GROUNDWORK
OPEN SOURCE

HOW TO – GDMA v0.5

(GroundWork Distributed Monitoring Agents)

Prepared by:
Revised Version sourced from 'GDMA Instructions' v0.4.1 (January 6, 2008)
Version 0.1 Dr. Dave Blunt (April 14, 2008)
Version 0.2 Hans Kriel (May 1, 2008)
Version 0.3 Dominic Nicholas (May 5, 2008)
Version 0.4 Glenn Herteg (May 16, 2008)
Version 0.5 Glenn Herteg (July 24, 2008)

Table of Contents

Summary

This document describes the steps necessary to set up GroundWork Distributed Monitoring Agents and the necessary GroundWork Monitor server components.

Briefly, the Parent server runs GroundWork Monitor and is configured with all host and service definitions. These definitions are extended with Monarch Externals entries. GDMA software on each host is configured to communicate with the Parent to pull Externals entries and use them as the basis for monitoring. Results of monitoring are then sent to the Parent using NSCA messages.

Prerequisites

- GroundWork Monitor Pro 5.1.3 or Enterprise 5.2.X correctly installed on the Parent server.
- Parent server configured with all hosts to be monitored.
- Target GDMA hosts with supported platforms (see Appendix A).
- Standard RPMs already installed on the target hosts to support GDMA communication and operating functionality: openssh-clients, openssl, perl.
- The ability to write to `/usr/local/groundwork` on the target GDMA hosts. (This may be an issue for sites which NFS-mount `/usr/local` as a read-only filesystem on the target hosts. In such a case, you will need to establish a `/usr/local/groundwork -> somewhere_else` symbolic link that points to a secondary directory that is known to be available on all target hosts which use such remote mounting. The *somewhere_else* directory must already exist on each target host before the GDMA RPMs are installed.)
- Communication from the GDMA hosts to the Parent on TCP port 22 (for SSH) is allowed.
- Communication from the GDMA hosts to the Parent on TCP port 5667 (for NSCA) is allowed.
- Updated Monarch modules to support Monarch Externals for GDMA deployments obtained from GroundWork support staff.[1]

GDMA Package Preparation

The GDMA software is provided as a pair of packages on each supported platform. A GDMA base package provides the target software, and a GDMA key package provides the credentials for target hosts to connect unassisted to the GroundWork Monitor server. As such, the GDMA key package will always need to be generated specially for the individual customer; see the separate build instructions for details. In addition, the GDMA base package may need customization to provide consistent UID/GID numeric values across target hosts. Again, see the build instructions for details.

[1] For version 5.1.3 only. These updates are included in GroundWork Monitor Enterprise 5.2.X.

GroundWork Monitor Setup

NSCA Communication Setup in GroundWork Monitor Professional 5.1.3

NSCA communications in this version of GroundWork Monitor are controlled by a list of allowed IP addresses. The limit for this list is 2047 characters. If the number of hosts is expected to exceed this limit, the customer is advised to upgrade to GroundWork Monitor Enterprise 5.2.X or contemplate upgrading the NSCA component of 5.1.3 from version 2.4 to version 2.7.2. This has been done successfully for several customers and works around other limitations seen in the earlier version of NSCA. Instructions for upgrading from NSCA 2.4 to 2.7.2 can be obtained from GroundWork Support.

If the number of hosts will result in a list of 2047 characters or less then follow these steps:

1. On the Parent server edit the file `/usr/local/groundwork/etc/nsca.cfg` and change the `allowed_hosts` directive to include the IP addresses of the GDMA hosts.
2. Restart the `nsca` daemon by executing `/etc/init.d/nsca restart` as user `root`.

NSCA Communication Setup in GroundWork Monitor Enterprise 5.2.X

NSCA communications in this version of GroundWork Monitor are controlled by a list of allowed IP addresses. The limit for this list is 2047 characters. However, the use of wildcards in each entry is supported and thus it is expected that blocks of network addresses can be allowed without unduly impacting security.

1. On the Parent server edit the file `/usr/local/groundwork/etc/bronx.cfg` and add a line with the directive `listener_allowed_hosts=`*comma-separated-list* and change the list to include the IP addresses of the monitored GDMA hosts. You can specify certain types of IP address ranges by using a `*` character as a wildcard that will match any given IP address to the end. For instance, `192.168.*` matches the entire range of `192.168.0.0` through `192.168.255.255`.
2. In *Configuration->Control->Nagios main configuration* make sure that the last page of options for the `nagios.cfg` file includes the following two Event Broker settings:
   Event broker options: `-1`
   Broker module (all on one line):
   ```
   /usr/local/groundwork/nagios/modules/libbronx.so
       -c/usr/local/groundwork/etc/bronx.cfg
   ```
3. Restart the `nagios` daemon. This is done automatically if you Commit the setting in the preceding step. Or if that setting was already in place, you can do so manually by executing
   ```
   /etc/init.d/nagios restart
   ```
   as user `root`.

SSH Communication Setup

SSH communication is initiated from each GDMA host. This is done using public-private key pairs, with the private key existing on each GDMA host and the public key existing on the GroundWork Monitor server. A `gdmakey` package is created by GroundWork using the host name and IP address of the GroundWork Monitor server, and this package contains both keys. The package is installed on each monitored GDMA host. The public key must be copied to the GroundWork Monitor server from one of the hosts where the `gdmakey` package was installed. For a site that monitors both Linux and Solaris machines with GDMA, separate keys will be provided for the different platforms, and the public keys from both platforms must be installed on the GW Monitor server.

The GDMA host software will not begin monitoring until it has in hand its own configuration of what probes to run. Normally, that configuration is obtained by fetching it from the GroundWork server, so monitoring will not begin until the host can contact the server. And that contact will not complete until the host's `~gdma/.ssh/known_hosts` file is updated with proper SSH credentials. There are three possible ways to handle this:

- While logged in as `gdma`, run `ssh` once manually on each host after the GDMA and GDMA key packages are installed, connecting to the GroundWork server. The `ssh` program will prompt you as to whether you wish to accept the server's credentials, and it will populate the `~gdma/.ssh/known_hosts` file with those credentials.
- Distribute an appropriate `~gdma/.ssh/known_hosts` file to each host after the GDMA and GDMA key packages are installed on the client, through means outside of the packages themselves.
- (often preferred) Run `ssh` manually on one client machine as above, capture a `known_hosts` file that contains just the proper credentials for accessing the GroundWork server, then have GroundWork Professional Services include this file in the generated GDMA key RPM.

To make the last of these choices happen, you must create and capture an appropriately populated `known_hosts` file at the customer site, transfer it back to GroundWork, and use it according to the GDMA key package build instructions specified in a separate document.

It is not possible to install the `gdma` package itself on the GroundWork Monitor server for the purpose of conveniently creating the `gdma` user and necessary directories for SSH key files. Instead you must perform the following procedure:

1. Create the `gdma` user on the GroundWork Server, substituting the correct UID and GID where in this example we show `31341`. It is useful to use a consistent numbering throughout and to use local user/group creation and not NIS or LDAP (to keep the monitoring running smoothly in case of an NIS or LDAP service failure).
   ```
   /usr/sbin/groupadd -g 31341 -o -f gdma
   /usr/sbin/useradd -c "GroundWork Agent" \
       -d /usr/local/groundwork/gdma -u 31341 -g gdma -m gdma
   ```
2. Make a `~gdma/.ssh` directory in which the SSH public key will be stored. An easy way to create it with the proper (700) permissions is by going further and locally generating SSH keys:

```
su – gdma
ssh-keygen –t dsa –b 2048
```

For the latter command, press return at each question to take the default answer.

3. Install the `gdma` package on at least one GDMA host.
4. Install the `gdmakey` package on that GDMA host.
5. Log in to a shell on the GDMA host as user `gdma` . Since the password for the `gdma` user on that host will likely be purposely invalid or locked, you will probably need to first `su` and then `su – gdma` to effect this login. Then change directory with:
   ```
   cd ~gdma/.ssh
   ```
6. In this step, you will populate the GroundWork server's `authorized_keys` file with the public key(s) the target hosts will use to connect to the server. If you have only Linux target hosts, all operating with exactly the same GDMA key RPM, you can completely replace the existing file by securely copying the `id_dsa.pub` file from the current directory on the GDMA host to the GroundWork server with this command:
   ```
   scp id_dsa.pub root@GW_Monitor_server_IP:~gdma/.ssh/authorized_keys
   ```
   On the other hand, if you have multiple platforms on which you will install the GDMA software, say both Linux and Solaris, or if for historical reasons you will have multiple versions of the GDMA key package installed on your machines, you will need to combine the respective public keys from the different GDMA key packages by copying the `id_dsa.pub` file from each distinct key package to the GroundWork server and appending its contents to the `~gdma/.ssh/authorized_keys` file.
7. Log in to a shell as user `root` on the GroundWork server and change directory with:
   ```
   cd ~gdma/.ssh
   ```
8. Change ownership and permissions of the `authorized_keys` file with:
   ```
   chown gdma.gdma authorized_keys
   chmod 600       authorized_keys
   ```

If the `gdmakey` package creation environment is not available for a given customer platform to be monitored, but the `gdma` package itself was installed on the hosts to be monitored, the followng simple instructions may be followed in lieu of installing the GDMA key package on the machines running that platform. (This scenario is highly unlikely, given that the `gdma` package itself would then not be available, either.)

1. Perform steps 1 and 2 from above.
2. Append the public key to the `authorized_keys` file, keeping care to preserve any existing entries in that file:
   ```
   su – gdma
   cd .ssh
   cat id_dsa.pub >> authorized_keys
   chmod 600         authorized_keys
   exit
   ```
3. Copy the private key `id_dsa` to each target host, using a secure file-transfer method because this is secret information. Since allowed communication paths vary from customer to customer, you will have to choose a method that works in your environment. The private key must go in `~gdma/.ssh` (which must have 700 permissions), be owned by `gdma.gdma`, and have 0600 permissions.

Monarch Group Configuration

At least one Monarch Group is required for GDMA hosts in order to correctly define a build directory for the Monarch Externals files.

1. Log in to the Parent web interface (`http://`*parenthostname*`/monitor/index.php`) as a user capable of accessing the *Configuration* application. The usual user for this purpose is `admin` .
2. Navigate to the *Configuration* application and then to the *Groups* tab.
3. Click the *New* link and in the *Name* field type an identifier to indicate this Group is for GDMA hosts, e.g. `gdma` . Click the *Add* button.
4. In the new screen that appears, enter some description of the GDMA hosts into the *Description* field.
5. In the *Build folder* field, type in `/usr/local/groundwork/gdma/config` .
6. Leave all other fields blank.
7. Click *Save.*
8. Select the *Hosts* tab for this new Group and assign all hosts that you wish to have monitored by GDMA.
9. From a `root` shell on the Parent server, create the directory defined in step 5 and change ownership and permissions of that directory with these commands:

```
chown nagios.nagios /usr/local/groundwork/gdma/config
chmod 775           /usr/local/groundwork/gdma/config
```

Create Externals Definitions

Monarch is used to define the monitored hosts, and to define the configuration file used by each GDMA host. In order to ease the process of defining GDMA host configuration files, a simple Monarch host profile for a UNIX host is provided by GroundWork. The host profile includes a service profile with the following attributes:

- Nagios Host definitions.
- Nagios service definitions for the passive services.
- External definitions matching the passive services.

To use the provided host profile, use the following procedure:

1. For **GroundWork Monitor Professional 5.1.3 only**, make backup copies of the following files under `/usr/local/groundwork/monarch/lib` :

   ```
   MonarchExternals.pm
   MonarchProfileExport.pm
   MonarchProfileImport.pm
   MonarchStorProc.pm
   ```

   Replace the original files with the corresponding files within the `Monarch_files_to_support_profile_externals_import` directory that came with the software package. This software package is available from GroundWork Professional Services. **This step is not required for GroundWork Monitor Enterprise 5.2.X.**
2. Enable externals in Monarch via the *Configuration->Control->Setup* option.

3. Copy the `host-profile-gwsp2-gdma.xml` and `perfconfig-gwsp2-gdma.xml` files to `/usr/local/groundwork/profiles` and set ownership to `nagios.nagios` and permissions to 660. Import this host profile using the C*onfiguration -> Profiles -> Profile Importer*.
4. Add the target monitored hosts using the standard Monarch facility and assign the `gwsp2-gdma` profile to these hosts. This will create the passive services for these hosts and ensure host and service externals are applied to them. Go to C*onfiguration -> Hosts -> Host externals -> Modify* and update the default host external with the correct IP address(es) for the GroundWork Monitor Parent server.
5. Generate the external configuration files by going to the *Configuration->Control* menu and selecting the *Run Externals* option. This will generate a configuration file in the directory specified in the Monarch Group build directory for each host that has been assigned the `gwsp2-gdma` GDMA service profile. This step has to be performed whenever an update to host or service definitions for GDMA hosts is required.
6. Execute a Monarch Commit to update the Nagios system.

GDMA Monitored-Host Setup

Special Notes for Solaris

1. Installation of Solaris packages can occur in several different contexts: on a standalone machine; into a diskless client's file tree from the server that supports that file tree; into a JumpStart repository, a LiveUpgrade repository, a network-install repository, or a Flash archive; in a non-global zone (under Solaris 10); into a virtual-machine copy of Solaris; and so forth. As of this writing, the Solaris GDMA packages have only been written and tested in the standalone-server mode, meaning that they must be installed while you are logged into the individual machine on which the packages are to be installed. No relocation or client support is included at this time. On Solaris 10, only global-zone installation has been tested so far.
2. Solaris 8 and earlier releases do not ship with a copy of SSH, either in the base OS or in the Software Companion packages. SSH is important to operation of GDMA because it allows the distributed agents to have their configuration files automatically updated. Specifically, the `scp` program is used for that purpose. If you install a copy in `/usr/local/bin/scp` (say, from `www.sunfreeware.com` packages, starting with the openssh distribution), you will need to create a symbolic link so this copy can be found by the GDMA scripts:
   ```
   su root
   cd /usr/bin
   ln -s /usr/local/bin/scp
   exit
   ```
3. On a Solaris 2.6 machine, some special setup must occur because the base operating system does not ship with a version of Perl already integrated. Perl is used by the GDMA software. The easiest way to install an up-to-date Perl is to visit `www.sunfreeware.com` and pick up the already-packaged copy of Perl for this version of Solaris. That copy of Perl installs the main binary as `/usr/local/bin/perl`

whereas the GDMA scripts look for it as `/usr/bin/perl`, so a symbolic link must be created:

```
su root
cd /usr/bin
ln -s /usr/local/bin/perl
exit
```

On newer releases such as Solaris 9 and Solaris 10, Perl comes as an integrated part of the OS, already available under `/usr/bin/perl`, so no special action in this regard is needed on those platforms unless the standard Perl packages were not originally installed along with the operating system.

4. The GDMA software runs as a fixed `gdma` user. If you wish to have this account utilize consistent numeric UID and GID values across your monitored machines, you must set that up before installing the GDMA software. This can be done through LDAP, NIS, or the local password, shadow, and group files, as desired at the customer site. The password should be locked because no logins are expected on this account.
   If the customer will create this account on the monitored machines, the relevant information is:
   User ID: `gdma`
   Group ID: `gdma`
   Home Directory: `/opt/groundwork/home/gdma`
   Password: locked (i.e., no direct logins are allowed)
   If this is not set up beforehand, installation of the Solaris packages will automatically create a new local `gdma` user with the settings above, via the standard `/usr/sbin/useradd`, `/usr/sbin/groupadd`, and `/usr/bin/passwd` programs.
5. If SSH is not available on the distributed machine being monitored, the GDMA software will not be able to initially fetch or later update its configuration file from the central GroundWork Monitor server. Failure to update is benign, in that the attempt to do so will be made periodically but it will fail without serious consequence. However, failure to fetch the initial configuration file is fatal to the monitoring, so it must be manually set in place. This is particularly an issue with Solaris 2.6 through Solaris 8, for which SSH does not come standard with either the base OS or the Software Companion packages. The customer can either compile it themselves or load prepackaged software from a trusted source such as the `www.sunfreeware.com` repository.
   If manual installation of the config file is used, it must be placed here:
   `/opt/groundwork/home/gdma/config/gwmon_`*hostname*`.cfg`
   where *hostname* is the unqualified name of the machine. This is the node name (found by `uname -n`), not necessarily a network-interface-specific name. When `scp` is used to fetch the configuration file from the GroundWork server, the software assumes that is the name by which the GroundWork server knows the distributed machine being monitored.
6. The `known_hosts` issue is not resolved (i.e., folded into the GDMA key package) on this platform as of this writing. Thus if fetching the GDMA configuration file periodically to keep it up to date is desired, it will be necessary to either distribute an appropriate copy of the `~gdma/.ssh/known_hosts` file separate from the GDMA packages after they are installed, or an SSH connection must be manually attempted from the Solaris platform to the GroundWork server to get `ssh` to populate the `known_hosts` file with the proper credentials.

Software Installation

1. Log in to a shell on the target host as user `root` .
2. Copy the RPM or package set appropriate to the OS and architecture to the host. This will include both a `gdma` package and a `gdmakey` package. On Solaris, these will be named `GWOSgdma` and either `GWOSgdmak` or `GWOSgdmakey`, respectively.
3. For Linux, run the command: `rpm –Uvh gdma*rpm`
4. For Solaris, you must install the base package before installing the key package. Use the following commands:
   `pkgadd –d` *path_to_package/gdma_package_file*
   `pkgadd –d` *path_to_package/gdmakey_package_file*
5. On a Solaris machine which does not have SSH installed, fetch and manually install the appropriately named GDMA configuration file as described in the Special Notes for Solaris above.
6. On a Solaris machine which does have SSH installed, either manually `ssh` to the GroundWork server as `gdma` to set up the `known_hosts` file, or obtain and install a `known_hosts` file from some trusted source, containing just the credentials for the central GroundWork server.
7. On Linux, if the `known_hosts` file is not embedded in your GDMA key RPM, you will either need to distribute a `known_hosts` file of your own to the target hosts, or perform the same kind of manual `ssh` login to the GroundWork server as described for the Solaris platform.

Software Configuration

Start the GDM Agent on the target host.

1. For Linux the command is: `/etc/rc.d/init.d/gdma start`
2. For Solaris the command is: `/etc/init.d/gdma start`

TESTING THE INSTALLATION

Testing Externals file creation

1. While still logged in to the Parent web interface, navigate to the *Configuration->Control* menu and click *Run externals*.
2. Log in to a root shell on the Parent server.
3. Change directory to `/usr/local/groundwork/config` and look at the contents of this subdirectory. There should be one configuration file per host, and the file timestamps should reflect the file generation you just invoked.

Testing Monitoring on the GDMA host

1. Log in to the GDMA Host as `root` .
2. Look at the process list using the command `ps –ef | grep gdma` and observe that the daemon is running. The script in question is `gdma_check.pl` .

3. Under Linux:
    a. Compare `/usr/local/groundwork/gdma/config/gwmon_`*hostname*`.cfg` with the corresponding file on the GW server to see that the contents are the same.
    b. Check the `/usr/local/groundwork/gdma/log/*.log` file for evidence of monitoring and evidence of a send string and successful transmission of a data packet to the Parent server.
4. Under Solaris:
    a. Compare `/opt/groundwork/gdma/config/gwmon_`*hostname*`.cfg` with the corresponding file on the GW server to see that the contents are the same.
    b. Check the `/opt/groundwork/gdma/log/*.log` file for evidence of monitoring and evidence of a send string and successful transmission of a data packet to the Parent server.

APPENDIX A: SUPPORTED GDMA PLATFORMS

The following table reflects the supported target GDMA platforms at the time of writing. Note that Linux GDMA RPMs (the base software, not the key RPMs) before the 2.0.5 release have had various build problems and should not be considered to be supportable if problems arise. Rather, such installations should be immediately upgraded to version 2.0.5 or later.

Vendor	OS and version	Architecture	GDMA version	GDMA key version
RedHat	EL 4	32-bit	2.0.5	2.0.3
	EL 4	64-bit	2.0.5	2.0.3
	EL 5	32-bit	2.0.5	2.0.3
	EL 5	64-bit	2.0.5	2.0.3
Novell	SuSE ES 9	32-bit	2.0.5	2.0.3
	SuSE ES 10	32-bit	2.0.5	2.0.3
	SuSE ES 10	64-bit	2.0.5	2.0.3
Sun	Solaris 2.6	SPARC	2.0.6	2.0.6
	Solaris 8	SPARC	2.0.6	2.0.6
	Solaris 9	SPARC	2.0.6	2.0.6
	Solaris 10	SPARC	2.0.6	2.0.6