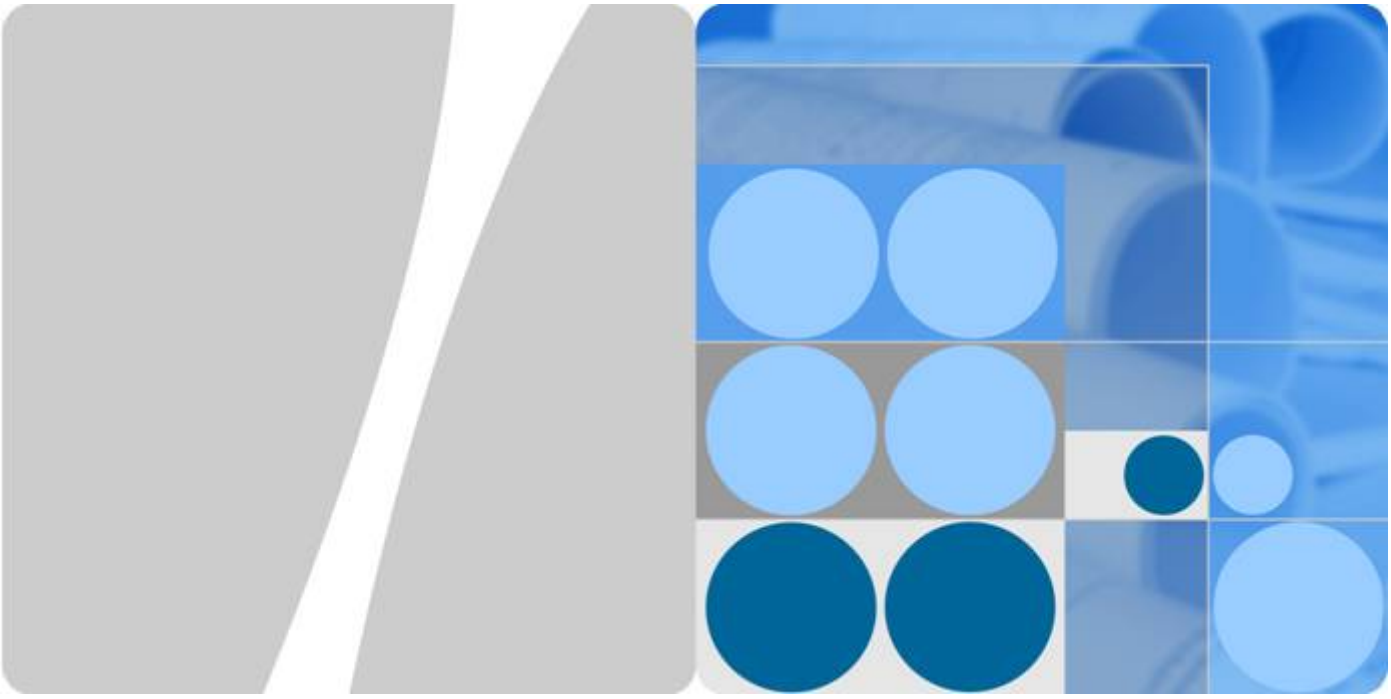


eSDK Storage Plugins

1.0.RC5

Quick Guide 01(SCOM, Plug-in)

Issue 01

Date 2017-04-27

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

Contents

1 About This Document

Purpose

This document describes the overview and background of the System Center Operations Manager Plug-in software and provides preparations, modes, and FAQs for installing the SCOM Plug-in software.

Intended Audience

This document is intended for:

ISV software development engineers

Symbol Conventions

The symbols that may be found in this document are defined as follows:

Symbol	Description
DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
CAUTION	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.

Symbol	Description
NOTE	Calls attention to important information, best practices and tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

2 Introduction

System Center Operations Manager Plug-in is a Huawei self-developed plug-in for Microsoft System Center Operations Manager (SCOM) and is used to monitor Huawei storage devices.

SCOM plug-in supports the Simple Network Management Protocol (SNMP) and has the following functions:

- Discovers storage devices.

  The status page displays basic device information including the device serial number, device type, version, status, total capacity, and used capacity.
- Reports alarms.

  The alarm page displays device alarm information including the alarm severity, alarm names, status, generation time, descriptions, alarm IDs, and recommended actions.
- Clears alarms.

  When an alarm is cleared, the alarm status becomes resolved.
- Monitors LUN information.

  The status page displays LUN information including the IDs, names, world wide names (WWNs), capacities, and IP addresses of owning devices.

3 Installation Preparations

3.1 Device Model and Version

The following table lists the device models and versions supported by SCOM Plug-in:

Model	Version
S2600T/S5500T/S5600T/S5800T/S6800T	V200R002C00 V200R002C10 V200R002C20 V200R002C30
OceanStor 18500/18800/18800F	V100R001C00 V100R001C10 V100R001C30
OceanStor 5300V3/5500V3/5600V3/5800V3/6800V3	V300R001C00 V300R001C30 V300R002C00 V300R002C10 V300R003C00 V300R003C10 V300R003C20 V300R003C20SPC100 V300R003C20SPC200 V300R006C00
OceanStor 2200V3/2600V3	V300R005C00SPC300 V300R006C00
OceanStor 18500 V3	V300R003C20 V300R003C20SPC100 V300R003C20SPC200 V300R006C00
OceanStor Dorado6000 V3	V300R001C00 V300R001C01

3.2 Operating Environment Requirements

SCOM Plug-in works only on the Windows-based server or host.

The Windows version and SCOM version are as follows:

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

3.3 Obtaining Installation Packages

Before installing the SCOM plug-in, obtain the installation package listed in **Table 3-1**.

NOTE

X.X.XX indicates the version number, please obtain the installation package with this manual before installation.

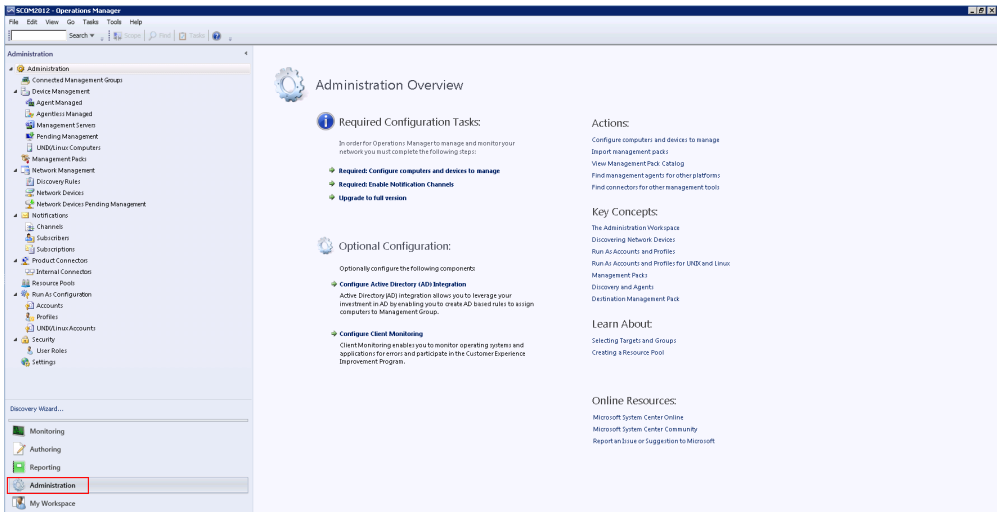
Table 3-1 Obtaining installation package

Software Package	Description	How to Obtain
● eSDK_Storage_SCOM_Plugin_X.X.XX_For_DoradoV3.zip ● eSDK_Storage_SCOM_Plugin_X.X.XX_For_OceanStorV3.zip	● SCOM plug-in package for Dorado V3 devices ● SCOM plug-in package for OceanStor V3 devices	Go to **http://support.huawei.com/enterprise/softdownload** and choosing **IT** > **Storage** > **Tools and Platform** > **eSDK Storage Plugins** to download the packages.

4 Installation and Deployment

4.1 Installing SCOM Plug-in

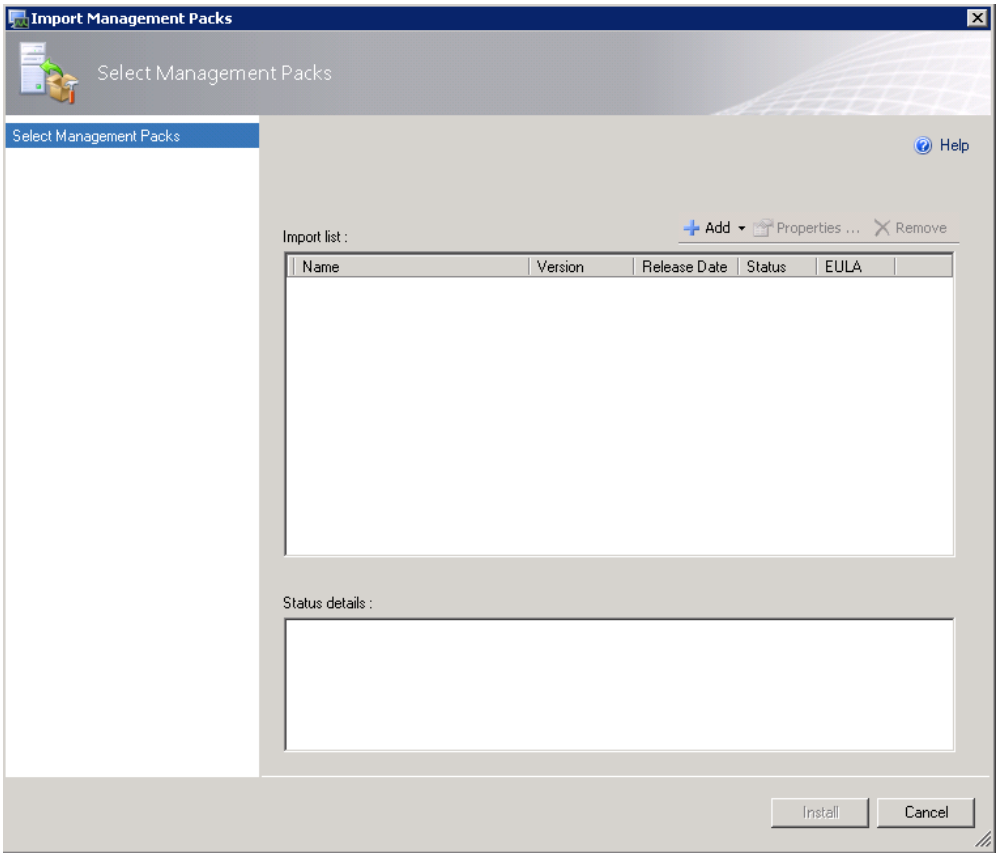
Step 1 Log in to the SCOM main window. In the navigation tree on the lower left, click **Administration**.



Step 2 In the navigation tree on the upper left, click **Management Packs**.

Step 3 In the function pane on the right, click **Import Management Packs**.

The **Import Management Packs** dialog box is displayed.



Step 4 Click **Add**. In the drop-down list, select **Add from disk**.

The **Select Management Packs** to import dialog box is displayed.

Step 5 Select the MP installation package that you want to import. Click **Open**.

NOTE

The MP installation package is a ***.mp** file which is decompressed by SCOM plug-in installation package **eSDK_Storage_SCOM_Plugin_X.X.XX_For_DoradoV3.zip** or **eSDK_Storage_SCOM_Plugin_X.X.XX_For_OceanStorV3.zip**.

Step 6 In **Import list**, select the imported installation package. Click **Install**.

After being installed, the SCOM plug-in function is automatically uploaded to the system.

----End

4.2 Configuring the SNMP

Before using SCOM to monitor Huawei storage devices, you need to configure SNMP community strings for Huawei storage devices. If SNMP community strings have been configured, skip this step.

Configuring the SNMP Community Strings

Step 1 Run a shell command to log in to the storage device.

Step 2 Enable SNMP v1 and v2c.

These two options are disabled by default. You need to manually enable them by running the following commands:

```
admin:/>change snmp version v1v2c_switch=On
CAUTION: You are about to enable SNMPv1 and SNMPv2c. But you are advised to use
the secure SNMPv3 protocol only.
Do you wish to continue?(y/n)y
Command executed successfully.
```

Step 3 Run the following command to configure the SNMP community strings.

```
admin:/>change snmp community read_community=**********
write_community=***********
Command executed successfully
```

NOTE

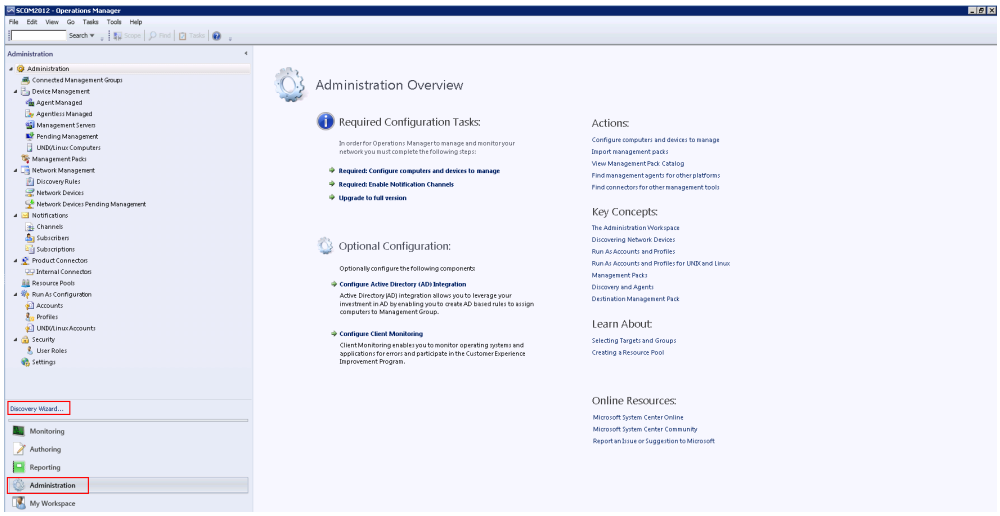
1. This command is used to set the read community string and write community string at the same time. The read community string and write community string cannot be the same.
2. When creating discovery policies, you need to use the read community string to connect to the storage device.

----End

4.3 Creating a Discovery Rule

Creating a Discovery Rule

Step 1 Log in to the SCOM main window. In the navigation tree on the lower left, click **Administration**.



Step 2 In the navigation tree on the upper left, click **Discovery Wizard**.

The **Computer and Device Management Wizard** dialog box is displayed.

Step 3 On the **Discovery Type** page, select **Network devices**.

Step 4 Click **Next**. On the **General Properties** page, set basic properties.

The following table describes related parameters:

Parameter	Description	Example
Name	Name of the network device to be discovered.	HUAWEI
Description	Description of the network device to be discovered.	Storage devices
Available servers	Name of the available management server. One discovery rule is configured for only for one server.	SCOMESDK2.china.huawei.com
Available pools	Name of the available management server pool.	All Management Servers Resource

Step 5 Click **Next**. On the **Discovery Method** page, set a discovery type to **Explicit discovery**.

- Explicit discovery: Operations Manager will discover only those network devices you specify.
- Recursive discovery: Operations Manager will discover the devices that you specify and all devices that are connected to the devices that you specify.

NOTE

For details about the operations related to Recursive discovery, see **https://technet.microsoft.com/en-us/library/hh278846.aspx** at the Microsoft official website.

Step 6 **(Optional)** Click **Next**. On the **Default Accounts** page, choose **SNMP v1 or SNMP v2**. The operating account is the default account for discovering a network device.

NOTE

- If the account list has no available operating accounts, click **Create Account** and create accounts as instructed.
- The community string of an operating account must be the same as that of the device to be discovered. If they are different, the network devices cannot be discovered.

Step 7 Click **Next**. On the **Devices** page, specify a network device that you want to discover and manage.

1. Click **Add**.

   The **Add a device** dialog box is displayed.

   NOTE

   Click **Import devices** and import a *.txt file that records the network device IP address.

2. Set parameters for the network device. The following table describes the parameters:

Parameter	Description	Example
Name or IP address	Name or IP address of the network device to be discovered.	192.168.0.100
Access mode	Access mode of the network device to the discovered. The value can be **ICMP** and **SNMP**, **ICMP**, or **SNMP**. The access mode required for this plug-in is **SNMP**.	SNMP
SNMP version	Version of SNMP. The value can be **v1** or **v2** or **v3**.	v1
Port number	Port number of the network device to be discovered. The value ranges from 1 to 65535. The port number required for this plug-in is **161**.	161
SNMP V1 or V2 RUN As account/SNMP V3 RUN As account	Default account of the network device to be discovered when SNMP version is **v1** or **v2**/**v3**.	admin@111

NOTE

- If the account list has no available operating accounts, click **Add SNMP V1 or V2 RUN As Account** and create accounts as instructed.
- The community strings of an **SNMP V1 or V2 RUN As Account** must be the same as that of the device to be discovered. If they are different, the network devices cannot be discovered.
- For each IP address in the discovery policy, SCOM regards it as an independent device. If multiple IP addresses are configured in the discovery policy and they are the controller IP addresses of the same device, SCOM will monitor the device repeatedly and repeated information will be displayed on the monitoring page.

Step 8 Click **Next**. On the **Schedule Discovery** page, specify the execution schedule of the discovery rule.

- Run the discovery rule at schedule times: Runs the discovery rule periodically.
- Run the discovery rule manually: Runs the discovery rule manually.

Step 9 Click **Next**. On the **Summary** page, confirm information.

Step 10 Click **Create**. The discovery rule is created.

Step 11 Select **Run the network discovery rule after the wizard is closed** and click **Close**.

Step 12 After a discovery rule is created, the system automatically runs the discovery rule and discovers the connected network devices.

----End

Deleting the Discovery Rule (Optional)

Step 1 In the navigation tree on the lower left, click **Administration**.

Step 2 In the navigation tree on the upper left, click **Discovery Rules**.

Step 3 In the function pane, right-click the discovery rule that you want to delete and choose **Delete**.

----End

4.4 Setting the Trap IP Address of Alarm Notification

Step 1 Log in to the ISM platform of a storage device.

Step 2 Choose **Settings** > **More** > **Alarm Settings** > **Trap IP Addresses Management**.

Step 3 Add the IP address of the SCOM server.

1. Click **Add**. The **Add Server IP Address** dialog box is displayed.
2. Enter the IP address of the created server. The details are as follows:

Parameter	Description	Example
Service IP Address	IP address of the server where the SCOM plug-in is installed	192.168.0.100
Port	Port information of the server IP address Value range: 1 to 65535 The port number required for this plug-in is 162.	162
Version	Version information of the server IP address The values include **SNMPv1**, **SNMPv2c**, and **SNMPv3**. The version required for this plug-in is SNMPv2c.	SNMPv2c

3. Click **OK**.

Step 4 Confirm the operation of adding a server IP address.

1. Click **Save**.

   The system displays the **Execution Result** dialog box, indicating that the operation is successful.

2. Click **Close**.

----End

5 Monitoring Storage Devices

NOTE

- The maximum number of objects being monitored is 3000. Objects being monitored include LUNs, LUN groups, hosts, host groups, ports, port groups, storage pools, and disk domains.
- The SCOM Plug-in does not support multi-controller switchover during monitoring configuration.

1. Log in to the SCOM main window. In the navigation tree on the lower left, click **Monitoring**.
2. In the navigation tree on the upper left, choose **Huawei Storage**.

View Basic Information

1. Choose **Huawei Storage** > **Basic Information**.
2. Choose **Device Information**. View device status information.
3. Choose **Controller**. View controller information.

View Block Storage Device information

1. Choose **Huawei Storage** > **Block Storage Service**.
2. Choose **Host**. View host information.
3. Choose **Host Group**. View host group information.
4. Choose **LUN**. View LUN information.
5. Choose **LUN Group**. View LUN group information.

View Configuration Information

1. Choose **Huawei Storage** > **Configuration**.
2. Choose **DiskDomain**. View disk domain information.
3. Choose **StoragePool**. View storage pool information.
4. Choose **Port**. View port information.
5. Choose **Port Group**. View port group information.

View Monitor Information

1. Choose **Huawei Storage** > **Monitor**.

2. Choose **Alarms**. View alarm information.

NOTE

If alarm information fails to be obtained, add inbound rules to firewalls to allow messages from UDP port 162 to flow in. For details, see **What can I do if SCOM plug-in fails to obtain alarm information about arrays**.

View Performance Information

1. Choose **Huawei Storage** > **Preformance**.
2. Choose **Controller**. View performance information of controllers.
3. Choose **LUN**. View performance information of LUNs.
4. Choose **LUN**. View performance information of ports.

6 Uninstalling SCOM Plug-in

Step 1 Log in to the SCOM main window. In the navigation tree on the lower left, click **Administration**.

Step 2 In the navigation tree on the upper left, click **Management Packs**.

Step 3 Select the installation package that you want to uninstall.

Step 4 In the function pane on the right, click **Delete**.

----End

7 Upgrading SCOM Plug-in

Step 1 Repeat the **Step1** to **Step4** in **4.1 Installing SCOM Plug-in**.

Step 2 Select the MP installation package that you want to import. Click **Open**.

NOTE

The MP installation package is a ***.mp** file.

Step 3 In **Import list**, select the imported installation package.

A message that a version of Huawei.ISM.Management.Pack has been imported is displayed in the status bar.

Step 4 Click **Install**.

Step 5 After being installed, the SCOM plug-in upgraded function is automatically uploaded to the system.

----End

8 FAQ

Question 1: Why do network devices fail to be discovered after a discovery rule is successfully set?

Answer: After a discovery rule is set, the system automatically discovers connected network devices. If the network devices fail to be discovered, confirm whether the SNMP service of the network devices is enabled. However, the time spent on discovering network devices ranges from 3 to 5 minutes depending on the performance of the server or host. If the time spent on discovering network devices is longer than 5 minutes, contact technical support.

Question 2: Why is new or modified LUN information not displayed after the LUN View page is displayed?

Answer: The default LUN discovery period is 4 hours. That is, LUN information is updated every 4 hours. Therefore, new or modified LUN information may not be displayed immediately. You can change the discovery period by performing the following operations:

1. On the navigation bar in the lower left part of the SCOM main window, click **Authoring**.
2. On the upper left navigation bar, choose **Management Pack Objects** > **Object Discoveries**.
3. In **Look for**, type **LUN** and choose **New LUNIdex Discovery**.
4. On the right toolbar, choose **Overrides** > **Override the Object Discovery** > **For all objects of class: Huawei Device Class**.
5. In the **Override Properties** dialog box, select **Interval Seconds** and enter a new discovery period (expressed in seconds) in **Override Value**.
6. Click **Apply**.
7. Click **OK**.

Question 3: Why is the LUN status different from its health status?

Answer: The default LUN discovery period is 4 hours. That is, LUN information is updated every 4 hours. Therefore, when the LUN status changes, it may not be updated immediately. You can change the discovery period by performing the following operations:

1. On the navigation bar in the lower left part of the SCOM main window, click **Authoring**.

2. On the upper left navigation bar, choose **Management Pack Objects** > **Monitors**.
3. In **Look for**, type **LUN** and choose **New LUN Status Monitor**.
4. On the right toolbar, choose **Overrides** > **Override the Monitor** > **For all objects of class: LUN Class**.
5. In the **Override Properties** dialog box, select **Interval** and enter a new discovery period (expressed in seconds) in **Override Value**.
6. Click **Apply**.
7. Click **OK**.

NOTE

The default discovery period for basic information, block devices, and objects in the configuration information is four hours. It can be changed using the preceding method.

Question 4: A new alarm will be generated on the SCOM alarm page when a new alarm is generated on the array page. Why can the alarm on the SCOM not be cleared or its status not change when an alarm on the array page is deleted?

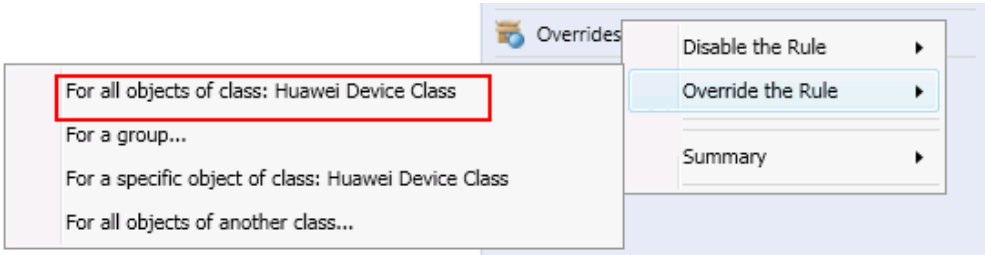
Answer: Check whether the network connection is normal. If the network connection is normal, you can perform the following steps:

1. On the navigation bar in the lower left part of the SCOM main window, click **Authoring**.
2. On the upper left navigation bar, choose **Management Pack Objects** > **Rules**.
3. In **Look for**, type **alarms resolved**, click **Find Now** and choose *Huawei alarms resolved rule*. See **Figure 8-1**.

Figure 8-1 Rules

4. On the right toolbar, choose **Overrides** > **Override the Rule** > **For all objects of class: Huawei Device Class**. See **Figure 8-2**.

Figure 8-2 Override the Rule

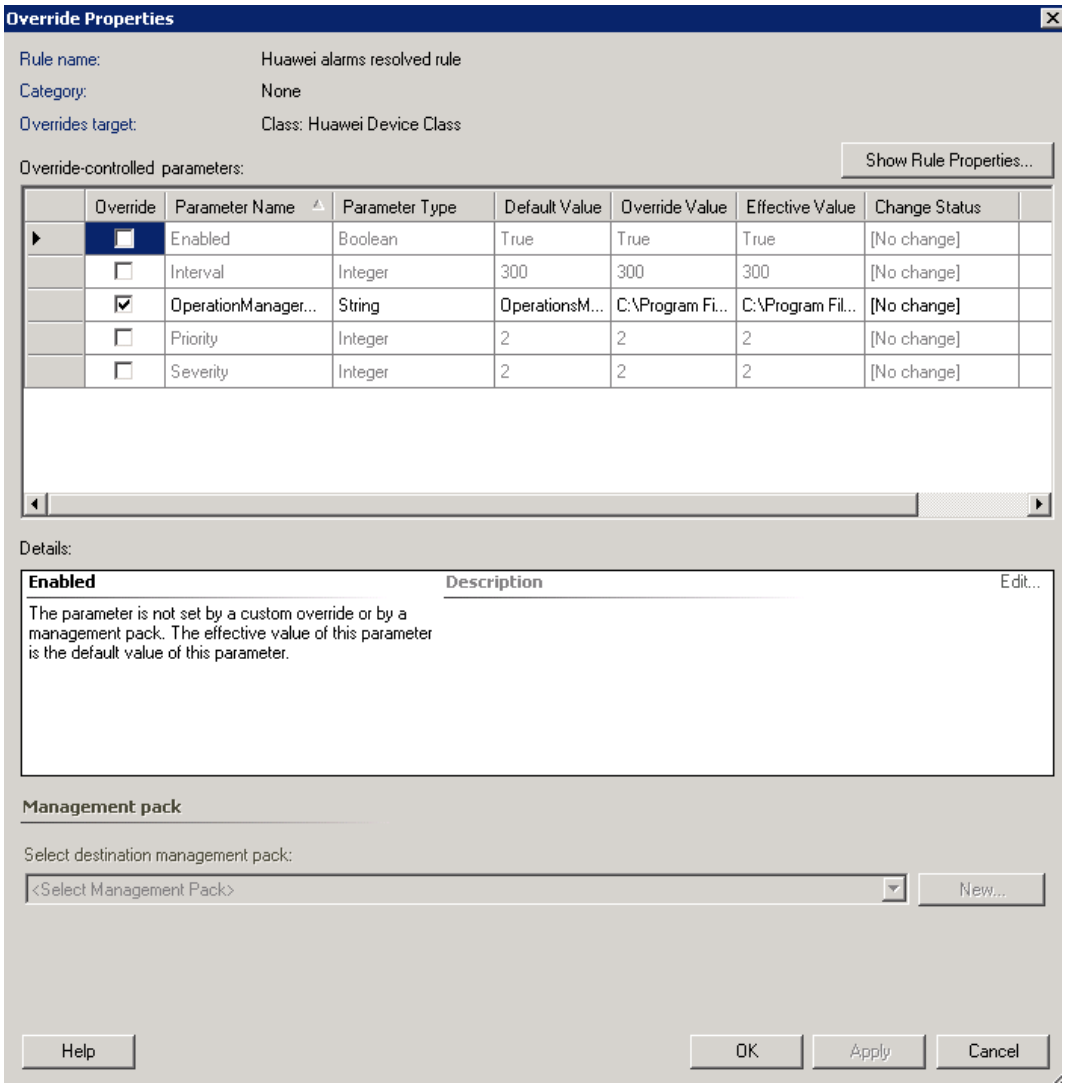


5. In the **Override Properties** dialog box, select *OperationManagerPath* and enter a new path in **Override Value**.

The default value is **OperationManager**. Change it to the path of the **OperationsManager.psm1** file, for example, **C:\Program Files\System Center 2012\Operations Manager\Powershell\OperationsManager\OperationsManager.psm1**.

See **Figure 8-3**.

Figure 8-3 Override Properties



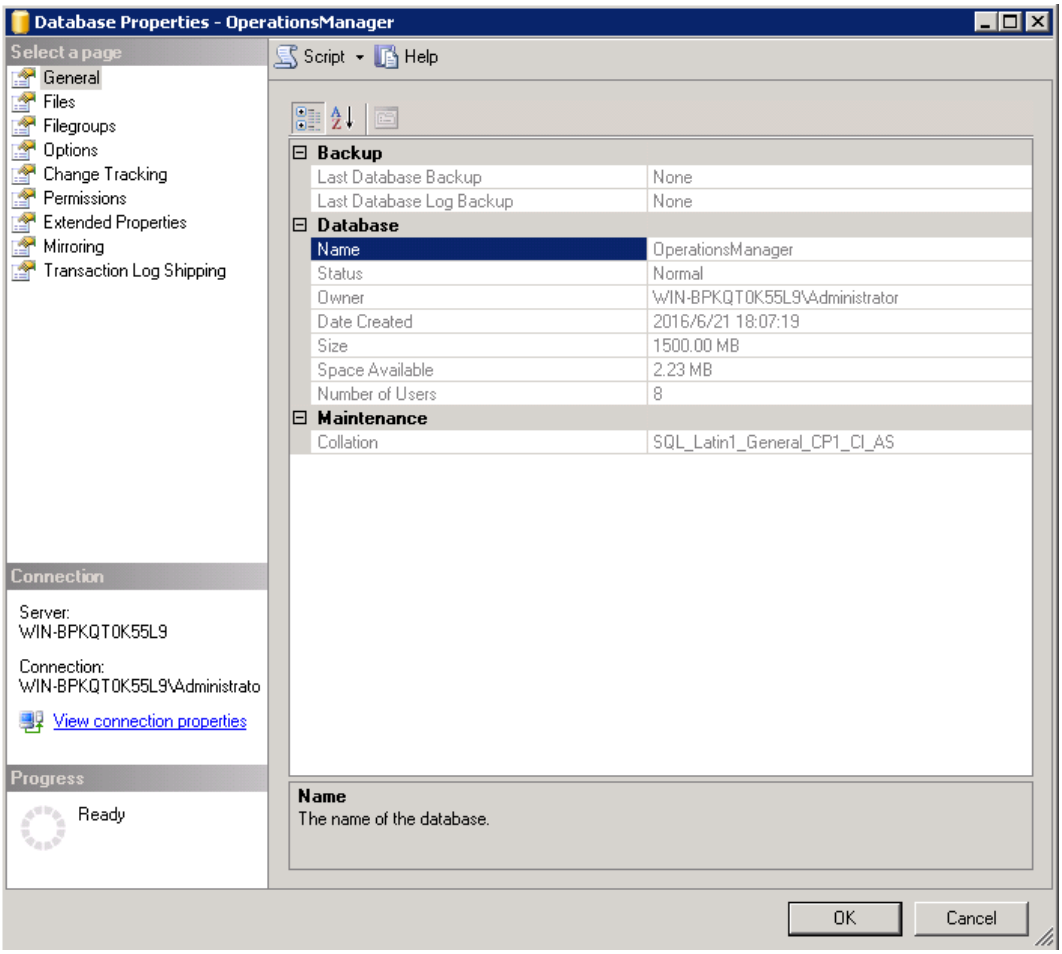
6. Click **Apply**.
7. Click **OK**.

Question 5: What can I do after a message indicating failed deletion is displayed when I uninstall the SCOM?

Answer: The database may be faulty and cannot allocate space to database objects. The solution is as follows:

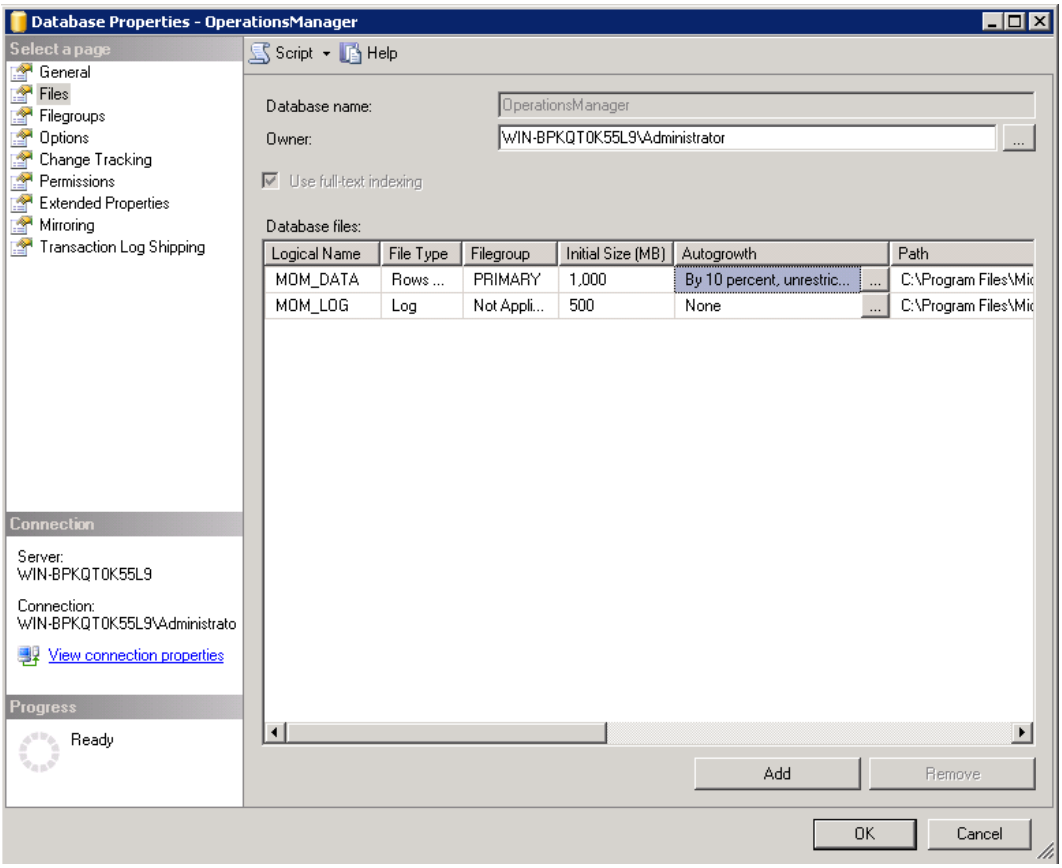
1. Start Microsoft SQL Server 2005. In the database list, select **OperationsManager** corresponding to the database to be shrank.
2. Right-click **OperationsManager**. From the drop-down list, select **Database Properties**, as shown in the **Figure 8-4**.

Figure 8-4 Database properties (1)



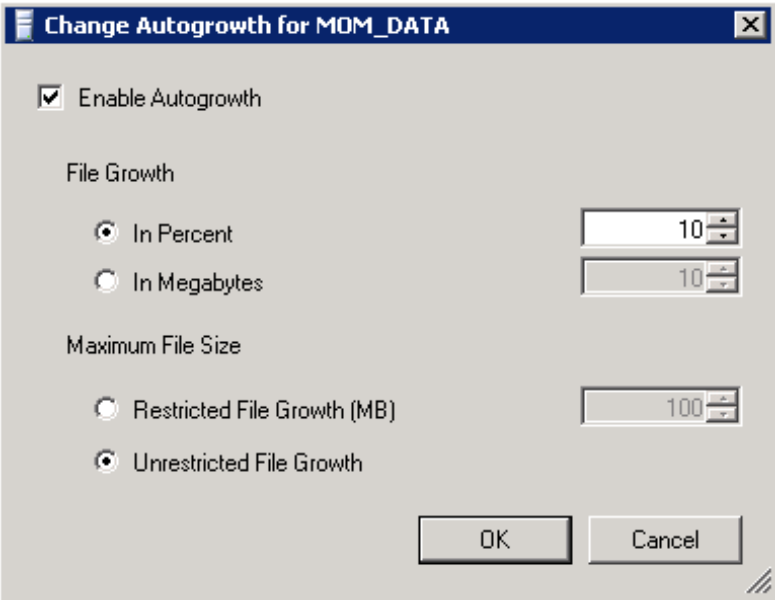
3. Select **Files**. In the **Database files** list, click the **...**button corresponding to the **MOM_DATA** file in the **Autogrowth** column, as shown in the **Figure 8-5**.

Figure 8-5 Database properties (2)



4. In the **Change Autogrowth for MOM_DATA** window that is displayed, set **Maximum File Size** to **Unrestricted File Growth** and click **OK**, as shown in the **Figure 8-6**.

Figure 8-6 Changing autogrowth configurations

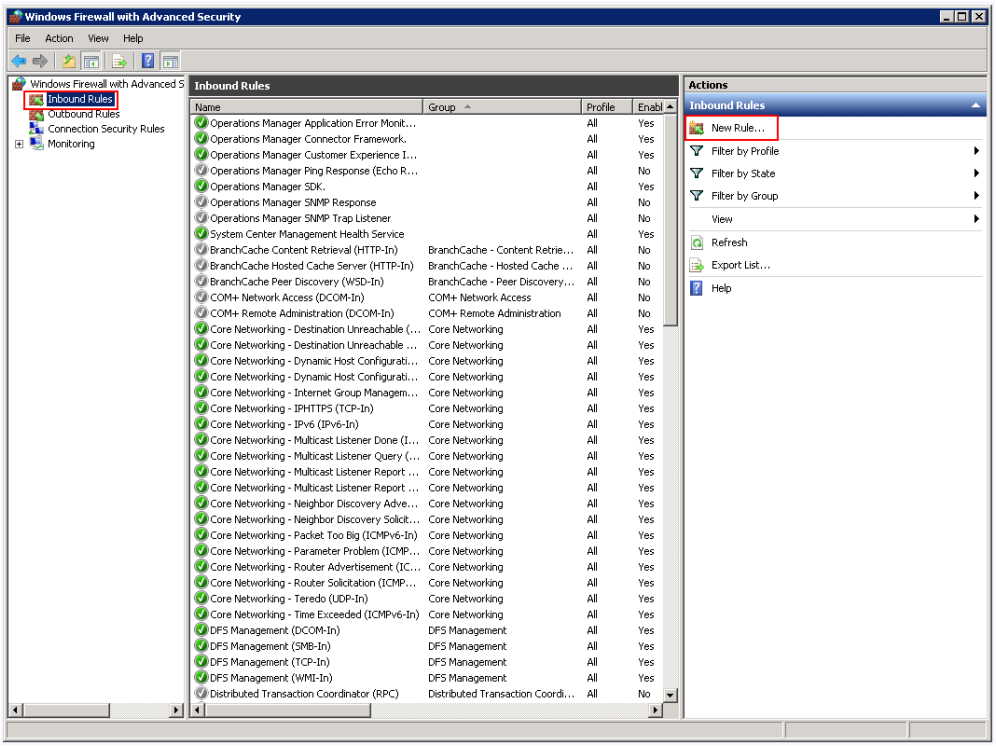


Question 6: What can I do if SCOM plug-in fails to obtain alarm information about arrays?

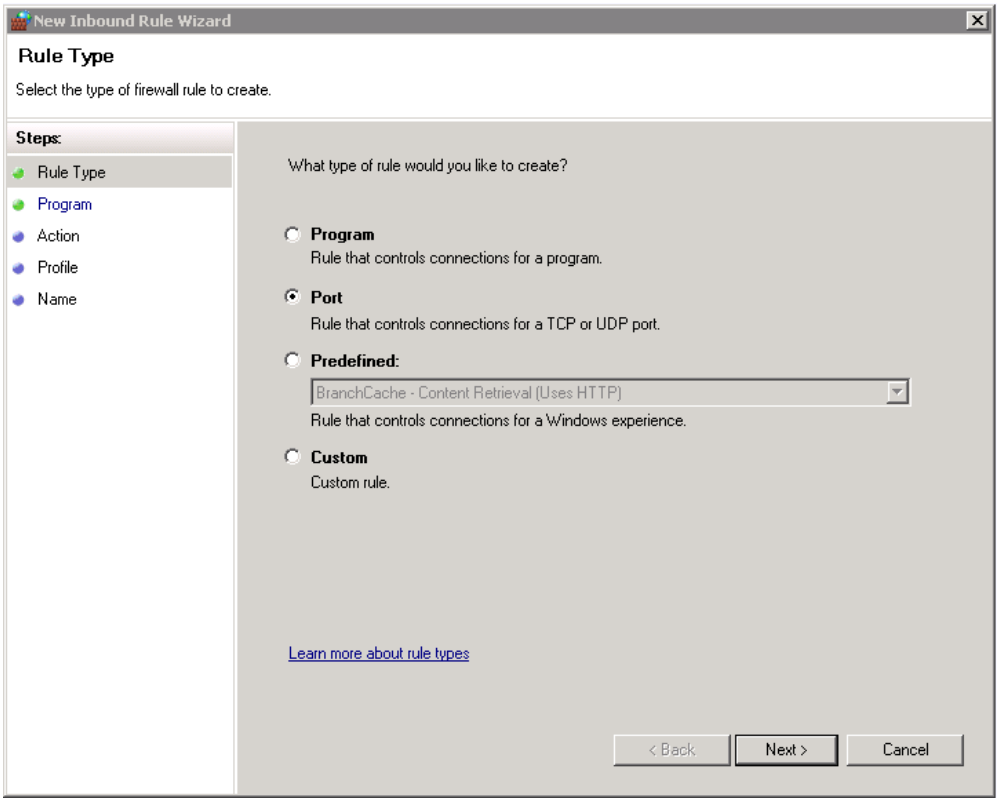
Answer: The possible cause of the problem is that alarm information about arrays is blocked by the firewall on the SCOM server. Add inbound rules to the firewall on the SCOM server to connect to UDP port 162 as follows:

1. On the SCOM server, choose **Control Panel** > **System and Security** > **Windows Firewall**, and go to the **Help protect your computer with Windows Firewall** page.
2. On the navigation bar on the left, click **Advanced settings**. The **Windows Firewall with Advanced Security** window is displayed.
3. On the menu bar on the left, click **Inbound Rules**. In the **Actions** area, click **New Rule**. The **New Inbound Rule Wizard** window is displayed.

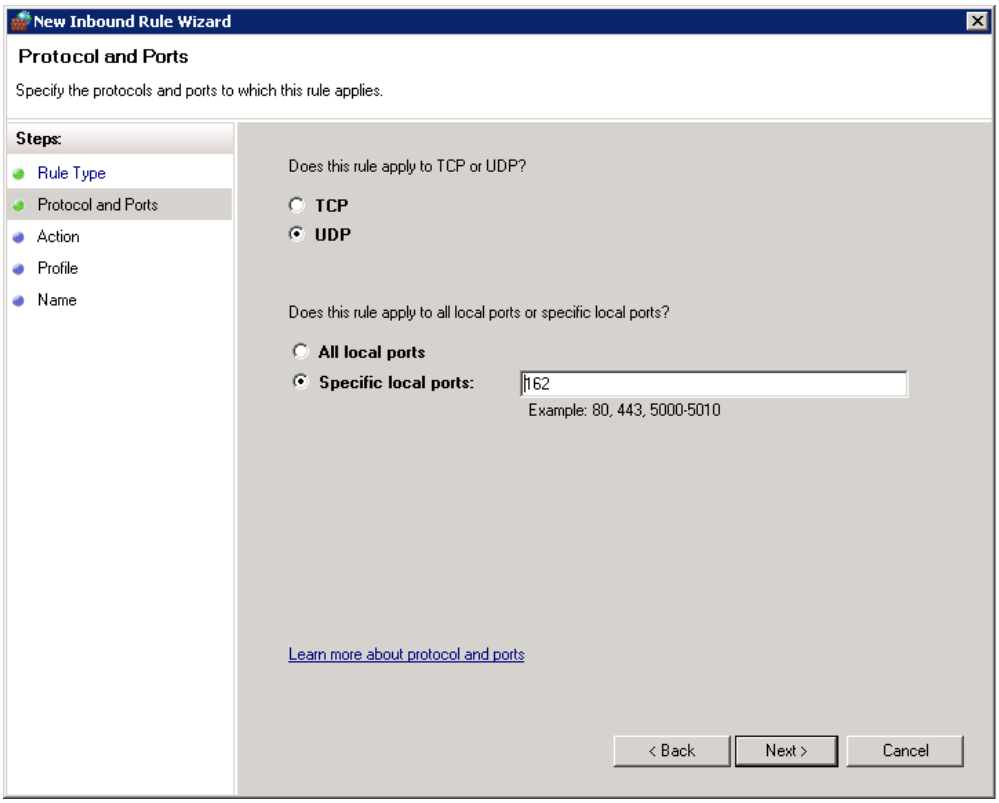
Figure 8-7 Creating an inbound rule



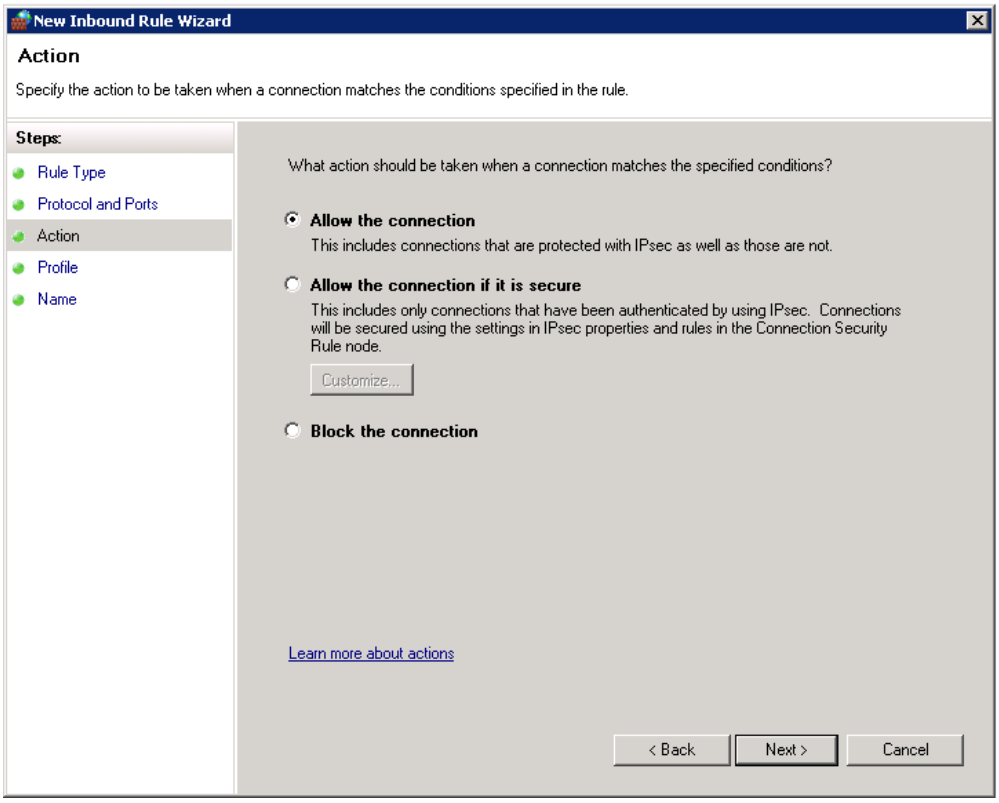
4. On the **Rule Type** tab page, click **Port**, and then click **Next**.



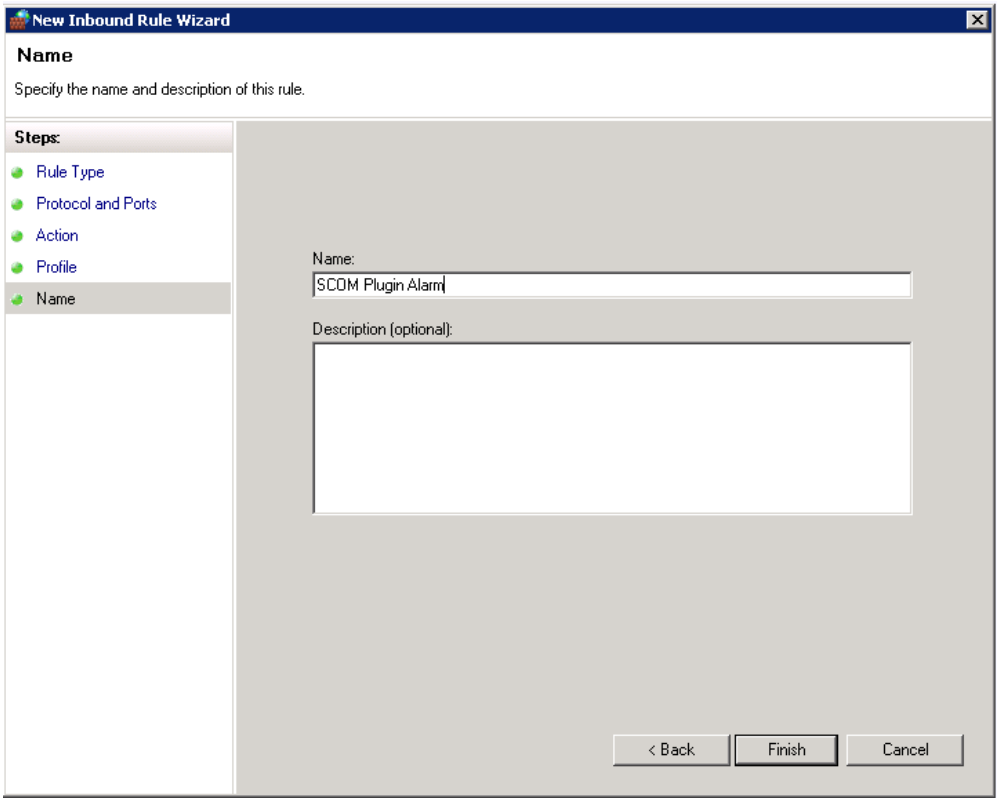
5. On the **Protocol and Ports** tab page, click **UDP**, and enter **162** in **Specific local ports**. Then click **Next**.



6. On the **Action** tab page, select **Allow the connection** and click **Next**.



7. On the **Profile** tab page, click **Next**.
8. On the **Name** tab page, enter a name for the rule in **Name**, for example, **SCOM Plugin Alarm**. Then click **Finish**.



Question 7:How can I do if SCOM acquires wrong community string?

Problem Description:

After installing the SCOM plug-in, the information is displayed quite slowly, sometimes even fails to be displayed while user checking the monitor information in device.

Problem Analysis:

Installing SCOM plug-in will trigger SCOM system problem － if the value of the SCOM system variable, **CommunityString**, is empty or incorrect, this issue will cause the security policy of storage devie being active, and then rejecting the request from SCOM for a while.

Solution:

No operation is required, and please be patient. Then it will be normal automatically after three minutes.

9 Acronyms and Abbreviations

Operation Console	Operation Console is an operation manager interface where operations such as monitoring, managing, creating, and reporting can be performed.
SCOM	Microsoft System Center Operations Manager (SCOM) is a component of Microsoft system center for monitoring infrastructure in a flexible, economical, and efficient manner. It can monitor data centers, public cloud, and private cloud and ensures the expected performance and availability of major programs.
MP	Manager Pack (MP) is a set of files that work with Operation Manager, enabling the administrator to monitor programs and add functions to Operation Manager.