Installing or Upgrading GroundWork Monitor

Overview

Welcome to the installation instructions for GroundWork Monitor Enterprise Edition, version 7.2.1. These instructions are maintained in the GroundWork knowledge base (kb.groundworkopensource.com). If you are reading these in a PDF or other offline form, you should check the online form for the most recent version.

This document covers the installation of GroundWork Monitor 7.2.1 and supported upgrades from 7.1.1 and 7.2.0. After reviewing **Read Me First** documents noted below, for new installs see SECTION I and for Upgrades see SECTION II.

> **Read Me First**
> Before performing an installation, please review the Release Notes which contain details of issues fixed, new features, and items of interest to those users who have customized or significantly enhanced GroundWork Monitor Enterprise, System Requirements, and any Technical Bulletins so you can prepare for any additional steps required either before or after the process.

CONTENTS

RELATED RESOURCES

- Release Notes
- Installation Options
- System Requirements
- Remote Database Installation
- Technical Bulletins

WAS THIS PAGE HELPFUL?

- Leave Feedback

SECTION I: New Install of GroundWork Monitor Enterprise 7.2.1

If you need a new installation of GroundWork Monitor versus an upgrade, first take a look at the Installation Options document, then follow the steps below to install. The major installation decisions and steps include:

- Decide if you want to split the install into a remote database server and front-end or all in one
- Decide if you want to have graphs generated using Grafana, RRD, or both
- Decide if you want to run two JVMs or one on your groundwork server
- Ensure you have all the System Requirements taken care of (host name in DNS, disk space allocated properly, enough RAM, etc.)
- Run the installer
- Do the post-install tasks to secure your GroundWork installation
- Configure any additional options, such as HTTPS, LDAP authentication, etc.
- Start monitoring

Installation steps

- **Software preparation**
  Transfer the GroundWork Monitor Enterprise software to the server it is being installed on.
  - As superuser (`root`), change the permissions of the binary to executable. For example:

    ```
    chmod +x groundworkenterprise-7.2.1-br494-gw3901-linux-64-installer.run
    ```

  - You can then launch the installer with one of the Installation Methods. These instructions will assume you launched it in text mode, interactive, as `root`:

    ```
    ./groundworkenterprise-7.2.1-br494-gw3901-linux-64-installer.run
    ```

- **Install questions**
  Using interactive text mode, the installer asks questions that must be answered correctly for a successful install. Most of them are

self-explanatory. Some of them are called out here so we can comment on them.

- Questions about the components to install:

```
-------------------------------------------------------------------------
Select the components you want to install; clear the components you do not want
to install. Click Next when you are ready to continue.

PostgreSQL Database [Y/n] :

GroundWork Monitoring Server [Y/n] :

Is the selection above correct? [Y/n]:
```

  If you are installing using a remote database that you have already set up with the Remote Database Installation, decline the installation of the PostgreSQL Database. If you are installing an all-in-one server, where the PostgreSQL database will run locally on the GroundWork Monitor machine, enter "Y" for yes. Also enter "Y" for yes for the GroundWork Monitoring Server, and "Y" for yes if you selected correctly for the confirmation.

- Next you will enter your postgres password. **Please record this password and keep it somewhere safe.** You will need it on upgrade, and certain support operations or customizations may also require it.

```
-------------------------------------------------------------------------
Please enter your database 'postgres' user password.

PostgreSQL postgres user password :
Re-enter password :
```

- The next question is about Log Archiving. Unless advised not to by GroundWork Support, you should enter "Y" for yes.

```
-------------------------------------------------------------------------
Log Archiving

Do you wish to have the installer enable a standard configuration of the
log-archive capability? [Y/n]:
```

- The next question should almost always be answered "Y" for yes, unless you are running a system where the user interface is very lightly or never used, like a child server or minimal installation. Dual JBoss configurations make better use of larger resource footprint machines to make the UI faster and more responsive.

```
-------------------------------------------------------------------------
Dual JBoss Installation

The GroundWork Monitor system capacity can be enhanced by enabling Dual JBoss
configuration on the system. Do you want to enable Dual JBoss?

 [Y/n]:
```

- An installation typically takes several minutes. The installer will prompt another two times, once to start the services and the last to display the URL to log in.

Post-install configuration

Starting and Stopping GroundWork Monitor
GroundWork Monitor includes all prerequisites and components within a single installation package. The software components of GroundWork Monitor are installed under `/usr/local/groundwork`, with the exception of the log rotation configuration and the start/stop script named `/etc/init.d/groundwork`. The start/stop script is usually used indirectly, as follows:

```
service groundwork status
service groundwork start
service groundwork stop
```

This script can also be used to stop, start, or restart individual services. For example:

```
service groundwork restart nagios
```

The `service` command generally resides in the `/sbin/` directory (`/usr/sbin/`, on Ubuntu). That directory will normally be part of the `root` user's command-search path. If not, or you experience issues with the mapping of the service command to systemd sysctl calls in your distro, you can run the `/etc/init.d/groundwork` script directly:

```
/etc/init.d/groundwork start
```

The `service` command is preferred because it is easier to remember and type. As of version 7.2.1 GroundWork supplies systemd compatible init scripts, but they are not automatically enabled. So if you are running on a systemd-enabled distribution, you have to either use the init script directly, or simply type:

```
systemctl enable groundwork
```

to use the service command.

- **Important default login information**

Security adjustments here are paramount
Documentation on changing passwords can be found in the How to change a users password page of the Bookshelf. Note the `root` and `admin` users are special and should not be renamed or deleted without special configuration steps.

- **Basic user-interface accounts and passwords**
  - There are 4 user-interface users defined in GroundWork by default. *Please be sure to adjust these user names and passwords according to your security policy, and do so quickly after the product is installed*. You can use the encryption tool on the GroundWork Administration > GroundWork License page to generate secure hashes of passwords, which can be used as random passwords if you like.
    - root (password: root)
    - admin (password: admin)
    - operator (password: operator)
    - user (password: user)
  - Associated file adjustment

You will also need to update the `portal.proxy.password` in `/usr/local/groundwork/config/foundation.properties` if you change the `user` account password. See How to configure LDAP.

- **Other accounts and passwords**
  - **GDMA**
    There is also a separate proxy user defined in GroundWork by default, that is used to support Automated Agent Registration. If you decide to use GDMA, we recommend you change this user's password as well. This user need have only very restricted permissions, as you will see if you set up GDMA. See Configuring Auto Registration.

- **License Required for Login**
  - At first login, there is a default license for up to 50 monitored devices installed. Unless you plan to use only the Core edition, limited to 50 devices, you will need to log in as the `admin` user and copy-and-paste your license key into the portal application under the GroundWork Administration > GroundWork License menu. Don't forget to click on Validate to make it active. Each GWOS installation has a single license file that controls access to the application user interface. Each license is valid for the subscription duration purchased. The license file affects only user access to the GWOS portal; *it does not affect the ability to start/stop application components or most of the data gathering, processing, or notification features of the product.*
  - License key validity is checked at user login and is affected by:
    - The subscription start and end dates.
    - The number of monitored devices configured.
    - Whether the date and time is accurate
  - Please see How do I know the total of used devices? for information regarding your license count and how to adjust.

    
    The SLA Management and SLA Dashboard features are not enabled in the GroundWork Core product.

- **Optionally Disabling ntop**
  ntop is bundled into the GWMEE 7.2.1 release. It promiscuously analyzes the network traffic it can see on your GroundWork Monitor server. Because the data can be quite useful, ntop is enabled by default. It is, however, incompatible with SSL-enabled GroundWork systems, and can be considered a security risk (it is a sniffer, after all). If you decide you do not want to use this component, it can be (reversibly) disabled as follows.
  - If the `config/ntop.properties` file is renamed before the `gwservices` component (or all of GroundWork Monitor) is started, the ntop UI will not be accessible under the Advanced > Protocol Analyzer menu item.
  - The `ntop` daemon itself can be disabled by first stopping it:

    ```
    service groundwork stop ntop
    ```

    and then changing permissions on the control script:

    ```
    cd /usr/local/groundwork/common/scripts
    chmod -x ctl-nms-ntop.sh
    ```

    
    To fully disable ntop, restrict the page
    Disabling the background daemon itself reduces the load it invokes by promiscuously examining your network traffic, but you will probably want to disable access to the page to avoid displaying an error message. See the GroundWork bookshelf under Portal Administration - memberships for details.

    
    Netflow/sflow functionality
    The ntop sniffer functions are largely replaced and enhanced in GroundWork Monitor 7.1.1 and above with the addition of netflow/sflow graphing and analysis in the NeDi package.

- **Remote Database Considerations**
  - Access to the database server is defined in configuration files like `cacti_feeder.conf`. The default (applicable to a local database) points to `localhost`. A known issue is that in the case of a remote database, the 7.2.1 installer fails to set the proper value in the `cacti_feeder.conf` file. If you are using a remote database, you will need to edit that file to make sure the `cactidbhost` specification is the actual remote database server FQDN or IP address.

    ```
    /usr/local/groundwork/config/cacti_feeder.conf:cactidbhost = localhost
    ```

  - After fixing that setting, you must bounce the Cacti feeder for it to pick up the new value. That will be done the next time you restart `gwservices`:

    ```
    service groundwork restart gwservices
    ```

    or you can bounce just the one process, more surgically:

    ```
    kill `ps --no-headers -C .perl.bin -o pid,args | fgrep cacti_feeder.pl | awk '{print
    $1}'`
    ```

  - For comparison and completeness, we note the following places in the config files that are successfully modified by the installer:

```
/usr/local/groundwork/config/cacti.properties:cacti.1.dbhost=localhost
/usr/local/groundwork/config/db.properties:collage.url=jdbc:postgresql://localhost:5432/gwco
= "localhost"
/usr/local/groundwork/config/log-archive-send.conf:runtime_dbhost = "localhost"
```

SECTION II: Upgrade Installation

Upgrades to 7.2.1 are supported **from version 7.1.1 and version 7.2.0 ONLY**. If you wish to do an upgrade, review this section. For a fresh installation, see SECTION I: New Install of GroundWork Monitor Enterprise 7.2.1 above.

If you are unsure if this has already been done or whether this applies to your installation, please contact GroundWork Support for assistance.

Prerequisites

Before you begin it is **critically important** that you test for each of these prerequisites and obtain them. For instance, getting partway into the process only to realize that you don't have the postgres user password and that no one can obtain it quickly means wasted time and disappointment, as well as the chance that the system may be down and require rolling back. Don't let this happen to you.

Special Considerations

- These instructions assume you are doing an in-place upgrade. If you wish to do a migration to a new server, please contact GroundWork Support for advice on your options and the trade-offs involved.
- Migration to a different machine may be required, if your current operating system version is no longer supported by GroundWork Monitor. See the OS Platform Requirements section in System Requirements.
- Some customers have additional add-on integrations installed (e.g., Ganglia Integration, AlertSite Integration, Webmetrics Integration, ServiceNow Integration, JIRA Integration, other helpdesk integrations). Special considerations apply in those cases. If these or other integrations or extensions were provided by GroundWork Professional Services, you must contact GroundWork Professional Services for advice. Otherwise, contact GroundWork Support for details.
- LDAP integration will NOT be reset by this upgrade unless you are using multiple endpoints, in which case you will need to follow the instructions described in post-upgrade tasks. Otherwise no action is needed post install to support LDAP configuration.
- HTTPS Support will be reset to HTTP, however restoring this is now scripted. See post-upgrade tasks below.

- **Checklist**
  - Make sure your existing GroundWork server is running version 7.1.1 or 7.2.0 with all applicable Technical Bulletins for 7.1.1 or Technical Bulletins for 7.2.0 applied.
  - If the Portal Root user was changed, what is the new name?
  - What is Portal Root user's password?
    - (try logging in to the portal as the root user.)
  - What is the "postgres" database-user password?
    - (try accessing `psql` from the command line, i.e., "`psql -U postgres`".)
  - Make sure that at the portal is running before you start the upgrade, since the installer will log in to make changes.
  - Make sure that name resolution is working and that you have an entry for the system in /etc/hosts (see System Requirements).
  - Make a backup of your full installation and, especially if you have customizations, separately make an on-disk backup of critical config files kept outside of the `/usr/local/groundwork/` file tree.

Backups

If you have a standard un-customized installation, simply make a backup of the GroundWork Monitor installation using the provided backup tool. Download the latest version of the backup utility from the knowledge base, and make a full backup of your installed system as described in the Backup utility description.

If any customizations have been applied, including additional scripts, plugins, etc., we recommend that you instead create a complete on-disk backup of /usr/local/groundwork directory, so that you can easily restore the files you added or changed. The installer will flag the files that are updated and that should be merged, but if you have the disk space available this step makes it easier to restore your customizations that the installer can't detect or anticipate. You should stop the GroundWork server and cron jobs, ensure you have adequate disk space, and make the copy like so (as root):

1. Check for space available:

```
df -h
```

2. Check for space used by GroundWork:

```
du -sh /usr/local/groundwork
```

3. Stop all GroundWork Processes and cron (called crond on some systems):

```
service groundwork stop
service cron stop
```

4. Copy the directory (in this example to `/tmp/gwbackup`):

```
mkdir /tmp/gwbackup
cp -a /usr/local/groundwork/* /tmp/gwbackup/
```

5. Start the services again (Note: You don't need all the services to be running for an upgrade to work, only postgresql):

```
service cron start
service groundwork start
```

(or)

```
service groundwork start postgresql
```

Permission and ownership check

From the command line run the following:

```
find /usr/local/groundwork -type f -group root -exec ls -la '{}' \; |grep -E "root" |grep -Ev "\->"
|grep -Ev "supervise"|grep -Ev "control" |grep -Ev "lock" |grep -Ev "status" |grep -Ev "mib_" |grep
-Ev ".ctl" |grep -Ev "backup/" |grep -Ev "Catalina" |grep -Ev "/scripts/" |grep -Ev "/ntop/" |grep -Ev
"apache2" |grep -Ev ".pid" |grep -Ev ".index" |grep -Ev ".log" |grep -Ev ".lck"
```

This will list files owned by root, and should not include any java libraries (.war, .jar, .ear) and configurations (.properties, .cfg). If any such files are found, change the user/owner to nagios.

Postgres user configuration on SLES

If you are upgrading a Groundwork Installation that is installed on SLES you will need to run the following command, prior to running the installer, to verify that the postgres user is set up properly.

```
if mkdir ~postgres; then chown $(id -u postgres):$(id -g postgres) ~postgres; fi
```

Installations with GDMA connecting to GroundWork server via HTTPS

If you are using GDMA and the GroundWork server version 7.1.1 or 7.2.0 you are upgrading from is using HTTPS, you will need to re-set most of the settings for HTTPS after upgrade. You will then be able to use the later version of GDMA (2.6.1) supplied with 7.2.1, and to transition the potentially large numbers of older agents without service interruptions. However, as of 7.1.1, the default SSL configuration uses only TLS 1.2, and *will not accept connections from older GDMA agents without adjustment.* You may have completed an upgrade to 7.1.1 or 7.2.0 and not enabled the stronger encryption, and so still be in this situation.

Please see the Post upgrade tasks section below for details. Be sure to plan for this activity after the upgrade is complete. You will eventually want to transition your GDMA agents one-by-one to the later versions (GDMA 2.5.0 or later) and eventually enable only the more secure settings of GroundWork Monitor Enterprise 7.2.1.

Upgrade options

Distributed database configurations are supported. Therefore, a GroundWork Monitor single-server installation can be upgraded to a configuration where the GroundWork Monitor software and the database are installed on different servers. The new database instance needs to be installed *before* the upgrade of GroundWork Monitor can be started.

> **Moving the PostgreSQL Database**
> These instructions only describe an upgrade that keeps the database where it already is, either separated from the GroundWork Monitor server or on the same machine. Additional steps not documented here will be needed for an upgrade that involves moving the PostgreSQL database to a separate machine as part of the upgrade. If you desire to run a separate database server, refer to the GroundWork Knowledge Base for further information, or contact GroundWork Support.

Upgrade procedure

The high-level upgrade steps for this transition are:

Step 1 - Complete the backup described above
Step 2 - Upgrade a Remote PostgreSQL Database, (if you were previously running a Remote PostgreSQL database, that component must be upgraded first)
Step 3 - Upgrade GroundWork Monitor Enterprise, and select your graphing option
Step 4 - Install new license key, if required
Step 5 - Re-merge any specialized configuration changes, Reset HTTPS settings, etc.

Step 1 - Backup (above)

Step 2 - Upgrade a Remote PostgreSQL Database

> Skip this step if you are running the PostgreSQL database directly on the GroundWork Monitor server.

In order to upgrade a PostgreSQL database running on a remote machine:

1. Run a backup as you would on a normal GroundWork server, see Backup utility description.
2. Download the installer (e.g., `groundworkenterprise-7.2.1-br494-gw3901-linux-64-installer.run`) to the Remote PostgreSQL database server.
3. Make the installer executable:

```
chmod +x groundworkenterprise-7.2.1-br494-gw3901-linux-64-installer.run
```

4. *Back on the GroundWork Monitor portal server*, stop the software for the duration of this part of the upgrade:

```
service groundwork stop
```

5. Run the installer on the Remote PostgreSQL database machine, and answer the prompts in the obvious ways. Note that you will be prompted for the root login and password.

```
./groundworkenterprise-7.2.1-br494-gw3901-linux-64-installer.run --mode text
```

   You **may** see a series of errors related to the file postgres-xtra-functions.sql. This is a known issue (see Release Notes). If so, just hit enter after each one.

6. Edit the file:

```
/usr/local/groundwork/postgresql/data/pg_hba.conf
```

   and add the line:

```
host    all             all             <ip address>/32             md5
```

   replacing the <ip address> with the IP address of the portal server, and using spaces and not tabs.

7. Edit the file:

```
/usr/local/groundwork/postgresql/data/postgresql.conf
```

and change:

```
listen_addresses = 'localhost'
```

to

```
listen_addresses = '*'
```

You may also want to increase the max_connections parameter to 500 in large installations. If you made changes to the default settings in this file as well, you'll have to merge any differences between the installed copy and the backed-up copy on a case-by-case basis.

8. Restart Groundwork on the server:

```
service groundwork restart
```

9. To take care of a known issue with this installer, *back on the GroundWork Monitor portal server*, execute the following three commands:

```
/usr/local/groundwork/postgresql/bin/psql -U postgres -d archive_gwcollagedb -f
/usr/local/groundwork/core/databases/postgresql/postgres-xtra-functions.sql
/usr/local/groundwork/postgresql/bin/psql -U postgres -d gwcollagedb -f
/usr/local/groundwork/core/databases/postgresql/postgres-xtra-functions.sql
/usr/local/groundwork/postgresql/bin/psql -U postgres -d postgres -f
/usr/local/groundwork/core/databases/postgresql/postgres-xtra-functions.sql
```

You will need to supply the postgres user password for each one.

10. Finally, *also on the GroundWork Monitor portal server*, start the system again:

```
service groundwork start
```

11. As usual, you will find the upgrade report in the `/usr/local/groundwork/upgrade-report.txt` file.

Step 3 - Upgrade of GroundWork Monitor Enterprise

Once you have a pre-upgrade backup, and (if necessary) the Remote PostgreSQL database upgraded, you may then proceed with the upgrade.

The upgrade has a dependency on the `curl` package being installed on the system. The curl package can be installed using the system package manager.
Example RHEL/CentOS: *yum install curl*, *apt-get install curl* for Ubuntu or *yast -i curl* for SLES

1. Download the installer (e.g., groundworkenterprise-7.2.1-br494-gw3901-linux-64-installer.run) to the GroundWork system that needs to be upgraded.
2. Make the installer executable:

```
chmod +x groundworkenterprise-7.2.1-br494-gw3901-linux-64-installer.run
```

3. Execute the installer. We recommend text mode.

```
./groundworkenterprise-7.2.1-br494-gw3901-linux-64-installer.run --mode text
```

Optional: Unattended installation options relating to GrafBridge

Use these options on the command line if you want to run an unattended upgrade. Be advised that these options will skip the selection of graphing technologies, and should be used only if you know exactly what you want to do, or are advised to do by GroundWork Support staff.
Select the options to use accordingly:

- InfluxDB only:

```
--mode unattended --postgres_password $PGPASSWORD
--groundwork_portal_root_user root --groundwork_portal_root_password root
```

- InfluxDB and RRD:

```
--mode unattended --postgres_password PGPASSWORD
--groundwork_portal_root_user root --groundwork_portal_root_password root
--tsdb_server_rrd 1
```

- RRD only:

```
--mode unattended --postgres_password PGPASSWORD
--groundwork_portal_root_user root --groundwork_portal_root_password root
--rrd_only_tsdb 1
```

4. The installer detects an upgrade. Choose yes to continue.

```
Export the display to user's IP address to see the installation wizard.
You may exit the installation at this point or continue with the
installation in text mode.
Do you wish to Continue? [y/N]: y

GroundWork is already installed. Do you want to upgrade? [Y/n]: y
```

5. Several questions here should be self-explanatory; answer them in the obvious ways (backup, database user verification, root login id and password).
6. When prompted as follows, you should enter "N" for no if you wish to use GrafBridge:

```
------------------------------------------------------------------------------

Do you want to use RRD as your only performance data time-series database? [y/N]:
```

7. If you enter "y" for yes here, you will have only RRD for graphing, as you had in 7.1.1. If you enter "N" for no, you will get the choice of technology:

```
------------------------------------------------------------------------------
Please select which time-series databases you wish to configure.

RRD [y/N]:

InfluxDB [Y/n]:
```

8. The defaults will install GrafBridge (InfluxDB and Grafana) and are recommended.
9. Allow the installer to complete on its own, don't interrupt it. In our testing on medium-grade equipment, this part ran for 15 minutes.

⚠ When upgrading directly from 7.1.1 to 7.2.1, the following message is displayed:

```
Warning: Problem running post-install step. Installation may not complete, or it
may be SERIOUSLY DAMAGED if it does complete.
Error running /usr/local/groundwork/perl/bin/perl
/usr/local/groundwork/core/migration/postgresql/pg_migrate_nedi.pl -U
/usr/local/groundwork/backup-2018-06-20/nedi/nedi.conf: child process exited
abnormally
Press [Enter] to continue:
```

This issue happens because your NeDi database schema is too old to support direct migration. When the upgrade completes, simply run:

```
/usr/local/groundwork/nedi/nedi.pl -i
```

to correct it with a new NeDi database.

1. Right before the end of the upgrade, a list of files you need to deal with manually will have been displayed:

```
Warning: During the upgrade procedure, the following files were detected to have
modifications. They were backed up to this directory,
/usr/local/groundwork/backup-2017-11-01. You will need to login in to this
server and manually merge these files. Some files may appear in this list
because you probably made local changes to certain options, and those changes
should now be brought forward.  Some files may appear in this list simply
because the content of the file has changed between releases. If that is the
case for a given file, and you had not changed any option values in the previous
release, you should not need to do any work to merge the old and new copies at
this time.

Press [Enter] to continue :
List of modified files:
-----------------------

/usr/local/groundwork/apache2/conf/httpd.conf
/usr/local/groundwork/apache2/conf/groundwork/apache2-noma.conf
/usr/local/groundwork/common/etc/snmp/snmptt.ini
/usr/local/groundwork/common/etc/syslog-ng.conf
/usr/local/groundwork/config/cloudhub.properties
/usr/local/groundwork/config/foundation.properties
/usr/local/groundwork/config/perfdata.properties
/usr/local/groundwork/config/status-feeder.properties
/usr/local/groundwork/config/status-viewer.properties
/usr/local/groundwork/config/ws_client.properties
/usr/local/groundwork/config/event-feeder.conf
/usr/local/groundwork/config/fping_process.conf
/usr/local/groundwork/config/log-archive-receive.conf
/usr/local/groundwork/config/log-archive-send.conf
/usr/local/groundwork/nedi/nedi.conf
/usr/local/groundwork/postgresql/data/postgresql.conf
/etc/logrotate.d/groundwork

(etc.)

Press [Enter] to continue :
```

For easy reference after the fact, this information is available in the upgrade report in the `/usr/local/groundwork/upgrade-report.txt` file.

Step 4 - Install new license (if needed)

Normally, old licenses that are still valid will continue to work after upgrade, but if you have been issued a new license file, this is a good time to

install it, (*GroundWork Administration* > *GroundWork License*).

Step 5 - Re-merge file changes you made

Once the installer has completely finished, you must compare the new copies of these files with the backup copies, and merge any local customizations in the old files into the new files. In certain cases, the backup copy may live under a different name. For the example above, the new and old files would be found in the following locations. For simplicity of presentation, all the non-absolute pathnames in this table are specified relative to the `/usr/local/groundwork/` directory. For example:

New file	Backup copy of old file
`apache2/conf/httpd.conf`	`backup-2017-11-01/apache2/conf/httpd.conf`
`common/etc/syslog-ng.conf`	`backup-2017-11-01/common/etc/syslog-ng.conf`
`config/bronx.cfg`	`backup-2017-11-01/config/bronx.cfg`
`config/cacti.properties`	`backup-2017-11-01/config/cacti.properties`
`config/console.properties`	`backup-2017-11-01/config/console.properties`
`config/db.properties`	`backup-2017-11-01/config/db.properties`
`config/foundation.properties`	`backup-2017-11-01/config/foundation.properties`
`config/perfdata.properties`	`backup-2017-11-01/config/perfdata.properties`
`config/status-feeder.properties`	`backup-2017-11-01/config/status-feeder.properties`
`config/status-viewer.properties`	`backup-2017-11-01/config/status-viewer.properties`
`config/ws_client.properties`	`backup-2017-11-01/config/ws_client.properties`
`postgresql/data/postgresql.conf`	`backup-2017-11-01/postgresql/data/postgresql.conf`
`/var/spool/cron/crontabs/nagios`	`backup-2017-11-01/crontab-nagios-2016-11-01`

Often, the differences you find between the new copy and the old copy will be due to small differences in timestamps, commenting, or spacing, and can be safely ignored. Sometimes, new information will be present in the new copy that should be left alone. Only change those areas of the new files that you know you are responsible for.

In case you had SSL enabled, the upgrade will absolutely break your settings in files like httpd.conf, because we revert to a default non SSL condition. Your best course may be to use the new tool as described below and here to restore the SSL capability. Following this step you can then review the differences between the backup and what is running, for **additional** changes you may have set up in 7.1.1 or 7.2.0

Understanding Installation Problems
The installer leaves a log file in a filename like `/tmp/bitrock_installer_10602.log` which contains a record of the install processing. In case of trouble during the installation phase, that's a primary place to look for clues.

- **Final Steps in Upgrade**
  Once the upgrade process is complete, you must take the following steps to fully instantiate the changes:
  - If you had to modify any files just above after the installer finished, you should bounce the entire system to make sure all components are restarted with the revised configurations.

    ```
    service groundwork restart
    ```

  - Log in to the UI as an administrative user.
  - Run a Configuration > Control > Commit operation to put the upgraded configuration data fully into production. This will establish that all of the database configuration and connections are working as intended, and that all areas of the monitoring configuration are fully synchronized.

> **Troubleshooting Advice**
> The most common reason we have seen in testing for a failure to access the monitoring system UI at this point is that the user's browser is retaining some data that is not automatically cleaned up by the new release. If you have trouble accessing the Configuration screens in the user interface, try logging out, clearing your browser cookies and cache, and logging back in again.

- If you have GroundWork Distributed Monitoring Agents (GDMA) in play, the GDMA clients periodically refresh their externals files from the server. However, immediately after the upgrade, those externals files are not present. They were backed up, but they're not in the production directory. To regenerate the externals files so you don't get stale check results from GDMA clients, run a *Configuration* > *Control* > *Build externals* operation.

Post upgrade tasks

After a successful upgrade to GroundWork Monitor Enterprise 7.2.1, some additional steps are necessary to finish the upgrade process. Please review the following notes and make sure that you apply the changes to your installation.

- **Feeder updates**
  If you are using Cacti, and especially the Cacti feeder, you will need to do a few more steps. Even if you aren't currently doing so, it's a good idea to migrate the default feeder files anyway, in case you want to make use of the Cacti features in the future. The following steps just show the minimal files for a default install. If you have more feeder endpoints configured, you will naturally have more files to migrate.
  1. Restore the master configuration file `cacti_feeder.conf` from the installer backup config directory (e.g., `/usr/local/groundwork/backup-2018-06-21/config`)
     - For example:

     ```
     cp /usr/local/groundwork/backup-2018-06-21/config/cacti_feeder.conf
     /usr/local/groundwork/config/cacti_feeder.conf
     ```

  2. Restore the GroundWork endpoint feeder config files, which may vary according to the endpoint directives in the master config file, e.g., `cacti_feeder_localhost.conf`
     - For example:

     ```
     cp /usr/local/groundwork/backup-2018-06-21/config/cacti_feeder_localhost.conf
     /usr/local/groundwork/config/cacti_feeder_localhost.conf
     ```

  3. Restore the web services properties files as defined in the endpoint config files with the `ws_client_config_file` directives, e.g., `/usr/local/groundwork/config/ws_client.properties`
     - For example:

     ```
     cp /usr/local/groundwork/backup-2018-06-21/config/ws_client.properties
     /usr/local/groundwork/config/ws_client.properties
     ```

  4. Make sure all of the files you just copied have `nagios:nagios` ownership, for example:

     ```
     chown nagios:nagios /usr/local/groundwork/config/cacti_feeder.conf
     chown nagios:nagios /usr/local/groundwork/config/cacti_feeder_localhost.conf
     chown nagios:nagios /usr/local/groundwork/config/ws_client.properties
     ```

  5. Migrate the restored master config files by running this script:

     ```
     /usr/local/groundwork/core/migration/migrate_RAPID_feeder_configs_711.sh
     ```

- **Restore any custom portal root user name definitions**
  If you changed the root user name, you will need to restore this change after upgrade. If you haven't changed the root user name, skip this step.
  1. Restore the `gatein.properties` file from the backup config directory (e.g., `/usr/local/groundwork/backup-2018-06-21/config`). For example:

     ```
     cp /usr/local/groundwork/backup-2018-06-21/config/gatein.properties
     /usr/local/groundwork/config/gatein.properties
     ```

2. Run the following command:

```
/usr/local/groundwork/java/bin/java -cp
/usr/local/groundwork/jpp/modules/com/groundwork/security/main/groundwork-jboss-security-7.1
com.groundwork.core.security.GateinConfigurationUtils -superuser svc_gwroot
```

- **Web Services API token**
  - If you had not done so before, establish non-default passwords for all of the standard GroundWork-supplied user accounts and API token listed in the Default Login Information subsection above for new installs.
  - If you change the API token and you are using Cloud Hub, be sure to modify all running connectors and replace the old token with the new one, to ensure that Cloud Hub can still contact the GroundWork server to post results. See Hybrid Cloud Monitoring .

- **Restore HTTPS/SSL Settings**
  The procedure for enabling HTTPS has changed since 7.1.1, and is now scripted. See How to enable HTTPS for details. If you were using HTTPS in 7.1.1 prior to upgrade, **this upgrade will disable it**. Please review these steps to ensure it is properly configured for your installation.

  
  Note that as the certificates you had previously were preserved, there is no need to regenerate them or to import them into the keystore. Per the How to notes you will need to have them available when you run the enabling script.

- **Restore Multi-endpoint LDAP configuration if necessary**
  In most cases LDAP configuration is preserved across upgrade to 7.2.1, however if you use the multiple endpoints configuration permitted in 7.1.1 with Technical Bulletin number 11, you will need to re-merge the configuration you had before upgrade. You can follow the directions in the article How to AD and LDAP configuration.

- **GDMA agents reporting to the GroundWork server with HTTPS/SSL enabled**
  Once you upgrade to 7.2.1 and install https, the server-side SSL settings will restrict communications to use the TLS 1.2 protocol only, and strong ciphers. If you are using GDMA with HTTPS, and you were using an older version (perhaps from a previous installation) of the GDMA agent before 2.5.0, as supplied with GroundWork Monitor 7.1.0 and older versions, then your GDMA may not support TLS 1.2. As such, they will not be able to retrieve new configurations from the default GroundWork Monitor 7.2.1 server setup with HTTPS. A different channel (NSCA) is used to send data monitoring results to the server, and that will still be working, at least until the GDMA client's configured `Poller_Pull_Failure_Interval` expires (default is 1 day). You will want to act immediately to allow the old agents to pull configurations, and to upgrade GDMA agents to the latest versions.

  Until you have all your old GDMA agents upgraded, the best approach is to leave as much of the upgraded protocol and cipher-list support in place as possible, and only open a hole large enough for the old GDMA clients to still connect. Here are the steps for that. All of the changes are made to the `/usr/local/groundwork/apache2/conf/extra/httpd-ssl.conf` file. We leave comments in the config file as breadcrumbs pointing the way back to locking down security once you no longer have any older GDMA clients in play.
  1. Change this line:

     ```
     SSLProtocol -all +TLSv1.2
     ```

     to this:

     ```
     # SSLProtocol -all +TLSv1.2
     # The preceding line should eventually be put back into play.
     # The following line is only in use until all GDMA clients have been converted to
     # run GDMA 2.5.0 or later, at which point the earlier line should be put back.
     SSLProtocol -all +TLSv1.2 +TLSv1
     ```

  2. Comment out this line (with lots of stuff in the middle of the long string elided here for clarity, but keep it intact in the file to preserve its exact current form):

     ```
     SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256: ... :!DES:!RC4:!3DES:!MD5:!PSK
     ```

     then make an uncommented copy of it underneath that, and add comments and change the new line so the set of lines reads:

     ```
     # SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256: ... :!DES:!RC4:!3DES:!MD5:!PSK
     # The preceding line should eventually be put back into play.
     # The following line is only in use until all GDMA clients have been converted to
     # run GDMA 2.5.0 or later, at which point the earlier line should be put back.
     SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256: ... :!DES:-RC4:!3DES:!MD5:!PSK:RC4-SHA
     ```

Which is to say, in the new uncommented line, change `!RC4` to `-RC4` and add `:RC4-SHA` at the end.

3. Change this line:

```
#SSLHonorCipherOrder on
```

   to this:

```
SSLHonorCipherOrder on
```

   so TLS 1.2 clients (browsers, and GDMA 2.5.0 clients) will prefer the modern set of ciphers over `RC4-SHA`.

4. After making those changes, restart Apache:

```
service groundwork restart apache
```

   Once you complete all the GDMA upgrades at your site, you can move the new (unaltered 7.2.1) settings of `SSLProtocol` and `SSLCipherSuite` back into place and restart Apache again. For more subtle configurations, and advice on managing this process, please contact GroundWork Support.