

# About System Maintenance

This page describes processes for creating backups of databases and files to be used in the event of redeployment of a GroundWork Monitor system or systems. This redeployment may occur as a consequence of the need to replicate an environment for expansion, for test, or for recovery from a disaster wherein essential equipment is lost.

## Contents

### 1.0 Weekly Maintenance

Weekly backup procedures are recommended for your GroundWork Monitor system including steps to backup all system databases and configuration settings.



Once a week maintenance is recommended so that a system can be quickly restored from a disaster or system failure. It's up to the System Administrator to decide how long backups should be stored. Additionally, it is highly recommended to backup the backup directory on an external device.

### 2.0 Backup and Restore

This page covers the individual backup and restore processes for GroundWork Monitor databases and configuration settings including; the Foundation database, JBoss framework, GroundWork Insight Reports, and Configuration (monarch). The operational databases used by GroundWork Monitor are GWCollageDB (Foundation) which contains state and event data, and the Dashboard database which contains historical information used by Insight and Availability Reports.

### 3.0 Data Retention

This section holds procedures for maintaining database events (log messages) and event reporting in case of low disk space or system performance issues. Additionally, you will find information on managing the different GroundWork Monitor generated logs files.

### 4.0 GroundWork Monitor Log Files

This page describes the various log files, their settings, and locations within the GroundWork Monitor system including; Java, GroundWork Monitor applications, Third Party applications log files and components.

### 5.0 Restore a System Configuration

This document outlines steps to restore a GroundWork Monitor configuration from a previous backup. After a system failure you may need to re-install GroundWork Monitor. In addition, the last available backup can be used to restore the data and the system configuration. The backup consists of all GroundWork databases and the Nagios and Foundation configuration files. If the backups are stored on an external device (tape other server) copy them over to the MonitorServer into the `/usr/local/groundwork/backup` directory. The following sections assume that all the backups are present in this directory. The restore procedure consists of four steps.

### 6.0 Automated Backup Strategies

This document refers to advanced configuration for automating the backup process of the GroundWork Monitor system.

#### Best Practices

##### *Install Packages*

The initial installation of the system, and many patches, are delivered as RPMs and .bin Bitrock packages along with defined steps for applying them. The base installation of the system from bare metal can be repeated exactly. The original sources and a log book or run book detailing the specific configuration entries (IP address, name, DNS, etc.) are necessary for this level of recovery.

##### *Databases*

GroundWork Monitor utilizes PostgreSQL as the database engine for storage of configuration, control, and monitored status and events. The several databases are named below but are not an exhaustive list as others may be added with the integration of more projects. Each of these databases is essential to the function of GroundWork Monitor so they must be included in a backup and recovery strategy.

- GWCollageDB - GroundWork Foundation database

- Monarch - Configuration database
- Dashboard - Insight and Availability Reports database
- JBoss Portal - User Interface, web applications and permission databases

Files GroundWork Monitor uses certain files which may be included in the RPMs or .bin packages for installing the product, as well as others which are added in customization. While the packages can rebuild most of them, tuning and localization must be specifically captured post install. Thus, these files must also be identified and dealt with by the backup and recovery strategy. Examples of these kinds of files include:

- /var/spool/cron/\*
- /etc/sysconfig/iptables/iptables.cfg
- /usr/local/groundwork/common/etc/\*

### ***Conclusion***

The backup and recovery must treat initial Installation, databases, and configuration files in different ways to insure a successful operation.