About GDMA

Contents

The page describes use cases, modes of operation, and the application design considerations for GDMAs.

1.0 Introduction

A GDMA consists of memory resident programs that perform monitoring checks on individually configurable time intervals and reports the results to GroundWork Monitor. Configuration files containing program directives, including alarm thresholds and other parameters are periodically downloaded from GroundWork Monitor. The agent performs monitoring checks by supplying necessary arguments to small disk resident programs called plugins and then running them with the supplied options. The plugin set provided for the agent is consistent with the plugins distributed with GroundWork Monitor, as well as useful plugins specific to the operating system of the monitored server, for example, VBS or PowerShell plugins for Windows systems.

GDMAs support multiple modes of operation, including installation and configuration, normal operations, and failure modes. Since GDMAs are designed to operate under the control of GroundWork Monitor, there are corresponding functions and features on the GroundWork system that support each of these operating modes, discussed in more detail below. GDMAs can be employed to monitor the single host on which they are installed (single host mode), or to monitor multiple hosts from a single GDMA installed on a single host which is referred to as the multi-host configuration. Multi-host configuration is used with the Windows GDMA to create the Windows Child server and with any supported operating system to provide economical monitoring on customer premises for the Managed Service Providers (MSPs).

Describing the normal operating mode for a single GDMA monitoring a single monitored server helps to introduce the subject.

1.1 GDMA Data and Control Flow

The GDMA consists of two Perl programs; a Poller and a Spooler, the binary program for Send_NSCA, and two or more configuration files. Also included are between 100 and 200 plugins, and a spool file containing monitoring and error messages which are waiting to be transmitted to GroundWork Monitor.

In normal operation, the Poller program reads the configuration file, calls the plugin, and supplies the required arguments to configure it to collect the required metric. It then executes the plugin as a *check* and writes the results to the Spool File. The Poller then waits until the scheduled time for the next check and repeats the process. Individual checks can be executed each cycle or on a defined multiple of cycles, giving the administrator individual control over each check's schedule.

At defined intervals the Spooler reads the Spool File, calls the Send_NSCA program and transmits one or more of the messages containing monitoring check results to the GroundWork system using the NSCA application protocol. Operation of the Poller, Spooler, and Send_NSCA modules are controlled by parameters contained within the GDMA configuration files.

> ⚠ The default port for NSCA communication is 5667, however, it can be reconfigured to a different port number on both sides of the interface if required.

The configuration file contains a number of error handling and control parameters which are used by the Poller and the Spooler to help ensure the reliable operation of the GDMA, including a subroutine that verifies the validity of the configuration file itself. Error messages are normally written to the Spool file for transmission to the GroundWork system where they can be reviewed and analyzed by system operators using the Event Console application.

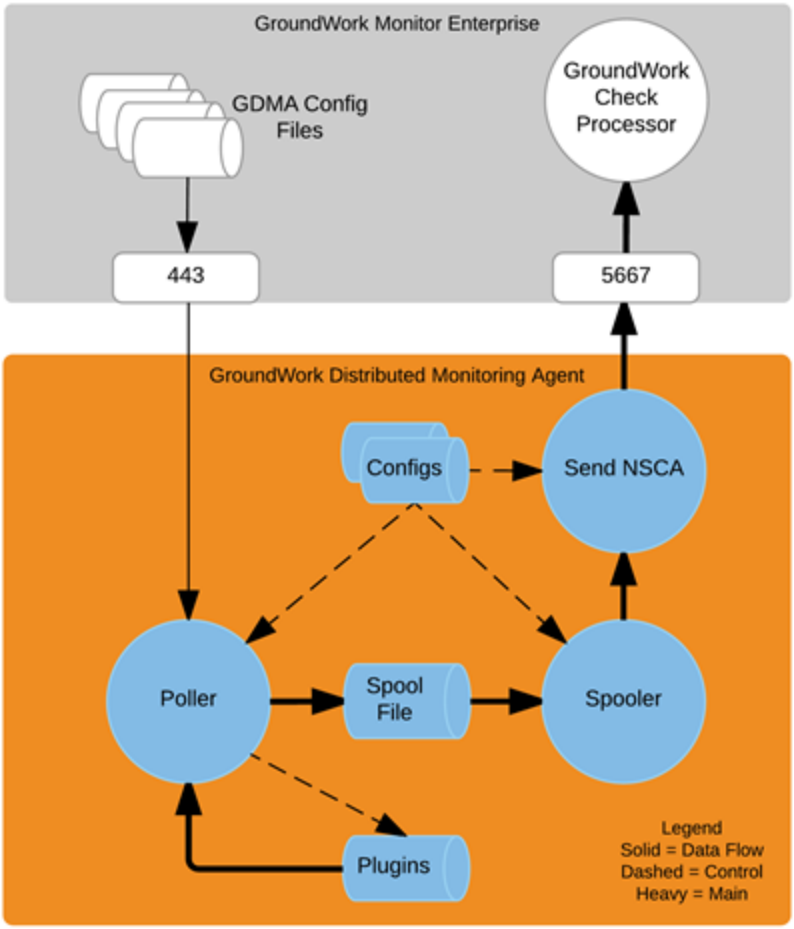
Monitoring results reported to GroundWork Monitor are presented as service check results. Host health checks can be performed actively from GroundWork Monitor if access to the monitored server is permitted. If active access is not permitted, an algorithm is used by the GroundWork server to distinguish between service alarm and host failure. Active checks of host health are preferred where permitted for performance reasons.

Routine maintenance of the GDMA configuration is performed by editing the externals text files within the Monarch subsystem on GroundWork Monitor. Either automatically or as an operator action, the Configuration application updates the externals configuration files in the appropriate directory for retrieval.

At regular intervals defined in the configuration files the Poller initiates an HTTP or HTTP(S) connection and looks up the time stamp of the configuration file stored on GroundWork Monitor. If the file on GroundWork Monitor is more recent that the configuration file on the GDMA, the Poller fetches the GDMA configuration file from GroundWork Monitor and replaces the older file on the GDMA with the most recently updated file.

A single Linux GDMA and GroundWork Monitor, which controls it, is illustrated in the following figure.

Figure: GDMA Data and Control Flow



1.2 About Automated Agent Registration

The combined GroundWork Monitor 6.7.0 and GDMA 2.3.0 and newer releases, contain support for a the GDMA client auto-registration capability. This facility is designed to allow hosts monitored via GDMA to be automatically added to the central server, with very little effort by the administrator. Automated Agent Registration was implemented to reduce the administrator's burden when adding many GDMA-monitored hosts to the monitored infrastructure. Many of the simple tasks are highly automated, allowing the administrator to concentrate more on exceptions and the overall monitoring design.

When Automated Agent Registration is active, each new GDMA client makes an auto-registration request to connect to GroundWork Monitor and receives its marching orders. GroundWork Monitor validates the request, corrects the submitted host attributes if necessary, adds the host to the configuration if it is not already there, builds an externals file containing the details of the monitoring checks the client should run, and finally returns the validated hostname (or error messages) to the client. For more information please refer to Quick Start Auto Registration.

2.0 Use Cases and Application Notes

GDMAs are intended to be used for the following use cases.

- **Cost Effective and Reliable Monitoring Capacity Enhancement** - GroundWork Monitor can be configured to collect monitoring information by active polling or to receive monitoring information passively from external sources. The number of hosts that can be monitored passively is generally an order of magnitude greater than the number that can be monitored by active polling. GDMAs submit monitoring results to the GroundWork system passively, and thus enable significantly larger scale monitoring systems than those based exclusively on active polling.

  A GDMA incorporates automation features to enable distribution and configuration of large numbers of agents with relative ease. In monitoring applications where passive checks can displace active polling in whole or in part, the number of servers performing active polling is substantially reduced or eliminated. This reduces or eliminates the need for redundant polling servers and maximizes overall system reliability by reducing complexity. The cost per monitored node will generally be lower in installations in which most data collection is performed with GDMAs.

Design Engineering Note
Design Engineering Notes provide informal and non-binding guidance that may be useful to customers and partners who are designing monitoring solutions for end user organizations.

Going forward, GroundWork is likely to encourage all of it's customers to make use of GDMAs for all server monitoring regardless of the number of devices. This change will be enabled by slowly converting existing profiles based on SSH and NRPE to GDMA. The reasons for this are the following:

- The loading imposed on the monitored server by the passive agent is not significantly different than that imposed by an active agent or SSH.
- Since the GDMA is the preferred method to achieve the most reliable operation at scale, it is the correct method to start with for organizations that may choose to deploy the system at volume, based either on existing infrastructure scale or that which may be reached in the future. Deploying initially with GDMAs will avoid having to make a transition in order to achieve reliability at scale, and will thus conserve training costs for customers.
- Due to the other use cases involving GDMA, this product is likely to receive more investment in automation of installation, configuration, and routine maintenance and over time will be more flexible and less costly to operate than other data collection methods.
- In the future, the only reason not to begin GroundWork Monitor deployments with GDMA is that the GroundWork deployment is succeeding a successful Nagios deployment in which Nagios active agents and plugins are in use with acceptable results. In this case, the avoidance of additional agent deployment at least in early phases of deployment provides attractive avoidance of risk.

- **Internal Security Zoning** - Network security policies often prohibit communication needed to employ active polling methods for certain security zones. Some of the specific examples where this requirement is encountered are bulleted below. The ability of the GDMA/GroundWork Monitor combination to be configured so that all necessary communications are initiated from the GDMA supports the use of GDMA in all security zones separated by firewall policies from the GroundWork system.

  Application Engineering Note
  This use case requires GDMA to be deployed in environments where bi-directional communication between GroundWork Monitor and the monitored server is not possible. In these environments standard *Host Alive* check methods are replaced with algorithmic checks of available service state information for each host. Contact GroundWork Support for more information on the required host check.

  - A DMZ
  - Domains containing servers managing clinical trials information
  - Domains containing database servers when the GroundWork server cannot be placed in the database server zone
  - A customer premise for a Managed Service Provider (MSP) which is separated from the MSP by the customer's firewall
- **Agentless Windows Server Monitoring** - The multi-host configuration of the Windows GDMA can be configured to perform active polling for Windows servers within the same Active Directory domain. This configuration uses plugs that run PowerShell and VBScript, and access PerfMon and WMI information on the monitored Windows servers. This avoids installation of individual agents on the monitored Windows servers, with the exception of the system on which the Windows multi-host GDMA is installed.
- **Cloud Computing Environments** - The unique requirements for monitoring in private and public cloud environments create additional requirements for distributed agents.
  - The use of GDMA distributes most of the workload for the monitoring function onto the servers that are being monitored, which means that monitoring capacity is much more self-contained and linear with regard to the number of cloud-based servers being monitored. This makes the monitoring system itself much more scalable and flexible without the need to plan for additional polling capacity.
  - When additional monitored servers are added to the cloud, GroundWork Monitor can query the cloud Application Programming Interface (API) to determine which image has been loaded on the virtual device. The corresponding monitoring profile can be selected and assigned. The use of GDMA simplifies this use case, since the configuration file can be automatically generated and made available to the GDMA poller on its next request for an update. This process is logged and can trigger instantiation of the updated configuration as needed.

3.0 Definitions and Abbreviations

The following definitions and abbreviations of commonly used terms are provided for standardization and reference.

- **GroundWork Monitor Enterprise Edition** is the standard GroundWork enterprise monitoring product which hosts the monitoring configurations and collects and presents the resulting availability and performance information. GroundWork Monitor refers to the top level GroundWork monitoring system, including the hardware that it runs on. The word *server* or *system* would normally not be added to the name. In a system containing GroundWork Child servers, it is understood that GroundWork Monitor includes the term *parent server*.
- **GroundWork Standby Notification server** or **Standby server** is a special configuration of the GroundWork Monitor product software which provides continuity of notifications in the event that GroundWork Monitor becomes unavailable. This term is not normally abbreviated, so for convenience this product may be referred to as *Standby server* provided that this usage occurs in the document after this definition or after first use of the complete term. The Standby server monitors GroundWork Monitor as a hot standby which is to say that it receives and processes all of the monitoring information received or processed by GroundWork Monitor, except that its notification process is continually reset to disabled by a process that verifies that GroundWork Monitor is functioning. Thus at any time that GroundWork Monitor becomes unavailable, notifications are immediately begun by the Standby server. A Standby server is designed to

provide continuity for notifications of outages during the period of time required to restore GroundWork Monitor to service. It is not a High Availability system nor is it designed to take over the monitoring configuration control functions of GroundWork Monitor during a GroundWork Monitor outage. For information about High Availability options for GroundWork Monitor, please contact GroundWork Sales.

- **GroundWork Linux Child server** or simply **Linux Child**, is a special configuration of GroundWork Monitor software which provides added capacity for performing active monitoring checks. In typical installations, one or more Linux Child servers receive configuration updates from GroundWork Monitor and report monitoring results to GroundWork Monitor and also to a Standby Notification server if one is installed. Traps, logs, and GDMA monitoring results are not normally directed to Linux Child servers and database updates, user interfaces, and notifications are not normally enabled on Linux Child servers.
- **GroundWork Distributed Monitoring Agent (GDMA)** consists of memory resident programs installed on client servers to be monitored that perform monitoring checks on individually configurable time intervals and report the results to GroundWork Monitor.
- **GroundWork Windows Child server** is a special multi-host configuration of the Windows GroundWork Distributed Monitoring Agent (GDMA) which provides added capacity for performing active monitoring checks of multiple Windows servers. In typical installations, one or more Windows Child servers receive configuration updates from GroundWork Monitor and report monitoring results to GroundWork Monitor and also to a Standby Notification server if one is installed.
- **GroundWork Network Management Suite (NMS)** is a combination of several open source modules which may be optionally added to GroundWork Monitor to extend the functionality for network monitoring and management. The GroundWork NMS can be co-hosted on the same server as GroundWork Monitor or distributed to one or more servers dedicated to this use.
- **Monitored Hos**t is a server, router, switch, load balancer, fire wall, storage device, or application which is being monitored for availability and performance by GroundWork Monitor. This is distinguished from a monitoring host which is GroundWork Monitor, Standby server, Child server, or GroundWork NMS server.
- **Plugins** are programs, normally invoked at the command line or by an agent like GDMA, which collect monitoring information such as CPU, swap, or disk utilization, lists of running processes, table space extents, etc., and return the results in a defined format. The results include whether the test exceeds either a warning or critical threshold value associated with the particular check, as well as any performance data collected, thus plugins return both state and metrics.
- A **Managed Service Provider (MSP)** provides delivery and management of network-based services, applications, and equipment to enterprises, residences, or other service providers. MSPs serve as outsourcing agents for companies looking to reduce IT operations costs.
- **Target System** is the title of one of the configuration directives in the GDMA which refers to the names or IP addresses to which the spooler is to transmit the spool file contents. We will not use this term in standard GroundWork product documentation to avoid confusion with common informal usage which refers to the system being monitored as a target system. Instead we will refer to the system to which results are sent from a GDMA as GroundWork Monitor and the Standby Notification server.

4.0 Description of GDMA Modes of Operation

GDMAs have been designed with modes of operation for installation, auto configuration, configuration maintenance, normal operation, and continued operation in failure modes. The following provides an overview of the major options available for each of these operating modes for the product.

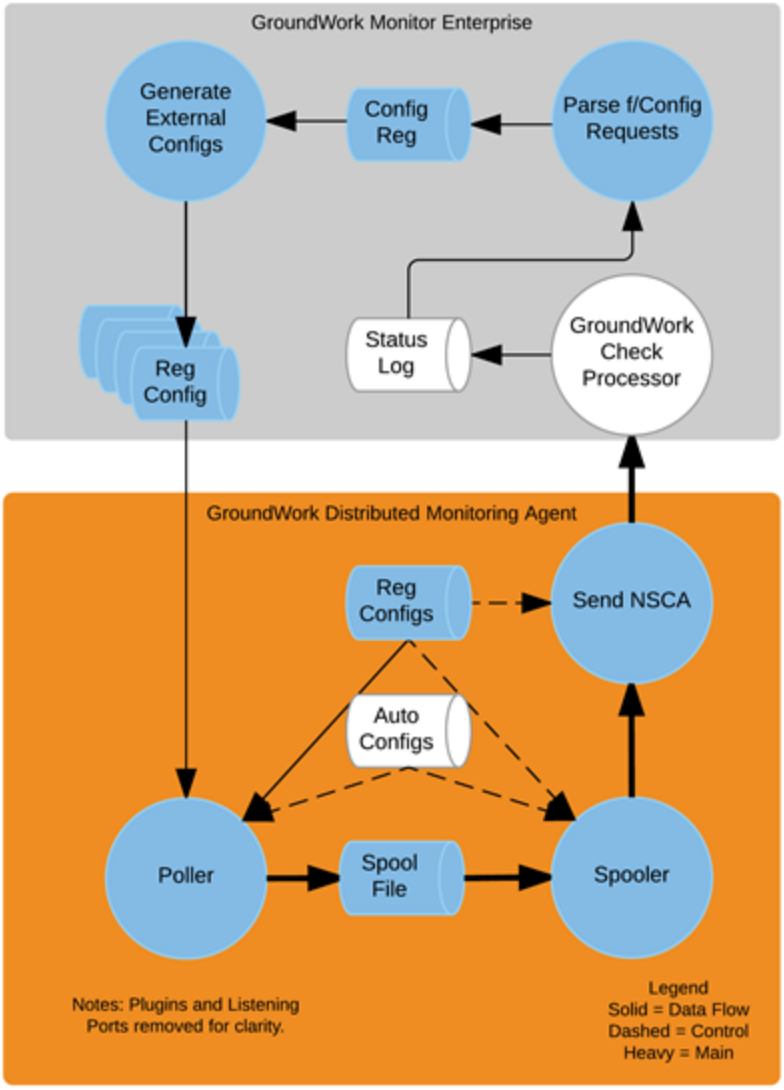
- **Installation Modes** - GDMAs can be installed on the server on which they are to run in several different ways, depending on plant conditions, life cycle point, and other circumstances. Regardless of the specific method, the Linux GDMA and its attendant files will be installed in a `usr/local/groundwork` directory that is created by the GDMA installer. Solaris and AIX will use `/opt/groundwork`, and the Windows GDMA will be installed in a directory determined by the Windows distribution and architecture. In English versions of 32-bit MS Windows this is `C:\Program Files`, and in 64-bit MS Windows it is `C:\Program Files (x86)`. This default may be different in different language distributions of Windows, and in the Windows case may be over-ridden by a user-supplied directory at install time.

  
  Linux, Solaris, and AIX versions of the GDMA cannot be installed in user-supplied directories.

  - One installation mode is to simply install the GDMA environment as part of a server installation image. Thus each time the server operating system and applications are installed, the GDMA and its attendant files are installed along with it. The installer would normally be configured for unattended operation in this case.
  - A second possible installation method is to package the GDMAs as required by the customer's software configuration management and patch distribution system. The GDMA is packaged in a binary installer, which is easily wrapped using a number of possible software distribution utilities (Puppet, CFEngine, etc). The installer would normally be configured for unattended operation in this case.
  - A third GDMA installation mode is to simply log in to the monitored host and download the GDMA installer specific to the server's operating system from GroundWork Monitor and proceed as with any other GroundWork software installation using the standard product installer. This process can be configured for either attended or unattended operation.

- **Auto Configuration Mode** - Multi-host configurations, including Windows Child server configurations, cannot use this mode. Auto configuration mode is recommended for the creation of initial configurations for all GDMA installations with a single agent monitoring a single host. For this mode the GDMA is initially deployed with a special auto configuration file instead of a standard configuration file. The following figure illustrates the data flow for auto configuration on both the GDMA and GroundWork Monitor.

  Figure: Auto Configuration Process Flow



Upon initialization of the Poller, the GDMA reads basic configuration directives from the auto configuration file, and then attempts to use these to find a normal configuration file. If this file is not present, and cannot be obtained, it continues in auto-mode.

Based on the auto configuration directives, the Poller determines the host name and the OS of the system it has been installed on and writes an auto registration message in the format of a standard service check result to the Spool File. The Spooler reads the message and under the control of directives contained in the auto configuration file and communicates the message to GroundWork Monitor as a result for a special automation host.

The delivery address of GroundWork Monitor in the auto configuration file is normally given as a name, rather than an address, so that DNS or an equivalent naming service is relied upon to provide the address. To use this feature, the administrator must create the corresponding naming service entry for GroundWork Monitor prior to first use of the auto configuration mode by GDMAs. The default name is `gdma-autohost`, though this is configurable at installation time. Alternatively, the administrator can place the IP address of GroundWork Monitor in the auto config file at install.

In this way the Poller's auto registration message is delivered by the Send_NSCA program to GroundWork Monitor as shown above. The arriving message from the GDMA is delivered to a monitoring service for a host named `gdma-autohost`. All such messages from GDMAs are delivered to the same host-service and written, like all other service check results to the Nagios Log.

> ⚠ There are normally no thresholds associated with this service and thus no alarms will result from this process.

Periodically, as scheduled by cron, a program reads the Nagios Status Log and writes all of the auto registration messages to a separate Configuration Request Log file. A second program scheduled by cron reads this file, and generates the regular configuration files (externals) that are appropriate to the operating system of the monitored host containing the GDMA. It also adds the GDMA hosts to the Monarch configuration database and associates the hosts with standard profiles based on the operating systems reported in the request

configuration message. The generated configuration files are placed into the distribution directory on GroundWork Monitor corresponding to the file path name which was placed in the GDMA auto configuration file. This permits the Poller to download its regular configuration file.

> ⚠ GDMA configuration files are also referred to as External files.

When the Poller cycle begins again, it downloads the regular configuration file, and uses it as the source of all program directives. The auto-configuration file is still read first, and defaults not overwritten in the regular configuration file are used. Thus, the monitoring checks called for in the regular configuration file begin to be made and written to the spool file for communication to GroundWork Monitor.

The final step in the auto configuration process is to run a Commit from the Configuration system which instantiates the self registered hosts to the GroundWork Nagios instance, the GroundWork Foundation databases, and to the user interface and notification processes. When this is complete the new self-registered hosts will be properly reflected in the user interface. When service freshness and host health checks are properly configured, the new hosts will be in full monitoring operation. The choice of host check used depends upon whether GroundWork Monitor can access the monitored host with ICMP, based upon existing security policies as discussed previously.

The following steps must be taken to enable the auto-configuration mode prior to GDMA deployment.

> **Application Notes**
> Clearly, auto configuration is a powerful technique that many GroundWork users will make use of for getting started with GDMA. There are some use cases involving embedded systems, the configuration of multi-host mode, etc. where it may be useful to pre-configure a complete configuration file prior to deploying the agent, and thus avoid the use of auto configuration. GroundWork Professional Services are available for consultation on such special cases. If the GroundWork/GDMA administrator doesn't have immediate access to make changes on DNS or other naming service, the GroundWork server address can be specified to the GDMA at install time, so that the spooler can properly communicate with the GroundWork system. The GDMA Quick Start contains procedural guidance on the installation and initial configuration of GDMAs and the GroundWork Monitor systems which control them. After the initial configuration of the GDMA, more complex monitoring profiles can be added by creating new external configuration files for additional services.

1. GroundWork Monitor server address and name must be added to DNS or other naming service (or the address specified to the GDMA at installation time)
2. Auto configuration host and service and its standard profile configured on GroundWork Monitor using the Configuration interface
3. Externals enabled on the configuration control menu
4. GroundWork configuration groups corresponding to Windows and Non-Windows GDMA need to be configured in order to permit externals configuration files to be generated upon request
5. GDMA related profiles must be loaded, or equivalent profiles created and referenced in the auto-configuration scripts

- **Configuration Maintenance Mode** - After initial configuration is completed with auto configuration, the GroundWork Administrator uses Configuration as usual, to update thresholds, add and delete service checks, assign and change host group assignments, etc. Optionally, each time a Commit and Build Externals is performed, the externals files will be renewed and made available to the GDMA poller when it requests them. No specific consideration must be made for the fact that the checks are being made by GDMA as opposed to any other method, except that text content of the externals files must be edited to affect configuration changes on GDMA monitored hosts and services, rather than using the nominal configuration screens.

  Agent and plugin updates currently require that the agent be uninstalled using the script that is supplied and installed with the agent and the new version of the agent installed using one of the available installation modes.

  > **Application Engineering Notes**
  > The plugins that are loaded onto the monitored system are a superset of the plugins needed to implement any particular coverage profile. Thus the addition of plugins is not frequently required after the initial load except for new plugins that may be written by GroundWork customers. GroundWork Monitor can host a set of plugins for download by architecture, allowing maintenance of existing plugins, and the addition of user-supplied plugins to multiple GDMAs.

- **Normal Operation Mode** - Normal operation of GDMAs is described in the first section of this document. To supplement that description, the following additions are made:
  - The GDMA can be configured to send its spool file contents to more than one GroundWork Monitor. The most common example is GroundWork Monitor and a Standby server.
  - When a GDMA is installed as a Windows Child server or a multi-host GDMA, the monitoring results are delivered to GroundWork Monitor addressed for the correct host/service. In this configuration, there will be a regular configuration file installed on the GDMA corresponding to each of the hosts that the GDMA is monitoring. Installation and configuration of Windows Child server is provided via a professional services engagement.

- **Failure Modes** - GDMAs are designed to be fault tolerant in the face of the following assumed modes of failure:
  - **Corruption of a ConfigurationFile** - The GDMA enters auto configuration mode when the regular configuration file is found to be corrupt. If the configuration file is present and is valid, but the new configuration file is not available due to a connection failure or it's having been removed or restricted on GroundWork Monitor, it keeps on executing in normal mode with the previously read valid configuration for a configurable period (default is 3 days).

- **Plugin Execution Error** - This failure is reported in the service check result as an unknown condition, indicating configuration error.
- **Plugin Time Out** - This is reported in the service check result as defined by the plugin, typically a critical condition.
- **Loss of Connectivity** - Temporary loss of connectivity to GroundWork Monitor is dealt with by spooling results on the monitored host. The default spooling period is 15 minutes, and can be adjusted.
- **Troubleshooting Modes** - These are supported through the use of command-line switches on the GDMA programs, as well as optional logging levels.
- **Crash or Halt of GDMA** - A crash or halt of any of the GDMA programs will be detected through host freshness checks running on GroundWork Monitor.

5.0 GDMA Profiles

- For GroundWork Distributed Monitoring Agent (GDMA) Profiles reference see *GroundWork Monitor* > *GroundWork Monitor Profiles* > *About Profiles*.