Agent 6.0 for Novell NetWare

User's Guide

April 2009

This document describes how to install and use the version 6.0 Agent for NetWare, for Windows and Web Agent Console Backups and Restores.

Contents

Table of Figures

Revision: This manual is updated for Version 6.0
Software Version: 6.00 (April, 2009)

Acknowledgements: Two encryption methods, DES and TripleDES, include cryptographic software written by Eric Young. The Windows versions of these algorithms also include software written by Tim Hudson. Bruce Schneier designed Blowfish encryption.

The Agent, Agent Console, Vault and Vault Console applications (version 4 and above) now have the added encryption option of 128bit AES (Advanced Encryption Standard). Advanced Encryption Standard algorithm (named Rijndael, pronounced "Rain Doll") was developed by cryptographers Dr. Joan Daemen and Dr. Vincent Rijmen. This algorithm was chosen by the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce to be the new Federal Information Processing Standard (FIPS). AES is not available when connecting to a Vault lower than version 4.1.
See:**http://csrc.nist.gov/encryption/aes/round2/r2report.pdf** for details.

Over the wire encryption is not available when connecting to a Vault lower than version 4.1

1 Introduction and Installation

This User's Guide is intended for the System Administrator responsible for ensuring that their Users' computers are properly configured to be backed up, and that Backups and Restores can be run successfully. The computer Users who use the Servers are not usually aware that their Systems are being backed up.

Different Servers may require different files and directories backed up, on different schedules, depending on what data needs to be secured. Some may require backing up more frequently, depending on how the data changes (its volatility).

This Guide will show the Administrator how to select data to be backed up, how to configure the Agents to do that, and how to schedule the backup times. Restores are also covered in detail.

The "Windows and Web Agent Console Operations Guide" manual cover all the details about Windows Agent Console and Agents, from the point of view of "how to operate" the program.

This Guide covers the functionality required to perform a Backup (and Restore) using those tools.

Note that BUAgents running under Web Agent Console are also described in the Web Agent Console documentation. The Agent installation uses the same program for installation for Windows Agent Console or Web Agent Console.

1.1 What's New

New features in this release:

This version only supports backup and restore with versions 5.53 and 6.0x of the Vault. It supports version 6.12+ of Windows Agent Console (32-bit) and version 6.21+ of Web Agent Console.

- Unicode support (UTF-8): Unicode is the international standard whose goal is to provide the means to encode the text of every document people want to store in computers. Unicode is considered the most complete character set and one of the largest, and has become the dominant encoding scheme in internationalization of software and multilingual environments. ANSI is the default (normal) representation of most "single" languages. Users using NSS volumes are able to display, search, and select files through Agent Console.
- Authenticated SMTP: this support is added for enhanced SMTP Notification settings. Additional settings are: Port number, Username, Password, and Domain.
- Improved bandwidth throttling. Each Job can now share (equally) the Agent's bandwidth throttling. If multiple Job instances run concurrently, they will not exceed the Agent-wide bandwidth throttling limit. The user can optionally turn off throttling for restores, if extra speed is needed.
- Logical Vault Recovery (LVR) Support. The Agent supports vaults configured for LVR. The Agent can automatically determine the correct vault and backup, if the logical vault has changed. For example, if the active vault has failed, and the passive one is now the active one, the Agent will synchronize and switch over to the new one. The log file will show this activity.
- The Agent can re-create a missing delta file. The Agent includes additional information with the backup that allows it to re-build the file, partially or wholly. This delta recovery only occurs with Vault 6.0+.
- Advanced Filtering, with Directory wildcards, to improve backup performance and usability.
- You can Restore from a range of safesets in a single run. You may chose a "from" and "to" in the two dropdown lists, to show multiple catalog entries.
- On a Restore, under "File Overwrite and Renaming options", you may additionally choose to rename existing files, or rename the incoming ones with a new extension (.0001, .0002, etc.).
- Long path name support. The Agent supports very long path names for both file system and plug-in data sources, when connected to a version 6 Vault. The maximum length is 31,999 characters. Older Agents only supported 511 characters. The supported length will show in the log files. The Agent is backward compatible with older Agents, but older Agents will not be able to restore from long path names. Note that this long path is only for Web Agent Console. Windows Agent Console only supports browsing of path lengths up to the buffer size of approximately 8,000 characters.
- Cross catalog searching. Users can search through all available catalogs when restoring files, without switching Restore Wizard screens.

- Restore from another computer. The User can restore from another computer when the Job name is identical on both computers.
- Safeset encryption now includes a stronger encryption algorithm, AES 256-bit.
- Job names can now be up to 30 characters long, and must consist of letters (A-Z and a z), numbers (0-9) and/or _, -, $ (underscore, dash, dollar sign).
- "Forcereseed" option in CLI. Delta recreation allows the user to rebuild a DTA (delta) file by using Job synchronization. This command line only option will force a re-seed, in case of a failure with delta recreation in rebuilding delta files.

  If the Vault supports delta recreation, and the recreated file is unusable, then the backup will be forced to reseed.

  The Syntax of this parameter is:

  ```
  VV backup Job_mame /param=Job_name.vpb /forcereseed
  ```

See the "Windows Agent Console Operations Guide", the "Web Agent Console User Guide", or the "Web Agent Console Administrator Guide" (or their Helps) for more details on these features.

1.2 Agent for NetWare Installation

1.2.1 System Requirements

Hardware

☑ CPU – a 32 bit x86 or compatible processor

Note: If your operating system suggests different minimum hardware requirements, employ whichever is greater.

☑ RAM

- 256MB for NetWare 6.0
- 512 MB for NetWare 6.5

☑ HDD - 100MB of available disk space.

Software

☑ An MS Windows workstation that has the latest version of the Novell Client for Windows, or Microsoft Client Service for NetWare installed.

☑ NetWare 6.0 or 6.5

- Support Pack 5 for NetWare 6.0
- Support Pack 7 for NetWare 6.5

☑ Vault version 5.53 and up.

☑ Windows Agent Console version 6.12 and up

☑ Web Agent Console version 6.21 and up

☑ NetWare Agent version 6.00

☑ Network:

- A Novell TCP/IP stack
- NETDB.NLM (for Network Database Access for NDS and NIS queries. Note that this NLM should be started before the Agent.)

☑ Optional software: Open File Manager * - OFM 9.601 or above.

Note: Using OFM on NetWare 6.5 NSS volume requires the following patch that can be obtained at:

http://download.novell.com/Download?buildid=vgIJ013SZ8c~

In addition, the Agent installation directories and any anti-virus directories must be excluded from open file protection. Do not back these up using any file-lock management utilities.

In the client's properties dialog, under OFM GUI, select the "Files" tab then add the Agent's directories and subdirectories to the "Files to be ignored by OFM". Make sure to check "Include subdirectories" check box.

*See the related OFM documentation for configuration.

1.2.2 Privilege Requirements

1.2.2.1 Installation

To install the Agent under NetWare, you need an ADMIN account or an account with security equal to ADMIN.

Note: Because TFS may not have the long path name support installed (the LONG namespace loaded or not), it is recommended to install the Agent on an NSS volume for long path names support.

1.2.2.2 Functional

To communicate with the Agent for NetWare from the Agent Console application, you need an ADMIN account, an account with security equal to ADMIN or an account with Supervisor rights to the [root] object of the NDS Tree.

1.2.3 Installation Procedures

The Agent for NetWare Installation kit is available in an executable file format with the file name Agent-NetWare-6-00-2xxx.exe. Your service provider may have renamed this file.

The installation wizard guides you through the appropriate steps. When the installation program concludes, you may choose to edit the Autoexec.NCF.

1.2.3.1 Installation Steps

When you run the install executable, from a MS Windows workstation, the Welcome screen appears. Click **Next** to continue.

The Support / Release Notes information screen appears. You may print these if you wish. Click **Next** to continue.

The Software License Agreement for the program appears. You must Accept to continue further with the installation. Click **Next** to continue.

The "Select NetWare Server" screen appears. Enter a name, or select one from the pull down list. Click **Next** to continue.

The "Set Installation Path" screen appears. Enter the Agent Installation Path (typically SYS:\<installation_directory>\). Click **Next** to continue.

Agent Management Method Selection screen appears next. Choose one of:

- I will manage my Agent using Web Agent Console hosted at <Web Agent Console URL>
- I will manage my Agent using Web Agent Console. I will specify the location.
- I will manage my Agent using Windows Agent Console only.

That is, you may be asked to use a known Web Agent Console URL address, or to supply one if you want to use Web Agent Console, or to only use Windows Agent Console.

Depending on how your installation kit is set-up, and what Agent you have installed already, you may see:

a) all three of these prompts, or
b) the first and third, or
c) the second and third.

If you have selected to manage your Agent with Windows Agent Console only, you will not see the next screen on "Registering the Agent with Web Agent Console". But, if you have selected one of the first two choices you will see that screen next. "Would you like to begin the installation?" Click **Yes**.

"Register Agent with Web Agent Console" screen. If you are using the Web Agent Console, you must Register the Agent with it so that it can be managed by the Web Agent Console. You may or may not have an address in the address field, depending on what you selected in the "Agent Management Method Selection". Enter the username and password that will allow this Agent to register with the Web Agent Console. This is a name and password created for this Agent by an Administrator on the Web Agent Console. Click Next. The Registration will fail if it cannot connect to the Web Agent Console. You can run the installation again to register if you cannot succeed here. (In that case use, "Skip Registration" to finish.)

You could "Skip Registration" here, and only manage the Agent with Windows Agent Console, if you wish. Click **Next**.

NOTE: If this is an upgrade from a previous version, the Agent binaries must be installed in the same location as the previous version. Otherwise it is likely that the user will continue using the older version, since the older version search path appears ahead of the upgraded version.

The "Setup Status" screen appears, to show the installation progressing. When the installation has completed, you see a message (Note) reminding you **"If you want to edit autoexec.ncf to load VVAgent and BUAgent automatically, please make sure VVAgent and BUAgent are loaded after OFM."** Click **OK** to continue

At this point, if this is a new (first time) installation, the Agent installation is finished. You can now edit the autoexec.ncf file, if you wish, or run it from the console (see the steps below in the AUTOEXEC.NCF command).

1.2.3.2 Editing the Autoexec.NCF File

To permanently install the Agent for NetWare so that it is started after each reboot of the NetWare server, add the commands below to the AUTOEXEC.NCF command procedure.

To edit the AUTOEXEC.NCF file, load the EDIT.NLM and open the AUTOEXEC.NCF file. Add the following lines after the point where the TCP/IP stack has been loaded and configured (the end of the file is a good place) and save the changes before closing:

```
> LOAD OFM.NLM (OFM is optional)

> LOAD SYS:\<installation_directory>\VVAGENT (VVAGENT manages
  connections to the Agent from Windows Agent Console)

> LOAD SYS:\<installation_directory>\BUAGENT (BUAGENT manages
  connections to the Agent from Web Agent Console)
```

1.2.4 Upgrading from earlier versions

The Agent (NetWare) 6.0 supports upgrades from version 5.05 only.

Upgrading an Agent to Version 6.0 includes the following tasks:

- Meeting System and Software Requirements
- Preparing the Computer
- Running the Installation Kit

1.2.4.1 Meeting System and Software Requirements

To upgrade to Agent (NetWare) 6.0, your system must meet the minimum requirements listed below.

System Requirements:

The server to be upgraded must be running one of the following:

- NetWare 6.0 server with Support Pack 5
- NetWare 6.5 server with Support Pack 7

Available free space of the volume that the Agent is installed on should be bigger than the size of all Delta files + the size of the largest Delta file + a reasonable cushion (at least 100MB).

There is no space restriction for the Agent installation directory.

An MS Windows workstation that has the latest version of the Novell Client for Windows, or Microsoft Client Service for NetWare installed.

Software and Other Requirements:

- Agent NetWare 5.05 installed.
- Agent (NetWare) 6.0 installation kit.
- Supervisor rights of the eDirectory tree. NetWare 6.0 requires a username in the format below: "`admin.dept_name.company_name`"

Preparing the Computer

To prepare your existing NetWare server for upgrading the Agent, complete the following tasks:

- Back up the previous Agent Files
- Clean up Server Profiles in Global.vvc
- Clean up Jobs
- Synchronize all backup Jobs
- Verify eligible Vault version (5.53 or greater)

Backing Up the previous Agent Files:

We strongly recommend that you make at least one backup of your previous Agent files, including all files and subdirectories under the Agent installation directory. Do not attempt an upgrade without a backup.

To do so, first unload VVAgent from the server console, manually copy those files to a different place. It is better to use a different volume. Then load VVAgent again.

Clean up Server Profiles in Global.vvc:

From the Agent Console, open up the Agent Configuration of the Agent that you want to upgrade. Go to Vaults section, check if there is any server configuration that no longer being used and delete it. Also, highlight every server configuration and click Edit, and double check that the information of this server profile is valid. Then click OK to save your changes.

Synchronize all backup Jobs:

After cleaning up Jobs, check the backup logs of each Job to see if any errors show "Validation failed". If so, you need to verify the validation information with your Vault Operator to make sure it is valid. If the latest backup log shows no errors, do a Synchronize with the Vault and check the Synch log.

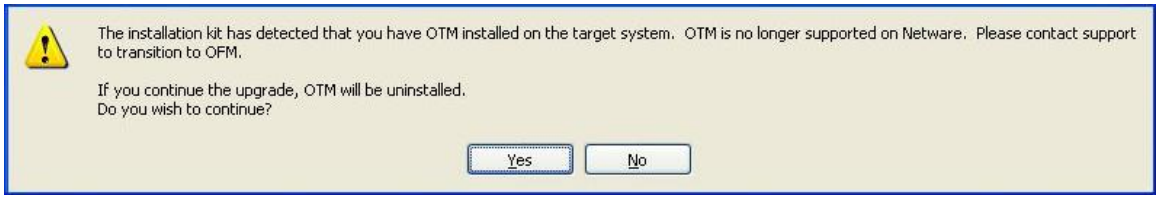
1.2.4.2 Running the Installation Kit

We recommend starting upgrading when all the Vaults in Agent Configuration are not busy on other Jobs.

Then run the Installation Kit Agent-NetWare-6.00.2xxx. The upgrade is done automatically through the Agent for NetWare installation.

Previous OTM installation

If OTM had been previously installed along with the Agent-NetWare 5.05, you will be prompted with the following message.



If you choose to continue OTM will be uninstalled. Then you will need to transition to OFM for open files protection.

If you choose not to continue, the installation will stop and rolls back. You will have to run the installation kit later.

Successful Upgrade

If the upgrade is successful, the user will not see any messages. The installation finishes like a fresh install and the agent files will have been upgraded.

Failed Upgrade

If the upgrade fails, a message is shown to the user saying that the upgrade has failed. That message will show the contents of the upgrade log file, which should indicate where the problem is. Then the user has to abort the installation, which will be rolled back. After having fixed the problem, the user can run the upgrade again later.

Undeterminable Upgrade Status

In case the installation kit is unable to determine the upgrade status, the user will be informed. The options, then, are either abort or continue the installation.

- If the user chooses to abort, the installation will be rolled back and the user will have to upgrade again later.
- If the user chooses to continue, the installation will proceed and complete. But in case the upgrade did, in fact, fail and the user had chosen to continue, then they will have to re-run the installation kit again to get the agent files to upgrade, otherwise their agent will not run.

1.2.4.3 Uninstalling the Agent for NetWare

To uninstall the Agent for NetWare (in permanent configuration):

Load the NWConfig program from the NetWare console or use RCONSOLE from an Agent workstation.

- Choose the **NCF Files Options** selection.
- Choose to edit the AUTOEXEC.NCF file.
- Remove the following entries:

```
> LOAD OFM.NLM (if used)

> LOAD <vv_volume>:\<vv_directory>\VVAGENT
  e.g.: SYS:\<installation_directory>\VVAGENT
  e.g.: SYS:\<installation_directory>\BUAGENT (if used)
```

Exit from NWConfig.NLM when completed.

1.3 How the Agent for NetWare Works

The Agent Console and Agent applications comprise a data protection software suite that securely backs up and restores file data from Servers across a network to a remote Vault. The applications provide an automated lights-out method for protecting your valuable computer data without the need for tape devices or other Backup media.

The Agent User's Guides explains how to configure the Agent installed on individual computers, and how to do Backups and Restores. The "Agent Console Operations Guide" further explains, in more detail, how to use the Agent Console application to configure Backups from those computers running the Agent.

1.3.1 Agent Software

The Agent software runs on the individual computers to be backed up. Backups and Restores on the Agent computers are configured and scheduled by the Agent Console computer. The Agent communicates its Backup data directly to the Vault.

The Agent consists of the following components:

The "VV" component performs the Backup and Restore functions to the vault.

The "VVAgent" and "BUAgent" components handle scheduling, configuration and communication with the Agent Console. They run as NetWare NLMs.

Note that the NetWare Agent is not multi cpu aware.

1.3.2 Agent Console Software

The Web/Windows Agent Console program provides a centralized point of control for managing all computers (not just NetWare) running the Agent software on a large computer network. Within an organization, the configuration and scheduling of Jobs is done through the system running the Agent Console software.

Note: The following description is for background information only, and is not necessary for using this document.

1.3.3 Vault Console Software

The Vault Console software controls and manages the pooling and storage of backup data at a remote secure Vault location. This data is communicated to the Vault from the Agent computers over a WAN, LAN, the Internet, or imported from an alternate media.

1.3.4 On Line Helps

The help in the Agent Console GUI is accessed from the main drop-down menu, or by using the F1 function key (Windows Agent Console). There is also context sensitive "WhatsThis?" help on each GUI screen (Windows Agent Console).

Web Agent Console is described in the Web Agent Console Administration User Guide, and the Web Agent Console on-line help.

1.3.5 Overview of Product Set

This diagram shows the relation between the various related products.

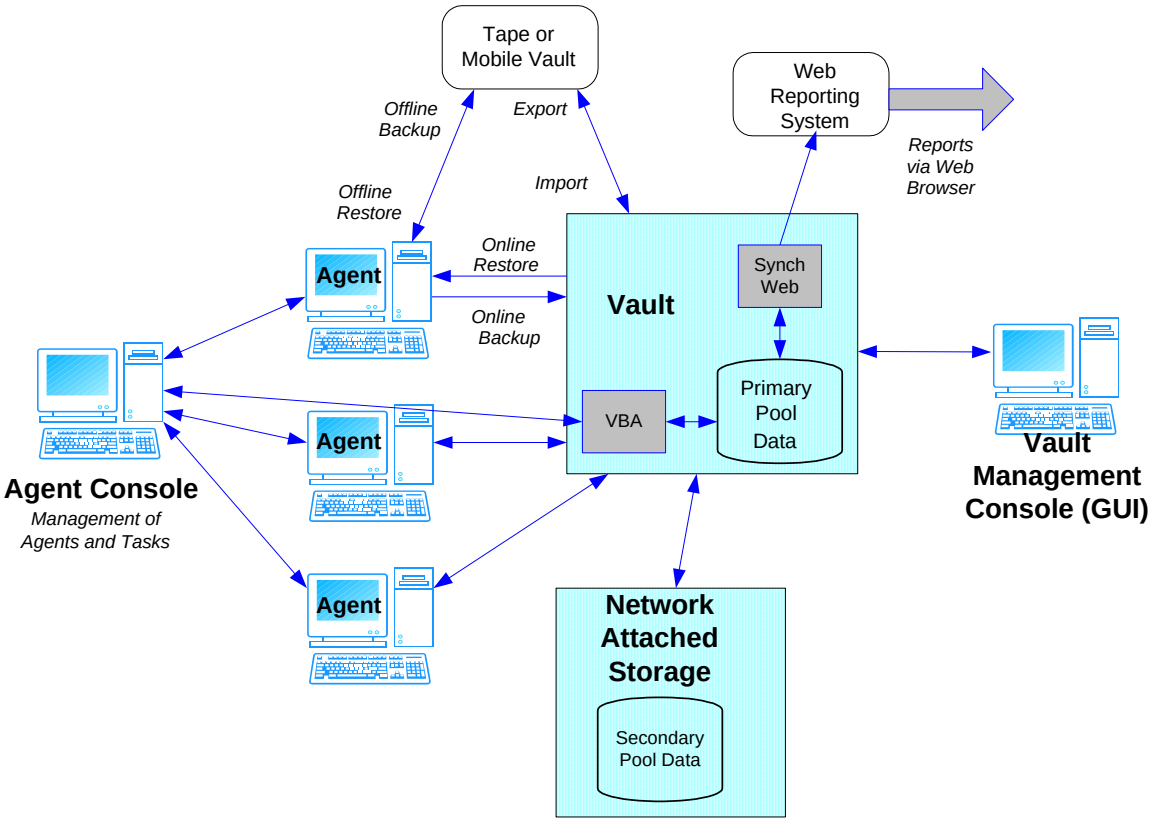


Figure 1. – Product Set

1.4 Agent Console Configuration Overview

The Agent program runs as an NLM on the server (computer) that will be backed up. You use the Agent Console program to control and direct it. One Agent Console program controls many Agents on many servers on a network.

Names, passwords, and permissions are needed to allow the Agent to connect with the Agent Console.

- Each server (computer to be backed up) needs an Agent.
- You need to connect (from the Agent Console) to an Agent (when you configure a new Agent).
- You must supply: a Name, IP address, and user/password.
- Then, you must Register the computer to the vault.

You must Register a computer to a vault to be able to "logon" to that vault and establish a connection. The vault must know that this Agent is valid and is authorized to perform its functions.

You will need to "re-register" a computer if you are restoring from another computer, or you are performing a bare-metal restore.

Jobs are registered during their configuration, and are used during a backup. They contain information such as:

- Which profile is used? (i.e.: which vault?)
- What data is to be backed up?
- What type of logs?
- What type of encryption (if any)?
- When is it scheduled?

Note: The first backup is a "seed" (complete backup), the next and subsequent ones are deltas (i.e. changes only), but they are still considered a "full" backup.

Depending on how your system is configured:

- There may be more than one vault you can connect to.
- One Agent Console usually controls all the Agents on your network.
- You can also backup to the Agent's local disk or tape.

2 Performing Backups

2.1 Introduction

These steps are described from the point of view of a user on a newly installed system. They will "get you going" to be able to perform a backup. The "Agent Console Operations Guide" manual describes all the features, options and further details of the Agent Console program.

An Agent configures, manages, runs and monitors backup Jobs. You can manage and control many Agents through one Agent Console application (GUI). An Agent may have multiple Jobs.

A Job defines the parameters associated with a backup, restore, or other commands. Examples of parameters include: file selections and filters; compression; and encryption settings. A Job always belongs to only one Agent. Job names are unique on that Agent.

A profile defines the vault configuration that will be used by your Agent. It matches a Job to an account on a vault. The Job uses the profile to validate the backup to the vault, and to know where to put the backup. A profile may be used by more than one Job.

Seeding / Re-Seeding is a full backup created on the Vault when you run your first Backup (safeset). This first safeset contains all the data selected for backup and is called a "seed". Subsequent backups are deltas (changes in file) that are applied to the first full backup to create subsequent safesets. This way a current full backup is always available.

If the Agent detects changes, such as the encryption type or password changing, the next backup will be a re-seed.

In the case of a re-seed, your backup will take longer to complete and a message about re-seeding is created in the log file.

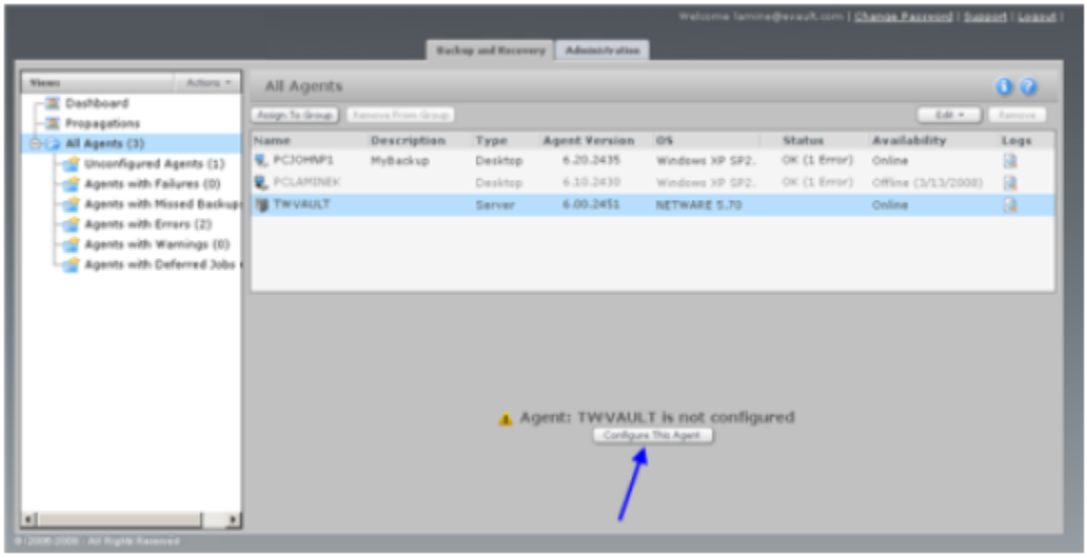


Figure 2. – Configure Agent

2.2 Configuring an Agent (creating a Job)

After having newly installed an Agent and registered it to Web Agent Console, it displays as Unconfigured on the Web Agent Console Dashboard. Note that by configuring the Agent, you are creating a new Job at the same time.

Click the button "Configure This Agent" to start the wizard that leads you through the configuration of the Agent.

2.2.1 Agent Description

Figure 3. – Agent Description

Enter a description (meaningful to you) of the Agent and click the button "Next"

This brings up the Backup Source Type selection screen

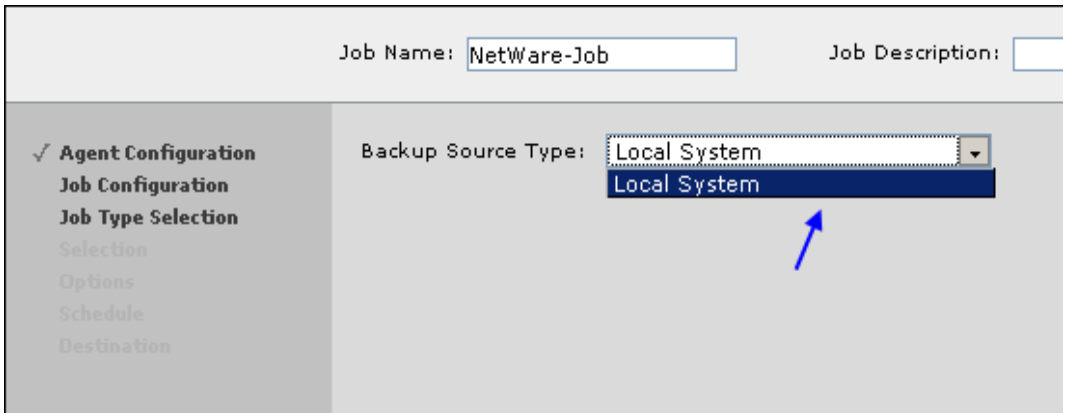


Figure 4. – Source Type

After having entered the Job's name, choose Local System then click the button "Next"

This brings up the files Selection screen

2.2.2 Data Selection

2.2.2.1 Common Files and Folders Inclusion

This screen allows you to select the files you wish to include to your backup Job.

You can "open" the tree in the left pane by clicking on the + signs. Click in the check box next to a folder or file name to select them.

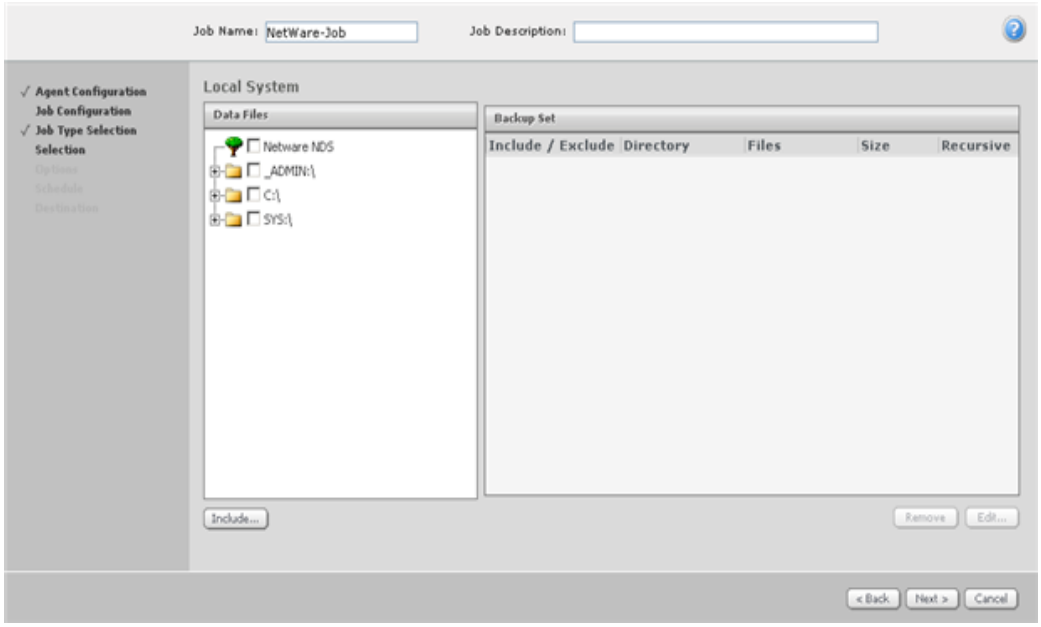


Figure 5. – Data selection

Click **Include**. The file/directory names are moved to the right hand side pane. The **Remove** button allows you to remove files from this list. The **Edit** button allows you to edit options for a folder.

If you have a directory with a large number of files, and you want to select most of them, it might be easier to select the directory, and then **Exclude** (from the list) the ones you don't want.

You should exclude any files and directories that will be busy (open) during the backup, and do not need to be backed up. This includes the directory where the Agent is installed. The backup will still work, but you will see error messages in the log file such as:

"`error opening file …`".

You may also select one directory (folder) at a time to be backed up. When you click **Include**, you will get a message asking if you want to include all files, or just some of them which match your selection criteria (filter).

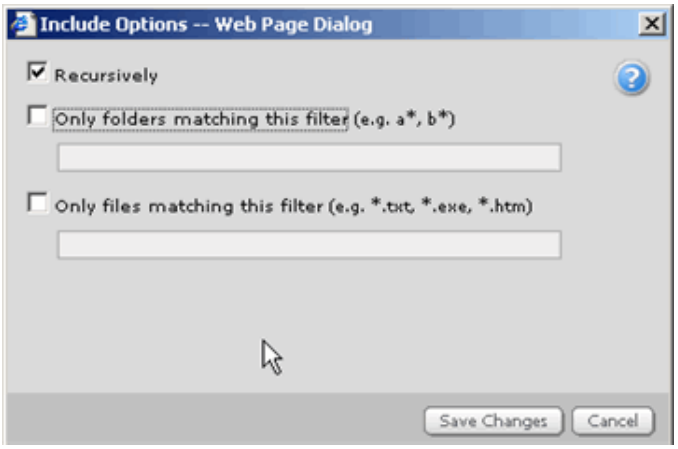


Figure 6. – Include Options

"Recursively" means to include all files and directories below this directory. Otherwise you may choose to select certain files, depending on their names and extensions. A period (.) means a recursive directory.

Previously, if a file selection contained nested exclusions and inclusions, the exclusions would always take precedence. Now, the selection with the most detail will take precedence. This allows for nesting of multiple inclusions and exclusions. In these cases, the filtering will avoid traversing excluded directories.

Wildcards in File Names and Directories

An asterisk (*) means all files with any (partial) name or extension, or a part (start, middle, end) of a Directory name.

A question mark (?) means a single character in a file name, or Directory.

Wildcards in Directory Paths

Wildcard path elements are handled and supported for Backup selections. The Vault does not support or recognize wildcard folder selections for the purposes of Restore. The Agent supports wild-carded path elements for both inclusion and exclusion.

For example, assume you have on your server, a directory called "Users", and below it are directories for each user's name, in alphabetical order (C:\Users\<all the A's>, C:\Users\<all the B's> and so on until <all the Z's>. You want to be able to backup up all these user directories.

If you just select "C:\Users" and select Recursive, you will get everything, in one backup. But as more users are added, the backup takes longer. What you want to do is break the backup into separate backups, with each taking a part of the data. For instance, one takes all the A to E, another takes all the F to J, or whatever "balance" you decide.

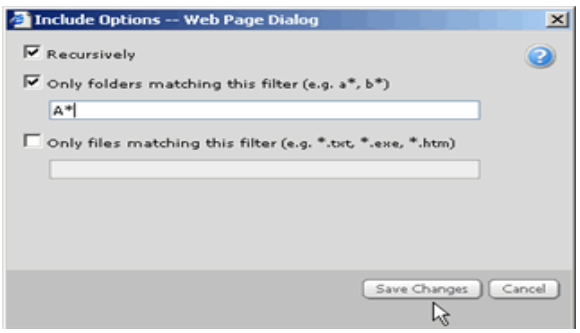


Figure 7. – Include Options

If you use a wildcard with each letter, A*, B*, C*, D*, E*, (and recursive) for one backup, you can get all the data, automatically including any new ones added, and excluding old ones deleted. Another backup Job may use F*, G*, H*, I*, J* (for example).

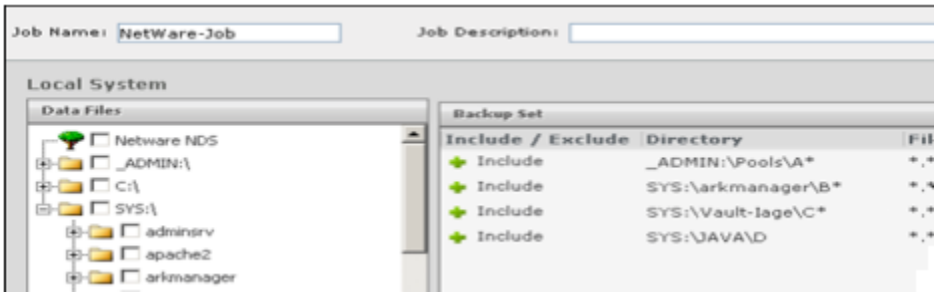


Figure 8. – Wildcard example

Of course, you can still filter further with "Only files matching this filter".

Wildcard Rules for Directories

In these examples, a path element is a part of the path (\ …\) of a directory. If the wildcards are not used in this way, you will see an error message. Note that the *.* at the end of the selection represents wildcards for the files. This is different than the wildcards for the folders.

Only the last path element of the selection can contain a wildcard:

Supported: SYS:\Projects\A*\.*.*

NOT supported: SYS:\P*\Active\.*.*

A path element of a selection can only contain one wildcard:

Supported: SYS:\Project*\.*.*

NOT supported SYS:\P*j*\.*.*

The wildcard can appear anywhere in the path element:

Supported: SYS:\Project*\.*.*

Supported: SYS:*Projects\.*.*

The Agent supports one path element with a wildcard per selection:

Supported: SYS:\Projects\User*\.*.*

NOT supported: SYS:\P*\U*\.*.*

2.2.2.2 NDS Tree Inclusion

If you choose to include the NDS tree in your backup Job, once you select it and click **Include**, you will be prompted to provide credentials for the NDS tree as well as to choose other options for the NDS tree backup.

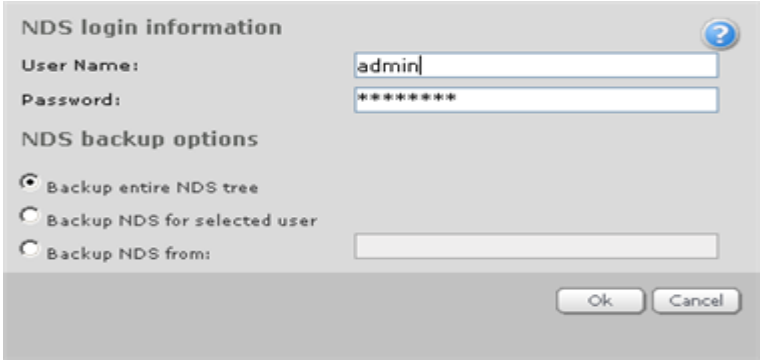


Figure 9. – NDS tree Inclusion

a) To backup the entire Novell Directory Service (NDS) tree, select Backup Entire NDS Tree. This backs up the NDS tree from the [root] object on down. This option requires that the NDS user specified have supervisor object rights to the tree root.

For example: To backup the entire NDS tree on behalf of user "admin" from the container "`mycompany`", you should specify "`.admin.mycompany`" as the user name and password;

b) Backup NDS for selected user backs up a selected user, which means that the backup commences from the partition root that the NDS user is on.

For example: To backup NDS for user "admin" from the container "`mycompany`", specify "`.admin.mycompany`" as the user name and password. Only the container with user admin (and all objects it contains) will be backed up;

c) Backup NDS from a specified location backs up any valid container or leaf object within the NDS tree. If the object is a container, then its descendant will also be backed up. This option requires that the NDS user have supervisor object rights to the object specified. Enter a location to start the NDS backup from.

For example: To backup only the container "`mycompany`", enter "`.admin.mycompany`", the password, and then specify "`.mycompany`" in the "Backup NDS from" field.

Note: In addition, you may use another method to backup and restore System State (as opposed to just NDS). This is applicable to eDirectory 8.7 and above, and is often called "Hot Continuous Backup". This method is described at:

http://www.novell.com/documentation/edir873/index.html?page=/documentation/edir873/edir873/data/a2n4mb7.html.

2.2.3 Job Options

2.2.3.1 Encryption and Advanced Backup Options

Once you have finished selecting the files to backup, click "Next" to go to the "Options" screen.

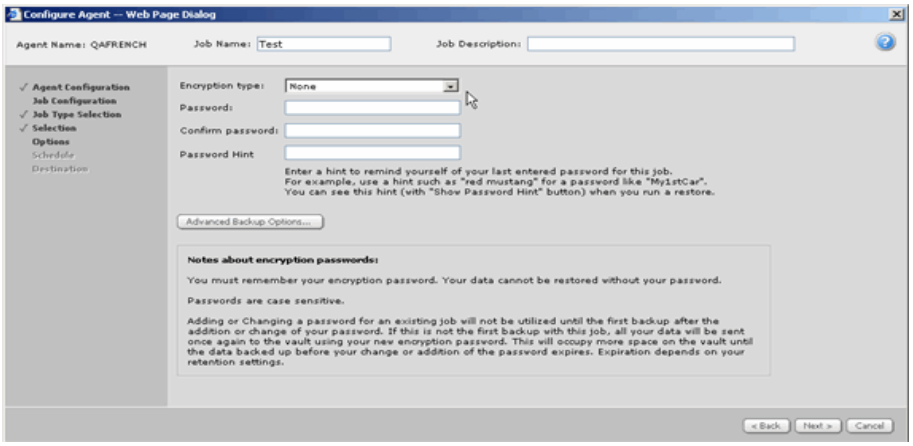


Figure 10. – Job Options

Here you can select an encryption type, and create a New Password (case sensitive, up to 31 characters). The different types have different cipher strengths, from DES-56 to AES-256.

- None – no password
- DES 56 bit
- Blowfish 56 bit
- TripleDES 112 bit
- Blowfish 128 bit
- AES 128 bit
- AES 256 bit

Confirm (re-enter) the password. You can enter a password hint to make you remember your password. For security reason the password hint should not be the same as the password.

The Advance Backup Options allows you to choose:

- A retention type (Daily, Weekly or Monthly)
- A compression type
- To Back up files opened for write or not
- To clear archive Bit processing or not
- To create log file or not and adjust the log file's detail level
- Support NetWare file compression

For detailed descriptions of the Advanced Backup Options, see the Agent Console help or user's guide.

Click "Next" to go to the schedule screen.

2.2.3.2 Notes on NetWare File Compression

If this check box is selected, the software backs up the NetWare file in compressed format. This feature is useful for files that are rarely modified. Note however, that the Backup Delta processing feature does not work on compressed files. Each time the compressed file is accessed, the Backup sees the entire file as new and must reseed it.

Advantages

1. Backing files up in their native compressed form ensures that they will be Restored in compressed form, reducing or eliminating the possibility of a disk full situation.

2. Backing files up in their native compressed form reduces CPU overhead by not having to compress and decompress on-the-fly during Backup and Restore.

Disadvantages

1. Files can only be backed up in their native compressed form if the O/S supports NetWare compression and compression is enabled on the volume that the files are Restored to.

2. When files change from compressed to uncompressed, or from uncompressed to compressed, the application must Backup that file in its entirety. If the compression settings in NetWare are too aggressive (meaning a lot of compression state changes are occurring) the Delta processing will be inefficient.

3. Currently, natively compressed files cannot be Restored to an NSS volume.

The Support NetWare File Compression check box is unselected by default. NetWare files are backed up in uncompressed form, enabling full Delta processing and often saving storage costs over the long term.

Be aware, however, that you will require significantly more room on your system for the Restored files if your original files were compressed.

If you have selected to support NetWare compression, you can detect changes during **Quick File Scanning**. This detects if the data has been converted by the O/S from non-compressed to compressed, causing a re-seed. Any file streams that are deemed unchanged since the last backup are skipped over. The default is to read files in their entirety.

2.2.4 Scheduling Jobs

A Job (a Backup or Synchronize, but not a Restore) can be run at pre-determined (scheduled) times. All Jobs can also be run "manually" (ad hoc or unscheduled) when desired.

Note that, if you wish, you may choose to finish the configuration without scheduling the Job and come back later for a schedule.

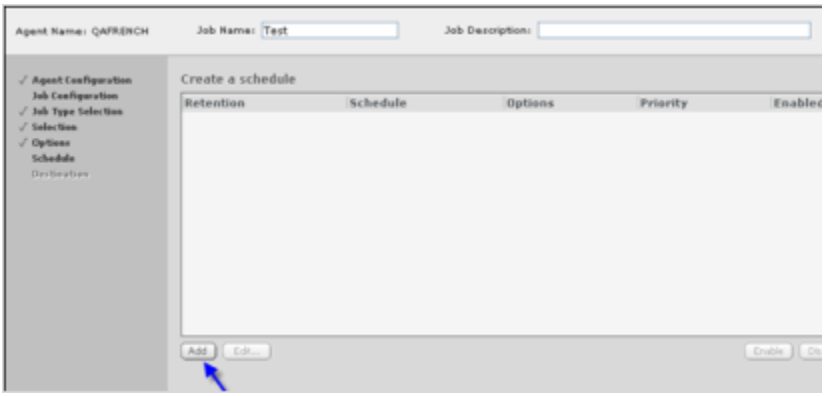


Figure 11. –Schedule Creation

Click the button "Add" to display the Schedule details screen.

Here you can:

- Change the schedule view mode,
- Check the days you want the backup to be done,
- Enter a time you want the backup to be done,
- Choose a retention scheme (this will determine how long your backup will be kept online),

Open the Advanced Schedule Options and:

- Select the compression mode,
- Choose to use deferring or not,
- Adjust the Backup time window.

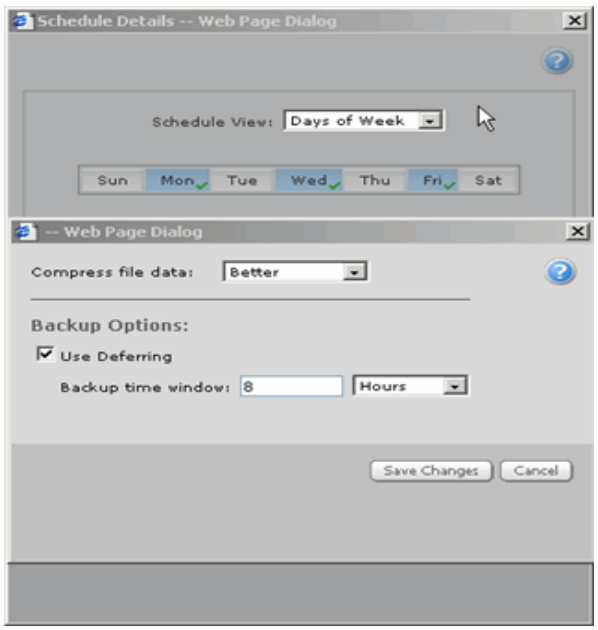


Figure 12. – Schedule Details

Once you have finished your schedule, click "Save changes" from the Advanced Schedule Options screen and then "Save changes" from the Schedule details screen.

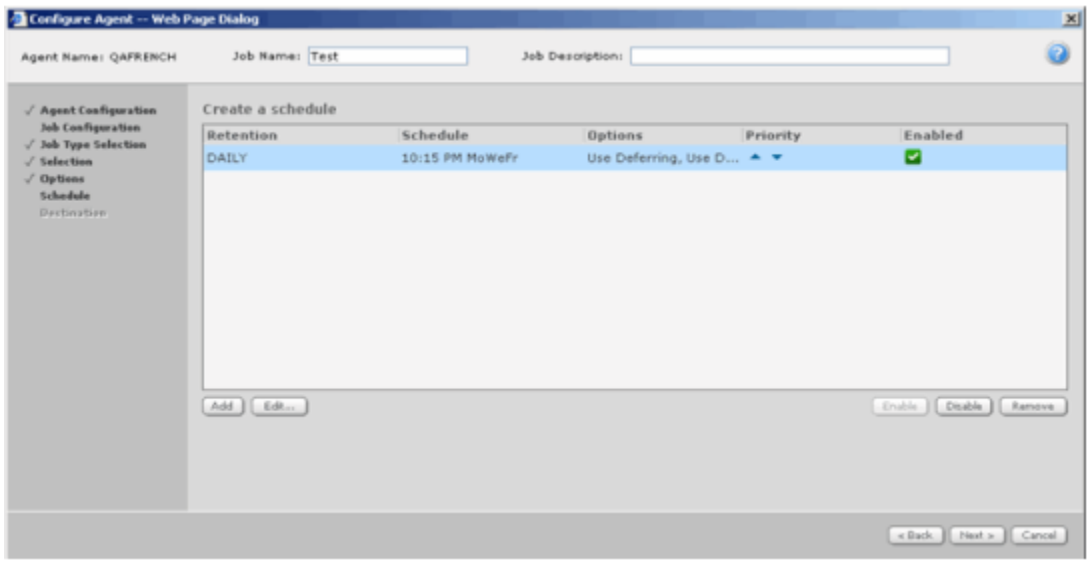


Figure 13. – Scheduled Job

Click "Next" to go to the Destination screen.

2.2.5 Registering Jobs to Vaults

The last step of the Agent configuration process, this screen is where the user enters all the information (profile) necessary to connect to the vault and send backups to it. If this is the first time you configure an Agent, the "New Vault" screen pops up automatically when you click the "Next" button from the "Schedule" screen.

Here you have to:

- Enter the vault name,
- Enter the vault's address and click "Add",
- Enter your credentials for the Vault.

Note that those credentials should be given to you by your Vault administrator who creates the accounts for connecting to the Vaults.

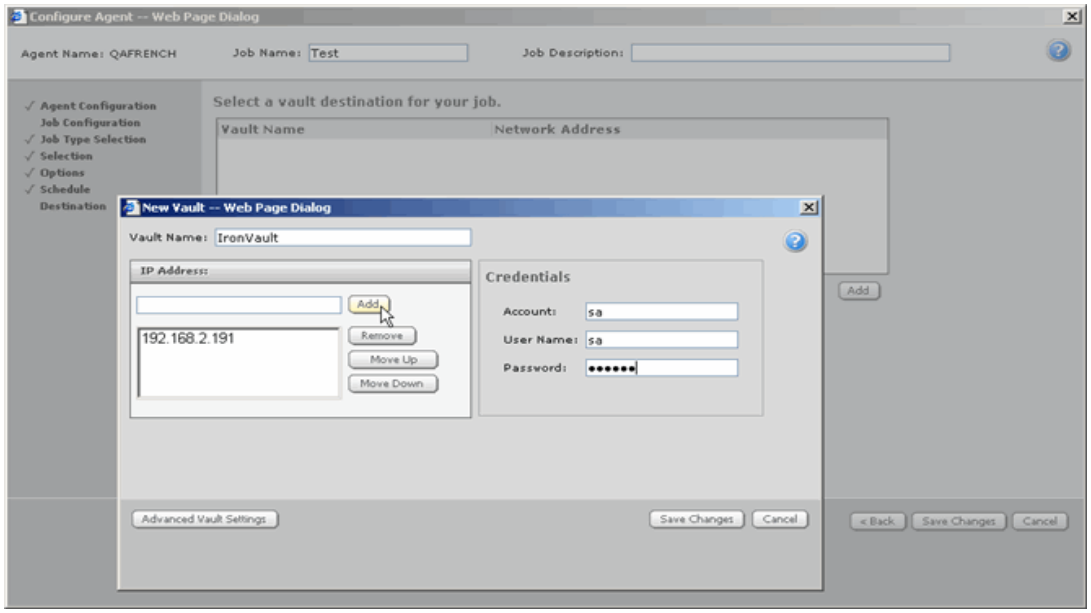


Figure 14. – New Vault

The Advanced Vault Settings allow you to:

- Choose a specific port number. Note that priority is given to the topmost port number in the list. Use Move Up/Down buttons to change the port number position.
- Set the reconnection intervals,
- Set the time period after which reconnection tries stop,
- Enable over the wire encryption

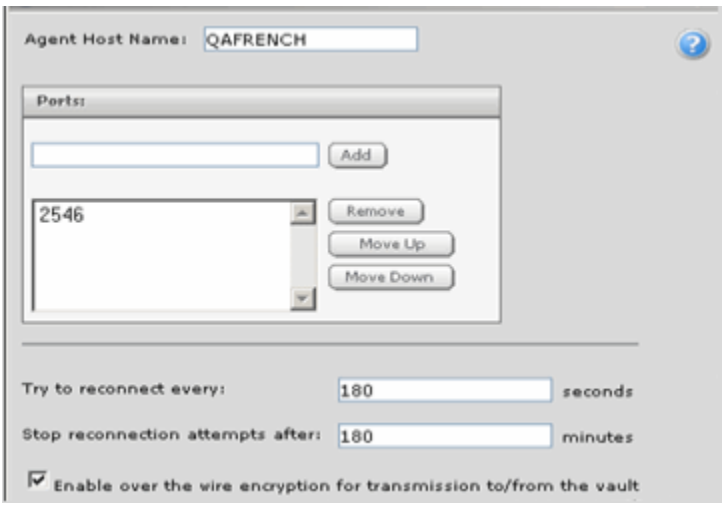


Figure 15. – Vault Configuration

Click "OK" to go back to the "New Vault" screen, then click "Save Changes" to finish registering the Job to the Vault.

Once you have finished registering the Job to a vault, click "Save Changes" to finish the Agent configuration. Now the Agent is configured with a new Job created.

If you want to go on creating another Job for that Agent, click the button "Add" which will lead you through the same wizard.

The next chapter will show how to run a backup.

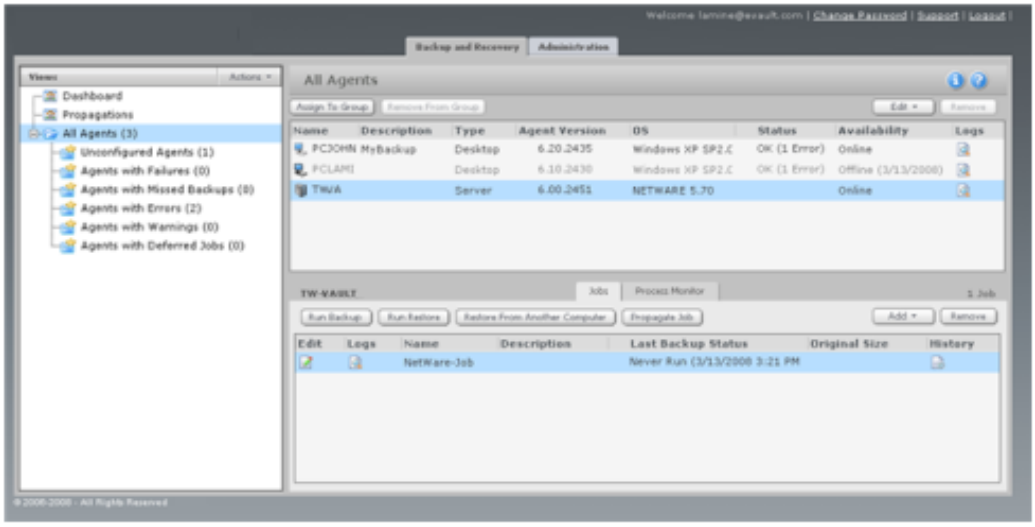


Figure 16. – Newly Created Job

2.3 Running Backups

Once all the Agent Configuration information has been entered, and a schedule set up, as in the previous chapter, the Backups will take place automatically at the scheduled time.

On occasions, you may need to run a "one-time" (Ad Hoc) Backup for a special reason. You can either use an existing Agent and Job (and modify it) or create one specifically for that Backup.

2.3.1 Ad Hoc Backup

To run an ad hoc Backup, click on a Job to highlight it and then click the button "Run Backup"

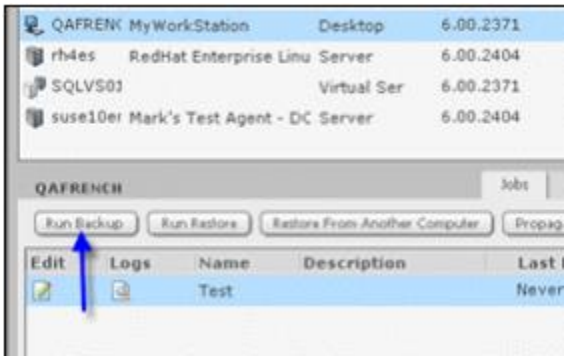


Figure 17. – Ad Hoc Backup

This brings up the "Run Backup" screen

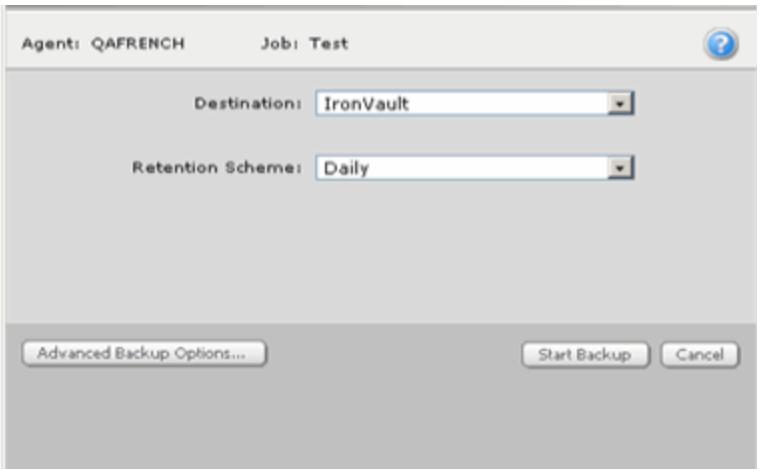


Figure 18. – Run backup

Here you choose a:

- Destination, the vault to send the backup to, or "Directory on Disk" if you want to send the backup to a directory on the same machine running the Agent.
- Retention scheme that determines how long the backup is kept on the Vault.

The Advanced Backup Options allow you to:

- Set "Quick File Scanning" on or off,
- Use deferring or not,
- Adjust the backup time window.

Click "OK" and then, on the "Run Backup" screen, click "Start Backup"

The backup starts with a screen showing the backup process that tells, at the end, whether the backup completed or failed.

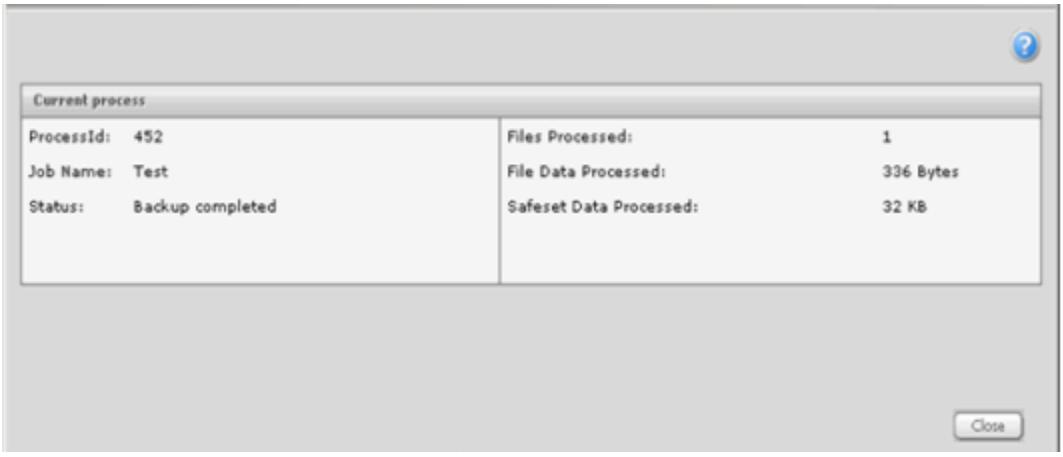


Figure 19. – Completed Backup

Once the backup is completed, the Process Information screen can be closed.

2.3.2 Log files

Log files are the System transcripts of what happened while the Backup, Synchronize or Restore function was running. To display a log file for a Job, click the icon under "Logs" column.

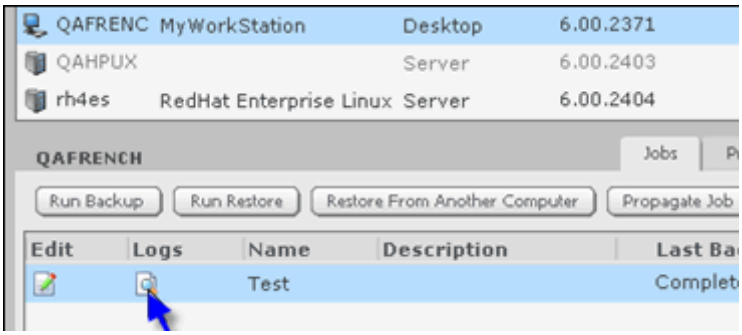


Figure 20. – View Logs

From the drop down "Log Files", choose "Backup", "Restore" or "Synchronize"

You can display the whole log info in a new window by clicking "View".

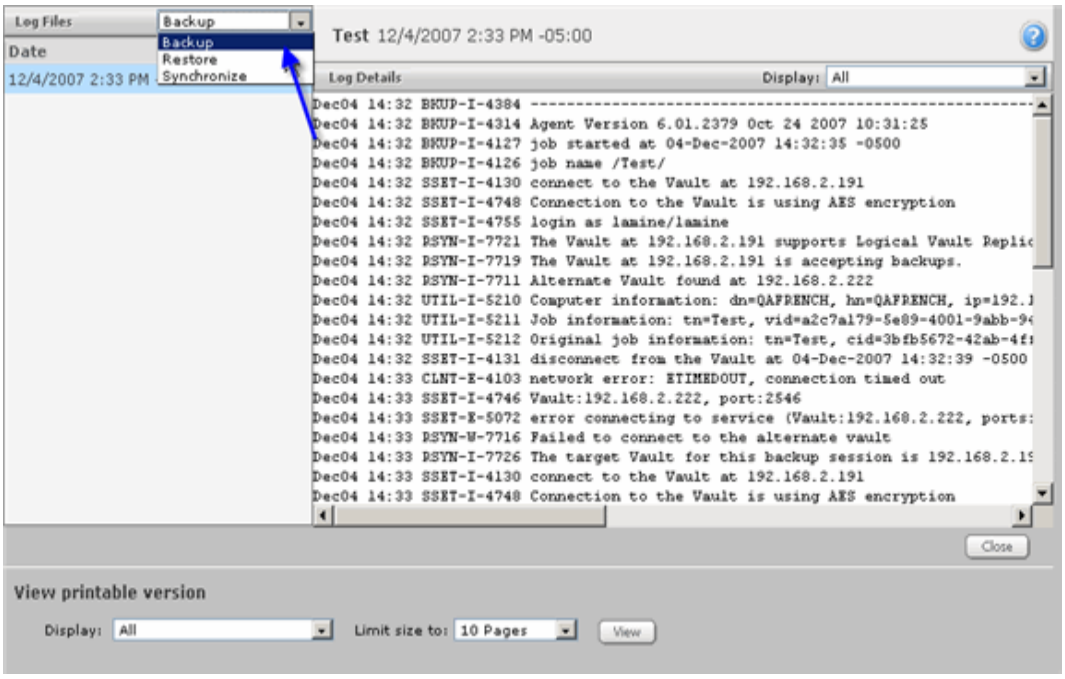


Figure 21. – Log Viewer

2.4 Editing Jobs

After having already created a Job, you may want to come back and change some of your options. The "Edit Job" option allows you to do so.

> **Note:** It's not possible to edit the "Backup Source Type" from the "Job Type Selection" tab. If the "Backup Source Type" you selected before does not suit your needs, you will have to create a new job or delete that job.

To edit a Job, from the Job's pane, click the icon under the column "Edit".

You can change your options, from tab to tab, in the same way you did it when you first created the Job and click "Save changes" when you are done.

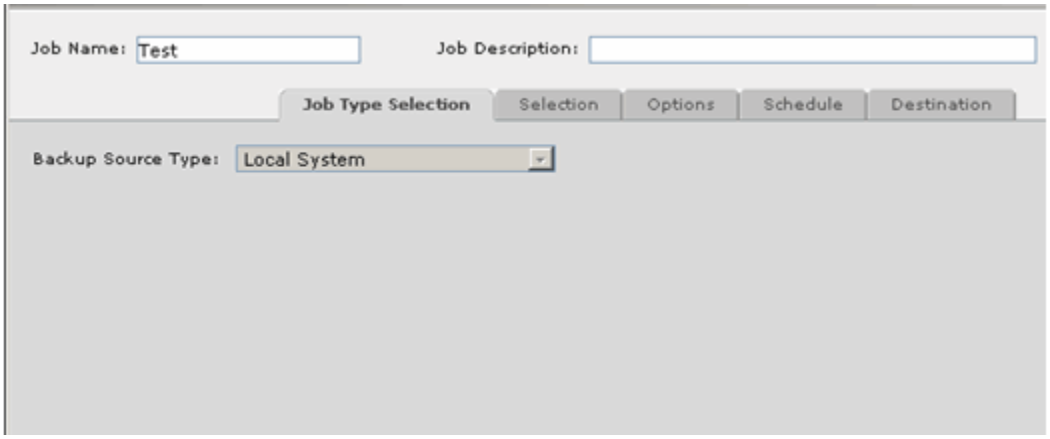


Figure 22. – Edit Job

3 Performing Restores

3.1 Restoring from a Backup

There are several circumstances or reasons why you may want to do Restores.

- To recover one or more data files or directories. You can Restore them to their original location, overwriting any that are there, or Restore them to a different location on that disk, so that you can then decide on which files you want to copy (restore).
- To recover data that was backed up from one computer, to be Restored on another (similar) computer System.
- To recover a complete System (from the "bare-metal" up) when the original System has been lost.

You can run multiple individual Restores at the same time (i.e.: simultaneous restores). Each one will start a new process, which you can monitor.

3.1.1 Restoring Common Folders and Files

Restoring from a Backup is the most common usage, allowing you to recover anything from a single file to a complete directory structure.

To start a Restore, click the Job you want to restore from and click the button "Run Restore". This brings up the "Restore from Backup" wizard.

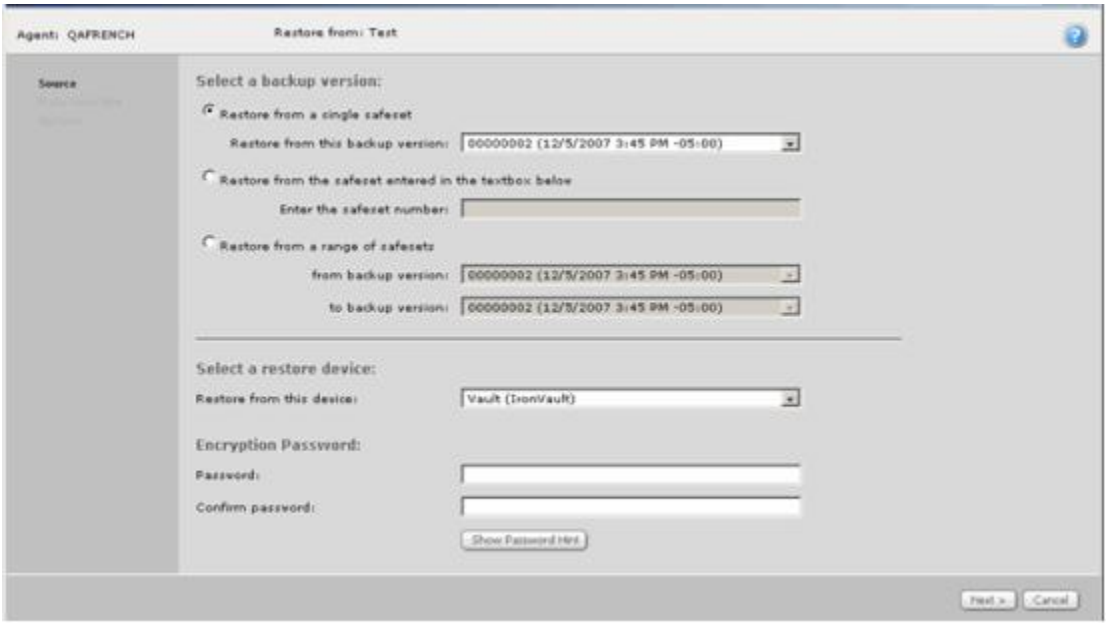


Figure 23. – Run Restore

3.1.1.1 Source screen

Here you can:

- Select a safeset, enter a Safeset number or select a range of Safesets.
- Select a Vault or Directory on Disk depending on where the Backup was sent.
- Enter the Password if the Backup is encrypted. You may not see the password section if the Backup was not encrypted. Click "Show Password Hint" if you have forgotten the password. Note that the password is case sensitive and if you have lost the password, you cannot access the Backup data.

3.1.1.2 Data Selection screen

Here you can:

- Select the Restore objects (files or directories).
- Expand the directories (if available) and select or deselect files to include in the Restore.

3.1.1.3 Destination screen

Here you can:

- Restore files to their original locations, or to alternate locations.

  If you choose to Restore to the original location, the initial directory structure is recreated. When this option is selected, the "Preserve folder structure" option is checked by default.

  When restoring to an alternate location, you may choose whether or not to preserve their folder structure. If you choose not to preserve their folder structure, all of your files will be Restored to one directory.

Note: If two files with the same name, but located in different volumes, are Restored to the same alternate location, Agent Console does not differentiate between volume names. The first file is Restored and then overwritten by the second file**.**

- Overwrite existing files with the restored ones.
- Do not restore existing files by overwriting the existing ones
- Rename restored files, so that they don't conflict with existing ones.
- Rename files that already exist, so that they don't conflict with restored ones.

Note: Renaming will append additional (cumulative) extensions to the file. These extensions start at .0001, then .0002, .0003, and so forth.

3.1.1.4 Advanced Restore Options

When restoring from a backup including common files and folders only, the Advanced Restore Options will be displayed as below. "Restore all data streams and trustees / space restrictions" is selected by default.

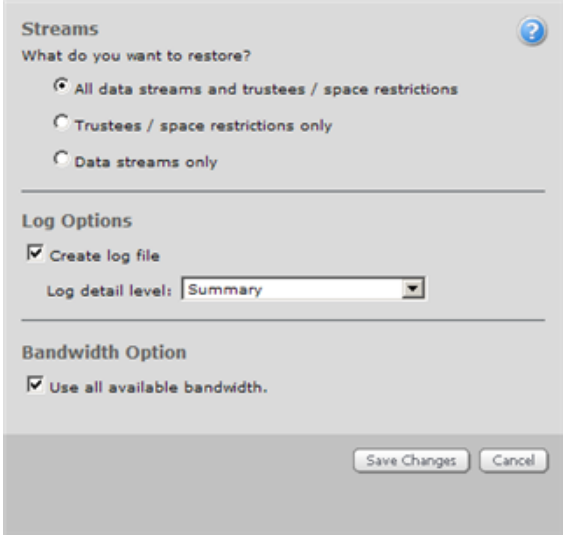


Figure 24. – Advanced Restore Options

Files and directories on NetWare may have additional information associated with them, such as trustee rights and space restrictions. Although, in typical Restore scenarios this information is restored together with files, the Agent is capable of restoring it separately from files it belongs to.

You may need to restore trustee rights and space restrictions only, without associated files, to re-apply this data to already restored files (regardless of the location they were restored to - original or alternate).

The Agent can also restore "Data streams only", without this additional information. For example, you may need to omit trustee rights and space restrictions from a Restore if you Restore data to a larger volume for which the space restrictions do not make sense, or if you need to remove trustee rights from restored files.

Note:

When trying to restore safesets on a NetWare system, you may get errors such as: "**O/S message: No space left on device**", and "**Job failed to complete**". This problem is caused by quotas on the directory at the source. As a fix, there is a new option (on the Command Line only) to disable directory space restrictions on Restore. A CLI example of this would be:

```
LOAD VV RESTORE Job_name /PARAM=job_name.VPR /IGNDIRSPACE
```

3.1.2 Restoring NDS Tree

If you have backed up the System State (NDS Tree) and now you want to restore it, more granularity is offered on the "Advanced Restore Options" screen. Those options are:

- Restore security objects
- Restore NDS server data

Note that these two options are unchecked by default. This is to give the user the choice to either restore those data or not.

But in case of a "Bare Metal" restore, the user may need to restore them so they can have the exact system state restored.

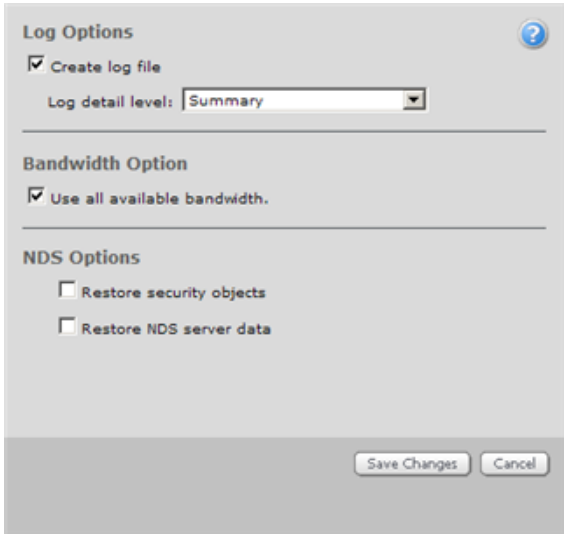


Figure 25. – NetWare NDS Restore Options

3.1.3 Restoring from CD or DVD

The Agent will allow restores directly from a CD or DVD drive, without having to copy safesets to the hard disk first. CDs and DVDs with safesets are created by Vault personnel.

CDs typically can store around 700 MB, while a DVD will store about 4 GB.

There are several ways the safesets can be stored on the media:

- A single SSI on a single CD/DVD.
- SSI files that are divided into many SSI files with a fixed length, but the whole set fits on a single medium.
- CDs or DVDs that contain a single backup that spans more than one media.

The user specifies "Directory on Disk" and then browses to the folder containing the SSI file. The SSI file on the CD/DVD must correspond correctly to the safeset number that is specified under "Restore from the following safeset". If not, the Agent Console will show an error when the restore operation begins, saying that the medium is not the right one.

When the Restore operation begins it will request a certain CD/DVD to be mounted in the drive, if there is no media mounted. If a second (or more) media is required, it will be prompted. It will not prompt if the requested SSI is on a CD/DVD that is already in use (i.e.: mounted).

3.1.4 Restore Process Information

Once you finish choosing your options, click "Run Restore" to begin the restore process.

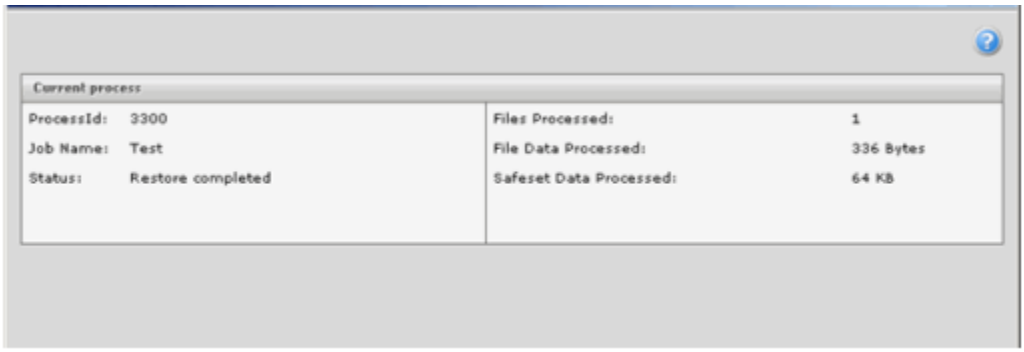


Figure 26. – Restore Process Information

3.1.5 Restore Log Files

To see the log file for a Restore, under the Agent's Jobs pane, click the Log icon, then on the "Log File Viewer", click the drop down "Log Files" and select "Restore".

3.2 Cross Computer Restores

Under "Backup and Recovery" tab, click the Agent you want to Import a Job to. Then click, under "Jobs" tab, "Restore from another Computer".

This brings up the "Restore from another Computer" wizard.

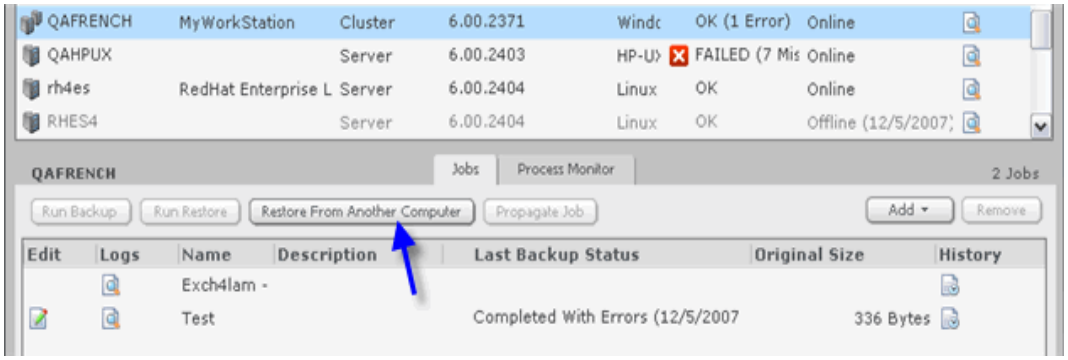


Figure 27. – Backup from another Computer

What the "restore from another computer" option does is it allows the User to redirect the (original) Restore Job to a different client (location). It re-registers where the configuration file was originally pointing, so that the Restore Job can be redirected to another location. It does this by getting, authenticating and copying configuration information - Vault name, computer name, and Job name - from the original configuration, and adding it to your location so that the Restore can be accomplished there.

The steps that the Wizard takes you through, to do this are:

- Select an existing Vault Profile.
- Select the computer that has backed up the Job that you wish to import.
- Select the Job you want to Restore.

From here, the Restore proceeds like a normal Restore, as outlined in the previous section.

4 Editing Settings and Configuration

Once you have configured an Agent, you have the possibility to come back and adjust its settings to your convenience.

4.1 Agent Settings

To edit an Agent's settings,

Click the Agent in question then click on "Agent Settings" from the dropdown "Edit" menu.

Figure 27. – Edit Agent Settings

You can change your options, from tab to tab and click "Save changes" when you are done. See the Web Agent Console Help or User Guide for detailed descriptions.

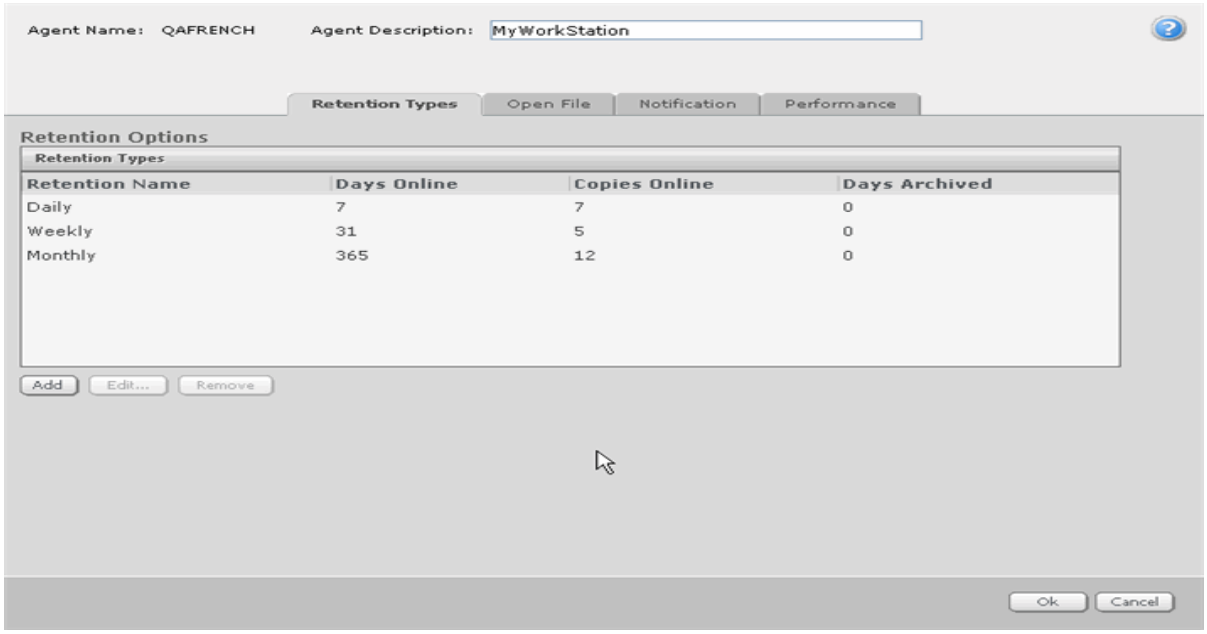


Figure 28. – Agent Settings

4.2 Vault Settings

To edit a vault's settings, click "Vault Settings" from the "Edit" drop down. With the Vault settings you can add, edit, remove a vault or reregister an Agent to a Vault.

To re-register an Agent to a Vault, from the "Vault Settings" screen, click "Reregister"

On the "Re-register" screen, enter the Vault's name; add its IP address; enter the credentials; then click "Load Computers".

From the list of computers, select the Agent you want to reregister to the vault and click "Save Changes"

Note: If you re-register an agent to a vault, you must then also synchronize any Jobs before they can be used again. If this is not done, the Job will fail, complaining that delta files are not preset. Synchronizing a Job is done via the History dialog for the Job.

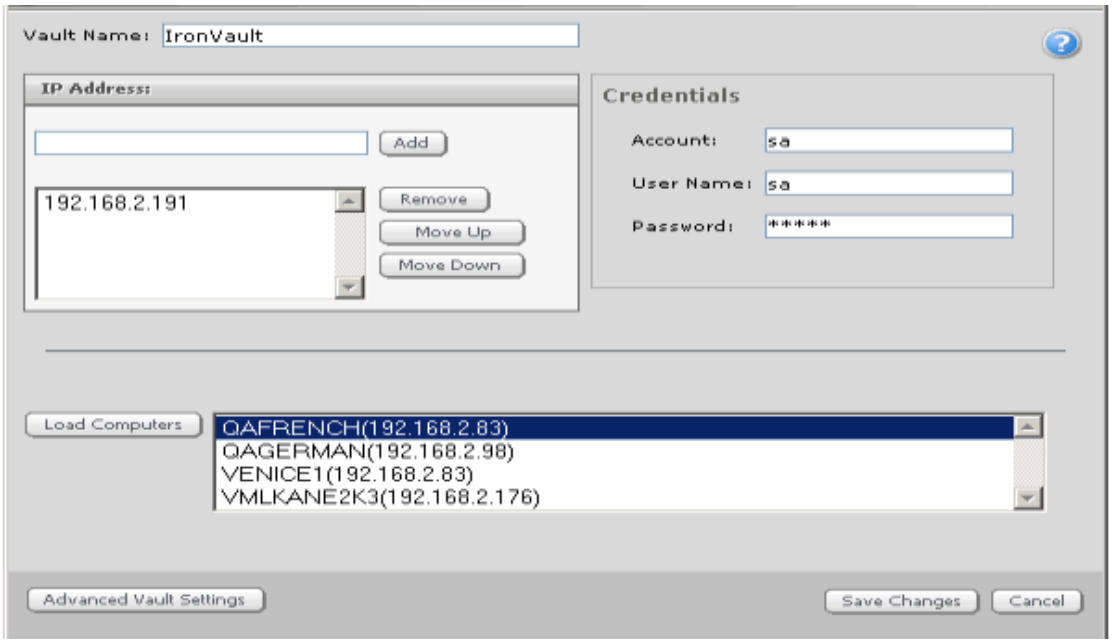


Figure 30. – Vault Settings

5 Appendix

5.1 Example Backup/Restore Scenarios

These examples are intended to allow a new User to be able to step through the major pieces of a Backup/restore process, by following an example. By using the beginning steps outlined in the chapters of this manual, and then by following the steps listed here, you should be able to complete a simple Backup and Restore. Further in-depth explanations and details about the steps can be resolved with the "Agent Console Operations Guide".

Note: These examples are provided assuming that the user is using Windows Agent Console though the steps for Web Agent Console are similar.

5.1.1 Example 1: Creating a Backup Job for Data Files

To create a Backup Job,

1. Right-click on an Agent and select **New Job** or select **New Job** from the File menu. The New Job Wizard launches.
2. Select a Backup Source Type. Select "Local Drive Only". Select Default or Unicode. Click **Next** when ready.
3. Select a Vault to Backup to. The list of Vaults should have at least one Vault Profile name in it. Click **Next** when ready.
4. Give the Job a name that is unique from all the other Backup Jobs you may have created for the computer being backed up. This name will need to be 1 to 30 characters. It is good to be descriptive rather than generic. Click **Next** when ready.
5. You should be now on the "Source" window. This window allows you to select the files you want backed up. This selection section will vary depending on the Backup Source Type.
6. Double-click the **Data Files** check box or select files and then click the **Add** button. A pop-up dialog box should appear where you can select all the files you want to Backup. For the purposes of this example you should probably pick just a few small text files.
7. Select your files/folders and click the **Include** button.
8. Repeat the previous step until your Backup file selection list is complete. Click **OK** when all your files you want backed up have been selected.
9. The pop-up dialog box should have disappeared and you should be back at the Source window. Click **Next** to continue.
10. You should be now on the Options window. This window allows you to enable/disable Quick File Scanning and to configure the amount of time to allow the Backup to complete and also to specify if you want the Backup to "defer" to the next day if it can't complete on time.
11. By default, Quick File Scanning is on. This option allows the Backup to quickly scan the System to figure out if any file has changed by reading the "header" information on each file that the System supplies. The alternative is for the Backup to read every file in the Backup completely to see if the file has changed and is a much slower

method but is 100% guaranteed to find all changes in files. For almost all situations you should leave Quick File Scanning on.

12. Disabling deferring means that the Backup time window settings will be ignored and all your selection will be backed up in one pass regardless of how long it takes. Normally it is preferable to defer a long Backup to the next time the Backup is scheduled; when this happens the Backup simply starts where it left off from the previous time.
13. The Backup Time Window indicates how long you are giving the Backup time to complete before stopping. It is normally set to 8 hours.
14. Accept all the defaults on this window and click **Next**.
15. You should be on the Encryption window. This allows you to indicate whether you want your data encrypted when it is stored on the Vault. If you do then you can select an encryption option and choose an encryption Password. **Be careful** if you do because the Vault operator will not know your Password when you want to Restore your data. Only you will know it. Note that the password is case sensitive.
16. Regardless of whether you choose to encrypt your data for storage on the Vault, during the actual transmission of the data over the network the Agent will (by default) encrypt the communications session to ensure privacy during the transfer of information. This Over The Wire encryption may be disabled in "Agent Properties", under the "Connectivity" tab. See the "Agent Console Operations Guide" for more details.
17. You should now be on the Log options window. Whenever a Backup is run, a log file of the activity is created. On this window you can select how detailed the logging information should be. The more detailed, the larger the log file and the more disk space the Backup uses. You can also select for how long the logs should be kept around. Viewing the Backup logs periodically is a good way to ensure that everything is working. After the very first Backup is run you should check the first log to make sure everything happened correctly.
18. For now use all the defaults and just click **Next.**
19. You should now be on the last window of the Wizard. This is the Finished window. Here you can select to run the Job, schedule it or just create it and do nothing else. The default should be to "just exit" and do nothing. If this is not selected then select it now.
20. Click **Finish.** At this point the application will attempt to contact the Vault that was selected in order to register this new Job. If the network is down or the Vault is otherwise unavailable or there are other unforeseen problems then an Error dialog box will pop up. Normally everything is working ok and this step completes quickly in just a few seconds.
21. This section should now be completed and the Wizard has disappeared from the screen. Your new Job should be listed in the list of Job under the Agent icon on the left hand pane of the screen. If instead you received an error message then you should contact your support staff to troubleshoot the problem.
22. You should now go to the next example "Running an Ad-Hoc Backup" to run the Backup Job that was newly created.

5.1.2 Example 2: Running an Ad Hoc Backup

An "ad hoc" Backup is usually a one-time only, unscheduled Backup, run for a special or unique reason.

1. Right-Click a Job, and choose "Backup".
2. Select a destination to Backup to: a Vault, a tape device or a disk directory.
3. There is an option to "Backup now", without further configuration, but for this exercise, click **Next**.
4. Choose a Retention scheme (used to specify how long we will keep the Backups on the Vault) – daily, weekly or monthly. There are defaults that we will use for this example: Daily is retained for seven days; Weekly is retained for a month; and Monthly is retained for a year.
5. You should be now on the Options window. This window allows you to enable/disable Quick File Scanning and to configure the amount of time to allow the Backup to complete and also to specify if you want the Backup to "defer" to the next day if it can't complete on time.
6. By default, Quick File Scanning is on. This option allows the Backup to quickly scan the System to figure out if any file has changed by reading the "header" information on each file that the System supplies. The alternative is for the Backup to read every file in the Backup completely to see if the file has changed and is a much slower method but is 100% guaranteed to find all changes in files. For almost all situations you should leave Quick File Scanning on.
7. Disabling deferring means that the Backup time window settings will be ignored and all your selection will be backed up in one pass regardless of how long it takes. Normally it is preferable to defer a long Backup to the next time the Backup is scheduled; when this happens the Backup simply starts where it left off from the previous time.
8. The Backup Time Window indicates how long you are giving the Backup time to complete before stopping. It is normally set to 8 hours. Accept all the defaults on this window and click **Next**.
9. Click **Finish** and the Backup Job starts, displaying the progress of the Backup.

5.1.3 Example 3: Scheduling a Backup Job

When you are creating a new Job, at the end of the New Job Wizard, you have the option to Run, Schedule or Exit. If you select the Schedule radio button and click **Finish** in the Job Wizard, the Schedule List panel appears.

To schedule an existing Job in the Agent Console, Right-Click the Agent, and choose Schedule Entries from the menus. The Schedule List panel appears.

1. Click the **New** button on the Schedule List panel. The schedule Wizard launches.
2. Welcome. Click **Next**.
3. Select **Backup** from the schedule command list. Click Next.
4. The Select a Backup Type window appears, but is grayed out. Click **Next**.
5. Select the Job you wish to schedule from the Job list window. Click **Next**.
6. The Retention window appears. Choose a Retention scheme (used to specify how long we will keep the Backups on the Vault) – daily, weekly or monthly. There are defaults that we will use for this exercise: Daily is retained for seven days; Weekly is retained for a month; and Monthly is retained for a year. For this exercise, choose (default) Daily, and Click **Next**.
7. You should be now on the Options window. This window allows you to enable/disable Quick File Scanning and to configure the amount of time to allow the Backup to complete and also to specify if you want the Backup to "defer" to the next day if it can't complete on time.
8. By default, Quick File Scanning is on. This option allows the Backup to quickly scan the System to figure out if any file has changed by reading the "header" information on each file that the System supplies. The alternative is for the Backup to read every file in the Backup completely to see if the file has changed and is a much slower method but is 100% guaranteed to find all changes in files. For almost all situations you should leave Quick File Scanning on.
9. Disabling deferring means that the Backup time window settings will be ignored and all your selection will be backed up in one pass regardless of how long it takes. Normally it is preferable to defer a long Backup to the next time the Backup is scheduled; when this happens the Backup simply starts where it left off from the previous time.
10. The Backup Time Window indicates how long you are giving the Backup time to complete before stopping. It is normally set to 8 hours. Accept all the defaults on this window and click **Next**.
11. Command cycle. Choose Weekly or Monthly. The screen describes how to select the schedules.
12. Click **Finish**. The Schedule List panel appears.
13. Click **OK**.

5.1.4 Example 4: Check the Backup Results

When your Backup is complete, the results appear in the log files in your Agent Console window. To confirm a successful Backup:

1. Click an Agent on the left pane of the Agent Console window.
2. Click a Job. The Safesets and Log files for the selected Job appear in the right pane of the Agent Console window.
3. Click on the Logs folder. A log report for your Backup appears in the right pane. Double click the Log file to view the details of the Backup. The bottom (last) portion of the Log file should indicate that the Backup was completed with no errors. If your Job was not completed or you encountered errors, contact your service provider.

5.1.5 Example 5: Running a Restore Job

After you have completed one or more Backups, you can execute a file Restore at any time.

1. Select the Agent Job from which you want to Restore the file(s).
2. Choose the Restore button on the Standard toolbar. This starts the Restore Wizard.
3. From the Select a Source dialog, you can view the most recent type of source device (e.g. Vault), specific source (e.g. name of Service Provider) and Safeset or Range of Safesets (e.g. number of Safeset – Safesets are numbered starting at one and in increasing order). Typically, these are what you want to restore from. However, you may change any of them as required. Click **Next**.
4. From the Encryption Options dialog, enter your encryption Password in the Password text box if your data was encrypted during Backup. Also, enter your Password in the Verify Password text box. Note that the password is case sensitive. Click **Next**.
5. From the Select Restore Objects dialog, select the file(s) you would like to include/exclude from the Restore.
6. From the Destination Options dialog, establish the location to which the files are to be restored, whether or not you want sub-directories created and if existing files should be overwritten. The defaults are to restore to an alternate location (you need to specify the location), create sub-directories and overwrite existing files.
7. From the Advanced Restore Options dialog, set any desired options. The defaults are to not restore the Local Registry/Novell Bindery/NDS (depending on the operating System), to restore all data and security streams, to create a log file, and to use all available bandwidth. You may change any or all of the defaults.
8. Click **Finish**.

Check the Restore log to see if the Restore was successful.

5.1.6 Example 6: Cross Computer Restore

Normally when a Job is created to do a Backup, the client uses a unique configuration file. You must create a Profile for the Server which you want to Restore from, with the same authentication information as the original computer used for Backup. You may want to use this method for a disaster recovery plan, as well as for normal data migration.

There are limitations on which operating Systems can successfully transfer data in this way. For example, different versions of the same O/S, such as NetWare6.0 and 6.5 are okay. O/S's that are part of the same family, or share similar origins, such as Linux and Solaris are also okay.

What the "restore from another computer" option (via a Wizard) does is allows the User to redirect the (original) Restore Job to a different client (location). It re-registers where the configuration file was originally pointing, so that the Restore Job can be redirected to another location. It does this by getting, authenticating and copying configuration information - Vault name, computer name, and Job name - from the original configuration, and adding it to your location so that the Restore can be accomplished there.

Steps in the Restore

1. Ensure that the data is fully available for Restore (i.e. updated) on the Vault. This means that the Backup is current, and will properly Restore all needed data.
2. Logon to the System that you will Restore the data to. This is the different System than the one that did (created) the Backup.
3. Create a Vault Profile for the Vault on which the data is stored. Use the authentication information that was used for the original Backups.
4. From the Tools menu select "Restore from another computer", from the Vault Profile dialog select the Vault Profile that was created above. Click **Next.**
5. On the Registered Computers dialog select the computer that originally stored the data being restored. Click **Next.**
6. On the Job dialog select the Job that protects the data to be retrieved. Click **Next.**
7. On the Import Job you are told that all information required has been collected to accomplish the Restore. Click **Next.**
8. This process downloads catalogs for all available Safesets for this Job.
9. This process, when complete, spawns the Restore Wizard starting with the Select a Source dialog.

The Restore now continues like a Restore from the original computer.

Note that now you will have a "new" Job in your list of Jobs, which came from the other Agent. It only performs Restores and does not allow Backups.

5.1.7 Example 7: Bare-metal Disaster Recovery

5.1.7.1 Bare-metal Disaster Recovery Best Practices

Below is an outline of the rules and practices required to make a bare-metal restore successful on the latest versions of NetWare. Several of these rules include steps that should be performed long before the NetWare server crashes and you need to restore it. Please familiarize yourself with these rules and make sure you implement them as soon as possible.

For this discussion, the 'old server' represents a NetWare server that needs to be reinstalled from scratch and the 'new server' represents the replacement server.

1. Never restore NDS in a multi-server tree. To restore a server in a multi-server tree, first delete information about the old server from the tree and then install the new server in the tree as specified by Novell in their documentation Novell Knowledgebase: (http://support.novell.com/search/kb_index.jsp), then install the Agent for NetWare to it and restore files only.

2. Backup the new server before restoring data to it. At least the DOS drive where NWSERVER directory resides (usually C:) and SYS: must be backed up. In addition, if this is a standalone server (not belonging to a multi-server tree), make sure you backup all NDS objects.

3. Install exactly the same software to the new server as was installed on the old. This includes exactly the same NetWare version, the same standard products, the same support packs and post-service pack fixes. If possible, use the same installation media. Do not install more products than were installed on the new server because they will not be updated during the restore. Do not install less products because some of them may generate information during installation that is stored neither in NDS nor in a publicly accessible file system, like the certificate server and its public/private key pairs. In particular, make sure that you select the same configuration when installing NWASPI/NWTAPE and configuring the new server as SLP agent.

4. Do not restore Security Objects when restoring NDS (this option is turned off by default). Security Objects are tied to the NetWare server public/private keys that are generated each time the server is installed. This means, in particular, that no manually generated certificates will be restored. You will need to recreate them after the restore.

5. Make sure you do not overwrite SYS:\PUBLIC\RootCert.der of the new server during the restore. Other files that you should not overwrite include SYS:\SYSTEM\NICI and SYS:\SYSTEM\CSLIB. We cannot provide a full list of files that are tied to the NetWare server public/private keys and hence should not be restored to a different (read: new) server, please consult the documentation provided with them or contact their vendors. This is true for standard products distributed with NetWare as well. If you accidentally overwrote files on the new server that were tied to the new server public/private keys, please use the previously created backup (rule 2) to restore them.

6. The new server should have exactly the same name as the old, the same server ID number, the same addresses bound to the same NICs (IP, IPX etc), the same primary and secondary IP addresses, the same host and domain names and the same admin name with the same password. NDS must be backed up with this name and password on the old server before the bare-metal restore (standalone servers only).

7. The new server must have the same locations for objects and containers in the tree, including admin object, server container, and iManage container (you will be prompted for them during NetWare installation).

8. The new server should be installed using the same NetWare licenses as the old. The licenses should not be time-bombed (including SEL licenses).

9. The new server should have the same hardware as the old, including slots the hardware is installed into. If the slots are different, you may need to edit STARTUP.NCF and/or AUTOEXEC.NCF or restore them from the previously created backup (rule 2).

10. Unload as many application as possible on the new server before performing bare-metal restore. Use either the UNLOAD command or comment them out from AUTOEXEC.NCF and restart the server (as any open files will not be updated during bare-metal restore, with potentially fatal consequences). In particular, this includes the X Window System and any Java applications. To unload Java, perform the following commands: UNLOAD JAVA and UNLOAD JVM.

11. Server settings (like SET VM GARBAGE COLLECTOR PERIOD and so on) will not be restored. Currently, the best way to set them persistently across bare-metal restores is to specify them explicitly in AUTOEXEC.NCF and STARTUP.NCF on the old server.

Notes on NetWare Restores: On NetWare 6.x and above most settings are persistent, i.e. you don't have to specify them in STARTUP.NCF or AUTOEXEC.NCF, the operating system takes care of restoring them after the server reboots. However, our agent for NetWare does not restore them during a bare metal restore. These settings are stored in several files in C:\NWSERVER, and although the files are restored, the server refuses restoring the settings from them. This may be caused by incorrect file times.

It may be important to adjust the settings for specific hardware, like directory entry numbers, packet sizes and so on. Resetting them to default values may leave the server in a not usable state.

Currently, the Agent software does not support this. Actual server settings are stored not in C:\NWSERVER but in SYS:_NETWARE. This is a special directory that is virtually inaccessible at all from programs other than the OS itself. It stores physical NDS databases and other highly sensitive information and is not supposed to be accessed directly.

As a workaround, servers that may be "bare-metal-restored" later should have their settings specified explicitly, either directly in STARTUP.NCF and/or AUTOEXEC.NCF, or in an NCF file which is called from AUTOEXEC.NCF.

5.1.7.2 Bare-metal Disaster Recovery Procedure

This section outlines the steps required to recover from a worst-case disaster whereby you have lost your entire Server System (i.e., hardware, operating System and data files). These steps will walk you through the Agent Console so as to get your new Server System up and running back to normal. **Please refer to the Best Practices above for detailed explanations and planning before a restore is required.**

The steps below may refer to the new System as a replacement System. Also, the old System may be referred to as the original System.

1. Reconfigure hardware that is similar (at least a minimal configuration) to the original hardware.
2. Create a logical drive that matches the original configuration. Although hardware does not always need to be identical, be aware that some drivers that are listed in the Backup set may be incompatible with hardware on the new Systems, and may require you to manually remove or install drivers in Safe mode.
3. You may optionally want to test your System state Restore on some other test hardware (different from your replacement hardware) before you actually perform the System state Restore on the replacement System.
4. Reinstall the same version of the operating System (as was installed previously) as a stand-alone Server to the same drives and paths to which the operating System was previously installed.
5. When re-installing the operating System, you must use the same Server names as those used on the original System.
6. When re-installing the operating System, you must install all relevant support packs/patches as those used on the original System.
7. Reinstall the Agent to the same installation directory as that used on the original System.
8. Reinstall Agent Console to the same installation directory as that used on the original System.
9. When a Job was first created, it was registered with the Vault, which still "remembers" the Registration, so you cannot register it again as if it was new, you must "re-register" it to tell the Vault that it is back. In Agent Console, under Agent Configuration -> New -> Vault Registration, choose "Re-register previously registered computer". Complete the rest of the registration as before.
10. Next, to do a Restore for recovering your full drive Backup (i.e. the Backup that includes your System state Backup as well as all of your other data) select the Agent Job from which you want to Restore the file(s).
11. Choose the Restore button on the Standard toolbar. This starts the Restore Wizard.
12. From the Select a Source dialog, you can view the most recent type of source device (e.g. Vault), specific source (e.g. name of the Service Provider) and Safeset (e.g. number of Safeset – Safesets are numbered starting at one and in increasing order). Typically, these are what you want to Restore from. However, you may change any of them as required. Click **Next**.

13. From the Encryption Options dialog, enter your encryption Password in the Password text box if your data was encrypted during Backup. Also, enter your Password in the Verify Password text box. Note that the password is case sensitive. Click **Next**.
14. From the Select Restore Objects dialog, select the file(s) (typically all the files, System and data) you would like to include/exclude from the Restore.
15. From the Destination Options dialog, establish the location to which the files are to be restored, whether or not you want sub-directories created and if existing files should be overwritten. The defaults are to Restore to an alternate location (you need to specify the location), create sub-directories and overwrite existing files.
16. From the Advanced Restore Options dialog, set any desired options. The defaults are to not restore locked files, to not restore the Local Registry/Novell Bindery/NDS (depending on the operating System) and to restore all data and security streams. You may change any or all of the defaults.
17. Click **Finish**. Check the Restore log to see if the Restore was successful.

A successful Restore should have your new System restored back to its state at the time the last Backup was performed.

6 Index