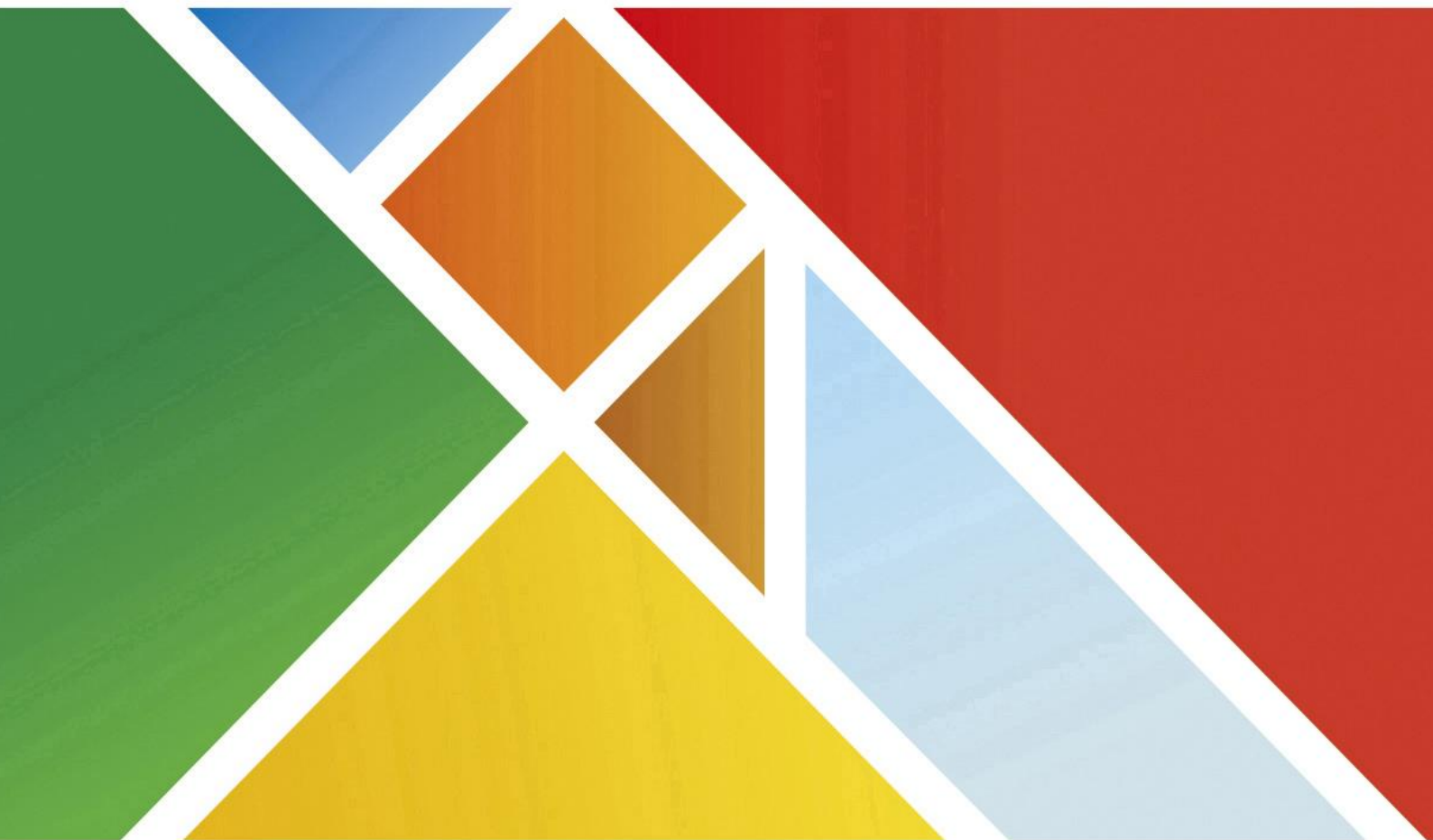




Rethink, to be better



User Manual

——EISOO AnyBackup Appliance 3.5

EISOO Software Co.,Ltd.

Copyright

©2003-2012 EISOO Software Co.,Ltd. All Rights Reserved.

No company or individual are allowed to copy, distribute and extract all or parts of this document without the permission of EISOO Software Co.,Ltd.

The content of this document may be added, deleted or modified and will be regularly added to new versions by EISOO Software Co.,Ltd. We are sorry that no prior notice will be given for any changes.

About EISOO

Being one of the fastest-growing suppliers of All-in-One solutions for backup, storage, and disaster recovery, EISOO persists in the criterion of innovation, profession and sincerity when researching and developing products, aiming to satisfy the needs of customers and make information more effective.

With the development of EISOO, it has experienced from data backup to network storage to disaster recovery by releasing a series of high cost-effective solutions and services which include widely-used EISOO AnyBackup Family, powerful EISOO T×3 Cloud Family and EISOO AnyShare which is an All-in-One device for document management, etc. Thus it has enabled hundreds and thousands users to experience the amazing features of data protection and business continuity, with customer groups spreading in governments, enterprises, electric power, education, health care, research institutions, etc.

It is EISOO's ceaseless innovation that leads users' needs, helping to ensure data security and enhancing business value under such high-speed development.

EISOO Software Co.,Ltd.

Address: 2nd, NO. 8 building, Pujiang Intelligence Valley,
NO. 1188 Lianhang Rd, Minhang District, Shanghai, China

Website: www.eisoo.com

Tel: +86-21- 54323072

Email: help@eisoo.com

Content

Copyright	I
About EISOO	II
Content.....	III
Preface.....	VIII
Chapter 1 Introduction	1
1.1About AnyBackup Appliance 3.5	1
1.2Features of AnyBackup Appliance 3.5	1
1.3Modules and Functions.....	1
Chapter 2 Introduction	6
2.1Notice for Deployment	6
2.1.1 Security Statement.....	6
2.1.2 Important Tips.....	7
2.1.3 Environment	7
2.2Hardware Installation	8
2.2.1 Device Electrification	8
2.2.2 Network Connection.....	8
2.2.3 Disk Installation.....	8
2.3 Start and Shutdown.....	8
2.4Login	9
2.4.1 Login Mode	9
2.4.2 First Login	10
2.4.3 How to User AnySetup	11
Chapter 3 Device Configuration	13
3.1 Management Console	13
3.1.1 System Requirement.....	13
3.1.2 Installation Wizard	14
3.1.3 Instructions	14
3.1.4 Uninstall	19
3.2 iSCSI Client	19
3.2.1 System Requirement.....	19
3.2.2 Installation Wizard	20
3.2.3Usage Instruction	20
3.2.4 Uninstall	25
3.3 LDAP Assistant	25
3.3.1 System Requirement.....	25
3.3.2 Installation Instruction.....	26

3.3.3 Configuration	26
3.3.4 Uninstall	27
3.4 Windows Client.....	27
3.4.1 System Requirements	27
3.4.2 Install by Web.....	28
3.4.3 Normal Client	28
3.4.4 Secure Client.....	29
3.4.5 Daemon Client.....	30
3.5 Linux Client.....	30
3.5.1 System Requirements	30
3.5.2 Installation	30
3.5.3 Uninstall	32
3.6 System Recovery Environment.....	32
3.6.1 System Requirement.....	32
3.6.2 Installation	33
Chapter 4 Centralized Management	34
4.1 Homepage.....	34
4.1.1 Management Console	34
4.1.2 Media Server	34
4.2 Operation	35
Chapter 5 System Management	37
5.1 Login to Management Console.....	37
5.2 User Management.....	37
5.2.1 Create and Manage User.....	38
5.2.2 Create and Manage User Group.....	39
5.2.3 Authorization.....	40
5.2.4 User Space Quota	41
5.3 Client Management.....	41
5.3.1 Client Group	41
5.3.2 Client Configuration	41
5.3.3 Delete Client.....	42
5.4 Disk Media Management.....	42
5.4.1 Media Operation	43
5.4.2 Media Server	43
5.5 Media Synchronization	44
5.6 Tape Media Management.....	46
5.7 Antivirus.....	47
5.8 License	47

5.8.1 Add and Delete License.....	47
5.8.2 Activate License.....	47
5.9 HA/Cluster.....	48
5.10 System Configuration	49
5.11 Warning.....	51
5.12 Update.....	54
5.13 Self-backup Management	55
5.14Log	56
5.14.1 Log Type	56
5.14.2 Log Content.....	56
5.14.3 Log Managment.....	57
Chapter 6 Backup and Restore.....	58
6.1 Backup	58
6.1.1 Regular Backup	58
6.1.2 Real-time Backup	64
6.1.3 Backup Policy	65
6.2 Restore.....	70
6.2.1 Browse to Restore.....	71
6.2.2 Instant Restore	71
6.3Execution	72
6.3.1Routine Execution	73
6.3.2 Continuous Execution.....	73
6.3.3 History List.....	74
6.4 Linux Backup and Restore.....	75
6.4.1 Linux System Backup	75
6.4.2 Linux System Restore.....	76
6.5 Backup and Restore for SQL Server	84
6.5.1 Introduction.....	84
6.5.2 Backup Notice	84
6.5.3 Backup Operation	85
6.5.4 Restore Operation.....	88
6.6Backup and Restore for Oracle.....	90
6.6.1 Introduction.....	90
6.6.2Backup Notice	90
6.6.3Oracle RAC Configuration Requirements	91
6.6.4 Backup Operation	93
6.6.5 Restore Operation.....	100
6.7 Backup and Restore for Exchange Server.....	104

6.7.1 Introduction.....	104
6.7.2 Backup Operation	104
6.7.3 Restore Operation.....	106
6.7.4 Notice after Restore.....	107
6.8 Backup and Restore for Sybase.....	109
6.8.1 Introduction.....	109
6.8.2 Backup Notice	109
6.8.3 Backup Operation	109
6.8.4 Restore Operation.....	112
6.9 Backup and Restore for Active Directory	113
6.9.1 Introduction.....	113
6.9.2 Backup Notice	113
6.9.3 Backup Operation	114
6.9.4 Restore Operation.....	116
6.10 Backup and Restore for VMware	116
6.10.1 Introduction of Backup Modes.....	117
6.10.2 VCB Functional Limitation.....	117
6.10.3 SAN Mode Virtual Machine Backup.....	118
6.10.4 Virtual Machine Restore	121
Chapter 7 System Recovery.....	124
7.1 System Recovery Environment.....	124
7.1.1 Boot from Local Disk	124
7.1.2 Boot from CD/DVD	124
7.1.3 Boot from USB Device	124
7.2 System Recovery.....	124
7.2.1 Manual System Recovery	124
7.2.2 Bare Metal Restore.....	126
Chapter 8 Storage	129
8.1 Disk	129
8.1.1 RAID	129
8.1.2 Volume.....	131
8.1.3 Disk List.....	132
8.2 Share.....	133
8.2.1 Shared Directory	134
8.2.2 Shared Service.....	140
8.2.3 Share Data	141
8.3 iSCSI.....	142
8.3.1 iSCSI Target	142

8.3.2 iSCSI Service	143
8.4 FC SAN	143
8.4.1 FC SAN Target	143
8.4.2 FC SAN Service	144
Chapter 9 Device Management	145
9.1 Virtual Machine	145
9.1.1 Storage	145
9.1.2 Virtual Machine	146
9.2 Network	148
9.3 Device	151
Chapter 10 AnySupport	154
Chapter 11 FAQ	155

Preface

Thanks for your choice of EISOO AnyBackup Appliance. To avoid unnecessary device damage, please read this document carefully before installation and usage. Any problems encountered, please refer to chapter 11 FAQ or contact EISOO Service Department for help.

This document is for:

- ◆ Network Engineer
- ◆ Network Administrator
- ◆ Anyone interested in our products or backup & storage

Chapter 1 Introduction

1.1 About AnyBackup Appliance 3.5

As a leading All-in-One device, EISOO AnyBackup 3.5 Appliance is designed to provide users with innovative solutions. It can satisfy centralized backup for Windows, Linux and Unix and various business continuity and virtualization as well. It supports auto synchronization and remote data protection. This device adopts a combination of multiple storage structures of NAS, IP SAN and FC SAN to satisfy the needs of data share and centralized storage.

1.2 Features of AnyBackup Appliance 3.5

- Based on CDP technology, real-time replication for Oracle/SQL Server/MySQL/ on Windows/Linux are supported.
- Transmission and storage is reduced due to deduplication.
- Rich network transmission control, transmission bandwidth compression and flow control are supported.
- D2D2R is supported for better data protection.
- New real-time replication engine supports full restore
- Built-in VMware Server virtualization platform support Windows, Linux, virtualization platform storage management, virtual machine status control, virtual machine snapshot and remote control.
- Comprehensive backup are supported, including backup for Windows on Intel Itanium, backup and restore for DB2, Sharepoint, virtualization platform, self-backup and self-restore.
- Support complete RAID for more requirements and protection.
- Support protection for battery to ensure secure, reliable and complete data.

1.3 Modules and Functions

EISOO AnyBackup Appliance is composed by the following modules:



◆ **Management Console**

Management Console is usually installed in the storage server and provides browser-based management and operating interface. The following operations can be done by Administrator on Management Console:

1. Assign users permission and storage space in a centralized way.
2. Install, manage and configure remote clients.
3. Synchronize backup data to remote media server.
4. Configure network reconnection and Backup Set status.
5. Execute data backup and restore.
6. View schedules, execution status and execution logs of backup jobs.

On management console, administrator can back up all data in local and remote Clients, including files, emails, Operating Systems and Database as Microsoft SQL Server, Oracle, Sybase, Exchange Server, Domino, Active Directory and DB2. Data can also be restored to Clients appointed or downloaded to local machine via web. The following are specified backup and restore features:

- Supports incremental backup for all kinds of files. Incremental Backup is usually adopted to back up modified or newly-added files to accelerate backup speed and save storage space.
- Supports full backup, differential backup for files, logs and database of

Microsoft SQL Server. Supports database consistency verification and media verification.

- Supports full backup, incremental backup for files, logs and database of Oracle. Supports backup and restore for the whole database, or just one or more Table Space. Supports to backup and restore Control Files and Archive Logs.
- Supports full backup, incremental backup and restore for Sybase on Windows.
- Supports backup and restore for database, logs and check files of Active Directory.
- Support full backup, incremental backup for Windows Exchange Server. Supports consistency verification of full backup and incremental backup data. Supports to backup and restore public file folders or emails.
- Supports incremental backup of Operating System in operation, and supports system recovery when it runs abnormally due to hardware failure and virus attack to reduce downtime and system maintenance workload.
- Supports incremental backup for Outlook, Outlook Express, Foxmail, Thunderbird, Windows mail and Windows Live mail, etc.
- Supports to schedule backup jobs to run at appointed time automatically.
- Supports rotation backup. Maximum copies for full backup and incremental backup can be set.
- Supports encryption and data compression during backup.
- Support precise restore. To realize this feature, users first select the client to be restored in browser, and then select backup job and backup time, at last choose data source to restore them.

Management Console also provides centralized backup, execution management, user and media management, etc. The following are the features in detail:

- **Login** on Management Console is based on B/S structure and used for administrator to login to Management Console in any computer.
- **Backup** on Management Console is used to schedule to create a series of backup job to backup Client data.
- **Restore** on Management Console is used to restore backed-up data to any appointed client or download them through Web by administrator or any authorized users.

- **Execution** on Management Console is used to display the status and process of backup and restore operation. And the history of each such an execution could be saved.
- **Log** on Management Console is used for administrator or users to view user logs, system logs and client logs.
- **User** on Management Console is used to create user accounts, modify user information and authorize users by administrator to access Clients as well as binding storage Media on Management Console.
- **Client** on Management Console is used to manage clients which could be grouped. And operations as deletion, remote installation and necessary uninstall of property configuration can also be executed on Management Console.
- **HA/Cluster** on Management Console is used to bind clients, and configure or delete such bindings.
- **Media Server** on Management Console is used to manage all Medias and Media Servers as well as to set space quota for Medias bundled with users.
- **License** on Management Console is used to manage license by administrator.
- **Configuration** is used to configure Management Console according to specific conditions to avoid port conflict effectively.

◆ **Management Tool**

Besides web management, EISOO AnyBackup Appliance also provides an auxiliary management software — EISOO AnyBackup Management Tool, which is used to set and monitor all the network info of EISOO AnyBackup Appliance in LAN.

◆ **iSCSI Client**

iSCSI client is offered by Microsoft for free. It is used to search and connect iSCSI target device, including Microsoft iSCSI Initiator and iSCSI Monitor Service. Once client is installed, admin can use storage space of EISOO AnyBackup Appliance by iSCSI.

◆ **LDAP Assistant**

LDAP assistant can be deployed on Windows AD to realize seamless authentication of Windows AD.

- Support LDAP Authentication and Windows AD authentication.
- Windows and Linux console can access to LDAP assistant to realize authentication regardless of platform.

- LDAP assistant can traverse all users and user groups in Windows AD to import user to management console quickly.

◆ **Media Server**

Besides installation of management console, if user wants to store data to other storage device, media server can be installed, which is different from media server on management console. This media server is installed on Windows to accept control of management console for backup and restore of client data.

- Provides media binding to serially connect several physical media device or logical media device to make more storage containers
- Support media space quota management to offer authorized max user media space.
- Receive backup data form client and store them to appointed media.
- Receive restore request form client or management console and restore data to client or download them from HTTP.

◆ **Windows Client**

Windows client is installed in server or PC that needs backup under Windows 2000 or higher edition system. It responds to demands from Management Console and provides backup and restore for files, OS, emails, database as Lotus Domino, SQL Server, Oracle, Exchange Server, Sybase, Active Directory, or DB2.

EISOO AnyBackup 3.5 provides the following three kinds of Windows Client for user' s choice:

➤ **Normal Client**

This kind of Client is usually installed in common user' s computer, all the data in such a computer can be checked and handled by administrator. The following components are included in this kind of Client: Client Engine which Management Console can visit at any time, Client Interface which used to display Client backup status, and Recovery Components which is integrated with System Resource Manager to facilitate file backup in Resource Manager.

➤ **Daemon Client**

It is usually installed in common user' s computer to do compulsory data backup for the enterprise, all of the data in such a computer can be checked and operated by administrator. This Client can be uninstalled only with passwords from Administrator.

➤ **Secure Client**

It is installed in computers with sensitive data and bound with a specific user. Only the bound user has the permission to access to the data in Secure Client,

which even administrator cannot access to. The only difference between Secure Client and Common Client is the former bound with a specific user.

◆ **Linux Client**

Linux Client is installed in Linux System to protect data on Linux platform. It responds to commands from Management Console and offer data backup for files and databases as Oracle. Linux Client of this version supports Daemon Client only. After the installation of AnyBackup Client, Procedure will start automatically to respond to commands from Management Console.

◆ **UNIX Client**

UNIX client is deployed on UNIX system to respond command from management console and backup and restore request.

◆ **System Recovery Environment**

System Recovery Environment runs independently. It is utilized to initiate System Recovery Wizard to finish Operating System Recovery when it fails to start, and it is an indispensable module in system backup:

- Supporting System Recovery for desktop or server environment.
- Supporting connection to Media Server to search for system backup set and to recover OS of client.
- Supporting binding System Recovery user when making System Recovery Environment, thus it can be auto-connected to Media Server to execute System Recovery.
- Supporting Bare Metal Recovery. Automatic recovery of standard System Backup set can be set while initiating machines. The work of desktop system maintenance will be greatly reduced.

Chapter 2 Introduction

2.1 Notice for Deployment

2.1.1 Security Statement

◆ **Carefull**

To avoid electronic shock, please do not open shell. There are no parts for user to repair inward, please contace channel parter if maintenance is necessary.

◆ **Security**

Please read this document carefully before installation and usage of EISOO AnyBackup Appliance.

Please do not try to repair this product, the damage caused by opening or removing shell may lead loss of your warranty.

◆ **Statement**

According to standard code GB9254-2008 , this product is A level product, which will cause radio interference. In such case, user should take measures to avode this interference. **Note:** Living environment refers to envirtionment which is 10 meters away from this device, in which radio and TV can be received.

◆ ⚡ **Warning**

Please ensure rack or desktop is strong enough for EISOO AnyBackup Appliance, in case it will collapse due to overweight.

Please avoid violent shake during working, otherwise physical damage will occur.

2.1.2 Important Tips

The RAID technology of EISOO AnyBackup Storage Appliance can make more reliable and secure data storage, but not absolutely. Poor physical environment, vibration, misuse or multiple disk failure will possibly cause device damage and data loss. So re-backup is needed for critical or uique data to prevent deathful loss in disasters. Meanwhile, please be careful on the operating circumstances of devices. If any warning such as sound, light, mail warning or disk failure, please feel free to contact EISOO to avoid unexpected data loss.

2.1.3 Environment

EISOO AnyBackup Appliance works under certain temperature and humidity, together with certain air circulation as shown in the following table:

Environment	Scope
Temperature	0°C~40°C (32°F~104°F)
Humidity	10%~85%

Figure 1 working environment

The following figure is the power environment of EISOO AnyBackup Appliance.

Environment	Scope
Voltage	200VAC ~ 240VAC or 100VAC ~ 125VAC
Current	<3.5A or <7A
Current Frequency	47Hz ~ 55Hz

Figure 2 Power Environment

⚡ **Warning:** EISOO AnyBackup Appliance should work under the above environment; otherwise, physical damage may be caused.

2.2 Hardware Installation

2.2.1 Device Electrification

Insert one end of power line to power input slot of EISOO AnyBackup Appliance with the other end to power socket or UPS. As shown in the following picture:



Figure 3 Power Connection

2.2.2 Network Connection

Insert one end of Ethernet cable to the Ethernet port of server with the other end to HUB or Switch port.

As shown in the following picture:

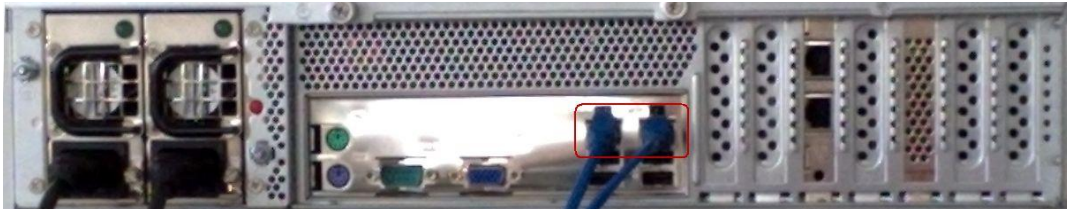


Figure 4 Network Cable

⚠ **Warning:** Please ensure power switch of front panel is off when connecting power; otherwise, damage will be caused.

2.2.3 Disk Installation

If you need to install or replace disk, you can pull out the disk tray and install as the following figure showed, tightening the screw:



Figure 5 Disk Insert/Pull

2.3 Start and Shutdown

◆ Start System

Ensure power line is connected to power slot on the back of EISOO AnyBackup Appliance and grounded receptacle.

Press power switch on the front panel and start EISOO AnyBackup Appliance.

◆ Restart System

Two ways to restart system are provided by EISOO AnyBackup Appliance:

- **Normal Restart:** Login to web management interface and click [Restart] to restart EISOO AnyBackup Appliance normally.
- **Forced Restart:** Press the pinhole above the restart icon by any needle-like objects with symbol of “” and system will restart within 5 seconds.

◆ Shutdown System

Two ways are provided by EISOO AnyBackup Appliance to shut down system:

- **Normal Shutdown:** Login to web management interface and click “EISOO AnyBackup Appliance” to enter operating interface. Click [Shutdown] to shut down system normally. About 30 seconds is needed until power light is off.
- **Forced Shutdown:** If pressing the switch for 5 seconds when system is running normally, forced shutdown will be started. System will auto check and restore during next start.

⚠ **Caution:** Forced shutdown may cause data loss and postponed service, and it is recommended to avoid forced shutdown.

2.4 Login

Three login ways are provided by EISOO AnyBackup Appliance: Based on Password, Based on USB-Key and Based on Password and USB-Key.

2.4.1 Login Mode

Enter login interface of console via such links as <http://192.168.0.253 : 9800> (Default address of Management Console), as shown in the following picture:

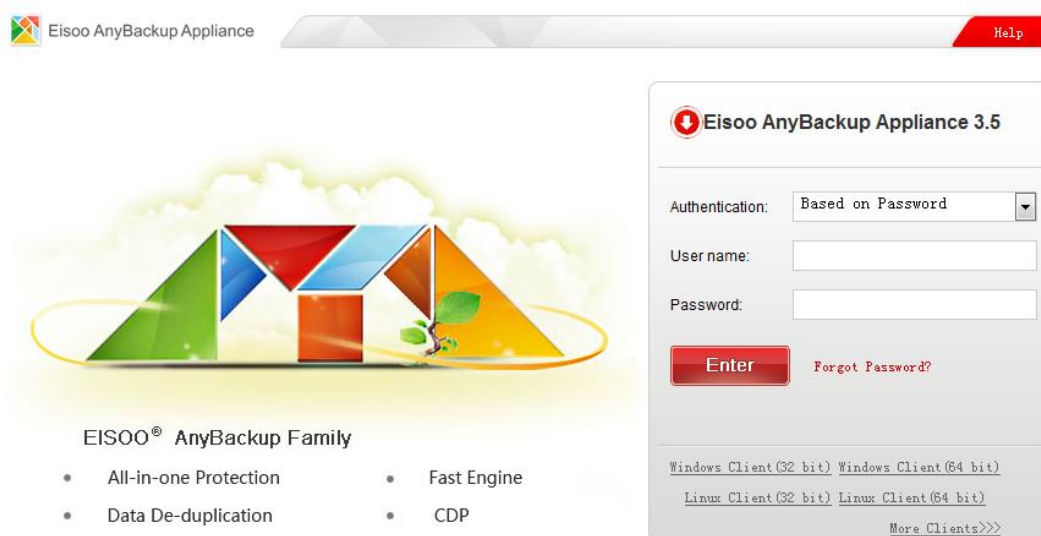


Figure 6 Login Interface

Select authentication type and login to management console:

◆ **Based on Password**

- Admin account has been pre-set by EISOO AnyBackup Appliance with username as "admin" and initial password "123456" .
- After login, admin can create user in [Configuration] >> [User] >> [New].
- When common user login, input username and initial password "123456" .
- If admin enable "audit" in [Configuration] >> [User], audit can login with user name: "audit" and initial password "123456" .

2.4.2 First Login

When you login the Management Console for the first time, a dialog box Password and Email Bound will pop out for Administrator to change the information.

◆ **Mail Configuration**

Another pop-up box is Email Configuration in which you can configure SMTP Server, Port (Default port is 25), User name and Password. After configuration, click **[Send Test Email]** and input the email address in the pop-up dialog box. Then, you can Login to your email box to check whether there is an email named Test Mail: This is a test mail sent by EISOO AnyBackup Appliance. Your receipt demonstrates that you have configured the Mail Notification successfully.

Meanwhile, after configuration, please check the top right corner of the page. There should list the following options: User, Modify Password, Modify Mail, Email Notification, Help and Exit.

◆ **Modify Password**

Modify the Login password.

◆ **Modify Email**

Modify the email address for event notification and password retrieval..

◆ **Email Notification**

Two kinds of mails are included, that is, notification when backup succeeds and notification when backup failed. You can select one or both or neither of them according to your own need.

◆ **Help**

Get familiar with the operating principle and process through Readme File.

◆ **Exit**

Exit to exit current operating interface and back to Login Page.

2.4.3 How to User AnySetup

EISOO AnyBackup Appliance integrates and manages a group of package to offer user a united installation management interface.



Double click to pop up a dialog box.

Select default language during installation.

If it is a 64-bit machine to install management console, a dialog box will pop up to select 32-bit or 64-bit. Click [Next] to pop up installation initial page, including [System Environment Detection], [Install Client], [Install Auxiliary Modules] and [Installation Instruction] as shown in the following picture:



Figure 8 Installation program-Initial Page

Before installation, please click **[System Environment Detection]** to check whether your computer can run EISOO AnyBackup Appliance.

◆ Environment Detection

System Environment Detection is employed to check whether targeted system can run all modules of EISOO AnyBackup Appliance, which includes the following parts: Operating System, CPU Frequency, Physical Memory, Disk Available Space, Default Browser, and Port Availability. If system meets the installation requirements of AnyBackup 3.5, the light will display in green; if it is below the minimal standard, such as memory space is less than 256 MB, the light will show in red; if system environment is request higher than default standard or if port is unavailable, the light will display in yellow as a warning.

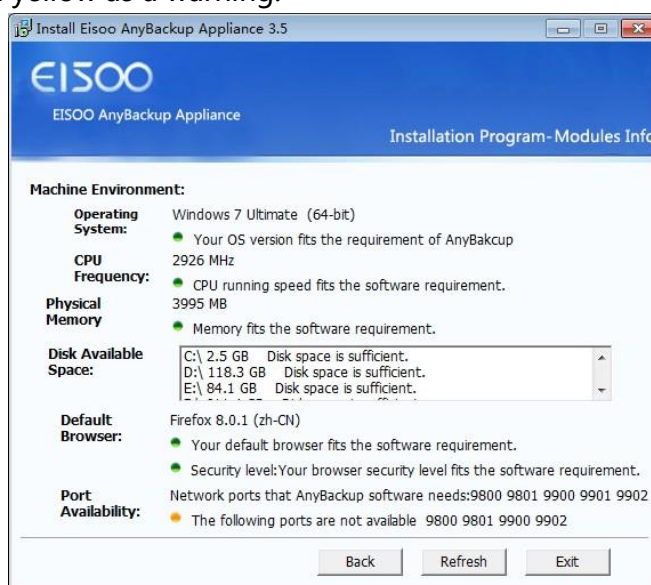


Figure 9 Environment Detection

◆ Installation Instructions

In this part, System Requirements, Installation Steps, Uninstall Instructions and Other information of each module will be introduced in details.

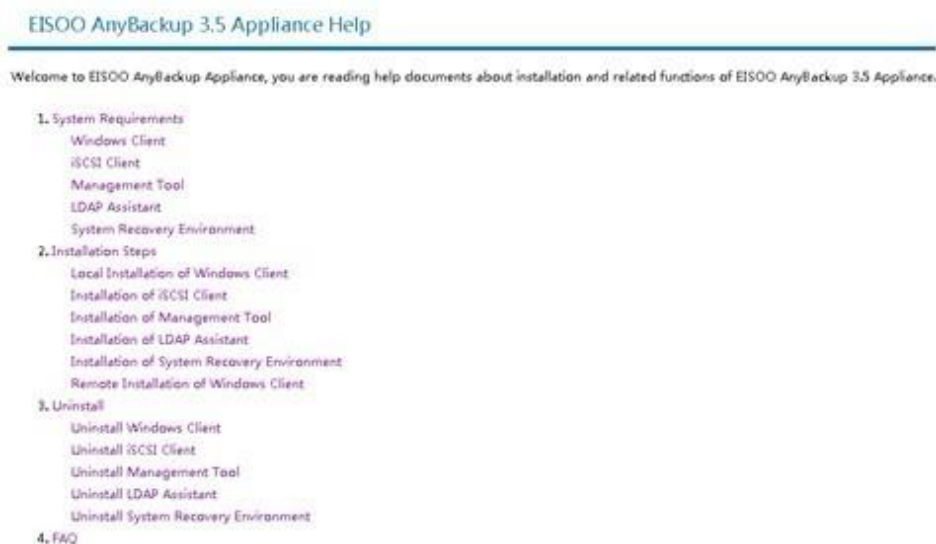


Figure 10 Installation Instruction

◆ Readme File

Enter [Installation program-initial page] and click [View Readme File] on the left.

Readme file of EISOO AnyBackup Appliance provides installation instruction, new features, introduction, modules, version difference, end user license, etc, by which user can better know EISOO AnyBackup Appliance.

Chapter 3 Device Configuration

Before installation and usage, system requirements for each module, feature configuration such as login account, management tool and clients should be learnt.

3.1 Management Console

Besides web management, EISOO AnyBackup Appliance provides a auxiliary management software——EIAOO AnyBackup Appliance Management Tool to configure and monitor network info of EISOO AnyBackup Appliance in LAN.

3.1.1 System Requirement

Item		Required	Recommended
CPU		766 MHz	900 MHz or above
Memory		256 MB	512 MB or more
Required	Free	500 MB	1 GB

Space		
OS	Windows 2000 SP4 or above, Windows Server 2003 SP1 or above, Windows XP SP2 or above	Windows Server 2003 SP2

Figure 11 System Requirement

3.1.2 Installation Wizard

Insert installation disk of management console and click AnySetup installation package to select default language to enter installation program-initial page.

Step One: Click "Install Auxiliary Module" to select [Management Tool] and click [Install].

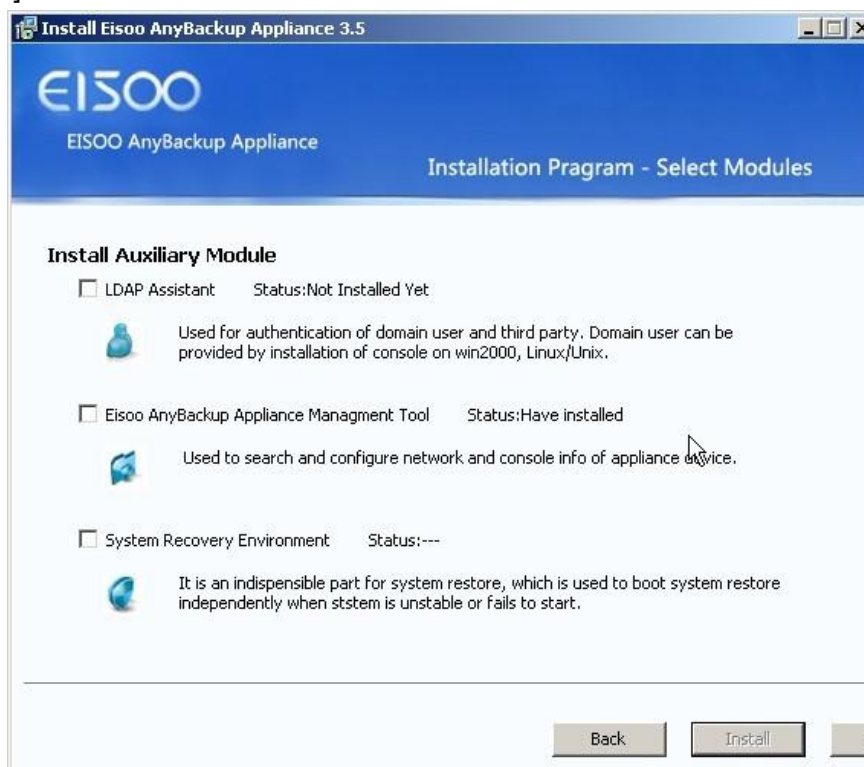


Figure 12 Install Auxiliary Module

Step Two: Finish installation according to installation tips.

3.1.3 Instructions

◆ Auto Search EISOO AnyBackup Appliance

Since the start of management tool, it will automatically search devices on Internet and device information will be shown on the left of main interface once the device is detected.

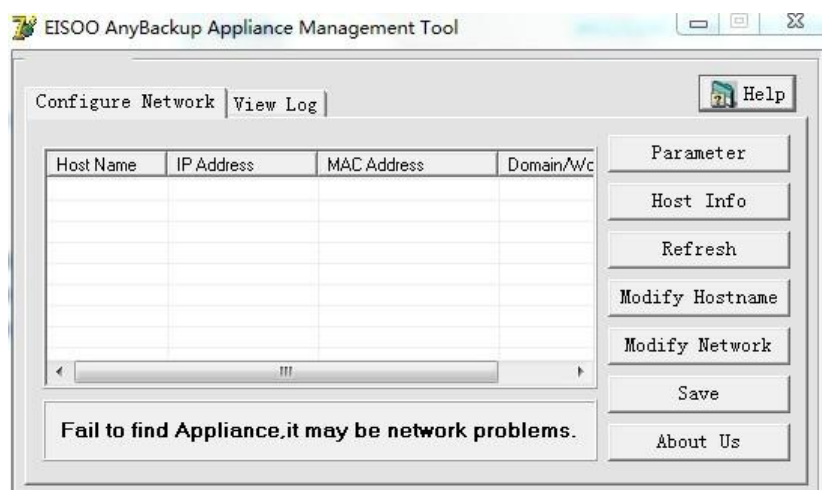


Figure 13 Management Tool Interface

◆ Parameter

Click [Parameter] to set refresh time interval. After each refresh, working EISOO AnyBackup Appliance will be displayed and time interval can be set between 1 minute to 60 minutes as shown in the following picture:

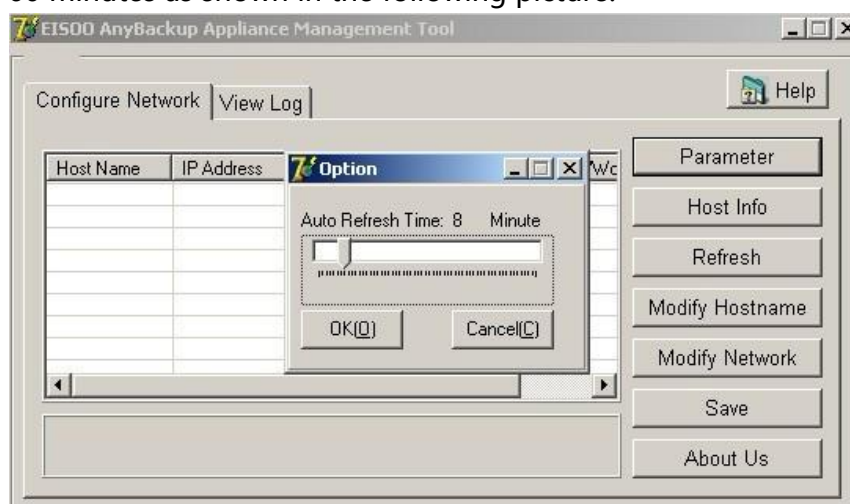


Figure 14 Parameter

Note: If "One host machine is starting network device and info can not be displayed, please try again later" dialog box pop up, click [Refresh] later to get all host info in LAN.

◆ Host Info

Click [Host] to display network info of host. If multiple hosts exist, info of specified host will be displayed; if only one host exist, current host info will be displayed as shown in the following picture:

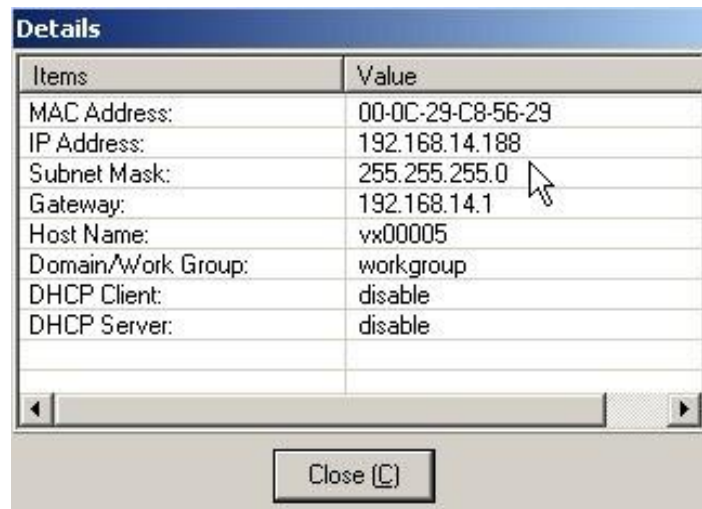


Figure 15 Host Info

Host Info includes:

- **MAC Address:** MAC is physical address of NIC to mark network device.
- **IP Address:** 32-bit binary adopted, it is mark address for communication with other network device.
- **Subnet Mask:** Integrated with IP address, it is used to distinguish network part and host part in IP address.
- **Gateway Address:** It is used to connect IP of device in two different networks.
- **Host name:** Appliance name in the network.
- **Domain name/Work Group:** letter or name easy to memorize is used to signify IP address.
- **DHCP Client:** It shows IP address in active/passive allocation.
"enable" means DHCP is used while "diable" means IP is set manually.
- **DHCP Server:** Provide features of DHCP server.

◆ **Refresh**

Click [Refresh] (or Enter key) to refresh and search host info in the network.

Oure software will also refresh automatically, whose time interval is controlled by [Parameter].

◆ **Modify Host Name**

Click [Modify Host Name] to modify appointed host name. Input user ID, password to modify host name and other info. Click [Apply] to finish modification as shown in the following picture:

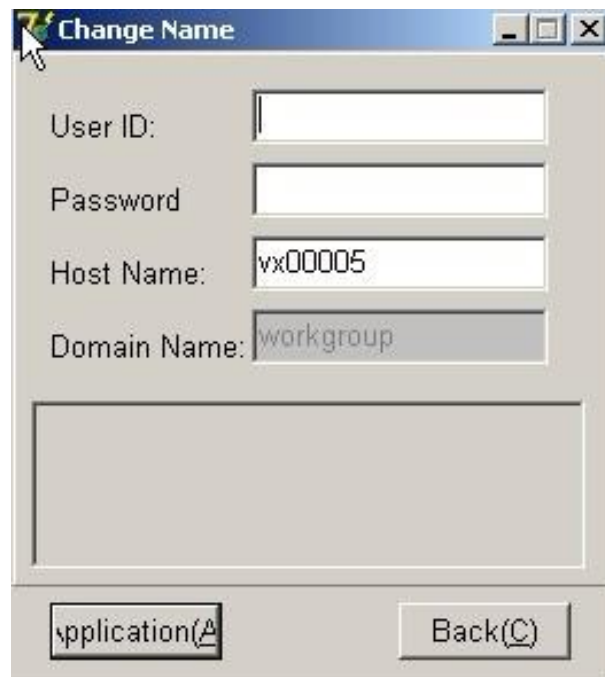


Figure 16 Modify Host Name

◆ **Modify Network**

Click [Modify Network] to change specified host network, including IP, subnet, gateway; DHCP can also be used to allocate address as shown in the following picture:

Figure 17 Modify Network

Step One: Select host to modify in host list.

Step Two: Click [Modify Network].

Step Three: Input user name and password and only admin is allowed to login.

Step Four: Modify network info in dialog box and if DHCP is selected, there is no need to input IP address and other info.

Step Five: Click [Apply] or click [Enter] on keyboard to send modified info.

Step Six: Click [Back] to close dialog box.

Note: System default admin account is "admin" without password "admin" .

◆ Save Info

Click [Save] to save all host info as log file.

If this file is saved in file folder log of directory NasNow, this software can be used to view this log file.

◆ View Log

If log has been saved in directory log of management too, this software can be used to view network configuration as shown in the following picture:

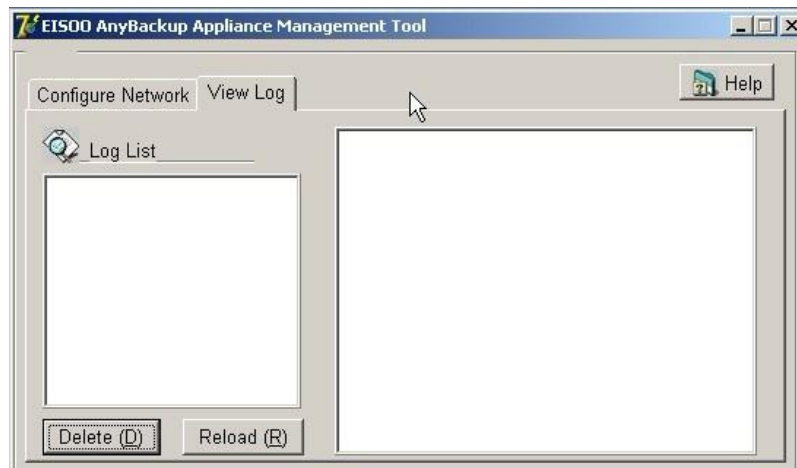


Figure 18 Log Interface

In “View Log” page, one file or multiple files can be viewed. [Delete] can be used to delete specified log. [Reload] can be used to reload all log files in log file folder.

Steps:

- Switch to “View Log ” page;
- Click [Reload] to refresh log list;
- Select one log or several logs on the left side and content of specified files will be displayed. Click [Delete] to delete specified log.

Note: After configuration, close management tool of EISOO AnyBackup Appliance and login to management console by host IP to configure user, backup and restore, etc.

3.1.4 Uninstall

EISOO AnyBackup Appliance Management Tool can be uninstalled by “Add/Remove Programs” in control panel.

3.2 iSCSI Client

iSCSI client is such a free iSCSI program software provided by Microsoft to search and connect iSCSI target device, including **Microsoft iSCSI Initiator** and **iSCSI monitor service**. Admin can manage storage space provide by EISOO AnyBackup Appliance in iSCSI mode after installation of client.

3.2.1 System Requirement

iSCSI clients in the following two environments are supported by EISOO AnyBackup Appliance and system requirements are as follows:

Item	Required	Recommended
CPU	766 MHz	900 MHz or above
Memory	256 MB	512 MB or more

Required Free Space	500 MB	1 GB
OS	Windows 2000 SP4 or above, Windows Server 2003 SP1 or above, Windows XP SP2 or above	Windows 2003 Server SP2

Figure1 32-bit iSCSI Client

Item	Required	Recommended
CPU	766 MHz	900 MHz or above
Memory	256 MB	512 MB or more
Required Free Space	500 MB	1 GB
OS	Windows XP (64bit)	Windows Server 2003 SP2(64bit)

Figure 2 64-bit iSCSI Client

3.2.2 Installation Wizard

There are two ways to install iSCSI client:

◆ By Web

Step One: Input default link of EISOO AnyBackup Appliance in client browser address: <http://192.168.0.253:9800> (Default console address). Access console and click "more clients" to skip to client download page. Click "Windows iSCSI Client (32 bit)" or "Windows iSCSI Client (64 bit)" to pop up tips to download installation package.

Step Two: Download installation package to local disk and double click to install.

Step Three: Select installation items and click [Next] to enter license page. Select "I agree" and click [Next] to enter system update program.

Step Four: After update, click [Done] to finish installation of iSCSI client and iSCSI client icon will appear on the desktop.

◆ By Disk

Step One: Insert disk to drive and run iSCSI client installation package. Double click to enter installation program welcome page.

Step Two: Refer to step three and four in [By Web] to finish client installation.

3.2.3 Usage Instruction

After configuration of iSCSI volume in EISOO AnyBackup Appliance, installed iSCSI manager can be used to manage it as follows:

Step One: Click iSCSI Initiator icon to pop up the following dialog box.

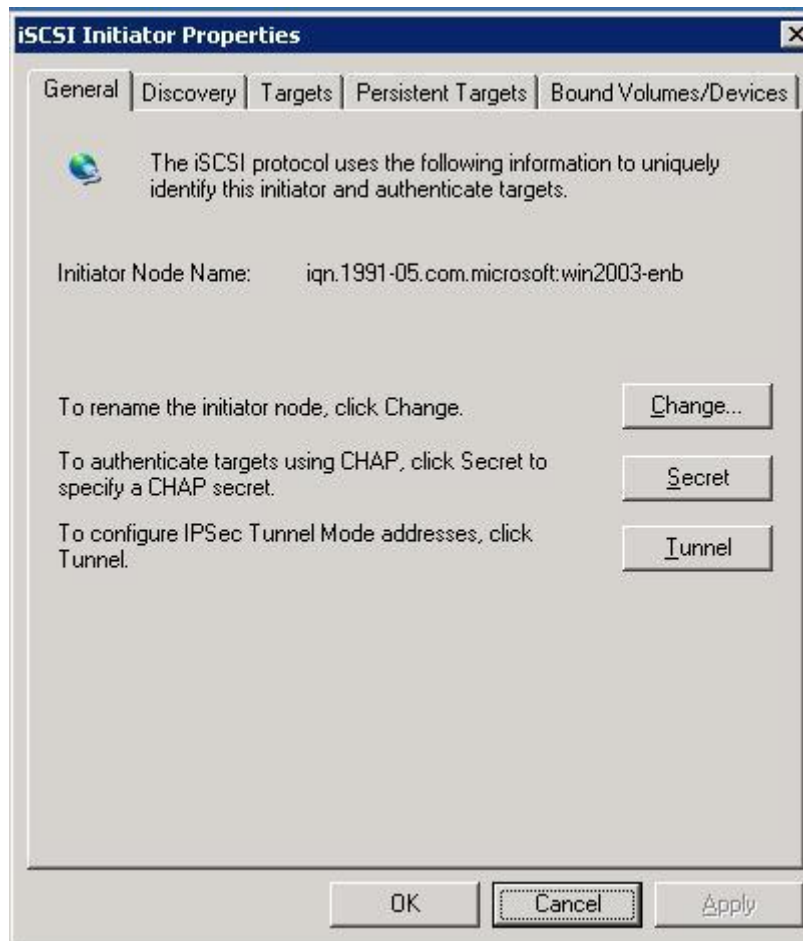


Figure 21 Login iSCSI Client

Step Two: Click "Discovery" to pop up the following dialog box.

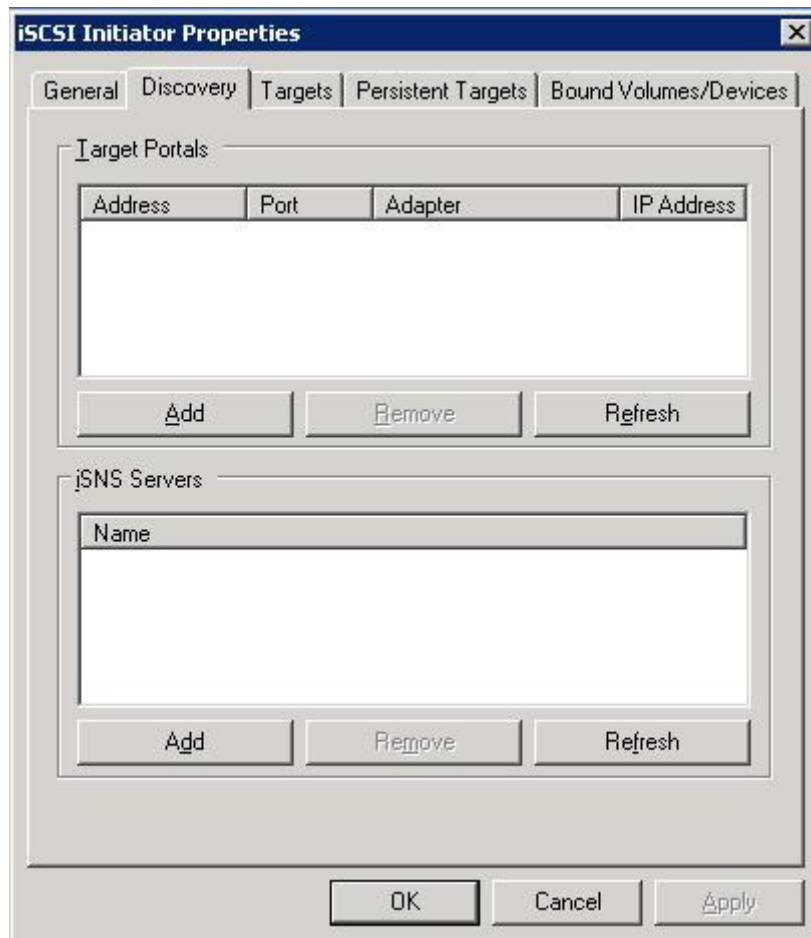


Figure 2 “Discovery” dialog box

- Click [Add] to add IP of EISOO AnyBackup Appliance with configured iSCSI volume, as shown in the following picture:

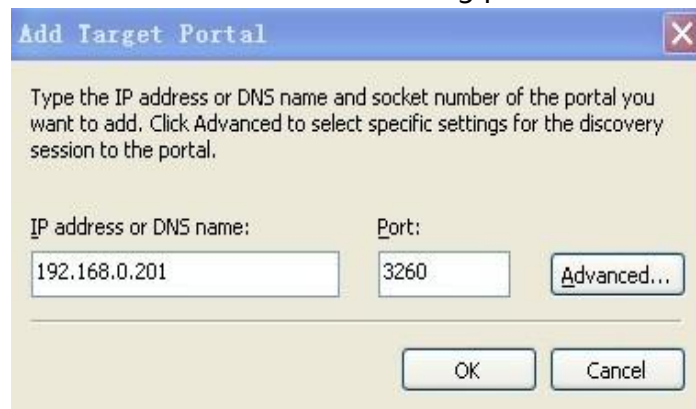


Figure 3 Add IP

- Click [OK] to save configuration.

Step Three: Click “Targets” to pop up the following dialog box.

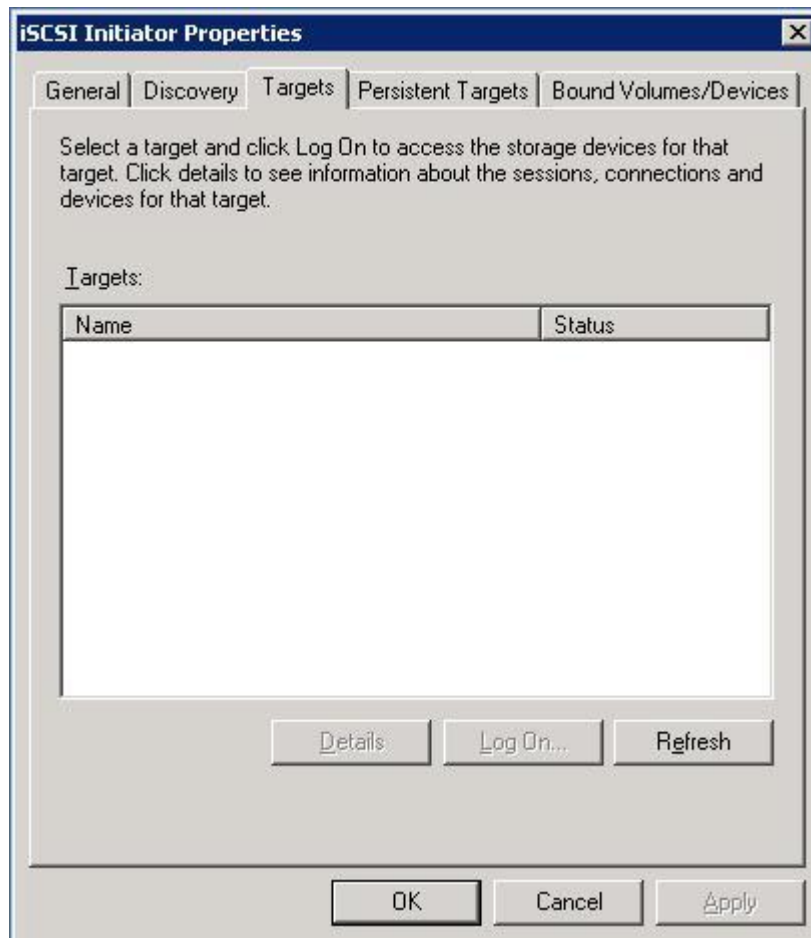


Figure 24 “Targets” dialog box

- Click [Log On...] to pop up the following dialog box.

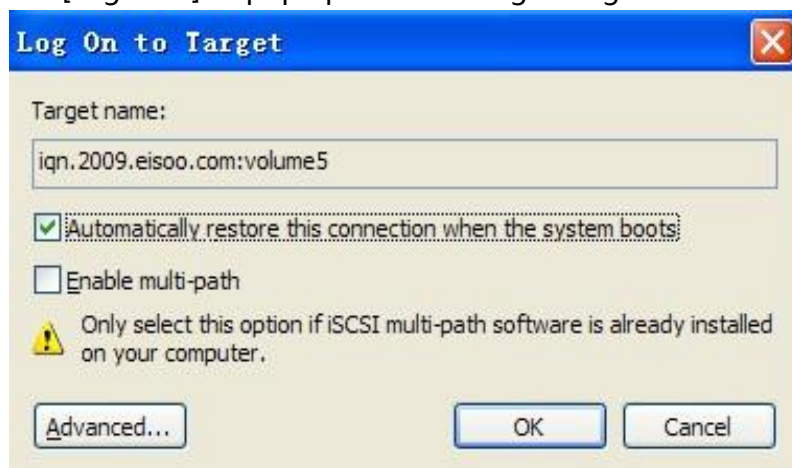


Figure 25 Activate iSCSI Volume

- ✓ Mark “Automatically restore this connection when the system reboots” as shown in figure 25 to enable reconnection when resarting/rebooting device.
- ✓ If you have modified user and password via “iSCSI target management/Modify Connected User” , click [Advanced...] and mark “CHAP logoninformation” check box as shown in figure 26.

Input info in “User name” and “Target secret” and click [OK]. If target secret value is right, you will login to target; otherwise login and authentication will fail.

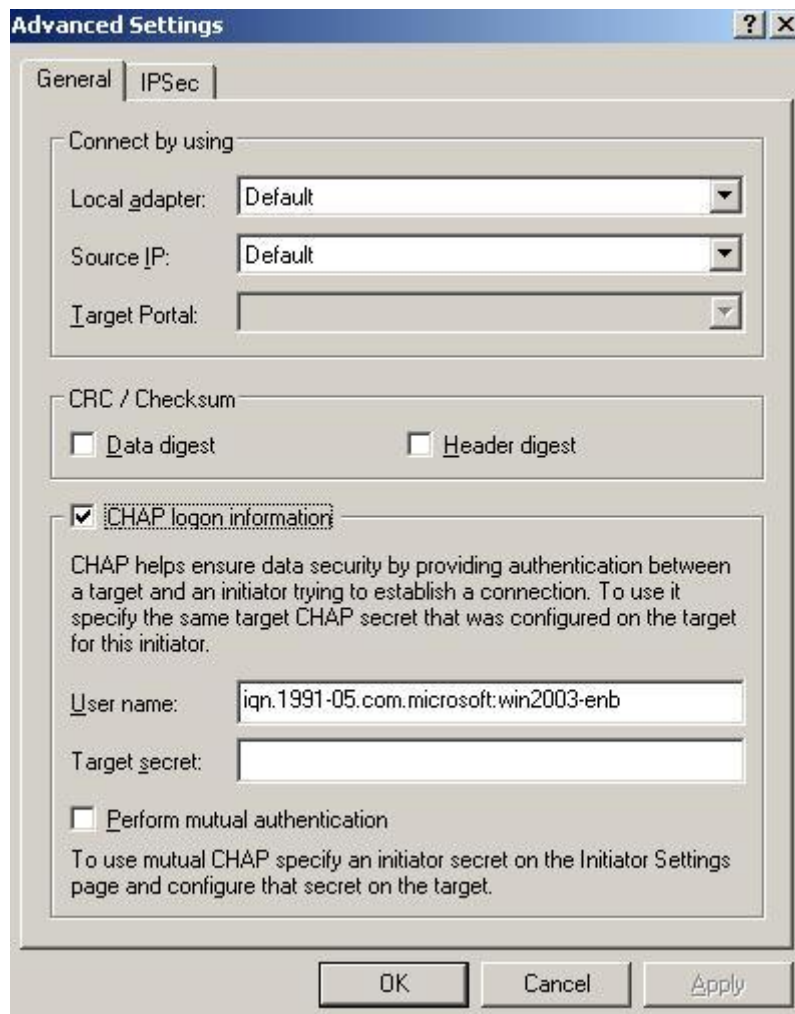


Figure 26 “Advanced Setteings” dialog box

- Click [OK] to save configuration.

Step Four: Right click “My Computer” and select “Manage” to enter corresponding page. Select “Disk Management” as shown in the following picture.

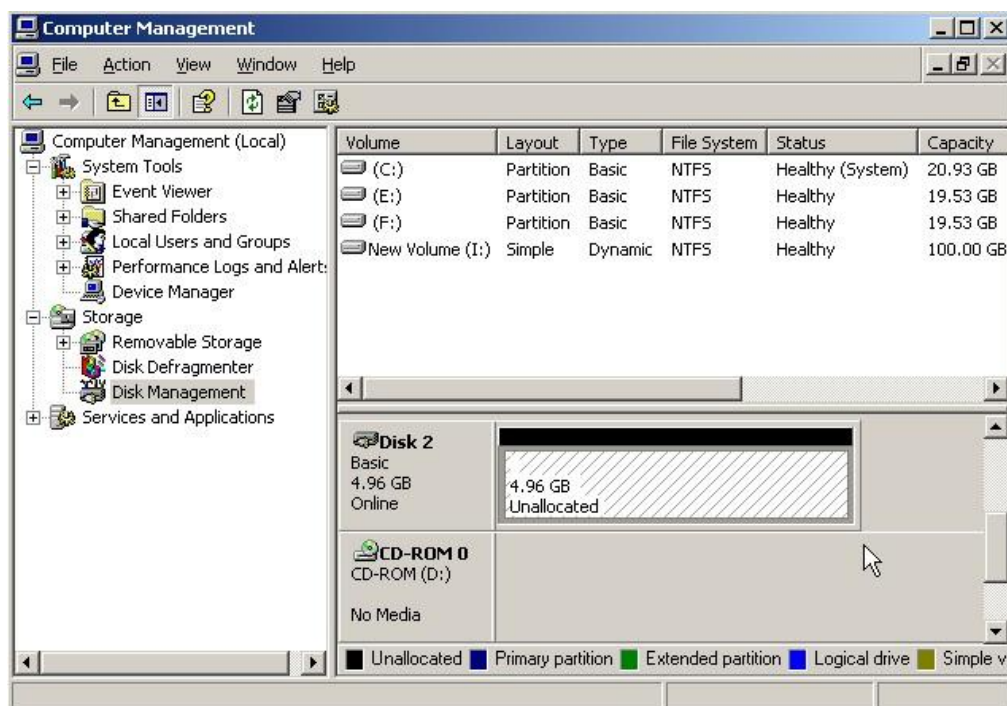


Figure 27 Login iSCSI Partition

Step Five: Right click created disk and select “Intialize disk” as shown in the following picture. Select “New Disk Partition” .



Figure 28 Intialize Disk

Step Six: Finish disk partition configuration according to wizard and configured disk partition can be seen in “My Computer” , that is, new volume and data storage can be executed in this volume.

3.2.4 Uninstall

In Windows desktop, enter “Start/Control Panel/ Add or Remove Programs” to select “Microsoft Initiator” and click [Delete] to uninstall iSCSI client.

3.3 LDAP Assistant

LDAP assistant can be deployed on Windows AD to realize seamless authentication based on Windows AD.

3.3.1 System Requirement

Item	Required	Recommended
CPU	900 MHz	1.2GHz or above
Memory	512 MB	1GB or more
Required Free Disk	5GB	20 GB

OS	Windows XP or above	Windows Server 2003
----	---------------------	------------------------

Figure 29 LDAP Assistant System Requirements

3.3.2 Installation Instruction

LDAP assistant can be installed via installation package as follows:

Step One: Enter Windows client to install LDAP assistant to start installation program of EISOO AnyBackup 3.5 Appliance and select default language to enter installation program-initial page.

Step Two: Click "Auxiliary Module" to select [LDAP Assistant] and click [Install].

Step Three: Enter "Installation Program-EISOO AnyBackup Appliance LDAP Assistant" and click [Next]. Read "EISOO End User License" and select [I agree]. Click [Next] to continue.

Step Four: In page to select installation file folder and click [Browse] to select installation path. Click [Next] to select other options such as shortcut, ect. Click [Install].

Step Five: After installation, click [Done] to return to installation page of other modules.

3.3.3 Configuration

After installation of LDAP assistant, click [Start] >> [All Program] >> [EISOO AnyBackup 3.5 Appliance] >> [LDAP Assistant] >> [LDAP Assistant Configuration] to pop up a configuration dialog box. LDAP assistant can connect to multiple management consoles.

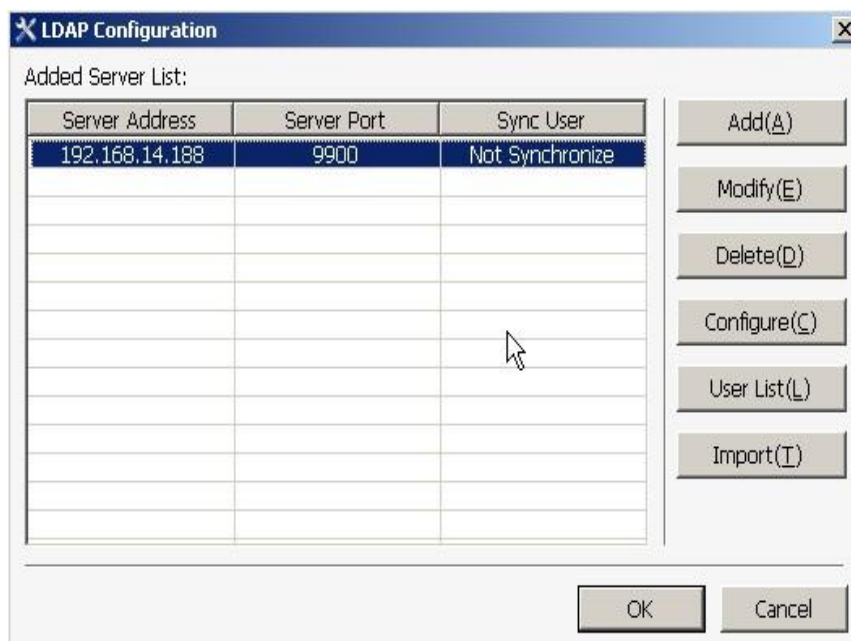


Figure 30 Configuration Interface

Click [Add] to pop up the following dialog box and input server address to connect, admin password, default port "9900" . Admin account is "admin" .

Figure 4 Add Server

3.3.4 Uninstall

◆ [Uninstall by System]

In Windows desktop, enter [Start/Control Panel/Add or Remove Program] and select [LDAP Assistant]. Click [Delete] to uninstall LDAP assistant.

◆ [Uninstall by EISOO AnyBackup Appliance]

In Windows desktop, select [Start/All Programs/EISOO AnyBackup 3.5 Appliance/LDAP Assistant] and click [Uninstall LDAP Assistant] to pop up a dialog box. Click [Yes] to uninstall LDAP Assistant.

3.4 Windows Client

Windows client is installed in server or PC that needs backup under Windows 2000 or higher edition system. It responds to demands from Management Console and provides backup and restore. Followed are the detailed system requirements, installation, and configuration and uninstall of Windows client.

3.4.1 System Requirements

Item	Required	Recommended
CPU	900 MHz	1.2GHz or above
Memory	512 MB	1GB or more
Required Disk Space	5GB	20 GB
OS	Windows Server 2003 or above/ Windows XP (64bit) or above	Windows Server 2003 以 /Windows Server 2008

		(64bit)
--	--	---------

Figure 5 Windows Client Requirements

There are three kinds of windows clients for installation, configuration and uninstall: normal client, deamon client and secure client. There are two ways to install: install by web and local install.

3.4.2 Install by Web

Login to management console and click links under login to download required Windows client and the following warning will pop up: Do you want to run or save this file? Click [Run] to install windows client.



Figure 33 Install by Web

3.4.3 Normal Client

◆ Installation

Step One: Enter windows client and start EISOO AnyBackup 3.5 Appliance installation program. Select language and click [Next] to continue.

Step Two: In the prompt "Installation Program-Initial Pge", click "Install Client" to enter [Installation program-Select Modules] and select [Backup Client]. Click [Install].

Step Three: Decompress installation package and pop up installation wizard. Click [Next] to read "License" and select [I agree]. Click [Next] to continue.

Step Four: Select client type: Normal Client and click [Next] to continue.

Step Five: Program will be installed to C : \program files\Eisoo Backup Storage Appliance\3.5 Client\ by default. Click [Browse] to change installation directory and click [Next] to continue.

Step Six: In [Backup Server] page, you should set IP of backup sever installed EISOO AnyBaackup 3.5 Appliance management console, thus client info can be written to management console automatically. Select [Use default server address]

and default IP and port: 127.0.0.1:9900 will be selected. Click [Next] to continue.

Step Seven: In [Client Service] page, select user for client service, which will decide local resource that this client can access to.

Step Eight: Installation page will pop up. Click [Install] to start client installation to specified user.

Note: After successful installation of client, login to management console as admin and enter "Client" window to view installed client in client list.

◆ Uninstall

There are two ways to uninstall windows client of EISOO AnyBackup Appliance:

➤ [Uninstall vis System]

In Windows desktop, click [Start/Control Panel/Add or Remove Programs] to enter uninstall interface. Select [EISOO AnyBackup 3.5 Appliance] and click [Delete] to pop up a dialog box. Click [OK] to delete Windows client.

➤ [Uninstall via EISOO AnyBackukp Appliance]

In Windows desktop, select [Start/All Programs/EISOO AnyBackup 3.5 Appliance Client/Uninstall Client] to pop up a dialog box. Click [OK] to uninstall client.

3.4.4 Secure Client

◆ Install

Installtion of secure client is the same as that of normal client. In client type, select [Secure Client].

◆ Configuration

After successful installation of secure client, login to management console and bind secure client with one user. Login by this user and input username and password of machine where secure client installed to activate secure client. Click [OK] to bind user with this secure client successfully. Click [Cancel] to return to homepage.

◆ Uninstall

➤ [Uninstall by System]

In windows desktop, click [Start/Control Panel/Add or Remove Program] to enter uninstall interface. Select [EISOO AnyBackup 3.5 Appliance Client] and click [Delete]. In prompt dialog box, click [OK] to delete windows client.

➤ [Uninstall by EISOO AnyBackup Appliance]

In Windows desktop, select [Start/All Programs/EISOO AnyBackup 3.5 Appliance Client/Uninstall Client] to pop up a dialog box. Click [OK] to uninstall client.

3.4.5 Daemon Client

◆ Installation

Installation of daemon client is the same as that of normal client. In [Client Type], select [Daemon Client].

◆ Configuraiton

Daemon client is forced client, which can be uninstalled only via management console.

In configuration page, click [Uninstall Password] to pop up a dialog box. In “Uninstall Daemon Client Password” dialog box, select [Set Uninstall Password] to input password and click [OK] to save configuration.

◆ Uninstall

Uninstall of daemon client, restart client installation package and select uninstall to pop up password verification dialog box. Input password and click [OK] to uninstall client or [Cancel] to return.

3.5Linux Client

Linux Client is deployed on Linux platform to protect data of Linux system. It responds to commands from Management Console and provides data backup functions, including file backup and Oracle backup. Current Linux Client only supports Daemon Client.

3.5.1 System Requirements

Item	Required	Recommended
CPU	1GHz	2G or above
Memory	1GB	2GB or more
Required Free Space	28MB	50MB or more
OS	RedHat Linux Enterprise 4	RedHat Enterprise Linux 5(32/64bit) or above
NIC	100M	1000M
Browser	None	IE 8.0 or Firefox 2.5

Figure 6 Linux Client Requirement

3.5.2 Installation

You can get installation package of Linux client by two ways: 1) Access to EISOO AnyBackup Appliance page by web and download Linux client to local. 2) Decompress installation package and find corresponding installation package of

Linux client in EISOO Backup Storage Appliance \Setup to install in the following steps:

Step One: Copy compressed file client.tar.gz of Linux client installation package to Linux environment to directory opt.

Step Two: Enter directory opt via cd opt command.

Notice: If protected object is Oracle, use su – oracle to switch to Oracle user and make oracle user have read and write right to directory that installation package locates, then decompress.

Step Three: Decompress installation package by tar -xzf: AnyBackup_client_rht4.tar.gz, after compression, folder AnyBackupClient will appear in directory eisoo.

Notice: If protected object is Oracle, after decompression use su root to switch to root user and make root user have oracle environment variables to execute installation. Please install after user switch.

Step Four: Enter file folder **AnyBackupClient** via command **cd AnyBackupClient** and run installation program via command **./install.sh**.

Step Five: Select default language, including Simplified Chinese, English and Traditional Chinese and continue.

Step Six: Input console IP and continue.

Step Seven: Select user type and only user, Oracle, Sybase, MySQL are optional. Select corresponding type and continue.

Step Eight: It will notify whether to install trans.ko, which is used for disaster recovery. If disaster recovery is necessary, install and continue.

Step Nine: All the selected options will be showed. Verify info and continue.

Step Ten: After installation, check whether client is normally installed via command **ps -e|grep eng** and all the above operation can be shown as follows:

```

[root@qey opt]# ls
a AnyBackupClient AnyBackup_client_3_5_8.tar.gz AnyBackup_client_rht4.tar.gz b debug
[root@qey opt]# cd AnyBackupClient/
[root@qey AnyBackupClient]# ./install.sh
*****
* Welcome to Install Eisoo AnyBackup 3.5 Client
*****

SELinux is Disabled.
Check root permission: OK
SELinux is Disabled.
Check environment: OK
(1) Select Install Language:
    [ (1)zh_CN | (2)en_US | (3)zh_TW_CN]
    Please input your select: 1
(2) Please Input Console IP Address:
10.10.1.212
(3) Select Database User For Installation:
    [ (1)no need(root) | (2)oracle | (3)sybase | (4)mysql]
    Please input your select: 1
(4) If you need to use disaster recovery, you should install trans.ko .
    Would you make and intall trans.ko ?
    [ (1)yes (2)no]
    Please input the number you select:1
*****
* (1) Installation Language type:      [zh_CN]
* (2) Console IP Address:              [10.10.1.212]
* (3) Database User For Installation:  [root]
* (4) make and intall trans.ko? :      [yes]
*****
Install ? y(yes) /n(no and quit)y

```

Figure 35 Linux Client

3.5.3 Uninstall

Step One: Login to Linux server and stop running client.

Step Two: Enter directory **AnyBackupClient** after client decompression via command. **/uninstall** to uninstall automatically.

Step Three: Delete client file: **rm -rf /usr/local/AnyBackupClient**.

3.6 System Recovery Environment

System Recovery Environment runs independently. It is utilized to initiate System Recovery Wizard to finish Operating System Recovery when it fails to start, and it is an indispensable module in system backup.

Provided by EISOO AnyBackup 3.5 Appliance, System Recovery Environment can run independently in hard disk, CD and USB device, which simplifies the operation of system recovery. The operation of system recovery is very easy for it is based on graphical interface; it also supports direct access through LAN, which helps enterprises and organizations to execute centralized backup and restore.

3.6.1 System Requirement

Item	Required	Recommended
CPU	900 MHz	1.2 GHz or higher
Memory	512 MB	1 GB or more
Required Disk	200 MB	400 MB or more

3.6.2 Installation

Step One: Login to Windows operating system and start EISOO AnyBackup 3.5 Appliance setup file.

Step Two: Click **[Install Auxiliary Modules]**, and choose **[System Recovery Environment]** to install.

Step Three: Enter **[System Recovery Environment --- Installation Wizard]**, click **[Next]**, select installation location and click **[Next]** to continue.

Step Four: In **[Select Default Language]** page, select language and click **[Next]** to continue.

Step Five: In the page **[Edit Menu Item Name]**, input a name (default name is EISOO System Recovery) and click **[Next]** to start installation.

Step Six: Now, install wizard shows it is copying file, and System Recovery Environment is installed in local hard disk.

Step Seven: After finishing copy, a message displays and click **[Finish]** to quit install wizard.

Chapter 4 Centralized Management

This chapter will introduce how to manage EISOO AnyBackup Appliance via Web. The following several kinds of management are provided by EISOO AnyBackup Appliance: Centralized management, backup and restore based on management console, disaster recovery, system, storage based on media server and device management. Centralized management via interface and root node will be introduced in details in this chapter.

4.1 Homepage

4.1.1 Management Console

Homepage here refers to that of management console, including product, enterprise, client risk status and client information. Login to management console of EISOO AnyBackup Appliance and click “Management Console” node on the left as shown in the following picture:

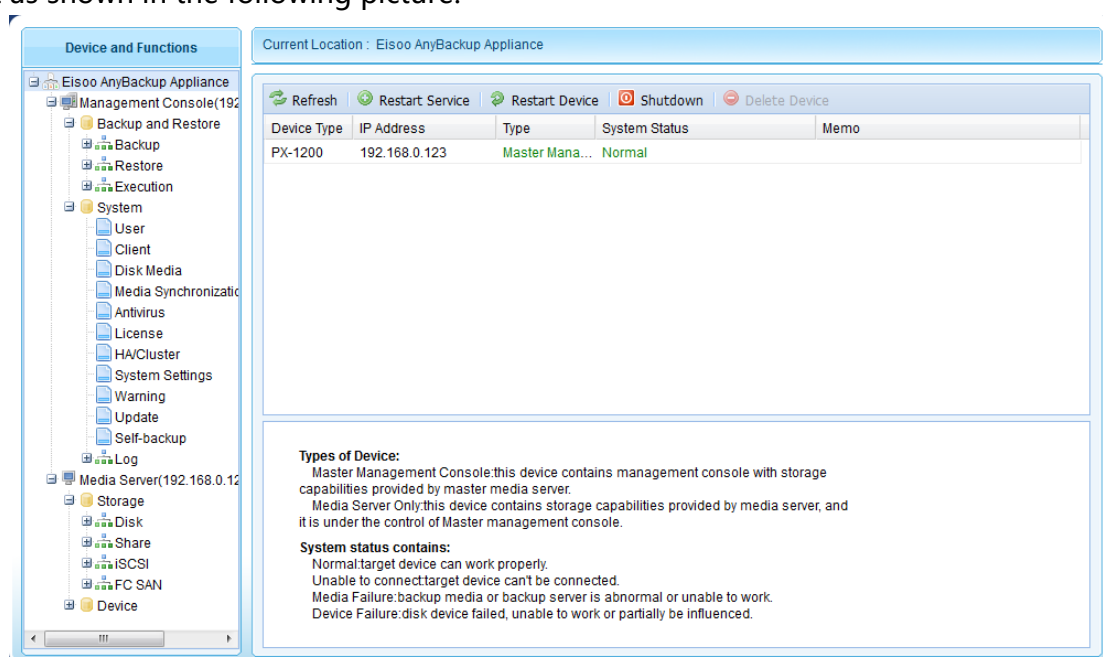


Figure 37 Management Console

4.1.2 Media Server

Homepage here refers to that of media server, displaying system, disk, RAID and storage status of media server. Login to EISOO AnyBackup Appliance and click “Media Server” on the left as shown in the following page:

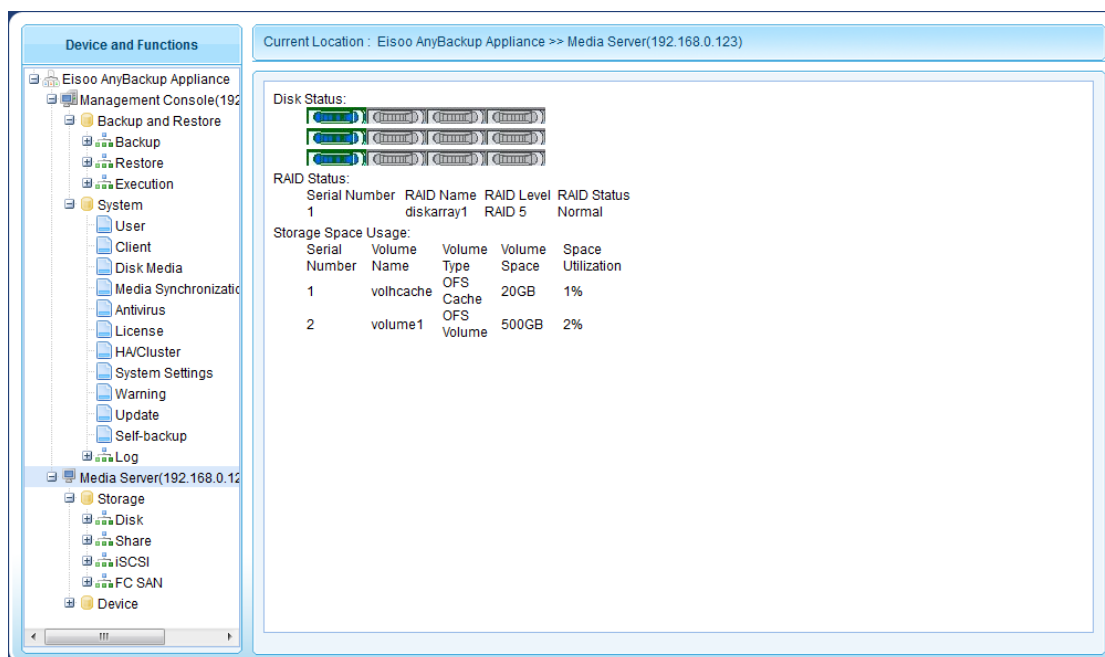


Figure 38 Media Sever

4.2 Operation

For centralized management of backup device, AnyBackup Appliance provides one interface for multiple devices. Login to EISOO AnyBackup Appliance and the interface prompt is the centralized management page, or click root to enter corresponding page. Device model, IP and system status will be displayed only when login as admin as shown in the following picture:

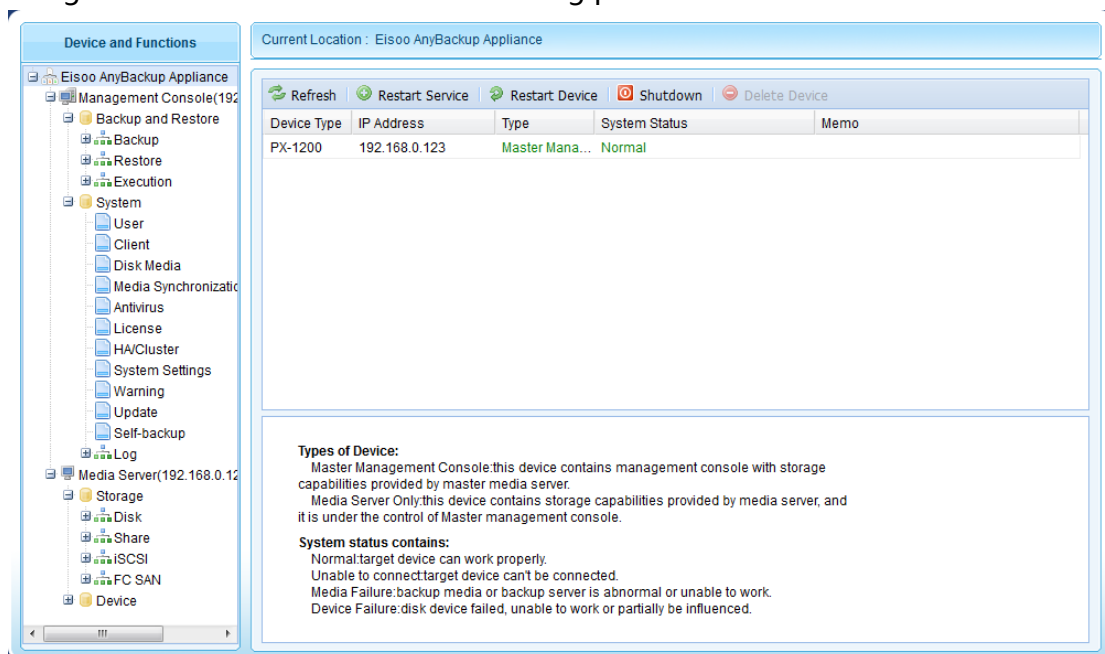


Figure 39 Cnetralized Management

◆ Refresh

Click [Refresh] to update the latest status of device.

◆ Restart Service

Select device to restart service and click [Restart Service] to pop up a dialog box: "Are you sure to restart all service of selected device?"

- Click [Yes] to restart service.
- Click [No] to return.

◆ **Restart Device**

Select device to restart and click [Restart Device] to pop up a dialog box: "Are you sure to restart selected device?"

- Click [Yes] to restart selected device.
- Click [No] to return.

◆ **Shutdown Device**

Select device to close and click [Shutdown Device] to pop up a dialog: "Are you sure to close selected device?"

- Click [Yes] to close selected device.
- Click [No] to return.

Chapter 5 System Management

5.1 Login to Management Console

Management console is a browser-based operation and management interface for management of user, data and client or backup and restore. User can be divided as “admin” and “user” ; admin can create account and password for common user.

User can Login to Management Console Web interface by corresponding path such as <http://192.168.0.253:9800>, input account and password and select default language for login. Meanwhile, you can choose whether to save user Login information; if so, you can Login directly to this computer next time.

Administrator can login to Management Console and create user, distribute users backup space, appoint storage path, check backup schedule of agents, execution status and execution log, create and manage backed up data and restore data through Web. After login, users will find the following buttons on tab bar: Home, Backup, Restore, Executions, Logs, Report and Configurations.

Common user can login to Management Console to check scheduled job, storage space status, back up log, create and manage backup data and store data. After login, users will find the following buttons on tab bar: Home, Backup, Restore, Executions, Logs and Configurations.

5.2 User Management

Every user should obtain a username first and then Login to Management Console to backup and restore data of authorized client. Login to Management Console as administrator, click [**Configuration**] > [**User**], and you can create User/Group in batch mode, Modify user/user group, Delete user/user group, and permission management.

In EISOO AnyBackup Appliance, user info includes:

- **Username:** username is used for login to Management Console and execute backup and restore in authorized client.
- **Description:** Note while creating user.
- **User Type:** Type of user.
- **Status:** Status of user.
- **Authentication:** As to authentication type of user login, Based on Password is available.
- **Free Space:** Free space for this user.
- **Used Space:** Used space by this user.

- **User Group:** The group user belongs to.

5.2.1 Create and Manage User

Login to management console as admin and click “System Management /User” to switch to user management window.

◆ Create User

Click [New] to input username, description, usergroup, authentication type and 点 space limit in the prompt dialog box as shown in the following picture:



Figure 40 Create User

The following three authentication type will be listed in the drop-down list:

- **Based on Password:** Default password is 123456 and it can be modified once login as this new user.
- **Based on USB-Key:** Insert USB-Key and bind it with this user.
- **Based on Password and USB-Key:** Insert USB-Key and bind it with current user. After successful binding, insert USB-Key and input user password (123456 is default) during login.

◆ Modify User

Select a user and click [Modify] to pop up a dialog box, in which description, user group, authentication type and space limit can be set. Click [OK] to finish modification.

◆ Delete User

Select one user and click [Delete] to pop up a dialog box. Click [Yes] to delete user or [No] to cancel.

Note: During user modification, domain user also supports authentication type modification.

◆ Import Domain User

Before importing domain user, make sure LDAP assistant has been installed. In the prompt "Import Windows Standard User" dialog box, select one user in windows domain user list and click [Yes] to finish domain user importing.

◆ **Enable**

If one user is disabled, select the user and click [Enable] to resume.

◆ **Disable**

If you want to disable one user, select the user and click [Disable].

5.2.2 Create and Manage User Group

Login to management console as admin and click "System Management" >> "User" to switch to user management window.

◆ **Create User Group**

Create new group to manage user in the same department.

Click [New] and input a group Name and Description in pop-up dialog box [New Group Info]. Select user in [Unverified List], click >> or << to move appointed User. At last click [OK] to finish as shown in the following picture:

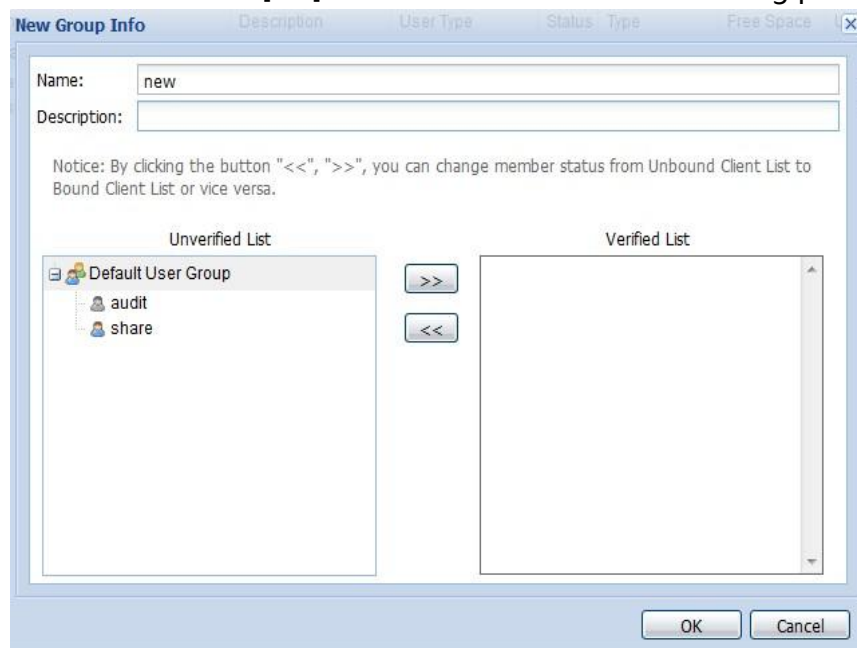


Figure 41 Create User Group

◆ **Modify User Group**

Modify the group name, description and attribution of the group member.

Choose one group, click [Modify] and modify relevant information in the dialog box [Modify Group Info]. You also can click >> or << to change the distribution of users. Finally, click [OK] to finish modifying group.

◆ **Delete User Group**

Click "System Management" >> "User" and enter corresponding page. Select user group to delete and click [User Group]. Select [Delete] in drop-down list to pop up a dialog box. Click [Yes] to delete or [No] to cancel.

Select a user group and click [Enable] or [Disable] to enable or disable the whole group.

5.2.3 Authorization

Authorize current user to back up appointed data and read & write data of appointed media.

◆ Client Authorization

Select specific user and click [**Authorization**], in the pop-up dialog box page of [**Client Authorization**], you can authorize user by moving client from Unauthorized Client List to Authorized Client List. Also you can change the configuration by clicking button of "<<" or ">>" or vice versa. Click [OK] to finish as shown in the following picture:

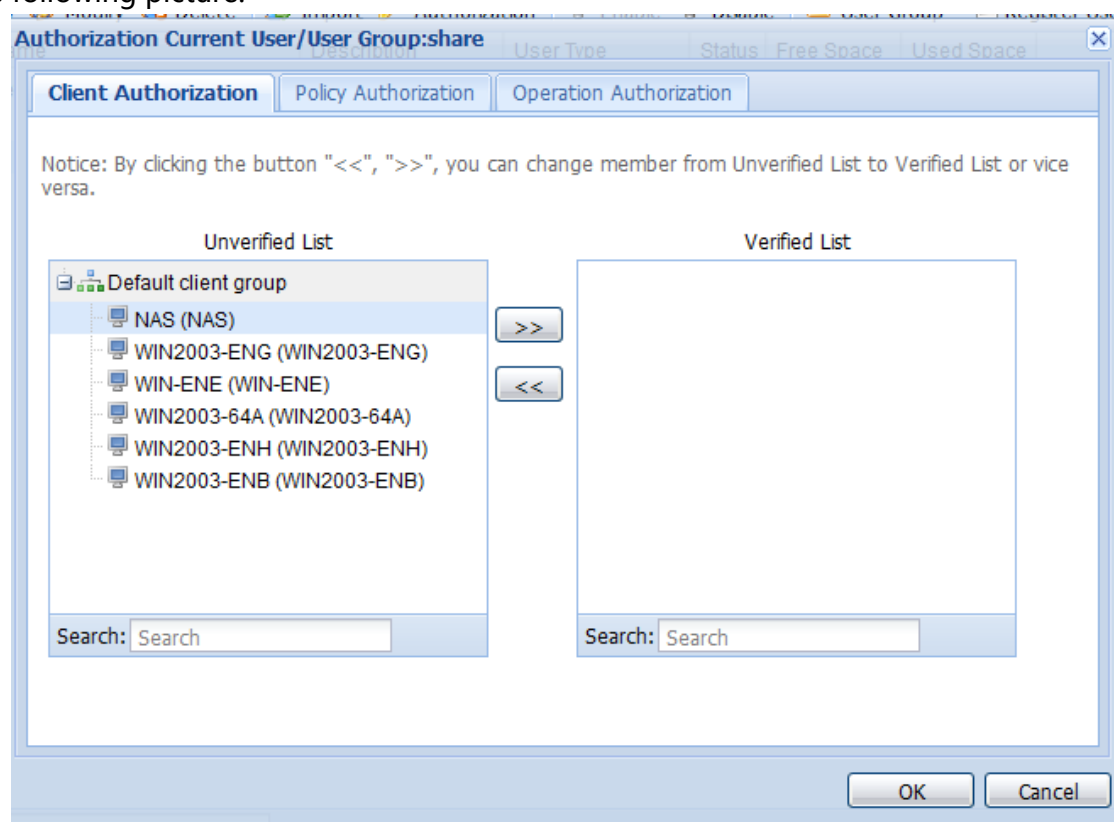


Figure 42 Client Authorization

◆ Policy Authorization

The left column is unauthorized Policy. Client Policy authorization can be changed via "<<" or ">>". Click [OK] to finish Policy authorization.

◆ Operation Authorization

It is used to authorize user with specific operation access such as backup, recovery, execution, log checking and so forth. Click "<<" or ">>" to change operation authorization.

5.2.4 User Space Quota

Click "System Management" >> "User" >> "New" or Click "Modify" to modify user quota space.

In space quota, default is no limit for user space. You can input specific value for user space limit (Decimal point can be used.) Click [OK] to finish user space quota.

Note: "Audit" does not support quota space management and it will be gray and unusable for "space limit" .

5.3 Client Management

Administrator can group all current clients, modify client group property, delete unnecessary client/group, bind user for secure client, appoint current client to backup certain databases, and provide upgrade function for remote client.

5.3.1 Client Group

Login to client group and click "System Management" >> "Client" to pop up corresponding window.

◆ **Refresh**

Refresh the page and display information of the client group.

◆ **New**

Click [New] to create client group.

◆ **Modify**

Click [Modify] to modify name and description of client group (the same as user group).

◆ **Delete**

Select a client group and click [Client Group]. Select [Delete] in drop-down list to pop up a dialog box. Click [Yes] to delete client group.

5.3.2 Client Configuration

Login to management console and click "System Management" >> "Client" to pop up corresponding window. Click [Configure] to pop up the following dialog box:

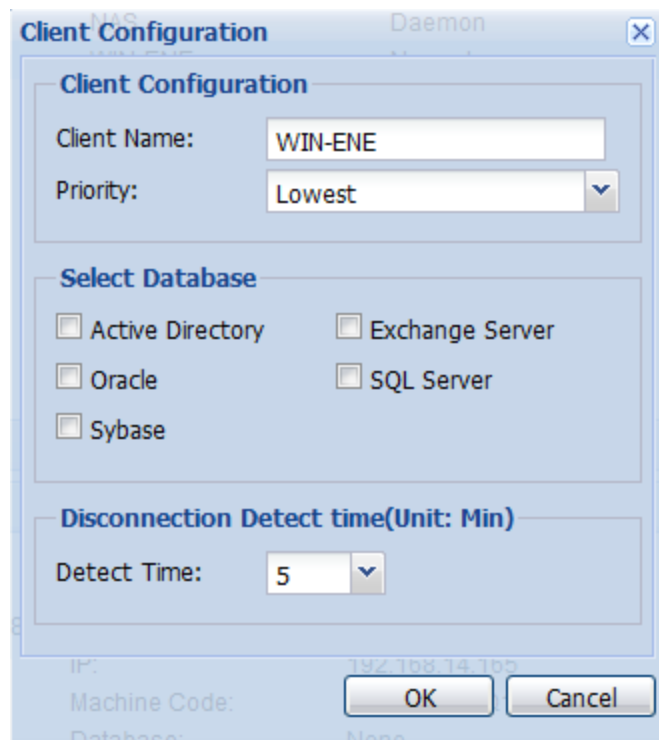


Figure 43 Client Configuration

◆ Priority

Client priority refers to execution sequence order of clients.

Select on client/client group and click [Configure] to pop up “Client Configuration” dialog box. In the drop-down list of priority, there are five levels: Lowest, Low, Common, High and Highest.

◆ Select Database

EISOO AnyBackup Appliance provides many databases and AD for users and specific database can be appointed for current client/client group for backup.

Note: If client group is selected, configuration will be applied to all the clients in the client group.

5.3.3 Delete Client

After deletion of selected client, this client will not be displayed in both authorized and unauthorized list. When it reconnects to management console, server IP should be set and tested (Please refer to [Windows Client Instruction]/[Set Backup Server IP] for details.)

Enter “Client” window and select a client to delete. Click [Delete] to read prompt info and click [Yes] to finish deletion.

5.4 Disk Media Management

“Disk Media” page provides management and operation platform for multiple media server in EISOO AnyBackup Appliance. After installation of subordinate media server and master media server on management console, admin can add other

media for storage of backup media modify or delete unnecessary media (media server), distribute storage space for specified media.

5.4.1 Media Operation

◆ Add Media

Add new media in selected media server and the following info will be necessary:

- **Server Name:** Select default media server or subordinate media server name.
- **Media Name:** Name added for this media server.
- **Media Type:** Traditional Media and OFS media are included.
- **Storage Path:** Path to save backup data on media server.
- **Media Space:** It is the max backup space of this media on media server. If backup data reached the max, new data cannot be written into corresponding storage path of this media.

Select a server and click [Add Media] to pop up [Add Media] dialog box as shown in the following picture. Input media name, media type, storage path and media space. Click [OK] to finish.

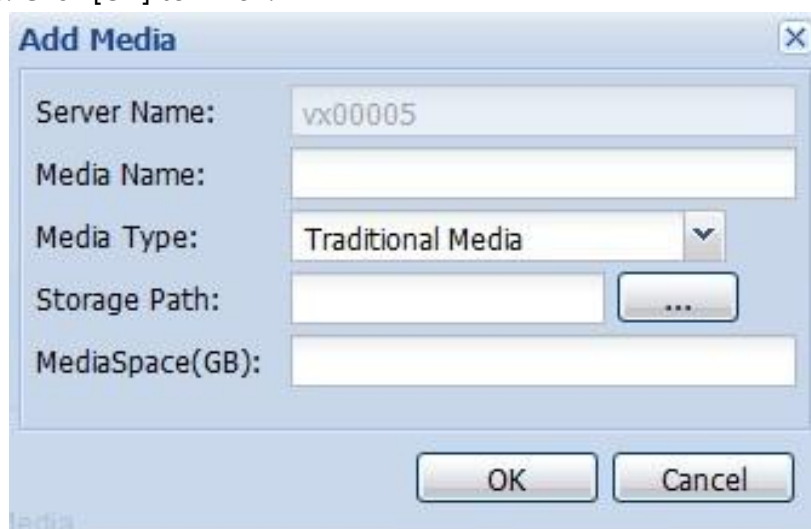


Figure 44 Add Media

◆ Delete Media

Select one media and click [Delete Media]. Read prompt info and click [Yes] to finish.

5.4.2 Media Server

◆ Modify Media Server

Select one media server and modify configuration of this media server.

- **Server Name:** Name of media server set during installation of media server. It can be modified.

- **Storage Port:** Port which is used for work status switch between media server and other modules such as client switch. Default port is 9902 and it can be modified when necessary.
- **IP Address:** IP address for client to access to media server.

Select one media server and click [Modify Media Server] to pop up "Modification of media server info will lead to system restart. Do you really want to modify?" Click [Yes] to pop up [Modify Media Server] dialog box.

- Server name and storage path can be modified.
- Click [Add] to pop up "Add IP" dialog box. Input valid IP and click [OK].
- Click [OK] to finish media server modification.



Figure 45 Modify Media Server

◆ **Delete Media Server**

Select one media server and click [Delete Media Server] to pop up a dialog box. Click [Yes] to finish.

◆ **Configure Media Server Type**

Select one media server and click [Configure Media Server Type] to pop up a dialog box. In the drop-down list, select media server type: Media Server, Media Sync Server. Click [Save] to finish.

5.5 Media Synchronization

Media Synchronization is mainly used to synchronize backup data among media, which means to synchronize local latest data to appointed remote media server and realize remote disaster recovery. EISOO AnyBackup Appliance support backup data of one media synchronized to one or several media, but not among

media on the same media server.

Note: Before creation of media sync job, make sure remote media server has been deployed.

◆ Create Media Sync Job

Step One: Click “System Management” >> “Media Synchronization” to enter media synchronization page.

Step Two: Click [New] to pop up [New Media Sync Job] window as shown in the following picture:

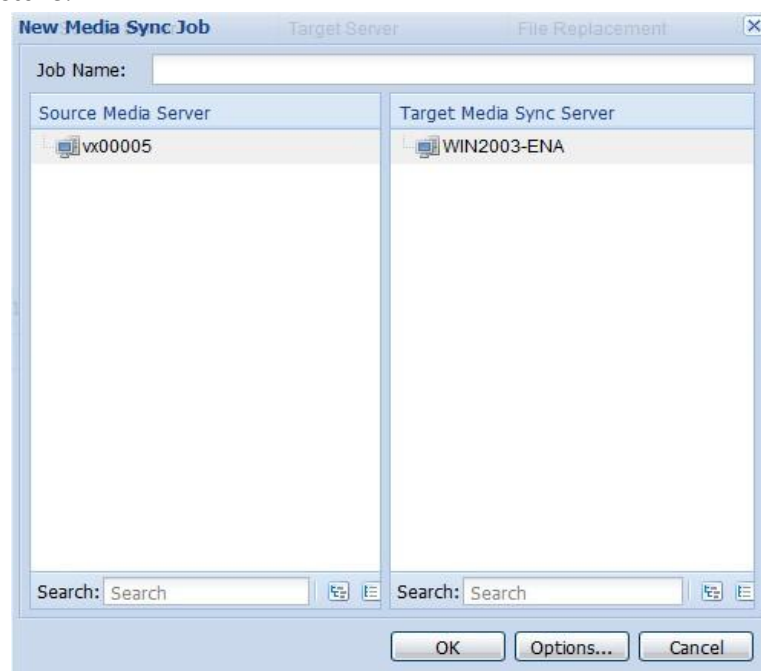


Figure 46 New Media Sync Job

Step Three: Input job name and select media in “Source Media Server” and “Target Media Sync Server” list.

- Click [Option] to select Network Retry, File Replacement and Gray Object and click [Save] to save modification or [Cancel] to keep default setting.

Step Four: Click [OK] to finish creation of media sync job or [Cancel] to return.

◆ Modify Media Sync Job

Step One: Select one sync job and click [Modify] to pop up “Modify Media Sync Job” dialog box.

Step Two: Job name, source media and target media can be modified in the window.

Step Three: Click [OK] to finish modification or [Cancel] to return.

◆ Delete Media Sync Job

Step One: Select one media sync job and click [Delete] to pop up the following dialog box:

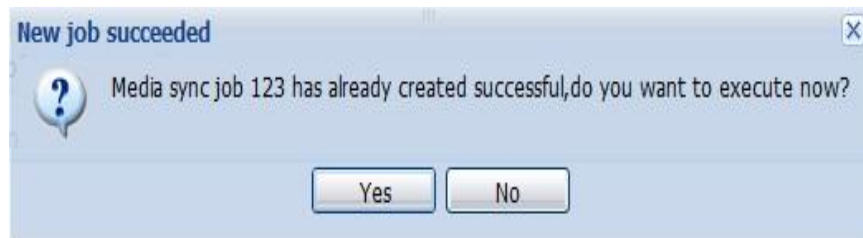


Figure 47 Operation Note

Step Two: Please read info carefully and click [OK] to delete or [Cancel] to return.

5.6 Tape Media Management

Admin can centrally manage tape media in this page, such as create, modify, delete or export tape media set, etc.

◆ Create Media Set

Click "Management Console" >> "System Management" >> "Tape Media" to enter tape media management page.

Step One: Click [New] to pop up the following dialog box:

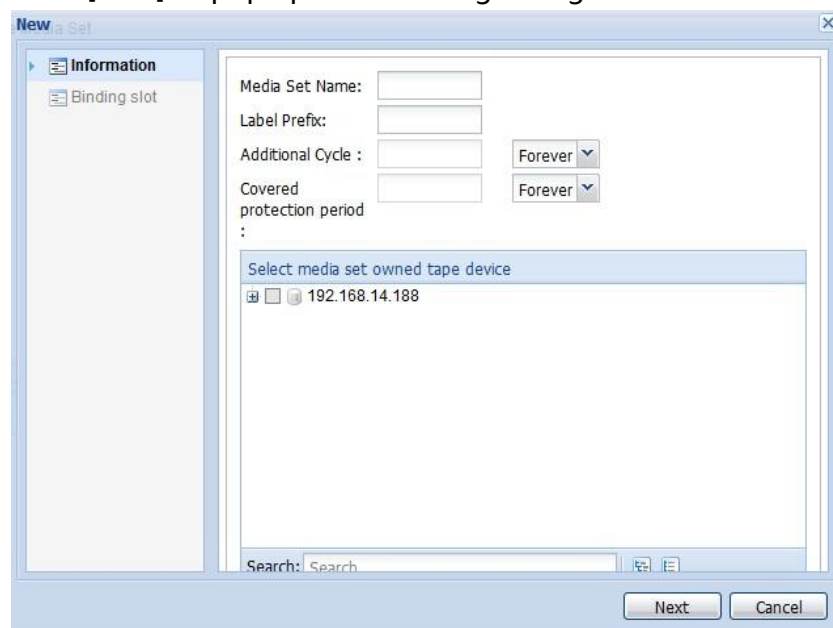


Figure 48 New Media Set

Step Two: In "Information" dialog box, input media set name, label prefix, and select tape device. Click [Next].

Step Three: In prompt "Binding Slot" dialog box, select slot and click [OK] to finish creation. If there is no free tape, corresponding info will pop up.

◆ Modify Media Set

Select media set and click [Modify] to pop up "Modify Media Set" dialog box. Media info and binding slot can be modified.

◆ Delete Media Set

Select media set and click [Delete] to pop up a dialog box. Click [Yes] to delete or [No] to return.

5.7 Antivirus

EISOO AnyBackup Appliance provides antivirus service, by which user can enjoy advanced security service. This chapter will introduce antivirus operation in details. Click “Management Console” >> “System Management” >> “Antivirus” to enter corresponding page.

◆ Scan Virus

Click [Scan Virus] to pop up corresponding dialog box. Select directory or files to scan and click [OK] to return to default page and start scanning; click [Cancel] to close the window and return.

◆ Stop Scan

Click [Stop] to pop up corresponding dialog box and click [Yes] to stop or [No] to return to default antivirus page.

◆ Update Virus Library

Click [Update] to pop up hint, click [Yes] to update virus library or [No] to cancel and return.

5.8 License

In EISOO AnyBackup Appliance, each client should be authorized to access management console. Enter management console and click “System Management” >> “License” to enter corresponding window, in which license can be added, deleted, online or manually activated, etc.

5.8.1 Add and Delete License

◆ Add License

Add license obtained from EISOO.

Click [License] and then click [Add]. In the dialog box [Add License], input license obtained from EISOO sales and click [OK] to finish adding.

Note: In all licenses from EISOO, basic license for [Management Console] should be added first, such as basic license.

◆ Delete License

Delete selected license. Select one license and click [Delete]. In prompt dialog box, select [Yes] to delete selected license.

5.8.2 Activate License

◆ Online Activate

EISOO AnyBackup Appliance provides free trial of 30 days, after which the software will be expired, thus official license should be purchased and activated for further usage.

Enter the page [License], select a license and click [Online Activate]. After activating successfully, the [Activation Status] will display as [activated].

◆ Manual Activate

In case of network failure, you can still activate the license by hand; detailed operations are as follows:

Click [Manual Activate] and input the license obtained from EISOO sales along with authentication code which is generated by license and your machine code. In the dialog box [Activate License Manually], input relevant authentication code and click [OK].

5.9 HA/Cluster

◆ Create Two-HA Binding

Click “Management Console/System Management/ HA/Cluster” to pop up corresponding page. Click [New HA Binding] to configure binding name, description, client in prompt dialog box. Click [OK] to bind successfully.

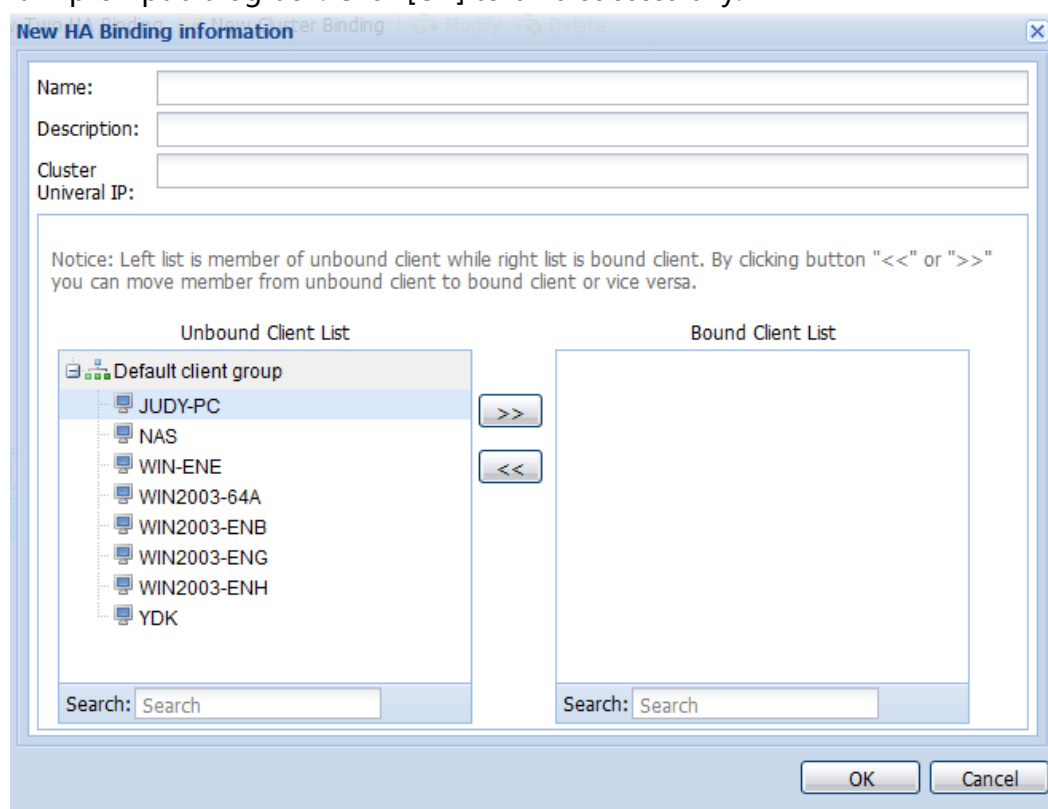


Figure 49 New HA Binding

◆ Create Cluster Binding

Click “Management Console/System Management/Two-HA/Cluster” to enter corresponding page. Click [New Cluster Binding] to input name, description, client, etc. Click [OK] to bind successfully.

◆ **Modify Binding**

Select bound two-HA or cluster group and click [Modify] to pop up the following dialog box. Input name, description and client in the prompt dialog box.

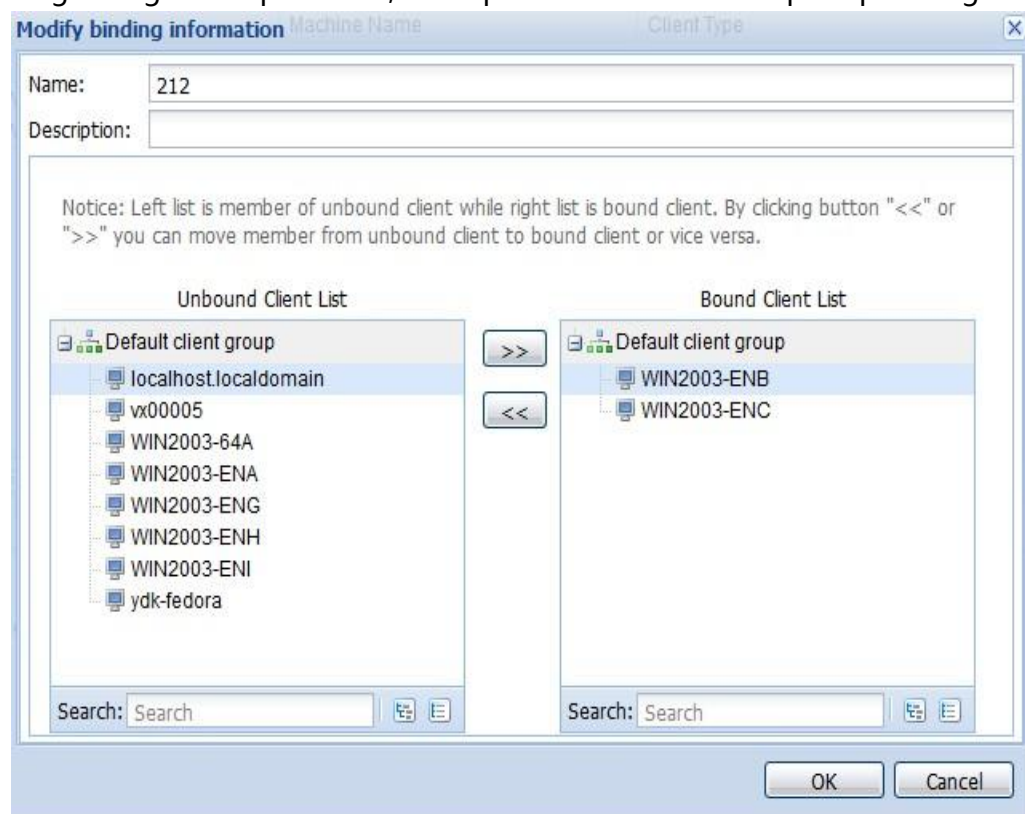


Figure 50 Modify Binding

◆ **Delete Binding**

Select bound two-HA/Cluster group and click [Delete]. Click [Yes] to delete in prompt dialog box or [No] to cancel.

Note: After deletion of binding, all info and binding backup job will be deleted.

5.10 System Configuration

Click “Management Console/System Management/System Configuration” to 点 pop up the following page:

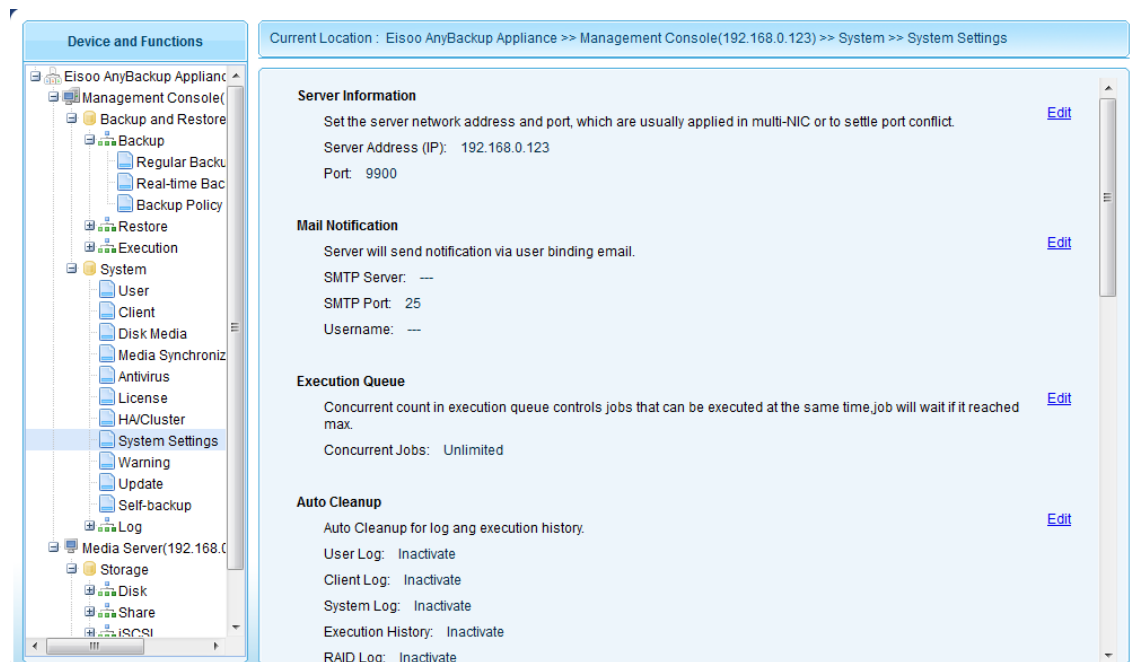


Figure 51 System Configuration

◆ **Server Information**

Configure Network Address and Port of Server. Click [System Configuration] > [Server Information] > [Edit], and change the network address and port of Server in dialog box [Modify Server Info; this is often applied to multi NIC environment and port conflict.

◆ **Mail Notification**

Mail Notification is used to configure the way of sending event notice to users' bound mails. Click [Email Notification] > [Edit], and configure SMTP Server, Port, Username and Password in pop-up dialog box.

◆ **Execution Queue**

Click [**Modify**] and configure the number of concurrent job.

◆ **Auto Cleanup**

Automatic cleanup is used to configure time period for log preservation. Click [Modify], and then you can decide to save User Log, Client Log, System Log and Execution History for two years, one year or half a year as your need.

◆ **Uninstall Password**

Click [Modify], choose to configure uninstall password or not in the prompt dialog box [Uninstall Password Management].

◆ **Forbid to Execute**

Click [Modify] on the right and set/modify/delete forbidden time in prompt dialog box.

- All executives in this period will be stopped, including executive scheduled to execute.

◆ Temporary Data Storage Path

Click [Modify] to set temporary data storage path in default media server on console and restore server in prompt dialog box.

- Notice: If path is unavailable or space is not enough, error may occur in default media server and restore server.

◆ Auto Creation of Shared Directory

Click [Modify] to pop up “Modify Auto Creation of Shared Directory” dialog 点击 box and set whether auto create shared directory when creation or importing users.

◆ Node Configuration

It is used to connect EISOO AnyBackup Appliance to EISOO Tx3 Cloud.

◆ Node Public IP

If node locates in LAN, a public IP can be set and authorized media sync server can connect to this node via public IP.

5.11 Warning

Email, sound and remote mail warnings are included in warning, which aim to send warning to system administrator via email or sound. Warning includes disk offline, disk failure, etc. Click “System Configuration/Warning” to enter the following page:

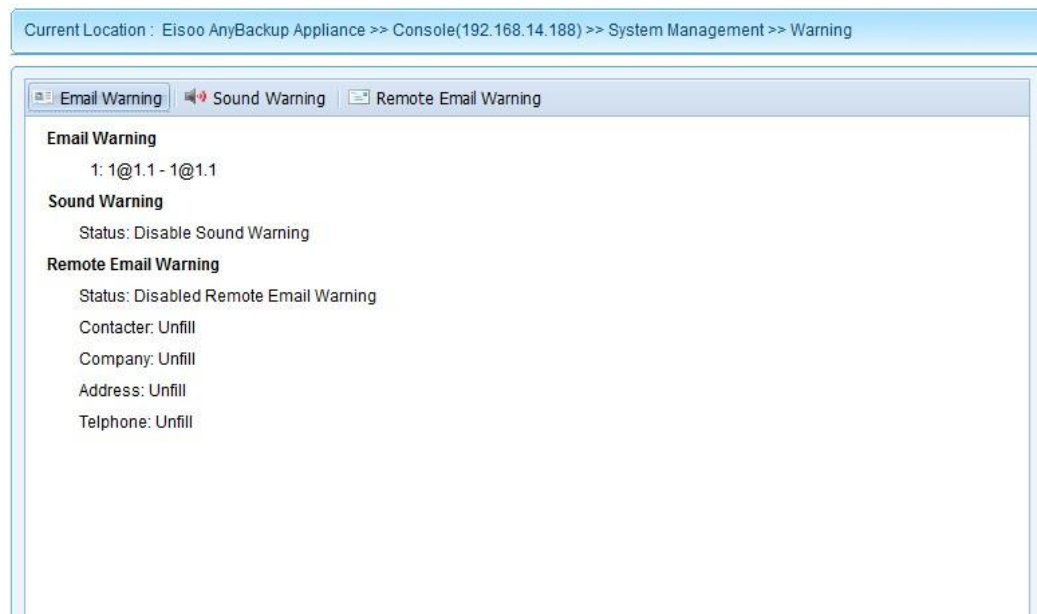


Figure 52 Warning

◆ Mail Warning

Click [Mail Warning] to pop up the following dialog box:

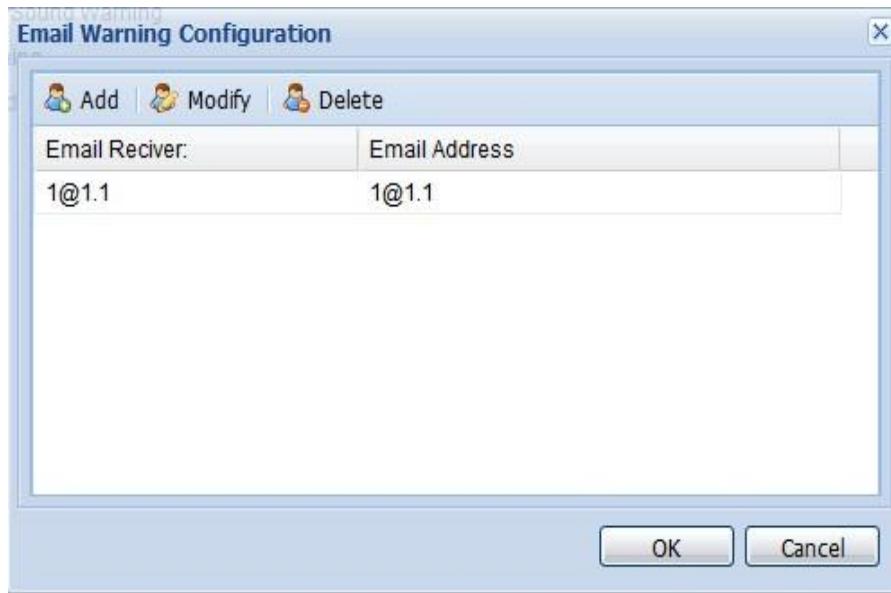


Figure 53 Mail Warning

- Click [Add] to pop up the following dialog box and input receiver and email address. Email address should be composed by "A~Za~z", "0~9" or "@" such as [yourname@domain.com](#). Both receiver and email should be included.
- Select one receiver and click [Modify]. User can modify email or receiver. Input receiver and email, click [OK] to finish modification or [Cancel] to return as shown in the following picture:



Figure 54 Modify Record

- Select one receiver and click [Delete] to pop up a dialog box. Click [Yes] to delete or [No] to return.
- Click [OK] to finish warning configuration or [Cancel] to return.

◆ **Sound Warning**

Click [Sound Warning] to pop up the following dialog box:



Figure 55 Sound Warning

- Default status is “Disable Sound Warning” .
- Select “Enable Sound Warning” and click [OK] to save or [Cancel] to return.

◆ Remote Email Warning

Remote warning refers to that warning info of EISOO AnyBackup Appliance will be sent to EISOO Software Corporation via email, in which user contact is included. EISOO will notify user at the very first time. Click [Remote Email Warning] to pop up the following dialog box:



Figure 56 Remote Email Warning

- Mark “Enable Remote Email Warning” and input corresponding information. Click [OK] to finish or [Cancel] to return.
- Click [Clear All] to clear all information.

5.12 Update

Login to management console as admin and in "System Configuration/Update" page, check, import, delete or configure update package to realize centralized management and central update.

◆ Update Configuration

Click [Configure] to set save path for update package and installation path is default. Click [OK] to save configuration.

◆ Check Update

Click [Check Update] to pop up "EISOO Software-Check Update" page and all available update packages will be displayed. Click update package to download to appointed path.

◆ Import Update

Step One: Click [Import] to pop up the following dialog box:

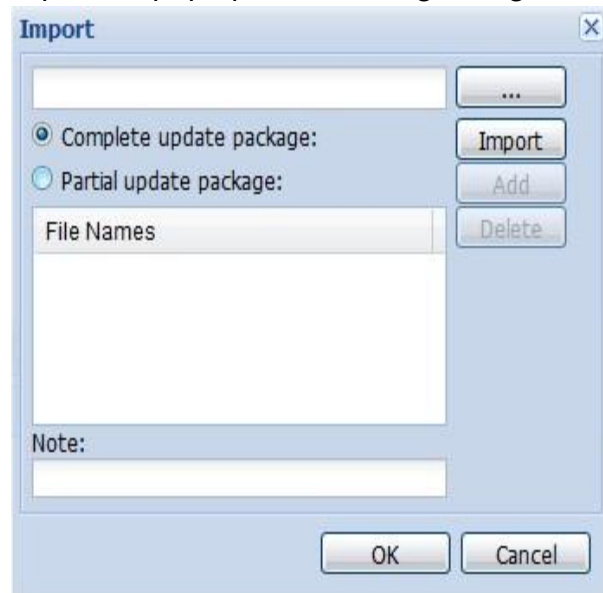


Figure 57 Import Update Package

Step Two: Click [Browse] to select downloaded update package.

- If there is only one update package, select import complete update package and click [Import] to pop up "Import Update Package to Server" dialog box.
- If multiple update packages exist, select segment update package and click [Add] to import segmented update package to server.

Step Three: Click [OK] to finish importing.

- Please make note for update package for convenience.

◆ Update

- Click [Update] to pop up "Update Target Machine" dialog box. Select appointed client and click [OK].
- Click [Yes] to allocate, update or [No] to cancel.

- Click one update package and the following information will be displayed: update package type, release date, size, version, update range, note and description.
- After update, "Update Report" dialog box will pop up to show update result.

◆ **Delete Update Package**

Select update package to delete and click [Delete] to pop up "Are you sure to delete update package?" ; Click [Yes] to delete or [Cancel] to stop deletion.

5.13 Self-backup Management

EISOO AnyBackup 3.5 Appliance supports backup for management console, including database information (Backup job, log, media server information, etc.), backup schedule, version, configuration, volume configuration, sharing, Linux user, warning, etc. All of these can be restored when necessary to rebuild management console. Self-backup includes: 1. Manual self-backup for database, schedule and configuration of management console. 2. Manual restore for management console to a time point. 3. Historical configuration can be imported to a new management console.

◆ **Self-Backup Property**

In [Self-Backup] page, save path and backup can be executed.

- Click [Configure] to pop up a dialog box. Click [...] to select save path in target computer directory. Click [OK] to select this path and [OK] to save the configuration.
- Click [Backup] to pop up a dialog box and input note for this backup. Click [OK] to save management console backup to save path.

◆ **Backup Package List**

In [Backup Package] page, all backup packages for management console will be displayed.

- Select backup package and click [Restore to Management Console] to pop up a dialog box. Input note and click [OK] to restore backup package to management console.
- Click [Delete] to delete backup package from list.

◆ **Backup History**

In [Backup History] page, all histories about self-backup will be displayed. Click [Export] to save this information.

◆ **Restore History**

In [Restore History] page, all histories about restore will be displayed

5.14 Log

In the page [Log], EISOO AnyBackup Appliance provides the following types of logs: User Log, Client Log, System Log, access log, RAID log, update Log and virtual machine log. Log records information of backup and restore and other operation. Through Log, users can trace operation record and examine the causes of failure.

5.14.1 Log Type

◆ Client Log

Click [Client Log], and then click corresponding client in [Client List] to check users' operation log of on this client.

◆ User Log

Click [User Log], and then you can check current users' operation, including modifying password or modifying mails.

◆ System Log

Login to Management Console as admin, and view [System Log] which records changes of clients and media.

◆ Access Log

Enter "Access Log" page and view logs that user access to EISOO AnyBackup Appliance via FTP, CIFS, NFS and iSCSI such as access time, directory, host name and IP.

◆ RAID Log

Enter "RAID Log" page and view RAID usage, including logs about RAID operation, volume and RAID changes.

◆ Update Log

Enter "Update Log" page, update operation about EISOO AnyBackup Appliance will be displayed, including type, event, update time, description, etc.

◆ Virtual Machine Log

Enter "Virtual Machine Log" to view all the logs during operation of virtual machine. All virtual machines will be listed on the left and virtual machine type, execution time, source and log description are displayed on the right. Click [Export] to export all selected virtual machine logs.

5.14.2 Log Content

In EISOO AnyBackup Appliance, each log includes the following items:

- **Type:** Error, Warning and Info are included.
- **Time:** Execution time and local time of log will be recorded.
- **Event:** Operation type, such as login, management, etc.
- **Source:** It records where logs come from and it usually generated by user.
- **Description:** Details about logs will be displayed.

5.14.3 Log Management

◆ Export Log

In log management page, select one log and click [Export] to export log in .txt. User can release log page space in this way.

◆ Delete Log

In log management page, select log on the left and click [Delete] to delete selected log or [Delete All] to delete all logs.

Note: Both audit and admin can view logs of all users and audit can view admin logs while admin cannot view logs of audit. When admin select audit, "You can view audit log" note will pop up.

Chapter 6 Backup and Restore

After configuration of user creation, license, client and system, you can login Management Console as administrator to back up and recover data of authorized client.

6.1 Backup

Backup can be divided as "Regular Backup" , "Real-time Backup" , "Backup Policy" and "Tape Backup" . Click "Backup and Restore" >> "Backup" to enter corresponding window.

In "Regular Backup" page, backup job, backup job options (backup schedule, data compression, encryption and backup Policy, ect are included.), backup group can be created, modified and deleted for authorized clients.

In "Real-time Backup" page, real-time backup job such as creating/ modifying / deleting job and job group can be executed.

In "Backup Policy" page, backup group can be selected to make / modify/ delete backup Policy and it also applied to one backup job.

In "Tape Backup" page, data on disk can be replicated or moved to tape.

6.1.1 Regular Backup

Click "Backup and Restore" >> "Backup" >> "Regular Backup" to enter corresponding page.

6.1.1.1 Create and Configure Backup Job

◆ Create Job

The following types are for creation of regular backup job:

Step One: Click [New] in "Regular Backup" page.

Step Two: Select job type in prompt "New Backup Job Wizard" window.

- If file, OS or email backup is selected, select "Backup Policy" in the drop-down list and click [Next].
- If database backup is selected, select database type in the drop-down list such as: SQL Server, Exchange Server, Oracle, Sybase, Lotus Domino, Active Directory and DB2. Click [Next] to continue.

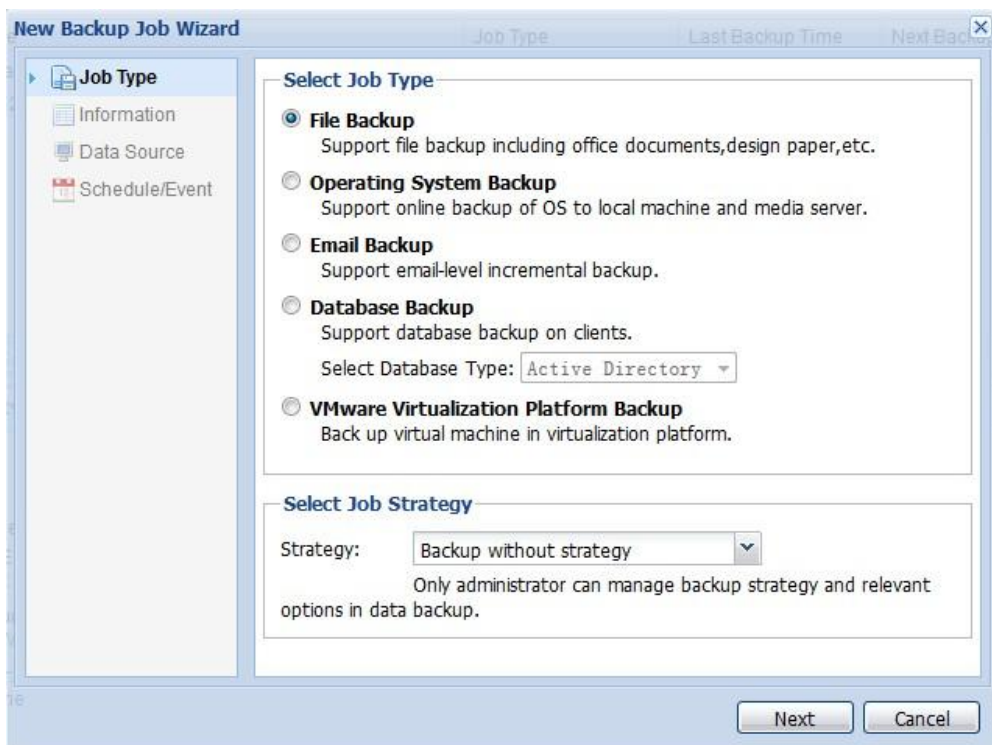


Figure 68 Select Job Type

Step Three: In prompt “Information” dialog box, set job name, job group, backup destination, backup media, data source and data type.

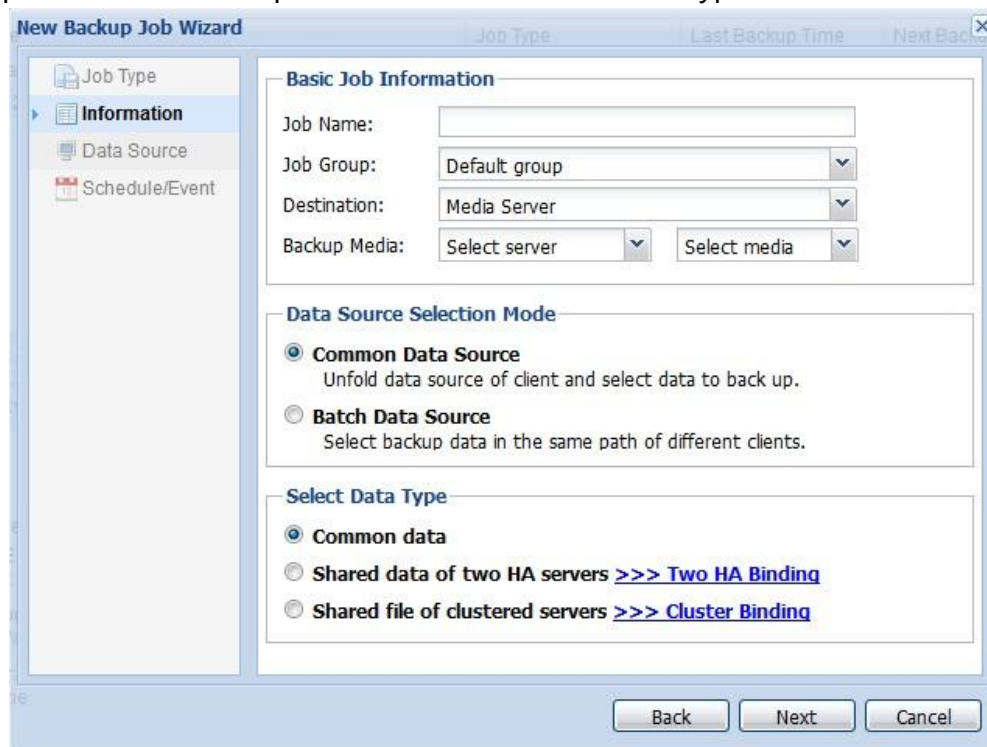


Figure 69 Information

Step Four: Click [Next] to select client for backup and unfold client data source.

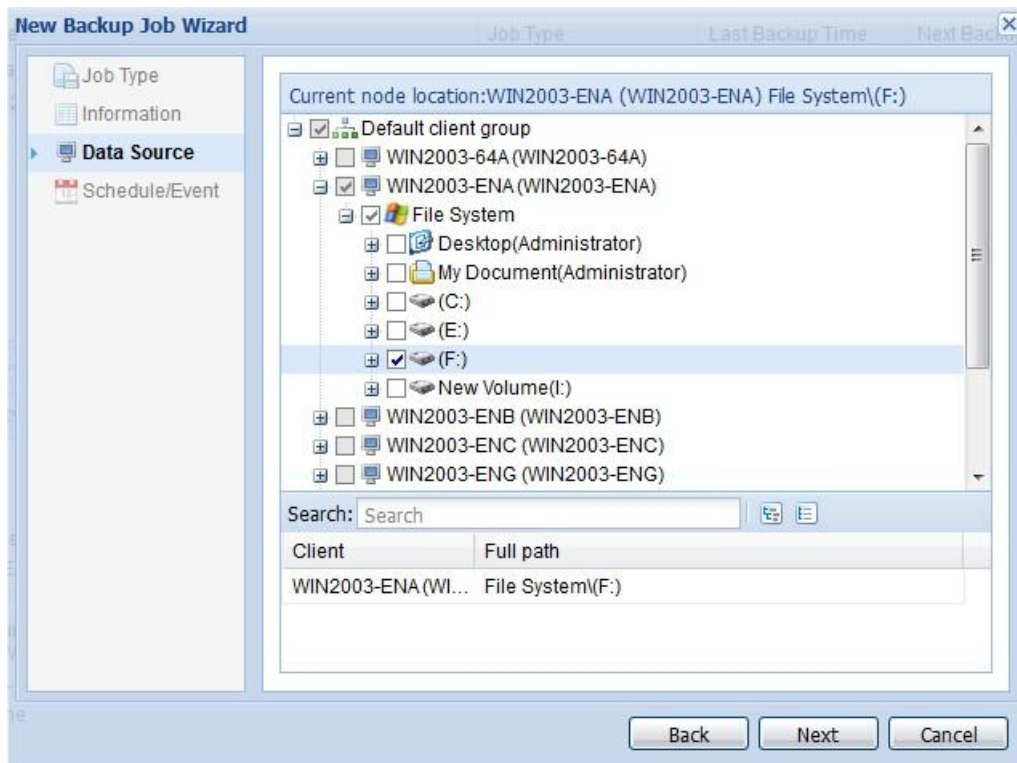


Figure 70 Select Data Source

Step Five: Click [**Next**] to configure job schedule and Option. Click [**Add**] > [**Schedule Type**]. Job Schedule Type includes Daily, Weekly, Monthly, Once and Event Trigger.

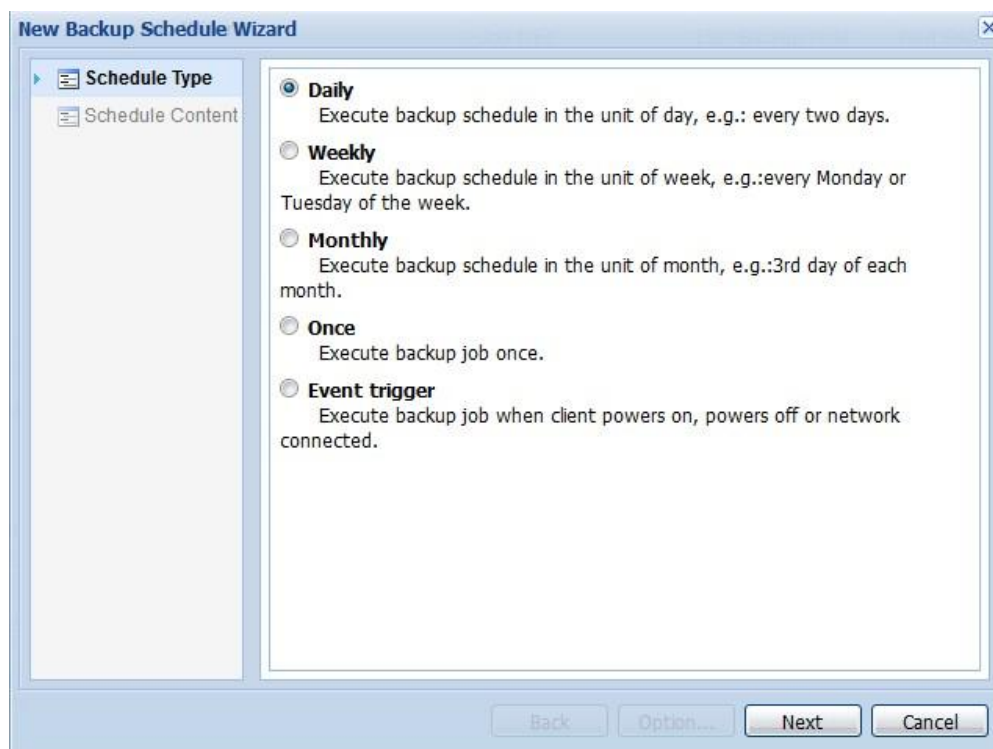


Figure 71 Schedule and Event

Step Six: After configuration of schedule type, click [**Next**] to enter

“Schedule” page, in which backup type, start time and execution period can be set. Click [OK] to save configuration as shown in the following picture:

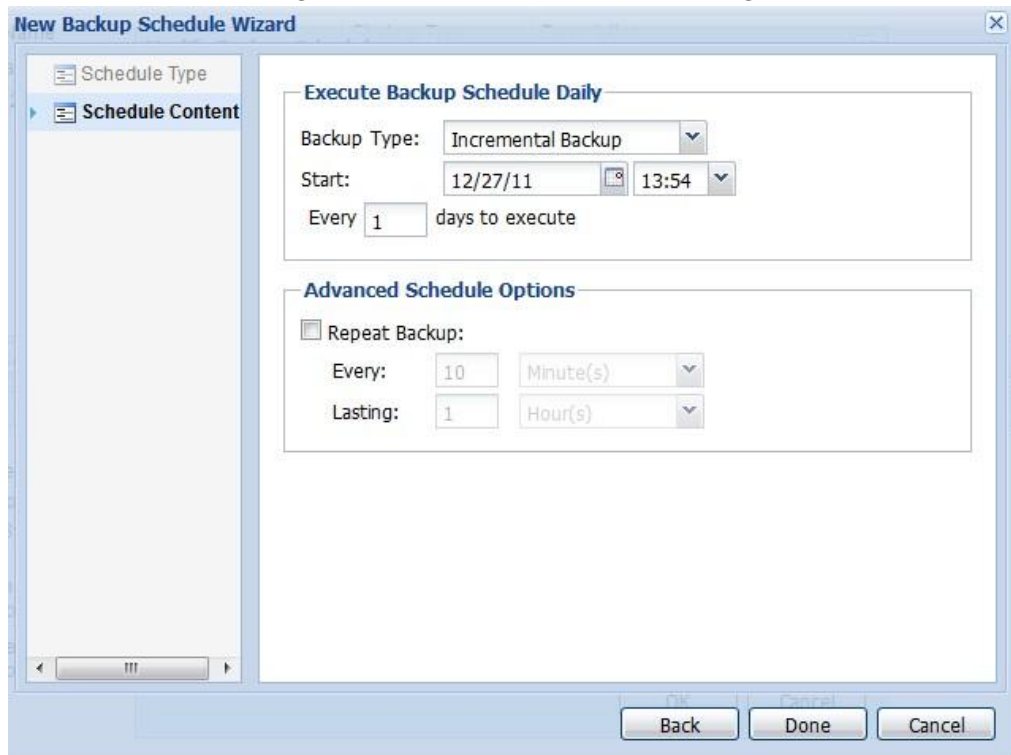


Figure 72 Schdule Configuration

◆ Options

Click “New Backup Job Wizard” >> “Schedule/Event” >> “Option” to pop up [Modify Job Option] window, in which compression, security, file filter, media and advanced options can be set.

➤ [File Filter]

Click [File Filter] > [Type]. And in the pop-up dialog box, select Filter Type and General Type.

➤ [Media Option]

Click [Media Option] to corresponding configuration page. Select [Allow synchronization of backup data to media server] or not.

➤ [Advanced Option]

Click [Advanced Option] to configure number of clients allowed to backup simultaneously.

Step Six: After configuration, click [Done] to finish.

◆ Modify Job

After job creation, you can modify job in “Regular Backup” page.

- Login to management console and select “Backup and Restore” >> “Backup” >> “Regular Backup” to switch to corresponding page.
- Select job and click [Modify].

- Click [Option] in prompt dialog box and modify job options and click [Schedule] to modify job schedule. For details, please refer to “6.1.3 Backup Policy” .

◆ **Schedule**

Click [Schedule] and you can modify, restore, pause and delete schedule.

◆ **Modify Option**

Select job and click [Modify] to modify options in “Regular Backup” page.

◆ **Delete Job**

Select job to delete and click [Delete] to pop up “All related configuration will be deleted if you delete the job. Do you really want to continue?” . Click [Yes] to delete.

◆ **Job Group**

Click [Job Group] and there are three options in the drop-down list: New, Modify and Delete.

- Click [New] to input job group name and description in [New Job Group Info] dialog box. Select user in [**Unverified List**], click >> or << to move appointed User. At last click [**OK**] to finish the operation.
- Choose one group, click [**Modify**] and modify relevant information in the dialog box [**Modify Group Info**]. You also can click >> or << to change the distribution of users. Finally, click [**OK**] to finish modifying group.
- Choose one group, click [**Delete**], read the prompt Info carefully, and then click [**Yes**] to delete selected job group..

◆ **Backup**

Select regular backup job and click [Backup] to input backup type, note in prompt dialog box. Click [OK] to finish operation.

6.1.1.2 Job Type

Job is a central object in backup, which organize data source, option, backup media, schedule, etc and generate backup report for effective management and audit of backup schedule and result. Job type is one property of job, including: file backup, system backup, SQL Server backup, Oracle backup, Sybase Backup, Lotus Domino Backup, Exchange Server Backup, Active Directory Backup, DB2 Backup and Mail Backup, etc.

◆ **File Backup**

Step One: Click [New] to select [File Backup] in “New Backup Job Wizard” and click [Next] to continue.

Step Two: In prompt [Information] dialog box, configure Job name, group, Policy, data source selection mode and so forth. There are two kinds of Data Source

to select: Common data source and Batch data source selection. The former one is to select data source from each client with unfolding each layer gradually, and the later one is to select data source with the same location of several clients. Data Type includes common data, shared data of two HA servers and shared file of clustered servers.

Step Three: In prompt “Data Source” dialog box, unfold clients in authorized client list and select file for backup. Click [Next] to enter “Schedule/ Event” configuration page.

Step Four: Click [Option] to set job options after schedule.

Step Five: Click [Done] to pop up dialog box. Select job type and add note for backup job. Click [OK] to submit job to execution queue.

◆ **Operation System Backup**

EISOO AnyBackup Appliance supports backup for Windows and Linux now.

➤ **Backup for Windows**

Step One: In “Selete Job Type” dialog box, select “Operating System Backup” and click [Next].

Step Two: Set job name, job group, backup destination, data source, ect in prompt backup dialog box, of which backup destination can be local system backup area and media server.

Note: Local backup area: Operating system of client can be backed up to local disk via management console to generate an invisible file folder or file in local disk for network burden release. Backup data will not be deleted until client is uninstalled.

Step Three: Please refer to “6.1.3 Backup Policy” for backup job option configuration and backup job submit.

➤ **Backup for Linux**

Please refer to “Linux System Backup and Restore/ Linux System Backp” for details.

◆ **Email Backup**

Step One: Select “Email Backup” in backup job type and click [Next].

Step Two: Set job name, job group, backup destination and backup media in prompt “Job Information” dialog box. Select data source and click [Next].

Step Three: In prompt “Select Data Source” dialog box, select data for backup and click [Next] to enter “Schedule/Event” page. Please refer to “6.1.3 Backup Policy” for detailed operation.

6.1.2 Real-time Backup

Click “Backup and Restore/Backup/Real-time Backup” to enter corresponding page.

◆ Create Job

Step One: Click [New] to pop up “New Backup Job Wizard” dialog box. Input job name, job group, destination (Media server is default) and data source in prompt dialog box.

Step Two: Click [Next] to pop up “Selete Data Source” dialog box.

- If data source is common data, current available Windows clients will be displayed. Select data source for backup.
- If data source is bath data, current available Windows clients will be displayed. Mark data source for backup and click [Add Data Source]. Input data source path in prompt dialog box.
- Click [Option] to set parameter, select compression, set security and filter type.
 - Real-time Parameter: Generate time interval (1 hour by default) and preserved copies (30 by default).
 - Data compression, security, filter, media operation can be set according to related information in 6.1.3 Backup Policy.

Step Three: Click [Done] to finish creation of real-time replication job.

◆ Modify Job

Select real-time replication job and click [Modify] to modify information, data source, etc.

◆ Modify Option

Select real-time replication job and click [Modify Option] to pop up a “ Backup Job Option” dialog box. Please refer to 6.1.3 Backup Policy for detailed operation.

◆ Delete Job

Select job and click [Delete] to pop up “Corresponding configuration and backup data will be deleted, are you sure to delete current selected job?” Click [OK] to finish.

◆ Job Group

Job group management includes creation, modification and deletion of job group; please refer to “Regulare Backup/Job Group” for detailed information.

Note: After creation of real-time replication job, enter “Continuous Execution” to execute this job.

6.1.3 Backup Policy

For better protection for file system, backup Policy is provided for management of backup. It is recommended to set according to actual conditions.

6.1.3.1 Backup Policy Management

Click [Backup and Restore] > > [Backup] > > [Backup Policy] to enter corresponding page.

◆ Create Policy

Step One: Click [New] to pop up “New Backup Policy Wizard” dialog box. Select the following backup Policy type: File Backup Policy, OS Backup Policy and Email Backup Policy and click [Next] to continue.

Step Two: Input Policy name, group, destination, media and description in “Information” page and click [Next] to continue.

Step Three: In “Schedule/Event” page, set schedule for backup Policy. Please refer to “Backup Policy Management” for detailed operation.

◆ Modify Policy

Select Policy and click [Modify] to pop up “Modfiy Backup Policy” dialog box. Policy name, group and description can be modified as shown in the following picture:



Figure 73 Modify Backup Policy

◆ Delete Policy

Select Policy and click [Delete] to pop up a dialog box. Click [Yes] to delete Policy.

◆ Policy Group

Backup Policy can be added to Policy group for cental management.

Backup Policy group management includes creation, modification and deletion of Policy group, please refer to “Regulare Backup/Job Group” for detailed information.

6.1.3.2 Job Schedule

◆ Job Schedule

Job schedule is used to run backup job in free time and backup job can run daily, weekly, monthly or a specified time (such as system starts). It is the basis of auto backup.

- In “Backup Policy” page, click [Schedule/Modify] to pop up the following dialog box:

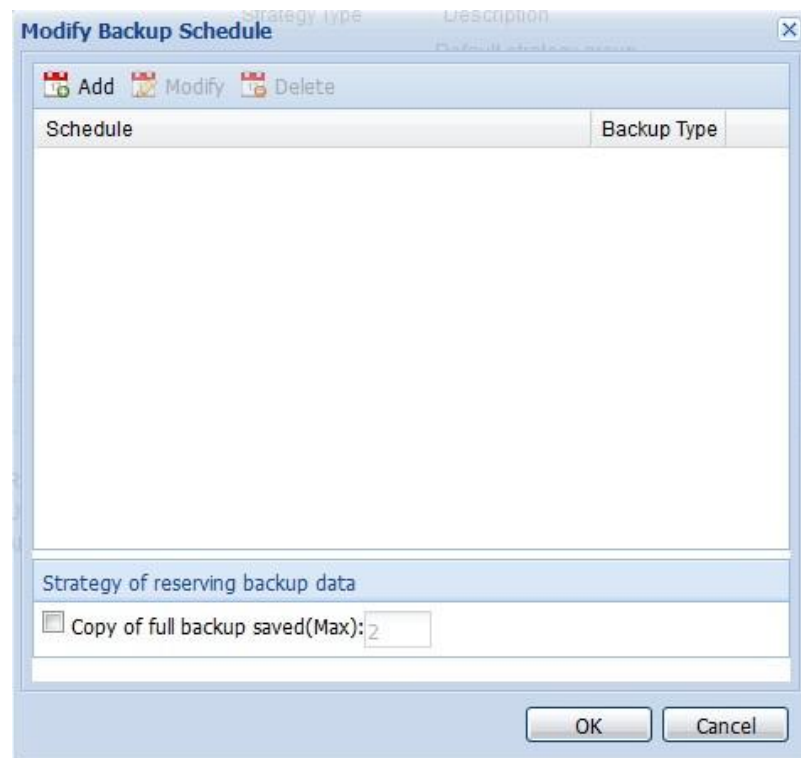


Figure 74 Job Schedule

- Click [Add] to pop up “Job Schedule Configuration Wizard” dialog box. EISOO AnyBackup Appliance provides [Backup Schedule Wizard] to guide execution of backup job daily, weekly, monthly, event-triggered or once as shown in picture 65. In [Schedule], detailed info such as backup type, start time, execution time and time interval can be viewed. In [Advanced Option], frequency and last time can be set as shown in picture 66.

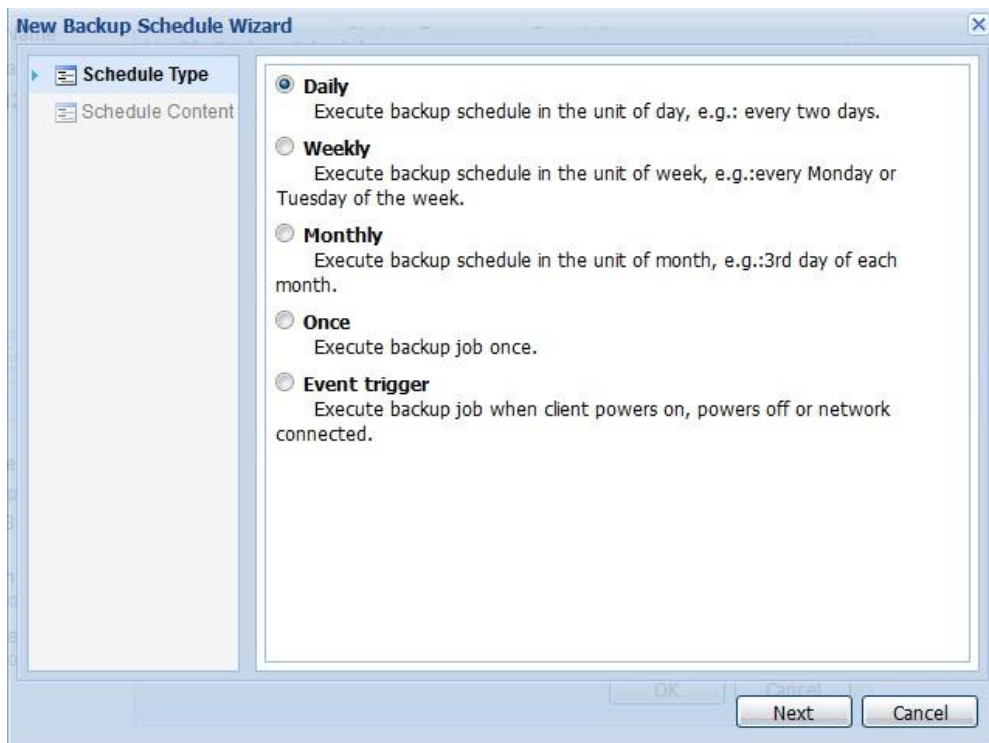


Figure 75 Schedule Type

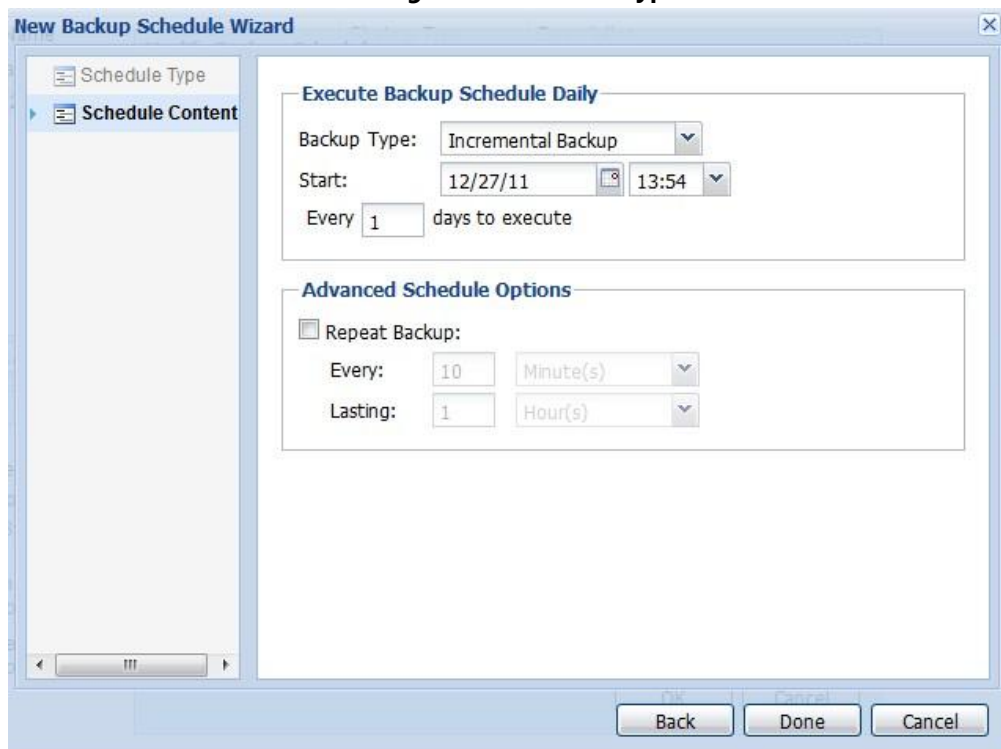


Figure 76 Schedules Content

- Click [Done] to return [Job Schedule] dialog box. In [Backup Policy Rotation], full backup and incremental backup copies can be set to save backup space.

◆ **Schedule**

After creation of backup job, schedule can be modified or deleted.

- Click [Schedule] >> [Modify] to pop up "Job Schedule Modification" dialog box. Backup schedule can be added, modified and deleted, full copies can be saved. Click [OK] to save.
- Click [Schedule] >> [Delete] in the drop-down list to delete job schedule.

6.1.3.3 Option

◆ File Filter

EISOO AnyBackup Appliance supports powerful file filter to include or exclude specified files/directories, which will greatly save space and improve backup speed.

- Login to management console and click [Backup and Restore /Backup / Backup Policy]. Click [Modify].
- In prompt [Job Option] dialog box, click [File Filter] to switch to corresponding page.
- **Filter Type:** Click [Filter Type] and in prompt dialog box, select files to include or exclude or input extension name of files in other types. Click [OK] to save configuration.

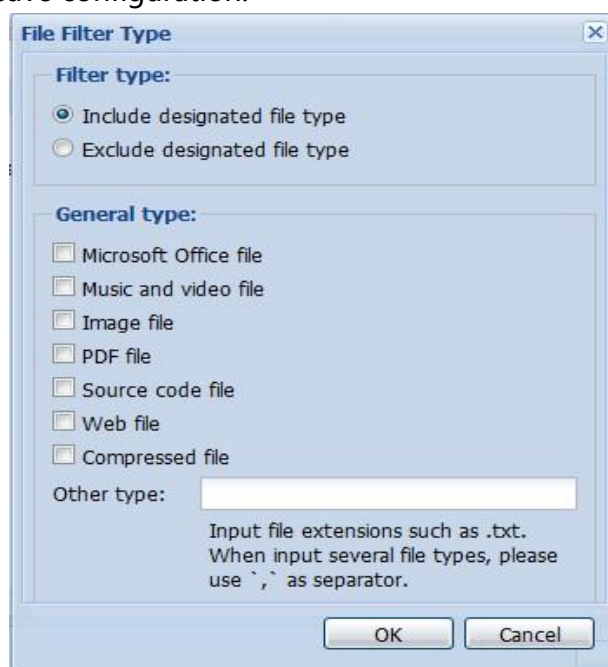


Figure 77 Filter Type

- **File Filter:** Click [File Filter] to select files to include or exclude or input file name. Click [Yes] to save configuration.

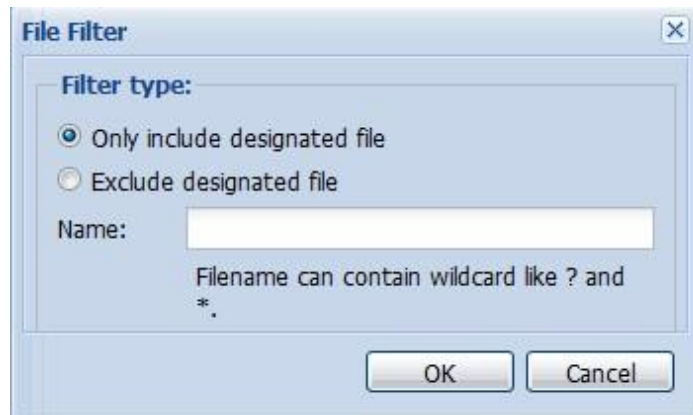


Figure 78 File Filter

- **Directory Filter:** Click [Directory Filter] to select including or declluding these directories or input directory name. Click [OK] to save configuration.



Figure 79 Directory Filter

- **Filter Type:** Click [Time Filter] and select [Include /Exclude this time] in the prompt dialog box. Specifiy time to filter and click [OK] to save configuration.

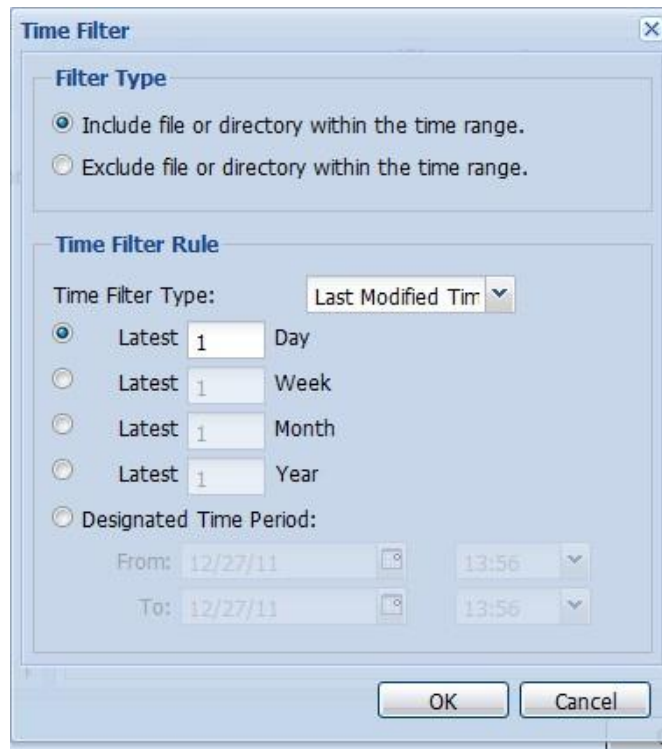


Figure 80 Time Filter

- **Delete Filter:** Select filter item to delete and click [Delete]. Click [OK] to delete or [Delete All] to delete all filter items.

◆ **Media Option**

Media synchronization can be set via [Media Option].

- Login to management console and click "Backup and Restore" >> "Backup" >> "Backup Policy" . Click [Modify Option].
- In the prompt dialog box, click [Media] to switch to media option configuration page.
- Mark or unmark "Synchronize data to media sync server" .

◆ **Advanced Option**

Concurrent clients can be set via "Advanced Option" , that is clients allowed for concurrent backup jobs.

- Login to management console and click "Backup and Restore" >> "Backup" >> "Backup Policy" . Click [Modify Option].
- In prompt dialog box, click [Advanced Option] to switch to advanced option configuration page.
- Concurrent clients can be set between 1 and 40, and 4 is default.
- After configuration, click [OK] to save configuration.

6.2 Restore

EISOO AnyBackup 3.5 provides three methods for data restore: Browse to Restore, Search to Restore and Download to Restore.

Login to Management Console, Click **[Restore]** > **[Browse]**. The following operations can be done: restore any backup data in the authorized clients to appointed client or download them to local via Web. Click **[Search]** and enter relevant page. In this page, EISOO AnyBackup provides search engine to find appointed files for recovery quickly. Click **[Download to Restore]** and download data to local client via Web browser.

6.2.1 Browse to Restore

Step 1: Click **[Restore]** > **[Browse]**.

Step 2: In **[Regular Backup Job]**, select a backup job and client where data source lies.

Step 3: Drop down the menu list of **[Time Point]** and select the time and data you want to restore.

Step 4: Click **[Restore]**, and enter **[Restore to Client]** dialog box. Client, Restore location and other info will be configured.

Step 5: Click **[Restore]** to start execution.



Picture 7 Restore to Client

6.2.2 Instant Restore

Eisoo AnyBackup Software provides iSCSI mounted technology that can restore backup data for use immediately.

Notice :

Instant restore only support mounted volume copy data.

Environment with antivirus software may not unmount mounted volume and you must restart system to umount as antivirus software may occupy and scan disk.

Client will finish mount with command from Microsoft iSCSI Initiator,thus Microsoft iSCSI Initiator should be installed during installation (Not necessary in Windows Vista or above);

After successful instant restore, all write operation will be removed.

It will take about 10 seconds to display disk when Windows XP mounted successfully.If disk of [Dynamic Disk] mounted successfully, it will displayed as offline and you should [Reactivate Disk] manually.

Mount Volume Data

Click [Restore] to switch to restore window.

Click [Instant Restore] to switch to instant restore window.

Click "Mount" to enter corresponding page. Select target client in "Target Client" list and select mounted volume job in [Information] dialog box. Select time point in the drop-down list of [Time Point] and click [Done] to finish mount.

Instant Restore

Once data loss of mounted client caused by accident, mounted disk can be used to restore data immediately for use in local

Or this function enables other virtual machine or physical machine to mount latest time point regularly for statistics, especially when database has mass data and query on production server will occupy a lot resources, while with mounted volume a lot production server resource can be saved

Umount Volume Data

Click [Restore] to switch to restore window.Click [Instant Restore] to switch to instant restore window.

- ◆ Click [Unmount] to enter corresponding page and select umount data and click [OK] to finish umount..

6.3Execution

Compared with traditional version that hand over data backup and restore job to Management Console for unified operation, EISOO AnyBackup 3.5 Appliance also gathers execution status, execution schedule and other info to an independent module [Execution] to offer users integrated management.

Login to **[Management Console]**, click **[Execution]** and view routine execution, continuous execution and execution history.

6.3.1 Routine Execution

Routine Execution organizes ongoing and forthcoming backup or restore job in groups, and shows detailed job info such as job name, operation type.

- Login to management console and click **[Execution]** to switch to "Routine Execution" . Here you view execution status in this window.
- Click **[Refresh]** to view latest job execution status.
- Click "Filter Type" drop-down list and the following types are included: All, download, delete backup data, backup, restore, tape backup and tape restore.
- Click "Others" drop-down list and the following types are included: All, waiting and running.
- Click **[Stop]** to stop running jobs.
- Click **[Stop All]** to stop all running jobs.
- Select one running job and execution information can be viewed in **[Output Information]** and process can be viewed in **[Details]**.

6.3.2 Continuous Execution

Real-time backup job, media sync job and disaster recovery job will be displayed in continuous execution window.

◆ Refresh

Click **[Refresh]** and system will refresh all execution status in this window.

◆ Start

If execution status is paused or stopped, select the job and click **[Start]** to make it running.

◆ Pause

If execution status is running, select the job and click **[Pause]** to make it paused.

◆ Stop

If execution status is running or paused, select the job and click **[Stop]** to make it stopped.

◆ Output Info

Click "Output Info" . Start, pause, stop operation, warning or error of each executive and execution time will be displayed .

◆ Execution Details

Click "Execution Details" to display executive name, current status and related information.

◆ Pause Period

Select one continuous execution job and click [Pause Period] to pop up a dialog box, in which pause period such as daily, weekly or monthly can be set.

- Click [Add] to pop up “Add Pause Period” dialog box and the following three items are included: Daily, Weekly and Monthly:
 - Daily: Pause period will take effect every day.
 - Weekly: Pause period will take effect in the days of each week.
 - Monthly: Pause period will take effect in the days of each month.
- Click [Modify] and modification is the same as pause period adding.
- Select one period in list and click [Delete] to delete it from list.

◆ **Auto Cleanup**

- Select one continuous execution job from list. Click [Auto Clean], then [Set Auto Clean] dialog box will pop up. You can configure auto clean time.
- Retention time of output information has five options: one day, two days, one week, two weeks and a month. One week is default.
- Click [OK] to save configuration.

◆ **Filter**

Job type of execution job list can be configured via [Filter].

- Type Filter: filter according to types of execution job, including All, Media Synchronization, Real-time backup (Replication) and disaster recovery.
- Other Filter: filter according to timely status of execution job, including All, Ongoing timely job, Paused real-time job and Stopped real-time job.

6.3.3 History List

All the executives, operation type and result of executed jobs will be displayed, of which backup execution result includes success, failure, success with warning, while other execution result only includes success and failure.

- Click “Restore/History List” to switch to corresponding page, in which results of executed backup, restore, remote synchronization and other jobs will be displayed.
- Click [Delete] to delete selected history list or [Delete All] to delete all history lists.
- Click [Export] and system will export all displayed executives for user download.
- Click [Type Filter] drop-down list and the following types are included: All, Download, Delete Backup Data, Backup, Restore, Tape Backup and Tape Restore.

- Click [Others] drop-down list and the following items will be displayed: All, Succeeded Item, Succeeded Item with Warning, Failed, Latest Day, Latest Week, etc.
- Click [Name] to input filter type name and click search icon to filter.
- Select one history list and execution information will be displayed in [Output Information].
- In [Execution Report] window, backup type, execution type, start and end time, time cost, original size and finish size will be displayed.

6.4 Linux Backup and Restore

6.4.1 Linux System Backup

◆ Linux Backup Theory

The following information is required for system backup:

- Physical Disk and Disk Information
- Detailed LVM Information
- System Logical Device-Detailed File System Information
- Related Information of System Boot Program

Backup process is shown in the following picture:

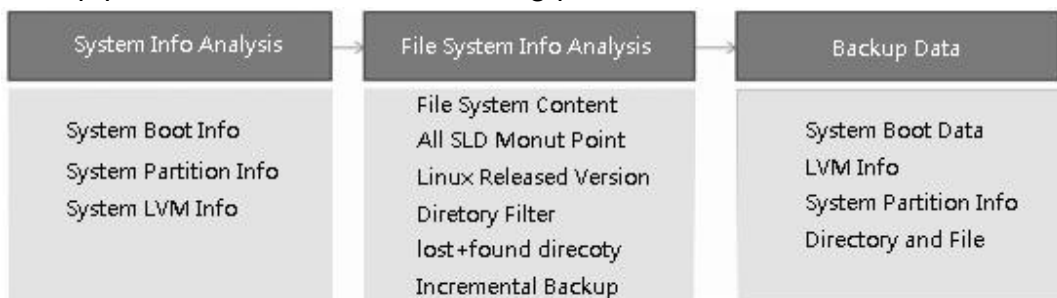


Figure 8 Linux Backup

◆ Linux Backup Operation

Login to management console and click "Backup and Restore/ Backup/ Regular Backup".

Step One: Click [New] to pop up "New Backup Job Wizard" dialog box.

Step Two: In "Select Job Type" dialog box, select [Operating System Backup] and backup Policy. Click [Next] to continue.

Step Three: Enter "Information" dialog box, input job name, job group, destination (media server or local system backup area) and click [Next].

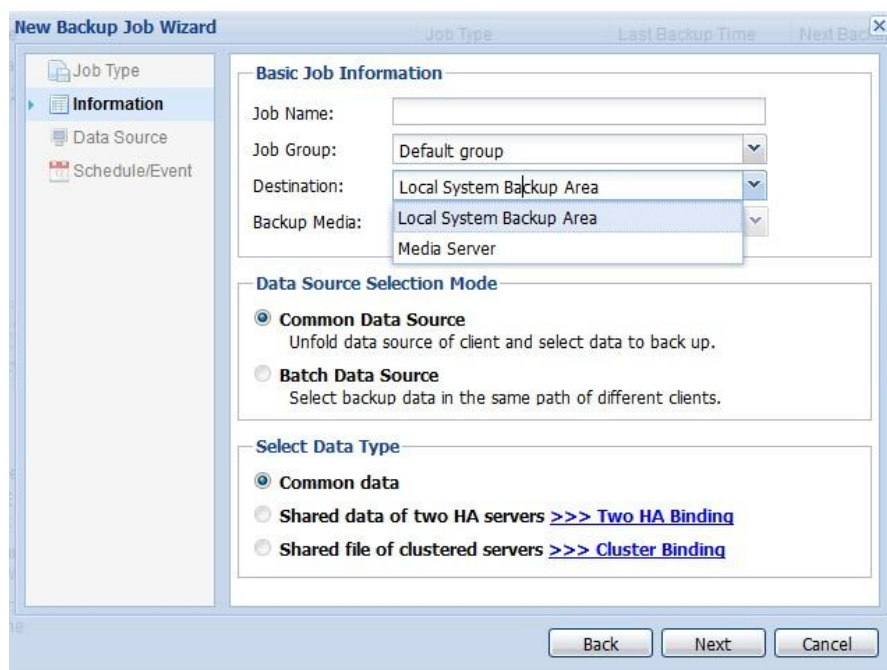


Figure 88 New Linux Backup Job

Step Four: Enter “Selete Data Source” dialog box and select data source to back up as shown in the following picture:

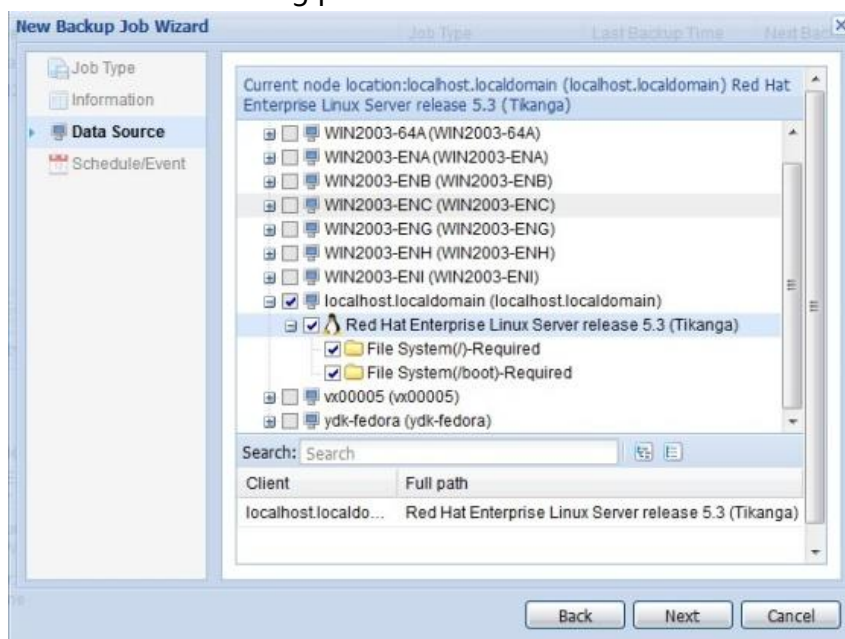


Figure 89 Select Data Source

Step Five: Enter “Schedule/Event” dialog box and add/modify/delete detailed schedule. Click [Option] to set compression, security, advanced option, etc. Please refer to “Backup/Backup Policy” for details. Click [Done] to finish.

Step Six: In prompt “Linux Backup Execution” dialog box, add backup note and click [OK] to start execution of backup job.

6.4.2 Linux System Restore

◆ Linux System Restore Theory

Linux system restore theory is shown as the following picture:



Figure 90 Linux System Restore Theory

◆ Linux System Restore Operation

Step One: Boot System Recovery Environment

- For normal boot of system recovery environment, please set BIOS boot options correctly according to system recovery environment installation.
- For disk/ISO Mirror/USB boot, boot order should be modified as of disk or USB priority.
- System recovery environment initial boot interface is shown in the following picture:



Figure 91 Boot Interface

Note: linuximg is the key file of system recovery environment; linuxbt is transition file when system recovery environment starts and some preparation should be done for when this file is running.

Step Two: Configure RAID/Disk Control Drive

- Disk controller/RAID controller should be loaded correctly for successful system restore and most of the disk controller and RAID controller can be driven now by system recovery environment.
- Boot by disk/ISO Mirror/USB and system will auto load correct drive.
- Some basic disk will be loaded when system recovery environment starts and identified disk partition will be listed for 5 seconds.



Figure 92 Disk Partition List

- If list is empty or inconsistent with system real disk/RAID information (Not all the disks/RAID have been driven.), enter any keyboard to enter “Disk/RAID Configuration” page within 5 seconds. All main manufactures of RAID/Disk controller and main server manufactures will be displayed. User can select manufacture according to their system hardware.

```

-----
Please select RAID controller vendor.
-----
1      IBM
2      HP/Compaq
3      Dell
4      Lenovo
5      Intel
6      3WARE
7      LSI
8      HighPoint
9      Adaptec
10     Promise
11     QLogic
12     Areca
13     SATA
14     PATA
15     Others
a      All
x      Exit
u      ByUsb
-----
Your choice :7_

```

Figure 93 Manufacture List

- Select one manufacture and all drive of this manufacture will be listed. User can select drive according to hardware model:

```

-----
Please select type of LSI :
-----
1      MegaRAID
2      MegaRAID_mbox
3      MegaRAID_SAS
4      FusionMPT_SPI
5      FusionMPT_SAS
6      MegaSoftRaid
0      Unknown
b      Back
x      Exit
-----
Input your choice:4_

```

Figure 94 Select Drive

- After selection of drive, system will load corresponding driver and display disk/partition again in the interface for user to check. If it is correct, input “y” and exit disk/RAID configuration page to continue booting system, or input “n” to return to manufacturer page to reselect.
- System recovery environment will load necessary file and system to finish system booting.

- After booting, start graphical interface and run system recovery program, thus system recovery environment is successfully started and user can execute system restore:



Figure 95 System Restore Wizard

Step Three: Select System Restore Method

- As Linux cannot be backed up to local, it must be restored from backup server or restored from shared network.

Step Four: "Backup Server Restore" : Network Configuration

- Select "EISOO AnyBackup Server Restore System" to enter "Local Network Configuration" page. Auto get IP or set IP manually.

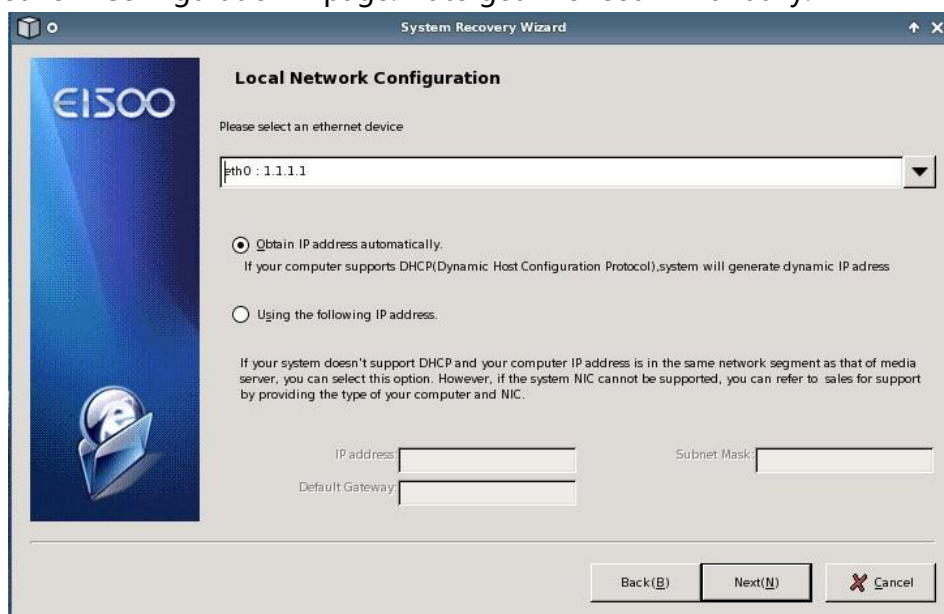


Figure 96 Local Network Configuration

Step Five: Login to Media server or network sharing machine.

- After configuration of local IP, enter “Login to Server” page and input “enterprise account” “ server IP” “ port” in this page. Select login method and input “username” and “password” . Click [Next] to connect to server.
- Restore system via EISOO AnyBackup Appliance, there is no need inputting enterprise account; For AnyVault, correct enterprise account is a must for connection to backup server. Default enterprise account is “enterprise” .

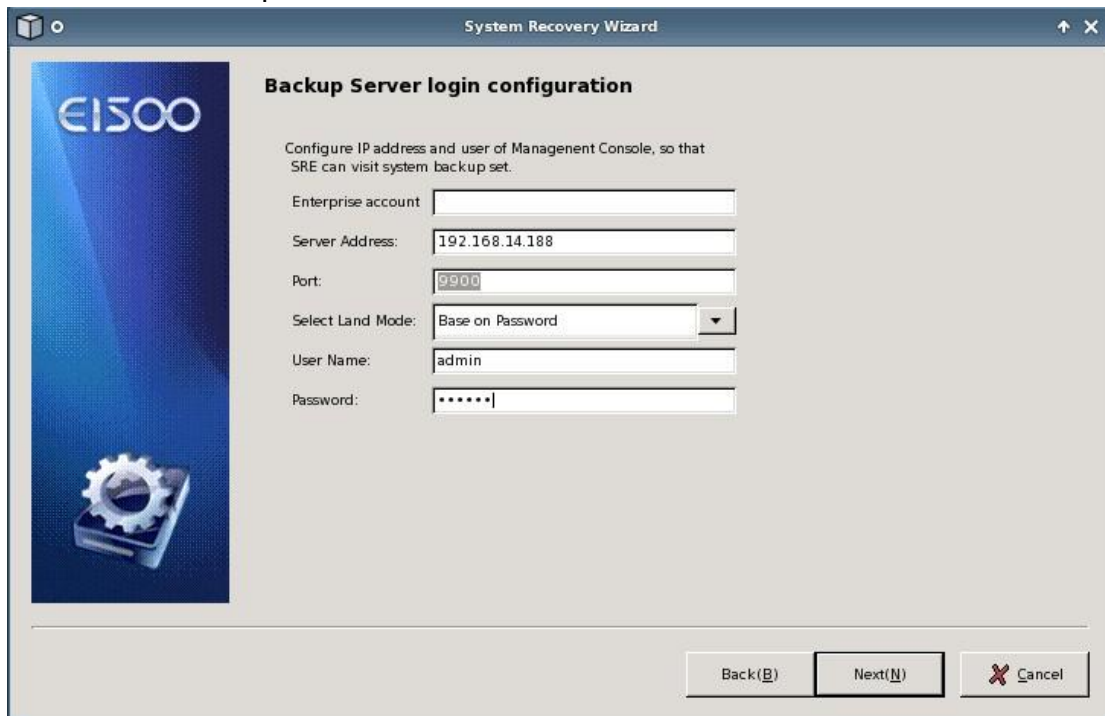


Figure 97 Login to Backup Server

- Select “Restore from local or shared network ” and click [Next]. Enter “Select backup data and time point” and click [Network Mapping] to set parameter of network sharing machine:

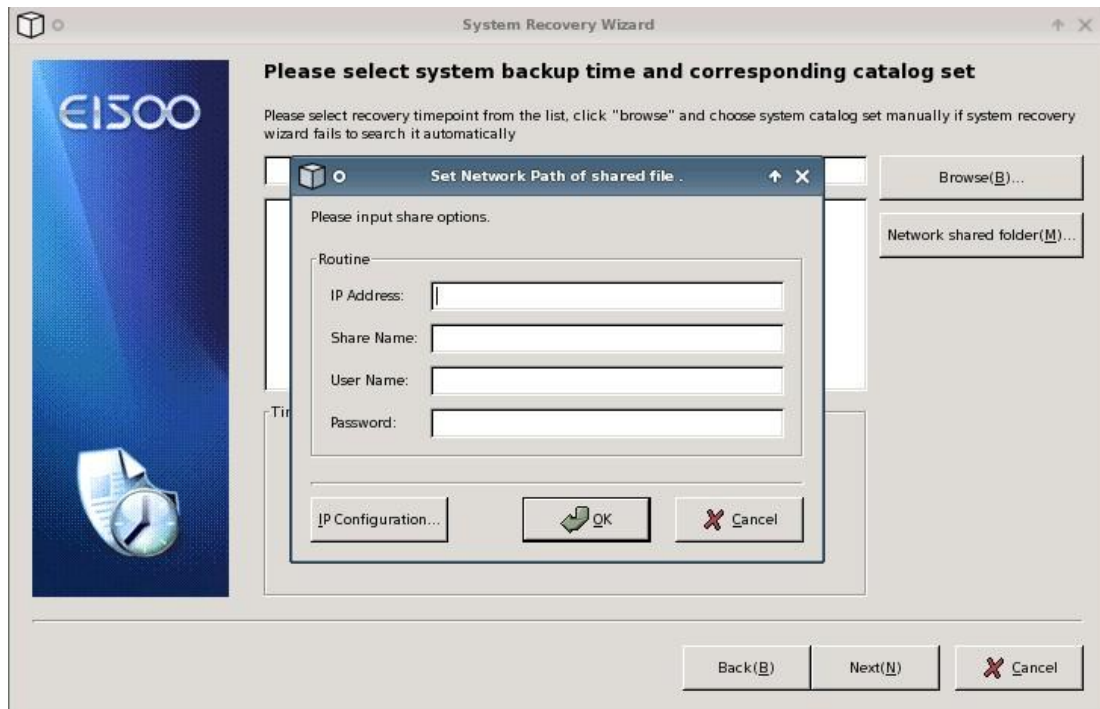


Figure 98 Mapping Network Path

Step Six: Select backup set or corresponding job

- After successful connection to backup server, all system backup job of this user will be listed and client can be viewed by unfolding each job. Select client and backup time point for system restore.

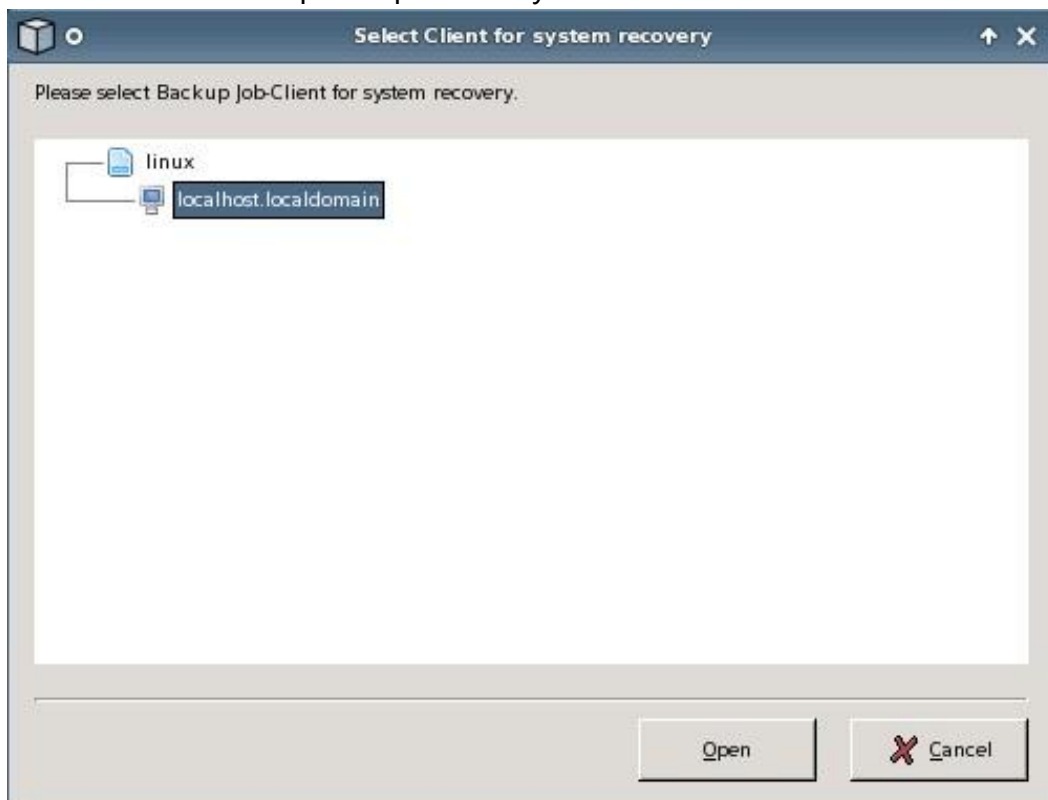


Figure 99 Select System Restore Job-Client

- After successful connection to network sharing machine, select backup set to restore (Backup set path will be displayed as shown in the following picture, path is VMP\1\2\4). Click [Open].

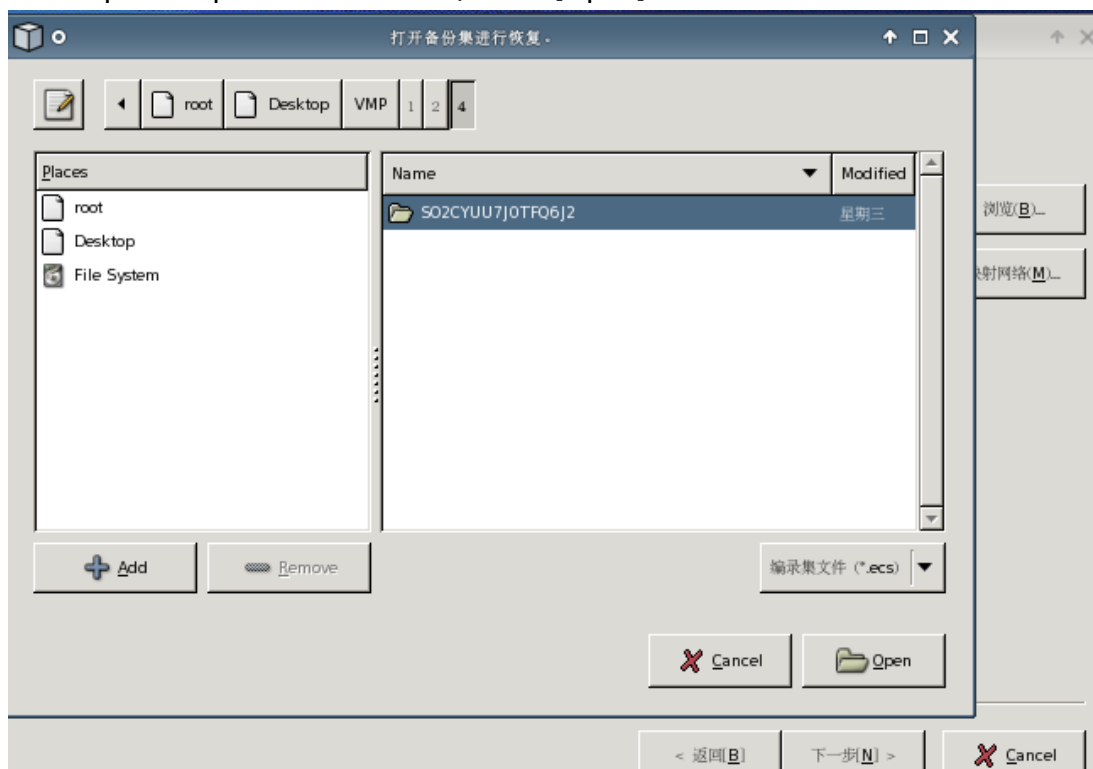


Figure 100 Open Backup Set to restore

Step Seven: Select backup time to restore

- Select system backup catalog set (Local network mapping) or job-client (network). All backup time point of system backup job will be displayed and select time point to restore. Click [Next] to start restore.

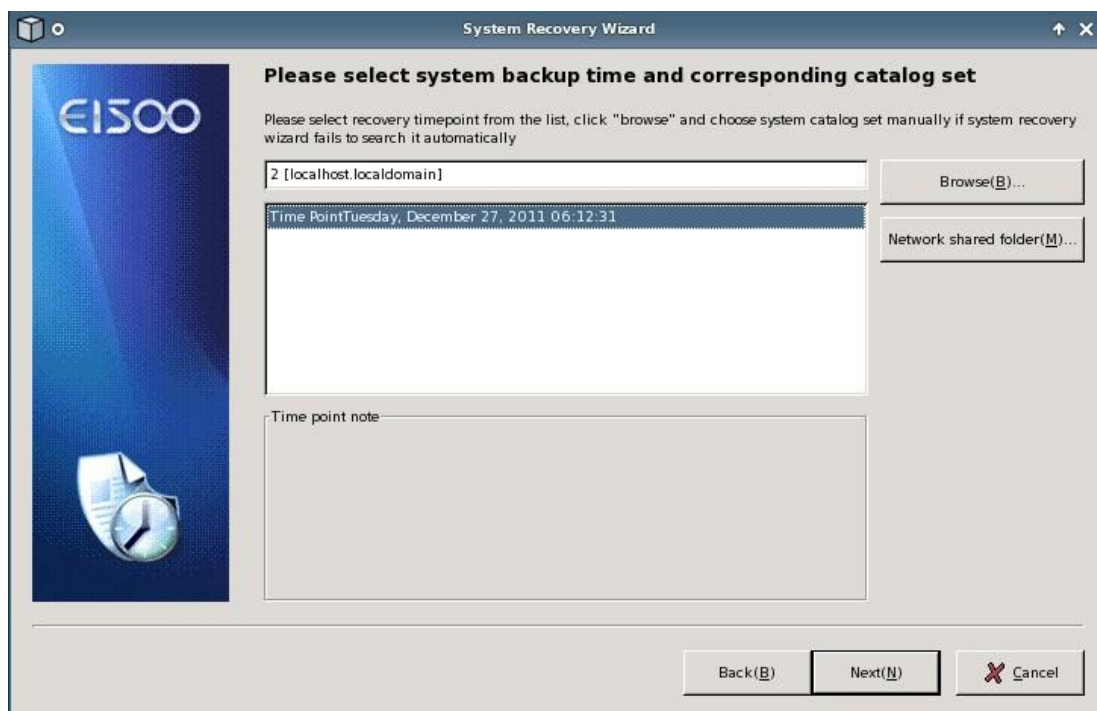


Figure 101 Select Restore Time Point

Step Eight: System Restore

- Restore program will display execution information in each stage; name and restore process of files in restore will be displayed in details.

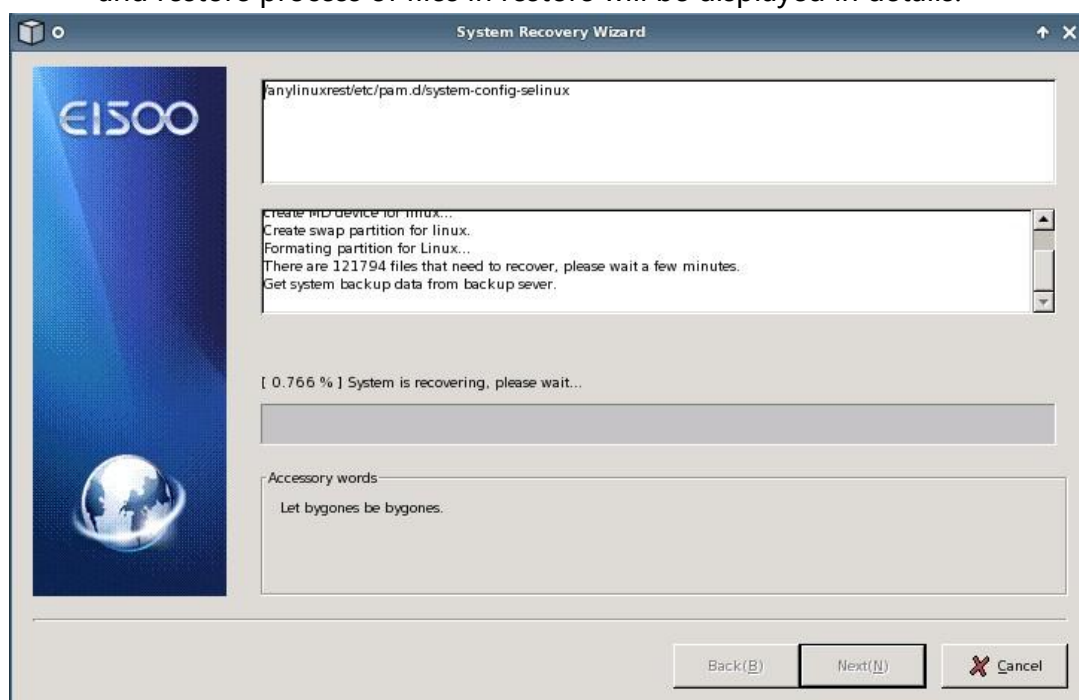


Figure 102 System Restore

Step Nine: After restore, reboot system.

- After restore, the following dialog box will pop up. Click [Yes] to restart system.



Figure 103 Successful Restore

- If system is restored from disk or USB, pull out disk or USB; or set boot order as disk priority to avoid rebooting of system recovery environment.

6.5 Backup and Restore for SQL Server

6.5.1 Introduction

MS SQL Server has a genuine Client/Server structure. As a database management system, it adopts graphical user interface, which makes the management of system and database easier and more intuitive. Meanwhile, it has several programming interface tools, which provides more Options for users to make programming.

Fully integrated with Windows NT, SQL Server makes use of many functions of NT, such as sending and receiving messages, security for management Login to, etc. SQL Server can be well integrated with Microsoft BackOffice, and it can be flexibly used in many kinds of platforms.

There are three kinds of backup for SQL Server: (1) full backup; (2) differential backup; (3) transaction log backup.

6.5.2 Backup Notice

- The server used to backup and restore SQL Server must allow Login to with Windows authentication.
- In order to support the combined backup mode of "full backup +differential backup+ transaction log backup" , the database is required to be at full recovery model. As to the reason to choose full recovery model, please refer to:
<http://www.eisoo.com/article/document/20080910/211.html?1228389483>
- Please make full backup for database after the recovery is finished. That is because the execution of recovery will truncate logs, which will cause errors in subsequent recovery. After making full backup, the following transaction log backup will use this full backup as a reference.

- When modifying backup job Option, full backup needed to be made to this job after adding or reducing data source. For example, full backup needed to be made after adding or reducing backup for test database.
- Cross backup cannot be made to data in the same database. That is to say, a database cannot appear in several jobs at the same time. When errors occur during cross backup and restore, please refer to:
<http://www.eisoo.com/article/document/20081013/222.html?1228389513>

6.5.3 Backup Operation

6.5.3.1 Configure SQL Server

Log into Management Console as administrator and click [Configuration] > [Client] > [Configure], a [Modify Client Configuration] dialog box will pop up, which says: Please select database(s) that client supports. Select [SQL Server], and then click [OK].

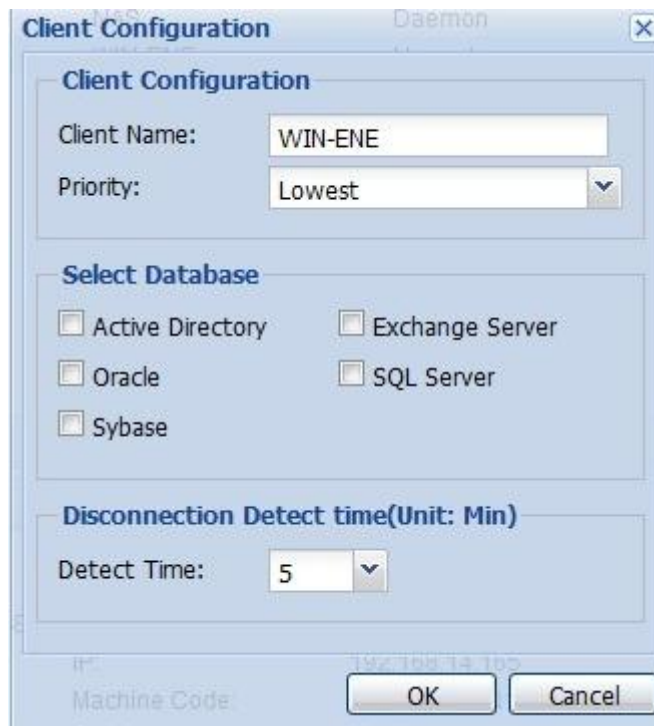


Figure 104 Modify Client Configuration

6.5.3.2 Create New Job

Step One: In Management Console, click [Backup] > [New], a [New Backup Job Wizard] dialog box will pop up. Select [Database Backup]. Select [SQL Server] in the drop-down list. Click [Next].

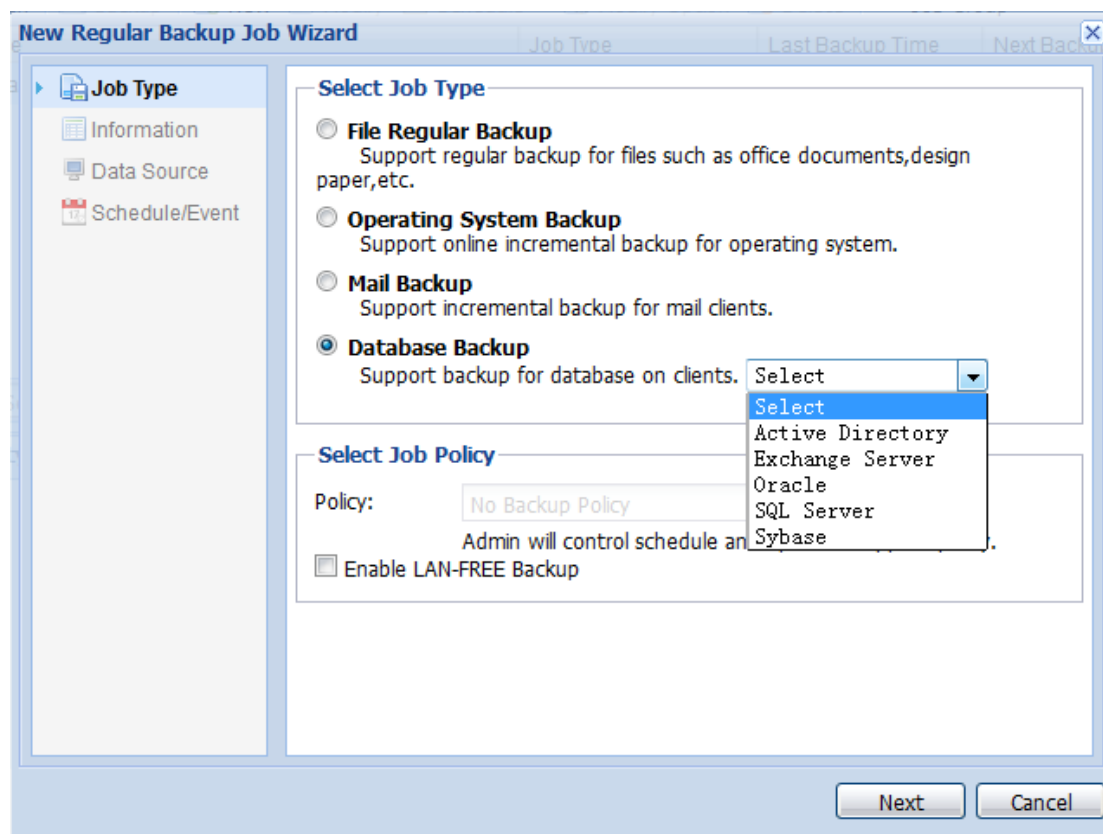


Figure 105 New SQL Server Backup Job

Step Two: In the [Information] dialog box, input job name, select data source selection mode and data type. Click [Next].

Step Three: In the [Data Source] dialog box, select databases under SQL Server (users are recommended to backup all of the databases. Unnecessary database could be neglected according to Client requirements). Click [Next].

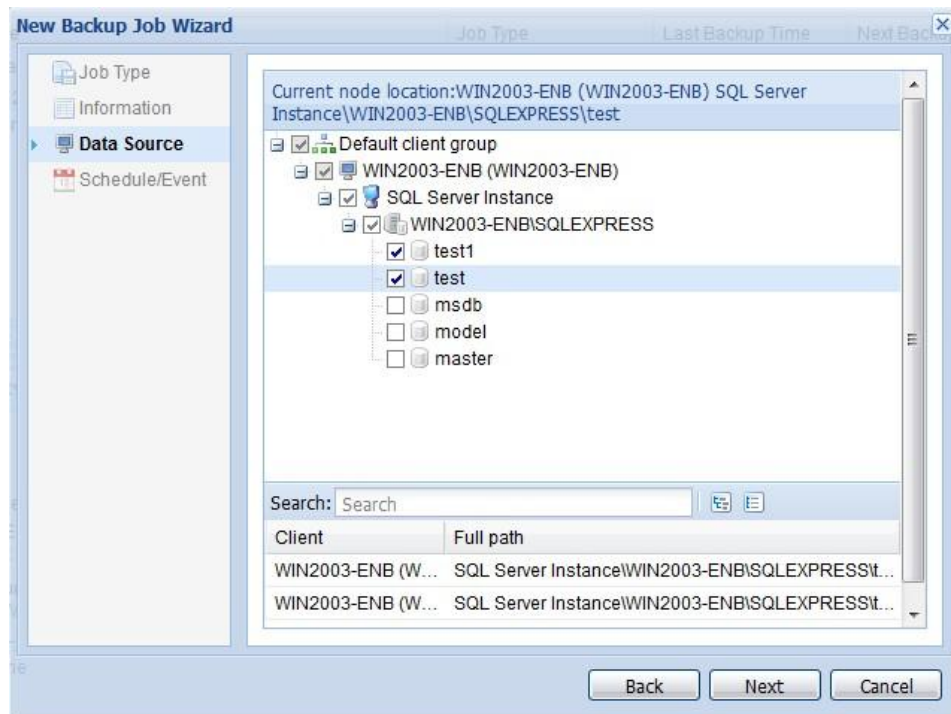


Figure 106 Select Data Source

Notes: For SQL Server database, we suggest create a job for each Client, and then select the whole SQL Server to backup.

Step Four: In [Schedule/Event] dialog box, users can “add, modify, delete” job schedules. Users can also click the button of [Option] at the bottom right, to set data compression, security settings and advanced Option. Click [OK] to finish the creation of new job.

6.5.3.3 Backup Policy Configuration

After selecting data source for backup, click [Next] and enter [schedule/event] dialog box. In the dialog box, users can “add, modify, delete” job schedules. Users also can click the button of [Option] at the bottom right, to set data compression, security settings and advanced Option.

- SQL job schedules: Full backup every weekend + differential backup every day+ transaction log backup every 5 (or more) hours.
- The start time is recommended to be set at the time when the server is free.
- Save the data for 4 weeks (4 full copies). This is optional for the user based on the storage space and the data storage time.

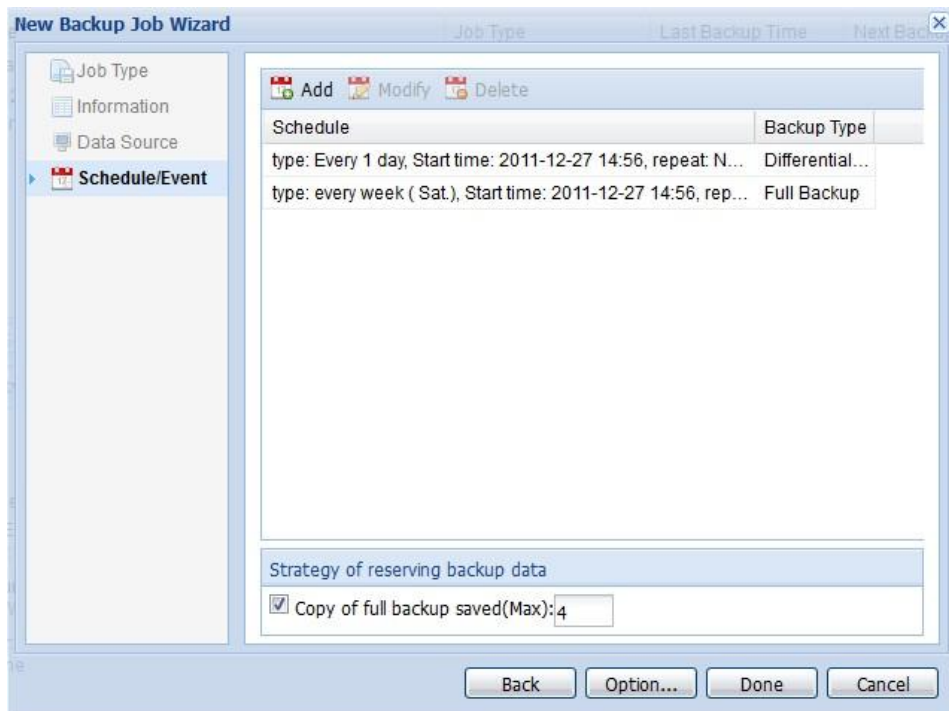


Figure 107 Schedule/Event

6.5.4 Restore Operation

6.5.4.1 Restore Notice

- To restore a database to another Client, a database server which has the same instance name with the database in source Client needs to be installed in the target Client.
- When restoring master database, SQL Server services must be restarted with single user mode. After recovery, the services will be started with multi-user mode. Therefore, all other related database services except SQL Server database services must be closed before restore.
- If the database is being used during restore, restore will fail.
- Make sure database is not connected with other applications during restore. Application connected with this database should be disconnected and enterprise manager should be closed.
- Heter-restore requires the same instance name.

6.5.4.2 Restore Operation

Step One: Login to management console and click "Backup and Restore/Restore/ Disk Data Restore" to enter corresponding page.

Step Two: Select a Client to restore from the [Client list].

Step Three: Click [Time Point] and select one time point. Then select the SQL Server database needing restore in the backup data list.

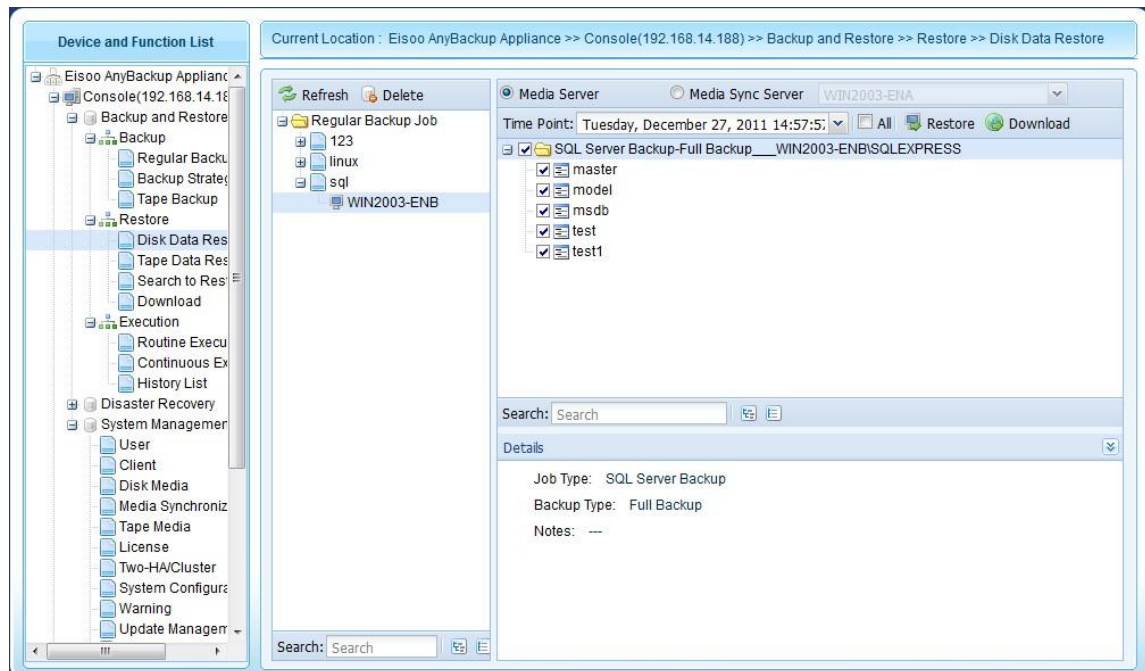


Figure 108 SQL Server Restore

Step Four: Click [Restore to client] and select client, database name and storage path in prompt dialog box.



Figure 109 Restore to Client

Step Five: Click [Restore] to submit it to execution queue.

Notes: For more details about Backup and Restore for SQL Server, please refer to best practice of Backup and Restore for SQL Server.

6.6 Backup and Restore for Oracle

6.6.1 Introduction

Oracle is a large relational database base on Structured Query Language (SQL). It is one of the most popular Client/Server structure databases.

Oracle consists of the following parts: Data, Operating system, Oracle Server, Oracle SQL Server program, Oracle tools (including SQL*PLUS, Developer 2000, and designer 2000, etc.), and all kinds of Oracle applications.

6.6.2 Backup Notice

6.6.2.1 Oracle Configuration Requirements

Before using AnyBackup Appliance to back up and restore Oracle databases, table space, control files or archive Logs, you should test whether each Oracle SID (database) needing protection meets the following conditions:

1. The AnyBackup 3.5 users should be assigned accounts which can be used to log into the Oracle database.
2. Oracle Server database log mode is set as [ARCHIVELOG].
3. Ensure that Oracle server had opened the option of "Automatic Archiving" .

6.6.2.2 Create Oracle User Account

In order to access Oracle database, the user account must has appropriate database permissions. You can use the existing user account which has the required permissions, or create new user account to meet the requirements.

To create an Oracle user account, please use Oracle Server Manager and input the following commands in prompt:

```
create user USERNAME identified by PASSWORD;  
grant sysdba to USERNAME ;
```

Replace [USERNAME] with assigned Login username, replace [PASSWORD] with appropriate password.

After inputting the above commands, the assigned user will have the appropriate permissions to protect the database.

6.6.2.3 Test Archive Log Mode

Configuring Oracle Listener before setting up archive:

Step One: Enter [net manager] > [oracle net configuration] > [Local] >

[Monitor procedures] > [LISTENER] > [Database Services].

Step Two: Add database, global database and the SID as the instance name for database. Set Oracle home directory as the installation directory.

Step Three: Click the file > Save the network configuration.

As show in the following picture:

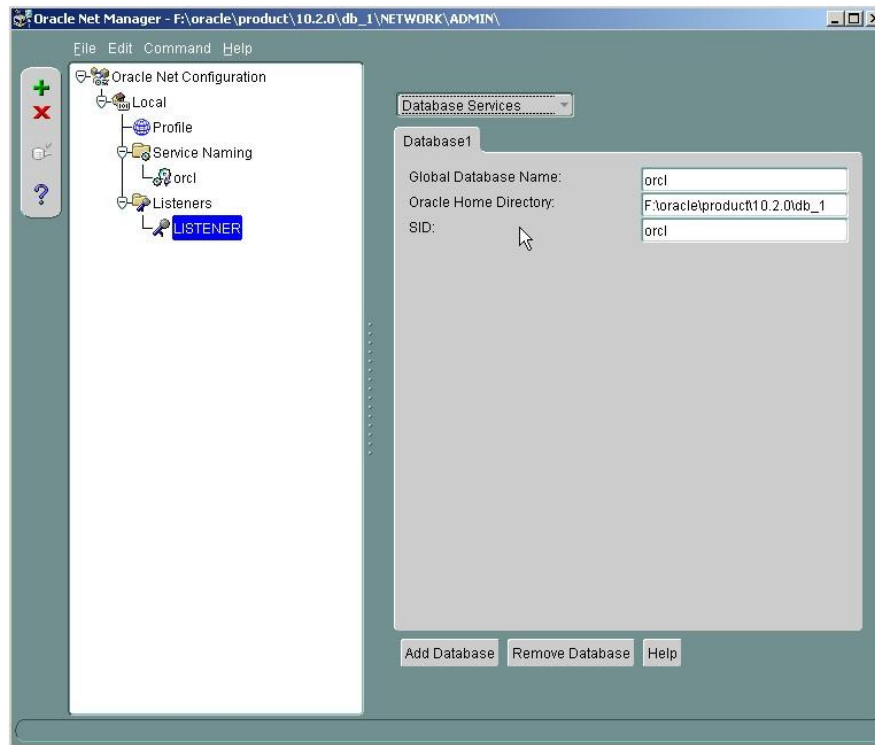


Figure 110 Archive Log Mode

Step Four: The listener configuration is finished, please check whether it is normal to start the two services.

OracleServiceEISOO (EISOO Instance name) STARTED

OracleOraHome92TNSListener STARTED

6.6.3 Oracle RAC Configuration Requirements

Oracle RAC is the abbreviation of Oracle Real Application Clusters, which supports real application operation for Oracle database in clusters. In clusters, all nodes in use share one storage location for data and have access to database directly. Data file, control file are saved in shared storage. While log files (including online log and archived log) can be stored either in shared storage or local nodes. Different RAC structures decide different storage spots but for all structures archived path can be configured as local path.

6.6.3.1 Listeners Configuration

Listeners need to be set before backup for Oracle RAC to have access to other RAC nodes of any RAC node.

Similar listeners need to be set on all nodes.

Open Listener [**Net Manager**]; add multiple nodes intense (Suppose there are two nodes in cluster.)

Node 1 adding is displayed in the following picture:

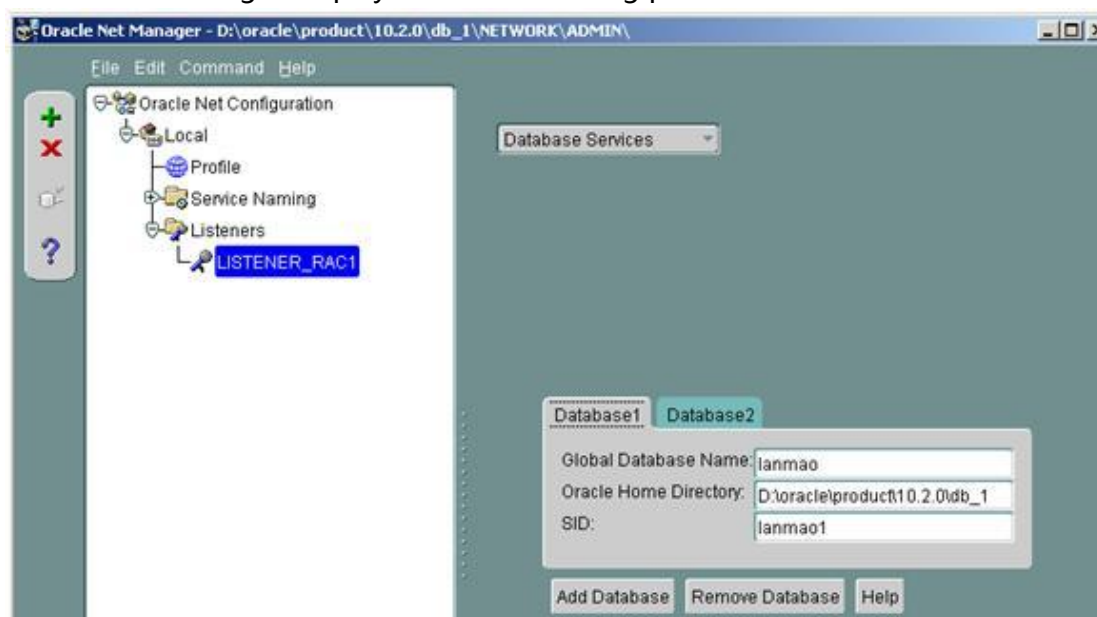


Figure 111 Listener Configuration

Node 2 adding is displayed in the following picture:

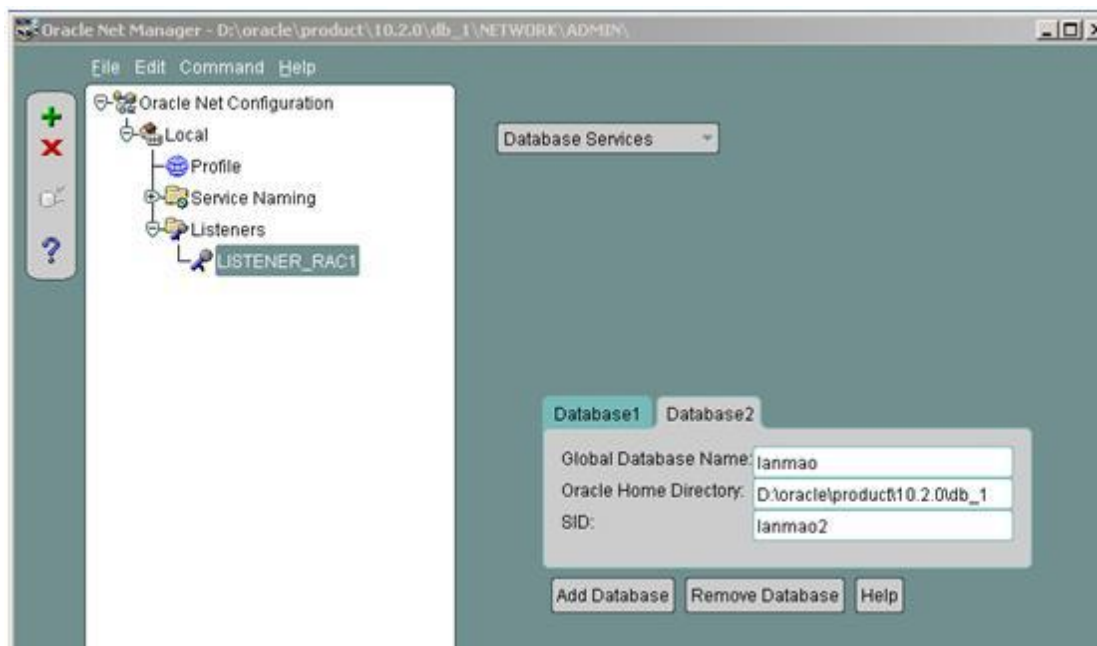


Figure 112 Listener Configuration

6.6.3.2 Archived Mode Configuration

Database need to be switched to Archived Mode and Archived Paths on each node have to be set to different local paths.

Use the statement below to configure archive on some nodes:

Execute statement under command line:

Srvctl stop database -d Global Database Name (turn off all nodes)

Login to sqlplus, and execute statement.

Sqlplus "sys/password @ instance name as sysdba" (connect to one node)

Startup mount

Alter system set log_archive_dest_1 = 'location=store absolute path of archived log node name' Sid= 'rac node name (Note: single quotation marks); (Path of every node should be different.)

Alter system set log_archive_dest_1 = 'location=save absolute path of archived log' sid= 'rac node name' (set all the existing nodes)
alter database archivelog ;

6.6.4 Backup Operation

6.6.4.1 Common Oracle Backup

◆ Oracle Configuration

Login to Management Console as administrator and click **[Client]** > **[Configure]**, a **[Modify Client Configuration]** dialog box will pop up. Select **[Oracle]** as the database supported by Client. Click **[OK]**.

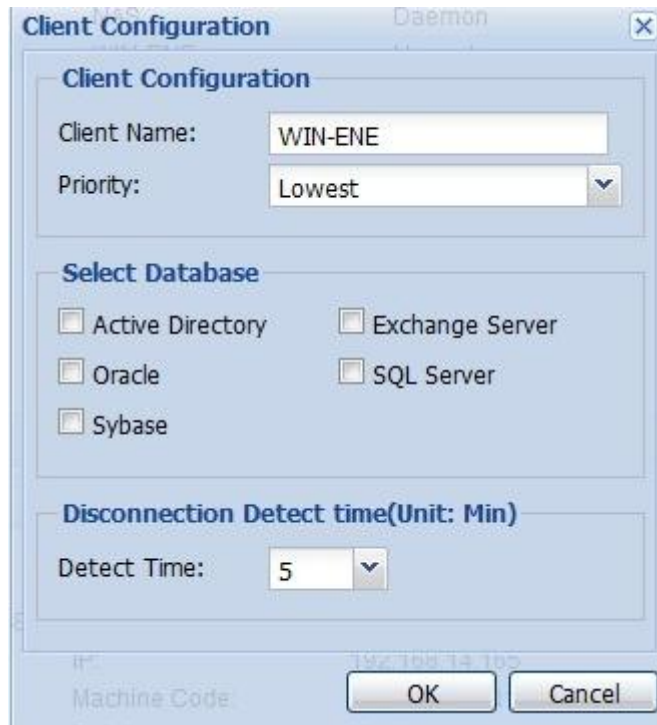


Figure 113 Oracle Client Configuration

◆ Create New Job

Step One: In Management Console, Click [Backup] >> [Regular Backup] > [New], a [New Backup Job Wizard] dialog box will pop up. In the dialog box, select [Database backup], and then select [Oracle] as the type of database. Click [Next].

Step Two: Enter the [Information] page. In the window, input the [Job name], select the [Job group], and Select the [Data source selection Mode] and [Data type]. Click [Next] to continue.

Step Three: Enter the [Data Source] page. Click [Add] in the window. And then input the [instance name], [username] and [password] for Oracle database. Click [OK]. As shown in the following picture:



Figure 114 Add Database

Unfold the Clients need to be backed up. Unfold Oracle database. As shown in the following picture:

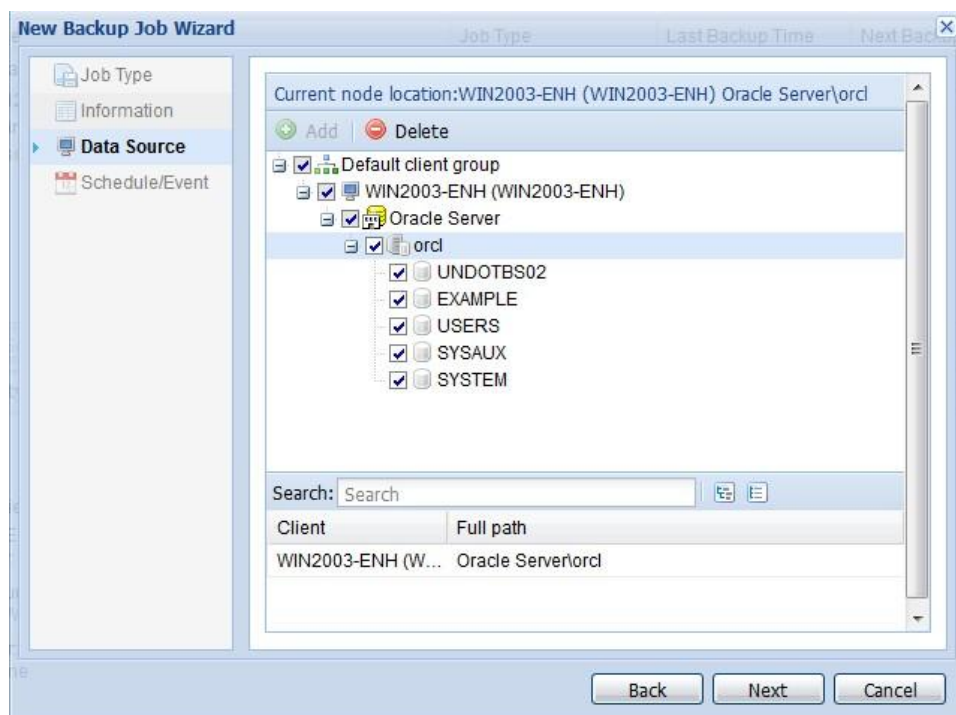


Figure 115 Select Data Source

Step Four: Enter [Schedule/Event] dialog box, you can [Add, Modify, Delete] to configure detailed schedule or you can click Option to set data compression, security configuration and advanced option according to requirements. Archived log option needs to be set to back up transaction log. Click [OK] to finish creation.

Notes: It's recommended that one client only create one job in Oracle database, and select the entire to back up.

6.6.4.2 Backup for Oracle RAC

◆ Create New Cluster

Oracle RAC Backup adopts cluster mode, that is, RAC Job is Oracle cluster job. Therefore, cluster binding needs to be established before backup for Oracle RAC.

Step One: Click [Clustered Client] in [Configuration] page to set cluster binding.

Step Two: Click [New Cluster Binding] to pop up cluster binding interface.

Step Three: Move all Oracle RAC nodes to clusters and unbound client list will not display bound two-node/cluster clients.

Step Four: Click [OK] to view client numbers. "This binding is cluster binding and must include two or more clients, please select client member again" will prompt up. Only enough clients can make a cluster.

◆ Client Configuration

Step One: Click [Configuration] > [Client] > [RAC client] > [Configure]

Step Two: Select Database Type as Oracle in Client Configuration Dialogue, displayed as follow:

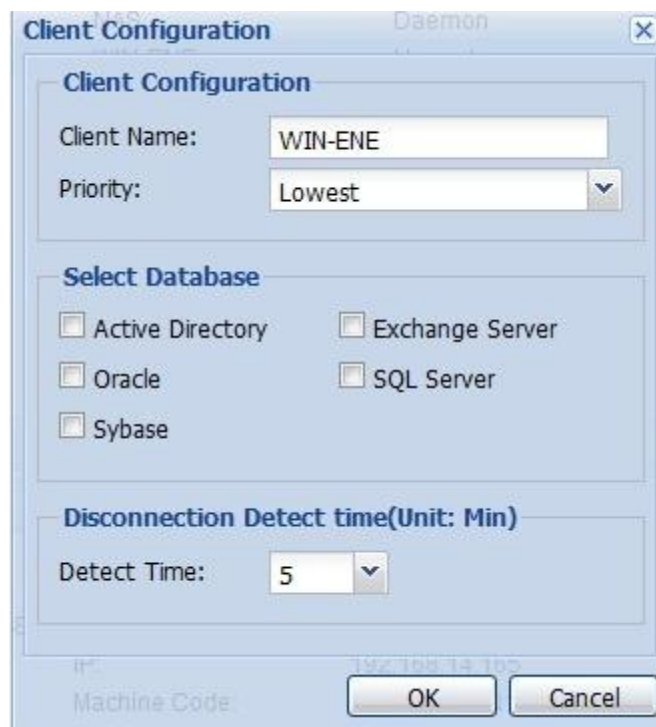


Figure 11 6 Client Configuration

◆ Create Backup Job

Step One: In Scheduled Backup Management page, click [New] and a Guide to New Backup Job dialog box will pop up. As shown in the following picture:

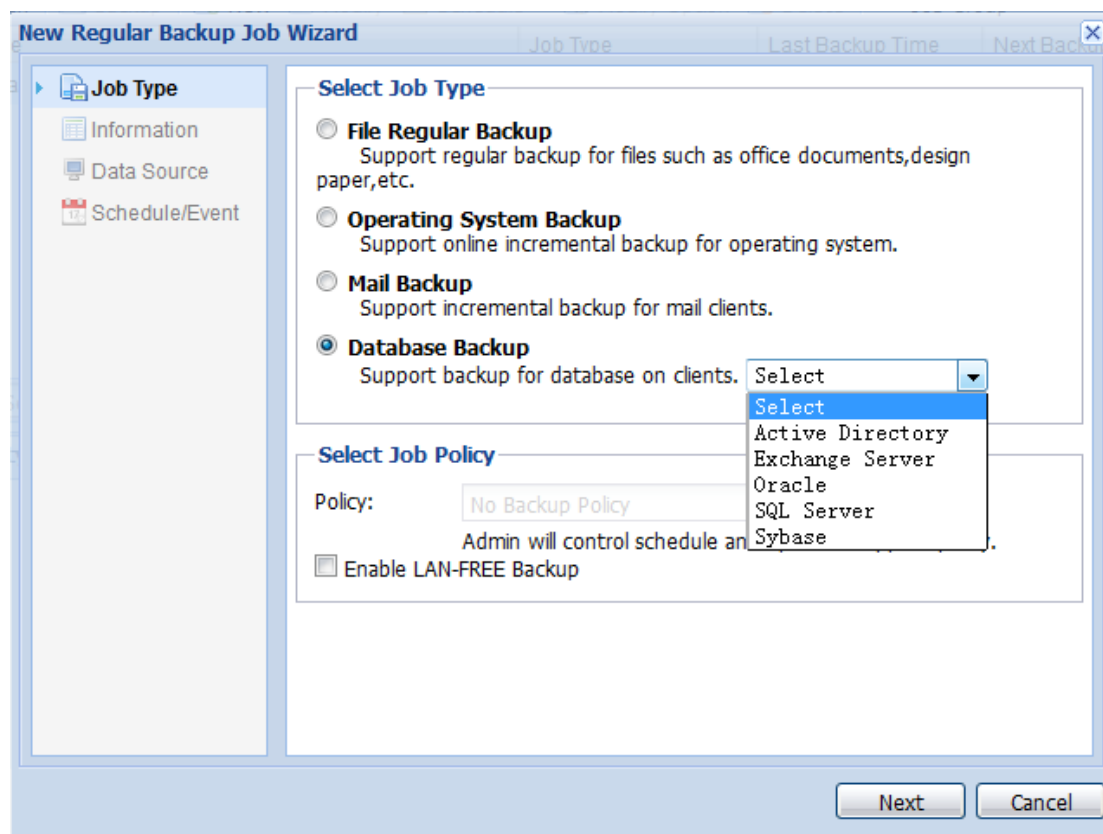


Figure 117 Select Job Type

Step Two: Select [Database Backup] in Job type and [Oracle] in Database Type, then click [Next].

Step Three: Input job name, job group, destination, and backup media. As Oracle RAC is Oracle Cluster, data type should be shared data of backup cluster server shown as the following picture. Then click [Next].



The image shows the 'New Backup Job Wizard' window, specifically the 'Information' tab. The left sidebar contains three options: 'Job Type', 'Information' (selected), 'Data Source', and 'Schedule/Event'. The main area is divided into three sections: 'Basic Job Information', 'Data Source Selection Mode', and 'Select Data Type'. In 'Basic Job Information', 'Job Name' is 'windows_rac', 'Job Group' is 'Default group', 'Destination' is 'Media Server', and 'Backup Media' has two dropdowns: 'Select server' and 'Select media'. In 'Data Source Selection Mode', 'Common Data Source' is selected with the description 'Unfold data source of client and select data to back up.', and 'Batch Data Source' is unselected with the description 'Select backup data in the same path of different clients.'. In 'Select Data Type', 'Common data' is unselected, 'Shared data of two HA servers >>> Two HA Binding' is unselected, and 'Shared file of clustered servers >>> Cluster Binding' is selected. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

Figure 118 Information

Step Four: In Data Source interface, list displays Clients of Oracle Backup with binding cluster. Click one Client Node > Oracle Server > Add and an Add Database of Oracle Server dialog box will pop up.



The image shows the 'Add Oracle Server Database' dialog box. It has three input fields: 'Instance:' with the value 'orcl', 'Username :' with the value 'sys', and 'Password:' with five dots. At the bottom are 'OK' and 'Cancel' buttons. There is a faint 'Search!' label at the bottom left.

Figure 119 Add Database

Step Five: Add all databases to Oracle Server of every client. Select all databases under the client shown in the picture below. Then click [Next].

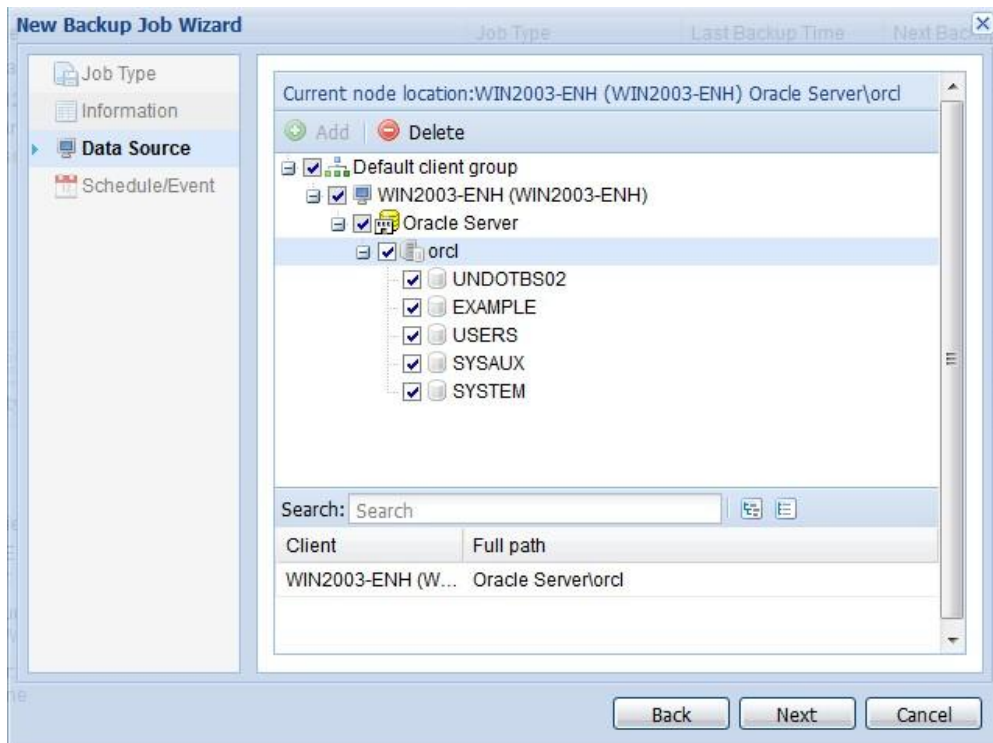


Figure 120 Select Data Source

Step Six: In [Schedule/Event] dialog box, users can “add, modify, delete” job schedules. Users can also click the button of [Option] at the bottom right, to set data compression, security settings and advanced Option. Click [OK] to finish the creation of new job.

6.6.4.3 Backup Schedule Configuration

The following contents are backup schedules to protect your Oracle Server:

- Full backup can be executed weekly and incremental backup daily for database in production, and full backup can be made in weekend, incremental backup in the evening.
- If database is few or data space is enough, full backup can be done twice a week, which depends on users’ environment.
- Save the data for one month (4 full copies). If users want to save the data for longer time, synchronizing the previous backup set to secondary media can realize it.
- Run dbcc to check database consistency before backup to ensure correctness of backup.

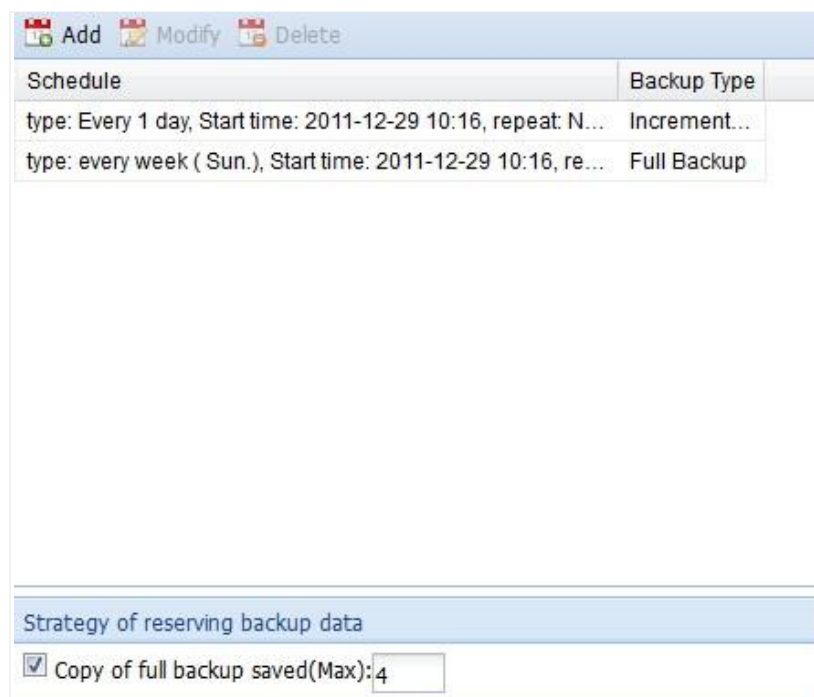


Figure 121 Backup Schedule

6.6.5 Restore Operation

6.6.5.1 Resore Physically Deleted Data or Control File

◆ Lost Data File Restore

Step One: Select the latest tiem point before data loss, then select database file in this time point as shown in the following picture:

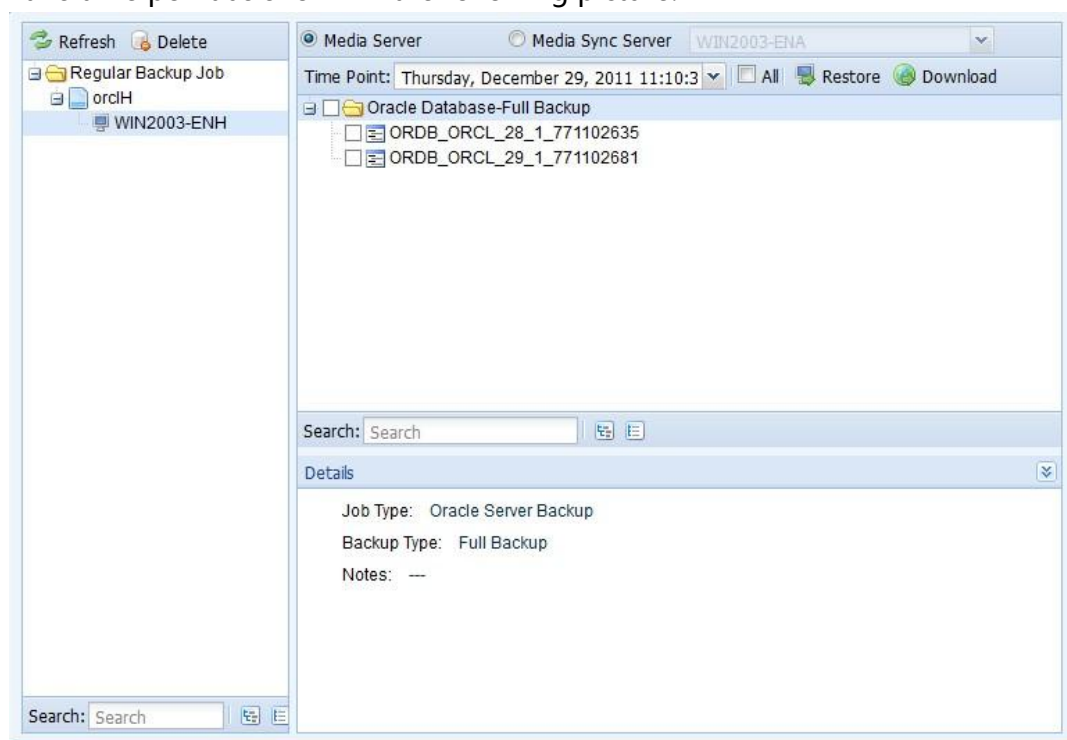


Figure 122 Backup Time Point

Step Two: Click [Restore] to pop up Oracle restore dialog box to select a specified client. In the [Redo archive log to] option, select [Latest Status of Database], then click [restore] and wait for the completion of the restore as shown in the following picture:

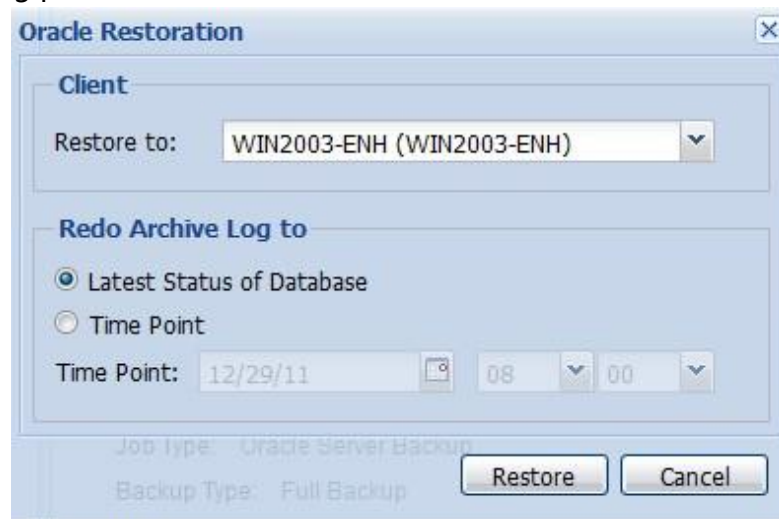


Figure 123 Oracle Restore

◆ Lost Control File Restore

Step One: Select the latest time point before data loss, and then select the corresponding control file on that point:

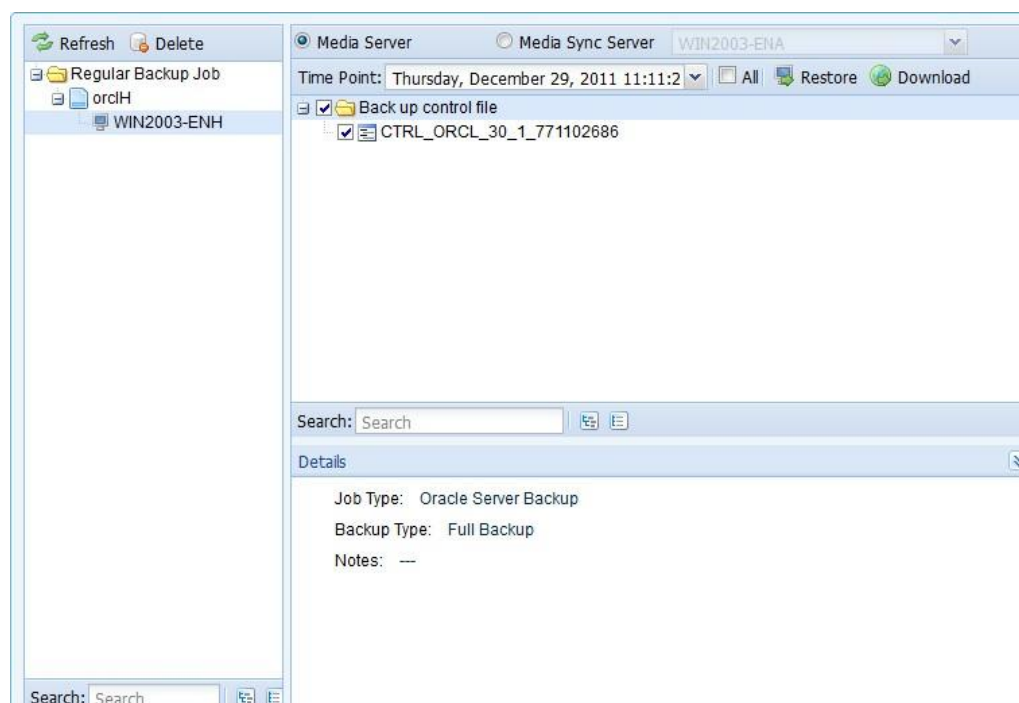


Figure 124 Oracle Data Source

Step Two: Click [Restore] to pop up the [Oracle Restore] dialog box, and then select the specified client. In the [Redo Archive Log to] option, select [Latest Status

of Database], then click [Restore] and wait for the completion of the restore.

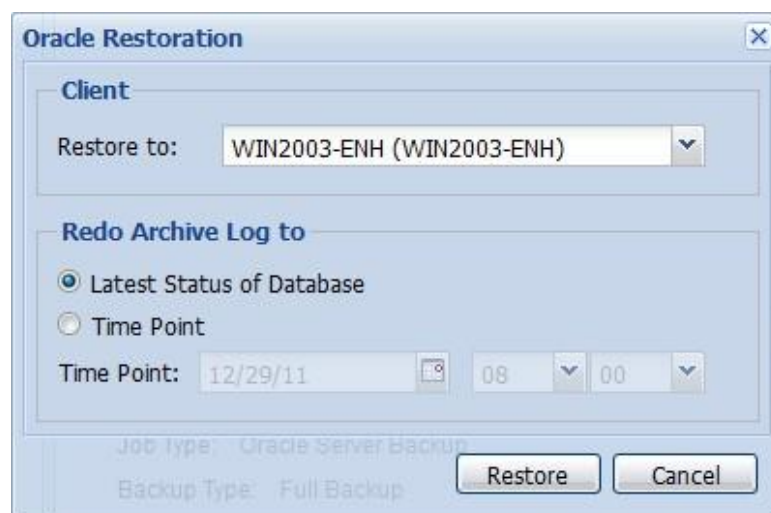


Figure 125 Oracle Archive Log

6.6.5.2 Restore Logically Deleted Table Space or Table

◆ Restore Logically Deleted Table Space

Step One: Select the latest time point before data loss, and then select the corresponding control files on the time point as shown in the following picture:

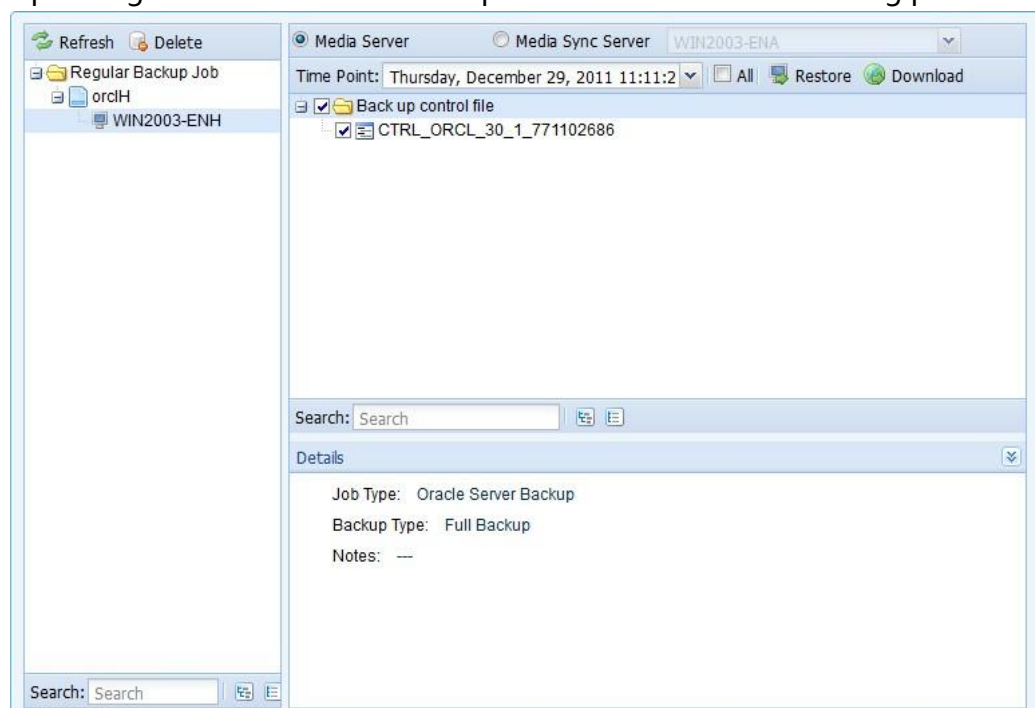


Figure 126 Select Control File

Step Two: Click [Restore] to pop up Oracle restore dialog box. Select client and [Latest Status of Database] in [Redo Archived Log]. Click [Restore] to submit restore to execution queue as shown in the following picture:



Figure 127 Oracle Restore

Step Five: Click [Restore] to submit it to execute queue.

◆ Restore Logically Deleted Table

Step One: Select the latest time point before the deletion, and select the corresponding data files at that point. Click [Restore] and an Oracle Restore dialog box will pop up.

Step Two: In the [Redo archived log to] option, select the [Latest Status of Database]. For example, a full backup is made at 8:48 but a table is deleted by mistake at 9:00, and to restore the table, the time point should be set at 8:59 as shown in the following picture:

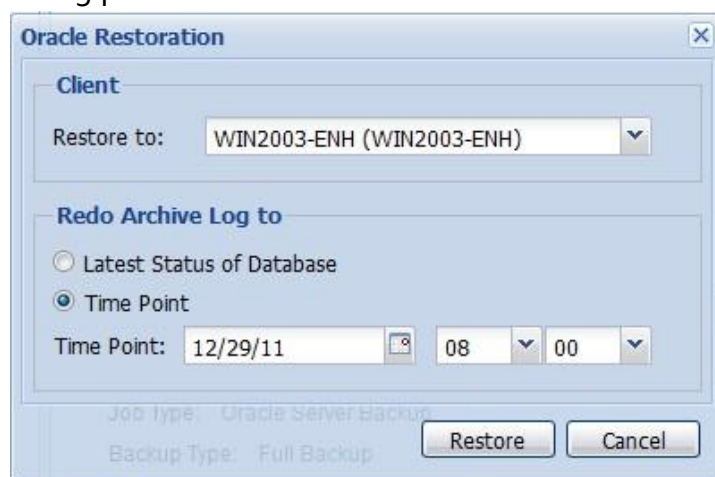


Figure 128 Oracle Archive Log

Step Three: Click [Restore] to submit it to execution queue.

Notes: For more details about backup and recovery for SQL Server, please refer to Best Practice of Backup and Restore for SQL Server.

6.7 Backup and Restore for Exchange Server

6.7.1 Introduction

When making online continuous backup for Exchange Server via EDK port, users do not need to stop Exchange Server database services, nor do they need to switch the database status. The backup execution will not pose evident impact on the performance of Exchange Server. Usually, when making full backup for Exchange Server, all the database files and log files will be backed up. After the backup, a break-in operation will be done to transaction log files. That is to say, the transaction log files which have been backed up will be deleted, and then the backup time point will be recorded. Meanwhile, when making incremental backup for Exchange Server, all the database log files will be backed up. After the backup, a break-in operation will also be done to transaction log files.

Notes: Exchange Server 2003 must upgrade SP1 service pack. Only SP1 and higher versions of Exchange Server support incremental backup and restore.

6.7.2 Backup Operation

6.7.2.1 Exchange Server Configuration

Login to Management Console as administrator and click [Configuration] > [Client] > [Configure], the [Modify Client Configuration] dialog box will pop up. Select [Exchange Server] as the database supported by Client. Click [OK].



Figure 129 Client Configuration

6.7.2.2 Create New Job

Step One: In Management Console, Click [Backup] > [New], the [New Backup Job Wizard] dialog box will pop up. In the dialog box, select [Database backup], and then select [Exchange Server] as the type of database.

Step Two: Click [Information], input job name, select data source and job type. Then click [Next].

Step Three: In the [Data Source] window, unfold the Clients need to be backed up, unfold Exchange Server database as follows:

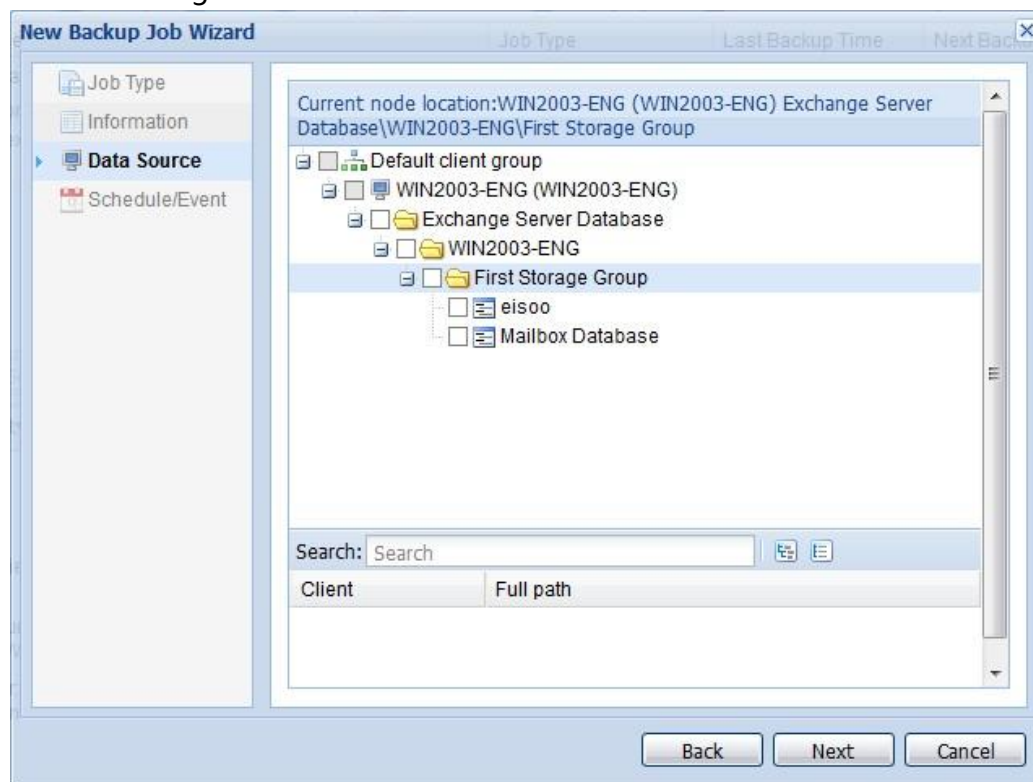


Figure 130 New Exchange Server Job

Step Four: In [Schedule/Event] dialog box, user can “add, modify, delete” job schedules. Users can also click the button of [Option] at the bottom to set data compression, security settings, file filter, media option and advanced option. Click [OK] to finish the creation of new job.

Note: It is recommended that one client only creates one job in Exchange Server database.

6.7.2.3 Backup Policy Configuration

In order to provide better protection for Exchange Server, we provide Backup Policy and the recommended configuration according to various situations.

Suggested Policy:

- Exchange Job Schedules: Full backup every weekend + daily incremental backup (According to user' s need)

- The start time is recommended to be set at the time when the server is free.
- Save the data for 4 weeks (4 full copies). This is optional for the user based on the storage space and the data storage time.

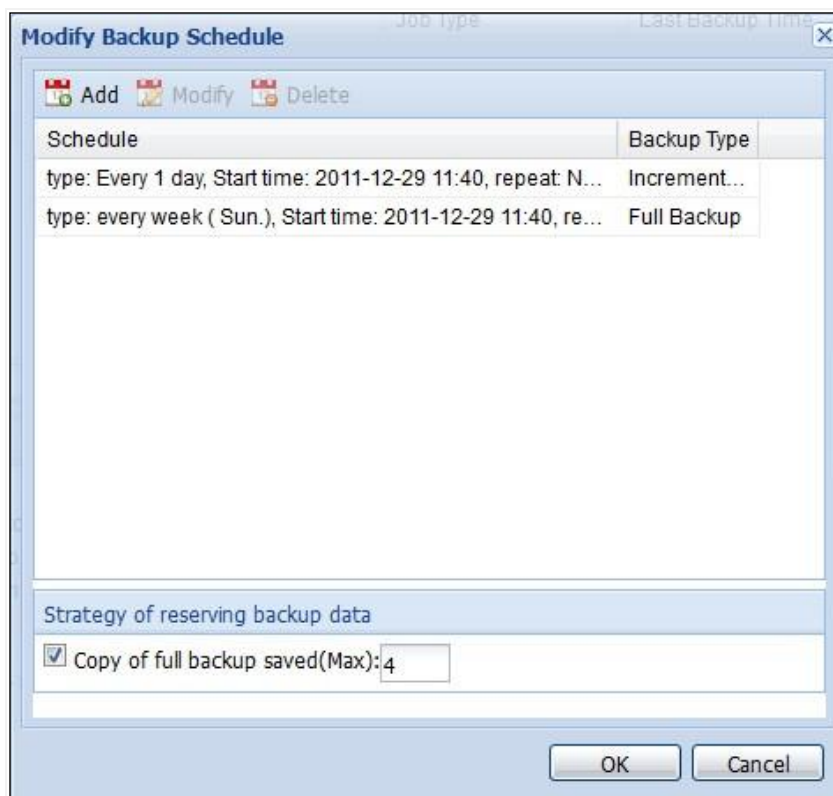


Figure 131 Backup Policy

6.7.3 Restore Operation

6.7.3.1 Restore to Specified Time Point

Step One: Check the default sharing of the partition where the Exchange Server is installed and set "write permission" .

Step Two: Uninstall the target databases from the Exchange Server Manager.

Step Three: Open the database in the Exchange Server System Manager and select the check box "Database won't be overwritten when being restored" .

Step Four: In Management Console, Click [Restore] to enter the default [Browse] page. Select Exchange Server, corresponding backup job and the time point, then click [Restore], and a [Exchange Server Restoration] dialog box will pop up. In this dialog box, do not select Auto-repeat transaction log after restore. Then click [Restore] as shown in the following picture:



Figure 132 Exchange Server Restore

Step Five: Redo the transaction log restored to the Exchange Server into a specific time point manually.

6.7.3.2 Restore to Downtime

Step 1~3 are the same as operation of "restoring to specified time point" (Please refer to 3.3.1 for details).

Step 4: In Management Console, click [Restore] to enter the default [Browse] page. Select Exchange Server, corresponding backup job and the time point, then click [Restore], and a [Exchange Server Restoration] dialog box will pop up. In this dialog box, select [Automatic repetition of transaction log]. Then click [Restore].



Figure 9 Exchange Server Restore

6.7.4 Notice after Restore

6.7.4.1 Notice

➤ When restore is finished, close the default sharing of the partition where the Exchange Server is installed. The opening of default sharing allows the capacity of remote execution; which is not conducive to system security.

- Full backup for Exchange Server is necessary to execute for the first time.

6.7.4.2 Notice for Restore Time Point

When making data restore for Exchange Server, users need to consider the actual situations and then choose a time point restore data. There are the following several cases on the whole.

1. If the logs of current Exchange Server database did not lose, the data can be restored to the following status:
 - Restore to the downtime, that is, restore to the time point when Exchange Server is stopped. To restore to this point, users need to select the last time point when the machine stopped and then click the option of Auto-repeat transaction log. And then AnyBackup Appliance will restore backups at this time point to server. Making use of transaction log files under working directory, and via the function of auto-repeat transaction log, AnyBackup Appliance will restore database to the point it stopped. Users do not need to make manual operation and interference in this process.
 - Restore to any historical backup time point. That is to say, restore to a certain, precise backup time point. To restore to this point, users can select any time point and uncheck the option of Auto-repeat transaction log, and then execute the command of ESEUTIL/CC, users need to modify the name for transaction log files under Exchange Server working directory. That is because logs in working path will be repeated to database when executing ESEUTIL/cc. When the selected time point is not the last time point when the machine stopped, the error “the existing logs are not continuous” will occur. If users select the last backup time point, the logs will be repeated to the last point when the machine stopped. Therefore, users need to modify or delete the name for Exchange log files first and then manually input the ESEUTIL/cc command according to prompts during restore, to restore the restored databases and files.
2. If the logs of current Exchange Server Database are lost, the backups can only be restored to a certain time point. The backups can't be restored to the point at which the machine stopped.

6.7.4.3 Notice for Heter-restore

Only conditional heter-restore is supported:

- Name of target machine should be the same as that of source machine.
- Path of database file should be set the same as that of log files.

Note: For more details about Backup and Restore for Exchange Server, please refer to best practice of Backup and Disaster Restore for Exchange Server.

6.8 Backup and Restore for Sybase

6.8.1 Introduction

Sybase is a relational database system, which is a typical large database system run in Client/Server environment of UNIX or Windows NT platforms. Sybase provides a set of application programming interfaces and databases, which enable it to integrate with data source and servers which are non-Sybase type. Sybase allows data replication in multiple databases, which enables it to be used to create multi-layer applications. The system has complete definitions for trigger, stored procedure, rule and integrity. It supports optimizing queries and has better data security.

6.8.2 Backup Notice

- Database Version: 12.5 ASE or higher.
- Backup Type: full backup and incremental backup.
- Database configuration: Data and logs should be put in different devices for incremental backup.
- Backup Object: System database, user database.
- Restore Granularity: database
- Full backup is default backup for database each time.
- Admin right (sa) is necessary during backup.

Notice: There are several important points during backup and restore for Sybase on Linux and AIX, please refer to *Best Practice for Sybackup Backup and Restore* for details.

6.8.3 Backup Operation

6.8.3.1 Sybase Configuration

Login to Management Console as administrator and click [Configuration] > [Client] > [Configure], a Modify Client Configuration dialog box will pop up. Select Sybase as the database supported by Client. Click [OK].

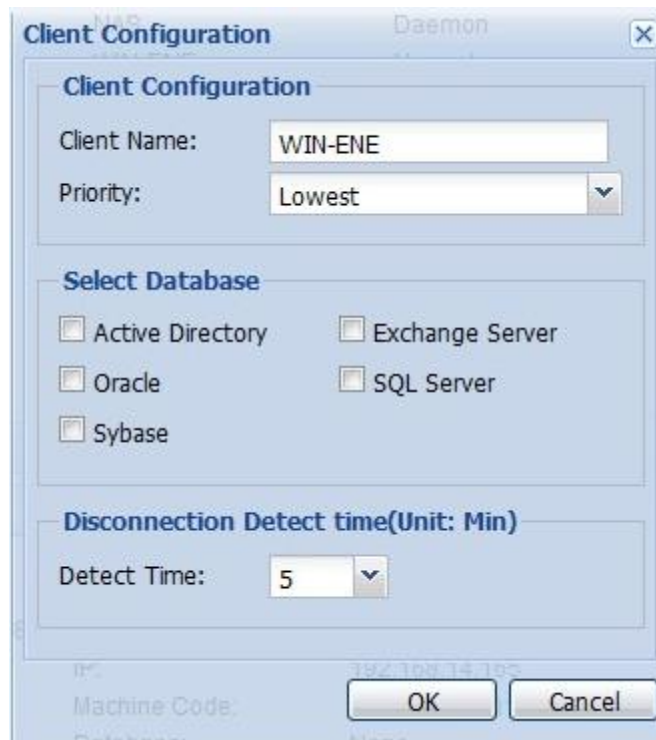


Figure 137 Sybase Client Configuration

6.8.3.2 Create New Job

Step One: In Management Console, click [Backup and Restore] > [Backup] > [Regular Backup], a [New Backup Job Wizard] dialog box will pop up. Select [Database Backup]. Select [Sybase] in the drop-down list. Click [Next].

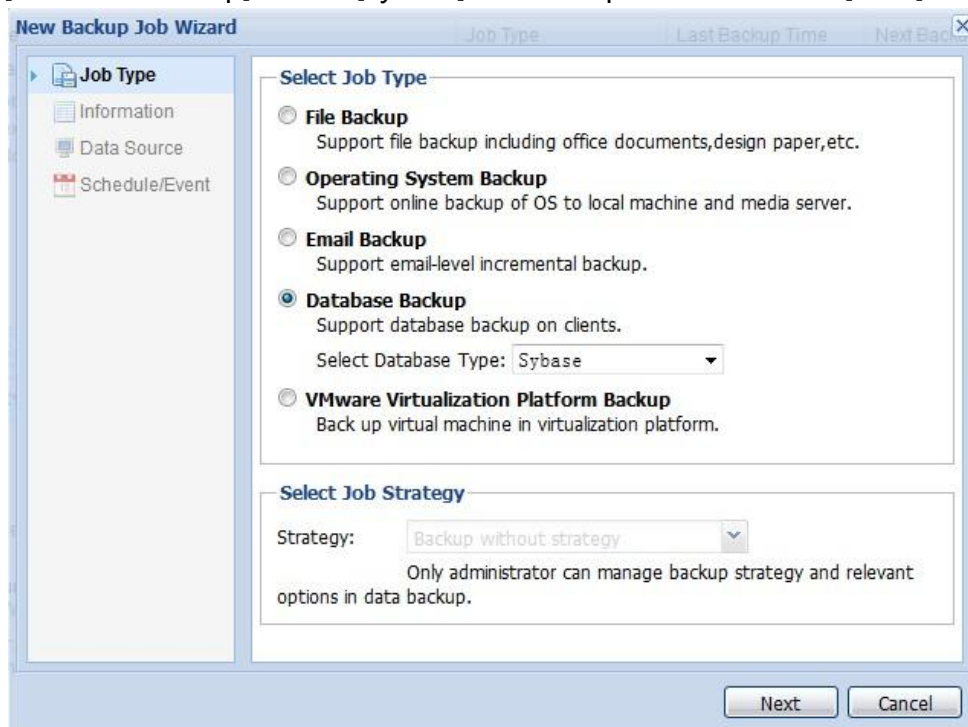


Figure 138 Sybase Backup

Step Two: In the [Basic Job Information] dialog box, input job name, select

data source selection methods and data type. Click **[Next]**.

Step Three: In the **[Data Source]** dialog box, select all the databases under Sybase (users are recommended to backup all the databases; however, users can also uncheck the databases unneeded). Click **[Next]**.

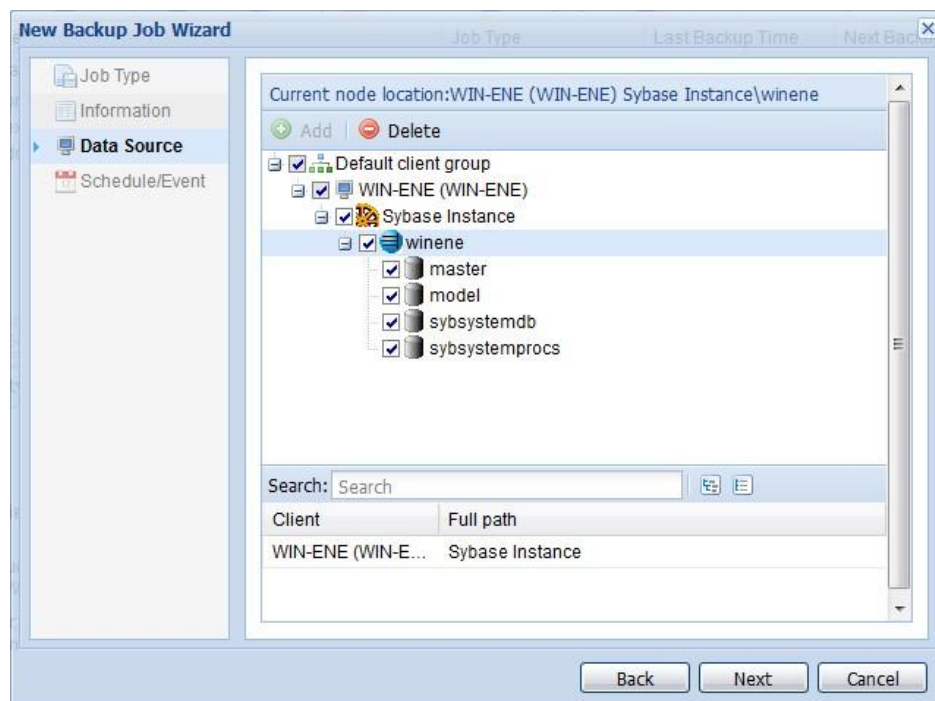


Figure 139 Sybase Data Source

Step Four: In **[Schedule/Event]** dialog box, users can “add, modify, delete” job schedules. Users can also click the button of Option at the bottom right, to set data compression, security settings and advanced Option. Click **[OK]** to finish the creation of new job.

Notes: It is recommended that one client can only create one job in Sybase database, and select the entire Sybase instance to backup.

6.8.3.3 Backup Policy Configuration

Select data source and click **[Next]** to enter **[Schedule/Event]** dialog box, in which schedule can be added, modified and deleted. Click **[Option]** to set compression, security, media option and advanced option in prompt dialog box.

- Sybase Schedule: Full backup every weekend + daily incremental backup (according to user requirements).
- Try to set the starting time at the time when the server is free.
- Preserve data for one month (4 full copies)

Notes: The database does not support saving of incremental copies. Please set “save full copies” during Configuration.

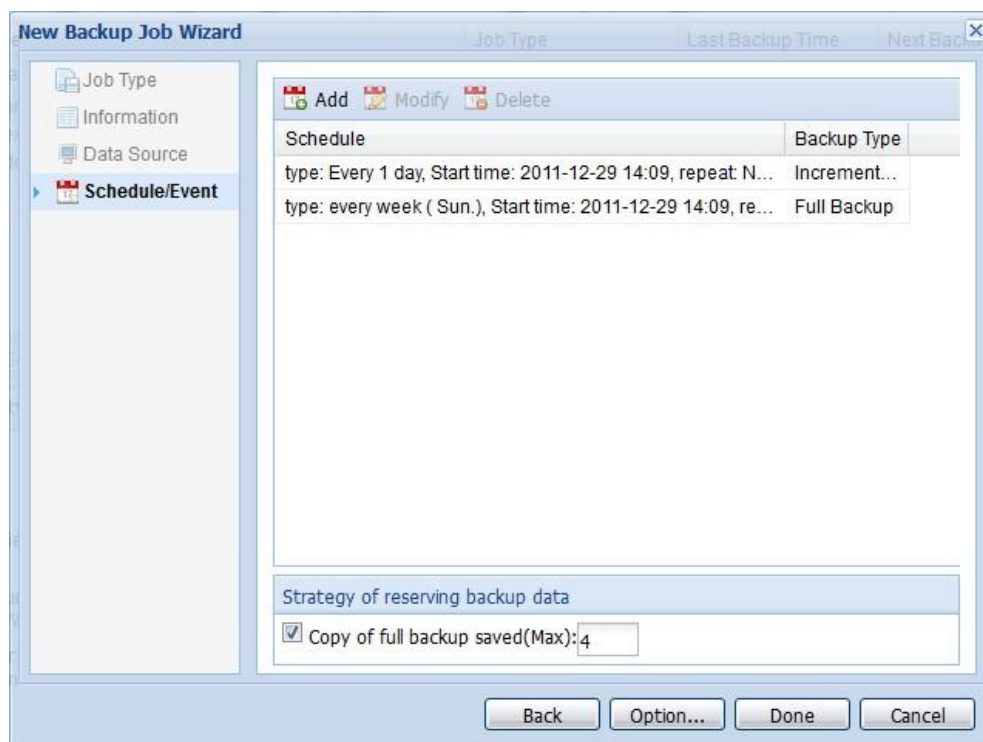


Figure 140 Sybase Schedule/Event

6.8.4 Restore Operation

6.8.4.1 Restore Mode

◆ Restore tables or data deleted by mistake:

Restore database to another client and manually import original database without influenc on busisness.

◆ Restore lost data caused by media damage:

Back up logs first, then restore.

◆ Restore database when server completely damaged by natural disaster:

Backup and disaster recovery.

6.8.4.2 Restore Operation

Step One: Log into Management Console. Click Restore to enter the default [Browse to Restore] operating system.

Step Two: Select a Client to restore from the Client list. Select the Sybase backup Job.

Step Three: Select a backup Time Point. Select Sybase database to restore in the backup data list.

Step Four: Click [Restore], a [Restore to Client] dialog box will pop up. Select the Client and position you want to restore the data to. Select the solution for "File with same name existed" .

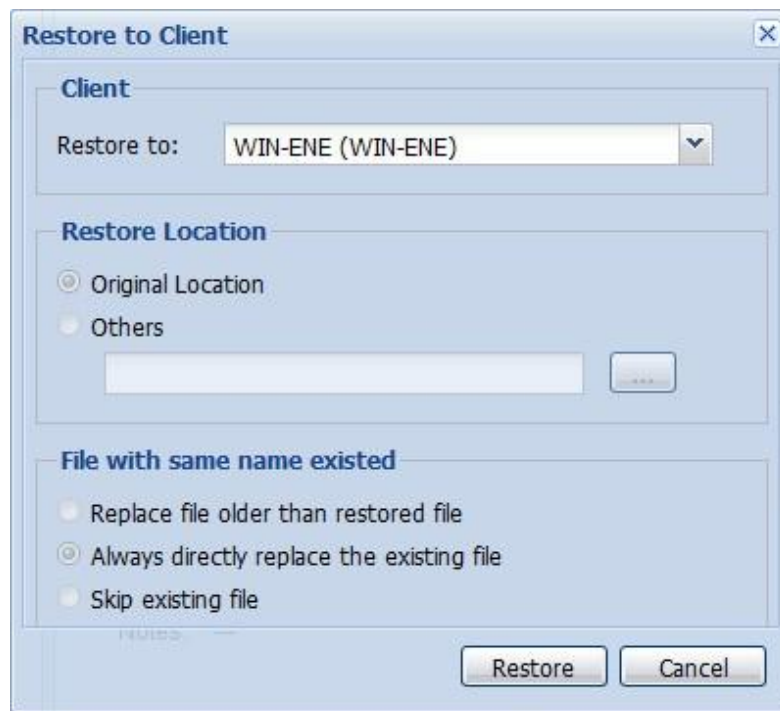


Figure 10 Sybase Client Configuration

Step Five: Click [**Restore**] to submit it to execution queue.

Notes: After the restore, users need to make full backup for the database as soon as possible.

6.9 Backup and Restore for Active Directory

6.9.1 Introduction

Active Directory services can be installed in servers running Windows Server 2000, Windows Server 2003 or Windows Server 2008. Active Directory saves the information of targets in networks; and it enables administrators and users to check and use this kind of information conveniently. Structured data storage is the base for the logic and tiered structure for the directory information of Active Directory.

6.9.2 Backup Notice

AnyBackup Appliance will make snapshot for AD via VSS first, then execute backup for database file andlog in AD snapshot. It adopts **component-based shadow copy** mode. Active Directory contains a component with the following file included:

- Ntds.dit: The Active Directory database.
- Edb.chk: The checkpoint file.
- Edb*.log: The transaction logs, each 10 megabytes (MB) in size.
- Res1.log and Res2.log: Reserved transaction logs. (No Need for Backup)

Notes: Since backup of AD only includes the above 3 files, every change of AD database would affect the 3 files. Therefore, AD only supports full backup.

6.9.3 Backup Operation

6.9.3.1 Configuration

Login to Management Console as administrator and click **[Configuration]** > **[Client]** > **[Configure]**, a **[Modify Client Configuration]** dialog box will pop up. Select Active Directory as the database supported by Client. Click **[OK]**.

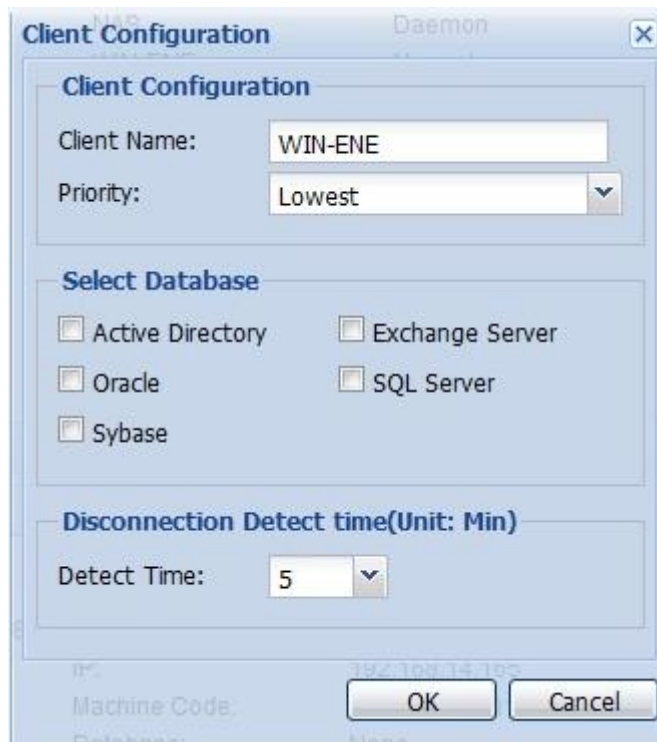


Figure 142 AD Client

6.9.3.2 Create New Job

Step One: In Management Console, click **[Backup and Restore]** > **[Regular Backup]** > **[Backup]** > **[New]**, a **[New Backup Job Wizard]** dialog box will pop up. Select Backup database. Select **[Active Directory]** in the drop-down list. Click **[Next]**.

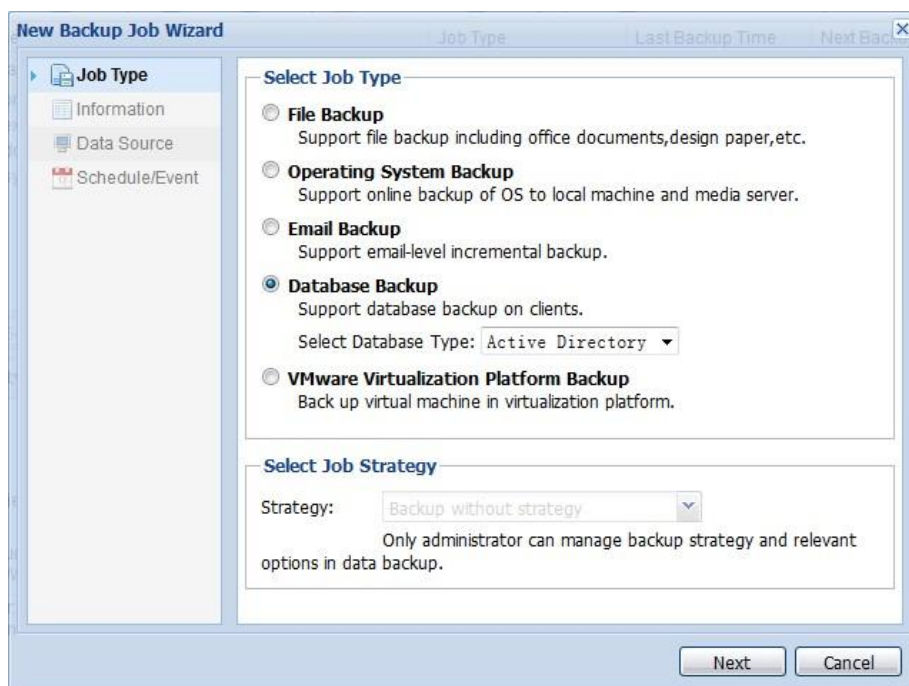


Figure 11 New Active Directory Job

Step Two: In the [Basic Job Information] dialog box, input job name, select data source selection methods and data type. Click [Next].

Step Three: In the [Data Source] dialog box, unfold Active Directory database. As shown in the following picture.

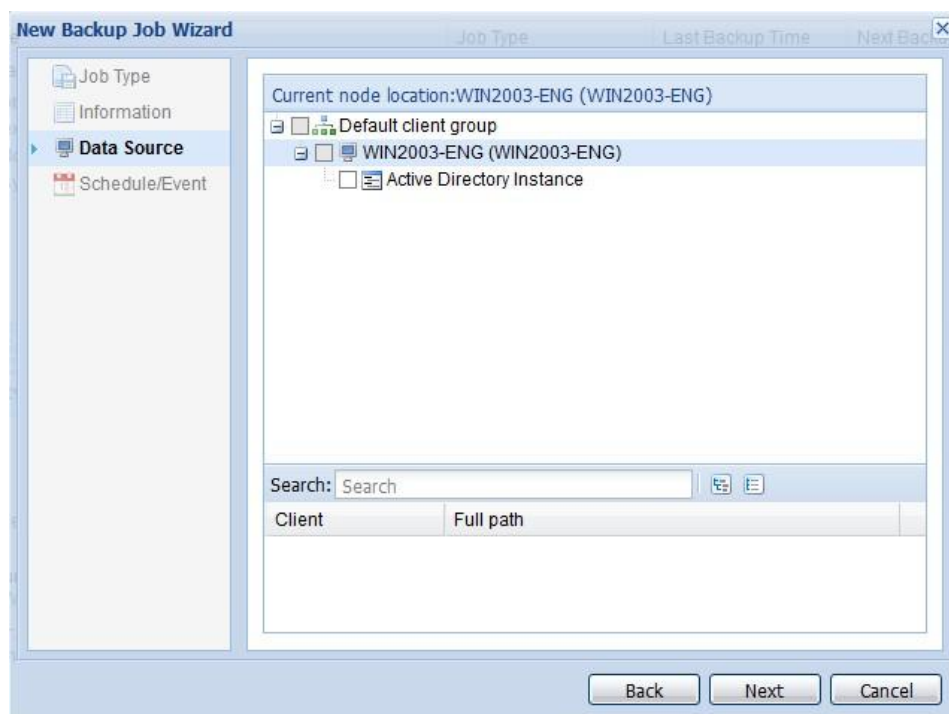


Figure 12 Active Directory Data Source

Step Four: In [Schedule/Event] dialog box, users can “add, modify, delete” job schedules. Users can also click the button of Option at the bottom right, to set

data compression security settings and advanced Option. Click [OK] to finish the creation of new job.

6.9.3.3 Backup Policy Configuration

Below are suggested backup Policy to offer better protection for your Active Directory Server. Users can make configuration according to their own needs.

- Active Directory Backup Job Schedule: full backup daily (This is flexible for user).
- Try to set the starting time at the time when the server is free.
- Save the data for one month (30 full copies). This is optional for the user based on the storage space and the data storage time.

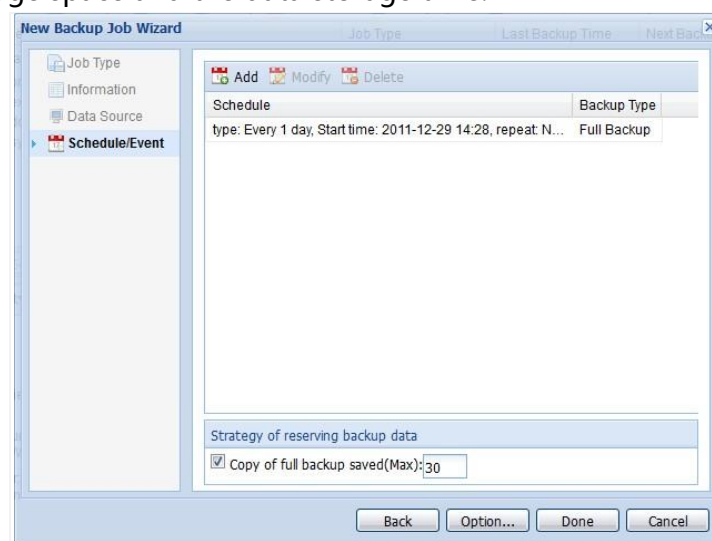


Figure 145 AD Backup Policy

6.9.4 Restore Operation

Step One: Login to management console and click [Restore] > > [Disk Data Restore] to enter corresponding page.

Step Two: In "Job-Client" list, unfold AD backup job to restore.

Step Three: Click [Time Point] to select a backup time point and select AD to restore in backup data list.

Step Four: Click [Restore to Client] and select client as restore destination. Set restore location and files with the same name.

Step Five: Click [Restore] to submit it to execution queue.

Notes: If you want to learn more about Backup and Restore for Active Directory, please refer to Best practice of Active Directory Backup and Restore.

6.10 Backup and Restore for VMware

VMware backup and restore provided by EISOO AnyBackup Appliance is based

on VCB (VMware Consolidated Backup), which is a backup solution by VMware Infrastructure 3. It is recommended to execute regular backup for virtual machine on FC or iSCSI SAN and you can also use Consolidated Backup to execute regular backup for virtual machine on ESX Server, which is inaccessible to shared storage.

6.10.1 Introduction of Backup Modes

◆ SAN

In VMware environment, if virtual disk file is saved in either FA SAN or iSCSI SAN, SAN mode can be selected for backup and backup load will be transferred to VCB Proxy. If VCB Proxy still backs up media server, LAN-free backup can be realized.

◆ SCSI Hot-Add

In this mode, a virtual machine can be set as VCB Proxy to back up other virtual machines, the storage of which should be visited by ESX service that VCB Proxy locates. There is no need to set a physical server as VCB Proxy and SAN LUN does not need mopping to Windows VCB Proxy in this mode.

VCB can be used to back up any virtual disk file of any kind of storages that are displayed in ESX server, including NAS and local disk, but for physical compatibility RDM.

VCB should create a snapshot for virtual machine that needs backup and add virtual disk file of snapshot to VCB Proxy online, thus it can access to data in virtual disk file. I/O stack of ESX host is used by VCB Proxy to read data.

🔥 Notice: If virtual machine in user's environment is not stored in FC SAN or iSCSI SAN and virtual machine to be backed up is of high performance, a new virtual machine can be created as VCB proxy server and hotadd mode can be selected for backup. Besides a VCB proxy assistant virtual machine should be created and backup speed will be twice as fast as nbd (nbdssl).

◆ LAN(NBD/NBDSSL)

If NAS is used as shared storage, NAS mode should be selected by VCB Proxy for backup. In this mode, ESX server will read data from NAS shared storage and transfer data to VCB proxy via network.

🔥 Note: nbdssl mode and nbd mode is similar to each other, also in speed, while nbdssl adopts encrypted backup for backup with high demand for security.

6.10.2 VCB Functional Limitation

1. VCB cannot back up virtual machine with RDM, but can support RDM with

virtual compatibility mode.

2. For virtual machine with local storage or NAS storage in virtual platform, only nbd mode backup can be used with low efficiency.

3. VCB proxy must be installed on Windows.

4. If VCB backup with LAN (nbd) mode is adopted, size of virtual disk file should be less than 1TB.

5. Virtual machine to be backed up should install VMware Tools; otherwise backup snapshot created by Consolidated Backup is only snapshot before breakdown and cannot guarantee consistency of application data.

Notice: Application data consistency here does not refer to read and write operation of IO during backup to ensure data consistency. For example, if a big file is being copied during virtual machine backup and finished before backup ends, the big file cannot be consistent when it is restored. That is, data consistency after data change during backup cannot be guaranteed. As static mechanism is adopted when virtual machine backup starts, virtual machine of static status will be backed up. After installation of VMtools, application data consistency can be guaranteed, which means original application can be normally used and data will be consistent with that before backup. For example, the number of tables and data in these tables of SQL Server before backup are consistent with these after restore and SQL server can also be normally started.

6. File backup can be supported for virtual machine with operating system such as Microsoft Windows NT 4.0, Windows 2000, and Windows XP, windows XP Professional, Windows 2003, Windows Vista or Windows Server 2008. All client OS can support image-level virtual machine backup.

Notice: File backup is not supported.

7. The following requirements should be satisfied during SAN mode backup:

- a) Virtual machine to be backed up with trusteeship of FC or iSCSI SAN storage.
- b) If FC SAN is adopted, physical system of host bus adapter that installs FC can be used as VCB proxy and virtual machine can also be used as VCB proxy.

8. Backup for independent disk set on virtual machine is not supported, as snapshot cannot be executed.

6.10.3 SAN Mode Virtual Machine Backup

6.10.3.1 Notice before Backup

◆ Environment Requirements

1. Back up ESX Server that virtual machine locates (virtual platform)
2. VCB proxy (VCB proxy server) .

3. AnyBackup Appliance (Backup Media Server).
4. Backup Destination.

Note: For detailed environment deployment, please refer to *Best Practice for VMware Backup and Restore*.

6.10.3.2 SAN Mode Backup Environment

The following two requirements should be satisfied for san mode backup:

- A. Virtual machine of ESX Server should be stored in FC SAN or iSCSI SAN;
- B. VCB proxy should have access to iSCSI SAN where virtual machines of ESX Server locate

Note: For detailed method, please refer to *Best Practice for VMware Backup and Restore*.

6.10.3.3 Virtual Machine Backup

Step One: Create an iSCSI volume in "Disk Media/Volume" of EISOO AnyBackup Appliance and mount VCB proxy as directory in backup virtual machine.

Step Two: In "System Management/Client" page, select client for backup and click "Virtualization Configuration" to pop up the following dialog box:

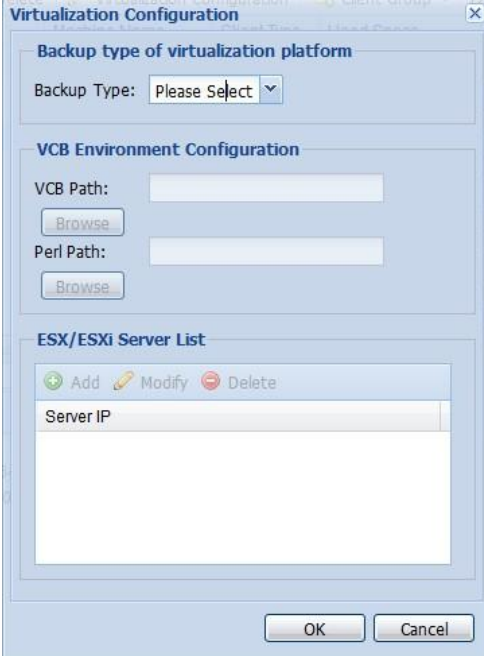


Figure 158 Virtualization Configuration

Step Three: Select "VCB" in backup type and configure VCB path and perl path. Add ESX Server address in ESX/ESXi Server list:

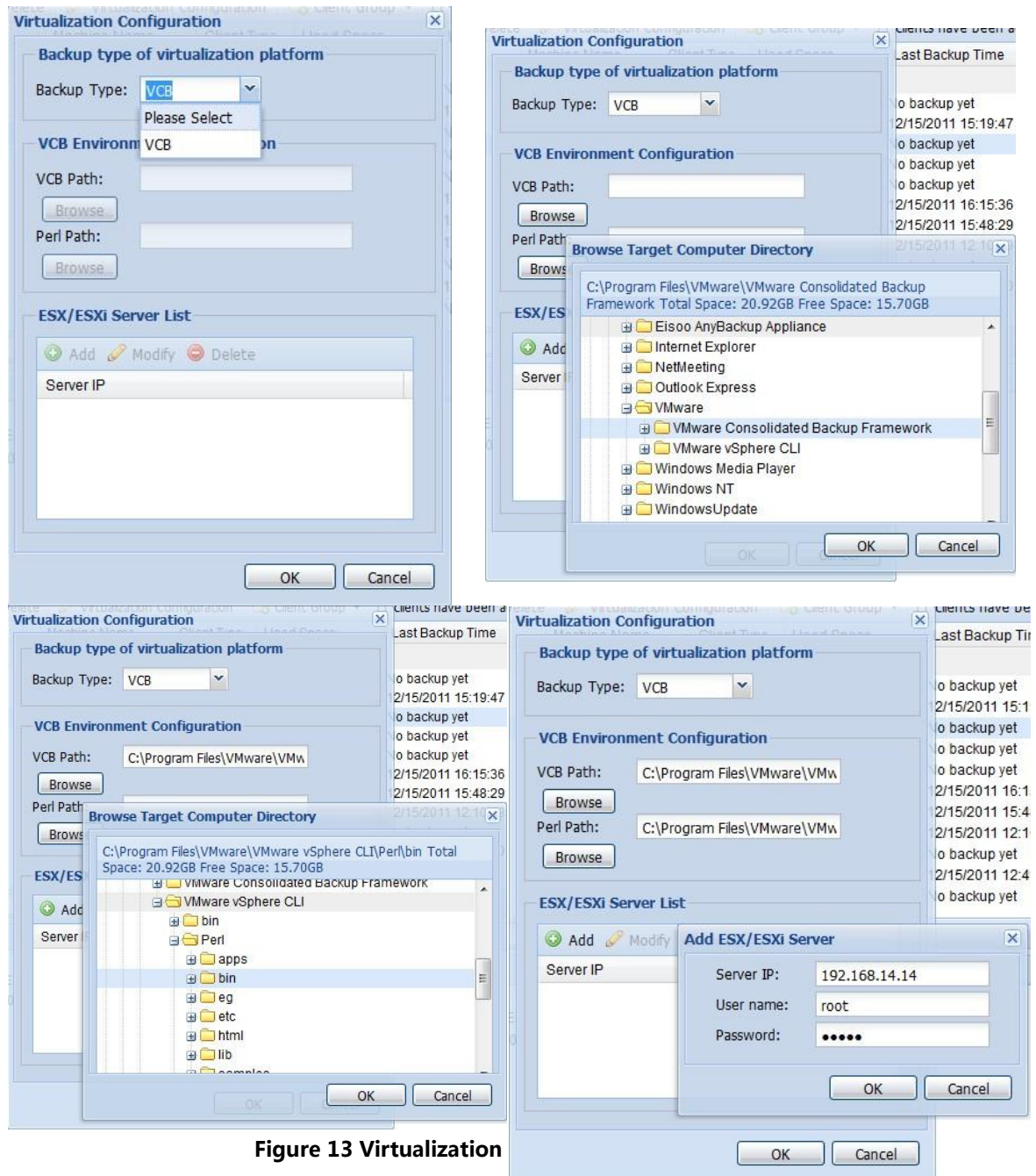


Figure 13 Virtualization

Step Four: Enter "Backup/Regular Backup" page and click [New] to pop up a dialog box. Select [VMware Virtualization Platform Backup] and click [Next].

Step Five: Input job name and select job group, data source, data type, ect in prompt dialog box. Click [Next] to continue.

Step Six: In data source dialog box, unfold backup client and mark virtual machine for backup. Click [Next] to continue.

Step Seven: In backup destination dialog box, click [Browse] to pop up a dialog box. Select iscsi volume mounted on VCB proxy as backup destination and click [Next].

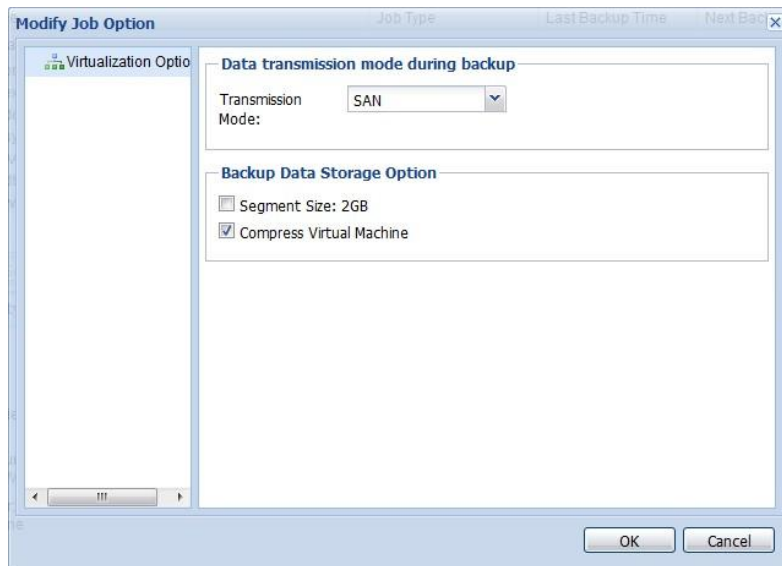


Figure 14 Backup Destination

Step Eight: In [Schedule/Event] dialog box, set schedule, backup type and copies for virtual machine backup. Click [Option] to select SAN in prompt dialog box or storage for backup:

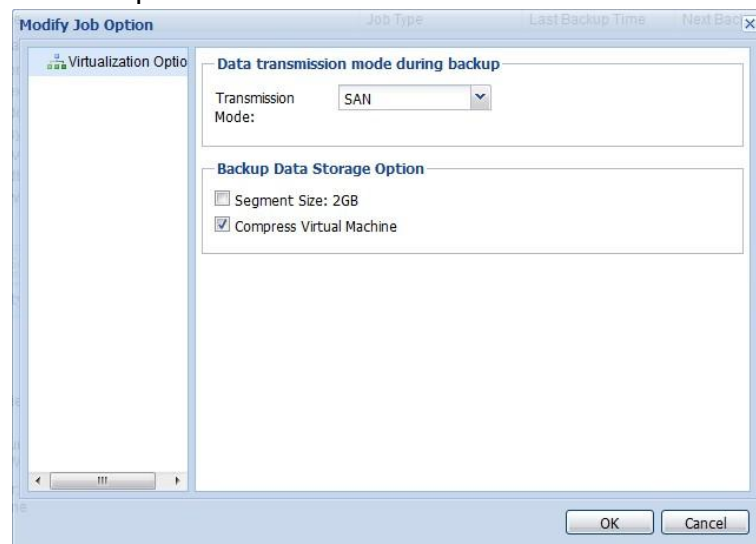


Figure 161 Job Option

Step Nine: Click [Done] to finish job configuration and execution dialog box will pop up. Select backup type (full backup is default) and click [OK] to enter execution page. You can view execution in “Execution/Routine Execution” for details.

Note: As only SAN mode virtual machine backup is introduced, please refer to *Best Practice for VMware Backup and Restore* for details.

6.10.4 Virtual Machine Restore

Step One: Run VMware Converter tool on VCB proxy.

Step Two: Data source type is **Backup image or third-party virtual machine**. Click [**Browse...**] and select virtual machine that has been backed up successfully as

shown in the following picture:

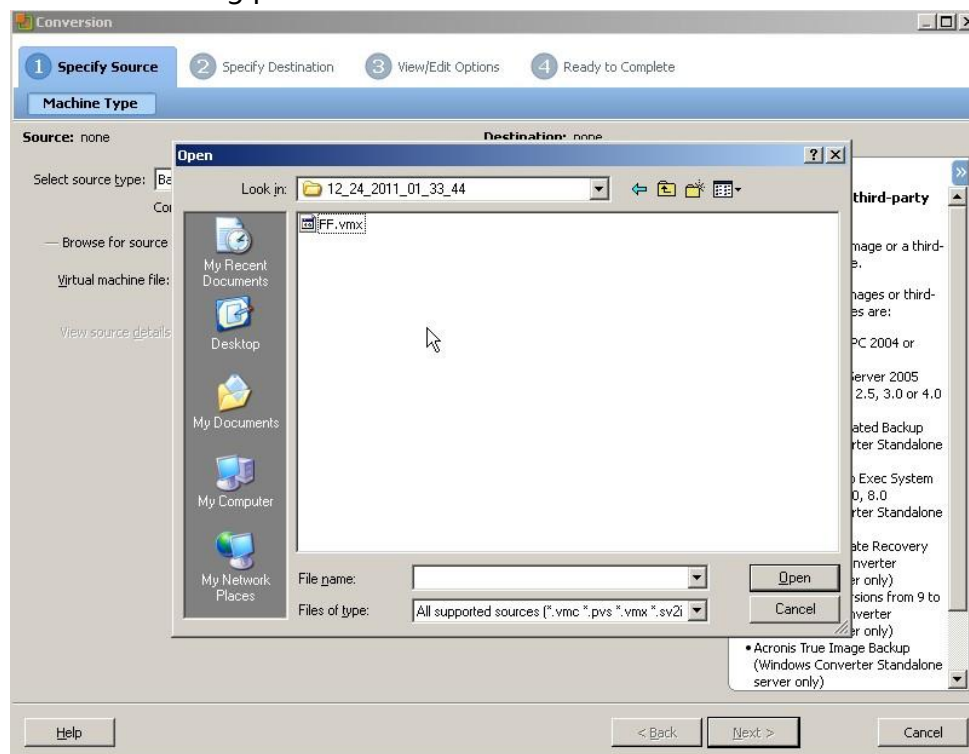


Figure15 Select Data Source

Step Three: Select ESX Server and its IP address, username and password for restore destination as shown in the following picture:

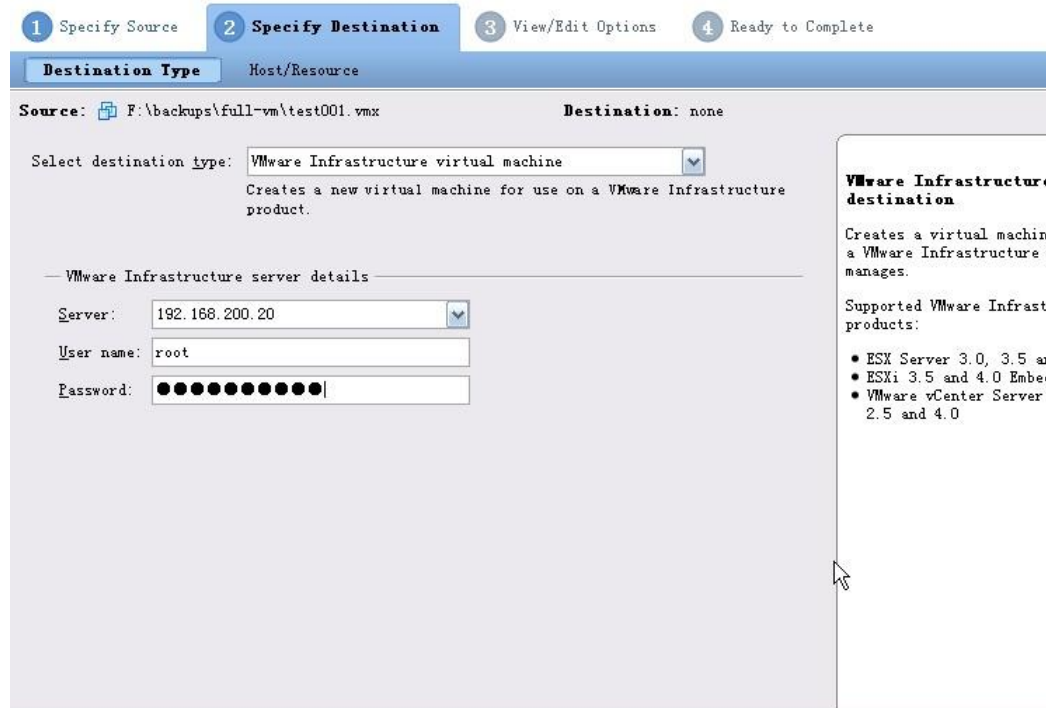


Figure 16 Restore Destination

Step Four: Select corresponding source pool of ESX Server platform and inout virtual machine name after restore as shown in the following picture:

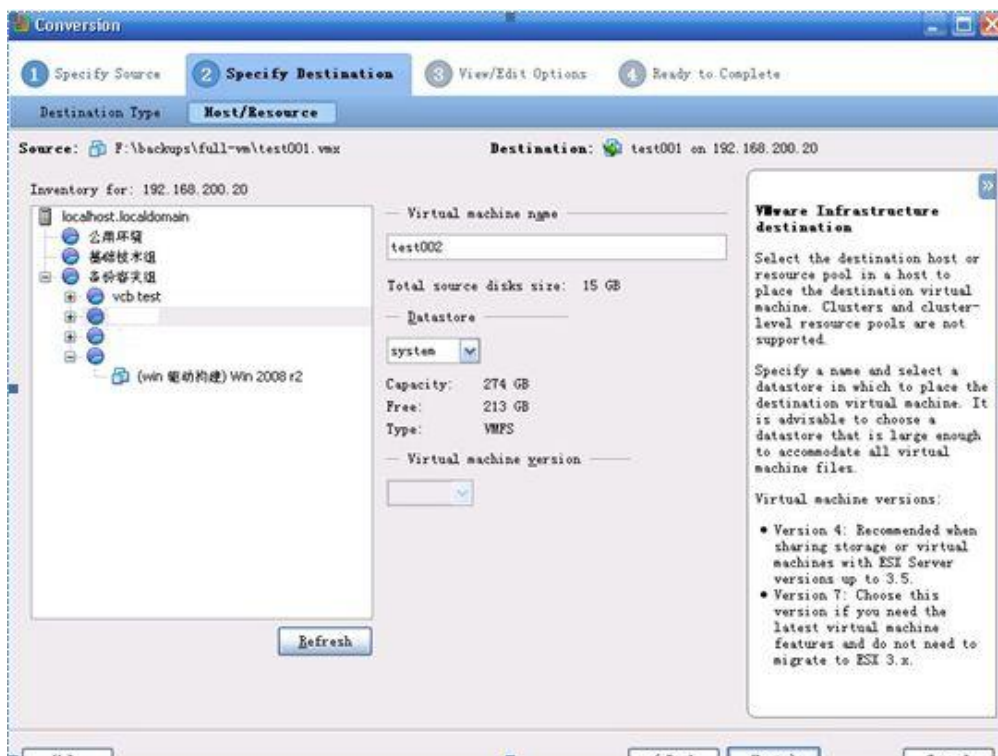


Figure 164 Source Pool

Step Five: Start restore and after restore status should be “Completed” as shown in the following picture:

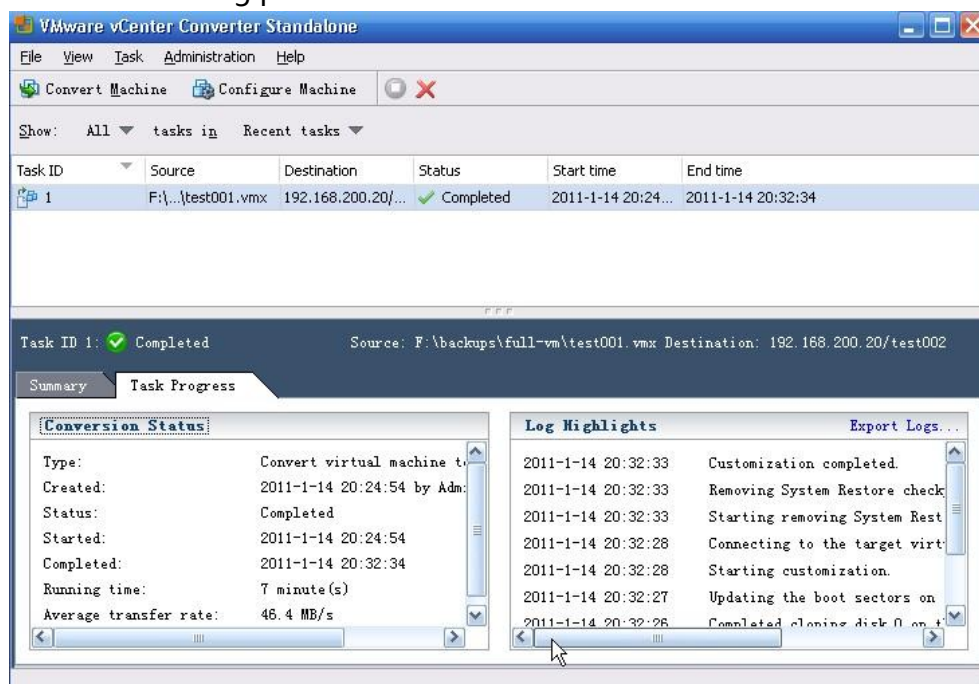


Figure17 Restore Completed

Chapter 7 System Recovery

7.1 System Recovery Environment

7.1.1 Boot from Local Disk

If you have installed System Recovery Environment in local disk, you can start System Recovery Environment directly from local disk. When users boot system, start menu item will display.

Step One: Start the computer.

Step Two: When Operating System is booted, please select EISOO System Recovery by moving the up and down arrow buttons on the keyboard.

Step Three: Press Enter to start SRE.

7.1.2 Boot from CD/DVD

If you have EISOO System Recovery CD or burnt System Recovery Environment to CD/DVD, you can boot System Recovery from CD/DVD.

Step One: Start computer, and configure CMOS\bios to ensure that the computer start from CD.

Step Two: Put System Recovery CD into CD driver.

Step Three: When computer detects CD and start from it, "Boot" will pop up.

Step Four: Press Enter to start SRE.

7.1.3 Boot from USB Device

If you have installed System Recovery Environment in USB device, you can boot System Recovery Environment from USB.

Step One: Start computer, and configure CMO\bios to ensure that computer start from USB driver.

Step Two: Connect USB to computer.

Step Three: When computer detects USB and start from it, "Boot" will pop up.

Step Four: Press Enter to start SRE.

7.2 System Recovery

7.2.1 Manual System Recovery

7.2.1.1 Restore System from Local Disk

If system backup set is saved in local Media Server, system can be restored as

follows:

Step One: Start your computer and enter System Recovery Environment, [System Recovery Wizard] will pop up automatically.

Step Two: In Welcome Page, select [Recover from Local or Windows Shared Network] and then click [Next] to continue.

Step Three: Select Disk that needs to be restored and click [Next] to continue.

Step Four: Click [Browse] in dialog box; [Select Backup Data and Time point].

Step Five: [Select Catalog Set for System Recovery] window will pop up. Click and unfold this partition to find system catalog set and click [OK] to continue.

Step Six: Back to the page of [Select Backup Data and Time point], you can select a point-in-time, and then click [Next].

Step Seven: Click [OK] to confirm system recovery information. A reallocate partition will pop up, select [NO] to execute recovery and restart computer after recovery. If not, partition will be reallocated at first, then recovery will be done, computer restarted, system restored.

Hint: Make sure that system backup set should not be stored in system disk. Local recovery is not supported by Linux system recovery.

7.2.1.2 Restore from Network

If system backup set is saved at remote Media Server, restore your system in the network as follows:

Step One: Administrator shares the directory of Media Server where backup data is saved and appoints specific user to visit it.

Step Two: Start System Recovery Environment on the remote client, in Welcome Page to select [Recover from local HDD or Shared Network Path], and then click [Next] to continue.

Step Three: Select Disk that needs to be restored and click [Next] to continue.

Step Four: Click [Map Network] in pop-up dialog box [Select Backup Data and Point-in-Time].

Step Five: The dialog box [Map Network Path Setting] will display, input IP address of Media Server, Share Name and User Name, and Password. Click [IP Setting...] at the bottom, you can input IP address, subnet mask and default gateway of your machine. Click [OK] to continue.

Step Six: In the pop-up page [Open Catalog set to Recover], double click the

folder under the directory or select the folder and click [Open] at the bottom to find out system catalog set you need. Click [OK].

Step Seven: Back to the page [Select Backup Data and Time point], select specific time point, and then click [Next].

Step Eight: Click [OK] to confirm system recovery information. A reallocate partition will pop up, select [NO] to execute restore and restart computer after recovery. If not, partition will be reallocated at first, then recovery will be done, computer restarted, system restored.

7.2.1.3 Restore from Backup Server

If system backup set has been saved on remote Media Server, restore your system as follows:

Step One: Start your computer and enter System Recovery Environment, [System Recovery Wizard] will pop up automatically.

Step Two: Select [Restore from Backup Server], then click [Next] to continue.

Step Three: If there are many disks in system, select Disk to restore and click [Next] to continue.

Step Four: In login to backup server page, input enterprise account, server address (IP of backup server installed management console), port and select login mode (Such as based on password). Input username and password to access and click [Test Connection] to connect and [OK] to continue.

Step Five: Login to Backup Server Configuration means that you need to input IP address and service port of Backup Server with Management Console installed. You also need to input the account and password of the user who has the right to visit the system backup set, then click [OK] to continue

Step Six: In prompt [Select Catalog Set to Restore] dialog box, click system backup set partition and find system catalog set to restore. Click [OK] to continue.

Step Seven: Return to "Select Backup Data and Time Point" dialog box and select restore time point. Click [Next] to continue.

Step Eight: Click [OK] to confirm system recovery information. A reallocate partition will pop up, select [NO] to execute recovery and restart computer after recovery. If not, partition will be reallocated at first, then recovery will be done, computer restarted, system restored.

7.2.2 Bare Metal Restore

7.2.2.1 Restore to Partitioned Disk

1. Use EISOO AnyBackup 3.5 Appliance to back up system to prepare original backup data for bare metal recovery.

2. Prepare a CD/DVD or USB device with EISOO System Recovery Environment installed.
3. Start your computer and configure CMOS to ensure that your computer will start from CD driver or USB device.
4. Put CD or connect USB into your computer.
5. Computer detects System Recovery CD or USB driver and start from CD or USB.
6. Press [Enter] to start System Recovery Environment.
7. Select to obtain backup data source from network or local backup server in pop-up dialog box.
8. Select system recovery backup set which needs to be restored, and click [Next] to continue.
9. If there are more than two disks in system, you can select the disk 's partition which will be restored to in pop-up dialog box [Select Job Type]. If there is only a disk, you do not have to choose.
10. Search a partition which meets the requirements of recovery in selected disk.
11. After finding the target partition, click [OK] to execute. Once execution is finished, restart your computer and the whole system is restored.

7.2.2.2 Restore to Unpartitioned Disk

1. Use EISOO AnyBackup 3.5 Appliance to back up system to prepare original backup data for bare metal recovery.
2. Prepare a CD/DVD or USB device with EISOO System Recovery Environment installed.
3. Start your computer and configure CMOS to ensure that your computer will start from CD driver or USB device.
4. Put CD or connect USB into your computer.
5. Computer detects System Recovery CD or USB driver and start from CD or USB.
6. Press [Enter] to start System Recovery Environment.
7. Select to obtain backup data source from network or local backup server in pop-up dialog box.

8. Select system recovery backup set which needs to be restored, and click [Next] to continue.
9. If there are more than two disks in system, you can select the disk 's partition which will be restored to in pop-up dialog box [Select Job Type]. If there is only a disk, you do not have to choose.
10. A dialog box is popped up to ask whether to partition new disk according to primary system. Click [OK], and dialog box [Create New Partition] will pop out.
11. Finish partitioning following the wizard.
12. After partitioning, click [OK] to execute. Once execution finished, restart your computer and the whole system is restored.

Chapter 8 Storage

Storage refers to detailed archive for all related storage functions, such as disk, sharing, iSCSI, FC SAN and mirror.

8.1 Disk

Disk management is a basic function of EISOO AnyBackup Appliance, which is realized by RAID and volume management. Admin can learn disk information and configure RAID and volume in disk management.

8.1.1 RAID

RAID is Redundant Array of Independent Disks, which is composed by many disks to improve transmission rate and fault tolerance. Click "Storage/Disk/RAID" to enter RAID management page, in which RAID can be created, configured and expanded.

◆ Create New RAID

Click [New RAID] to pop up the following dialog box:

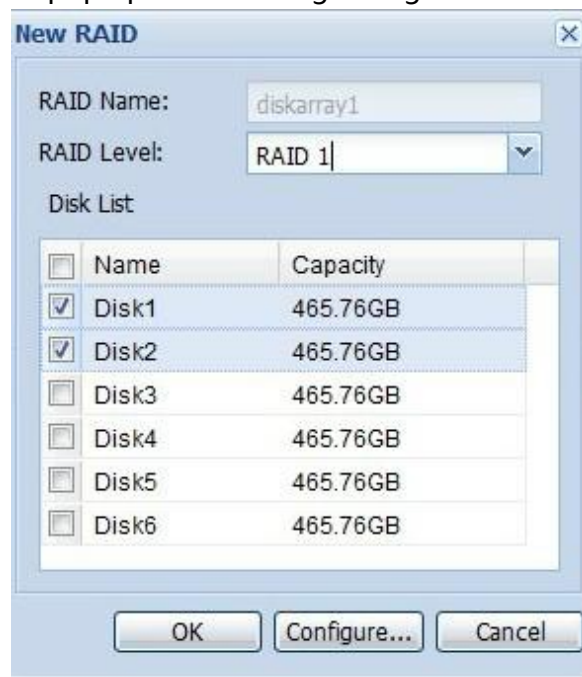


Figure 223 New RAID

- RAID Name: It is used to mark RAID, which can be named as diskarray1~diskarrayN, automatically allocated by system.
- RAID Type: RAID0/1/10/5/50/6/60. It will list created RAID type according to current disks.
 - At least two disks are necessary for creation of RAID0; Only two disks are necessary for creation of RAID1 while four or more even number disks are required for creation of RAID 10; At least three disks are

necessary for creation of RAID 5, 6 for RAID50, 4 for RAID6 and 8 for RAID60.

- In "Disk List" check bot, slect RAID disk to create.
- Click [Configure] to pop up "RAID Parameter Configuration" dialog box as the following picture:

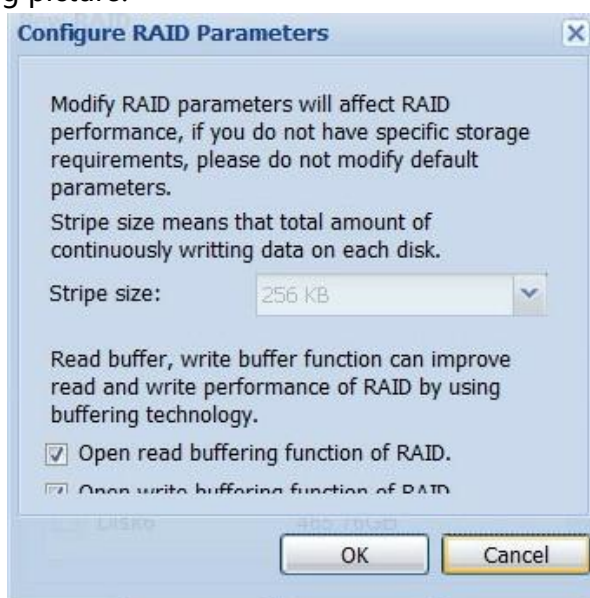


Figure 224 RAID Parameter

- Stripe siza, read/write buffer can be set in this dialog box. Click [OK] to save configuration or [Cancel] to return. It is not recommended to modify default RAID parameter.
- Click [OK] to finish creation and you can check it in work menu.

◆ Delete RAID

Select object to delete and click [Delete RAID] to pop up the following dialog box:

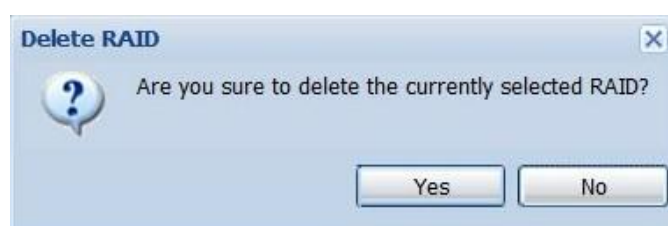


Figure 225 Delete RAID

- Click [Yes] to delete selected RAID.
- Click [No] to cancel and return.

Note: Please make sure there is no volume on RAID before deletion.

◆ Configure RAID

RAID configuration refers to parameter modification, which is similar to creation of RAID but script size in gray cannot be modified.

◆ Rebuild RAID

- If RAID status is “degrade” , select this RAID and click [Rebuild RAID].
- If no available disk exists, the dialog box will pop up “There is no available disk and RAID cannot be created” . Click [OK] to return to main interface.
- Select available disk in the list to rebuild RAID and click [OK] to finish RAID rebuilding or [Cancel] to return to main interface.

◆ **Expand RAID**

- Click [Expand RAID]. If there is no available disk, the dialog box “There is no available disk to expand RAID.” will pop up. Click [OK] to return to main interface or [No] to pop up Expand RAID dialog box.
- Select available disk to expand RAID. Click [OK] to finish expansion or [Cancel] to return.

8.1.2 Volume

Volume is created on logical partition of physical disk, that is, logical volume for data storage.

◆ **Create New Volume**

Step One: Click [New Volume] to pop up the following dialog box:

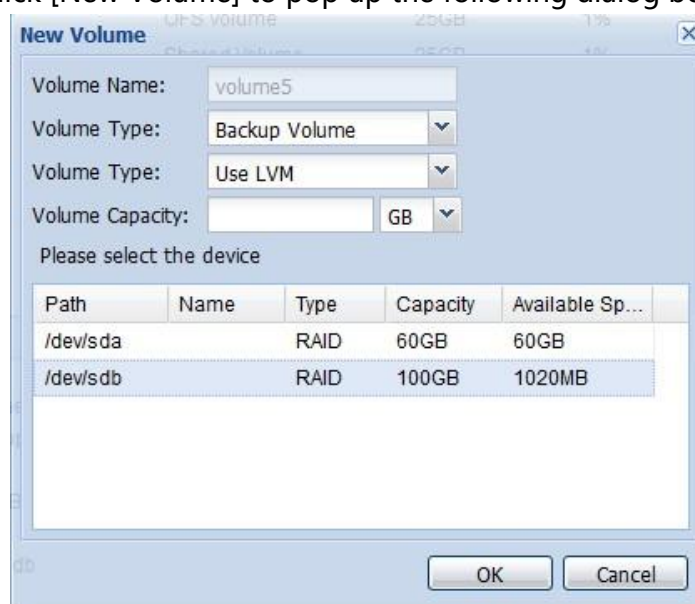


Figure 18 New Volume

- Volume Name: It is automatically generated by system and cannot be modified.
- Volume Type: Backup volume, OFS volume, Shared volume, iSCSI volume and FC volume are included and backup volume is default.
 - Backup Volume: It is for data backup.
 - OFS Volume: It is for storage of disaster recovery data.
 - Shared Volume: It is for data sharing.
 - iSCSI Volume: It is used to package SCSI protocol via TCP/IP and user can use iSCSI volume as local disk.

- FC Volume: Transmission via FC protocol and user can use FC volume as local disk.
- Volume Type: Use LVM.
- Volume Capacity: Input volume size to create and there are three units exist in the drop-down list: MB, GB and TB, of which GB is default. Input value should be numerals between 1 and 10000.

Step Two: Select device to create volume and click [OK] to finish or [Cancel] to return.

◆ **Delete Volume**

Select volume to delete and a dialog box will pop up. Click [Yes] to delete volume or [No] to cancel.

Note: After deletion of volume, all the data on volume will be lost. It is recommended to execute carefully.

8.1.3 Disk List

In "Disk List" page, you can view disk information and usage, including detected disk name, status, physical size, usage and type.

- Slot displays disk slot in device.
 - Status: Current disk status.
 - Normal: Disk works normally.
 - Failure: Disk failure occurs.
 - Initialization: Disk is initializing.
 - No Disk: No disk has been detected in slot.
 - Name: It is named by slot that disk locates from Disk1 to DiskN.
 - Volume: Actual volume of disk.
 - Type: Disk Type.
 - Usage: Current usage of disk, including initialization progress of disk.
- ◆ **Refresh**
- Click [Refresh] to display the latest disk status.
- ◆ **Initialization**
- Select disk to initialize and click [Initialization] to initialize disk.
- ◆ **Create Hot Spare Disk**

Select an available disk and click [New Hot Spare Disk] to pop up the following dialog box:



Figure 227 New Hot Spare Disk

Select RAID: Global and all created RAID of level 0, 1, 2. Click [OK] to finish or [Cancel] to return.

◆ Delete Hot Spare Disk

Select hot spare disk to delete and click [Delete Hot Spare Disk] to pop up corresponding dialog box. Click [OK] to finish deletion.

- Only created hot spare disks will be displayed.
- If hot spare disk exists in AnyBackup Appliance, [Delete Hot Spare Disk] can be used. After deletion of hot spare disk, the deleted disk will be free and can be used to create RAID or Hot Spare Disk.

8.2 Share

Share management refers to manage sharing and right of directory for directory, sharing it with some users, which does not only enable user easy accessibility, also guarantees security of directory. This chapter will introduce details operation about directory, right, quota and sharing. Click

“Storage/Share” to enter the following interface:

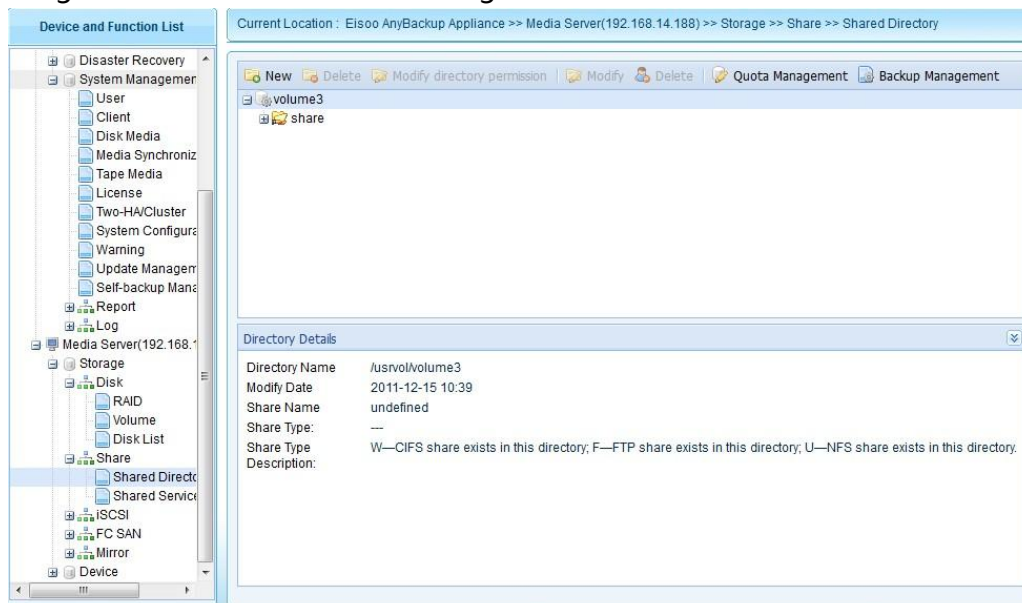


Figure 228 Share

8.2.1 Shared Directory

Shared directory management refers to management of directory sharing and rights. Admin can set directory sharing right according to user requirements. Direcoty files are or not allowed to share simultaneously and files are not allowed to read or write at the same time.

◆ Create Directory

Step One: Enter " Shared Direcoty" page and select location to create direcoty. Click [New] and select position to create directory as shown in the following dialog box:



Figure 229 New Directory

Step Two: Input directory name, click [OK] to finish or [Cancel] to return.

- Directory can be creaed only in volume X and subdirectory. Please make sure volume has been created in storage.
- Directory name can only be composed by: case letters, Arabic numerals, Chinese characters, underline "_" and horizontal line "-" .

◆ Delete Directory

Step One: Select directory to delete and click [Delete Directory] to pop up "Are you sure to delete this share?"

Step Two: Click [Yes] to delete directory or [No] to cancel.

Note: Only directory and subdirectory in shared volume will be deleted.

◆ Modify Directory

Step One: Enter "Shared Directory" page and select directory to modify. Click [Modify] to pop up the following dialog box and mark "Modify directory permission" check box.

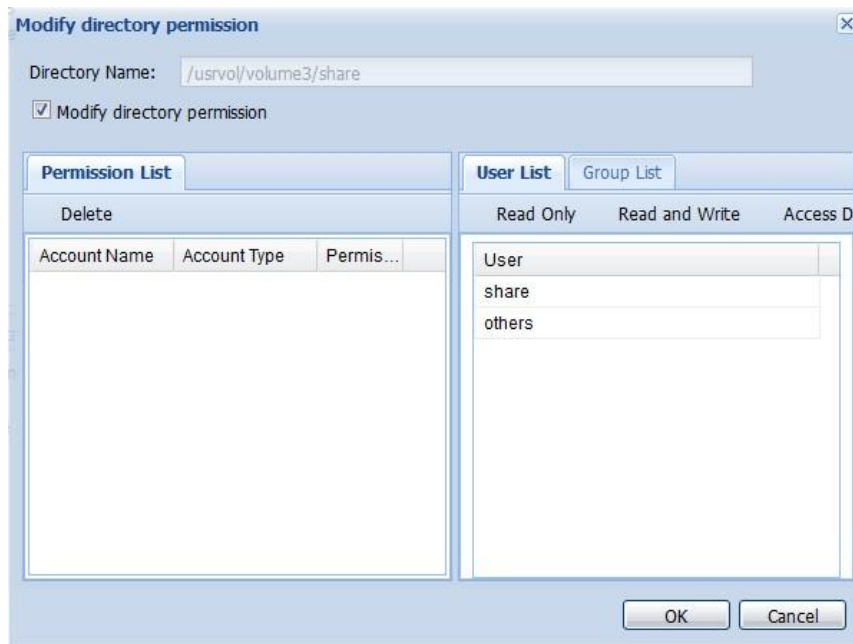


Figure 230 Modify Directory Permission

Step Two: Configure user permission: select user to configure and click [Read Only], [Read & Write] and [Access Denied] to set permission.

- Special Account others :others is in user list by default. If others is added to permission list, it means all users and group not in permission list will execute this operation to change read and write permission. Others can not be deleted.
- If directory is shared, after modification, permission will be executed according to permission priority. For example, if one user group is set "Read Only" in share modification and "Read & Write" in directory modification, thus this file will be "Read Only" at last.
- Once there are several directories in one volume, subdirectory without permission will inherit permission of parent directory.

Step Three: Click [OK] to finish configuration or [Cancel] to return.

◆ **Modify Share**

After creation of one directory, modify its share, thus multiple users can access to this directory. One directory can support multiple shares without influence on others, as they can be set separately.

Step One: Select directory to share and click [Modify] to pop up the following dialog box:



Figure 231 Sharing Configuration

Step Two: Select share type and input share name and permission.

- Share Name: It should be unique and customized by user, that is, share name should be unique for both new share or existed system share. Share name can only be composed by: case letter, Arabic numerals, Chinese characters, excluding other characters and space. Besides, global and host cannot be used for share name.
- Share Type: Select share type in the dialog box:
 - CIFS (Windows): Access to data via CIFS protocol. System will share storage space to Windows client via CIFS protocol. Users can search storage device via my internet or client to access to data.
 - FTP (Web): Access to data via FTP protocol. Shared data can be accessed via LAN or WAN directly.
 - NFS (Unix/Linux): If client has Linux or Unix system environment, EISOO AnyBackup Appliance can set NFS share and data can be accessed by mount command of NFS protocol.
- Set Access Permission: Click [Add] to pop up "Add user/user group permission" dialog box.
 - If CIFS or FTP share is selected, select user/user group to set in dialog box and click [OK].
 - If NFS share is selected, set host type, allow ROOT in dialog box. If single host is selected, host IP should be input. Click [OK].

- User/User group permission is read only by default. Click Operation Permission to select the following permission: Read only, Read & Write, Ownship as shown in the following picture:



Figure 232 Modify Sharing

Step Three: Click [OK] to finish sharing configuration or [Cancel] to return.

◆ Delete Sharing

Step One: Select share to delete in share list and click [Delete] to pop up "Are you sure to delete this share?" dialog box.

Step Two: Click [Yes] to delete share or [No] to cancel.

◆ Quota Management

Admin can track and control used space on volume via quota management. Admin can set disk quota for user space on volume and warning when user space exceeds quota space.

After quota management enabled, admin can set max user space and warning space. Quota management can effectively control user max space and warning space on volume. Default quota refers to the max space for user, while warning space is that when user space exceeds the default space, it will notify user and default space should be set as maximum for users. For example, if one user is set 500M space, he will be notified when 450M has been used. The left 50M can still be used and the max space for this user is 500M.

Quota configuration is for single user. Default quota is for new user, by which each user will be set one quota. If default is unlimited, disk space for this user is unlimited.

Step One: Select volume to set and click [Quota Management] to pop up the following dialog box as shown in the following dialog box:

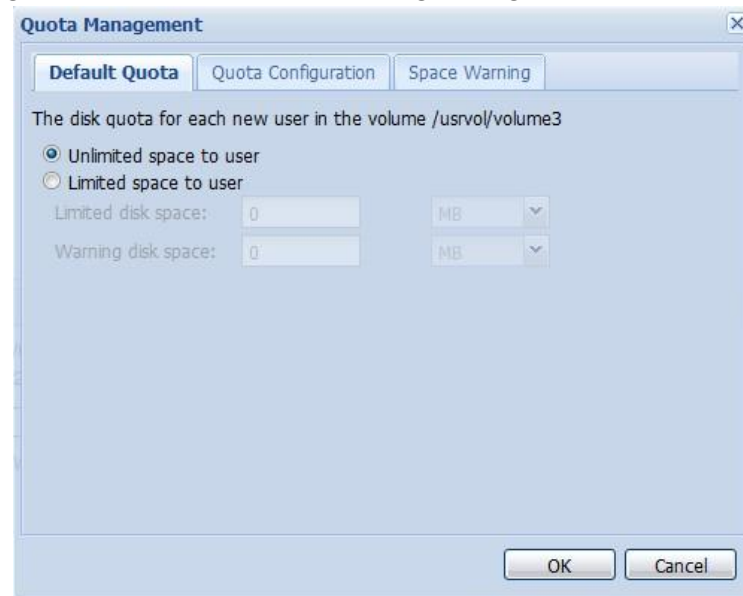


Figure 19 Quota Management

During modification of quota management, make sure whether set default limit for this volume. If so, limit and warning space should be set and figures and unit should be selected. Disk space is calculated by KB, MB and GB. Input correct figures as decimal numbers, which can interger and floating point less than 8 (decimal point included). Unit is important. Two significant digits will be reserved.

- Mark "Unlimit space to user" and user will have unlimited space.
- Mark "Limited space to user" and select KB, MB and GB in the drop-down list.
- Click [OK] to finish or [Cancel] to return.

Step Two: Set selected volume and click [Quota Management] to pop up the following dialog box and all users will be listed as shown in the following picture:

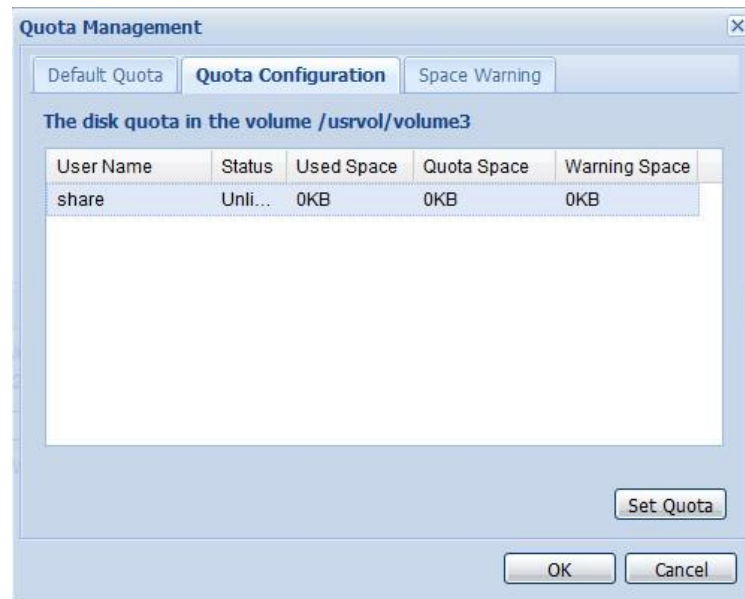


Figure 234 Quota Management

When admin modify user quota, space for user should not be limited. During creation, it is set as unlimited by default. Input figures and unit in warning and limit to limit user space. Disk space unit is KB, MB and GB. Input correct figures in decimal scale and figures can be integer and floating point, which should be less than 1000GB, thus unit is very important.

- Select one user and click [Quota Management] to set limit for user space.
- Click [OK] to finish or [Cancel] to return.

Step Three: Switch to "Space Warning" page and mark "Enable space warning" . When a user's available space of share directories is less than the setting warning space size, an email will be sent to administrator to remind that user space is not enough and need for timely processing.

◆ Backup

Backup should be created for each created volume thus detailed backup data can be managed.

Step One: Enter "Shared Directory" page and select shared volume to back up. Enter [Shared Directory] page and select shared volume for backup. Click [Backup Management] to enter the following dialog box:

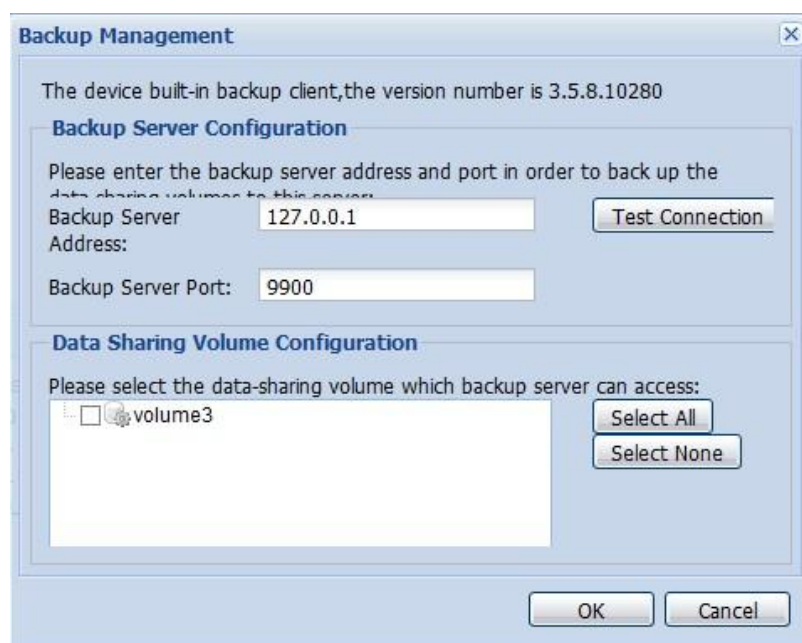


Figure 235 Backup Management

Step Two: Input information in "Backup Server IP" and "Backup Server Port" and test connection.

Step Three: Select data sharing volume for backup and click [OK] to finish configuration.

8.2.2 Shared Service

Service can be started, stopped or configured in shared service management page. Click "Storage/Share/Shared Service" to pop up the following dialog box:

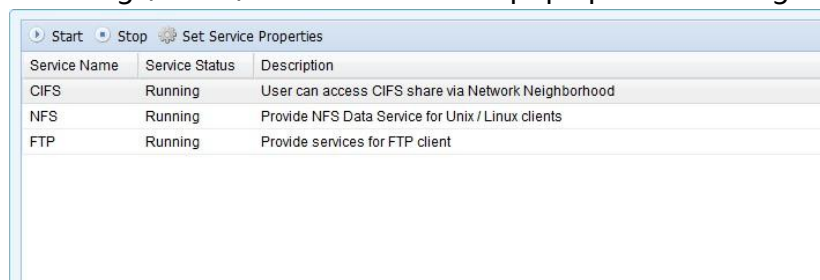


Figure 236 Shared Service

◆ Start Service

Select service and click [Start] to start corresponding service.

◆ Stop Service

Select service and click [Stop] to stop corresponding service.

◆ Set Service Property

Select service and click [Set Service Property] to set corresponding configuration:

- Set CIFS Property: Server description can be any character and can also be empty. Server and host name is default such as Nas(S116209001); default work group is: workgroup, which can be modified by user.

- Set NFS Property: Set and Modify NFS service progress and the following value can be selected: 8, 16, 32, 64, 128 (Default is 8).
- Set FTP Property: FTP property configuration includes the following five items:
 - Port: FTP default port is 21 and port should be interger larger than 0 and cannot conflict with other service port. Once input port conflicts with other ports, FTP service cannot be started.
 - Max Clients: The max clients server allowed is 50 by default (0 means unlimited clients). User can set it according to requirements and it must be interger larger than 0.
 - Max Client Connections: It refers to connections for one IP and default is 0 (0 means unlimited). User can set according to requirements and it must be integer larger than 0.
 - Unmark "Allow Anonymous User" and default login directory is gray and cannot be used.
 - Mark "Allow Anonymous User" and default login directory can be used. You can select default shared directory name or select in drop-down list (Directory of all shares are included.). Selected directory name will be the default login directory and if there is no shared direcoty name in drop-down list, no directory can be used for anonymous user login.
 - Click [OK] to finish service configuration.

8.2.3 Share Data

EISOO AnyBackup Appliance newly adds shared data management for common user. If admin has allocated right to this user, user can create, delete and modify shared directory. Login to management console as admin and select "Storage/Share/Shared Data" to pop up corresponding page.

◆ Create Directory

Select shared directory in list and click [New] to pop up "New Directory" dialog box. Default path for shared directory is gray and cannot be modified. Input shared directory name and click [OK] to finish creation.

◆ Delete Directory

Select shared directory to delete and click [Delete Directory].

◆ Modify Directory

- Select shared directory and click [Modify] to pop up a dialog box as shown in the following picture:

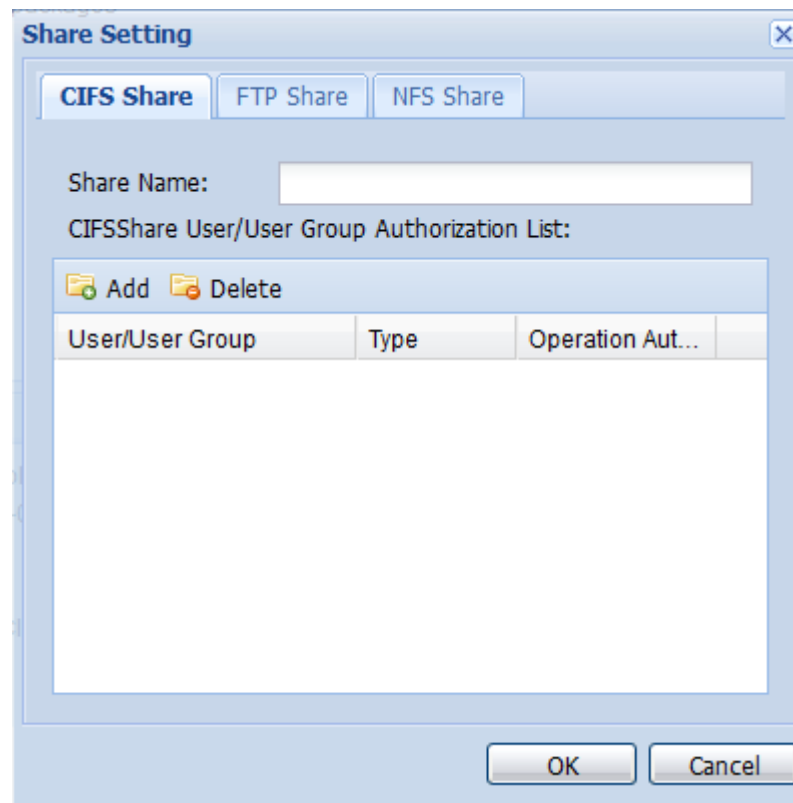


Figure 237 Shared Directory Configuration

- Input share name and click [Add] to pop up “Add User/User Group Permission” dialog box. Select user to share and click [OK] to finish.
- Double click added user and user permission can be modified: Read Only, Read & Write and Ownership.
- Click [OK] to finish configuration.

8.3 iSCSI

Set one logical volume as iSCSI volume and admin can start iSCSI service in Iscsi service management page. Once client is authorized, it can access to iSCSI partition by iSCSI manager to realize storage. (Please refer to chapter 4 for detailed iSCSI client operation.). This chapter is divided as target and service management and followed are the detailed introduction.

8.3.1 iSCSI Target

If Iscsi volume is created on RAID, click “Storage/Iscsi target” to pop up corresponding page, in which detailed information and running status of iSCSI volume can be viewed.

◆ Modify Connection User

Select target and click [Modify Connection User] to pop up the following dialog box:



Figure 238 Modify Connection User

- Target name cannot be modified. Input user name and password.
- Click [OK] to save modification or [Cancel] to return.
- Click [Clear User] to clear selected user.

◆ **Delete Target**

Select target and click [Delete Target] to pop up corresponding dialog box.

- Click [Yes] to delete or [No] to cancel.

8.3.2 iSCSI Service

Click "Storage/iSCSI/iSCSI Service" to pop up corresponding page, in which 服务 all running service can be viewed.

◆ **Start Service**

Select service and click [Start Service] to start corresponding service.

◆ **Stop Service**

Select service and click [Stop Service].

Note: If service is running, [Start Service] button is gray and cannot be used while [Stop Service] can be used, vice versa.

8.4 FC SAN

FC SAN realizes communication via FC protocol. EISOO AnyBackup 3.5 Appliance support FC protocol and user just add HBA card in backup device and client to create logical volume. Then logical volume will be mapped to client via software (WWN of HBA should be learnt in configuration) and client also needs a FC HBA card to connect to AnyBackup Appliance. A local disk will be generated client after successful mapping, which means a disk added in local and it can be partitioned and formatted.

8.4.1 FC SAN Target

◆ **Create FC Target**

Step One: Click [New] to pop up a dialog box and select existed FC volume in "FC Target Device" drop-down list and select FC target size, including 712, 1024, 2048, 4096 (Default is 4096.). User can set it according to requirements.

Step Two: Select a client in WWN list and click [OK] to finish creation of FC

target.

Step Three: Click [Add] to pop up a dialog box. Input client WWN and click [OK] to add client.

◆ **Configure FC Target**

Step One: Select a FC target and click [Configure FC Target] to pop up a dialog box. Select FC target size in drop-down list.

Step Two: Click [Add] to pop up a dialog box. Input client WWN and click [OK] to add client.

◆ **Delete FC Target**

Select target and click [Delete FC Target] to pop up a dialog box. Click [Yes] to delete or [No] to return.

8.4.2 FC SAN Service

◆ **Start Service**

Select service and click [Start Service] to start corresponding service.

◆ **Stop Service**

Select service and click [Stop Service] to stop corresponding service.

Note: If service is running, [Start Service] button is in gray cannot be used while [Stop Service] can be used, vice versa.

Chapter 9 Device Management

You can learn device current status and configuration of each device, such as virtual machine, energy consumption, network, etc.

9.1 Virtual Machine

EISOO AnyBackup Appliance 3.5 VX and GX integrate with VMware Server to support creation, management, control, storage, remote VM, etc, together with all management that VMware server supports. In virtual machine management page, virtual machine can be added, created, started, stopped, etc and storage can be added to VM platform.

9.1.1 Storage

Storage refers to storage management of VM platform, including adding, renaming and deleting storage. Click “Device/Virtual Machine” to enter corresponding page.

◆ Add Storage

Add storage path for VM platform.

Step One: In “Storage” drop-down list, click [Add Storage] to pop up the following dialog box:



Figure 241 Add Storage

Step Two: Input valid storage name in dialog box and you can manually input valid path in mapping path or click [Browse] to select storage path.

Step Three: Click [OK] to add storage.

Note: Select added storage and its property will be displayed in property bar.

◆ Rename

Select storage and click [Rename] to pop up corresponding dialog box. Input new storage name and click [OK] to finish.

◆ Delete

Select storage and click [Delete] to pop up a dialog box. Click [OK] to delete selected storage from list.

9.1.2 Virtual Machine

◆ Create Virtual Machine

Step One: Select a storage path from storage list and click [VM] to pop up the following dialog box:

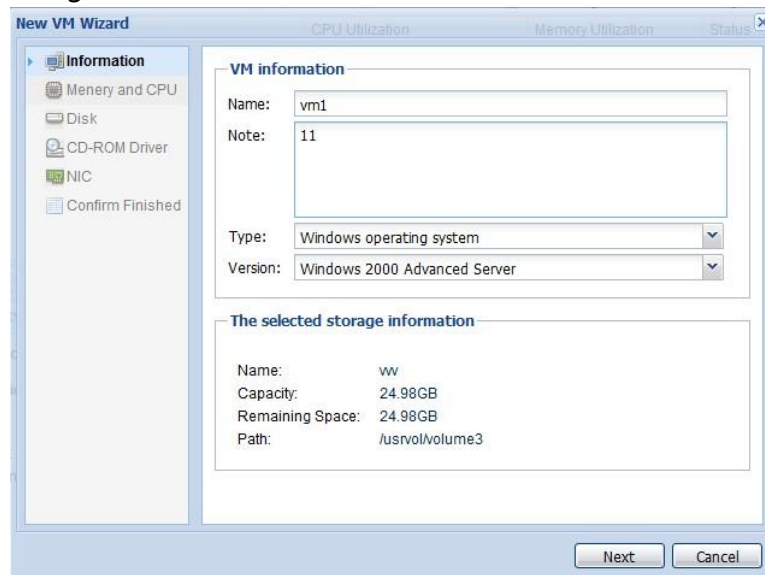


Figure 242 New Virtual Machine

Step Two: Input name, note and select operation system and type in Information dialog box. Click [Next] to continue.

Step Two: Select memory size (integer) in “Memory and CPU” dialog box and select CPU count (Default is 1). Click [Next].

Step Three: In “Disk” dialog box, there are two options:

- Create A New Virtual Disk: Disk size, file, disk mode and optimized Policy are included.
- Add no disk.

Click [Next].

Step Four: In “Driver” dialog box, there are two options:

- Use one ISO Image: set ISO image file path and reconnection when power on.
- Add no driver.

After configuration, click [Next] to verify hardware information of virtual machine. Click [Done] to finish creation of virtual machine. Select added virtual machine and basic information of virtual machine can be viewed in “Property” .

◆ Modify Parameter

In “Virtual Machine” page, select a virtual machine and switch to hardware page to display detailed hardware information of virtual machine and hardware parameter can be modified.

- **Add**

Click [Add] to pop up “Add Hardware” dialog box, including harddisk, driver and finish. Please refer to “New Virtual Machine” for details.

➤ **Modify Memory**

Click [Modify] to pop up a dialog box, in which default memory of this virtual machine can be allocated.

➤ **Modify Hardware**

Click [Modify] on the right of hardware to pop up a dialog box. Select disk mode and optimized Policy.

➤ **Modify NIC**

Click [Modify] on the right side of hard disk to pop up a dialog box.

➤ **Modify Driver**

Click [Modify] on the right of driver to pop up a dialog box, in which two options are provided:

- Host: Set file path of ISO image and auto connection when power on.
- Client: User driver or ISO image file.

◆ **Add Existed VM**

Click “Virtual Machine/Add Existed VM” to pop up a dialog box. Click [Browse] to select .vmx file and click [OK] to add this virtual machine to virtual machine list.

◆ **Clone VM**

Click “Virtual Machine/Clone VM” to pop up a dialog box. Input name for new virtual machine and click [Browse] to select storage path. Click [OK] to display cloning process and it will auto close after clone.

◆ **Configure VM**

Select one virtual machine and click “Virtual Machine/Configure VM” to pop up a dialog box, in which virtual machine name, note and auto start up when system powers on can be set.

◆ **Delete Virtual Machine**

Select a virtual machine and click “Virtual Machine/Delete VM” to pop up a dialog box. Click [Yes] to delete selected virtual machine from virtualization platform.

◆ **Make Snapshot to Virtual Machine**

Only one snapshot can be made for one virtual machine. Click [Make a snapshot to virtual machine] to execute directly for vm without snapshot; for virtual machine with snapshot, the following dialog box will pop up:

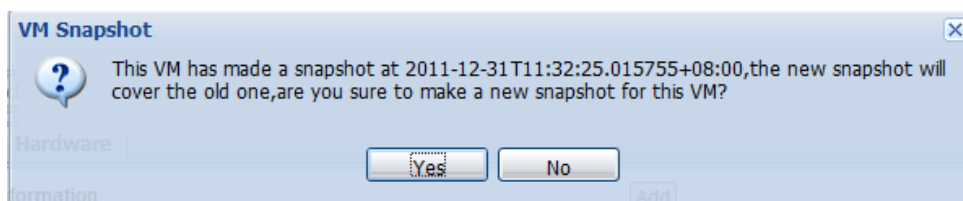


Figure 243 Make a snapshot to virtual machine

Click [Yes] to make new snapshot for virtual machine.

◆ **Restore Virtual Machine to Snapshot**

Select virtual machine to delete in virtual machine list and click "Virtual Machine/Restore VM to snapshot". Click [Yes] in prompt dialog box and restore virtual machine to snapshot.

◆ **Delete VM Snapshot**

Select virtual machine to delete and click "VM/Delete VM Snapshot" to pop up a dialog box. Click [Yes] to delete latest snapshot.

◆ **Install VMware Tools**

Select a running virtual machine without VMware Tools and click "VM/VMware Tools" to pop up "System will mount a VMware Tools in installation ISO disk and please click remote control to enter installation after mounting."

◆ **Uninstall VMware Tools**

Select a running virtual machine without VMware Tools and click "VM/VMware Tools" to pop up "System will mount a VMware Tools in installation ISO disk and please click remote control to uninstall."

◆ **Remote Control**

Remote control is used for control of remote running virtual machine. Ensure browser plug-ins have been added before remote control.

◆ **Refresh**

Click [Refresh] to refresh virtual machine list automatically.

◆ **Start**

Select a "Suspended" or "Stopped" virtual machine and click [Start].

◆ **Suspend**

Select a "Running" virtual machine and click "Suspend".

◆ **Stop**

Select a running virtual machine and click [Stop].

◆ **Restart**

Select a "running" virtual machine and click [Restart].

9.2 Network

There are many network ports in EISOO AnyBackup Appliance such as NIC (100M, 1000M). Admin can configure IP of network port via web page. Admin can

get IP of network port via DHCP or BOOTP and configure static IP. This chapter will introduce in details. Click “Media Server/Device/Network” as shown in the following picture:

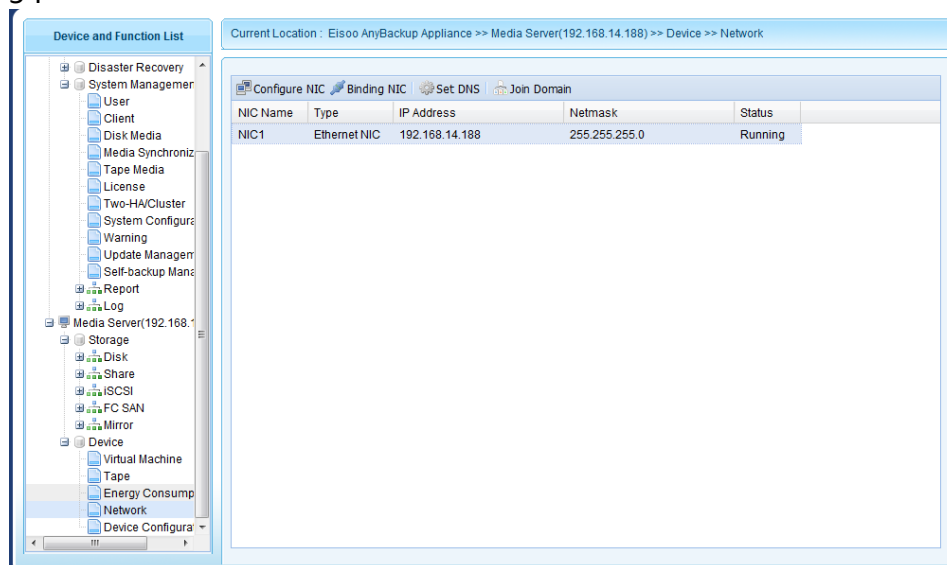


Figure 254 Network Management

◆ NIC Configuration

Each computer has its own IP in network. Admin can set IP of network port via “NIC Configuration” .

Select NIC and click [Configure NIC] to pop up the following dialog box:

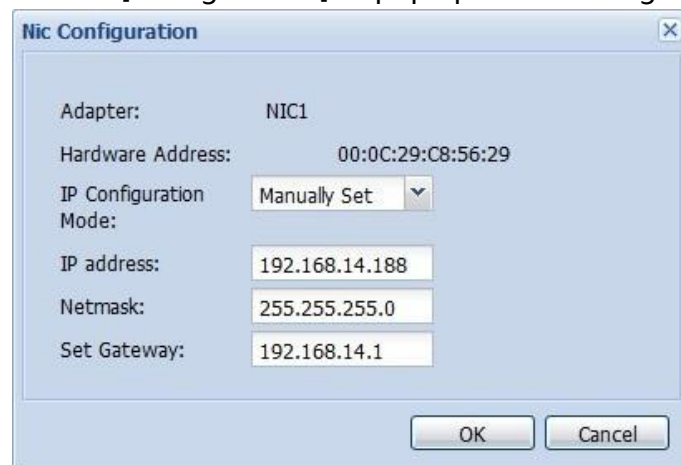


Figure 255 NIC Configuration

- Please select IP mode (DHCP, BOOTP, Manual Configuration).
 - DHCP: Auto IP via DHCP protocol.
 - Manual Configuration: Input IP of network port and input IP, subnet mask and gateway.

Click [OK] to finish NIC configuration or [Cancel] to return.

Note: After modification of IP of network port, client browser may cannot access to Web and user must change a new IP to access.

◆ NIC Binding

If there are two or more NIC existed, admin can bind NIC to get larger bandwidth and high stability.

Click [NIC Binding] to pop up the following dialog box:

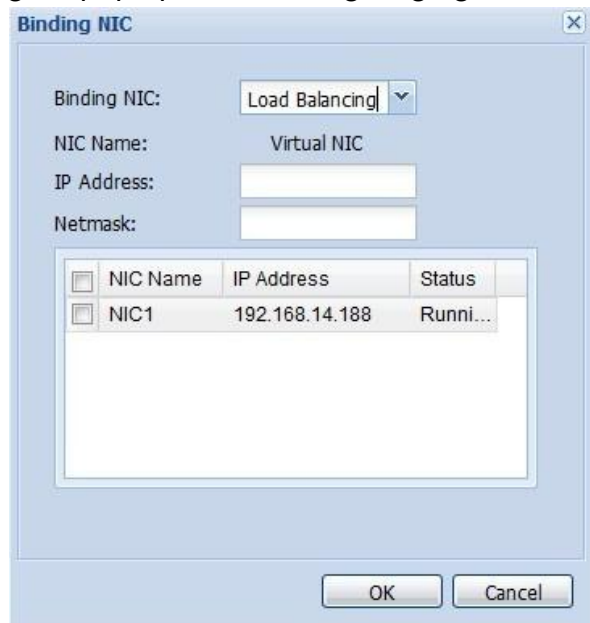


Figure 256 NIC Binding

- If "NIC Binding" type is multi access, user can access to appliance via any NIC IP. Click [OK] to finish configuration or [Cancel] to return.
- If "NIC Binding" is load balancing or fault redundancy, user must input valid IP and Network mask. Mark NIC to bind and click [OK] to finish configuration or [Cancel] to return.
 - Load Balancing: Binding NIC will allocate transmission flow and if one of it fails, the others will take the burden.
 - Fault Redundancy: One work NIC is used, once it fails, other NIC will auto take over and take thte network flow.
 - Multi Access: Each NIC works independently and locates in different network segment.
- ◆ **Set DNS**
 - Click [Set DNS] to pop up a dialog box.
 - Input preferred DNS and spare DNS. If preferred DNS fails to work, spare DNS will auto take over job of preferred DNS.
 - Click [OK] to finish configuration of DNS or [Cancel] to return.

◆ **Join Domain**

Click [Join Domain] to pop up the following dialog box:



Figure 257 Join Domain

- Host name can be modified (Host name will be displayed in windows networks as marker). Host name should start with letter and can be composed by 26 letters, 0-9 numerals and underline. After modification of host name, Windows (CIFS) service can restart.
- Mark "Work Group" and click [OK] to finish configuration or [Cancel] to return.
- Mark "Domain" to input domain, domain name, master AD, domain admin and password. Click [OK] to finish configuration or [Cancel] to return.

Note: Domain and domain name should be capitalized, while host name of AD should be small letters.

9.3 Device

Host name and modification of EISOO Anybackup appliance can be viewed in device page. Click "Media Server/Device/Device Configuration" to pop up the following dialog box:

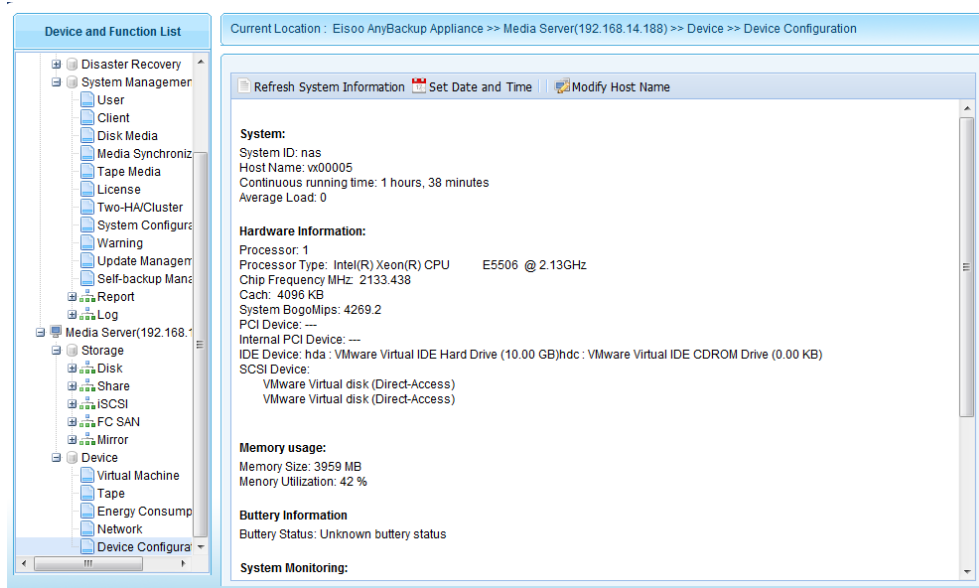


Figure 258 Device Configuration

◆ Refresh System Information

Click [Refresh System Information] to view detailed system information in details:

- **System:** System ID, host name, continuous running time, average load will be displayed.
- **Hardware Information:** Processor, type, chip frequency, cache can be viewed.
- **Memory Usage:** Memory size and utilization will be displayed.
- **Battery Info:** Battery protection with temperature, left power, etc can be viewed.
- **System Monitor:** CPU voltage, temperature, fan speed, etc can be viewed.
- **Date and Time:** Current system date and time will be displayed.

◆ Set Time and Date

Click [Set Date and Time] to pop up the following dialog box:

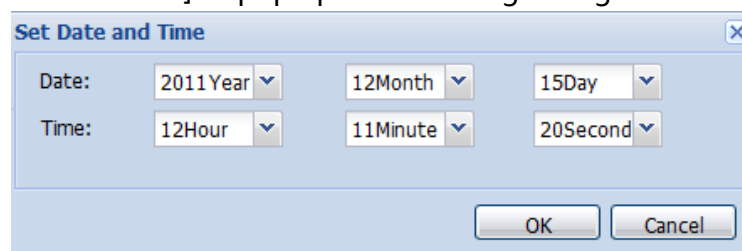


Figure 259 Set Date and Time

- Select month, year and day in date.
- Select hour, minute, second in time.
- Click [OK] to set time and date or [Cancel] to return.

◆ Modify Host Name

Click [Modify Host Name] to pop up the following dialog box:

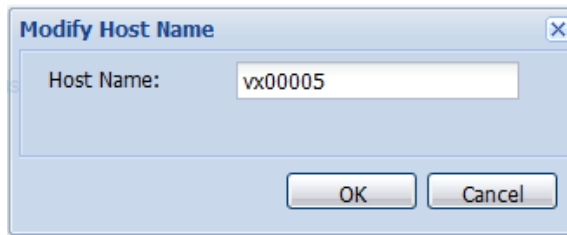


Figure 260 Modify Host Name

- Input host name and it should start with letter and composed by letter and numerals.
- Click [OK] to modify or [Cancel] to return.

Note: Host name should be composed by letter and numerals and start with letter.

Chapter 10 AnySupport

AnySupport is a new type of service product to meet users' requirement on data backup and restore management. Based on enterprises' data, EISOO AnySupport not only responds to customers' problem in 24 hours, but also plays the role of **[Data Health Management Consultant]** and **[Exclusive Technical Expert]**.

The service tenet of AnySupport is professional, excellent and active. In other words, we plan data management program for customers actively, examine customers' data periodically, and help customers to build an effective backup system with professional and excellent service. AnySupport contains technical support service, professional service and training certification service.

EISOO provides complimentary phone support for our customers and partners. If you have any technical problem or doubts about our product, please feel free to contact us:

- ◆ National Free Technical Hotline : [400-880-1569](tel:400-880-1569)
- ◆ Global Hotline: [086-21-54222601](tel:086-21-54222601)
- ◆ Quality Supervision Hotline: [021-54326440-8201](tel:021-54326440-8201)
- ◆ Technical Support Email : support@eisoo.com

Chapter 11 FAQ

- ◆ For FAQ of EISOO AnyBackup Appliance, please click the following URL to

access our knowledge base:

http://www.eisoo.com/support/index.php?_m=knowledgebase&_a=view

- ◆ For more information about product, please refer to <http://www.eisoo.com>



EISOO Software Co.,Ltd.

Add: 2nd Floor, NO.8 Building, Pujiang Intelligence Valley

NO. 1188 Lianhang Rd, Minhang District, Shanghai, China

Tel: 86-21-54222601;400-800-01569

Fax: 86-21-54326440-8118

www.eisoo.com

©2003-2012 EISOO Software Co.,Ltd.