

GroupWise Disaster Recovery Installation Guide

January 2024

Legal Notice

Copyright 2006 - 2024 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors ("Open Text") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Contents

Preface	5
1 Introduction to GroupWise Disaster Recovery	7
2 Planning Your GroupWise Disaster Recovery System	9
Designing Your GroupWise System for Disaster	9
Designing Your GroupWise Disaster Recovery Server Setup	11
Understanding GWDR Server Disk Space Requirements	12
Understanding the GWDR Connection to GroupWise	13
3 GroupWise Disaster Recovery System Requirements	15
Server Requirements	15
GroupWise Requirements	15
4 Installation	17
Prerequisites	17
Installing GroupWise Disaster Recovery	18
Uninstalling GroupWise Disaster Recovery	18
Reinstalling GroupWise Disaster Recovery	18
5 Upgrading GroupWise Disaster Recovery	19
Upgrading GroupWise Disaster Recovery	19
Web Console	19
Command Line	20
Automatic Upgrades	21
Upgrading the Collector	21
Upgrading from Reload 5.x to GroupWise Disaster Recovery 18	21

Preface

This GroupWise Disaster Recovery Installation and Configuration 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.

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 [GroupWise Disaster Recovery documentation](#) website.

Knowledge Base articles can be found on the [OpenText Support](#) website.

1 Introduction to GroupWise Disaster Recovery

GroupWise Disaster Recovery provides live, hot backup and restore for OpenText GroupWise. GroupWise Disaster Recovery integrates with GroupWise post offices and domains to provide reliable backups. 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.

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.

Multiple GroupWise Disaster Recovery servers can also be tied together to add multiple redundant layers of protection for complete off-site backups of GroupWise.

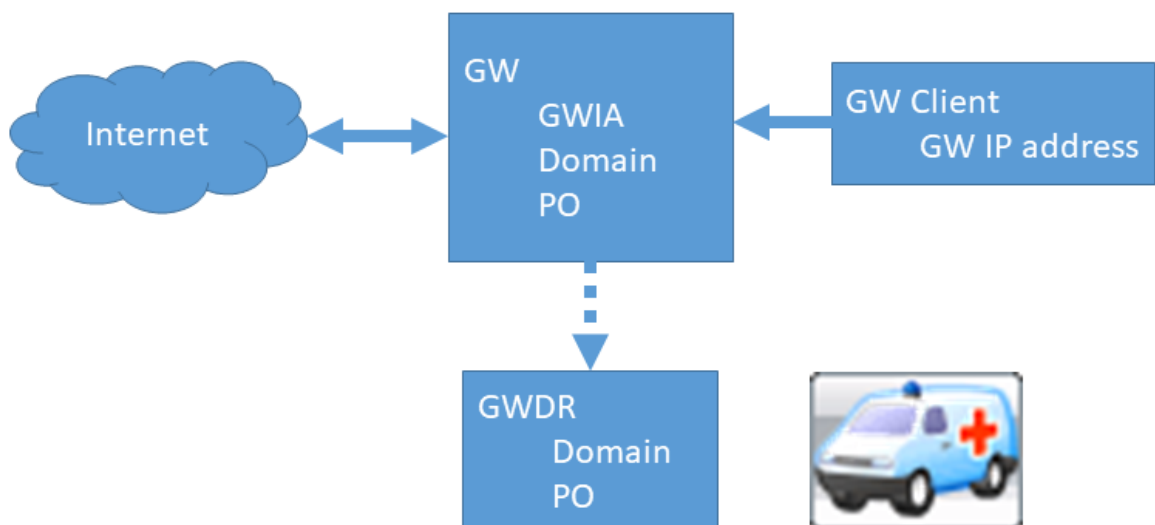
2 Planning Your GroupWise Disaster Recovery System

Just adding a GroupWise Disaster Recovery server to your GroupWise system and backing up the domain and post offices is not necessarily going to help all that much in a disaster, depending on what type of disaster your system might experience. Proper system design will make all the difference. The following sections will guide you in your system design goals:

- ♦ [“Designing Your GroupWise System for Disaster” on page 9](#)
- ♦ [“Designing Your GroupWise Disaster Recovery Server Setup” on page 11](#)

Designing Your GroupWise System for Disaster

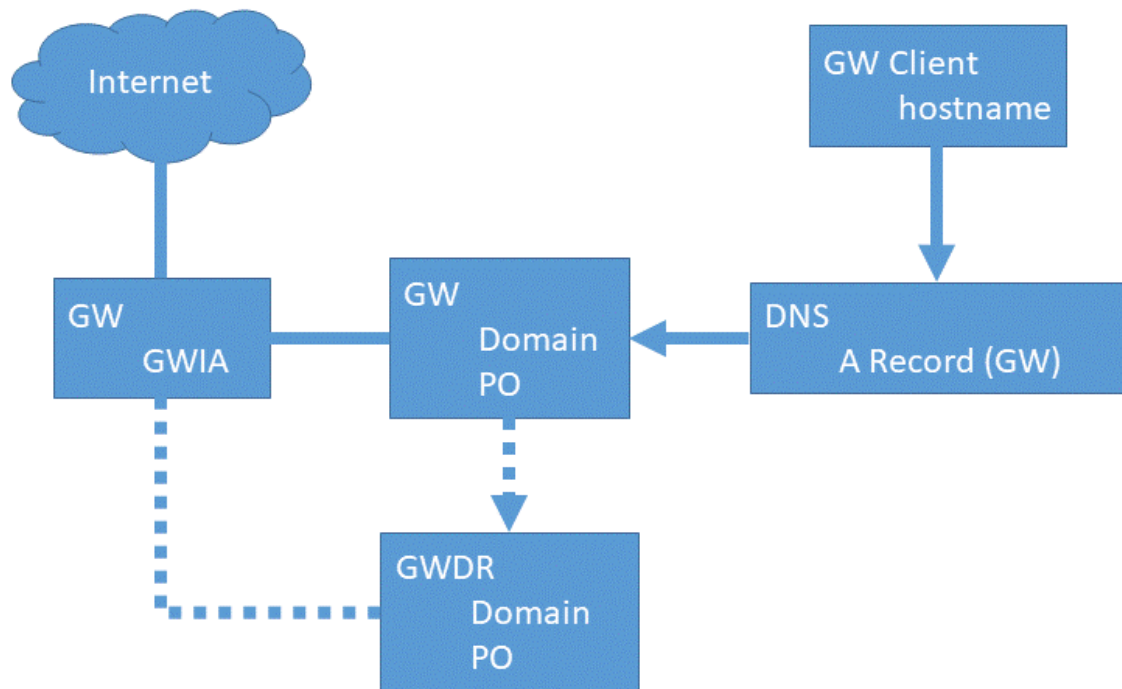
When you set up your GroupWise system, make sure that you do not set it up in a fragile manner. The most fragile way to set up your GroupWise system is to have the Domain, Post Office, and GWIA all on the same server and have your GroupWise client connecting using an IP address to the GroupWise server.



Setting up your GroupWise system this way means that if your GroupWise server fails, you can switch the GWDR server to Disaster Recovery mode, but you will have to tell each user to change the IP address their GW client uses, and they will only be able to email between users on the system. However, without a GWIA your users will not be able to send or receive mail from the Internet. So this will work if just the MTA or POA goes down and won't come up for some reason.

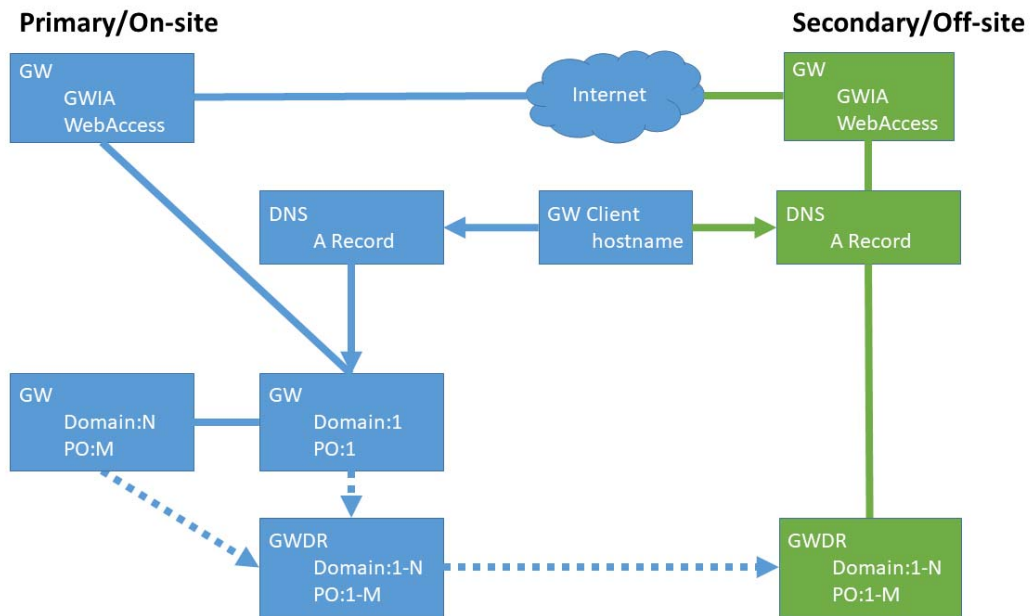
We can make this system more robust by making a few changes:

- ♦ Set up an A record in your DNS so that the GroupWise client will connect to the server you specify with a hostname instead of an IP address. This way you only have to change the A record in the DNS when you need to have your users connect to another GroupWise server or the GroupWise Disaster Recovery server.
- ♦ Set up multiple GroupWise servers and split up the agents across those server so if one server goes down, your GroupWise system will still work. This includes setting up the GWIA on a separate server so if the GW server fails, GWDR can use the GWIA for external messages.



Making these changes allows your system to deal with the GroupWise server going down. This is better, but this design will not be able to withstand multiple server failures. For that we need to design for site robustness. Site robustness is having a secondary, off-site, or disaster recovery site that may include the following:

- ♦ A secondary DNS server where you can update the A record that will direct the users to the proper location.
- ♦ A GroupWise WebAccess server so users can access their mail anywhere.
- ♦ A secondary GWIA for GroupWise to fail over to if the primary GWIA fails.



Designing Your GroupWise Disaster Recovery Server Setup

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 primary POA goes down. Because there are many minor things that might cause the primary system to go down (like nightly maintenance mode), GWDR is designed so that it won't go into disaster recovery mode unless you enable it.

GWDR can backup multiple domains and post offices and run them in disaster recovery mode. It might run like a herd of turtles through a field of peanut butter but it will run, depending on the resources available. If you wish to run multiple post offices at the same time, you will need to bind an IP address for each to use.

How you implement your GroupWise Disaster Recovery system also depends on what your GroupWise is hosted on. If hosted on SLES Linux then you can use the Collector model, if Windows then you must use the Server Only model.

GroupWise Disaster Recovery is a backup system and recovery system. It is built around the idea that two is one and one 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.

Each GWDR server can support up to 20 profiles.

On the GroupWise Disaster Recovery server you need to create a profile for each domain and post office. It is highly recommended to allocate and bind a separate IP address for each domain and post office to be hosted by the GWDR server.

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. We have found by experience that data grows by about 11% per day.

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`

- ♦ [“Understanding GWDR Server Disk Space Requirements” on page 12](#)
- ♦ [“Understanding the GWDR Connection to GroupWise” on page 13](#)

Understanding GWDR Server Disk Space Requirements

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.

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.

Calculating Disk Space

The rule of thumb is 2.5 times the post office size per profile, for the recommended 14 days of backups, plus the OS.

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, about 11% per day per 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.

Understanding the GWDR Connection to GroupWise

GroupWise Disaster Recovery can connect to GroupWise using either a Collector or a Server only model. If your GroupWise agents are on Windows, you can only use the Server only model. GroupWise agents on Linux can use either the Collector or the Server only model. For more information about these two connection, see the sections below:

- ♦ [“Collector Model” on page 13](#)
- ♦ [“Server Only Model” on page 14](#)

Collector Model

The Collector model is built for speed. Backups that take too long to create are not very useful. The collector will copy the files locally before sending them to the GWDR server, so provide adequate space on the GroupWise Server.

The collector agent is installed 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.

Using the Collector model requires disk space on your GroupWise server. To calculate the disk space required for the Collector, do the following:

- ☐ Calculate the size of the Post Office OFUSER, OFMSG, and GWDMS directories and add them together.

IMPORTANT: Do not include the OFUSER/INDEX directory in this calculation.

- ☐ Multiple the size determined in the previous step by 2. This will tell you the amount of space you need to run the collector model on the server.

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.

Server Only Model

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. It uses DBCopy to copy the data.

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. This is slow and requires a lock on the database for the duration of the transfer.

3 GroupWise Disaster Recovery System Requirements

GroupWise Disaster Recovery (GWDR) has the following system requirements:

- ♦ [“Server Requirements” on page 15](#)
- ♦ [“GroupWise Requirements” on page 15](#)

Server Requirements

❑ Supported OS Versions:

GWDR only runs on the following SUSE Linux Enterprise Server Versions:

- ♦ SLES 15 64-Bit
- ♦ SLES 12 64-Bit
- ♦ SLES 11 32-Bit or 64-Bit

❑ Memory: Minimum 2 GB of RAM

❑ CPU: Intel x86 Platform.

NOTE: The faster the CPU the better. While Symmetric Multiprocessing (SMP) is not a requirement, testing has shown that SMP is beneficial for GWDR.

❑ Disk Space:

Disk space must be carefully considered for you GWDR server. If you run out of disk space, GWDR can no longer create backups. The GroupWise Disaster Recovery server requires the following disk space per profile (a profile needs to be created in GWDR for each GW Domain and Post Office):

- ♦ 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, about 11% per day per post office.
- ♦ Remember to take Post Office growth and the host Operating system into account while calculating disk space needs.

IMPORTANT: For more specific information about server disk space, see [“Understanding GWDR Server Disk Space Requirements” on page 12.](#)

GroupWise Requirements

❑ GroupWise Versions: The following versions of GroupWise are supported by GWDR:

- ♦ GroupWise 24.x series

- ♦ GroupWise 23.4
 - ♦ GroupWise 18.x series
 - ♦ GroupWise 2014 R2
 - ♦ GroupWise 2014
 - ♦ GroupWise 2012
 - ♦ GroupWise 8.0.3
- ❑ **GroupWise Server Software:** You must install (but not configure) the GroupWise server software on your GWDR server for the version of GroupWise that you are using. We recommend that you install the GroupWise server software after you install GWDR.

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

To successfully integrate with GroupWise, you need to install but not configure the GroupWise server software for your version of GroupWise on the GWDR server. GWDR requires the GroupWise server software to be installed on the server to be able to copy the database files during a backup and run a POA during disaster recovery mode. Before installing the GroupWise server software, make sure the following is installed on your GWDR server:

- ♦ Motif (This can be installed through YaST > Software Mangement).
- ♦ (Optional) If installing on SLES 12 or 15, install rpm-32bit from YaST as well.

After you have these installed on your server, install the GroupWise server software and then continue with [“Installing GroupWise Disaster Recovery” on page 18](#).

Installing GroupWise Disaster Recovery

To Install GroupWise Disaster Recovery for the first time or to upgrade from Reload 5.x, please follow these instructions:

- ☐ Unzip the installer archive.
- ☐ Make the install script executable by running the command `sudo chmod +x *.sh`.
- ☐ Install GroupWise Disaster Recovery by running the following command in the same directory the download is in: `sudo ./install.sh`
- ☐ Select “1. Install” to begin the installation process.
- ☐ The installer will present the EULA. Press the Space Bar to accept or Ctrl-C to exit.
- ☐ Create an administrator name and password.
- ☐ Provide the path to the license file. This will enable GWDR and Blueprint. You can skip this step and install the license after the install following the steps in “[License GroupWise Disaster Recovery](#)” in the *GroupWise Disaster Recovery Admin Guide*.
- ☐ Optional: Provide a certificate and key file for securing the Web Admin Console. Press Enter to continue.
- ☐ GroupWise Disaster Recovery and Blueprint will be installed.

What’s Next

Follow the steps in “[Initial Setup](#)” in the *GroupWise Disaster Recovery Admin Guide* to setup your GroupWise Disaster Recovery system.

Uninstalling 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
```

Reinstalling GroupWise Disaster Recovery

To reinstall GroupWise Disaster Recovery Software Package, run:

```
reloadu
```

or run the installer and select Repair:

```
./install.sh
```

5 Upgrading GroupWise Disaster Recovery

Use the following sections to upgrade your GroupWise Disaster Recovery system:

- ♦ [“Upgrading GroupWise Disaster Recovery” on page 19](#)
- ♦ [“Upgrading from Reload 5.x to GroupWise Disaster Recovery 18” on page 21](#)

Upgrading GroupWise Disaster Recovery

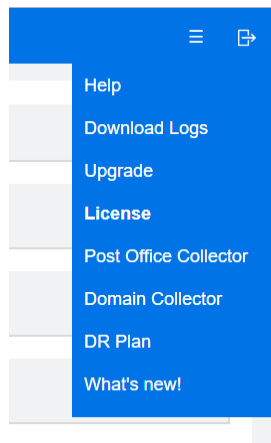
There are a few ways to upgrade GroupWise Disaster Recovery:

- ♦ [“Web Console” on page 19](#)
- ♦ [“Command Line” on page 20](#)
- ♦ [“Automatic Upgrades” on page 21](#)
- ♦ [“Upgrading the Collector” on page 21](#)

Web Console

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

- ❑ In the GroupWise Disaster Recovery Admin console, select the menu button at the top right and select **Upgrade**.



- ☐ Select **Upgrade Now**.



Automated Software Download and Automated Upgrade

NOTE: This automated upgrade feature does require that the server have HTTP (Port 80) access to the Internet. If the 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 daemon to check to see if there is a newer version of the server. If there is a newer version, the daemon will upgrade the software package automatically.

To determine if GroupWise Disaster Recovery should be upgraded to a newer release, follow these steps:

The currently installed version is: **18.1.0 Build (1810240)**

1. Check the [GroupWise Disaster Recovery Support Forum Patches Section](#) to see if a newer version is available
2. To upgrade the server, select: **Upgrade Now** which will install the latest version



Manual Software Download and Automated Upgrade



Advanced Upgrade Options

- ☐ Review the EULA and select **Accept & Update**.

Command Line

There are a few ways you can upgrade from the command line:

- ♦ ["Using the Install Script" on page 20](#)
- ♦ ["Using Reloadu" on page 20](#)

Using the Install Script

- ☐ Download the GWDR installer, unzip the files, and run `./install.sh` from a terminal.
- ☐ Select option 2 in the prompt to **Upgrade/Repair GroupWise Disaster Recovery**. The installer upgrades your GWDR software.

Using Reloadu

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 contents of the install folder 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 copies the upgrade into:

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

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

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

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

Upgrading from Reload 5.x to GroupWise Disaster Recovery 18

When upgrading from Reload 5.1.1 or earlier, use the install script. Blueprint will be installed and licensed with a current valid Reload or GWDR license.

GWDR18 Installer Package:

After downloading and extracting the GWDR18 installer package.

Open the terminal and enable execution rights on the installer script by running in the package directory: `chmod +x *.sh`.

Run `./install.sh`.

Select "2. Upgrade".

