

GroupWise Disaster Recovery

Version 5.1.1

November 2017

Legal Notices

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.novell.com/company/legal/>.

Copyright © 2017 Micro Focus Software, Inc. All Rights Reserved.

Contents

Preface	7
1 GroupWise Disaster Recovery version 5.1	9
Overview	9
Micro Focus GWAVA Family of Message Handling Products	10
Technical Support	11
Sales	11
Copyright Notice	11
2 System Requirements	13
GroupWise Versions	13
Supported OS versions	13
Memory	13
CPU	13
Disk	14
3 System Design	17
GroupWise Disaster Recovery	17
GroupWise on Linux	17
Collector/Server Model	18
Server Only	18
Restore Options	18
GroupWise on Windows	19
Server Only Model	19
Restore Options	19
4 Installation	21
Install GroupWise Disaster Recovery	22
License GroupWise Disaster Recovery	22
Upgrading GroupWise Disaster Recovery	24
Web Console	24
GroupWise Disaster Recovery Administration	25
Command Line	26
Automatic Upgrades	27
Upgrading the Collector	27
Uninstall GroupWise Disaster Recovery	27
Reinstall GroupWise Disaster Recovery	28
5 Configuration	29
Post-Install Tasks	29
Set the GroupWise version in GroupWise Disaster Recovery Administration	29
Configure Maintenance Purge	32
Configure Notifications	32
GroupWise on Linux	35
Collector/Paired Server Profiles	35
Prerequisites	37

Configure Profiles	37
Troubleshooting Collector Connectivity Issues	37
Collector Model Domain Profiles	38
Paired Collector/Paired Server Model	38
Prerequisites	38
Configure Profiles	38
Switching from Server model to Collector Model	52
Collector Model Post Office Profiles	53
Paired Collector/Server Model	53
Prerequisites	54
Configure Profiles	54
Switching from Server model to Collector Model	68
Server Only Profiles	70
Server Only Model	70
Creating Profiles On Linux GroupWise Systems	70
Configure Profiles	70
Creating Server Only Model Domain Profiles	71
Domain Profile: Server Only Model	71
Creating Server Only Post Office Profiles	81
Post Office Profile: Server Only Model	81
GroupWise Cluster	91
Installing GroupWise Disaster Recovery in a GroupWise Cluster	91
Installation Collector/Server Model	91
Upgrading Collectors in a Cluster	95
Configure Restore Area on Linux	95
On the GroupWise Disaster Recovery Server, enable NFS Server	95
On the Linux GroupWise Server	97
In GroupWise Administration	98
Confirmation	100
On the GroupWise Disaster Recovery server, load a backup for the profile	100
On a workstation with a GroupWise client	100
GroupWise on Windows	102
Server Only Profiles on Windows	102
Prerequisites	102
On the GroupWise Disaster Recovery Server: Create backup data directory	102
Configure Profiles	107
Creating Domain Profiles with GroupWise on Windows	107
Domain Profile: Server Only Model	108
Creating Post Office Profiles with GroupWise on Windows	115
Post Office Profile: Server Only Model	115
Configure Restore Area on Windows	123
On the GroupWise Disaster Recovery Server	123
Confirmation	130
On the GroupWise Disaster Recovery server, load a backup for the profile	130
On a workstation with a GroupWise client	130
Troubleshooting	132
Backup Jobs	132
Domain Backup Jobs	132
Post Office Backup Jobs	136
Post-Backup Tasks	140
Configure Auto-GroupWise Disaster Recovery	140
Configure Tape Backups	141
Configure Number of Backups to Keep	143
Disaster Recovery Configuration	144
Configure Disaster Recovery	145
Testing Disaster Recovery	151
Create Disaster Recovery GWIA	152
Retain Integration	153

Prerequisites	153
GroupWise Disaster Recovery Setup	153
Retain Setup	154
6 Restoration	155
Restoring Items Overview	155
Prerequisites	155
Loading a Backup	155
Restore Mail Items	156
Restore Mode	156
Access Mode	158
Restore a User's Address Book	163
Access Mode	163
Restore a User's Calendar Items	166
Access Mode	166
Restore Documents to Document Management	169
Access Mode	169
Restore Deleted User	170
Prerequisites	171
Download wdomain.db from GroupWise Disaster Recovery	171
Restore the User	173
Restore All Items	174
Restore From a Tape Backup	175
On the GroupWise Disaster Recovery Server	176
Post Restore Tasks	177
7 Disaster Recover Mode	179
Activating Disaster Recovery mode	179
Post Disaster Migration	179
8 Logs	181
GroupWise Disaster Recovery Web Console	181
Command line	181
Details	181
9 Blueprint	183
Blueprint for GroupWise Disaster Recovery version 1.6 Overview	183
Intended Audience	184
Installation	184
Installation	184
Licensing	186
Upgrading Blueprint	187
Configuration	187
General Settings	187
Summary Report Settings	188
Users Report Settings	188
Resources Report Settings	189
Advanced Settings	189
Administration	192
Starting a Blueprint Report Job	193
Summary Report	194
Users Report	195
Blueprint Command Line Options	196

Preface

GroupWise Disaster Recovery powered by Reload.

About This Guide

This GroupWise Disaster Recovery Installation and User Guide helps you integrate this software into your existing GroupWise system.

Audience

This manual is intended for IT administrators in their use of GroupWise Disaster Recovery or anyone wanting to learn more about GroupWise Disaster Recovery. It includes installation instructions and feature descriptions.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comment feature at the bottom of each page of the online documentation.

Additional Documentation

Online documentation can be found on the [GWAVA \(http://support.gwava.com/documentation/Reveal/index.html\)](http://support.gwava.com/documentation/Reveal/index.html) website and the [Micro Focus \(https://www.microfocus.com/products/\)](https://www.microfocus.com/products/) website.

Knowledge Base articles can be found on the [GWAVA Support \(http://support.gwava.com/\)](http://support.gwava.com/) website and the [Micro Focus Knowledge Base \(https://www.microfocus.com/support-and-services/knowledge-base/\)](https://www.microfocus.com/support-and-services/knowledge-base/) website.

1

Chapter Title GroupWise Disaster Recovery version 5.1 / Title

Sect1 Title Overview / Title

Para GroupWise Disaster Recovery is a disaster recovery, hot backup, and quick restore system for Novell GroupWise. GroupWise Disaster Recovery integrates with GroupWise post offices and domains on NetWare, Linux and Windows to provide reliable backups. All the mail in those backups can then be examined using any Novell GroupWise client. GroupWise Disaster Recovery backs up post offices and domains from GroupWise 8 or greater. / Para

Para GroupWise Disaster Recovery is a Disaster and Recovery solution for GroupWise mail systems that provides live backups and recovery for GroupWise post offices and domains. In the event of a disaster where the post office or domain is unusable or lost, GroupWise Disaster Recovery can provide a temporary post office and domain for the GroupWise system to run off of, making messages flow seamlessly, even in a crisis. / Para

Para GroupWise Disaster Recovery performs this function by creating backup copies of the post office and domain databases, which it then can load with GroupWise agents. GroupWise Disaster Recovery also can load post office agents against any post office backup, allowing users to transparently restore deleted or lost mail to the live post office, directly from the user's GroupWise client. With GroupWise Disaster Recovery, losing mail in a system is no longer a crisis, and in most cases, not even an inconvenience. / Para

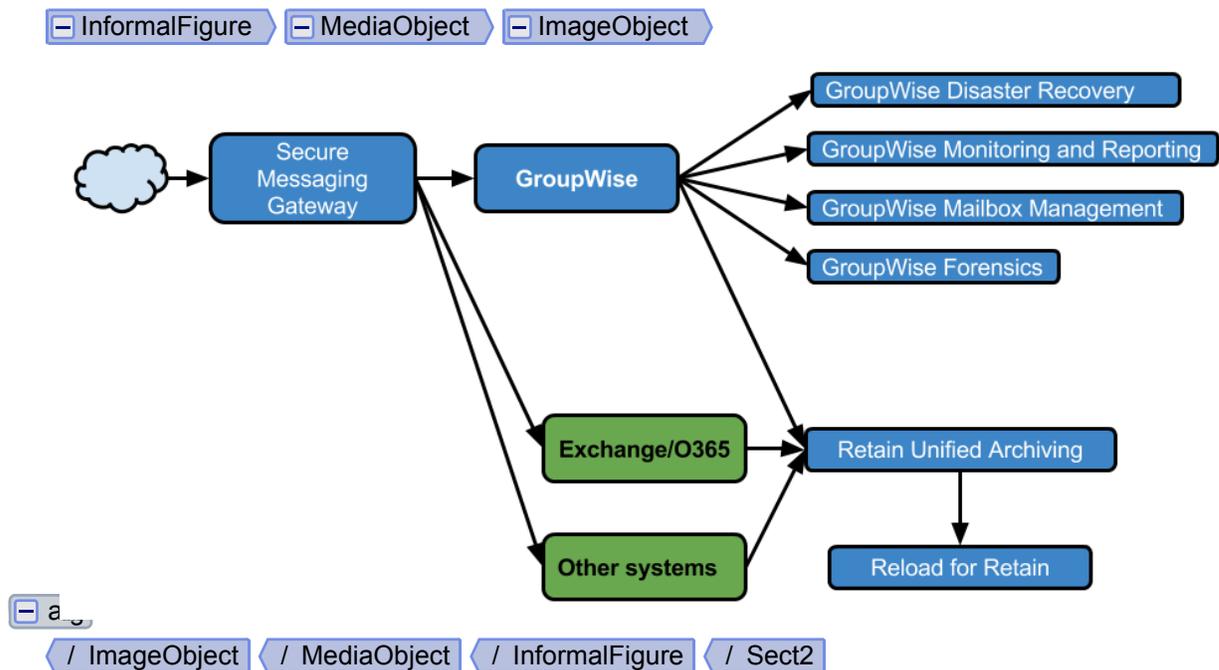
Para Multiple GroupWise Disaster Recovery servers can also be tied together to add multiple redundant layers of protection for complete offsite backups of the GroupWise message system. / Para

Para GroupWise Disaster Recovery only runs on the Linux platform and requires that one setting in GroupWise Administration be enabled, as well as on the host machine for both the GroupWise system and the GroupWise Disaster Recovery Server. GroupWise Disaster Recovery does not require eDirectory, Active Directory or any TSA components. / Para

Para Setting-up GroupWise Disaster Recovery can seem to be an intimidating process, but this guide will walk you through the process. There also is online documentation, an extensive knowledgebase, full support, and consulting services available to aid you in customizing and perfecting your GroupWise Disaster Recovery system. / Para

[- Sect2 [- Title **Micro Focus GWAVA Family of Message Handling Products** / Title

- ◆ [- ItemizedList [- ListItem [- Para [- Emphasis *Secure Messaging Gateway* / Emphasis is a message scanning product that protects your system from malware and spam. / Para / ListItem
- ◆ [- ListItem [- Para [- Emphasis *Retain Unified Archiving* / Emphasis is an archive storage product that is designed to keep messages from GroupWise, Exchange/O365, GMail, BlackBerry, Bloomberg, Notes, mobile, social and other messaging platforms for the long term to meet data retention legal requirements and has powerful search capabilities for eDiscovery. / Para / ListItem
- ◆ [- ListItem [- Para [- Emphasis *GroupWise Disaster Recovery powered by Reload for GroupWise* / Emphasis is a hot-backup and disaster recovery product for GroupWise. It keeps a few weeks of data and can easily restore messages, calendar items, address books, and even whole users. It can also act as a fully functional Post Office in times when the GroupWise POA is down. / Para / ListItem
- ◆ [- ListItem [- Para [- Emphasis *Reload for Retain* / Emphasis is a hot-backup product for Retain. The Retain archive keeps items for the long term and often becomes the only repository of an item. Without a backup you can leave yourself open to legal liability if the items are lost before the retention period has passed. Reload for Retain provides high speed backups of your Retain archive. / Para / ListItem
- ◆ [- ListItem [- Para [- Emphasis *GroupWise Reporting & Monitoring powered by Redline* / Emphasis is a comprehensive, customizable, monitoring and reporting tool for GroupWise. / Para / ListItem
- ◆ [- ListItem [- Para [- Emphasis *GroupWise Forensics powered by Reveal* / Emphasis provides essential auditing and oversight capabilities that legal, human resources, and auditing personnel need within GroupWise. / Para / ListItem
- ◆ [- ListItem [- Para [- Emphasis *GroupWise Mailbox Management powered by Vertigo* / Emphasis is the Enterprise Mailbox Management tool for GroupWise. / Para / ListItem / ItemizedList



Technical Support

If you have a technical support question, please consult the Micro Focus Technical Support at <http://support.gwava.com> (<http://support.gwava.com>)

Sales

Micro Focus contact information and office locations: www.microfocus.com (<http://www.microfocus.com>)

To contact a Micro Focus sales team member, please e-mail info@gwava.com (<mailto:info@gwava.com>) or call 866-GO-GWAVA ((866) 464-9282), or +1 (514) 639-4850 in North America.

Copyright Notice

The content of this manual is for informational use only and may change without notice. Micro Focus assumes no responsibility or liability for any errors or inaccuracies that may appear in this documentation.

© 2017 GWAVA Inc., a Micro Focus company. All rights reserved.

Micro Focus, Retain, the Retain logo, GWAVA, and GroupWise, among others, are trademarks or registered trademarks of Micro Focus or its subsidiaries or affiliated companies in the United Kingdom, United States and other countries. All other marks are the property of their respective owners.

2 System Requirements

GroupWise Disaster Recovery is a backup system and will use significant amounts of disk space.

GroupWise Versions

- ♦ GroupWise 2014 R2
- ♦ GroupWise 2014
- ♦ GroupWise 2012
- ♦ GroupWise 8.0.3

Supported OS versions

The GroupWise Disaster Recovery server must be run on the Linux platform, but it backs up GroupWise post offices on NetWare, Linux or Windows platforms.

- ♦ SUSE Linux Enterprise Server 12 (SLES12) 64-Bit.
- ♦ SUSE Linux Enterprise Server 11 (SLES11) 32-Bit or 64-Bit.

Memory

2 gigabytes of available RAM should be sufficient for most environments. More memory is helpful.

CPU

Type

The GroupWise Disaster Recovery server only supports the Intel Platform x-86 Platform

Speed

The faster the better; SMP is not to be considered a requirement, however, testing of GroupWise Disaster Recovery on SMP has shown that GroupWise Disaster Recovery is benefited by SMP.

Disk

Disk space must be carefully considered for each GroupWise Disaster Recovery Server. When the GroupWise Disaster Recovery server reaches the error threshold for disk space, it will no longer create backups. Make sure the target system has plenty of space to accommodate the needs of your GroupWise Disaster Recovery backups.

GroupWise Disaster Recovery backs up GroupWise post offices and domains according to profiles that the administrator specifies, which tells GroupWise Disaster Recovery what to backup, where it is located, and where to store the data. The Profile can also keep track of disk space and when to expire the backups it creates. After the initial backup, each successive backup takes an average of 12% the full size of the live post office, also saving network and disk resources.

Disk speed directly impacts GroupWise Disaster Recovery performance. A disk that is tuned for fast writes to disk is highly recommended and will improve performance. When considering disk space requirements, also take into account future growth of GroupWise post offices, and the space that will be required to sustain that growth.

If GroupWise Disaster Recovery runs out of hard disk space, backups will no longer be created. A GroupWise Disaster Recovery profile has a threshold of days to keep in hot backups. This can help prevent systems from running out of disk space.

Server Only Backup Method

This backup method in with the GroupWise Disaster Recovery Server gets a client connection via a Linux mount point to the post office or domain to be backed up. GroupWise Disaster Recovery would then copy data from the live server to the GroupWise Disaster Recovery server via the mount point it had established to the live server housing GroupWise. Prior to GroupWise Disaster Recovery 5, this was the only method of performing backups. In this scenario, the GroupWise Disaster Recovery Server should be in close network proximity to the GroupWise servers that are being backed up with GroupWise Disaster Recovery. If a GroupWise Disaster Recovery Server and some GroupWise post offices are on a Gigabit switch, it would be best to have a network card in the GroupWise Disaster Recovery server that supports a Gigabit speed.

Paired Collector/Server Model

This backup method is new to GroupWise Disaster Recovery 5. A “Collector” runs on the server that houses a GroupWise post office or domain. The Collector then uses Rsync as the transport to get data from the GroupWise server to the GroupWise Disaster Recovery Server. This model requires the following disk space on the GroupWise server:

Post Office

2 times the size of the post office OFUSER, OFMSG and GWDMS directories. But not including the OFUSER/INDEX directory.

So for example, if the OFUSER directory contents was 1.5 GB and the OFMSG directory was 2.5 GB and the GWDMS directory was 1 GB the total space needed to service the Collector would be $1.5+2.5+1 = 5 \times 2 = 10$ GB needed somewhere on the GroupWise server to sustain the GroupWise Disaster Recovery Collector.

Disk Space on The GroupWise Disaster Recovery Server

The disk space may reside on the GroupWise Disaster Recovery server or on a SAN. The requirements of the disk solution are as follows:

- ♦ The disk solution should always be mounted for use with GroupWise Disaster Recovery.
- ♦ The disk solution should be formatted with a Linux based file system, specifically a file system that supports symbolic links.
- ♦ If the disk is not a SAN, but a NAS solution for example, the mount should be an NFS mount. No other protocol other than NFS.

Calculating Disk Space

The rule of thumb is 2.5 times the post office size per profile.

The GroupWise Disaster Recovery server requires the following disk space per profile:

- ♦ Initial backup: 100% of the size of the post office.
- ♦ Then 14 days of backups (on average) will be retained: 150% of the size of the post office.
- ♦ Remember to take Post Office growth and the host Operating system into account while calculating disk space needs.

For example: A 100 gigabyte post office, for example, would require approximately 250 GB of disk space to retain 14 days worth of backups.

3 System Design

How you implement your GroupWise Disaster Recovery system depends on what your GroupWise is hosted on.

GroupWise Disaster Recovery is a backup system and recovery system. It is built around the idea that 2 is 1 and 1 is none, in other words. if you have two copies of your data then if something happens you still have one copy available.

GroupWise Disaster Recovery can be configured save a backup of your production system, send a copy to an off-site server and to a cloud host to maximize data safety.

GroupWise Disaster Recovery

GroupWise Disaster Recovery backs up your domain and post offices so you can restore items and users. There is also a disaster recovery mode that allows you to use the GroupWise Disaster Recovery server as a POA if a POA goes down.

On the GroupWise Disaster Recovery server you need to create a profile for each domain and post office.

On the GroupWise server you need to set up a restore area.

You should expect to allocate 150% of the space your current GroupWise Post Office is taking up on the GroupWise Disaster Recovery server to accommodate 14 days worth of backups.

The databases and other files are copied to the GroupWise Disaster Recovery server into `~/<profile>/backup/weeknow/<day>`

The BLOB (Binary Large Object) files are copied to the GroupWise Disaster Recovery server into `~/<profile>/blobs`

GroupWise on Linux

If GroupWise is on Linux, there are two models for backing up the data:

- ♦ Collector/Server
- ♦ Server Only

Collector/Server Model

The collector model is built for speed. Backups that take too long to create are not very useful.

The collector agent sits on the GroupWise server, uses DBCopy to make a local copy of the post office databases, then sends the databases, BLOBs and other files to one or more GroupWise Disaster Recovery servers with rsync. This is fast and has minimal impact on the server.

Server Only

The server model uses DBCopy across NFS to copy the production POA across the network to the GroupWise Disaster Recovery server. This is slow and requires a lock on the database for the duration of the transfer.

Restore Options

Restore Mode Restore

With GroupWise on Linux, you have the option to restore emails using the GroupWise Restore Area, which allows users to restore items themselves just by going to File | Open Backup, if the item is in the latest backup. This sets up the links in `~/<profile>/connect/restore` for GroupWise to use.

Access Mode Restore

When a backup is loaded a POA is activated. The client can connect to the GroupWise Disaster Recovery Access Mode POA. Items can be saved to a local archive and unarchived to the production GroupWise server.

Restore all items for a user from GroupWise Disaster Recovery via GroupWise Administration

With a Restore Area in place, you can restore all items for a user from GroupWise Administration.

Restore all items for all users from GroupWise Disaster Recovery, via a bash script

With Disaster Recovery setup, you can use a bash script to restore all items back to the production GroupWise Post Office.

GroupWise on Windows

Server Only Model

If GroupWise is on Windows, you may only use the Server model for backing up the data.

Restore Options

Restore Mode Restore

With GroupWise on Linux, you have the option to restore emails using the GroupWise Restore Area, which allows users to restore items themselves just by going to File | Open Backup, if the item is in the latest backup.

Access Mode Restore

When a backup is loaded a POA is activated. The client can connect to the GroupWise Disaster Recovery Access Mode POA. Items can be saved to a local archive and unarchived to the production GroupWise server.

4 Installation

Installation performs the following tasks:

1. Installs the GroupWise Disaster Recovery System software to the path: /opt/beginfinite/reload.
2. Creates initialization scripts to start the GroupWise Disaster Recovery Daemon on server bootup.
3. Creates various GroupWise Disaster Recovery initialization scripts such as "reload, reload, reloadm, and reloadj" in the /usr/sbin directory, so that they are available to the Linux administrator "root".
4. Sets up a default GroupWise Disaster Recovery System configuration.
5. Starts the GroupWise Disaster Recovery Daemon.
6. If needed, the installation also installs the GroupWise DBCOPY and GroupWise Agent packages, unless these packages have been installed before, or if the installation determines that other GroupWise agent software is already installed.
7. If the GroupWise Disaster Recovery server has a connection to the Internet and can browse the web, then the GroupWise Disaster Recovery server will attempt to install a piece of software called Xdialog. The Xdialog is used to view GroupWise Disaster Recovery log files in a graphical user interface. It cannot be bundled with GroupWise Disaster Recovery, because of licensing issues, so GroupWise Disaster Recovery downloads it to the GroupWise Disaster Recovery server if the server has a connection to the Internet. Xdialog is not required.
8. Installs a GroupWise Disaster Recovery Administration icon to the root user's Xwindows desktop. If you are in an XWindows type session, you should see an icon on the root user's desktop. This icon is compatible with a basic GNOME or KDE installation. The icon is for convenience, and may not work in all Linux desktop environments.

Prerequisites

GroupWise 2014 or 2014 R2: To successfully integrate with GroupWise 2014 or 2014 R2, GroupWise server needs to be installed on the GroupWise Disaster Recovery server for necessary utilities to be installed. It is necessary to install openmotif for GroupWise.

1. Open YaST, then Software Management and install motif.
2. Install GroupWise 2014 server RPM.

Install GroupWise Disaster Recovery

Download GroupWise Disaster Recovery <http://download.gwava.com/download.php?product=Reload&version=rpm> or

```
wget "http://download.gwava.com/download.php?product=Reload&version=current"
```

Unzip the archive

```
unzip reload5.zip
```

If installing under SLES 12, install rpm-32bit from YaST.

Install GroupWise Disaster Recovery by running the following command in the same directory the download is in:

```
rpm -ivh reload5.rpm
```

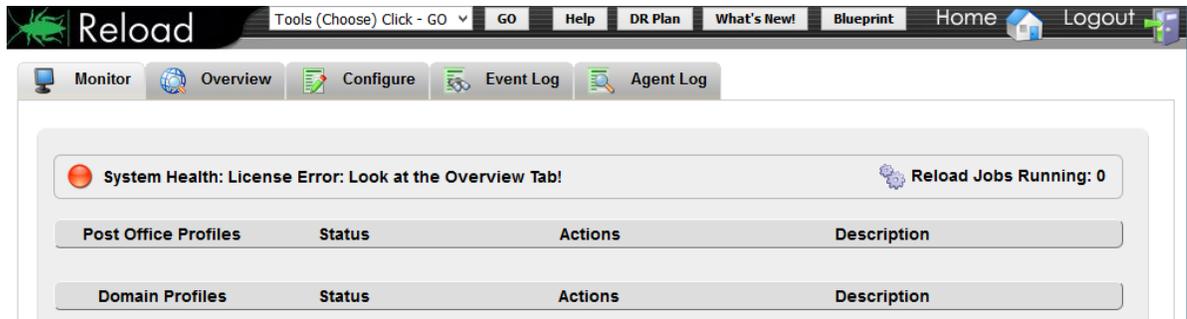
```
reload172:~ # rpm -ivh reload5.rpm
Preparing...                               ##### [100%]
 1:beginfinite-reload                       ### ( 10%)
```

License GroupWise Disaster Recovery

License GroupWise Disaster Recovery by browsing to the <https://licenses.gwava.com/> Licensing Website, entering your validation keys and downloading the PEM file.

Browse to the GroupWise Disaster Recovery Web Administration console

http://<GroupWise Disaster Recovery_Server_Address>:5555



On the Toolbar, select Tools | License



Browse to the license PEM file

 [CLICK HERE TO OBTAIN A LICENSE FILE, IF YOU DO NOT HAVE ONE YET](#)

 [Click Here to License Blueprint for Reload](#)

To submit the Reload license file do the following:

- 1. Select the "Browse" button, to select the license file called: *.pem
- 2. Select the "Submit License File" button

The Reload Daemon will then implement the new license and restart the browser session

reload.pem

Submit the license file by clicking the *Submit License File* button.

Wait for GroupWise Disaster Recovery to consume the license.



The license file was uploaded successfully. Please wait for 45 seconds while the daemon consumes the new license file, and restarts.

When 45 seconds has passed, this page will be redirected to the Home page.

You will be required to re-authenticate if authentication is enabled.

Upgrading GroupWise Disaster Recovery

Web Console

To upgrade GroupWise Disaster Recovery from the Web Console, choose upgrade from the Tools dropdown menu, press Go.



Select Upgrade Now



[Automated Software Download and Automated Upgrade](#)

NOTE: This automated upgrade feature does require that the Reload server have HTTP (Port 80) access to the Internet. If the Reload server does not have HTTP access to the Internet because of a proxy or some other reason, then open the "Manual Software Download and Automated Upgrade" panel below.

By selecting the "Upgrade Now" link, a request is made for the Reload Daemon to check to see if there is a newer version of Reload. If there is a newer version, the Reload Daemon will upgrade the Reload software package automatically.

To determine if Reload should be upgraded to a newer release, follow these steps:



The currently installed version of Reload is: [Reload 5.1 Build \(510125\)](#)



1. Check the [GWAVA Reload Support Forum Patches Section](#) to see if a newer version is available



2. To upgrade Reload select:  [Upgrade Now](#) which will install the latest version of Reload



[Manual Software Download and Automated Upgrade](#)



[Advanced Upgrade Options](#)

GroupWise Disaster Recovery Administration

To upgrade GroupWise Disaster Recovery from the Retain Administration, run:

```
reload
```

GWAVA Reload Main Menu

Daemon Status: **Running** - Profiles Status: **Good**

Choose using [UP] [DOWN], [Enter] to Select

Access	Access Backups
Recovery	Disaster Recovery
WARNING	Read Warning
Profiles	Administer Profiles
Jobs	Start/Stop Backup Jobs
Logs	View System Logs
Create	Create New Profiles
System	Administer System
Monitor	Profile Monitor
Overview	Program Information
DOCS	Documentation

< **OK** > < **Exit** > < **Help** >

Choose *System* | *Tools* | *Upgrade* | *Upgrade*

Upgrade Menu

Choose Using [UP] [DOWN], [Enter] to Select

Upgrade	Upgrade Reload Software Package
View	View Rolling Upgrade Log
Static	View Static Upgrade Log
Advanced	Advanced Upgrade Options

< **OK** > < **Back** > < **Main Menu** >

Progress will be shown onscreen.

Command Line

To upgrade GroupWise Disaster Recovery from the command line, run:

```
reloadu
```

`reloadu -r` will force a download of the available version even if you previously downloaded it.

`reloadu -h` shows a help page

If the GroupWise Disaster Recovery server does not have access to the internet then the update can be downloaded from <http://download.gwava.com/download.php?product=Reload&version=current>

Copy the file to the GroupWise Disaster Recovery Server and place in

```
/opt/beginfinite/reload/upgrade
```

At a command prompt, type:

```
reloadu
```

Automatic Upgrades

To have GroupWise Disaster Recovery automatically upgrade itself, create a cron job:

```
crontab -e
```

and enter

```
00 1 * * 3 root /usr/sbin/reloadu
```

Upgrading the Collector

If you are using the Collector/Server Model, the collector will upgrade itself from the server when the next job begins:

When the GroupWise Disaster Recovery server is upgraded it dumps the upgrade rpm in:

```
/reload/[POprofile]/gre_data/sync/gre_data/proc/upgrade
```

When a backup job runs the collector uses rsync to check for an rpm upgrade file. If it does it transfers the rpm to:

```
/opt/beginfinite/reload/upgrade
```

If successful the collector upgrades itself, then corrupts the rpm on the GroupWise Disaster Recovery server so it can't upgrade again. The GroupWise Disaster Recovery server will check the rpm for corruption and if it is, deletes the corrupt rpm since the upgrade has been completed.

Uninstall GroupWise Disaster Recovery

This only removes the GroupWise Disaster Recovery Software Package. The configuration data, profiles and profile backups are left in their storage directories. The data can be removed manually.

To uninstall the GroupWise Disaster Recovery Software Package, run:

```
/opt/beginfinite/reload/uninstall
```

Reinstall GroupWise Disaster Recovery

To reinstall GroupWise Disaster Recovery Software Package, run:

```
reloadu
```

5 Configuration

Post-Install Tasks

There are a few post-install tasks that need to be taken care of once GroupWise Disaster Recovery has been installed.

1. Setting the GroupWise version in GroupWise Disaster Recovery so GroupWise Disaster Recovery uses the correct GroupWise software
2. Enable Maintenance Purge in GroupWise so messages are not deleted from disk before GroupWise Disaster Recovery is able to backup all messages
3. Configure Notifications of system status
4. Configure GroupWise Disaster Recovery Backup Profiles for each GroupWise Domain and Post Office
5. Configure the Restore Area between GroupWise Disaster Recovery and GroupWise so items can be easily restored
6. Configure Auto-GroupWise Disaster Recovery so the most recent backup is always available
7. Configure Tape Backup for long term storage

Set the GroupWise version in GroupWise Disaster Recovery Administration

To run most effectively GroupWise Disaster Recovery should use the version of GroupWise software that the GroupWise server is using

Select GroupWise Version

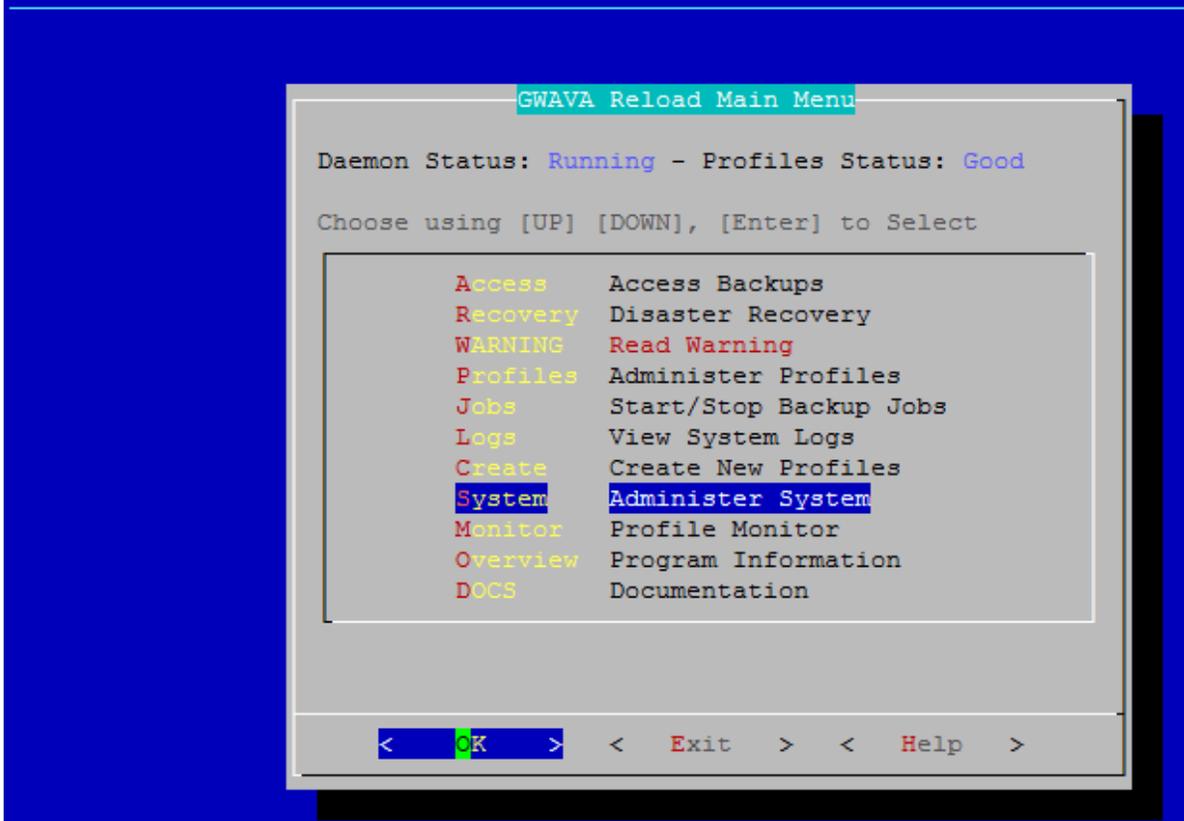
Go to GroupWise Disaster Recovery Administration by running:

```
reload
```

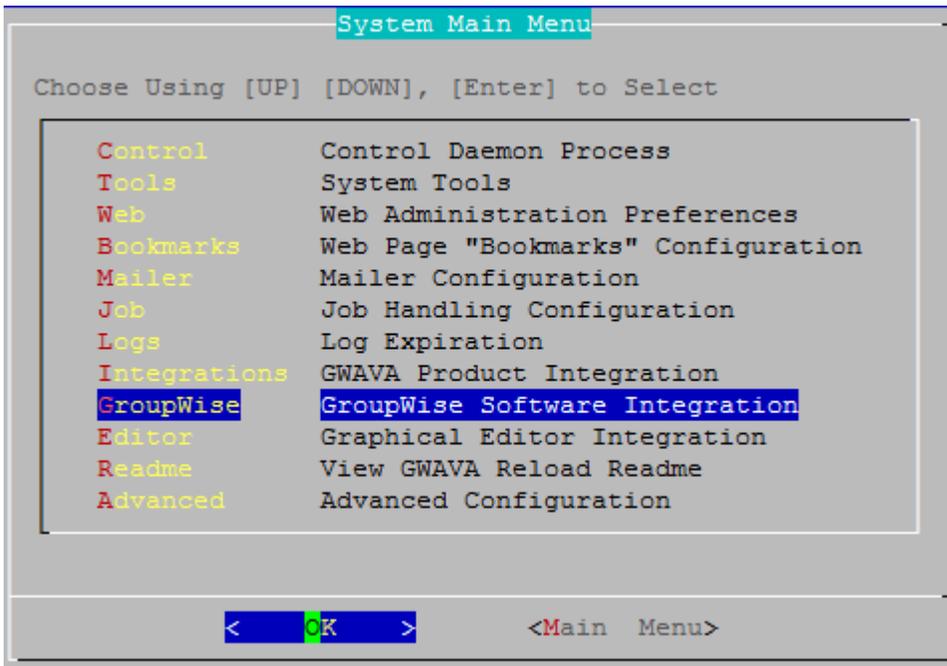
The first time it is run you will be shown the readme page.

Then go to *System | GroupWise | Version* and press Space to select the appropriate version of GroupWise.

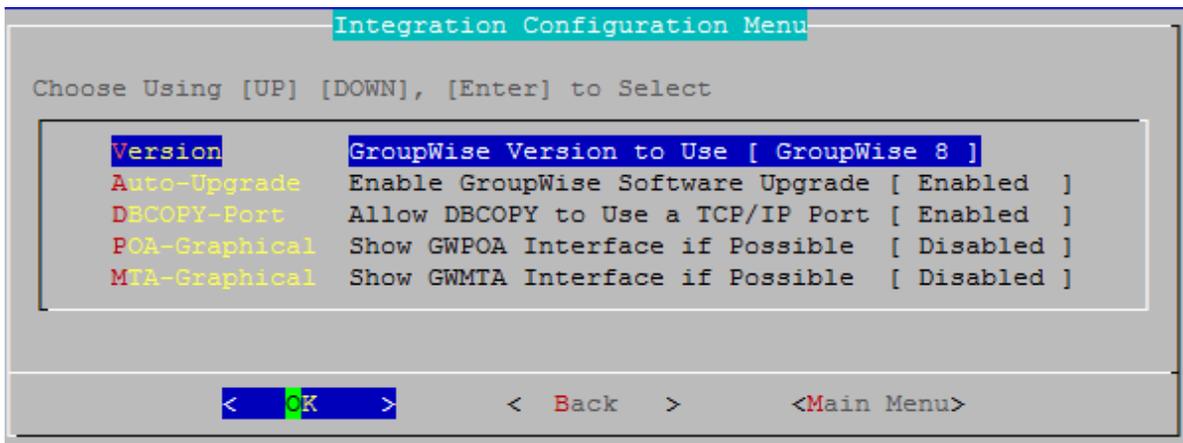
Select System: Administer System



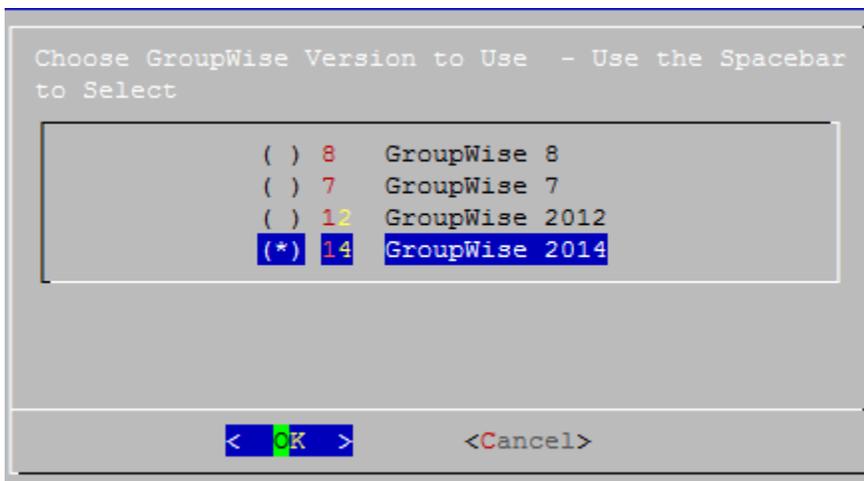
Select GroupWise: GroupWise Software Integration



Select Version: GroupWise Version to Use



Press Space to select your GroupWise version



Manually installing the GroupWise software

Should that fail the GroupWise software can be added manually:

Determine what, if any, GroupWise software is already loaded. Get a list of installed GroupWise software by running:

```
rpm -qa | grep groupwise
```

This will return a list of GroupWise components already installed or just return to the command line if nothing is installed. For example, novell-groupwise-dbcopy and novell-groupwise-agents

Uninstall existing software by running:

```
rpm -e <software>
```

To uninstall GroupWise 8 and 2012:

```
rpm -e novell-groupwise-dbcopy
```

```
rpm -e novell-groupwise-agents
```

To uninstall GroupWise 2014:

```
rpm -e novell-groupwise-server
```

Install the GroupWise software:

For GroupWise 8 and 2012, DBCopy and the agent software must be installed from the GroupWise installation software package. DBCopy is found in the "admin" directory and the agent software is found in the "agents" directory.

For example, GroupWise 2012:

```
rpm -ivh novell-groupwise-agents-12.0.2-108211.i586
```

```
rpm -ivh novell-groupwise-dbcopy-12.0.2-108211.i586
```

For GroupWise 2014 and 2014R2, install the server software found in the "server" directory.

```
./install_server.sh
```

NOTE: Once the GroupWise software is installed, GroupWise Disaster Recovery and Blueprint can immediately use the version of software that you install. The version of GroupWise will eventually be reported correctly in the GroupWise Disaster Recovery Web Administration and GroupWise Disaster Recovery Console menu. It can take up to an hour because GroupWise Disaster Recovery only checks the version of the GroupWise software that is installed every hour.

Configure Maintenance Purge

This is optional but without it, you will only get a snapshot and not a complete backup.

To prevent items from being deleted from GroupWise before they are backed up, it is recommended to enable Message Retention Services across the Domain.

1. Go into *GroupWise Administration | Domain | <specific system> | Client Options | Environment | Cleanup | Maintenance*
2. Enable "*Do not purge items until they are backed up*"

Configure Notifications

GroupWise Disaster Recovery will send notifications about Daily Status, Errors, Warnings, Job Completion and Audit events.

Configure Reports & Notifications

1. Browse to the GroupWise Disaster Recovery Web Administration Console
2. Select the Configure tab
3. Open the "*Reports & Notifications*" section

Reload Tools (Choose) Click - GO GO Help DR Plan W

Monitor Overview Configure Event Log Agent Log

Reports & Notifications

DAILY STATUS REPORT

! Reload Can Send a Daily Consolidated Status Report of All Reload Profiles

▶ Send the Status Report Message Now

● Send a Daily Consolidated Status Report E-mail:

● Send a Backup of All Configuration Files Daily:

● Include Reload System Event Log: **Disabled**

● Daily Status Report FROM Address:

● Daily Status Report TO Recipient:

● Send Status Report to a CC Recipient: **Disabled**

● Daily Status Report CC Recipient:

4. Configure each section:
 - a. Enable each type of notification you wish to receive
 - b. Enable each section with a Notification TO Recipient

Confirmation

To see if this worked, press the Send button for each section and check your mailbox.

TIP: You can change the From address for each section. You may want to consider using different From addresses and filtering the status messages to go to a folder while errors and warnings go to your inbox to make managing your inbox easier.

Troubleshooting Notifications

If you are unable to receive messages from GroupWise Disaster Recovery you can check the Agent log for errors. GroupWise Disaster Recovery uses postfix to send mail. Searching for postfix in the log may help you find out what is happening.

A common issue is that the GroupWise Disaster Recovery server cannot find the SMTP relay host. You can set this manually.

1. Browse to the GroupWise Disaster Recovery Web Administration Console
2. Select the Configure tab
3. Open the "*GroupWise Disaster Recovery Mailer Preferences, Help & Troubleshooting*" section
4. Set the "*SMTP Relay Host*" to your mail server, and save

The screenshot shows the Reload web interface. At the top, there is a navigation bar with the Reload logo and a search bar containing "Tools (Choose) Click - GO". To the right of the search bar are buttons for "GO", "Help", "DR Plan", and "What's I". Below the navigation bar is a menu with five items: "Monitor", "Overview", "Configure", "Event Log", and "Agent Log". The main content area is divided into four sections, each with an icon and a link:

- Reports & Notifications** (Icon: folder with red arrow)
- Web Administration & System Preferences** (Icon: server rack)
- Job Handling Preferences** (Icon: gear with checkmark)
- Reload Mailer Preferences, Help & Troubleshooting** (Icon: envelope with checkmark)

The "Reload Mailer Preferences, Help & Troubleshooting" section contains several items:

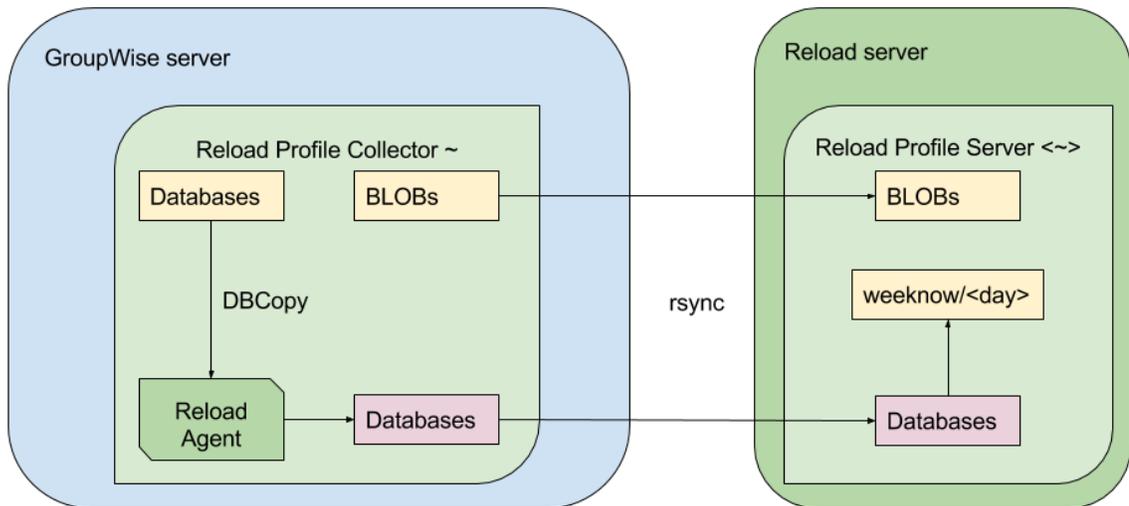
- Reload Can Send E-mailed Reports and Notifications** (Info icon)
- SMTP Relay Host:**
- Help Understanding What the Reload Mailer Settings Do**
- Reload and Postfix Mailer Troubleshooting and Customization**
- Reload Can Embed the Reload Server URL in All Mail Messages Sent by Reload** (Info icon)
- Embed Reload Server URL in All Mail Messages** **Disabled**
- Reload Server URL:**

5. Send another test message.

GroupWise on Linux

Collector/Paired Server Profiles

The Collector model creates a software agent called a collector that handles transferring the data to the GroupWise Disaster Recovery server.

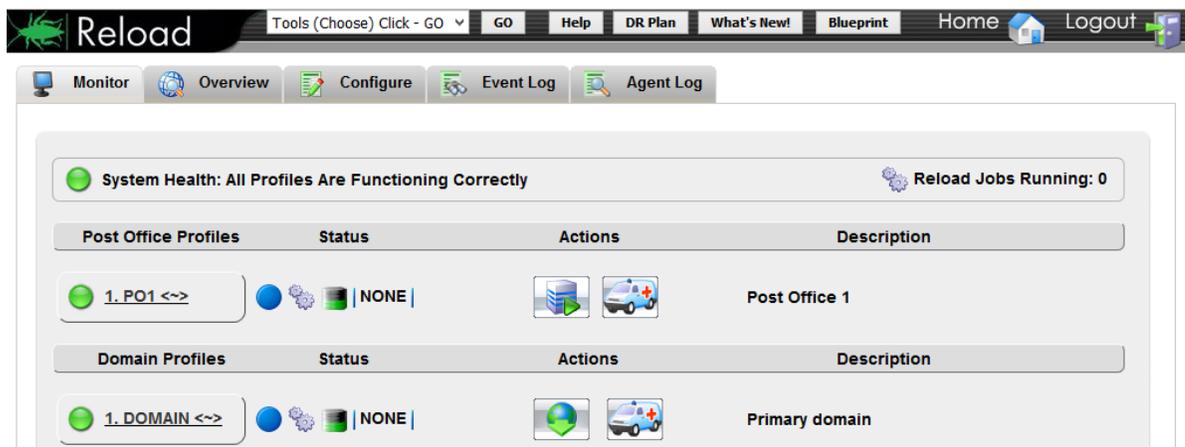


It is faster than the Server Only model and can send the data to up to three different GroupWise Disaster Recovery server.

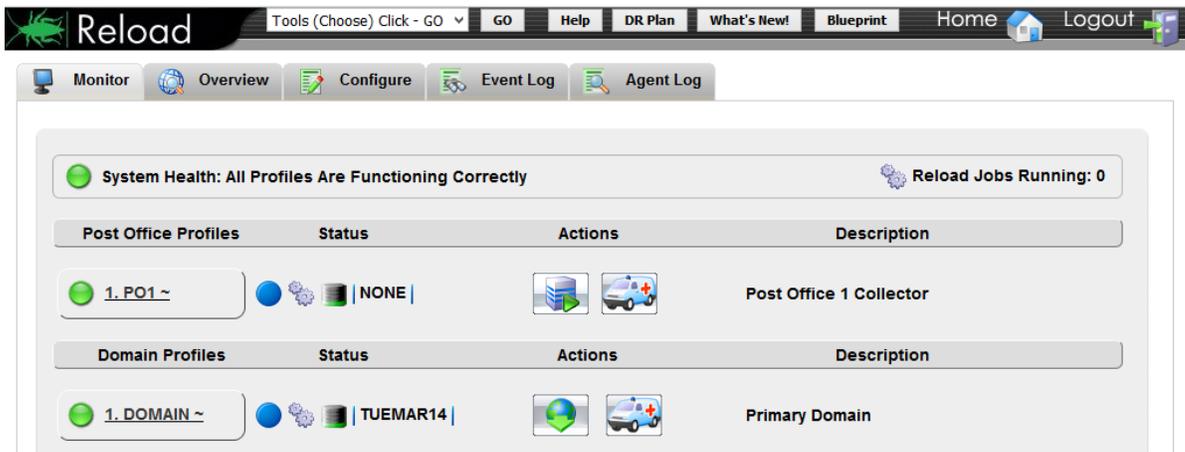
The BLOB files are copied to the GroupWise Disaster Recovery server via rsync.

Because database files need to be locked during copy operations the GroupWise Disaster Recovery agent will use DBCopy to make a copy of the databases locally on the GroupWise server to minimize the impact of the copy, then transfer the databases to a temporary directory on the GroupWise Disaster Recovery server. Once successfully transferred to the GroupWise Disaster Recovery server the databases are moved to the appropriate backup directory.

You first set up a receiving server profile (marked with a <~>) on the *GroupWise Disaster Recovery server*.



Then setup a sending collector profile (marked with a ~) on the *GroupWise server*.



Prerequisites

You will need to create a directory on the GroupWise Disaster Recovery and the GroupWise server for the backup data. The name of the profile will be used to create sub-directories for each profile. For example:

```
/reload/
```

You will need to know the directories on the GroupWise server for the live data. For example:

```
/groupwise/domain
```

```
/groupwise/pol
```

Configure Profiles

There are two kinds of Collector/Server Model profiles: [Domain \(Collector_Model_Domain_Profiles.htm\)](#) and [Post Office \(Collector_Model_Post_Office_Profiles.htm\)](#).

Troubleshooting Collector Connectivity Issues

That are occasionally issues with the Collector connecting properly to the GroupWise Disaster Recovery server during profile testing and an error like this appears:

```
The authenticity of host <ip address> can't be established. ECDSA key fingerprint is <numeric value> [MD5]
```

Are you sure you want to continue connecting (yes/no)?

On the server with the GroupWise Disaster Recovery Collector:

1. Go to the directory:

```
/root/.ssh
```

2. Delete all files in the directory
3. In the terminal, enter the command

```
ssh-keygen -t rsa
```

4. Take the default values or enter your own, if desired

5. Exchange the ssh keys with the GroupWise Disaster Recovery server by entering the command:

```
ssh-copy-id -i /root/.ssh/id_rsa.pub <address of Paired GroupWise Disaster Recovery Server>
```


For example, `ssh-copy-id -i /root/.ssh/id_rsa.pub 10.1.1.123`
6. Return to the GroupWise Disaster Recovery Console and retest the Profile

Collector Model Domain Profiles

Paired Collector/Paired Server Model

The Collector model creates a software agent called a collector that handles transferring the data to the GroupWise Disaster Recovery server.

You first set up a receiving server profile (marked with a <~>) on the GroupWise Disaster Recovery server, then a sending collector profile (marked with a ~) on the GroupWise server.

It is faster than the Server Only model and can send the data to up to three different GroupWise Disaster Recovery server, but requires copying parts of the domain or post office to another directory before sending the data so it has a snapshot of the data.

Prerequisites

You will need to create a directory on the GroupWise Disaster Recovery and the GroupWise server for the backup data. The name of the profile will be used to create sub-directories for each profile. For example:

```
/reload/
```

You will need to know the directories on the GroupWise server for the live data. For example:

```
/groupwise/domain
```

```
/groupwise/po1
```

Configure Profiles

Domain Profile: Collector/Paired Server Model

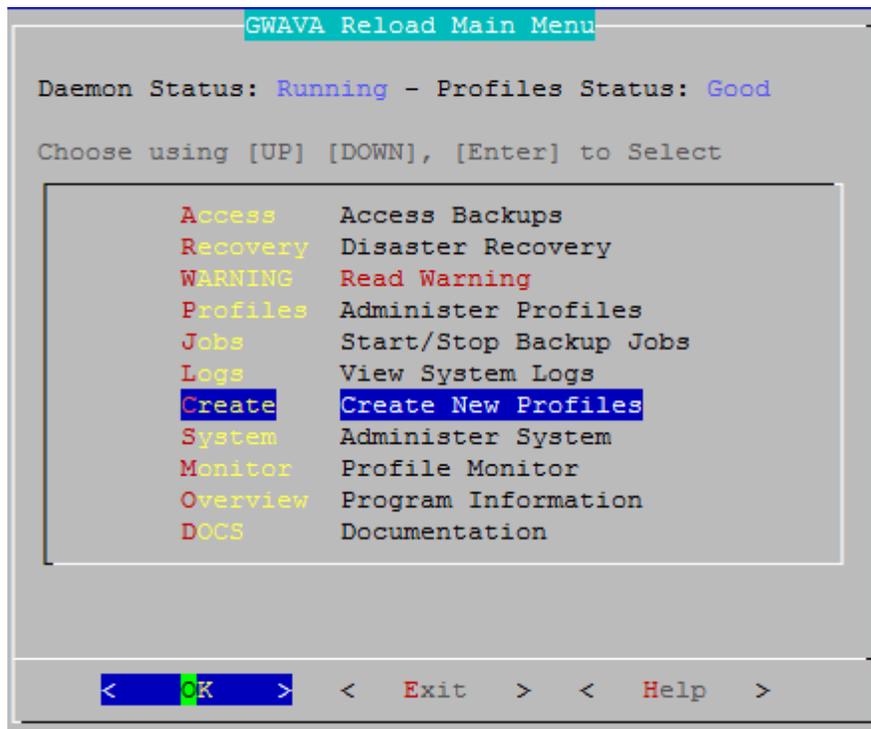
Create a Paired Server to receive the data sent by the Collector:

On the GroupWise Disaster Recovery Server, create the Paired Server:

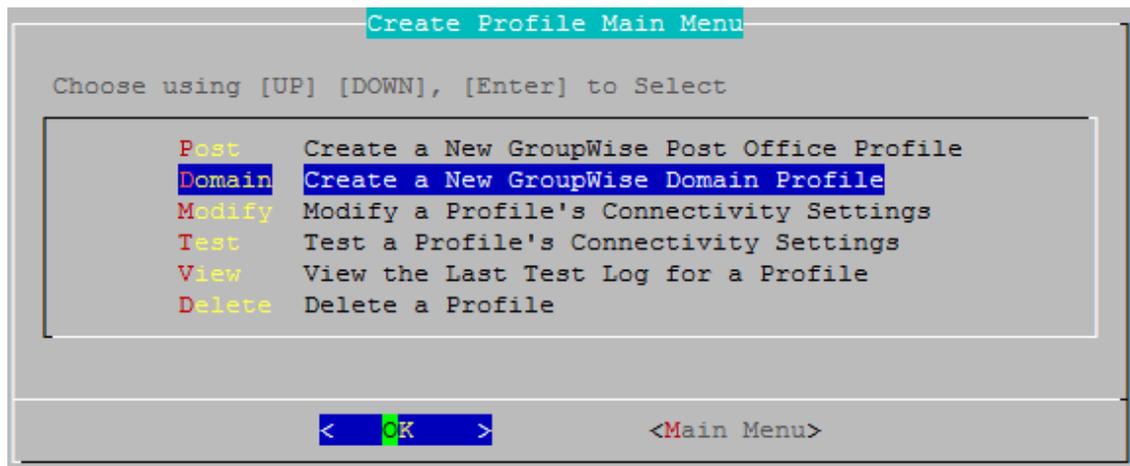
1. Create a directory for the backup data. For example:

```
mkdir /reload
```
2. Start the GroupWise Disaster Recovery Administration Console by typing on the command line:

```
reload
```
3. Select "Create (Create Profile)"



4. Select "Domain (Create a New GroupWise Domain Profile)"



5. Give the Profile a Name. The profile name should not exceed eight characters. Use letters and numbers only, no spaces or other characters. For example: Domain Be aware, that a profile cannot be renamed, once it has been created. Choose the name wisely. Perhaps you will want to name the profile so that its name is the same as the GroupWise post office or domain that the profile represents. Select the Next button.

Profile Name

Choose < Next > to Accept

Use letters and numbers only, no spaces or other characters!

The profile name SHOULD NOT EXCEED 8 characters.

Enter the name of the profile in the field below:

< Next > < Cancel >

6. Give the Profile a Description. The profile description should not exceed 60 characters and should not have comma(,), nor dollar sign(\$) characters. For example: Primary Domain. The description of the profile will be added to the Agent Log when backup jobs are run for the profile. Select the Next button.

Profile Description

Choose < OK > to Accept

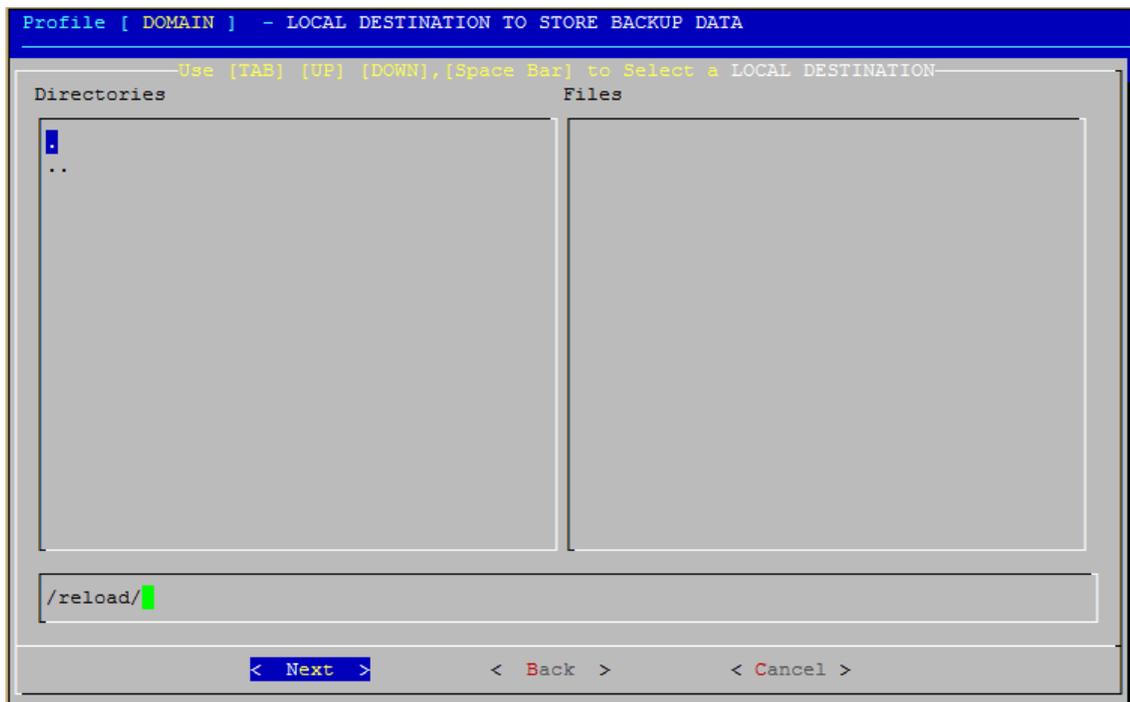
The profile description should not exceed 60 characters.

NOTE: Do not use a comma or dollar sign (, \$) character.

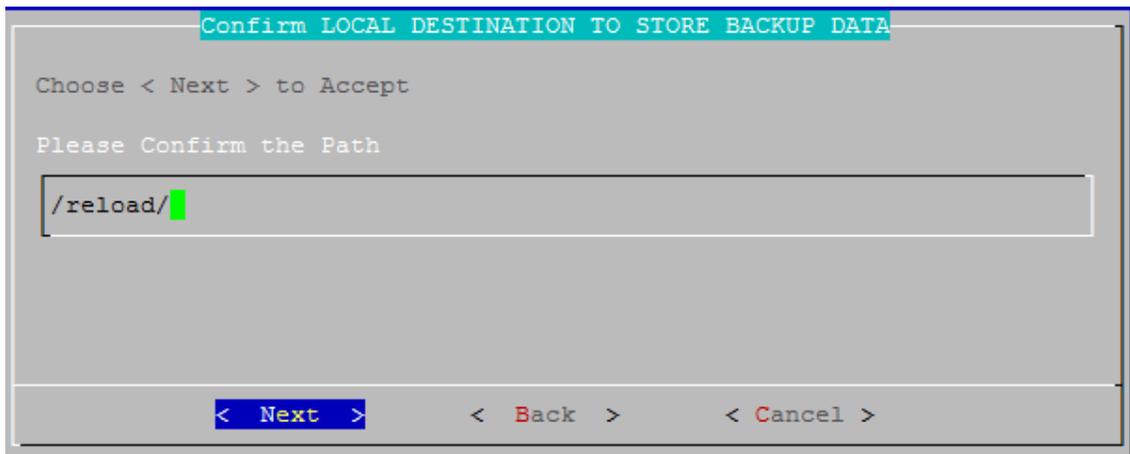
Enter the profile description in the field below:

< OK > < Cancel >

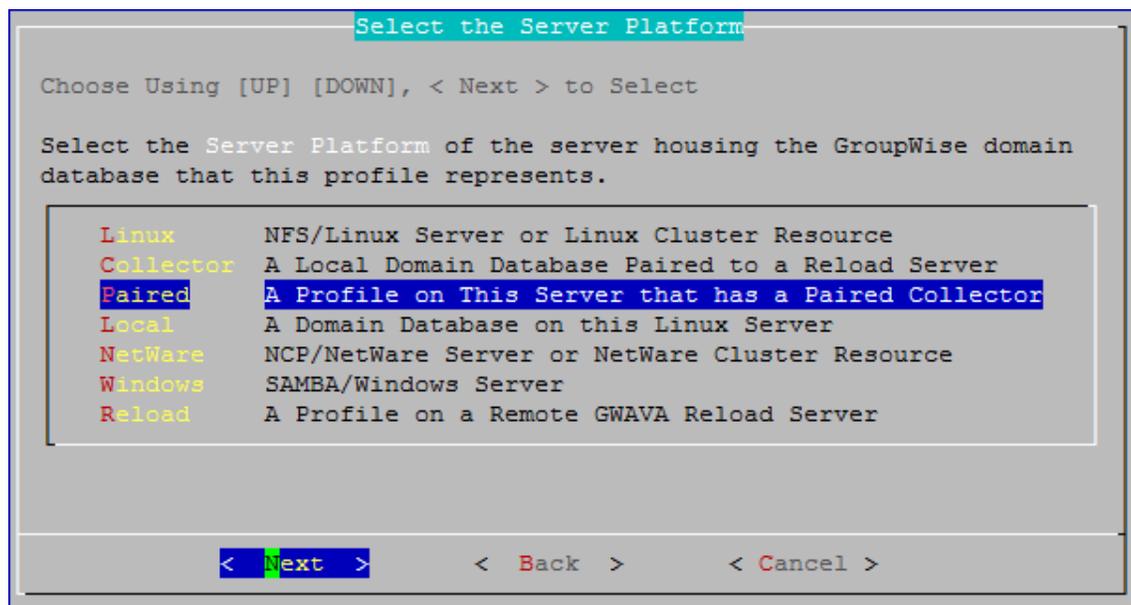
7. Backup Path: Enter the path or browse to the local destination directory to store the backup data. For example: /reload. This path can be a location on the Linux server, or an NFS mount to another Linux/Unix server, or to a SAN. Do not use a NAS as it doesn't allow the right kind of access. The path should always be available; GroupWise Disaster Recovery is not configured to mount paths in order to access stored data. Also, the path should be to a location that has a lot of disk space available. Select the Next button.



8. Confirm the path to the local destination directory

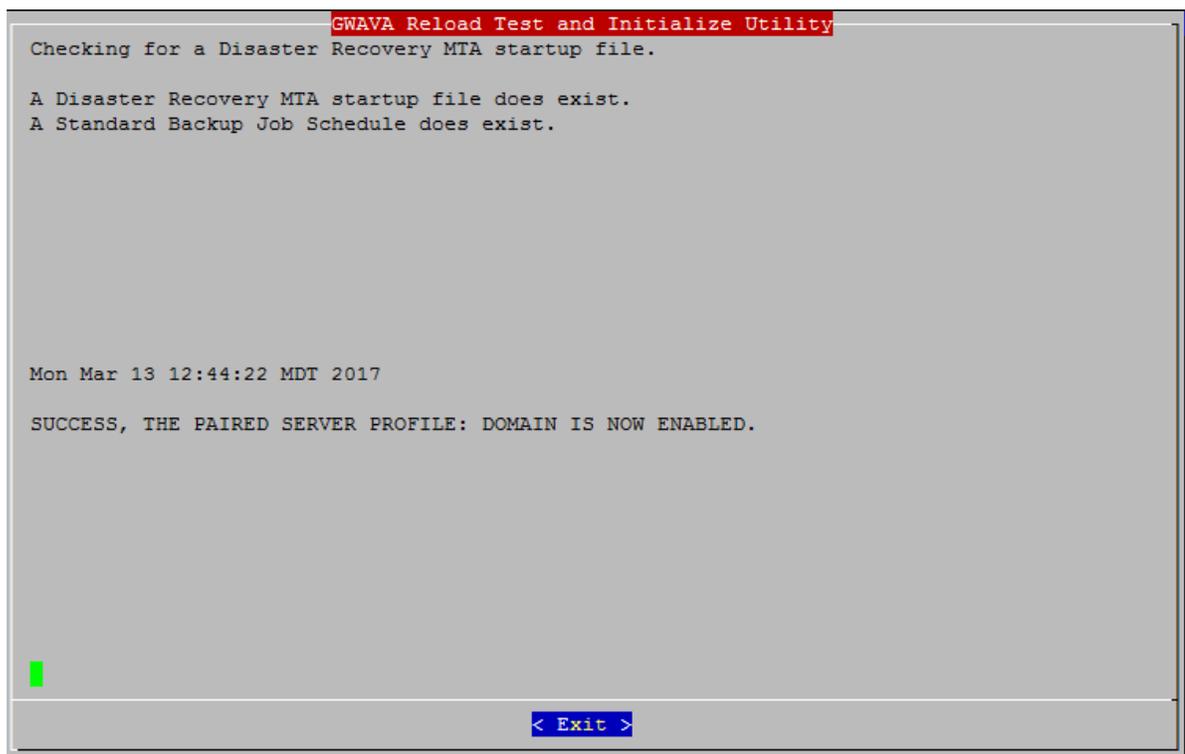


9. Choose the server type: "Paired (A Profile on This Server that has a Paired Collector)". Select the Next button.



10. The profile creation wizard tests and initializes the newly created profile and prepares it to accept a pairing request from a Paired Collector, and initializes the newly created profile and prepares it to accept a pairing request from a Paired Collector.

Testing and initializing a profile does not backup the post office or domain in any way.



Once a profile is tested and initialized successfully, the profile is available to be configured further. The default configuration of a profile is sufficient for making quickly accessible backups with GroupWise Disaster Recovery. Further configuration of the profile should be done in GroupWise Disaster Recovery Web Administration.

To be able to backup the data, a collector needs to be created on the GroupWise server.

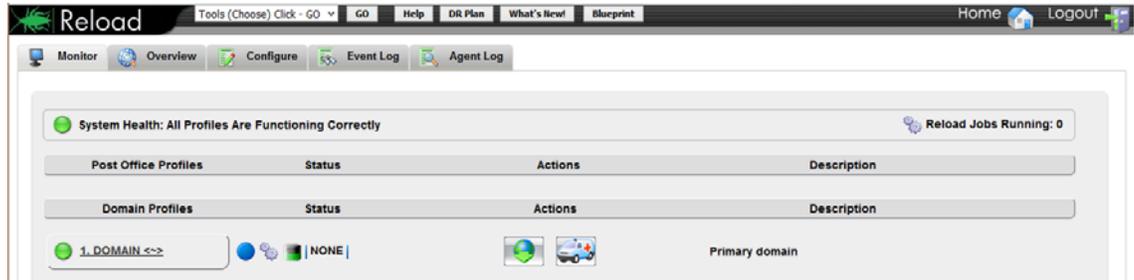
On the GroupWise Server, create the Collector:

- ♦ On the GroupWise server, the collector will need to be downloaded, installed and configured to connect to the GroupWise Disaster Recovery server.

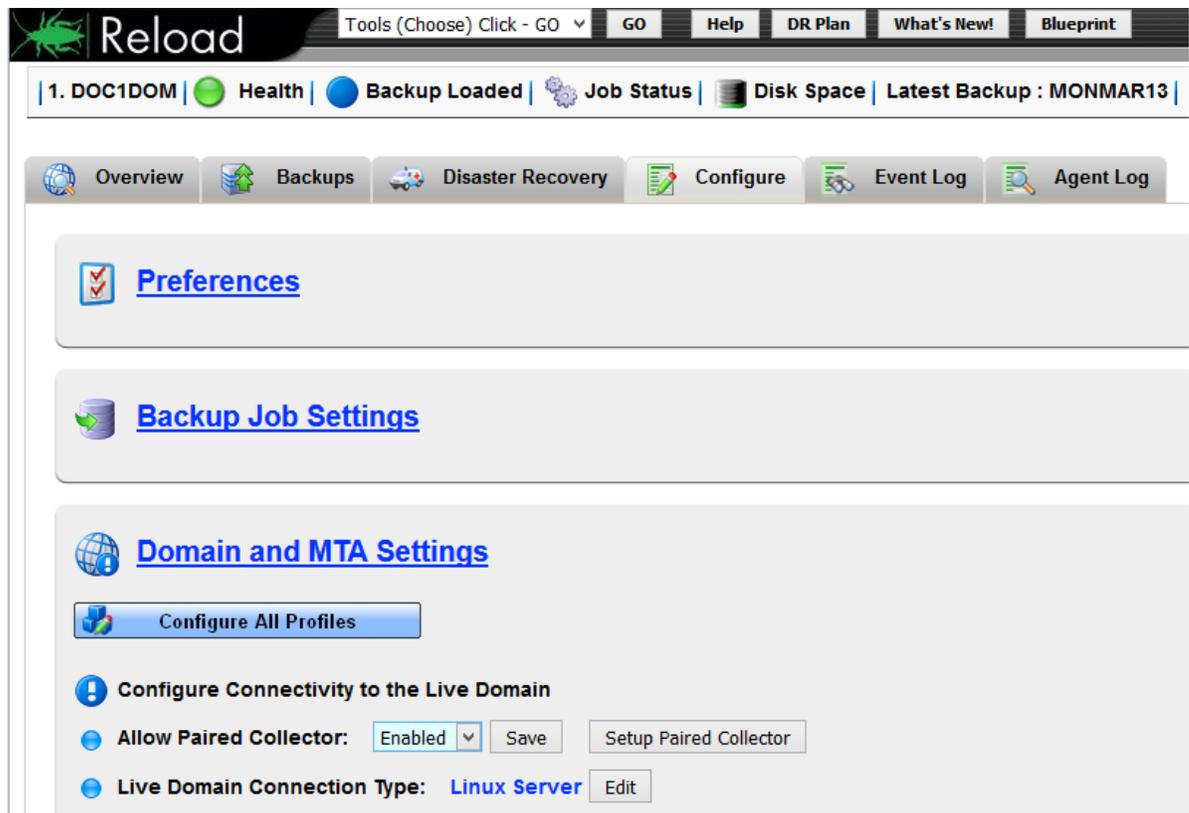
If this is an *existing GroupWise Disaster Recovery installation* with an existing Server model connection for the profile:

On the GroupWise Disaster Recovery server, browse to the GroupWise Disaster Recovery Web Administration Console: http://<GroupWise Disaster Recovery_Server_IP_or_Hostname>:5555

1. Select the profile



2. Click on the Configure tab
3. Open the Domain and MTA Settings panel
4. Enable "Allow Paired Collector", press Save, and click on "Setup Paired Collector" to have GroupWise Disaster Recovery copy the Collector Agent software to the GroupWise server.



On the GroupWise server, in the Domain directory a new directory (/collect) will be created and the file "reload_collector.rpm" will be created.

- ♦ Open a terminal window, go to where the file is and run:

```
rpm -i reload_collector.rpm
```

If this is a *new installation* with no preexisting connection:

On the GroupWise server, browse to the GroupWise Disaster Recovery Web Administration Console. http://<GroupWise Disaster Recovery_Server_IP_or_Hostname>:5555

1. From the Tool dropdown menu select Domain Collector



2. Click on 2. Installing the GroupWise Disaster Recovery Collector Software to open the section

ONLINE COLLECTOR DOCUMENTATION

2. Installing The Reload Collector Software

▶ Here are the steps for installing the Reload Collector Software:

- Get a terminal session to the live Linux based server that houses the GroupWise domain.
- Obtain and install the GroupWise DBCOPY Utility to the GroupWise server.
NOTE: With GroupWise 2014, DBCOPY is already installed. Don't worry about this step!
- Go to the domain directory and look for a directory named: **collect**
- In the **collect** directory look for the file: **reload_collector.rpm**
- Install the **reload_collector.rpm** with the following command:

```
rpm -i reload_collector.rpm
```

NOTE: If the Reload Collector software is not on the live GroupWise server, you can download the collector here: [reload_collector.rpm](#) or find the collector RPM file on the [Reload Server](#) at this path:

[/opt/beginfinite/reload/setup/collect](#)

Copy the the **reload_collector.rpm** file to the live GroupWise server, and install the software as explained above.

3. Click on reload_collector.rpm to download
4. Open a terminal window, go to where the file is and run:

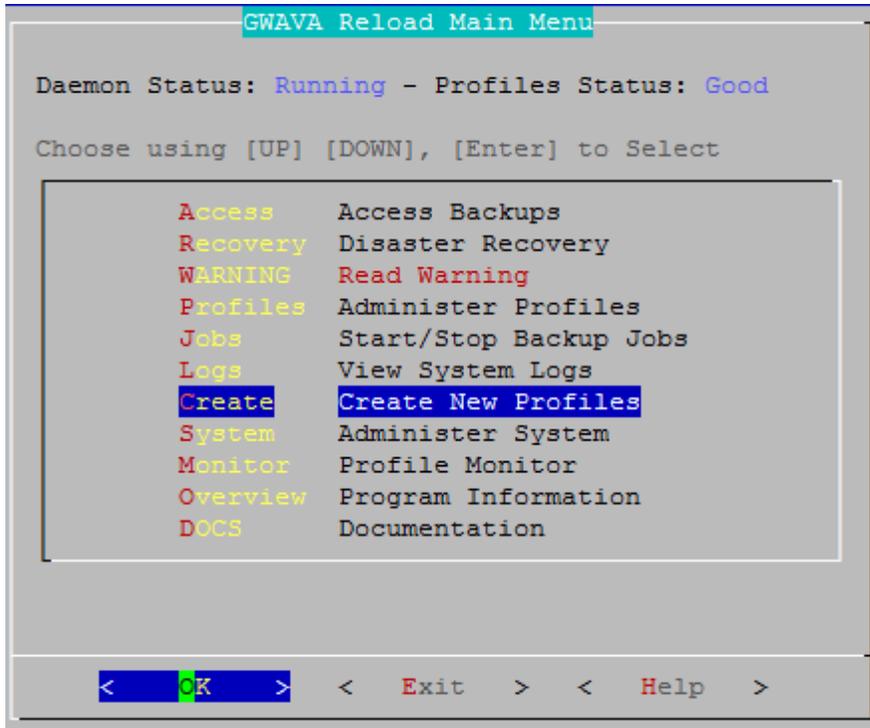
```
rpm -i reload_collector.rpm
```

Configure Collector Agent

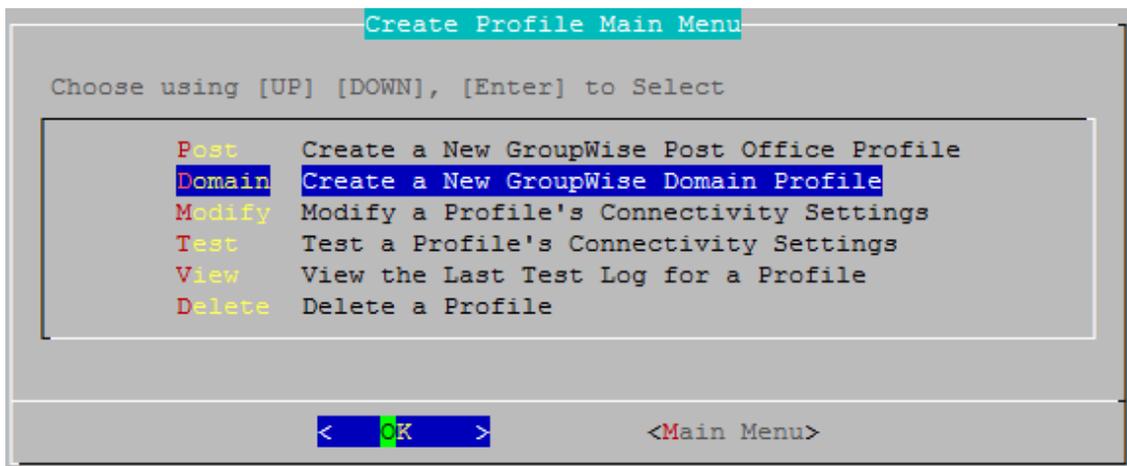
Once the collector is installed, on the GroupWise server, start the GroupWise Disaster Recovery Administration Console by typing on the command line:

reload

1. Select "Create (Create Profile)"



2. Select "Domain (Create a New GroupWise Domain Profile)"



3. Give the Profile a Name. The profile name should not exceed eight characters. Use letters and numbers only, no spaces or other characters. For example: domain. Be aware, that a profile cannot be renamed, once it has been created. Choose the name wisely. Perhaps you will want to name the profile so that its name is the same as the GroupWise post office or domain that the profile represents. Select the Next button.

Profile Name

Choose < Next > to Accept

Use letters and numbers only, no spaces or other characters!

The profile name SHOULD NOT EXCEED 8 characters.

Enter the name of the profile in the field below:

Domain

< Next > < Cancel >

4. Give the Profile a Description. The profile description should not exceed 60 characters and should not have comma(,), nor dollar sign(\$) characters. For example: Domain Collector. The description of the profile will be added to the Agent Log when backup jobs are run for the profile. Select the Next button.

Profile Description

Choose < OK > to Accept

The profile description should not exceed 60 characters.

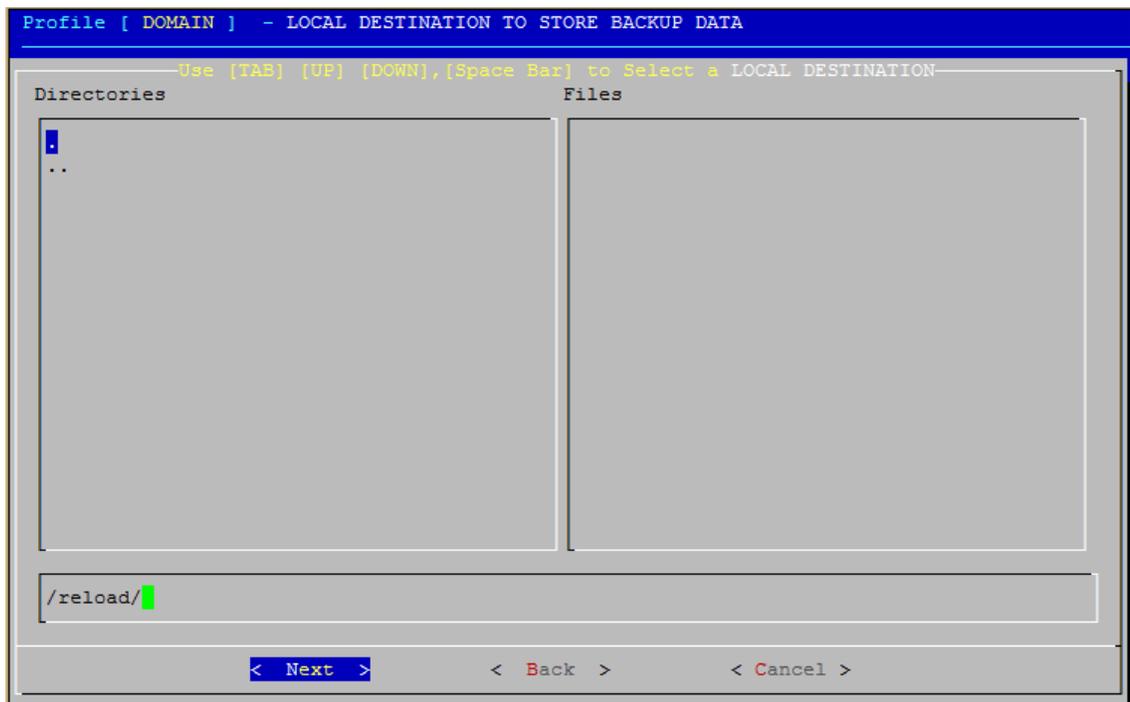
NOTE: Do not use a comma or dollar sign (, \$) character.

Enter the profile description in the field below:

Primary domain

< OK > < Cancel >

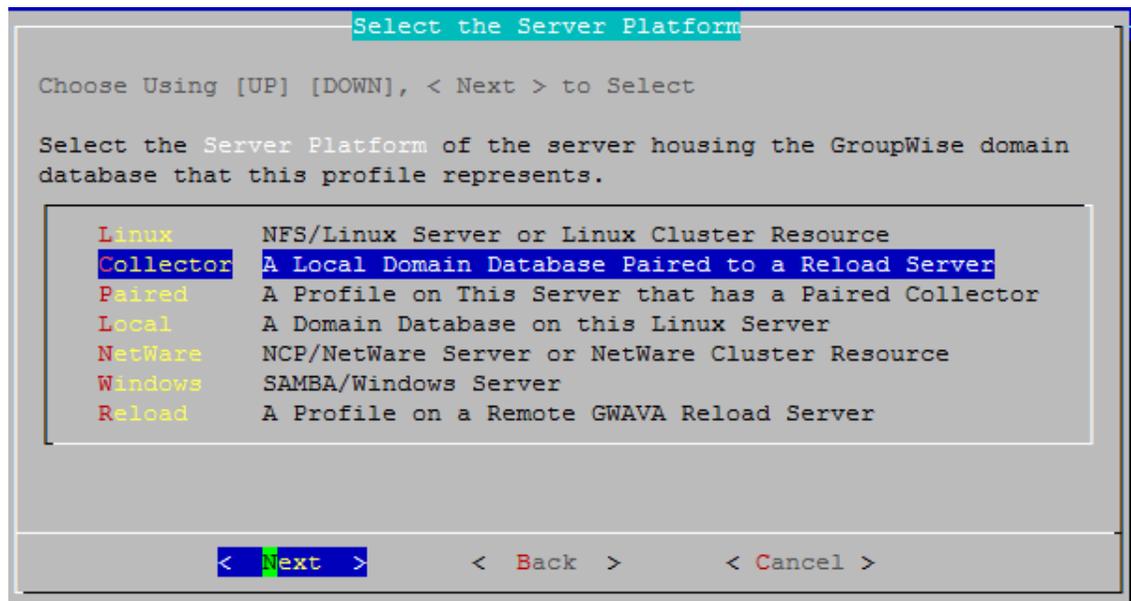
5. Backup Path: Enter the path or browse to the local destination directory to store the backup data. For example: /reload. The profile directory will be added to this path. This path can be a location on the Linux server, or an NFS mount to another Linux/Unix server, or to a SAN. The path should always be available; GroupWise Disaster Recovery is not configured to mount paths in order to access stored data. Also, the path should be to a location that has a lot of disk space available. Select the Next button.



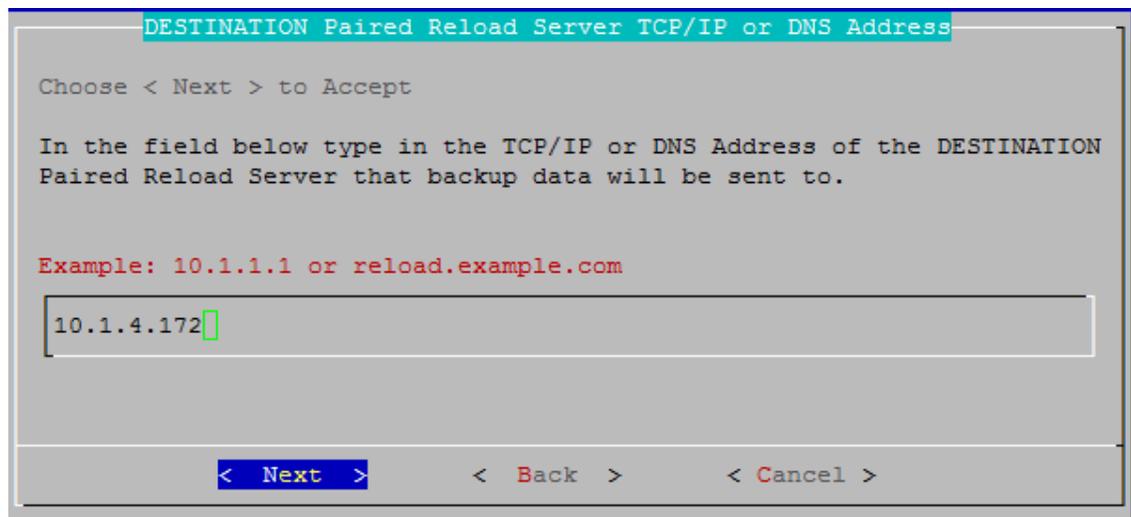
6. Confirm the path to the local destination directory



7. Choose the server type: "Collector (A Local Post Office/Domain Paired to a GroupWise Disaster Recovery Server)". Select the Next button.



8. Enter the TCP/IP Address or DNS hostname for the GroupWise Disaster Recovery server this collector will be paired with. (Do not use the number pad.) Select the Next button.



9. A terminal session will appear to prompt you to accept an SSH key and enter the password for the GroupWise Disaster Recovery server. If another profile was created to the same server it will only update.

```

I know this isn't a normal screen!

But we need to replicate the local SSH key . .
to the DESTINATION Paired Reload Server: 10.1.4.172

This is the command that is being run:

ssh-copy-id -i /root/.ssh/id_rsa.pub 10.1.4.172

*****
NOTE: IF PROMPTED ANSWER: yes AND THEN ENTER THE PASSWORD TO THE RELOAD SERVER
*****

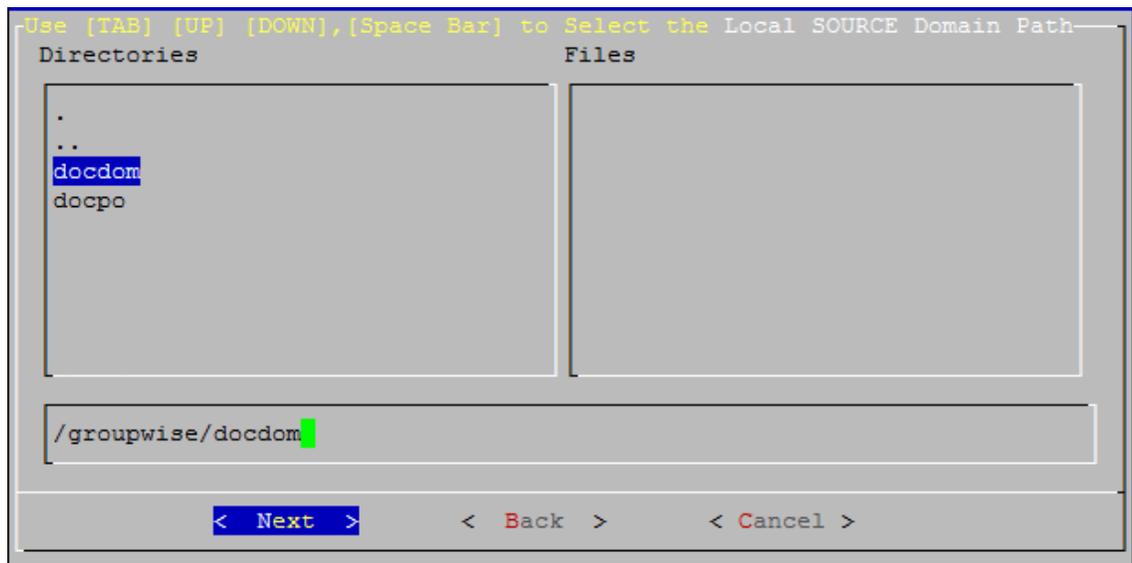
The authenticity of host '10.1.4.172 (10.1.4.172)' can't be established.
ECDSA key fingerprint is b3:9c:e3:cd:c0:59:82:21:c3:66:40:83:eb:38:7d:0a [MD5].
Are you sure you want to continue connecting (yes/no)? yes

```

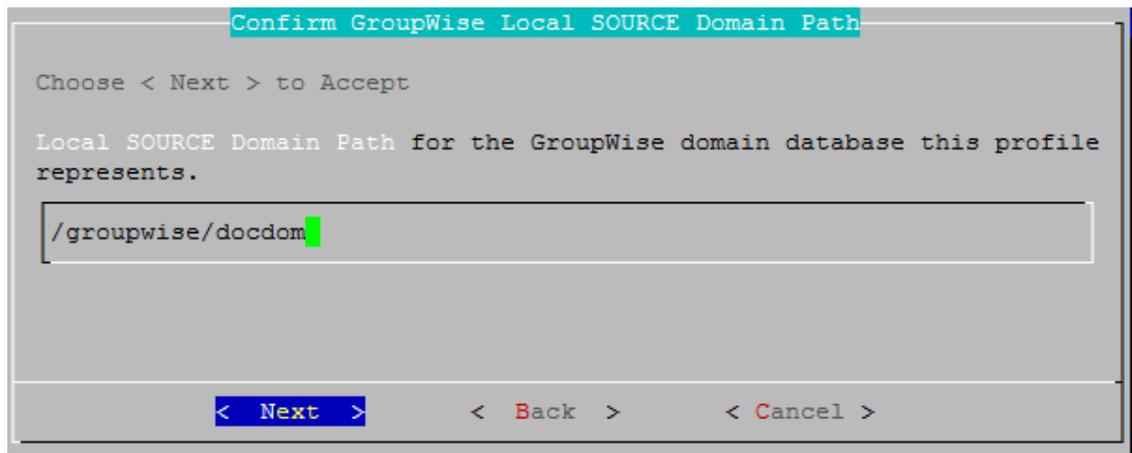
10. Enter the SSH port used by the GroupWise Disaster Recovery server (default port: 22)

11. Backup Path: Enter the destination path the data will be stored in on the GroupWise Disaster Recovery server. This is the destination directory you entered when creating the Paired Server on the GroupWise Disaster Recovery server.

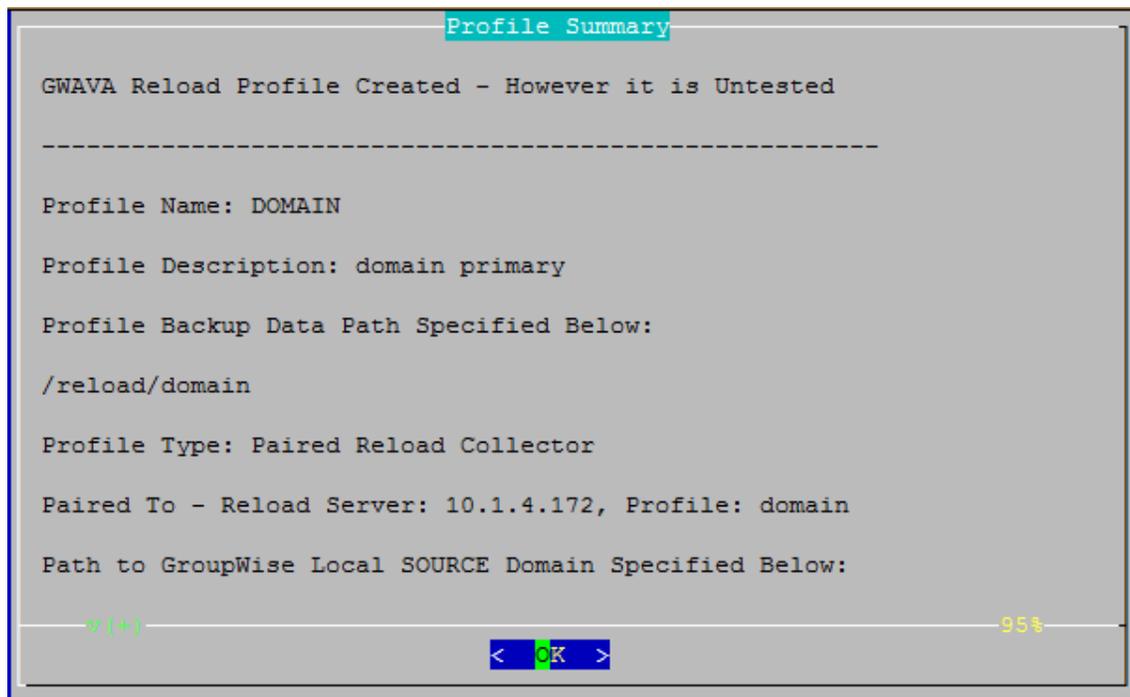
12. Source Path of the GroupWise files: Enter the source path to the local destination directory entered earlier on the GroupWise server. For example: /groupwise/domain



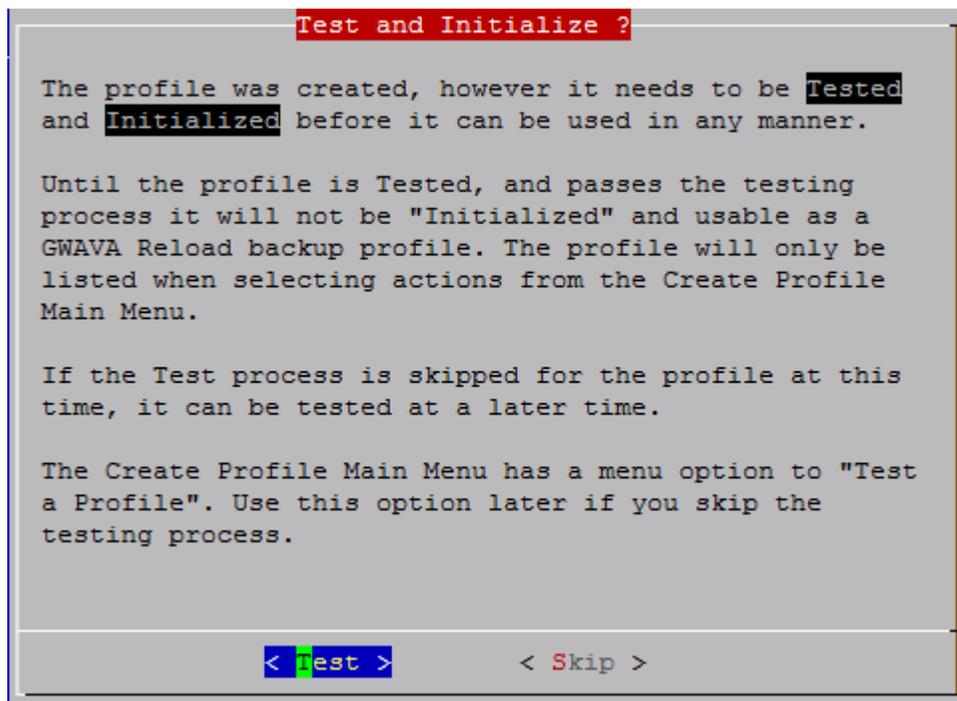
13. Confirm the path to the local source directory



14. A summary of the profile settings will appear. Select the OK button.



15. Test and Initialization:



16. If the profile is correct, select the Test button.
17. If the profile is not correct, select the Skip button.
18. The profile creation wizard tests and initializes the newly created profile and prepares it to accept a pairing request from a Paired Collector and initializes the newly created profile and prepares it to accept a pairing request from a Paired Collector.

```
GWAVA Reload Test and Initialize Utility

Command Executed: ./gre_dom_sync -p domain -f F3 -i /opt/beginfinite/reloa
Profile Specified: domain
LATEST_BACKUP_LOCATION = /reload/domain/backups/
Running Specified Function: F3
[I] DATE: Mon_Mar_13 TIME: 13:34:40 PROFILE: DOMAIN - [GRE_DOM_SYNC]- Now
RSYNC Options: -v -e ssh -p 22 -o ConnectTimeout=30 --progress
[I] DATE: Mon_Mar_13 TIME: 13:34:40 PROFILE: DOMAIN - [GRE_DOM_SYNC]- Runn
[I] DATE: Mon_Mar_13 TIME: 13:34:41 PROFILE: DOMAIN - [GRE_DOM_SYNC]- Sent
[I] DATE: Mon_Mar_13 TIME: 13:34:41 PROFILE: DOMAIN - [GRE_DOM_SYNC]- NOTE
[I] DATE: Mon_Mar_13 TIME: 13:34:41 PROFILE: DOMAIN - [GRE_DOM_SYNC]- Succ

SUCCESS, THIS RELOAD COLLECTOR PROFILE: DOMAIN IS NOW PAIRED
WITH THE RELOAD SERVER PROFILE: DOMAIN ON SERVER: 10.1.4.172

█

< Exit >
```

19. The Collector should find the license from the Server. If it fails, then backups will not occur. The license file can be loaded to the Collector in the Web Console as during the install procedure.

Switching from Server model to Collector Model

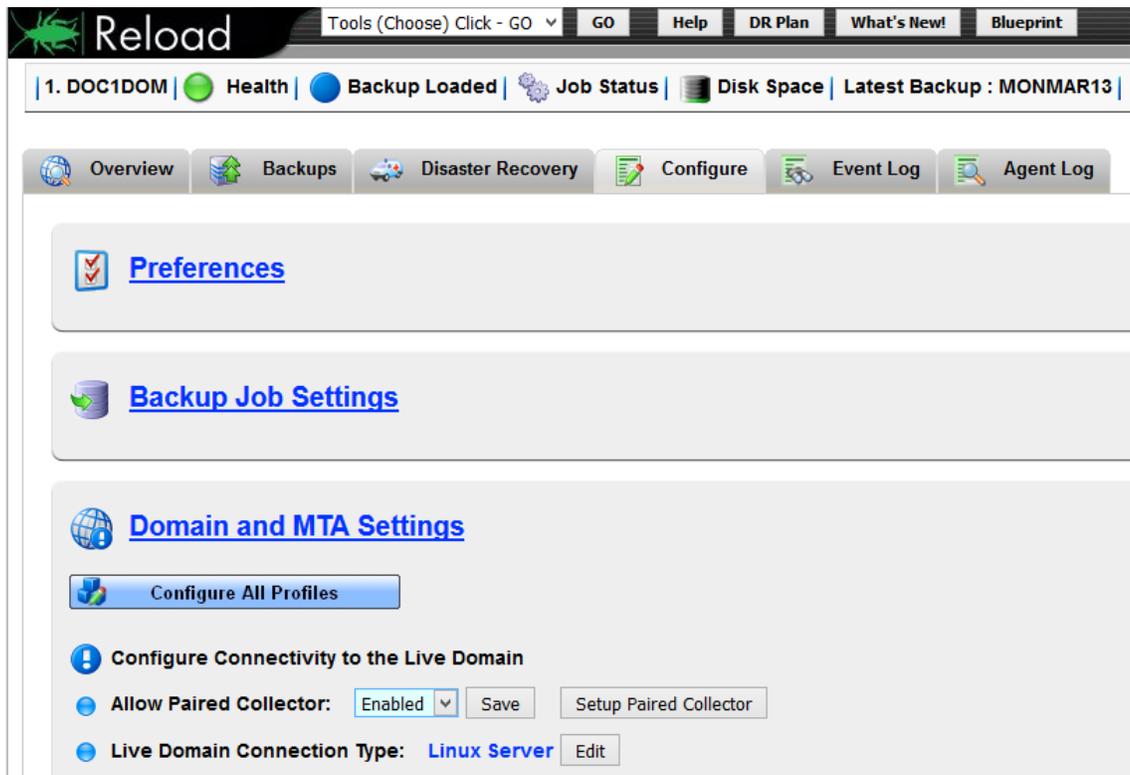
If you have been running GroupWise Disaster Recovery using the server model and the GroupWise Domain and/or Post Office is on Linux, then you can easily switch to the collector model.

- ♦ **On the GroupWise server**, create a directory for the GroupWise Disaster Recovery Agent to copy the databases to before sending to the GroupWise Disaster Recovery server. For example,

```
mkdir /reload
```

If switching the Domain profile:

1. Browse to the GroupWise Disaster Recovery Web Administration console http://<GroupWise Disaster Recovery_Server_Address>:5555
2. Select the Domain Profile
3. Select the Configure tab and open "Domain and MTA Settings"
4. Enable "Allow Paired Collector" and press Save



5. Click on "Setup Paired Collector". This will create the directory /collect in the domain directory on the GroupWise server and copy the file "reload_collector.rpm" to it.
6. Connect to the GroupWise server and run


```
rpm -ivh reload_collector.rpm
```
7. Setup up the collector by running


```
reload
```
8. See Domain Profile: Collector/Server Model to complete the setup process
9. Start a backup job on the collector and the profile on the GroupWise Disaster Recovery will change to a Collector/Server with a <~> after the name

Collector Model Post Office Profiles

Paired Collector/Server Model

The Collector model creates a software agent called a collector that handles transferring the data to the GroupWise Disaster Recovery server.

You first set up a receiving server profile (marked with a <~>) on the GroupWise Disaster Recovery server, then a sending collector profile (marked with a ~) on the GroupWise server.

It is faster than the Server Only model and can send the data to up to three different GroupWise Disaster Recovery server, but requires copying parts of the domain or post office to another directory before sending the data so it has a snapshot of the data.

Prerequisites

You will need to create a directory on the GroupWise Disaster Recovery and the GroupWise server for the backup data. The name of the profile will be used to create sub-directories for each profile. For example:

```
/reload/
```

You will need to know the directories on the GroupWise server for the live data. For example:

```
/groupwise/domain
```

```
/groupwise/po1
```

Configure Profiles

Post Office Profile: Collector/Server Model

On the GroupWise Disaster Recovery Server, create the Server:

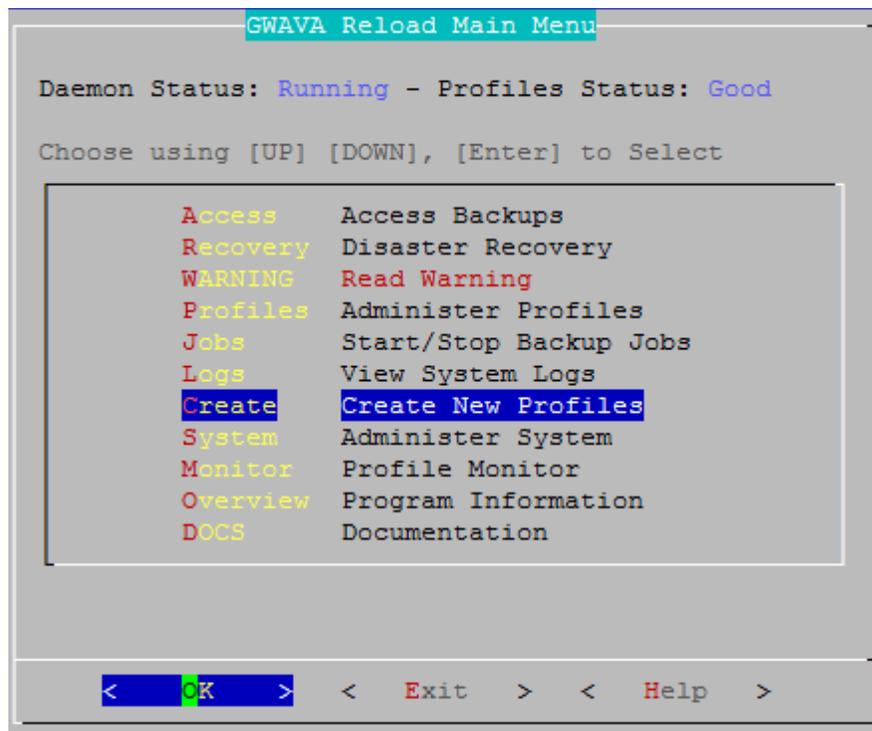
1. Create a directory for the backup data. For example:

```
mkdir /reload
```

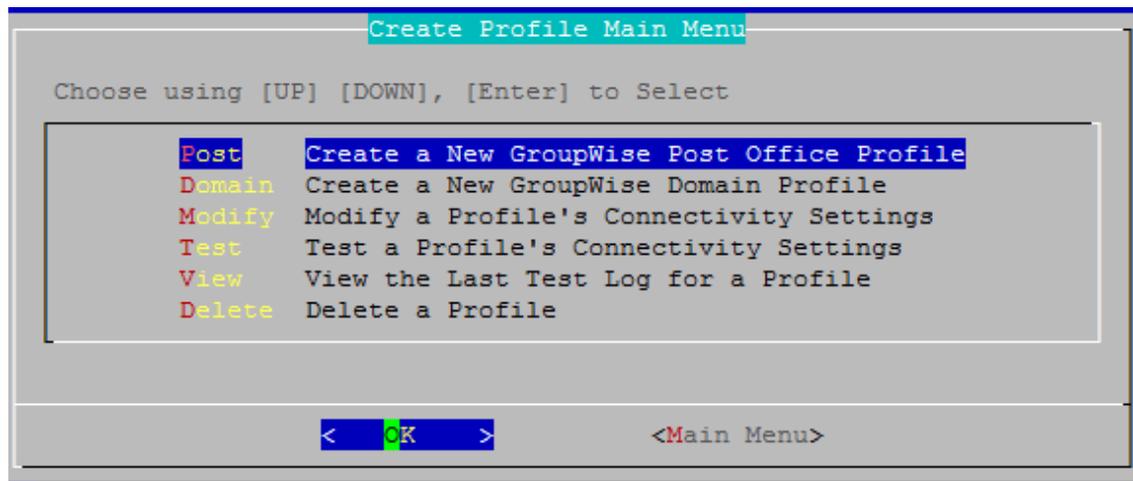
2. Start the GroupWise Disaster Recovery Administration Console by typing on the command line:

```
reload
```

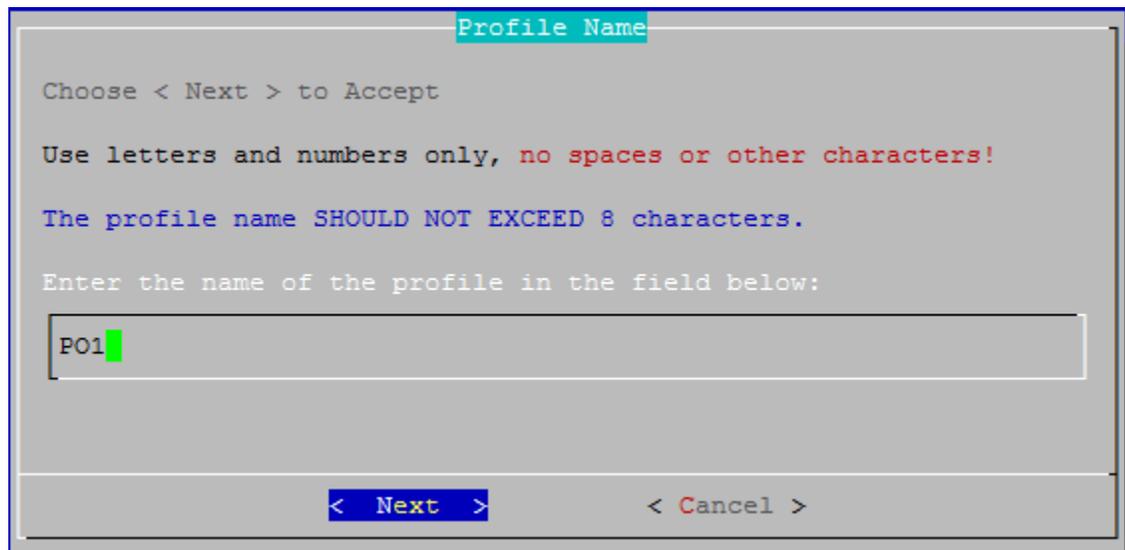
3. Select "Create (Create Profile)"



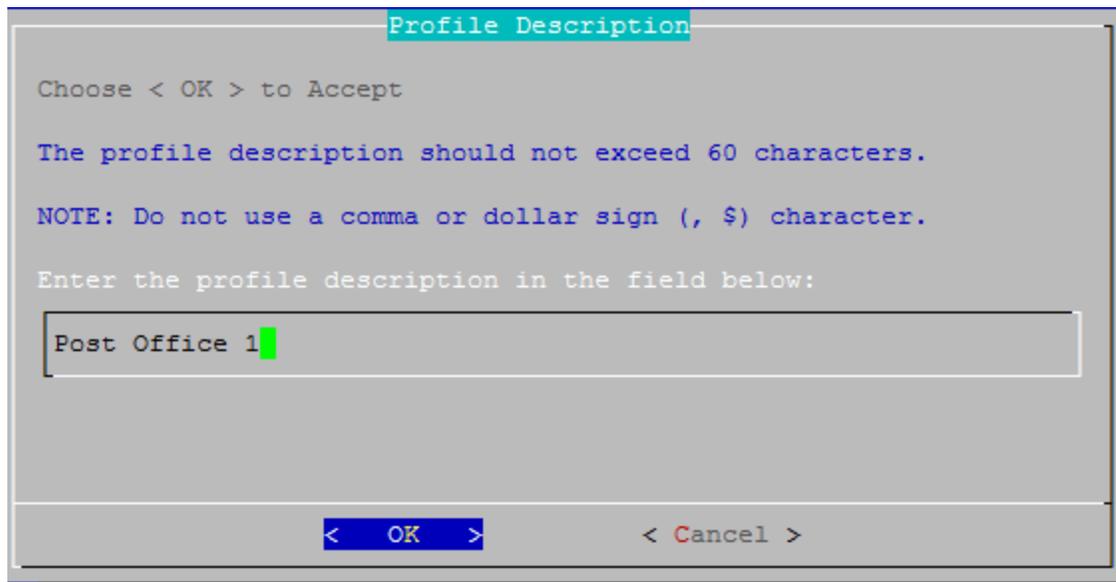
4. Select "Post Office (Create a New GroupWise Post Office Profile)"



5. Give the Profile a Name. The profile name should not exceed eight characters. Use letters and numbers only, no spaces or other characters. For example: Post Office. Be aware, that a profile cannot be renamed, once it has been created. Choose the name wisely. Perhaps you will want to name the profile so that its name is the same as the GroupWise post office or domain that the profile represents. Select the Next button.



6. Give the Profile a Description. The profile description should not exceed 60 characters and should not have comma(,), nor dollar sign(\$) characters. For example: Primary Post Office. The description of the profile will be added to the Agent Log when backup jobs are run for the profile. Select the Next button.



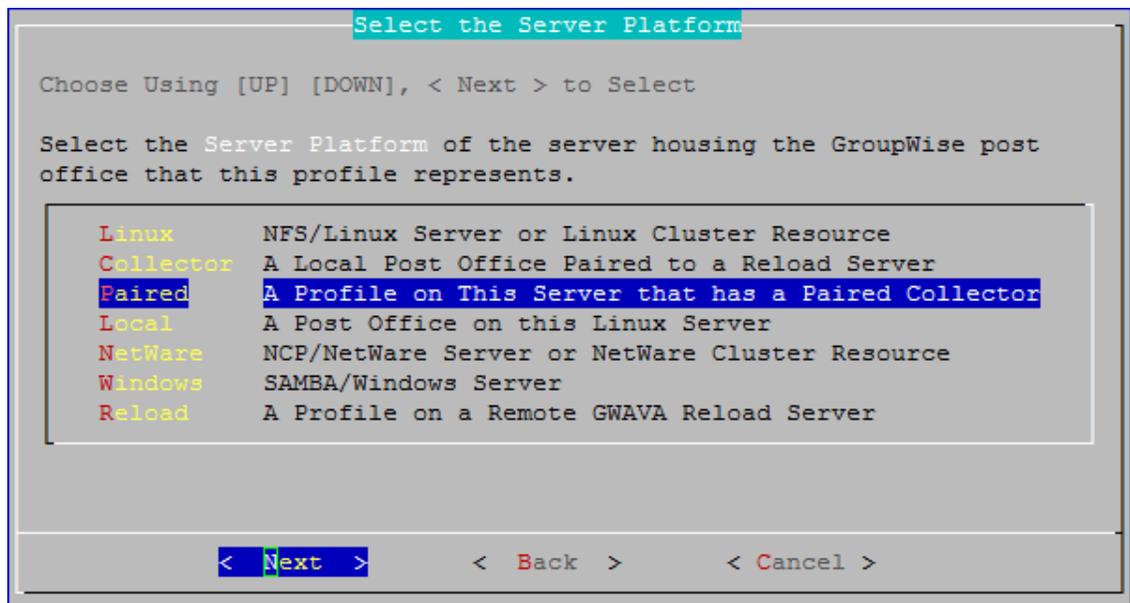
7. Enter the path or browse to the local destination directory to store the backup data. For example: /reload. The profile directory will be added to this path. This path can be a location on the Linux server, or an NFS mount to another Linux/Unix server, or to a SAN. The path should always be available; GroupWise Disaster Recovery is not configured to mount paths in order to access stored data. Also, the path should be to a location that has a lot of disk space available. Select the Next button.



8. Confirm the path to the local destination directory



9. Choose the server type: "Paired (A Profile on This Server that has a Paired Collector)". Select the Next button.



10. The profile creation wizard tests and initializes the newly created profile and prepares it to accept a pairing request from a Paired Collector and initializes the newly created profile and prepares it to accept a pairing request from a Paired Collector.

```
GWAVA Reload Test and Initialize Utility
cp: missing destination file operand after `'/reload/po1/gre_data/gwpo.dc'
Try `cp --help' for more information.

Finishing preparation steps on data copied from post office.

Mon Mar 13 14:01:45 MDT 2017

SUCCESS, THE PAIRED SERVER PROFILE: PO1 IS NOW ENABLED.

[

< Exit >
```

Testing and initializing a profile does not backup the post office or domain in any way.

Once a profile is tested and initialized successfully, the profile is available to be configured further. The default configuration of a profile is sufficient for making quickly accessible backups with GroupWise Disaster Recovery. Further configuration of the profile should be done in GroupWise Disaster Recovery Web Administration.

To be able to backup the data, a collector needs to be created on the GroupWise server.

On the GroupWise Server, the collector will need to be downloaded, installed and configured to connect to the GroupWise Disaster Recovery server.

If this is a *new installation* with no preexisting connection:

1. *On the GroupWise server*, browse to the GroupWise Disaster Recovery Web Administration Console. http://<GroupWise Disaster Recovery_Server_IP_or_Hostname>:5555
2. From the Tool dropdown menu select Post Office Collector



3. Click on 2. Installing the GroupWise Disaster Recovery Collector Software to open the section
4. Click on reload_collector.rpm to download

Reload Tools (Choose) Click - GO GO Help DR Plan What's New! Blueprint

ONLINE COLLECTOR DOCUMENTATION

 [1. Creating The Reload Server Profile](#)

 [2. Installing The Reload Collector Software](#)

 Here are the steps for installing the Reload Collector Software:

-  Get a terminal session to the live Linux based server that houses the GroupWise post office.
-  Obtain and install the GroupWise DBCOPY Utility to the GroupWise server.

NOTE: With GroupWise 2014, DBCOPY is already installed. Don't worry about this step!

-  Go to the post office directory and look for a directory named: [collect](#)
-  In the [collect](#) directory look for the file: [reload_collector.rpm](#)
-  Install the [reload_collector.rpm](#) with the following command:

```
rpm -i reload_collector.rpm
```

NOTE: If the Reload Collector software is not on the live GroupWise server, you can download the collector here: [reload_collector.rpm](#) or find the collector RPM file on the [Reload Server](#) at this path:

```
/opt/beginfinite/reload/setup/collect
```

Copy the the [reload_collector.rpm](#) file to the live GroupWise server, and install the software as explained above.

5. Open a terminal window, go to where the file is and run:

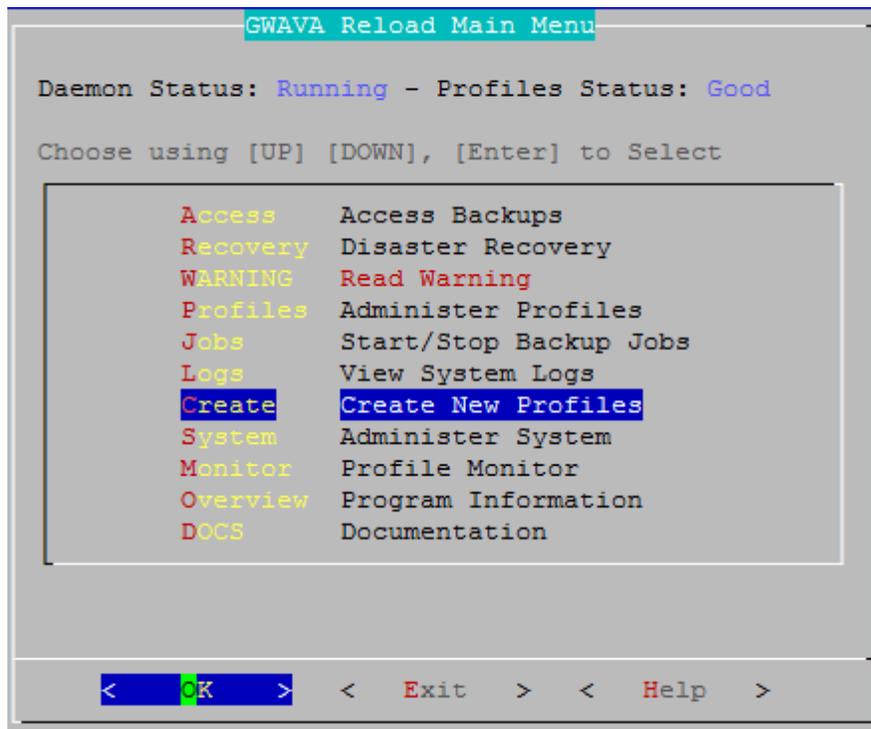
```
rpm -i reload_collector.rpm
```

Configure Collector Agent

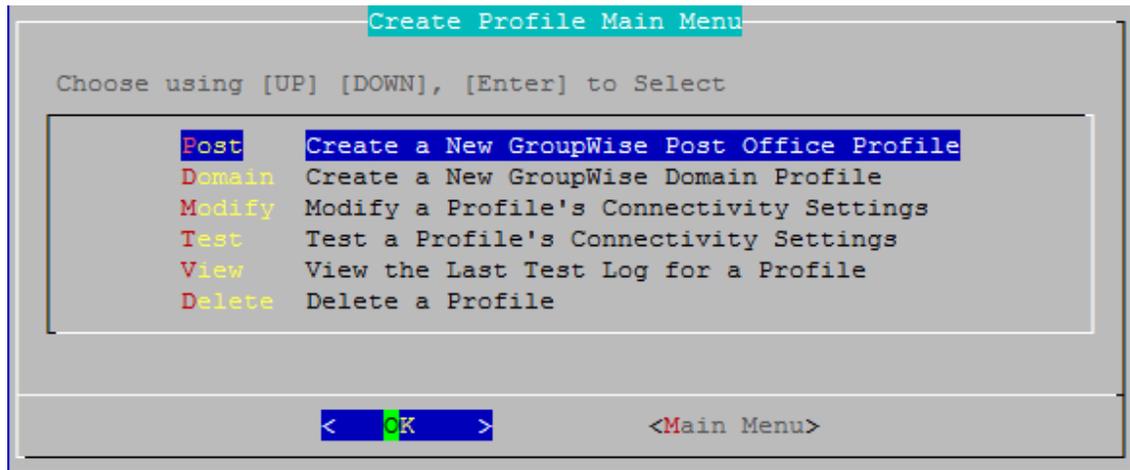
Once the collector agent is installed, on the GroupWise server, start the GroupWise Disaster Recovery Administration Console by typing on the command line:

```
reload
```

1. Select "Create (Create Profile)"



2. Select "Post Office (Create a New GroupWise Post Office Profile)"



3. Give the Profile a Name. The profile name should not exceed eight characters. Use letters and numbers only, no spaces or other characters. For example: po. Be aware, that a profile cannot be renamed, once it has been created. Choose the name wisely. Perhaps you will want to name the profile so that its name is the same as the GroupWise post office or domain that the profile represents, but it does not have to match. Select the Next button.

Profile Name

Choose < Next > to Accept

Use letters and numbers only, no spaces or other characters!

The profile name SHOULD NOT EXCEED 8 characters.

Enter the name of the profile in the field below:

< Next > < Cancel >

4. Give the Profile a Description. The profile description should not exceed 60 characters and should not have comma(,), nor dollar sign(\$) characters. For example: Domain Collector. The description of the profile will be added to the Agent Log when backup jobs are run for the profile. Select the Next button.

Profile Description

Choose < OK > to Accept

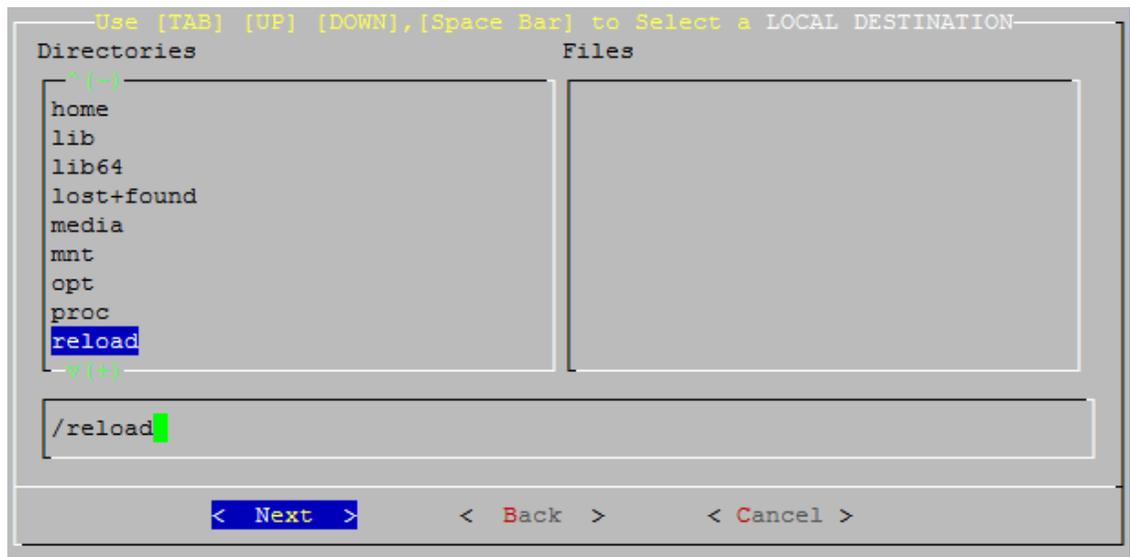
The profile description should not exceed 60 characters.

NOTE: Do not use a comma or dollar sign (, \$) character.

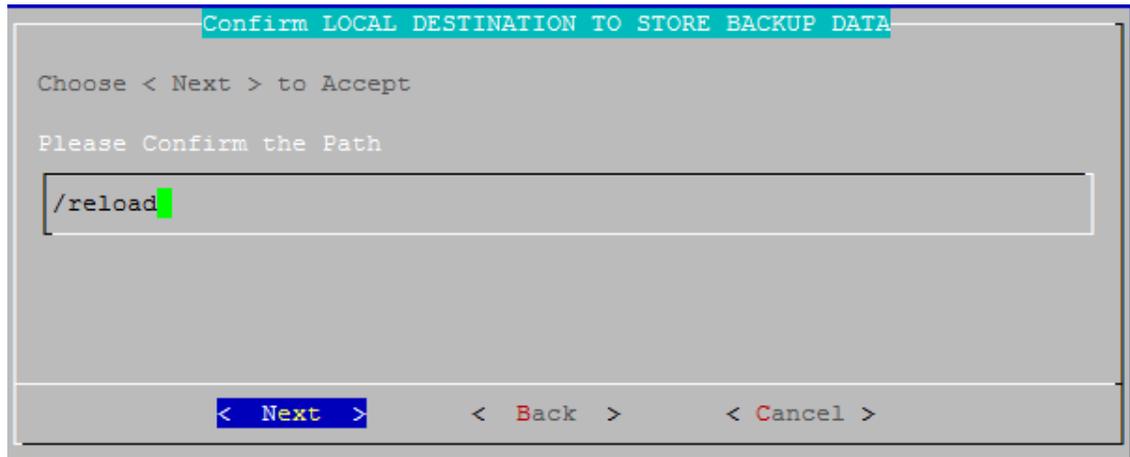
Enter the profile description in the field below:

< OK > < Cancel >

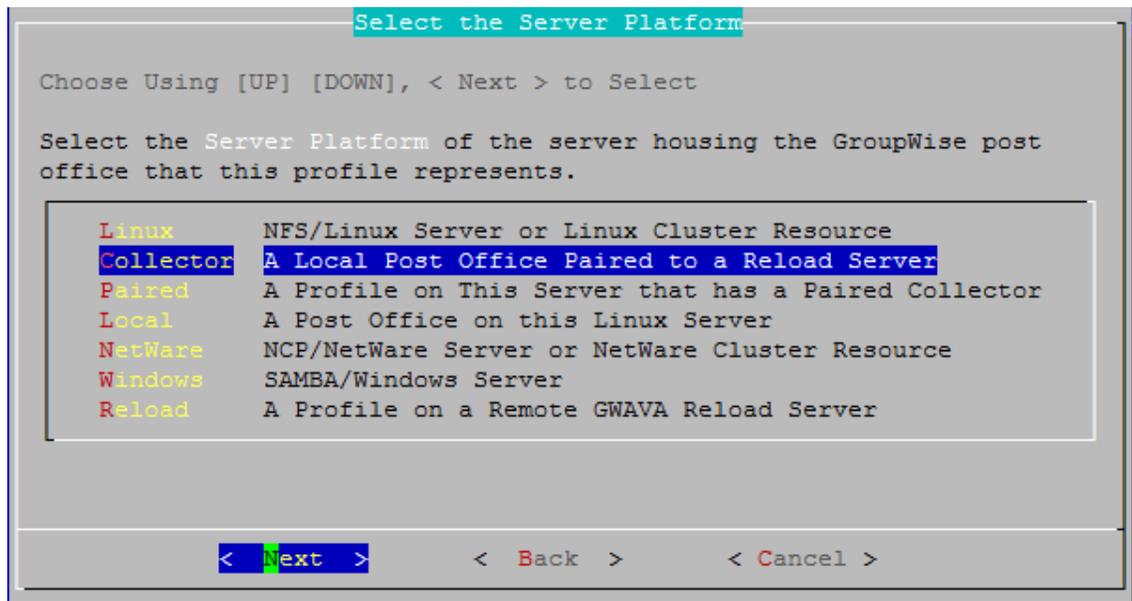
5. Enter the path or browse to the local destination directory to store the backup data. For example: /reload. This path can be a location on the Linux server, or an NFS mount to another Linux/Unix server, or to a SAN. The path should always be available; GroupWise Disaster Recovery is not configured to mount paths in order to access stored data. Also, the path should be to a location that has a lot of disk space available. Select the Next button.



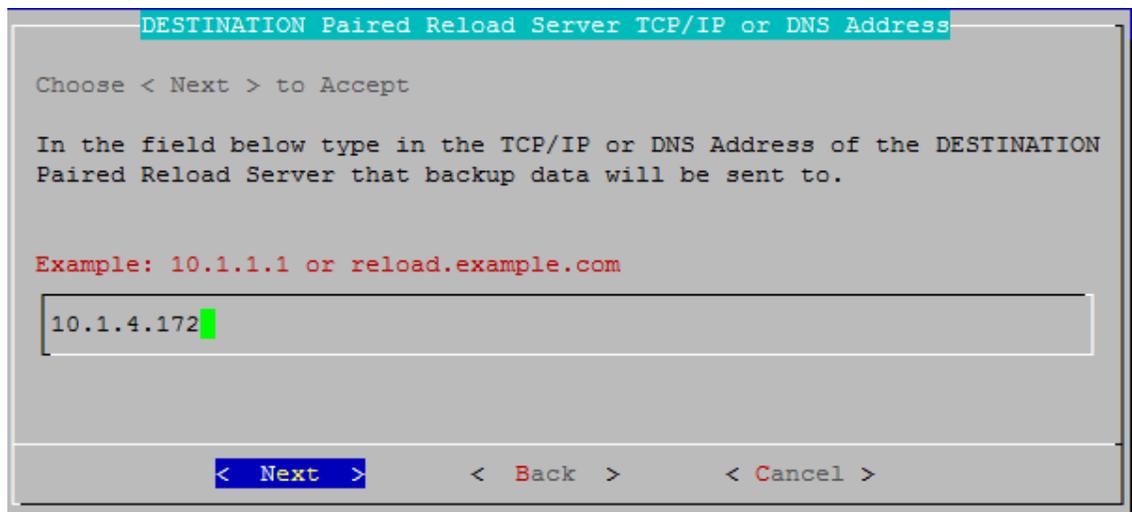
6. Confirm the path to the local destination directory



7. Choose the server type: "Collector (A Local Post Office/Domain Paired to a GroupWise Disaster Recovery Server)". Select the Next button.



8. Enter the TCP/IP Address or DNS hostname for the GroupWise Disaster Recovery server this collector will be paired with. Select the Next button.



9. A terminal session will appear to prompt you to accept an SSH key and enter the password for the GroupWise Disaster Recovery server. If another profile was created to the same server it will only update.

```
I know this isn't a normal screen!

But we need to replicate the local SSH key . .
to the DESTINATION Paired Reload Server: 10.1.4.172

This is the command that is being run:

ssh-copy-id -i /root/.ssh/id_rsa.pub 10.1.4.172

*****
NOTE: IF PROMPTED ANSWER: yes AND THEN ENTER THE PASSWORD TO THE RELOAD SERVER
*****

The authenticity of host '10.1.4.172 (10.1.4.172)' can't be established.
ECDSA key fingerprint is b3:9c:e3:cd:c0:59:82:21:c3:66:40:83:eb:38:7d:0a [MD5].
Are you sure you want to continue connecting (yes/no)? yes
```

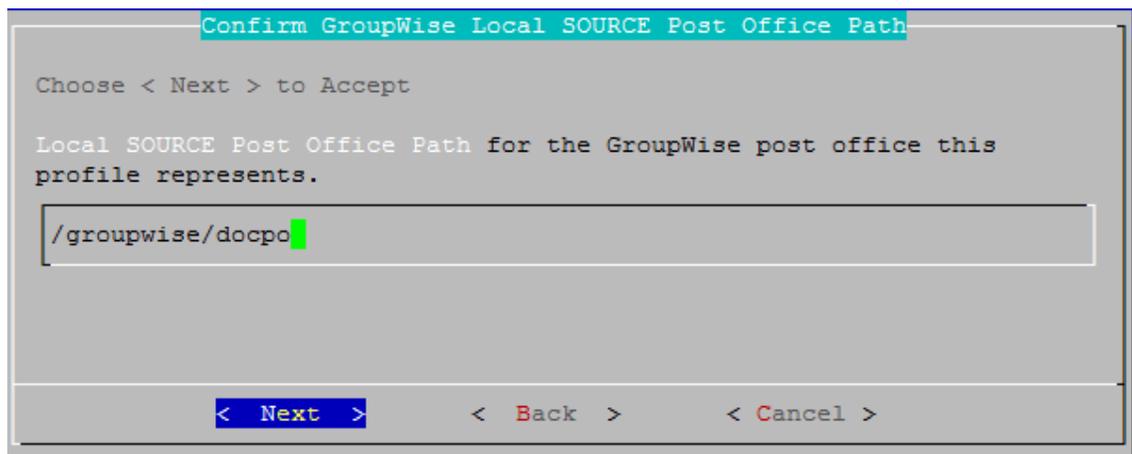
- 10. Enter the SSH port used by the GroupWise Disaster Recovery server (default port: 22)

- 11. Enter the destination path the data will be stored in on the GroupWise Disaster Recovery server. This is the destination directory you entered when creating the Paired Server on the GroupWise Disaster Recovery server.

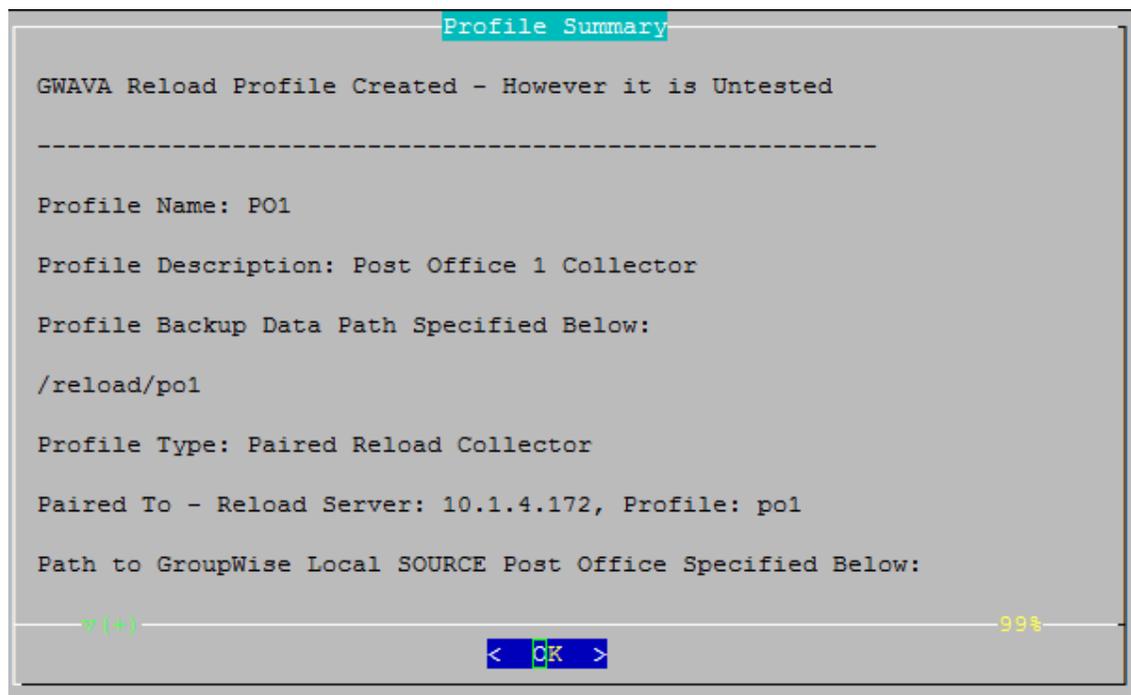
- 12. Source Path to the GroupWise files: Enter the source path to the local destination directory entered earlier on the GroupWise server. For example: /groupwise/po



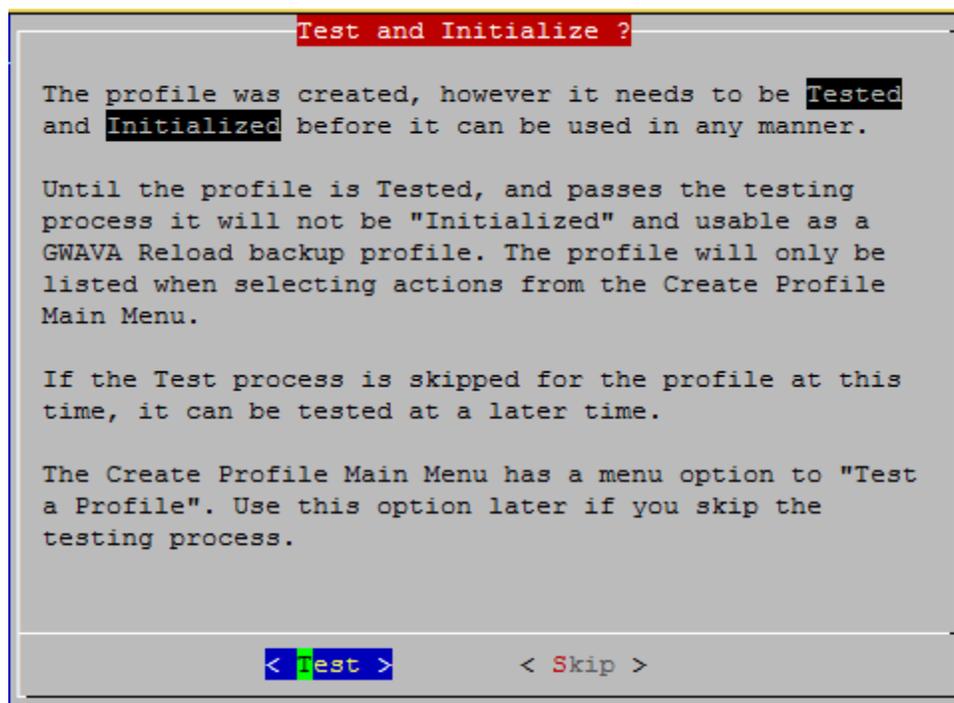
13. Confirm the path to the local source directory



14. A summary of the profile settings will appear. Select the OK button.



15. Test and Initialization:



16. If the profile is correct, select the Test button.
17. If the profile is not correct, select the Skip button.
18. The profile creation wizard tests and initializes the newly created profile and prepares it to accept a pairing request from a Paired Collector and initializes the newly created profile and prepares it to accept a pairing request from a Paired Collector.

```
GWAVA Reload Test and Initialize Utility
[I] DATE: Mon_Mar_13 TIME: 14:53:01 PROFILE: PO1 - [GRE_PO_SYNC]- Successf
removed `/opt/beginfinite/reload/temp/remote_pairing_request.bin.148943838
`/opt/beginfinite/reload/temp/GRE_TEXT_EDITOR_REPLACE.32409' -> `/opt/begi
removed `/opt/beginfinite/reload/temp/remote_pairing_request.bin.148943838
`/opt/beginfinite/reload/temp/GRE_TEXT_EDITOR_REPLACE.32409' -> `/opt/begi
removed `/opt/beginfinite/reload/temp/remote_pairing_request.bin.148943838
`/opt/beginfinite/reload/temp/GRE_TEXT_EDITOR_REPLACE.32409' -> `/opt/begi
[I] DATE: Mon_Mar_13 TIME: 14:53:01 - [GRE_PO_SYNC] - Sent Remote Pairing
[I] DATE: Mon_Mar_13 TIME: 14:53:01 PROFILE: PO1 - [GRE_PO_SYNC]- Sent Rem
[I] DATE: Mon_Mar_13 TIME: 14:53:01 - [GRE_PO_SYNC] - NOTE: No Need to Obt
[I] DATE: Mon_Mar_13 TIME: 14:53:01 PROFILE: PO1 - [GRE_PO_SYNC]- NOTE: No
[I] DATE: Mon_Mar_13 TIME: 14:53:01 - [GRE_PO_SYNC] - NOTE: No Need to Obt
[I] DATE: Mon_Mar_13 TIME: 14:53:01 PROFILE: PO1 - [GRE_PO_SYNC]- NOTE: No

SUCCESS, THIS RELOAD COLLECTOR PROFILE: PO1 IS NOW PAIRED
WITH THE RELOAD SERVER PROFILE: PO1 ON SERVER: 10.1.4.172

[

< Exit >
```

If this is an *existing* GroupWise Disaster Recovery installation with an existing Server model connection for the profile:

1. On the *GroupWise Disaster Recovery* server, browse to the GroupWise Disaster Recovery Web Administration Console. http://<GroupWise Disaster Recovery_Server_IP_or_Hostname>:5555
2. Select the profile
3. Click on the Configure tab
4. Open the Post Office and POA Settings section
5. Enable "Allow Paired Collector"

Click on "Setup Paired Collector" to have GroupWise Disaster Recovery copy the collector agent to the GroupWise server.

1. *On the GroupWise server*, in the Post Office directory a new directory (/collect) will be created and the file "reload_collector.rpm" will be created.
2. Open a terminal window, go to where the file is and run:

```
rpm -i reload_collector.rpm
```

Switching from Server model to Collector Model

If you have been running GroupWise Disaster Recovery using the server model and the GroupWise Domain and/or Post Office is on Linux, then you can easily switch to the collector model.

- ♦ **On the GroupWise server**, create a directory for the GroupWise Disaster Recovery Agent to copy the databases to before sending to the GroupWise Disaster Recovery server. For example,

```
mkdir /reload
```

If switching the Post Office profile:

1. Browse to the GroupWise Disaster Recovery Web Administration console `http://<GroupWise Disaster Recovery_Server_Address>:5555`
2. Select the Post Office Profile

3. Select the Configure tab and open "Post Office and POA Settings"
4. Enable "Allow Paired Collector" and press Save

The screenshot shows the Reload web interface. At the top, there is a navigation bar with the Reload logo and several menu items: Tools (Choose) Click - GO, GO, Help, DR Plan, What's New!, and Blueprint. Below this is a status bar with indicators for 1. DOC1PO, Health, Backup Loaded, Job Status, Disk Space, and Latest Backup : MONMAR13. The main navigation area includes tabs for Overview, Backups, Disaster Recovery, Configure, Event Log, and Agent Log. The 'Configure' tab is active, showing a list of configuration options: Preferences, User Access to Backups, Backup Job Settings, and Post Office and POA Settings. The 'Post Office and POA Settings' section is expanded, showing a 'Configure All Profiles' button, a warning icon, and the 'Allow Paired Collector' option set to 'Enabled' with a 'Save' button and a 'Setup Paired Collector' button. A note indicates 'NOTE: Disk Space Required For Collector: 49 MB'.

5. Click on "Setup Paired Collector". This will create the directory /collect in the post office directory on the GroupWise server and copy the file "reload_collector.rpm" to it.
6. Confirm there is sufficient space on the GroupWise server for the GroupWise Disaster Recovery agent to copy the post office databases to. For example, 49MB.
7. Connect to the GroupWise server and run

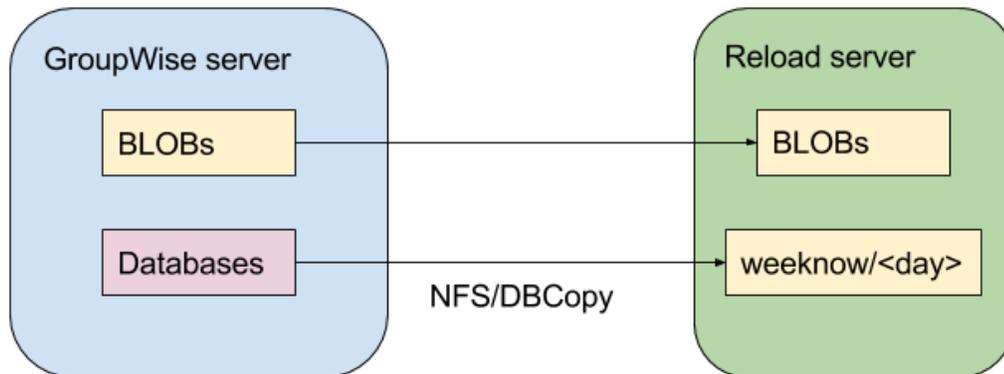

```
rpm -ivh reload_collector.rpm
```
8. Setup up the collector by running


```
reload
```
9. See Post Office Profile: Collector/Server Model to complete the setup process
10. Start a backup job on the collector and the profile on the GroupWise Disaster Recovery will change to a Collector/Server with a <~> after the name

Server Only Profiles

Server Only Model

The Server model requires an NFS connection from the GroupWise server to the GroupWise Disaster Recovery server and uses DBCopy to copy the databases and BLOB files between servers. This is slower than the rsync connection that the collector uses, but does not require any extra disk space on the GroupWise server.



Creating Profiles On Linux GroupWise Systems

There are two kinds of profiles: Domain and Post Office.

You will need to create a directory on the GroupWise Disaster Recovery server for the backup data. The name of the profile will be used to create sub-directories for each profile. For example:

```
/reload/
```

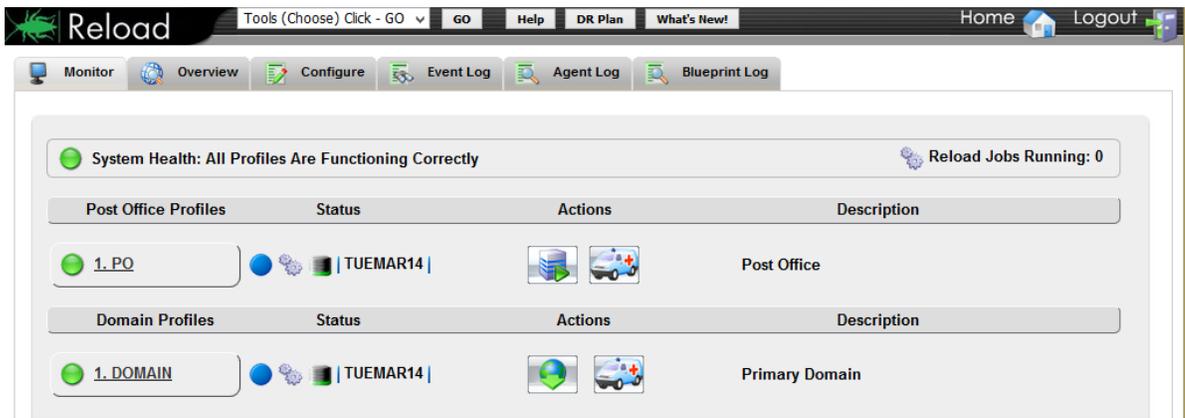
You will need to know the directories on the GroupWise server for the live data. For example:

```
/groupwise/domain
```

```
/groupwise/po1
```

Configure Profiles

There are two kinds of Server Only Model Profiles: [Domain \(Creating_Server_Only_Model_Domain_Profiles.htm\)](#) and [Post Office \(Creating_Server_Only_Post_Office_Profiles.htm\)](#).

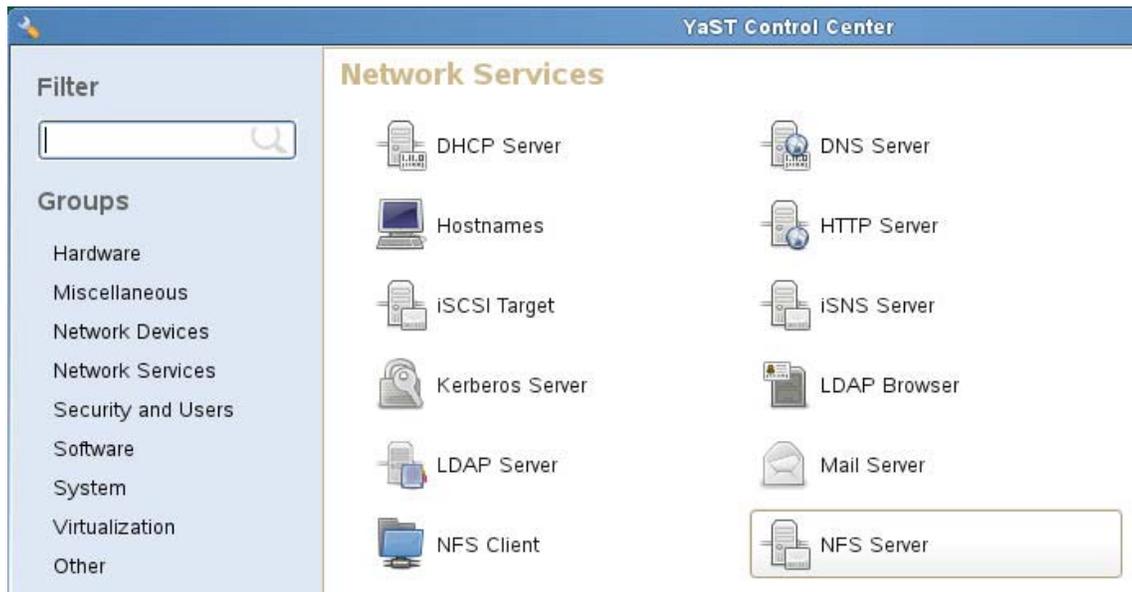


Creating Server Only Model Domain Profiles

Domain Profile: Server Only Model

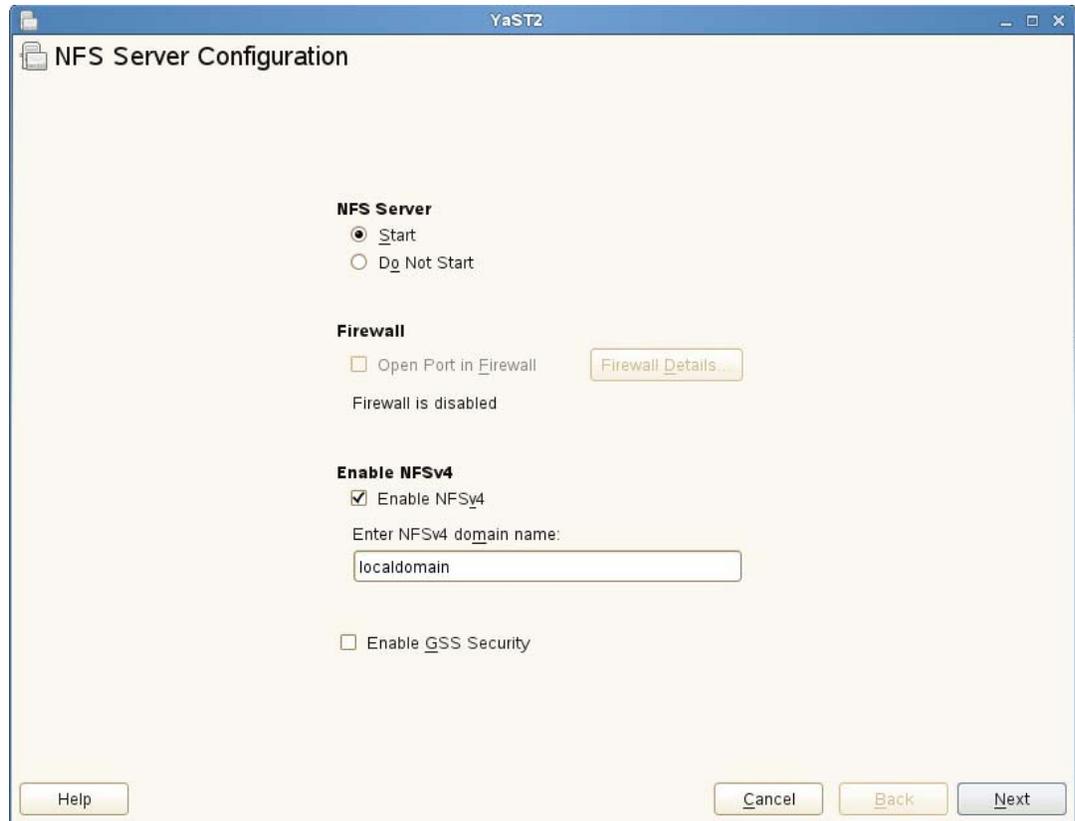
On the GroupWise server, create an NFS mount. Each domain and post office must receive their own mount points.

1. Start YaST2
2. Install NFS Server



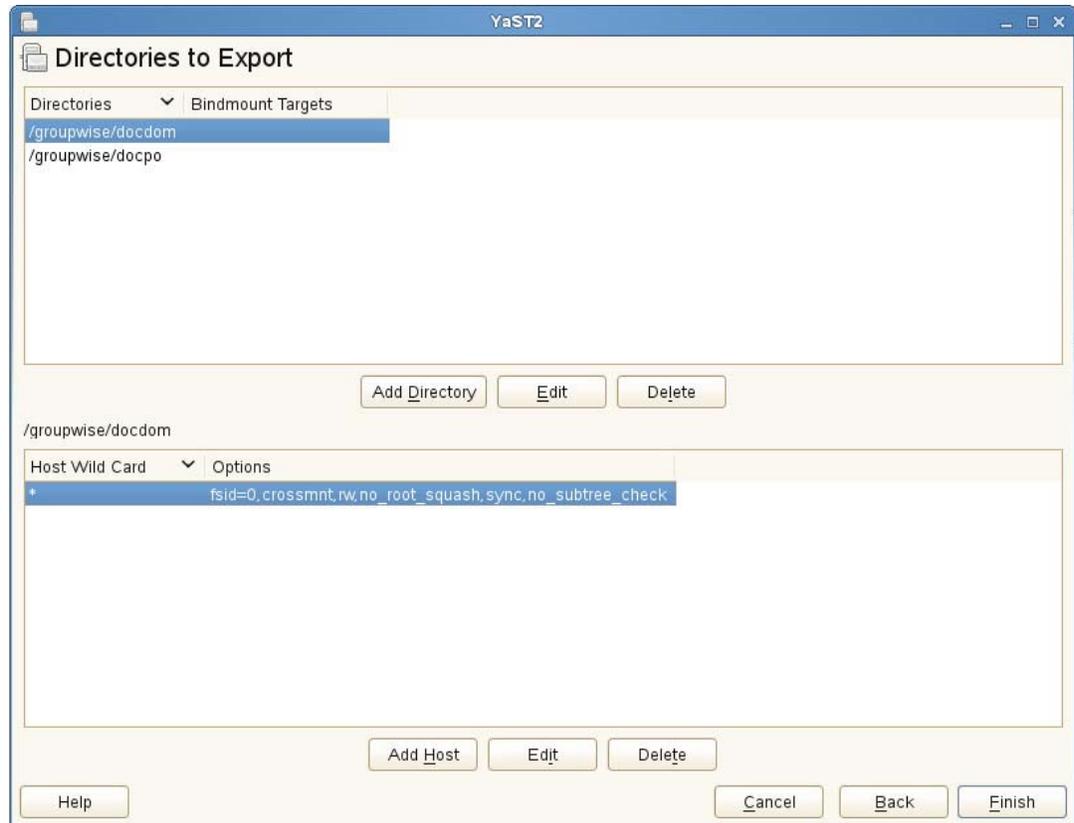
3. Configure NFS Server:
 - a. Set NFS Server to start

- b. Open the port in the firewall, if applicable.



4. Add Directory:
 - a. Browse to the domain directory. For example /groupwise/domain

- b. Set options to: *rw,no_root_squash,sync*



5. Press Finish to complete setup.

On the GroupWise Disaster Recovery server, create a data directory and a profile

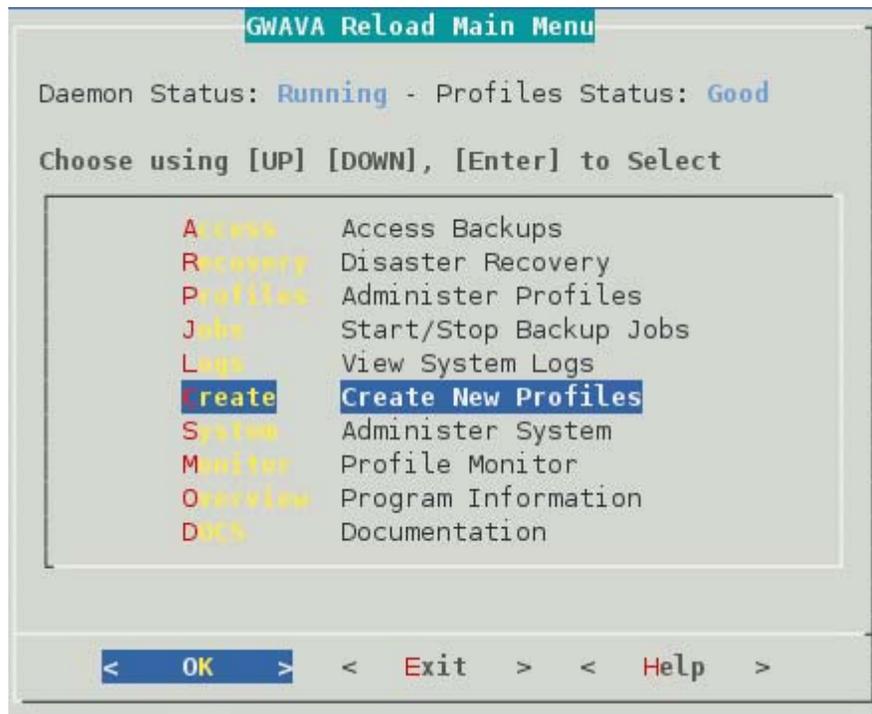
6. Create a directory for the backup data. For example:

```
mkdir /reload
```

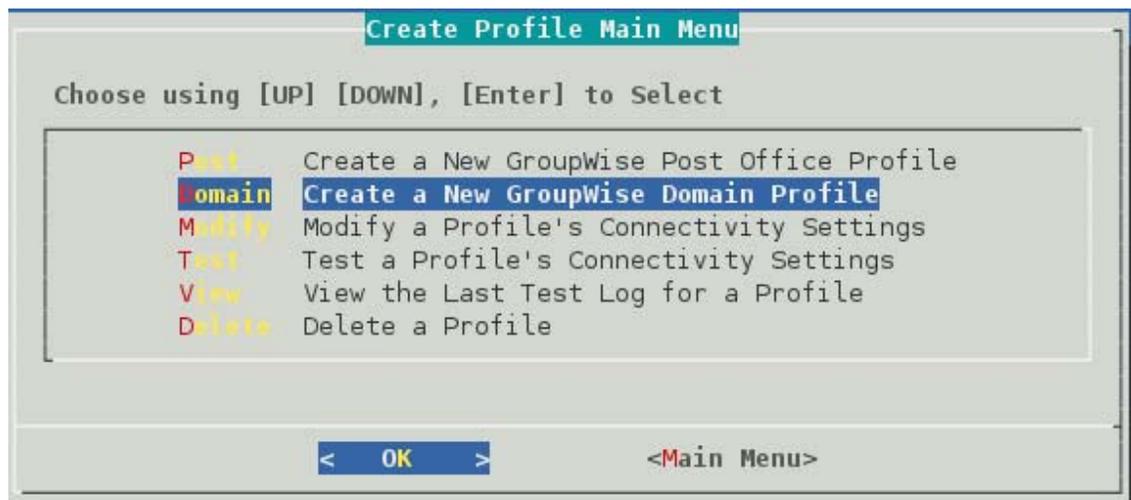
7. Start the GroupWise Disaster Recovery Administration Console by typing on the command line:

```
reload
```

8. Select "Create (Create Profile)"



9. Select "Domain (Create a New GroupWise Domain Profile)"



10. Give the Profile a Name. The profile name should not exceed eight characters. Use letters and numbers only, no spaces or other characters. For example: Domain Be aware, that a profile cannot be renamed, once it has been created. Choose the name wisely. Perhaps you will want to name the profile so that its name is the same as the GroupWise post office or domain that the profile represents, but it does not have to match. Select the Next button.

Profile Name

Choose < Next > to Accept

Use letters and numbers only, no spaces or other characters!

The profile name SHOULD NOT EXCEED 8 characters.

Enter the name of the profile in the field below:

DOMAIN

< Next > < Cancel >

11. Give the Profile a Description. The profile description should not exceed 60 characters and should not have comma(,), nor dollar sign(\$) characters. For example: Primary Domain. The description of the profile will be added to the Agent Log when backup jobs are run for the profile. Select the Next button.

Profile Description

Choose < OK > to Accept

The profile description should not exceed 60 characters.

NOTE: Do not use a comma or dollar sign (, \$) character.

Enter the profile description in the field below:

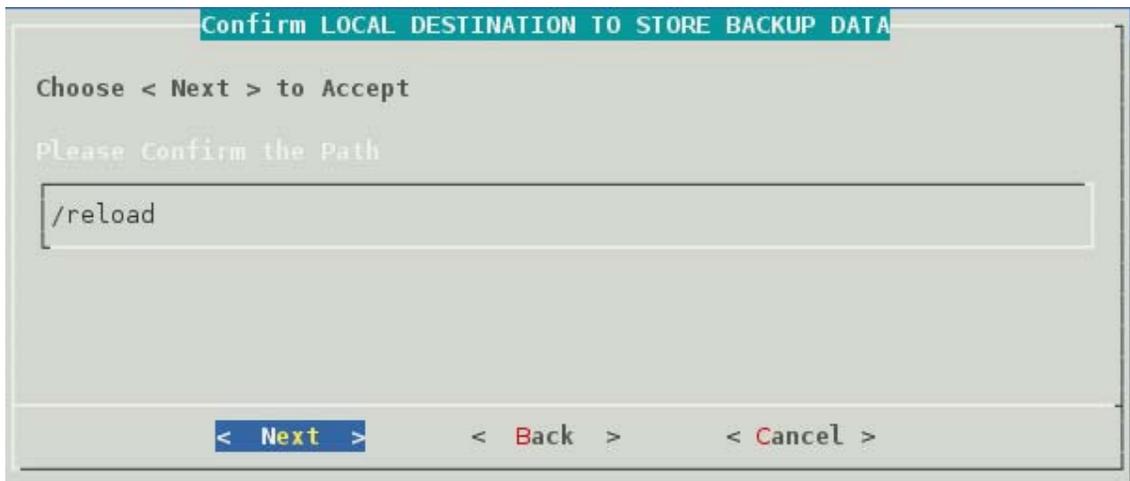
Primary Domain

< OK > < Cancel >

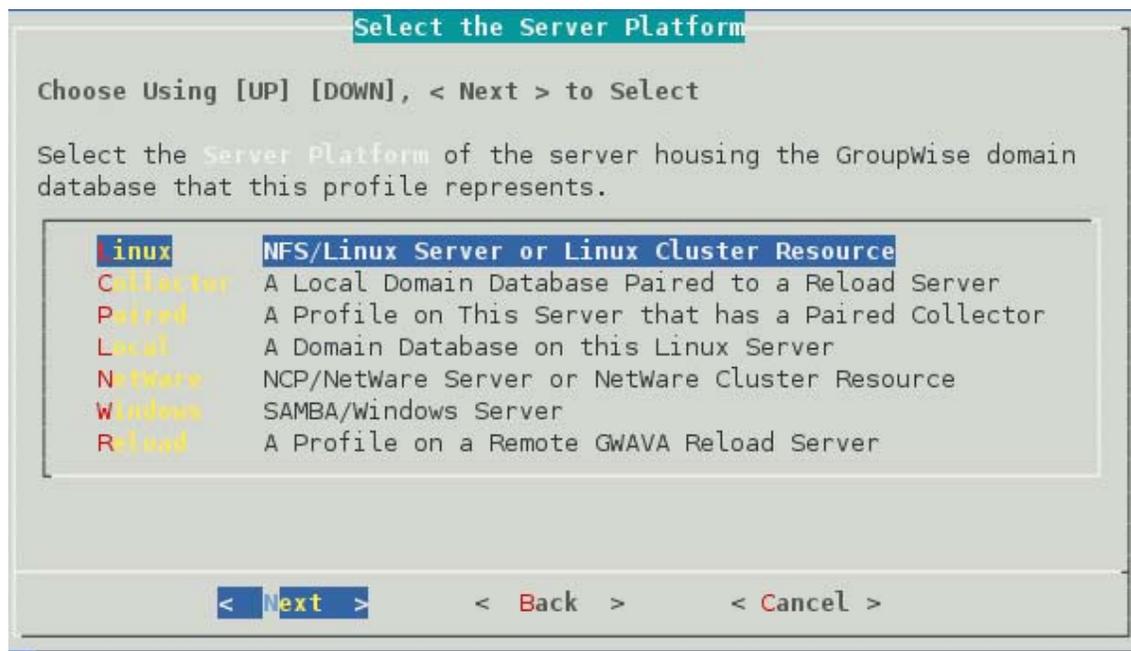
12. Enter the path or browse to the local destination directory to store the backup data. For example: /reload. This path can be a location on the Linux server, or an NFS mount to another Linux/Unix server, or to a SAN. The path should always be available; GroupWise Disaster Recovery is not configured to mount paths in order to access stored data. Also, the path should be to a location that has a lot of disk space available. Select the Next button.



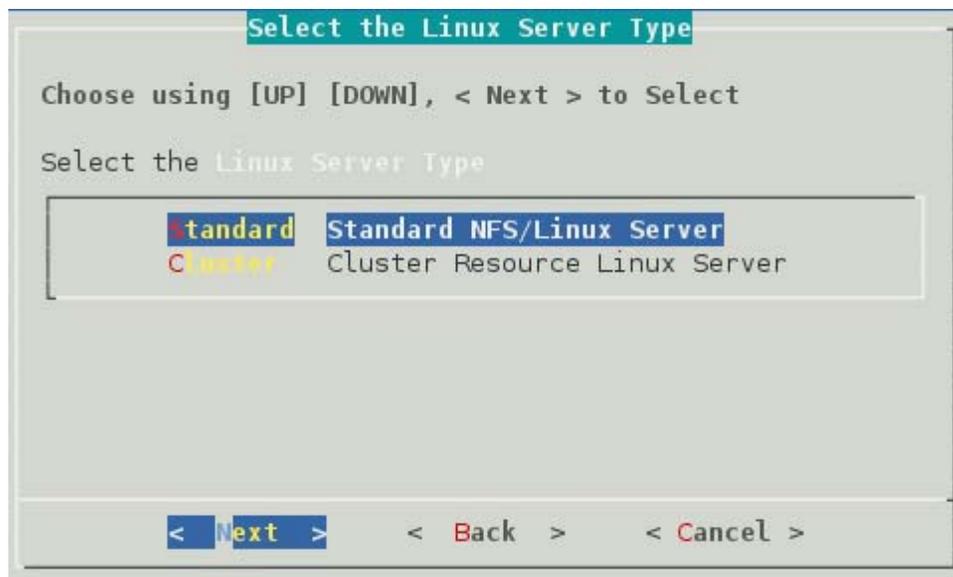
13. Confirm the path to the local destination directory



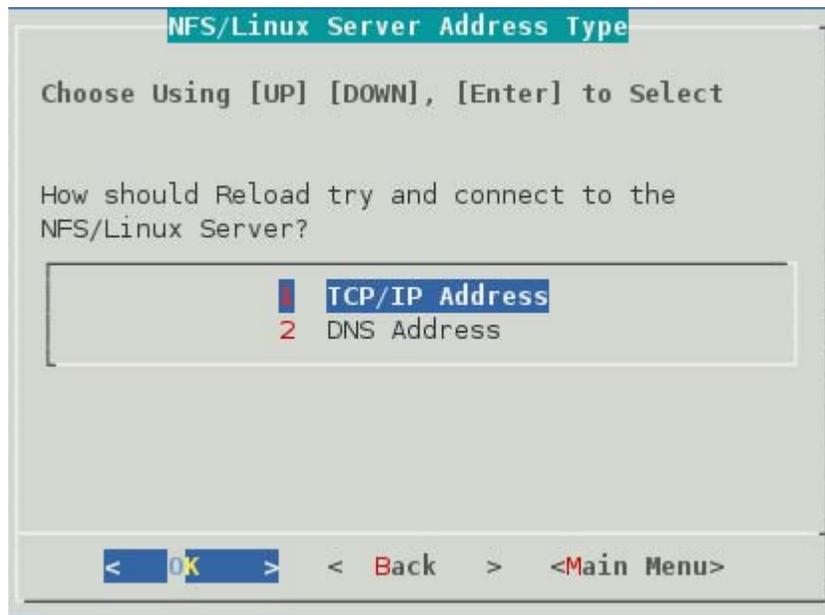
14. Select the Server Platform: "Linux (NFS/Linux Server or Linux Cluster Resource)"



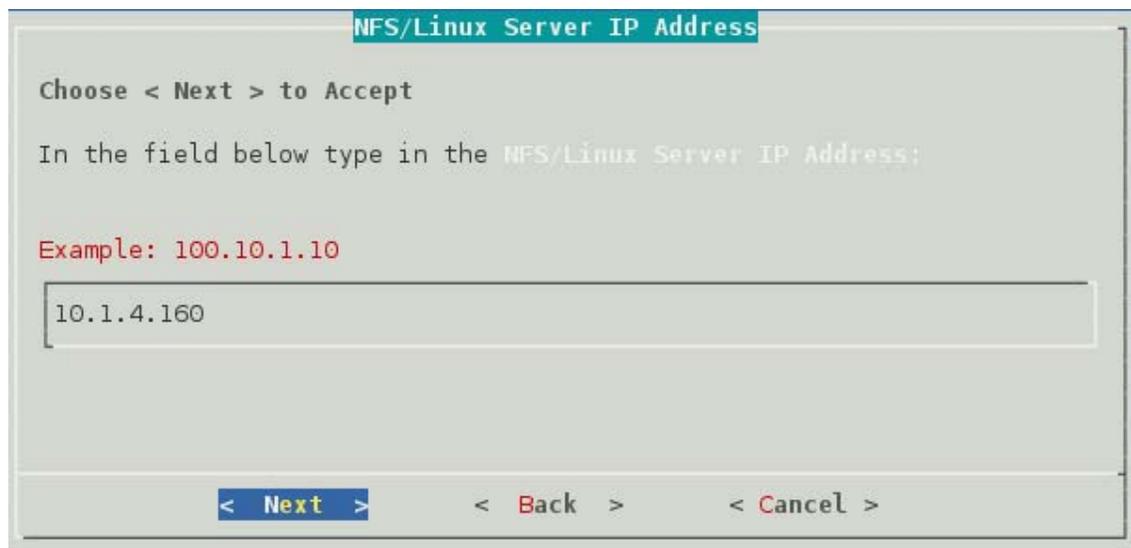
15. Select Linux Server Type: "Standard (Standard NFS/Linux Server)"



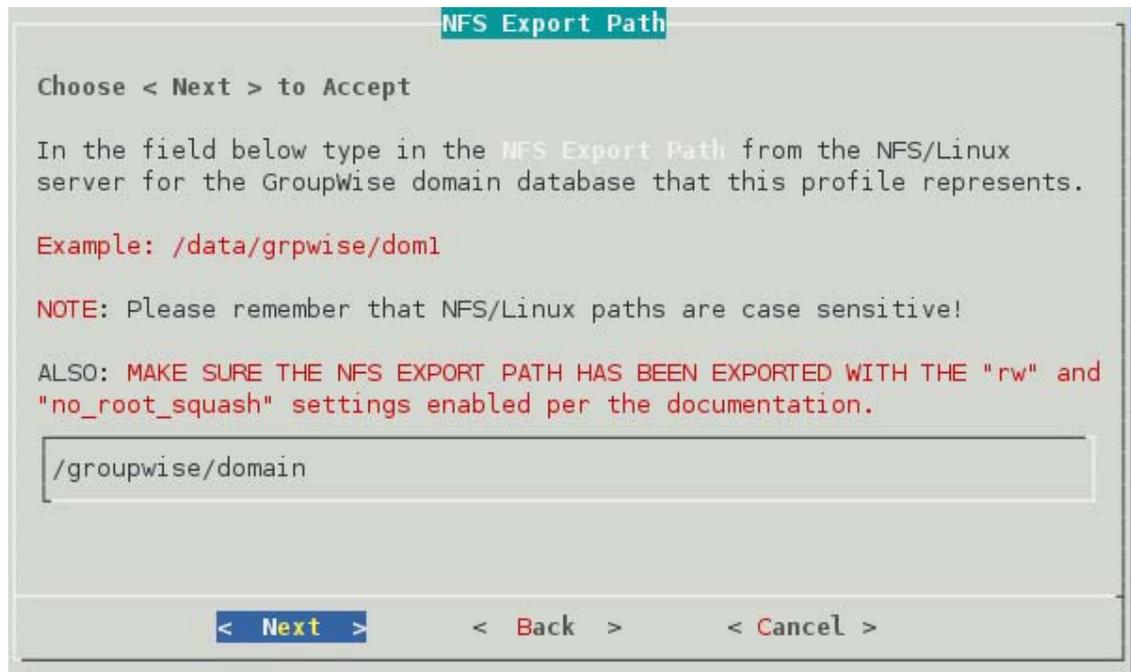
16. Select NFS/Linux Server Address Type: "1 (TCP/IP Address)" or "2 (DNS Address)"



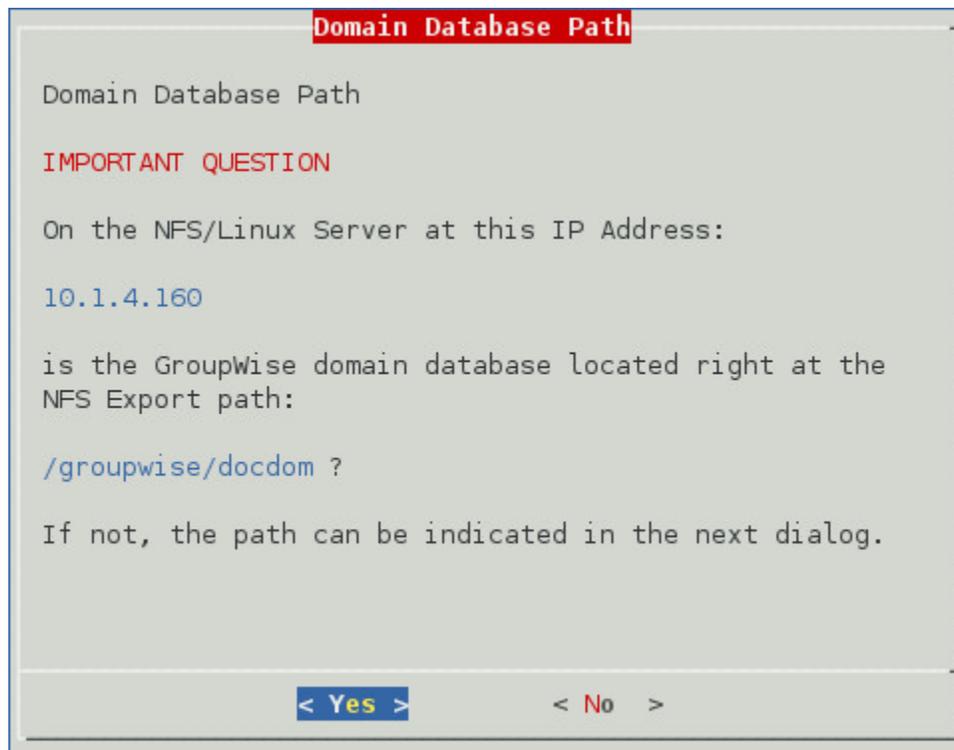
17. Enter the NFS/Linux Server IP Address or DNS hostname Address



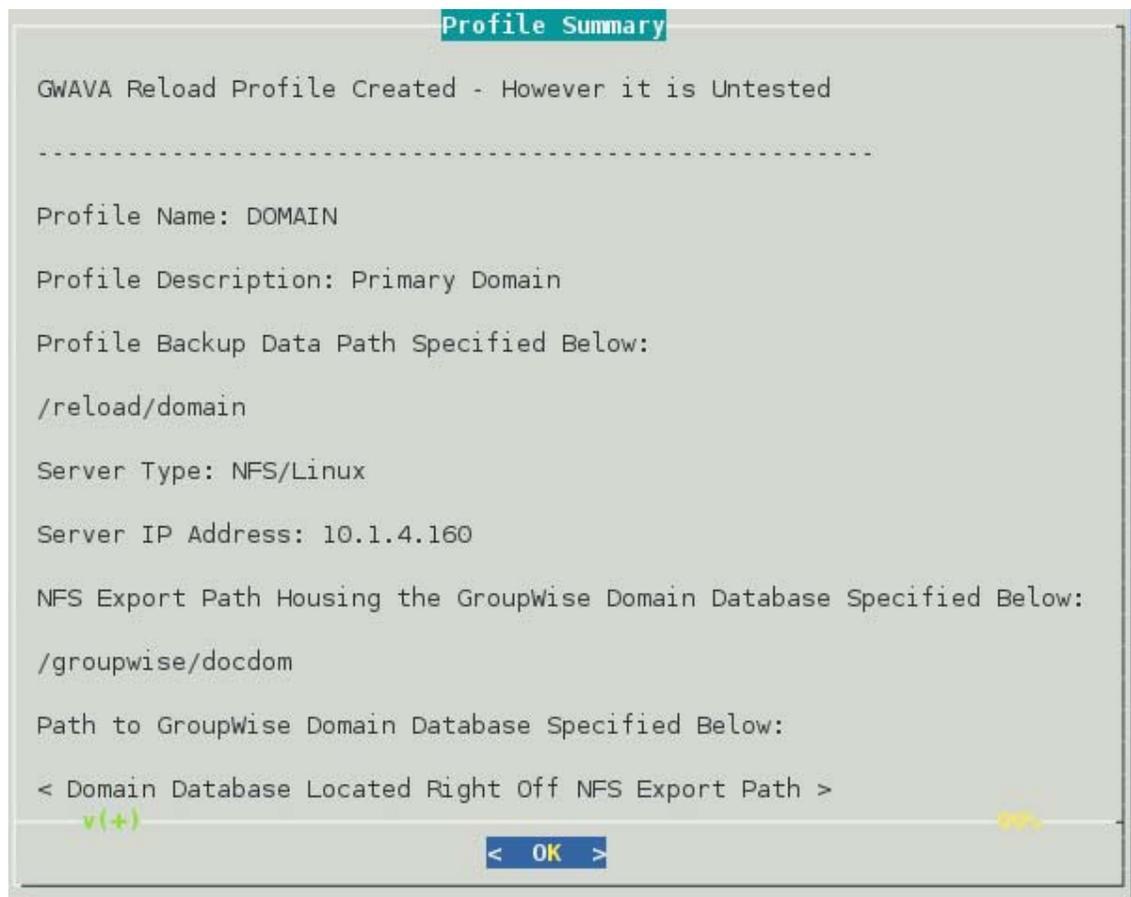
18. Enter the NFS Export Path on the GroupWise server from above. For example: /groupwise/domain



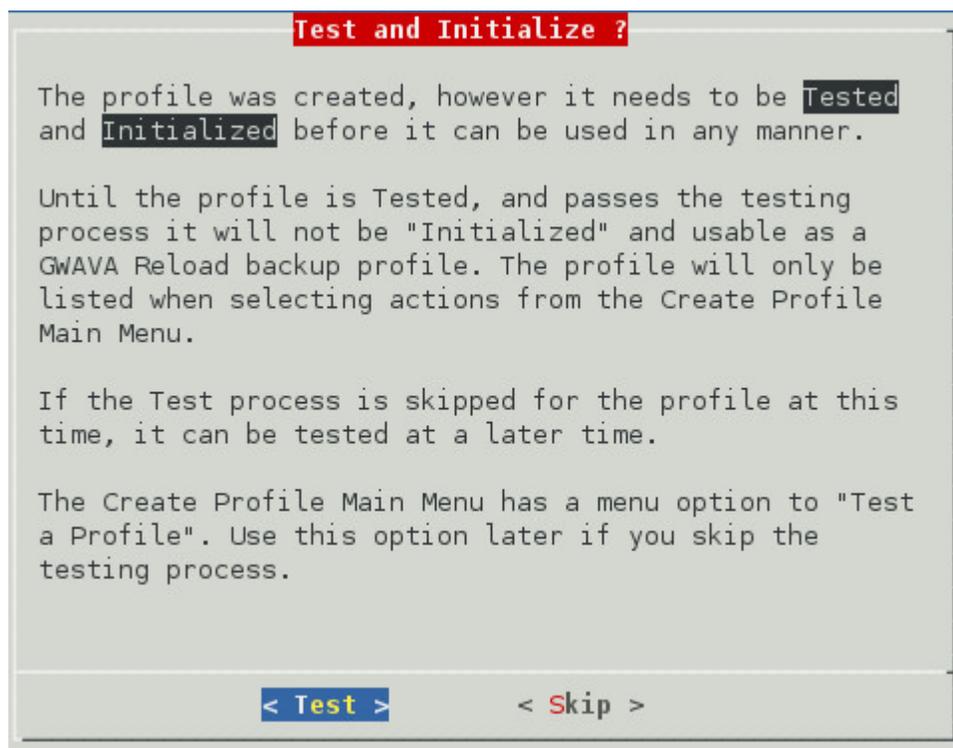
19. A warning page appears that asks if the IP Address and Export path are correct.



20. A Profile Summary page appears



21. The Test and Initialize page allows you to finalize the profile by selecting Test.



22. If the configuration is incorrect, select Skip and makes your changes.
23. Run the test and it will indicate success or failure.



```
GWAVA ReLoad Test and Initialize Utility
A Standard Backup Job Schedule will be created.

Tue Mar 14 11:18:57 MDT 2017

SUCCESS, THE PROFILE: DOMAIN IS NOW ENABLED.

< Exit >
```

Creating Server Only Post Office Profiles

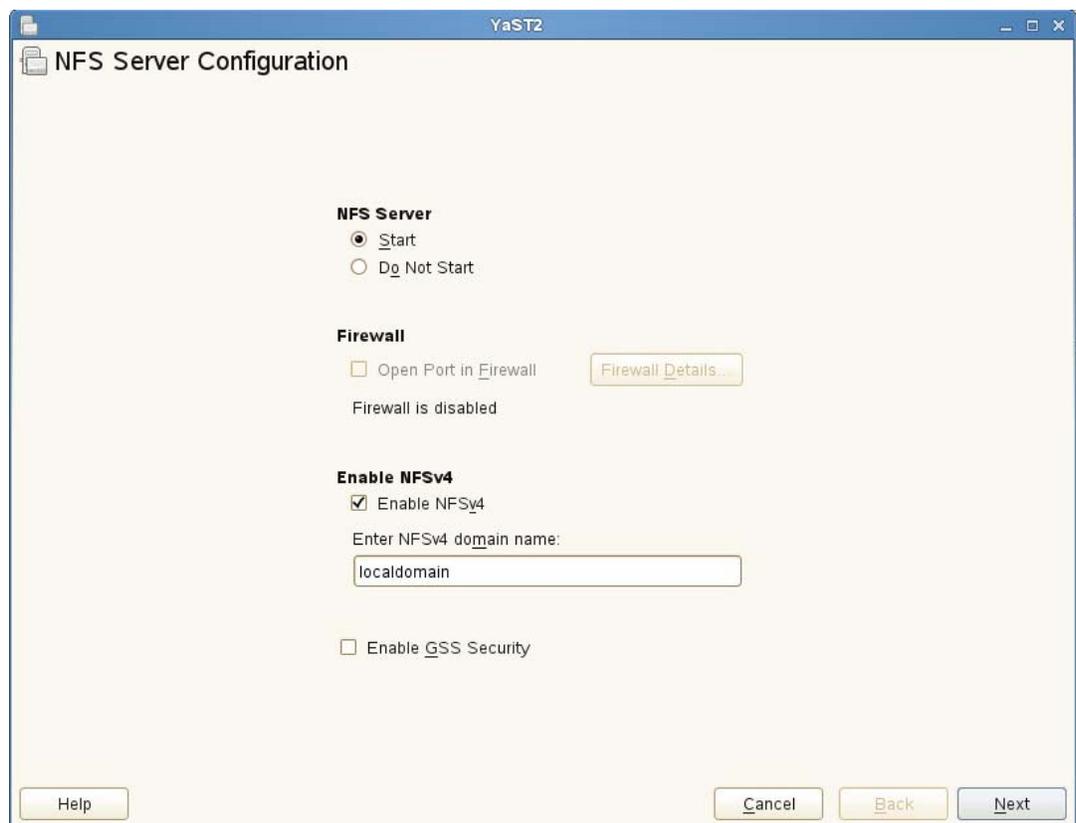
Post Office Profile: Server Only Model

On the GroupWise server, create an NFS mount. Each domain and post office must receive their own mount points.

1. Start YaST2
2. Install NFS Server

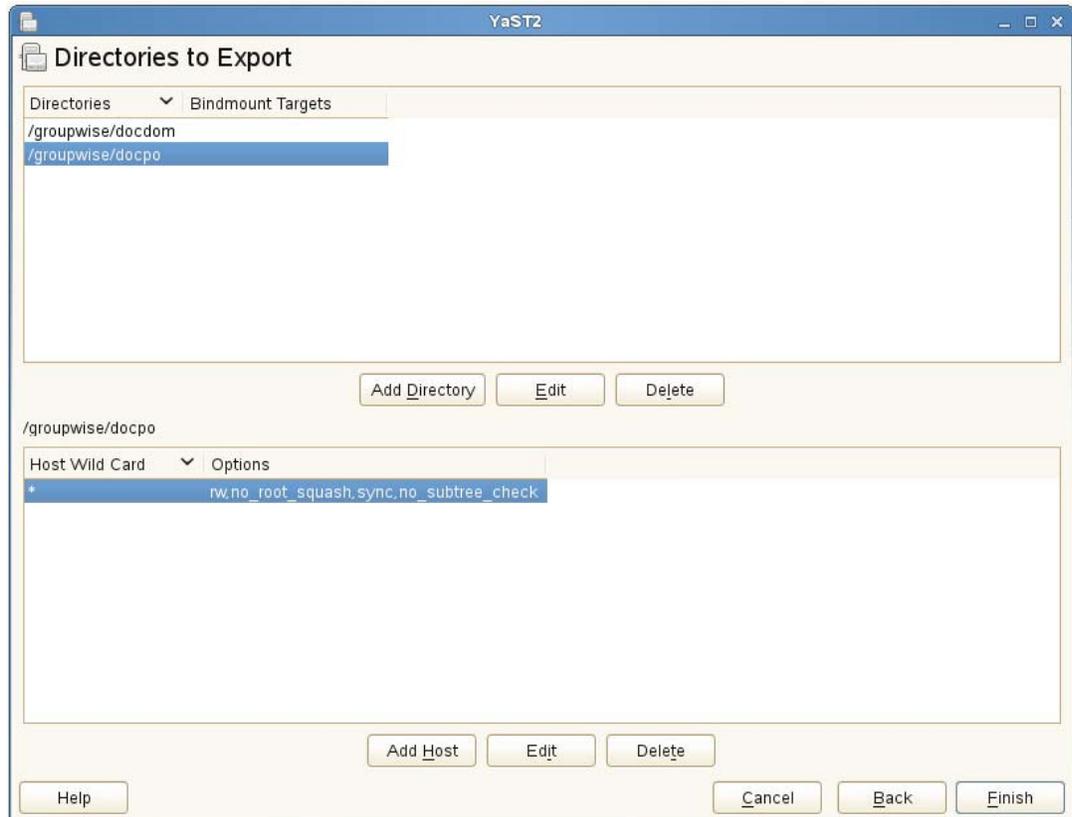


3. Configure NFS Server:
 - a. Set NFS Server to start
 - b. Open the port in the firewall, if applicable.



4. Add Directory:
 - a. Browse to the Post Office directory. For example /groupwise/po

- b. Set options to: *rw,no_root_squash,sync*



5. Press Finish to complete setup.

On the GroupWise Disaster Recovery server, create a data directory and a profile

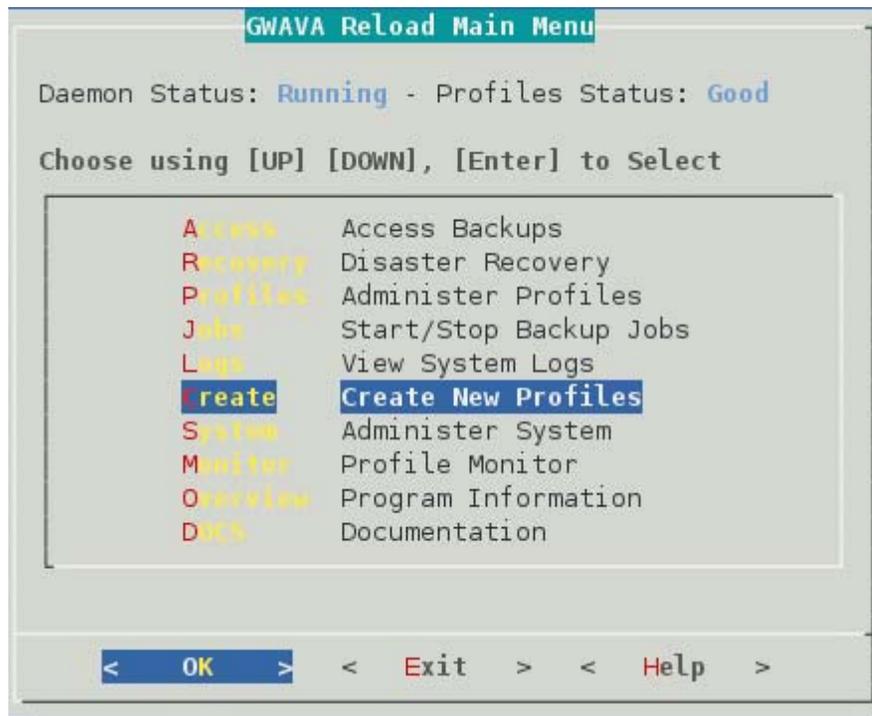
6. Create a directory for the backup data, if necessary. For example:

```
mkdir /reload
```

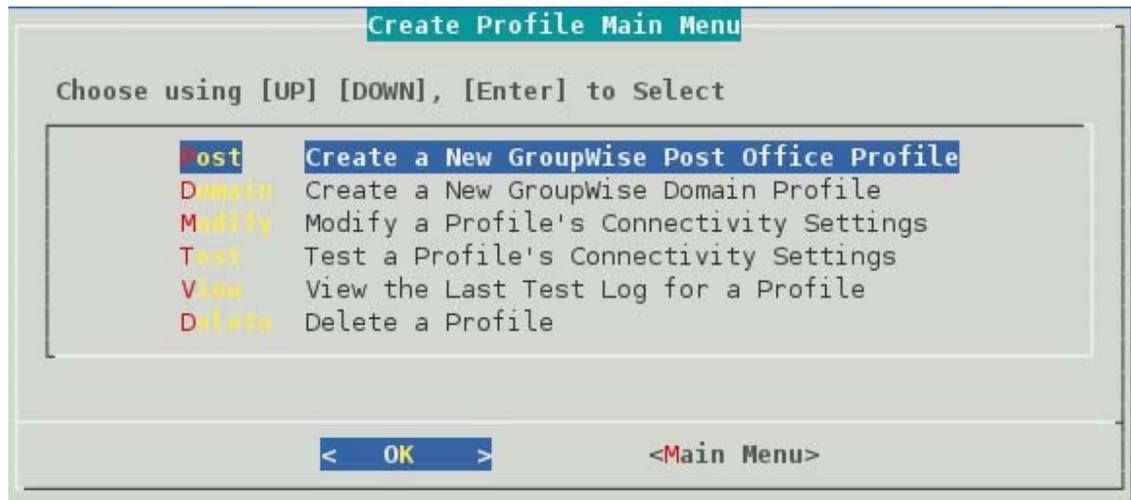
7. Start the GroupWise Disaster Recovery Administration Console by typing on the command line:

```
reload
```

8. Select "Create (Create Profile)"



9. Select "Post (Create a New GroupWise Post Office Profile)"



10. Give the Profile a Name. The profile name should not exceed eight characters. Use letters and numbers only, no spaces or other characters. For example: Post Office. Be aware, that a profile cannot be renamed, once it has been created. Choose the name wisely. Perhaps you will want to name the profile so that its name is the same as the GroupWise post office or domain that the profile represents, but it does not have to match. Select the Next button.

Profile Name

Choose < Next > to Accept

Use letters and numbers only, **no spaces or other characters!**

The profile name **SHOULD NOT EXCEED 8 characters.**

Enter the name of the profile in the field below:

< **Next** > < Cancel >

11. Give the Profile a Description. The profile description should not exceed 60 characters and should not have comma(,), nor dollar sign(\$) characters. For example: Primary Post Office. The description of the profile will be added to the Agent Log when backup jobs are run for the profile. Select the Next button.

Profile Description

Choose < OK > to Accept

The profile description should not exceed 60 characters.

NOTE: Do not use a comma or dollar sign (, \$) character.

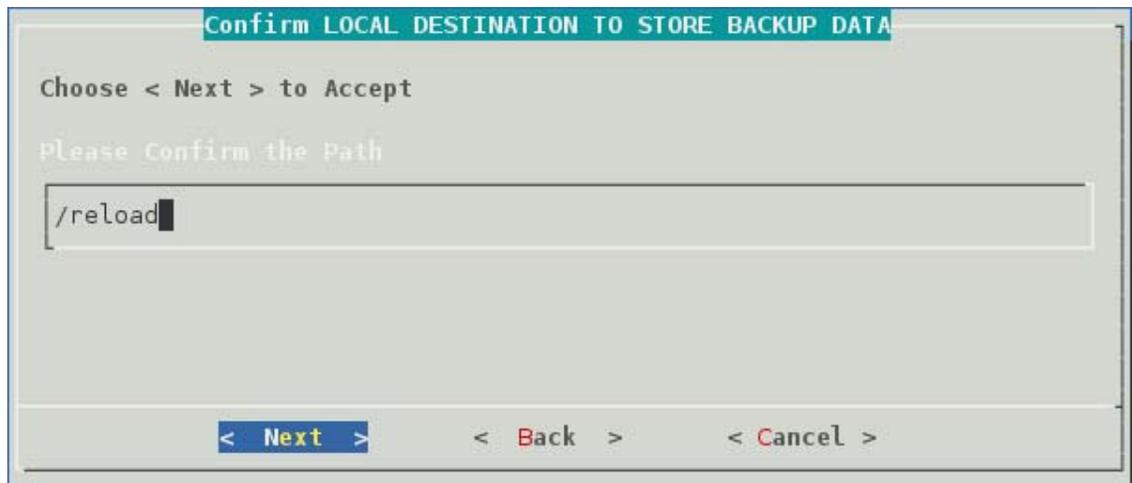
Enter the profile description in the field below:

< **OK** > < Cancel >

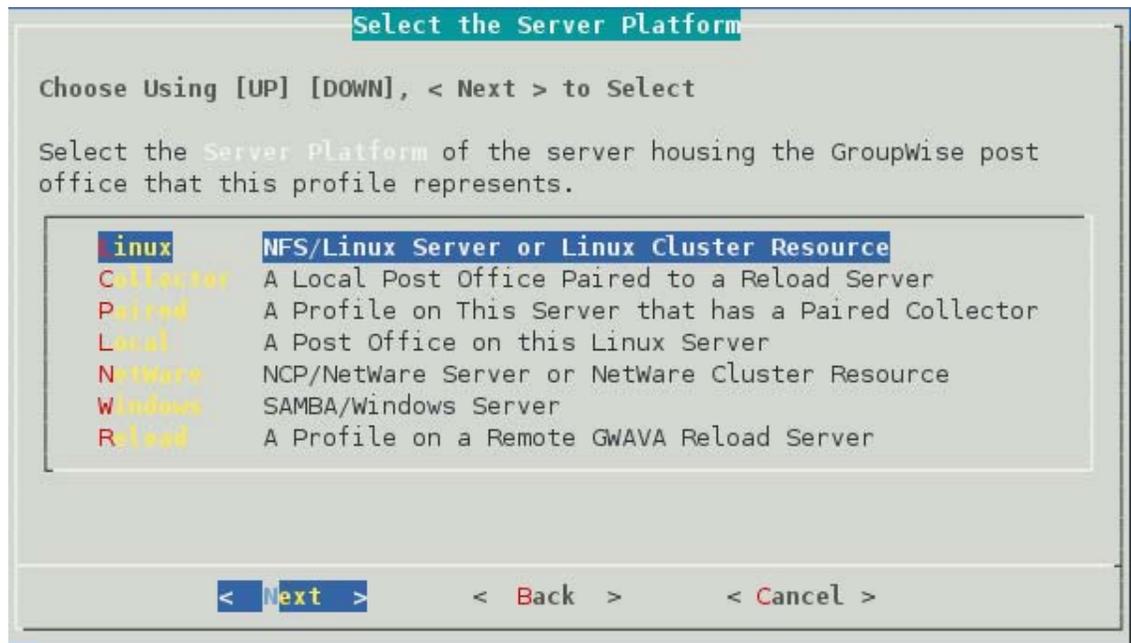
12. Enter the path or browse to the local destination directory to store the backup data. For example: /reload. This path can be a location on the Linux server, or an NFS mount to another Linux/Unix server, or to a SAN. The path should always be available; GroupWise Disaster Recovery is not configured to mount paths in order to access stored data. Also, the path should be to a location that has a lot of disk space available. Select the Next button.



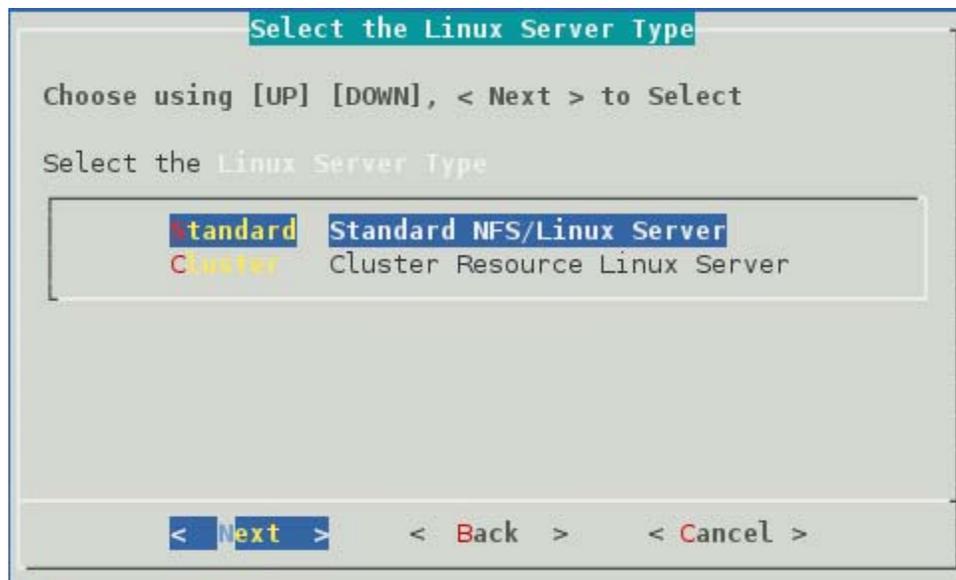
13. Confirm the path to the local destination directory



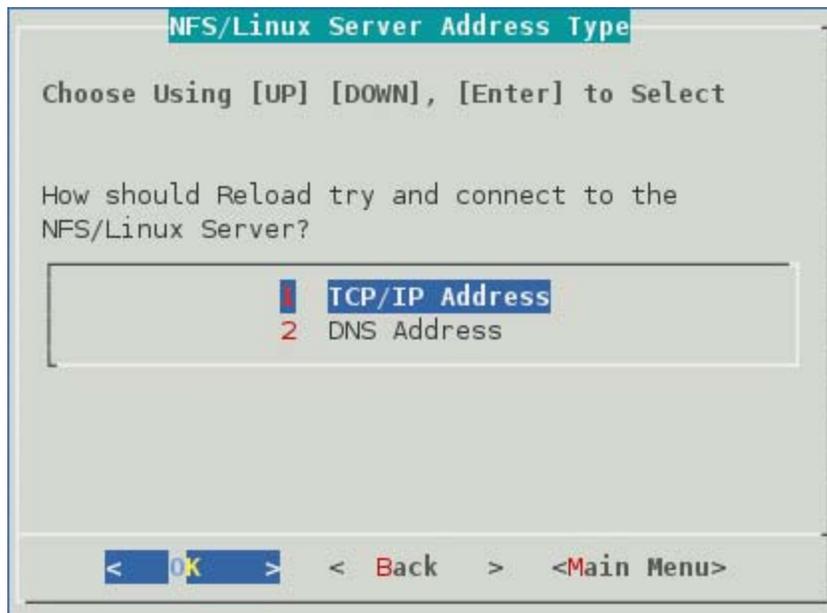
14. Select the Server Platform: "Linux (NFS/Linux Server or Linux Cluster Resource)"



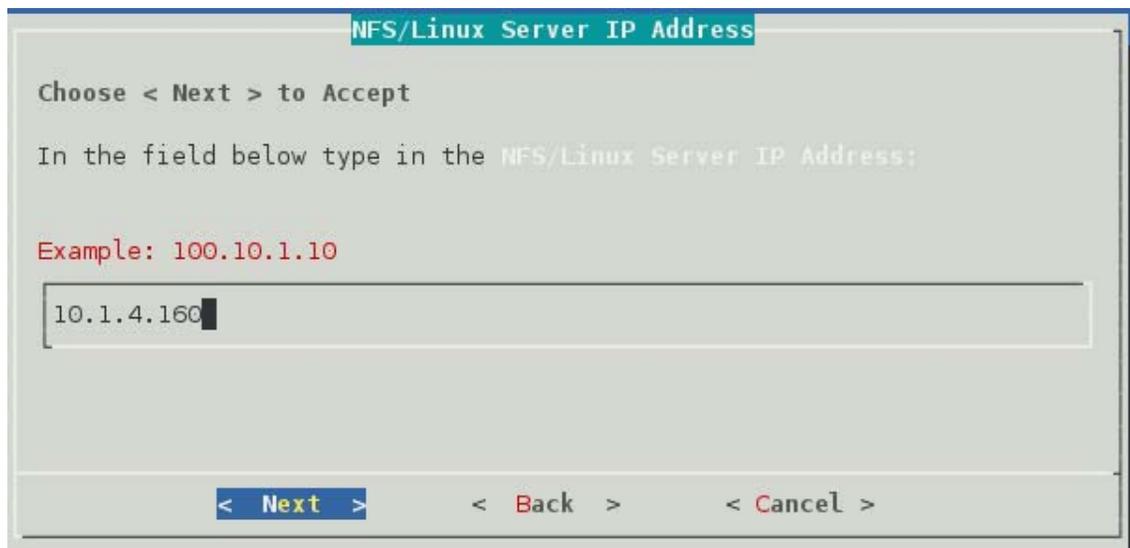
15. Select Linux Server Type: "Standard (Standard NFS/Linux Server)"



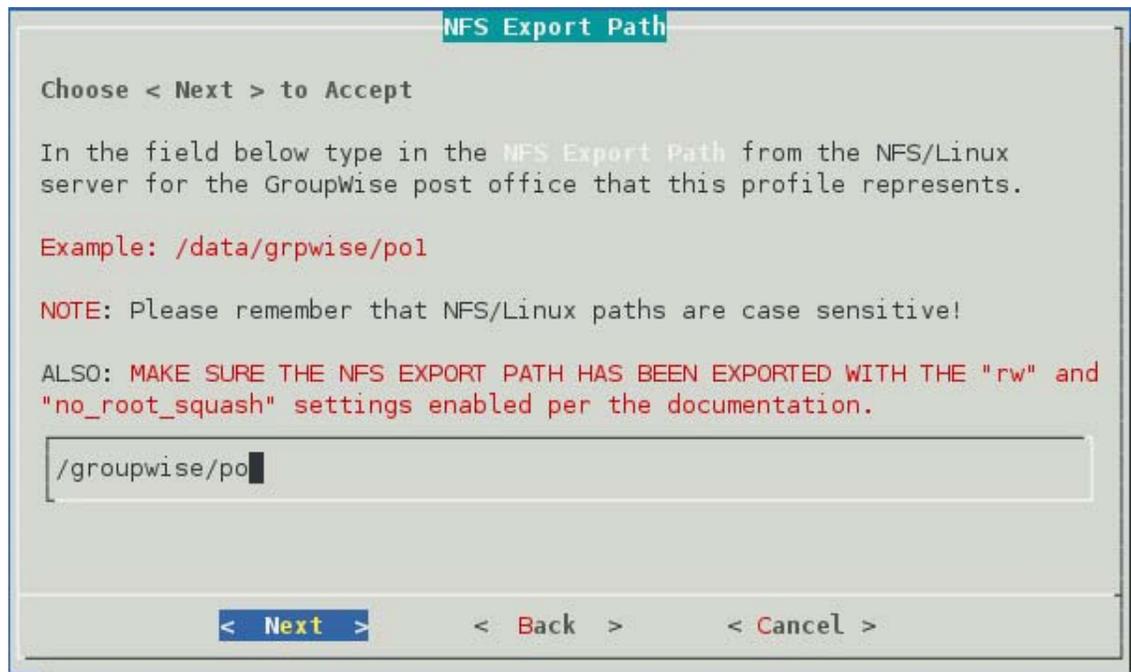
16. Select NFS/Linux Server Address Type: "1 TCP/IP Address" or "2 DNS Address"



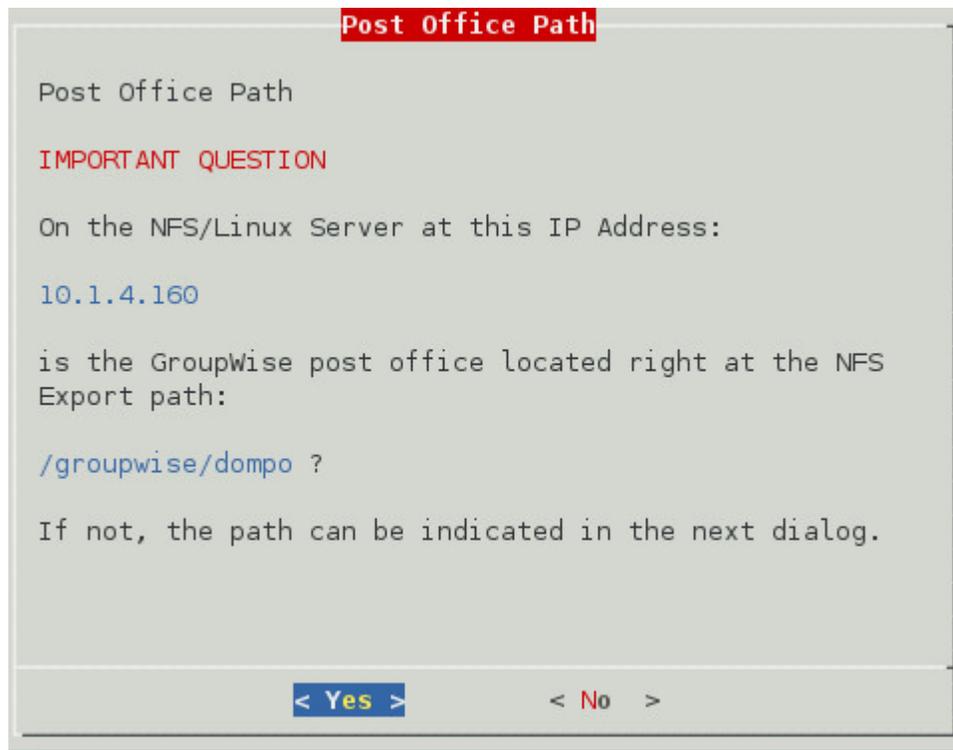
17. Enter the NFS/Linux Server IP Address or DNS Hostname



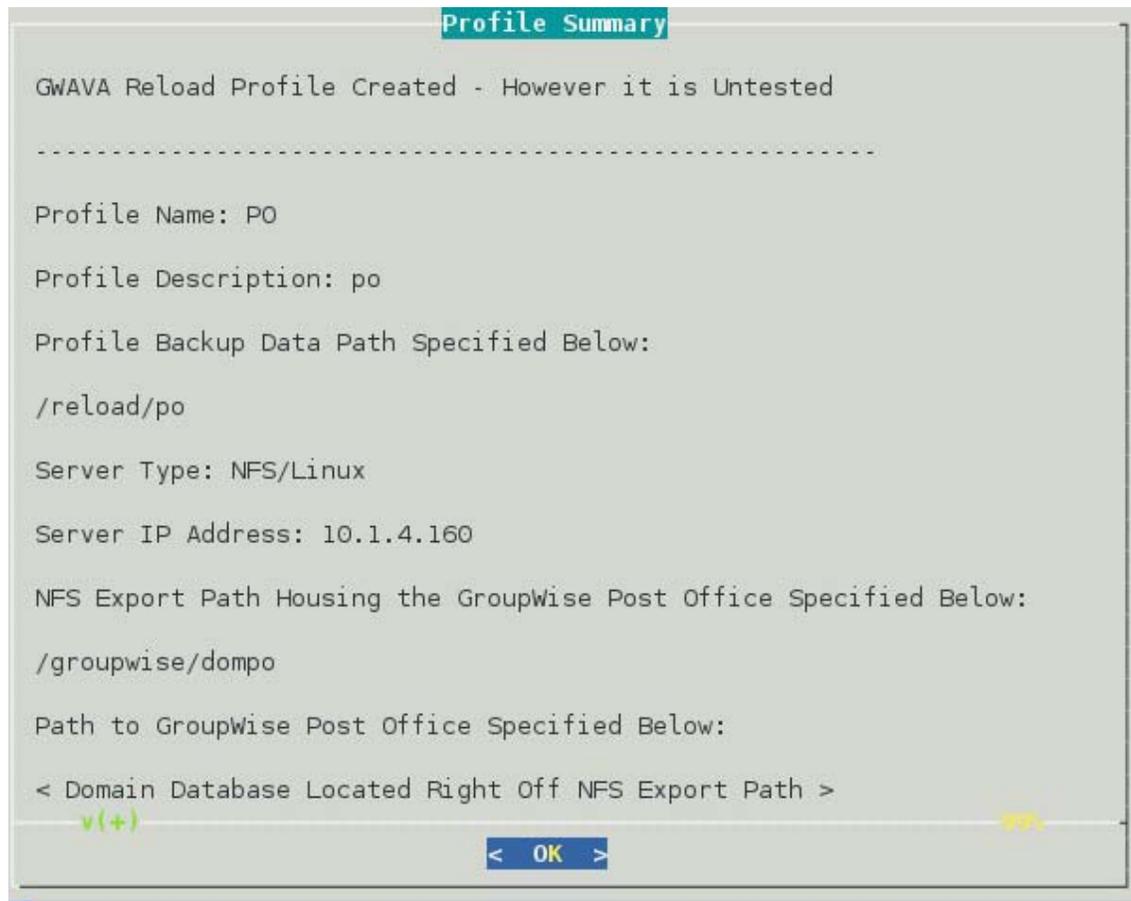
18. Enter the NFS Export Path on the GroupWise server from above. For example: /groupwise/po



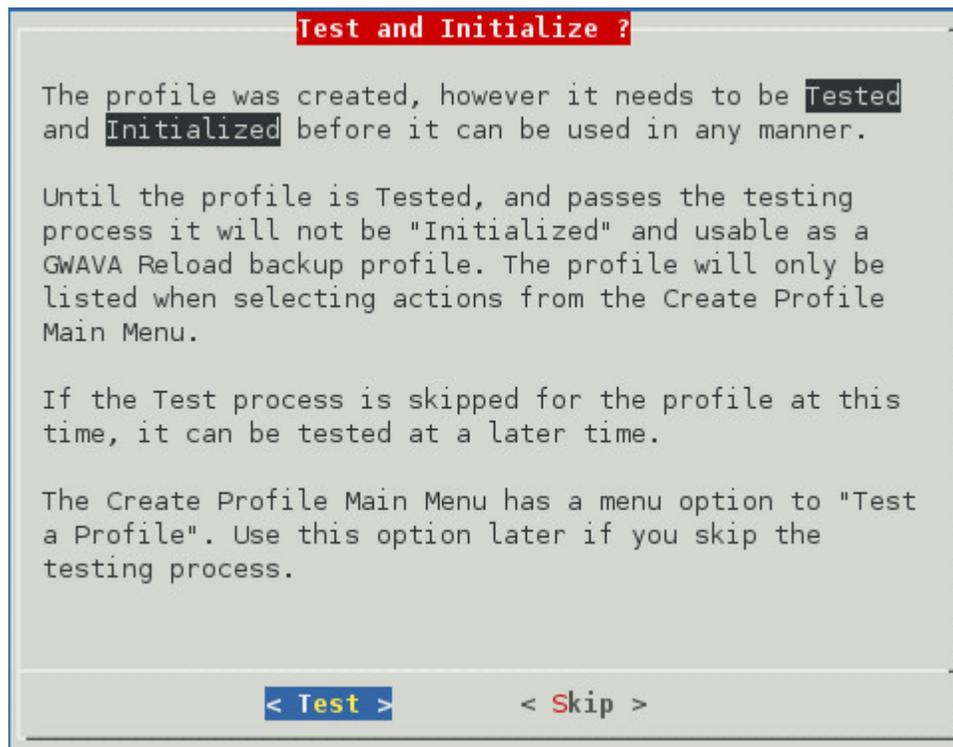
19. A warning page appears that asks if the IP Address and Export path are correct.



20. A Profile Summary page appears



21. The Test and Initialize page allows you to finalize the profile by selecting Test.



22. If the configuration is incorrect, select Skip and makes your changes.
23. Run the test and it will indicate success or failure.



```
GWAVA Reload Test and Initialize Utility
Finishing preparation steps on data copied from post office.

Tue Mar 14 12:41:58 MDT 2017

SUCCESS, THE PROFILE: PO IS NOW ENABLED.

< Exit >
```

GroupWise Cluster

Installing GroupWise Disaster Recovery in a GroupWise Cluster

GroupWise Disaster Recovery can be implemented where GroupWise is in a cluster.

When GroupWise is implemented in a cluster there are a few extra steps needed to configure GroupWise Disaster Recovery to operate successfully.

In this example there are three servers:

- ◆ GroupWise Disaster Recovery Server
- ◆ GroupWise Cluster Node 1 (NODE1)
- ◆ GroupWise Cluster Node 2 (NODE2)

Installation Collector/Server Model

On the GroupWise Disaster Recovery Server

Install GroupWise Disaster Recovery on the GroupWise Disaster Recovery server

Create a Post Office Profile for the Post Office on the GroupWise Cluster

If upgrading a standard server model profile to a Collector/Server model profile:

In GroupWise Disaster Recovery Web Administration, choose the profile and go to the Configure tab for the profile.

Select the Post Office and POA Settings panel

Find the line Note: Disk Space Required for Collector

Check on each node that there is sufficient space for the collector and data on each node. Note: This calculation does not take Document Management Libraries into account. If you wish to add DMS, multiple the size of the GWDMS directory structure by 2.

Set "Allow Paired Collector" to Enabled

On GroupWise Cluster Node 1 (NODE1)

Install the GroupWise Disaster Recovery Collector Software on NODE1

Browse to the GroupWise Disaster Recovery Server and select the appropriate collector software from the Tools dropdown menu and select go, or copy the software from the GroupWise Disaster Recovery server found in the directory:

```
/opt/beginfinite/reload/setup/collector/reload_collector.rpm
```

Run the following command from the terminal:

```
rpm -ivh reload_collector.rpm
```

Exchange SSH keys with the GroupWise Disaster Recovery Server

Run the following command from the terminal:

```
ssh-copy-id -i /root/.ssh/id_rsa.pub <address of the GroupWise Disaster Recovery Server>
```

This is to setup the ssh connection so NODE1 can rsync with GroupWise Disaster Recovery without being prompted for a password. This must be successful before proceeding.

Create a GroupWise Disaster Recovery Collector Profile

1. Run the following command from the terminal:

```
reload
```

2. Choose Create Profile
3. Select "Create (Create Profile)"
4. Select "Post Office (Create a New GroupWise Post Office Profile)"
5. Give the Profile a Name. The profile name should not exceed eight characters. Use letters and numbers only, no spaces or other characters. For example: po. Be aware, that a profile cannot be renamed, once it has been created. Choose the name wisely. Perhaps you will want to name the profile so that its name is the same as the GroupWise post office or domain that the profile represents, but does not have to match. Select the Next button.
6. Give the Profile a Description. The profile description should not exceed 60 characters and should not have comma(,), nor dollar sign(\$) characters. For example: Domain Collector. The description of the profile will be added to the Agent Log when backup jobs are run for the profile. Select the Next button.

7. Enter the path or browse to the local destination directory to store the backup data. For example: /reload. This path can be a location on the Linux server, or an NFS mount to another Linux/Unix server, or to a SAN. The path should always be available; GroupWise Disaster Recovery is not configured to mount paths in order to access stored data. Also, the path should be to a location that has a lot of disk space available. Select the Next button.
8. Confirm the path to the local destination directory
9. Choose the server type: "Collector (A Local Post Office/Domain Paired to a GroupWise Disaster Recovery Server)". Select the Next button.
10. Enter the TCP/IP Address or DNS hostname for the GroupWise Disaster Recovery server this collector will be paired with. Select the Next button.
11. A terminal session will appear to prompt you to accept an SSH key and enter the password for the GroupWise Disaster Recovery server.
12. Enter the SSH port used by the GroupWise Disaster Recovery server (default port: 22)
13. Enter the destination path the data will be stored in on the GroupWise Disaster Recovery server. This is the destination directory you entered when creating the Paired Server on the GroupWise Disaster Recovery server.
14. Source Path to the GroupWise files: Enter the source path to the local destination directory entered earlier on the GroupWise server. For example: /groupwise/po
15. Confirm the path to the local source directory
16. A summary of the profile settings will appear. Select the OK button.
17. Test and Initialization:
 - If the profile is correct, select the Test button.
 - If the profile is not correct, select the Skip button.
18. The profile creation wizard tests and initializes the newly created profile and prepares it to accept a pairing request from a Paired Collector and initializes the newly created profile and prepares it to accept a pairing request from a Paired Collector.

Browse to the GroupWise Disaster Recovery Web Administration page on NODE1. For example, <http://NODE1:5555>.

1. Choose the profile being configured
2. Select the Configure tab and open the GroupWise Disaster Recovery Collector Settings panel
3. Set "This Collector is on a Cluster Node" to Enabled
4. Select the Backups tabs, open the Reload Job Control panel and click on "Start a Standard Backup Job [SmartPurge Disabled]" to run a backup job, allow the backup to complete normally.

On GroupWise Cluster Node 2 (NODE2)

Profile settings are not shared across the cluster automatically, this needs to be done manually when setting up or when settings are changed.

1. Install the GroupWise Disaster Recovery Collector Software on NODE1
 - a. Browse to the GroupWise Disaster Recovery Server and select the appropriate collector software from the Tools dropdown menu and select go, or copy the software from the GroupWise Disaster Recovery server found in the directory: /opt/beginfinite/reload/setup/collector/reload_collector.rpm
 - b. Run the following command from the terminal: `rpm -ivh reload_collector.rpm`

2. Exchange SSH keys with the GroupWise Disaster Recovery Server
 - a. Run the following command from the terminal: `ssh-copy-id -i /root/.ssh/id_rsa.pub <address of the GroupWise Disaster Recovery Server>`
 - b. This is to setup the ssh connection so NODE1 can rsync with GroupWise Disaster Recovery without being prompted for a password. This must be successful before proceeding.
3. Obtain the following files from NODE1 and copy them to the same directories on NODE2
 - a. The contents of the `/opt/beginfinite/reload/conf` directory (including the `../conf/cron` directory)
 - b. The license file `/opt/beginfinite/reload/license/reload.pem`
4. Restart the GroupWise Disaster Recovery daemon on NODE2 with the following command:
`reload restart`
5. Browse to the GroupWise Disaster Recovery Web Administration page on NODE2. For example, `http://NODE2:5555`.
 - a. Select the Backups tabs, open the Reload Job Control panel and click on "Start a Standard Backup Job [SmartPurge Disabled]" to run a backup job.
 - b. This backup should "fail"

In the Event Log the failure will look like:

```
DATE: Fri_Dec_11 TIME: 14:57:25 PROFILE: COLLECT1 - STARTING JOB FOR PROFILE: COLLECT1
```

```
DATE: Fri_Dec_11 TIME: 14:57:25 PROFILE: COLLECT1 - DISK SPACE IN USE AT JOB BEGINNING: 46%
```

```
DATE: Fri_Dec_11 TIME: 14:57:25 PROFILE: COLLECT1 - JOB TYPE: COLLECTOR (INCREMENTAL) BACKUP
```

```
DATE: Fri_Dec_11 TIME: 14:57:25 PROFILE: COLLECT1 - [GRE_DBS_AGENTS] Start Database Backup
```

```
DATE: Fri_Dec_11 TIME: 14:57:34 PROFILE: COLLECT1 - [GRE_DBS_OFUSER] Start OFUSER Backup
```

```
DATE: Fri_Dec_11 TIME: 14:57:38 PROFILE: COLLECT1 - [GRE_DBS] Terminating Processing, Post Office Volume for Profile Not Mounted.
```

```
DATE: Fri_Dec_11 TIME: 14:57:38 PROFILE: COLLECT1 - [GRE_DBS] This must not be the active node for the Post Office
```

On NODE1 & NODE2

Only the GroupWise Disaster Recovery server requires Backup Age monitoring

1. Disable Backup Age Monitoring
 - a. Browse to the GroupWise Disaster Recovery Web Administration page on each node
 - b. Go to the Collector Profile, under the Configure tab, open the Preferences panel
 - i. Under Backup Age Monitoring, set "Monitor How Old the Most Current Backup Is" to Disabled

Upgrading Collectors in a Cluster

Clusters are a bit of a challenge to work with as an inactive node does not do anything since it is inactive, therefore you will have to upgrade each node manually.

1. Browse to the GroupWise Disaster Recovery Server and select the appropriate collector software from the Tools dropdown menu and select Go, or copy the software from the GroupWise Disaster Recovery server found in the directory: `/opt/beginfinite/reload/setup/collector/reload_collector.rpm`
2. Place the file on each "inactive" node in: `/opt/beginfinite/reload/upgrade`
3. Upgrade the GroupWise Disaster Recovery Collector software from the terminal by running the command: `reloadu`

Configure Restore Area on Linux

Once a backup has been created the link to the Restore Area can be made.

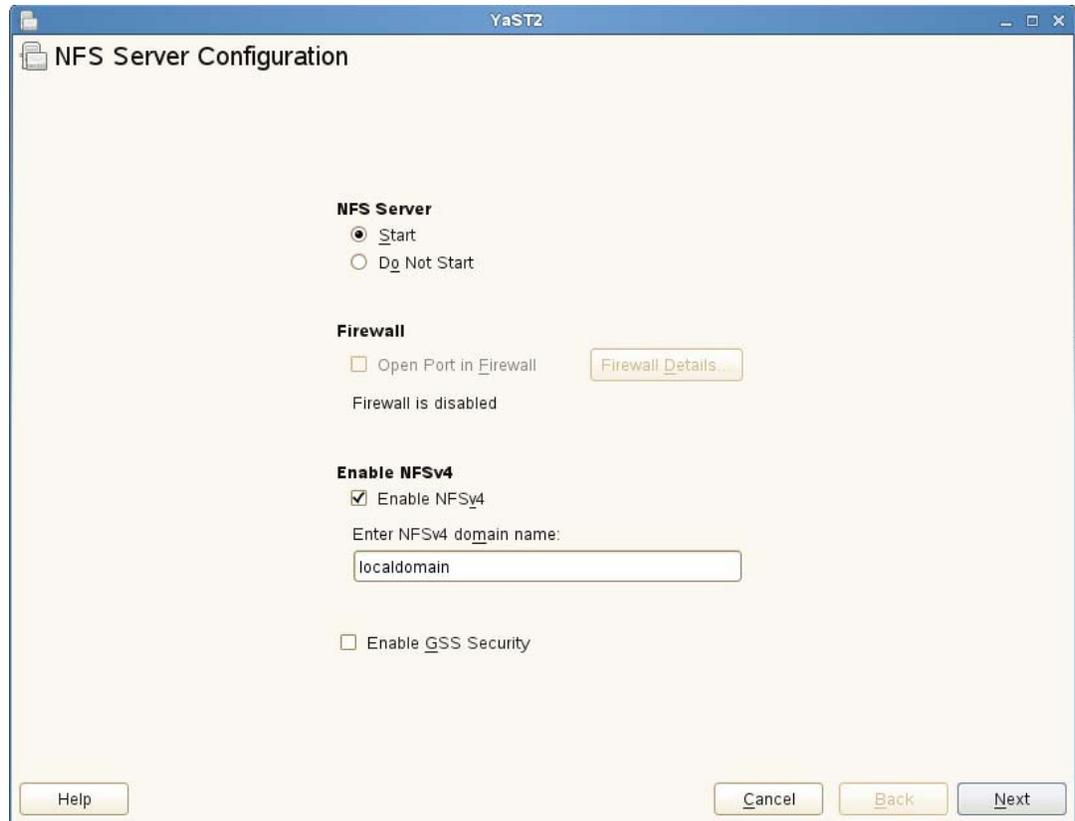
On the GroupWise Disaster Recovery Server, enable NFS Server

1. Open YaST2 and select *Network Services | NFS Server*

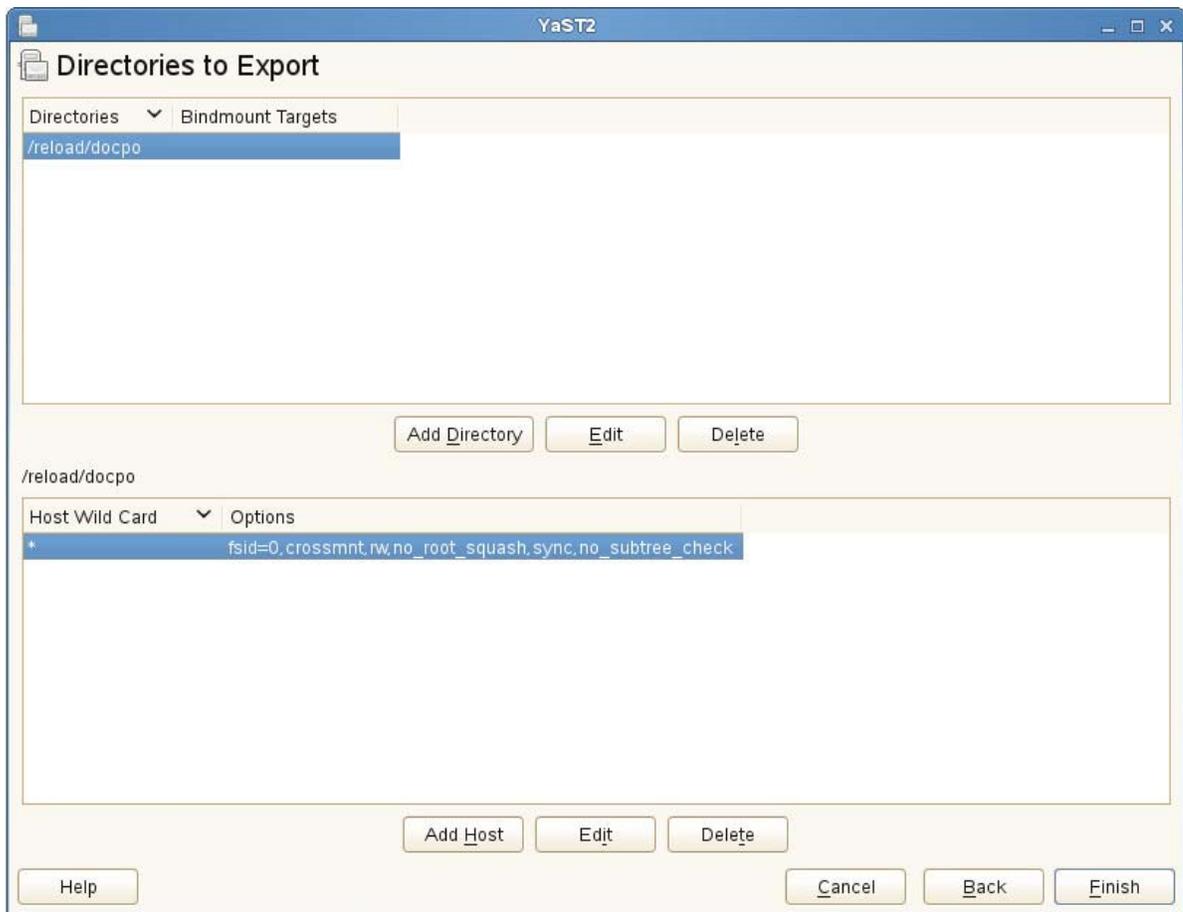


2. Configure NFS Server:
 - a. Set NFS Server to start

- b. Open the port in the firewall, if applicable.



3. Select Add Directory button:
 - a. Set options: *rw,no_root_squash,sync*
 - b. Browse to the post office backup directory. For example: */reload/po*



On the Linux GroupWise Server

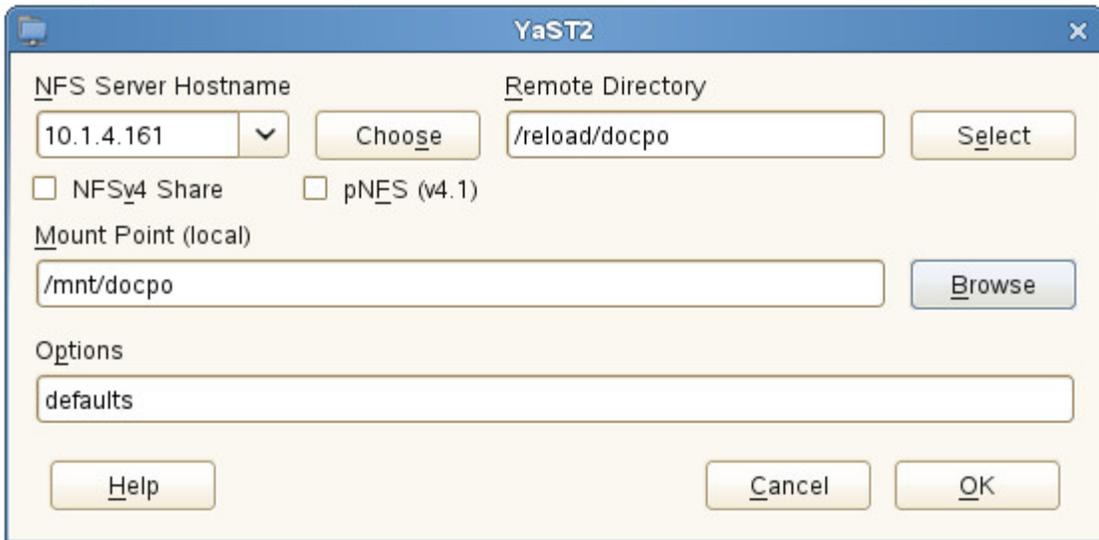
Create a mount point:

1. Open a terminal window
2. Create a local directory for the mount point. Generally, this is placed in the /mnt directory. For example:

```
mkdir /mnt/restore
```

Enable NFS Client:

1. Open YaST2 and select *Network Services | NFS Client*
2. Click on *Add*
 - ◆ Set the NFS Server Hostname to the GroupWise Disaster Recovery server IP address or hostname
 - ◆ Set the Remote Directory to the backup directory on the GroupWise Disaster Recovery server. For example: /reload/po
 - ◆ Set the Mount Point to the one created on the GroupWise server



In GroupWise Administration

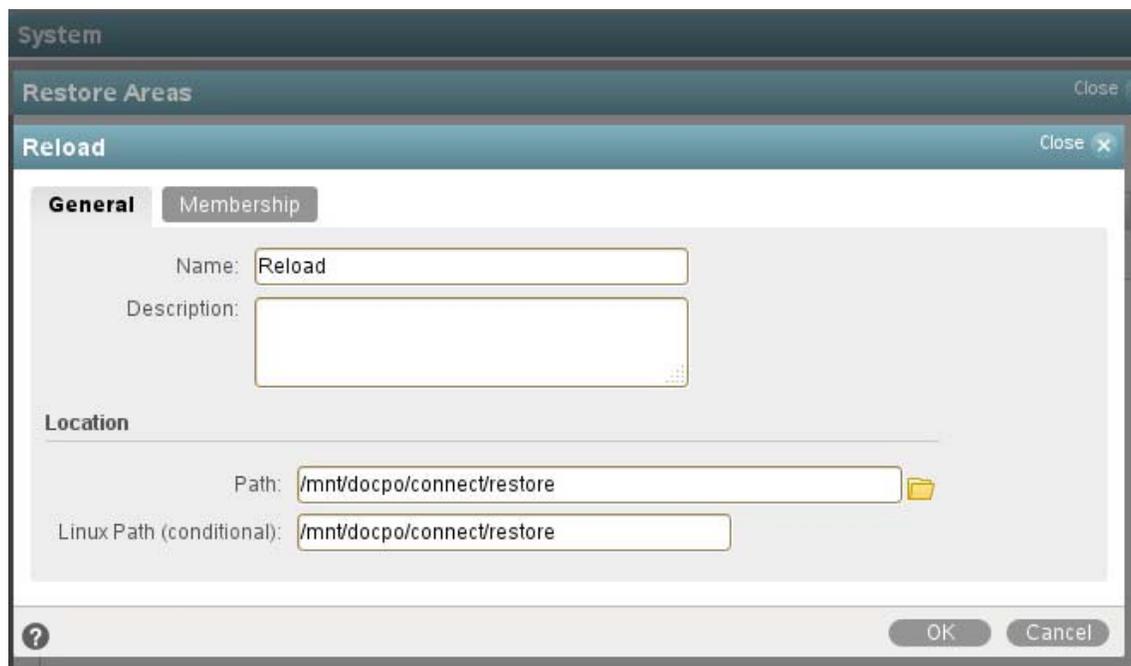
The Restore Area needs to be defined and the users given access to it.

Create Post Office Restore Area, this will need to be done for each Post Office:

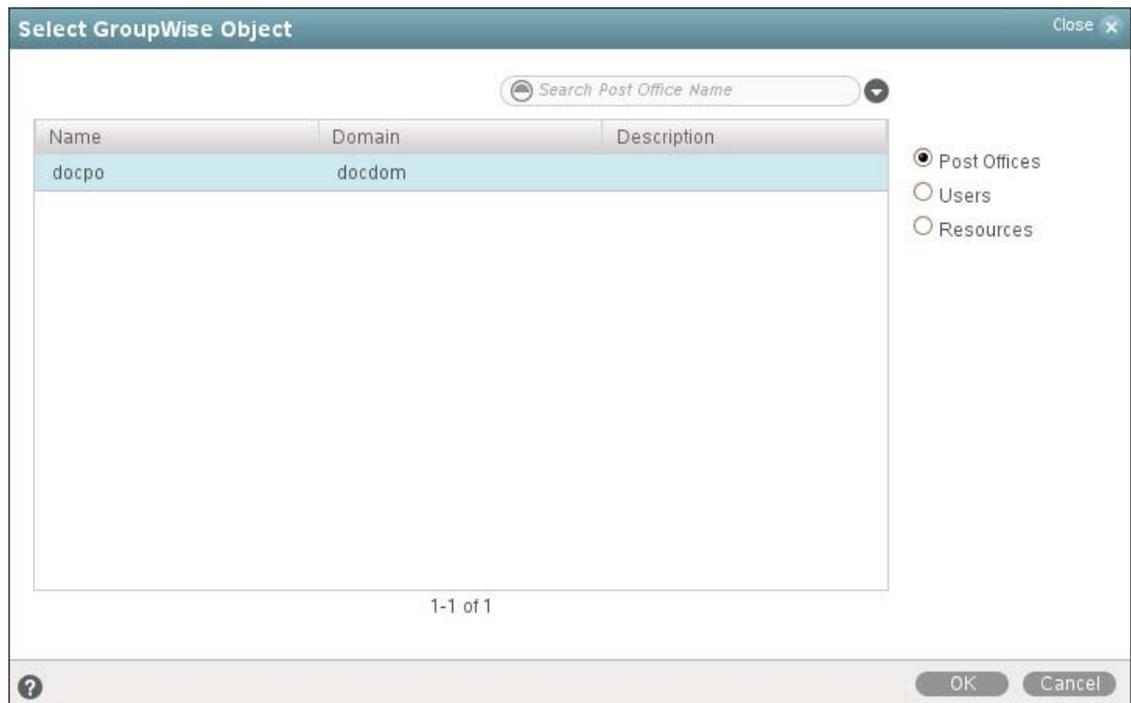
1. Browse to GroupWise Administration https://<GroupWise_Server_Address>:9710
2. Open *System | Restore Area Management*



3. Select New
4. Enter a Name and Description:
5. Set the Path and Linux Path to the mount point adding /connect/restore. For example: /mnt/backup/connect/restore.



6. Under the Membership tab, click Add:
7. Select Post Offices
8. Add Post Office



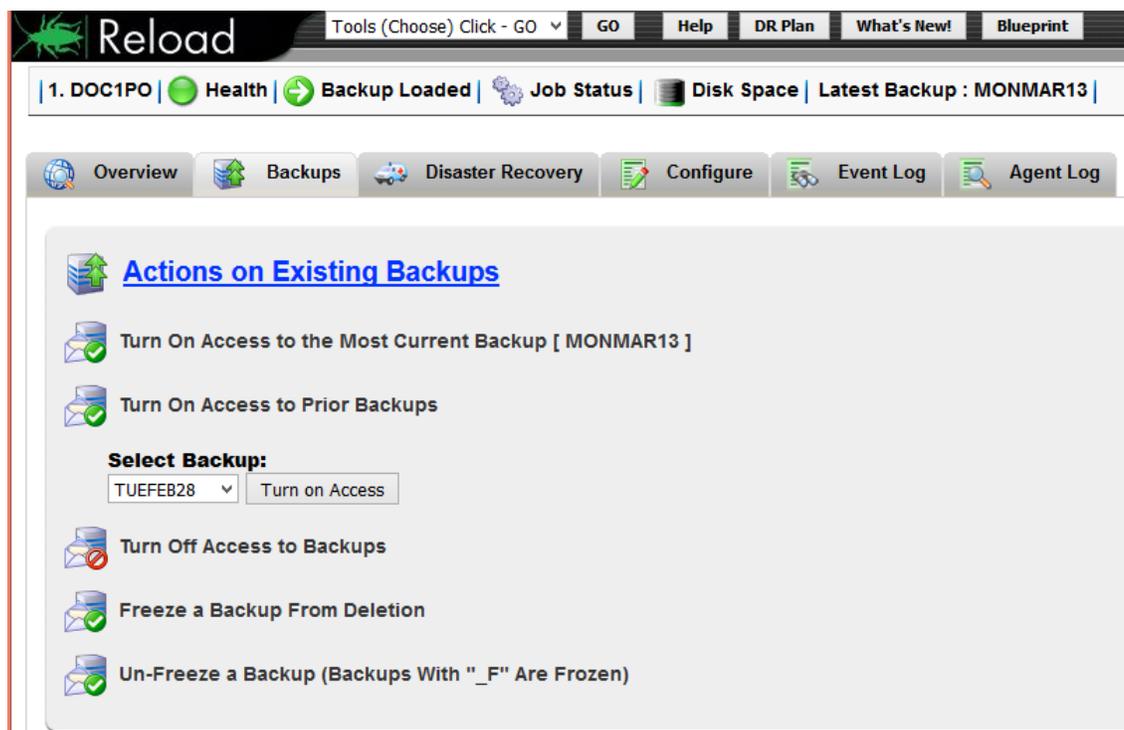
9. Click Ok
10. Click Ok
11. Click Close

Confirmation

To confirm that this worked:

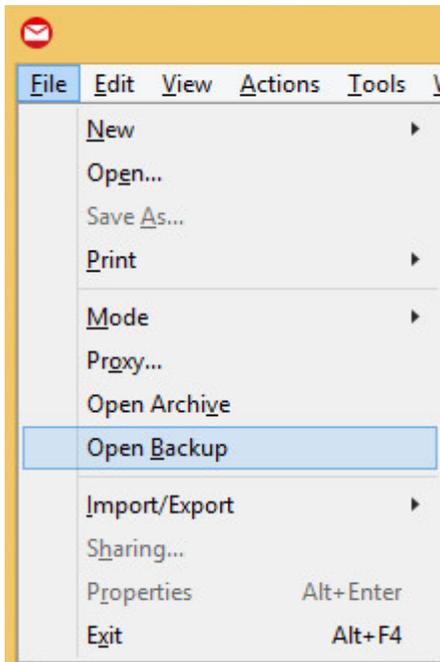
On the GroupWise Disaster Recovery server, load a backup for the profile

1. From the GroupWise Disaster Recovery Web Console, select a *Post Office profile*
2. Select the *Backups* tab
3. From the *Actions of Existing Backups*, select "Turn On Access to the Most Current Backup" or "Turn on Access to Prior Backups"

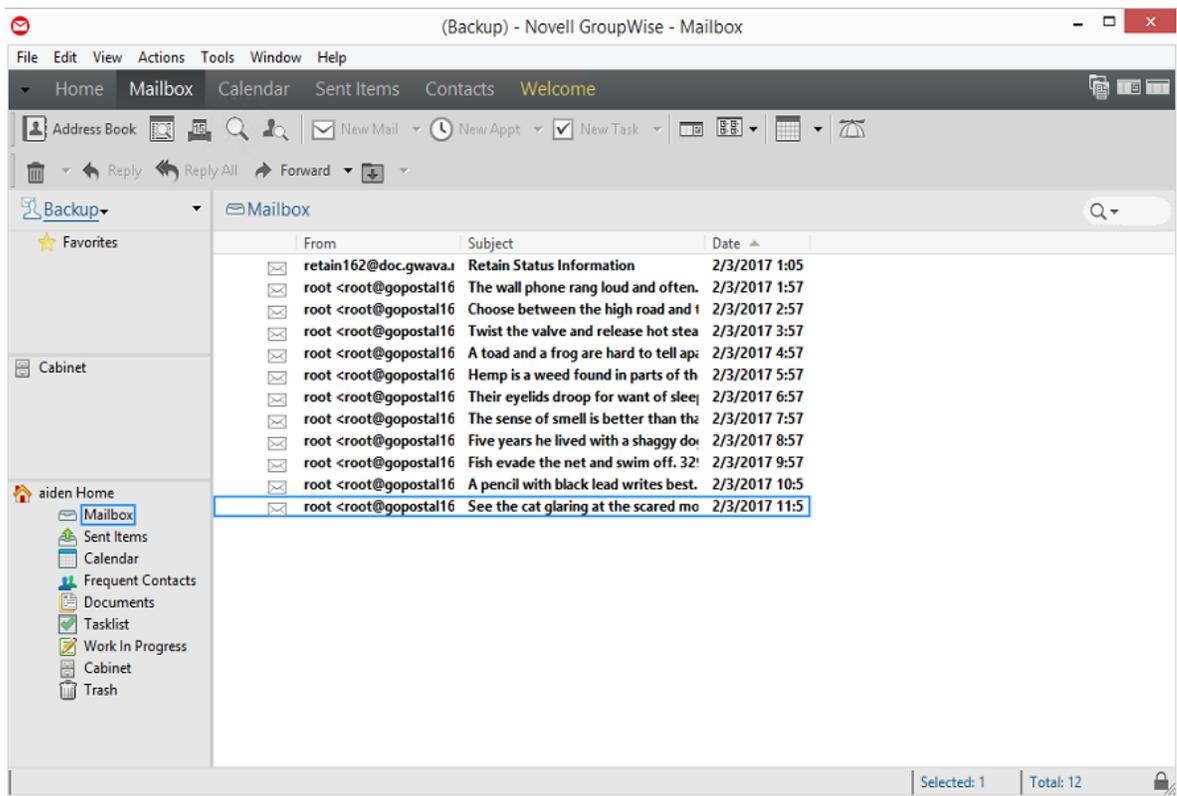


On a workstation with a GroupWise client

1. Move a few items that exist in the backup to the Trash
2. Select *File | Open Backup*.



This view will show the items in the GroupWise Disaster Recovery backup, and NOT on the production GW server for the user.



GroupWise on Windows

Server Only Profiles on Windows

When GroupWise is on Windows, the Server Only model must be used.

Prerequisites

- ♦ Create backup data directory on the GroupWise Disaster Recovery server
- ♦ Install Server for NFS on the Windows Server

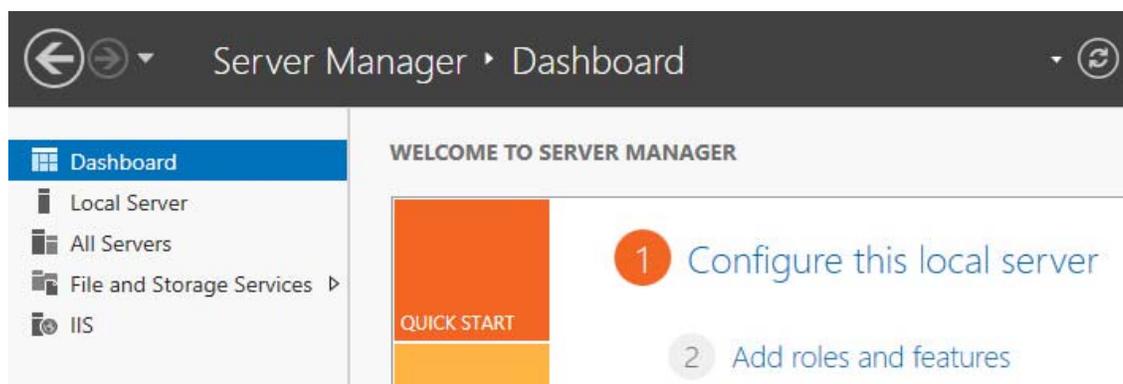
On the GroupWise Disaster Recovery Server: Create backup data directory

You will need to create a directory on the GroupWise Disaster Recovery server for the backup data. The name of the profile will be used to create sub-directories for each profile. For example:

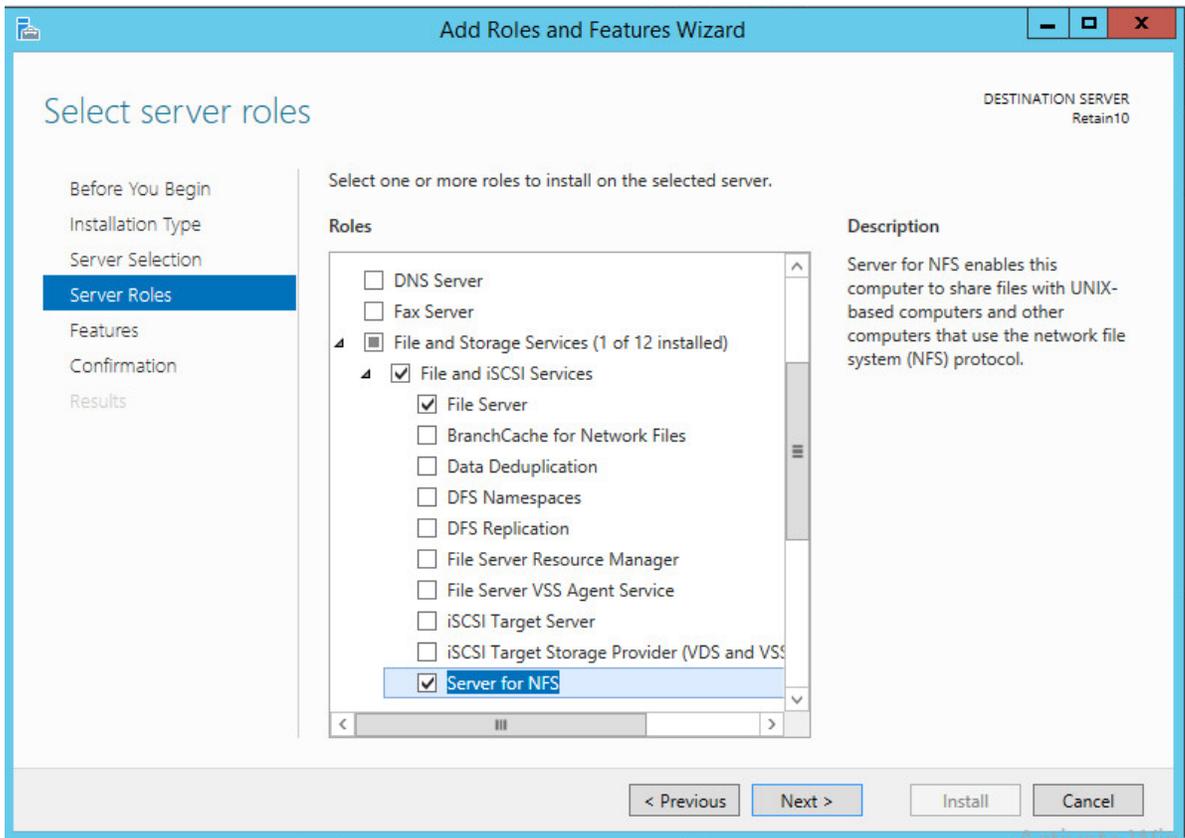
```
mkdir /reload/
```

On the Windows GroupWise server: Install and Configure Server for NFS

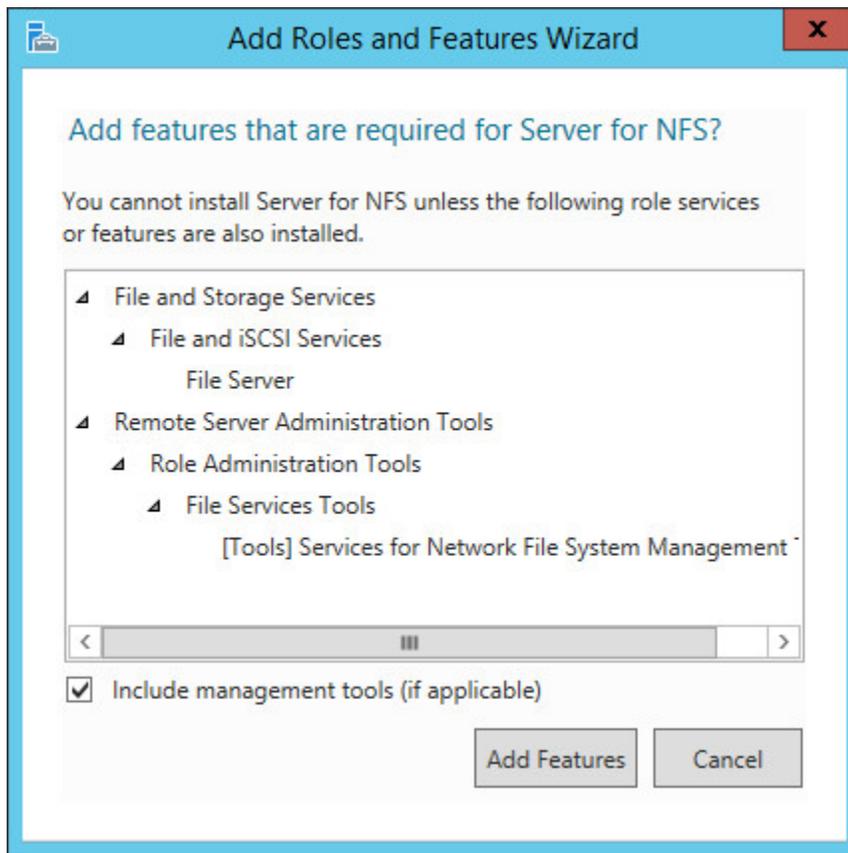
1. Open Server Manager and select *Add roles and features*



2. Install the Server Role *File and Storage Services | Server for NFS*. A restart will be required.



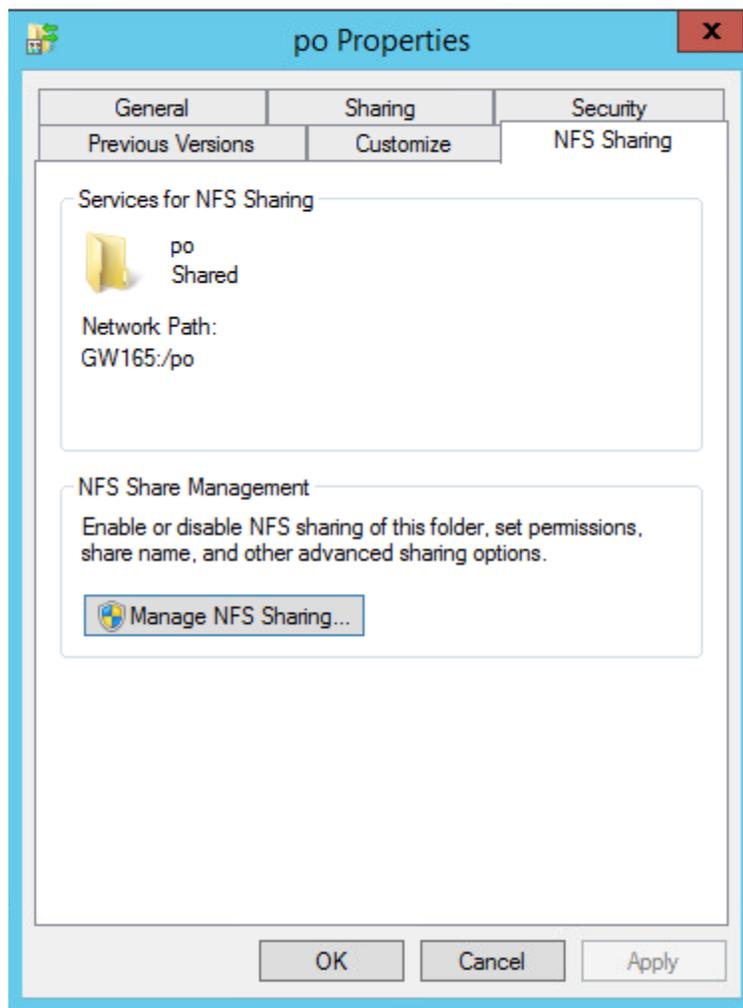
And add the Features



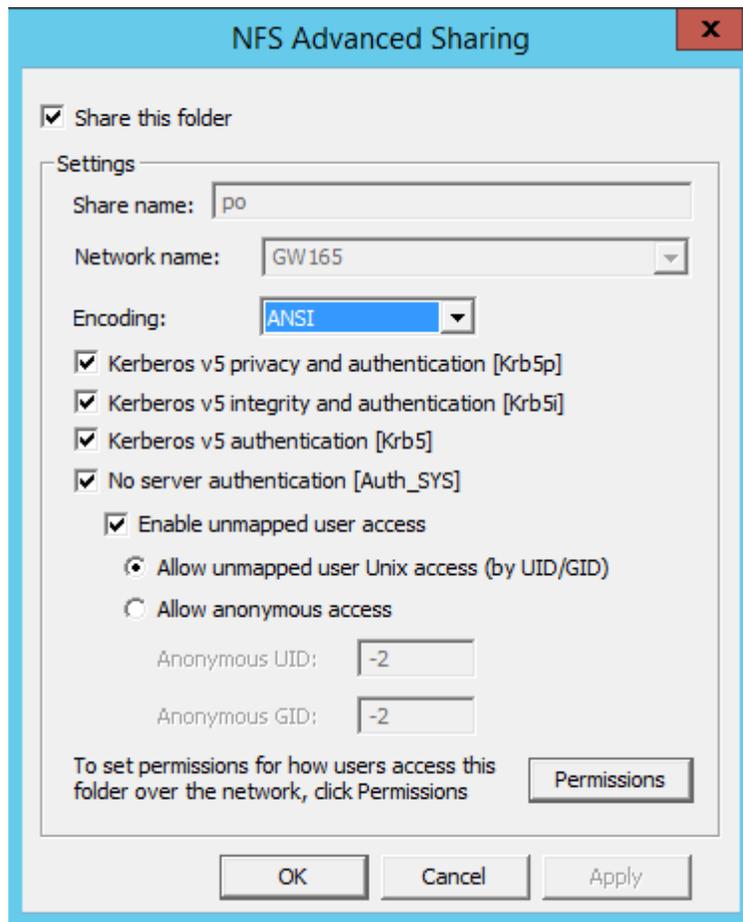
The server will restart once the installation is complete.

Create the share point for the *domain* and *post office* folders:

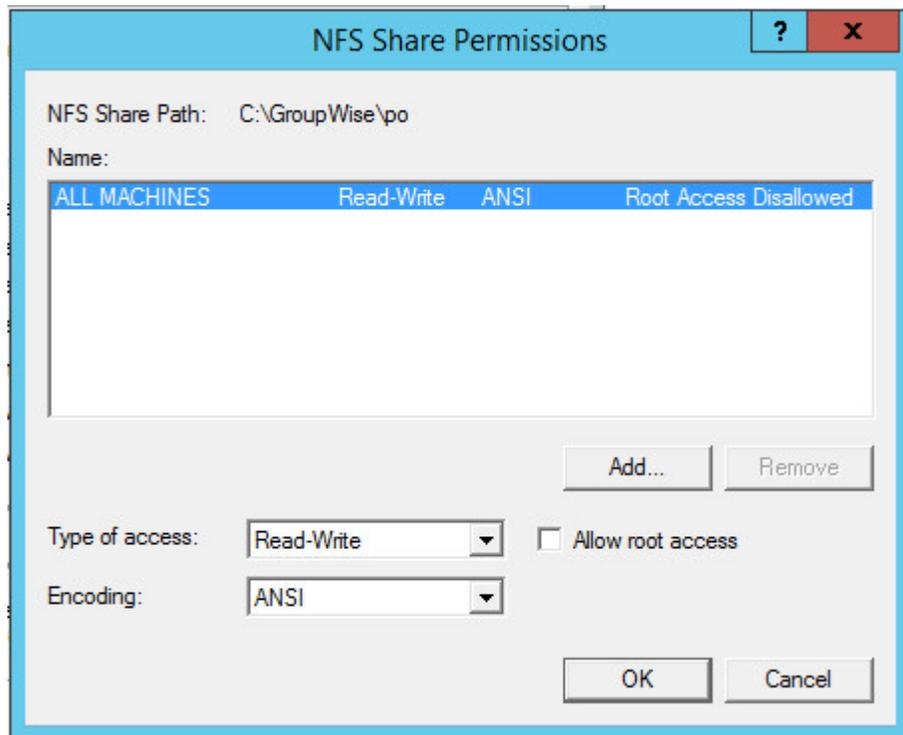
1. In File Explorer browse to the GroupWise folder
2. Right-click the folder to be shared and select Properties
3. Select the *NFS Sharing* tab



4. Click Manage NFS Sharing
5. Enable *Share this folder*



6. Select Permissions and set *Type of Access* to *Read-Write* and click OK



7. Click OK
8. Click Close

Do this for the domain as well.

On the GroupWise Disaster Recovery server:

1. Create a mount point. For example,

```
mkdir /mnt/po
```

2. Mount the NFS point from the Windows server

```
mount -t nfs <address of GW Windows server>:/<shared folder> <local mount point>
```

For example: `mount -t nfs 10.1.1.123:/po /mnt/po`

Configure Profiles

There are two kinds of profiles: [Domain \(Create_Domain_Profiles_on_Windows.htm\)](#) and [Post Office \(Create_Post_Office_Profiles_on_Windows.htm\)](#).

Creating Domain Profiles with GroupWise on Windows

When GroupWise is on Windows the Server Only model must be used to backup the data to GroupWise Disaster Recovery.

Domain Profile: Server Only Model

On the GroupWise Disaster Recovery server, create a data directory and a profile

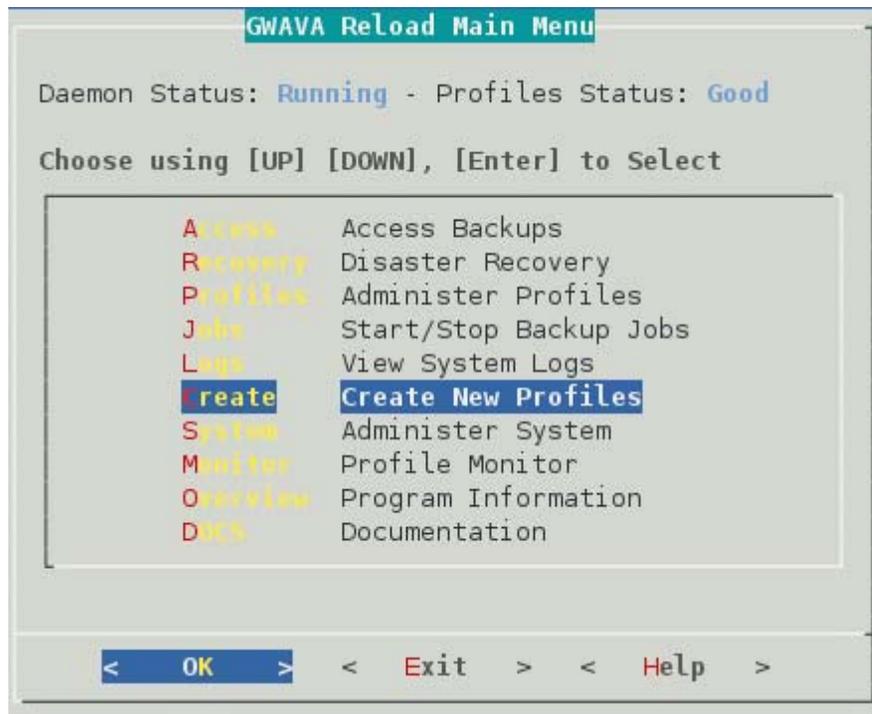
1. Create a directory for the backup data. For example:

```
mkdir /reload
```

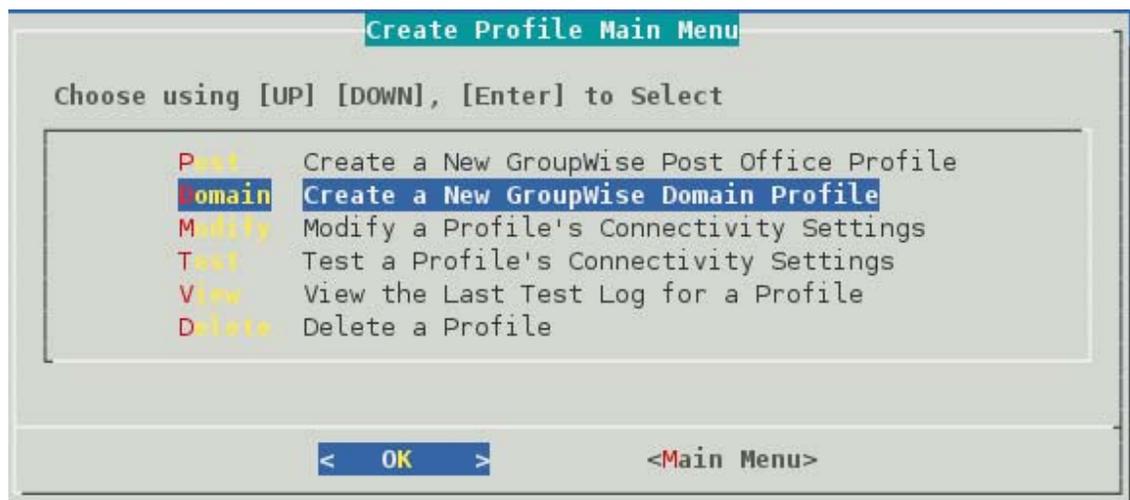
2. Start the GroupWise Disaster Recovery Administration Console by typing on the command line:

```
reload
```

3. Select "Create (Create Profile)"



4. Select "Domain (Create a New GroupWise Domain Profile)"



5. Give the Profile a Name. The profile name should not exceed eight characters. Use letters and numbers only, no spaces or other characters. For example: Domain Be aware, that a profile cannot be renamed, once it has been created. Choose the name wisely. Perhaps you will want to name the profile so that its name is the same as the GroupWise post office or domain that the profile represents. Select the Next button.

The screenshot shows a dialog box titled "Profile Name". The text inside reads: "Choose < Next > to Accept", "Use letters and numbers only, no spaces or other characters!", "The profile name SHOULD NOT EXCEED 8 characters.", and "Enter the name of the profile in the field below:". A text input field contains the word "DOMAIN". At the bottom, there are two buttons: "< Next >" and "< Cancel >".

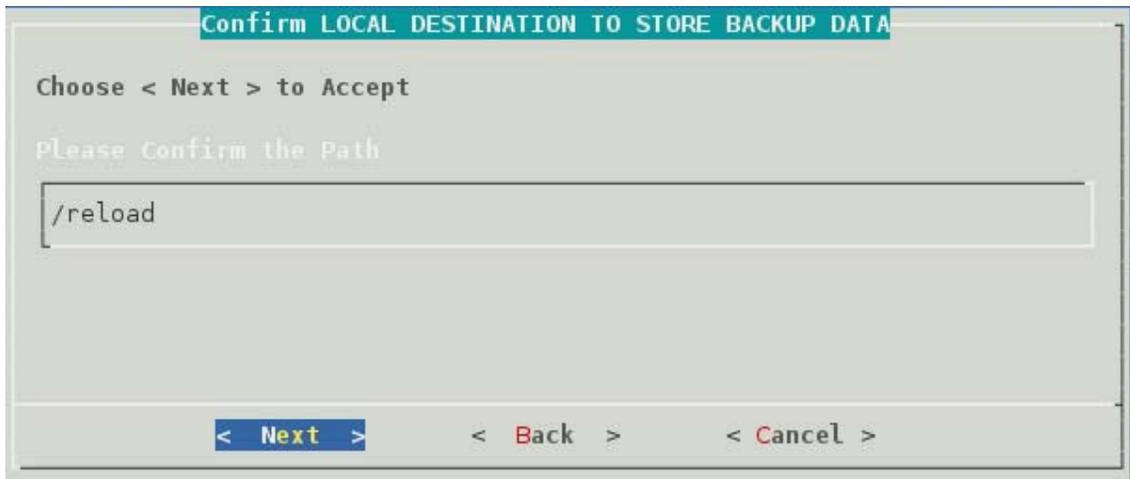
6. Give the Profile a Description. The profile description should not exceed 60 characters and should not have comma(,), nor dollar sign(\$) characters. For example: Primary Domain. The description of the profile will be added to the Agent Log when backup jobs are run for the profile. Select the Next button.

The screenshot shows a dialog box titled "Profile Description". The text inside reads: "Choose < OK > to Accept", "The profile description should not exceed 60 characters.", "NOTE: Do not use a comma or dollar sign (, \$) character.", and "Enter the profile description in the field below:". A text input field contains the text "Primary Domain". At the bottom, there are two buttons: "< OK >" and "< Cancel >".

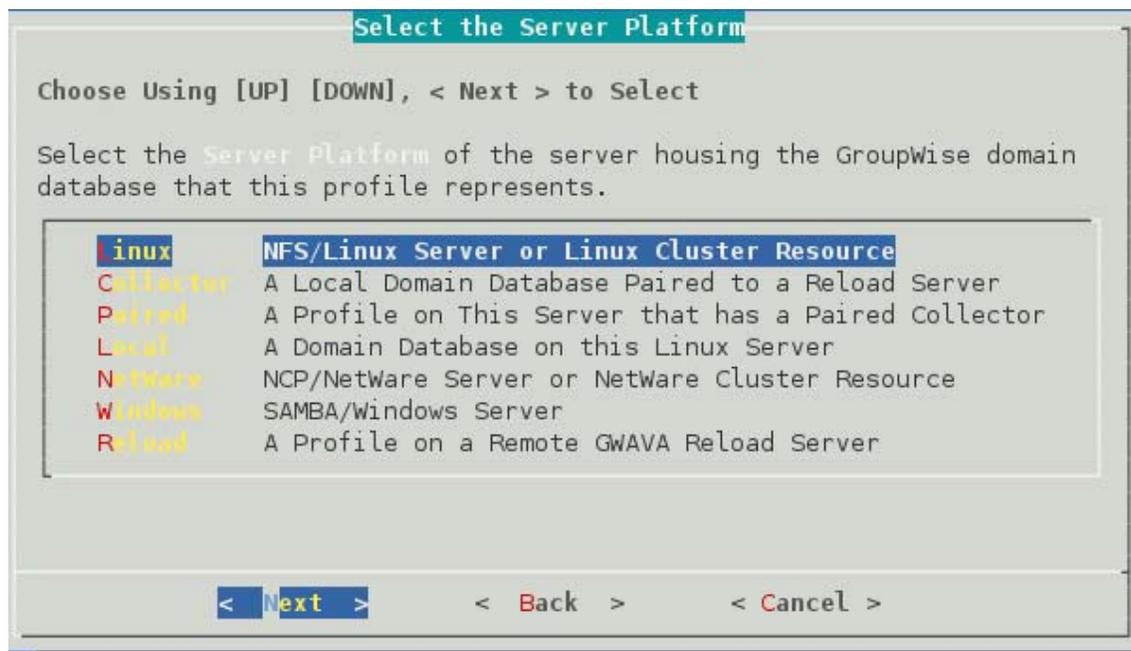
7. Enter the path or browse to the local destination directory to store the backup data. For example: /reload. This path can be a location on the Linux server, or an NFS mount to another Linux/Unix server, or to a SAN. The path should always be available; GroupWise Disaster Recovery is not configured to mount paths in order to access stored data. Also, the path should be to a location that has a lot of disk space available. Select the Next button.



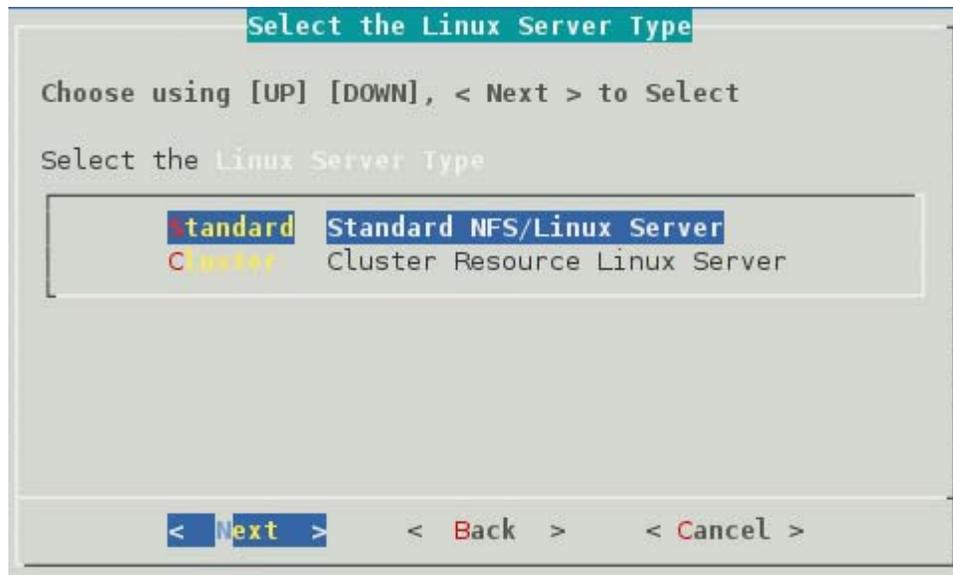
8. Confirm the path to the local destination directory



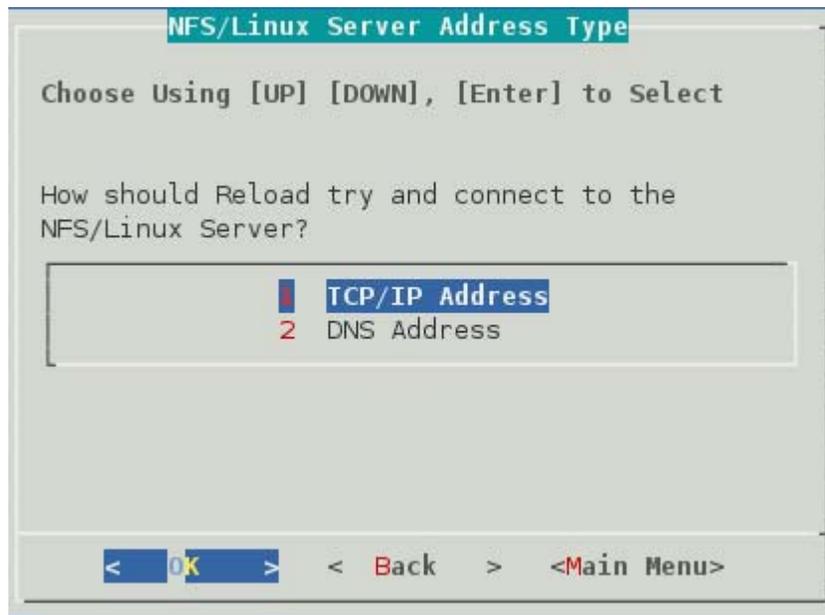
9. Select the Server Platform: "Linux (NFS/Linux Server or Linux Cluster Resource)" [Yes, the GroupWise server is Windows, but the share is NFS, which is the important part]



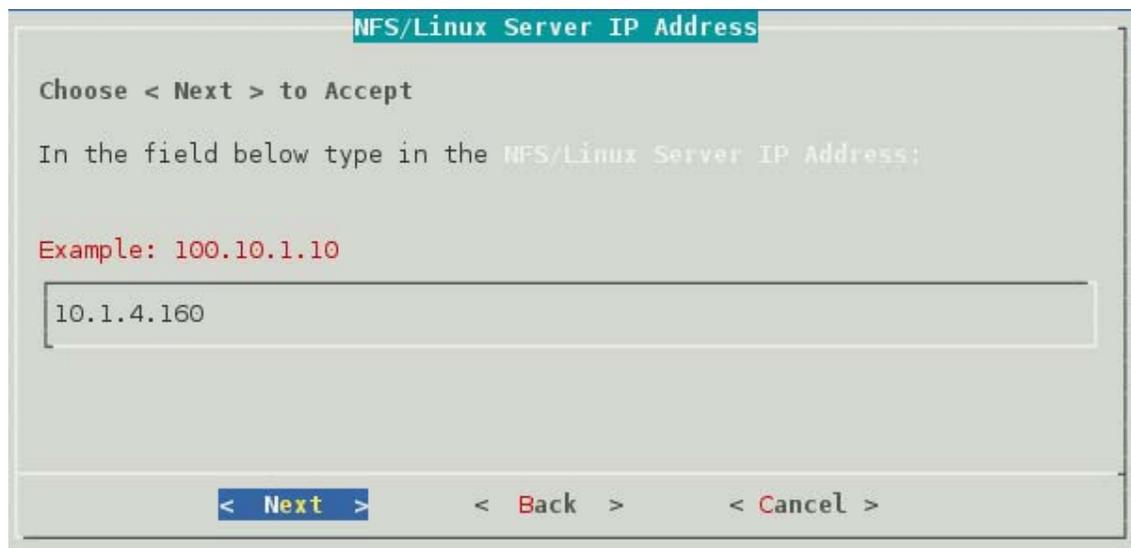
10. Select Linux Server Type: "Standard (Standard NFS/Linux Server)"



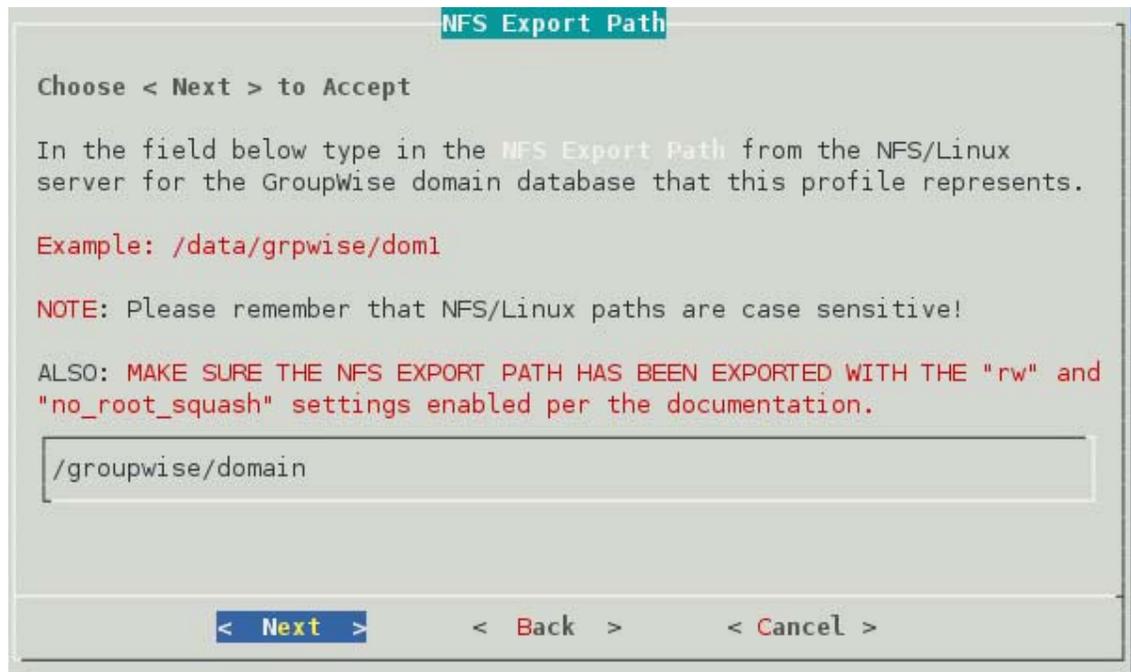
11. Select NFS/Linux Server Address Type: "1 (TCP/IP Address)" or "2 (DNS Address)"



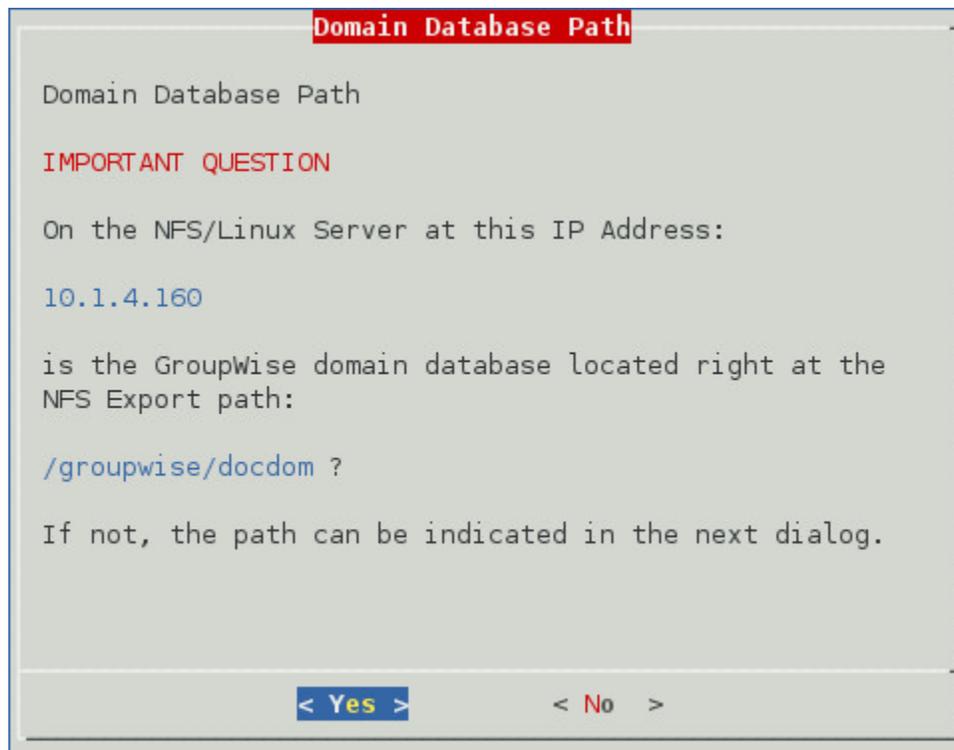
12. Enter the NFS/Linux Server IP Address or DNS hostname Address



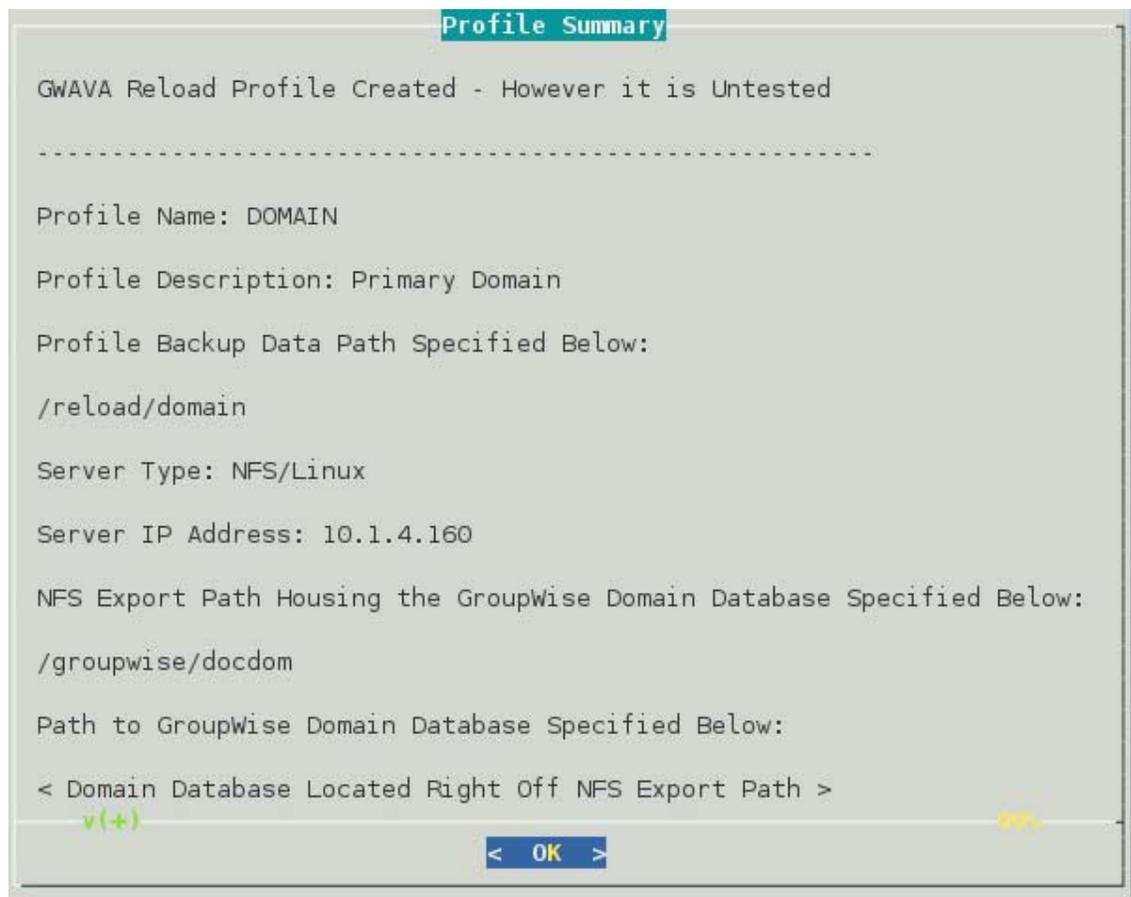
13. Enter the NFS Export Path on the GroupWise server from above. For example: /groupwise/domain



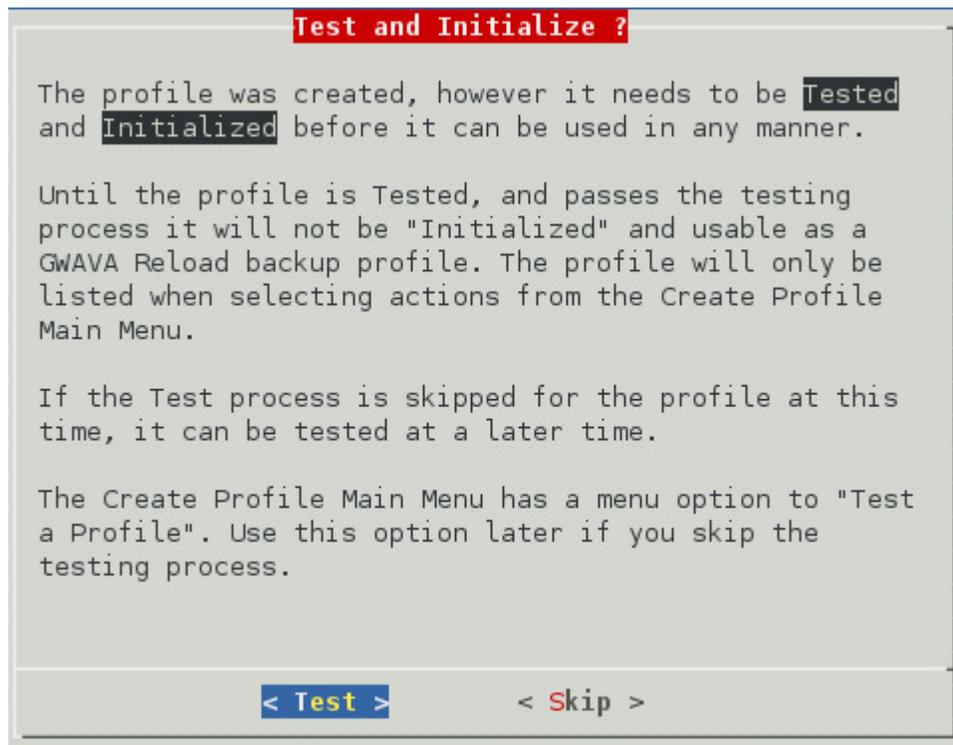
14. A warning page appears that asks if the IP Address and Export path are correct.



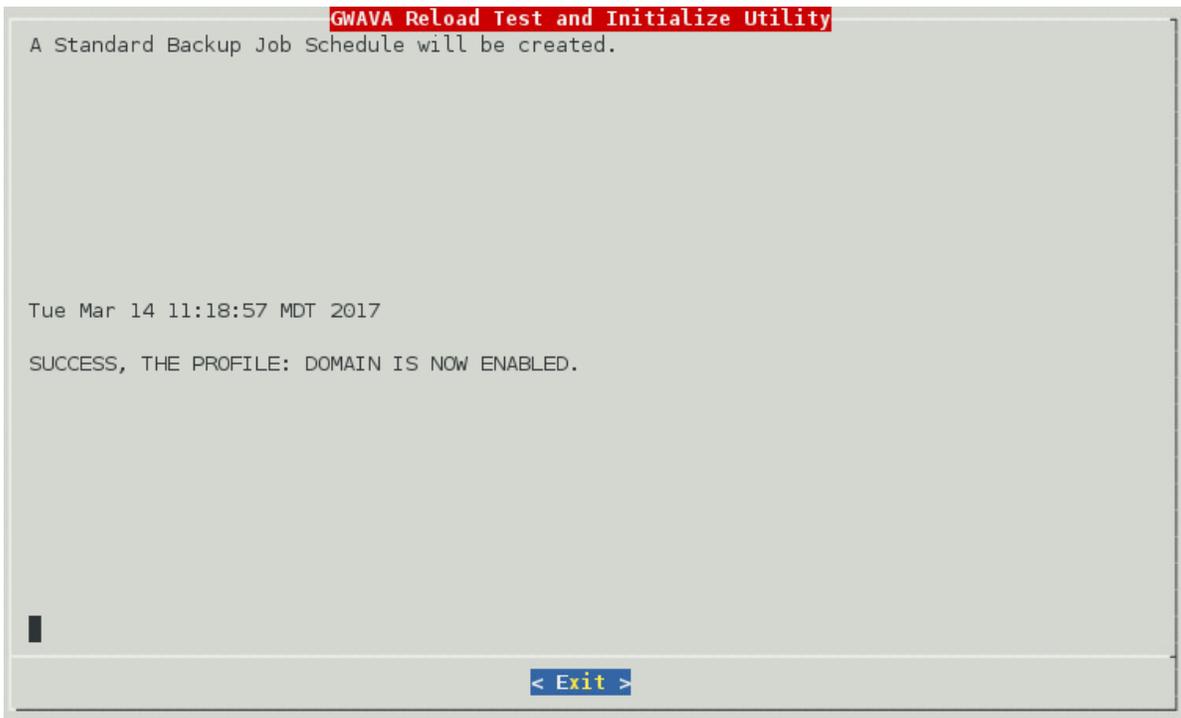
15. A Profile Summary page appears



16. The Test and Initialize page allows you to finalize the profile by selecting Test.



17. If the configuration is incorrect, select Skip and makes your changes.
18. Run the test and it will indicate success or failure.



Creating Post Office Profiles with GroupWise on Windows

When GroupWise is on Windows the Server Only model must be used to backup the data to GroupWise Disaster Recovery.

Post Office Profile: Server Only Model

On the GroupWise Disaster Recovery server, create a data directory and a profile

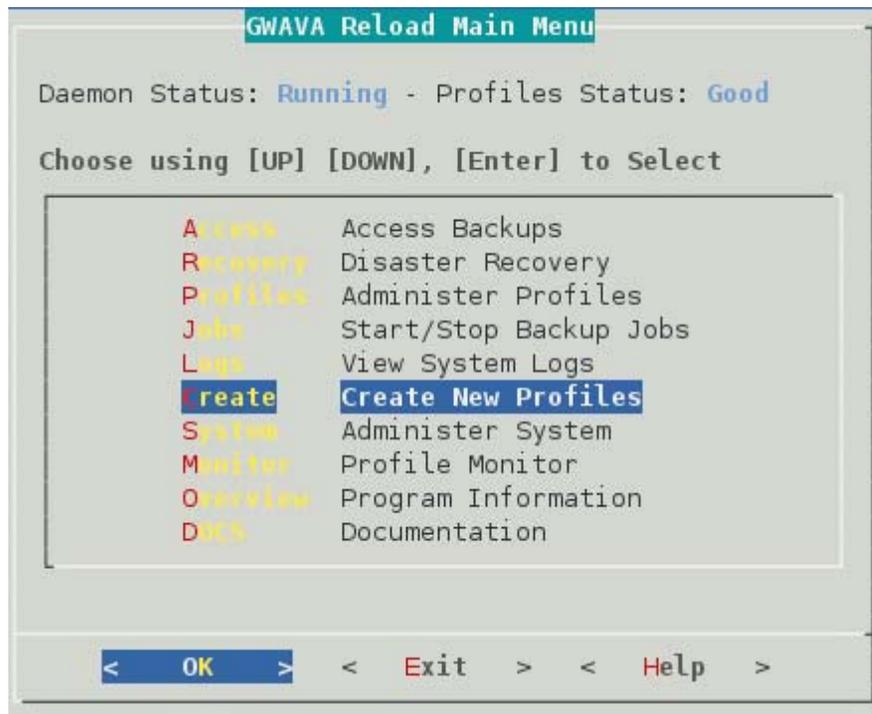
1. Create a directory for the backup data, if necessary. For example:

```
mkdir /reload
```

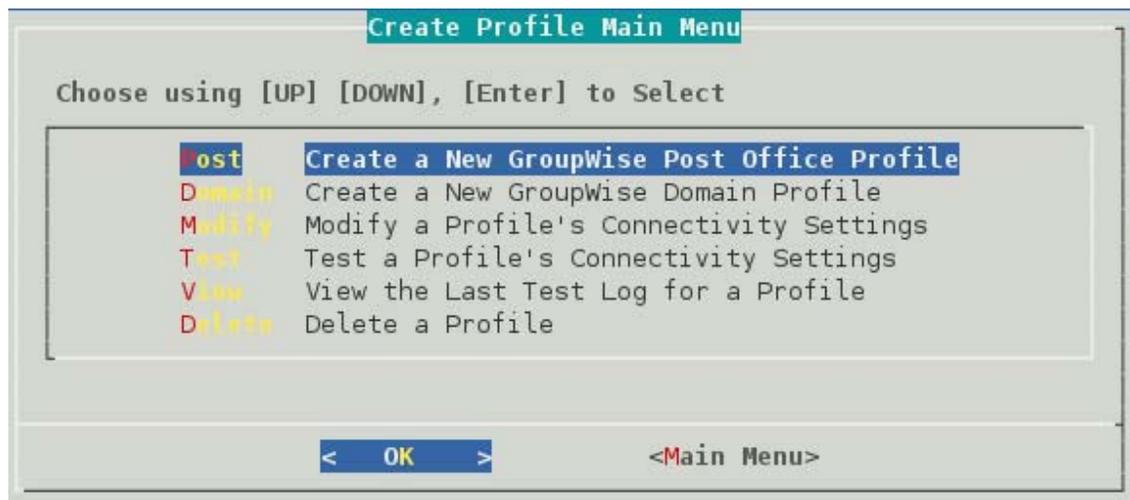
2. Start the GroupWise Disaster Recovery Administration Console by typing on the command line:

```
reload
```

3. Select "Create (Create Profile)"



4. Select "Post (Create a New GroupWise Post Office Profile)"



5. Give the Profile a Name. The profile name should not exceed eight characters. Use letters and numbers only, no spaces or other characters. For example: Post Office. Be aware, that a profile cannot be renamed, once it has been created. Choose the name wisely. Perhaps you will want to name the profile so that its name is the same as the GroupWise post office or domain that the profile represents. Select the Next button.

Profile Name

Choose < Next > to Accept

Use letters and numbers only, no spaces or other characters!

The profile name SHOULD NOT EXCEED 8 characters.

Enter the name of the profile in the field below:

< Next > < Cancel >

6. Give the Profile a Description. The profile description should not exceed 60 characters and should not have comma(,), nor dollar sign(\$) characters. For example: Primary Post Office. The description of the profile will be added to the Agent Log when backup jobs are run for the profile. Select the Next button.

Profile Description

Choose < OK > to Accept

The profile description should not exceed 60 characters.

NOTE: Do not use a comma or dollar sign (, \$) character.

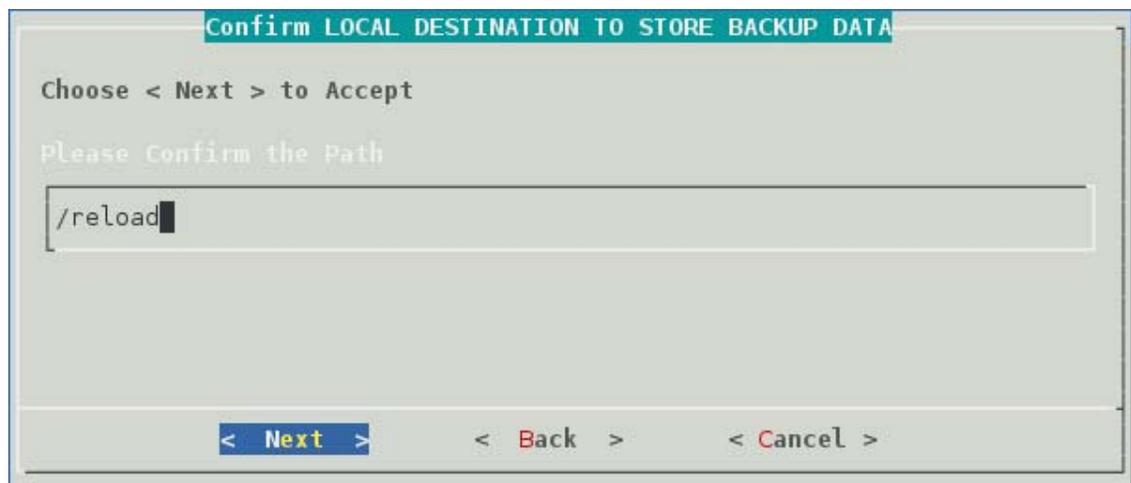
Enter the profile description in the field below:

< OK > < Cancel >

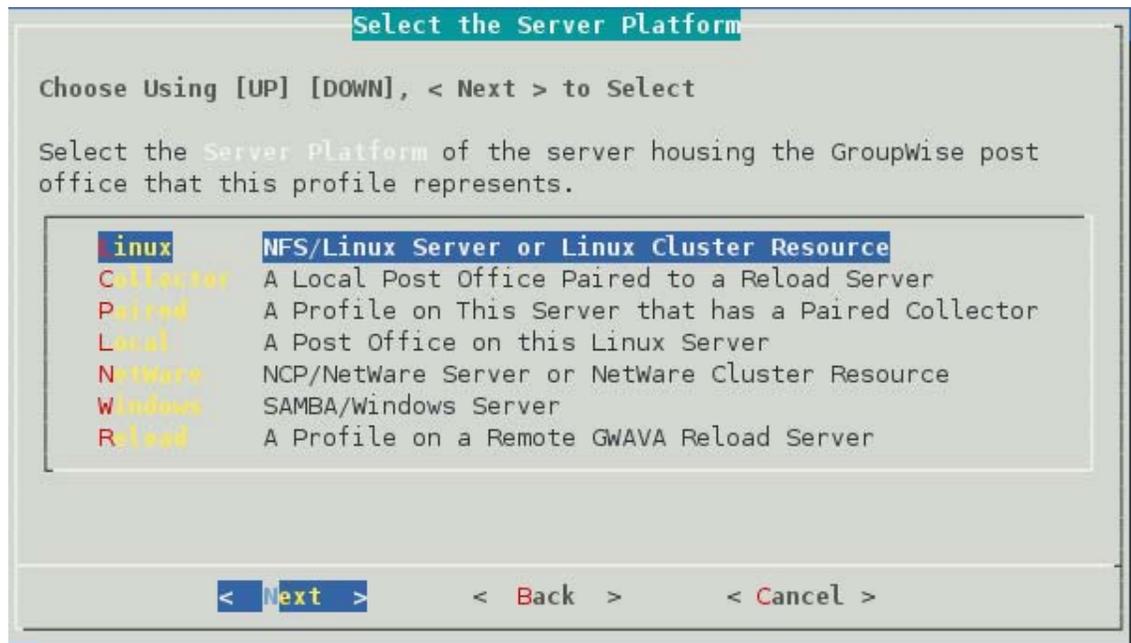
7. Enter the path or browse to the local destination directory to store the backup data. For example: /reload. This path can be a location on the Linux server, or an NFS mount to another Linux/Unix server, or to a SAN. The path should always be available; GroupWise Disaster Recovery is not configured to mount paths in order to access stored data. Also, the path should be to a location that has a lot of disk space available. Select the Next button.



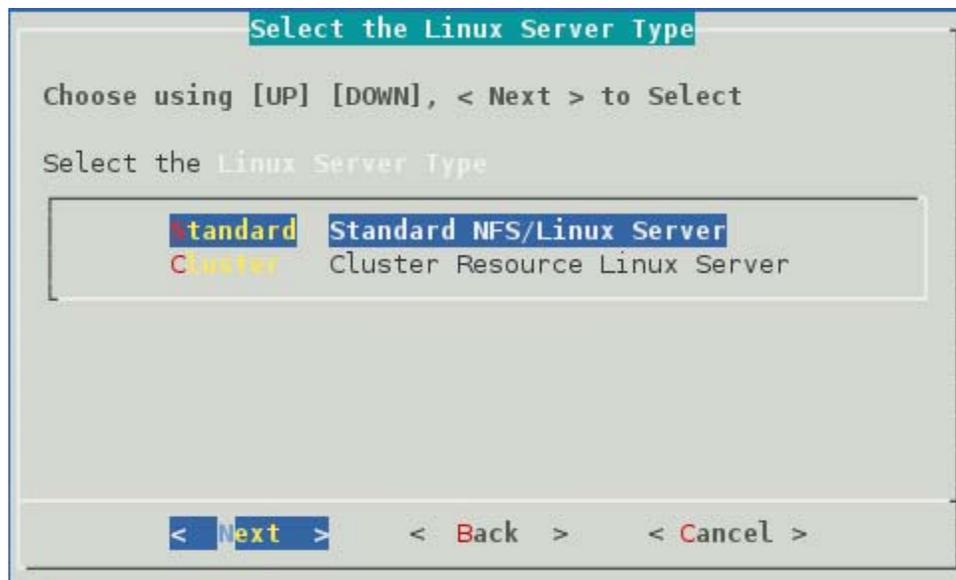
8. Confirm the path to the local destination directory



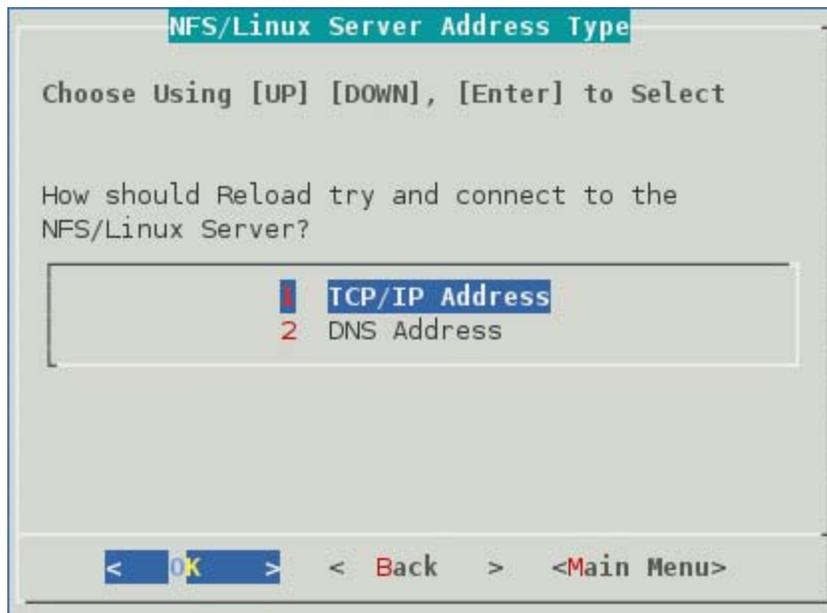
9. Select the Server Platform: "Linux (NFS/Linux Server or Linux Cluster Resource)" [Yes, the GroupWise server is Windows, but the share is NFS, which is the important part]



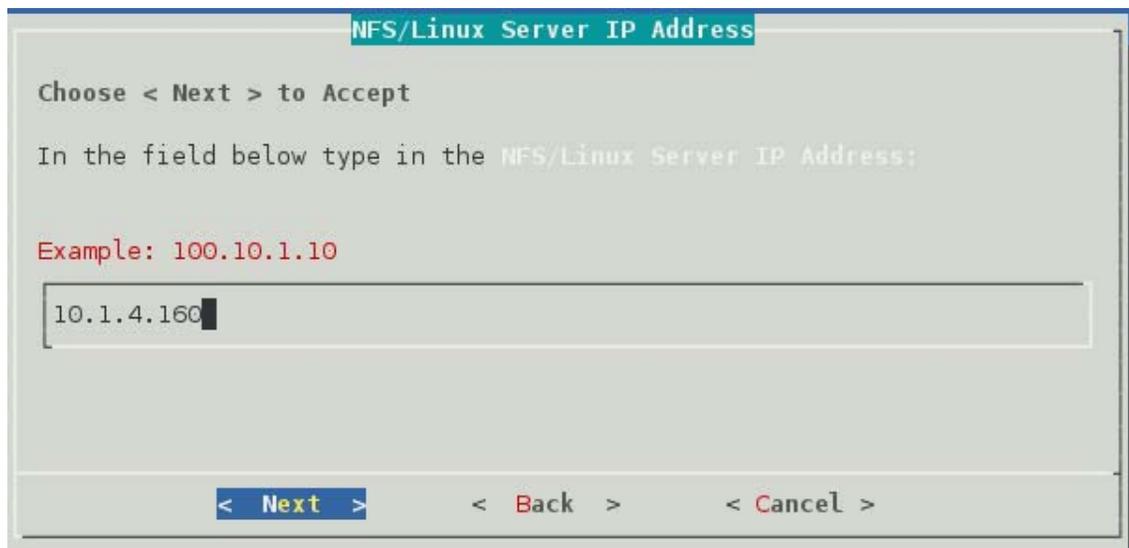
10. Select Linux Server Type: "Standard (Standard NFS/Linux Server)"



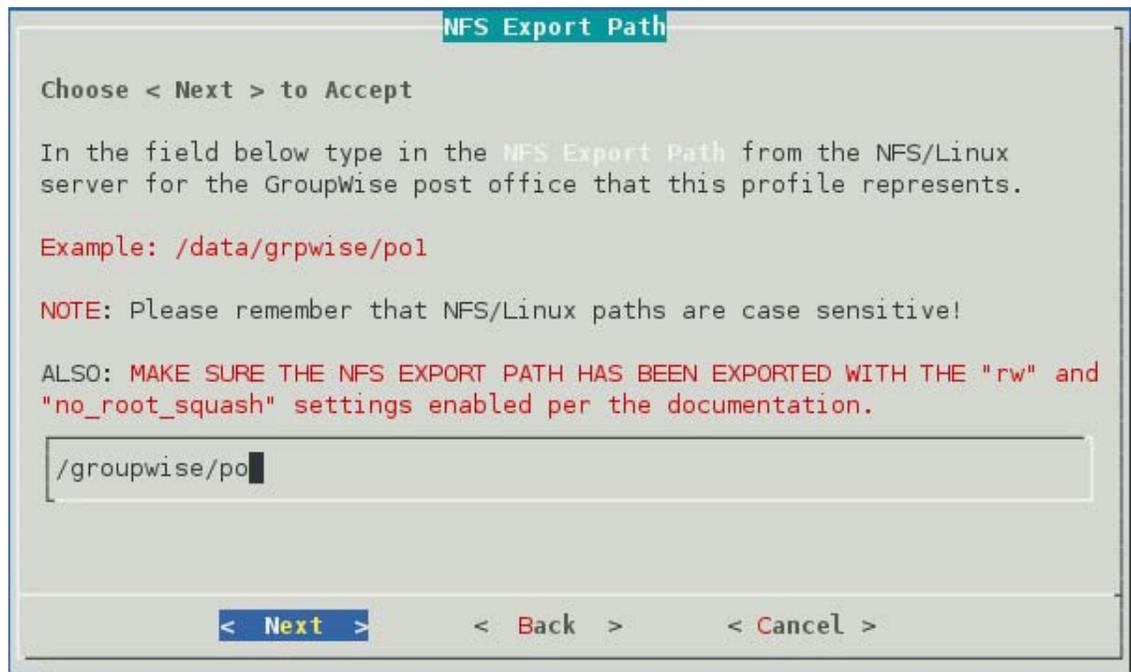
11. Select NFS/Linux Server Address Type: "1 TCP/IP Address" or "2 DNS Address"



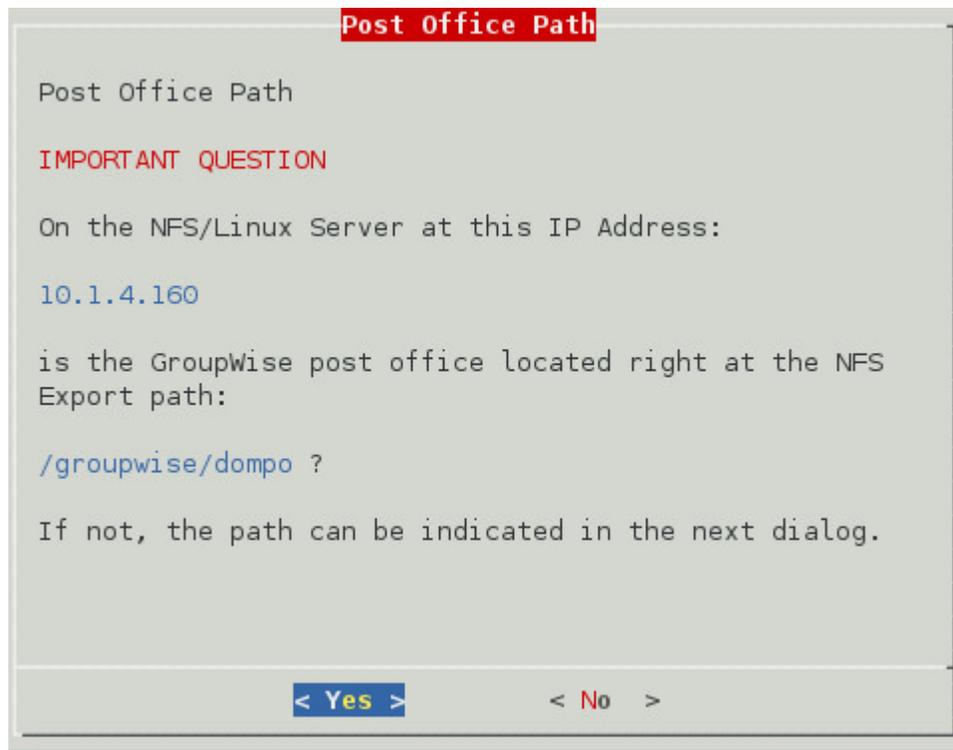
12. Enter the NFS/Linux Server IP Address or DNS Hostname



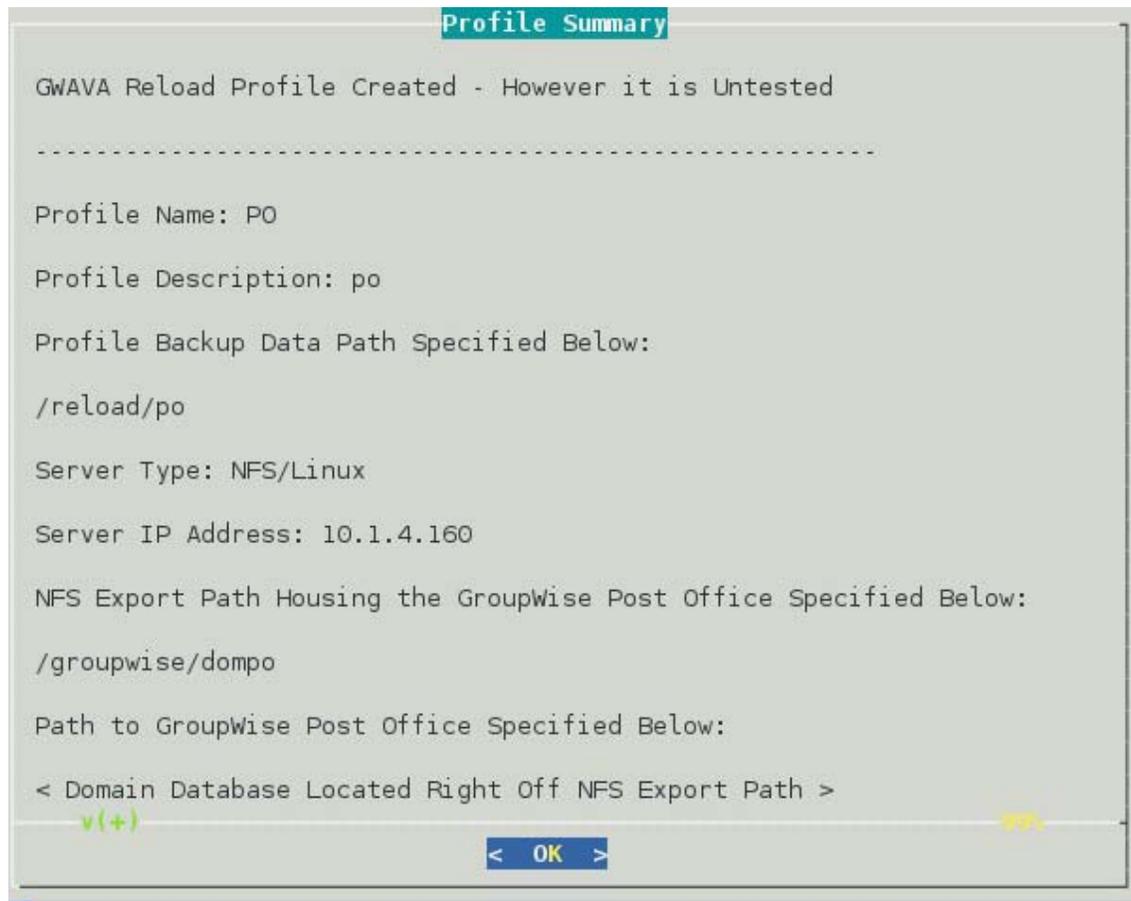
13. Enter the NFS Export Path on the GroupWise server from above. For example: /groupwise/po



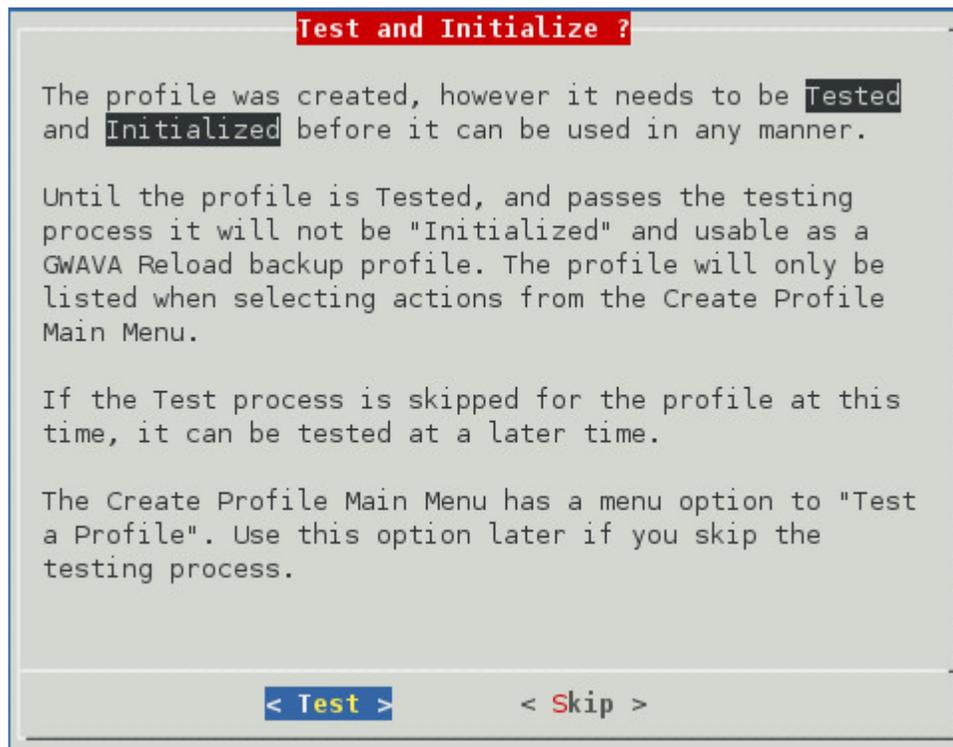
14. A warning page appears that asks if the IP Address and Export path are correct.



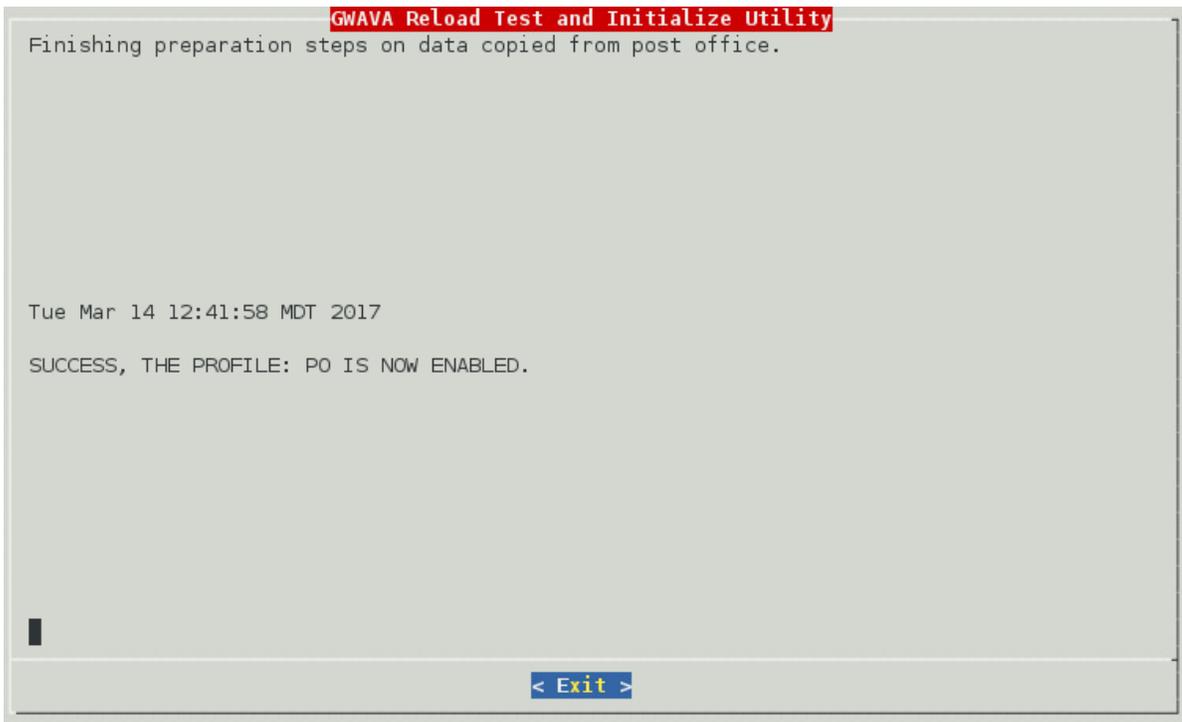
15. A Profile Summary page appears



16. The Test and Initialize page allows you to finalize the profile by selecting Test.



17. If the configuration is incorrect, select Skip and makes your changes.
18. Run the test and it will indicate success or failure.



Configure Restore Area on Windows

Once a backup has been created the link to the Restore Area can be made.

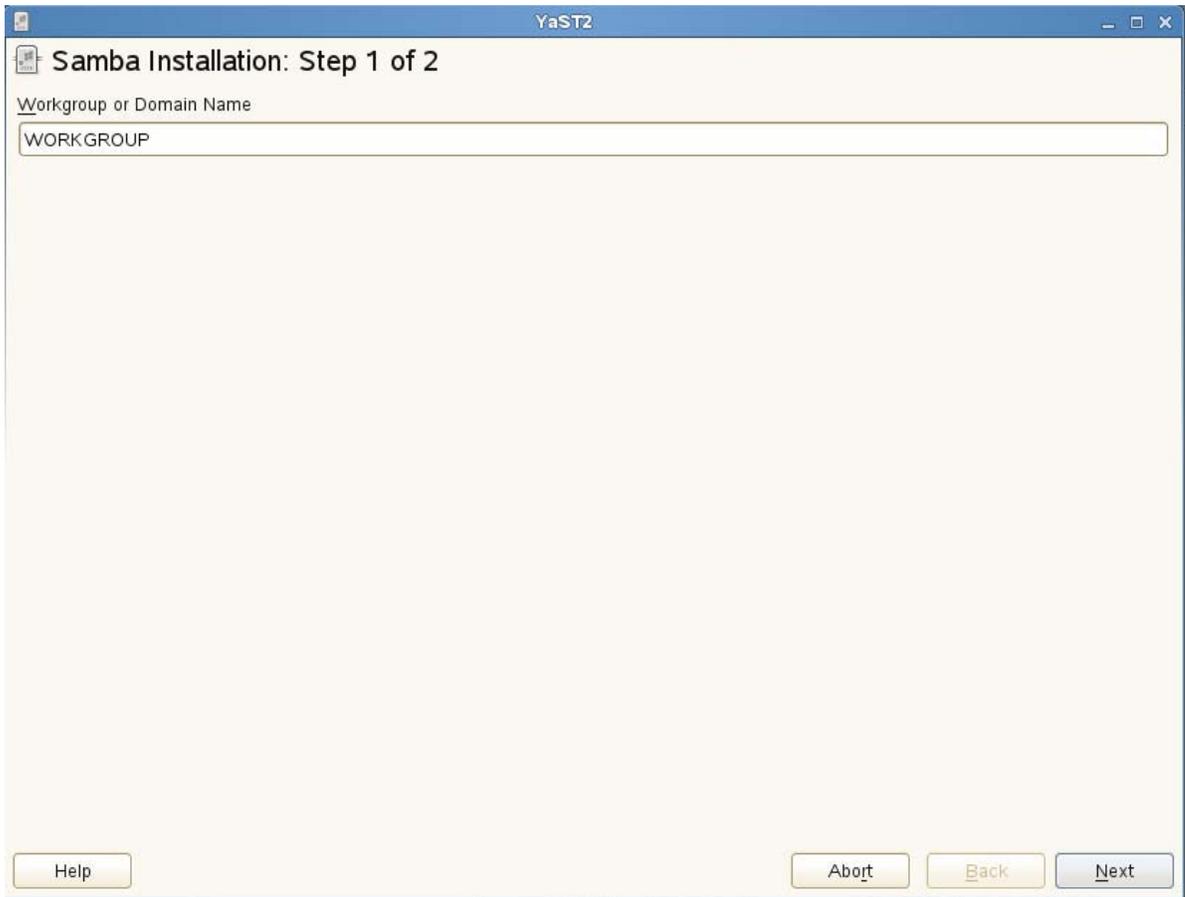
On the GroupWise Disaster Recovery Server

Install Samba Server on the GroupWise Disaster Recovery server

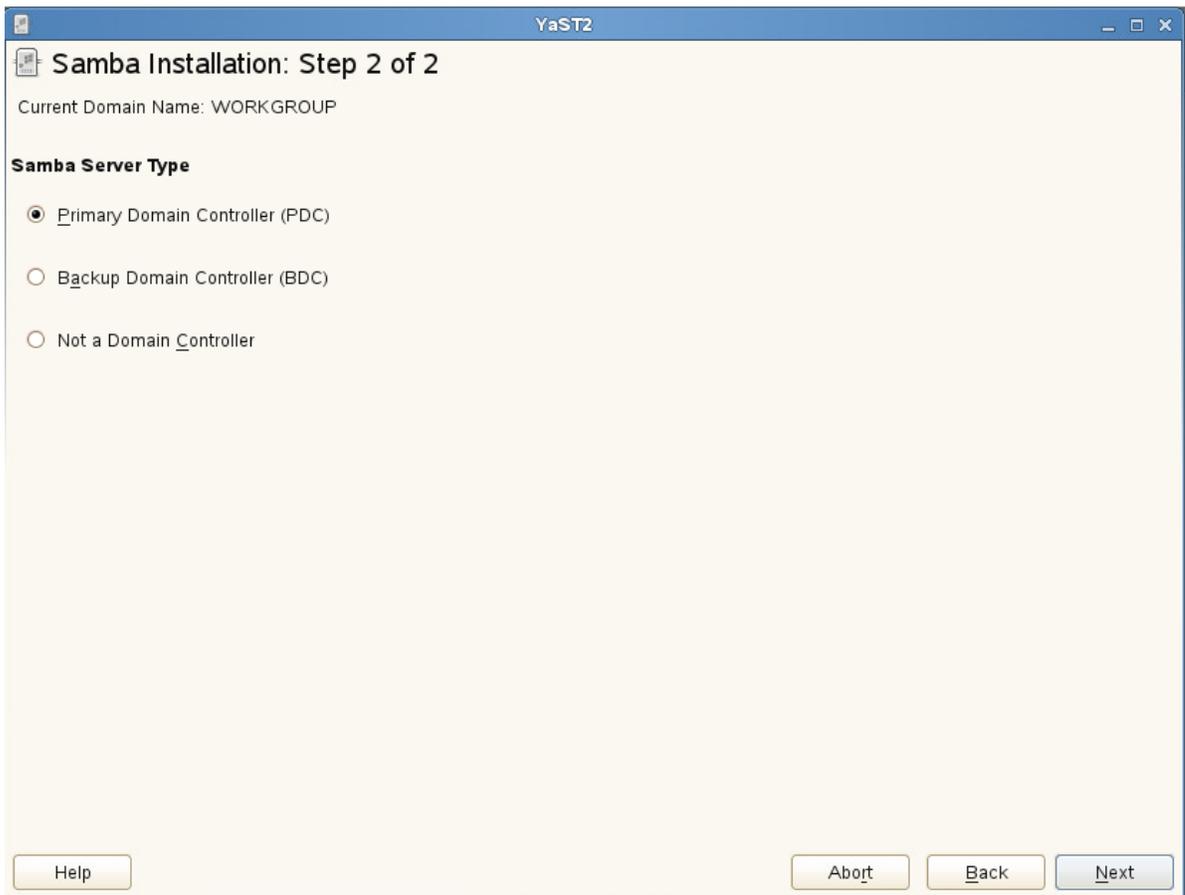
Open YaST | Samba Server



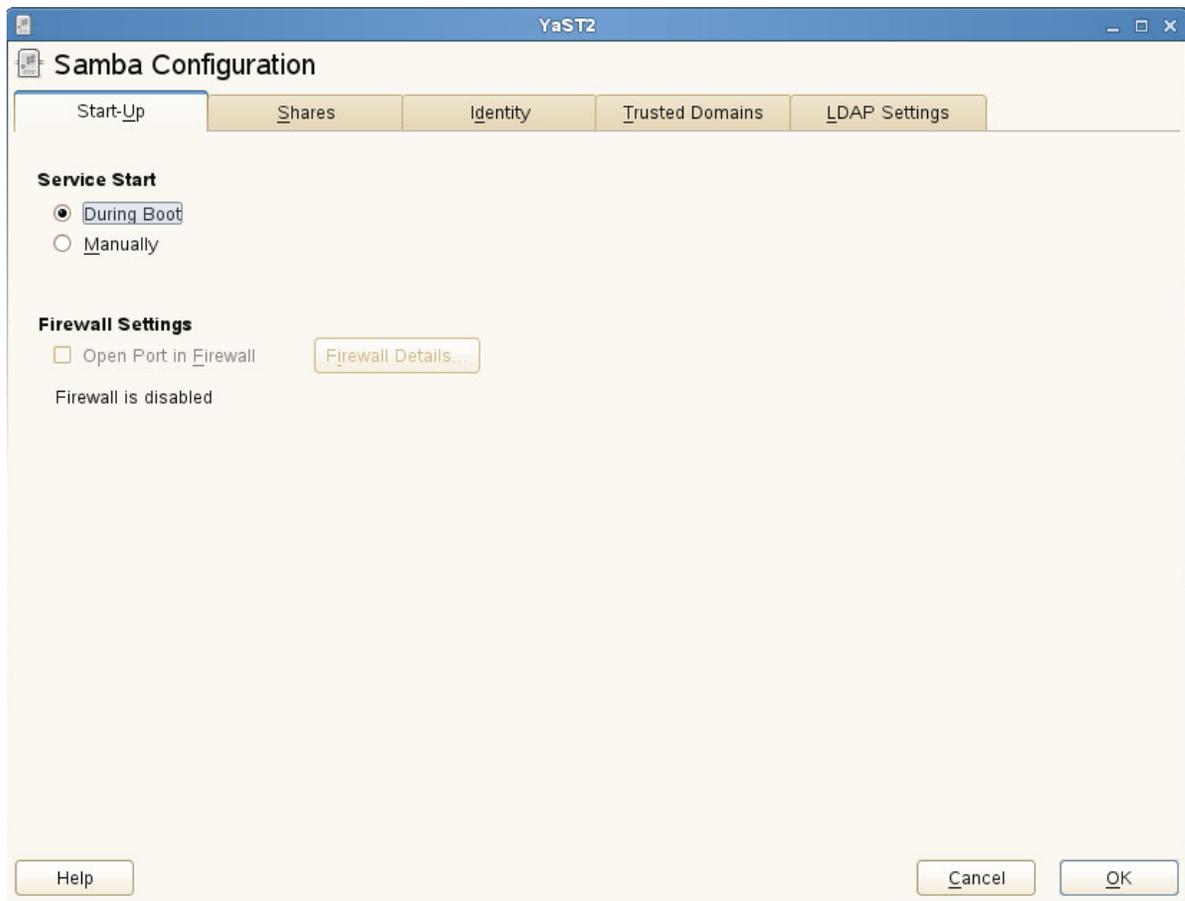
Provide a Workgroup or Domain Name (default WORKGROUP), Press Next



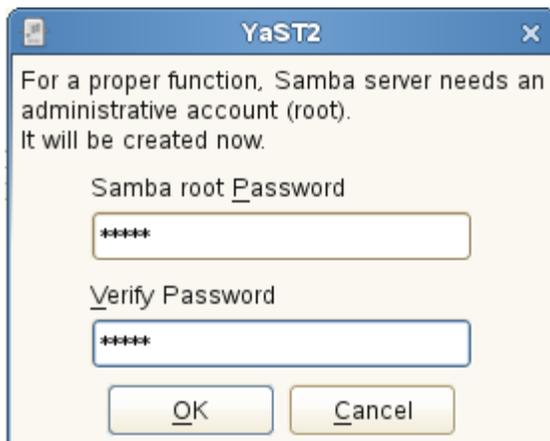
Choose Samba Server Type (default Primary Domain Controller), Press Next



Set Service Start to During Boot, Press OK

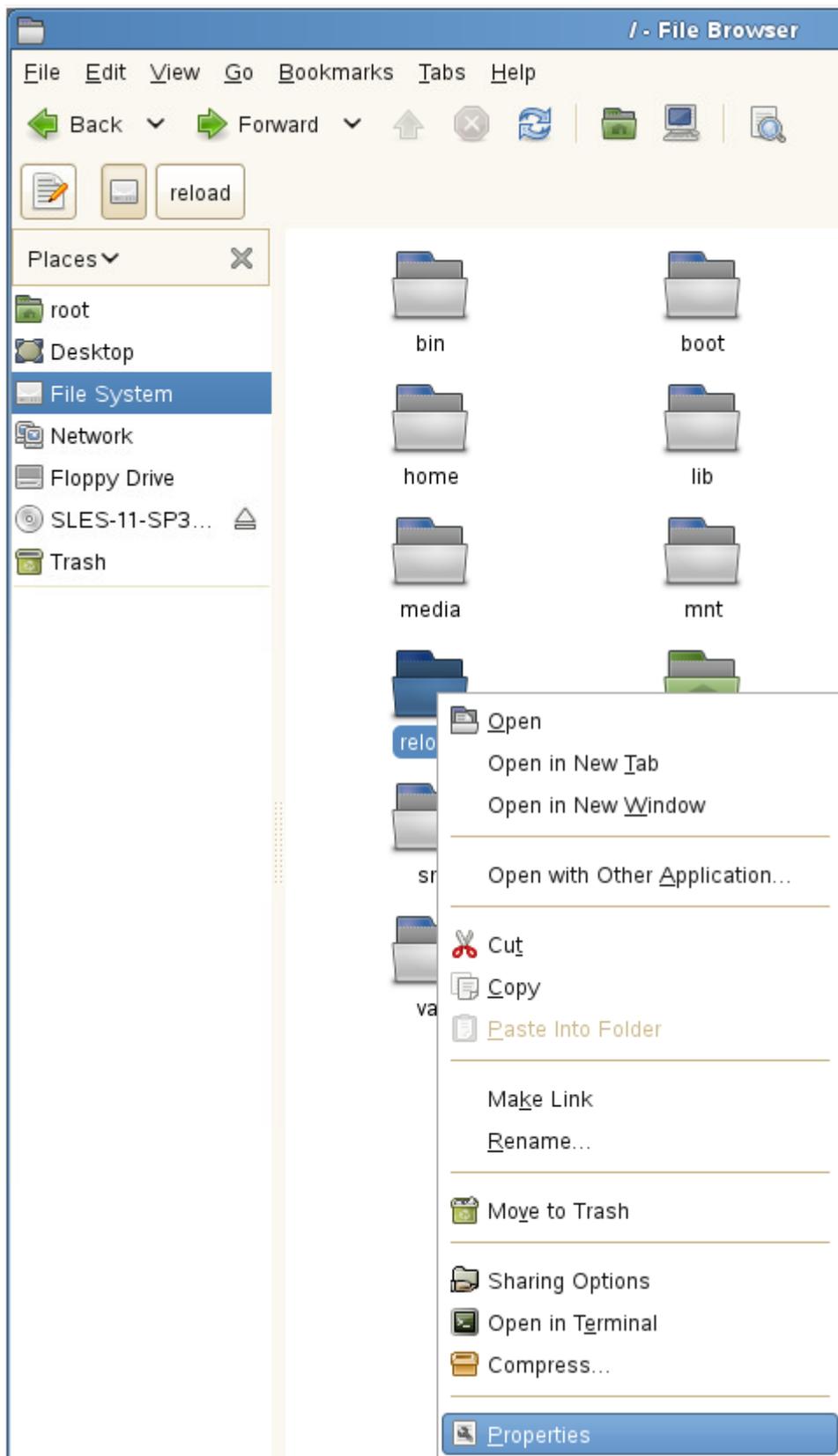


Provide an admin password



Setup Share

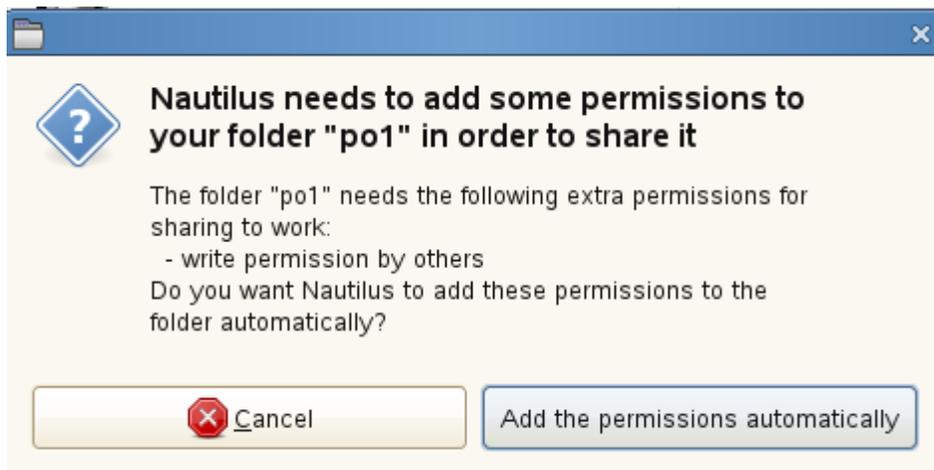
1. Using the "Nautilus File Browser" Browse to the parent directory of the profiles. For example, / reload, with /reload/po under it
2. Right-click on the parent directory of your profiles and select "Properties"



3. Select the Share tab
 - a. Enable "Share this folder" and give it a share name
 - b. Enable "Allow other people to writing in this folder"
 - c. Click "Create Share"



4. Click on "Add the permissions automatically" when prompted



In GroupWise Administration

The Restore Area needs to be defined and the users given access to it.

Create Post Office Restore Area, this will need to be done for each Post Office:

1. Browse to GroupWise Administration
2. Open *System | Restore Area Management*

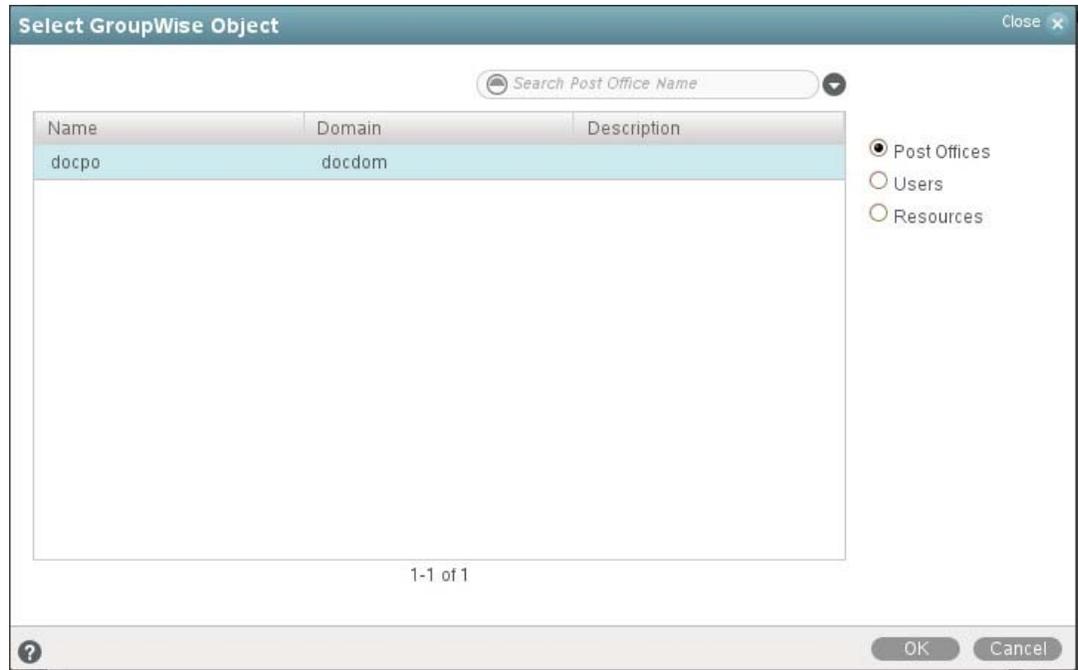


3. Select New
4. Enter a Name and Description
5. Set the Path to the Samba share, adding \connect\restore
\\<GroupWise Disaster Recovery Server Address>\<Post Office Directory>\connect\restore
For example, \\10.1.1.123\po1\connect\restore
6. Do not complete the Linux path field



7. Under the Membership tab, Click Add
 - ◆ Select Post Offices

- ◆ Add Post Office

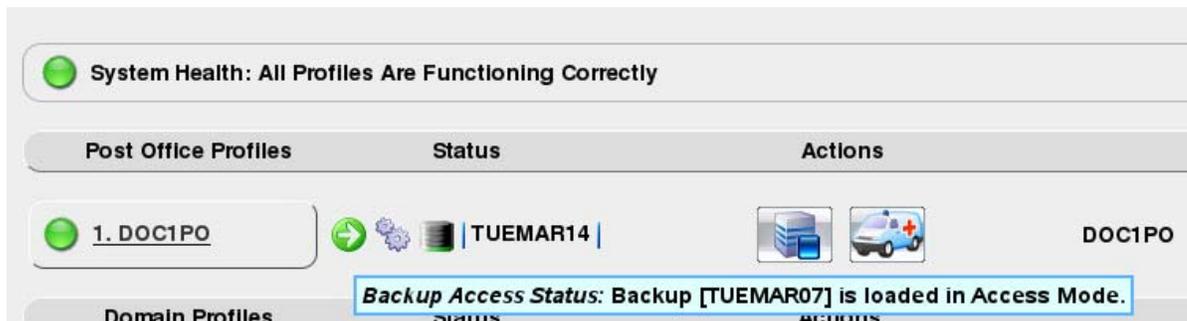


Confirmation

To confirm that this worked:

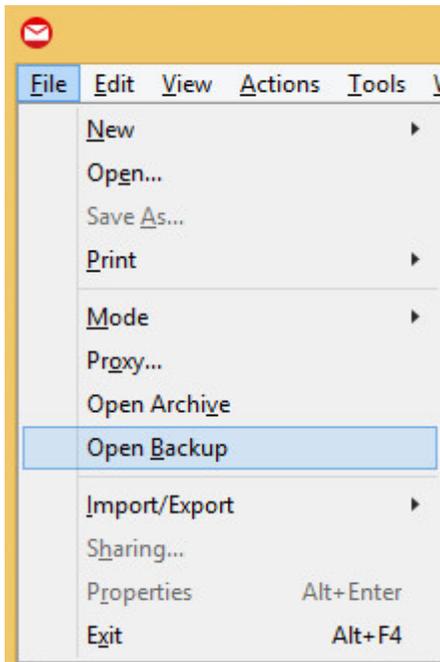
On the GroupWise Disaster Recovery server, load a backup for the profile

1. From the GroupWise Disaster Recovery Web Console, select a Post Office profile
2. Select the Backups tab
3. From the Actions of Existing Backups, select "Turn On Access to the Most Current Backup"

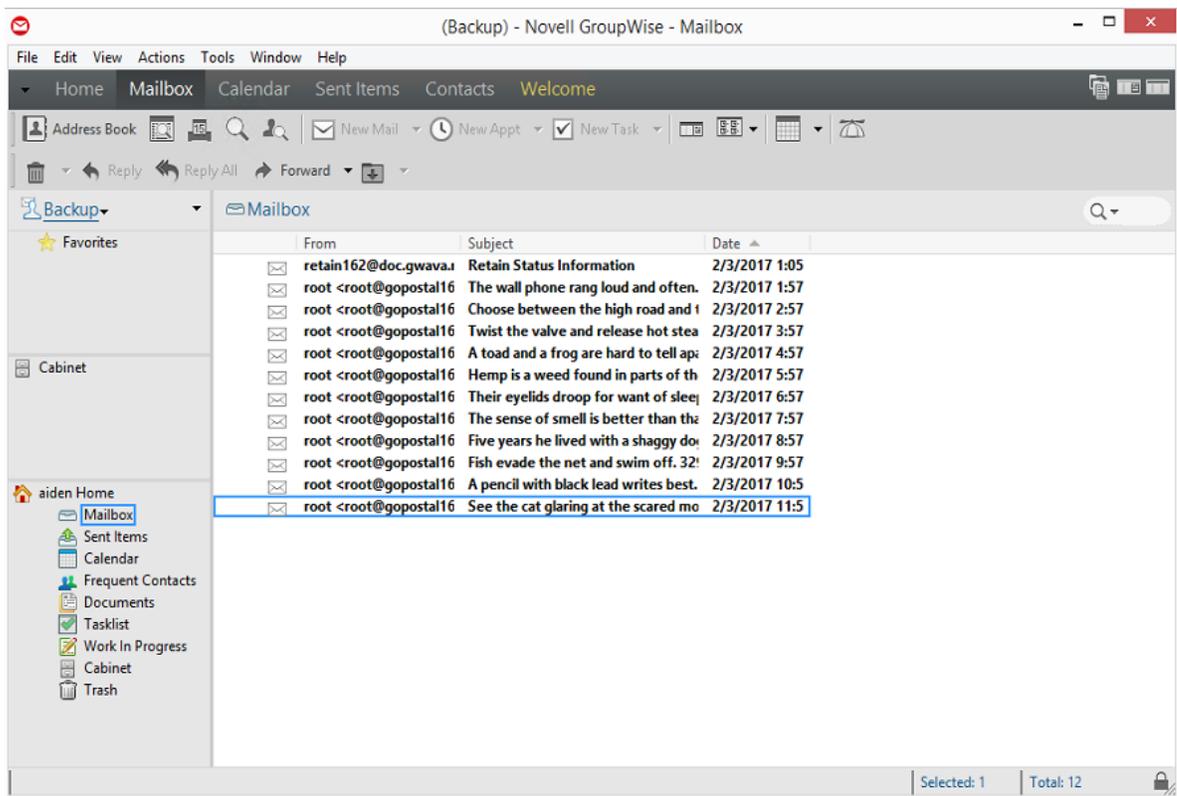


On a workstation with a GroupWise client

1. Move a few items that exist in the backup to the Trash
2. Select *File | Open Backup*.



This view will show the items in the GroupWise Disaster Recovery backup, and NOT on the production GW server for the user.



Troubleshooting

Sometimes the Samba connection fails due to insufficient rights on the GroupWise Disaster Recovery serve side. Providing full rights to the backup directory can help temporarily. The permissions will hold until the mount is unmounted.

On the command line `chmod -R 777 <directory>`. For example,

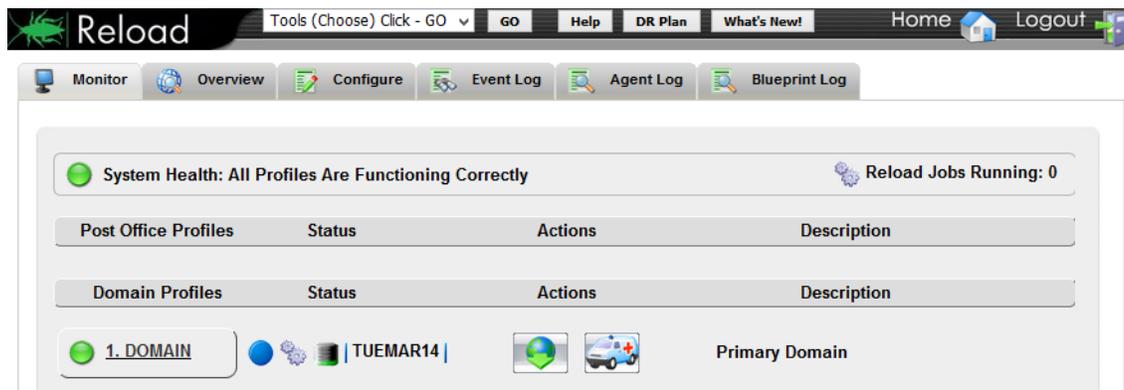
```
chmod -R 777 /reload/
```

Backup Jobs

There are two kinds of backup jobs: “[Domain Backup Jobs](#)” on page 132 and “[Post Office Backup Jobs](#)” on page 136

Domain Backup Jobs

1. Browse to the GroupWise Disaster Recovery Web Administration Console `http://<GroupWise Disaster Recovery_Server_Address>:5555`



2. Select the Profile

The screenshot shows the Reload web interface. At the top, there is a navigation bar with the Reload logo, a search bar containing 'Tools (Choose) Click - GO', and links for 'GO', 'Help', 'DR Plan', 'What's New!', 'Home', and 'Logout'. Below the navigation bar is a breadcrumb trail: '| 1. DOMAIN | Health | Backup Loaded | Job Status | Disk Space | Latest Backup : TUEMAR14 |'. A secondary navigation bar contains tabs for 'Overview', 'Backups', 'Disaster Recovery', 'Configure', 'Event Log', and 'Agent Log'. The main content area is titled '[1. DOMAIN] Domain Profile Status & Information'. It features a 'View All Profiles' button and a list of status items:

- Profile Status: This profile is functioning correctly.
- Backup Access Status: Normal - Disaster Recovery is not enabled
- Job Status: No job is running for this profile
- Disk Space in Use: 12%
- Name of Latest Backup: TUEMAR14
- Profile Description: Primary Domain
- Disaster Recovery Testing: [Untested]
- Profile Path: /reload/domain

Below this list is a 'Domain Information' button. Further down, there are five summary links: 'Latest Backup Status Information', 'Reload Profile Configuration Summary', 'Disaster Recovery Configuration Summary', and 'Backup Configuration Summary'.

3. Enable Intra-Day backups, because you are only as secure as your last backup: Select the *Configure* tab. Open the *Backup Job Settings* panel. Press the *Intra-Day Backup Schedule* button to reveal and enable Intra-Day Backups. The time is the number of hours after the last full backup it will run.
4. Configure Backup Schedule: Press the *Configure All Schedules* button to reveal when the backups will occur, by default: 1:00 AM.

Overview Backups Disaster Recovery Configure Eve

Backup Job Settings

Configure All Profiles

Use This Section to Configure Backups

Number of Backups to Keep: 20

Advanced Settings

Intra-Day Backup Schedule

1st Intra-Day Backup: **Enabled** Hour: 4 Minute: 0

2nd Intra-Day Backup: **Enabled** Hour: 12 Minute: 0

Remove All Reload Job References from CRON: **Do It**

Standard Backup Schedule

Configure All Schedules

Use Standard Backup Schedule: **Enabled**

Sunday	OFF	<input type="button" value="Edit"/>
Monday	01:00	<input type="button" value="Edit"/>
Tuesday	01:00	<input type="button" value="Edit"/>
Wednesday	01:00	<input type="button" value="Edit"/>
Thursday	01:00	<input type="button" value="Edit"/>
Friday	01:00	<input type="button" value="Edit"/>
Saturday	01:00	<input type="button" value="Edit"/>

5.

6. Select the *Backups* tab and open the *GroupWise Disaster Recovery Job Control* panel. Select "Start a Backup Job" to run a job manually.

Reload Tools (Choose) Click - GO GO Help DR Plan What's New! Home

| 1. DOMAIN |  Health |  Backup Loaded |  Job Status |  Disk Space | Latest Backup : TUEMAR14 |

[Overview](#) [Backups](#) [Disaster Recovery](#) [Configure](#) [Event Log](#) [Agent Log](#)

 [Access Backups for Download](#)

-  Download Most Current Domain Backup [TUEMAR14]
-  Select Another Domain Backup For Download
-  Download the Most Recently Selected Backup

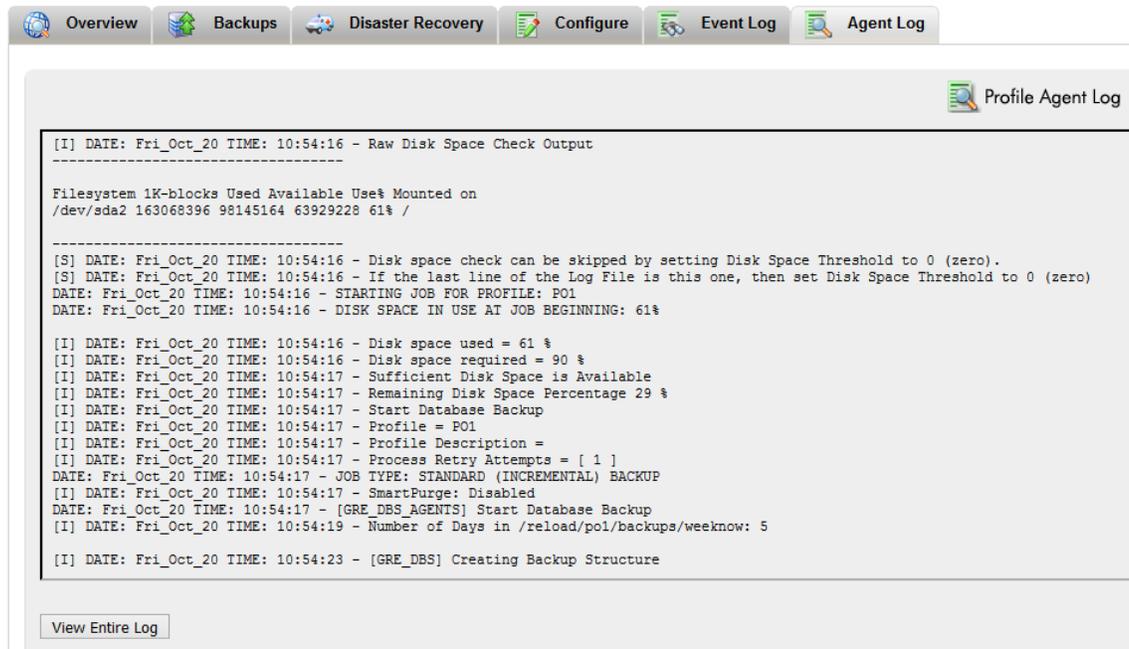
 [Reload Job Control](#)

-  Start a Backup Job
-  Clear Queued Jobs for This Profile 
-  Stop the Currently Running Job for This Profile 

7. On the Home page, the gears will turn green and spin as the job runs.

Domain Profiles	Status	Actions	Description
 1. DOMAIN	   TUEMAR14	 	Primary Domain

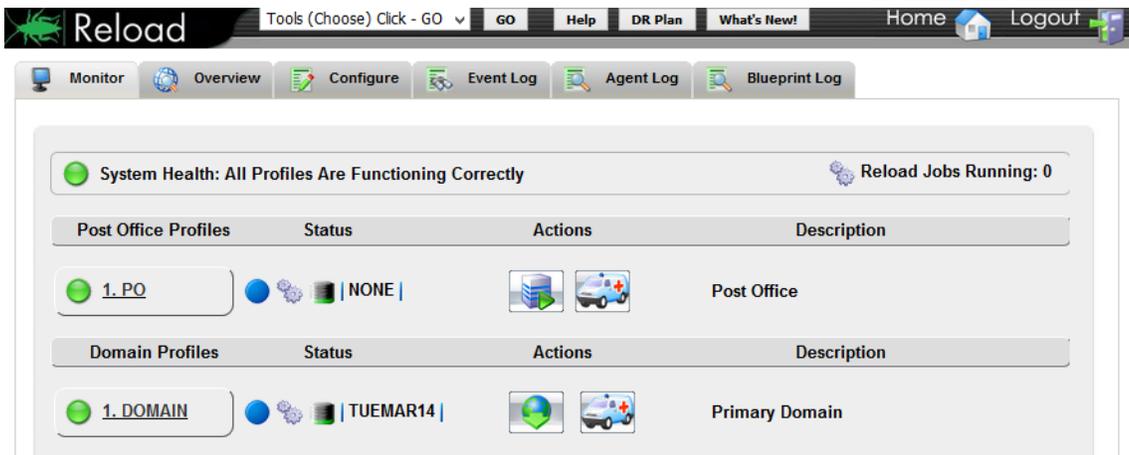
- Job progress can be observed in the Agent Log. This screen is static and will need to be refreshed.



9.

Post Office Backup Jobs

- Browse to the GroupWise Disaster Recovery Web Administration Console http://<GroupWise Disaster Recovery_Server_Address>:5555



- Select the Profile

The screenshot shows the Reload web interface. At the top, there is a navigation bar with the Reload logo, a search bar, and links for Tools, Help, DR Plan, What's New!, Home, and Logout. Below the navigation bar, there is a breadcrumb trail: | 1. PO | Health | Backup Loaded | Job Status | Disk Space | Latest Backup : NONE |. The main content area has a tabbed interface with tabs for Overview, Backups, Disaster Recovery, Configure, Event Log, and Agent Log. The active tab is Overview, which displays the [1. PO] Post Office Profile Status & Information page. This page includes a 'View All Profiles' button and a list of status items: Profile Status (This profile is functioning correctly), Backup Access Status (Normal - No backup is loaded), Job Status (No job is running for this profile), Disk Space in Use (12%), Name of Most Current Backup (NONE), Profile Description (Post Office), and Profile Path (/reload/po). Below the status items is a 'Post Office Information' button. At the bottom of the page, there are five summary links: Latest Backup Summary, Reload Profile Configuration Summary, Disaster Recovery Configuration Summary, and Backup Configuration Summary.

3. Enable Intra-Day backups, because you are only as secure as your last backup: Select the *Configure* tab. Open the *Backup Job Settings* panel. Press the *Intra-Day Backup Schedule* button to reveal and enable Intra-Day Backups. The time is the number of hours after the last full backup it will run.
4. Configure Backup Schedule: Press the *Configure All Schedules* button to reveal when the backups will occur, by default: 1:00 AM.

Overview Backups Disaster Recovery Configure Eve

Backup Job Settings

Configure All Profiles

Use This Section to Configure Backups

Number of Backups to Keep: 20

Advanced Settings

Intra-Day Backup Schedule

1st Intra-Day Backup: **Enabled** Hour: 4 Minute: 0

2nd Intra-Day Backup: **Enabled** Hour: 12 Minute: 0

Remove All Reload Job References from CRON: **Do It**

Standard Backup Schedule

Configure All Schedules

Use Standard Backup Schedule: **Enabled**

Sunday	OFF	<input type="button" value="Edit"/>
Monday	01:00	<input type="button" value="Edit"/>
Tuesday	01:00	<input type="button" value="Edit"/>
Wednesday	01:00	<input type="button" value="Edit"/>
Thursday	01:00	<input type="button" value="Edit"/>
Friday	01:00	<input type="button" value="Edit"/>
Saturday	01:00	<input type="button" value="Edit"/>

5.

6. Select the *Backups* tab and open the *GroupWise Disaster Recovery Job Control* panel. Select "Start a Standard Backup Job [SmartPurge Disabled]" to run a job manually.

Reload Tools (Choose) Click - GO GO Help DR Plan What's New! Home

| 1. PO | Health | Backup Loaded | Job Status | Disk Space | Latest Backup : NONE |

[Overview](#) [Backups](#) [Disaster Recovery](#) [Configure](#) [Event Log](#) [Agent Log](#)

Actions on Existing Backups

- Turn On Access to the Most Current Backup [NONE]
- Turn On Access to Prior Backups
- Turn Off Access to Backups
- Freeze a Backup From Deletion
- Un-Freeze a Backup (Backups With "_F" Are Frozen)

Reload Job Control

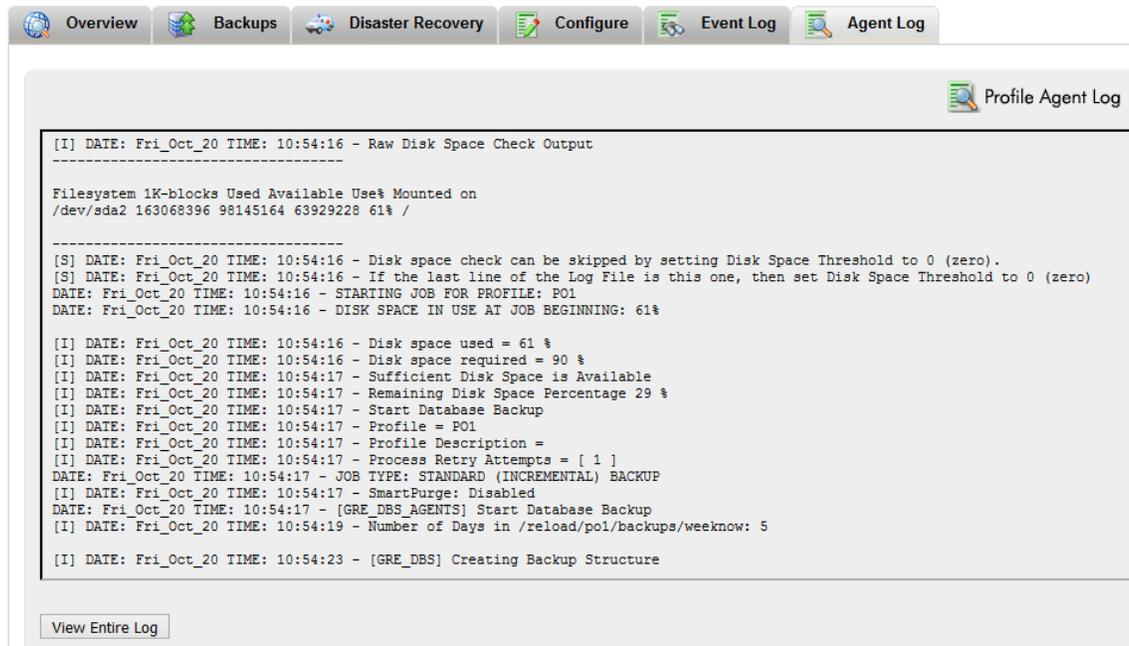
- Start a Standard Backup Job [SmartPurge Disabled] ?
- Start a Standard Backup Job [SmartPurge Enabled] ?
- Clear Queued Reload Jobs for This Profile ?

NOTE: [SmartPurge Disabled] is the Preferred Option!
 Starting a Standard Backup Job manually is fine to do.
 However Reload is designed to start Standard Backup Jobs according to a schedule. At that point, Reload will use the SmartPurge API to advance the Backup Time Stamp in each user's database.

7. On the Home page, the gears will turn green and spin as the job runs.

Post Office Profiles	Status	Actions	Description
1. PO	NONE		Post Office

8. Job progress can be observed in the Agent Log. This screen is static and will need to be refreshed. It will start with a database backup and creating the backup structure, then list users.



The screenshot shows the 'Agent Log' tab in a software interface. The log content is as follows:

```
[I] DATE: Fri_Oct_20 TIME: 10:54:16 - Raw Disk Space Check Output
-----
Filesystem 1K-blocks Used Available Use% Mounted on
/dev/sda2 163068396 98145164 63929228 61% /
-----
[S] DATE: Fri_Oct_20 TIME: 10:54:16 - Disk space check can be skipped by setting Disk Space Threshold to 0 (zero).
[S] DATE: Fri_Oct_20 TIME: 10:54:16 - If the last line of the Log File is this one, then set Disk Space Threshold to 0 (zero)
DATE: Fri_Oct_20 TIME: 10:54:16 - STARTING JOB FOR PROFILE: PO1
DATE: Fri_Oct_20 TIME: 10:54:16 - DISK SPACE IN USE AT JOB BEGINNING: 61%

[I] DATE: Fri_Oct_20 TIME: 10:54:16 - Disk space used = 61 %
[I] DATE: Fri_Oct_20 TIME: 10:54:16 - Disk space required = 90 %
[I] DATE: Fri_Oct_20 TIME: 10:54:17 - Sufficient Disk Space is Available
[I] DATE: Fri_Oct_20 TIME: 10:54:17 - Remaining Disk Space Percentage 29 %
[I] DATE: Fri_Oct_20 TIME: 10:54:17 - Start Database Backup
[I] DATE: Fri_Oct_20 TIME: 10:54:17 - Profile = PO1
[I] DATE: Fri_Oct_20 TIME: 10:54:17 - Profile Description =
[I] DATE: Fri_Oct_20 TIME: 10:54:17 - Process Retry Attempts = [ 1 ]
DATE: Fri_Oct_20 TIME: 10:54:17 - JOB TYPE: STANDARD (INCREMENTAL) BACKUP
[I] DATE: Fri_Oct_20 TIME: 10:54:17 - SmartPurge: Disabled
DATE: Fri_Oct_20 TIME: 10:54:17 - [GRE_DBS_AGENTS] Start Database Backup
[I] DATE: Fri_Oct_20 TIME: 10:54:19 - Number of Days in /reload/po1/backups/weeknow: 5

[I] DATE: Fri_Oct_20 TIME: 10:54:23 - [GRE_DBS] Creating Backup Structure
```

At the bottom of the log window, there is a button labeled 'View Entire Log'.

9.

Post-Backup Tasks

Once GroupWise Disaster Recovery has been installed, profiles created, backups saved and Restore Areas setup, additional configuration tasks may be completed.

These tasks include:

Auto-GroupWise Disaster Recovery for always on backup access

Tape backups for long term storage

The number of backups to keep

Configure Auto-GroupWise Disaster Recovery

GroupWise Disaster Recovery can be set to always have the latest backup available so users can just use the Restore area without having to make a call to the helpdesk. This won't help if they deleted something a week ago, an older backup will need to be activated but it does reduce calls to the helpdesk.

Prerequisites

1. Profile created
2. Backup stored
3. Restore Area setup

Configure Auto-GroupWise Disaster Recovery

1. Browse to the GroupWise Disaster Recovery Server Web Administration Console
2. Select the Profile for the Post Office
3. Under the *Configure* tab, under the section "User Access to Backups", enable "[Auto-Reload] Load the Most Recent Backup:"

The screenshot shows the Reload web administration console. The top navigation bar includes 'Tools (Choose) Click - GO', 'GO', 'Help', 'DR Plan', and 'What's New!'. Below this is a status bar with '1. PO | Health | Backup Loaded | Job Status | Disk Space | Latest Backup : TUEMAR14'. The main navigation tabs are 'Overview', 'Backups', 'Disaster Recovery', 'Configure', 'Event Log', and 'Agent Log'. The 'Configure' tab is active, showing a 'Preferences' section and a 'User Access to Backups' section. The 'User Access to Backups' section includes a 'Configure All Profiles' button and a warning icon with the text 'Use This Section to Configure What Happens When Access to a Backup is Turned On'. Below this are several configuration items: 'Load the Access Mode GroupWise POA: Enabled' with an 'Edit' button; 'Access Mode POA TCP/IP Address: 10.1.4.161' with an 'Edit' button; 'Client/Server Port: 1677' with an 'Edit' button; 'POA HTTP Configuration' and 'POA SOAP Configuration' buttons; 'Link Backup to Restore Area: Enabled' with an 'Edit' button; '[Auto-Reload] Load the Most Recent Backup: Enabled' with a 'Save' button; and '[Auto-Restore] Connect Backup to Restore Area: Disabled' with an 'Edit' button.

Configure Tape Backups

GroupWise Disaster Recovery can create TAR files for long term backup storage. GroupWise Disaster Recovery creates a single file from the previous week's worth of backups, but can be set to split it into smaller chunks that will fit the backup media. Advanced settings can be used to run bash scripts before and/or after the tape backup runs.

Prerequisite

- ♦ Create a directory for the tape backup TAR files. This can be a mount to another server. For example,

```
mkdir /reload/tape
```

Configure Tape Backups

1. Browse to the GroupWise Disaster Recovery Web Console
2. Select the Profile
3. Select the Configure tab
4. Open the Tape Backup panel
5. Set *Create Tape Archive Files* to Enabled, and save.
6. Set the *Tape Archive File Storage Path*, and save.

By default, the schedule is Saturday at 2:00AM. This can be changed under Tape Backup Schedule.

The screenshot shows the Reload web administration interface. At the top, there is a navigation bar with the Reload logo and a menu with items: Tools (Choose) Click - GO, GO, Help, DR Plan, and What's New!. Below this is a status bar with: 1. PO | Health | Backup Loaded | Job Status | Disk Space | Latest Backup : TUEMAR14 |. The main navigation menu includes: Overview, Backups, Disaster Recovery, Configure, Event Log, and Agent Log. The main content area displays several configuration sections: Post Office and POA Settings, Disaster Recovery [FAILOVER], Migration, Disaster Recovery [FAILBACK], QuickFinder Resolution Agent, and Tape Backups. The Tape Backups section is expanded, showing a 'Configure All Profiles' button and three settings: 'Create Tape Archive Files' (Enabled), 'Expire Previously Created Tape Archive Files' (Enabled), and 'Tape Archive File Storage Path' (/reload/tape). Below these are buttons for 'TAR Split/ZIP Settings', 'Advanced Settings', and 'Tape Backup Schedule'.

Configure Number of Backups to Keep

By default, GroupWise Disaster Recovery keeps 14 days of backups. You can increase or decrease the amount as needed.

This setting is found in the GroupWise Disaster Recovery Web Administration under the *Profile configuration* | <select desired profile> | *Configure* | *Backup Job Settings* | *Number of Backups To Keep*

Disaster Recovery Configuration

Disaster Recovery Mode allows the GroupWise Disaster Recovery server to take over the duties of the domain, MTA, GWIA and/or one or more POs.

Configuring Disaster Recovery (DR) takes substantial time, while it could be done during a disaster it would be best to configure Disaster Recovery prior to an actual disaster, when loss of communications may be an issue.

When setup correctly, during a disaster you will only need to enable Disaster Recovery Mode and change the DNS A record to point to the correct server. Your users will need to restart their client to connect to the new server but it should continue on without further disruption.

When designing your disaster recovery plan there are, basically, two types of disasters to prepare for:

- ◆ Server failure
- ◆ Site failure

A Server failure is just that: the server fails. The power supply or hard drive system fails and the server goes down and doesn't come back up. A system update goes bad or malware got through.

A Site failure is the server room is no longer functional. There is a power failure, or perhaps the sprinkler system went off by accident or the site was hit by a tornado.

Configure Disaster Recovery

This step takes some time to setup, so it is best to do this before the disaster. While it can be done during the disaster it is much harder and takes much longer until mail flow is reestablished.

If Disaster Recovery is setup correctly, it will take only seconds to be live on the GroupWise Disaster Recovery server as the DNS A record is updated and the Disaster Recovery POA is enabled.

IP Addresses

On the GroupWise Disaster Recovery server, for each Post Office Profile:

Provide an available IP address. None of these should be the IP address of the GroupWise Disaster Recovery server.

Bind the IP address to the NIC on the GroupWise Disaster Recovery server. It is recommended to provide an alias to distinguish them easily. This can be set up in: YaST >> Network Devices >> Network Settings, select the appropriate NIC device, select 'Edit', and add the IP address aliases there.

DNS

You will need to set several A Record names in your DNS. This is the one setting you'll have to change outside of GroupWise Disaster Recovery during a disaster. When the disaster is over and the production GroupWise server is ready to go live the A Record will need to be changed back.

By configuring names and using them throughout your system your users will not need to change any settings and will see minimal disruption.

Configure DNS A Records:

For each domain, and post office, create an A Record in the DNS.

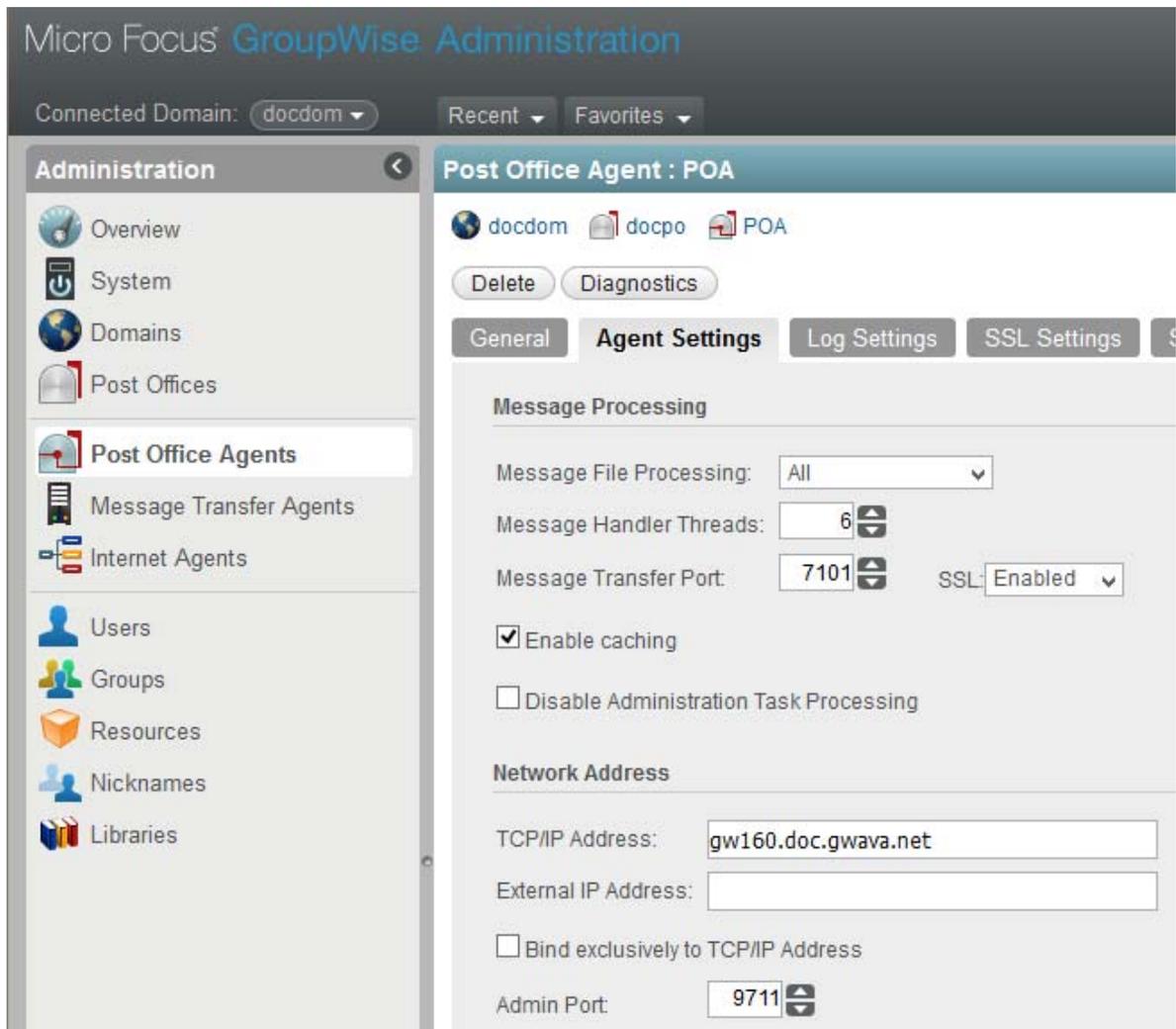
- ♦ *GroupWise Server*. For example, gw100.company.com 10.1.1.100
- ♦ *Domain*. For example, gwdom.company.com 10.1.1.100
- ♦ *Post Office*. For example, gwpo.company.com 10.1.1.100
- ♦ *MTA*. For example, gwmta.company.com 10.1.1.100

GroupWise Server

Configure the Live GroupWise server to use domain names.

POA

1. Set the POA to use the hostname, in *Groupwise Administration | Post Office Agents | <poa> | Agent Settings | Network Address | TCP/IP Address*
2. Disable "*Bind exclusively to TCP/IP Address*" and Save
3. Confirm that the MTP port is specified, by default 7101. MTP communication is not only a faster means of communication between MTAs and POAs, but it is essential disaster recovery purposes. If the MTP port is different that will need to be entered into GroupWise Disaster Recovery later on.



MTA

1. Set the MTA to use the hostname, in *Groupwise Administration | Message Transfer Agents | <mta> | Agent Settings | Network Address | TCP/IP Address*
2. Disable "*Bind exclusively to TCP/IP Address*" and Save
3. Confirm that the MTP port is specified, by default 7100. MTP communication is not only a faster means of communication between MTAs and POAs, but it is essential disaster recovery purposes. If the MTP port is different that will need to be entered into GroupWise Disaster Recovery later on.

Micro Focus GroupWise Administration

Connected Domain: docdom Recent Favorites

Administration

- Overview
- System
- Domains
- Post Offices
- Post Office Agents
- Message Transfer Agents**
- Internet Agents
- Users
- Groups
- Resources
- Nicknames
- Libraries

MTA : MTA

docdom MTA

Delete Diagnostics

General **Agent Settings** Log Settings SSL Settings

Scan Cycle: 15 seconds

Scan High: 5 seconds

Attach Retry: 60 seconds

Enable Automatic Database Recovery

Use 2nd High Priority Scanner

Use 2nd Mail Priority Scanner

SNMP Community "Get" String:

Network Address

TCP/IP Address: gw160.doc.gwava.net

Admin Port: 9710

Bind exclusively to TCP/IP Address

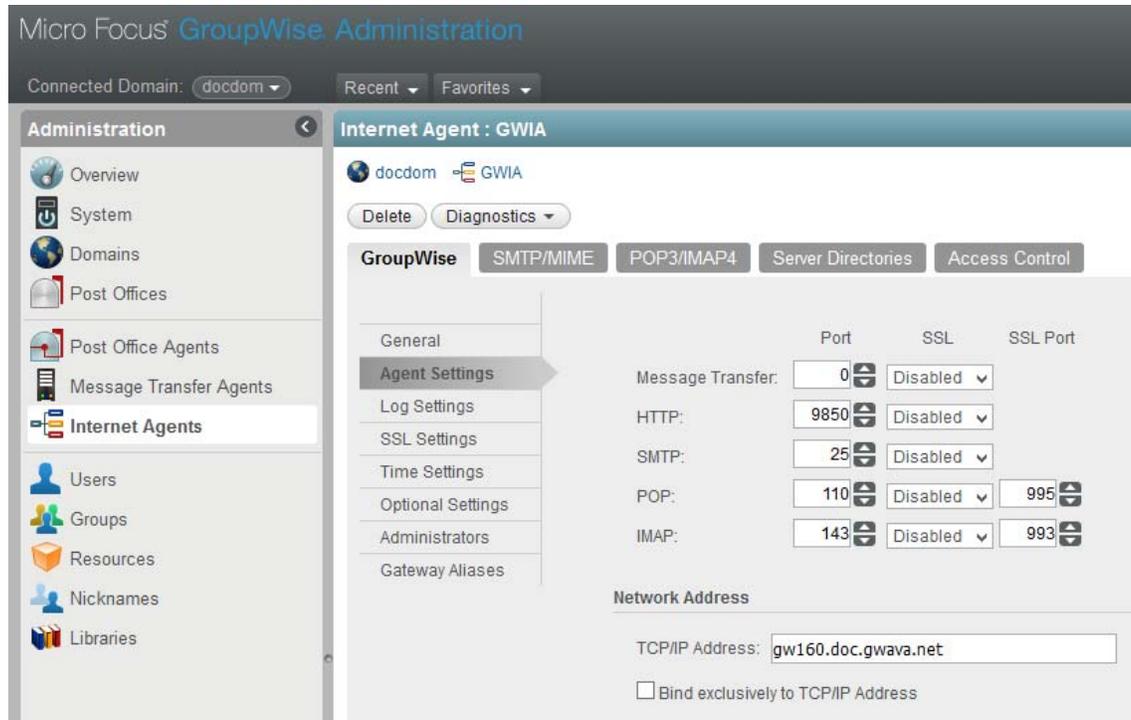
Message Transfer

Port: 7100 SSL: Enabled

GWIA

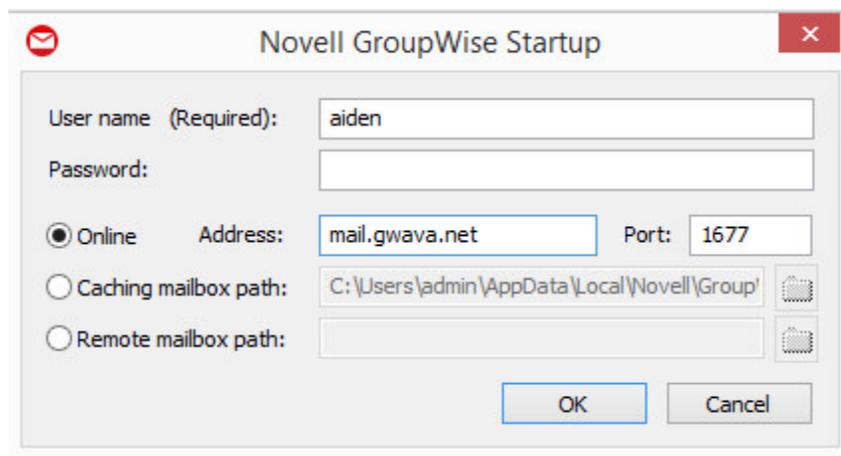
1. Set the GWIA to use the hostname, in *Groupwise Administration* | *Message Transfer Agents* | *<gwia>* | *Agent Settings* | *Network Address* | *TCP/IP Address*

2. Disable "Bind exclusively to TCP/IP Address" and Save



GroupWise Client

- ◆ Set the GroupWise Client on all workstations to connect using a domain name. For example, gwpo.company.com. This allows the DNS A Record for the Post Office to be changed and the users will not notice a difference. If this is not set, then during a disaster you will be trying to contact all users and telling them what address to connect to.



GroupWise Disaster Recovery Server

Configure Domain

1. Browse to the Web Administration Console and select the *Domain* profile.

2. Under the Configure tab, open the *Disaster Recovery {FAILOVER}* section
3. The TC/IP Address should be pre-set to the GroupWise Disaster Recovery server.
4. MTAs and POAs should always be configured to communicate via MTP (Message Transfer Protocol vs. message file queuing and message file scanning) to one another. MTP communication is not only a faster means of communication between MTAs and POAs, but it is essential for disaster recovery purposes.

Make sure that the MTAs and the POAs have an MTP port specified. Typically the MTP port for the MTA is 7100, and the MTP port for the POA is 7101.

5. Configure the profile settings to match those of the live GroupWise domain. Confirm the ports used.

If you have multiple domains you will want to set this to separate addresses bound to the network card.

The screenshot shows the Reload web interface. At the top, there is a navigation bar with the Reload logo and several menu items: Tools (Choose) Click - GO, GO, Help, DR Plan, and What's New!. Below this is a status bar showing: 1. DOMAIN | Health | Backup Loaded | Job Status | Disk Space | Latest Backup : WEDMAR15 |. The main navigation area includes tabs for Overview, Backups, Disaster Recovery, Configure, Event Log, and Agent Log. The Configure tab is active, and the Disaster Recovery [FAILOVER] section is selected. This section contains a 'Configure All Profiles' button, a warning icon with the text 'Use This Section to Configure What Reload Does When Disaster Recovery [FAILOVER] is Enabled', and a 'Disaster Recovery MTA Settings' section. Under MTA Settings, there are two fields: 'TCP/IP Address: 10.1.4.161' and 'MTP Port: 7100', each with an 'Edit' button. Below these are three more configuration buttons: 'MTA HTTP Configuration', 'Failover Settings', and 'Advanced Failover Settings'.

Configure Post Office

1. Browse to the GroupWise Disaster Recovery Web Administration Console and select the *Post Office* profile
2. Under the Configure tab, open the *Disaster Recovery {FAILOVER}* section
3. The TC/IP Address should be pre-set to the GroupWise Disaster Recovery server
4. Configure the profile settings to match those of the live GroupWise domain
If you have multiple post offices you will want to set this to separate addresses bound to the network card.
5. Outbound Message Transfer Port (Domain MTA) (MTP) Address

The screenshot shows the Reload web administration console. The top navigation bar includes a logo, a search box, and buttons for Tools, GO, Help, DR Plan, and What's New!. Below this is a status bar with indicators for PO, Health, Backup Loaded, Job Status, Disk Space, and Latest Backup (TUEMAR14). The main navigation menu contains Overview, Backups, Disaster Recovery, Configure, Event Log, and Agent Log. The Configure tab is active, showing several configuration sections: User Access to Backups, Backup Job Settings, Post Office and POA Settings, and Disaster Recovery [FAILOVER]. The Disaster Recovery [FAILOVER] section is expanded, displaying a 'Configure All Profiles' button and a warning message: 'Use This Section to Configure What Reload Does When Disaster Recovery [FAILOVER] is Enabled'. Underneath, there are 'Disaster Recovery POA Settings' with the following fields: TCP/IP Address (10.1.4.161), Client/Server Port (1677), Inbound Message Transfer Port (MTP) (7101), and Outbound Message Transfer Port (Domain MTA) (MTP) Address (10.1.4.161) and Port (7100). At the bottom of this section are buttons for POA HTTP Configuration, POA SOAP Configuration, Failover Settings, and Advanced Failover Settings.

Testing Disaster Recovery

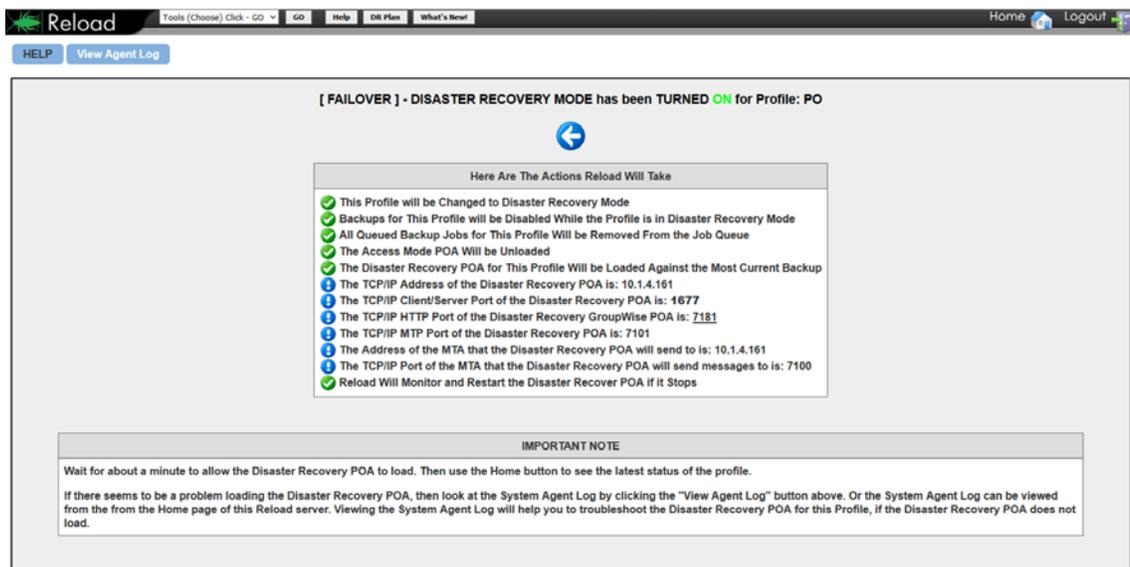
Disaster Recovery can be tested without downing the production GroupWise server by activating the Disaster Recovery POA and connecting to it with a GroupWise client.

A full-scale test should be run that shuts down the production mail server. Attempts to send and receive from external email systems so all parts are tested and mail flows properly. DNS changes, or GroupWise systems changes can effect Disaster Recovery Mode functionality. A full-scale test where the product GroupWise POA is shut down should be run yearly.

Post Office Test

The simplest test is to enable Disaster Recovery mode POA and see if a client can connect by entering the IP of the GroupWise Disaster Recovery server DR POA

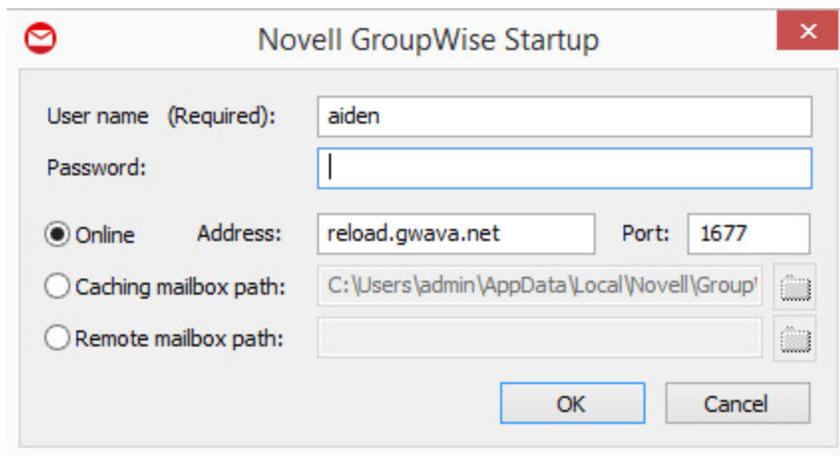
1. Close the GroupWise client if it is open
2. Browse to the GroupWise Disaster Recovery Web Administration Console
3. Click on the Post Office profile ambulance to engage Disaster Recovery Failover Mode



4. Went Ambulance lights are on and the Red Arrow is up the DR POA is active.



5. Open the GroupWise client and instead of logging into the production Post Office, enter the hostname or IP address of the GroupWise Disaster Recovery server.



Test the Disaster Recovery system:

1. Send a message internally to someone on the same Post Office.
2. Send a message internally to someone on the same Domain.
3. Send a message externally to someone on the Internet.

End the test:

4. Click on the Post Office profile ambulance to disengage Disaster Recovery Failover Mode.

The ambulance lights will turn off.

If a backup was loaded before Disaster Recovery mode was enabled, the red up arrow will change to a green right arrow.

Otherwise, the red up arrow will change to a blue dot.

Create Disaster Recovery GWIA

This step is optional, it depends on the design of your GroupWise system, and has nothing to do with GroupWise Disaster Recovery itself.

If your GroupWise server fails you may lose the GWIA as well and mail will not flow. It is prudent to set up a secondary GWIA for disaster recovery.

Setting up a GWIA is a GroupWise function. Please see GroupWise documentation for [setting up an alternate GWIA for a domain \(https://www.novell.com/documentation/groupwise2014r2/gw2014_guide_admin/data/adm_gwia_config_alternate.html\)](https://www.novell.com/documentation/groupwise2014r2/gw2014_guide_admin/data/adm_gwia_config_alternate.html).

Prerequisite

Set up, configure and test Disaster Recovery before a disaster.

Concept

1. Create a secondary GW domain on a server in the off-site disaster recovery location.
2. Create the GWIA off the secondary GW domain.
3. In GroupWise administration, define the GWIA as the secondary GWIA.

Retain Integration

Retain archives best when archiving the items directly. However, as an alternative to archiving messages directly from GroupWise, GroupWise Disaster Recovery can run a POA that Retain can archive from. This is useful for archiving data from unstable GroupWise servers or dealing with archiving from tape backups. This is different from the GroupWise Disaster Recovery for Retain product which backs up the Retain server to the GroupWise Disaster Recovery server.

This feature sets up a POA that is active almost all the time for Retain to connect to archive from, except for short periods as GroupWise Disaster Recovery switches to the latest backup.

Prerequisites

Since this requires running a POA, it is best to bind an extra IP address to the server for the Retain POA or you will need to make sure to change the POA settings in such a way that it does not interfere with the Access Mode POA or Disaster Recovery POA.

There must be an existing Post Office Profile and backup in place.

GroupWise Disaster Recovery Setup

Retain Integration is setup on a per Profile basis. Each Post Office Profile will have to be configured to use this feature.

On the GroupWise Disaster Recovery server, go to GroupWise Disaster Recovery Administration by running:

reload

Then go to *Profiles | Post Office Profile*

1. Select the desired profile
2. Select "Advanced Profile Configuration Menu"
3. Select "Retain Integration Settings"
4. Select "Retain to Reload Integration Configuration Wizard"
 - a. Enter the GroupWise Post Office name
 - b. Enter the GroupWise Domain name
 - c. Enter the Retain Worker Password (This can be set in the Retain Console, by default it is the Retain admin password)

- d. Enter the IP address and ports the Retain POA will bind to. If this POA will be sharing the IP address with any other GroupWise Disaster Recovery POA, the Client, SOAP, and HTTP connection ports must be unique to avoid port conflicts. GroupWise Disaster Recovery should be installed on a machine other than the live POA server, but the standard ports are usually best used for one of the other GroupWise Disaster Recovery POAs, (Disaster, Restore, and Access). Pick a port for each connection which you know is open. Retain will pull all necessary connection information from the GroupWise Disaster Recovery server. There is no need to enter these settings into the Retain Server.
- e. To mitigate the chances of getting Retain Worker archive errors while working against a GroupWise Disaster Recovery POA, it is **STRONGLY** recommended that GroupWise Disaster Recovery is set to create highly consistent backups. This setting is located at *Main menu | Profiles | (Select Profile) | Standard | Advanced | Consistency: Set to highest.*

Retain Setup

On the Retain Web Console:

1. Set the worker password:
 - a. This can be set in the Retain Web Console under *Workers | <desired worker> | Connection tab*, by default it is the Retain admin password
 - b. If the password is changed, the Worker bootstrap will need to be updated.
 - c. To remove an existing Worker bootstrap:
 - i. On the Retain server, stop tomcat
 - ii. Navigate to */opt/beginfinite/retain/RetainWorker/WEB-INF/cfg/* or wherever the worker is stored and remove *RetainWorker2.cfg*
 - iii. Start tomcat
2. Create a Profile for use with GroupWise Disaster Recovery:
 - a. Set the Scope "Date Range to Scan":
 - b. If using *Retain 4.1 or higher*. set to New Items stores which items have been archived internally.
 - c. If using *Retain 4.0.3.1 or lower*. set to Publish all messages newer than last stored message (fast) and the "Set Storage Flags" must be set to "Item Store Flag"
3. Create a Job as normal with Schedule, Profile, and Worker:
 - a. Under the *Reload tab*:
 - i. Set "Enable Reload Integration"
 - ii. Set "Server Protocol" http or https
 - iii. Set "Server Host Name" to the Reload server hostname or IP address
 - iv. Set "Server Port", default 5555
 - b. Select Mailboxes to dredge

Now the job will dredge the GroupWise Disaster Recovery server rather than the GroupWise server.

6 Restoration

Restoring Items Overview

Since GroupWise Disaster Recovery is a backup solution it has the ability to restore items to GroupWise.

That are two methods for restoring items: Restore mode and Access mode.

Restore mode uses the GroupWise restore area manager to allow GroupWise to access the backed up items directly.

Access mode uses a POA on the GroupWise Disaster Recovery server that the GroupWise client can access directly, the items can be archived and then restored after reconnecting to the production GroupWise system.

Prerequisites

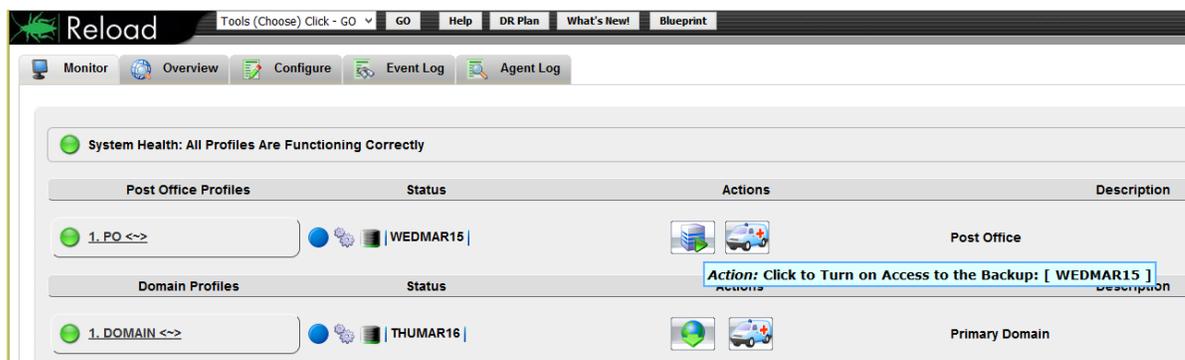
1. Configure the Restore Area
2. Have backups

Loading a Backup

On the GroupWise Disaster Recovery server

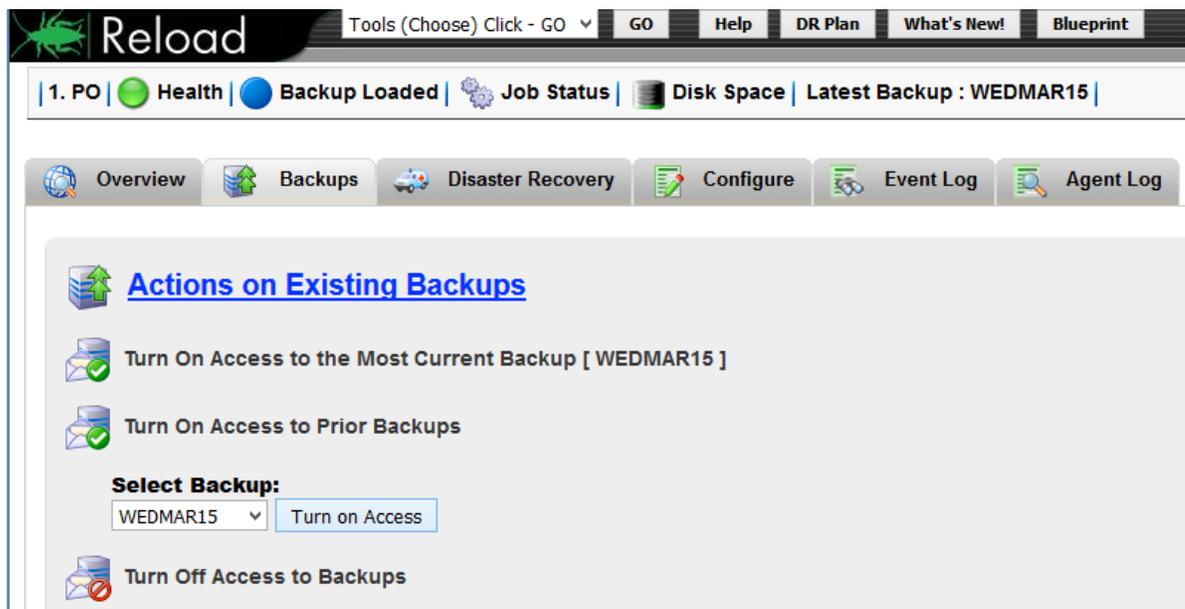
Most Recent Backup

1. To load the most recent backup browse to *GroupWise Disaster Recovery Web Administration Console* | *<Profile>* | *Turn On Access to Backup* action button



Prior Backup

1. To load a prior backup browse to *GroupWise Disaster Recovery Web Administration Console* | *<Profile>* | *Backups tab* | *Turn On Access To Prior Backups* | *<Backup>*



Restore Mail Items

One or more items can be restored to the user's mailbox. There are two modes for restoring items: Restore mode and Access mode.

- ♦ “[Restore Mode](#)” on page 156 uses GroupWise's restore area to allow the user to use the GroupWise client to restore their items.
- ♦ “[Access Mode](#)” on page 158 has the Client access the GroupWise Disaster Recovery POA directly where the item(s) can be archived and then unarchived once attached to the production GroupWise server.

Restore Mode

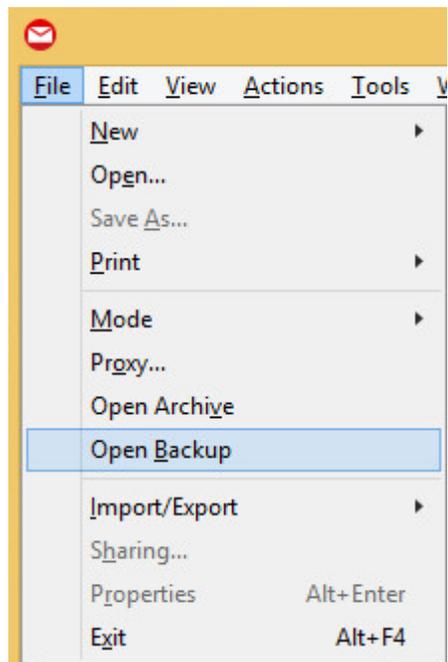
Restore mode uses GroupWise's restore area to allow the user to use the GroupWise client to restore their items.

On the GroupWise Disaster Recovery server

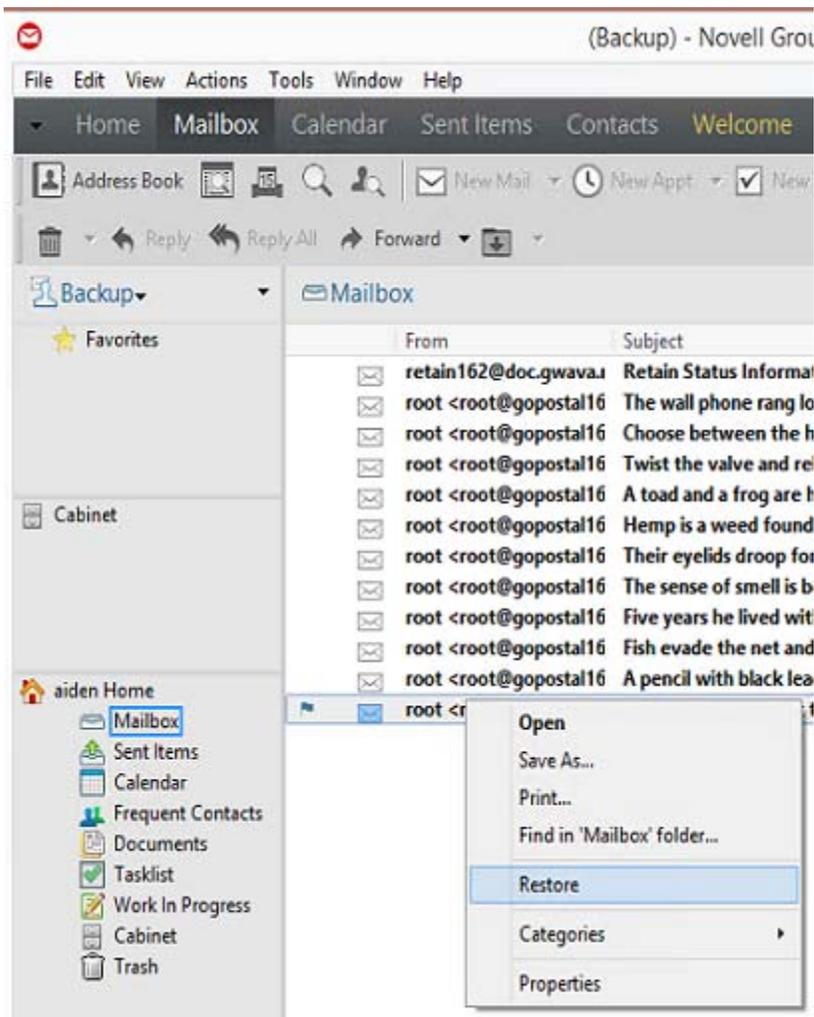
- ♦ Load a backup on the GroupWise Disaster Recovery server from a time period where the item existed

On the GroupWise Client Workstation

1. On the user's workstation open the GroupWise client
2. Select "*File | Open Backup*". This will show the items on the GroupWise Disaster Recovery POA and *not* available on the production GroupWise server



3. Select the item(s) to be restored
4. Right-click and select "Restore"



Access Mode

Access mode has the Client access the GroupWise Disaster Recovery POA directly where the item(s) can be archived and then unarchived once attached to the production GroupWise server.

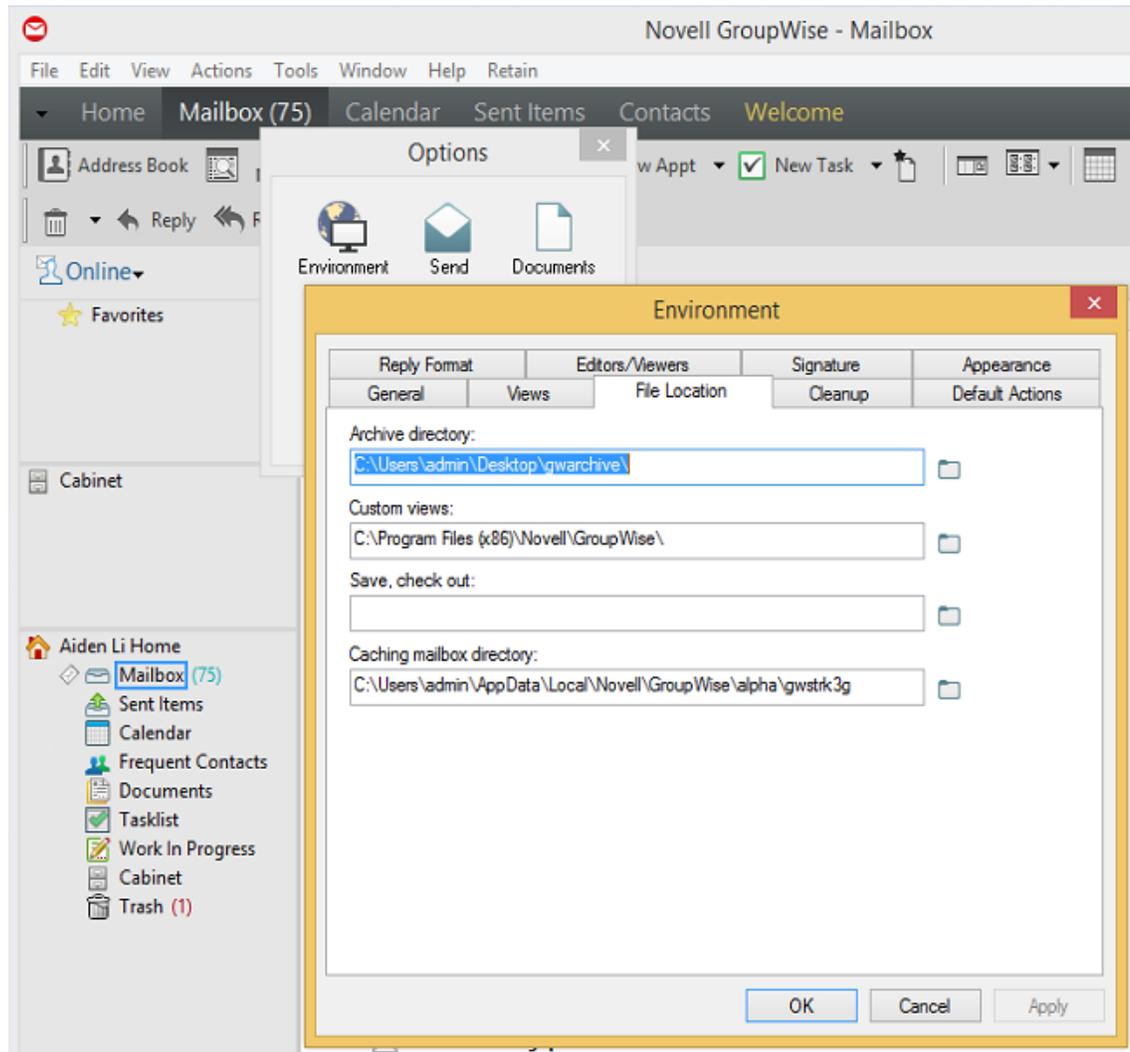
Personal archives must be enabled in GroupWise Administration.

On the GroupWise Disaster Recovery server

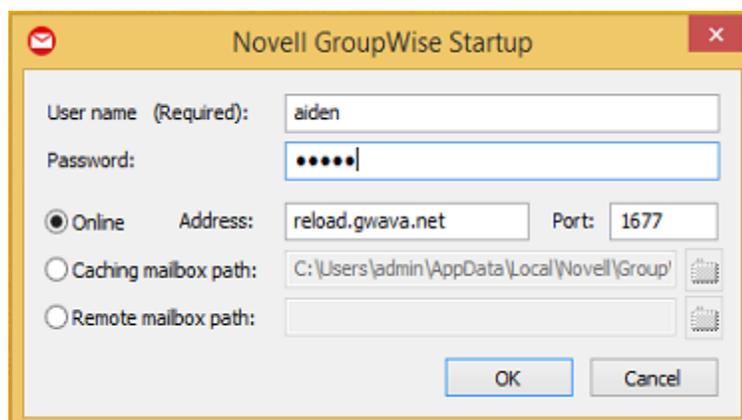
1. If needed, enable the access mode POA in *GroupWise Disaster Recovery Web Administration Console* | <Profile> | *Configure* | *User Access to Backups*
2. Load a backup on the GroupWise Disaster Recovery server from a time period where the item existed
3. The address the client must connect to can be found in the *GroupWise Disaster Recovery Web Administration Console* | <Profile> | *Backups tab* | *GroupWise Client Access to GroupWise Disaster Recovery Backups*

On the GroupWise Client Workstation

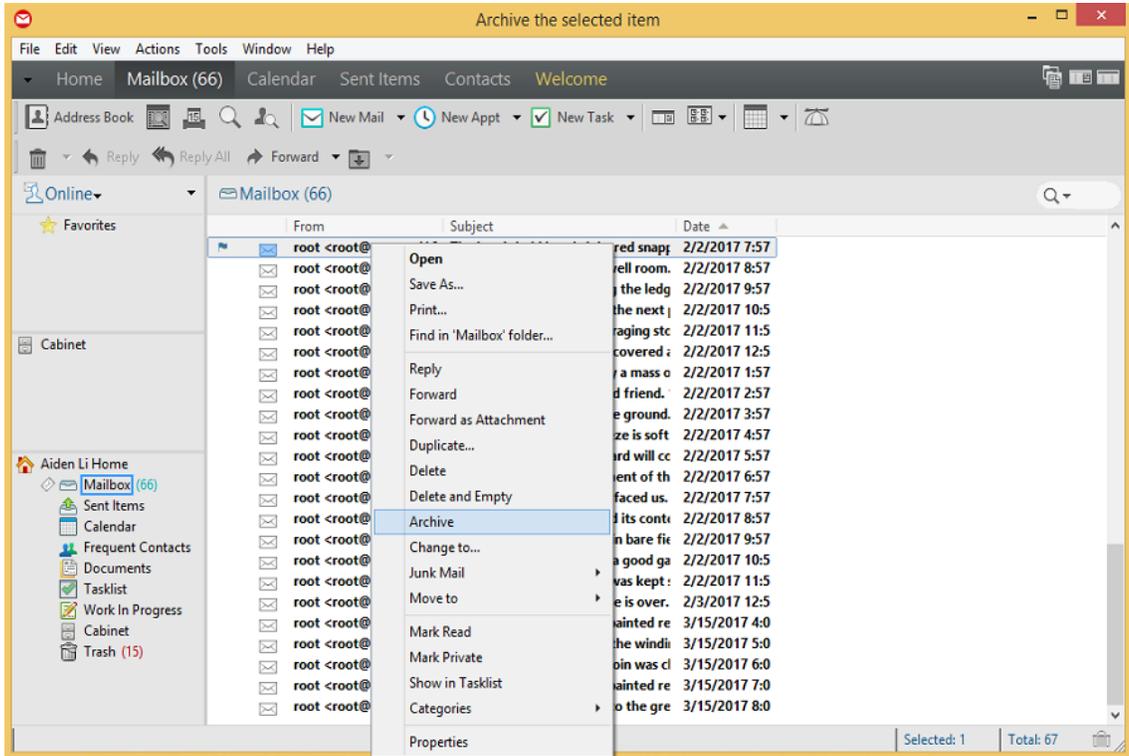
1. An archive directory must be set in *GroupWise Client | Tools | Options | Environment | File Locations | Archive Directory*



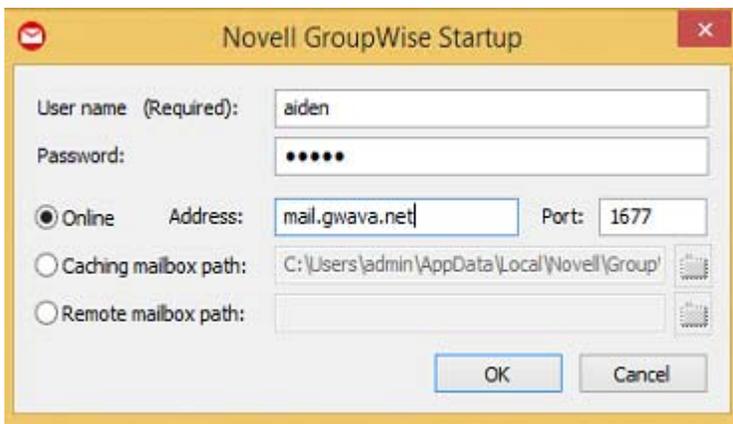
2. Open the GroupWise client and connect to the POA on the *GroupWise Disaster Recovery server*



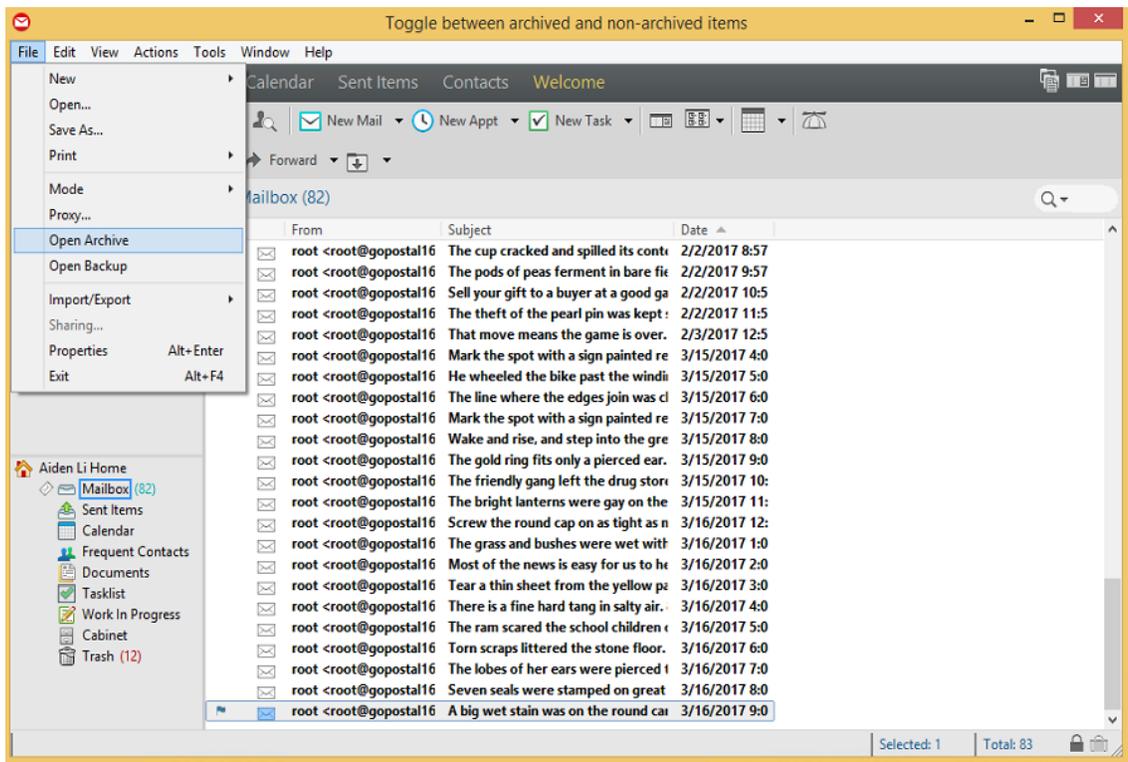
3. Right-click on the item and select "Archive"



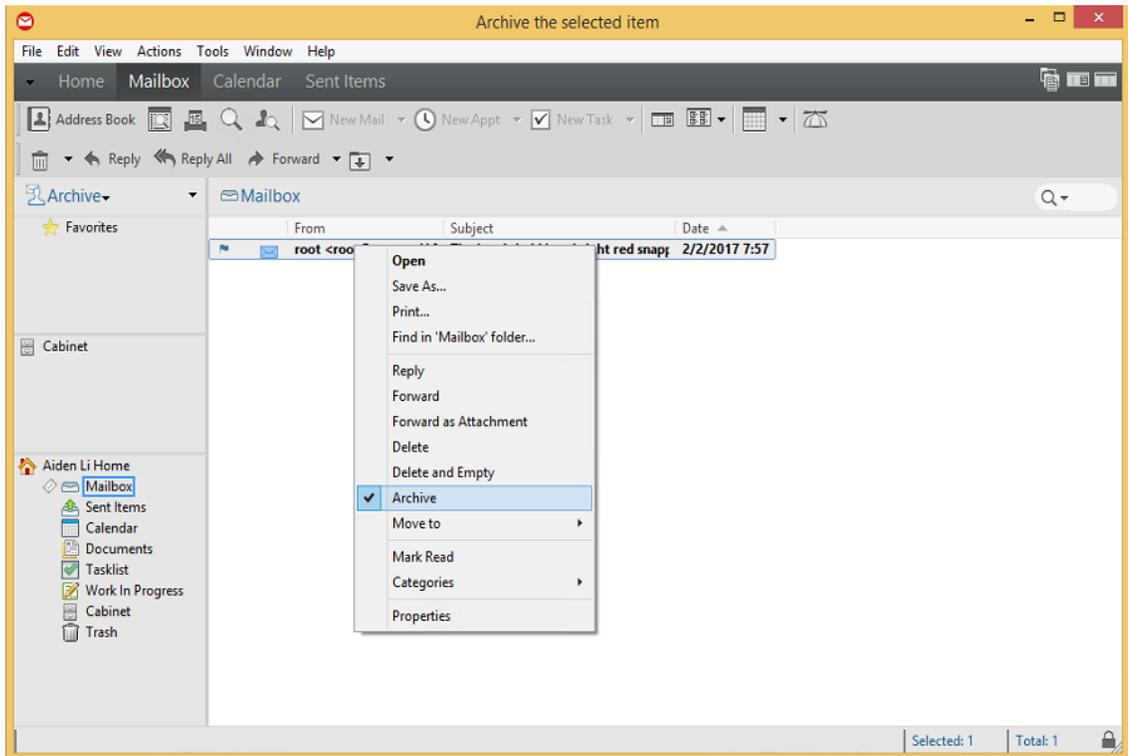
4. Exit GroupWise Client
5. Reopen the GroupWise Client and connect to the POA on the *Production GroupWise* server



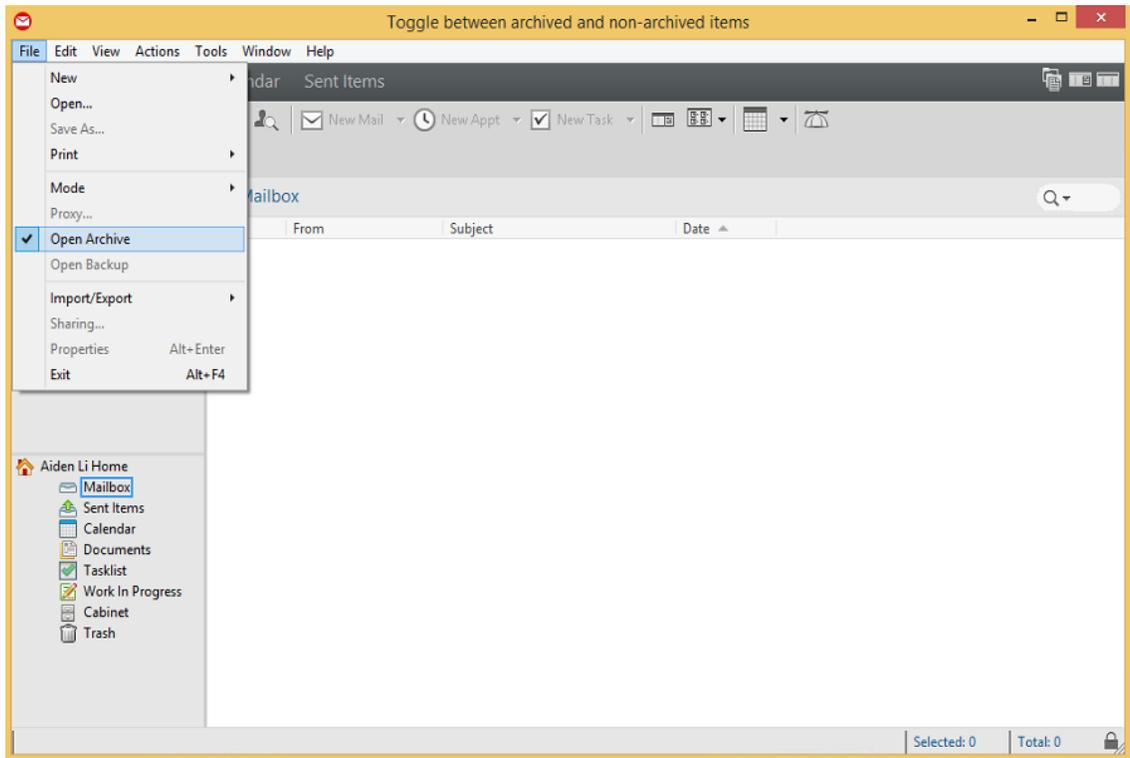
6. Select "File | Open Archive"



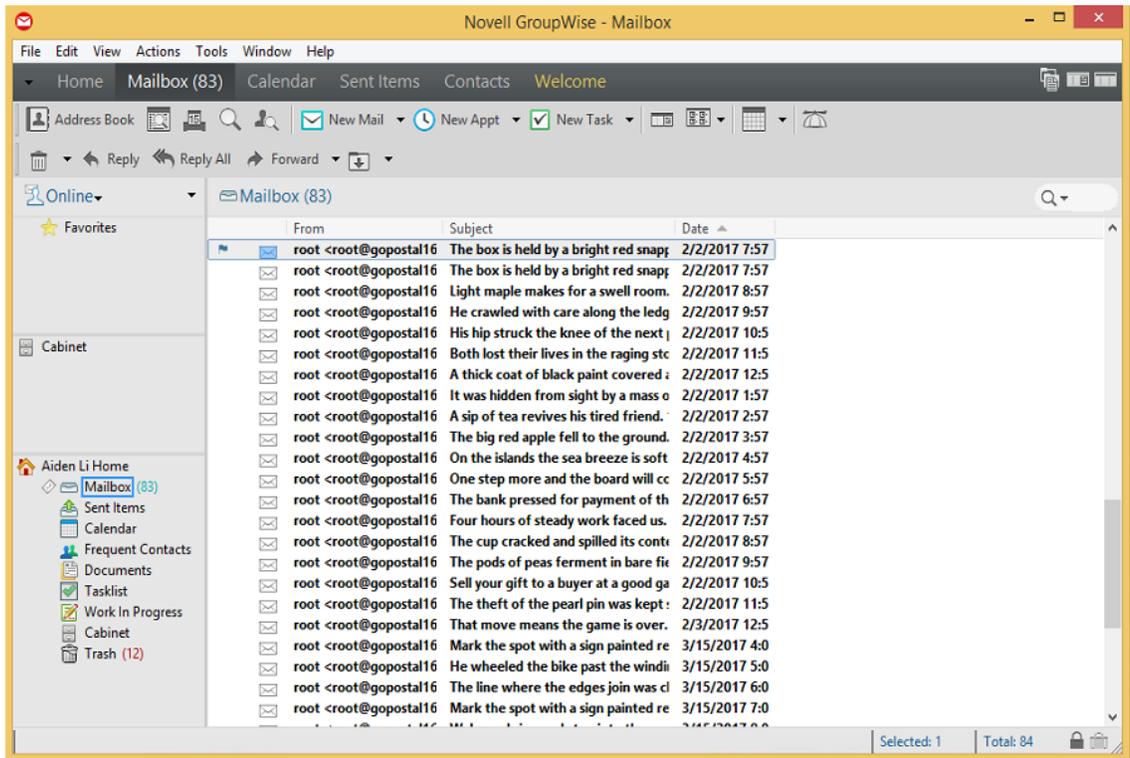
7. Right-click on the item and disable "Archive"



8. Select "File" and disable "Open Archive"



9. The item will appear in the mailbox



Restore a User's Address Book

Address book items can only be restored using Access Mode. The address book includes the GroupWise Address Book, Frequent Contacts, the user's Address Book, &etc.

Access Mode

Access mode has the Client access the GroupWise Disaster Recovery POA directly where the item or items can be archived and then unarchived once attached to the production GroupWise server.

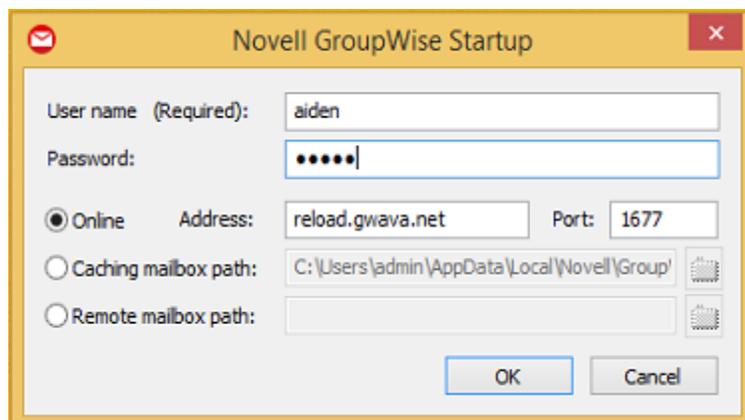
Personal archives must be enabled in GroupWise Administration.

On the GroupWise Disaster Recovery server

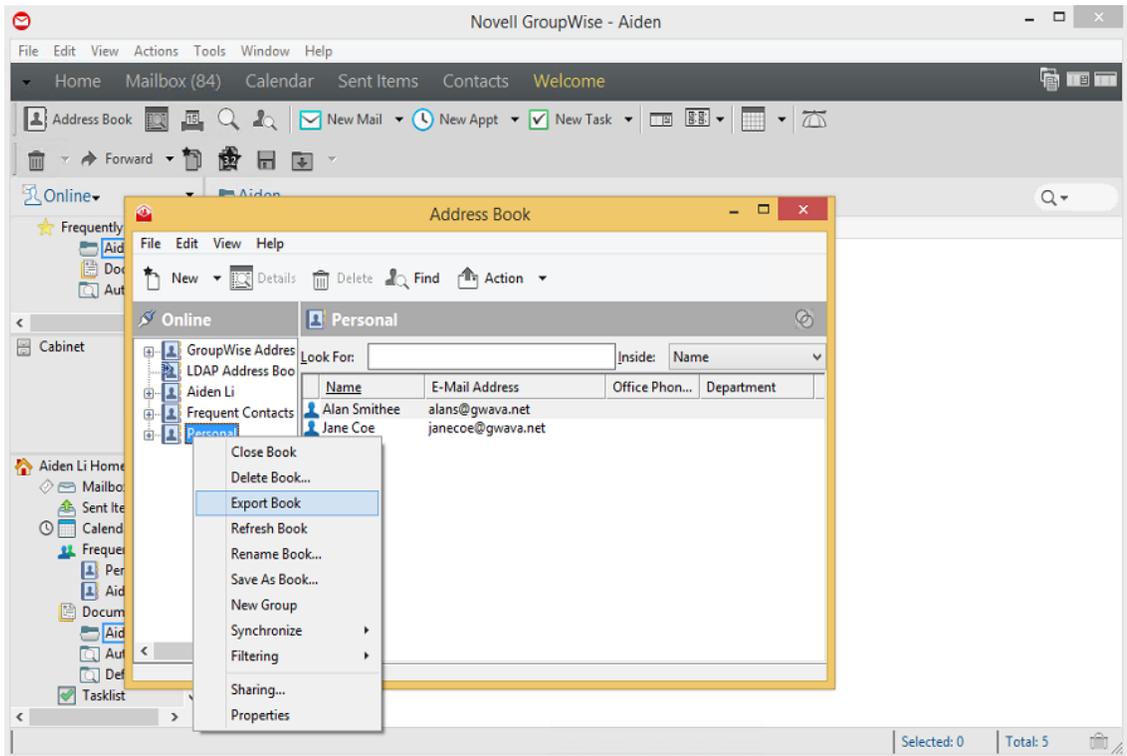
1. If needed, enable the access mode POA in *GroupWise Disaster Recovery Web Administration Console* | <Profile> | *Configure* | *User Access to Backups*
2. Load a backup on the GroupWise Disaster Recovery server from a time period where the item existed
3. The address the client must connect to can be found in the *GroupWise Disaster Recovery Web Administration Console* | <Profile> | *Backups tab* | *GroupWise Client Access to GroupWise Disaster Recovery Backups*

On the user's GroupWise client

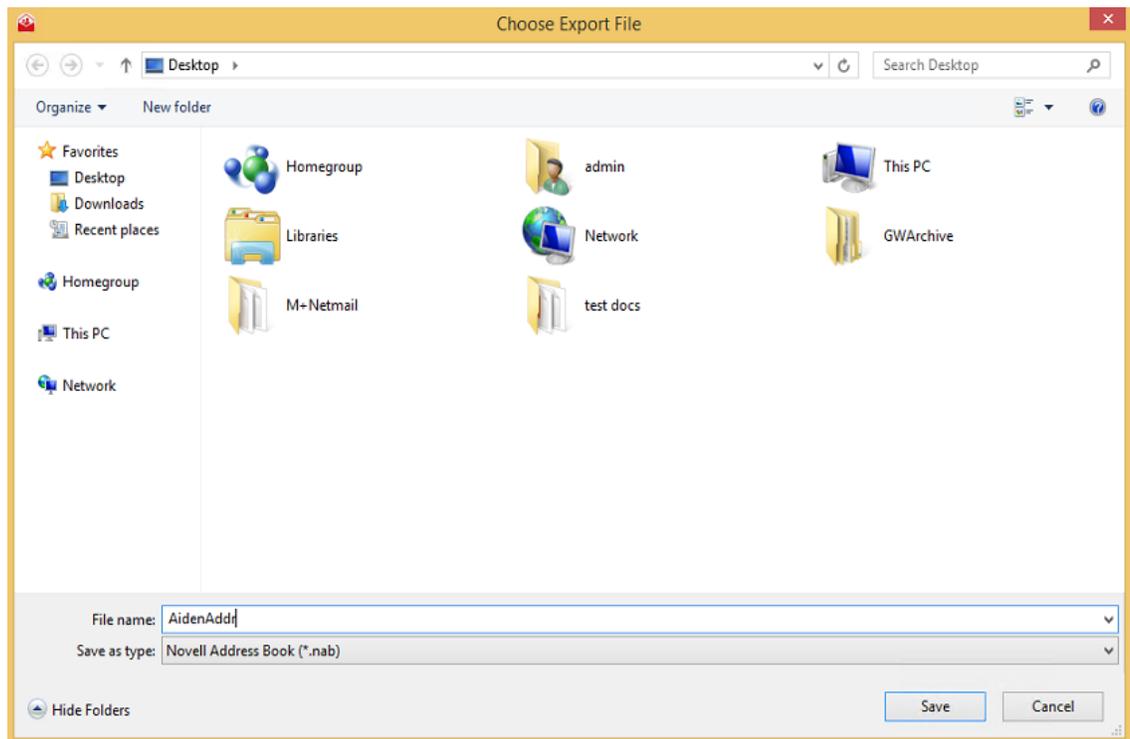
1. Open the GroupWise client and connect to the POA on the *GroupWise Disaster Recovery server*



2. Select the contacts to restore or an address book
3. Select "*File* | *Export*"



4. Export the items to a local .NAB file

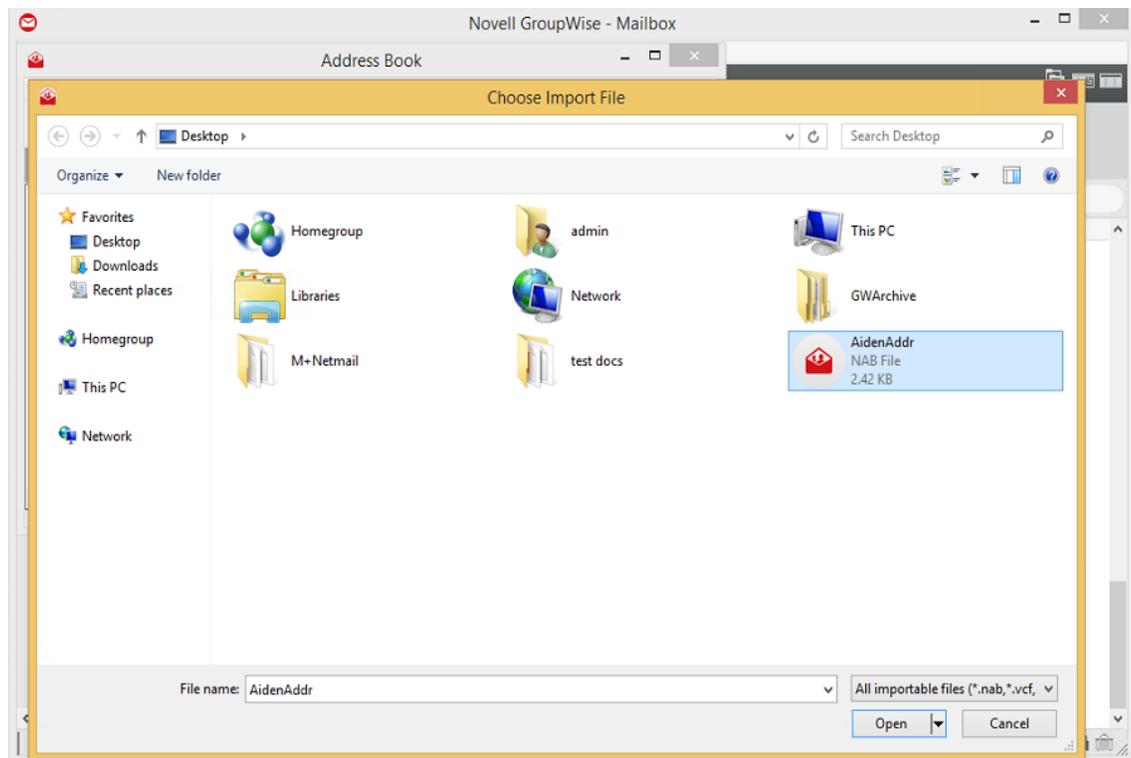


5. Close the client

6. Reopen the GroupWise Client and connect to the POA on the *Production GroupWise server*

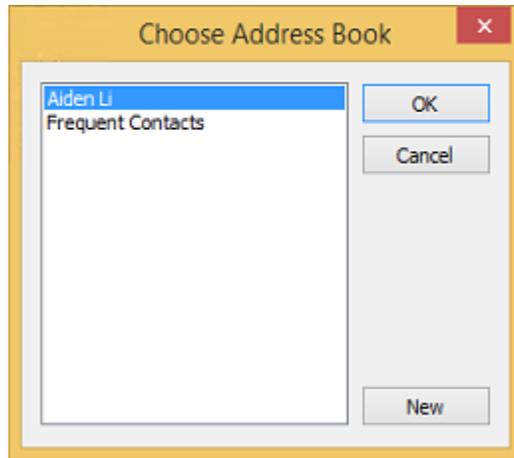


7. Open the address book and select a book
8. Select "*File | Import*"



9. Browse to the file and Open it

10. Select the book to import to



Restore a User's Calendar Items

Calendar items can only be restored using Access Mode.

Access Mode

Access mode has the Client access the GroupWise Disaster Recovery POA directly where the item or items can be archived and then unarchived once attached to the production GroupWise server.

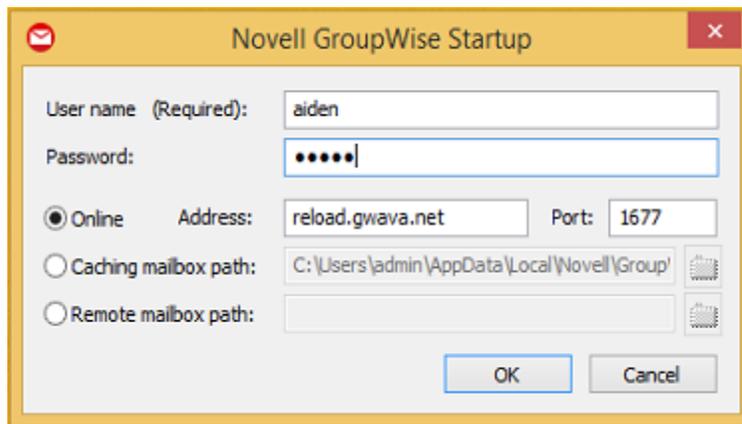
Personal archives must be enabled in GroupWise Administration.

On the GroupWise Disaster Recovery server

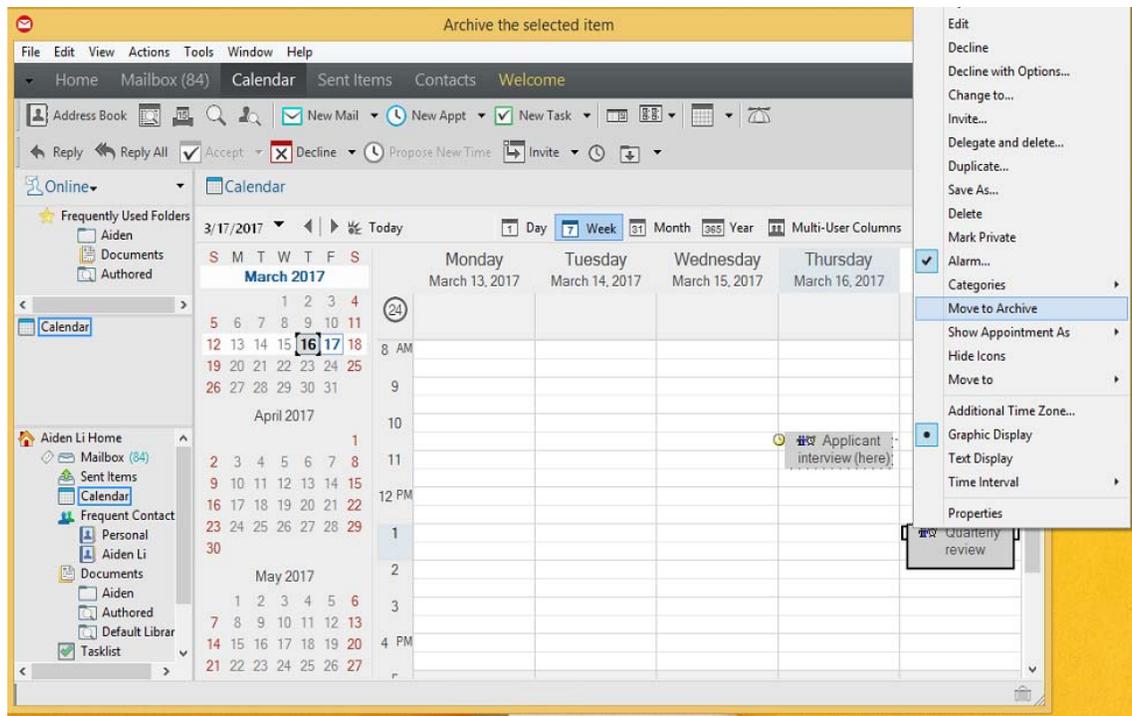
1. If needed, enable the access mode POA in *GroupWise Disaster Recovery Web Administration Console* | <Profile> | *Configure* | *User Access to Backups*
2. Load a backup on the GroupWise Disaster Recovery server from a time period where the item existed
3. The address the client must connect to can be found in the *GroupWise Disaster Recovery Web Administration Console* | <Profile> | *Backups tab* | *GroupWise Client Access to GroupWise Disaster Recovery Backups*

On the user's GroupWise client

1. Open the GroupWise client and connect to the POA on the *GroupWise Disaster Recovery server*



2. Select the calendar item to restore
3. Right-click and select "Move to Archive"



4. Close the client
5. Reopen the GroupWise Client and connect to the POA on the *Production GroupWise server*
6. Select "File | Open Archive"

Restore Documents to Document Management

Document items can only be restored using Access Mode

Access Mode

Access mode has the Client access the GroupWise Disaster Recovery POA directly where the item(s) can be archived and then unarchived once attached to the production GroupWise server.

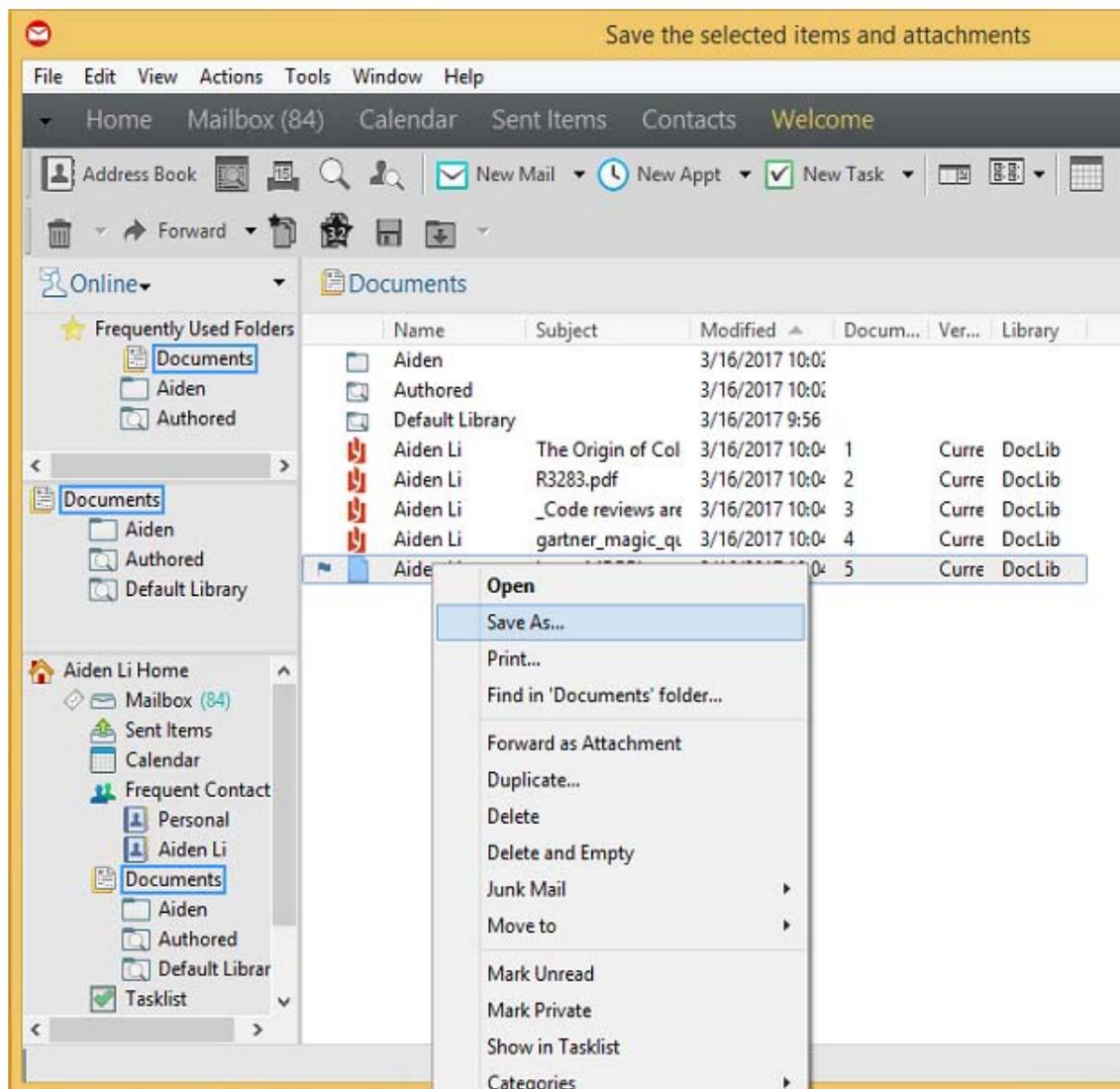
Personal archives must be enabled in GroupWise Administration.

On the GroupWise Disaster Recovery server

1. If needed, enable the access mode POA in *GroupWise Disaster Recovery Web Administration Console | <Profile> | Configure | User Access to Backups*
2. Load a backup on the GroupWise Disaster Recovery server from a time period where the item existed
3. The address the client must connect to can be found in the *GroupWise Disaster Recovery Web Administration Console | <Profile> | Backups tab | GroupWise Client Access to GroupWise Disaster Recovery Backups*

On the user's GroupWise client

1. Open the GroupWise client and connect to the POA on the *GroupWise Disaster Recovery server*
2. Select the document to restore
3. Save to disk



4. Close the client
5. Reopen the GroupWise Client and connect to the POA on the *Production GroupWise server*
6. Re-introduce the document to GroupWise

Restore Deleted User

Occasionally a user and all their items is inadvertently deleted from GroupWise. GroupWise Disaster Recovery can restore the user and their items.

This assumes that the deletion was caught and the user was not recreated in GroupWise Administration, which would create the user with a different FID.

If the user was recreated in GroupWise with a different FID, that user will have to be renamed so the original user can be restored. If that new user has received mail, the mail will need to be forwarded once the restoration is complete.

Prerequisites

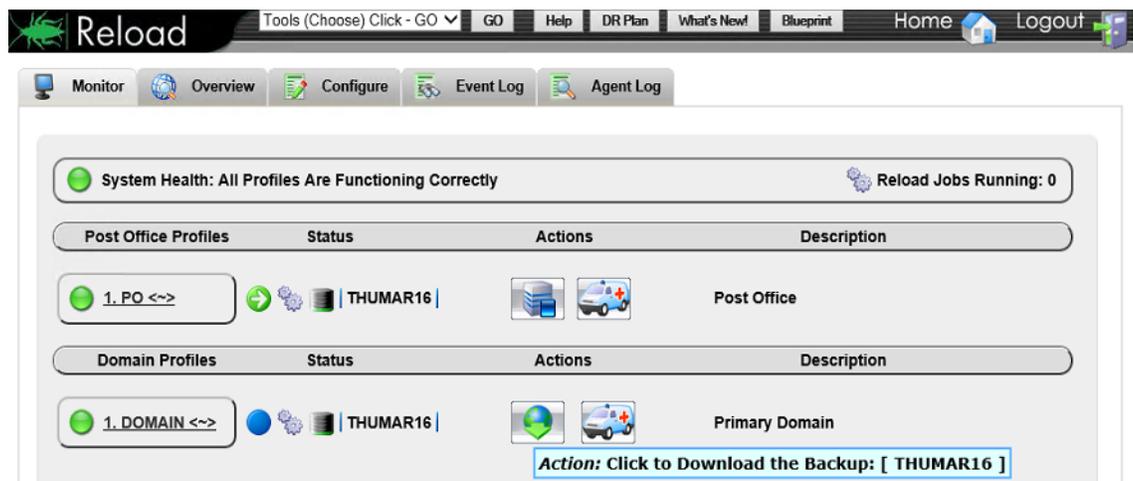
1. GroupWise 2014, or 2014 R2
2. Domain backup
3. Post Office backup
4. Restore Area setup

Download wpdomain.db from GroupWise Disaster Recovery

From the GroupWise server:

Current Domain Backup

1. Browse to *GroupWise Disaster Recovery Web Administration Console* | <Profile> | Click to *Download the Backup* action button



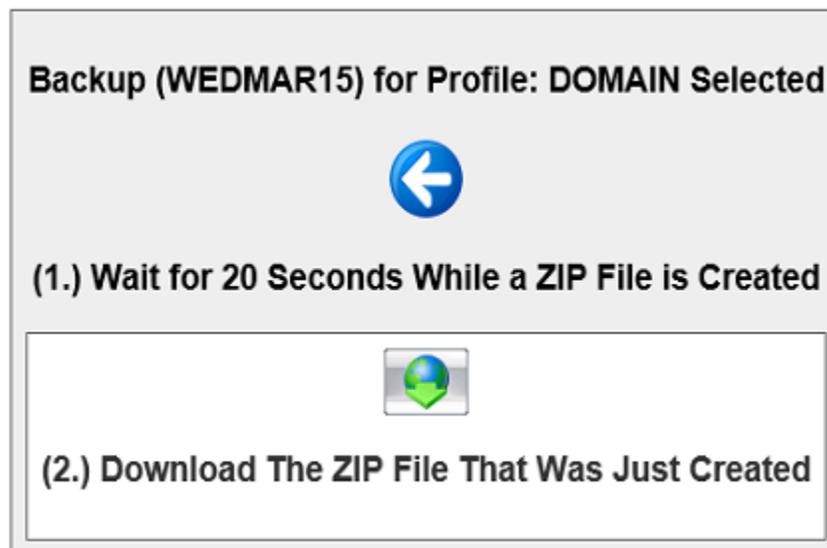
2. Download the ZIP File
3. If not on the GroupWise server, copy the ZIP file to the GroupWise server

Previous Domain Backup

1. Browse to *GroupWise Disaster Recovery Web Administration Console* | <Profile> | *Backups tab* | *Select Another Domain Backup to Download*



2. Select the Domain backup the user was a part of, press Select Backup, and a new window will appear
3. Wait about 20 seconds for the zip to be created
4. Click on "Download The ZIP File That Was Just Created"

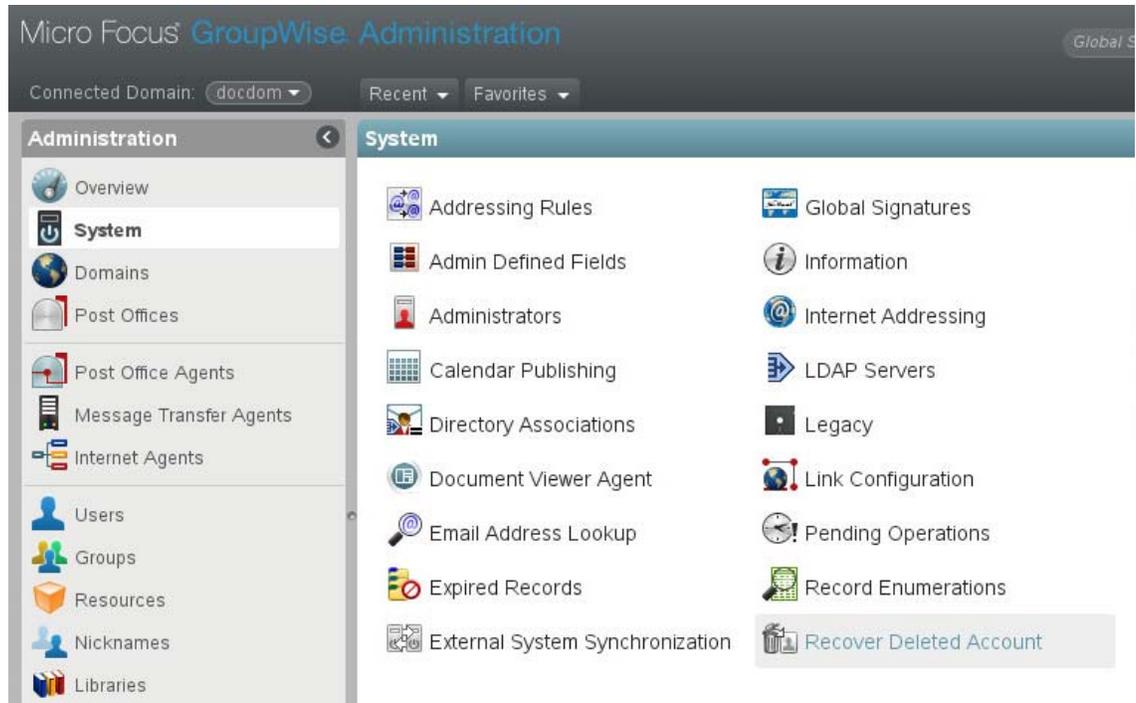


5. Download the ZIP File
6. If not on the GroupWise server, copy the ZIP file to the GroupWise server

Restore the User

On The GroupWise server:

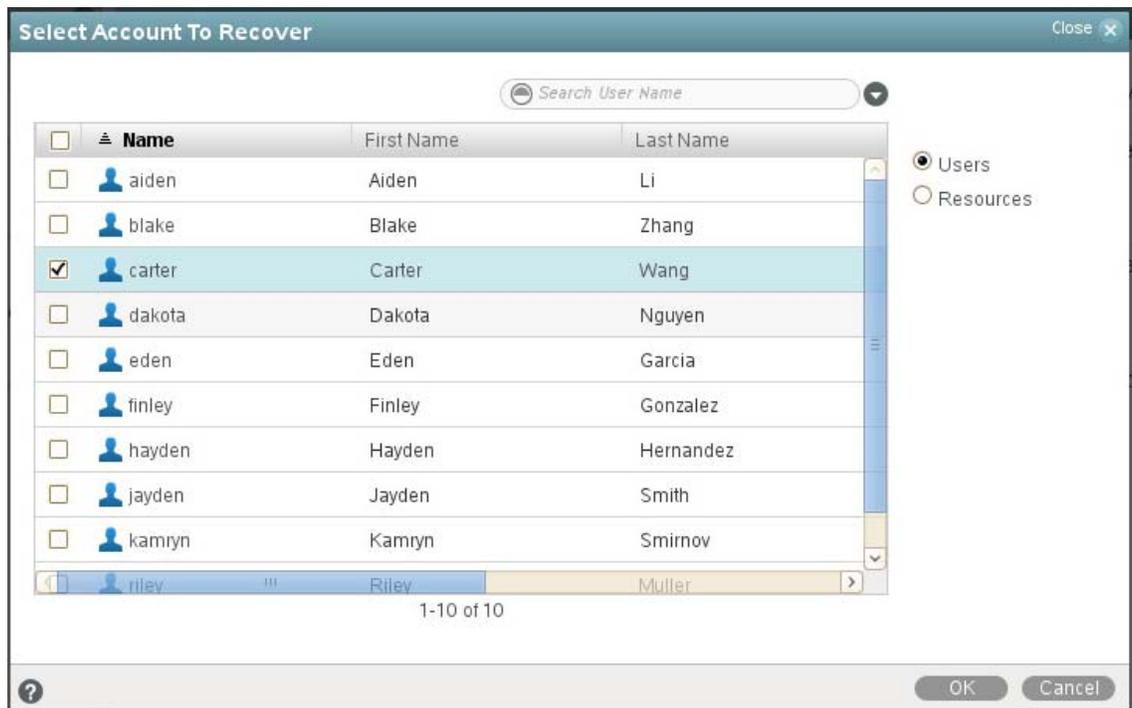
1. Unzip the wpdomain.db file
2. Browse to *GroupWise Administration | System | Recover Deleted Account*



3. Browse to the location of the wpdomain.db file



4. Click on the Groupwise world icon in the section "Account to Restore"
5. Select the user to be restored



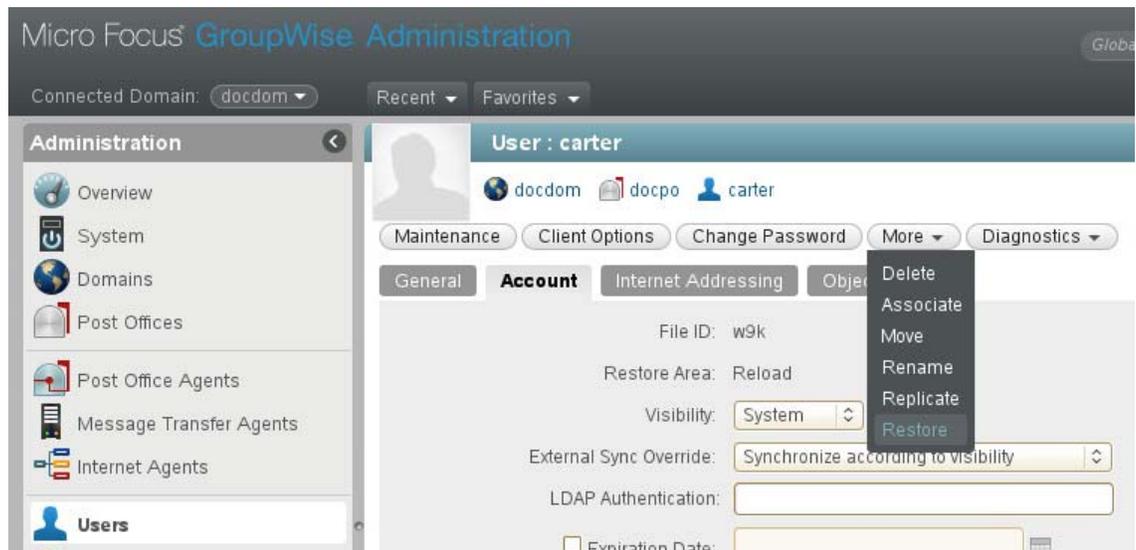
6. Click Restore



7. Click Done when recovery is complete

Restore All Items

1. Load a backup on the GroupWise Disaster Recovery server from a time period where the user existed
2. Browse to *GroupWise Administration | User| <Restored User>*



3. Select "More | Restore | Yes"



4. Items will be restored to the mailbox, this will take time depending on the amount of mail and the speed of the system

Restore From a Tape Backup

GroupWise Disaster Recovery can create TAR files for long term storage and can restore from those TAR files if they are made available.

The simplest way to restore items from a tape backup is to create a new profile, copy the backup to the folder of the new profile and connect to the Access Mode POA. This prevents the need to merge BLOB files in an existing profile.

NOTE: Keeping backups frozen for the long term will impact disk space as GroupWise Disaster Recovery will not be able to remove items.

For long term access to data we recommend our [Retain \(https://www.gwava.com/unified-archiving\)](https://www.gwava.com/unified-archiving) archiving product.

On the GroupWise Disaster Recovery Server

1. Increase the number of backups to keep so they are not removed by the cleanup routine (doubling is good) *GroupWise Disaster Recovery Web Administration Console* | <Profile> | *Configure* | *Backup Job Settings panel* | *Number of Backups to Keep*
2. Copy the TAR file to the GroupWise Disaster Recovery server
3. Extract the file with the tar command. This will merge the data to the profile as long as it has the same name. If the profile was renamed between the tape backup and the restore then a profile with the old name will need to be created. For example `tar -xf <file.tar> /<GroupWise Disaster Recovery Data Directory>`
4. Browse to *GroupWise Disaster Recovery Web Administration Console* | <Profile> | *Configure* | *User Access to Backups panel* | *POA SOAP Configuration section* | *Re-create Backup Indexes Now* | *Do It* and press Save

The screenshot shows the Reload GroupWise Disaster Recovery Web Administration Console. The top navigation bar includes 'Tools (Choose) Click - GO', 'GO', 'Help', 'DR Plan', 'What's New!', and 'Blueprint'. Below this is a status bar with '2. UNTAPE | Health | Backup Loaded | Job Status | Disk Space | Latest Backup : NONE'. The main navigation menu contains 'Overview', 'Backups', 'Disaster Recovery', 'Configure', 'Event Log', and 'Agent Log'. The 'Configure' section is active, showing 'Preferences' and 'User Access to Backups'. The 'User Access to Backups' section includes a 'Configure All Profiles' button and instructions: 'Use This Section to Configure What Happens When Access to a Backup is Turned On'. Configuration options include: 'Load the Access Mode GroupWise POA: Enabled' (with an 'Edit' button), 'Access Mode POA TCP/IP Address: 10.1.4.161' (with an 'Edit' button) and 'Client/Server Port: 1677' (with an 'Edit' button). There are buttons for 'POA HTTP Configuration' and 'POA SOAP Configuration'. Below these are: 'SOAP: Disabled' (with an 'Edit' button), 'Port: 7191' (with an 'Edit' button), and 'SSL: Disabled' (with an 'Edit' button). At the bottom, there are two options: 'Delete and Re-Create the Access Mode POA Startup File Now: Do It' (with an 'Edit' button) and 'Re-create Backup Indexes Now: Do It' (with a dropdown menu) and a 'Save' button.

5. Allow several minutes for the GroupWise Disaster Recovery daemon to scan the directory and add the files
6. Browse to *GroupWise Disaster Recovery Web Administration Console* | <Profile> | *Backups* | *Freeze a Backup From Deletion*
7. Browse to *GroupWise Disaster Recovery Web Administration Console* | <Profile> | *Backups* | *Turn On Access to Prior Backups*
8. Choose the desired backup and press "Turn on Access"

9. Allow the backup to load
10. Connect to the [Access Mode POA \(Restore_Mail_Items.htm#Access_Mode\)](#) and restore the items.

Post Restore Tasks

Once the restore operation is complete the TAR file or files can be removed, extra backups will need to be unfrozen, and number of backups kept reduced to free up space on the GroupWise Disaster Recovery server. Once backups are un-frozen GroupWise Disaster Recovery will remove them during the next backup job.

1. Browse to *GroupWise Disaster Recovery Web Administration Console | <Profile> | Backups | Un-Freeze a Backup (Backups With "_F" Are Frozen)*
2. Reduce the number of backups to keep to normal levels. Default is 14 days. *GroupWise Disaster Recovery Web Administration Console | <Profile> | Configure | Backup Job Settings panel | Number of Backups to Keep*
3. Remove old TAR files from the server

7 Disaster Recover Mode

Activating Disaster Recovery mode

If the Production GroupWise server has gone down it is obvious that it isn't coming backup anytime soon, it is time to activate GroupWise Disaster Recovery's Disaster Recovery mode.

This involves enabling Disaster Recovery Failover Mode on the GroupWise Disaster Recovery server and changing the A Record of the post office server on the DNS.

1. Browse to the GroupWise Disaster Recovery Web Administration Console
2. Click on the Post Office profile ambulance to engage *Disaster Recovery Failover Mode*
3. Go to the DNS and *change the DNS A Record IP address* of the post office server to the IP address of the GroupWise Disaster Recovery server
4. Test mail flow with a client
5. Contact [GroupWise Disaster Recovery Technical Support \(http://support.gwava.com/\)](http://support.gwava.com/) for assistance

Post Disaster Migration

After the disaster is over you will have data on the GroupWise Disaster Recovery server that does not exist on the GroupWise server. That data will need to be migrated to the GroupWise server.

Pre-migrate Data

1. Run the migration tool. This gets the messages you sent or received during the DR period back to the production post office. This can only be done from the GroupWise Disaster Recovery administration console.
 - 1a. *Recovery | POST OFFICE PROFILE | [post office] | Migrate*
 - 1b. Start at "Step #1" - highlight it and press ENTER to begin the pre-migration process.
 - 1c. After Step 1 has completed, have the users exit the client and press ENTER on "Step #2". This takes you to the Disaster Recovery POA Settings menu. Go to "Unload" and press ENTER. This unloads the DR POA but leaves GroupWise Disaster Recovery in disaster recovery mode.
 - 1d. Once Step 2 has completed, go back to the migration menu and initiate Step #3 (full migration). Wait until this process has completed before moving to the next task (turning off DR).

Revert to Normal Mode

1. Turn off Disaster Recovery (click on the ambulance button from the web interface).
2. Verify that GroupWise Disaster Recovery has properly re-enabled your backup schedules and that the DR POA has unloaded.
3. Change the DNS A record for the production POA. It should now reflect the IP address of the actual post office or live POA.

Migrate Final Data

1. Load the production post office POA.

- ♦ If running GroupWise 2014 or higher on Linux, there is a script for restoring all mail:

A script was created by GWAVA with the assistance of Micro Focus that makes merging two versions of a post office very simple. This script requires the version of GroupWise to be GroupWise 2014 or higher.

1. Set up a Restore Area that uses the GroupWise Disaster Recovery server, see the GroupWise Disaster Recovery configuration documentation for more details
2. Use the GroupWise Restore Script (gwrestore.sh) [<http://reload.gwava.com/gwrestore.sh>] script
3. Make sure to modify the Variables section of the GroupWise Restore Script

NOTE: If you modify the script on a Windows machine, to convert the script to Linux format use the "dos2unix" command on the Linux server once it is saved on the Linux server. Example:

```
dos2unix gwrestore.sh
```

4. Make the gwrestore.sh script executable:

```
chmod 777 gwrestore.sh
```

5. Run the gwrestore.sh script

```
./gwrestore.sh
```

6. The GroupWise Restore Script tells the GroupWise system to create a restore request for each user in the post office specified in the variable section of the script.
7. The GroupWise POA then looks inside of the message store in the GroupWise Restore Area associated with the GroupWise Disaster Recovery server, and brings across any mail items on the version of the post office on the GroupWise Disaster Recovery Server into the message store on the GroupWise post office.

8 Logs

GroupWise Disaster Recovery logs what it does to make troubleshooting easier.

GroupWise Disaster Recovery Web Console

The GroupWise Disaster Recovery Web Console has tabs to display the most recent entries of the Event, Agent and, if installed, the Blueprint logs. There are also links to the day's full logs as well as the Daemon, Error and Audit logs

For support purposes, GroupWise Disaster Recovery will create a single zip file of all the logs which can be downloaded from the GroupWise Disaster Recovery Web Administration page:

- ◆ Browse to GroupWise Disaster Recovery Web Administration
- ◆ Select "Tools | Download Logs | GO | "Download The RELOAD SUPPORT.ZIP File"

Command line

Alternatively, the log files may found on the GroupWise Disaster Recovery server in:

```
/opt/beginfinite/reload/logs
```

```
/opt/beginfinite/reload/save
```

```
/opt/beginfinite/reload/support/reload_support.zip
```

Details

There are a number of logs: found in `/opt/beginfinite/reload/logs`

EVENT.LOG = General logging.

AGENT.LOG = Detailed log file of all GroupWise Disaster Recovery activity.

ERROR.LOG = Error state reported to the system. The error that occurred and its time stamp

MONITOR.LOG = GroupWise Disaster Recovery version and build, license information, profile names, Groupwise agent version, and other general GroupWise Disaster Recovery configuration information.

DAEMON.LOG = Checks for jobs, generating the diagnostic log, and the support (reload_support.zip) log file.

DIAGNOSTICS.LOG = Server statistics like kernel version, disk space, processor, memory, NIC, resolv.cfg, hosts, and fstab.

<profile>.EVENT.LOG = Contains almost all of the data that is in the event.log that is specific to the profile.

<profile>.AGENT.LOG = Contains almost all of the data that is in the agent.log that is specific to the profile.

*.TEST.LOG = test connectivity, rights, enables profile, and lists what OS the GroupWise is installed on.

UPGRADE.LOG = Upgrade process activity.

AUDIT.LOG = Record of all actions.

9 Blueprint

Blueprint for GroupWise Disaster Recovery version 1.6 Overview

Blueprint for GroupWise Disaster Recovery extracts important business intelligence data from your GroupWise message store by performing in-depth analysis on your GroupWise Disaster Recovery backups.

Driven by customer needs, *Blueprint for GroupWise Disaster Recovery* plugs directly into your existing GroupWise Disaster Recovery server and leaves your GroupWise system stress-free while delivering timely reports that you can easily analyze and put into action — even on your mobile device or tablet computer.

GroupWise Mail Analysis — *Blueprint for GroupWise Disaster Recovery* will help you analyze, down to a user level, how much space you need for your message store and for your archive solution.

With *Blueprint for GroupWise Disaster Recovery*, you can create mailbox usage policies with all of this information and more:

- ♦ The cumulative size of all users' mailbox items over X days (90 days, 60 days, etc.)
 - ♦ The cumulative size of all users' mailbox items under X days (90 days, 60 days, etc.)
 - ♦ How many and what type of items are in a user's mailbox
 - ♦ Which users have mailbox storage limits, what the limits are, and how close a user is to their limit
- Reduce Costs* — *GWAVA Blueprint for GroupWise Disaster Recovery* can help you cut your IT costs.
- ♦ Identifies inactive users
 - ♦ Determines client types (full license vs. limited license)
 - ♦ Assesses clients' GroupWise versions to help assure that all users have upgraded
 - ♦ Provides the information you need to accurately calculate your GroupWise and archiving storage needs
 - ♦ Identifies users that are over-using resources

Usable Reporting — *Blueprint for GroupWise Disaster Recovery* generates navigable HTML reports for each post office and sends them to your email. View and print these reports from anywhere, including iPhones, iPads and Android devices.

Summary Reports — provide at-a-glance information for executive review and quick analysis.

User Analysis Reports — lets you drill down by each user and provide action items for follow-up. View mailbox limits, usage, item types, activity, license and version information and more.

Spreadsheet Reports — *Blueprint for GroupWise Disaster Recovery* generates *.CSV files with all of the information in the HTML reports, and much more. These *.CSV files can then be pulled into a spreadsheet application so you can sort and manipulate the data, making it easy to analyze and localize the data.

Simply Usable — Blueprint for GroupWise Disaster Recovery e-mailed reports are friendly to all platforms and configurations. If you want to share mailbox size information with a particular user, just click on the user's name within the Blueprint report, and a mail message will open up with the user's mailbox size information in the message body.

Intended Audience

This manual is intended for IT administrators in their use of Blueprint or anyone wanting to learn more about Blueprint. It includes installation instructions and feature descriptions.

Installation

Blueprint comes with every installation of GroupWise Disaster Recovery, but will not be installed by default. It can be [downloaded \(http://download.gwava.com/download.php?product=Blueprint&version=current\)](http://download.gwava.com/download.php?product=Blueprint&version=current) separately.

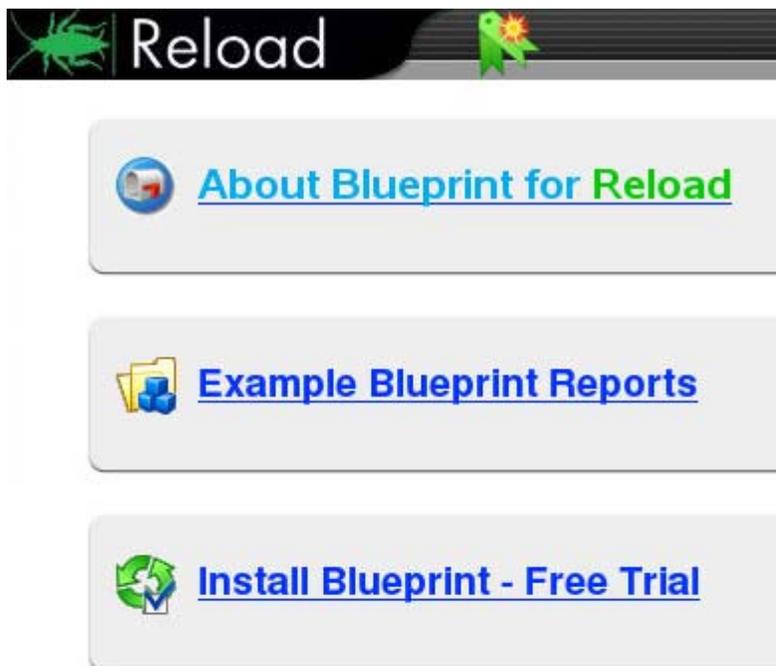
As it is a separate product, Blueprint requires a separate “[Licensing](#)” on page 186.

Installation

Install Blueprint by clicking the Blueprint button on the top navigation bar of the GroupWise Disaster Recovery Web Administration page.

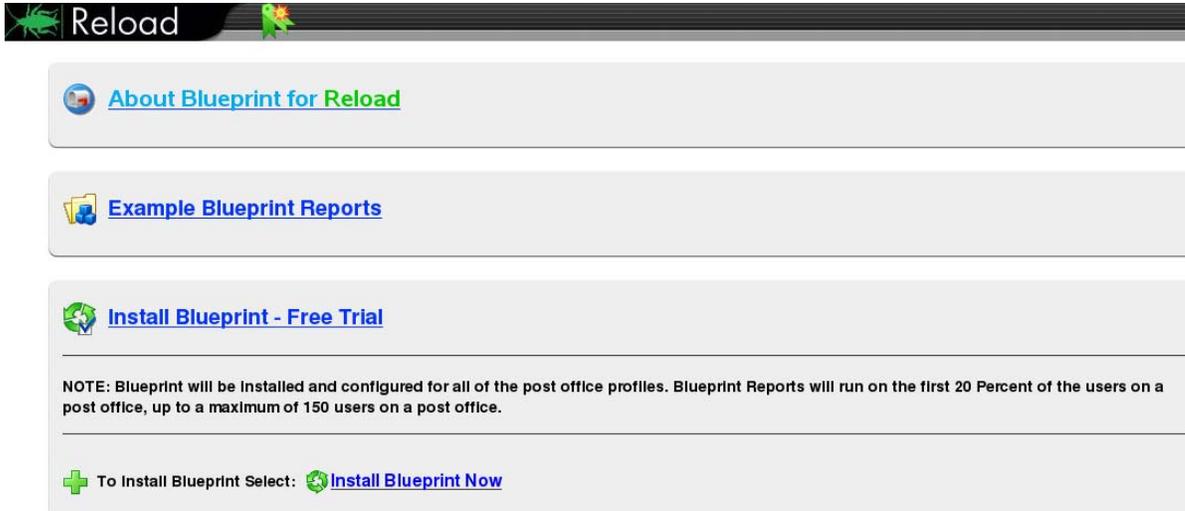


This will open a new tab.



You may open each panel for more information.

- ◆ **About Blueprint for GroupWise Disaster Recovery** provides bulletpoints on the benefits of Blueprint
- ◆ **Example Blueprint Reports** provides fictitious example reports to show you how it looks
- ◆ **Install Blueprint - Free Trial** allows you to install Blueprint with a 30-day free trial license

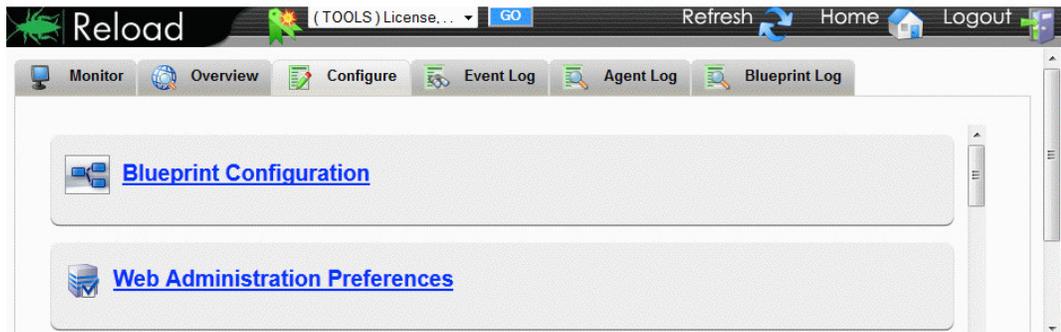


The screenshot shows the Reload web interface with three main panels. The top panel is titled "About Blueprint for Reload" and contains a brief description. The middle panel is titled "Example Blueprint Reports" and shows a list of reports. The bottom panel is titled "Install Blueprint - Free Trial" and includes a note: "NOTE: Blueprint will be installed and configured for all of the post office profiles. Blueprint Reports will run on the first 20 Percent of the users on a post office, up to a maximum of 150 users on a post office." Below the note is a green plus icon followed by the text "To Install Blueprint Select:" and a link "Install Blueprint Now" with a green plus icon.

Select *Install Blueprint Now*, a new tab will open as a request to the GroupWise Disaster Recovery daemon to install Blueprint is sent. It will take a short time for Blue to be installed.

A request for the Reload Daemon to install the **Blueprint for Reload** software package was created.

When Blueprint has been successfully installed you will see the "Blueprint Configuration" panel in the system level "Configure" tab.



The screenshot shows the Reload web interface with the "Configure" tab selected. The main content area displays two panels: "Blueprint Configuration" and "Web Administration Preferences". The "Blueprint Configuration" panel is highlighted. The top navigation bar includes "Monitor", "Overview", "Configure", "Event Log", "Agent Log", and "Blueprint Log". The "Configure" tab is active, and the "Blueprint Configuration" panel is visible.

NOTE: The installation process usually takes about 3 minutes to perform.

The installation will be complete when the Blueprint Log tab appears.



The screenshot shows the Reload web interface with the "Blueprint Log" tab selected in the navigation bar. The top navigation bar includes "Tools (Choose) Click - GO", "GO", "Help", "DR Plan", and "What's New!". The "Blueprint Log" tab is active, and the "Blueprint Log" panel is visible.

Licensing

Blueprint comes with a 30-day free trial period, once the trial period is over reports will no longer be created.

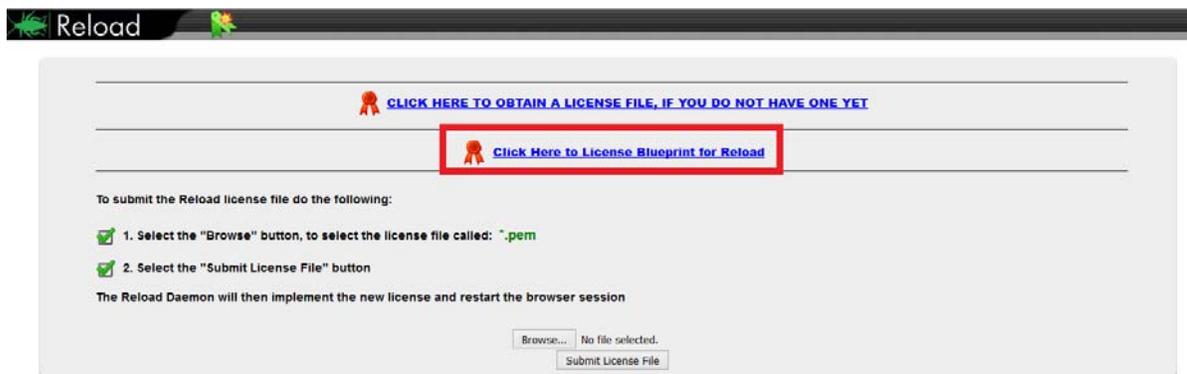
To license Blueprint talk to your sales representative for a validation key

Enter the validation key at licenses.gwava.com (<https://licenses.gwava.com/>) to download your license PEM file

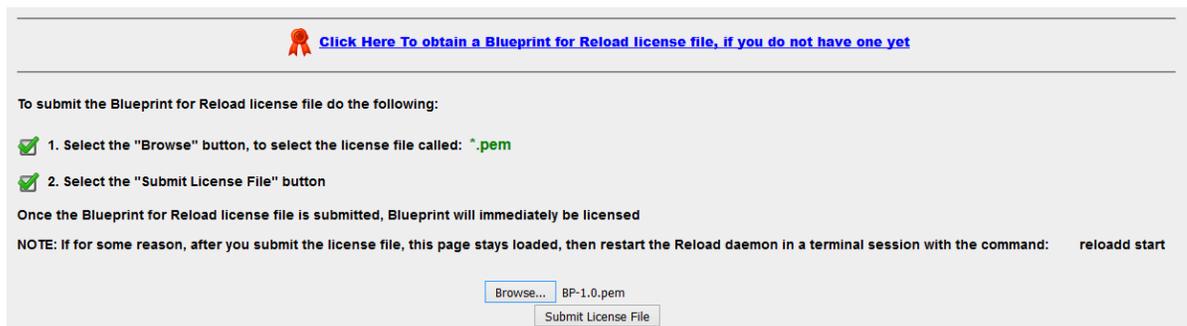
Browse to the GroupWise Disaster Recovery Administration Console and select License from the top navigation bar drop-down menu and press Go



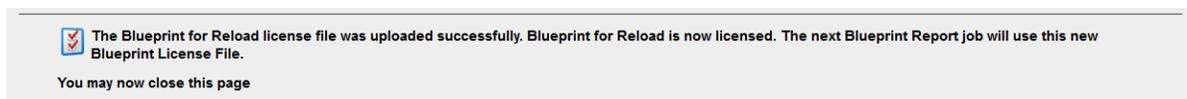
Select [Click Here to License Blueprint for GroupWise Disaster Recovery](#) this will open a new tab



Browse to the location of the PEM file and Submit the license file



The license will be uploaded successfully



Upgrading Blueprint

Blueprint will check for upgrades every 3 days. It will download a small manifest file to determine if there has been a version change and if so it will download and install the update.

If the GroupWise Disaster Recovery server does not have access to the internet then the update can be downloaded from <http://download.gwava.com/download.php?product=Blueprint&version=current>

Copy the file to the GroupWise Disaster Recovery Server and place in

```
/opt/beginfinite/blueprint/upgrade
```

At a command prompt, type:

```
blueprint upgrade
```

Configuration

Once Blueprint has completed installation, it needs to be configured.

Select the Configure tab and open the Blueprint panel.



The screenshot shows the Reload web interface. The top navigation bar includes the Reload logo, a search bar, and buttons for Tools, GO, Help, DR Plan, and What's New!. Below this is a secondary navigation bar with tabs for Monitor, Overview, Configure, Event Log, Agent Log, and Blueprint Log. The main content area displays the Blueprint configuration panel, which includes the Blueprint logo and the following settings:

- About Blueprint
- Send Blueprint Reports to Email: **Enabled** Edit
- General Settings
- Summary Report Settings
- Users Report Settings
- Resources Report Settings
- Advanced Settings
- Turn Off All Blueprint Reporting: **Disabled** Edit

General Settings

1. Set your *Preferred Internet Domain Name* to your email system
2. You may enable *Attach HTML Reports to E-mail Messages*

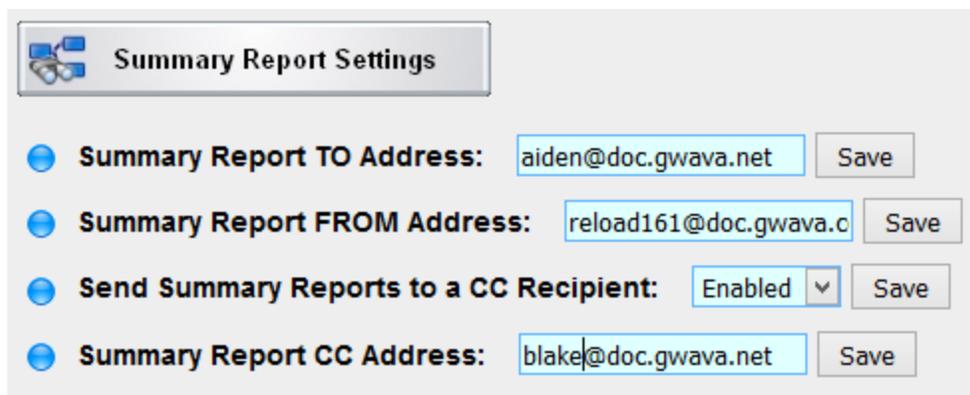
3. *Number of Days for GWCHECK Mailbox Contents Contrast* is set to 90 days, by default



The screenshot shows the 'General Settings' section of a configuration interface. It features a header with a checkmark icon and the text 'General Settings'. Below the header are three settings, each with a blue circular icon on the left and a 'Save' button on the right. The first setting is 'Preferred Internet Domain Name' with the value 'doc.gwava.net'. The second is 'Attach HTML Reports to E-mail Messages' with a dropdown menu set to 'Enabled'. The third is 'Number of Days for GWCHECK Mailbox Contents Contrast' with the value '90' and an 'Edit' button next to it.

Summary Report Settings

1. **Summary Report TO Address** Who should receive the summary
2. **Summary Report FROM Address** This is arbitrary so it can be something easy to understand where it came from
3. **Send Summary Reports to a CC Recipient** This is optional
4. **Summary Report CC Address** An additional user can receive a copy of the report.

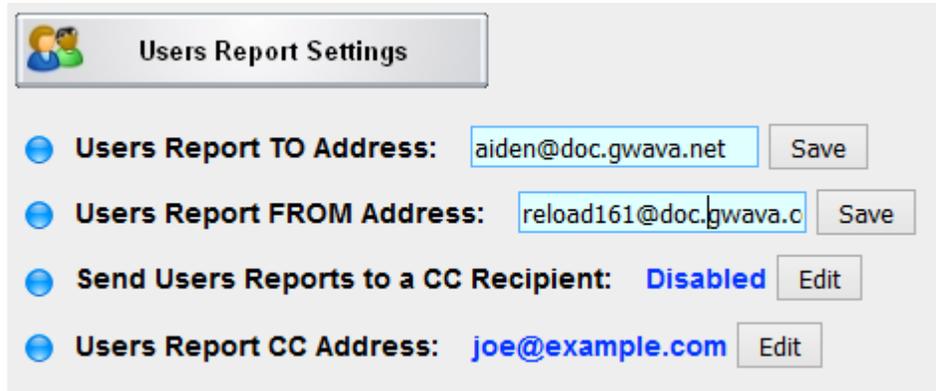


The screenshot shows the 'Summary Report Settings' section of a configuration interface. It features a header with a document and checkmark icon and the text 'Summary Report Settings'. Below the header are four settings, each with a blue circular icon on the left and a 'Save' button on the right. The first setting is 'Summary Report TO Address' with the value 'aiden@doc.gwava.net'. The second is 'Summary Report FROM Address' with the value 'reload161@doc.gwava.c'. The third is 'Send Summary Reports to a CC Recipient' with a dropdown menu set to 'Enabled'. The fourth is 'Summary Report CC Address' with the value 'blake@doc.gwava.net'.

Users Report Settings

1. **Users Report TO Address** Who should receive the summary
2. **Users Report FROM Address** This is arbitrary so it can be something easy to understand where it came from
3. **Send Users Reports to a CC Recipient** This is optional

4. **Users Report CC Address** An additional user can receive a copy of the report.

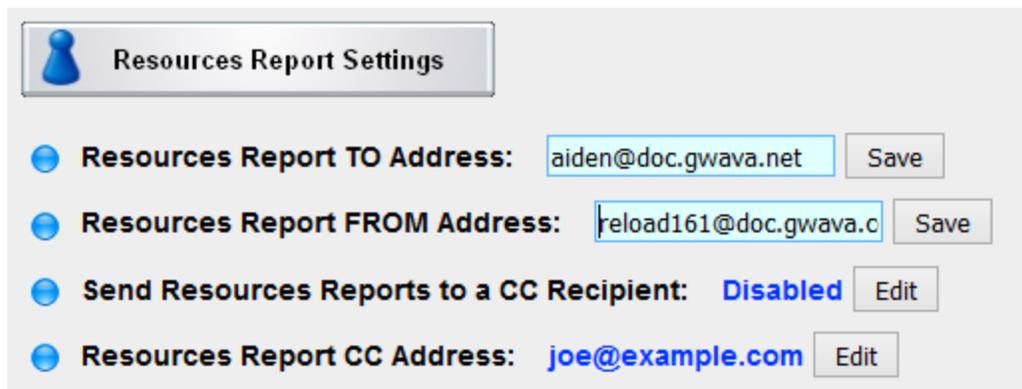


The screenshot shows the 'Users Report Settings' form. It has a title bar with a user icon and the text 'Users Report Settings'. Below the title bar are four settings, each with a blue circular icon on the left:

- Users Report TO Address:**
- Users Report FROM Address:**
- Send Users Reports to a CC Recipient:** **Disabled**
- Users Report CC Address:**

Resources Report Settings

1. **Resources Report TO Address** Who should receive the summary
2. **Resources Report FROM Address** This is arbitrary so it can be something easy to understand where it came from
3. **Send Resources Reports to a CC Recipient** This is optional
4. **Resources Report CC Address** An additional user can receive a copy of the report.



The screenshot shows the 'Resources Report Settings' form. It has a title bar with a blue pushpin icon and the text 'Resources Report Settings'. Below the title bar are four settings, each with a blue circular icon on the left:

- Resources Report TO Address:**
- Resources Report FROM Address:**
- Send Resources Reports to a CC Recipient:** **Disabled**
- Resources Report CC Address:**

Advanced Settings

Clicking on Advanced Settings button will open the Advanced Settings page

Personal Mailbox Reports

These are reports Blueprint will send to each user.

- ♦ **Send Mailbox Reports to Active Users** You may enable or disable this feature here
- ♦ **Personal Mailbox Report FROM Address** Set the email address the report is sent from

- ♦ **Send Only To Users in The Inclusion List** Limit reports to included users. The inclusion list is a simple ASCII text file saved as:

`/opt/beginfinite/blueprint/conf/individual_report_inclusion_list.conf`

- ♦ **Exclude Users in The Exclusion List** exclude users from the report. The exclusion list is a simple ASCII text file saved as:

`/opt/beginfinite/blueprint/conf/individual_report_exclusion_list.conf`

- ♦ **Include Custom Message in Personal Mailbox Reports** Add a custom message text. A custom message can be added to the Personal Mailbox Report email, perhaps to warn a user they are reaching their storage limit

- ♦ **Custom Message Text File** The location of the custom message test file. Be default, the custom message is saved as:

`/opt/beginfinite/blueprint/conf/custom_content.txt`

Threshold Highlighting

Reports can highlight when users exceed certain thresholds. The colors are set by [HTML color codes](http://htmlcolorcodes.com/) (<http://htmlcolorcodes.com/>).

Highlight "All Mailbox & Calendar Items" Over a Certain Threshold Enables or disables this feature

All Mailbox and Calendar Items

- ♦ "All Mailbox & Calendar Items" Warning Threshold (in Bytes)
- ♦ "All Mailbox & Calendar Items" Error Threshold (in Bytes)
- ♦ Highlight "All Mailbox & Calendar Items" Over a Certain Threshold - Normal Highlight Color
- ♦ Highlight "All Mailbox & Calendar Items" Over a Certain Threshold - Warning Highlight Color
- ♦ Highlight "All Mailbox & Calendar Items" Over a Certain Threshold - Error Highlight Color
- ♦ Highlight "All Items Under X Days" Over a Certain Threshold
All Items Under X Days
- ♦ "All Items Under X Days" Warning Threshold (in Bytes)
- ♦ "All Items Under X Days" Error Threshold (in Bytes)

- ♦ Highlight "All Items Under X Days" Over a Certain Threshold - Normal Highlight Color
- ♦ Highlight "All Items Under X Days" Over a Certain Threshold - Warning Highlight Color
- ♦ Highlight "All Items Under X Days" Over a Certain Threshold - Error Highlight Color
- ♦ Highlight "All Items Over X Days" Over a Certain Threshold
All Items Over X Days
- ♦ "All Items Over X Days" Warning Threshold (in Bytes)
- ♦ "All Items Over X Days" Error Threshold (in Bytes)
- ♦ Highlight "All Items Over X Days" Over a Certain Threshold - Normal Highlight Color
- ♦ Highlight "All Items Over X Days" Over a Certain Threshold - Warning Highlight Color
- ♦ Highlight "All Items Over X Days" Over a Certain Threshold - Error Highlight Color

 **Threshold Highlighting**

Show Me - Example 1 Show Me - Example 2

Highlight "All Mailbox & Calendar Items" Over a Certain Threshold: **Disabled**

All Mailbox and Calendar Items

"All Mailbox & Calendar Items" Warning Threshold (in Bytes): **2147483648**

"All Mailbox & Calendar Items" Error Threshold (in Bytes): **2684354560**

Highlight "All Mailbox & Calendar Items" Over a Certain Threshold - Normal Highlight Color: **FFFFFF**

Highlight "All Mailbox & Calendar Items" Over a Certain Threshold - Warning Highlight Color: **FFF06A**

Highlight "All Mailbox & Calendar Items" Over a Certain Threshold - Error Highlight Color: **FF9797**

Highlight "All Items Under X Days" Over a Certain Threshold: **Disabled**

All Items Under X Days

"All Items Under X Days" Warning Threshold (in Bytes): **524288000**

"All Items Under X Days" Error Threshold (in Bytes): **786432000**

Highlight "All Items Under X Days" Over a Certain Threshold - Normal Highlight Color: **FFFFFF**

Highlight "All Items Under X Days" Over a Certain Threshold - Warning Highlight Color: **FFF06A**

Highlight "All Items Under X Days" Over a Certain Threshold - Error Highlight Color: **FF9797**

Highlight "All Items Over X Days" Over a Certain Threshold: **Disabled**

All Items Over X Days

"All Items Over X Days" Warning Threshold (in Bytes): **1073741824**

"All Items Over X Days" Error Threshold (in Bytes): **1610612736**

Highlight "All Items Over X Days" Over a Certain Threshold - Normal Highlight Color: **FFFFFF**

Highlight "All Items Over X Days" Over a Certain Threshold - Warning Highlight Color: **FFF06A**

Highlight "All Items Over X Days" Over a Certain Threshold - Error Highlight Color: **FF9797**

Administration

Once Blueprint is installed jobs can be run against a profile.

When Blueprint is installed a report job will run. Report jobs will also run after backup jobs or when you select a report job to start.

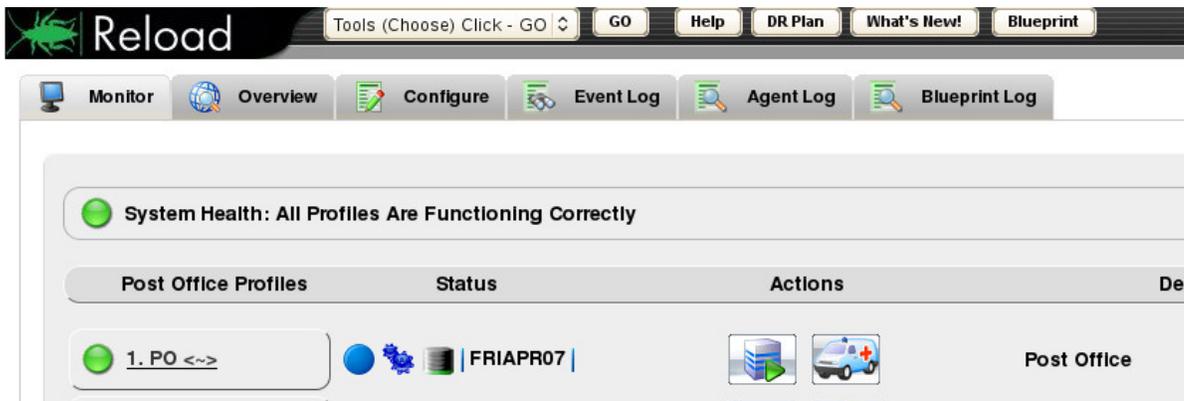
Starting a Blueprint Report Job

1. Browse to the GroupWise Disaster Recovery Web Administration page and select a Post Office profile.
2. Under the Backups tab, open the *GroupWise Disaster Recovery & Blueprint Job Control* panel
3. There will be two new options:
 - a. Start a Blueprint Report Job
 - b. Stop the Currently Running Blueprint Report Job



Blueprint Job

When a Blueprint Report job is running the gears will be colored blue



Summary Report

The Summary report contains an overview of the post office

Blueprint for Reload | Summary | BEG2PO

Report Summary

Statistics for GroupWise Post Office: BEG2PO
Reload Profile Name: POST1
Report Date: 1/26/2013
Report Creation Run Time: 2 Hours, 16 Minutes
Mailbox Statistis Analysis: 90 Days
Action Item Alerts: 70 (See Users Analysis Report)

User Mailbox Summary

Total Number of User Mailboxes: 111
Active Mailboxes: 41
Inactive Mailboxes: 70
All User Mailbox Items: 27.35 GB
Mailbox Items Under 90 Days: 5.09 GB (18%)
Mailbox Items Over 90 Days: 22.25 GB (82%)
Size of Inactive Mailboxes: 11.93 GB (43%)

Resource Mailbox Summary

Number of Resource Mailboxes: 1
All Resource Mailbox Items: 5 KB
Mailbox Items Under 90 Days: 0 bytes (0%)
Mailbox Items Over 90 Days: 5 KB (100%)

Blueprint Server Information

License Lease Information: Feb 4 04:59:59 2013 GMT
Blueprint for Reload Version: 5.1
GWAVA Reload Version: Reload 4.0 Build (400800)
GWAVA Reload Server Name: RELOADDEMO

Users Report

The Users report contains and analysis of each user in the post office.

At the top of the report is a quick summary, and links to users by name and action item sections

Blueprint for Reload | Users Analysis | BEG2PO

All Users Mailbox Analysis Report

Post Office: BEG2PO
Profile Name: POST1
Report Date: 01/26/2013
Number of User Mailboxes: 111
Active Mailbox Licenses: 41
Inactive Mailboxes Licenses: 70
All User Mailbox Items: 27.35 GB
Items Under 90 Days: 5.09 GB (18%)
Items Over 90 Days: 22.25 GB (82%)
Inactive Mailboxes: 11.93 GB (43%)

Quick Navigation Index

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#)
[G](#) [H](#) [I](#) [J](#) [K](#) [L](#)
[M](#) [N](#) [O](#) [P](#) [Q](#) [R](#)
[S](#) [T](#) [U](#) [V](#) [W](#) [X](#)
[Y](#) [Z](#) [Report End](#)

[70 Action Items](#)

Each user gets a section

AKRISTINACHUNG Mailbox Summary [\[Top\]](#)

User: [AKRISTINACHUNG](#) (Kristina Chung)
Department: N/A
Last Login: Inactive for 1019 Days

Mailbox Size Analysis

All Mail & Calendar Items: 127 MB
All Items Under 90 Days: 80 KB (1%)
All Items Over 90 Days: 127 MB (99%)
Mailbox Storage Limit: 300 MB (42% Used)

Item Count Analysis

All Mail & Calendar Items: 2046
All Items Under 90 Days: 8 (1%)
All Items Over 90 Days: 2038 (99%)
Mail Items Over 90 Days: 2038
Calendar Items Over 90 Days: 0

Item Location Analysis

All Inbox Items: 1005
All Outbox Items: 1041
All Posted Calendar Items: 0
All Draft Items: 0
All Trash Items: 0

At the end of the report is a list of recommended action items

User Mailbox Action Items Report

Action Items for Post Office: BEG2PO
Report Date: 01/26/2013

Action Item #1 [\[Top\]](#)

User: [AKRISTINACHUNG](#) (Kristina Chung)
Alert: Account Inactive for 1019 Days

Action Item #2 [\[Top\]](#)

User: [ASHERRIMELTON](#) (Sherri Melton)
Alert: Account Inactive for 1984 Days

Action Item #3 [\[Top\]](#)

User: [AGRETCHENHILL](#) (Gretchen Hill)
Alert: Last Login: 01/18/13

Action Item #4 [\[Top\]](#)

User: [AR](#) (Elsie Hamilton)
Alert: Account Inactive for 50 Days

Blueprint Command Line Options

Blueprint can be controlled from the command line.

For a list of options, type:

```
blueprint
```

View Blueprint Agent Log - Syntax:

```
blueprint log
```

Run Job Syntax:

```
blueprint job start <GWAVA GroupWise Disaster Recovery profile name>
```

Stop Job Syntax:

```
blueprint job stop
```

Stop One Profile's Current Running Job:

```
blueprint job stop <GWAVA GroupWise Disaster Recovery profile name>
```

Remove "Stop All Jobs" Syntax:

```
blueprint job stop
```

Single User Syntax:

```
blueprint job start post1 "tkratzer"
```

Single User - Live P.O. Syntax:

```
blueprint live job start post1 "tkratzer"
```

Report Job Status:

```
blueprint status
```

Configure Post Office Syntax:

```
blueprint -r <GroupWise Disaster Recovery profile name> -c <GroupWise post office name>
```

- ◆ **Upgrade Blueprint** (Check status before using this command, do not use when a blueprint job is running!)

```
blueprint upgrade
```

Report Version:

```
blueprint -v
```

