Services	7.0.8560.0	Yes	8/23/2012 10:13:00
Microsoft Data Warehouse Reports	7.0.8560.0	Yes	8/23/2012 10:28:14
Microsoft Generic Report Library	7.0.8560.0	Yes	8/23/2012 10:14:35
Microsoft Service Level Report Library	7.0.8560.0	Yes	8/23/2012 10:28:18
Microsoft System Center Application Monitoring 360 Template Library	7.0.8560.0	Yes	8/23/2012 10:15:45
Microsoft System Center Operations Manager Library	7.0.8560.0	Yes	8/23/2012 10:12:36
Microsoft System Center Visualization Network Library	7.0.8560.0	Yes	8/23/2012 10:15:34
Microsoft SystemCenter OperationsManager Summary Dashboard	7.0.8560.0	Yes	8/23/2012 10:15:56
Microsoft SystemCenter Visualization Configuration Library	7.0.8560.0	Yes	8/23/2012 10:15:35
Microsoft SystemCenter Visualization Network Dashboard	7.0.8560.0	Yes	8/23/2012 10:15:38
Microsoft.SQLServer.Library.CHS	6.3.173.0	Yes	8/23/2012 10:48:06
Microsoft.SQLServer.Library.DEU	6.3.173.0	Yes	8/23/2012 10:48:15
Microsoft.SQLServer.Library.FRA	6.3.173.0	Yes	8/23/2012 10:48:16
Microsoft.SystemCenter.DataProviders.Library	7.0.8560.0	Yes	8/23/2012 10:12:48
Microsoft.SystemCenter.SecureReferenceOverride	7.0.8560.0		8/23/2012 10:29:15
Microsoft.SystemCenter.Visualization.Internal	7.0.8560.0	Yes	8/23/2012 10:12:47
Microsoft.SystemCenter.Visualization.Library	7.0.8560.0	Yes	8/23/2012 10:12:44
Microsoft.SystemCenter.Visualization.ServiceLevelComponents	7.0.8560.0	Yes	8/23/2012 10:16:11

Figure 20 – Importing Management Pack in SCOM Console – Step 2

3. Select the Management pack.



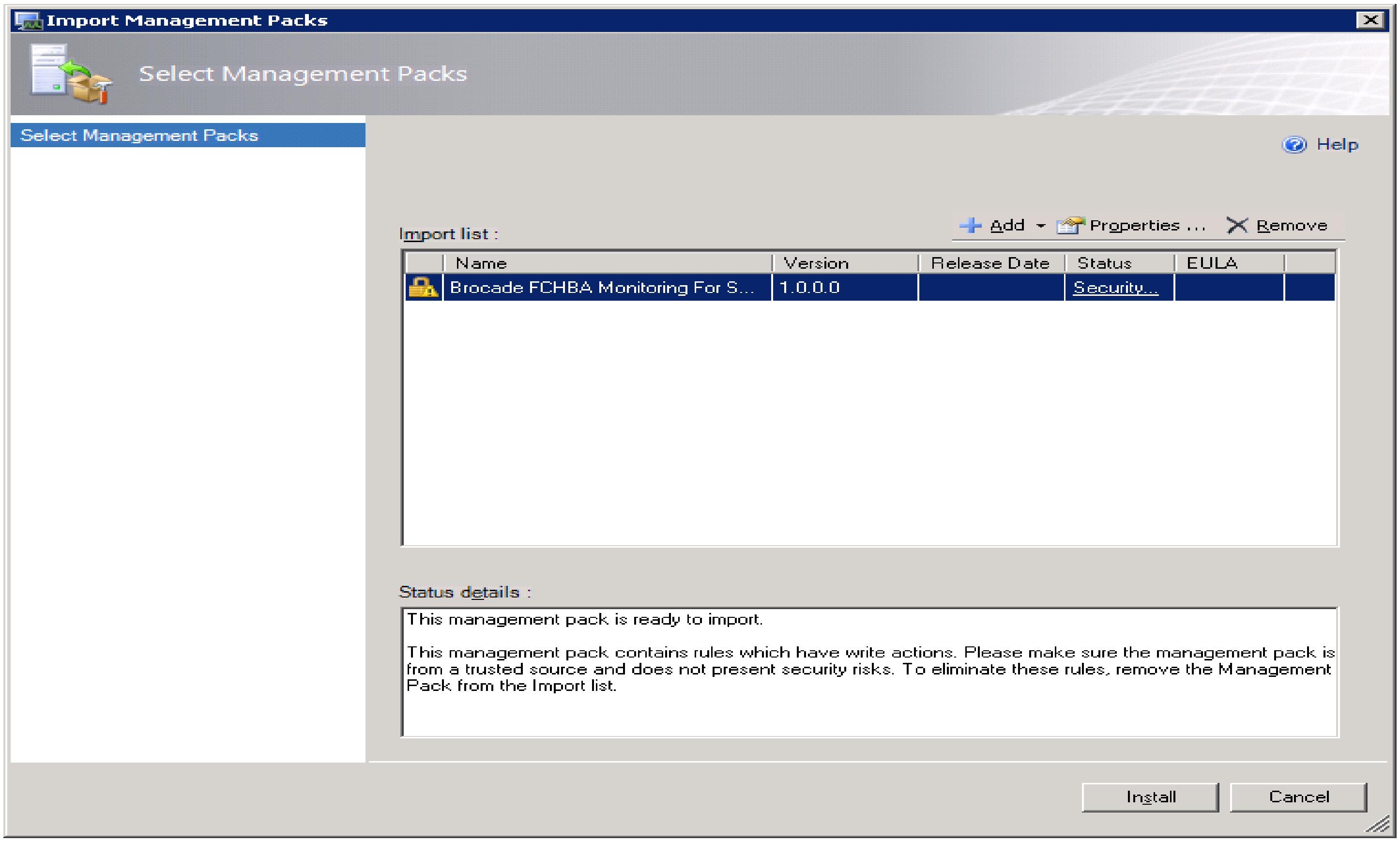
Name	Date modified	Type
Brocade.FCHBA.Monitoring.2012.mp	12/4/2012 4:25 PM	MP File
Brocade.FCHBA.Monitoring.2012	12/11/2012 1:05 AM	XML Document

File name: Brocade.FCHBA.Monitoring.2012.mp

All Management Packs (*.mp;*

Figure 21 – Importing Management Pack in SCOM Console – Step 3

4. Import the Management Pack.



Import list :

Name	Version	Release Date	Status	EULA
Brocade FCHBA Monitoring For S...	1.0.0.0		Security...	

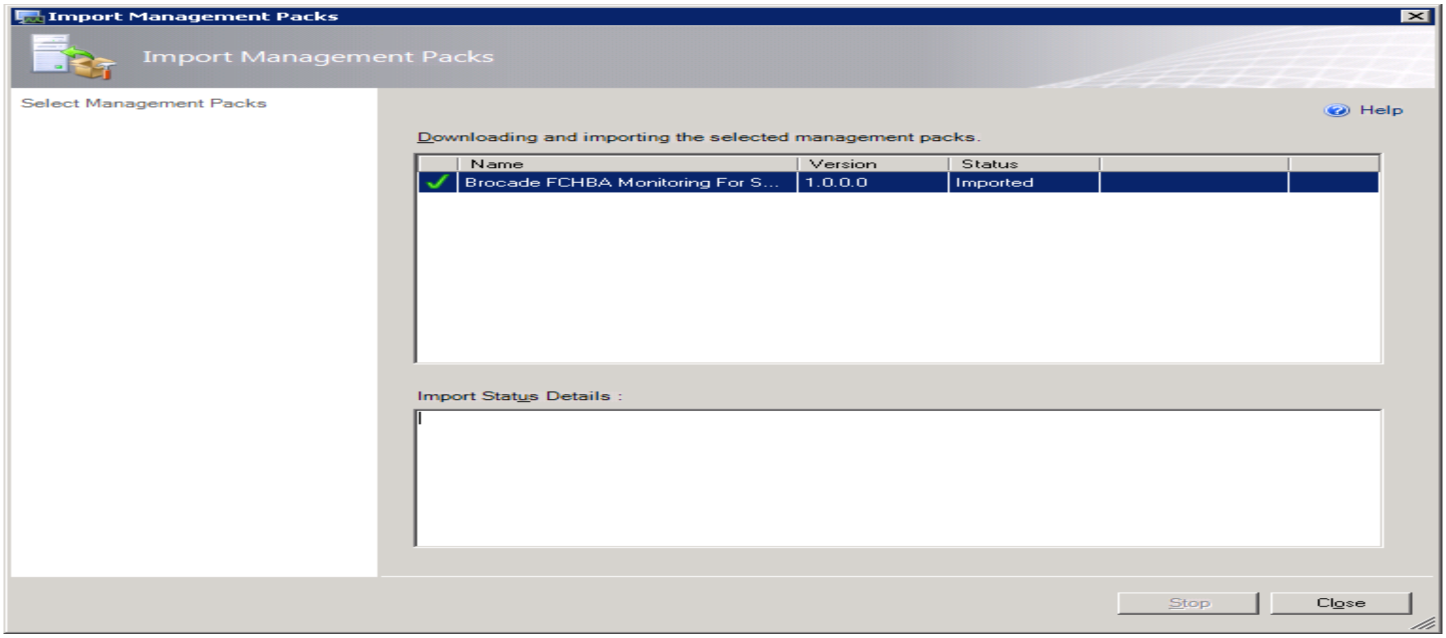
Status details :

This management pack is ready to import.

This management pack contains rules which have write actions. Please make sure the management pack is from a trusted source and does not present security risks. To eliminate these rules, remove the Management Pack from the Import list.

Figure 22 – Importing Management Pack in SCOM Console – Step 4

5. Once the import is successful, click **Close**.

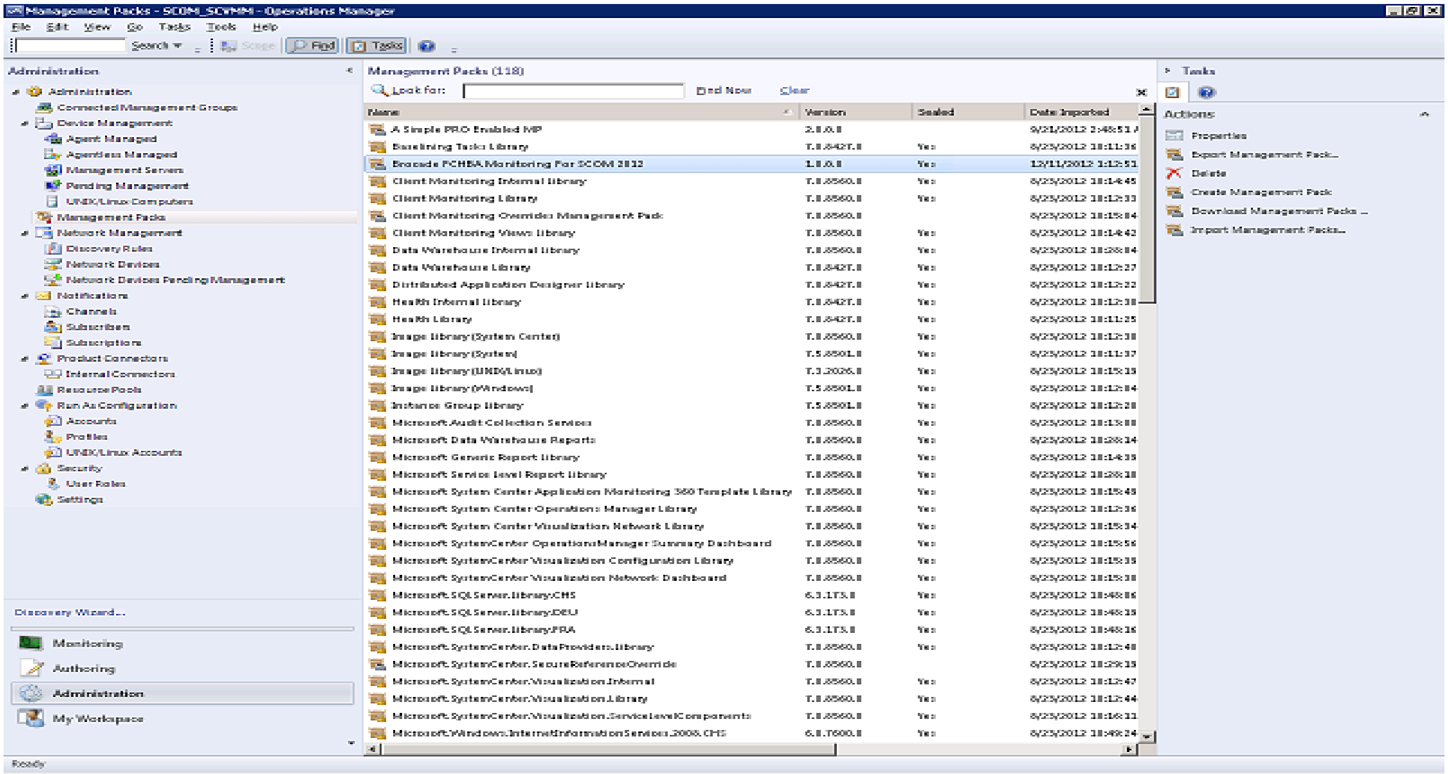


Downloading and importing the selected management packs.

Name	Version	Status
✓ Brocade FCHBA Monitoring For S...	1.0.0.0	Imported

Import Status Details :

Figure 23 – Importing Management Pack in SCOM Console – Step 5



Management Packs (118)

Name	Version	Sealed	Date Imported
A Simple PRO Enabled MP	2.0.0.0		9/21/2012 2:48:51 A
Baselining Tasks Library	7.0.8427.0	Yes	8/23/2012 10:11:36
Brocade FCHBA Monitoring For SCOM 2012	1.0.0.0	Yes	12/11/2012 1:12:51
Client Monitoring Internal Library	7.0.8560.0	Yes	8/23/2012 10:14:45
Client Monitoring Library	7.0.8560.0	Yes	8/23/2012 10:12:33
Client Monitoring Overrides Management Pack	7.0.8560.0		8/23/2012 10:15:04
Client Monitoring Views Library	7.0.8560.0	Yes	8/23/2012 10:14:42
Data Warehouse Internal Library	7.0.8560.0	Yes	8/23/2012 10:20:04
Data Warehouse Library	7.0.8427.0	Yes	8/23/2012 10:12:27
Distributed Application Designer Library	7.0.8427.0	Yes	8/23/2012 10:12:22
Health Internal Library	7.0.8427.0	Yes	8/23/2012 10:12:30
Health Library	7.0.8427.0	Yes	8/23/2012 10:11:25
Image Library (System Center)	7.0.8560.0	Yes	8/23/2012 10:12:30
Image Library (System)	7.5.8501.0	Yes	8/23/2012 10:11:37
Image Library (UNIX/Linux)	7.3.2026.0	Yes	8/23/2012 10:15:35
Image Library (Windows)	7.5.8501.0	Yes	8/23/2012 10:12:04
Instance Group Library	7.5.8501.0	Yes	8/23/2012 10:12:20
Microsoft Audit Collection Services	7.0.8560.0	Yes	8/23/2012 10:13:00
Microsoft Data Warehouse Reports	7.0.8560.0	Yes	8/23/2012 10:20:34
Microsoft Generic Report Library	7.0.8560.0	Yes	8/23/2012 10:14:35
Microsoft Service Level Report Library	7.0.8560.0	Yes	8/23/2012 10:20:30
Microsoft System Center Application Monitoring 360 Template Library	7.0.8560.0	Yes	8/23/2012 10:15:48
Microsoft System Center Operations Manager Library	7.0.8560.0	Yes	8/23/2012 10:12:36
Microsoft System Center Visualization Network Library	7.0.8560.0	Yes	8/23/2012 10:15:34
Microsoft SystemCenter OperationsManager Summary Dashboard	7.0.8560.0	Yes	8/23/2012 10:15:56
Microsoft SystemCenter Visualization Configuration Library	7.0.8560.0	Yes	8/23/2012 10:15:35
Microsoft SystemCenter Visualization Network Dashboard	7.0.8560.0	Yes	8/23/2012 10:15:30
Microsoft.SQLServer.Library.CHS	6.3.173.0	Yes	8/23/2012 10:48:06
Microsoft.SQLServer.Library.DEU	6.3.173.0	Yes	8/23/2012 10:48:15
Microsoft.SQLServer.Library.FRA	6.3.173.0	Yes	8/23/2012 10:48:16
Microsoft.SystemCenter.DataProviders.Library	7.0.8560.0	Yes	8/23/2012 10:12:48
Microsoft.SystemCenter.SecureReferenceOverride	7.0.8560.0		8/23/2012 10:29:15
Microsoft.SystemCenter.Visualization.Internal	7.0.8560.0	Yes	8/23/2012 10:12:47
Microsoft.SystemCenter.Visualization.Library	7.0.8560.0	Yes	8/23/2012 10:12:44
Microsoft.SystemCenter.Visualization.ServiceLevelComponents	7.0.8560.0	Yes	8/23/2012 10:16:11
Microsoft.Windows.InternetInformationServices.2008.CHS	6.0.7600.0	Yes	8/23/2012 10:49:24

Figure 24 – Imported Brocade FCHBA Management Pack in SCOM Console

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

4.2.5 Create 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 in the management pack file. However, you can create customizations, such as overrides or new monitoring objects, and save them to a different management pack. By default, Operations Manager 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 that 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.
- You can delete the original management pack without deleting 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 made to individual management packs.

Please see the section on Tuning Performance Threshold Rules for the default threshold values in use in the management pack and procedures to override the default values on a per port basis or for all ports (by overriding the monitor for the port type).

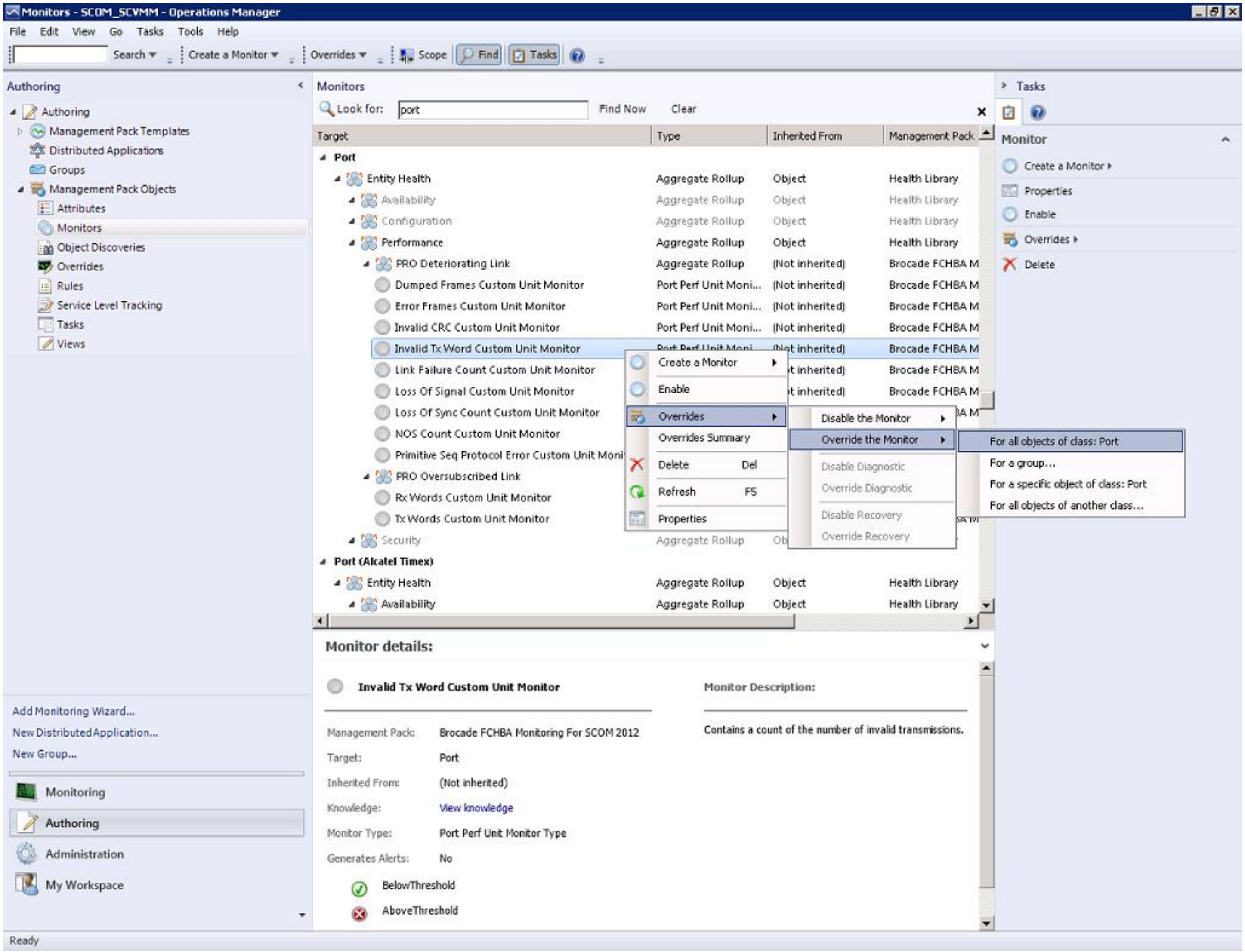
4.2.6 Tuning Performance Threshold Rules

The following table lists performance threshold rules with default thresholds that might require additional tuning to suit your environment. You should evaluate these rules to determine whether the default thresholds are appropriate for your environment. 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 default thresholds, perform the following steps:

1. Select the **Authoring** node in the operation console, and then select Brocade.FCHBA.Monitoring.Port monitor and expand it. As shown in the following figure, select **Entity Health**, expand the tree under **Performance**, and then right-click the monitor for which you want to change the threshold.



Target	Type	Inherited From	Management Pack
Port			
Entity Health	Aggregate Rollup	Object	Health Library
Availability	Aggregate Rollup	Object	Health Library
Configuration	Aggregate Rollup	Object	Health Library
Performance	Aggregate Rollup	Object	Health Library
PRO Deteriorating Link	Aggregate Rollup	(Not inherited)	Brocade FCHBA M
Dumped Frames Custom Unit Monitor	Port Perf Unit Moni...	(Not inherited)	Brocade FCHBA M
Error Frames Custom Unit Monitor	Port Perf Unit Moni...	(Not inherited)	Brocade FCHBA M
Invalid CRC Custom Unit Monitor	Port Perf Unit Moni...	(Not inherited)	Brocade FCHBA M
Invalid Tx Word Custom Unit Monitor	Port Perf Unit Moni...	(Not inherited)	Brocade FCHBA M
Link Failure Count Custom Unit Monitor		t inherited)	Brocade FCHBA M
Loss Of Signal Custom Unit Monitor		t inherited)	Brocade FCHBA M
Loss Of Sync Count Custom Unit Monitor			A M
NOS Count Custom Unit Monitor			
Primitive Seq Protocol Error Custom Unit Moni			
PRO Oversubscribed Link			
Rx Words Custom Unit Monitor			
Tx Words Custom Unit Monitor			A M
Security	Aggregate Rollup	Ob	
Port (Alcatel Timex)			
Entity Health	Aggregate Rollup	Object	Health Library
Availability	Aggregate Rollup	Object	Health Library

Monitor details:

Invalid Tx Word Custom Unit Monitor

Management Pack: Brocade FCHBA Monitoring For SCOM 2012
Target: Port
Inherited From: (Not inherited)
Knowledge: View knowledge
Monitor Type: Port Perf Unit Monitor Type
Generates Alerts: No

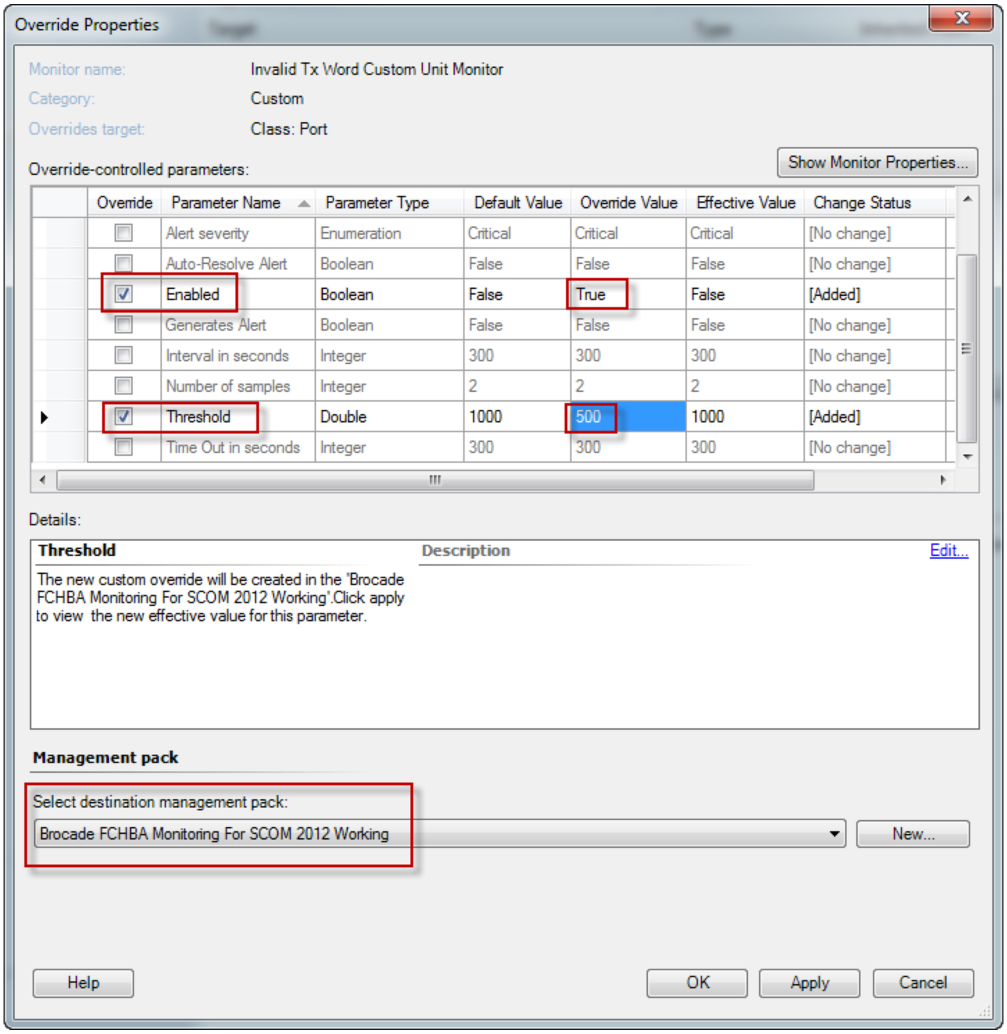
BelowThreshold
AboveThreshold

Monitor Description:

Contains a count of the number of invalid transmissions.

Figure 25 – Overriding the threshold for a monitor

2. Select **Overrides→ Override the Monitor → for All Objects of type** from the popup window.
3. Select the property that you want to change from the port **Override Properties** dialog box, and then provide the new value in the Override Setting column
4. Select the Enforced check box to override the default values.
   - Override "**Enabled**" to "True" for all unit monitors.
   - Override the "**Threshold**" value to the desired threshold value.
5. Select the destination management pack to save the overridden changes in.
6. Click **OK** to save the changes.



Monitor name: Invalid Tx Word Custom Unit Monitor

Category: Custom

Overrides target: Class: Port

Override-controlled parameters:

Override	Parameter Name	Parameter Type	Default Value	Override Value	Effective Value	Change Status
□	Alert severity	Enumeration	Critical	Critical	Critical	[No change]
□	Auto-Resolve Alert	Boolean	False	False	False	[No change]
☑	Enabled	Boolean	False	True	False	[Added]
□	Generates Alert	Boolean	False	False	False	[No change]
□	Interval in seconds	Integer	300	300	300	[No change]
□	Number of samples	Integer	2	2	2	[No change]
☑	Threshold	Double	1000	500	1000	[Added]
□	Time Out in seconds	Integer	300	300	300	[No change]

Details:

Threshold

The new custom override will be created in the 'Brocade FCHBA Monitoring For SCOM 2012 Working'.Click apply to view the new effective value for this parameter.

Description

Management pack

Select destination management pack: Brocade FCHBA Monitoring For SCOM 2012 Working

Figure 26 – Threshold value override

5 Understanding Management Pack Operations

The Brocade FCHBA Monitoring Management Pack (MP) discovers Hyper-V hosts with Brocade, QLogic, or Emulex HBA drivers installed. It then discovers the HBAs and HBA ports installed on the managed hosts.

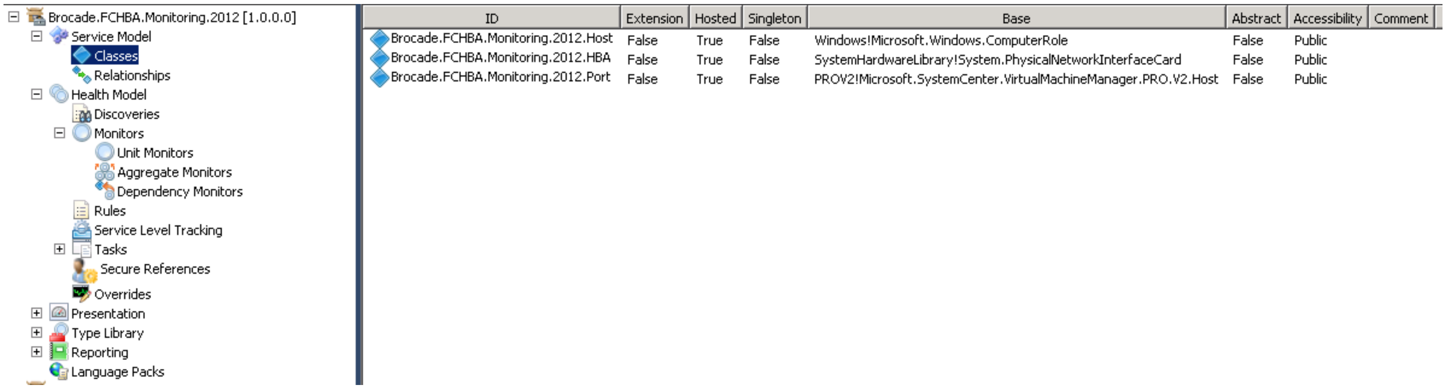
The MP also monitors the HBA port state by monitoring the port statistics counters, and then rolls up the state of port to the HBA and Host. MP also generates PRO tips targeted to the port class. The SCVMM administrator can view these in the PRO tip window and implement them or configure MP to implement them automatically. When a PRO tip is implemented, one or more VMs are migrated to another host.

The following descriptions are same for both 2012 and 2007 versions of Brocade FCHBA Monitoring management packs.

5.1 Classes

The following classes are defined in the service model:

- **Brocade.FCHBA.Monitoring.2012.Host** – This is the brocade driver application which is a **Microsoft.Windows.ComputerRole**.
- **Brocade.FCHBA.Monitoring.2012.HBA** – This is the Host Bus Adapter class which **is a** System.PhysicalNetworkInterfaceCard. This class is hosted by Brocade.FCHBA.Monitoring.2012.Host.
- **Brocade.FCHBA.Monitoring.2012.Port** – This is the Port class which is a Microsoft.SystemCenter.VirtualMachineManager.PRO.V2.Host. This class is contained by Brocade.FCHBA.Monitoring.2012.HBA.



ID	Extension	Hosted	Singleton	Base	Abstract	Accessibility	Comment
Brocade.FCHBA.Monitoring.2012.Host	False	True	False	Windows!Microsoft.Windows.ComputerRole	False	Public	
Brocade.FCHBA.Monitoring.2012.HBA	False	True	False	SystemHardwareLibrary!System.PhysicalNetworkInterfaceCard	False	Public	
Brocade.FCHBA.Monitoring.2012.Port	False	True	False	PROV2!Microsoft.SystemCenter.VirtualMachineManager.PRO.V2.Host	False	Public	

Figure 27 - Management Pack Service Model Classes

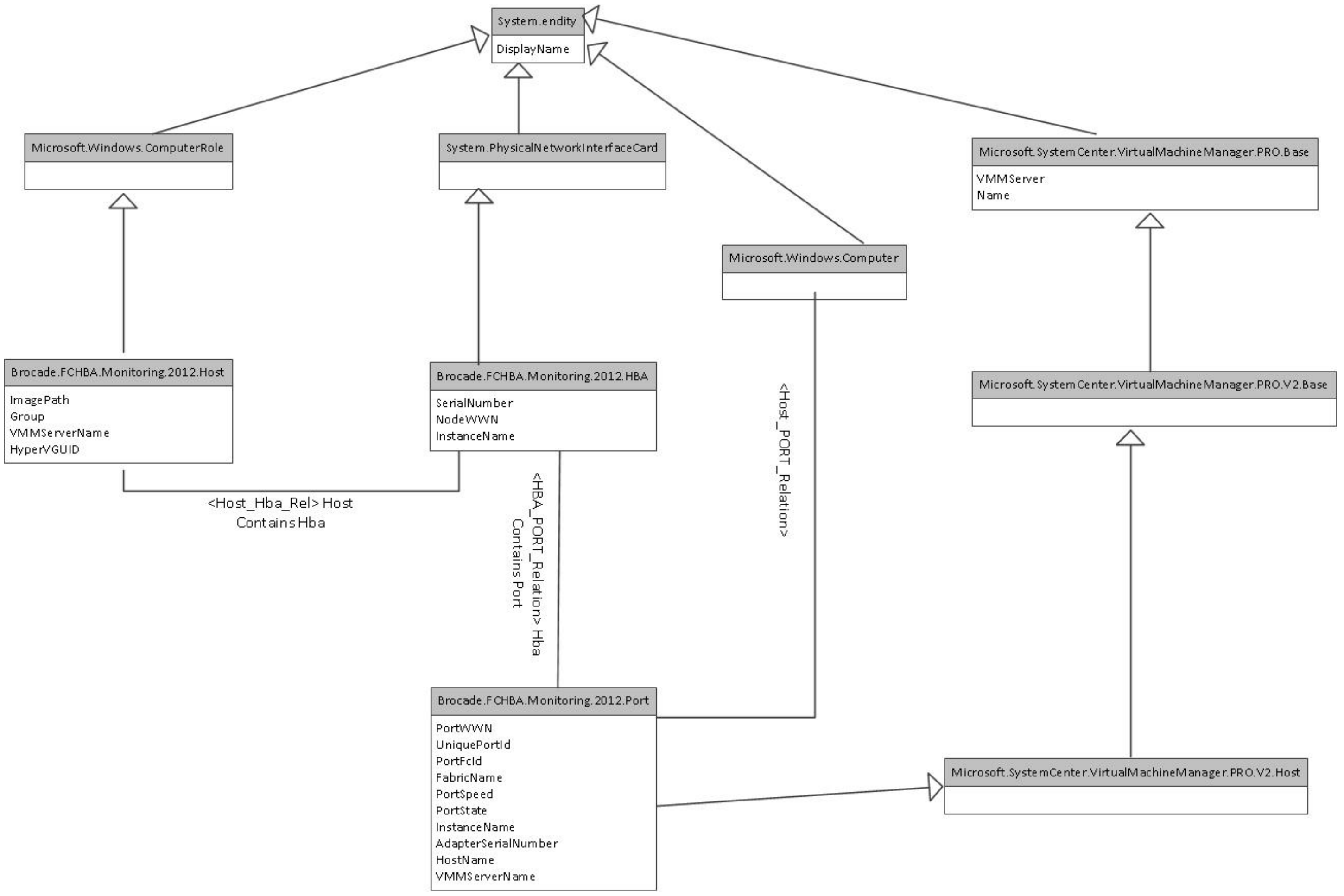

System.endity
DisplayName
Microsoft.Windows.ComputerRole
System.PhysicalNetworkInterfaceCard
Microsoft.SystemCenter.VirtualMachineManager.PRO.Base
VMMServer
Name
Microsoft.Windows.Computer
Brocade.FCHBA.Monitoring.2012.Host
ImagePath
Group
VMMServerName
HyperVGUID
Brocade.FCHBA.Monitoring.2012.HBA
SerialNumber
NodeWWN
InstanceName
Microsoft.SystemCenter.VirtualMachineManager.PRO.V2.Base
<Host_Hba_Rel> Host
Contains Hba
<HBA_PORT_Relation> Hba
Contains Port
<Host_PORT_Relation>
Brocade.FCHBA.Monitoring.2012.Port
PortWWN
UniquePortId
PortFcId
FabricName
PortSpeed
PortState
InstanceName
AdapterSerialNumber
HostName
VMMServerName
Microsoft.SystemCenter.VirtualMachineManager.PRO.V2.Host

Figure 28 – Class Diagram

Brocade.FCHBA.Monitoring.2012.Host class has the following properties:

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

Brocade.FCHBA.Monitoring.2012.HBA class has following properties:

- SerialNumber. Key property. This is serial number of adapter.
- NodeWWN
- 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.2012.Port class has following properties:

- PortWWN. Key property
- UniquePortId. GUID for port.
- PortFcId
- FabricName
- PortSpeed
- PortState
- InstanceName. Key property for WMI class MSFC_FibrePortHBAAttributes.
- AdapterSerialNumber
- HostName
- VMMServerName

The instance of this class is populated with WMI query to class MSFC_FibrePortHBAAttributes.

There are three types of relationships in SCOM:

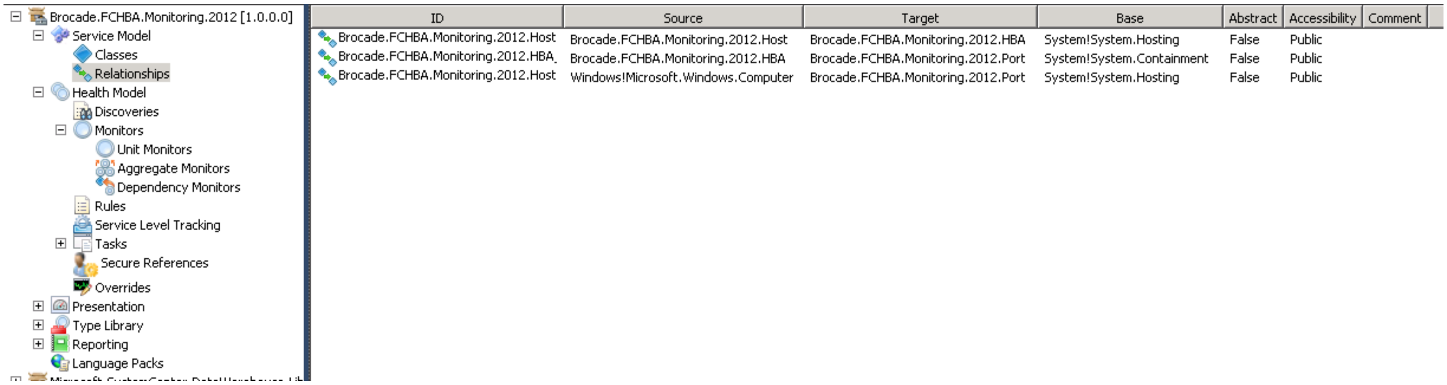
1. Hosting
2. Containment
3. Reference

Hosting is the most restrictive relationship. Hosting means that the hosted class instance can only exist within only one and not multiple class instances. Also, since the lifetime of the hosted class instance is same as the HBA class instance, an HBA class instance cannot co-exist in multiple Host instances, and if you remove the Host class instance, the hosted HBA instance is removed with it.

Containment is less restrictive and means that a contained class instance can also exist even when containing class is removed. For example, the Windows Server Group contains Windows Server. Windows server will not cease to exist if the Windows Group is removed.

Please refer to the SCOM Key Concepts document for details.

The following figure shows the source and target classes of the two relationships we have defined in the Brocade FCHBA MP.



ID	Source	Target	Base	Abstract	Accessibility	Comment
Brocade.FCHBA.Monitoring.2012.Host	Brocade.FCHBA.Monitoring.2012.Host	Brocade.FCHBA.Monitoring.2012.HBA	System!System.Hosting	False	Public	
Brocade.FCHBA.Monitoring.2012.HBA_	Brocade.FCHBA.Monitoring.2012.HBA	Brocade.FCHBA.Monitoring.2012.Port	System!System.Containment	False	Public	
Brocade.FCHBA.Monitoring.2012.Host	Windows!Microsoft.Windows.Computer	Brocade.FCHBA.Monitoring.2012.Port	System!System.Hosting	False	Public	

Figure 29 – Management Pack Service Model Relationships

5.2 Objects the Management Pack Discovers

This management Pack uses the following types of discovery:

- Registry based
- Script based

Registry based: this discovery 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 entries is available then, SCOM will detect it as ahost object.

1. **"HKLM\SYSTEM\CurrentControlSet\Services\bfad"** – for Brocade FCHBA Driver
2. **"HKLM\SYSTEM\CurrentControlSet\Services\ql2300"** – for QLogic 2300 FCHBA Driver
3. **"HKLM\SYSTEM\CurrentControlSet\Services\Elxstor**" – for Emulex FCHBA Driver

The registry entry will be created once Brocade, QLogic, and Emulex FC HBA drivers are installed.

Disclaimer: Very minimal testing has been done for QLogic and Emulex FC HBAs.

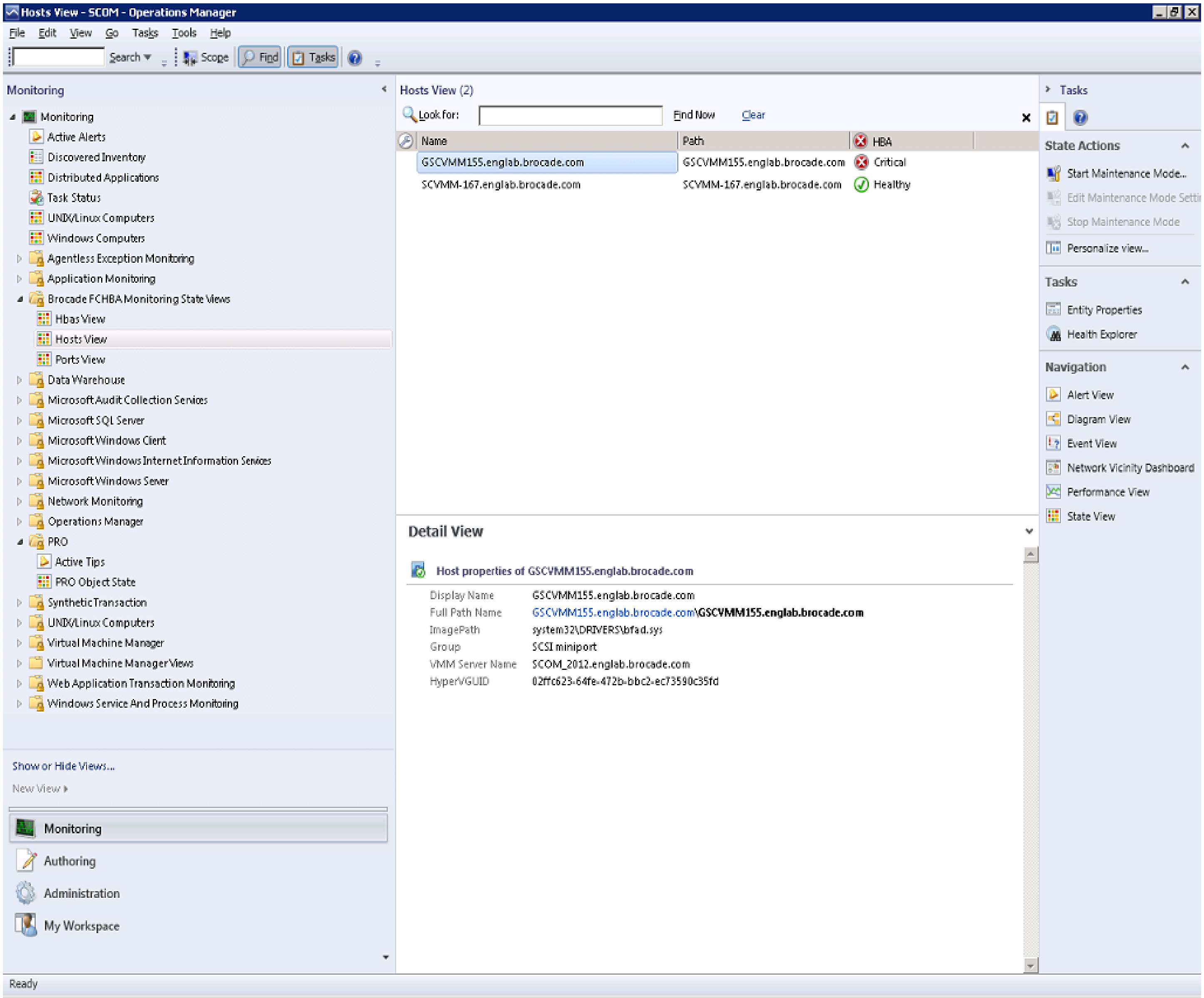
Script based: This discovers the HBAs and port information through a VB Script and create instances in the SCOM.

You can view the discovered Host, Brocade HBA, and ports in the monitoring tab. Host, HBA, and port discovery takes a few minutes once the management pack is installed.

In the Monitoring Tab the Brocade FCHBA Monitoring State Views directory displays the following three items:

- Hbas View
- Hosts View
- Ports View

Selecting Brocade FCHBA Monitoring State Views.HostsView will provide the Host information.



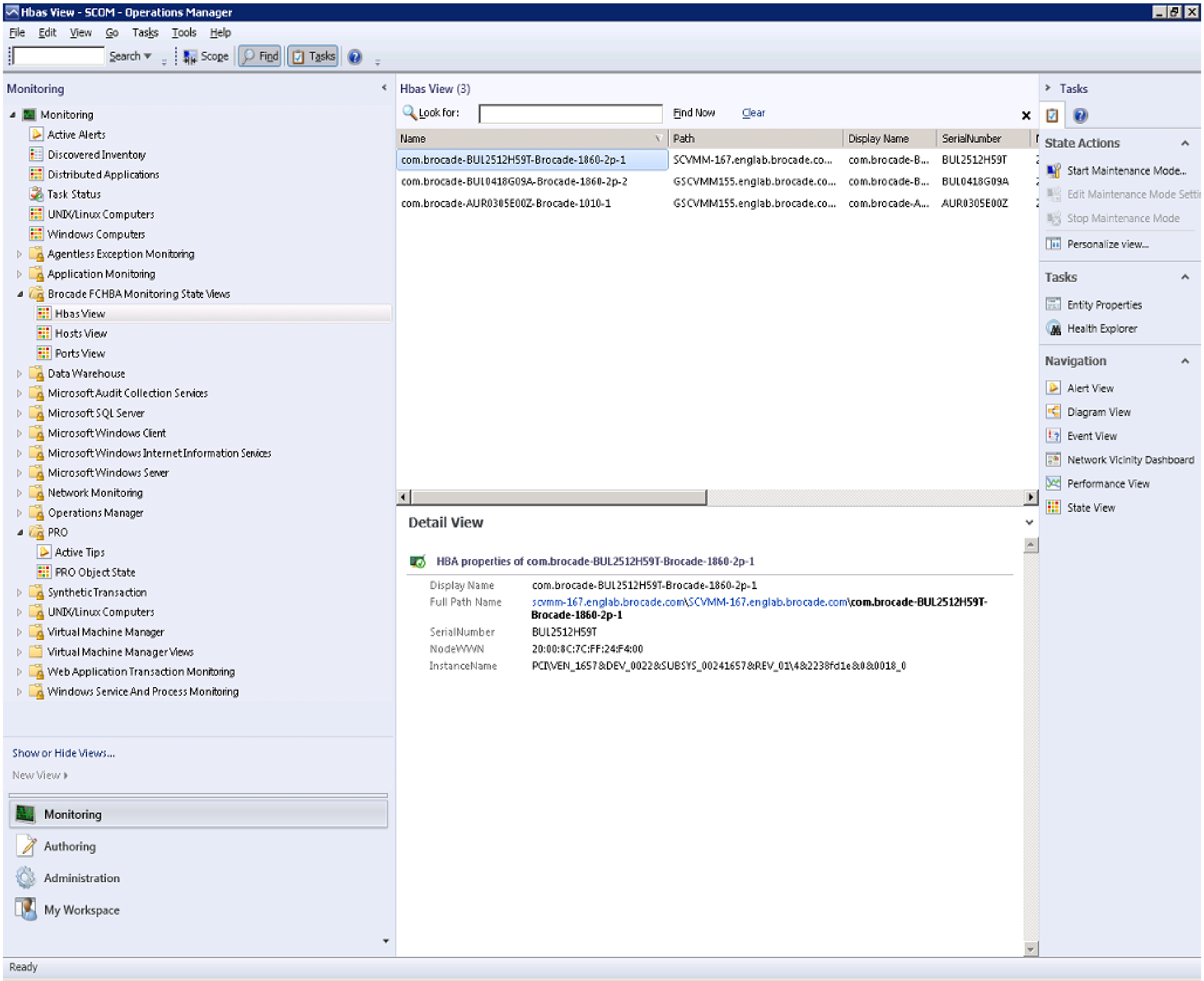
Name	Path	HBA
GSCVMM155.englab.brocade.com	GSCVMM155.englab.brocade.com	Critical
SCVMM-167.englab.brocade.com	SCVMM-167.englab.brocade.com	Healthy

Host properties of GSCVMM155.englab.brocade.com

Display Name	GSCVMM155.englab.brocade.com
Full Path Name	GSCVMM155.englab.brocade.com\GSCVMM155.englab.brocade.com
ImagePath	system32\DRIVERS\bfad.sys
Group	SCSI miniport
VMM Server Name	SCOM_2012.englab.brocade.com
HyperVGUID	02ffc623-64fe-472b-bbc2-ec73590c35fd

Figure 30 – Hosts View

Select the Hbas View to provide discovered HBA information.



Name	Path	Display Name	SerialNumber
com.brocade-BUL2512H59T-Brocade-1860-2p-1	SCVMM-167.englab.brocade.co...	com.brocade-B...	BUL2512H59T
com.brocade-BUL0418G09A-Brocade-1860-2p-2	GSCVMM155.englab.brocade.co...	com.brocade-B...	BUL0418G09A
com.brocade-AUR0305E00Z-Brocade-1010-1	GSCVMM155.englab.brocade.co...	com.brocade-A...	AUR0305E00Z

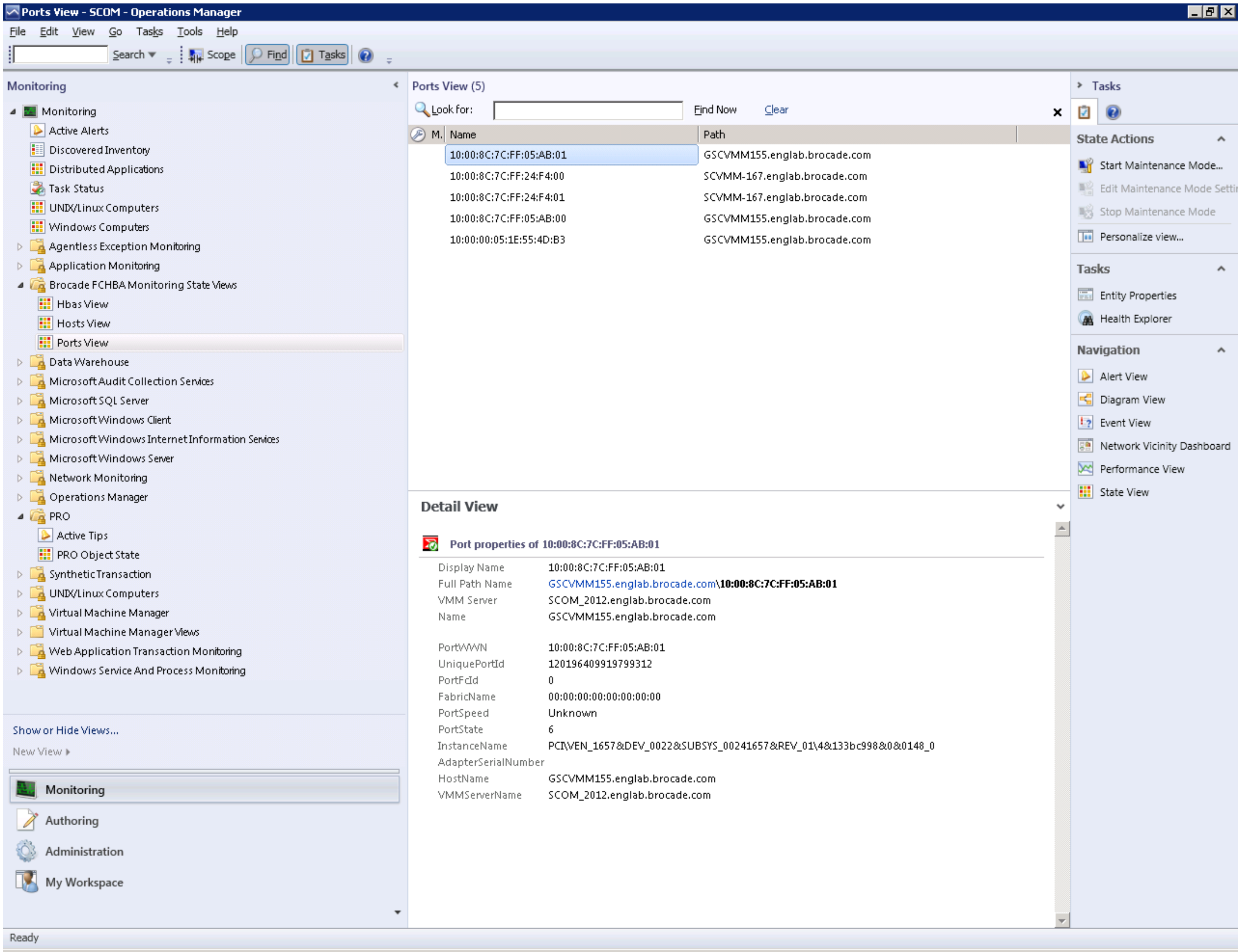
Detail View

HBA properties of com.brocade-BUL2512H59T-Brocade-1860-2p-1

Display Name	com.brocade-BUL2512H59T-Brocade-1860-2p-1
Full Path Name	scvmm-167.englab.brocade.com\SCVMM-167.englab.brocade.com\com.brocade-BUL2512H59T-Brocade-1860-2p-1
SerialNumber	BUL2512H59T
NodeWWN	20:00:8C:7C:FF:24:F4:00
InstanceName	PCI\VEN_1657&DEV_0022&SUBSYS_00241657&REV_01\4&2238fd1e&0&0018_0

Figure 31 – HBAs View

Select the Ports View to view the discovered HBA port information.



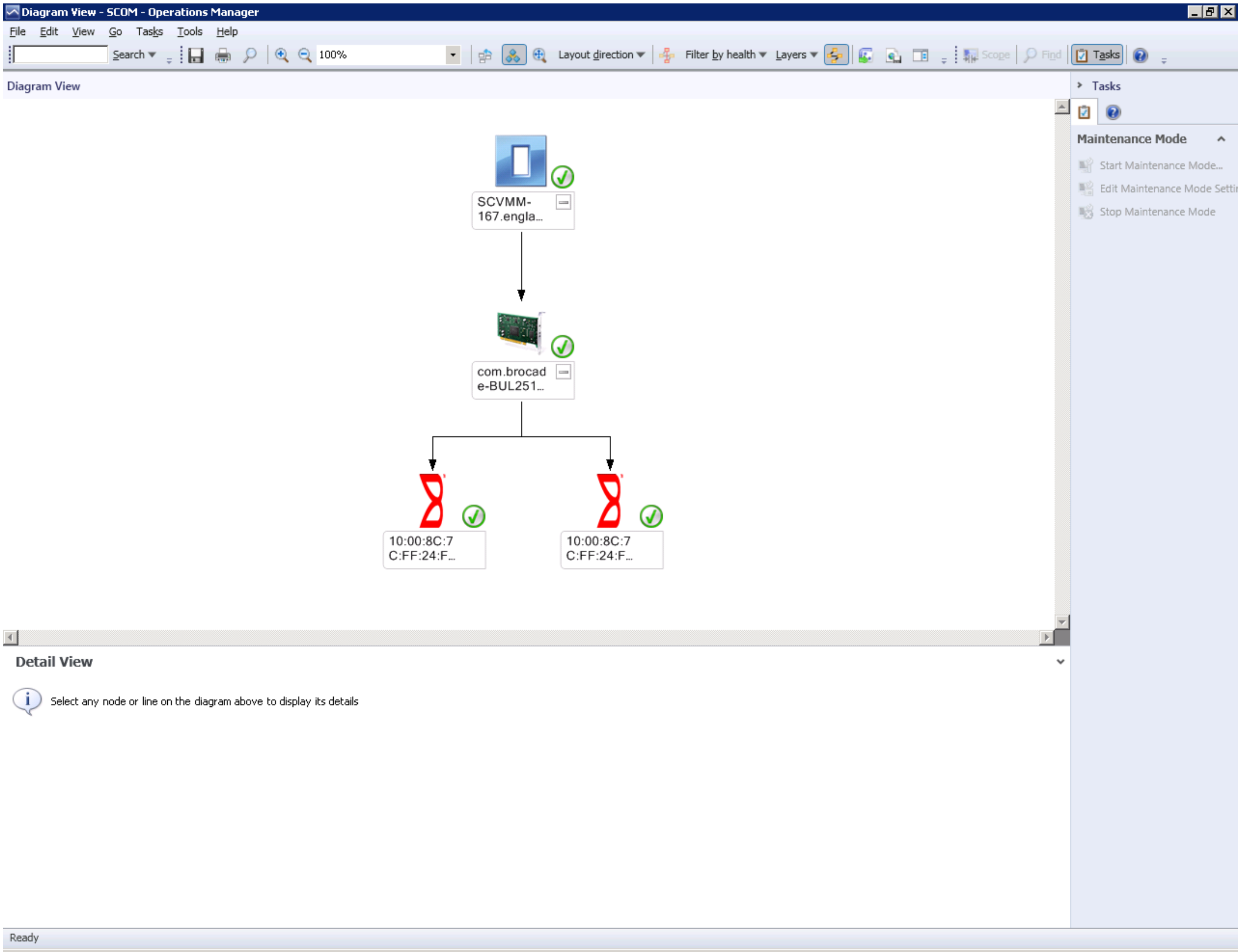
M.	Name	Path
	10:00:8C:7C:FF:05:AB:01	GSCVMM155.englab.brocade.com
	10:00:8C:7C:FF:24:F4:00	SCVMM-167.englab.brocade.com
	10:00:8C:7C:FF:24:F4:01	SCVMM-167.englab.brocade.com
	10:00:8C:7C:FF:05:AB:00	GSCVMM155.englab.brocade.com
	10:00:00:05:1E:55:4D:B3	GSCVMM155.englab.brocade.com

Port properties of 10:00:8C:7C:FF:05:AB:01

Display Name	10:00:8C:7C:FF:05:AB:01
Full Path Name	GSCVMM155.englab.brocade.com**10:00:8C:7C:FF:05:AB:01**
VMM Server	SCOM_2012.englab.brocade.com
Name	GSCVMM155.englab.brocade.com
PortWWN	10:00:8C:7C:FF:05:AB:01
UniquePortId	120196409919799312
PortFcId	0
FabricName	00:00:00:00:00:00:00:00
PortSpeed	Unknown
PortState	6
InstanceName	PCI\VEN_1657&DEV_0022&SUBSYS_00241657&REV_01\4&133bc998&0&0148_0
AdapterSerialNumber	
HostName	GSCVMM155.englab.brocade.com
VMMServerName	SCOM_2012.englab.brocade.com

Figure 32 – Ports View

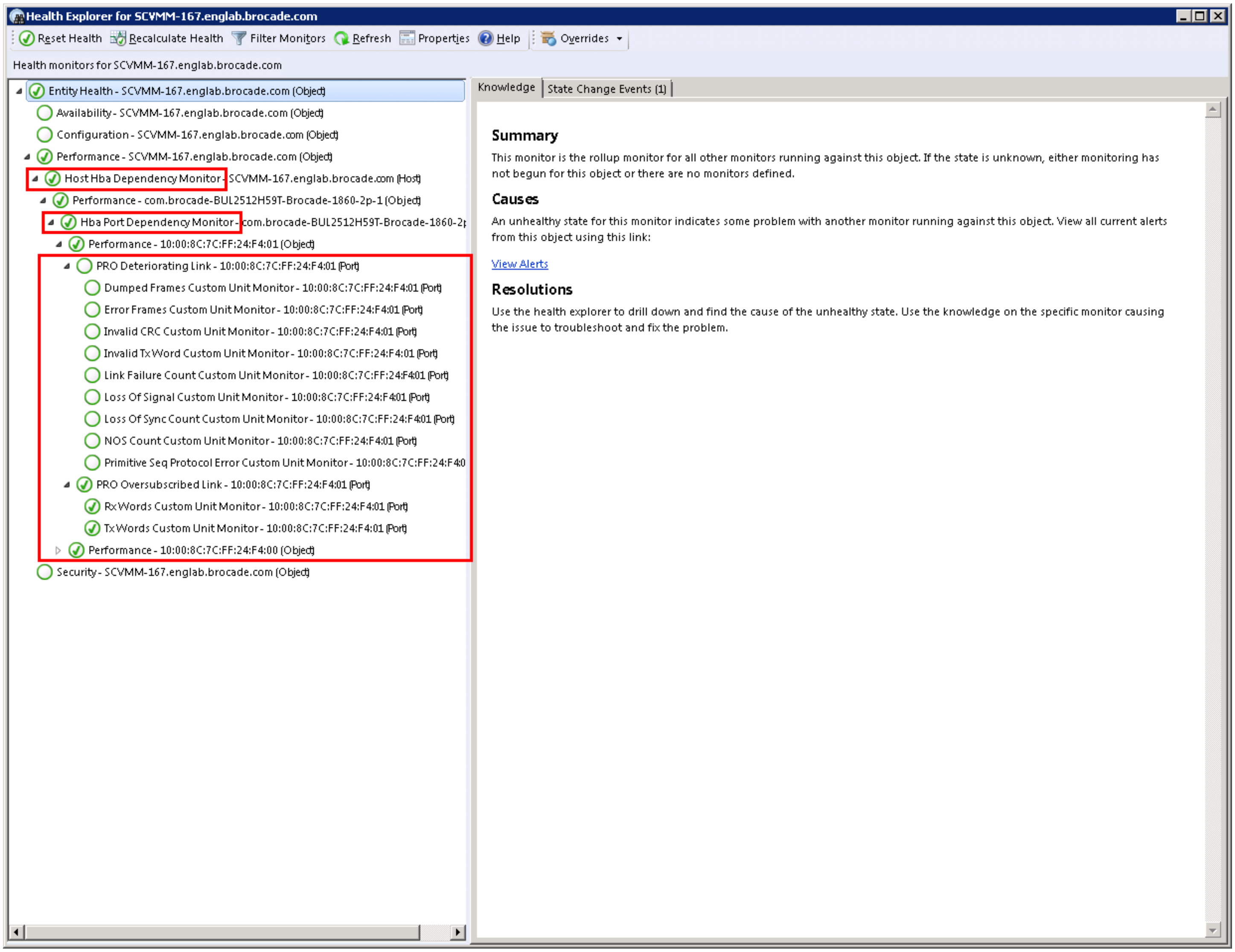
Right-click on the Host, HBA, or Port and display the Diagram view.



Select any node or line on the diagram above to display its details

Figure 33 – Host, HBAs and Ports seen in Host Level Diagram View

To view the health explorer of a host, right-click a host from the Hosts view and select open>health explore. The following window displays, showing the health state of the host, HBAs on the host, and the ports on the HBAs.



Health Explorer for SCVMM-167.englab.brocade.com

Health monitors for SCVMM-167.englab.brocade.com

- ✓ Entity Health - SCVMM-167.englab.brocade.com (Object)
  - ○ Availability - SCVMM-167.englab.brocade.com (Object)
  - ○ Configuration - SCVMM-167.englab.brocade.com (Object)
  - ✓ Performance - SCVMM-167.englab.brocade.com (Object)
    - ✓ Host Hba Dependency Monitor - SCVMM-167.englab.brocade.com (Host)
      - ✓ Performance - com.brocade-BUL2512H59T-Brocade-1860-2p-1 (Object)
        - ✓ Hba Port Dependency Monitor - com.brocade-BUL2512H59T-Brocade-1860-2
          - ✓ Performance - 10:00:8C:7C:FF:24:F4:01 (Object)
            - ○ PRO Deteriorating Link - 10:00:8C:7C:FF:24:F4:01 (Port)
              - ○ Dumped Frames Custom Unit Monitor - 10:00:8C:7C:FF:24:F4:01 (Port)
              - ○ Error Frames Custom Unit Monitor - 10:00:8C:7C:FF:24:F4:01 (Port)
              - ○ Invalid CRC Custom Unit Monitor - 10:00:8C:7C:FF:24:F4:01 (Port)
              - ○ Invalid Tx Word Custom Unit Monitor - 10:00:8C:7C:FF:24:F4:01 (Port)
              - ○ Link Failure Count Custom Unit Monitor - 10:00:8C:7C:FF:24:F4:01 (Port)
              - ○ Loss Of Signal Custom Unit Monitor - 10:00:8C:7C:FF:24:F4:01 (Port)
              - ○ Loss Of Sync Count Custom Unit Monitor - 10:00:8C:7C:FF:24:F4:01 (Port)
              - ○ NOS Count Custom Unit Monitor - 10:00:8C:7C:FF:24:F4:01 (Port)
              - ○ Primitive Seq Protocol Error Custom Unit Monitor - 10:00:8C:7C:FF:24:F4:0
            - ✓ PRO Oversubscribed Link - 10:00:8C:7C:FF:24:F4:01 (Port)
              - ✓ Rx Words Custom Unit Monitor - 10:00:8C:7C:FF:24:F4:01 (Port)
              - ✓ Tx Words Custom Unit Monitor - 10:00:8C:7C:FF:24:F4:01 (Port)
          - ✓ Performance - 10:00:8C:7C:FF:24:F4:00 (Object)
  - ○ Security - SCVMM-167.englab.brocade.com (Object)

Knowledge | State Change Events (1)

Summary

This monitor is the rollup monitor for all other monitors running against this object. If the state is unknown, either monitoring has not begun for this object or there are no monitors defined.

Causes

An unhealthy state for this monitor indicates some problem with another monitor running against this object. View all current alerts from this object using this link:

View Alerts

Resolutions

Use the health explorer to drill down and find the cause of the unhealthy state. Use the knowledge on the specific monitor causing the issue to troubleshoot and fix the problem.

Figure 34 – Health Explorer showing all performance monitors at Host, HBA, and Port levels

5.3 Oversubscribed Link and Deteriorated Link Alerts

These events will be raised when the following counter values are exceeded.

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

Oversubscribed link:

- TXWords
- RXWords

Following is the summary for each of the monitors generating these alerts:

PRO 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 these unit monitors cross the set threshold and becomes unhealthy, then this aggregate monitor also becomes unhealthy.

- **Dumped 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.

PRO Oversubscribed Link monitor – Oversubscribed Link Aggregate Monitor
Causes - Oversubscribed link condition indicates that either 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.

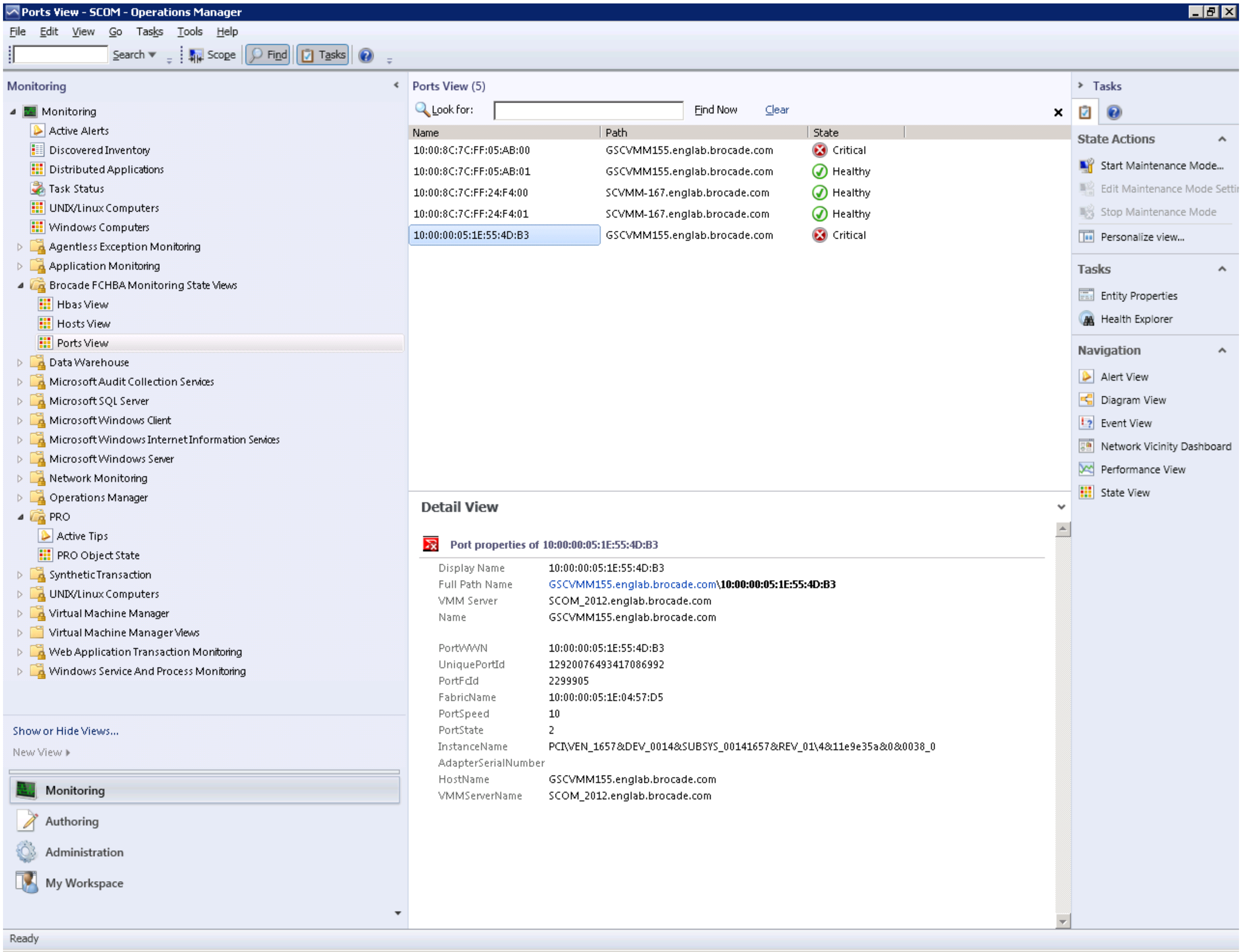
This monitor is an aggregate of the following monitors. If any of the unit monitors cross the set threshold and becomes unhealthy, then this aggregate monitor will also become unhealthy.

- **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 values exceeds the set threshold for the given port, that port's health state will change from healthy to critical. The state can be viewed in **Ports View**.

Hba Port Dependency Monitor. This is a dependency monitor that depends on the Oversubscribed link and Deteriorated link port-level aggregate. When all ports on the HBA become unhealthy then this monitor's state becomes unhealthy and the health state of this monitor rolls up to the HBA's health state and HBA becomes unhealthy too. (Please see Figure 34 - 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. An alert will be generated in the operation manager when an event occurs.



Name	Path	State
10:00:8C:7C:FF:05:AB:00	GSCVMM155.englab.brocade.com	☒ Critical
10:00:8C:7C:FF:05:AB:01	GSCVMM155.englab.brocade.com	✓ Healthy
10:00:8C:7C:FF:24:F4:00	SCVMM-167.englab.brocade.com	✓ Healthy
10:00:8C:7C:FF:24:F4:01	SCVMM-167.englab.brocade.com	✓ Healthy
10:00:00:05:1E:55:4D:B3	GSCVMM155.englab.brocade.com	☒ Critical

Port properties of 10:00:00:05:1E:55:4D:B3

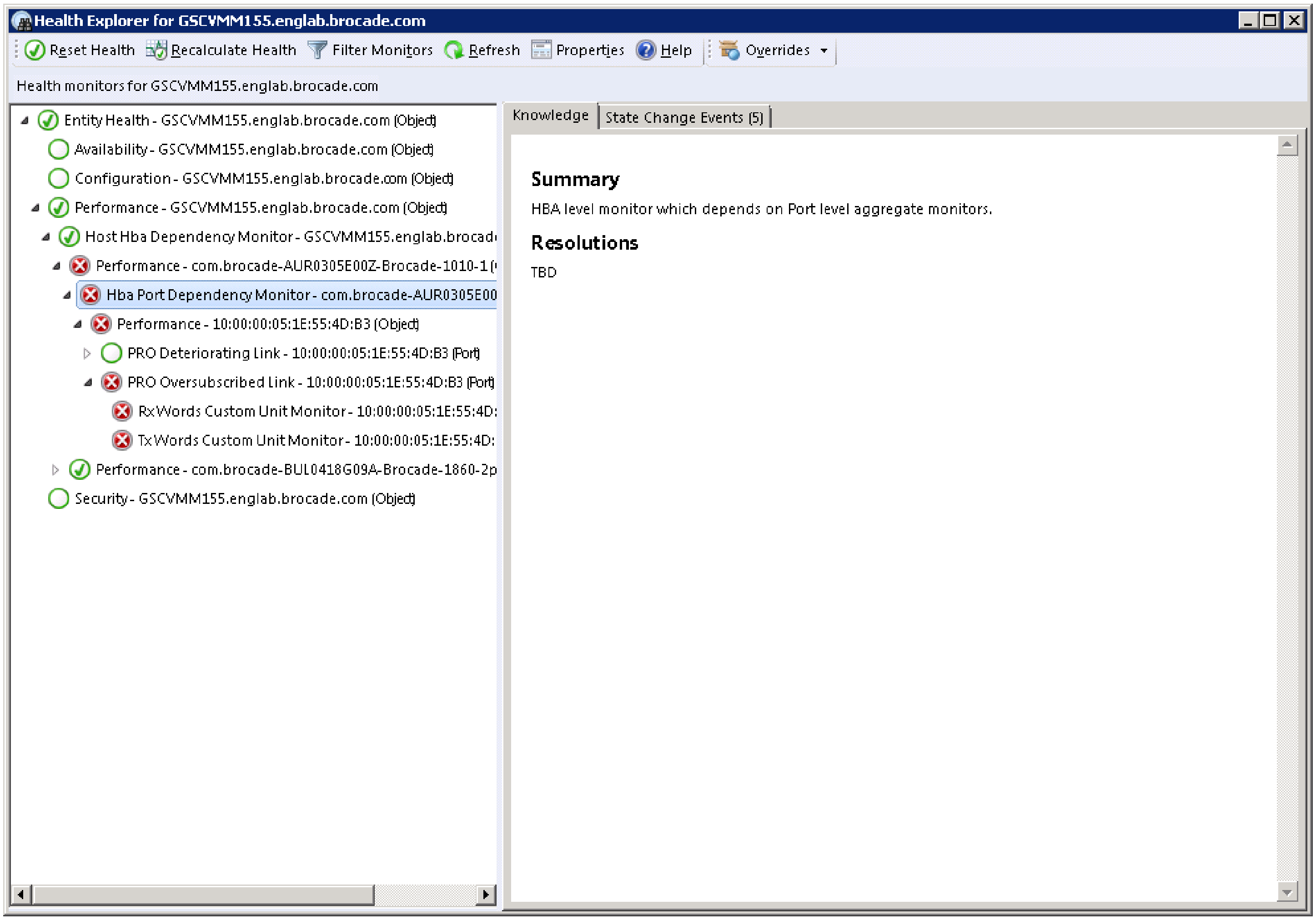
Display Name	10:00:00:05:1E:55:4D:B3
Full Path Name	GSCVMM155.englab.brocade.com\10:00:00:05:1E:55:4D:B3
VMM Server	SCOM_2012.englab.brocade.com
Name	GSCVMM155.englab.brocade.com
PortWWN	10:00:00:05:1E:55:4D:B3
UniquePortId	12920076493417086992
PortFcId	2299905
FabricName	10:00:00:05:1E:04:57:D5
PortSpeed	10
PortState	2
InstanceName	PCI\VEN_1657&DEV_0014&SUBSYS_00141657&REV_01\4&11e9e35a&0&0038_0
AdapterSerialNumber	
HostName	GSCVMM155.englab.brocade.com
VMMServerName	SCOM_2012.englab.brocade.com

Figure 35 – Port goes unhealthy when Rx Words monitor went unhealthy

5.4 Health Roll Up

When a unit monitor for a port becomes unhealthy, the corresponding Aggregate Monitor (DeteriorateLinkAgMonitor or OversubscribedLinkAgMonitor) becomes unhealthy.

The Unhealthy state rolls up to **HbaPortDependencyMonitor** which in turn rolls up the Unhealthy state to the **HostHbaDependencyMonitor.**



Health monitors for GSCVMM155.englab.brocade.com

- Entity Health - GSCVMM155.englab.brocade.com (Object)
  - Availability - GSCVMM155.englab.brocade.com (Object)
  - Configuration - GSCVMM155.englab.brocade.com (Object)
  - Performance - GSCVMM155.englab.brocade.com (Object)
    - Host Hba Dependency Monitor - GSCVMM155.englab.brocad
      - Performance - com.brocade-AUR0305E00Z-Brocade-1010-1 (
        - Hba Port Dependency Monitor - com.brocade-AUR0305E00
          - Performance - 10:00:00:05:1E:55:4D:B3 (Object)
            - PRO Deteriorating Link - 10:00:00:05:1E:55:4D:B3 (Port)
            - PRO Oversubscribed Link - 10:00:00:05:1E:55:4D:B3 (Port)
              - RxWords Custom Unit Monitor - 10:00:00:05:1E:55:4D:
              - TxWords Custom Unit Monitor - 10:00:00:05:1E:55:4D:
      - Performance - com.brocade-BUL0418G09A-Brocade-1860-2p
  - Security - GSCVMM155.englab.brocade.com (Object)

Summary

HBA level monitor which depends on Port level aggregate monitors.

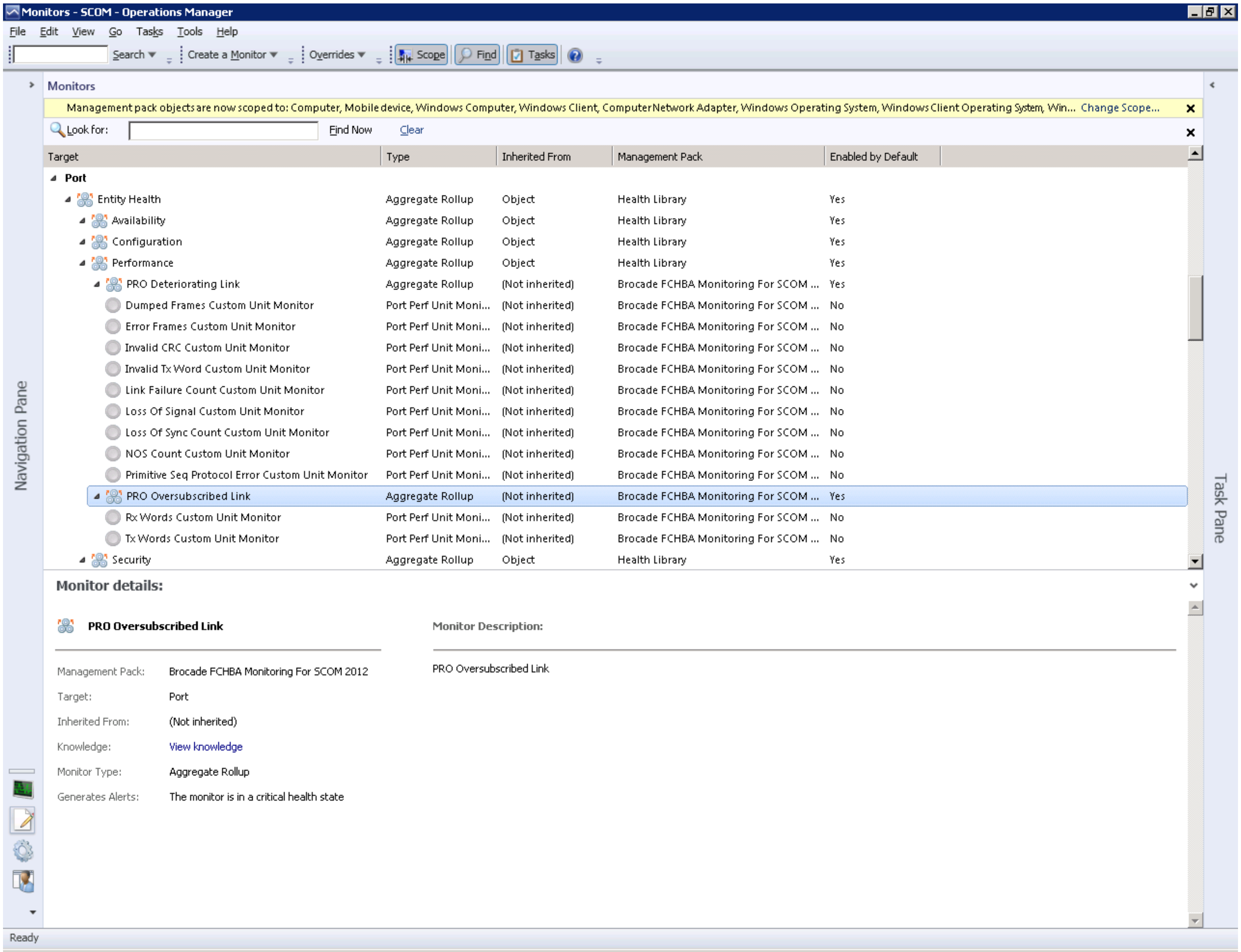
Resolutions

TBD

Figure 36 – Both Ports in HBA are unhealthy, so HBA becomes unhealthy too

5.5 PRO-Tip generation

When the port state goes from Healthy to Critical the Aggregate Monitor on the port object raises the alert. This Alert will be picked as a PRO-Tip sent to the SCVMM server. The following illustration shows the Aggregate Monitor hierarchy on port object.



Monitors

Management pack objects are now scoped to: Computer, Mobile device, Windows Computer, Windows Client, Computer Network Adapter, Windows Operating System, Windows Client Operating System, Win... Change Scope...

Look for: Find Now Clear

Target	Type	Inherited From	Management Pack	Enabled by Default
Port				
Entity Health	Aggregate Rollup	Object	Health Library	Yes
Availability	Aggregate Rollup	Object	Health Library	Yes
Configuration	Aggregate Rollup	Object	Health Library	Yes
Performance	Aggregate Rollup	Object	Health Library	Yes
PRO Deteriorating Link	Aggregate Rollup	(Not inherited)	Brocade FCHBA Monitoring For SCOM ...	Yes
Dumped Frames Custom Unit Monitor	Port Perf Unit Moni...	(Not inherited)	Brocade FCHBA Monitoring For SCOM ...	No
Error Frames Custom Unit Monitor	Port Perf Unit Moni...	(Not inherited)	Brocade FCHBA Monitoring For SCOM ...	No
Invalid CRC Custom Unit Monitor	Port Perf Unit Moni...	(Not inherited)	Brocade FCHBA Monitoring For SCOM ...	No
Invalid Tx Word Custom Unit Monitor	Port Perf Unit Moni...	(Not inherited)	Brocade FCHBA Monitoring For SCOM ...	No
Link Failure Count Custom Unit Monitor	Port Perf Unit Moni...	(Not inherited)	Brocade FCHBA Monitoring For SCOM ...	No
Loss Of Signal Custom Unit Monitor	Port Perf Unit Moni...	(Not inherited)	Brocade FCHBA Monitoring For SCOM ...	No
Loss Of Sync Count Custom Unit Monitor	Port Perf Unit Moni...	(Not inherited)	Brocade FCHBA Monitoring For SCOM ...	No
NOS Count Custom Unit Monitor	Port Perf Unit Moni...	(Not inherited)	Brocade FCHBA Monitoring For SCOM ...	No
Primitive Seq Protocol Error Custom Unit Monitor	Port Perf Unit Moni...	(Not inherited)	Brocade FCHBA Monitoring For SCOM ...	No
PRO Oversubscribed Link	Aggregate Rollup	(Not inherited)	Brocade FCHBA Monitoring For SCOM ...	Yes
Rx Words Custom Unit Monitor	Port Perf Unit Moni...	(Not inherited)	Brocade FCHBA Monitoring For SCOM ...	No
Tx Words Custom Unit Monitor	Port Perf Unit Moni...	(Not inherited)	Brocade FCHBA Monitoring For SCOM ...	No
Security	Aggregate Rollup	Object	Health Library	Yes

Monitor details:

PRO Oversubscribed Link

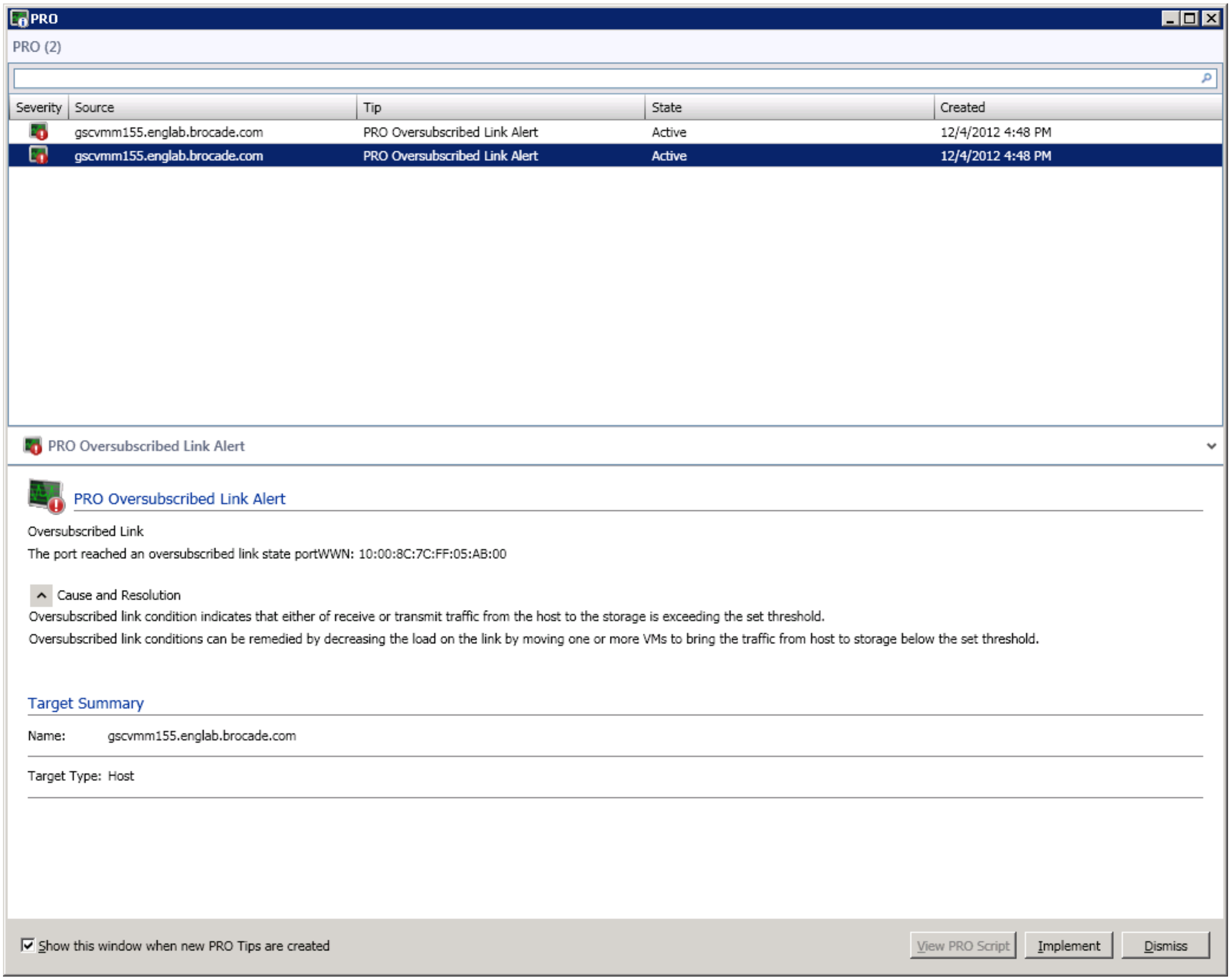
Management Pack:	Brocade FCHBA Monitoring For SCOM 2012
Target:	Port
Inherited From:	(Not inherited)
Knowledge:	View knowledge
Monitor Type:	Aggregate Rollup
Generates Alerts:	The monitor is in a critical health state

Monitor Description:

PRO Oversubscribed Link

Figure 37 – Aggregate Monitor alerts get sent as PRO Tips

When the 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.



Severity	Source	Tip	State	Created
	gscvmm155.englab.brocade.com	PRO Oversubscribed Link Alert	Active	12/4/2012 4:48 PM
	gscvmm155.englab.brocade.com	PRO Oversubscribed Link Alert	Active	12/4/2012 4:48 PM

PRO Oversubscribed Link Alert

PRO Oversubscribed Link Alert

Oversubscribed Link

The port reached an oversubscribed link state portWWN: 10:00:8C:7C:FF:05:AB:00

Cause and Resolution

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

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.

Target Summary

Name: gscvmm155.englab.brocade.com

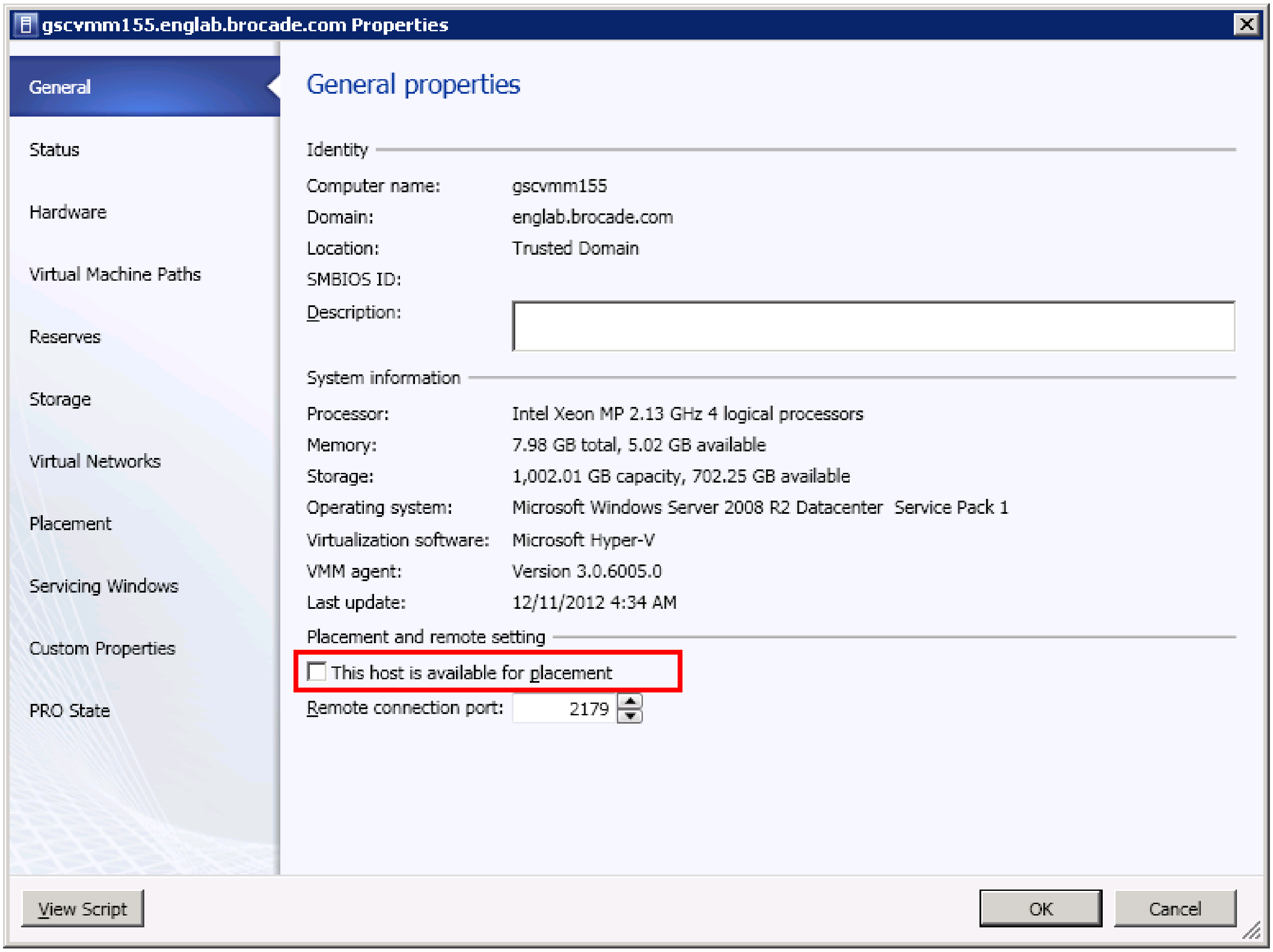
Target Type: Host

☑ Show this window when new PRO Tips are created

Figure 38 – PRO Tip Window showing Oversubscribed Link Alert

5.6 Setting the Host Unavailable for VM Placement

When all ports of one HBA are in a critical state, health of the HBA will be set as critical. When all HBAs on one host are in a critical state, the host object will be set as critical. Once the host object is critical, an alert will be generated and recovery will run to write an event with event ID 102 to the Windows Application event log. The corresponding Rule that reads the event log will execute a power shell script to mark the Host as 'Un Available For Placement' in SCVMM.



gscvmm155.englab.brocade.com Properties

General properties

Identity

Computer name:	gscvmm155
Domain:	englab.brocade.com
Location:	Trusted Domain
SMBIOS ID:	
Description:	

System information

Processor:	Intel Xeon MP 2.13 GHz 4 logical processors
Memory:	7.98 GB total, 5.02 GB available
Storage:	1,002.01 GB capacity, 702.25 GB available
Operating system:	Microsoft Windows Server 2008 R2 Datacenter Service Pack 1
Virtualization software:	Microsoft Hyper-V
VMM agent:	Version 3.0.6005.0
Last update:	12/11/2012 4:34 AM

Placement and remote setting

☐ This host is available for placement

Remote connection port: 2179

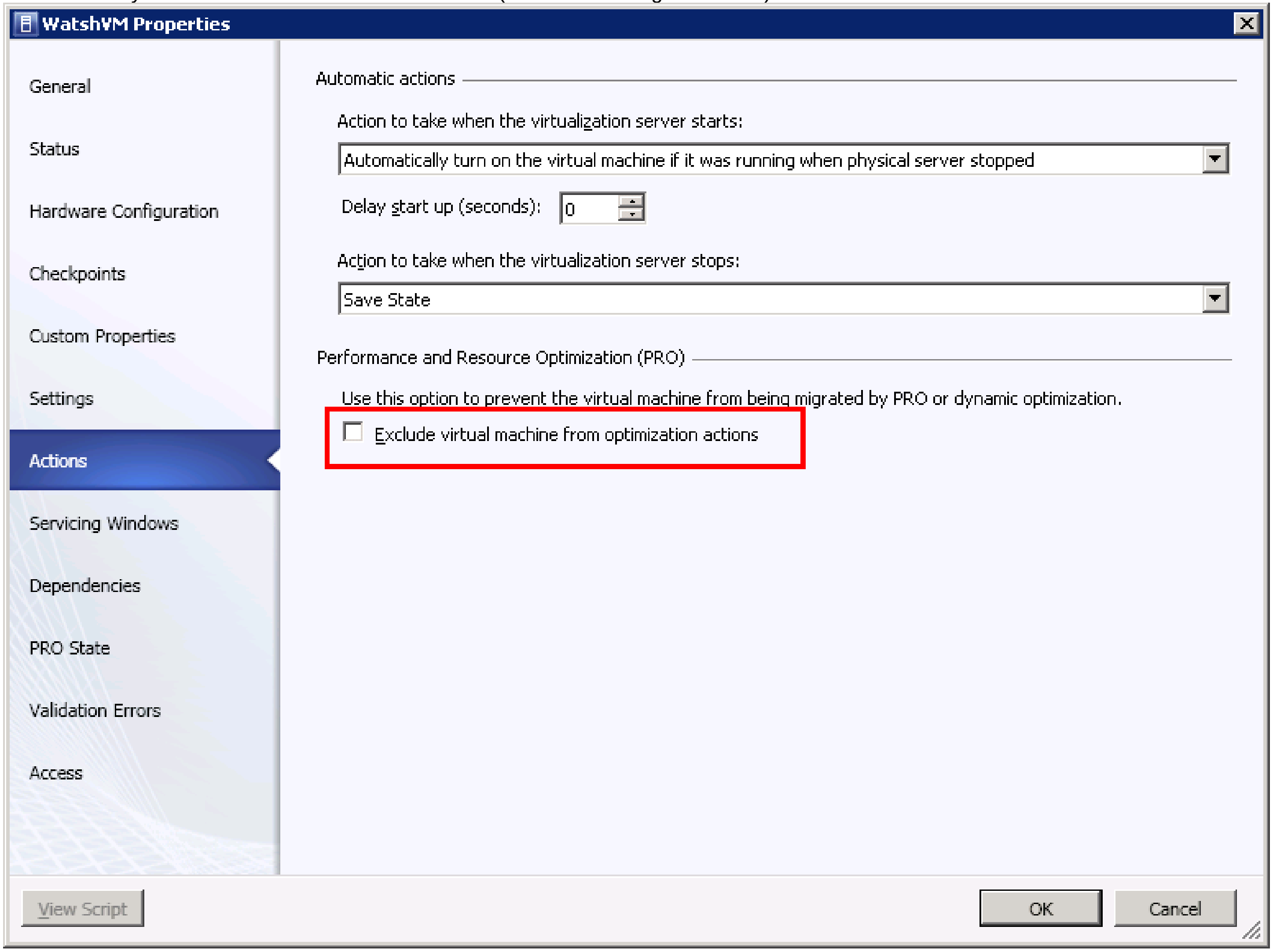
Figure 39 – Host marked as Unavailable for VM Placement

6 Troubleshooting

6.1 Troubleshooting PRO for Brocade HBA Management Pack

If the 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 host, HBA, or relations takes a very long time then make sure that ‘OpsMgr Health Service’ is started and running on the HyperV Host machines. If started, try restarting this service. This can resolve the discovery issue.
4. You can force discovery of PRO Tips by executing the following 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 the following illustration).



Automatic actions

Action to take when the virtualization server starts:

Automatically turn on the virtual machine if it was running when physical server stopped

Delay start up (seconds): 0

Action to take when the virtualization server stops:

Save State

Performance and Resource Optimization (PRO)

Use this option to prevent the virtual machine from being migrated by PRO or dynamic optimization.

☐ Exclude virtual machine from optimization actions

Figure 40 – VM Excluded from PRO setting

8. For execution flow specific errors, refer event ID 70/80 in the Windows Event log (Application log.

7 FAQ

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 user role under Administrator privilege.

2. What are the methods to push SCOM agent to remote machines?
Answer: There are two ways to push the SCOM agent to remote machines.
Manual Installation: Install the agent setup in the remote machines.
Pushing Agent: Push the agent from SCOM server to remote machines by providing privileges to the remote machines.

3. If I already have imported the MP, can I try importing again?
Answer: If both the Management Packs have different version then there is will be no problem in importing, but if Management Packs with the same version are imported then there will be a conflict.

4. After importing the MP, 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 the Brocade driver for discovering the HBAs through Brocade FCHBA Management Pack?
Answer: Yes.

8 Appendix: Scripts

This management pack includes following scripts:

Script	Purpose	Parameters	Default Frequency
Port Performance Script	Provides monitoring of HBA port statistics counters.	IntervalSeconds	300 secs (5 mins)
Discover HBAs Script	Discovers the HBAs on a Host.	ImagePath NetworkName	14400 secs (4 hrs)
Discover Ports Script	Discovers HBA ports.	ImagePath SerialNumber DisplayName PrincipalName HyperVGUID	14400 secs (4 hrs)
VM Migration Oversubscribed Link Recovery Task	Provides the recovery task for a PRO tip of oversubscribed link alerts and initiates migration of one VM at a time on the host.	<HostName>*<VMMServer>* <EventOriginId>*<PortWWN>* ONE	NA
Set Host Unavailable Recovery Task	Migrates the recovery task which 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	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
VM Migration power shell 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, whereas for a deteriorating link, all VMs on the affected port are migrated.	EventDescription	NA
Set Host Unavailable power shell Script	Marks the host as unavailable from further VM placement.	EventDescription	NA

8.1 Port Performance Script

Name: PortPerfScript.vbs

Performance Counters:

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

- TxWords
- RxWords
- NOSCount
- ErrorFrames
- DumpedFrames
- LinkFailureCount
- LossOfSyncCount
- LossOfSignalCount
- PrimitiveSeqProtocolErrCount
- InvalidTxWordCount
- InvalidCRCCount

Refer to MSFC_FibrePortHBAStatistics class for details.

How the script works:
This script polls the performance counters for HBA ports every interval (300 seconds by default) and computes the delta value between the counter values. It then takes average of 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, PortSpeed is in Gbps and WORD length is 32 bits.

The mapping from PortSpeed to Gbps value is done as shown below:

Port Speed (Integer value)	Port Speed (In Gbps)
0	Unknown
1	1 Gbps
2	2 Gbps
4	10 Gbps
8	4 Gbps

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

Effective values for:
NumSamples is 2
Threshold for each counter is defined here.
IntervalSeconds is 300 seconds.

8.2 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***

8.3 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***

8.4 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 then 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 seconds.

8.5 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, the host is made unavailable for further VM placement. This recovery task initiates marking a 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 it finds an event with ID 102, it executes a power shell script that marks the host as unavailable for placement.

8.6 VM Migration Deteriorated Link Recovery Task

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

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 then executes a power shell script causing the actual VM Migration. For a deteriorating link, all VMs on the host are moved to a destination host.

Timeout: 300 seconds.

8.7 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, whereas for a deteriorating link, all VMs on the affected port are migrated.

How the script works:
It reads the event ID 101 logged by event source **BrocadeMP**. If such an event is found, then it obtains the event description and migrates one or all VMs on the affected port.

Timeout: 300 seconds.

8.8 Set Host Unavailable Power Shell Script

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

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

Timeout: 300 seconds.