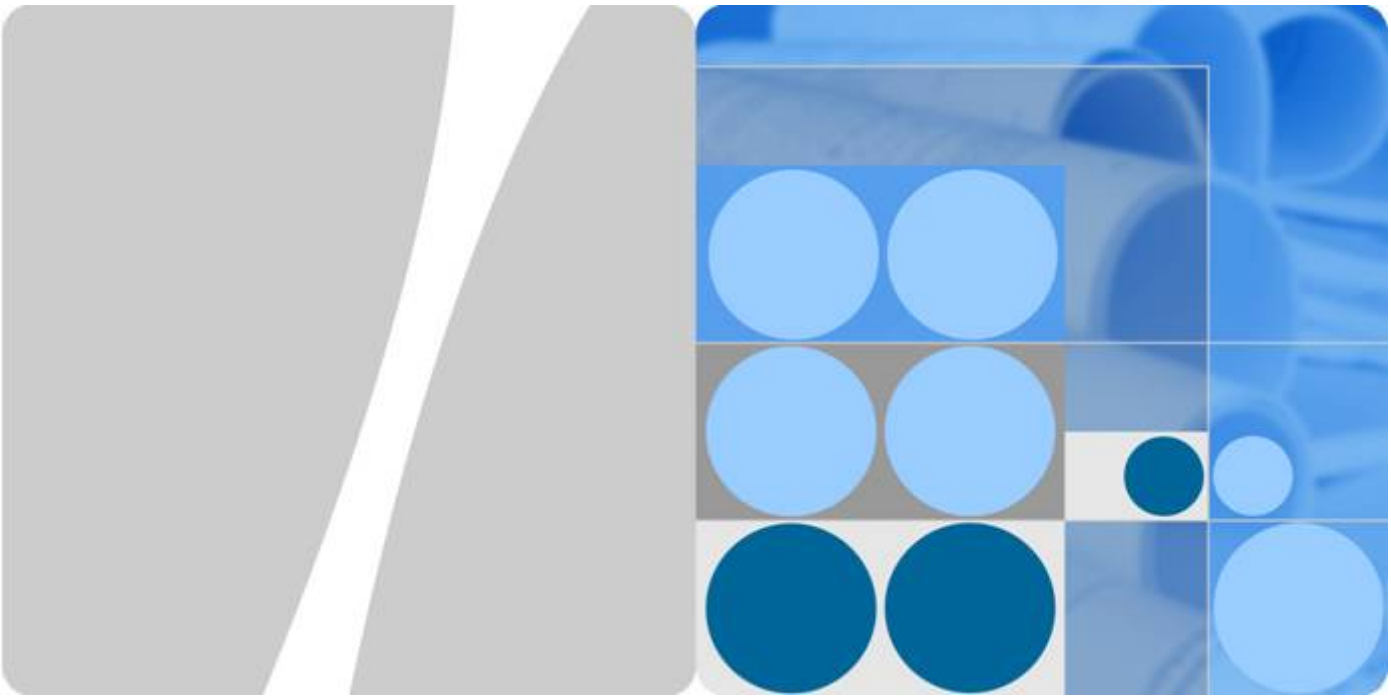


OceanStor InfraControl

V100R002C01

Admin Guide

Issue 04

Date 2015-02-28

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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://enterprise.huawei.com

About This Document

Purpose

This document describes the operations on the InfraControl NMS.

Intended Audience

This document is intended for:

- Installation and Commissioning Engineer
- Data Configuration Engineer
- System Maintenance Engineer

Symbol Conventions

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

Symbol	Description
DANGER	Indicates a hazard with a high level or medium level of risk which, if not avoided, could result in death or serious injury.
WARNING	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.
CAUTION	Indicates a potentially hazardous situation that, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results.
TIP	Provides a tip that may help you solve a problem or save time.
NOTE	Provides additional information to emphasize or supplement important points in the main text.

Command Conventions

The command conventions that may be found in this document are defined as follows.

Convention	Description
Boldface	The keywords of a command line are in **boldface**.
Italic	Command arguments are in *italic*.
[ ]	Items (keywords or arguments) in square brackets [ ] are optional.
{ x | y | ... }	Alternative items are grouped in braces and separated by vertical bars. One is selected.
[x | y | ...]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected.
{ x | y | ... } *	Alternative items are grouped in braces and separated by vertical bars. A minimum of one or a maximum of all can be selected.
[x | y | ...] *	Optional alternative items are grouped in square brackets and separated by vertical bars. A maximum of all or none can be selected.

GUI Conventions

Convention	Description
Boldface	Buttons, menus, parameters, tabs, window, and dialog titles are in **boldface**. For example, click **OK**.
>	Multi-level menus are in **boldface** and separated by the ">" signs. For example, choose **File** > **Create** > **Folder**.

Change History

Updates between document versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Issue 04 (2015-02-28)

The interface descriptions are modified.

Issue 03 (2014-09-30)

The contexts are modified.

Issue 02 (2014-04-21)

The contexts are optimized.

Issue 01 (2013-09-16)

This issue is the first official release.

Contents

1 Overview

About This Chapter

This chapter provides a general description of the InfraControl and basic operations on the InfraControl.

1.1 InfraControl Overview
The InfraControl provides comprehensive functions and complies with the unified interface standard. Managing network resources on the InfraControl improves service quality of transmission network and lowers maintenance costs.

1.2 Basic Configuration
Before managing a network element (NE) on the management system, you need to perform basic configuration on the NE and the management system. For the detailed configuration procedures of the automatic discovery function for various network elements (NEs), please see the ***OceanStor InfraControl V100R002C01 Initial Discovery Configuration Guide 01***.

1.3 Customizing the Home Panel
You can select frequently used components to customize the management system home page and save the home page layout.

1.4 Changing the Current Password
It is recommended that you periodically change your password to ensure security. This section describes how to change your password.

1.5 Viewing the Software Version
This section explains how to view the software version and support information of the management system.

1.6 Obtaining Help Information
This section describes how to obtain help information of the management system and get to know basic operations on the management system.

1.7 Logout
Logout enables you to exit the management system or log in to the management system again as another user.

1.1 InfraControl Overview

The InfraControl provides comprehensive functions and complies with the unified interface standard. Managing network resources on the InfraControl improves service quality of transmission network and lowers maintenance costs.

The InfraControl software is intended for enterprise data centers and used to manage SAN network environments in a unified fashion. The software provides the System Manager, System Reporter, and SAN Insight components. The System Manager is used for centralized management of Huawei T series, network attached storage (NAS) series, virtual intelligent storage (VIS) series and virtual tape library (VTL) backup products. The System Manager provides centralized alarm monitoring, storage capacity management, logical relationship and status management of internal system components, and logical management of storage systems and external hosts. The System Reporter provides built-in capacity reports and performance reports for storage systems. In addition, it provides periodic task report and self-defined report functions, identifying bottlenecks in performance and capacity increase trends based on different statistical granularities. The storage area network (SAN) Insight provides end-to-end management of storage, internet small computer system interface (iSCSI) switches, Fibre Channel switches, physical hosts (Windows, RedHat Linux, or SUSE Linux), VMware virtual machines, and applications. It manages both storage systems and storage directories in a graphical user interface (GUI) manner, simplifying management.

The InfraControl focuses on service management and integrates management of network resources and various applications, providing network administrators with an integrated solution that embodies resources management and network service management. It has the following functions:

- Resource Management

  Resource management: You can manage and monitor discovered storage devices, switches, hosts/virtual machines, and database applications.

- Alarm Management

  Alarm management: By viewing the current alarms on a network element (NE), you can discover and handle the NE faults in time.

  The alarm notification means is user-defined, including mail, short message (SMS), and sound alarm notification means. You can set alarm masking to mask alarms that you do not want to receive. You can also synchronize alarms manually or periodically on a monitored NE.

- **7 Report Management**

  Performance statistics: You can learn about the operating status of a storage device by viewing performance statistics on the InfraControl. This function provides performance and capacity reports, facilitating quick and periodic checking of the storage system performance. The reports show performances of LUNs, ports, controllers, and files system during the past 24 hours, 7 days, and 30 days. Detailed performance data of these objects during the periods are sorted by input and output operations per second (IOPS), bandwidth, latency, and other factors. Disks, ports, central processing unit (CPU), LUNs, and file systems ranking the top five are displayed on the report. Capacity usage of file systems, storage pools, and thin LUNs during the 24 hours, 7 days, and 30 days are provided by the capacity usage report. You can self-define reports and auxiliary period implementation policies to periodically generate reports of performance indicators and capacity usage that

you are concerned with. The report will be automatically sent to the specified administrator. The self-defined performance and capacity reports meet tailored user demands. This function enables you to define all performance indicators and capacity usage of all the objects in a past period of time you specify in the reports.

- **2 System Management**

  System management: This function enables you to perform configuration of system security policies, system performance monitoring, data maintenance management, operation log management, task management, license management, hierarchical management, notification server settings, system resource management, Simple Network Management Protocol (SNMP) module management, and secure file transfer protocol (SFTP) server settings.

NOTE

If the description in the online help differs from that on the InfraControl interface, the latter prevails.

1.2 Basic Configuration

Before managing a network element (NE) on the management system, you need to perform basic configuration on the NE and the management system. For the detailed configuration procedures of the automatic discovery function for various network elements (NEs), please see the ***OceanStor InfraControl V100R002C01 Initial Discovery Configuration Guide 01***.

1.3 Customizing the Home Panel

You can select frequently used components to customize the management system home page and save the home page layout.

Context

The management system presets summaries about certain important functions. These summaries serve as components for users to choose.

After selecting **Faults and Risks**, click  . The **Details About Faults and Risks** dialog box is displayed. In the dialog box, you can view fault and risk details about the device. You can also click **Send Email** to set (add or delete) a recipient's email address. The fault and disk details will be sent to the added email address.

After you select the **Device Status**component, click the **Status Distribution** bar chart to go to the **Device Status List** dialog box. In the **Device Status List** dialog box, you can click a device name to view details about the device status.

Procedure

Step 1 Customizing panel

1. On the menu bar, click **Home**.
2. Click **Customize Panels**.

   The **Customize Panels** dialog box is displayed.
3. Select the components to be displayed on the management system home page.

4. Click **OK**, The panel is customized successfully.

Step 2 Saving the layout

1. (Optional) Click the component name, and move the components to proper positions.
2. Click **Save Layout**, The current layout is saved successfully.

----End

1.4 Changing the Current Password

It is recommended that you periodically change your password to ensure security. This section describes how to change your password.

Context

The specified password must meet the requirements of the password policy. For details about the requirements of the password policy, see **2.1.6 Configuring the System Security Policy**.

Procedure

Step 1 Click  on the upper right of the page.

Step 2 In the **Change Password** dialog box, enter the old password.

Step 3 Enter a new password and confirm the password.

Step 4 Click **OK**.

The **Success** dialog box is displayed and you have finished changing the password.

----End

1.5 Viewing the Software Version

This section explains how to view the software version and support information of the management system.

Procedure

Step 1 Click  on the upper right of the page.

The **About** dialog box is displayed.

Step 2 View the software version and support information of the management system.

Step 3 Click  .

----End

1.6 Obtaining Help Information

This section describes how to obtain help information of the management system and get to know basic operations on the management system.

Procedure

Step 1 Click  on the upper right of the page.

The management system help information is displayed.

Step 2 Check the help information.

Step 3 Click  .

----End

1.7 Logout

Logout enables you to exit the management system or log in to the management system again as another user.

Procedure

Step 1 Click  on the upper right of the page.

The **Warning** dialog box is displayed.

Step 2 Carefully read the content in the dialog box and click **OK**.

The management system login page is displayed.

----End

2 System Management

About This Chapter

This chapter describes system management on the management system, including functions such as system administrators configuration, system monitoring, data maintenance, log management, task management, license management, and hierarchical management. These functions enable you to configure system security policies, monitor service management and system performance, export and dump system operation logs, manage rights and domains, import and export licenses, and monitor background tasks on the management system.

The hierarchical management function of the InfraControl balances processing capabilities among InfraControl servers. Each InfraControl server can be connected to network elements directly or through a lower-layer InfraControl server.

2.8 Discovery Management

After the NE is discovered, it is automatically displayed in the resource list of the management system. In the case of an NE discovery failure caused by network interruption, you can manually add NEs or stop discovering NEs.

2.9 Template Management

The management system provides three default SNMP templates. You can also create new SNMP templates as required.

2.10 Server Information

This section describes how to manage information about SFTP servers, including protocol types, user names, and passwords.

2.1 System Administrators

Configuring the system administrators helps guarantee the management system and data security.

2.1.1 Introduction to System Administrators

Configuring the system administrators can implement the configuration of system security policy, permission/domain-specific management of the management system, restriction to the IP addresses that access the management system, and can monitor and manage online administrators in real time.

The system security policy contains the password policy, login policy, and session timeout duration.

- The password policy defines the minimum length and complexity of the passwords of the system administrators.
- The session timeout duration refers to the period in which the session between the system administrator and the management system has been interrupted because of timeout. Any operations of the system administrator on the management system will clear the session timeout duration and restart the time counting.

  If the system administrator performs no operation within the timeout duration after logging in to the management system, the current session will be interrupted because of timeout. When the system administrator wants to perform operations on the management system again, the system administrator needs to re-log in to the management system.
- The login policy defines whether the system will be locked after the password has been entered incorrectly for a certain consecutive times within 10 minutes and when the system will be unlocked automatically if the system is locked.

The permission/domain management of the management system and the restriction to the IP addresses that access the management system are implemented by configuring the administrator groups and administrators as follows:

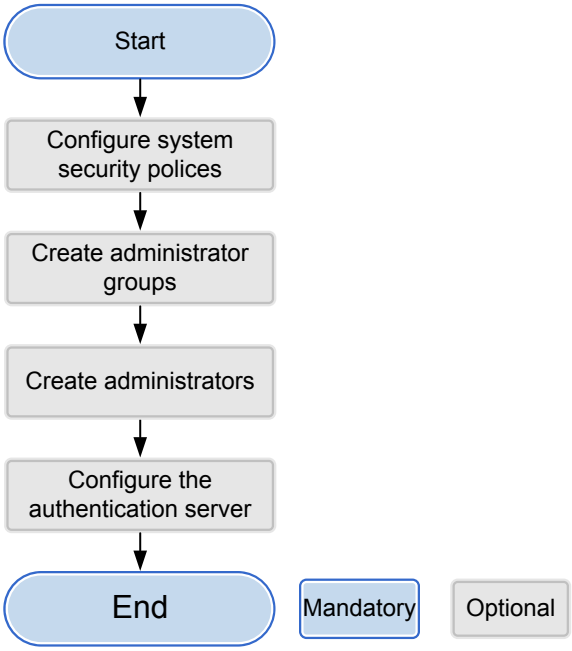
- The administrator groups are collections of the operation permissions. You can assign an administrator group to administrator so that the administrator can have the permission on this administrator group.
- The system provides the default administrator **admin**. The default administrator has all operation permission and can manage all resources. In addition, the default administrator cannot be modified. You can create a new administrator and select an administrator group and resources for this administrator to implement the permission/domain-specific management of the management system.
- You can select the IP address segments that can access the management system for an administrator to implement the restriction of IP addresses that access the management system.

2.1.2 Configuration Process

The configuration process provides the procedures for configuring the system security policy, administrator groups, and administrators.

Figure 2-1 shows the process for configuring the system administrators.

Figure 2-1 Process for configuring the system administrators



The following table lists the tasks for configuring the system administrators.

Table 2-1 Tasks for configuring the system administrators

Task	Description
Configuring the System Security Policy	Optional The management system provides the default security policy. You can modify the configuration of the security policy to guarantee the system security.
Creating an Administrator Group	Optional The management system provides three default administrator groups. This task is required when the permissions of the default administrator groups cannot meet the requirements on permissions.
Creating an Administrator	Optional The system provides the default administrator **admin**. This task is required when you need to implement permission/domain-specific management of the management system.

Task	Description
Configuring the Authentication Server	Optional This task is required when RADIUS authentication is adopted for the administrator.

2.1.3 Managing Administrators

The system provides one default administrator **admin**. The default administrator has all permissions, can manage all NEs, and can log in the management system from any IP addresses. To implement permission/domain-specific management of the management system, you can create administrators and modify, lock, unlock, or delete them.

1. On the menu bar, choose **Management**.
2. In the navigation tree, choose **System Administrators** > **Administrators**.
3. Set related information of system administrators by referring to the following table.

Operation	Description
Create	Click **Create** to create an administrator. For details about this operation, see **Creating an Administrator Account**.
Modify	Click  corresponding to the administrator to modify its information. For details about this operation, see **Modifying an Administrator**.
Modify Administrator Authentication Mode and Password	Click  corresponding to the administrator to modify its information. For details about this operation, see **Modifying an Administrator**.
Delete	Select one or more administrators and click **Delete** to delete them.
View	Click the user name of an administrator to view its description, associated administrator group, managed NEs, and allowed IP address segment.
Lock	To restrict the login of an administrator to the management system, select the administrator and click **Lock** to lock the administrator.

Operation	Description
Unlock	Select the locked administrator and click **Unlock** to unlock the administrator.

Creating an Administrator Account

When you need to perform the permission/domain specific management on the management system, you can join an administrator group to obtain the permission on this administrator group, select the NEs, and set the IP address segment for logging in to the management system.

Prerequisites

An administrator group has been created.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **System Administrators** > **Administrators**.

Step 3 In the function pane, click **Create**.

The **Create Administrator** dialog box is displayed.

Step 4 Set the parameters of the new administrator. The following table describes the parameters.

Parameter	Description	Value
User name	User name for logging in to the management system. After an administrator is created, its user name cannot be changed.	[Example] user01

Parameter	Description	Value
Authentic	Mode for authenticating the login of a system administrator to the management system, **Password** or **RADIUS**. ● Password authentication is a local authentication mode that the user name and password are directly specified on the management system server. Advantages of the password authentication: high speed, and low operation expenditure. Disadvantages of the password authentication: low security, and storage capacity restricted by the management system server hardware conditions. ● RADIUS authentication means that the user information is configured on the Remote Authentication Dial In User Service (RADIUS) server, and the management system communicates with the RADIUS server as the client and it performs the remote authentication through the RADIUS protocol. Advantages of the RADIUS authentication: High security and reliability when the third-party server is used for authentication because it supports the resending mechanism and standby server mechanism. Disadvantages of the RADIUS authentication: High operation expenditure as it requires the deployment of the RADIUS server.	[Example]

Parameter	Description	Value
ation Mode	**NOTE** When RADIUS authentication is adopted, you need to configure the RADIUS server. For details, see **2.1.7 Configuring the Authentication Server**.	Password
Password	Password for logging in to the management system when the password authentication is used. ● The password must contain no less than eight characters, no more than 64 characters. ● The password must contain special characters, uppercase letters, lowercase letters, and digits. Special characters include: `~!@#$%^&*()-_=+|[{}];:'",<.>/? and blank space. A specific password is subject to the password policy configured in the system security policy. For details about the specific requirements, see **2.1.6 Configuring the System Security Policy**.	[Example] A23!@23a
Confirm password	Enter the password again. The two passwords must be identical. The parameter value must be the same as that in **Password**.	[Example] A23!@23a
Description	Brief description of the administrator, helping identifying the administrator.	[Example] None

NOTE

The administrator users are created by **admin** user, and administrator users cannot modify, delete, lock, unlock or forced offline other administrator users and **admin** user.

Step 5 Click the **Administrator Group** tab, and select an administrator group for the administrator.

When multiple administrator groups are selected, the permission of the administrator is the permission collection of all the selected administrator groups.

Step 6 **Optional:** Click the **Resource** tab, and select manageable NEs.

- You can select **According to Resource Group** to select resources by resource group for the new administrator to manage.
- You can select **According to Resource Type** to select resources by resource type for the new administrator to manage.

Step 7 **Optional:** Click the **Login Network Segment** tab. Perform the following operations to configure the IP address segment list and then select one allowed IP address segment for the administrator.

Perform the following operations to set the IP network segment.

NOTE

The first field of an IP address must be an integer ranging from 1 to 223 (excluding 127), the last field must not be 0, and the other fields must be integers ranging from 0 to 255.

- Creating an IP network segment
  1. Click **Add**.

     The **Add Login Network Segment** dialog box is displayed.
  2. Set **Start IP address**, **End IP address**, and **Description**.
  3. Click **OK**.
- Modifying an IP network segment
  1. Select an IP network segment and click **Modify**.

     The **Modify Login Network Segment** dialog box is displayed.
  2. Set **Start IP address**, **End IP address**, and **Description**
  3. Click **OK**.
- Deleting an IP network segment
  1. Select an IP network segment and click **Delete**.

     The **Warning** dialog box is displayed.
  2. Click **OK**.

Step 8 Click **OK**.

The **Success** dialog box is displayed indicating that the operation succeeded.

Step 9 Click **OK**.

The newly created administrator is displayed in **Administrators**.

----End

Modifying an Administrator

Modifying an administrator includes modifying the authentication mode, password, description, and permission. You can also modify the administrator's domain and permission.

Context

- The default administrator **admin** can be modified only by itself. Editable information includes the password, description, and IP network segment for accessing the management system.

- If you forget the password of the default administrator **admin**, contact technical support engineers.
- The administrator users cannot modify, delete, lock, unlock or forced offline other administrator users and **admin** user.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **System Administrators** > **Administrators**.

Step 3 You can modify the administrator's description, domain, and permission.

1. Click  corresponding to the administrator to be modified.
   The **Modify Administrator Information** dialog box is displayed.
2. Set the parameters of the administrator, as described in **Creating an Administrator Account**.
3. Modify the permission, managed NEs, and allowed IP address segment of the administrator.
   - Click the **Select Administrator Group** tab, and select the administrator group as required from the administrator group list.
     When multiple administrator groups are selected, the administrator's permission is the combined permission of all the selected administrator groups.
   - On the **Select Resource** tab page, select NEs to manage.
   - On the **Select Login Network Segment** tab page, select an IP address for the administrator to log in to the management system.

   NOTICE

   The modification of administrator permission takes effect only after the administrator re-logs in to the management system. The modification of the NE information takes effect immediately after the modification is performed without requiring relogin.
4. Click **OK**.
   The **Success** dialog box is displayed.
5. Click **OK**.

Step 4 You can modify the administrator's authentication mode and password.

1. Click  corresponding to the administrator to be modified.
   The **Modify Administrator Information** dialog box is displayed.
2. Set the parameters of the new administrator. The following table describes the parameters.

Parameter	Description	Value
Authentication Mode	Mode for authenticating the login of a system administrator to the management system, **Local authentication** or **RADIUS**. ● Local authentication is a local authentication mode that the user name and password are directly specified on the management system server. Advantages of the password authentication: high speed, and low operation expenditure. Disadvantages of the password authentication: low security, and storage capacity restricted by the management system server hardware conditions. ● RADIUS authentication means that the user information is configured on the Remote Authentication Dial In User Service (RADIUS) server, and the management system communicates with the RADIUS server as the client and it performs the remote authentication through the RADIUS protocol. Advantages of the RADIUS authentication: High security and reliability when the third-party server is used for authentication because it supports the resending mechanism and standby server mechanism. Disadvantages of the RADIUS authentication: High operation expenditure as it requires the deployment of the RADIUS server. **NOTE** When RADIUS authentication is adopted, you need to configure the RADIUS server. For details, see **2.1.7 Configuring the Authentication Server**.	[Example] RADIUS
Current user password	The current user password for logging in to the management system when the password authentication is used.	[Example] A23!@23a

Parameter	Description	Value
New password	Configure the new password for logging in to the management system when the password authentication is used. ● The password must contain no less than eight characters, no more than 64 characters. ● The password must contain special characters, uppercase letters, lowercase letters, and digits. Special characters include: `~!@#$%^&*()-_=+ |[{}];:'",<.>/? and blank space . A specific password is subject to the password policy configured in the system security policy. For details about the specific requirements, see **2.1.6 Configuring the System Security Policy**.	[Example] -
Confirm password	Enter the password again. The two passwords must be identical. The parameter value must be the same as that in **New password**.	[Example] -

NOTE

The administrator users are created by **admin** user, and administrator users cannot modify, delete, lock, unlock or forced offline other administrator users and **admin** user.

3. Click **OK**.

   The **Success** dialog box is displayed.

4. Click **OK**.

----End

2.1.4 Managing Administrator Groups

Different administrator groups have different permission sets. When creating an administrator account, select the administrator group for it so that the account has related permission of the administrator group. The system provides three default administrator groups: administrator, operator, and auditor groups. These three default administrator groups cannot be modified or deleted.

1. On the menu bar, choose **Management**.
2. In the navigation tree, choose **System** > **Administrator Groups**.
3. Set related information about system administrators by referring to the following table.

Operation	Description
Create	Click **Create** to create an administrator group. For details about this operation, see **Creating an Administrator Group**.
Modify	Click  corresponding to the administrator group to modify its description and permission set. For details about this operation, see **Modifying an Administrator Group**. When the administrator group has associated administrators, the permissions of these administrators will also be modified after the administrator group permission is modified. The modification of administrator permissions takes effect upon the next login.
Delete	Select one or more administrator groups, and click **Delete** to delete the selected administrator groups. An administrator group can be deleted only when it has no associated administrator.
View	Click the name of the administrator group, and view its description and permission set.
Associated Administrators	Click the number of administrators associated with an administrator group to view the information about these associated administrators.

Creating an Administrator Group

The system provides three default administrator groups: **Administrator**, **Operator**, and **Auditor**. When the default administrator groups' permission cannot meet permission assignment requirements, you can create a new administrator group.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **System Administrators** > **Administrator Groups**.

Step 3 In the function pane, click **Create**.

The **Create Administrator Group** dialog box is displayed.

Step 4 Set information about the created administrator group.

1. The following table describes the parameters.

Parameter	Description	Setting
Name	Name of the administrator group.	[Example] Operator

Parameter	Description	Setting
Description	Description of the administrator group.	[Example] Operational role

2. In the **Permission Set**, set the permission of the administrator group.

Step 5 Click **OK**.

The **Success** dialog box is displayed indicating that the creation succeeded.

Step 6 Click **OK**.

----End

Modifying an Administrator Group

The current administrator can modify the description and permission set of a non-default administrator group. When the administrator group has associated users, the modification of the administrator group's permission applies to these users. The modification of user permission takes effect upon the next login.

Context

The administrator is not allowed to modify the three default administrator groups **Administrator**, **Operator**, and **Auditor**.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **System Administrators** > **Administrator Groups**.

Step 3 Click  corresponding to the administrator group to be modified.

The **Modify Administrator Group** dialog box is displayed.

Step 4 Modify the description or permission set of the administration group. For description about related parameters, see **Creating an Administrator Group**.

Step 5 After the modification is complete, click **OK**.

The **Success** dialog box is displayed.

Step 6 Click **OK**.

----End

2.1.5 Managing Online Administrators

To prevent unauthorized login to the management system, you can monitor online administrators in real time and forcibly log off the unauthorized administrators.

Prerequisites

- To view the online administrators, the current administrator must have the permission to view the online administrators.
- To forcibly log off an online administrator, the current administrator must have the permission to forcibly log off an online administrator.

Context

Session is the connection set up between the browser and the server. One administrator can generate multiple sessions. The forcible logout operation is applicable to only the administrator that generates the session concerned. For example, administrator **user** logs in to the same server from clients A and B and generates sessions a and b. When you forcibly log off the administrator **user** that generates session a, the administrator **user** that generates session b will not be affected.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **System Administrators** > **Online Administrator**.

Step 3 View online administrators and their login information on the **Online Administrators** page.

Step 4 Forcibly log out an administrator.

1. Select an administrator you want to log out and click **Force Offline**.
   The **Warning** dialog box is displayed.
2. Click **OK**.

----End

2.1.6 Configuring the System Security Policy

The system security policy contains the password policy, login policy, and session timeout duration. Configuring the system security policy can improve the system security.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **System Administrators** > **Security Policies**.

Step 3 In the function pane, click **Modify**.
The **Modify Security Policy** dialog box is displayed.

Step 4 Set security policy parameters on the **Modify Security Policy** page, as described in the following table.

Table 2-2 Security policy parameters

Parameter	Description	Value
Minimum length	Minimum length of the password, avoiding too short passwords.	Default value: 8 characters.

Parameter	Description	Value
Complexity	Complexity of the password, avoiding too simple passwords.	Default value: Must contain special characters, uppercase letters, lowercase letters, and digits
Set a validity period for the password	Enabling the setting of the password's validity period.	[Example] -
Validity period	Validity period of the administrator password. When this period has passed, the system asks to change the password in a timely manner. This parameter is available only when **Set a validity period for the password** is enabled.	[Value Range] An integer ranging from 60 to 360. [Example] 360
Min.Password Lifespan(minutes)	Minimum password lifespan of the administrator password. When this time has passed, you can change the password. This parameter is available only when **Set a validity period for the password** is enabled.	[Value Range] An integer ranging from 1 to 9999. [Example] 10
Timeout (minutes)	If the online user performs no operation within this timeout duration, the system will display the message of timeout upon the next operation. In this case, click **OK** to return to the login page.	[Value Range] An integer ranging from 1 to 100. [Example] 10
Incorrect password lock	After the incorrect password lock is enabled, the administrator will be locked when its password is entered incorrectly reaches the **Allowed attempts** times within 10 minutes.	[Example] -
Attempts	Times allowed for consecutively entering incorrect passwords. When the number of error times reaches the specified value, the management system automatically locks the account. **NOTE** After the administrator is locked, it can be manually unlocked by the default administrator **admin** or another administrator who has the unlock permission, or automatically unlocked after the lock time is up. After the incorrect password lock is enabled, you can set this parameter.	[Value Range] An integer ranging from 1 to 9. [Example] 3

Parameter	Description	Value
Lock(minutes)	You can set how long the administrator will be automatically locked by the system. When the specified time period comes, the administrator is automatically unlocked. ● This parameter is only valid for the automatic lock. If the administrator is locked manually, it can only be unlocked manually. ● After the incorrect password lock is enabled, you can set this parameter.	[Value Range] An integer ranging from 3 to 2000. For example, because the administrator **test** enters incorrect passwords for reaching **Allowed attempts** times, the administrator is locked automatically. If **Lock (minutes)** is set **3**, the administrator will be unlocked automatically three minutes later. [Example] 3

Step 5 Click **OK**.

The **Success** dialog box is displayed indicating that the operation succeeded.

Step 6 Click **OK**.

----End

2.1.7 Configuring the Authentication Server

The authentication server needs to be correctly configured if administrator authentication uses the Remote Authentication Dial-In User Service (RADIUS).

Prerequisites

An authentication server is available.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **System Administrators** > **Authentication Server**.

Step 3 Click **Modify**.

The **Modify RADIUS Server** dialog box is displayed.

Step 4 Set RADIUS server parameters that are listed in the following table.

Parameter	Description	Value
Auth mode	Mode for the RADIUS server to authenticate administrators. ● **PAP**: uses a plain text password and requires two-way handshakes. Compared with challenge handshake authentication protocol (CHAP) authentication, it is superior in authentication efficiencies but inferior in security. ● **CHAP**: uses a cipher text password and requires three-way handshakes. Compared with password authentication protocol (PAP) authentication, it is superior in security but inferior in authentication efficiencies. Main and spare RADIUS servers use the same authentication method.	[Example] CHAP **NOTE** You are advised to select the **CHAP** which is superior in security, compared with **PAP** authentication protocol .
Main IP address	IP address of the main RADIUS server.	[Value range] The first field of an IP address must be an integer ranging from 1 to 223 (excluding 127), the last field must not be 0, and the other fields must be integers ranging from 0 to 255. [Example] 192.168.10.13
Spare IP address	IP address of the spare RADIUS server.	[Value range] The first field of an IP address must be an integer ranging from 1 to 223 (excluding 127), the last field must not be 0, and the other fields must be integers ranging from 0 to 255. [Example] 192.168.10.16

Parameter	Description	Value
Port	Port of the RADIUS server. Main and spare RAIDUS servers use the same port.	[Value range] An integer between 1 and 65,535 [Example] 1812
Shared key	Encrypts RADIUS authentication packets to safeguard authentication information during transfer. ● To authenticate the identities of involved parties, the shared key must be the same as the key configured on the RADIUS server. ● Main and spare RADIUS servers use the same shared key.	[Example] -

Step 5 Click **OK**.

The **Success** dialog box is displayed indicating that the operation succeeded.

Step 6 Click **OK**.

----End

2.2 System Monitoring

This section describes system performance management.

2.2.1 System performance

This section describes how to discover and handle exceptions in time, ensuring normal and efficient operating of the management system.

Modifying Thresholds

When hardware usage exceeds the specified threshold, the system generates an alarm to facilitate monitoring of resource usage. This section describes how to modify CPU, memory, and hard disk usage thresholds.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **System Monitoring** > **System Performance**.

Step 3 In the function pane, click **Modify** in the **Threshold Setting** area.

The**Modify Threshold** dialog box is displayed.

Step 4 Modify related thresholds, as described in the following table.

Parameter	Description	Value
CPU usage threshold (%)	Threshold of CPU usage. The value ranges from 1 to 99.	[Example] 50
Memory usage threshold (%)	Threshold of memory usage. The value ranges from 1 to 99.	[Example] 50
Disk usage threshold (%)	Threshold of disk usage. The value ranges from 1 to 99.	[Example] 50

Step 5 After the modification is complete, click **OK**.

The **Success** dialog box is displayed indicating that the operation succeeded.

Step 6 Click **OK**.

----End

Monitoring System Performance

System performance indicates usage of system resources. By monitoring system performance, you can check usage of CPU, memory, and hard disks to learn about the system working conditions and detect faults in time.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **System Monitoring** > **System Performance**.

Step 3 In the **System Performance** area of the function pane, check usage of CPU, memory, and hard disks. The following table describes related parameters in the **System Performance** area.

The system collects the performance data periodically.

Parameter	Description
CPU	If the CPU usage has exceeded the threshold for three consecutive times, the management system generates an alarm. When the CPU usage becomes lower than the threshold, the alarm is cleared automatically. The red line represents the threshold.

Parameter	Description
Memory	If the memory usage has exceeded the threshold for three consecutive times, the management system generates an alarm. When the memory usage becomes lower than the threshold, the alarm is cleared automatically. The red line represents the threshold.
Disk	If the disk usage exceeds the threshold, the management system generates an alarm. When the disk usage becomes lower than the threshold, the alarm is cleared automatically.

----End

2.3 Data Maintenance

During the system operation, operation logs and alarms will be generated, recording operating conditions of the system. With the data maintenance function on the management system, you can dump operation logs and alarms and save them to the management system server.

2.3.1 Operation Log Dump

The system operation logs record operations performed by administrators on the management system. The operation log dump function of the management system enables you to dump system operation logs and manage historical dump records.

Setting Dump Parameters

This section describes how to set related parameters of system operation log dump. The system periodically dumps system operation logs in the database and saves it in a .txt file to a specified directory on the management system server. Meanwhile, the system deletes the operation logs in the database to save space and improve operating efficiency of the management system.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **Data Maintenance** > **Log Dump**.

Step 3 In the **Dump Settings** area of the function pane, click **Modify**.
The **Modify Dump Parameter** dialog box is displayed.

Step 4 Modify dump parameters, as described in the following table.

Parameter	Description	Setting
Dump schedule	Time when the management system automatically dumps operation logs. The dumping time is usually specified to a point in time the management system is idle, for example, 02:00:00.	[Example] 02:00:00
Dump period (days)	Period after which the management system starts to dump logs.	[Value range] An integer ranging from 7 to 120. [Example] 50
Reserve recent data records (days)	Days during which generated logs are to be reserved.	[Value range] An integer ranging from 7 to 120. [Example] 50
File format	Format of the dumping file. The universal format of the operating log dump file is **Excel** and **CSV**.	[Example] Excel
Language	Language of the dumping file, **English** or **Simple Chinese**.	[Example] English

Step 5 After the modification is complete, click **OK**.

The **Success** dialog box is displayed indicating that the operation succeeded.

Step 6 Click **OK**.

----End

Managing Dump History

This section describes how to manage dump history of operation logs.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **Data Maintenance** > **Log Dump**.

Step 3 In the **Dump History** area of the function pane, view dump history of operation logs. The following table describes the parameters.

Parameter	Description	Value
Started Time	Time when the operation log dump started.	[Example] -
End Time	Time when the operation log dump ended.	[Example] -
Execution Result	Execution result of the operation log dump.	[Example] Success
Operation	Download of the operation log.	[Example] -

NOTE

In the **Dump History** area, you can choose one historical dump record and click **Delete** to delete the record.

----End

2.3.2 Alarm Dump

This section describes how to dump system alarms and manage alarm dump history.

Setting Dump Parameters

This section describes how to set dump parameters. The system periodically dumps system alarms in the database and saves it in a .txt file to a specified directory on the management system server. Meanwhile, the system deletes the alarm information in the database to save space and improve operating efficiency of the management system.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **Data Maintenance** > **Alarm Dump**.

Step 3 In the **Dump Settings** area of the function pane, click **Modify**.

The **Modify Dump Parameter** dialog box is displayed.

Step 4 Modify dump parameters, as described in the following table.

Parameter	Description	Value
Dump schedule	Time when alarm dump starts. The dumping time is usually set to offpeak time of the management system, for example, 02:00:00.	[Example] 02:00:00

Parameter	Description	Value
Dump period (days)	Days when the alarm information is stored on the management system server before it is dumped. If the dumping period is specified to 7 days, the management system dumps alarms once every 7 days.	[Value range] An integer ranging from 7 to 120. [Example] 50
Reserve recent data records (days)	Logs that were generated in the recent X days are reserved.	[Value Range] An integer ranging from 7 to 120. [Example] 50
File format	Format of the dumping file, **Excel** or **CSV**.	[Example] Excel
Language	Language of the dumping file, **English** or **Simple Chinese**.	[Example] English

Step 5 After the modification is complete, click **OK**.

The **Success** dialog box is displayed indicating that the operation succeeded.

Step 6 Click **OK**.

----End

Managing Dump History

This section describes how to manage dump history of alarm information.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **Data Maintenance** > **Alarm Dump**.

Step 3 In the **Dump History** area of the function pane, view dump history of alarm information. The following table describes the parameters.

Parameter	Description	Value
Started Time	Time when the operation alarm dump started.	[Example] -
End Time	Time when the operation alarm dump ended.	[Example] -

Parameter	Description	Value
Execution Result	Execution result of the operation alarm dumping.	[Example] Success
Operation	Download of the operation alarm.	[Example] -

NOTE

In the **Dump History** area, you can choose a historical record and click **Delete** to delete the record.

----End

2.3.3 Exporting an Acceptance Report

This task helps you export device hardware information to learn about basic information about devices.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **Data Maintenance** > **Export Report**.

Step 3 In the function pane, click **Export**.

Step 4 In the dialog box that is displayed, click **Save**. Select a location to save the file to be exported and click **Save**.

----End

2.4 Log Management

This section describes how to manage system operation logs. The system operation logs record operations performed by administrators on the management system. The log management function of the management system enables you to query, view, and export operation logs.

All operations are logged if they are initiated by management system users and affect the database. Those operations that do not affect the database are not logged, such as viewing, searching, and refreshing. The management system provides the functions of browsing operation logs and filtering logs by log level, administrator, log category, operation results, and log start time and end time. Logs help learn about users' operations. For example, you can view operations performed by a user on the management system.

Different users have different permission for the management system. Super administrators have all permission. Administrators that are granted the access permission can only view their operation logs. Administrators without the access permission cannot view any operation log.

Periodic operation log dumping stores the logs recorded in the database to the **installation directory/Runtime/LegoRuntime/datastorage/sysoptlog** path on the management system

server. You can download the dumped operation logs to the client and view them locally. In addition, you can delete the logs that are no longer needed from the management system server, reducing the recording times of the database operations and ensuring sufficient database space.

Operation log level identifies how severe a log is. An operation log level can be danger, minor, warning, or info in descending severity sequence. The following table describes the four operation log levels.

Table 2-3 Log levels

Level	Definition
Danger	Indicates operations causing problems or failures of the system of function modules.
Warning	Indicates operations causing data inconsistency between the system and function modules.
Minor	Indicates normal operations related to the system or function modules.
Info	Indicates data access to the system or function modules.

2.4.1 Viewing System Operation Logs

A system operation log records operations performed by a user after logging in to the management system. This section describes how to view detailed operation information by viewing system operation logs.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **Log Management** > **System Logs**.

Step 3 In the **Severity** list, select a log level. In the **Result** list, select a result to query. Click **Search** to query operation information about the selected result of the selected log level.

Step 4 In the function pane, view information about the system log. The following table describes the parameters.

Parameter	Description	Value
Name	Name of the system log.	[Example] Log In
Severity	Level of the system log.	[Example] Info
Administrator	Name of the current logged-in administrator.	[Example] admin

Parameter	Description	Value
Occurred At	Time when the system log was generated.	[Example] 2012-05-08 17:11:26
Result	Execution result of the system log.	[Example] Succeeded
Client IP Address	IP address of the management terminal that executes the system log.	[Example] 10.27.80.92
Object	Name or IP address of the device that executes the system log. **NOTE** If the device is a Fibre Channel switch, **Object** will be displayed as **Model-IP address**.	[Example] Quidway-192.168.100.68
Detail	Details of the system log.	[Example] -

----End

2.5 Task Management

This chapter describes background task management on the management system.

2.5.1 Managing Background Tasks

Some tasks taking a long time to implement are run in background to avoid waiting for the system to return the result. This section describes how to view, query, and delete background tasks.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, select the **Task Management** > **Background Tasks**.

Step 3 In the **Results** drop-down list, choose the result you want to query. Click **Search** to query information about the corresponding task.

Step 4 In the function pane, view information about the background task. The following table describes the parameters.

Parameter	Description	Value
Name	Name of the background task.	[Example] Refreshing a VIS system

Parameter	Description	Value
Object Name	Name of an object of the back ground task.	[Example] VIS-001
Operator	User who performs the background task.	[Example] admin
Start Time	Time when the background task starts.	[Example] 2012-05-08 17:11:26
End Time	Time when the background task ends.	[Example] 2012-05-08 17:14:20
Task Progress	Progress of the background task.	[Example] 100%
Result	Result of the background task, including **Succeeded**, **Failed**, and **Processing**.	[Example] Succeeded
Task Details	Task details of the background task, click the details, the **Task Result Details** dialog is opened.	[Example] -

Step 5 Delete one or more task records.

1. Select one or more tasks and click **Delete**.
   The **Warning** dialog box is displayed.
2. Click **OK**.

----End

2.5.2 Viewing Details About Background Task Results

This operation allows you to view details about background task results.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **Task Management** > **Background Tasks**.

Step 3 From the drop-down list on the right of **Results**, choose the result that you want to query and click **Search** to search for related task information.

Step 4 In **Task Details**, click desired information.

The **Task Result Details** dialog box is displayed. **Table 2-4** lists parameters in task details.

Table 2-4 Parameters in task result details

Parameter	Description	Value
Name	Name of a task.	[Example] Refreshing a VIS system
Result	Execution result of a task. The result can be **Succeeded**, **Processing** or **Failed**.	[Example] Succeeded
Task Details	Details about a task result.	[Example] sf

Step 5 Click **Close**. The **Task Result Details** dialog box is closed.

----End

2.6 License Management

A license controls application scope, functions, and expiration date of products. This chapter describes how to view license information, and import and export license files on the management system.

2.6.1 Applying for a License

The management system license decides which functions to be supported by the management system. You must import the management system license file upon your first login to the management system. Therefore, you have to apply for a management system license first.

Context

- The license file is not delivered on the management system installation compact disc read-only memory (CD-ROM). You have to apply for the management system license with the license authorization code (LAC) and equipment serial number (ESN).
- The ESN is determined by the media access control (MAC) address of the server's network adapter. Multiple network adapters have multiple ESNs. Save all ESNs. If you store only one ESN and the corresponding network adapter is replaced, you have to apply for a new license.

Procedure

Step 1 Obtain the LAC from the license authorization certificate.

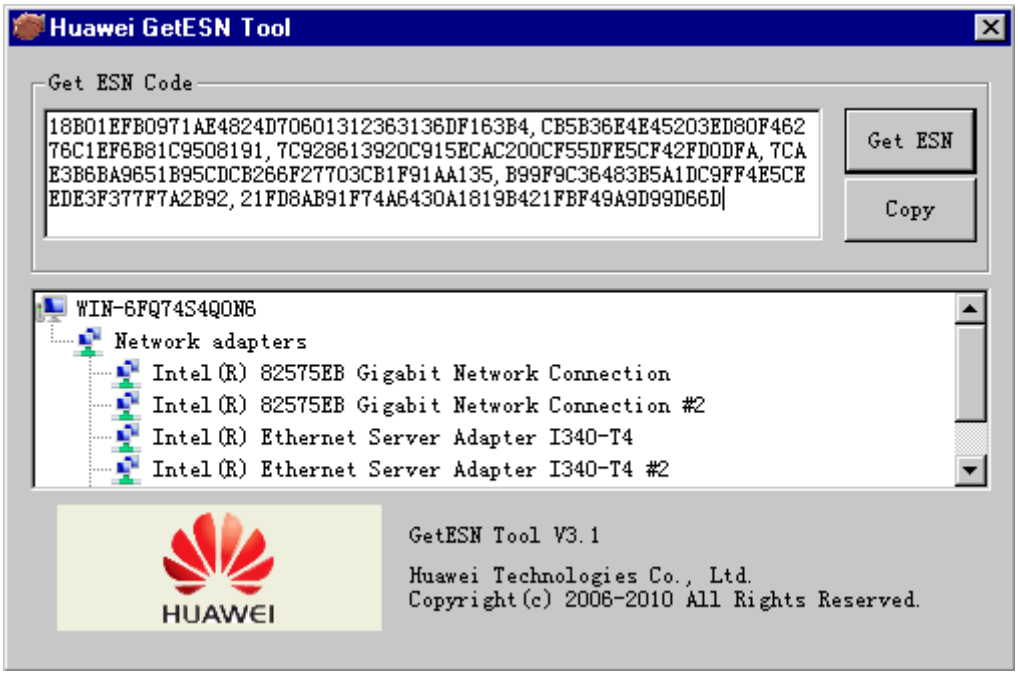
Step 2 Obtain the server's ESN by using the ESN tool provided by the management system, or view the server's ESN in the ESN list upon your initial login.

- On Windows:

  After installing the management system, you can obtain the server ESN by using the management system ESN tool.

On the NMS server, go to the location of the **GetESN.exe** file (**installation directory\Runtime\LegoRuntime\tools** directory), for example, **C:\Runtime\LegoRuntime\tools**, and run the **GetESN.exe** to view the ESN of the server, as shown in **Figure 2-2**.

Figure 2-2 Obtain the ESN.



- On Linux:

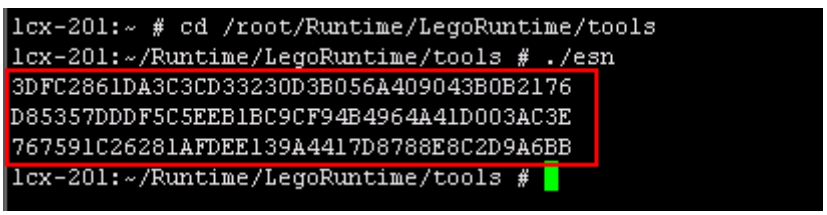
  After installing the management system, you can obtain the server ESN by using the management system ESN tool.

  On the NMS server, go to the location of the **esn** file (**installation directory\Runtime\LegoRuntime\tools** directory), for example, **root\Runtime\LegoRuntime\tools**, and run the **./esn** command to view the ESN of the server, as shown in **Figure 2-3**.

  NOTE

  If the NMS server has N network adapters, N ESNs will be displayed. On the screen, one ESN occupies a single line, as shown in **Figure 2-3**. If there are N ESNs, separate the ESNs with commas.

Figure 2-3 Obtain the ESN.



Step 3 Send the LAC and server's ESN to **license@huawei.com**.

After receiving your email, technical support engineers will confirm the information and send the license to your email box if the information is correct. You can download the license file to any local directory and import it upon your first login to the management system.

----End

2.6.2 Importing a System License

This section describes how to import a purchased license file to the management system.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **License Management** > **System License**.

Step 3 In the function pane, click **Import**.
The **Import License** dialog box is displayed.

Step 4 Click **Browse**.
The **Select a License File** dialog box is displayed.

Step 5 Select a valid license file and click **Open**.
The **Import License** dialog box is displayed.

NOTE

The size of a license file cannot exceed 2 MB.

Step 6 Click **OK**.
The license is imported.

----End

2.6.3 Exporting a System License

This section describes how to export a system license file to the local system.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **License Management** > **System License**.

Step 3 Click **Export** above the function pane.
The **File Download** dialog box is displayed.

NOTICE

The download means varies with different web browsers. Download by referring to prompted messages.

Step 4 Click **Save**.
The **Save As** dialog box is displayed.

Step 5 Click **Save** to select a path for saving the file.
The system indicates the download is complete.

----End

2.6.4 Viewing a System License

This section describes how to view license information and learn about the expiration date of a license.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **License Management** > **System License**.

Step 3 In the **License Feature Item** area of the function pane, query license information. The following table describes the parameters.

Parameter	Description
Name	Name of the license feature item.
Expired On	Expiration date of the license feature item.

Step 4 On the lower part of the function pane, click **Function Item** to query information about a function license. The following table describes the parameters.

Parameter	Description	Parameter Setting
Feature Segment	Information about the license feature.	SAN Insight
Function	Name of the license function item.	SAN Insight-Base License

Step 5 On the lower part of the function pane, click **Resource Item** to query information about a resource license. The following table describes the parameters.

Parameter	Description	Parameter Setting
Feature Segment	Information about the license feature.	System Reporter
Resource Type	Type of the resource that corresponds to the license.	System Reporter-Manage 1 Storage Device - Base License
Used Resources	Used resources of the license.	7
Available Resources	Available resources of the license.	93

----End

2.7 Hierarchical Management

The hierarchical management function of the InfraControl balances processing capabilities among InfraControl servers. Each InfraControl server can be connected to network elements directly or through a lower-layer InfraControl server.

2.7.1 Hierarchical NMS

After a hierarchical network management system (NMS) is configured, the InfraControl can manage the hierarchical NMS and test the connectivity with the hierarchical NMS.

Procedure

1. On the menu bar, choose **Management**.
2. In the navigation tree, choose **Layered NMS** > **Layered NMS**.
3. Refer to the following table to configure hierarchical NMS.

Operation	Description
Modify	Click  corresponding to the hierarchical NMS to be modified.
Add	Click **Add** to add a hierarchical NMS. For details, see **Adding a Hierarchical NMS**.
Delete	Select one or more hierarchical NMSs and click **Delete** to delete the hierarchical NMS or NMSs.
Enable	Select one or more hierarchical NMS whose status is **Disabled** and click **Enable** to enable the hierarchical NMS.
Disable	Select one or more hierarchical NMS whose status is **Enabled** and click **Disable** to disable the hierarchical NMS.
Test	Click  to test the hierarchical NMS.

Modifying the Service Configuration

This task helps you modify the service configuration.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **Layered NMS** > **Layered NMS**.

Step 3 In the **Service Configuration**, click **Modify**.

The **Modify Service Configuration** dialog box is displayed.

Step 4 Enter the new IP address.

Step 5 Click **OK** to finish modifying the report configuration.

----End

Adding a Hierarchical NMS

This task helps you add a hierarchical network management system (NMS).You can add a hierarchical NMS only when two or more NMSs are running the InfraControl.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **Layered NMS** > **Layered NMS**.

Step 3 In the **Service Configuration** area, click **Modify**.

The **Modify Service Configuration** dialog box is displayed.

Step 4 Click **Add**.

The **Add Layered NMS** dialog box is displayed.

Step 5 In **IP Address**, enter the management IP address of the NMS.

NOTE

- A hierarchical NMS can be successfully added only after both its upper-layer and lower-layer NMSs are correctly configured.
- You need to set the actual IP address of the NMS. If the NMS has multiple network adapters, you can choose one of them and ensure that the network adapter's IP address resides on the same subnet as the peer hierarchical NMS.
- For an NMS running HA service, set a floating IP address.

Step 6 Set the parameters related to hierarchical NMS.

Parameter	Description
NMS address	Address of the NMS to be added. For example, **https://192.168.0.1**. **NOTE** The address must start with *https*. Add the actual port number if the NMS does not use the default port.
Username	User name of the NMS to be added.
Password	User password of the NMS to be added.
NMS name	Name of the NMS to be added.
Data Report Status	Specifies whether to enable the data report function. **NOTE** The data report function is also known as the alarm report function.

Parameter	Description
Description	Brief description of the hierarchical NMS.

Step 7 Click **OK** to complete adding a hierarchical NMS.

----End

2.7.2 Managing Trap IP Addresses

After you configure a Trap IP address, the other network management systems (NMSs) can receive alarms from the management system.

Context

1. On the menu bar, choose **Management**.
2. In the navigation tree, choose **Layered NMS** > **Trap IP Address Management**.
3. Set related information about system administrators, as described in the following table.

Operation	Description
Add	You can click **Add** to add a Trap IP address. For details, see **Adding a Trap IP Address**.
Modify	Click  corresponding to a Trap IP address to modify related information. For details, see **Modifying a Trap IP Address**.
Delete	Select one or more Trap IP addresses and click **Delete** to delete them.

Adding a Trap IP Address

You can add a Trap IP address to enable the other network management systems (NMSs) to receive alarms from the management system using the Trap IP address.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **Layered NMS** > **Trap IP Address Management**.

Step 3 Click **Add**.

The **Add Trap IP Address** dialog box is displayed.

Step 4 Set **IP address** for the other NMSs to receive alarms and **Port** for accessing an NE.

Step 5 Click **OK**.

----End

Modifying a Trap IP Address

Modifying a Trap IP address includes modifying the IP address and the port number for receiving alarms.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **Layered NMS** > **Trap IP Address Management**.

Step 3 Click the corresponding to the Trap IP address.

The **Modify Trap IP Address** dialog box is displayed.

Step 4 Set the **IP address** and **Port** for receiving alarms.

Step 5 Click **OK**.

----End

2.7.3 Trap Configuration

To enable devices to be loaded to the network management system (NMS) by the automatic discovery function, configure the NMS northbound Trap reporting parameters and hierarchical NMS Trap parameters.

Context

1. On the menu bar, choose **Management**.
2. In the navigation tree, choose **Layered NMS** > **Trap Configuration**.
3. Set related information about Trap, as described in the following table.

Item	Description
Northbound Trap reporting parameters	Click or **Modify** corresponding to a Trap to modify related information. For details, see **Modifying Northbound Trap Reporting Parameters**. Click to refresh the information.
Hierarchical NMS Trap parameters	Click or **Modify** corresponding to a Trap to modify related information. For details, see **Modifying Hierarchical NMS Trap Parameters**. Click to refresh the information.

Modifying Northbound Trap Reporting Parameters

To enable devices to be loaded to the network management system (NMS) by the automatic discovery function, configure the NMS northbound Trap reporting parameters.

Context

NOTICE

The storage arrays use the MD5 to encrypt device users' passwords. There is a possibility that device users' passwords are cracked and leaked.

NOTE

The northbound default user is **user**, and default **Authentication password** is **Admin@123**, change the password as prompted. You are prompted to change the password regularly.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **Layered NMS** > **Trap Configuration**.

Step 3 Click the or **Modify**.

The **Modify northbound Trap reporting parameters** dialog box is displayed.

Step 4 Set related information about northbound Trap reporting parameters, as described in the **Table 2-5**.

Table 2-5 Northbound Trap reporting parameters

Parameter	Description	Setting
Username	Indicates the user name of the storage device.	[Value range] The name is a string of 1 to 64 characters. [Example] user
Context name	Name of the environment engine.	[Value range] The name is a string of 1 to 64 characters. [Example] sa
Context engine ID	Unique identifier of an SNMP engine. This ID is used together with the environment name to determine an environment that uniquely identifies an SNMP entity.	[Example] -
Authentication protocol	Protocol used for verifying messages, select **HMACMD5**, **HMACSHA** or not select.	[Example] HMACSHA

Parameter	Description	Setting
Authentication password	If the **HMACMD5** or **HMACSHA** protocol is selected, you need to set the authentication password. In the right textbox, click **Modify** to modify the password; click **Cancel** to cancel the modify.	[Example] -
Privacy protocol	Encryption protocol used when encapsulating data, select **DES**, **AES** or not select. ● **DES**: indicates the Data Encryption Standard (DES), which is an international encryption algorithm with the key length of 56 characters. ● **AES**: indicates the Advanced Encryption Standard (AES). There are three types of key lengths, including 128 characters, 192 characters, and 256 characters. These types of key length can provide the security protection of different levels.	[Example] DES
Privacy password	If the **Privacy protocol** is **DES** or**AES**, you need to set the data encryption password. In the right textbox, click **Modify** to modify the password; click **Cancel** to cancel the modify.	[Example] -

Step 5 Click **OK**, the **Succeed** dialog box is displayed.

Step 6 Click **OK**.

----End

Modifying Hierarchical NMS Trap Parameters

To enable devices to be loaded to the network management system (NMS) by the automatic discovery function, configure the NMS hierarchical NMS Trap parameters.

Context

NOTICE

The storage arrays use the MD5 to encrypt device users' passwords. There is a possibility that device users' passwords are cracked and leaked.

NOTE

The hierarchical NMS Trap default user is **user**, and default **Authentication password** is **Admin@123**, change the password as prompted. You are prompted to change the password regularly.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **Layered NMS** > **Trap Configuration**.

Step 3 Click the or **Modify**.

The **Modify hierarchical NMS Trap parameters** dialog box is displayed.

Step 4 Set related information about hierarchical NMS Trap parameters, as described in the **Table 2-6**.

Table 2-6 Hierarchical NMS Trap parameters

Parameter	Description	Setting
Username	Indicates the user name of the storage device.	[Value range] The name is a string of 1 to 64 characters. [Example] user
Authentication protocol	Protocol used for verifying messages, select **HMACMD5**, **HMACSHA** or not select.	[Example] HMACSHA
Authentication password	If the **HMACMD5** or **HMACSHA** protocol is selected, you need to set the authentication password. In the right textbox, click **Modify** to modify the password; click **Cancel** to cancel the modify.	[Example] -
Privacy protocol	Encryption protocol used when encapsulating data, select **DES**, **AES** or not select. ● **DES**: indicates the Data Encryption Standard (DES), which is an international encryption algorithm with the key length of 56 characters. ● **AES**: indicates the Advanced Encryption Standard (AES). There are three types of key lengths, including 128 characters, 192 characters, and 256 characters. These types of key length can provide the security protection of different levels.	[Example] DES
Privacy password	If the **Privacy protocol** is **DES** or**AES**, you need to set the data encryption password. In the right textbox, click **Modify** to modify the password; click **Cancel** to cancel the modify.	[Example] -

Step 5 Click **OK**, the **Succeed** dialog box is displayed.

Step 6 Click **OK**.

----End

2.8 Discovery Management

After the NE is discovered, it is automatically displayed in the resource list of the management system. In the case of an NE discovery failure caused by network interruption, you can manually add NEs or stop discovering NEs.

2.8.1 Resources Management

You can modify an NE discovery policy and delete the discovered NEs.

1. Go to the **Resources** page.
   a. On the menu bar, choose **Management**.
   b. In the navigation tree, choose **Discover Management** > **Resources**.
2. Set related information about resource management by referring to the following table.

Operation	Description
Delete	Select one or more tasks and click **Delete** to delete the selected NEs.
Modify Basic Information	Click the name of an NE to modify basic information, input the name and location in the **Modify basic information** dialog.
Modify Alias	Click  of an NE to modify alias.
Modify Protocol	Click  of an NE to modify related information. For details, see **Modifying Protocol**.

Modifying Protocol

If parameters on an NE are changed, you can modify management protocol parameters or the switch management protocol type on the management system to keep the protocol parameters on the NE and the management system consistent.

Context

NOTICE

When the parameters on an NE are consistent to the management system, if you change the management protocol parameters to cause the protocol parameters on the NE and the management system not consistent. The modified management protocol parameters take effect when InfraControl obtain the connection again.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **Discover Management** > **Resources**.

Step 3 In the function pane, click next to the resource whose management protocol you want to modify.

The **Modify Protocol** dialog box is displayed.

Step 4 Modify management protocol parameters.

Step 5 Click **OK**.

----End

2.8.2 Managing Resource Discovery

You can create an NE discovery policy. By implementing a configured discovery policy, you can discover different types of NEs, and monitor and manage online NEs. All resource discovery results are displayed in the discovery result list. You can view and delete the discovery results, and stop the discovery results that are running, and rediscover the NEs based on the preset discovery policy.

NOTICE

The storage arrays use the MD5 to encrypt device users' passwords. There is a possibility that device users' passwords are cracked and leaked.

1. Go to the **Discover Resources Results** page.
   a. On the menu bar, choose **Management**.
   b. In the navigation tree, choose **Discover Management** > **Discover Resources**.
2. Set the resource management parameters, as described in the following table.

Operation	Description
Automatic Discovery	Click **Automatic Discover** to set a discovery policy on the management system. For details, see **Creating a Automatic Discovery Policy**.
View	In the **Discovery Resources** area, you can click the name of a discovery result to view details about the discovery result. In the **Discovery Resources** area,you can click number of discovered devices to view discovery result.
Delete	You can select one or more discovery results and click **Delete** to delete from the list. **NOTE** If a discovery result is running, you must stop it before you delete it from the list.
Rediscover	Select one or more NEs and click **Rediscover** to rediscover them based on the preset discovery policy.
Stop	You can select one or more discovery results that are running and click **Stop** to stop them. **NOTE** After the discovery results are stopped, **Progress** becomes **Manual Stop**.

Creating a Automatic Discovery Policy

This section describes how to configure an NE discovery policy on the management system. After the NE discovery policy is configured, the management system automatically starts discovering NEs based on the policy.

Creating a Policy for Discovering Huawei's Storage Devices

For the InfraControl to discover Huawei's storage devices, first complete required configurations on the InfraControl.

Prerequisites

- The storage array agent is enabled. Agent is enabled by default.
- The SNMP service of the storage array is enabled. The SNMP service is not enabled on HVSC99 and TV2 arrays by default.

Data Preparation

Table 2-7 Basic Information

Parameter	Description	Settings
Start IP address	Start IP address for discovering resources.	[Value range] ● The first number ranges from 1 to 223 (excluding 127). ● Other numbers range from 0 to 255. ● The start IP address must not be larger than the end IP address. [Example] 10.10.10.70
End IP address	End IP address for discovering resources.	[Value range] ● The first number ranges from 1 to 223 (excluding 127). ● Other numbers range from 0 to 255. ● The end IP address must not be smaller than the start IP address. [Example] 10.10.10.100
Location	Geological location of the resource.	[Example] Chengdu
Resource Group	Resource group of the resource.	[Example] CD
NE type	Type of NEs to be discovered. The type can be selected from a drop-down list.	[Example] Storage
Manufacturer	Manufacturer of the NEs to be discovered. This option is available if the selected NE type has any sub type.	[Example] Huawei

Table 2-8 Select Parameters

Protocol	Description
Default Protocol	1. In the **Protocol** drop-down list, select **Default Protocol**. 2. Set the following parameters. **NOTICE** Check whether the device to be discovered supports Secure Sockets Layer (SSL), the default value is **Enabled**. If the device does not support SSL, select **Disabled** in **SSL**. Otherwise, the InfraControl cannot discover the device. ● **Username**: user name for logging in to the storage device. ● **Password**: password for logging in to the storage device.

Protocol	Description
SNMP	1. In the **Protocol** drop-down list, select **SNMP**. 2. Set the following parameters. ● **Type**: type of the SNMP template used for storage device management. ● SNMPv3 – **SNMP template**: SNMP template used for storage device management, which is selected from the drop-down list. – **Attempts**: times for sending an SNMP operation. If this number of times is exceeded, the SNMP operation will be discarded. – **Timeout(s)**: wait time after a protocol message is sent. The value ranges from 1 to 5. – **Port**: port number used for access a specific network element (NE). The value ranges from 1 to 65,535. – **Username**: User name used for accessing the storage device. – **Context name**: Name of the environment engine. – **Context engine ID**: Unique identifier of an SNMP engine. This ID is used together with the environment name to determine an environment that uniquely identifies an SNMP entity. The SNMP message packet is processed only when the environments of the sender terminal and the recipient terminal are the same; otherwise, the SNMP message packet will be discarded. This parameter supports two input mode: – Hexadecimal input mode: The ID must be in the format of **#**.**.****. The validity verification involves the value length and each hexadecimal value. The value length is limited to 97 characters (including #). – Non-hexadecimal input mode: Enter the ID directly. The validity verification involves only the length. The value length is limited to 32 characters. – **Authentication protocol**: Protocol used for verifying messages. The parameter value can be the **HMACMD5** or **HMACSHA** protocol or no protocol. If the **HMACMD5** or **HMACSHA** protocol is selected, you need to set the authentication password.

Protocol	Description

	- **Authentication password**: If the authentication protocol is used when verifying messages, you need to set the authentication password.
	- **Privacy protocol**: Encryption protocol used when encapsulating data. The parameter value can be the **DES** or **AES** encryption protocol or no encryption. If the **DES** or **AES** encryption protocol is selected, you need to set the encryption password.
	  - DES: It indicates the Data Encryption Standard (DES), which is an international encryption algorithm with the key length of 56 characters.
	  - AES: It indicates the Advanced Encryption Standard (AES). There are three types of key lengths, including 128 characters, 192 characters, and 256 characters. These types of key length can provide the security protection of different levels.
	- **Privacy password**: If the encryption algorithm is used when encapsulating data, you need to set the data encryption password.
	● SNMPv2c/SNMPv1
	- **SNMP template**: SNMP template used for storage device management, which is selected from the drop-down list.
	- **Attempts**: times for sending an SNMP operation. If this number of times is exceeded, the SNMP operation will be discarded.
	- **Timeout(s)**: wait time after a protocol message is sent. The value ranges from 1 to 5.
	- **Port**: port number used for access a specific network element (NE). The value ranges from 1 to 65,535.
	- **Read community**: name of the community that has read permission.
	- **Write community**: name of the community that has write permission.

REST	1. In the **Protocol** drop-down list, select **REST**. 2. Set the following parameters. ● **Username**: user name for logging in to the storage device. ● **Password**: password for logging in to the storage device.

NOTE

In the **Protocol** drop-down list, select **Default Protocol**, the **Alarm Reporting Settings** information is displayed, **Table 2-9** shows the parameters.

Table 2-9 Alarm Reporting Settings

Description	Settings
Type: The type of the SNMP template used for storage device management.	[Default Value] SNMPv3

Description	Settings
Select **SNMPv3** in the **Type**	● **SNMP template**: SNMP template used for storage device management, which is selected from the drop-down list. ● **Attempts**: times for sending an SNMP operation. If this number of times is exceeded, the SNMP operation will be discarded. ● **Timeout(s)**: wait time after a protocol message is sent. The value ranges from 1 to 5. ● **Port**: port number used for access a specific network element (NE). The value ranges from 1 to 65,535. ● **Username**: User name used for accessing the storage device. ● **Context name**: Name of the environment engine. ● **Context engine ID**: Unique identifier of an SNMP engine. This ID is used together with the environment name to determine an environment that uniquely identifies an SNMP entity. The SNMP message packet is processed only when the environments of the sender terminal and the recipient terminal are the same; otherwise, the SNMP message packet will be discarded. This parameter supports two input mode: – Hexadecimal input mode: The ID must be in the format of **#**.**.****. The validity verification involves the value length and each hexadecimal value. The value length is limited to 97 characters (including #). – Non-hexadecimal input mode: Enter the ID directly. The validity verification involves only the length. The value length is limited to 32 characters. ● **Authentication protocol**: Protocol used for verifying messages. The parameter value can be the **HMACMD5** or **HMACSHA** protocol or no protocol. If the **HMACMD5** or **HMACSHA** protocol is selected, you need to set the authentication password.

Description	Settings
	● **Authentication password**: If the authentication protocol is used when verifying messages, you need to set the authentication password. ● **Privacy protocol**: Encryption protocol used when encapsulating data. The parameter value can be the **DES** or **AES** encryption protocol or no encryption. If the **DES** or **AES** encryption protocol is selected, you need to set the encryption password. – DES: It indicates the Data Encryption Standard (DES), which is an international encryption algorithm with the key length of 56 characters. – AES: It indicates the Advanced Encryption Standard (AES). There are three types of key lengths, including 128 characters, 192 characters, and 256 characters. These types of key length can provide the security protection of different levels. ● **Privacy password**: If the encryption algorithm is used when encapsulating data, you need to set the data encryption password.
Select **SNMPv2c** in the **Type**	● **Community**: The community to check the reported Trap. ● **Trap IP**: IP address is used to transmit and report the alarm to the InfraControl.

Procedure

Step 1 Go to the **Automatic Discovery** page.

1. On the menu bar, choose **Management**.
2. In the navigation tree, choose **Discover Management** > **Discover Resources**.
3. Click **Automatic Discovery**.

Step 2 Set the parameters related to automatic discovery.

1. In the **Basic Information** area, set basic information. For details about the parameters, see **Table 2-7**.

   In **Manufacturer**, select **Huawei**.
2. In the **Select Parameters** area, set other automatic discovery parameters. For details about the parameters, see **Table 2-8**.

The protocols used for device discovery as shown in **Table 2-10**.

Table 2-10 Protocols used for device discovery

Device Type	Device Name (Version)	Protocol
Disk array	S2600 V1R2/S2600 V1R5/ S5000 V1R5	SMI-S
	S5600 V1R1	SNMP
	T series(V1R1/V1R2/ V1R5)	SMI-S
	T series(V2R1)	TLV
	HVS C99	TLV
	Dorado 5100 V1R1C00	SMI-S
Unified storage device	N8000 V1R2, N8000 V2R1	SMI-S
	T series(V1R5)	SMI-S
Virtual intelligent storage device	VIS6000 V1R2C02, VIS6000T V2R3, S8100 V1R2C00	SMI-S
Cloud storage	UDS V1R2C00	REST

Step 3 Click **Start Discovery**.

NOTE

Discover storage devices as an administrator. Otherwise, device alarms cannot be received.

----End

Result

After qualified NEs are discovered, the value of **Number of Discovered Devices** increases depending on the number of discovered NEs, and the records of discovered NEs are displayed in **Resources List**.

Creating a Policy for Discovering Heterogeneous Storage Devices

For the InfraControl to discover heterogeneous storage devices, first complete required configurations on the InfraControl.

Prerequisites

- A supported version of the SMI-S Provider for the heterogeneous storage devices must be installed and running.
- The SMI Provider must be configured to access the heterogeneous storage devices.

- The SNMP service of the Storage Devices discovered by SNMP protocol must be enabled. For example, Inspur AS400, Sugon DS600.

Data Preparation

Table 2-11 Basic Information

Parameter	Description	Settings
Start IP address	Start IP address for discovering resources.	[Value range] ● The first number ranges from 1 to 223 (excluding 127). ● Other numbers range from 0 to 255. ● The start IP address must not be larger than the end IP address. [Example] 10.10.10.70
End IP address	End IP address for discovering resources.	[Value range] ● The first number ranges from 1 to 223 (excluding 127). ● Other numbers range from 0 to 255. ● The end IP address must not be smaller than the start IP address. [Example] 10.10.10.100
Location	Geological location of the resource.	[Example] Chengdu
Resource Group	Resource group of the resource.	[Example] CD
NE type	Type of NEs to be discovered. The type can be selected from a drop-down list.	[Example] Storage
Manufacturer	Manufacturer of the NEs to be discovered. This option is available if the selected NE type has any sub type.	[Example] DFT

Table 2-12 Select Parameters

Protocol	Description
SMI-S	1. In **NE type**, select **Storage**. In **Manufacturer**, select a vendor. Possible values are **DFT**, **EMC**, **HP**, **IBM**, **Inspur**, **NetApp**, and **Sugon**. 2. Set the following parameters. ● **Username**: user name for logging in to a storage system. ● **Password**: password for logging in to a storage system. ● **Port**: port to be opened. The value ranges from 1 to 65,535. ● **Namespace**: namespace of a storage system. **NOTE** ● By default, the corresponding namespace of the **NetApp** device is **interop**. ● By default, the corresponding namespace of the **EMC** device is **root/emc**.

Protocol	Description
SNMP	1. In **NE type**, select **Storage**. In **Manufacturer**, select **Inspur** or **Sugon**. 2. In **Protocol**, select **Others**. ● In the **SNMP** area, set the following parameters. – **Type**: type of the SNMP template used for storage device management. – SNMPv3 – **SNMP template**: SNMP template used for storage device management, which is selected from the drop-down list. – **Attempts**: times for sending an SNMP operation. If this number of times is exceeded, the SNMP operation will be discarded. – **Timeout(s)**: wait time after a protocol message is sent. The value ranges from 1 to 5. – **Port**: port number used for access a specific network element (NE). The value ranges from 1 to 65,535. – **Username**: User name used for accessing the storage device. – **Context name**: Name of the environment engine. – **Context engine ID**: Unique identifier of an SNMP engine. This ID is used together with the environment name to determine an environment that uniquely identifies an SNMP entity. The SNMP message packet is processed only when the environments of the sender terminal and the recipient terminal are the same; otherwise, the SNMP message packet will be discarded. This parameter supports two input mode: – Hexadecimal input mode: The ID must be in the format of **#**.**.****. The validity verification involves the value length and each hexadecimal value. The value length is limited to 97 characters (including #). – Non-hexadecimal input mode: Enter the ID directly. The validity verification involves only the length. The value length is limited to 32 characters. – **Authentication protocol**: Protocol used for verifying messages. The parameter value can be

Protocol	Description
	the **HMACMD5** or **HMACSHA** protocol or no protocol. If the **HMACMD5** or **HMACSHA** protocol is selected, you need to set the authentication password. - **Authentication password**: If the authentication protocol is used when verifying messages, you need to set the authentication password. - **Privacy protocol**: Encryption protocol used when encapsulating data. The parameter value can be the **DES** or **AES** encryption protocol or no encryption. If the **DES** or **AES** encryption protocol is selected, you need to set the encryption password. - DES: It indicates the Data Encryption Standard (DES), which is an international encryption algorithm with the key length of 56 characters. - AES: It indicates the Advanced Encryption Standard (AES). There are three types of key lengths, including 128 characters, 192 characters, and 256 characters. These types of key length can provide the security protection of different levels. - **Privacy password**: If the encryption algorithm is used when encapsulating data, you need to set the data encryption password. - SNMPv2c/SNMPv1 - **SNMP template**: SNMP template used for storage device management, which is selected from the drop-down list. - **Attempts**: times for sending an SNMP operation. If this number of times is exceeded, the SNMP operation will be discarded. - **Timeout(s)**: wait time after a protocol message is sent. The value ranges from 1 to 5. - **Port**: port number used for access a specific network element (NE). The value ranges from 1 to 65,535. - **Read community**: name of the community that has read permission. - **Write community**: name of the community that has write permission. ● In the **CLI** area, set the following parameters.

Protocol	Description
	NOTE If **Manufacturer** is set to **Sugon**, the following parameters are available: - **Username**: user name for logging in to the storage device. - **Password**: password for logging in to the storage device.

Table 2-13 Alarm Reporting Settings

Description	Settings
Type: The type of the SNMP template used for storage device management.	[Default Value] SNMPv3

Description	Settings
Select **SNMPv3** in the **Type**	● **SNMP template**: SNMP template used for storage device management, which is selected from the drop-down list. ● **Attempts**: times for sending an SNMP operation. If this number of times is exceeded, the SNMP operation will be discarded. ● **Timeout(s)**: wait time after a protocol message is sent. The value ranges from 1 to 5. ● **Port**: port number used for access a specific network element (NE). The value ranges from 1 to 65,535. ● **Username**: User name used for accessing the storage device. ● **Context name**: Name of the environment engine. ● **Context engine ID**: Unique identifier of an SNMP engine. This ID is used together with the environment name to determine an environment that uniquely identifies an SNMP entity. The SNMP message packet is processed only when the environments of the sender terminal and the recipient terminal are the same; otherwise, the SNMP message packet will be discarded. This parameter supports two input mode: – Hexadecimal input mode: The ID must be in the format of **#**.**.****. The validity verification involves the value length and each hexadecimal value. The value length is limited to 97 characters (including #). – Non-hexadecimal input mode: Enter the ID directly. The validity verification involves only the length. The value length is limited to 32 characters. ● **Authentication protocol**: Protocol used for verifying messages. The parameter value can be the **HMACMD5** or **HMACSHA** protocol or no protocol. If the **HMACMD5** or **HMACSHA** protocol is selected, you need to set the authentication password.

Description	Settings
	● **Authentication password**: If the authentication protocol is used when verifying messages, you need to set the authentication password. ● **Privacy protocol**: Encryption protocol used when encapsulating data. The parameter value can be the **DES** or **AES** encryption protocol or no encryption. If the **DES** or **AES** encryption protocol is selected, you need to set the encryption password. – DES: It indicates the Data Encryption Standard (DES), which is an international encryption algorithm with the key length of 56 characters. – AES: It indicates the Advanced Encryption Standard (AES). There are three types of key lengths, including 128 characters, 192 characters, and 256 characters. These types of key length can provide the security protection of different levels. ● **Privacy password**: If the encryption algorithm is used when encapsulating data, you need to set the data encryption password.
Select **SNMPv2c** in the **Type**	● **Community**: The community to check the reported Trap. ● **Trap IP**: IP address is used to transmit and report the alarm to the InfraControl.

Procedure

Step 1 Go to the **Automatic Discovery** page.

1. On the menu bar, choose **Management**.
2. In the navigation tree, choose **Discover Management** > **Discover Resources**.
3. Click **Automatic Discovery**.

Step 2 Set the parameters related to automatic discovery.

1. In the **Basic Information** area, set basic information.

   The storage devices developed by **Inspur** and **Sugon** can be discovered based on Simple Network Management Protocol (SNMP). For details about the parameters, see **Table 2-11**.

NOTICE

Check whether the device to be discovered supports Secure Sockets Layer (SSL). If the device does not support SSL, select **Disable** in **SSL**. Otherwise, the InfraControl cannot discover the device.

2. In the **Select Parameters** area, set other automatic discovery parameters. For details about the parameters, see **Table 2-12**.

   The protocols used for device discovery as shown in **Table 2-14**.

Table 2-14 Protocols used for device discovery

Manufacturer	Device Name (Version)	Protocol
EMC	CLARiiON CX3/CX4 series	SMI-S
NetApp	FAS3160	SMI-S
HP	EVA4400/EVA8400	SMI-S
IBM	DS8000	SMI-S
Inspur	AS400	SNMP
	AS2000(OEM NetApp 7900)	SMI-S
DFT	GS3992(OEM NetApp 3992)	SMI-S
Sugon	DS600-F10(OEM Infortrend)	SNMP
	DS8348(OEM NetApp 3994), DS8340(OEM NetApp 3992)	SMI-S

Step 3 Click **Start Discovery**.

----End

Result

After qualified NEs are discovered, the value of **Number of Discovered Devices** increases depending on the number of discovered NEs, and the records of discovered NEs are displayed in **Resources List**.

Creating a Policy for Discovering Ethernet Switchs

For the InfraControl to discover ethernet switchs, first complete required configurations on the InfraControl.

Data Preparation

Table 2-15 Basic Information

Parameter	Description	Settings
Start IP address	Start IP address for discovering resources.	[Value range] ● The first number ranges from 1 to 223 (excluding 127). ● Other numbers range from 0 to 255. ● The start IP address must not be larger than the end IP address. [Example] 10.10.10.70
End IP address	End IP address for discovering resources.	[Value range] ● The first number ranges from 1 to 223 (excluding 127). ● Other numbers range from 0 to 255. ● The end IP address must not be smaller than the start IP address. [Example] 10.10.10.100
Location	Geological location of the resource.	[Example] Chengdu
Resource Group	Resource group of the resource.	[Example] CD
NE type	Type of NEs to be discovered. The type can be selected from a drop-down list.	[Example] Ethernet Switch
Manufacturer	Manufacturer of the NEs to be discovered. This option is available if the selected NE type has any sub type.	[Example] Huawei

Table 2-16 Select Parameters

NE	Description
Ethernet Switch	1. In **NE type**, select **Ethernet Switch**. In **Manufacturer**, select **Huawei**. 2. Set the following parameters. ● **Type**: SNMP module type of the management switch. ● **SNMP template**: SNMP template of the management switch, available from the list. ● **Attempts**: allowed times of resending an SNMP operation. If the times is exceeded, resending is aborted. The value ranges from 0 to 5. ● **Timeout(s)**: time for you to wait after the protocol message is sent. The value ranges from 1 to 5. ● **Port**: port number of the specified device to be accessed. The value ranges from 1 to 65,535. ● **Read community**: name of the community that has the read permission. ● **Write community**: name of the community that has the write permission. ● **Username**: User name used for accessing the switch. ● **Context name**: Name of the environment engine. ● **Context engine ID**: Unique identifier of an SNMP engine. This ID is used together with the environment name to determine an environment that uniquely identifies an SNMP entity. The SNMP message packet is processed only when the environments of the sender terminal and the recipient terminal are the same; otherwise, the SNMP message packet will be discarded. This parameter supports two input mode: – Hexadecimal input mode: The ID must be in the format of **#**.**.****. The validity verification involves the value length and each hexadecimal value. The value length is limited to 97 characters (including #). – Non-hexadecimal input mode: Enter the ID directly. The validity verification involves only the length. The value length is limited to 32 characters. ● **Authentication protocol**: Protocol used for verifying messages. The parameter value can be the **HMACMD5** or **HMACSHA** protocol or no protocol. If the **HMACMD5** or **HMACSHA** protocol is selected, you need to set the authentication password. ● **Authentication password**: If the authentication protocol is used when verifying messages, you need to set the authentication password.

NE	Description
	● **Privacy protocol**: Encryption protocol used when encapsulating data. The parameter value can be the **DES** or **AES** encryption protocol or no encryption. If the **DES** or **AES** encryption protocol is selected, you need to set the encryption password. – DES: It indicates the Data Encryption Standard (DES), which is an international encryption algorithm with the key length of 56 characters. – AES: It indicates the Advanced Encryption Standard (AES). There are three types of key lengths, including 128 characters, 192 characters, and 256 characters. These types of key length can provide the security protection of different levels. ● **Privacy password**: If the encryption algorithm is used when encapsulating data, you need to set the data encryption password.

Procedure

Step 1 Go to the **Automatic Discovery** page.

1. On the menu bar, choose **Management**.
2. In the navigation tree, choose **Discover Management** > **Discover Resources**.
3. Click **Automatic Discovery**.

Step 2 Set the parameters related to automatic discovery.

1. In the **Basic Information** area, set basic information. For details about the parameters, see **Table 2-15**.
2. In the **Select Parameters** area, set other automatic discovery parameters. For details about the parameters, see **Table 2-16**.

Step 3 Click **Start Discovery**.

----End

Result

After qualified NEs are discovered, the value of **Number of Discovered Devices** increases depending on the number of discovered NEs, and the records of discovered NEs are displayed in **Resources List**.

Follow-up Procedure

If the SNMP parameters undergo changes on an NE, click the corresponding  in **Resources List** to modify the SNMP parameters on the InfraControl to be consistent with those on the NE.

Creating a Policy for Discovering Fibre Channel Switchs

For the InfraControl to discover FC switchs, first complete required configurations on the InfraControl.

Data Preparation

Table 2-17 Basic Information

Parameter	Description	Settings
Start IP address	Start IP address for discovering resources.	[Value range] ● The first number ranges from 1 to 223 (excluding 127). ● Other numbers range from 0 to 255. ● The start IP address must not be larger than the end IP address. [Example] 10.10.10.70
End IP address	End IP address for discovering resources.	[Value range] ● The first number ranges from 1 to 223 (excluding 127). ● Other numbers range from 0 to 255. ● The end IP address must not be smaller than the start IP address. [Example] 10.10.10.100
Location	Geological location of the resource.	[Example] Chengdu
Resource Group	Resource group of the resource.	[Example] CD
NE type	Type of NEs to be discovered. The type can be selected from a drop-down list.	[Example] FC Switch

Parameter	Description	Settings
Manufacturer	Manufacturer of the NEs to be discovered. This option is available if the selected NE type has any sub type.	[Example] Brocade

Table 2-18 Select parameters

NE	Description
FC switch of Qlogic	1. Selected **FC Switch** for **NE type** and **Qlogic** for **Manufacturer**. 2. Set the following parameters. ● **Type**: SNMP module type of the management switch. ● **SNMP template**: SNMP template of the management switch, available from the list. ● **Attempts**: allowed times of resending an SNMP operation. If the times is exceeded, resending is aborted. The value ranges from 0 to 5. ● **Timeout(s)**: time for you to wait after the protocol message is sent. The value ranges from 1 to 5. ● **Port**: port number of the specified device to be accessed. The value ranges from 1 to 65,535. ● **Read community**: name of the community that has the read permission. ● **Write community**: name of the community that has the write permission. ● **Username**: User name used for accessing the switch. ● **Context name**: Name of the environment engine. ● **Context engine ID**: Unique identifier of an SNMP engine. This ID is used together with the environment name to determine an environment that uniquely identifies an SNMP entity. The SNMP message packet is processed only when the environments of the sender terminal and the recipient terminal are the same; otherwise, the SNMP message packet will be discarded. This parameter supports two input mode: – Hexadecimal input mode: The ID must be in the format of **#**.**.****. The validity verification involves the value length and each hexadecimal value. The value length is limited to 97 characters (including #). – Non-hexadecimal input mode: Enter the ID directly. The validity verification involves only the length. The value length is limited to 32 characters. ● **Authentication protocol**: Protocol used for verifying messages. The parameter value can be the **HMACMD5** or **HMACSHA** protocol or no protocol. If the **HMACMD5** or **HMACSHA** protocol is selected, you need to set the authentication password. ● **Authentication password**: If the authentication protocol is used when verifying messages, you need to set the authentication password.

NE	Description
	● **Privacy protocol**: Encryption protocol used when encapsulating data. The parameter value can be the **DES** or **AES** encryption protocol or no encryption. If the **DES** or **AES** encryption protocol is selected, you need to set the encryption password. – DES: It indicates the Data Encryption Standard (DES), which is an international encryption algorithm with the key length of 56 characters. – AES: It indicates the Advanced Encryption Standard (AES). There are three types of key lengths, including 128 characters, 192 characters, and 256 characters. These types of key length can provide the security protection of different levels. ● **Privacy password**: If the encryption algorithm is used when encapsulating data, you need to set the data encryption password.
FC switch of Brocade	1. Selected **FC Switch** for **NE type** and **Brocade** for **Manufacturer**. 2. Set parameters for the NEs. ● **Username**: user name for logging in to the Brocade Fibre Channel switch Smi-Agent. ● **Password**: password for logging in to the Brocade Fibre Channel switch Smi-Agent.

NOTE

In the **Manufacturer** drop-down list, select **Brocade**, the **Alarm Reporting Settings** information is displayed, **Table 2-19** shows the parameters.

Table 2-19 Alarm Reporting Settings

Description	Settings
Type: The type of the SNMP template used for switch management.	[Default Value] SNMPv3

Description	Settings
Select **SNMPv3** in the **Type**	● **SNMP template**: SNMP template used for switch management, which is selected from the drop-down list. ● **Attempts**: times for sending an SNMP operation. If this number of times is exceeded, the SNMP operation will be discarded. ● **Timeout(s)**: wait time after a protocol message is sent. The value ranges from 1 to 5. ● **Port**: port number used for access a specific network element (NE). The value ranges from 1 to 65,535. ● **Username**: User name used for accessing the switch. ● **Context name**: Name of the environment engine. ● **Context engine ID**: Unique identifier of an SNMP engine. This ID is used together with the environment name to determine an environment that uniquely identifies an SNMP entity. The SNMP message packet is processed only when the environments of the sender terminal and the recipient terminal are the same; otherwise, the SNMP message packet will be discarded. This parameter supports two input mode: – Hexadecimal input mode: The ID must be in the format of **#**.**.****. The validity verification involves the value length and each hexadecimal value. The value length is limited to 97 characters (including #). – Non-hexadecimal input mode: Enter the ID directly. The validity verification involves only the length. The value length is limited to 32 characters. ● **Authentication protocol**: Protocol used for verifying messages. The parameter value can be the **HMACMD5** or **HMACSHA** protocol or no protocol. If the **HMACMD5** or **HMACSHA** protocol is selected, you need to set the authentication password.

Description	Settings
	● **Authentication password**: If the authentication protocol is used when verifying messages, you need to set the authentication password. ● **Privacy protocol**: Encryption protocol used when encapsulating data. The parameter value can be the **DES** or **AES** encryption protocol or no encryption. If the **DES** or **AES** encryption protocol is selected, you need to set the encryption password. – DES: It indicates the Data Encryption Standard (DES), which is an international encryption algorithm with the key length of 56 characters. – AES: It indicates the Advanced Encryption Standard (AES). There are three types of key lengths, including 128 characters, 192 characters, and 256 characters. These types of key length can provide the security protection of different levels. ● **Privacy password**: If the encryption algorithm is used when encapsulating data, you need to set the data encryption password.
Select **SNMPv2c** in the **Type**	● **Community**: The community to check the reported Trap. ● **Trap IP**: IP address is used to transmit and report the alarm to the InfraControl.

Procedure

Step 1 Go to the **Automatic Discovery** page.

1. On the menu bar, choose **Management**.
2. In the navigation tree, choose **Discover Management** > **Discover Resources**.
3. Click **Automatic Discovery**.

Step 2 Set the parameters related to automatic discovery.

1. In the **Basic Information** area, set basic information. For details about the parameters, see **Table 2-17**.
2. In the **Select Parameters** area, set other automatic discovery parameters. For details about the parameters, see **Table 2-18**.

Step 3 Click **Start Discovery**.

----End

Result

After qualified NEs are discovered, the value of **Number of Discovered Devices** increases depending on the number of discovered NEs, and the records of discovered NEs are displayed in **Resources List**.

Follow-up Procedure

If the SNMP parameters undergo changes on an NE, click the corresponding  in **Resources List** to modify the SNMP parameters on the InfraControl to be consistent with those on the NE.

Creating a Policy for Discovering Virtual Servers

For the InfraControl to discover virtual servers on a network, first complete required configurations on the virtual servers and InfraControl. This chapter describes the configurations for discovering virtual servers.

Prerequisites

The VMware Tools software has been installed on the virtual servers to be discovered.

Data Preparation

Table 2-20 Basic Information

Parameter	Description	Settings
Start IP address	Start IP address for discovering resources.	[Value range] ● The first number ranges from 1 to 223 (excluding 127). ● Other numbers range from 0 to 255. ● The start IP address must not be larger than the end IP address. [Example] 10.10.10.70

Parameter	Description	Settings
End IP address	End IP address for discovering resources.	[Value range] ● The first number ranges from 1 to 223 (excluding 127). ● Other numbers range from 0 to 255. ● The end IP address must not be smaller than the start IP address. [Example] 10.10.10.100
Location	Geological location of the resource.	[Example] Chengdu
Resource Group	Resource group of the resource.	[Example] CD
NE type	Type of NEs to be discovered. The type can be selected from a drop-down list.	[Example] Virtualization Server
Manufacturer	Manufacturer of the NEs to be discovered. This option is available if the selected NE type has any sub type.	[Example] VMware

Table 2-21 Select parameters

NE	Description
Virtualization server	1. Selected **Virtualization Server** for **NE type** and **VMware** for **Manufacturer**. 2. Set parameters for the NEs. ● **Virtualization server username**: user name for logging to the virtualization server. ● **Virtualization server password**: password for logging to the virtualization server. ● **Virtual machine username**: user name for logging in to the virtual machine (optional). ● **Virtual machine password**: password for logging in to the virtual machine (optional). ● **File transfer protocol**: file transfer protocol used by the host running a Windows operating system. The values include **SFTP (Windows)**. ● **Database authentication mode**: authentication mode. The mode include **Database authentication** and **Operating system authentication**. ● **Optional: Database username**: user name for logging in to the database. ● **Optional: Database password**: password for logging in to the database.

Procedure

Step 1 The file transfer service is enabled for the InfraControl to discover Windows-based virtual machines, and accordingly do the configuration on the corresponding virtual machine, for details, see Configuring Servers.

1. On the menu bar, choose **Management** > **Server Information** > **SFTP Server**.
2. Set the **Server Status** in the **SFTP Server** to **Enable**.

Step 2 On the menu bar, choose **Management**.

Step 3 In the navigation tree, choose **Discover Management** > **Discover Resources**.

Step 4 Click **Automatic Discover**.

Step 5 Set the parameters related to automatic discovery.

1. In the **Basic Information** area, set basic information. For details about the parameters, see **Table 2-20**.
2. In the **Select Parameters** area, set other automatic discovery parameters. For details about the parameters, see **Table 2-21**.

Step 6 Click **Start Discovery**.

----End

Result

After qualified NEs are discovered, the value of **Number of Discovered Devices** increases depending on the number of discovered NEs, and the records of discovered NEs are displayed in **Resources List**.

Follow-up Procedure

If you want to find other virtual machines on this virtual server, please do the following.

1. Go to the **Modify** page.
   a. On the menu bar, choose **Management**.
   b. In the navigation tree, choose **Discover Management** > **Resources**.
   c. Click the  corresponding to the virtual server.
2. Click the **Contained Virtual Machine** tab.
3. Update the virtual machine parameters such as user names and passwords in the list of virtual machines.
4. Click **Ok**.
5. Refresh the virtual server.
   a. On the menu bar, choose **Resources**.
   b. In the navigation tree, choose **Hosts** > **Virtualization Servers**.
   c. In the function pane, click **Refresh** corresponding to the virtual server.

Creating a Policy for Discovering Servers

For the InfraControl to discover servers, first complete required configurations on the InfraControl.

Prerequisites

The file transfer service is enabled for the InfraControl to discover Windows-based servers.

Data Preparation

Table 2-22 Basic Information

Parameter	Description	Settings
Start IP address	Start IP address for discovering resources.	[Value range] ● The first number ranges from 1 to 223 (excluding 127). ● Other numbers range from 0 to 255. ● The start IP address must not be larger than the end IP address. [Example] 10.10.10.70
End IP address	End IP address for discovering resources.	[Value range] ● The first number ranges from 1 to 223 (excluding 127). ● Other numbers range from 0 to 255. ● The end IP address must not be smaller than the start IP address. [Example] 10.10.10.100
Location	Geological location of the resource.	[Example] Chengdu
Resource Group	Resource group of the resource.	[Example] CD
NE type	Type of NEs to be discovered. The type can be selected from a drop-down list.	[Example] Server

Table 2-23 Select Parameters

NEs	Description
Server	1. Selected **Server** for **NE type**. 2. Set parameters for the NEs. ● **Optional: The bastion host provides service parameters**: you cannot input the **Server username** and the **Server password** after choosing it, the bastion host provides the information of the server. ● **Server username**: user name for logging in to the host. ● **Server password**: password for logging in to the host. ● **File transfer protocol**: file transfer protocol of the host whose operating system type is Windows. The values include **SFTP (Windows)**. ● **Database authentication mode**: authentication mode. The mode include **Database authentication** and **Operating system authentication**. ● **Optional: Database username**: user name for logging in to the database. ● **Optional: Database password**: password for logging in to the database.

Procedure

Step 1 The file transfer service is enabled for the InfraControl to discover Windows-based servers, and accordingly do the configuration on the corresponding virtual machine, for details, see Configuring Servers.

1. On the menu bar, choose **Management** > **Server Information** > **SFTP Server**.
2. Set the **Server Status** in the **SFTP Server** to **Enable**.

Step 2 Go to the **Automatic Discovery** page.

1. On the menu bar, choose **Management**.
2. In the navigation tree, choose **Discover Management** > **Discover Resources**.
3. Click **Automatic Discovery**.

Step 3 Set the parameters related to automatic discovery.

1. In the **Basic Information** area, set basic information. For details about the parameters, see **Table 2-22**.
2. In the **Select Parameters** area, set other automatic discovery parameters. For details about the parameters, see **Table 2-23**.

Step 4 Click **Start Discovery**.

----End

Result

After qualified NEs are discovered, the value of **Number of Discovered Devices** increases depending on the number of discovered NEs, and the records of discovered NEs are displayed in **Resources List**.

Creating a Policy for Discovering VTLs

For the InfraControl to discover VTLs on a network, first complete required configurations on the InfraControl. This chapter describes the configurations for discovering VTLs.

Data Preparation

Table 2-24 Basic Information

Parameter	Description	Settings
Start IP address	Start IP address for discovering resources.	[Value range] ● The first number ranges from 1 to 223 (excluding 127). ● Other numbers range from 0 to 255. ● The start IP address must not be larger than the end IP address. [Example] 10.10.10.70
End IP address	End IP address for discovering resources.	[Value range] ● The first number ranges from 1 to 223 (excluding 127). ● Other numbers range from 0 to 255. ● The end IP address must not be smaller than the start IP address. [Example] 10.10.10.100
Location	Geological location of the resource.	[Example] Chengdu
Resource Group	Resource group of the resource.	[Example] CD

Parameter	Description	Settings
NE type	Type of NEs to be discovered. The type can be selected from a drop-down list.	[Example] VTL
Manufacturer	Manufacturer of the NEs to be discovered. This option is available if the selected NE type has any sub type.	[Example] Huawei

Table 2-25 Select parameters

NE	Description
VTL	1. Selected **VTL** for **NE type**. 2. Set parameters for the NEs. ● **Username**: user name for logging in to the virtual tape library (VTL). ● **Password**: password for logging in to the VTL.

Table 2-26 Alarm Reporting Settings

Description	Settings
Type: The type of the SNMP template used for VTL management.	[Default Value] SNMPv3

Description	Settings
Select **SNMPv3** in the **Type**	● **SNMP template**: SNMP template used for VTL management, which is selected from the drop-down list. ● **Attempts**: times for sending an SNMP operation. If this number of times is exceeded, the SNMP operation will be discarded. ● **Timeout(s)**: wait time after a protocol message is sent. The value ranges from 1 to 5. ● **Port**: port number used for access a specific network element (NE). The value ranges from 1 to 65,535. ● **Username**: User name used for accessing the VTL. ● **Context name**: Name of the environment engine. ● **Context engine ID**: Unique identifier of an SNMP engine. This ID is used together with the environment name to determine an environment that uniquely identifies an SNMP entity. The SNMP message packet is processed only when the environments of the sender terminal and the recipient terminal are the same; otherwise, the SNMP message packet will be discarded. This parameter supports two input mode: – Hexadecimal input mode: The ID must be in the format of **#**.**.****. The validity verification involves the value length and each hexadecimal value. The value length is limited to 97 characters (including #). – Non-hexadecimal input mode: Enter the ID directly. The validity verification involves only the length. The value length is limited to 32 characters. ● **Authentication protocol**: Protocol used for verifying messages. The parameter value can be the **HMACMD5** or **HMACSHA** protocol or no protocol. If the **HMACMD5** or **HMACSHA** protocol is selected, you need to set the authentication password.

Description	Settings
	● **Authentication password**: If the authentication protocol is used when verifying messages, you need to set the authentication password. ● **Privacy protocol**: Encryption protocol used when encapsulating data. The parameter value can be the **DES** or **AES** encryption protocol or no encryption. If the **DES** or **AES** encryption protocol is selected, you need to set the encryption password. – DES: It indicates the Data Encryption Standard (DES), which is an international encryption algorithm with the key length of 56 characters. – AES: It indicates the Advanced Encryption Standard (AES). There are three types of key lengths, including 128 characters, 192 characters, and 256 characters. These types of key length can provide the security protection of different levels. ● **Privacy password**: If the encryption algorithm is used when encapsulating data, you need to set the data encryption password.
Select **SNMPv2c** in the **Type**	● **Community**: The community to check the reported Trap. ● **Trap IP**: IP address is used to transmit and report the alarm to the InfraControl.

Procedure

Step 1 Go to the **Automatic Discovery** page.

1. On the menu bar, choose **Management**.
2. In the navigation tree, choose **Discover Management** > **Discover Resources**.
3. Click **Automatic Discovery**.

Step 2 Set the parameters related to automatic discovery.

1. In the **Basic Information** area, set basic information. For details about the parameters, see **Table 2-24**.
2. In the **Select Parameters** area, set other automatic discovery parameters. For details about the parameters, see **Table 2-25**.

Step 3 Click **Start Discovery**.

----End

Result

After qualified NEs are discovered, the value of **Number of Discovered Devices** increases depending on the number of discovered NEs, and the records of discovered NEs are displayed in **Resources List**.

2.8.3 Managing Resource Groups

You can centrally manage discovered resources by adding them into a resource group.

1. Go to the resource list page.
   a. On the menu bar, choose **Management**.
   b. In the navigation tree, choose **Discover Management** > **Resource Group**.
2. Refer to the following table to configure resource management.

Operation	Description
Create	Click Create to create a resource group, and set the name, description, and resource list for the resource group.
Delete	Select one or more resource groups and click Delete to delete the resource group or groups.
Modify	Click the corresponding to a resource group to modify the resource group.

Creating a Resource Group

This task helps you create a resource group.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **Discover Management** > **Resource Group**.

Step 3 In the function pane, click **Create**.
The **Create Resource Group** dialog box is displayed.

Step 4 Enter a name and description for the resource group. Select the resources that you want to add to this resource group and move them to the selected resource list.

Step 5 Click **OK**.

----End

2.9 Template Management

The management system provides three default SNMP templates. You can also create new SNMP templates as required.

2.9.1 Managing SNMP Templates

The management system provides three default SNMP templates: **default_SNMPv1_template**, **default_SNMPv2c_template**, and **default_SNMPv3_template**. You can modify but cannot delete the three default parameter templates. You can create an SNMP parameter template based on SNMP versions supported by an NE. In addition, you can also modify or delete the created template.

Context

On the menu bar, choose **Management** > **Template Management** > **SNMP Templates** to manage SNMP templates.

Operation	Description
New	Click **Create** and select a different SNMP version to create an SNMP parameter template. For details, see **Creating an SNMP Template**.
Modify	Click  of the parameter template to modify related parameters. For details, see **Modifying SNMP Templates**.
Delete	Select one or more unused parameter templates, click **Delete** to delete them. If the parameter template to be deleted is in use, you must unbind the discovery policy with the template before deletion.
View	Click the name of a created SNMP parameter template. The **Template Details** page is displayed. You can view information about the template. For details about this parameter template, see **Creating an SNMP Template**.

Creating an SNMP Template

Before the management system discovers an NE which discovered though SNMP protocol, it uses the SNMP parameter template to match the specified NE. Therefore, you need to create an SNMP parameter template before you perform the NE discovery operation.

Prerequisites

The SNMP parameters have been configured on the NE.

Context

Currently, the management system supports SNMPv1, SNMPv2c, and SNMPv3. The differences among these three versions are as follows:

- SNMPv1 uses the community name authentication method to control the access of the management system server to the managed NEs. If the community name carried by an SNMP packet is not authenticated by the NEs, the packet will be discarded.
- SNMPv2c also uses the community name authentication method, but it extends this function over SNMPv1. It supports more types of operations and data and provides rich error codes, distinguishing among errors more subtly.
- SNMPv3 uses the user security model-based authentication. You can set the authentication and encryption functions. The authentication function verifies the validity of the packet sender, blocking accesses from unauthorized users. The encryption function encrypts the packets transmitted between the management system server and its managed devices, avoiding eavesdropping. SNMPv3 improves the communication security by combining the authentication and encryption functions.

You can create a parameter template according to the SNMP protocol version supported by the NE.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **Template Management** > **SNMP Templates**.

Step 3 In the function pane, click **Create**.

The **Create SNMP Template** dialog box is displayed.

Step 4 Create an SNMP template.

1. Select an SNMP template type.

   You can select **v1**, **v2c**, or **v3**.

   NOTE

   The SNMP versions must be the same on the management system and the NE.

   - If you select v1 or v2c, write and read communities must be the same on the management system and the NE.
   - If you select v3, user names, data encryption protocols and passwords, authorization protocol and passwords must be the same on the management system and the NE.

2. Set SNMP template parameters.

   - The following table describes **v1** and **v2c** parameters.

Table 2-27 v1/v2c template parameters

Parameter	Description	Setting
Name	Name of the parameter template. You can find the SNMP template by its name when creating a discovery policy.	[Value range] ● The name is a string of 1 to 32 characters. ● The name contains letters, digits, underscores (_), and hyphens (-) and must start with a letter or underscore (_). [Example] test
Attempts	Number of attempts to resend an SNMP operation. If this number is exceeded, the resending is aborted.	[Value range] ● An integer ranging from 0 to 5. ● Default value: 3. [Example] 3
Timeout(s)	Time for you to wait after the protocol message is sent.	[Value range] ● An integer ranging from 1 to 5. ● Default value: 5. [Example] 3
Port	Port number of the specified NE to be accessed.	[Value range] ● An integer ranging from 1 to 65,535. ● Default value: 161. [Example] 3
Read community	Name of the community that has the read permission.	[Value range] Default value: public.
Write community	Name of the community that has the write permission.	[Value range] Default value: private.

- The following table describes the parameters of the **v3** template.

NOTE

Username, **Environment name**, **Environment engine ID**, **Authentication protocol**, **Authentication password**, **Data encryption protocol**, and **Data encryption password** parameters are available only when the **Protocol Version** is **SNMPv3**.

Table 2-28 v3 template parameters

Parameter	Description	Setting
Name	Name of the parameter template. You can find the SNMP template by its name when creating a discovery policy.	[Value range] The name is a string of 1 to 32 characters. It can contain letters, digits, underscores (_), and hyphens (-) and must begin with a letter or underscore (_). [Example] test
Attempts	Times of attempts to resend an SNMP operation. If this number is exceeded, the resending is aborted.	[Value range] ● An integer ranging from 0 to 5. ● Default value: 3. [Example] 3
Timeout(s)	Time for you to wait after the protocol message is sent.	[Value range] ● An integer ranging from 1 to 5. ● Default value: 5. [Example] 3
Port	Port number of the specified NE to be accessed.	[Value range] ● An integer ranging from 1 to 65,535. ● Default value: 161. [Example] 3
Username	User name for accessing the NE.	-

Parameter	Description	Setting
Context name	Name of the context engine.	[Value range] This parameter value is either the same as the context name on the NE or blank.
Context engine ID	Unique identifier of an SNMP engine. This ID is used together with the context name to determine an environment that uniquely identifies an SNMP entity. The SNMP message packet is processed only when the environment of the sender terminal is the same as that of the recipient terminal. Otherwise, the SNMP message packet will be discarded. This parameter supports two input modes: ● Hexadecimal input mode: The ID must be in the format of #**.**.**. The validity verification involves the value length and each hexadecimal value. The value contains a maximum of 97 characters (including #). ● Non-hexadecimal input mode: Enter the ID directly. The value must contain not more than 32 characters.	[Value range] The same as the context engine ID on the NE.

Parameter	Description	Setting
Authentication protocol	Protocol used for verifying messages. The parameter value can be **HMACMD5**, **HMACSHA** or blank. If you select **HMACMD5** or **HMACSHA**, set the authentication password.	-
Authentication password	You need to set this parameter after you select an authentication protocol for message verification.	-
Privacy protocol	Encryption protocol used for encapsulating data. The parameter value can be **DES**, **AES**, or empty. If you select **DES** or **AES**, set the encryption password. ● Data encryption standard (DES) is a globally accepted encryption algorithm and provides a 56-bit key. ● Advanced encryption standard (AES) provides 128-bit, 192-bit, and 256-bit keys for different security levels.	-
Privacy password	You need to set this parameter after you select an encryption algorithm for data encapsulation.	-

Step 5 Click **OK**.

The **Success** dialog box is displayed indicating that the operation succeeded.

Step 6 Click **OK**.

----End

Modifying SNMP Templates

If the SNMP parameters on a network element (NE) undergo changes, you need to modify the parameter template of the specified NE on the management system.

Prerequisites

SNMP parameter templates have been created. For details about how to create an SNMP parameter template, see **Creating an SNMP Parameter Template**.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **Template Management** > **SNMP Templates**.

Step 3 Click  corresponding to the SNMP parameter template to be modified.

The **Modify SNMP Template** dialog box is displayed.

Step 4 Modify the parameters of the template except its name. For description about the parameters, see **Creating an SNMP Template**.

Step 5 After the modification is complete, click **OK**.

The **Success** dialog box is displayed indicating that the modification succeeded.

Step 6 Click **OK**.

----End

2.10 Server Information

This section describes how to manage information about SFTP servers, including protocol types, user names, and passwords.

2.10.1 Notification Server

You can configure the email or short message service (SMS) server to send the alarm information to the specified email address or mobile phone number.

Modifying the Email Server

This section describes how to send alarm information to a specific mailbox by email on the management system.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **Server Information** > **Notification Server**.

Step 3 In the **Email Server** area of the function pane, click **Modify**.

The **Modify Email Server** dialog box is displayed.

Step 4 Set parameters for the email server. The following table describes the parameters.

Parameter	Description	Value
SMTP server	The information of the SMTP server for sending alarm notifications by email.	Notes You can input any value. [Example] 192.168.1.82
Server port	Port number of the SMTP server. The value is an integer between 1 and 65,535.	[Example] 25
Sender email	Email address that sends alarm notifications.	[Example] zhangsan@163.com
Test email	Email address used for verifying the communication between the management system server and mail server.	[Example] -
Security protocol	Security protocol used in SMTP server and InfraControl communication. The value is **Disable security protocols**, **SSL** or **TLS**. **NOTE** If the **SSL** protocol is used, may lead to the SMTP server and InfraControl communication is a security risk. You are advised to use the **TLS** protocol.	[Default Value] TLS [Example] TLS
SSL port	Port number of the SSL of the SMTP server. This parameter is available when **SSL** is selected in **Security protocol**.	[Value range] The value is an integer from 1 to 65,535. [Example] 45
SMTP server identity authentication	Indicating whether the SMTP will verify the identification of the email sender. If **SMTP server identity authentication** is not selected, **Username** and **Password** are unavailable.	[Example] -

Parameter	Description	Value
Username	User name for accessing the SMTP server. This parameter is available when **SMTP server identity authentication** is selected.	Note: The user name must be specified. [Example] zhangsan@163.com
Password	Password used for accessing the SMTP server. This parameter is available when **SMTP server identity authentication** is selected.	[Value range] A string of 1 to 64 characters [Example] aJ1p23dySQ
Proxy server	Information about the proxy sever.	[Example] -
Proxy server IP address	IP address of the proxy server. This parameter is available when **Proxy server** is selected.	[Example] 192.168.1.152
Proxy server port	Port number of the proxy server. This parameter is available when **Proxy server** is selected. The value is an integer between 1 and 65,535.	[Example] 1080

Step 5 After the parameters are specified, you can click **Test** to check whether the testing email box can receive the testing message about the communication status between the management system server and the mail server.

- If the test email address can receive the test message, communication between the ISM server and the email server is normal.
- If the test email address fails to receive the test message, communication between the ISM server and the email server is abnormal. Troubleshoot the fault as prompted.

Step 6 Click **OK**.

The **Success** dialog box is displayed indicating that the operation succeeded.

Step 7 Click **OK**.

----End

Modifying the SMS Modem

The configured short message service (SMS) modem sends alarm information to a specified mobile phone number.

Prerequisites

you need to ensure that the SMS modem is properly connected to the management system server.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **Server Information** > **Notification Server**.

Step 3 In the **SMS Modem** area of the function pane, click **Modify**.
The **Modify SMS Modem** dialog box is displayed.

Step 4 Set parameters for the email server. The following table describes the parameters.

Parameter	Description	Value
Serial port identifier	Identifier of the management system server serial port through which the management system is connected to the SMS modem. Set this parameter according to the actual condition. For example, if the management system server is connected to the SMS modem through serial port COM1 of the management system server, set this parameter to COM1. ● On Windows, if the NMS server is connected with the SMS modem through serial port COM1, set the serial port identifier to COM1. ● On Linux, if the NMS server is connected to the SMS modem through serial port COM1, set the serial port identifier to /dev/ttyS0.	[Example] COM1
Baud usage	Baud rate of the SMS modem. Set the baud rate according to the actual condition.	[Example] 115,200
Country code	Code of the country where the equipment carrier is located.	[Example] 86
Test phone number	Mobile phone number used for verifying communication between the management system server and SMS modem.	[Example] 13500001234

Step 5 You can click **Test** to check whether the test mobile phone can receive the test message.

- If the test mobile phone can receive the test message, communication is normal between the management system server and the SMS modem.
- If the test mobile phone fails to receive the test message, communication is abnormal between the ISM server and the SMS modem. Troubleshoot the fault as prompted.

Step 6 After the setting is complete, click **OK**.

----End

2.10.2 Modifying the SFTP Server

This section describes how to manage information about SFTP servers, including protocol status, user names, and passwords.

Context

NOTE

The SFTP server default user is **ismv2r5**, and default password is **Admin@1234**, change the password as prompted. You are prompted to change the password regularly.

Procedure

Step 1 On the menu bar, choose **Management**.

Step 2 In the navigation tree, choose **Server Information** > **SFTP server**.

Step 3 In the **SFTP Server** area, click  .
The **Modify** dialog box is displayed.

Step 4 Modify related information about the SFTP server. The following table describes the parameters.

Parameter	Description	Setting
SFTP Server	Protocol status of the SFTP server. The value can be either **Enable** or **Disabled**.	[Example] Enable
Username	User name for logging in to the SFTP server.	[Example] -
Password	Password for logging in to the SFTP server. ● The password must contain no less than eight characters, no more than 64 characters. ● The password must contain special characters, uppercase letters, lowercase letters, and digits. Special characters include: `~!@#$%^&*()-_=+|[{}];:'",<.>/? and blank space.	[Example] Admin@1234

----End

3 Managing InfraControl System User

About This Chapter

This topic describes default users of the InfraControl system, including OS users, northbound users. This topic also provides methods of modifying the default user passwords.

3.1 Default User Information

This topic describes the InfraControl system default users and user passwords.

User	Description
admin	The system provides one default administrator **admin**. The default administrator has all permissions, can manage all NEs, and can log in the InfraControl. The initial password is **Admin@123**. To change the password when first login, see "Logging In to the InfraControl" in *OceanStor InfraControl V100R002C01 Software Installation Guide*.
root	The **root** user is MySQL default user.
user	● The northbound SNMP V3 user. The initial password is **Admin@123**, to change the password, see **Modifying Northbound Trap Reporting Parameters**. ● The hierarchical NMS Trap user. The initial password is **Admin@123**, to change the password, see **Modifying Hierarchical NMS Trap Parameters**. ● SNMP V3 template user, it is used when devices are discovered by SNMP protocol.
ismv2r5	The SFTP user when connect the host, you need enable the SFTP service. The initial password is **Admin@1234**, to change the password, see **2.10.2 Modifying the SFTP Server**.
ICUser	In Linux, indicates a running user that starts and monitors the background processes. It can also be a maintenance user. By default, you are not allowed to log in to InfraControl as user **ICUser**.
Tomcat	In Linux, indicates a running user that starts foreground web processes. You are not allowed to log in to InfraControl as user **Tomcat**.
LEGO	The user group of **ICUser** and **Tomcat** users.
mysql	● Indicates a running mysql user, is not allowed to execute interactive login by default. ● Indicates a user group of mysql users.
Network Service	In Windows, indicates a running user that starts foreground, background and MySQL DB, is not allowed to execute interactive login by default.
System	In Windows, indicates a Monitor user, is not allowed to execute interactive login by default

3.2 Password Changing Rules

This topic describes the InfraControl system default users and user passwords.

- Password Changing Scenarios
  - Changing initial passwords
  - Password change after system maintenance handover
  - Regular password change

    It is recommended that passwords be changed regularly to ensure system security. The change frequency can be customized. The recommended password change frequency is 90 days.
- Password Complexity Requirements
  - The new password contains no less than eight characters.
  - The new password must contains special characters, uppercase letters, lowercase letters, and digits.
  - Special characters:

    `~!@#$%^&*()-_=+\|[{}];:'",<.>/? and blank space

4 Topology Management

About This Chapter

Topology management allows you to build a topology for a network and use it to monitor the whole network in real time.

4.1 Physical View

You can adjust the global topology to generate a clear topology view.

Procedure

Step 1 Choose **Topology** from the menu bar.

Step 2 In the navigation tree, choose **Topology** > **Physical View**.

The topology of the entire network is displayed.

You can move your cursor over a topology object to view its basic information. A topology object, which is visual and operable, represents an object on the actual network.

Step 3 Use the menu on the topology view to adjust the topology.

Name	Operation
Zoom in/out and reset	● Click  to zoom in the topology view. ● Click  to zoom out the topology view. ● Click  to reset the topology view to its default size.
Browse	Click  to automatically adjust the topology to a suitable size.
Full Screen	Click  to display the topology in full screen. To exit the full screen view, click  again or press **Esc**.
Select	Click  to go to the selecting mode.
Expand	Click  to hide the navigation tree. Click  again to display the navigation tree.
Save	Click  to save the current topology view.
Refresh	Click  to refresh the current topology view.
Export	Click  to export the current topology view.
Search	Click  . The **Topology Search** dialog box is displayed. You can enter search criteria to search for desired topologies.
OverView	Click  to display the aerial view. Click  again to hide the aerial view.
Legend	Click  to hide the legends of the topology view. Click  again to display the legends of the topology view.

Name	Operation
Set Background	Click  to set the background for the topology view.
Show Alarm	Select or deselect **Show Alarm** to display or hide alarm information.

----End

4.2 User-Defined View

In user-defined view, You can create,delete and modify topology view.

Procedure

Step 1 Choose **Topology** from the menu bar.

Step 2 In the navigation tree, choose **Topology** > **User-Defined View**.

Step 3 Right-click **User-Defined View** and choose **Create User-Defined View**.

The **Create User-Defined View** dialog box is displayed.

Step 4 In **Name**, enter a name for the view that you want to create.

Step 5 **Optional:** In **Description**, enter description about the view.

Step 6 Click **OK**.

NOTE

You can right-click a view that you have created and choose **Modify User-Defined View** or **Delete User-Defined View** to modify or delete the view.

Step 7 You can right-click on a topology view and choose shortcut menus to edit, delete, and adjust a topology view.

Name	Operation
New Node	Right-click and choose **New Node**. On the **New Node** dialog box, select a device to add it as a node.
Create Group	Right-click and choose **Create Group** from the shortcut menu to create a group on the topology.
Create Subnet	Right-click and choose **Create Subnet** from the shortcut menu to create a subnet on the topology.
Create Link	Right-click and choose **Create Link** from the shortcut menu. Click **Source Node** and **Destination Node**. On the **Create Link** dialog box, enter a link name and create the link.

Step 8 Use the menu on the topology view to adjust the topology.

Name	Operation
Zoom in/out and reset	● Click  to zoom in the topology view. ● Click  to zoom out the topology view. ● Click  to reset the topology view to its default size.
Browse	Click  to automatically adjust the topology to a suitable size.
Full Screen	Click  to display the topology in full screen. To exit the full screen view, click  again or press **Esc**.
Select	Click  to go to the selecting mode.
Expand	Click  to hide the navigation tree. Click  again to display the navigation tree.
Save	Click  to save the current topology view.
Refresh	Click  to refresh the current topology view.
Export	Click  to export the current topology view.
Search	Click  . The **Topology Search** dialog box is displayed. You can enter search criteria to search for desired topologies.
OverView	Click  to display the aerial view. Click  again to hide the aerial view.
Legend	Click  to hide the legends of the topology view. Click  again to display the legends of the topology view.
Set Background	Click  to set the background for the topology view.
Show Alarm	Select or deselect **Show Alarm** to display or hide alarm information.

----End

5 Resource Management

About This Chapter

You can discover different types of network elements (NEs) by using the configured discovery policies. You can monitor and manage the discovered NEs.

This section describes how to manage all virtual machines, including viewing the summary, hardware information, host path graph, free space, and current alarms of virtual machines.

5.8 Managing Oracle Instances
This chapter describes how to manage Oracle instances, including viewing Oracle instance information, tablespace, and file information.

5.9 Managing SQL Server Instances
This chapter describes how to manage SQL Server instances, including viewing SQL Server instances, databases, and files.

5.1 Overview

Different types of network elements (NEs) on the network may use different versions of network management protocols. Therefore, to implement unified and remote visualized management of NEs, the management system must be compatible with different versions of network management protocols, and support discovering, managing, and monitoring the networked devices by setting resource discovery policies.

Discovering an NE

You can create a parameter template based on the NE communication protocol and configure an NE discovery policy. Then the management system can use the template to discovery NEs by IP address or IP address segment.

- The Simple Network Management Protocol (SNMP) is used for communication between the management system server and NEs managed by the management system. The management system can access the NEs using the SNMP. If you manually create an NE discovery policy, the management system uses the created SNMP parameter template to discover specified NEs. When the NE access protocol parameters are changed, you need to modify the access protocol parameters of the specified NE on the management system to keep consistency. For details, see Creating an SNMP Template.
- Discover online NEs using the discovery policy and manage and monitor the discovered NEs. For details, see Creating a Discovery Policy.

Managing Devices

The management system supports monitoring and management of storage systems. The visualized interface facilitates device monitoring and management.

Device management includes:

- Managing Storage Systems
  - Managing disk arrays
  - Managing VIS systems
  - Managing unified storage systems
  - Managing VTLs
- Managing switches
  - Managing Fibre Channel switches
  - Managing Ethernet switches
- Managing hosts
  - Managing servers
  - Managing virtual servers
  - Managing virtual machines
- Managing applications
  - Managing Oracle instances
  - Managing SQL Server instances

5.2 Managing Disk Arrays

This section describes how to view details about a storage device's status and capacity. By doing so, you can optimize and recover storage devices in time for proactive maintenance and protection.

5.2.1 Managing All Disk Arrays

You can manage all disk arrays on the management system, including viewing disk array information, querying disk arrays, and refreshing disk arrays to obtain all information about monitored disk arrays.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Storage** > **Disk Arrays**.

Step 3 In the **Original Capacity Summary** area of the function pane, view the capacity summary of disk arrays.

In the **Original Capacity Summary** area, used capacity and remaining capacity of all disk arrays are displayed.

Step 4 In the **Capacity of Top 5 Unmapped LUNs** area of the function pane, view information about LUNs that have not been mapped.

Step 5 In the **Current Alarms** area of the function pane, view current alarm statistics of disk arrays. The following table describes the parameters.

Parameter	Description
Severity	Alarms at different severities have different impact on the system. ● **Critical**: A critical alarm interrupts services on a large scale or causes NEs to break down. A critical alarm must be handled immediately. Otherwise, the system may break down. ● **Major**: A major alarm affects a part of NEs or system functions. A major alarm must be handled as soon as possible. Otherwise, important functions will work improperly. ● **Warning**: A warning has no impact on NEs, but potentially affects services. The purpose of sending a warning is to inform the maintenance engineer of querying the alarm cause and rectifying potential faults. ● **Info**: This type of alarm has no impact on system functions or customer services. However, it has potential impact on the service quality of NEs or resources. Some **Info** alarms are to indicate that devices are back to normal. Warnings help maintenance engineers know the operating status of the network and NEs. Handle the alarms according to the actual condition.
Total	Quantity of all alarms.

Parameter	Description
Unconfirmed	Quantity of alarms that have not been confirmed.
Confirmed	Quantity of alarms that have been confirmed.

Step 6 In the **Disk Arrays** area of the function pane, query information of disk arrays.

- Select **Name** and enter a disk array name you want to query in the right text box. Click **Search** to query information of the corresponding disk array.
- Select **Status** and choose the status you want to query in the right drop-down list. Click **Search** to query information of corresponding disk arrays in the selected state.
- Select **IP address** and enter a IP address you want to query in the right text box. Click **Search** to query information of disk arrays corresponding to the selected IP address.
- Select **Model** and enter a model you want to query in the right text box. Click **Search** to query information about corresponding disk arrays of the model.

Step 7 In the **Disk Arrays** area of the function pane, view information about disk arrays. The following table describes the parameters.

Parameter	Description
Name	Name of the disk array.
Status	Status of the disk array, **Normal**, **Faulty**, or **Offline**.
IP Address	IP address of the management network port.
Total Capacity	Total capacity of the disk array.
LUN Capacity	Total capacity of LUNs.
Mapped LUN(%)	Percentage of mapped LUNs to all LUNs
Model	Model of the disk array.
Device Management	Opening the device management page when clicked.
Refresh	Refreshing selected devices when clicked.

----End

5.2.2 Viewing the Summary

By viewing the summary of a disk array, you can learn about its basic information, disk statistics, and port operating status.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Storage** > **Disk Arrays**.

Step 3 Select a disk array.

Step 4 In the function pane, select **Summary**.

Step 5 In the **Basic Information** area, view basic information of the selected disk array. The following table describes the parameters.

NOTE

Click **more** to view all of the basic information.

Parameter	Description
Name	Name of the disk array.
IP address	IP address of the disk array.
Model	Model of the disk array.
Total capacity	Total capacity of the disk array.
Block storage pools or Storage pools	Block storage pool or storage pool quantity of the disk array.
Manufacturer	Manufacturer of the disk array.
Last refreshed at	Time when the disk array was last refreshed.
Device Management	Opening the device management page when clicked.
Status	Status of the disk array, **Normal**, **Offline**, or **Faulty**.
SN	Serial number of the disk array.
Software version	Software version of the disk array.
Disks	Disk quantity of the disk array.
LUNs	Quantity of LUNs.
Location	Geological location of the disk array.
Resource Group	Resource group of the disk array.

Step 6 In the **Disk Health Status** area, view the port status of the selected disk array. The following table describes the parameters.

Parameter	Description
Normal	The functions and running parameters of the hard disk are normal.
Faulty	Some or all functions of the hard disk fail and the fault cannot be rectified.
Unknown	The system cannot report the health status of the hard disk.
Single link failure	In dual-controller mode, hard disks are identified by only one controller.

Parameter	Description
Unauthenticated	The hard disk has not been authenticated.
Spun down	The disk spins down.
Failing	The disk is failing.
Isolated	The disk slot is faulty and causes the hard disk in it to be automatically isolated.
Disk write protection	The hard disk is in the write protection state.

Step 7 In the **Port Operating Status** area, view the port operating status of the selected disk array. The following table describes the parameters.

Parameter	Description
Port Type	Types of ports on the disk array: ● **FC** ● **iSCSI**
Status Distribution	Quantity of online/offline ports.

----End

5.2.3 Managing Storage Resources

By managing storage resources, you can obtain information about hard disks, RAID groups, LUNs, controllers, and ports of the disk array, as well as mappings between these storage resources.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Storage** > **Disk Arrays**.

Step 3 Select a disk array.

Step 4 In the function pane, select **Storage Resource**.

Step 5 On the **Storage Resource** page, you can view mappings between storage resources.

NOTE

You can select **Show legends** to view icons used on the page. These icons enable you to view information about resources in an easier and more direct way.

You can click a RAID group to view mappings between objects. That is, mappings between disks, LUNs, owning controllers, and corresponding ports of mapped LUNs.

Step 6 You can view storage resource information by putting your mouse pointer on the storage resource.

1. Check controller information. The following table describes the parameters.

Parameter	Description
Name	Name of the controller.
Health status	Health status of the controller, **Normal**, **Faulty**, or **Unknown**.
Operating status	Operating status of the controller, **Online** or **Offline**.
IPv4 address	IPv4 address of the controller.
IPv6 address	IPv6 address of the controller.
Primary/ Secondary status	Working status of the controller, **Primary** or **Secondary**.

2. View hard disk information. The following table describes the parameters.

   NOTE

   Right-click the disk, and choose **View the Effect Range** from the shortcut menu. The **View the Effect Range** dialog box is displayed. And you can view the information about affected hosts and affected applications.

Parameter	Description
Enclosure ID	ID of the enclosure where the hard disk resides.
Slot ID	ID of the slot where the hard disk is inserted.
Physical type	Physical type of the hard disk.
Logical type	Logical type of the hard disk.
Capacity	Total capacity of the hard disk.
Owning block storage pool or Owning storage pool	Name of the block storage pool or storage pool that the hard disk belongs to, which can be a RAID group or thin pool.
Health status	Health status of the hard disk. The value can be **Normal**, **Faulty**, **Unknown**, **Single link failure**, **Unauthenticated**, **Spun down**, **Isolated**, **Failing**, or **Write protection**.
Operating status	Operating status of the hard disk. The value can be **Online**, **Offline**, **Reconstructing**, **Reconstructed**, **Copying back**, **Free hot spare disk**, **Used hot spare disk**, **Redundant copy**, or **Faulty**.

3. View port information. The following table describes the parameters.

Parameter	Description
Module ID	ID of the module where the port resides.

Parameter	Description
Port ID	ID of the port.
Type	Type of the port.
Health status	Health status of the port, **Normal**, **Faulty**, or **Unknown**.
Operating status	Operating status of the port. The value can be **Connected**, **Disconnected**, **Faulty**, or **Absent**
MAC address	MAC address of the iSCSI port. This parameter is valid when the port type is iSCSI.
IPv4 address	IPv4 address of an iSCSI port. This parameter is valid when the port type is iSCSI.
IPv6 address	IPv6 address of an iSCSI port. This parameter is valid when the port type is iSCSI.
WWN	Worldwide Name (WWN) of a Fibre Channel port or Serial Attached SCSI (SAS) port. This parameter is valid when the port type is Fibre Channel or SAS.
Operating rate	Operating rate of the port.
Owning controller	ID of the controller to which the port belongs.

4. View RAID group information. The following table describes the parameters.

Parameter	Description
Name	Name of the RAID group.
ID	ID of the RAID group.
Type	Type of the block RAID group, **RAID Group** or **Block Storage Pool**.
RAID level	The RAID level of the RAID group.
Capacity	Capacity of the RAID group.
Health status	Health status of the RAID group. The value can be **Normal**, **Faulty**, **Initializing**, **Deleting**, **Expanding**, **Spun down** or **Degraded**.
Operating status	Operating status of the RAID group, **Online** or **Offline**.

5. Check LUN information. The following table describes the parameters.

Parameter	Description
Name	Name of the LUN.

Parameter	Description
ID	ID of the LUN.
Owning block storage pool or Owning storage pool	The block storage pool or storage pool to which the LUN belongs.
RAID level	RAID level of the block storage pool to which the LUN belongs.
Capacity	Capacity of the LUN.
Health status	Health status of the LUN, **Normal**, **Faulty**, or **Unknown**.
Operating status	Operating status of the LUN. The value can be **Online**, **Offline**, **Unformatted**, **Formatting**, **Initializing**, or **Deleting**.

Step 7 In the text box on the upper right, enter a LUN name and click **Search**. The LUN is located.

----End

5.2.4 Managing Mappings

This section describes how to obtain information about host groups/mapping views, hosts and LUNs, as well as mappings between these objects.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Storage** > **Disk Arrays**.

Step 3 Select a disk array.

Step 4 In the function pane, select **Mapping**.

Step 5 In the **Mapping** area, you can check the mapping between different objects.

Step 6 You can view storage resource information by putting your mouse pointer on the storage resource.

1. View information about a host group/mapping view. The following table describes the parameters.

Parameter	Description
Name	Name of the host group/mapping view.
ID	ID of the host group/mapping view.
Hosts	Quantity of hosts contained in the host group/mapping view.
Mapped LUNs	Quantity of mapped LUNs.

2. View host information. The following table describes the parameters.

Parameter	Description
Name	Name of the host.
Whether or not to associate service hosts	Indicating whether to associate the host with service hosts.
Operating system	Operating system of the host.
Initiators	Quantity of the host initiators.
Mapped LUNs	Quantity of mapped LUNs.

3. View initiator information. The following table describes the parameters.

Parameter	Description
Identifier	Alias of the initiator.
HBA type	Type of the host bus adapter (HBA).
Status	Status of the initiator.

4. View LUN information. The following table describes the parameters.

Parameter	Description
Name	Name of the LUN.
ID	ID of the LUN.
WWN	WWN of the LUN.
Health status	Health status of the LUN, **Normal**, **Faulty**, or **Unknown**.
Operating status	Operating status of the LUN, **Online**, **Offline**, **Unformatted**, **Formatting**, **Initializing**, or **Deleting**.
Capacity	Capacity of the LUN.
Owning block storage pool or Owning storage pool	The block storage pool or storage pool to which the LUN belongs.

----End

5.2.5 Viewing Free Space

This section describes how to view free space of storage devices, hard disks, block storage pools, unmapped LUNs, and hosts.

Viewing Free Space of a Storage Device

By viewing free space of a storage device, you can learn about the space usage of the storage device.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Storage** > **Disk Arrays**.

Step 3 Select a disk array.

Step 4 In the function pane, choose **Free Space** > **Storage Device**. Select a storage device to view its space usage. The following table describes the parameters.

Parameter	Description
Device Name	Name of the disk array.
Total Capacity	Total capacity of the disk array.
Capacity of Mapped LUNs	Capacity of mapped LUNs.
Capacity of Private LUNs	Capacity of private LUNs **NOTE** If a LUN is used to extend storage capacity, its **Type** becomes **Private**. A private LUN cannot be mapped to a host or host group.
Capacity of Unmapped LUNs	Capacity of unmapped LUNs.
Used Hot Spare Capacity	Used capacity of the hot spare capacity.
Free Hot Spare Capacity	Free capacity of the hot spare capacity.
Free Capacity of Block Storage Pools or Free Capacity of Storage Pools	Free capacity of block storage pools or storage pools.
Free Disk Capacity	Capacity of free disks.
Hot Spare Disk Capacity	Capacity of hot spare disks.

----End

Viewing Free Space of a Hard Disk

By viewing free space of hard disks, you can learn about the space usage of the hard disks.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Storage** > **Disk Arrays**.

Step 3 Select a disk array.

Step 4 In the function pane, choose **Free Space** > **Disk** to view disk space usage. The following table describes the parameters.

Parameter	Description
Total Capacity	Total capacity of hard disks.
Free Disk Capacity	Capacity of free disks.
Member Disk Capacity	Capacity of member disks.
Hot Spare Disk Capacity	Capacity of hot spare disks.

----End

Viewing Free Space of a Block Storage Pool or a Storage Pool

By viewing free space of a block storage pool or a storage pool, you can learn about the space usage of the block storage pool or the storage pool.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Storage** > **Disk Arrays**.

Step 3 Select a disk array.

Step 4 In the function pane, choose **Free Space** > **Block Storage Pools** or **Free Space** > **Storage Pools**. Select a block storage pool or a storage pool to view its space usage. The following table describes the parameters.

Parameter	Description
Name	Name of the block storage pool or the storage pool.
ID	ID of the block storage pool or the storage pool.
RAID Level	RAID level of the block storage pool. **NOTE** This parameter is available only when selected **Free Space** > **Block Storage Pools**.

Parameter	Description
Type	Types of the block storage pool: ● **RAID group** ● **Thin Pool** **NOTE** This parameter is available only when selected **Free Space** > **Block Storage Pools**.
Total Capacity	Total capacity of the block storage pool or the storage pool.
Preset Capacity	Preset capacity of a thin pool. **NOTE** This parameter is available only when selected **Free Space** > **Block Storage Pools**.
Capacity of Mapped LUNs	Capacity of mapped LUNs in the block storage pool or the storage pool.
Capacity of Private LUNs	Capacity of private LUNs in the block storage pool. **NOTE** This parameter is available only when selected **Free Space** > **Block Storage Pools**. If a LUN is used to extend storage capacity, its **Type** becomes **Private**. A private LUN cannot be mapped to a host or host group.
Capacity of Unmapped LUNs	Capacity of unmapped LUNs in the block storage pool or the storage pool.
Used Hot Spare Capacity	Used capacity of the hot spare capacity. **NOTE** This parameter is available only when selected **Free Space** > **Storage Pools**.
Free Hot Spare Capacity	Free capacity of the hot spare capacity. **NOTE** This parameter is available only when selected **Free Space** > **Storage Pools**.
Free Capacity	Free capacity of the block storage pool or the storage pool.
Capacity Ratio	● Selected **Free Space** > **Block Storage Pools**, it is the respective percentages of **Capacity of Mapped LUNs**, **Capacity of Private LUNs**, **Capacity of Unmapped LUNs**, and **Free Capacity** in the block storage pool. ● Selected **Free Space** > **Storage Pools**, it is the respective percentages of **Capacity of Mapped LUNs**, **Capacity of Unmapped LUNs**, **Used Hot Spare Capacity**, **Free Hot Spare Capacity**, and **Free Capacity** in the storage pool.

Step 5 In the function pane, query information about a block storage pool or a storage pool.

- Select **Name** and enter a block storage pool or a storage pool name in the right text box. Click **Search** to query information about the corresponding block storage pool or storage pool.

- Select **ID** and enter a block storage pool or a storage pool ID in the right text box. Click **Search** to query information about the corresponding block storage pool or storage pool.

----End

Viewing Free Space of Unmapped LUNs

By viewing free space of unmapped LUNs, you can learn about space usage of the unmapped LUNs.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Storage** > **Disk Arrays**.

Step 3 Select a disk array.

Step 4 In the function pane, choose **Free Space** > **Unmapped LUNs** to view space usage of unmapped LUNs. The following table describes the parameters.

Parameter	Description
Name	Name of the unmapped LUN.
ID	ID of the unmapped LUN.
Type	Types of an unmapped LUN are described as follows: - **Common**: common LUNs - **Expansion**: An expansion LUN becomes an extended LUN after LUN expansion. The capacity of the extended LUN is the total capacity of the extending primary LUN and extending secondary LUNs. - **Thin**: A thin LUN is one whose owning block storage pool or storage pool is a thin pool.
Capacity	Total capacity of unmapped LUNs.
Owning Block Storage Pool or Owning Storage Pool	Block storage pool or storage pool that the unmapped LUN belongs to.

----End

Viewing Free Space of a Host

By viewing free space of a host, you can learn about the space usage of the host.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Storage** > **Disk Arrays**.

Step 3 Select a disk array.

Step 4 In the function pane, choose **Free Space** > **Hosts**. Select a host to view its space usage. The following table describes the parameters.

Parameter	Description
Host	Name of the host.
Operating System	Operating system of the host. Operating systems include: ● **Windows** ● **Linux** ● **Solaris** ● **HP-UX** ● **AIX** ● **XenServer** ● **Mac OS**
IP Address	IP address of the host.
Mapped LUNs	Quantity of LUNs mapped to the host.
Total Capacity of Mapped LUNs	Total capacity of LUNs mapped to the host.
Used Capacity	Used capacity of LUNs on the host.
Free Capacity	Free capacity of LUNs on the host.
Usage	Usage of LUN capacity mapped to the host.

Step 5 In the function pane, query information about a host.

- Select **Name** and enter the host name in the right text box. Click **Search** to query information about the corresponding host.
- Select **IP Address** and enter the host's IP address in the right text box. Click **Search** to query information about the corresponding host.

----End

5.2.6 Managing Current Alarms

Current alarms consist of current unconfirmed and confirmed alarms. This section describes to how to confirm a current alarm or cancel its confirmation, clear an alarm, and export alarms from the alarm database in a file.

Procedure

Step 1 View alarms on a disk array device.

1. On the menu bar, choose **Resources**.

2. In the left navigation tree, choose **Storage** > **Disk Arrays**.
3. Select a disk array device.
4. In the **Current Alarms** area of the right function pane, view the current alarms.

Step 2 Confirm alarms.

1. Select one or more alarms whose **Confirm Status** is **Unconfirmed**.
2. Click **Confirm**.

   The **Warning** dialog box is displayed.
3. Click **OK**.

   The **Success** dialog box is displayed.
4. Click **OK**.

   The alarms' **Confirm Status** becomes **Confirmed**.

   NOTE

   After the management system receives an alarm confirmation request, it records the personnel who confirmed the alarms, refreshes alarms displayed on all client PCs, and updates data in the alarm database.

Step 3 Cancel alarm confirmation.

Cancel the confirmation of a confirmed alarm.

1. Select one or more alarms whose **Confirm Status** is **Confirmed**.
2. Click **Cancel Confirmation**.

   The **Warning** dialog box is displayed.
3. Click **OK**.

   The **Success** dialog box is displayed.
4. Click **OK**.

   The status of the selected alarms becomes **Unconfirmed**.

Step 4 Clear alarms.

NOTE

In some special situations, for example, when communication between the management system and a network element (NE) breaks, the cleared alarms reported from the NE may be lost. In this case, these alarms will not be cleared automatically if the NE does not support the function of alarm verification. To resolve this problem, the management system supports manual alarms clearing. In other words, you can manually change the state of the alarms from uncleared to cleared.

1. Select one or more alarms whose **Confirm Status** is **Confirmed**.
2. Click **Clear**.

   The **Warning** dialog box is displayed.
3. Click **OK**.

   The **Success** dialog box is displayed.
4. Click **OK**.

   All the selected alarms are removed from the current alarm list to the historical alarm list. The management system records the clearance person and time, refreshes all the alarm displaying windows on the client, and updates data in the alarm database.

Step 5 Export alarms.

Export some important alarms in a file, helping the administrator to locate and analyze problems.

NOTE

If the default security policy has been set on the Internet Explorer, the system displays a message stating `To help protect you security, Internet Explorer blocked this site from downloading file from to your computer` upon your export operation. In this case, select the message, right-click it, and choose **Download File** from the shortcut menu. After the page is refreshed, export alarms.

1. Select one or multiple alarms.
2. Click **Export**.

   The **File Download** dialog box is displayed.
3. Click **Save**.

   The **Save As** dialog box is displayed.
4. Select a path for saving the alarm file, enter a name for the file or use the default file name, and click **Save**.

   The selected alarms are exported to the specified local path.

Step 6 Export all alarms.

Export all current alarms in a file, helping the administrator to locate and analyze problems.

NOTICE

You can export 20,000 alarms at most each time. If the alarm quantity exceeds 20,000, export them in several times.

1. Click **Export All**.

   The **File Download** dialog box is displayed.
2. Click **Save**.

   The **Save As** dialog box is displayed.
3. Select a path for saving the alarm file, enter a name for the file or use the default file name, and click **Save**.

   All current alarms are exported to the specified local path.

Step 7 Refresh alarms.

The refresh policy can be **Refresh every 15 seconds**, **Refresh every 30 seconds**, **Refresh every 60 seconds**, or **Stop refresh**.

Refresh every 30 seconds is selected by default. This means that the management system server performs a round robin every 30 seconds. Once a new alarm occurs, the management system will refresh it to the current alarm list.

Step 8 Search alarms.

Set the conditions to search for the desired alarms. The search method can be the basic search or advanced search.

- When you select **Search**, you can search for alarms by alarm severity.

- When you select **Advanced Search**, you can search for alarms by alarm severity, alarm type, confirmation status, alarm source, and alarm occurrence time.

NOTE

You can click **Reset** to clear all the specified parameter values.

Step 9 View alarms.

- You can click the name of an alarm to view its details.
  1. Click the name of an alarm.

     The page showing the details about the alarm is displayed.
  2. View the basic information and modification suggestions of the alarm.
  3. (Optional) Click **Create** in the **Maintenance Experiences** area to record the experiences in locating and handling the alarm into the alarm knowledge repository. This enables the alarm to be handled quickly next time the same type of fault occurs.

     You can also modify and delete the created maintenance experiences.
- You can click the times of an alarm to view the occurrence time, confirmation status and time, clearance status and time, and notification type of the alarm.

  According to the alarm notification type, you can know whether the alarm is a new alarm, manual clear, or automatic clear.

----End

5.3 Managing Fibre Channel Switches

This chapter describes how to viewing the summary, port, and zone information and manage current alarms of Fibre Channel switches.

5.3.1 Managing All Fibre Channel Switches

This section describes how to manage all Fibre Channel switches on the management system, including viewing information about FC switches and querying and refreshing FC switchs.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Switches** > **FC Switches**.

Step 3 In the **FC Switches** area of the function pane, query information about Fibre Channel switches.

- Select **IP Address** and enter a Fibre Channel switch's IP address you want to query in the right text box. Click **Search** to query information about the Fibre Channel switch.
- Select **Status** and choose the state you want to query in the right drop-down list. Click **Search** to query information about the Fibre Channel switches in the state.

Step 4 In the **FC Switches** area of the function pane, query information about Fibre Channel switches. The following table describes the parameters.

Parameter	Description
IP Address	IP address of the Fibre Channel switch.
Status	Status of the Fibre Channel switch. The value can be **Normal**, **Offline**, **Degraded**, **Faulty**, **Unused**, **Unknown**, **Warning**, **Other**, **Starting**, **Stopping**, **Stopped**, or **Spun Down**.
WWN	Worldwide Name (WWN) of the Fibre Channel switch.
Description	Description of the Fibre Channel switch.
Port	Ports on the Fibre Channel switch.
Connected Port	Connected ports on the Fibre Channel switch.
Device Management	Opening the device management page when clicked.
Refresh	Refreshing the selected device when clicked.

----End

5.3.2 Viewing the Summary

This section describes how to view the summary about a Fibre Channel switch, including its basic information and port connection status.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Switches** > **FC Switches**.

Step 3 Select a Fibre Channel switch.

Step 4 In the function pane, select **Summary**.

Step 5 In the **Basic Information** area, view basic information about the selected Fibre Channel switch. The following table describes the parameters.

Parameter	Description
IP address	IP address of the Fibre Channel switch.
SMI-Agent IP	IP address of the SMI-Agent. **NOTE** The parameter is available when a Brocade Fibre Channel switch is selected.

Parameter	Description
Status	Status of the Fibre Channel switch. Possible values for Qlogic and Brocade Fibre Channel switches are as follows: ● Qlogic FC **Normal**, **Offline**, **Faulty**, **Unused**, **Unknown**, or **Warning**. ● Brocade FC **Normal**, **Offline**, **Faulty**, **Unknown**, **Warning**, **Other**, **Degraded**, **Starting**, **Stopping**, **Stopped**, or **Spun down**.
WWN	Worldwide Name (WWN) of the Fibre Channel switch.
Port	Ports on the Fibre Channel switch.
Connected port	Connected ports on the Fibre Channel switch.
Location	Geological location of the Fibre Channel switch.
Description	Description of the Fibre Channel switch.
Resource group	Resource group of the Fibre Channel switch.
Last refreshed at	The last time that the device is refreshed.
Device Management	Opening the device management page when clicked.

Step 6 In the **Port Connection Status** area, view the port connection status of the selected Fibre Channel switch.

In the **Port Connection Status** area, the status of connected and disconnected ports is displayed.

NOTE

Click the **Port Connection Status** pie chart of the selected Fibre Channel switch. The **Connected Port Details** or **Disconnected Port Details** dialog box is displayed. And you can view the information about connected and disconnected ports.

----End

5.3.3 Viewing Port Information

This section describes how to view detailed information of a Fibre Channel switch port.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Switches** > **FC Switches**.

Step 3 Select a Fibre Channel switch.

Step 4 In the **Ports** area of the function pane, query information about a Fibre Channel switch port. The following table describes the parameters.

Parameter	Description
Port Number	Port number of the Fibre Channel switch.
Connection Status	Connection status of the Fibre Channel switch port, **Connected** or **Disconnected**.
WWN	Worldwide Name (WWN) of the Fibre Channel switch.
Peer WWN	WWN of the peer port that connects to the Fibre Channel switch.
Connected Object	Name of the device that is connected to the Fibre Channel switch.
Performance Monitoring	Monitored performance information of the Fibre Channel switch. You can click **Monitoring** to view monitored performance information of the port.

----End

5.3.4 Viewing Zone Information

This section describes how to view detailed information of a Fibre Channel switch zone.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Switches** > **FC Switches**.

Step 3 Select a Fibre Channel switch.

Step 4 In the **Zones** area of the function pane, query information about a Fibre Channel switch zone. The following table describes the parameters.

Parameter	Description
Zone Name	Name of the Fibre Channel switch zone.
Zone Set Name	Name of the Fibre Channel switch zone set.
Member Port	Quantity of the member ports in the Fibre Channel zone. You can click the value to view detailed information of the member port.

----End

5.3.5 Managing Current Alarms

Current alarms consist of current unconfirmed and confirmed alarms. This section describes to how to confirm a current alarm or cancel its confirmation, clear an alarm, and export alarms from the alarm database in a file.

Procedure

Step 1 View alarms on an FC switch.

1. On the menu bar, choose **Resources**.
2. In the left navigation tree, choose **Switches** > **FC Switches**.
3. Select an FC switch.
4. In the **Current Alarms** area of the right function pane, view the current alarms.

Step 2 Confirm alarms.

1. Select one or more alarms whose **Confirm Status** is **Unconfirmed**.
2. Click **Confirm**.

   The **Warning** dialog box is displayed.
3. Click **OK**.

   The **Success** dialog box is displayed.
4. Click **OK**.

   The alarms' **Confirm Status** becomes **Confirmed**.

   NOTE

   After the management system receives an alarm confirmation request, it records the personnel who confirmed the alarms, refreshes alarms displayed on all client PCs, and updates data in the alarm database.

Step 3 Cancel alarm confirmation.

Cancel the confirmation of a confirmed alarm.

1. Select one or more alarms whose **Confirm Status** is **Confirmed**.
2. Click **Cancel Confirmation**.

   The **Warning** dialog box is displayed.
3. Click **OK**.

   The **Success** dialog box is displayed.
4. Click **OK**.

   The status of the selected alarms becomes **Unconfirmed**.

Step 4 Clear alarms.

NOTE

In some special situations, for example, when communication between the management system and a network element (NE) breaks, the cleared alarms reported from the NE may be lost. In this case, these alarms will not be cleared automatically if the NE does not support the function of alarm verification. To resolve this problem, the management system supports manual alarms clearing. In other words, you can manually change the state of the alarms from uncleared to cleared.

1. Select one or more alarms whose **Confirm Status** is **Confirmed**.
2. Click **Clear**.

   The **Warning** dialog box is displayed.
3. Click **OK**.

   The **Success** dialog box is displayed.
4. Click **OK**.

All the selected alarms are removed from the current alarm list to the historical alarm list. The management system records the clearance person and time, refreshes all the alarm displaying windows on the client, and updates data in the alarm database.

Step 5 Export alarms.

Export some important alarms in a file, helping the administrator to locate and analyze problems.

NOTE

If the default security policy has been set on the Internet Explorer, the system displays a message stating `To help protect you security, Internet Explorer blocked this site from downloading file from to your computer` upon your export operation. In this case, select the message, right-click it, and choose **Download File** from the shortcut menu. After the page is refreshed, export alarms.

1. Select one or multiple alarms.
2. Click **Export**.

   The **File Download** dialog box is displayed.
3. Click **Save**.

   The **Save As** dialog box is displayed.
4. Select a path for saving the alarm file, enter a name for the file or use the default file name, and click **Save**.

   The selected alarms are exported to the specified local path.

Step 6 Export all alarms.

Export all current alarms in a file, helping the administrator to locate and analyze problems.

NOTICE

You can export 20,000 alarms at most each time. If the alarm quantity exceeds 20,000, export them in several times.

1. Click **Export All**.

   The **File Download** dialog box is displayed.
2. Click **Save**.

   The **Save As** dialog box is displayed.
3. Select a path for saving the alarm file, enter a name for the file or use the default file name, and click **Save**.

   All current alarms are exported to the specified local path.

Step 7 Refresh alarms.

The refresh policy can be **Refresh every 15 seconds**, **Refresh every 30 seconds**, **Refresh every 60 seconds**, or **Stop refresh**.

Refresh every 30 seconds is selected by default. This means that the management system server performs a round robin every 30 seconds. Once a new alarm occurs, the management system will refresh it to the current alarm list.

Step 8 Search alarms.

Set the conditions to search for the desired alarms. The search method can be the basic search or advanced search.

- When you select **Search**, you can search for alarms by alarm severity.
- When you select **Advanced Search**, you can search for alarms by alarm severity, alarm type, confirmation status, alarm source, and alarm occurrence time.

NOTE

You can click **Reset** to clear all the specified parameter values.

Step 9 View alarms.

- You can click the name of an alarm to view its details.
  1. Click the name of an alarm.

     The page showing the details about the alarm is displayed.
  2. View the basic information and modification suggestions of the alarm.
  3. (Optional) Click **Create** in the **Maintenance Experiences** area to record the experiences in locating and handling the alarm into the alarm knowledge repository. This enables the alarm to be handled quickly next time the same type of fault occurs.

     You can also modify and delete the created maintenance experiences.
- You can click the times of an alarm to view the occurrence time, confirmation status and time, clearance status and time, and notification type of the alarm.

  According to the alarm notification type, you can know whether the alarm is a new alarm, manual clear, or automatic clear.

----End

5.4 Managing Ethernet Switches

This chapter describes how to view the summary, port, VLAN, and trunk information of Ethernet switches and manage current alarms on them.

5.4.1 Managing All Ethernet Switches

This section describes how to manage all Ethernet switches on the management system, including viewing information about Ethernet switches and querying and refreshing Ethernet switches.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Switches** > **Ethernet Switches**.

Step 3 In the **Ethernet Switches** area of the function pane, query information about Ethernet switches.

- Select **IP address** and enter an Ethernet switch's IP address you want to query in the right text box. Click **Search** to query information about the corresponding Ethernet switch.
- Select **Status** and choose the state you want to query in the right drop-down list. Click **Search** to query information about Ethernet switches in the state.

Step 4 In the **Ethernet Switches** area of the function pane, view information about Ethernet switches. The following table describes the parameters.

Parameter	Description
IP Address	IP address of the Ethernet switch.
Status	Status of the Ethernet switch, **Normal** or **Offline**.
Description	Description of the Ethernet switch.
Port	Ports on the Ethernet switch.
Connected Port	Connected ports on the Ethernet switch.
Device Management	Opening the device management page when clicked.
Refresh	Refreshing the selected device when clicked.

----End

5.4.2 Viewing Summary

This section describes how to view summary about an Ethernet switch, including its basic information and port connection status.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Switches** > **Ethernet Switches**.

Step 3 Select an Ethernet switch.

Step 4 In the function pane, select **Summary**.

Step 5 In the **Basic Information** area, view basic information about the selected Ethernet switch. The following table describes the parameters.

Parameter	Description
IP address	IP address of the Ethernet switch.
Status	Status of the Ethernet switch, **Normal** or **Offline**.
Port	Ports on the Ethernet switch.
Connected ports	Connected ports on the Ethernet switch.
Location	Geological location of the Ethernet switch.

Parameter	Description
Description	Description of the Ethernet switch.
Resource group	Resource group of the Ethernet switch.
Last refreshed at	The last time that the device is refreshed.
Device Management	Opening the device management page when clicked.

Step 6 In the **Port connection status** area, view port connection status of the selected Ethernet switch.

In the **Port connection status** area, status of connected and disconnected ports of the selected Ethernet switch is displayed.

NOTE

Click the **Port Connection Status** pie chart of the selected Ethernet switch. The **Connected Port Details** or **Disconnected Port Details** dialog box is displayed. And you can view the information about connected and disconnected ports.

----End

5.4.3 Viewing Port Information

This section describes how to view details of an Ethernet switch port.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Switches** > **Ethernet Switches**.

Step 3 Select an Ethernet switch.

Step 4 In the **Ports** area of the function pane, query information about an Ethernet switch port. The following table describes the parameters.

Parameter	Description
Port Number	Port number of the Ethernet switch.
Connection Status	Connection status of the Ethernet switch port, **Connected** or **Disconnected**.
Peer MAC Address	MAC address of the host network adapter that is connected to the Ethernet switch.
Connected Object	Name of the device that is connected to the Ethernet switch.
Performance Monitoring	Description of the Ethernet switch. You can click **Monitoring** to view monitored performance information about the switch ports.

----End

5.4.4 Viewing VLANs Information

This section describes how to view VLAN information about an Ethernet switch.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Switches** > **Ethernet Switches**.

Step 3 Select an Ethernet switch.

Step 4 In the **VLANs** area of the function pane, query virtual local area network (VLAN) information about the selected Ethernet switch. The following table describes the parameters.

Parameter	Description
VLAN ID	VLAN ID of the Ethernet switch.
IP Address	IP address of the Ethernet switch.
Member Port	Quantity of ports on the Ethernet switch. You can click the value to view detailed information of the member port.

----End

5.4.5 Viewing Trunks Information

This section describes how to view Trunk information of an Ethernet switch.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Switches** > **Ethernet Switches**.

Step 3 Select an Ethernet switch.

Step 4 In the **Trunks** area of the function pane, query Trunk information about the selected Ethernet switch. The following table describes the parameters.

Parameter	Description
Trunk ID	Trunk ID of the Ethernet switch.
Connection Status	Connection status of the Trunk of the Ethernet switch.
Member Port	Quantity of Trunk ports on the Ethernet switch. You can click the value to view detailed information of the member port.

----End

5.4.6 Managing Current Alarms

Current alarms consist of current unconfirmed and confirmed alarms. This section describes to how to confirm a current alarm or cancel its confirmation, clear an alarm, and export alarms from the alarm database in a file.

Procedure

Step 1 View alarms on an Ethernet switch.

1. On the menu bar, choose **Resources**.
2. In the left navigation tree, choose **Switches** > **Ethernet Switches**.
3. Select an Ethernet switch.
4. In the **Current Alarms** area of the right function pane, view the current alarms.

Step 2 Confirm alarms.

1. Select one or more alarms whose **Confirm Status** is **Unconfirmed**.
2. Click **Confirm**.
   The **Warning** dialog box is displayed.
3. Click **OK**.
   The **Success** dialog box is displayed.
4. Click **OK**.
   The alarms' **Confirm Status** becomes **Confirmed**.

   NOTE

   After the management system receives an alarm confirmation request, it records the personnel who confirmed the alarms, refreshes alarms displayed on all client PCs, and updates data in the alarm database.

Step 3 Cancel alarm confirmation.

Cancel the confirmation of a confirmed alarm.

1. Select one or more alarms whose **Confirm Status** is **Confirmed**.
2. Click **Cancel Confirmation**.
   The **Warning** dialog box is displayed.
3. Click **OK**.
   The **Success** dialog box is displayed.
4. Click **OK**.
   The status of the selected alarms becomes **Unconfirmed**.

Step 4 Clear alarms.

NOTE

In some special situations, for example, when communication between the management system and a network element (NE) breaks, the cleared alarms reported from the NE may be lost. In this case, these alarms will not be cleared automatically if the NE does not support the function of alarm verification. To resolve this problem, the management system supports manual alarms clearing. In other words, you can manually change the state of the alarms from uncleared to cleared.

1. Select one or more alarms whose **Confirm Status** is **Confirmed**.
2. Click **Clear**.

The **Warning** dialog box is displayed.

3. Click **OK**.

   The **Success** dialog box is displayed.

4. Click **OK**.

   All the selected alarms are removed from the current alarm list to the historical alarm list. The management system records the clearance person and time, refreshes all the alarm displaying windows on the client, and updates data in the alarm database.

Step 5 Export alarms.

Export some important alarms in a file, helping the administrator to locate and analyze problems.

NOTE

If the default security policy has been set on the Internet Explorer, the system displays a message stating `To help protect you security, Internet Explorer blocked this site from downloading file from to your computer` upon your export operation. In this case, select the message, right-click it, and choose **Download File** from the shortcut menu. After the page is refreshed, export alarms.

1. Select one or multiple alarms.
2. Click **Export**.

   The **File Download** dialog box is displayed.

3. Click **Save**.

   The **Save As** dialog box is displayed.

4. Select a path for saving the alarm file, enter a name for the file or use the default file name, and click **Save**.

   The selected alarms are exported to the specified local path.

Step 6 Export all alarms.

Export all current alarms in a file, helping the administrator to locate and analyze problems.

NOTICE

You can export 20,000 alarms at most each time. If the alarm quantity exceeds 20,000, export them in several times.

1. Click **Export All**.

   The **File Download** dialog box is displayed.

2. Click **Save**.

   The **Save As** dialog box is displayed.

3. Select a path for saving the alarm file, enter a name for the file or use the default file name, and click **Save**.

   All current alarms are exported to the specified local path.

Step 7 Refresh alarms.

The refresh policy can be **Refresh every 15 seconds**, **Refresh every 30 seconds**, **Refresh every 60 seconds**, or **Stop refresh**.

Refresh every 30 seconds is selected by default. This means that the management system server performs a round robin every 30 seconds. Once a new alarm occurs, the management system will refresh it to the current alarm list.

Step 8 Search alarms.

Set the conditions to search for the desired alarms. The search method can be the basic search or advanced search.

- When you select **Search**, you can search for alarms by alarm severity.
- When you select **Advanced Search**, you can search for alarms by alarm severity, alarm type, confirmation status, alarm source, and alarm occurrence time.

NOTE

You can click **Reset** to clear all the specified parameter values.

Step 9 View alarms.

- You can click the name of an alarm to view its details.
  1. Click the name of an alarm.

     The page showing the details about the alarm is displayed.
  2. View the basic information and modification suggestions of the alarm.
  3. (Optional) Click **Create** in the **Maintenance Experiences** area to record the experiences in locating and handling the alarm into the alarm knowledge repository. This enables the alarm to be handled quickly next time the same type of fault occurs.

     You can also modify and delete the created maintenance experiences.
- You can click the times of an alarm to view the occurrence time, confirmation status and time, clearance status and time, and notification type of the alarm.

  According to the alarm notification type, you can know whether the alarm is a new alarm, manual clear, or automatic clear.

----End

5.5 Managing Servers

This chapter describes how to manage all servers on the management system, including viewing the summary, hardware information, host path graph, logical relationship graph, free space, and current alarms of servers.

5.5.1 Managing All Servers

This section describes how to view server information and query and refresh servers.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Hosts** > **Servers**.

Step 3 In the **Servers** area of the function pane, query information about servers.

- Select **Name** and enter a server name you want to query in the right text box. Click **Search** to query information about the server.
- Select **Status** and choose the state you want to query in the right drop-down list. Click **Search** to query information about servers in the state.
- Select **IP Address** and enter a server's IP address you want to query in the right text box. Click **Search** to query information about the server.

Step 4 In the **Servers** area of the function pane, view information about servers. The following table describes the parameters.

Parameter	Description
Name	Name of the server.
Status	Status of the server, **Online** or **Offline**.
Operating System	Operating system of the server.
IP Address	IP address of the server.
CPU Frequency (MHz)	CPU frequency of the server.
Memory Size	Memory size of the server.
Total Disk Capacity	Total capacity of disks on the server.
File System Capacity	Total capacity of file systems on the server.
File System Usage (%)	Capacity usage of file systems on the server.
Refresh	Refreshing the selected device when clicked.

----End

5.5.2 Viewing Summary

This section describes how to view basic information, file system capacity summary, hard disk status, and application status of a selected server.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Hosts** > **Servers**.

Step 3 Select a target server.

Step 4 In the function pane, select **Summary**.

Step 5 In the **Basic Information** area, view basic information about the selected server. The following table describes the parameters.

Parameter	Description
Name	Name of the server.
Status	Status of the server, **Normal** or **Offline**.
IP address	IP address of the server.
Operating system	Operating system of the server. Operating system types include Windows and Linux. [Example] Windows
Total file system capacity	File system total capacity and capacity usage of the server.
Manufacturer	Manufacturer of the server.
Location	Geological location of the server.
Resource group	Resource group of the server.
Last refreshed at	Time when the server was last refreshed.

Step 6 In the **Disk Status** area, view hard disk usage of the selected server.

In the **Disk Status** area, quantities of activated and unactivated hard disks on the server are displayed.

Step 7 In the **Application Status** area, view basic information about applications of the server. The following table describes the parameters.

Parameter	Description
Name	Name of the application.
Status Distribution	Status of the application, **Online** or **Offline**.

----End

5.5.3 Viewing Hardware Information

This section describes how to view a server's hardware information on the management system, including CPU, memory, network ports, HBA ports, and hard disks.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Hosts** > **Servers**.

Step 3 Select a server.

Step 4 In the function pane, select **Hardware Information**.

Step 5 In the **CPU and Memory** area, view basic information about the selected server. The following table describes the parameters.

Parameter	Description
CPU Name	CPU name of the server.
CPU cores	CPU cores of the server.
Frequency	CPU frequency of the server.
Physical memory size	Physical memory size of the server.
Virtual memory size	Virtual memory size of the server.

Step 6 In the **Network Ports** area, view network port information of the selected server. The following table describes the parameters.

Parameter	Description
Name	Name of the network port.
Status	Status of the network port. The value can be **Non_operational**, **Unreachable**, **Disconnected**, **Connecting**, **Connected**, or **Operational**.
Rate (Mbit/s)	Rate of the network port.
MAC Address	MAC address of the network port.
IPv4 Address	IPv4 address of the network port.
IPv6 Address	IPv6 address of the network port.

Step 7 In the **HBA Ports** area, view basic information about HBA ports. The following table describes the parameters.

Parameter	Description
Name	Name of the HBA port.
Type	Type of the HBA port.
Status	Status of the HBA port.
Rate (Gbit/s)	Rate of the HBA port.
WWN/IQN	WWN (for a Fibre Channel port) or IQN (for an iSCSI port) of the network port.

Step 8 In the **Disks** area, view basic information about server disks. The following table describes the parameters.

Parameter	Description
Name	Name of the hard disk.
SN/WWN	Serial number or WWN of the hard disk.
Status	Status of the hard disk, **Active** or **Inactive**.
Total Capacity	Total capacity of the hard disk.
Usage (%)	Usage of the hard disk.
Manufacturer	Manufacturer of the hard disk.

----End

5.5.4 Viewing Host Path Graph

This section describes how to learn about path relationship between a selected server and its storage resources by viewing the host path graph.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Hosts** > **Servers**.

Step 3 Select a server.

Step 4 In the function pane, select **Host Path Graph**.

Step 5 View host path information about the selected server. The following table describes the parameters.

Parameter	Description
Disk	Hard disk that a LUN/volume belongs to.
Port	Port of the server.
Switch	Switch IP address.
Controller/Node	Controller/Node that a LUN/volume belongs to.
Storage Device	Storage device that a LUN/volume belongs to.
LUN/Volume	Name of a LUN/volume.

Step 6 In the **Path View** area, view path graph of the selected server.

NOTE

- Select **Show UltraPath**, view ultra path graph of the selected server.
- Select **Show Legend**, view legend graph of the selected server.

----End

5.5.5 Viewing Logical Relationship Graph

This section describes how to learn about the logical relationship between database of a selected server and the disk where the database resides.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Hosts** > **Servers**.

Step 3 Select a server.

Step 4 In the function pane, select **Logical Relationship Graph**.

Step 5 View logical relationship of the selected server.

----End

5.5.6 Viewing Free Space

This section describes how to view the summaries and details of hard disks and file systems.

Viewing Free Space of a Hard Disk

This section describes how to view space usage of a hard disk.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Hosts** > **Servers**.

Step 3 Select a server.

Step 4 In the function pane, choose **Free Space** > **Disks**. The following table describes the parameters.

Parameter	Description
Name	Name of the hard disk.
Type	Type of the hard disk.
SN/WWN	Serial number or WWN of the hard disk.
Total Capacity	Total capacity of the hard disk.
Capacity Allocated	Allocated capacity of the hard disk.
Free Capacity	Free capacity of the hard disk.
Usage (%)	Usage of the hard disk.

----End

Viewing Free Space of a File System

This section describes how to view space usage of a file system.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Hosts** > **Servers**.

Step 3 Select a server.

Step 4 In the function pane, choose **Free Space** > **File Systems**. The following table describes the parameters.

Parameter	Description
Name	Name of the file system.
Type	Type of the file system.
Owning Disk	Disk where the file system resides.
Total Capacity	Total capacity of the file system.
Used Capacity	Used capacity of the file system.
Free Capacity	Free capacity of the file system.
Usage (%)	Usage of the file system.

NOTE

The value of the **Free Capacity** could be negative, please check whether the file system is anomalous or the device has rebooted.

----End

5.5.7 Managing Current Alarms

Current alarms consist of current unconfirmed and confirmed alarms. This section describes to how to confirm a current alarm or cancel its confirmation, clear an alarm, and export alarms from the alarm database in a file.

Procedure

Step 1 View alarms on a server.

1. On the menu bar, choose **Resources**.
2. In the left navigation tree, choose **Hosts** > **Servers**.
3. Select a server.
4. In the **Current Alarms** area of the right function pane, view the current alarms.

Step 2 Confirm alarms.

1. Select one or more alarms whose **Confirm Status** is **Unconfirmed**.
2. Click **Confirm**.

   The **Warning** dialog box is displayed.
3. Click **OK**.

   The **Success** dialog box is displayed.
4. Click **OK**.

   The alarms' **Confirm Status** becomes **Confirmed**.

   NOTE

   After the management system receives an alarm confirmation request, it records the personnel who confirmed the alarms, refreshes alarms displayed on all client PCs, and updates data in the alarm database.

Step 3 Cancel alarm confirmation.

Cancel the confirmation of a confirmed alarm.

1. Select one or more alarms whose **Confirm Status** is **Confirmed**.
2. Click **Cancel Confirmation**.

   The **Warning** dialog box is displayed.
3. Click **OK**.

   The **Success** dialog box is displayed.
4. Click **OK**.

   The status of the selected alarms becomes **Unconfirmed**.

Step 4 Clear alarms.

NOTE

In some special situations, for example, when communication between the management system and a network element (NE) breaks, the cleared alarms reported from the NE may be lost. In this case, these alarms will not be cleared automatically if the NE does not support the function of alarm verification. To resolve this problem, the management system supports manual alarms clearing. In other words, you can manually change the state of the alarms from uncleared to cleared.

1. Select one or more alarms whose **Confirm Status** is **Confirmed**.
2. Click **Clear**.

   The **Warning** dialog box is displayed.
3. Click **OK**.

   The **Success** dialog box is displayed.
4. Click **OK**.

   All the selected alarms are removed from the current alarm list to the historical alarm list. The management system records the clearance person and time, refreshes all the alarm displaying windows on the client, and updates data in the alarm database.

Step 5 Export alarms.

Export some important alarms in a file, helping the administrator to locate and analyze problems.

NOTE

If the default security policy has been set on the Internet Explorer, the system displays a message stating `To help protect you security, Internet Explorer blocked this site from downloading file from to your computer` upon your export operation. In this case, select the message, right-click it, and choose **Download File** from the shortcut menu. After the page is refreshed, export alarms.

1. Select one or multiple alarms.
2. Click **Export**.

   The **File Download** dialog box is displayed.
3. Click **Save**.

   The **Save As** dialog box is displayed.
4. Select a path for saving the alarm file, enter a name for the file or use the default file name, and click **Save**.

   The selected alarms are exported to the specified local path.

Step 6 Export all alarms.

Export all current alarms in a file, helping the administrator to locate and analyze problems.

NOTICE

You can export 20,000 alarms at most each time. If the alarm quantity exceeds 20,000, export them in several times.

1. Click **Export All**.

   The **File Download** dialog box is displayed.
2. Click **Save**.

   The **Save As** dialog box is displayed.
3. Select a path for saving the alarm file, enter a name for the file or use the default file name, and click **Save**.

   All current alarms are exported to the specified local path.

Step 7 Refresh alarms.

The refresh policy can be **Refresh every 15 seconds**, **Refresh every 30 seconds**, **Refresh every 60 seconds**, or **Stop refresh**.

Refresh every 30 seconds is selected by default. This means that the management system server performs a round robin every 30 seconds. Once a new alarm occurs, the management system will refresh it to the current alarm list.

Step 8 Search alarms.

Set the conditions to search for the desired alarms. The search method can be the basic search or advanced search.

- When you select **Search**, you can search for alarms by alarm severity.

- When you select **Advanced Search**, you can search for alarms by alarm severity, alarm type, confirmation status, alarm source, and alarm occurrence time.

NOTE

You can click **Reset** to clear all the specified parameter values.

Step 9 View alarms.

- You can click the name of an alarm to view its details.
  1. Click the name of an alarm.

     The page showing the details about the alarm is displayed.
  2. View the basic information and modification suggestions of the alarm.
  3. (Optional) Click **Create** in the **Maintenance Experiences** area to record the experiences in locating and handling the alarm into the alarm knowledge repository. This enables the alarm to be handled quickly next time the same type of fault occurs.

     You can also modify and delete the created maintenance experiences.
- You can click the times of an alarm to view the occurrence time, confirmation status and time, clearance status and time, and notification type of the alarm.

  According to the alarm notification type, you can know whether the alarm is a new alarm, manual clear, or automatic clear.

----End

5.6 Managing Virtualization Servers

This chapter describes how to manage all virtualization servers on the management system, including viewing the summary, hardware information, host path graph, free space, and current alarms of virtualization servers.

5.6.1 Managing All Virtualization Servers

This section describes how to view virtualization server information and query and refresh virtualization servers.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Hosts** > **Virtualization Servers**.

Step 3 In the **Virtualization Servers** area of the function pane, view information about virtualization servers.

- Select **Name** and enter a virtualization server name you want to query in the right text box. Click **Search** to query information about the corresponding virtualization server.
- Select **Status** and choose the state you want to query in the right drop-down list. Click **Search** to query information about corresponding virtualization servers in the state.
- Select **IP Address** and enter a virtualization server's IP address you want to query in the right text box. Click **Search** to query information about the corresponding virtualization server.

Step 4 In the **Virtualization Servers** area of the function pane, view information about virtualization servers. The following table describes the parameters.

Parameter	Description
Name	Name of the virtualization server.
Status	Status of the virtualization server, **Running**, **Offline**, **Standby**, **Unknown**, or **Closed**.
Software Version	Software version of the virtualization server.
IP Address	IP address of the virtualization server.
CPU Frequency (MHz)	CPU frequency of the virtualization server.
Memory Size	Memory size of the virtualization server.
Total Disk Capacity	Total capacity of disks on the virtualization server.
Disk Usage (%)	Capacity usage of disks on the virtualization server.
Total Data Storage Capacity	Total capacity of data storage on the virtualization server.
Data Storage Usage (%)	Usage of data storage on the virtualization server.
Refresh	Refreshing the selected device when clicked.

----End

5.6.2 Viewing Summary

This section describes how to view basic information, data storage summary, hard disk status, and virtual machine status of a selected virtualization server.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Hosts** > **Virtualization Servers**.

Step 3 Select a virtualization server.

Step 4 In the function pane, select **Summary**.

Step 5 In the **Basic Information** area, view basic information about the selected virtualization server. The following table describes the parameters.

Parameter	Description
Name	Name of the virtualization server.

Parameter	Description
Status	Status of the virtualization server, **Running**, **Offline**, **Standby**, **Unknown**, or **Closed**.
IP address	IP address of the virtualization server.
Software version	Software version of the virtualization server.
Total data storage capacity	Total data storage capacity and capacity usage of the virtualization server.
Manufacturer	Manufacturer of the virtualization server.
Location	Geological location of the virtualization server.
Resource group	Resource group of the virtualization server.
Last refreshed at	Time when the server was last refreshed.

Step 6 In the **Disk Status** area, view hard disk usage of the selected virtualization server.

In the **Disk Status** area, quantity of disks in different states are displayed.

The state of a disk can be **Normal**, **Closed**, **Degraded**, **Error**, **Inactive**, **Unknown**, or **Offline**.

Step 7 In the **Virtual Machine Status** area, view quantities of virtual machines in different states of the selected virtualization server.

In the **Virtual Machine Status** area, quantities of virtual machines in different states of the selected virtualization server are displayed.

The state of a virtual machine can be **Running**, **Closed**, or **Suspended**.

----End

5.6.3 Viewing Hardware Information

This section describes how to view a virtualization server's hardware information on the management system, including CPU, memory, network ports, HBA ports, and hard disks.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Hosts** > **Virtualization Servers**.

Step 3 Select a virtualization server.

Step 4 In the function pane, select **Hardware Information**.

Step 5 In the **CPU and Memory** area, view basic information about the selected virtualization server. The following table describes the parameters.

Parameter	Description
CPU name	CPU name of the virtualization server.
CPU cores	CPU cores of the virtualization server.
Frequency	CPU frequency of the virtualization server.
Physical memory size	Physical memory size of the virtualization server.

Step 6 In the **Network Ports** area, view network port information of the selected virtualization server. The following table describes the parameters.

Parameter	Description
Name	Name of the network port.
Type	Type of the network port. The value can be **Virtual Network Port** or **Physical Network Port**.
Status	Status of the virtualization server. This parameter is valid when the port type is **Physical Network Port**. The value can be either **Connected** or **Disconnected**.
MAC Address	MAC address of the network port.
IPv4 Address	IPv4 address of the network port.
IPv6 Address	IPv6 address of the network port.

Step 7 In the **HBA Ports** area, view basic information about HBA ports. The following table describes the parameters.

Parameter	Description
Name	Name of the HBA port.
Type	Type of the HBA port.
Status	Status of the HBA port.
Rate (Gbit/s)	Rate of the HBA port.
WWN/IQN	WWN (for a Fibre Channel port) or IQN (for an iSCSI port) of the HBA port.

Step 8 In the **Disks** area, view basic information about virtualization server disks. The following table describes the parameters.

Parameter	Description
Name	Name of the hard disk.

Parameter	Description
Type	Type of the hard disk.
SN/WWN	Serial number or WWN of the hard disk.
Status	Status of the hard disk, **Normal**, **Closed**, **Degraded**, **Error**, **Inactive**, **Unknown**, or **Offline**.
Total Capacity	Total capacity of the hard disk.
Usage (%)	Usage of the hard disk.
Manufacturer	Manufacturer of the hard disk.

----End

5.6.4 Viewing the Host Path Graph

This section describes how to learn about end-to-end relationship between a selected virtualization server and its storage resources by viewing the host path graph.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Hosts** > **Virtualization Servers**.

Step 3 Select a virtualization server.

Step 4 In the function pane, select **Host Path Graph**.

Step 5 View host path information about the selected virtualization server. The following table describes the parameters.

Parameter	Description
Disk	Hard disk that a LUN/volume belongs to.
Port	Port of the virtualization server.
Switch	Switch IP address.
Controller/Node	Controller/Node that a LUN/volume belongs to.
Storage Device	Storage device that a LUN/volume belongs to.
LUN/Volume	Name of a LUN/volume.

Step 6 In the **Path View** area, view path relationship between the selected virtualization server and its used storage devices.

NOTE

- Select **Show UltraPath**, view ultra path graph of the selected server.
- Select **Show Legend**, view legend graph of the selected server.

----End

5.6.5 Viewing Free Space

This section describes how to view summary and detailed information about hard disks and data storage.

Viewing Free Space of a Hard Disk

This section describes how to view space usage of a hard disk.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Hosts** > **Virtualization Servers**.

Step 3 Select a virtualization server.

Step 4 In the function pane, choose **Free Space** > **Disks**. The following table describes related parameters.

Parameter	Description
Name	Name of the hard disk.
Type	Type of the hard disk.
SN/WWN	Serial number or Worldwide Name of the hard disk.
Total Capacity	Total capacity of the hard disk.
Capacity Allocated	Allocated capacity of the hard disk.
Free Capacity	Free capacity of the hard disk.
Usage (%)	Usage of the hard disk.

----End

Viewing Free Space of Data Storage

This section describes how to view space usage of data storage.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Hosts** > **Virtualization Servers**.

Step 3 Select a virtualization server.

Step 4 In the function pane, choose **Free Space** > **Data Storage**. The following table describes the parameters.

Parameter	Description
Name	Name of the hard disk.
Path	Path of the hard disk.
Member Disk	Type of the hard disk.
Total Capacity	Total capacity of the hard disk.
Capacity Allocated	Allocated capacity of the hard disk.
Free Capacity	Free capacity of the hard disk.
Usage (%)	Usage of the hard disk.

----End

5.6.6 Managing Current Alarms

Current alarms consist of current unconfirmed and confirmed alarms. This section describes to how to confirm a current alarm or cancel its confirmation, clear an alarm, and export alarms from the alarm database in a file.

Procedure

Step 1 View alarms on a virtualization server.

1. On the menu bar, choose **Resources**.
2. In the left navigation tree, choose **Hosts** > **Virtualization Servers**.
3. Select a virtualization server.
4. In the **Current Alarms** area of the right function pane, view the current alarms.

Step 2 Confirm alarms.

1. Select one or more alarms whose **Confirm Status** is **Unconfirmed**.
2. Click **Confirm**.

   The **Warning** dialog box is displayed.
3. Click **OK**.

   The **Success** dialog box is displayed.
4. Click **OK**.

   The alarms' **Confirm Status** becomes **Confirmed**.

   NOTE

   After the management system receives an alarm confirmation request, it records the personnel who confirmed the alarms, refreshes alarms displayed on all client PCs, and updates data in the alarm database.

Step 3 Cancel alarm confirmation.

Cancel the confirmation of a confirmed alarm.

1. Select one or more alarms whose **Confirm Status** is **Confirmed**.
2. Click **Cancel Confirmation**.

   The **Warning** dialog box is displayed.
3. Click **OK**.

   The **Success** dialog box is displayed.
4. Click **OK**.

   The status of the selected alarms becomes **Unconfirmed**.

Step 4 Clear alarms.

NOTE

In some special situations, for example, when communication between the management system and a network element (NE) breaks, the cleared alarms reported from the NE may be lost. In this case, these alarms will not be cleared automatically if the NE does not support the function of alarm verification. To resolve this problem, the management system supports manual alarms clearing. In other words, you can manually change the state of the alarms from uncleared to cleared.

1. Select one or more alarms whose **Confirm Status** is **Confirmed**.
2. Click **Clear**.

   The **Warning** dialog box is displayed.
3. Click **OK**.

   The **Success** dialog box is displayed.
4. Click **OK**.

   All the selected alarms are removed from the current alarm list to the historical alarm list. The management system records the clearance person and time, refreshes all the alarm displaying windows on the client, and updates data in the alarm database.

Step 5 Export alarms.

Export some important alarms in a file, helping the administrator to locate and analyze problems.

NOTE

If the default security policy has been set on the Internet Explorer, the system displays a message stating `To help protect you security, Internet Explorer blocked this site from downloading file from to your computer` upon your export operation. In this case, select the message, right-click it, and choose **Download File** from the shortcut menu. After the page is refreshed, export alarms.

1. Select one or multiple alarms.
2. Click **Export**.

   The **File Download** dialog box is displayed.
3. Click **Save**.

   The **Save As** dialog box is displayed.
4. Select a path for saving the alarm file, enter a name for the file or use the default file name, and click **Save**.

   The selected alarms are exported to the specified local path.

Step 6 Export all alarms.

Export all current alarms in a file, helping the administrator to locate and analyze problems.

NOTICE

You can export 20,000 alarms at most each time. If the alarm quantity exceeds 20,000, export them in several times.

1. Click **Export All**.

   The **File Download** dialog box is displayed.
2. Click **Save**.

   The **Save As** dialog box is displayed.
3. Select a path for saving the alarm file, enter a name for the file or use the default file name, and click **Save**.

   All current alarms are exported to the specified local path.

Step 7 Refresh alarms.

The refresh policy can be **Refresh every 15 seconds**, **Refresh every 30 seconds**, **Refresh every 60 seconds**, or **Stop refresh**.

Refresh every 30 seconds is selected by default. This means that the management system server performs a round robin every 30 seconds. Once a new alarm occurs, the management system will refresh it to the current alarm list.

Step 8 Search alarms.

Set the conditions to search for the desired alarms. The search method can be the basic search or advanced search.

- When you select **Search**, you can search for alarms by alarm severity.
- When you select **Advanced Search**, you can search for alarms by alarm severity, alarm type, confirmation status, alarm source, and alarm occurrence time.

NOTE

You can click **Reset** to clear all the specified parameter values.

Step 9 View alarms.

- You can click the name of an alarm to view its details.
  1. Click the name of an alarm.

     The page showing the details about the alarm is displayed.
  2. View the basic information and modification suggestions of the alarm.
  3. (Optional) Click **Create** in the **Maintenance Experiences** area to record the experiences in locating and handling the alarm into the alarm knowledge repository. This enables the alarm to be handled quickly next time the same type of fault occurs.

     You can also modify and delete the created maintenance experiences.
- You can click the times of an alarm to view the occurrence time, confirmation status and time, clearance status and time, and notification type of the alarm.

According to the alarm notification type, you can know whether the alarm is a new alarm, manual clear, or automatic clear.

----End

5.7 Managing Virtual Machines

This section describes how to manage all virtual machines, including viewing the summary, hardware information, host path graph, free space, and current alarms of virtual machines.

5.7.1 Viewing Information About ALL Virtual Machines

This section describes how to view virtual machine information and query and refresh virtual machines.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Hosts** > **Virtual Machines**.

Step 3 In the **Virtual Machines** area of the function pane, query information about virtual machines.

- Select **Name** and enter a virtual machine name you want to query in the right text box. Click **Search** to query information about the corresponding virtual machine.
- Select **Status** and choose the state you want to query in the right drop-down list. Click **Search** to query information about corresponding virtual machines in the state.
- Select **IP address** and enter a virtual machine's IP address you want to query in the right text box. Click **Search** to query information about the corresponding virtual machine.

Step 4 In the **Virtual Machines** area of the function pane, view information of virtual machines. The following table describes the parameters.

Parameter	Description
Name	Name of the virtual machine.
Status	Status of the virtual machine, **Running**, **Closed**, or **Suspended**.
Operating System	Operating system of the virtual machine. Types of operating systems: ● **Windows** ● **Linux**
IP Address	IP address of the virtual machine.
CPU Frequency (MHz)	CPU frequency of the virtual machine.
Memory Size	Memory size of the virtual machine.
Total Disk Capacity	Total capacity of disks on the virtual machine.

Parameter	Description
Disk Usage (%)	Capacity usage of disks on the virtual machine.
Owning Virtualization Server	Name of the virtualization server that the virtual machine belongs to.
Owning Data Storage	Name of the data storage that the virtual machine belongs to.

----End

5.7.2 Viewing Summary

This section describes how to view basic information, file system capacity summary, hard disk status, and application status of a selected virtual machine.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Hosts** > **Virtual Machines**.

Step 3 Select a virtual machine.

Step 4 In the function pane, select **Summary**.

Step 5 In the **Basic Information** area, view basic information of the selected virtual machine. The following table describes the parameters.

Parameter	Description
Name	Name of the virtual machine.
Status	Status of the virtual machine, **Running**, **Closed**, or **Suspended**.
IP address	IP address of the virtual machine.
Operating system	Operating system of the host. Types of operating systems: ● **Windows** ● **Linux**
Total file system capacity	Total file system capacity and capacity usage of the virtual machine.
Owning virtualization server	Name of the virtualization server that the virtual machine belongs to.
Used data storage	Name of used data storage.

Step 6 In the **Disk Status** area, view hard disk usage of the selected virtual machine.

In the **Disk Status** area, quantities of activated and unactivated hard disks on the virtual machine are displayed.

Step 7 In the **Application Status** area, view information about applications of the virtual machine. The following table describes the parameters.

Parameter	Description
Name	Name of the application.
Status Distribution	Status of the application. Possible values as follows: ● **Online** ● **Offline**

----End

5.7.3 Viewing Hardware Information

This section describes how to view a virtual machine's hardware information on the management system, including CPU, memory, network ports, HBAs, and hard disks.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Hosts** > **Virtual Machines**.

Step 3 Select a virtual machine.

Step 4 In the function pane, select **Hardware Information**.

Step 5 In the **CPU and Memory** area, view basic information about the selected virtual machine. The following table describes the parameters.

Parameter	Description
CPU Name	Name of the virtual machine.
CPU Cores	Quantity of CPU cores of the virtual machine.
Frequency	CPU frequency of the virtual machine.
Physical Memory Size	Physical memory size of the virtual machine.
Virtual Memory Size	Virtual memory size of the virtual machine.

Step 6 In the **Network Ports** area, view network port information about the selected virtual machine. The following table describes the parameters.

Parameter	Description
Name	Name of the network port.
Status	Status of the virtual machine. The value can be **Non_operational**, **Unreachable**, **Disconnected**, **Connecting**, **Connected**, or **Operational**. **NOTE** The following two cases, the components of the state may be "--": ● Virtual machine discovery parameter information is not configured. ● Virtual machine OS does not recognize the component information.
Rate (Mbit/s)	Rate of the network port.
MAC Address	MAC address of the network port.
IPv4 Address	IPv4 address of the network port.
IPv6 Address	IPv6 address of the network port.

Step 7 In the **HBA Ports** area, view basic information about HBA ports. The following table describes the parameters.

Parameter	Description
Name	Name of the HBA port.
Type	Type of the HBA port.
Status	Status of the HBA port.
Rate (Gbit/s)	Rate of the HBA port.
WWN/IQN	WWN (for a Fibre Channel port) or IQN (for an iSCSI port) of the HBA port.

Step 8 In the **Disks** area, view basic information about virtual machine disks. The following table describes the parameters.

Parameter	Description
Name	Name of the hard disk.
Type	Type of the hard disk.
SN/WWN	Serial number or WWN of the hard disk.
Status	Status of the hard disk, **Active** or **Inactive**. **NOTE** The following two cases, the components of the state may be "--": ● Virtual machine discovery parameter information is not configured. ● Virtual machine OS does not recognize the component information.

Parameter	Description
Total Capacity	Total capacity of the hard disk.
Usage (%)	Usage of the hard disk.
Manufacturer	Manufacturer of the hard disk.

----End

5.7.4 Viewing Host Path Graph

This section describes how to learn about path relation between a selected virtual machine and its storage resources by viewing the host path graph.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Hosts** > **Virtual Machines**.

Step 3 Select a virtual machine.

Step 4 In the function pane, select **Host Path Graph**.

Step 5 View host path information about the selected server. The following table describes the parameters.

Parameter	Description
Disk	Hard disk that a LUN/volume belongs to.
Type	Type of a hard disk.
Data Storage	Name of the data storage.
Virtualization Server Disk	Name of a virtualization server disk.
Port	Port of the virtual machine.
Switch	Switch IP address.
Controller/Node	Controller/Node that a LUN/volume belongs to.
Storage Device	Storage device that a LUN/volume belongs to.
LUN/Volume	Name of a LUN/volume.

Step 6 In the **Path View** area, view path relationship between the selected virtual machine and its used storage resources.

----End

5.7.5 Viewing Free Space

This section describes how to view summary and detailed information about hard disks and file systems.

Viewing Free Space of a Hard Disk

This section describes how to view space usage of a hard disk.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Hosts** > **Virtual Machines**.

Step 3 Select a virtual machine.

Step 4 In the function pane, choose **Free Space** > **Disks**. The following table describes the parameters.

Parameter	Description
Name	Name of the hard disk.
Type	Type of the hard disk.
SN/WWN	Serial number or WWN of the hard disk.
Total Capacity	Total capacity of the hard disk.
Capacity Allocated	Allocated capacity of the hard disk.
Free Capacity	Free capacity of the hard disk.
Usage (%)	Usage of the hard disk.

----End

Viewing Free Space of a File System

This section describes how to view space usage of a file system.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Hosts** > **Virtual Machines**.

Step 3 Select a virtual machine.

Step 4 In the function pane, choose **Free Space** > **File Systems**. The following table describes the parameters.

Parameter	Description
Name	Name of the file system.

Parameter	Description
Type	Type of the file system.
Owning Disk	Disk where the file system resides.
Total Capacity	Total capacity of the file system.
Used Capacity	Used capacity of the file system.
Free Capacity	Free capacity of the file system.
Usage (%)	Usage of the file system.

----End

5.7.6 Managing Current Alarms

Current alarms consist of current unconfirmed and confirmed alarms. This section describes to how to confirm a current alarm or cancel its confirmation, clear an alarm, and export alarms from the alarm database in a file.

Procedure

Step 1 View alarms on a virtual machine.

1. On the menu bar, choose **Resources**.
2. In the left navigation tree, choose **Hosts** > **Virtual Machines**.
3. Select a virtual machine.
4. In the **Current Alarms** area of the right function pane, view the current alarms.

Step 2 Confirm alarms.

1. Select one or more alarms whose **Confirm Status** is **Unconfirmed**.
2. Click **Confirm**.
   The **Warning** dialog box is displayed.
3. Click **OK**.
   The **Success** dialog box is displayed.
4. Click **OK**.
   The alarms' **Confirm Status** becomes **Confirmed**.

   NOTE

   After the management system receives an alarm confirmation request, it records the personnel who confirmed the alarms, refreshes alarms displayed on all client PCs, and updates data in the alarm database.

Step 3 Cancel alarm confirmation.

Cancel the confirmation of a confirmed alarm.

1. Select one or more alarms whose **Confirm Status** is **Confirmed**.
2. Click **Cancel Confirmation**.

The **Warning** dialog box is displayed.

3. Click **OK**.

   The **Success** dialog box is displayed.

4. Click **OK**.

   The status of the selected alarms becomes **Unconfirmed**.

Step 4 Clear alarms.

NOTE

In some special situations, for example, when communication between the management system and a network element (NE) breaks, the cleared alarms reported from the NE may be lost. In this case, these alarms will not be cleared automatically if the NE does not support the function of alarm verification. To resolve this problem, the management system supports manual alarms clearing. In other words, you can manually change the state of the alarms from uncleared to cleared.

1. Select one or more alarms whose **Confirm Status** is **Confirmed**.
2. Click **Clear**.

   The **Warning** dialog box is displayed.

3. Click **OK**.

   The **Success** dialog box is displayed.

4. Click **OK**.

   All the selected alarms are removed from the current alarm list to the historical alarm list. The management system records the clearance person and time, refreshes all the alarm displaying windows on the client, and updates data in the alarm database.

Step 5 Export alarms.

Export some important alarms in a file, helping the administrator to locate and analyze problems.

NOTE

If the default security policy has been set on the Internet Explorer, the system displays a message stating `To help protect you security, Internet Explorer blocked this site from downloading file from to your computer` upon your export operation. In this case, select the message, right-click it, and choose **Download File** from the shortcut menu. After the page is refreshed, export alarms.

1. Select one or multiple alarms.
2. Click **Export**.

   The **File Download** dialog box is displayed.

3. Click **Save**.

   The **Save As** dialog box is displayed.

4. Select a path for saving the alarm file, enter a name for the file or use the default file name, and click **Save**.

   The selected alarms are exported to the specified local path.

Step 6 Export all alarms.

Export all current alarms in a file, helping the administrator to locate and analyze problems.

NOTICE

You can export 20,000 alarms at most each time. If the alarm quantity exceeds 20,000, export them in several times.

1. Click **Export All**.

   The **File Download** dialog box is displayed.

2. Click **Save**.

   The **Save As** dialog box is displayed.

3. Select a path for saving the alarm file, enter a name for the file or use the default file name, and click **Save**.

   All current alarms are exported to the specified local path.

Step 7 Refresh alarms.

The refresh policy can be **Refresh every 15 seconds**, **Refresh every 30 seconds**, **Refresh every 60 seconds**, or **Stop refresh**.

Refresh every 30 seconds is selected by default. This means that the management system server performs a round robin every 30 seconds. Once a new alarm occurs, the management system will refresh it to the current alarm list.

Step 8 Search alarms.

Set the conditions to search for the desired alarms. The search method can be the basic search or advanced search.

- When you select **Search**, you can search for alarms by alarm severity.
- When you select **Advanced Search**, you can search for alarms by alarm severity, alarm type, confirmation status, alarm source, and alarm occurrence time.

NOTE

You can click **Reset** to clear all the specified parameter values.

Step 9 View alarms.

- You can click the name of an alarm to view its details.
  1. Click the name of an alarm.

     The page showing the details about the alarm is displayed.
  2. View the basic information and modification suggestions of the alarm.
  3. (Optional) Click **Create** in the **Maintenance Experiences** area to record the experiences in locating and handling the alarm into the alarm knowledge repository. This enables the alarm to be handled quickly next time the same type of fault occurs.

     You can also modify and delete the created maintenance experiences.
- You can click the times of an alarm to view the occurrence time, confirmation status and time, clearance status and time, and notification type of the alarm.

  According to the alarm notification type, you can know whether the alarm is a new alarm, manual clear, or automatic clear.

----End

5.8 Managing Oracle Instances

This chapter describes how to manage Oracle instances, including viewing Oracle instance information, tablespace, and file information.

5.8.1 Viewing Information About All Oracle Instances

This section describes how to view information about all Oracle instances and query Oracle instances.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Applications** > **Oracles**.

Step 3 In the **Oracle Instances** area of the function pane, query information about Oracle instances.

- Select **Name** and enter an Oracle instance name in the right text box. Click **Search** to query information about the corresponding Oracle instance.
- Select **Status** and choose the status you want to query in the right drop-down list. Click **Search** to query information of corresponding Oracle instances in the state.

Step 4 In the **Oracle Instance** area of the function pane, view information about Oracle instances. The following table describes the parameters.

Parameter	Description
Name	Name of the Oracle instance.
Status	Status of the Oracle instance, **Online** or **Offline**.
Version	Version of the Oracle instance.
Owning server/ virtual machine	Name of the server/virtual machine where the Oracle instance is.
Owning virtualization server	Name of the server that the Oracle instance belongs to.

Step 5 Click an Oracle instance name to view detailed information.

For details, see **5.8.2 Viewing Detailed Oracle Instance Information**.

----End

5.8.2 Viewing Detailed Oracle Instance Information

This section describes how to view detailed information about a selected Oracle instance, including its basic information, tablespace, and files.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Applications** > **Oracles**.

Step 3 Select an Oracle instance.

Step 4 In the **Basic Information** area of the function pane, query information about the selected Oracle instance.

Parameter	Description
Name	Name of the Oracle instance.
Status	Status of the Oracle instance, **Online** or **Offline**.
Version	Version of the Oracle instance.
Database name	Name of the Oracle instance database.
Owning server/ virtual machine	Name of the server/virtual machine where the Oracle instance is.
Owning virtualization server	Name of the server that the Oracle instance belongs to.

Step 5 Click the **Tablespace** tab to view tablespace information of the selected Oracle instance. The following table describes the parameters.

Parameter	Description
Name	Name of the tablespace.
Status	Status of the tablespace.
Total Capacity	Total capacity of the tablespace.
Used Capacity	Used capacity of the tablespace.
Usage (%)	Capacity usage of the tablespace.
Contained Data Files	Data files contained in the tablespace.

Step 6 Click the **File** tab to view file information about the selected Oracle instance. The following table describes the parameters.

Parameter	Description
Name	Name of the file.
Owning File System/Disk	File system or disk where the file resides.

Parameter	Description
Type	Type of the file, **Data File**, **Log File**, or **Control File**.
Owning Tablespace	Name of the tablespace that the file belongs to.

----End

5.9 Managing SQL Server Instances

This chapter describes how to manage SQL Server instances, including viewing SQL Server instances, databases, and files.

5.9.1 Viewing Information About All SQL Server Instances

This section describes how to view information about all SQL Server instances and query SQL Server instances.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Applications** > **SQL Servers**.

Step 3 In the **SQL Server Instances** area of the function pane, query information about SQL Server instances.

- Select **Name** and enter an SQL Server instance name in the right text box. Click **Search** to query information about the corresponding SQL Server instance.
- Select **Status** and choose the status you want to query in the right list. Click **Search** to query information about corresponding SQL Server instances.

Step 4 In the **SQL Server Instances** area of the function pane, view information about SQL Server instances. The following table describes the parameters.

Parameter	Description
Name	Name of the SQL Server instance.
Status	Status of the SQL Server instance, **Online** or **Offline**.
Version	Version of the SQL Server instance.
Owning server/ virtual machine	Name of the Server/virtual machine where the SQL Server instance is.
Owning virtualization server	Name of the server that the SQL Server instance belongs to.

Step 5 Click an SQL Server instance name to view detailed information.

For details, see **5.9.2 Viewing Detailed Information About a SQL Server Instance**.

----End

5.9.2 Viewing Detailed Information About a SQL Server Instance

This section describes how to view detailed information about a selected SQL Server instance, including its basic information, database, and files.

Procedure

Step 1 On the menu bar, choose **Resources**.

Step 2 In the navigation tree, choose **Applications** > **SQL Servers**.

Step 3 Select an SQL Server instance.

Step 4 In the **Basic Information** area of the function pane, query information about the selected SQL Server instance.

Parameter	Description
Name	Name of the SQL Server instance.
Status	Status of the SQL Server instance, **Online** or **Offline**.
Version	Version of the SQL Server instance.
Owning server/ virtual machine	Name of the server/virtual machine where the SQL Server instance resides.
Owning virtualization server	Name of the server that the SQL Server instance belongs to.

Step 5 Click the **Database** tab to view file information about the selected SQL Server instance. The following table describes the parameters.

Parameter	Description
Name	Name of the database.
Status	Status of the database.
Total Capacity	Total capacity of the database.
Used Capacity	Used capacity of the database.
Usage (%)	Capacity usage of the database.
Contained Data Files	Data files contained in the database.

Step 6 Click the **File** tab to view file information about the selected SQL Server instance. The following table describes the parameters.

Parameter	Description
Name	Name of the file.

Parameter	Description
Owning File System	File system where the file resides.
Type	Type of the file.
Owning Database	Name of the database that the file belongs to.

----End

6 Alarm Management

About This Chapter

The alarm management module provides such functions as alarm statistics, alarm notification, alarm synchronization, and alarm masking. By viewing the alarm information, you can monitor the network exceptions in real time and take measures to recover the network in time.

This section describes how to set thresholds of performance indicators and capacity usage for the device and its components. If the performance or capacity usage exceeds the specified threshold, an alarm occurs.

6.1 Overview

By viewing the current alarms on a network element (NE), you can discover and handle the NE faults in time.

Alarms and Events

- Similarity

  Both alarms and events are methods of reflecting the changes detected by the management system on the managed objects.

- Difference
  - Alarms are special events. Alarms indicate that the management system or its managed objects are abnormal or faulty. Alarms must be handled as soon as possible to protect services from being affected.
  - Events indicate changes of the managed objects, but the changes may not cause service exceptions.

Alarm Severity

Alarm severity indicates the urgency and importance of an alarm. The management system classifies alarms into the four severities: critical, major, minor, and warning. **Table 6-1** describes definitions and handling procedures of different alarm severities.

Table 6-1 Alarm severities

Severity	Icon	Definition	Handling Urgency
Critical		A critical alarm interrupts services on a large scale or causes NEs to break down.	A critical alarm must be handled immediately. Otherwise, the system may break down.
Major		A major alarm affects a part of NEs or system functions.	A major alarm must be handled as soon as possible. Otherwise, important functions will work improperly.

Severity	Icon	Definition	Handling Urgency
Warning		A minor alarm has no impact on NEs, but potentially affects services.	The purpose of sending a minor alarm is to instruct the maintenance personnel of querying the alarm cause and rectifying potential faults.
Info		A warning has no impact on the system functions or customer services. However, it has potential impact on the service quality of NEs or resources. Some warnings are to indicate that devices are back to normal.	Warnings help maintenance engineers know the operating status of the network and NEs. A warning is handled according to the actual condition.

Alarm Status

Alarm status indicates whether an alarm is confirmed. A confirmed alarm indicates that the alarm has been handled.

- Confirmed: The alarm has been handled by users.
- Unconfirmed: The alarm is not handled.

Alarm Type

According to alarm features, alarms are divided into the following types:

- Communication alarm

  Concerns communication failures between NEs, an NE and the management system, and different management system software.
- Environment alarm

  Concerns power supply system and equipment room environment, such as temperature, humidity, and door access control.
- NE alarm

  Concerns physical resources faults.
- Service quality alarm

  Concerns service quality degradation.
- Faulty operation alarm

Concerns software error or faulty operation.

- Security alarm

  Concerns the management system and NE security.

Alarm Management Function

- Alarm statistics

  You can search for the current alarms at different severities of all devices on the management system, and learn about the experiences in handling the alarms by viewing the alarm details on the management system.

- Alarm synchronization

  The management system provides alarm synchronization to ensure that the alarm data is accurate and up to date. The alarm synchronization is categorized as manual synchronization and periodic synchronization.

- Alarm masking

  After alarm masking is enabled, the management system will display alarms reported by NEs only in the masked alarm list.

- Alarm notification

  The management system provides multiple means for notifying alarms (by short message, email, or sound). The management system sends the alarm information to the specified mobile phone or email address, or notifies the maintenance personnel of the alarms through the client sound box. This helps ensure timely and efficient troubleshooting.

- Alarm dump

  This function dumps the historical alarms in a file to the specified folder, improving the management system performance.

- Miscellaneous function

  You can use the alarm confirmation mechanism to verify that the current alarm is handled in time. You can manually confirm the specified alarm or cancel the confirmation, and clear the confirmed alarms from the current alarm list. In addition, you can add maintenance experiences to each alarm. That is, you can record experiences in locating, analyzing, and handling alarms in the alarm knowledge repository, helping other administrators learn about the operations performed to an alarm and sharing the maintenance experiences.

Alarm Notification

The management system supports remote alarm notification by the following methods:

- Email

  In this method, remote alarm notification is sent by email. The alarm information is sent to the specified email address. The maintenance engineer can learn about the alarm information by viewing the mail message.

- Short message

  In this method, remote alarm notification is sent by short message. The alarm information is sent to the mobile phone number of the maintenance engineer through the SMS service provided by the service provider or the SMS modem connected to the management system server. The maintenance engineer can learn about the alarm information by reading the short message.

- Sound

  In this method, alarm notification is implemented by sound. Once an alarm is generated, the client sound box plays an alarm sound. After hearing the sound, the maintenance engineer will check alarm information received by the management system server.

6.2 Managing Alarms

The alarm confirmation mechanism can identify whether a current alarm is handled in time. In addition, you can add alarm maintenance experiences to each alarm, facilitating system maintenance and sharing experiences.

6.2.1 Managing Current Alarms

Current alarms consist of current unconfirmed and confirmed alarms. This section describes to how to confirm a current alarm or cancel its confirmation, clear an alarm, and export alarms from the alarm database in a file.

Procedure

Step 1 Go to the **Current Alarms** page in any of the following ways:

- 1. View alarms on all devices.
  1. On the menu bar, choose **Alarms**.
  2. In the navigation tree, choose **Alarm Management** > **Current Alarms**.
- 2. View alarms on the storage device.
  1. On the menu bar, choose **Resources**.
  2. In the navigation tree, choose **Storage**.
  3. Select a storage device.
  4. In the function pane, select **Current Alarms**.
- 3. Viewing alarms on a switch.
  1. On the menu bar, choose **Resources**.
  2. In the navigation tree, choose **Switches**.
  3. Select a switch.
  4. In the function pane, select **Current Alarms**.
- 4. Viewing alarms on a host.
  1. On the menu bar, choose **Resources**.
  2. In the navigation tree, choose **Hosts**.
  3. Select a host.
  4. In the function pane, select **Current Alarms**.

Step 2 Confirm alarms.

1. Select one or more alarms whose **Confirm Status** is **Unconfirmed**.
2. Click **Confirm**.

   The **Warning** dialog box is displayed.

3. Click **OK**.

   The **Success** dialog box is displayed.

4. Click **OK**.

   The alarms' **Confirm Status** becomes **Confirmed**.

   NOTE

   After the management system receives an alarm confirmation request, it records the personnel who confirmed the alarms, refreshes alarms displayed on all client PCs, and updates data in the alarm database.

Step 3 Cancel alarm confirmation.

Cancel the confirmation of a confirmed alarm.

1. Select one or more alarms whose **Confirm Status** is **Confirmed**.
2. Click **Cancel Confirmation**.

   The **Warning** dialog box is displayed.

3. Click **OK**.

   The **Success** dialog box is displayed.

4. Click **OK**.

   The status of the selected alarms becomes **Unconfirmed**.

Step 4 Clear alarms.

NOTE

In some special situations, for example, when communication between the management system and a network element (NE) breaks, the cleared alarms reported from the NE may be lost. In this case, these alarms will not be cleared automatically if the NE does not support the function of alarm verification. To resolve this problem, the management system supports manual alarms clearing. In other words, you can manually change the state of the alarms from uncleared to cleared.

1. Select one or more alarms whose **Confirm Status** is **Confirmed**.
2. Click **Clear**.

   The **Warning** dialog box is displayed.

3. Click **OK**.

   The **Success** dialog box is displayed.

4. Click **OK**.

   All the selected alarms are removed from the current alarm list to the historical alarm list. The management system records the clearance person and time, refreshes all the alarm displaying windows on the client, and updates data in the alarm database.

Step 5 Export alarms.

Export some important alarms in a file, helping the administrator to locate and analyze problems.

NOTE

If the default security policy has been set on the Internet Explorer, the system displays a message stating `To help protect you security, Internet Explorer blocked this site from downloading file from to your computer` upon your export operation. In this case, select the message, right-click it, and choose **Download File** from the shortcut menu. After the page is refreshed, export alarms.

1. Select one or multiple alarms.

2. Click **Export**.

   The **File Download** dialog box is displayed.

3. Click **Save**.

   The **Save As** dialog box is displayed.

4. Select a path for saving the alarm file, enter a name for the file or use the default file name, and click **Save**.

   The selected alarms are exported to the specified local path.

Step 6 Export all alarms.

Export all current alarms in a file, helping the administrator to locate and analyze problems.

NOTICE

You can export 20,000 alarms at most each time. If the alarm quantity exceeds 20,000, export them in several times.

1. Click **Export All**.

   The **File Download** dialog box is displayed.

2. Click **Save**.

   The **Save As** dialog box is displayed.

3. Select a path for saving the alarm file, enter a name for the file or use the default file name, and click **Save**.

   All current alarms are exported to the specified local path.

Step 7 Refresh alarms.

The refresh policy can be **Refresh every 15 seconds**, **Refresh every 30 seconds**, **Refresh every 60 seconds**, or **Stop refresh**.

Refresh every 30 seconds is selected by default. This means that the management system server performs a round robin every 30 seconds. Once a new alarm occurs, the management system will refresh it to the current alarm list.

Step 8 Search alarms.

Set the conditions to search for the desired alarms. The search method can be the basic search or advanced search.

- When you select **Search**, you can search for alarms by alarm severity.
- When you select **Advanced Search**, you can search for alarms by alarm severity, alarm type, confirmation status, alarm source, and alarm occurrence time.

NOTE

You can click **Reset** to clear all the specified parameter values.

Step 9 View alarms.

- You can click the name of an alarm to view its details.

1. Click the name of an alarm.

   The page showing the details about the alarm is displayed.

2. View the basic information and modification suggestions of the alarm.
3. (Optional) Click **Create** in the **Maintenance Experiences** area to record the experiences in locating and handling the alarm into the alarm knowledge repository. This enables the alarm to be handled quickly next time the same type of fault occurs.

   You can also modify and delete the created maintenance experiences.

- You can click the times of an alarm to view the occurrence time, confirmation status and time, clearance status and time, and notification type of the alarm.

  According to the alarm notification type, you can know whether the alarm is a new alarm, manual clear, or automatic clear.

----End

6.2.2 Managing Historical Alarms

Past alarms are cleared alarms. You can export one or multiple past alarms.

Procedure

Step 1 On the menu bar, choose **Alarms**.

Step 2 In the navigation tree, choose **Alarm Management** > **Historical Alarms**.

Step 3 You can perform the following operations to manage past alarms:

- Export

  This operation exports some important alarms in a file, helping the administrator locate and analyze problems.

  NOTE

  If the Internet Explorer executes the default security policy, the **To help protect you security, Internet Explorer blocked this site from downloading file from to your computer** message is displayed upon an export operation. In this case, right-click the message, and choose **Download File** from the shortcut menu. After the ISM is refreshed, export the event information again.

  1. Select one or more alarms.
  2. Click **Export**.

     The **File Download** dialog box is displayed.

  3. Click **Save**.

     The **Save As** dialog box is displayed.

  4. Select a path for saving the alarm file, enter a name for the file or use the default file name, and click **Save**.

     The selected alarms are exported to the specified local path.

- Export all

  Export all past alarms in a file, helping the administrator to locate and analyze problems.

NOTICE

You can export 20,000 alarms at most each time. If the alarm quantity exceeds 20,000, export them in several times.

1. Click **Export All**.

   The **File Download** dialog box is displayed.

2. Click **Save**.

   The **Save As** dialog box is displayed.

3. Select a path for saving the alarm file, enter a name for the file or use the default file name, and click **Save**.

   All past alarms are exported to the specified local path.

- Search

  Set the conditions to search for the desired alarms. The search method can be basic search or advanced search.

  - When you select **Search**, you can search for alarms by alarm severity.
  - When you select **Advanced Search**, you can search for alarms by alarm severity, confirmation status, alarm source, and alarm occurrence time.

  NOTE

  You can click **Reset** to clear all the specified parameter values.

- View
  - You can click the name of an alarm to view its details.

    1. Click the name of an alarm.

       The page showing details about the alarm is displayed.

    2. View basic information and modification suggestions of the alarm.
    3. (Optional) Click **Create** in the **Maintenance Experiences** area to record the experiences in locating and handling the alarm in the alarm knowledge repository. This enables the alarm to be handled quickly next time the same type of fault occurs.

       You can also modify and delete the created maintenance experiences.

  - You can click the times of an alarm to view the occurrence time, confirmation status and time, clearance status and time, and notification type of the alarm.

    According to the alarm notification type, you can know whether the alarm is a new alarm, manual clear or automatic clear.

----End

6.2.3 Managing Events

Event is a general designation for all the situations occurring on the managed objects. For example, adding, deleting, and modifying an object and changing the status of an object. You can export one or multiple events.

Procedure

Step 1 On the menu bar, choose **Alarms**.

Step 2 In the navigation tree, choose **Alarm Management** > **Events**.

Step 3 You can perform the following operations to manage events

- Export

  This operation exports some important events in a file, helping the administrator to locate and analyze problems.

  1. Select one or more events.
  2. Click **Export**.

     The **File Download** dialog box is displayed.
  3. Click **Save**.

     The **Save As** dialog box is displayed.
  4. Select a path for saving the event file, enter a name for the file or use the default file name, and click **Save**.

     The selected events are exported to the specified local path.

- Export all

  This operation exports all events in a file, helping the administrator to locate and analyze problems.

  NOTICE

  You can export 20,000 alarms at most each time. If the alarm quantity exceeds 20,000, export them in several times.

  1. Click **Export All**.

     The **File Download** dialog box is displayed.
  2. Click **Save**.

     The **Save As** dialog box is displayed.
  3. Select a path for saving the event file, enter a name for the file or use the default file name, and click **Save**.

     All the events are exported to the specified local path.

- Search

  Set the conditions to search for the desired events. The search method can be the basic search or advanced search.

  - When you select **Search**, you can search for events by event source.
  - When you select **Advanced Search**, you can search for events by event source and event occurrence time.

  NOTE

  You can click **Reset** to clear all the specified parameter values.

- View

You can click the name of an event to view its details.

1. Click the name of an event.

   The page showing the details about the event is displayed.

2. View basic information and modification suggestions of the event.

----End

6.2.4 Managing Alarm Filtering

Alarm filtering refers to that users filter out the list of alarms on non-Huawei storage devices. You can set alarm filtering rules.

Procedure

Step 1 On the menu bar, choose **Alarms**.

Step 2 In the navigation tree, choose **Alarm Management** > **Alarm Filtering**.

Step 3 You can perform the following operations to manage alarm filter

- Setting Filter Rules
  1. Click **Setting Filtering Rules**. The **Setting Filtering Rules** dialog box is displayed.
  2. In the **Name**, input the alarm part name of the non-Huawei storage devices.
  3. **Optional:** In the **Description**, input the alarm information of the heterogeneous storage devices.
  4. Click **Add Rule** or  . The **Success** dialog box is displayed. Click **OK**, the alarm filter rule is added.
- Deleting Filter Rules
  1. Click **Setting Filtering Rules**. The **Setting Filtering Rules** dialog box is displayed.
  2. In the **Operation** list, click  . The **Warning** dialog box is displayed. Click **OK**, the **Success** dialog box is displayed, the alarm filter is deleted.

----End

6.3 Synchronizing the Alarms

The management system supports the ability to synchronize NE alarms. The synchronization can be manual or periodic. In other words, you can manually start the alarm synchronization to a specific NE on the client interface, or configure the periodic synchronization policy. When the management system is restarted or its communication with a NE recovers from interruption, the management system actively sends the alarm synchronization command to the NE to synchronize the alarms missed by the management system.

The following are rules for synchronizing alarms:

- If an alarm is cleared on the NE but uncleared on the management system, the management system clears the alarm.
- If an alarm exists on the NE but not on the management system, the management system adds the alarm.

6.3.1 Manual Synchronization

If alarms on an NE and in the management system database are inconsistent due to restarting of the management system server or other reasons, you can manually synchronize the alarms.

Context

Manual synchronization means that users manually start the alarm synchronization on the NMS client interface and the management system updates the alarms in the database according to the alarms on the NE.

Procedure

Step 1 On the menu bar, choose **Alarms**.

Step 2 In the navigation tree, choose **Alarm Synchronization** > **Manual Synchronization**.

Step 3 You can manually start a alarm synchronization or delete a synchronization record. The procedures are as follows:

- Adding a manual alarm synchronization record
  1. Click **Add**.
  2. Select one type of NEs whose alarms need to synchronize from the NE tree on the left. The selected NEs are displayed in the NE list on the right.
  3. Select one or more NEs from the NE list.
  4. Click **OK**.

     Perform the manual alarm synchronization. The management system starts the alarm synchronization immediately. After the NE alarms are synchronized successfully, the number of synchronized alarms is displayed in the manual alarm synchronization list. You can go to **Current Alarms** to view the synchronized alarms.
- Re-synchronizing alarms

  When you find that the NE alarms have not been synchronized to the NMS interface for a long time, you can click **Synchronize** to restart the alarm synchronization. This guarantees that the NE alarms can be reported to the management system interface in time.
- Deleting a manual alarm synchronization record

  When alarms on an NE do not need synchronization, you can select the corresponding alarm synchronization and click **Delete** to delete the synchronization record from the list.
- Searching for a manual alarm synchronization record

  Set the conditions to search for the desired alarm synchronization records. The search method can be basic search or advanced search.
  - When you select **Search**, you can search for alarm synchronization records by NE name.
  - When you select **Advanced Search**, you can search for alarm synchronization records by NE name, NE IP address, start synchronization time, and end synchronization time.

  NOTE

  You can click **Reset** to clear all the specified parameter values.

----End

6.3.2 Automatic Synchronization

After you set the alarm synchronization time, the NMS automatically starts the synchronization of NE alarms from the specified point in time, ensuring that the alarms on the NE and NMS are consistent.

Context

- Automatic synchronization means that the NMS synchronizes the alarm information automatically every cycle and updates the data in the database according to the alarm data reported from the NE.
- The automatic alarm synchronization is for NEs that support alarm synchronization.

Procedure

Step 1 On the menu bar, choose **Alarms**.

Step 2 In the navigation tree, choose **Alarm Synchronization** > **Periodic Synchronization**.

Step 3 You can set a new automatic alarm synchronization, or search for an existing one. The procedures are as follows:

- Setting an automatic alarm synchronization
  1. Click **Periodic Alarm Settings**.
  2. Select **Enable**.
  3. Select a start time for the automatic alarm synchronization from the **Time** drop-down list box.
  4. Input a cycle for the automatic alarm synchronization in the **Interval(hours)**.
  5. Click **OK**.

     NOTE

     After setting an automatic alarm synchronization, NEs will auto display in the automatic synchronization list at the fixed time.
- Searching for an automatic alarm synchronization records

  Set the conditions to search for the desired alarm synchronization records. The search method can be the basic search or advanced search.
  - When you select **Search**, you can search for alarm synchronization records by NE name.
  - When you select **Advanced Search**, you can search for alarm synchronization records by NE name, NE IP address, start synchronization time, and end synchronization time.

  NOTE

  You can click **Reset** to clear all the specified parameter values.

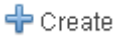
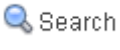
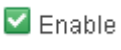
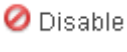
----End

6.4 Masking the Alarms

Masking the alarms means masking the unnecessary or valueless alarms by setting the alarm mask rules. For example, the alarms that are generated during the maintenance and testing period of the NEs are valueless and can be masked. Masking alarms helps mask unnecessary alarms when many NEs are managed.

1. On the menu bar, choose **Alarms**.
2. In the navigation tree, choose **Alarm Mask** > **Mask Rules**.

   You can perform the following operations to manage an alarm masking rule.

Operation	Description
Create	Click  to create an alarm mask rule. For details about this operation, see **6.4.1 Creating a Mask Rule**.
Modify	Click the name of a mask rule to modify its start time, end time, enabling status, and description. For details about this operation, see **6.4.2 Modifying a Mask Rule**.
Search	Enter the full or partial name of an alarm mask rule or resource in the upper right corner of the **Rule Mask** page, and click  to search for the desired alarm mask rules.
Enable	Select one or more alarm mask rules and click  to enable the selected mask rules. After an alarm mask rule is enabled, the alarms occurring on the masked NE specified in the mask rule will not be displayed in the current alarm list but in the masked alarm list.
Disable	Select one or more alarm mask rules and click  to disable the selected mask rules. After an alarm mask rule is disabled, the alarms occurring on the masked NE specified in the mask rule will be displayed in the current alarm list.
Delete	Select one or more alarm mask rules and click  to delete the selected mask rules. **NOTE** Deleting the mask rules cannot be undone. Perform this operation with caution.
View	Click the name of an alarm mask rule. The **Rule Mask Details** page is displayed. You can view or modify information about the rule. For details about this parameter, see **6.4.1 Creating a Mask Rule**.

6.4.1 Creating a Mask Rule

You can set an alarm mask rule according to the maintenance requirements to filter those unimportant NE alarms, facilitating management and improving alarm monitoring efficiency.

Procedure

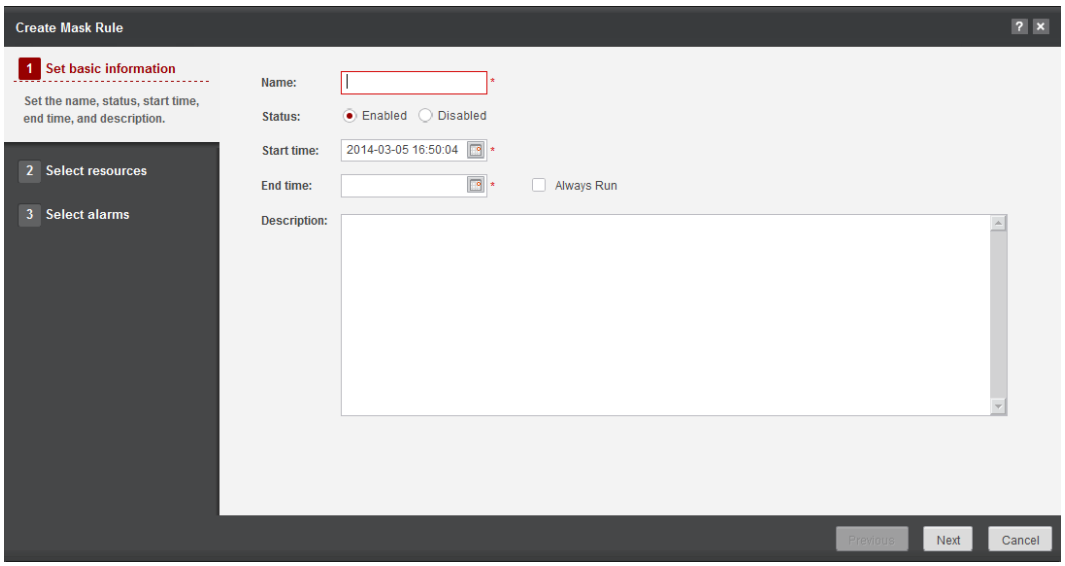
Step 1 On the menu bar, choose **Alarms**.

Step 2 In the navigation tree, choose **Alarm Mask** > **Mask Rules**.

Step 3 Click **Create**.

The **Create Mask Rule** dialog box is displayed.

Figure 6-1 Create Mask Rule



Step 4 Set the alarm masking rule, as described in the following table.

Parameter	Description	Setting
Name	Name of the alarm mask rule. This parameter is required.	The name can contain only 1 to 32 letters, Chinese characters, digits, hyphens (-), or underscores (_) and must begin with a letter, a Chinese character, or underscore (_).
Status	Indicates whether the alarms mask rule is enabled. You can set the parameter to either **Enable** or **Disable**.	Select **Enable** or **Disable**.
Start time	Time when the alarm mask starts to take effect. The start time of the alarm mask cannot be later than the end time.	Click  to select the start time. Click **OK** or double-click the selected time.

Parameter	Description	Setting
End time	Time when the validity of the alarm mask ends. The end time of the alarm mask cannot be earlier than the start time.	Click  to select the end time. Click **OK** or double-click the selected time.
Always Run	Indicates whether the alarms mask rule is always run.	Choose or not choose **Always Run**.
Description	Brief description of the alarm mask rule.	-

Step 5 Click **Next**. Select the type of NE on which the alarm mask rule will be applied from the NE tree on the left, and select one or more NEs from the NE list on the right.

NOTE

Only one NE type can be selected. In the NE list on the right, you can search for the desired NE by NE name or IP address.

Step 6 Click **Next**. Select the alarms to mask.

You can search for the desired alarms by setting the alarm severity level (critical, major, minor, or warning). Then, select the specific alarms to mask. For example, you can set **Warning** for the alarm severity level to search for all the warning alarms on the NE and select those unnecessary alarms to mask.

NOTE

This list includes device model has been selected under all alarms, the device under this model may support different versions of alarms differences.

Step 7 Click **Finish**.

----End

Result

- If the status of the mask rule is set to **Enable**, the management system enables the mask rule immediately when the alarm mask rule is created successfully. Once the alarm that is specified in the mask rule is reported by the masked NE, the alarm will be displayed in the masked alarm list.
- If the status of the alarm mask rule is set to **Disable**, you can choose whether to enable the mask rule according to the NE status after the alarm mask rule is created successfully.

6.4.2 Modifying a Mask Rule

Modifying an alarm mask rule enables you to reset basic information about the alarm mask rule and re-select the alarm NE and alarm information.

Procedure

Step 1 On the menu bar, choose **Alarms**.

Step 2 In the navigation tree, choose **Alarm Mask** > **Mask Rules**.

Step 3 Click the name of an alarm mask rule.

Step 4 Modify basic information about the alarm mask rule.

1. Click 

in the **Basic Information** area.
2. Modify the information except the name.
   For details about how to set the alarm mask rule parameters, see **6.4.1 Creating a Mask Rule**.
3. Click **OK**.

Step 5 (Optional) Select the alarm NE.

You can do as follows to re-select the alarm NE.

- Click 

in the **Resources** area to select the alarm NE.
- Select the NE whose alarms do not need to mask and click 

to delete the selected NE from the resource list.

  You can also enter the full or partial name of a NE and click 

to search for the NEs that you want to delete.

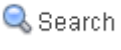
Step 6 (Optional) Select the alarms to mask.

You can do as follows to re-select the alarms to mask.

- Click 

in the **Alarms** area to select the alarms to mask.
- Select the alarms that do not need to mask and click 

to delete the selected alarms from the alarm list.

  You can also select the security from the drop-down box and click 

to search for the alarms that you want to delete.

----End

6.4.3 Managing Masked Alarms

Masking the alarms means masking the unnecessary alarms by setting the alarm mask rules. The management system reserves the masked alarms in the masked alarm list for future use.

Procedure

Step 1 On the menu bar, choose **Alarms**.

Step 2 In the navigation tree, choose **Alarm Mask** > **Masked Alarms**.

Step 3 You can perform the following operations to manage masked alarms

- Export

  This operation exports some important masked alarms in a file, helping the administrator locate and analyze problems.

1. Select one or more masked alarms.
2. Click 

.

   The **File Download** dialog box is displayed.
3. Click **Save**.

   The **Save As** dialog box is displayed.
4. Select a path for saving the alarm file, enter a name for the file or use the default file name, and click **Save**.

   The selected masked alarms are exported to the specified local path.

- Export all

  Export all the masked alarms in a file, helping the administrator locate and analyze problems.

  1. Click 

.

     The **File Download** dialog box is displayed.
  2. Click **Save**.

     The **Save As** dialog box is displayed.
  3. Select a path for saving the alarm file, enter a name for the file or use the default file name, and click **Save**.

     All the masked alarms are exported to the specified local path.

- Search

  Set the conditions to search for the desired masked alarms. The search method can be basic search and advanced search.

  - When you select **Search**, you can search for alarms by alarm severity.
  - When you select **Advanced Search**, you can search for alarms by alarm severity, alarm source, alarm occurrence time, and mask rule name.

  NOTE

  You can click **Reset** to clear all the specified parameter values.

----End

6.5 Alarm Notification

The management system provides remote notification (by email and short message) alarms and client audio alarms to notify maintenance engineers of alarm information of NEs. This ensures real-time efficient handling of alarms.

6.5.1 Managing Remote Notification

The management system provides two remote alarm notification methods (by email or short message). This enables that the maintenance personnel can learn about the NE alarms anytime and anywhere.

1. On the menu bar, choose **Alarms**.
2. In the navigation tree, choose **Alarm Notification** > **Remote Notification**.

Managing remote alarm notification

Operation	Description
Create	Click Create to create the remote alarm notification rule. For details about this operation, see **Creating a Notification Rule**.
Modify	Click the name of a remote notification rule. The page shows details about the remote notification rule. Click Modify on this page to modify the basic information, notification target, resource information, and alarm information about the notification rule. For details about this operation, see **Modifying Remote Alarm Notification**.
Enable	Select one or more remote notification rules that are in the **Disabled** state, and click Enable to enable the selected remote notification rules. After the remote notification rules are enabled, the alarm information will be sent to the specified email address or mobile phone number.
Disable	Select one or more remote notification rules that are in the **Enabled** state, and click Disable to disable the selected remote notification rules. After the remote notification rules are disabled, the alarm information will not be sent to the specified email address or mobile phone number.
Search	Enter the full or partial name of a remote notification rule or resource and click Search. The remote notification rules that meet the search condition will be displayed in the **Remote Notifications**. If no remote notification rule meets the search conditions, the **Remote Notifications** will be empty.
Delete	Select one or more remote notification rule and click Delete to delete the selected remote notification rules. **NOTE** Deleting the notification rules cannot be undone. Perform this operation with caution.
View	Click the name of a remote notification. The **Remote Notifications Details** page is displayed. You can view or modify information about the remote notification. For details about this parameter, see **Creating a Notification Rule**.

Setting Alarm Notification

This section describes how to set the sender of alarm notification. Alarms can be sent by mails or short messages. The default alarm sender is the management system.

Procedure

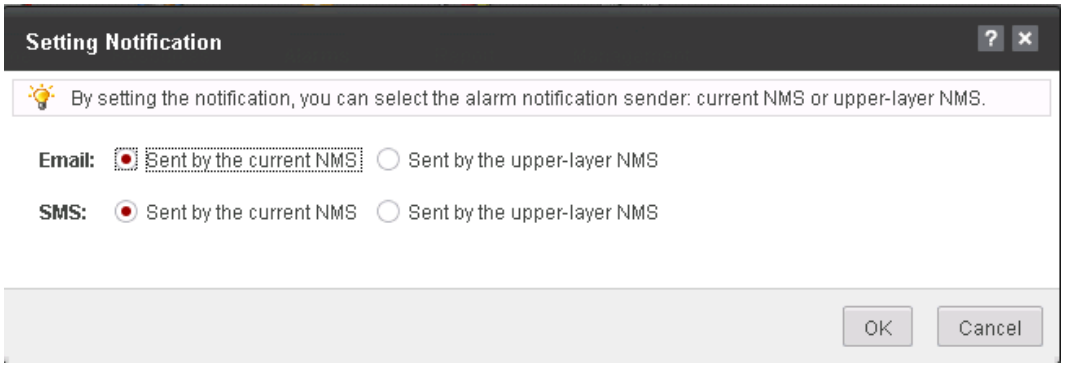
Step 1 On the menu bar, choose **Alarms**.

Step 2 In the navigation tree, choose **Alarm Notification** > **Remote Notification**.

Step 3 Click **Notification Setting**.

The **Notification Setting** dialog box is displayed.

Figure 6-2 Notification Setting dialog box



Step 4 Set the management system that sends alarm notification.

Step 5 Click **OK**.

----End

Creating a Notification Rule

After you create and enable the remote alarm notification, the alarm information will be sent to the maintenance engineer by email or short message. This enables the maintenance engineer to learn about the network status in time.

Context

You can use the configured mail or SMS server to send the alarm information to the specified email address or mobile phone number to learn about the device status in time. For details about how to configure the notification server, see **Setting Alarm Notification**.

Procedure

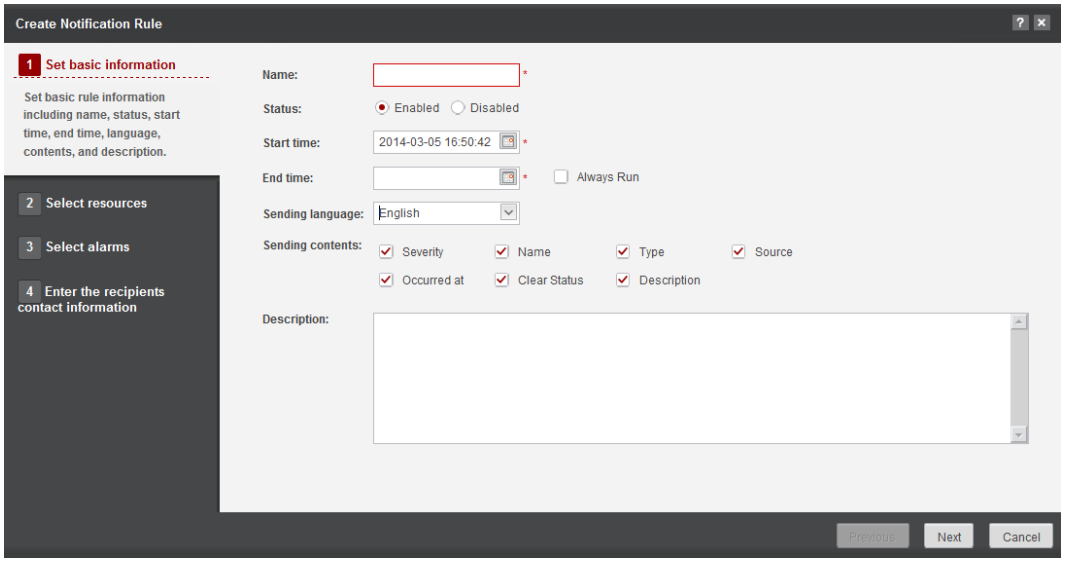
Step 1 On the menu bar, choose **Alarms**.

Step 2 In the navigation tree, choose **Alarms Notification** > **Remote Notification**.

Step 3 Click **Create**.

The **Create Notification Rule** page is displayed.

Figure 6-3 Create Notification Rule page



Step 4 Set the remote alarm notification rule, as described in **Table 6-2**.

Table 6-2 Setting a remote alarm notification rule

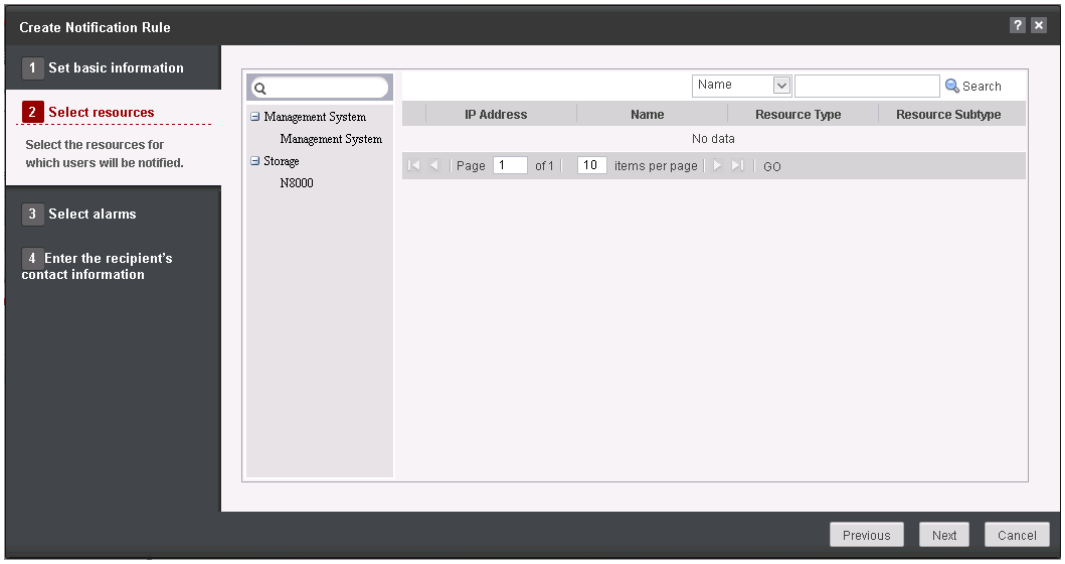
Parameter	Description	Settings
Name	Specifies the name of the remote alarm notification	The name can contain only 1 to 32 letters, digits, and underscores (_) and must start with a letter or underscore.
Status	Indicates whether the remote alarm notification is enabled. When you do not use the remote alarm notification, set this parameter to **Disable**. You can click **Enable** to enable it again later.	You can set the parameter either **Enable** or **Disable**.
Start time	Specifies the time when the remote notification becomes effective. The start time of the remote notification cannot be later than the end time.	Click the icon, select the start time and click **OK** or double-click the time.

Parameter	Description	Settings
End time	Specifies the time when the remote notification becomes invalid. The end time of the remote notification cannot be earlier than the start time.	Click the icon, select the end time and click **OK** or double-click the time.
Always Run	Indicates whether the alarms remote notification rule is always run.	Choose or not choose **Always Run**.
Sending language	Indicates the language of the remote alarm notification.	You can set the parameter to either **Simplified Chinese** or **English**.
Sending contents	Specifies the content of the remote alarm notification.	The sending fields include **Severity**, **Name**, **Type**, **Source**, **Occurred at**, **Clear Status**, and **Description**.
Description	Provides a brief description about the remote alarm notification rule, helping the maintenance engineer learn about the rule without viewing the rule details.	-

Step 5 Click **Next**.

The **Select resources** dialog box is displayed. Select the type of NE on which the remote alarm notification will be applied from the NE tree on the left, and select the NE from the NE list on the right.

Figure 6-4 Select resources dialog box



NOTE

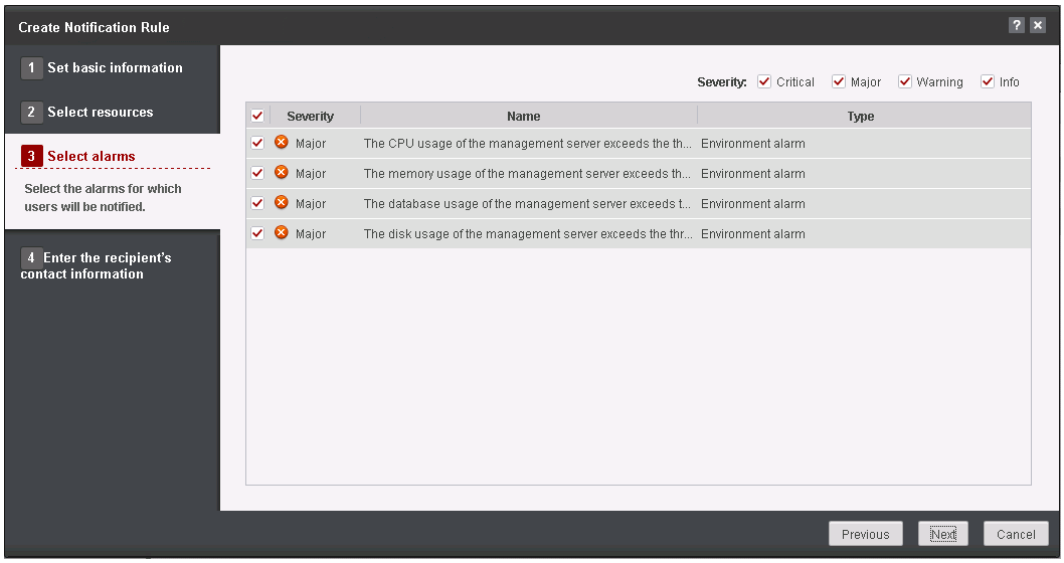
Only one NE type can be selected. In the NE list on the right, you can search for the desired NE by NE name or IP address.

Step 6 Click **Next**.

The **Select alarms** dialog box is displayed. Select the alarm to send for the remote notification.

You can search for the desired alarms by setting the alarm severity (critical, major, minor, or warning). Then, select specific alarms to send. For example, you can set **Critical** for the alarm severity to search for all critical alarms of the NE, and select a specific alarm to send.

Figure 6-5 Select alarms dialog box



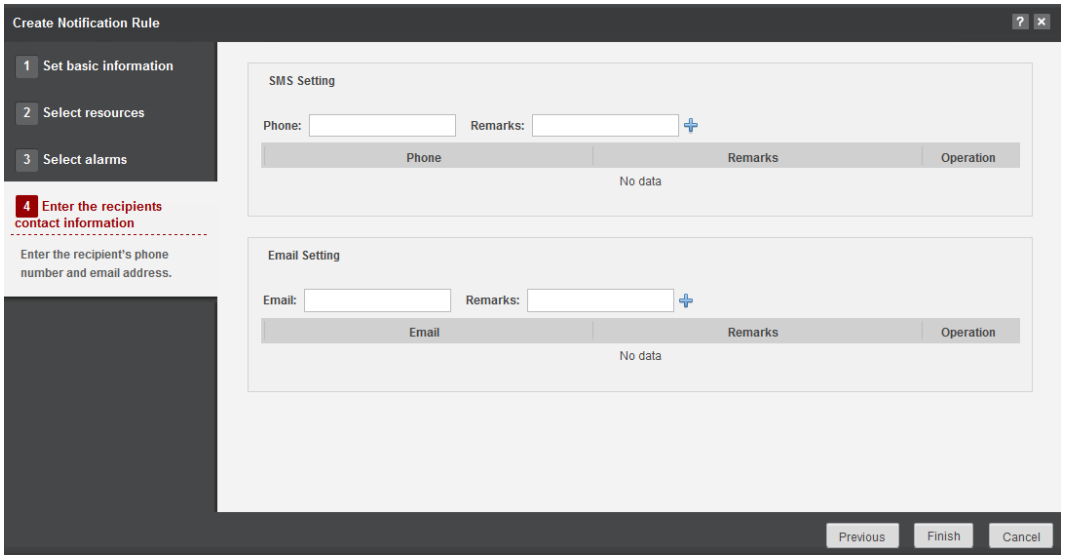
NOTE

This list includes device model has been selected under all alarms, the device under this model may support different versions of alarms differences.

Step 7 Click **Next**.

The **Enter the recipient's contact information** dialog box is displayed. Add the mobile phone number or email address for receiving remote notification messages.

Figure 6-6 Enter the recipient's contact information dialog box



- You can click to add a mobile phone number or email address, or to delete an existing one. You can set relevant information about the mobile phone number or email address to be added.
- Either the mobile phone number or the email address must be specified.
- A maximum of 10 mobile phone numbers or email addresses can be added at a time. The mobile phone number or email address must be unique.

Step 8 Click **Finish**.

The **Success** dialog box is displayed.

----End

Modifying Remote Alarm Notification

This section describes how to modify remote alarm notification, including basic information, alarm sending means, alarm NEs, and alarm information.

Procedure

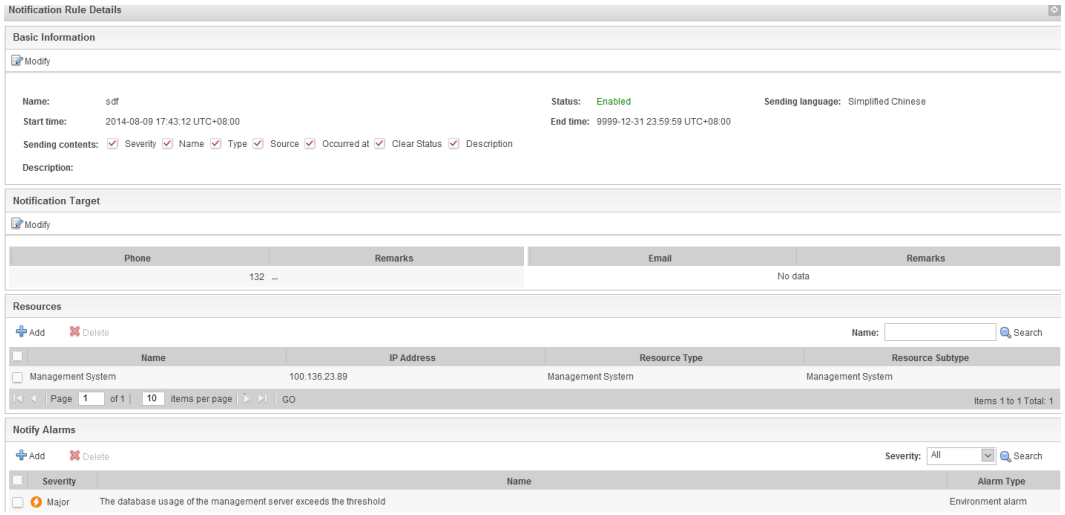
Step 1 On the menu bar, choose **Alarms**.

Step 2 In the navigation tree, choose **Alarm Notification** > **Remote Notification**.

Step 3 Click a remote notification name.

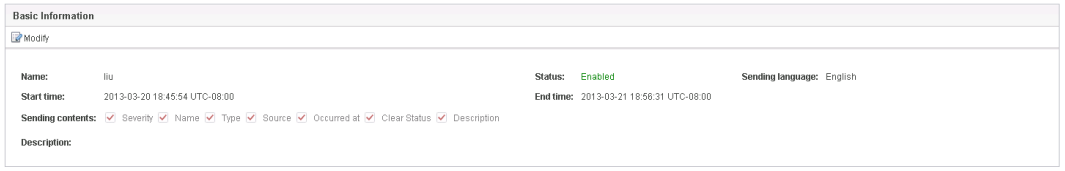
The **Notification Rule Details** page is displayed.

Figure 6-7 Notification Rule Details



Step 4 Modify the basic information about the remote notification.

Figure 6-8 Basic Information



1. Click Modify in the **Basic Information** area.
2. Modify the information except the name.

   For details about how to set the remote notification parameters, see **Creating a Notification Rule**.
3. Click **OK**.

Step 5 (Optional) Modify the notification target.

1. Click Modify in the **Notification Target** area.
2. Add the mobile phone number or email address for receiving the alarm information.
3. Click **OK**.

NOTE

On Windows 2008, click to delete the notification target in the **Modify Notification Target** dialog box in the IE 8.0. When it failed, please select **Internet Options** > **Security** > **Custom level**, and set **Active scripting** to **Enable** in the **Security Settings** dialog box.

Step 6 (Optional) Select the alarm NEs.

You can do as follows to re-select the alarm NEs.

- Click Add in the **Resources** area to select the alarm NEs.
- Select the NEs that do not need the remote alarm notification and click Delete to delete the selected NEs from the resource list.

  You can also enter the full or partial name of a NE and click Search to search for the NEs that you want to delete.

Step 7 (Optional) Select the alarms to send.

You can do as follows to re-select the alarms to send.

- Click Add in the **Alarms** area to select the alarms to send.
- Select the alarms that do not need to send and click Delete to delete the selected alarms from the alarm list.

  You can also select the security from the drop-down box and click Search to search for the alarms that you want to delete.

----End

6.5.2 Configuring the Sound Notification

You can set different sounds for alarms at different levels. When the NMS receives an alarm, the client host sound box plays the audio notification for the highest level and **Uncleared and Unconfirmed** alarms.

Context

- The alarm severity level can be critical, major, minor, or warning. The sound can be a **Minor** or a **Cyclic**.

  If the sound type is set **Minor**, the system plays the audio notification per thirteen seconds for the highest severity and **Uncleared and Unconfirmed** alarms. If the sound type is set **Cyclic**, the system plays cyclic audio notifications for the **Uncleared and Unconfirmed** alarms. It is recommended to set **Cyclic** for critical and major alarms in case that the maintenance personnel is not on site temporarily and cannot hear the alarm sound.
- You can click **Restore Defaults** to set the alarm sound to the default value. The sound notification is enabled for the **Critical** alarms by default.
- There will be no sound notification for the alarms occurring on the masked resources or the confirmed alarms.
- It is not recommended that sound notification be disabled for all severities of alarms. This prevents delayed handling of alarms.

Procedure

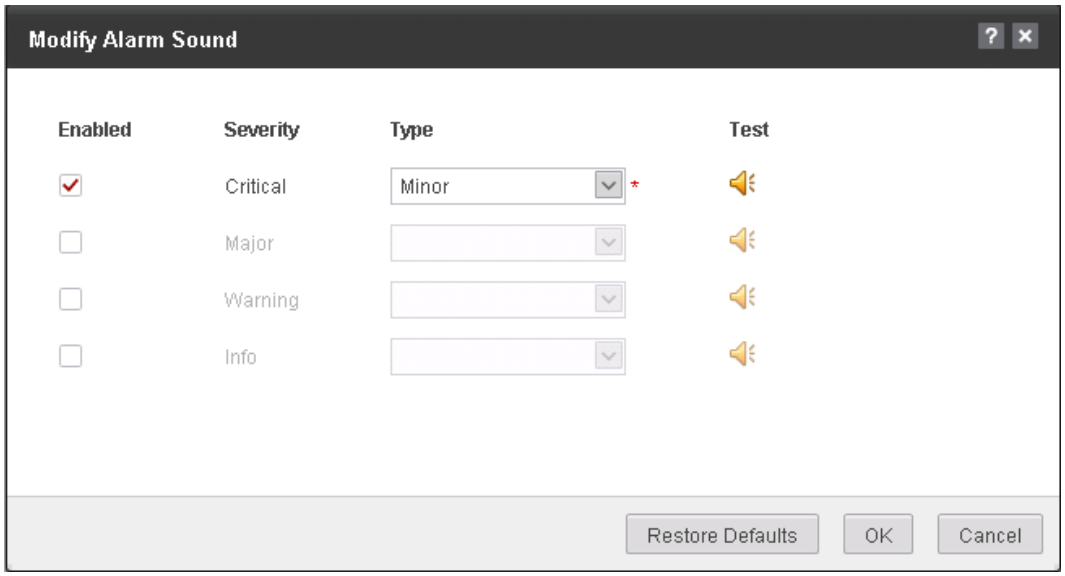
Step 1 On the menu bar, choose **Alarms**.

Step 2 In the navigation tree, choose **Alarm Notification** > **Audible Notification**.

Step 3 Click **Modify**.

The **Modify Alarm Sound** dialog box is displayed.

Figure 6-9 Modify Alarm Sound



Step 4 On the **Modify Alarm Sound** page, select an alarm severity to enable the sound notification function for this alarm severity.

Step 5 Select a sound file in the **Type** drop-down list.

NOTE

You can click  to test the selected sound file.

Step 6 Click **OK**.

NOTE

You can click **Restore Defaults** to set the alarm sound to the default value.

----End

Follow-up Procedure

You can click the mute button at the upper right corner of the management system interface to enable or disable the mute function.

6.6 Threshold Alarms

This section describes how to set thresholds of performance indicators and capacity usage for the device and its components. If the performance or capacity usage exceeds the specified threshold, an alarm occurs.

Procedure

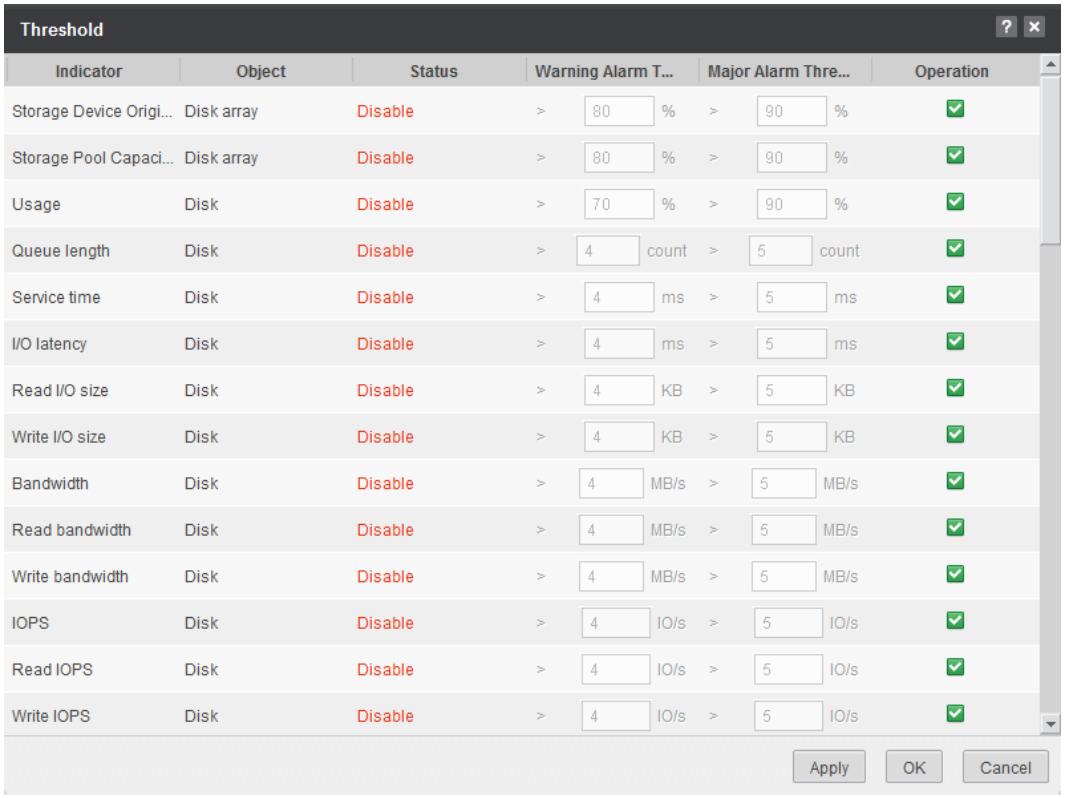
Step 1 On the menu bar, choose **Alarms**.

Step 2 In the navigation tree, choose **Alarm Threshold** > **Alarm Threshold**.

Step 3 In the **Alarm Threshold** area, click next to the device you want to modify.

Step 4 (Optional) Configure the alarm threshold.

Figure 6-10 Threshold



If you do not need to change the threshold, skip the following steps.

Step 5 Set the threshold alarm status.

- You can click to enable the threshold alarm function.
- You can click to disable the threshold alarm function.

Step 6 Click **OK**.

----End

7 Report Management

About This Chapter

Report management includes managing preset report, custom report, report task, and report configuration. You can use a default report template or define your desired report template.

7.1 Preset Report Management

The preset reports provide storage capacity and performance statistics. You can read the preset reports to learn about the device operating status.

7.1.1 Viewing the System Performance Summary

The system performance summary enables you to learn about the performance statistics of disk arrays and unified storage.

Context

- The management system provides the disk array performance statistics collected within the latest 1 hour and 24 hours. The following uses the 1-hour period as an example.
- The management system provides the storage unit performance statistics collected within the latest 1 hour and 24 hours. The following uses the 1-hour period as an example.

Procedure

Step 1 View the disk array performance statistics collected within the latest hour.

1. On the menu bar, choose **Report**.
2. In the navigation tree, choose **Preset Report** > **Disk Arrays Performance** > **Latest Hour**.
3. In the function pane, click the disk array whose performance statistics you want to view.

   A dialog box is displayed detailing the LUN bandwidth, LUN IOPS, LUN I/O latency, and disk array IOPS.

   You can export the performance graph to analyze the operating status of the disk array.

   - Click  to open or save the graph in PDF format.
   - Click  to open or save the graph in EXCEL format.
   - Click  to open or save the graph in HTML format.
4. Click **Close**.

Step 2 View the unified storage performance within the latest hour.

1. On the menu bar, choose **Report**.
2. In the navigation tree, choose **Preset Report** > **Unified Storage Devices Performance** > **Latest Hour**.
3. In the function pane, click the unified storage system whose performance statistics you want to view.

   A dialog box is displayed detailing the LUN bandwidth, LUN IOPS, LUN I/O latency, and unified storage IOPS.

   You can export the performance graph to analyze the operating status of the unified storage.

   - Click  to open or save the graph in PDF format.

- Click to open or save the graph in EXCEL format.
- Click to open or save the graph in HTML format.

4. Click **Close**.

----End

7.1.2 Preset Report of a Disk Array

The preset report of a disk array provides storage capacity and performance statistics of the disk array. You can read the preset report to learn about the operating status of the disk array.

Disk Array Capacity Summary

The disk array capacity summary enables you to learn about the usage statistics of the system capacity, disk capacity, thin pool capacity, storage pool capacity, and LUN capacity.

Prerequisites

At least one storage device exists on the management system.

Context

The management system provides the disk array capacity statistics collected within the latest 30 days.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Disk Arrays Performance**.

Step 3 Under **Disk Arrays Performance**, select the disk array whose capacity statistics you want to view.

Step 4 Under the selected disk array, choose **Capacity Summary** > **Latest 30 Days**.

In the function pane, the disk array capacity statistics collected within the latest 30 days are displayed.

You can export the capacity graph to analyze the capacity usage trend.

- Click to open or save the graph in PDF format.
- Click to open or save the graph in EXCEL format.
- Click to open or save the graph in HTML format.
- Click to open or save the graph in CSV format.

----End

Top 5 Thin LUN Capacity

The thin LUN capacity statistics help you analyze the usage trend of the thin LUN capacity.

Prerequisites

At least one storage device exists on the management system.

Context

The management system provides the thin capacity statistics collected within the latest 24 hours, 7 days, and 30 days. The following uses the 24-hour period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Disk Arrays Performance**.

Step 3 Under **Disk Arrays Performance**, select the disk array whose capacity statistics you want to view.

Step 4 Under the selected disk array, choose **Top 5 Thin LUN Capacity Usage** > **Latest 24 Hours**.

In the function pane, the usage of the thin LUN capacity is displayed.

You can export the capacity graph to analyze the capacity usage trend.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.
- Click  to open or save the graph in CSV format.

NOTE

Opening the detail information web page of the thin LUN when clicked its name.

----End

Top 5 Storage Pool Capacity

The storage pool capacity statistics help you learn about the usage history of the storage pool capacity, and manage the disk array accordingly.

Prerequisites

At least one storage device exists on the management system.

Context

The management system provides the storage pool capacity statistics collected within the latest 7 days and 30 days. The following uses the 7-day period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Disk Arrays Performance**.

Step 3 Under **Disk Arrays Performance**, select the disk array whose capacity statistics you want to view.

Step 4 Under the selected disk array, choose **Top 5 Storage Pool Capacity Usage** > **Latest 7 Days**.

In the function pane, the storage pool capacity usage is displayed.

You can export the capacity graph to analyze the capacity usage trend.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.
- Click  to open or save the graph in CSV format.

NOTE

Opening the detail information web page of the storage pool when clicked its name. And you can view the data distribution status of storage tiers in the **Storage Pool Details**.

----End

Top 5 Thin Pool Capacity

A thin pool uses the thin provisioning technology to enable dynamic and on-demand storage space allocation. The thin pool capacity statistics help you analyze the usage trend of the thin pool capacity and manage the thin pool accordingly.

Prerequisites

At least one storage device exists on the management system.

Context

The management system provides the thin pool capacity statistics collected within the latest 7 days and 30 days. The following uses the 7-day period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Disk Arrays Performance**.

Step 3 Under **Disk Arrays Performance**, select the disk array whose capacity statistics you want to view.

Step 4 Under the selected disk array, choose **Top 5 Thin Pool Capacity Usage** > **Latest 7 Days**.

In the function pane, the usage of the thin pool capacity is displayed.

You can export the capacity graph to analyze the capacity usage trend.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.

- Click  to open or save the graph in CSV format.

----End

Top 5 Disk Performance

The disk performance statistics help you analyze the disk performance trend, and locate and troubleshoot faulty disks accordingly.

Prerequisites

At least one storage device exists on the management system.

Context

The management system provides the disk performance statistics collected within the latest 24 hours, 7 days, and 30 days. The following uses the 24-hour period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Disk Arrays Performance**.

Step 3 Under **Disk Arrays Performance**, select the disk array whose capacity statistics you want to view.

Step 4 Under the selected disk array, choose **Top 5 Disk Performance** > **Latest 24 Hours**.

In the function pane, the disk performance statistics are displayed.

You can export the performance graph to analyze the disk performance trend.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.

----End

Top 5 Storage Pool Performance

The storage pool performance statistics help you learn about the storage pool performance history, and locate and troubleshoot faulty storage pools accordingly.

Prerequisites

At least one storage device exists on the management system.

Context

The management system provides the storage pool performance statistics collected within the latest 24 hours, 7 days, and 30 days. The following uses the 24-hour period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Disk Arrays Performance**.

Step 3 Under **Disk Arrays Performance**, select the disk array whose capacity statistics you want to view.

Step 4 Under the selected disk array, choose **Top 5 Storage Pool Performance** > **Latest 24 Hours**.
In the function pane, the storage pool performance history is displayed.

You can export the performance graph to analyze the storage pool performance trend.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.

----End

Top 5 Host Port Performance

The host port performance statistics help you analyze the host port performance trend, and locate and troubleshoot faulty host ports accordingly.

Prerequisites

At least one storage device exists on the management system.

Context

The management system provides the host port performance statistics collected within the latest 24 hours, 7 days, and 30 days. The following uses the 24-hour period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Disk Arrays Performance**.

Step 3 Under **Disk Arrays Performance**, select the disk array whose capacity statistics you want to view.

Step 4 Under the selected disk array, choose **Top 5 Host Port Performance** > **Latest 24 Hours**.
In the function pane, the host port performance statistics are displayed.

You can export the performance graph to analyze the host port performance trend.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.

----End

Top 5 LUN Performance

A logical unit number (LUN) is a logical disk provided by a controller to application servers for storage. LUNs help application servers make better use of storage resources. The LUN performance statistics help you learn about the LUN performance history and analyze the LUN performance trend.

Viewing the LUN performance includes the following operations:

Cache

The LUN cache performance statistics help you learn about the read and write cache hit ratios of each LUN, and monitor LUNs' operating status accordingly.

Prerequisites

- At least one storage device exists on the management system.
- At least one LUN exists on the management system and is running correctly.

Context

The management system provides the LUN cache performance statistics collected within the latest 24 hours, 7 days, and 30 days. The following uses the 24-hour period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Disk Arrays Performance**.

Step 3 Under **Disk Arrays Performance**, select the disk array whose capacity statistics you want to view.

Step 4 Under the selected disk array, choose **Top 5 LUN Performance** > **Cache in Latest 24 Hours**.

- In the function pane, the read and write cache hit ratios are displayed.
- In the function pane, the LUN parameters are displayed, as described in the following table:

Parameter	Description	Value
Name	Name of the LUN.	[Example] LUN001
Max.Read Cache Hit Ratio (%)	Maximum read cache hit ratio of the LUN.	[Example] 100
Min.Read Cache Hit Ratio (%)	Minimum read cache hit ratio of the LUN.	[Example] 40
Max.Write Cache Hit Ratio (%)	Maximum write cache hit ratio of the LUN.	[Example] 100

Parameter	Description	Value
Min.Write Cache Hit Ratio (%)	Minimum write cache hit ratio of the LUN.	[Example] 40
Owning Disk Array	Owning disk array of the LUN.	[Example] array001

You can export the LUN cache performance graph to analyze the read/write cache hit ratio trend.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.
- Click  to open or save the graph in CSV format.

----End

Bandwidth

LUN bandwidth is the rate of the links between storage devices. The LUN bandwidth statistics help you learn about the bandwidth for each LUN, and monitor the service status of each LUN accordingly.

Prerequisites

- At least one storage device exists on the management system.
- At least one LUN exists on the management system and is running correctly.

Context

The management system provides the LUN bandwidth statistics collected within the latest 24 hours, 7 days, and 30 days. The following uses the 24-hour period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Disk Arrays Performance**.

Step 3 Under **Disk Arrays Performance**, select the disk array whose capacity statistics you want to view.

Step 4 Under the selected disk array, choose **Top 5 LUN Performance** > **Bandwidth in Latest 24 Hours**.

- In the function pane, the LUN bandwidth graph is displayed.
- In the function pane, the LUN parameters are displayed, as described in the following table:

Parameter	Description	Value
Name	Name of the LUN.	[Example] LUN001
Max.Bandwidth (MB/s)	Maximum bandwidth for the LUN.	[Example] 2
Min.Bandwidth (MB/s)	Minimum bandwidth for the LUN.	[Example] 0
Owning Disk Array	Owning disk array of the LUN.	[Example] array001

NOTE

In the function pane, click the desired LUN. The management system displays the performance information about the objects related to this LUN.

You can export the performance graph to analyze the bandwidth trend of the LUN.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.
- Click  to open or save the graph in CSV format.

----End

IOPS

Input/Output operations per second (IOPS) measures the random read/write performance. The LUN IOPS statistics help you learn about the speeds of reading data from and writing data to each LUN.

Prerequisites

- At least one storage device exists on the management system.
- At least one LUN exists on the management system and is running correctly.

Context

The management system provides the LUN IOPS statistics collected within the latest 24 hours, 7 days, and 30 days. The following uses the 24-hour period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Disk Arrays Performance**.

Step 3 Under **Disk Arrays Performance**, select the disk array whose capacity statistics you want to view.

Step 4 Under the selected disk array, choose **Top 5 LUN Performance** > **IOPS in Latest 24 Hours**.

- In the function pane, the LUN IOPS graph is displayed.
- In the function pane, the LUN parameters are displayed, as described in the following table:

Parameter	Description	Value
Name	Name of the LUN.	[Example] LUN001
Max.IOPS	Maximum IOPS of the LUN.	[Example] 100
Min.IOPS	Minimum IOPS of the LUN.	[Example] 1
Owning Disk Array	Owning disk array of the LUN.	[Example] array001

NOTE

In the function pane, click the desired LUN. The management system displays the performance information about the objects related to this LUN.

You can export the IOPS graph to analyze the IOPS trend of the LUN.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.
- Click  to open or save the graph in CSV format.

----End

I/O Latency

The I/O latency statistics help you analyze the I/O latency trend of a LUN.

Prerequisites

- At least one storage device exists on the management system.
- At least one LUN exists on the management system and is running correctly.

Context

The management system provides the I/O latency statistics collected within the latest 24 hours, 7 days, and 30 days. The following uses the 24-hour period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Disk Arrays Performance**.

Step 3 Under **Disk Arrays Performance**, select the disk array whose capacity statistics you want to view.

Step 4 Under the selected disk array, choose **Top 5 LUN Performance** > **I/O Latency in Latest 24 Hours**.

- In the function pane, the LUN I/O latency graph is displayed.
- In the function pane, the LUN parameters are displayed, as described in the following table:

Parameter	Description	Value
LUN Name	Name of the LUN.	[Example] LUN001
Max.I/O Latency (ms)	Maximum I/O latency of the LUN.	[Example] 50
Min.I/O Latency (ms)	Minimum I/O latency of the LUN.	[Example] 0
Owning Disk Array	Owning disk array of the LUN.	[Example] array001

NOTE

In the function pane, click the desired LUN. The management system displays the performance information about the objects related to this LUN.

You can export the I/O latency graph to analyze the I/O latency trend of the LUN.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.
- Click  to open or save the graph in CSV format.

----End

Top 5 Controller Performance

Controllers are the core components of a controller enclosure. The controller performance (cache usage and CPU usage) statistics help you learn about controllers' operating status.

Context

The management system provides the controller performance statistics collected within the latest 24 hours, 7 days, and 30 days. The following uses the 24-hour period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Disk Arrays Performance**.

Step 3 Under **Disk Arrays Performance**, select the disk array whose capacity statistics you want to view.

Step 4 Under the selected disk array, choose **Top 5 Controller Performance** > **Latest 24 Hours**.

In the function pane, the cache usage and the CPU usage are displayed.

You can export the cache and CPU usage graphs to analyze the controller performance.

- Click  to open or save the graphs in PDF format.
- Click  to open or save the graphs in EXCEL format.
- Click  to open or save the graphs in HTML format.

----End

7.1.3 Preset Report of a Heterogeneous Array

The preset report of a heterogeneous array provides storage capacity and performance statistics of the disk array. You can read the preset report to learn about the operating status of the heterogeneous array.

Top 5 Disk Performance

The disk performance statistics help you analyze the disk performance trend, and locate and troubleshoot faulty disks accordingly.

Prerequisites

At least one storage device exists on the management system.

Context

The management system provides the disk performance statistics collected within the latest 24 hours, 7 days, and 30 days. The following uses the 24-hour period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Disk Arrays Performance**.

Step 3 Under **Disk Arrays Performance**, select the heterogeneous array whose capacity statistics you want to view.

Step 4 Under the selected heterogeneous array, choose **Top 5 Disk Performance** > **Latest 24 Hours**.

In the function pane, the disk performance statistics are displayed.

You can export the performance graph to analyze the disk performance trend.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.

----End

Top 5 Host Port Performance

The host port performance statistics help you analyze the host port performance trend, and locate and troubleshoot faulty host ports accordingly.

Prerequisites

At least one storage device exists on the management system.

Context

The management system provides the host port performance statistics collected within the latest 24 hours, 7 days, and 30 days. The following uses the 24-hour period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Disk Arrays Performance**.

Step 3 Under **Disk Arrays Performance**, select the heterogeneous array whose capacity statistics you want to view.

Step 4 Under the selected heterogeneous array, choose **Top 5 Host Port Performance** > **Latest 24 Hours**.

In the function pane, the host port performance statistics are displayed.

You can export the performance graph to analyze the host port performance trend.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.

----End

Top 5 LUN Performance

A logical unit number (LUN) is a logical disk provided by a controller to application servers for storage. LUNs help application servers make better use of storage resources. The LUN performance statistics help you learn about the LUN performance history and analyze the LUN performance trend.

Viewing the LUN performance includes the following operations:

Cache

The LUN cache performance statistics help you learn about the read and write cache hit ratios of each LUN, and monitor LUNs' operating status accordingly.

Prerequisites

- At least one storage device exists on the management system.
- At least one LUN exists on the management system and is running correctly.

Context

The management system provides the LUN cache performance statistics collected within the latest 24 hours, 7 days, and 30 days. The following uses the 24-hour period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Disk Arrays Performance**.

Step 3 Under **Disk Arrays Performance**, select the heterogeneous array whose capacity statistics you want to view.

Step 4 Under the selected heterogeneous array, choose **Top 5 LUN Performance** > **Cache in Latest 24 Hours**.

- In the function pane, the read and write cache hit ratios are displayed.
- In the function pane, the LUN parameters are displayed, as described in the following table:

Parameter	Description	Value
Name	Name of the LUN.	[Example] LUN001
Max.Read Cache Hit Ratio (%)	Maximum read cache hit ratio of the LUN.	[Example] 100
Min.Read Cache Hit Ratio (%)	Minimum read cache hit ratio of the LUN.	[Example] 40
Max.Write Cache Hit Ratio (%)	Maximum write cache hit ratio of the LUN.	[Example] 100
Min.Write Cache Hit Ratio (%)	Minimum write cache hit ratio of the LUN.	[Example] 40
Owning Disk Array	Owning disk array of the LUN.	[Example] array001

You can export the LUN cache performance graph to analyze the read/write cache hit ratio trend.

- Click  to open or save the graph in PDF format.

- Click to open or save the graph in EXCEL format.
- Click to open or save the graph in HTML format.
- Click to open or save the graph in CSV format.

----End

Bandwidth

LUN bandwidth is the rate of the links between storage devices. The LUN bandwidth statistics help you learn about the bandwidth for each LUN, and monitor the service status of each LUN accordingly.

Prerequisites

- At least one storage device exists on the management system.
- At least one LUN exists on the management system and is running correctly.

Context

The management system provides the LUN bandwidth statistics collected within the latest 24 hours, 7 days, and 30 days. The following uses the 24-hour period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Disk Arrays Performance**.

Step 3 Under **Disk Arrays Performance**, select the heterogeneous array whose capacity statistics you want to view.

Step 4 Under the selected heterogeneous array, choose **Top 5 LUN Performance** > **Bandwidth in Latest 24 Hours**.

- In the function pane, the LUN bandwidth graph is displayed.
- In the function pane, the LUN parameters are displayed, as described in the following table:

Parameter	Description	Value
Name	Name of the LUN.	[Example] LUN001
Max.Bandwidth (MB/s)	Maximum bandwidth for the LUN.	[Example] 2
Min.Bandwidth (MB/s)	Minimum bandwidth for the LUN.	[Example] 0
Owning Disk Array	Owning disk array of the LUN.	[Example] array001

NOTE

In the function pane, click the desired LUN. The management system displays the performance information about the objects related to this LUN.

You can export the performance graph to analyze the bandwidth trend of the LUN.

- Click to open or save the graph in PDF format.
- Click to open or save the graph in EXCEL format.
- Click to open or save the graph in HTML format.
- Click to open or save the graph in CSV format.

----End

IOPS

Input/Output operations per second (IOPS) measures the random read/write performance. The LUN IOPS statistics help you learn about the speeds of reading data from and writing data to each LUN.

Prerequisites

- At least one storage device exists on the management system.
- At least one LUN exists on the management system and is running correctly.

Context

The management system provides the LUN IOPS statistics collected within the latest 24 hours, 7 days, and 30 days. The following uses the 24-hour period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Disk Arrays Performance**.

Step 3 Under **Disk Arrays Performance**, select the heterogeneous array whose capacity statistics you want to view.

Step 4 Under the selected heterogeneous array, choose **Top 5 LUN Performance** > **IOPS in Latest 24 Hours**.

- In the function pane, the LUN IOPS graph is displayed.
- In the function pane, the LUN parameters are displayed, as described in the following table:

Parameter	Description	Value
Name	Name of the LUN.	[Example] LUN001
Max.IOPS	Maximum IOPS of the LUN.	[Example] 100

Parameter	Description	Value
Min.IOPS	Minimum IOPS of the LUN.	[Example] 1
Owning Disk Array	Owning disk array of the LUN.	[Example] array001

NOTE

In the function pane, click the desired LUN. The management system displays the performance information about the objects related to this LUN.

You can export the IOPS graph to analyze the IOPS trend of the LUN.

- Click to open or save the graph in PDF format.
- Click to open or save the graph in EXCEL format.
- Click to open or save the graph in HTML format.
- Click to open or save the graph in CSV format.

----End

Top 5 Controller Performance

Controllers are the core components of a controller enclosure. The controller performance (cache usage and CPU usage) statistics help you learn about controllers' operating status.

Context

The management system provides the controller performance statistics collected within the latest 24 hours, 7 days, and 30 days. The following uses the 24-hour period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Disk Arrays Performance**.

Step 3 Under **Disk Arrays Performance**, select the heterogeneous array whose capacity statistics you want to view.

Step 4 Under the selected heterogeneous array, choose **Top 5 Controller Performance** > **Latest 24 Hours**.

In the function pane, the cache usage and the CPU usage are displayed.

You can export the cache and CPU usage graphs to analyze the controller performance.

- Click to open or save the graphs in PDF format.
- Click to open or save the graphs in EXCEL format.

- Click  to open or save the graphs in HTML format.

----End

7.1.4 Preset Report of a Unified Storage System

The preset report of a unified storage system provides storage capacity and performance statistics of the unified storage system. You can read the preset report to learn about the operating status of the unified storage system.

Storage Unit Capacity Summary

The storage unit capacity summary helps you learn about the usage history of the system capacity, disk capacity, thin pool capacity, storage pool capacity, and LUN capacity.

Prerequisites

At least one storage device exists on the management system.

Context

The management system provides the storage unit capacity statistics collected within the latest 30 days.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Unified Storage Devices Performance**.

Step 3 Under **Unified Storage Devices Performance**, select a storage unit.

Step 4 Under the selected storage unit, choose **Capacity Summary** > **Latest 30 Days**.

In the function pane, the storage unit capacity statistics collected within the latest 30 days are displayed.

You can export the capacity graph to analyze the capacity usage trend.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.
- Click  to open or save the graph in CSV format.

----End

Top 5 Thin LUN Capacity

The thin LUN capacity statistics help you analyze the usage trend of the thin LUN capacity and manage the disk array accordingly.

Prerequisites

At least one storage device exists on the management system.

Context

The management system provides the thin capacity statistics collected within the latest 24 hours, 7 days, and 30 days. The following uses the 24-hour period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Unified Storage Devices Performance**.

Step 3 Under **Unified Storage Devices Performance**, select a unified storage system.

Step 4 Under the selected unified storage system, choose **Top 5 Thin LUN Capacity Usage** > **Latest 24 Hours**.

In the function pane, the usage of the thin LUN capacity is displayed.

You can export the capacity graph to analyze the capacity usage trend.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.
- Click  to open or save the graph in CSV format.

----End

Top 5 Thin Pool Capacity

A thin pool uses the thin provisioning technology to enable dynamic and on-demand storage space allocation. The thin pool capacity statistics help you analyze the usage trend of the thin pool capacity and manage the thin pool accordingly.

Prerequisites

At least one storage device exists on the management system.

Context

The management system provides the thin pool capacity statistics collected within the latest 7 days and 30 days. The following uses the 7-day period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Unified Storage Devices Performance**.

Step 3 Under **Unified Storage Devices Performance**, select a unified storage system.

Step 4 Under the selected unified storage system, choose **Top 5 Thin Pool Capacity Usage** > **Latest 7 Days**.

In the function pane, the usage of the thin pool capacity is displayed.

You can export the capacity graph to analyze the capacity usage trend.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.
- Click  to open or save the graph in CSV format.

----End

Top 5 Disk Performance

The disk performance statistics help you analyze the disk performance trend, and locate and troubleshoot faulty disks accordingly.

Prerequisites

At least one storage device exists on the management system.

Context

The management system provides the disk performance statistics collected within the latest 24 hours, 7 days, and 30 days. The following uses the 24-hour period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Unified Storage Devices Performance**.

Step 3 Under **Unified Storage Devices Performance**, select a unified storage system.

Step 4 Under the selected unified storage system, choose **Top 5 Disk Performance** > **Latest 24 Hours**.

In the function pane, the disk performance statistics are displayed.

You can export the performance graph to analyze the disk performance trend.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.

----End

Top 5 Host Port Performance

The host port performance statistics help you learn about the host port performance statistics, and locate and troubleshoot faulty host ports accordingly.

Prerequisites

At least one storage device exists on the management system.

Context

The management system provides the disk performance statistics collected within the latest 24 hours, 7 days, and 30 days. The following uses the 24-hour period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Unified Storage Devices Performance**.

Step 3 Under **Unified Storage Devices Performance**, select a unified storage system.

Step 4 Under the selected unified storage system, choose **Top 5 Host Port Performance** > **Latest 24 Hours**.

In the function pane, the host port performance statistics are displayed.

You can export the performance graph to analyze the host port performance trend.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.

----End

Top 5 LUN Performance

A logical unit number (LUN) is a logical disk provided by a controller to application servers for storage. LUNs help application servers make better use of storage resources. The LUN performance statistics help you learn about the LUN performance history and analyze the LUN performance trend.

Viewing the LUN performance includes the following operations:

Cache

The LUN cache performance statistics help you learn about the read and write cache hit ratios of each LUN, and monitor the LUNs' operating status accordingly.

Prerequisites

- At least one storage device exists on the management system.
- At least one LUN exists on the management system and is running correctly.

Context

The management system provides the LUN cache performance statistics collected within the latest 24 hours, 7 days, and 30 days. The following uses the 24-hour period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Unified Storage Devices Performance**.

Step 3 Under **Unified Storage Devices Performance**, select a unified storage system.

Step 4 Under the selected disk array, choose **Top 5 LUN Performance** > **Cache in Latest 24 Hours**.

- In the function pane, the read and write cache hit ratios are displayed.
- In the function pane, the LUN parameters are displayed, as described in the following table:

Parameter	Description	Value
Name	Name of the LUN.	[Example] LUN001
Max.Read Cache Hit Ratio (%)	Maximum read cache hit ratio of the LUN.	[Example] 100
Min.Read Cache Hit Ratio (%)	Minimum read cache hit ratio of the LUN.	[Example] 40
Max.Write Cache Hit Ratio (%)	Maximum write cache hit ratio of the LUN.	[Example] 100
Min.Write Cache Hit Ratio (%)	Minimum write cache hit ratio of the LUN.	[Example] 40
Owning Storage Unit	Owning storage unit of the LUN.	[Example] array001

You can export the LUN cache performance graph to analyze the read/write cache hit ratio trend.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.
- Click  to open or save the graph in CSV format.

----End

Bandwidth

LUN bandwidth is the rate of the links between storage devices. The LUN bandwidth statistics help you learn about the bandwidth for each LUN, and monitor the service status of each LUN accordingly.

Prerequisites

- At least one storage device exists on the management system.

- At least one LUN exists on the management system and is running correctly.

Context

The management system provides the LUN bandwidth statistics collected within the latest 24 hours, 7 days, and 30 days. The following uses the 24-hour period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Unified Storage Devices Performance**.

Step 3 Under **Unified Storage Devices Performance**, select a unified storage system.

Step 4 Under the selected disk array, choose **Top 5 LUN Performance** > **Bandwidth in Latest 24 Hours**.

- In the function pane, the LUN bandwidth graph is displayed.
- In the function pane, the LUN parameters are displayed, as described in the following table:

Parameter	Description	Value
Name	Name of the LUN.	[Example] LUN001
Max.Bandwidth (MB/s)	Maximum bandwidth for the LUN.	[Example] 2
Min.Bandwidth (MB/s)	Minimum bandwidth for the LUN.	[Example] 0
Owning Storage Unit	Owning storage unit of the LUN.	[Example] array001

NOTE

In the function pane, click the desired LUN. The management system displays the performance information about the objects related to this LUN.

You can export the performance graph to analyze the bandwidth trend of the LUN.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.
- Click  to open or save the graph in CSV format.

----End

IOPS

Input/output operations per second (IOPS) measures the random read/write performance. The LUN IOPS statistics help you learn about the speeds of reading data from and writing data to each LUN.

Prerequisites

- At least one storage device exists on the management system.
- At least one LUN exists on the management system and is running correctly.

Context

The management system provides the LUN IOPS statistics collected within the latest 24 hours, 7 days, and 30 days. The following uses the 24-hour period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Unified Storage Devices Performance**.

Step 3 Under **Unified Storage Devices Performance**, select a unified storage system.

Step 4 Under the selected disk array, choose **Top 5 LUN Performance** > **IOPS in Latest 24 Hours**.

- In the function pane, the LUN IOPS graph is displayed.
- In the function pane, the LUN parameters are displayed, as described in the following table:

Parameter	Description	Value
Name	Name of the LUN.	[Example] LUN001
Max.IOPS	Maximum IOPS of the LUN.	[Example] 100
Min.IOPS	Minimum IOPS of the LUN.	[Example] 1
Owning Storage Unit	Owning storage unit of the LUN.	[Example] array001

NOTE

In the function pane, click the desired LUN. The management system displays the performance information about the objects related to this LUN.

You can export the IOPS graph to analyze the IOPS trend of the LUN.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.

- Click to open or save the graph in HTML format.
- Click to open or save the graph in CSV format.

----End

I/O Latency

The I/O latency statistics help you analyze the I/O latency trend of a LUN.

Prerequisites

- At least one storage device exists on the management system.
- At least one LUN exists on the management system and is running correctly.

Context

The management system provides the I/O latency statistics collected within the latest 24 hours, 7 days, and 30 days. The following uses the 24-hour period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Unified Storage Devices Performance**.

Step 3 Under **Unified Storage Devices Performance**, select a unified storage system.

Step 4 Under the selected disk array, choose **Top 5 LUN Performance** > **I/O Latency in Latest 24 Hours**.

- In the function pane, the LUN I/O latency graph is displayed.
- In the function pane, the LUN parameters are displayed, as described in the following table:

Parameter	Description	Value
LUN Name	Name of the LUN.	[Example] LUN001
Max.I/O Latency (ms)	Maximum I/O latency of the LUN.	[Example] 50
Min.I/O Latency (ms)	Minimum I/O latency of the LUN.	[Example] 0
Owning Storage Unit	Owning storage unit of the LUN.	[Example] array001

NOTE

In the function pane, click the desired LUN. The management system displays the performance information about the objects related to this LUN.

You can export the I/O latency graph to analyze the I/O latency trend of the LUN.

- Click to open or save the graph in PDF format.
- Click to open or save the graph in EXCEL format.
- Click to open or save the graph in HTML format.
- Click to open or save the graph in CSV format.

----End

Top 5 Controller Performance

Controllers are the core components of a controller enclosure. The controller performance (cache usage and CPU usage) statistics help you learn about controllers' operating status.

Context

The management system provides the controller performance statistics collected within the latest 24 hours, 7 days, and 30 days. The following uses the 24-hour period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Unified Storage Devices Performance**.

Step 3 Under **Unified Storage Devices Performance**, select a unified storage system.

Step 4 Under the selected unified storage system, choose **Top 5 Controller Performance** > **Latest 24 Hours**.

In the function pane, the cache usage and the CPU usage are displayed.

You can export the cache and CPU usage graphs to analyze the controller performance.

- Click to open or save the graph in PDF format.
- Click to open or save the graph in EXCEL format.
- Click to open or save the graph in HTML format.

----End

Top 5 Service Port Performance

The service port performance data include the number of outgoing packets, the number of incoming packets, read traffic volume, and write traffic volume. The service port performance data helps to locate a fault on the unified storage system.

Context

The management system provides the service port performance statistics collected within the latest 24 hours, 7 days, and 30 days. The following uses the 24-hour period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Unified Storage Devices Performance**.

Step 3 Under **Unified Storage Devices Performance**, select a unified storage system.

Step 4 Under the selected unified storage system, choose **Top 5 Service Port Performance** > **Latest 24 Hours**.

In the function pane, the service port performance statistics are displayed.

You can export the service port performance graph to analyze the operating status of the service ports.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.

----End

Top 5 CPU Performance of a File Engine Node

This section describes how to view the CPU usage of a file engine node.

Context

The management system provides the CPU usage statistics collected within the latest 24 hours, 7 days, and 30 days. The following uses the 24-hour period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Unified Storage Devices Performance**.

Step 3 Under **Unified Storage Devices Performance**, select a unified storage system.

Step 4 Under the selected unified storage system, choose **Top 5 File Engine Node CPU Performance** > **Latest 24 Hours**.

In the function pane, the CPU usage is displayed.

You can export the CPU usage graph to analyze the CPU performance of the file engine node.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.

----End

Top 5 File Engine Node Performance

The file engine performance data include the number of outgoing packets, the number of incoming packets, read traffic volume, and write traffic volume. The file engine performance data helps to locate a fault on the unified storage system.

Context

The management system provides the file engine node performance statistics collected within the latest 24 hours, 7 days, and 30 days. The following uses the 24-hour period as an example.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Unified Storage Devices Performance**.

Step 3 Under **Unified Storage Devices Performance**, select a unified storage system.

Step 4 Under the selected unified storage system, choose **Top 5 File Engine Node Performance** > **Latest 24 Hours**.

In the function pane, the file engine node performance statistics are displayed.

You can export the performance graph to analyze the file engine performance.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.

----End

Top 5 File Storage Pool Capacity

The file storage pool capacity statistics enable you to learn about the usage history of the file storage pool capacity.

Context

The management system provides the file storage pool capacity statistics collected within the latest 30 days.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Unified Storage Devices Performance**.

Step 3 Under **Unified Storage Devices Performance**, select a unified storage system.

Step 4 Under the selected unified storage system, choose **Top 5 File Storage Pool Capacity Usage** > **Latest 30 Days**.

In the function pane, the file storage pool capacity graph is displayed.

You can export the capacity graph to analyze the file storage pool usage.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.
- Click  to open or save the graph in CSV format.

----End

Top 5 Data Disk Capacity

The data disk capacity statistics enable you to learn about the usage history of data disk capacity.

Context

The management system provides the data disk capacity statistics collected within the latest 30 days.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Unified Storage Devices Performance**.

Step 3 Under **Unified Storage Devices Performance**, select a unified storage system.

Step 4 Under the selected unified storage system, choose **Top 5 Data Disk Capacity Usage** > **Latest 30 Days**.

In the function pane, the data disk capacity graph is displayed.

You can export the capacity graph to analyze the data disk capacity usage.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.
- Click  to open or save the graph in CSV format.

----End

Top 5 Shared File System Capacity

The protocols Common Internet File System (CIFS) and Network File System (NFS) can enable file sharing across the unified storage systems that run different operating systems. You can view the shared file system capacity to learn about how files are shared on a unified storage system.

Context

The management system provides the usage of the shared file system capacity within the latest 30 days.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Unified Storage Devices Performance**.

Step 3 Under **Unified Storage Devices Performance**, select a unified storage system.

Step 4 Under the selected unified storage system, choose **Top 5 Shared File System Capacity Usage** > **Latest 30 Days**.

In the function pane, the usage of NFS shared capacity and the usage of CIFS shared capacity are displayed.

You can export the usage graphs to analyze the usage of shared file system capacity.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.
- Click  to open or save the graph in CSV format.

----End

Top 5 File System Capacity

You can view the file system capacity of a unified storage system to analyze the capacity usage of the entire file system.

Context

The management system provides the file system capacity statistics collected within the latest 30 days.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Preset Report** > **Unified Storage Devices Performance**.

Step 3 Under **Unified Storage Devices Performance**, select a unified storage system.

Step 4 Under the selected unified storage system, choose **Top 5 File System Capacity Usage** > **Latest 30 Days**.

In the function pane, the file system capacity usage is displayed.

You can export the capacity usage graph to analyze the usage of the file system capacity on a unified storage system.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.

- Click  to open or save the graph in CSV format.

----End

7.2 Custom Report Management

You can set filter criteria for viewing specific capacity and performance reports.

Custom report involve the following operations:

7.2.1 Viewing a User-defined Disk Array Report

You can set filter criteria for viewing specific disk array capacity and performance reports.

Viewing a user-defined disk array report includes the following operations:

Storage Device Performance Summary

You can set filter criteria for viewing the performance summary of a specific storage device. Then you can learn about the operating status of the storage device accordingly.

Prerequisites

At least one storage device exists on the management system.

Procedure

Step 1 Go to the disk array or storage unit performance summary page by either of the following methods:

- Method 1: viewing the disk array performance summary
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Disk Arrays**.
  3. In the function pane, choose **Disk array performance summary** from the **Report name** list.
- Method 2: viewing the storage unit performance summary
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Unified Storage**.
  3. In the function pane, choose **Storage unit performance summary** from the **Report name** list.

Step 2 Set a time range.

If you set **Time range** to **Custom**, specify the start time and end time.

Step 3 Click **Search**.

In the list on the lower part of the function pane, the storage device performance statistics are displayed.

You can export the storage device performance summary graph to analyze the performance trend.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.

----End

Controller Performance

You can set filter criteria for viewing the performance statistics of a specific controller. Then you can learn about the operating status of the controller accordingly.

Prerequisites

At least one storage device exists on the management system.

Procedure

Step 1 Go to the controller performance page by either of the following methods:

- Method 1: viewing the performance of the controllers on a disk array
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Disk Arrays**.
  3. In the function pane, choose **Controller performance** from the **Report name** list.
- Method 2: viewing the performance of the controllers on a unified storage system
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Unified Storage**.
  3. In the function pane, choose **Controller performance** from the **Report name** list.

Step 2 Set a report that you desire. The following table describes the related parameters.

Parameter	Description	Value
Report view	Type of the report view, **Tendency** or **Comparison**.	[Example] Tendency

Parameter	Description	Value
Object	● If the statistical object is **Select object** 1. In the **Object** list, select the objects whose statistics you want to view. 2. In **Controllers**, select controllers and click  to add them to **Selected Controllers**. In **Selected Controllers**, select controllers and click  to relocate them to **Controllers**. **NOTE** You can also click  to add all controllers to **Selected Controllers**, or click  to relocate all of them to **Controllers**. ● If the statistical object is **Select device** In **Devices**, select devices and click  to add them to **Selected Devices**. In **Selected Devices**, select devices and click  to relocate them to **Devices**. **NOTE** You can also click  to add all devices to **Selected Devices**, or click  to relocate all of them to **Devices**.	[Example] S5000T_10_11-A
Key performance indicators	Key performance indicators (KPIs) of the user-defined report.	[Example] Usage
Granularity	Granularity of the user-defined report.	[Example] High

Parameter	Description	Value
Time range	Time range for collecting performance statistics. **NOTE** If you set **Time range** to **Custom**, specify the start time and end time.	[Example] Latest 1 week
Format	Method for collecting performance statistics.	[Example] Average

Parameter	Description	Value
Sort	Method for sorting the user-defined report. ● If you set **Sort** to **Default**, the custom report sorts all objects by each preset key performance indicator respectively. For example, if you set **Key performance indicators** to **Usage** and **IOPS** and **Sort** to **Default**, the custom report displays all object information sorted by **Usage** and **IOPS** respectively in two results. ● If you set **Sort** to a key performance indicator, the custom report displays key performance indicators about all objects sorted by the specified key performance indicator. For example, if you set **Key performance indicators** to **Usage** and **IOPS** and **Sort** to **Usage**, the custom report displays **Usage** and **IOPS** information about all objects sorted by **Usage** respectively. ● If **TOP** is set to n ($1 \leqslant n \leqslant 10$), the self-defined report displays a maximum of n statistics objects. – If you select **Maximum** or **Average** for **Format**, the top n indicator values are displayed. – If you select **Minimum** for	[Example]

Parameter	Description	Value
	Format, the smallest n indicator values are displayed.	Default

Step 3 Click **Search**.

In the function pane, the preset KPI graph is displayed.

You can export the KPI graph to analyze the controller performance.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.

----End

Host Port Performance

You can set filter criteria for viewing the performance statistics of a specific host port. Then you can learn about the overall host port performance accordingly.

Prerequisites

At least one storage device exists on the management system.

Procedure

Step 1 Go to the host port performance page by either of the following methods:

- Method 1: viewing the performance of the host ports on a disk array
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Disk Arrays**.
  3. In the function pane, choose **Host port performance** from the **Report name** list.
- Method 2: viewing the performance of the host ports on a unified storage system
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Unified Storage**.
  3. In the function pane, choose **Front-end host port performance** from the **Report name** list.

Step 2 Set a report that you desire. The following table describes the related parameters.

Parameter	Description	Value
Report view	Type of the report view, **Tendency** or **Comparison**.	[Example] Tendency

Parameter	Description	Value
Object	● If the statistical object is **Select object** 1. In the **Object** list, select the host ports whose statistics you want to view. 2. In **Ports**, select host ports and click  to add them to **Selected Ports**. In **Selected Ports**, select host ports and click  to relocate them to **Ports**. **NOTE** You can also click  to add all host ports to **Selected Ports**, or click  to relocate all of them to **Ports**. ● If the statistical object is **Select device** In **Devices**, select devices and click  to add them to **Selected Devices**. In **Selected Devices**, select devices and click  to relocate them to **Devices**. **NOTE** You can also click  to add all devices to **Selected Devices**. or click  to relocate all of them to **Devices**.	[Example] S5000T_10_11-A
Key performance indicators	Key performance indicators (KPIs) of the user-defined report.	[Example] Usage
Granularity	Granularity of the user-defined report.	[Example] High

Parameter	Description	Value
Time range	Time range for collecting performance statistics. **NOTE** If you set **Time range** to **Custom**, specify the start time and end time.	[Example] Latest 1 week
Format	Method for collecting performance statistics.	[Example] Average

Parameter	Description	Value
Sort	Method for sorting the user-defined report. ● If you set **Sort** to **Default**, the custom report sorts all objects by each preset key performance indicator respectively. For example, if you set **Key performance indicators** to **Usage** and **IOPS** and **Sort** to **Default**, the custom report displays all object information sorted by **Usage** and **IOPS** respectively in two results. ● If you set **Sort** to a key performance indicator, the custom report displays key performance indicators about all objects sorted by the specified key performance indicator. For example, if you set **Key performance indicators** to **Usage** and **IOPS** and **Sort** to **Usage**, the custom report displays **Usage** and **IOPS** information about all objects sorted by **Usage** respectively. ● If **TOP** is set to n ($1 \leqslant n \leqslant 10$), the self-defined report displays a maximum of n statistics objects. – If you select **Maximum** or **Average** for **Format**, the top n indicator values are displayed. – If you select **Minimum** for	[Example]

Parameter	Description	Value
	Format, the smallest n indicator values are displayed.	Default

Step 3 Click **Search**.

In the function pane, the preset KPI graph is displayed.

You can export the KPI graph to analyze the host port performance.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.

----End

Disk Performance

You can set filter criteria for viewing the performance statistics of a specific disk. Then you can learn about the overall disk performance, and locate and troubleshoot faulty disks accordingly.

Prerequisites

At least one storage device exists on the management system.

Procedure

Step 1 Go to the disk performance page by either of the following methods:

- Method 1: viewing the performance of the hard disks on a disk array
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Disk Arrays**.
  3. In the function pane, choose **Disk performance** from the **Report name** list.
- Method 2: viewing the performance of the hard disks on a unified storage system
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Unified Storage**.
  3. In the function pane, choose **Disk performance** from the **Report name** list.

Step 2 Set a report that you desire. The following table describes the related parameters.

Parameter	Description	Value
Report view	Type of the report view, **Tendency** or **Comparison**.	[Example] Tendency

Parameter	Description	Value
Object	● If the statistical object is **Select object** 1. In the **Object** list, select the hard disks whose statistics you want to view. 2. In **Disks**, select hard disks and click  to add them to **Selected Disks**. In **Selected Devices**, select hard disks and click  to relocate them to **Disks**. **NOTE** You can also click  to add all hard disks to **Selected Disks**, or click  to relocate all of them to **Disks**. ● If the statistical object is **Select device** In **Devices**, select devices and click  to add them to **Selected Devices**. In **Selected Devices**, select devices and click  to relocate them to **Devices**. **NOTE** You can also click  to add all devices to **Selected Devices**. or click  to relocate all of them to **Devices**.	[Example] S5000T_10_11-A
Key performance indicators	Key performance indicators (KPIs) of the user-defined report.	[Example] Usage
Granularity	Granularity of the user-defined report.	[Example] High

Parameter	Description	Value
Time range	Time range for collecting performance statistics. **NOTE** If you set **Time range** to **Custom**, specify the start time and end time.	[Example] Latest 1 week
Format	Method for collecting performance statistics.	[Example] Average

Parameter	Description	Value
Sort	Method for sorting the user-defined report. ● If you set **Sort** to **Default**, the custom report sorts all objects by each preset key performance indicator respectively. For example, if you set **Key performance indicators** to **Usage** and **IOPS** and **Sort** to **Default**, the custom report displays all object information sorted by **Usage** and **IOPS** respectively in two results. ● If you set **Sort** to a key performance indicator, the custom report displays key performance indicators about all objects sorted by the specified key performance indicator. For example, if you set **Key performance indicators** to **Usage** and **IOPS** and **Sort** to **Usage**, the custom report displays **Usage** and **IOPS** information about all objects sorted by **Usage** respectively. ● If **TOP** is set to n ($1 \leqslant n \leqslant 10$), the self-defined report displays a maximum of n statistics objects. – If you select **Maximum** or **Average** for **Format**, the top n indicator values are displayed. – If you select **Minimum** for	[Example]

Parameter	Description	Value
	Format, the smallest n indicator values are displayed.	Default

Step 3 Click **Search**.

In the function pane, the preset KPI graph is displayed.

You can export the KPI graph to analyze the disk performance.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.

----End

Storage Pool Performance

You can set filter criteria for viewing the performance statistics of a specific storage pool.

Prerequisites

At least one storage device exists on the management system.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Custom Report** > **Disk Arrays**.

Step 3 In the function pane, choose **Storage pool performance** from the **Report name** list.

Step 4 Set a report that you desire. The following table describes the related parameters.

Parameter	Description	Value
Report view	Type of the report view, **Tendency** or **Comparison**.	[Example] Tendency

Parameter	Description	Value
Object	● If the statistical object is **Select object** 1. In the **Object** list, select the object whose statistics you want to view. 2. In **Storage Pools**, select storage pools and click  to add them to **Selected Storage Pools**. In **Selected Storage Pools**, select storage pools and click  to relocate them to **Storage Pools**. **NOTE** You can also click  to add all storage pools to **Selected Storage Pools**, or click  to relocate all of them to **Storage Pools**. ● If the statistical object is **Select device** In **Devices**, select devices and click  to add them to **Selected Devices**. In **Selected Devices**, select devices and click  to relocate them to **Devices**. **NOTE** You can also click  to add all devices to **Selected Devices**, or click  to relocate all of them to **Devices**.	[Example] S5000T_10_11-A
Key performance indicators	Key performance indicators (KPIs) of the user-defined report.	[Example] Usage
Granularity	Granularity of the user-defined report.	[Example] High

Parameter	Description	Value
Time range	Time range for collecting performance statistics. **NOTE** If you set **Time range** to **Custom**, specify the start time and end time.	[Example] Latest 1 week
Format	Method for collecting performance statistics.	[Example] Average

Parameter	Description	Value
Sort	Method for sorting the user-defined report. ● If you set **Sort** to **Default**, the custom report sorts all objects by each preset key performance indicator respectively. For example, if you set **Key performance indicators** to **Usage** and **IOPS** and **Sort** to **Default**, the custom report displays all object information sorted by **Usage** and **IOPS** respectively in two results. ● If you set **Sort** to a key performance indicator, the custom report displays key performance indicators about all objects sorted by the specified key performance indicator. For example, if you set **Key performance indicators** to **Usage** and **IOPS** and **Sort** to **Usage**, the custom report displays **Usage** and **IOPS** information about all objects sorted by **Usage** respectively. ● If **TOP** is set to n ($1 \leqslant n \leqslant 10$), the self-defined report displays a maximum of n statistics objects. – If you select **Maximum** or **Average** for **Format**, the top n indicator values are displayed. – If you select **Minimum** for	[Example]

Parameter	Description	Value
	Format, the smallest n indicator values are displayed.	Default

Step 5 Click **Search**.

In the function pane, the preset KPI graph is displayed.

You can export the KPI graph to analyze the storage pool performance.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.

----End

LUN Performance

A logical unit number (LUN) is a logical disk provided by a controller to application servers for storage. LUNs help application servers make better use of storage resources. You can set filter criteria for viewing the performance statistics of a specific LUN.

Prerequisites

At least one storage device exists on the management system.

Procedure

Step 1 Go to the LUN performance page by either of the following methods:

- Method 1: viewing the performance of the LUNs on a disk array
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Disk Arrays**.
  3. In the function pane, choose **LUN performance** from the **Report name** list.
- Method 2: viewing the performance of the LUNs on a unified storage device
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Unified Storage**.
  3. In the function pane, choose **LUN performance** from the **Report name** list.

Step 2 Set a report that you desire. The following table describes the related parameters.

Parameter	Description	Value
Report view	Type of the report view, **Tendency** or **Comparison**.	[Example] Tendency

Parameter	Description	Value
Object	● If the statistical object is **Select object** 1. In the **Object** list, select the LUNs whose statistics you want to view. 2. In **LUNs**, select LUNs and click  to add them to **Selected LUNs**. In **Selected LUNs**, select LUNs and click  to relocate them to **LUNs**. **NOTE** You can also click  to add all LUNs to **Selected LUNs**, or click  to relocate all of them to **LUNs**. ● If the statistical object is **Select device** In **Devices**, select devices and click  to add them to **Selected Devices**. In **Selected Devices**, select devices and click  to relocate them to **Devices**. **NOTE** You can also click  to add all devices to **Selected Devices**. or click  to relocate all of them to **Devices**.	[Example] S5000T_10_11-A
Key performance indicators	Key performance indicators (KPIs) of the user-defined report.	[Example] Usage
Granularity	Granularity of the user-defined report.	[Example] High

Parameter	Description	Value
Time range	Time range for collecting performance statistics. **NOTE** If you set **Time range** to **Custom**, specify the start time and end time.	[Example] Latest 1 week
Format	Method for collecting performance statistics.	[Example] Average

Parameter	Description	Value
Sort	Method for sorting the user-defined report. ● If you set **Sort** to **Default**, the custom report sorts all objects by each preset key performance indicator respectively. For example, if you set **Key performance indicators** to **Usage** and **IOPS** and **Sort** to **Default**, the custom report displays all object information sorted by **Usage** and **IOPS** respectively in two results. ● If you set **Sort** to a key performance indicator, the custom report displays key performance indicators about all objects sorted by the specified key performance indicator. For example, if you set **Key performance indicators** to **Usage** and **IOPS** and **Sort** to **Usage**, the custom report displays **Usage** and **IOPS** information about all objects sorted by **Usage** respectively. ● If **TOP** is set to n ($1 \leqslant n \leqslant 10$), the self-defined report displays a maximum of n statistics objects. – If you select **Maximum** or **Average** for **Format**, the top n indicator values are displayed. – If you select **Minimum** for	[Example]

Parameter	Description	Value
	Format, the smallest n indicator values are displayed.	Default

Step 3 Click **Search**.

In the function pane, the preset KPI graph is displayed.

You can export the KPI graph to analyze the LUN performance.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.

----End

Storage Device Capacity Summary

You can set filter criteria for viewing the capacity summary of a specific storage device.

Prerequisites

At least one storage device exists on the management system.

Procedure

Step 1 Go to the disk array or storage unit capacity summary page by either of the following methods:

- Method 1: viewing the disk array capacity summary
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Disk Arrays**.
  3. In the function pane, choose **Disk array capacity summary** from the **Report name** list.
- Method 2: viewing the storage unit capacity summary
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Unified Storage**.
  3. In the function pane, choose **Storage unit capacity summary** from the **Report name** list.

Step 2 Set a report that you desire. The following table describes the related parameters.

Parameter	Description	Value
Object	1. In the **Object** list, select the objects whose statistics you want to view. **NOTE** You can group multiple storage devices and collect the capacity statistics of this group. 2. In **Disk Arrays**/**Available Storage Unit**/**Resource Groups Available for Selection**, select the objects whose statistics you want to view. Click  to add the selected objects to **Selected Disk Arrays**/**Selected Storage Unit**/**Selected Resource Groups**. In **Selected Disk Arrays**/**Selected Storage Unit**/**Selected Resource Groups**, select objects and click  to relocate them to **Disk Arrays**/**Available Storage Unit**/**Resource Groups Available for Selection**. **NOTE** You can also click  to add all objects to **Selected Disk Arrays**/**Selected Storage Unit**/**Selected Resource Groups**, or click  to relocate all of them to **Disk Arrays**/**Available Storage Unit**/**Resource Groups Available for Selection**.	[Example] S5600T_205_206
Time range	Time range for collecting capacity statistics. **NOTE** If you set **Time range** to **Custom**, specify the start time and end time.	[Example] Latest 1 week

Step 3 Click **Search**.

In the function pane, the preset capacity graph is displayed.

You can export the capacity graph to analyze the storage capacity usage.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.
- Click  to open or save the graph in CSV format.

----End

Storage Device Capacity

You can set filter criteria for viewing the capacity usage of a specific storage device.

Prerequisites

At least one storage device exists on the management system.

Procedure

Step 1 Go to the disk array or storage unit capacity usage page by either of the following methods:

- Method 1: viewing the disk array capacity usage
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Disk Arrays**.
  3. In the function pane, choose **Disk array capacity** from the **Report name** list.
- Method 2: viewing the storage unit capacity usage
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Unified Storage**.
  3. In the function pane, choose **Storage unit capacity** from the **Report name** list.

Step 2 Set a report that you desire. The following table describes the related parameters.

Parameter	Description	Value
Object	1. In the **Object** list, select the objects whose statistics you want to view. **NOTE** You can group multiple disk arrays and collect the capacity statistics of this group. 2. In **Disk Arrays**/**Available Storage Unit**/**Resource Groups Available for Selection**, select the objects whose capacity statistics you want to view. Click  to add the selected objects to **Selected Disk Arrays**/**Selected Storage Unit**/**Selected Resource Groups**. In **Selected Disk Arrays**/**Selected Storage Unit**/**Selected Resource Groups**, select objects. Then click  to relocate them to **Disk Arrays**/**Available Storage Unit**/**Resource Groups Available for Selection**. **NOTE** You can also click  to add all objects to **Selected Disk Arrays**/**Selected Storage Units**/**Selected Resource Groups**, or click  to relocate all of them to **Disk Arrays**/**Available Storage Unit**/**Resource Groups Available for Selection**.	[Example] S5600T_205_206
Sort	Method for sorting the user-defined report. **NOTE** If **TOP** is set to n ($1 \leqslant n \leqslant 10$), the self-defined report displays a maximum of n statistics objects.	[Example] 5

Parameter	Description	Value
Time range	Time range for collecting capacity statistics. **NOTE** If you set **Time range** to **Custom**, specify the start time and end time.	[Example] Latest 1 week

Step 3 Click **Search**.

In the function pane, the preset capacity graph is displayed.

You can export the capacity graph to analyze the storage capacity usage.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.
- Click  to open or save the graph in CSV format.

----End

Storage Pool Capacity

You can set filter criteria for viewing the capacity statistics of a specific storage pool.

Prerequisites

At least one storage device exists on the management system.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Custom Report** > **Disk Arrays**.

Step 3 In the function pane, choose **Storage pool capacity** from the **Report name** list.

Step 4 Set a report that you desire. The following table describes the related parameters.

Parameter	Description	Value
Object	1. In the **Object** list, select the objects whose statistics you want to view. **NOTE** You can group multiple disk arrays and collect the capacity statistics of this group. 2. In **Disk Arrays/ Resource Groups Available for Selection**, select the objects whose capacity statistics you want to view. Click  to add the selected objects to **Selected Disk Arrays/ Selected Resource Groups**. In **Selected Disk Arrays/Selected Resource Groups**, select objects. Then click  to add the selected objects to **Disk Arrays/Resource Groups Available for Selection**. **NOTE** You can also click  to add all objects to **Selected Disk Arrays/Selected Resource Groups**, or click  to relocate all of them to **Disk Arrays/Resource Groups Available for Selection**.	[Example] Array_201A
Sort	Method for sorting the user-defined report. **NOTE** If **TOP** is set to n ($1 \leqslant n \leqslant 10$), the self-defined report displays a maximum of n statistics objects.	[Example] 5
Time range	Time range for collecting capacity statistics. **NOTE** If you set **Time range** to **Custom**, specify the start time and end time.	[Example] Latest 1 week

Step 5 Click **Search**.

In the function pane, the preset storage pool capacity graph is displayed.

You can export the capacity graph to analyze the storage pool capacity usage.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.
- Click  to open or save the graph in CSV format.

NOTE

Opening the detail information web page of the storage pool when clicked its name. And you can view the data distribution status of storage tiers in the **Storage Pool Details**.

----End

Thin LUN Capacity

A thin logical unit number (LUN) is a logical storage unit created in a thin pool. It is a logical disk accessible to hosts, and allocates storage space to users based on the actual capacity demand. You can set filter criteria for viewing the capacity statistics of a specific thin LUN.

Prerequisites

At least one storage device exists on the management system.

Procedure

Step 1 Go to the thin LUN capacity page by either of the following methods:

- Method 1: viewing the statistics of a thin LUN on a disk array
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Disk Arrays**.
  3. In the function pane, choose **Thin LUN capacity** from the **Report name** list.
- Method 2: viewing the statistics of a thin LUN on a unified storage system
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Unified Storage**.
  3. In the function pane, choose **Thin LUN capacity** from the **Report name** list.

Step 2 Set a report that you desire. The following table describes the related parameters.

Parameter	Description	Value
Object	1. In the **Object** list, select the objects whose statistics you want to view. **NOTE** You can group multiple disk arrays and collect the capacity statistics of this group. 2. In **Disk Arrays**/**Available Storage Unit**/**Resource Groups Available for Selection**, select the objects whose capacity statistics you want to view. Click  to add the selected objects to **Selected Disk Arrays**/**Selected Storage Unit**/**Selected Resource Groups**. In **Selected Disk Arrays**/**Selected Storage Unit**/**Selected Resource Groups**, select objects. Then click  to relocate the selected objects to **Disk Arrays**/**Available Storage Unit**/**Resource Groups Available for Selection**. **NOTE** You can also click  to add all objects to **Selected Disk Arrays**/**Selected Storage Unit**/**Selected Resource Groups**, or click  to relocate all of them to **Disk Arrays**/**Available Storage Unit**/**Resource Groups Available for Selection**.	[Example] Array_201A
Sort	Method for sorting the user-defined report. **NOTE** If **TOP** is set to n ($1 \leqslant n \leqslant 10$), the self-defined report displays a maximum of n statistics objects.	[Example] 5

Parameter	Description	Value
Time range	Time range for collecting capacity statistics. **NOTE** If you set **Time range** to **Custom**, specify the start time and end time.	[Example] Latest 1 week

Step 3 Click **Search**.

In the function pane, the preset thin LUN capacity graph is displayed.

You can export the capacity graph to analyze the thin LUN capacity usage.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.
- Click  to open or save the graph in CSV format.

----End

Thin Pool Capacity

A thin pool uses the thin provisioning technology to enable dynamic and on-demand storage space allocation. You can set filter criteria for viewing the capacity statistics of a specific thin pool.

Prerequisites

At least one storage device exists on the management system.

Procedure

Step 1 Go to the thin pool capacity page by either of the following methods:

- Method 1: viewing the statistics of a thin pool on a disk array
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Disk Arrays**.
  3. In the function pane, choose **Thin pool capacity** from the **Report name** list.
- Method 2: viewing the statistics of a thin pool on a unified storage system
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Unified Storage**.
  3. In the function pane, choose **Thin pool capacity** from the **Report name** list.

Step 2 Set a report that you desire. The following table describes the related parameters.

Parameter	Description	Value
Object	1. In the **Object** list, select the objects whose statistics you want to view. 2. In **Disk Arrays/ Available Storage Unit**, select the objects whose capacity statistics you want to view. Click  to add the selected objects to **Selected Disk Arrays/ Selected Storage Unit**. In **Selected Disk Arrays/ Selected Storage Unit**, select objects. Then click  to relocate them to **Disk Arrays/Available Storage Unit**. **NOTE** You can also click  to add all objects to **Selected Disk Arrays/Selected Storage Unit**, or click  to relocate all of them to **Disk Arrays/Available Storage Unit**.	[Example] Array_201A
Sort	Method for sorting the user-defined report. **NOTE** If **TOP** is set to n (1 ⩽ n ⩽ 10), the custom report displays a maximum of n statistics objects.	[Example] 5
Time range	Time range for collecting thin pool capacity statistics. **NOTE** If you set **Time range** to **Custom**, specify the start time and end time.	[Example] Latest 1 week

Step 3 Click **Search**.

In the function pane, the preset thin pool capacity graph is displayed.

You can export the capacity graph to analyze the thin pool capacity usage.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.

- Click  to open or save the graph in HTML format.
- Click  to open or save the graph in CSV format.

----End

7.2.2 Viewing a User-defined Report for Unified Storage

You can set filter criteria for viewing the performance reports for a specific unified storage system.

Viewing a user-defined report for unified storage includes the following operations:

Storage Unit Performance Summary

You can set filter criteria for viewing the performance summary of a specific storage unit. Then you can learn about the running status of the storage unit accordingly.

Prerequisites

At least one storage device exists on the management system.

Procedure

Step 1 Go to the disk array or storage unit performance summary page by either of the following methods:

- Method 1: viewing the disk array performance summary
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Disk Arrays**.
  3. In the function pane, choose **Disk array performance summary** from the **Report name** list.
- Method 2: viewing the storage unit performance summary
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Unified Storage**.
  3. In the function pane, choose **Storage unit performance summary** from the **Report name** list.

Step 2 Set a time range.

If you set **Time range** to **Custom**, specify the start time and end time.

Step 3 Click **Search**.

In the list on the lower part of the function pane, the storage device performance statistics are displayed.

You can export the storage device performance summary graph to analyze the performance trend.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.

- Click  to open or save the graph in HTML format.

----End

Controller Performance

You can set filter criteria for viewing the performance statistics of a specific controller. Then you can learn about the running status of the controller accordingly.

Prerequisites

At least one storage device exists on the management system.

Procedure

Step 1 Go to the controller performance page by either of the following methods:

- Method 1: viewing the performance of the controllers on a disk array
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Disk Arrays**.
  3. In the function pane, choose **Controller performance** from the **Report name** list.
- Method 2: viewing the performance of the controllers on a unified storage system
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Unified Storage**.
  3. In the function pane, choose **Controller performance** from the **Report name** list.

Step 2 Set a report that you desire. The following table describes the related parameters.

Parameter	Description	Value
Report view	Type of the report view, **Tendency** or **Comparison**.	[Example] Tendency

Parameter	Description	Value
Object	● If the statistical object is **Select object** 1. In the **Object** list, select the objects whose statistics you want to view. 2. In **Controllers**, select controllers and click  to add them to **Selected Controllers**. In **Selected Controllers**, select controllers and click  to relocate them to **Controllers**. **NOTE** You can also click  to add all controllers to **Selected Controllers**, or click to relocate all of them to **Controllers**. ● If the statistical object is **Select device** In **Devices**, select devices and click  to add them to **Selected Devices**. In **Selected Devices**, select devices and click  to relocate them to **Devices**. **NOTE** You can also click  to add all devices to **Selected Devices**, or click  to relocate all of them to **Devices**.	[Example] S5000T_10_11-A
Key performance indicators	Key performance indicators (KPIs) of the user-defined report.	[Example] Usage
Granularity	Granularity of the user-defined report.	[Example] High

Parameter	Description	Value
Time range	Time range for collecting performance statistics. **NOTE** If you set **Time range** to **Custom**, specify the start time and end time.	[Example] Latest 1 week
Format	Method for collecting performance statistics.	[Example] Average

Parameter	Description	Value
Sort	Method for sorting the user-defined report. ● If you set **Sort** to **Default**, the custom report sorts all objects by each preset key performance indicator respectively. For example, if you set **Key performance indicators** to **Usage** and **IOPS** and **Sort** to **Default**, the custom report displays all object information sorted by **Usage** and **IOPS** respectively in two results. ● If you set **Sort** to a key performance indicator, the custom report displays key performance indicators about all objects sorted by the specified key performance indicator. For example, if you set **Key performance indicators** to **Usage** and **IOPS** and **Sort** to **Usage**, the custom report displays **Usage** and **IOPS** information about all objects sorted by **Usage** respectively. ● If **TOP** is set to n ($1 \leqslant n \leqslant 10$), the self-defined report displays a maximum of n statistics objects. – If you select **Maximum** or **Average** for **Format**, the top n indicator values are displayed. – If you select **Minimum** for	[Example]

Parameter	Description	Value
	Format, the smallest n indicator values are displayed.	Default

Step 3 Click **Search**.

In the function pane, the preset KPI graph is displayed.

You can export the KPI graph to analyze the controller performance.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.

----End

Host Port Performance

You can set filter criteria for viewing the performance statistics of a specific host port. Then you can learn about the overall host port performance accordingly.

Prerequisites

At least one storage device exists on the management system.

Procedure

Step 1 Go to the host port performance page by either of the following methods:

- Method 1: viewing the performance of the host ports on a disk array
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Disk Arrays**.
  3. In the function pane, choose **Host port performance** from the **Report name** list.
- Method 2: viewing the performance of the host ports on a unified storage system
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Unified Storage**.
  3. In the function pane, choose **Front-end host port performance** from the **Report name** list.

Step 2 Set a report that you desire. The following table describes the related parameters.

Parameter	Description	Value
Report view	Type of the report view, **Tendency** or **Comparison**.	[Example] Tendency

Parameter	Description	Value
Object	● If the statistical object is **Select object** 1. In the **Object** list, select the host ports whose statistics you want to view. 2. In **Ports**, select host ports and click  to add them to **Selected Ports**. In **Selected Ports**, select host ports and click  to relocate them to **Ports**. **NOTE** You can also click  to add all host ports to **Selected Ports**, or click  to relocate all of them to **Ports**. ● If the statistical object is **Select device** In **Devices**, select devices and click  to add them to **Selected Devices**. In **Selected Devices**, select devices and click  to relocate them to **Devices**. **NOTE** You can also click  to add all devices to **Selected Devices**. or click  to relocate all of them to **Devices**.	[Example] S5000T_10_11-A
Key performance indicators	Key performance indicators (KPIs) of the user-defined report.	[Example] Usage
Granularity	Granularity of the user-defined report.	[Example] High

Parameter	Description	Value
Time range	Time range for collecting performance statistics. **NOTE** If you set **Time range** to **Custom**, specify the start time and end time.	[Example] Latest 1 week
Format	Method for collecting performance statistics.	[Example] Average

Parameter	Description	Value
Sort	Method for sorting the user-defined report. ● If you set **Sort** to **Default**, the custom report sorts all objects by each preset key performance indicator respectively. For example, if you set **Key performance indicators** to **Usage** and **IOPS** and **Sort** to **Default**, the custom report displays all object information sorted by **Usage** and **IOPS** respectively in two results. ● If you set **Sort** to a key performance indicator, the custom report displays key performance indicators about all objects sorted by the specified key performance indicator. For example, if you set **Key performance indicators** to **Usage** and **IOPS** and **Sort** to **Usage**, the custom report displays **Usage** and **IOPS** information about all objects sorted by **Usage** respectively. ● If **TOP** is set to n ($1 \leqslant n \leqslant 10$), the self-defined report displays a maximum of n statistics objects. – If you select **Maximum** or **Average** for **Format**, the top n indicator values are displayed. – If you select **Minimum** for	[Example]

Parameter	Description	Value
	Format, the smallest n indicator values are displayed.	Default

Step 3 Click **Search**.

In the function pane, the preset KPI graph is displayed.

You can export the KPI graph to analyze the host port performance.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.

----End

Disk Performance

You can set filter criteria for viewing the performance statistics of a specific disk. Then you can learn about the overall disk performance, and locate and troubleshoot faulty disks accordingly.

Prerequisites

At least one storage device exists on the management system.

Procedure

Step 1 Go to the disk performance page by either of the following methods:

- Method 1: viewing the performance of the hard disks on a disk array
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Disk Arrays**.
  3. In the function pane, choose **Disk performance** from the **Report name** list.
- Method 2: viewing the performance of the hard disks on a unified storage system
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Unified Storage**.
  3. In the function pane, choose **Disk performance** from the **Report name** list.

Step 2 Set a report that you desire. The following table describes the related parameters.

Parameter	Description	Value
Report view	Type of the report view, **Tendency** or **Comparison**.	[Example] Tendency

Parameter	Description	Value
Object	● If the statistical object is **Select object** 1. In the **Object** list, select the hard disks whose statistics you want to view. 2. In **Disks**, select hard disks and click  to add them to **Selected Disks**. In **Selected Devices**, select hard disks and click  to relocate them to **Disks**. **NOTE** You can also click  to add all hard disks to **Selected Disks**, or click  to relocate all of them to **Disks**. ● If the statistical object is **Select device** In **Devices**, select devices and click  to add them to **Selected Devices**. In **Selected Devices**, select devices and click  to relocate them to **Devices**. **NOTE** You can also click  to add all devices to **Selected Devices**. or click  to relocate all of them to **Devices**.	[Example] S5000T_10_11-A
Key performance indicators	Key performance indicators (KPIs) of the user-defined report.	[Example] Usage
Granularity	Granularity of the user-defined report.	[Example] High

Parameter	Description	Value
Time range	Time range for collecting performance statistics. **NOTE** If you set **Time range** to **Custom**, specify the start time and end time.	[Example] Latest 1 week
Format	Method for collecting performance statistics.	[Example] Average

Parameter	Description	Value
Sort	Method for sorting the user-defined report. ● If you set **Sort** to **Default**, the custom report sorts all objects by each preset key performance indicator respectively. For example, if you set **Key performance indicators** to **Usage** and **IOPS** and **Sort** to **Default**, the custom report displays all object information sorted by **Usage** and **IOPS** respectively in two results. ● If you set **Sort** to a key performance indicator, the custom report displays key performance indicators about all objects sorted by the specified key performance indicator. For example, if you set **Key performance indicators** to **Usage** and **IOPS** and **Sort** to **Usage**, the custom report displays **Usage** and **IOPS** information about all objects sorted by **Usage** respectively. ● If **TOP** is set to n ($1 \leqslant n \leqslant 10$), the self-defined report displays a maximum of n statistics objects. – If you select **Maximum** or **Average** for **Format**, the top n indicator values are displayed. – If you select **Minimum** for	[Example]

Parameter	Description	Value
	Format, the smallest n indicator values are displayed.	Default

Step 3 Click **Search**.

In the function pane, the preset KPI graph is displayed.

You can export the KPI graph to analyze the disk performance.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.

----End

LUN Performance

A logical unit number (LUN) is a logical disk provided by a controller to application servers for storage. LUNs help application servers make better use of storage resources. You can set filter criteria for viewing the performance statistics of a specific LUN.

Prerequisites

At least one storage device exists on the management system.

Procedure

Step 1 Go to the LUN performance page by either of the following methods:

- Method 1: viewing the performance of the LUNs on a disk array
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Disk Arrays**.
  3. In the function pane, choose **LUN performance** from the **Report name** list.
- Method 2: viewing the performance of the LUNs on a unified storage device
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Unified Storage**.
  3. In the function pane, choose **LUN performance** from the **Report name** list.

Step 2 Set a report that you desire. The following table describes the related parameters.

Parameter	Description	Value
Report view	Type of the report view, **Tendency** or **Comparison**.	[Example] Tendency

Parameter	Description	Value
Object	● If the statistical object is **Select object** 1. In the **Object** list, select the LUNs whose statistics you want to view. 2. In **LUNs**, select LUNs and click  to add them to **Selected LUNs**. In **Selected LUNs**, select LUNs and click  to relocate them to **LUNs**. **NOTE** You can also click  to add all LUNs to **Selected LUNs**, or click  to relocate all of them to **LUNs**. ● If the statistical object is **Select device** In **Devices**, select devices and click  to add them to **Selected Devices**. In **Selected Devices**, select devices and click  to relocate them to **Devices**. **NOTE** You can also click  to add all devices to **Selected Devices**. or click  to relocate all of them to **Devices**.	[Example] S5000T_10_11-A
Key performance indicators	Key performance indicators (KPIs) of the user-defined report.	[Example] Usage
Granularity	Granularity of the user-defined report.	[Example] High

Parameter	Description	Value
Time range	Time range for collecting performance statistics. **NOTE** If you set **Time range** to **Custom**, specify the start time and end time.	[Example] Latest 1 week
Format	Method for collecting performance statistics.	[Example] Average

Parameter	Description	Value
Sort	Method for sorting the user-defined report. ● If you set **Sort** to **Default**, the custom report sorts all objects by each preset key performance indicator respectively. For example, if you set **Key performance indicators** to **Usage** and **IOPS** and **Sort** to **Default**, the custom report displays all object information sorted by **Usage** and **IOPS** respectively in two results. ● If you set **Sort** to a key performance indicator, the custom report displays key performance indicators about all objects sorted by the specified key performance indicator. For example, if you set **Key performance indicators** to **Usage** and **IOPS** and **Sort** to **Usage**, the custom report displays **Usage** and **IOPS** information about all objects sorted by **Usage** respectively. ● If **TOP** is set to n ($1 \leqslant n \leqslant 10$), the self-defined report displays a maximum of n statistics objects. – If you select **Maximum** or **Average** for **Format**, the top n indicator values are displayed. – If you select **Minimum** for	[Example]

Parameter	Description	Value
	Format, the smallest n indicator values are displayed.	Default

Step 3 Click **Search**.

In the function pane, the preset KPI graph is displayed.

You can export the KPI graph to analyze the LUN performance.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.

----End

Service Port Performance

You can set filter criteria for viewing performance statistics of a specific service port. Then you can learn about the overall service port performance, and locate and troubleshoot faulty service ports accordingly.

Prerequisites

At least one unified storage system exists on the management system.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Custom Report** > **Unified Storage**.

Step 3 In the function pane, choose **Service port performance** from the **Report name** list.

Step 4 Set a report that you desire. The following table describes the related parameters.

Parameter	Description	Value
Report view	Type of the report view, **Tendency** or **Comparison**.	[Example] Tendency

Parameter	Description	Value
Object	● If the statistical object is **Select object** 1. In the **Object** list, select the ports whose statistics you want to view. 2. In **Ports**, select ports and click  to add them to **Selected Ports**. In **Selected Ports**, select ports and click  to relocate them to **Ports**. **NOTE** You can also click  to add all ports to **Selected Ports**, or click  to relocate all of them to **Ports**. ● If the statistical object is **Select device** In **Devices**, select devices and click  to add them to **Selected Devices**. In **Selected Devices**, select devices and click  to relocate them to **Devices**. **NOTE** You can also click  to add all devices to **Selected Devices**, or click  to relocate all of them to **Devices**.	[Example] Evil-Evil_01
Key performance indicators	Key performance indicators (KPIs) of the user-defined report.	[Example] Number of outgoing packets
Granularity	Granularity of the user-defined report.	[Example] High
Time range	Time range for collecting port performance statistics. **NOTE** If you set **Time range** to **Custom**, specify the start time and end time.	[Example] Latest 1 week

Parameter	Description	Value
Format	Data format of the user-defined report.	[Example] Average

Parameter	Description	Value
Sort	Method for sorting the user-defined report. ● If you set **Sort** to **Default**, the custom report sorts all objects by each preset key performance indicator respectively. For example, if you set **Key performance indicators** to **Usage** and **IOPS** and **Sort** to **Default**, the custom report displays all object information sorted by **Usage** and **IOPS** respectively in two results. ● If you set **Sort** to a key performance indicator, the custom report displays key performance indicators about all objects sorted by the specified key performance indicator. For example, if you set **Key performance indicators** to **Usage** and **IOPS** and **Sort** to **Usage**, the custom report displays **Usage** and **IOPS** information about all objects sorted by **Usage** respectively. ● If **TOP** is set to n ($1 \leqslant n \leqslant 10$), the self-defined report displays a maximum of n statistics objects. – If you select **Maximum** or **Average** for **Format**, the top n indicator values are displayed. – If you select **Minimum** for	[Example]

Parameter	Description	Value
	Format, the smallest n indicator values are displayed.	Default

Step 5 Click **Search**.

In the function pane, the preset KPI graph is displayed.

You can export the KPI graph to analyze the service port performance.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.

----End

File Engine Node Performance

You can set filter criteria for viewing the performance statistics of a specific file engine node. Then you can locate and rectify device faults accordingly.

Prerequisites

At least one unified storage system exists on the management system.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Custom Report** > **Unified Storage**.

Step 3 In the function pane, choose **File engine node performance** from the **Report name** list.

Step 4 Set a report that you desire. The following table describes the related parameters.

Parameter	Description	Value
Report view	Type of the report view, **Tendency** or **Comparison**.	[Example] Tendency

Parameter	Description	Value
Object	● If the statistical objects are **Select object** 1. In the **Object** list, select the objects whose statistics you want to view. 2. In **Nodes**, select nodes and click  to add them to **Selected Nodes**. In **Selected Nodes**, select nodes and click  to relocate them to **Nodes**. **NOTE** You can also click  to add all nodes to **Selected Nodes**, or click  to relocate all of them to **Nodes**. ● If the statistical object is **Select device** In **Devices**, select devices and click  to add them to **Selected Devices**. In **Selected Devices**, select devices and click  to relocate them to **Devices**. **NOTE** You can also click  to add all devices to **Selected Devices**, or click  to relocate all of them to **Devices**.	[Example] Evil-Evil_01
Key performance indicators	Key performance indicators (KPIs) of the user-defined report.	[Example] Number of outgoing packets
Granularity	Granularity of the user-defined report.	[Example] High

Parameter	Description	Value
Time range	Time range for collecting file engine performance statistics. **NOTE** If you set **Time range** to **Custom**, specify the start time and end time.	[Example] Latest 1 week
Format	Data format of the user-defined report.	[Example] Average

Parameter	Description	Value
Sort	Method for sorting the user-defined report. ● If you set **Sort** to **Default**, the custom report sorts all objects by each preset key performance indicator respectively. For example, if you set **Key performance indicators** to **Usage** and **IOPS** and **Sort** to **Default**, the custom report displays all object information sorted by **Usage** and **IOPS** respectively in two results. ● If you set **Sort** to a key performance indicator, the custom report displays key performance indicators about all objects sorted by the specified key performance indicator. For example, if you set **Key performance indicators** to **Usage** and **IOPS** and **Sort** to **Usage**, the custom report displays **Usage** and **IOPS** information about all objects sorted by **Usage** respectively. ● If **TOP** is set to n ($1 \leqslant n \leqslant 10$), the self-defined report displays a maximum of n statistics objects. – If you select **Maximum** or **Average** for **Format**, the top n indicator values are displayed. – If you select **Minimum** for	[Example]

Parameter	Description	Value
	Format, the smallest n indicator values are displayed.	Default

Step 5 Click **Search**.

In the function pane, the preset KPI graph is displayed.

You can export the KPI graph to analyze the file engine performance.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.

----End

CPU Performance of a File Engine Node

You can set filter criteria for viewing the CPU performance of a specific file engine node.

Prerequisites

At least one unified storage system exists on the management system.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Custom Report** > **Unified Storage**.

Step 3 In the function pane, choose **File engine node CPU performance** from the **Report name** list.

Step 4 Set a report that you desire. The following table describes the related parameters.

Parameter	Description	Value
Report view	Type of the report view, **Tendency** or **Comparison**.	[Example] Tendency

Parameter	Description	Value
Object	● If the statistical object is **Select object** 1. In the **Object** list, select the objects whose statistics you want to view. 2. In **File Engine Nodes**, select file engine nodes and click  to add them to **Selected File Engine Nodes**. In **Selected File Engine Nodes**, select file engine nodes and click  to relocate them to **File Engine Nodes**. **NOTE** You can also click  to add all file engine nodes to **Selected File Engine Nodes**, or click  to relocate all of them to **File Engine Nodes**. ● If the statistical object is **Select device** In **Devices**, select devices and click  to add them to **Selected Devices**. In **Selected Devices**, select devices and click  to relocate them to **Devices**. **NOTE** You can also click  to add all devices to **Selected Devices**, or click  to relocate all of them to **Devices**.	[Example] Evil-Evil_01
Key performance indicators	Key performance indicators (KPIs) of the user-defined report.	[Example] CPU usage
Granularity	Granularity of the user-defined report.	[Example] High

Parameter	Description	Value
Time range	Time range for collecting CPU statistics. **NOTE** If you set **Time range** to **Custom**, specify the start time and end time.	[Example] Latest 1 week
Format	Data format of the user-defined report.	[Example] Average

Parameter	Description	Value
Sort	Method for sorting the user-defined report. ● If you set **Sort** to **Default**, the custom report sorts all objects by each preset key performance indicator respectively. For example, if you set **Key performance indicators** to **Usage** and **IOPS** and **Sort** to **Default**, the custom report displays all object information sorted by **Usage** and **IOPS** respectively in two results. ● If you set **Sort** to a key performance indicator, the custom report displays key performance indicators about all objects sorted by the specified key performance indicator. For example, if you set **Key performance indicators** to **Usage** and **IOPS** and **Sort** to **Usage**, the custom report displays **Usage** and **IOPS** information about all objects sorted by **Usage** respectively. ● If **TOP** is set to n ($1 \leqslant n \leqslant 10$), the self-defined report displays a maximum of n statistics objects. – If you select **Maximum** or **Average** for **Format**, the top n indicator values are displayed. – If you select **Minimum** for	[Example]

Parameter	Description	Value
	Format, the smallest n indicator values are displayed.	Default

Step 5 Click **Search**.

In the function pane, the preset KPI graph is displayed.

You can export the KPI graph to analyze the CPU performance.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.

----End

Storage unit Capacity Summary

You can set filter criteria for viewing the capacity summary of a specific storage unit.

Prerequisites

At least one storage device exists on the management system.

Procedure

Step 1 Go to the disk array or storage unit capacity summary page by either of the following methods:

- Method 1: viewing the disk array capacity summary
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Disk Arrays**.
  3. In the function pane, choose **Disk array capacity summary** from the **Report name** list.
- Method 2: viewing the storage unit capacity summary
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Unified Storage**.
  3. In the function pane, choose **Storage unit capacity summary** from the **Report name** list.

Step 2 Set a report that you desire. The following table describes the related parameters.

Parameter	Description	Value
Object	1. In the **Object** list, select the objects whose statistics you want to view. **NOTE** You can group multiple storage devices and collect the capacity statistics of this group. 2. In **Disk Arrays**/**Available Storage Unit**/**Resource Groups Available for Selection**, select the objects whose statistics you want to view. Click  to add the selected objects to **Selected Disk Arrays**/**Selected Storage Unit**/**Selected Resource Groups**. In **Selected Disk Arrays**/**Selected Storage Unit**/**Selected Resource Groups**, select objects and click  to relocate them to **Disk Arrays**/**Available Storage Unit**/**Resource Groups Available for Selection**. **NOTE** You can also click  to add all objects to **Selected Disk Arrays**/**Selected Storage Unit**/**Selected Resource Groups**, or click  to relocate all of them to **Disk Arrays**/**Available Storage Unit**/**Resource Groups Available for Selection**.	[Example] S5600T_205_206
Time range	Time range for collecting capacity statistics. **NOTE** If you set **Time range** to **Custom**, specify the start time and end time.	[Example] Latest 1 week

Step 3 Click **Search**.

In the function pane, the preset capacity graph is displayed.

You can export the capacity graph to analyze the storage capacity usage.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.
- Click  to open or save the graph in CSV format.

----End

Storage Unit Capacity

You can set filter criteria for viewing the capacity usage of a specific storage unit.

Prerequisites

At least one storage device exists on the management system.

Procedure

Step 1 Go to the disk array or storage unit capacity usage page by either of the following methods:

- Method 1: viewing the disk array capacity usage
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Disk Arrays**.
  3. In the function pane, choose **Disk array capacity** from the **Report name** list.
- Method 2: viewing the storage unit capacity usage
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Unified Storage**.
  3. In the function pane, choose **Storage unit capacity** from the **Report name** list.

Step 2 Set a report that you desire. The following table describes the related parameters.

Parameter	Description	Value
Object	1. In the **Object** list, select the objects whose statistics you want to view. **NOTE** You can group multiple disk arrays and collect the capacity statistics of this group. 2. In **Disk Arrays/ Available Storage Unit/ Resource Groups Available for Selection**, select the objects whose capacity statistics you want to view. Click  to add the selected objects to **Selected Disk Arrays/ Selected Storage Unit/ Selected Resource Groups**. In **Selected Disk Arrays/Selected Storage Unit/Selected Resource Groups**, select objects. Then click  to relocate them to **Disk Arrays/ Available Storage Unit/ Resource Groups Available for Selection**. **NOTE** You can also click  to add all objects to **Selected Disk Arrays/Selected Storage Units/Selected Resource Groups**, or click  to relocate all of them to **Disk Arrays/Available Storage Unit/Resource Groups Available for Selection**.	[Example] S5600T_205_206
Sort	Method for sorting the user-defined report. **NOTE** If **TOP** is set to n ($1 \leqslant n \leqslant 10$), the self-defined report displays a maximum of n statistics objects.	[Example] 5

Parameter	Description	Value
Time range	Time range for collecting capacity statistics. **NOTE** If you set **Time range** to **Custom**, specify the start time and end time.	[Example] Latest 1 week

Step 3 Click **Search**.

In the function pane, the preset capacity graph is displayed.

You can export the capacity graph to analyze the storage capacity usage.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.
- Click  to open or save the graph in CSV format.

----End

Thin Pool Capacity

A thin pool uses the thin provisioning technology to enable dynamic and on-demand storage space allocation. You can set filter criteria for viewing the capacity statistics of a specific thin pool.

Prerequisites

At least one storage device exists on the management system.

Procedure

Step 1 Go to the thin pool capacity page by either of the following methods:

- Method 1: viewing the statistics of a thin pool on a disk array
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Disk Arrays**.
  3. In the function pane, choose **Thin pool capacity** from the **Report name** list.
- Method 2: viewing the statistics of a thin pool on a unified storage system
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Unified Storage**.
  3. In the function pane, choose **Thin pool capacity** from the **Report name** list.

Step 2 Set a report that you desire. The following table describes the related parameters.

Parameter	Description	Value
Object	1. In the **Object** list, select the objects whose statistics you want to view. 2. In **Disk Arrays/ Available Storage Unit**, select the objects whose capacity statistics you want to view. Click  to add the selected objects to **Selected Disk Arrays/ Selected Storage Unit**. In **Selected Disk Arrays/ Selected Storage Unit**, select objects. Then click  to relocate them to **Disk Arrays/Available Storage Unit**. **NOTE** You can also click  to add all objects to **Selected Disk Arrays/Selected Storage Unit**, or click  to relocate all of them to **Disk Arrays/Available Storage Unit**.	[Example] Array_201A
Sort	Method for sorting the user-defined report. **NOTE** If **TOP** is set to n (1 ⩽ n ⩽ 10), the custom report displays a maximum of n statistics objects.	[Example] 5
Time range	Time range for collecting thin pool capacity statistics. **NOTE** If you set **Time range** to **Custom**, specify the start time and end time.	[Example] Latest 1 week

Step 3 Click **Search**.

In the function pane, the preset thin pool capacity graph is displayed.

You can export the capacity graph to analyze the thin pool capacity usage.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.

- Click  to open or save the graph in HTML format.
- Click  to open or save the graph in CSV format.

----End

Thin LUN Capacity

A thin logical unit number (LUN) is a logical storage unit created in a thin pool. It is a logical disk accessible to hosts, and allocates storage space to users based on the actual capacity demand. You can set filter criteria for viewing the capacity statistics of a specific thin LUN.

Prerequisites

At least one storage device exists on the management system.

Procedure

Step 1 Go to the thin LUN capacity page by either of the following methods:

- Method 1: viewing the statistics of a thin LUN on a disk array
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Disk Arrays**.
  3. In the function pane, choose **Thin LUN capacity** from the **Report name** list.
- Method 2: viewing the statistics of a thin LUN on a unified storage system
  1. On the menu bar, choose **Report**.
  2. In the navigation tree, choose **Custom Report** > **Unified Storage**.
  3. In the function pane, choose **Thin LUN capacity** from the **Report name** list.

Step 2 Set a report that you desire. The following table describes the related parameters.

Parameter	Description	Value
Object	1. In the **Object** list, select the objects whose statistics you want to view. **NOTE** You can group multiple disk arrays and collect the capacity statistics of this group. 2. In **Disk Arrays**/**Available Storage Unit**/**Resource Groups Available for Selection**, select the objects whose capacity statistics you want to view. Click  to add the selected objects to **Selected Disk Arrays**/**Selected Storage Unit**/**Selected Resource Groups**. In **Selected Disk Arrays**/**Selected Storage Unit**/**Selected Resource Groups**, select objects. Then click  to relocate the selected objects to **Disk Arrays**/**Available Storage Unit**/**Resource Groups Available for Selection**. **NOTE** You can also click  to add all objects to **Selected Disk Arrays**/**Selected Storage Unit**/**Selected Resource Groups**, or click  to relocate all of them to **Disk Arrays**/**Available Storage Unit**/**Resource Groups Available for Selection**.	[Example] Array_201A
Sort	Method for sorting the user-defined report. **NOTE** If **TOP** is set to n ($1 \leqslant n \leqslant 10$), the self-defined report displays a maximum of n statistics objects.	[Example] 5

Parameter	Description	Value
Time range	Time range for collecting capacity statistics. **NOTE** If you set **Time range** to **Custom**, specify the start time and end time.	[Example] Latest 1 week

Step 3 Click **Search**.

In the function pane, the preset thin LUN capacity graph is displayed.

You can export the capacity graph to analyze the thin LUN capacity usage.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.
- Click  to open or save the graph in CSV format.

----End

File Engine Capacity Summary

You can set filter criteria for viewing the capacity summary of a specific storage device.

Prerequisites

At least one storage device exists on the management system.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Custom Report** > **Unified Storage**.

Step 3 In the function pane, choose **File engine capacity summary** from the **Report name** list.

Step 4 Set a report that you desire. The following table describes the related parameters.

Parameter	Description	Value
Object	1. In the **Object** list, select the objects whose statistics you want to view. 2. In **File Engines**, select file engines and click  to add them to **Selected File Engines**. In **Selected File Engines**, select file engines and click  to relocate them to **File Engines**. **NOTE** You can also click  to add all file engines to **Selected File Engines**, or click  to relocate all of them to **File Engines**.	[Example] S5600T_205_206
Time range	Time range for collecting capacity statistics. **NOTE** If you set **Time range** to **Custom**, specify the start time and end time.	[Example] Latest 1 week

Step 5 Click **Search**.

In the function pane, the preset capacity graph is displayed.

You can export the capacity graph to analyze the storage capacity usage.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.
- Click  to open or save the graph in CSV format.

----End

File Engine Node Capacity

You can set filter criteria for viewing the capacity usage of a specific file engine node.

Prerequisites

At least one storage device exists on the management system.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Custom Report** > **Unified Storage**.

Step 3 In the function pane, choose **File engine node capacity** from the **Report name** list.

Step 4 Set a report that you desire. The following table describes the related parameters.

Parameter	Description	Value
Object	1. In the **Object** list, select the objects whose statistics you want to view. 2. In **File Engines**, select file engines and click  to add them to **Selected File Engines**. In **Selected File Engines**, select file engines and click  to relocate them to **File Engines**. **NOTE** You can also click  to add all file engines to **Selected File Engines**, or click  to relocate all of them to **File Engines**.	[Example] S5600T_205_206
Sort	Method for sorting the user-defined report **NOTE** If **TOP** is set to n ($1 \leqslant n \leqslant 10$), the self-defined report displays a maximum of n statistics objects.	[Example] 5
Time range	Time range for collecting capacity statistics **NOTE** If you set **Time range** to **Custom**, specify the start time and end time.	[Example] Latest 1 week

Step 5 Click **Search**.

In the function pane, the preset capacity graph is displayed.

You can export the capacity graph to analyze the storage capacity usage.

- Click  to open or save the graph in PDF format.

- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.
- Click  to open or save the graph in CSV format.

----End

File Storage Pool Capacity

A file storage pool is used to create file systems. You can set filter criteria for viewing the capacity usage of a specific file storage pool.

Prerequisites

At least one unified storage system exists on the management system.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Custom Report** > **Unified Storage**.

Step 3 In the function pane, choose **File storage pool capacity** from the **Report name** list.

Step 4 Set a report that you desire. The following table describes the related parameters.

Parameter	Description	Value
Object	1. In the **Object** list, select the objects whose statistics you want to view. 2. In **File Engines**/**Resource Groups Available for Selection**, select file engines and click  to add them to **Selected File Engines**/**Selected Resource Groups**. In **Selected File Engines**/**Selected Resource Groups**, select file engines and click  to relocate them to **File Engines**/**Resource Groups Available for Selection**. **NOTE** You can also click  to add all file engines to **Selected File Engines**/**Selected Resource Groups**, or click  to relocate all of them to **File Engines**/**Resource Groups Available for Selection**.	[Example] Evil-Evil_01
Sort	Method for sorting the user-defined report. **NOTE** If **TOP** is set to n ($1 \leqslant n \leqslant 10$), the self-defined report displays a maximum of n statistics objects.	[Example] 5
Time range	Time range for collecting the performance statistics of unified storage systems. **NOTE** If you set **Time range** to **Custom**, specify the start time and end time.	[Example] Latest 1 week

Step 5 Click **Search**.

In the function pane, the preset file storage pool capacity graph is displayed.

You can export the capacity graph to analyze the file storage pool capacity usage.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.
- Click  to open or save the graph in CSV format.

----End

Data Disk Capacity

You can set filter criteria for viewing the capacity usage of a specific data disk on a unified storage system.

Prerequisites

At least one unified storage system exists on the management system.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Custom Report** > **Unified Storage**.

Step 3 In the function pane, choose **Data disk capacity** from the **Report name** list.

Step 4 Set a report that you desire. The following table describes the related parameters.

Parameter	Description	Value
Object	1. In the **Object** list, select the objects whose statistics you want to view. 2. In **File Engines**/**Resource Groups Available for Selection**, select objects and click  to add them to **Selected File Engines**/**Selected Resource Groups**. In **Selected File Engines**/**Selected Resource Groups**, select objects and click to relocate them to **File Engines**/**Resource Groups Available for Selection**. **NOTE** You can also click  to add all objects to **Selected File Engines**/**Selected Resource Groups**, or click  to relocate all of them to **File Engines**/**Resource Groups Available for Selection**.	[Example] Evil-Evil_01
Sort	Method for sorting the user-defined report. **NOTE** If **TOP** is set to n (1 ⩽ n ⩽ 10), the self-defined report displays a maximum of n statistics objects.	[Example] 5
Time range	Time range for collecting the performance statistics of unified storage systems. **NOTE** If you set **Time range** to **Custom**, specify the start time and end time.	[Example] Latest 1 week

Step 5 Click **Search**.

In the function pane, the preset data disk capacity graph is displayed.

You can export the capacity graph to analyze the data disk capacity usage.

- Click to open or save the graph in PDF format.
- Click to open or save the graph in EXCEL format.
- Click to open or save the graph in HTML format.
- Click to open or save the graph in CSV format.

----End

File System Capacity

You can set filter criteria for viewing the capacity usage of a specific file system on a unified storage system.

Prerequisites

At least one unified storage system exists on the management system.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Custom Report** > **Unified Storage**.

Step 3 In the function pane, choose **File system capacity** from the **Report name** list.

Step 4 Set a report that you desire. The following table describes the related parameters.

Parameter	Description	Value
Object	1. In the **Object** list, select the objects whose statistics you want to view. 2. In **File Engines**, select objects and click to add them to **Selected File Engines**. In **Selected File Engines**, select objects and click to relocate them to **File Engines**. **NOTE** You can also click to add all objects to **Selected File Engines**, or click to relocate all of them to **File Engines**.	[Example] Evil-Evil_01

Parameter	Description	Value
Sort	Method for sorting the user-defined report. **NOTE** If **TOP** is set to n (1 ⩽ n ⩽ 10), the self-defined report displays a maximum of n statistics objects.	[Example] 5
Time range	Time range for collecting the performance statistics of unified storage systems. **NOTE** If you set **Time range** to **Custom**, specify the start time and end time.	[Example] Latest 1 week

Step 5 Click **Search**.

In the function pane, the file system capacity usage is displayed.

You can export the capacity graph to analyze the file system capacity usage.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.
- Click  to open or save the graph in CSV format.

----End

Shared File System Capacity

The protocol Common Internet File System (CIFS) and Network File System (NFS) can enable file sharing across the unified storage systems that run different operating systems. You can set filter criteria for viewing the shared capacity of a specific file system.

Prerequisites

At least one unified storage system exists on the management system.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Custom Report** > **Unified Storage**.

Step 3 In the function pane, choose **Shared file system capacity** from the **Report name** list.

Step 4 Set a report that you desire. The following table describes the related parameters.

Parameter	Description	Value
Object	1. In the **Object** list, select the objects whose statistics you want to view. 2. In **File Engines**, select objects and click  to add them to **Selected File Engines**. In **Selected File Engines**, select objects and click  to relocate them to **File Engines**. **NOTE** You can also click  to add all objects to **Selected File Engines**, or click  to relocate all of them to **File Engines**.	[Example] Evil-Evil_01
Sort	Method for sorting the user-defined report. **NOTE** If **TOP** is set to n ($1 \leqslant n \leqslant 10$), the self-defined report displays a maximum of n statistics objects.	[Example] 5
Time range	Time range for collecting the performance statistics of unified storage systems. **NOTE** If you set **Time range** to **Custom**, specify the start time and end time.	[Example] Latest 1 week

Step 5 Click **Search**.

In the function pane, the NFS and CIFS capacity graphs are displayed.

You can export the capacity graphs to analyze the usage of shared file system capacity.

- Click  to open or save the graph in PDF format.
- Click  to open or save the graph in EXCEL format.
- Click  to open or save the graph in HTML format.
- Click  to open or save the graph in CSV format.

----End

7.2.3 Viewing Capacity Trend Prediction Reports

This task helps you view customized capacity trend prediction reports of disk arrays and storage pools.

Viewing capacity trend prediction reports include:

Disk Array Capacity Report

A customized disk array capacity report allows you to analyze the capacity usage of a disk array based on the capacity trend prediction of the disk array.

Prerequisites

Disk arrays have been discovered.

Procedure

Step 1 Go to the **Capacity Trend Prediction** page.

1. On the menu bar, choose **Report**.
2. In the navigation tree, choose **Custom Report** > **Capacity Trend Prediction**.

Step 2 Select the disk array that you want to query.

1. In the function pane, select **Disk Array Capacity** in the **Report name** drop-down list.
2. In the **Available Disk Arrays** list, select a disk array and click  .
3. In the **Selected Disk Arrays** list, select the disk array that you want to query.

Step 3 Set the time range.

Possible values of **Time range** are **Latest 24 hours**, **Latest 1 week**, and **Latest 1 month**.

Step 4 Click **Search**.

- View the capacity trend prediction of the disk array in the **Disk Array Capacity Utilization Usage** area.

  You can export the detailed information about the capacity trend prediction to facilitate capacity usage analysis of the disk array.

  - Click  to open or save the figure as a PDF file.
  - Click  to open or save the figure as an EXCEL file.
  - Click  to open or save the figure as an HTML file.

- You can view the detailed information about disk arrays in the **Counted Disk Arrays** area.

  The information of a disk array includes **Name**, **SN**, **IP Address**, **Total Capacity**, **Used Capacity**, and **Usage (%)**.

----End

Storage Pool Capacity Report

A customized storage pool capacity report allows you to analyze the capacity usage of a storage pool based on the capacity trend prediction of the storage pool.

Prerequisites

- Disk arrays have been discovered.
- The selected disk array has storage pools.

Procedure

Step 1 Go to the **Capacity Trend Prediction** page.

1. On the menu bar, choose **Report**.
2. In the navigation tree, choose **Custom Report** > **Capacity Trend Prediction**.

Step 2 Select the storage pool that you want to query.

1. In the function pane, select **Storage Pool Capacity Report** in the **Report name** drop-down list.
2. In the **Available Disk Arrays** list, select a disk array and click  .
3. In the **Selected Disk Arrays** list, select a disk array. The storage pool list of the selected disk array is displayed in **Available Storage Pools**.
4. Select the storage pool that you want to query.

Step 3 Set the time range.

Possible values of **Time range** are **Latest 24 hours**, **Latest 1 week**, and **Latest 1 month**.

Step 4 Click **Search**.

View the capacity trend prediction of the storage pool in the **Storage Pool Capacity Trend Prediction** area.

You can export the detailed information about the capacity trend prediction to facilitate capacity usage analysis of the storage pool.

- Click  to open or save the figure as a PDF file.
- Click  to open or save the figure as an EXCEL file.
- Click  to open or save the figure as an HTML file.

----End

7.3 Report Task Management

You can set periodic reports to obtain periodic system running information.

7.3.1 Periodic Report Task

A periodic report task generates periodic reports on the management system. You can view those periodic reports to learn about the operating status of the storage system.

Periodic report tasks involve the following operations:

Creating a Periodic Report Task

You can create a periodic report task to collect the statistics of device performance and capacity reports, and to send statistical results to specified email addresses.

Prerequisites

At least one storage device exists on the management system.

Procedure

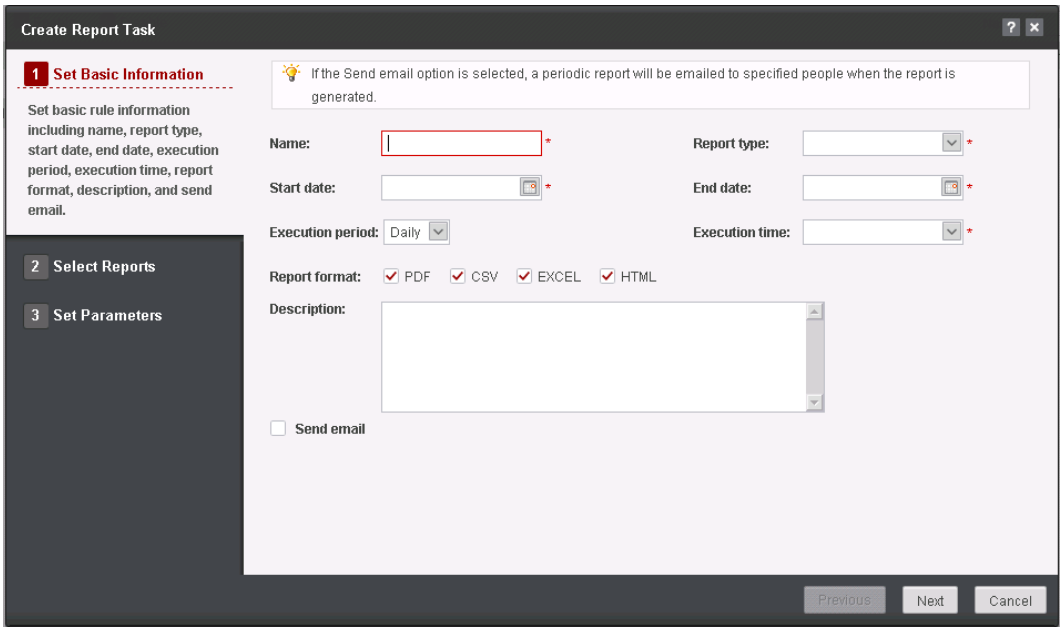
Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Report Task** > **Scheduled Task**.

Step 3 In the function pane, click **Create**.

The **Create Report Task** dialog box is displayed.

Figure 7-1 Create Report Task



Step 4 Set the parameters for the new periodic report task. The following table describes the parameters.

Parameter	Description	Value
Name	Name of the periodic report task.	[Value range] The name can contain only digits, letters, underscores (_), and hyphens (-), and must start with a letter or underscore (_). [Example] report01

Parameter	Description	Value
Report type	Type of the periodic report task, **Performance** or **Capacity**.	[Example] Capacity
Start date	Date when the periodic report task will start. Click  to select a date. The start date cannot be later than the end date.	[Example] 2014-04-04
End date	Date when the periodic report task will stop. Click  to select a date.	[Example] 2014-05-05
Execution period	Frequency for the periodic report task, **Daily**, **Weekly**, **Monthly**, or **Yearly**.	[Example] Daily
Execution time	Time when the periodic report task will start. Select a time from the **Execution time** list.	[Example] 01:00:00
Report format	Format of periodic reports, **PDF**, **CSV**, **EXCEL**, or **HTML**. **NOTE** To select a format, select the check box for it.	[Example] PDF
Description	Description of the periodic report task.	[Example] -
Send email	Recipient mailbox for periodic reports. **NOTE** Select **Send email** and enter an email address in **Email**. Add a description for this email address in **Remarks**. Then click **Add** to add this email address to the email address area.	[Example] report@huawei.com

Step 5 Click **Next**.

Step 6 On the right of the dialog box that is displayed, select the periodic report task that you want to add and click **Next**.

Step 7 Click  and set the parameters of the periodic report task.

NOTE

If you have selected two or more periodic report tasks, you can select **Consolidate all** to consolidate the selected periodic report tasks.

Step 8 Click **Finish**.

The **Success** dialog box is displayed.

Step 9 Click **OK**.

----End

Deleting a Periodic Report Task

You can delete a periodic report task that is no longer useful or has become invalid.

Prerequisites

At least one periodic report task exists on the management system and can be deleted.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Report Task** > **Scheduled Task**.

Step 3 Under **Tasks** in the function pane, select periodic report tasks and click **Delete**.

The **Warning** dialog box is displayed.

Step 4 Click **OK**.

The **Success** dialog box is displayed.

Step 5 Click **OK**.

----End

Enabling a Periodic Report Task

You can enable a disabled periodic report task for this task to continue.

Prerequisites

At least one disabled periodic report task exists on the management system.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Report Task** > **Scheduled Task**.

Step 3 Under **Tasks** in the function pane, select periodic report tasks and click **Enable**.

The **Warning** dialog box is displayed.

Step 4 Click **OK**.

The **Success** dialog box is displayed.

Step 5 Click **OK**.

----End

Disabling a Periodic Report Task

You can disable an ongoing periodic report task for this task to stop.

Prerequisites

At least one enabled periodic report task exists on the management system.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Report Task** > **Scheduled Task**.

Step 3 Under **Tasks** in the function pane, select periodic report tasks and click **Disable**.
The **Warning** dialog box is displayed.

Step 4 Click **OK**.
The **Success** dialog box is displayed.

Step 5 Click **OK**.

----End

Viewing and Modifying a Periodic Report Task

You can view the details about a periodic report task, and modify the periodic report as required.

Prerequisites

At least one periodic report task exists on the management system.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Report Task** > **Scheduled Task**.

Step 3 From the periodic report task list in the function pane, click the task that you want to view or modify.
The management system displays the task details, including the basic information, email address, and report list.

- To modify the basic information about the task, perform **Step 4** to **Step 6**.
- To modify the email address, perform **Step 7** to **Step 9**.
- To modify the report list, perform **Step 10** to **Step 13**.

Step 4 In the **Basic Information** area, click **Modify**.
The **Modify the Basic Information** dialog box is displayed.

Step 5 Modify the basic information about the periodic report task. The following table describes the parameters.

Parameter	Description	Value
Name	Name of the periodic report task.	Value range The name can contain only digits, letters, underscores (_), and hyphens (-), and must start with a letter or underscore (_). [Example] report01
Status	Status of the periodic report task, **Disabled** or **Enabled**. **NOTE** Click **Disabled** or **Enabled** to change the status.	[Example] Disabled
Start date	Date when the periodic report task will start. Click  to select a date. The start date cannot be later than the end date.	[Example] 2014-04-04
End date	Date when the periodic report task will stop. Click  to select a date.	[Example] 2014-05-05
Execution period	Frequency for the periodic report task, **Daily**, **Weekly**, **Monthly**, or **Yearly**.	[Example] Daily
Execution time	Time when the periodic report task will start. Select a time from the **Execution time** list.	[Example] 01:00:00
Report format	Format of periodic reports, **PDF**, **CSV**, **EXCEL**, or **HTML**. **NOTE** To select a format, select the check box for it.	[Example] PDF
Consolidate all	If you have selected two or more periodic report tasks, you can select **Consolidate all** to consolidate the selected periodic report tasks.	[Example] -

Parameter	Description	Value
Description	Description of the periodic report task.	[Example] -

Step 6 Click **OK**. Till now, the basic information about the periodic report task has been modified.

Step 7 In the **Email** area, click **Modify**.

The **Change Email Address** dialog box is displayed.

Step 8 In **Email**, enter an email address and click  .

Add the email address to the email address list.

NOTE

To delete an email address from the list, click  next to this email address.

Step 9 Click **OK**. Till now, the email address has been modified.

Step 10 In the **Report Task** area, click **Add**.

The **Add the report** dialog box is displayed.

NOTE

To delete a report from **Report Task**, select the report and click **Delete**.

Step 11 On the right of the dialog box that is displayed, select the periodic report that you want to add and click **Next**.

Step 12 Click  to set the added periodic report.

Step 13 Click **Finish**. Till now, the periodic report list has been modified.

----End

Searching For a Periodic Report Task

You can search for the desired periodic report task by task name.

Prerequisites

At least one periodic report task exists on the management system.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Report Task** > **Scheduled Task**.

Step 3 In the function pane, enter a periodic report task name in **Name** and click **Search**.

The desired periodic report task is displayed in the report list.

----End

Searching For a Periodic Report Task Using Filter Criteria

You can set filter criteria to search for the desired periodic report task.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Report Task** > **Scheduled Task**.

Step 3 In the function pane, click **Advanced Search**.

Step 4 Set the filter criteria. The following table describes the related parameters.

Parameter	Description	Value
Name	Name of the periodic report task.	Value range The name can contain only digits, letters, underscores (_), and hyphens (-), and must start with a letter or underscore (_). [Example] report01
Report type	Type of the periodic report task, **All**, **Performance**, or **Capacity**.	[Example] Capacity
Status	Status of the periodic report task, **All**, **Enabled**, **Disabled**, or **Expired**.	[Example] Enabled
Period	Frequency for the periodic report task, **All**, **Daily**, **Weekly**, **Monthly**, or **Yearly**.	[Example] Daily

Step 5 Click **Search**.

The desired periodic report task is displayed in the report list.

You can also click **Reset** to reset the filter criteria.

----End

7.3.2 Run Log

You can view the run log of a periodic report task to learn about system status.

Run logs involves the following operations:

Deleting a Report Result

You can delete a report result that is no longer necessary.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Report Task** > **Running Log**.

Step 3 Under **Task log** in the function pane, select a report result and click **Delete**.
The **Warning** dialog box is displayed.

Step 4 Click **OK**.
The **Success** dialog box is displayed.

Step 5 Click **OK**.

----End

Downloading a Report Result

You can download the result of a periodic report task, and then read the result to learn about system status.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Report Task** > **Running Log**.

Step 3 Under **Task log** in the function pane, click  next to a report result and download the report result.

----End

Searching For a Report Result

You can search for the desired report result by report result name.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Report Task** > **Running Log**.

Step 3 In the function pane, enter a report result name in **Name** and click **Search**.
The desired report result is displayed in the result list.

----End

Searching For a Periodic Report Result Using Filter Criteria

You can set filter criteria to search for the desired periodic report result.

Procedure

Step 1 Choose **Report** > **Report Task** > **Running Log**.

Step 2 In the function pane, click **Advanced Search**.

Step 3 Set the filter criteria. The following table describes the related parameters.

Parameter	Description	Value
Name	Name of the periodic report result.	[Example] report01
Period	Frequency for the periodic report task, **All**, **Daily**, **Weekly**, **Monthly**, or **Yearly**.	[Example] Daily
Execution time	Time when the periodic report task will start. Click  to set the start time and end time.	[Example] 2012-04-23 09:30:00 to 2012-04-25 09:30:00
Status	Status of the periodic report result, **All**, **Succeeded** or **Failed**.	[Example] Succeeded

Step 4 Click **Search**.

The desired report result is displayed in the result list.

You can also click **Reset** to reset the filter criteria.

----End

7.4 Report Configuration Management

This section describes how to add a device for statistical collection and perform related settings for reports.

Report configuration management includes the following operations:

7.4.1 Configuring Data Collection

This section describes how to add a storage device on the management system and collect data of this storage device.

Changing the Collection Period

You can set an appropriate device performance collection period to collect desired performance data.

Prerequisites

At least one storage device exists on the management system.

Procedure

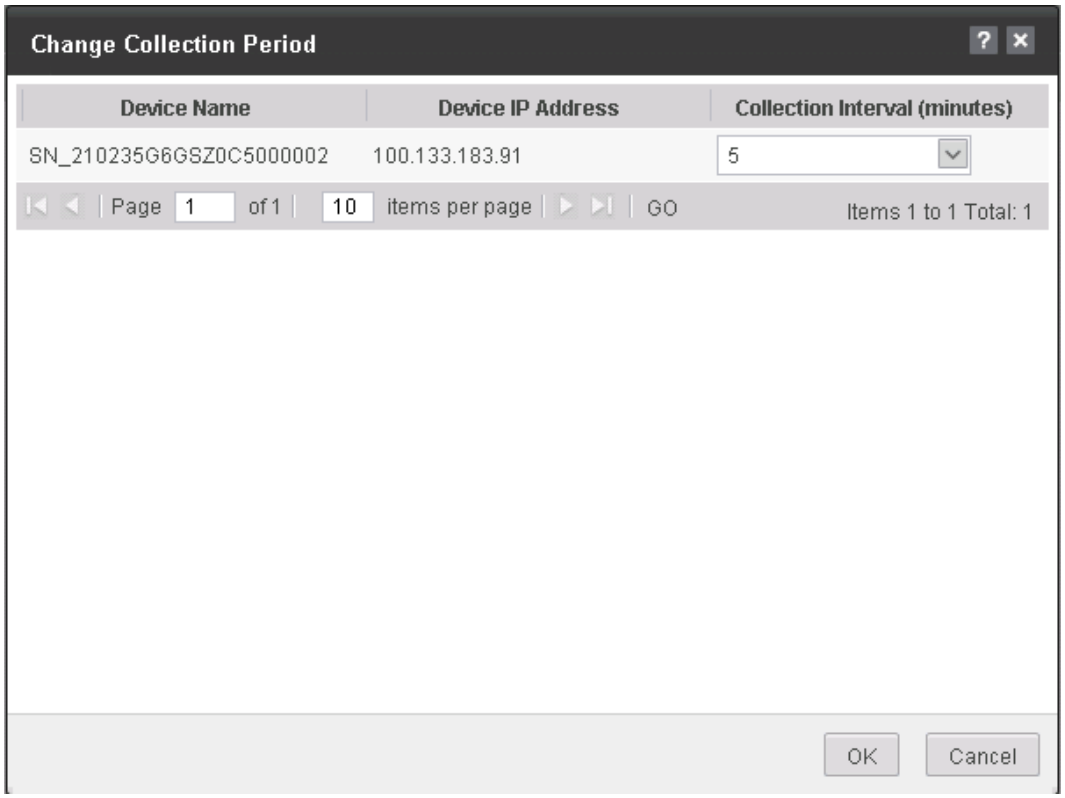
Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Report Configuration** > **Data Collection Configuration**.

Step 3 Under the device list in the function pane, click **Change Collection Period**.

The **Change Collection Period** dialog box is displayed.

Figure 7-2 Change Collection Period



Step 4 Under **Collection Interval (1-60 minutes)**, enter a new collection period.

The collection period ranges from 1 to 60 minutes.

Step 5 Click **OK**.

The **Warning** dialog box is displayed.

Step 6 Click **OK**.

The **Success** dialog box is displayed.

Step 7 Click **OK**.

----End

Enabling Performance Collection

This section describes how to enable performance collection for a storage device.

Procedure

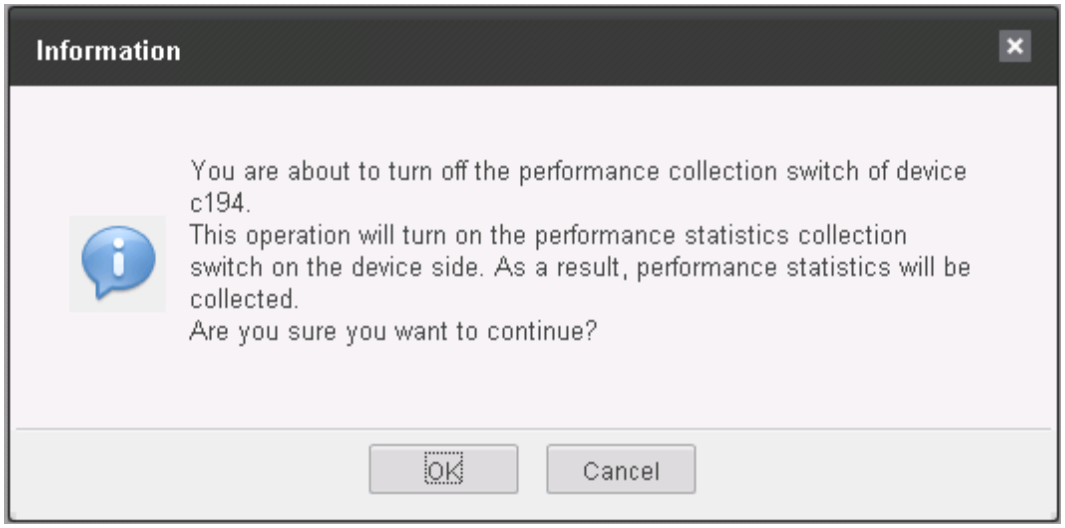
Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Report Configuration** > **Data Collection Configuration**.

Step 3 Under the device list in the function pane, click next to the storage device for which you want to enable performance collection.

The **Information** dialog box is displayed.

Figure 7-3 Information



Step 4 Carefully read the content of the dialog box. Then click **OK**.

The **Success** dialog box is displayed.

Step 5 Click **OK**.

----End

Disabling Performance Collection

This section describes how to disable performance collection for a storage device.

Procedure

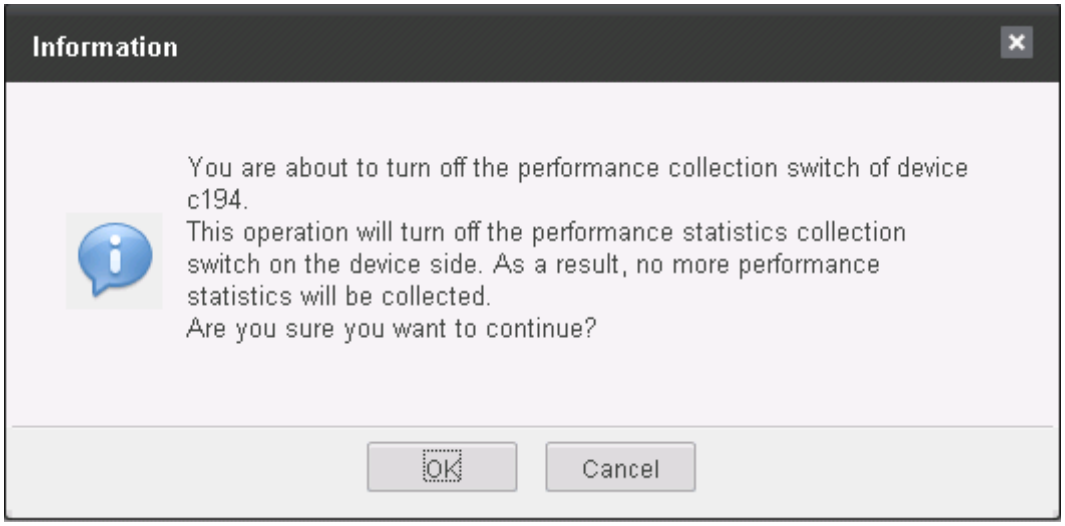
Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Report Configuration** > **Data Collection Configuration**.

Step 3 Under the device list in the function pane, click next to the storage device for which you want to disable performance collection.

The **Information** dialog box is displayed.

Figure 7-4 Information



Step 4 Carefully read the content of the dialog box. Then click **OK**.

The **Success** dialog box is displayed.

Step 5 Click **OK**.

----End

7.4.2 Configuring a Resource Group

You can consolidate storage devices and block storage pools into a resource group. By performing applicable settings, you can then search for the report on each object in the resource group.

Configuring a resource group includes the following operations:

Creating a Resource Group

This section describes how to create a resource group to manage multiple devices in a unified way.

Procedure

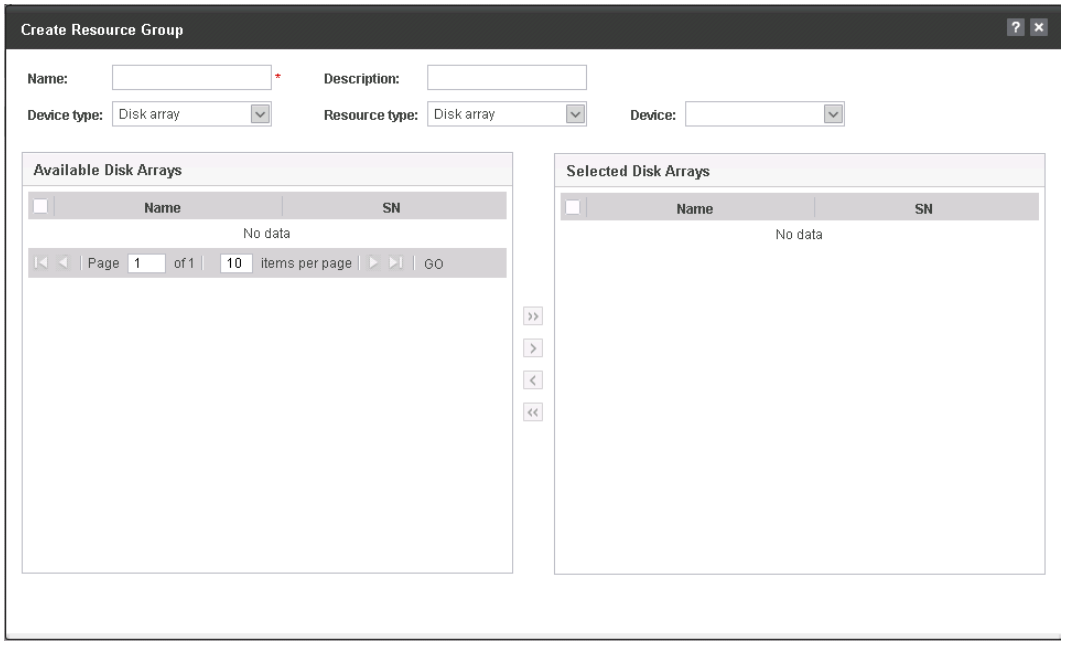
Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Report Configuration** > **Resource Group Configuration**.

Step 3 In the function pane, click **Create**.

The **Create Resource Group** dialog box is displayed.

Figure 7-5 Create Resource Group



Step 4 Set the parameters for the resource group. The following table lists the parameters.

Parameter	Description	Value
Name	Name of the resource group.	[Example] group01
Description	Description of the resource group.	[Example] -
Device type	Type of an object in the resource group, **Disk array** or **Unified storage**.	[Example] Disk array
Resource type	Type of a resource included in a device type. ● When **Device type** is **Disk array**, **Resource type** is **Disk array**, **Storage pool**, or **LUN**. ● When **Device type** is **Unified storage**, **Resource type** is **Storage unit**, **LUN**, or **File system**.	[Example] Storage pool

Parameter	Description	Value
Device	Name of the device. ● This parameter is editable when **Device type** is **Disk array** and **Resource type** is **Storage pool** or **LUN**. ● This parameter is editable when **Device type** is **Unified storage** and **Resource type** is **LUN** or **File system**.	[Example] array

Step 5 Select objects for the new resource group.

- Select objects and click  or  to move them in the specified direction.
- Click  or  to move all objects in the specified direction.

Step 6 Click **OK**.

The **Success** dialog box is displayed.

Step 7 Click **OK**.

----End

Viewing Details About a Resource Group

This section describes how to view details about a resource group.

Prerequisites

At least one resource group exists on the management system.

Procedure

Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Report Configuration** > **Resource Group Configuration**.

Step 3 Under **Resource Group Configuration** in the function pane, details about the resource group are displayed.

- Select **Name** and enter a disk array name in the text box on the right. Then click **Search** to view details about the found disk array.
- Select **Type**. Select a state from the drop-down list on the right. Then click **Search** to view details about the resource groups in the selected state.

Step 4 On the resource group list in the function pane, click the resource group whose details you want to view.

The **Resource Group Details** dialog box is displayed showing details about the selected resource group.

----End

Modifying a Resource Group

This section describes how to rename a resource group and modify its description and objects.

Context

The type of a resource group is unmodifiable.

Procedure

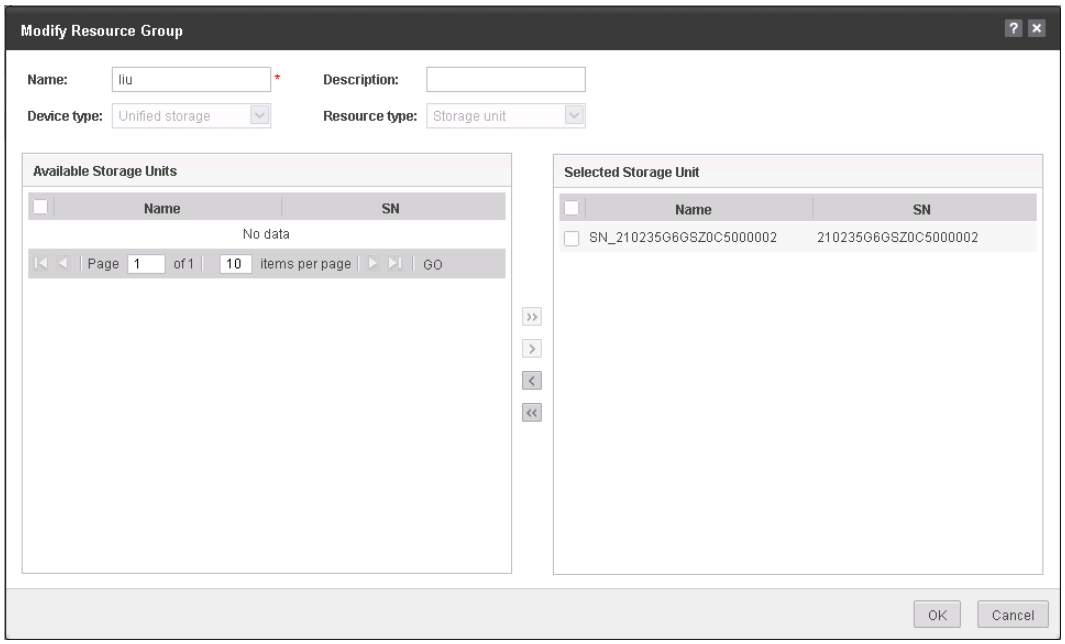
Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Report Configuration** > **Resource Group Configuration**.

Step 3 On the resource group list in the function pane, select a resource group and click **Modify**.

The **Modify Resource Group** dialog box is displayed.

Figure 7-6 Modify Resource Group



Step 4 Rename the resource group or modify its description or objects.

Step 5 Click **OK**.

The **Success** dialog box is displayed.

Step 6 Click **OK**.

----End

Deleting a Resource Group

This section describes how to delete a resource group. After a resource group is deleted, its members can no longer be centrally managed.

Prerequisites

At least one resource group exists on the management system.

Procedure

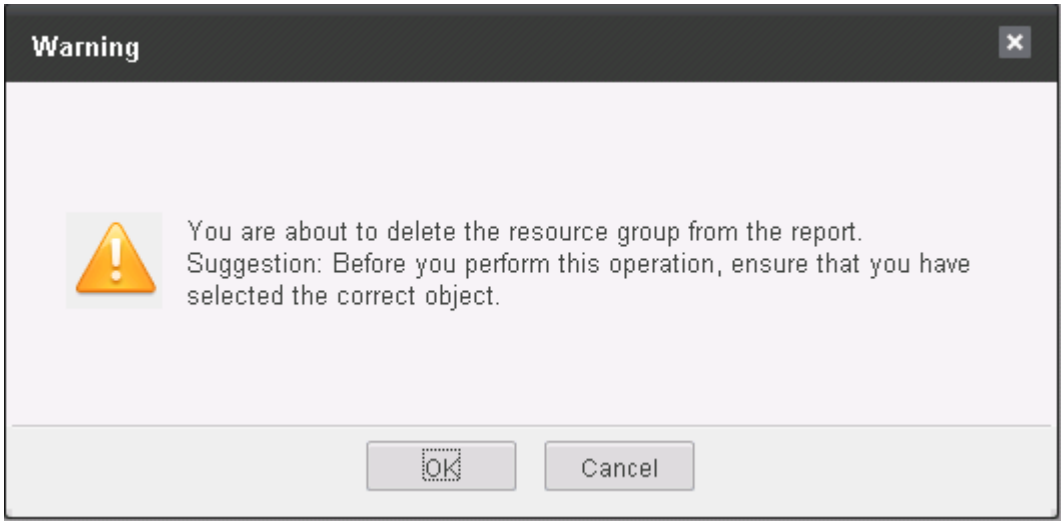
Step 1 On the menu bar, choose **Report**.

Step 2 In the navigation tree, choose **Report Configuration** > **Resource Group Configuration**.

Step 3 On the resource group list in the function pane, select a resource group and click **Delete**.

The **Warning** dialog box is displayed.

Figure 7-7 Warning



Step 4 Click **OK**.

The **Success** dialog box is displayed.

Step 5 Click **OK**.

----End

8 FAQ

About This Chapter

This chapter describes the frequently asked questions (FAQs) about the InfraControl installation and solutions to these questions.

8.1 InfraControl Reports User Account Lockout When Discovering a Device

Symptom

After discovering a device, the InfraControl reports "The user account has been locked. Please try later.".

Possible Causes

1. An incorrect user name or password has been used to scan for devices.
2. The device is discovered, but the user's password for logging in to the device is changed.

Procedure

Step 1 If an administrator attempts to discover a device using an incorrect user name or password, the device locks the user name for 15 minutes. In that case, the administrator has to wait 15 minutes until the device unlocks the user account. The administrator can then enter the correct user name and password to discover the device.

Step 2 A password change on the device also leads to user account lockout. In that case, choose **Management** > **Discover Management** > **Resources** to find the device and clicks **Modify** to change the user account, password, and SSL. Then wait 15 minutes for the device to unlock the user account.

----End

8.2 Firefox Displays an Adobe Flash Plugin Crash When the Firefox Is Used to Open the Topology Management Page of the InfraControl

Symptom

Firefox Displays an Adobe Flash Plugin Crash When the Firefox Is Used to Open the Topology Management Page of the InfraControl.

Possible Causes

In some circumstances, Adobe Flash 11.3 or later has sandbox enabled and is therefore likely to crash.

Procedure

Step 1 Disable the Flash sandbox according to the instructions at Adobe.com and restart the Firefox. It is often an effective measure.

Step 2 Download a Flash Installer from Adobe.com to update Flash.

Step 3 If updating Flash to the latest version does not resolve the problem, you can try downgrading the Flash version to 10.3.

----End

8.3 There are some mistakes Displayed After a User Enters the IP Address in the Address Box of Internet Explorer and Presses Enter

Symptom

There are some mistakes Displayed After a User Enters the IP Address in the Address Box of Internet Explorer and Presses Enter.

Possible Causes

The access request is blocked by the Internet Explorer.

Procedure

Step 1 Open the Internet Explorer and choose **Tools** > **Internet**.

The **Internet** dialog box is displayed.

Step 2 Click the **Security** tab. In **Select a zone to view or change security settings**, select **Trusted Sites** and click **Sites**.

The **Trusted Sites** dialog box is displayed.

Step 3 Add the APM's IP address to trusted sites.

----End

8.4 Statistical Object Missing in an Exported Report When the Name of NetApp Arrays Contains a

Symptom

Statistical Object Missing in an Exported Report When the Name of NetApp Arrays Contains a #.

Possible Causes

The # is a key character that is used inside the arrays. The problem occurs because the report software does not support devices whose names contain the #.

Procedure

Step 1 It is recommended that you delete the # in the device name using device management software.

----End

8.5 InfraControl Report Time Is Different from the Actual Time

Symptom

The time in an InfraControl report is different from the actual time.

Possible Causes

- The system time of the client is incorrect.
- The system time of the InfraControl server is incorrect.
- The system time zone of the client is different from that of the InfraControl server.

Procedure

Step 1 Check whether the system time of the client is correct. If the time is incorrect, set it to a correct time.

Step 2 Check whether the system time of the InfraControl server is correct. If the time is incorrect, set it to a correct time.

Step 3 Check whether the system time zone of the client is the same as that of the InfraControl server. If they are different, set them to the same time zone.

----End

8.6 Some URLs Fail to Be Used to Access the Network Management Page

Symptom

The following URLs cannot be used to access the network management page.

- http://ipaddress/ws
- http://ipaddress/ws/nbiservice?wsdl
- http://ipaddress/ws/WsNmsService?wsdl

Possible Causes

The preceding URLs serve as interfaces of the web service inside the network management system but cannot be used to access the network management page.

- **http://ipaddress/ws** indicates the portal to the web service.

- **http://ipaddress/ws/nbiservice?wsdl** and **http://ipaddress/ws/WsNmsService?wsdl** indicate the portal to the web service for northbound communications inside the network management system.