Quick Start Auto Registration

Contents

This page references Automated Agent Registration and is designed to quickly get you started monitoring hosts with GDMA. Outlined below are the steps necessary to configure an existing GroundWork server to support GDMA agents, and install and configure the agent on Linux and Windows hosts. Solaris installations are similar to Linux, with the exception of the location of the agent directories and certain paths. Once you have the basic install working, you can then refer to the GDMA Advanced section to see how to customize the configuration of GDMA to meet your needs.

1.0 Adding/Changing GDMA Credentials

The credentials used by the deployed GDMA agents needs to be added to the JBoss Application Server so calls to the legacy REST API succeed. By default the server is configured to use the credentials `gdma/gdma`, however it is recommended to change the password regularly. Follow the steps below on the GroundWork Monitor server to add the credentials to the authentication store.

1.1 Generate and change credentials

> ⚠ **Regarding backslash character**
> Before you start, if the USER or PWD part of the string to be hashed contains a '\' character, start instead at section 1.2 Generate and change credentials (with '\' character) below.

In the properties file the GDMA default password is set to `gdma=8ae0d35b1f513c066178c3eaf805a0fa`. To change the password you need to first create a MD5 Hex. In the example below we use: {USER}: `gdma`, {PWD}: `#changeME`, and the command: `echo -n "{USER}:ApplicationRealm:{PWD}"|md5sum`

1. As the `root` user enter the following command (using the appropriate USER and PWD):

   ```
   echo -n gdma:ApplicationRealm:#changeME|md5sum
   ```

   Which produces a MD5 Hex value:

   ```
   6f46676d7c793eaae2ed13f5bb676a46
   ```

2. Edit the properties file with the following command:

   ```
   vi /usr/local/groundwork/jpp/standalone/configuration/application-users.properties
   ```

3. Locate and change the GDMA username and password hash to the new MD5 Hex value (example shown, use your own Hex value):
   - from:

     ```
     gdma=8ae0d35b1f513c066178c3eaf805a0fa
     ```

   - to:

     ```
     gdma=6f46676d7c793eaae2ed13f5bb676a46
     ```

Dual JBoss Systems
Before you continue, if you are running a dual JBoss system you will need to change an additional file as describ
below.
To check if you are running a dual JBoss system enter the command:
`ps -ef | grep java`
Dual JBoss systems will have two processes starting with: "/usr/local/groundwork/java/bin/java -D[Standalone]"

- Edit the properties file with the following command:
  `vi /usr/local/groundwork/jpp2/standalone/configuration/application-users.propert`
- Locate and change the GDMA username and password hash to the new MD5 Hex value: (example is shown, use your own Hex value)
  - from:
    `gdma=8ae0d35b1f513c066178c3eaf805a0fa`
  - to:
    `gdma=6f46676d7c793eaae2ed13f5bb676a46`

4. Save the file. From this point on the requests through the legacy REST API will succeed. Continue at section 2.0 Configuring GDMA.

1.2 Generate and change credentials (with '\' character)

In the case of the USER or PWD part of the string to be hashed contains a '\' character, the '\' characters must be properly escaped before piping to md5sum. For example one might use the netbios naming convention domain\username with a password such as `A\gjhjhg`. Both '\' characters in this case must be properly escaped before piping to md5sum. Use the string `\u005c` in every place that you have a '\'.

In the properties file the GDMA default user and password is set to `gdma=8ae0d35b1f513c066178c3eaf805a0fa`. To change the password you need to first create a MD5 Hex. In the example below we use: {DOMAIN}/{USER}: `example.com/gdma`, {PWD}: `A\gjhjhg`, and the command: `echo -n "{DOMAIN}{USER}:ApplicationRealm:{PWD}"|md5sum`

1. As the `root` user enter the following command: (using the appropriate USER and PWD)

   ```
   echo -n example.com\u005cgdma:ApplicationRealm:A\u005cgjhjhg|md5sum
   ```

   Which produces a MD5 Hex values:

   ```
   29aecce20dfaf39c0050696d5d9b9589
   ```

2. Edit the properties file with the following command:

   ```
   vi /usr/local/groundwork/jpp/standalone/configuration/application-users.properties
   ```

3. Locate and change the GDMA username and password hash to the new MD5 Hex value: (example shown)
   - from:

     ```
     gdma=8ae0d35b1f513c066178c3eaf805a0fa
     ```

   - to:

     ```
     example.com\gdma=29aecce20dfaf39c0050696d5d9b9589
     ```

Dual JBoss Systems
Before you continue, if you are running a dual JBoss system you will need to change an additional file as describ
below.
To check if you are running a dual JBoss system enter the command:
`ps -ef | grep java`

- Edit the properties file with the following command:
  `vi /usr/local/groundwork/jpp2/standalone/configuration/application-users.propert`
- Locate and change the GDMA username and password hash to the new MD5 Hex value: (example shov
  - from:
    `gdma=8ae0d35b1f513c066178c3eaf805a0fa`
  - to:
    `example.com\gdma=29aecce20dfaf39c0050696d5d9b9589`

4. Save the file. From this point on the requests through the legacy REST API will succeed.

2.0 Configuring GDMA

The first section below outlines steps to configure a GroundWork Monitor server as the target server for GDMA results and a source for GDMA configuration data. The next section outlines the configuration for GDMA client servers.

2.1 Configuring the GroundWork Monitor target server

The following steps should be followed for new installations and upgrades. If you are upgrading an existing GDMA target server the following steps may already be in place however should be verified.

1. **Back up the Monarch database**
   - It is highly recommended in a production environment to back up the Monarch database before beginning a GDMA configuration, see [DOCDEV:How to back up and restore].
2. **Create port accessibility**
   - The GDMA agents on the GDMA client servers must have access to the GDMA target on ports 80 (HTTP) or 443 (HTTPS). Also, the GDMA client servers must be able to *write* to the GDMA target port 5667 (NSCA). Make sure these ports are accessible before you try to deploy. The GroundWork Server firewall needs to have these ports open.
3. **Synchronize target server and GDMA monitored hosts clocks**
   - The GDMA operation requires a unified time base for target servers and monitored systems. This is normally accomplished using an external clock source such as NTP (Network Time Protocol) for all systems. Messages from systems with out-of-sync clocks may be dropped silently by the Nagios Event Broker (Bronx).
4. **Set up NSCA communication**
   - GroundWork Monitor (6.0 and later) uses Bronx to process passive check results for Nagios and it listens at port 5667 for NSCA messages. Most of the GDMA messages will arrive in real time, although there may be short network outages and GDMA can buffer messages during these short interruptions. While communication is down, monitored results are locally *spooled* on the hosts and when communication is restored GDMA sends the spooled results with their original timestamps. The GroundWork server and all monitored hosts clocks must be synchronized to within the tolerances specified in the server Bronx configuration, typically plus or minus 15 minutes.
   - To set times edit the Bronx file:

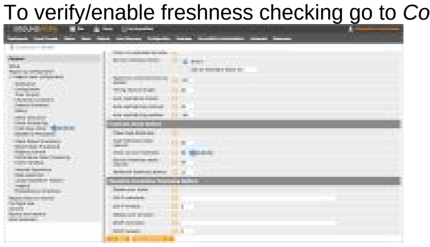
     ```
     vi /usr/local/groundwork/config/bronx.cfg
     ```

   - Scroll down to the *LISTENER MAX PACKET AGE* section and edit the `listener_max_packet_age` to `900` seconds to allow for 15 minutes of GDMA spooling. Longer durations are possible, but may result in transient overload conditions on the GroundWork server while large data volumes are processed. Similarly, packets will be dropped by Bronx if they contain a future timestamp. This can be an issue in environments where perfect time synchronization is not possible. Setting the `listener_max_packet_imminence` parameter will compensate for a small amount of future time variance between the monitored node and the Target server. We suggest leaving the default of `1` second unless this is determined to be a problem in the environment. Finally, the `use_client_timestamp` parameter should be left at the default of `1` to allow the timestamp from the monitored node to be used. This is useful in collecting the performance data and graphing it in time series graphs in the interface. If this parameter is set to `0`, the server timestamp will be used and graphing may not be accurate.

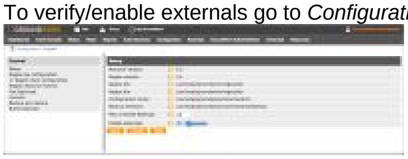
     The following settings are from the Bronx configuration file `/usr/local/groundwork/config/bronx.cfg`. If any changes are made, Nagios must be restarted to put them into effect, `service groundwork restart nagios`.

```
# LISTENER MAX PACKET IMMINENCE
# The max allowed "future age", in seconds, of the passive check result received.
# Any newer results are dropped to the floor.
# The maximum allowed value is "900" seconds.
# Set the value to "0" to disallow passive checks with newer timestamps.
# If not specified, the value will be "1" second, which should be just
# enough to allow for possible slight discrepancies which can arise even
# between time-synchronized client and server machines.  In general, we
# highly recommend that the site use NTP or similar time-synchronization
# software to tie together the software clocks on disparate machines to
# high accuracy, to prevent misunderstandings about when events actually
# occur.  Note that time synchronization for a VM guest machine can be
# problematic; see your vendor's documentation on this topic.
# The GroundWork-recommended value is 900, largely because Windows
# machines often have trouble maintaining Internet time synchronization.
listener_max_packet_imminence=900 \\ \\
# USE CLIENT TIMESTAMP
# This parameter, if set to a positive value, configures the listener thread
# to use the timestamp in the passive check result received for processing,
# rather than the time on the server when the check result is processed.
# To prevent confusion in handling data from clients which are not
# time-synchronized to the server, such a check result timestamp will be
# automatically overridden and replaced with the server timestamp if the
# passive check result timestamp is found by the server to be in the future.
# If not specified, the value will be "1".
#use_client_timestamp=0
```

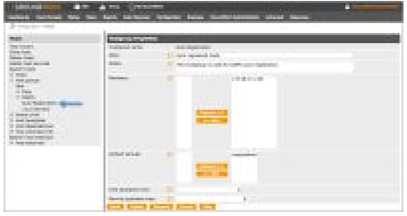
5. **Freshness Checking**
    - The *Check service freshness* option determines whether or not Nagios will periodically check the *freshness* of service results. Historically freshness checking has not been enabled at a global level in the GroundWork Monitor default *Nagios Main Configuration*, and this will suppress freshness checking for GDMA-run services. Enabling this option is useful for ensuring that passive checks are received in a timely manner. A checked value means the freshness checking is enabled. This setting should be verified and enabled on a GDMA target server.
    - To verify/enable freshness checking go to *Configuration* > *Control* > *Nagios main configuration* > *Freshness Check*.



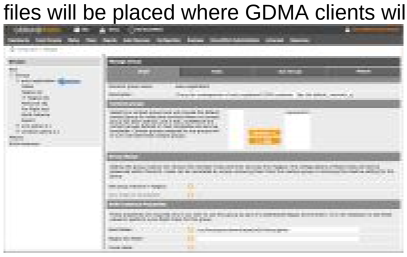
6. **Enable Externals**
    - The configuration for GDMA monitored hosts must have Externals enabled to allow access to all the externals-related screens and options. Depending on the version of GroundWork Monitor you are using this directive may already be enabled.
    - To verify/enable externals go to *Configuration* > *Control* > *Setup* > *Enable externals*.

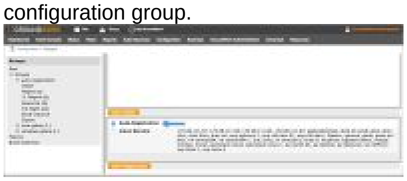
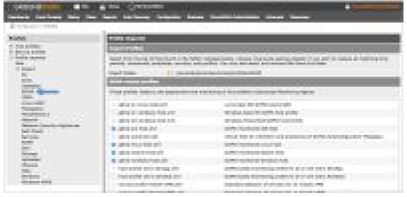
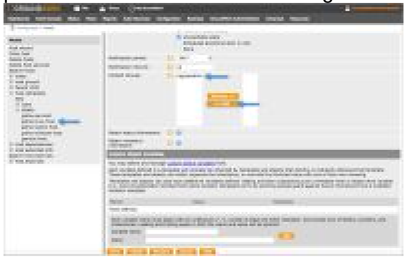


7. **Set up Auto-Registration Host Group**
    - Depending on the version of GroundWork Monitor you are using the *Auto-Registration* host group may already be configured by default.
    - To verify go to *Configuration* > *Hosts* > *Host groups* > *Modify* . If the host group does not yet exist, add a host group named `Auto-Registration` (using the exact character format), under *Configuration* > *Hosts* > *Host groups* > *New*.



8. **Set up auto-registration Monarch Group**
    - Depending on the version of GroundWork Monitor you are using the *auto-registration* host group may already be configured by default.

- To verify go to *Configuration* > *Groups* > *Groups* > *auto-registration* > *Detail*. If the monarch group does not yet exist, add a group named `auto-registration` (using the exact character format), under *Configuration* > *Groups* > *New*. Further down on the same page verify or set the *Build folder* to be `/usr/local/groundwork/apache2/htdocs/gdma` so that the externals files will be placed where GDMA clients will be looking to pick them up.
  

9. **Add Auto-Registration to auto-registration**
   - It is generally recommended that you add the *Auto-Registration* hostgroup to the *auto-registration* Monarch configuration group. This step is not a system default, you should consider making this change.
   - Go to *Configuration* > *Groups* > *Groups* > *auto-registration* > *Detail* > select the *Hosts* tab. Scroll down to *Add Hostgroup(s)*, check and add *Auto-Registration*. This will simplify the actions when new hosts are added, by allowing the individual hosts to be indirectly associated with the Monarch configuration group via the hostgroup, instead of being assigned directly to the Monarch configuration group.
     
10. **Import GDMA host profiles**
    - The host profiles will form the basis for configuring new auto-registered GDMA hosts running the respective operating-system types. You are not required to use these profiles as the GDMA client installer allows you to select an alternate host profile and an optional service profile to be applied on the server to the auto-registered client's configuration.
    - To add new host profiles and related objects, select *Configuration* > *Profiles* > *Profile importer* > *Import*. Choose the *GDMA* category and select the appropriate host-profile files; *gdma-aix-host.xml*, *gdma-linux-host.xml*, *gdma-solaris-host.xml*, *gdma-windows-host.xml,* then click *Import* at the bottom of the screen.
      
11. **Add a default contact group to the host templates**
    - Edit each of the new host templates just imported; *gdma-aix-host.xml*, *gdma-linux-host.xml*, *gdma-solaris-host.xml*, *gdma-windows-host.xml*, and add one or more default contact groups.
    - Navigate to *Configuration* > *Hosts* > *Host Templates* > *Modify*, then select each one of the GDMA host templates listed and establish the basic contact group(s) for hosts using this host template (perhaps just *nagiosadmin* at this point, as a kind of safe default). Save each host template after making this change. The setting here can be overridden later on at other levels, but this provides at least a standard setting for all auto-registered hosts.
      

2.2 Configuring a client server

> ⚠ If upgrading an existing GDMA client server, start with step **1. Uninstall the legacy client**. If this is a new installation, start with step **2. Download the agent**.

1. **Uninstall the legacy client**
   - **For Linux**:
     - Access a command line interface for the Linux GDMA client server, (e.g. PuTTY).
     - Backup any custom plugins in the `/usr/local/groundwork` directory structure, you may have added. You will need to move these to the new location.
     - Next, run the following script to uninstall the agent:

```
        /usr/local/groundwork/uninstall
        ```

        - You will be prompted with the question *Do you want to uninstall GroundWork Distributed Monitoring Agent and all of its modules?*, confirm the uninstall.
        - Remove the `groundwork` sub-directory and all sub-directories:

        ```
        rm -Rf /usr/local/groundwork
        ```

        - On the GroundWork server delete the GDMA client host within the *Auto Registration* host group (*Configuration* > *Hosts* > *Hosts* > *Auto-Registration* > <*hostname*> > *Detail* > *delete*), and run a *Commit* operation (*Configuration* > *Control* > *Commit*).
    - **For Windows**:
        - Access the File Manager for the Windows GDMA client server, (e.g. Start, Computer).
        - Back up any custom plugins in the `C:\Program Files (x86)\groundwork` directory structure, you may have added. You will need to move these to the new location.
        - Next, from the `C:\Program Files (x86)\groundwork` directory, select and run the `uninstall.exe` file. You will be prompted with the question *Do you want to uninstall GroundWork Distributed Monitoring Agent and all of its modules?*, answer *Yes* to uninstall and proceed.
        - Using the File Manager remove the `groundwork` directory all all sub-directories.
        - On the GroundWork server delete the GDMA client host within the *Auto Registration* host group and run a *Commit* operation.
2. **Download the agent**
    - You can download the GDMAs from the GroundWork server at the base URL `http://<groundwork_server>/agents/`. The available packages include Windows GDMA, Linux 32-bit GDMA, Linux 64-bit GDMA, Solaris Intel GDMA, and Solaris SPARC GDMA.
    - Browsing of the above URL is disable by default. To enable browsing of this directory, edit the `httpd.conf` file:

    ```
    vi /usr/local/groundwork/apache2/conf/httpd.conf
    ```

    - Add the following lines:

    ```
    <Directory /usr/local/groundwork/apache2/htdocs/agents>
        Options +Indexes -FollowSymLinks -ExecCGI -Includes
        AllowOverride None
        Order Allow,Deny
        Allow from all
    </Directory>
    ```

    - Save the file and restart apache:

    ```
    service groundwork restart apache
    ```

3. **Install the Agent**
    - **For Linux**:
        - If necessary, relocate the agent to the client server. Make the installer executable (example below, please use the current .run file):

        ```
        chmod +x groundworkagent-2.4.0-80-linux-64-installer.run
        ```

        - Launch the agent (example below, please use the current .run file):

        ```
        ./groundworkagent-2.4.0-80-linux-64-installer.run
        ```

        - Continue with the installation. You will be prompted with a series of questions. Make sure to enter:

```
GDMA requires clock synchronization between this system and the master GroundWork
system. Before installing, ensure that the clock on this system is correct. GDMA
requires network name resolution (DNS) to locate and communicate with the master
GroundWork system. Before installing, ensure that name resolution is functional on
this system.
Continue? [Y/n]: Y
```

Make sure to enter the name of the GroundWork server in place of [\gdma-autohost].

```
Enter the name of the GroundWork server. This can be a resolvable short name, a
fully-qualified domain name, or an IP address. It will be used to download the
configuration for this agent, as well as to send the monitoring results to.
Target Server [gdma-autohost]:
```

```
Please specify the user name to be used by the Agent.
GDMA username [gdma]:
```

```
Please select which protocol will be used for communication with the GroundWork
server.
[1] HTTP
[2] HTTPS: If you choose HTTPS, you will need to manually set up certificates as
well.
Please choose an option [1] :
```

Use the credentials here you added in section 1.0 above.

```
Enter the user name and password to be used for auto-registration of this GDMA
machine. If these credentials are not provided, auto-registration will be disabled
on this machine, and the older auto-configuration protocol will be used instead.
Registration username []: Registration password:
```

```
Enter the host profile and service profile names to be applied to this machine's
monitoring setup during auto-registration. These values are optional; if left
blank, the host profile will be defaulted on the server, and no extra service
profile will be applied.
Host profile name [gdma-linux-host]:
Service profile name []:
```

```
Do you want to start the GDMA service after the installation? [Y/n]:
```

```
Setup is now ready to begin installing GroundWork Distributed Monitoring Agent on
your computer.
Do you want to continue? [Y/n]:
```

- **For Windows**:
    - If necessary, relocate the agent to the client server. Find and run the installer file, e.g. `groundworkagent-2.4.0-82-windows-installer`, on each of your GDMA client machines.
    - Continue with the installation. You will be prompted with a series of questions:

```
GDMA requires clock synchronization between this system and the master GroundWork
system. Before installing, ensure that the clock on this system is correct. GDMA
requires network name resolution (DNS) to locate and communicate with the master
GroundWork system. Before installing, ensure that name resolution is functional on
this system.
Continue? Yes
```

```
Welcome to the GroundWork Distributed Monitoring agent Setup Wizard. Next.
```

```
Installation directory: c:\Program Files (x86)\groundwork. Next.
```

```
Enter the name of the GroundWork server. This can be a resolvable short name, a
fully-qualified domain name, or an IP address. It will be used to download the
configuration for this agent, as well as to send the monitoring results to.
Target Server: e.g. 10.0.10.109. Next.
```

```
Please select which protocol will be used for communication with the GroundWork
server.
HTTP or HTTPS: If you choose HTTPS, you will need to manually set up certificates
as well. Next.
```

```
Enter the user name and password to be used for auto-registration of this GDMA
machine. If these credentials are not provided, auto-registration will be disabled
on this machine, and the older auto-configuration protocol will be used instead.
Registration username: e.g. gdma Registration password: e.g. gdma Re-enter
password: e.g. gdma. Next.
```

```
Enter the host profile and service profile names to be applied to this machine's
monitoring setup during auto-registration. These values are optional; if left
blank, the host profile will be defaulted on the server, and no extra service
profile will be applied.
Host profile name: e.g. gdma-windows-host, Service profile name: <blank>. Next.
```

```
Setup is now ready to begin installing GroundWork Distributed Monitoring Agent on
your computer. Next.
```

4. **Commit**
    - Just like the addition of any other host, you will need to run a *Configuration* > *Control* > *Commit* operation to allow the monitoring engine to recognize the host and see it in Status.
5. **Build Externals**
    - Additionally, since this is an addition of a GDMA host you will need to run a *Configuration* > *Control* > *Build externals* operation so the configuration changes can be picked up by GDMA hosts.