Datagram Consulting
Östermalmsgatan 21, 114 26 Stockholm, Sweden
Tel +46 8 544 952 00
www.datagram.se

Datagram

Datagram SyslogAgent manual

Version 3.6

April 2011

Table of contents:

Introduction

Welcome to the Manual and Installation Guide for Datagram SyslogAgent.

Here you will find a detailed installation procedure as well as full descriptions of the configuration alternatives. If you miss any information in this file please inform us (info@syslogserver.com). You can also read the FAQ at www.syslogserver.com.

Customers can always contact us at support@syslogserver.com.

What is SyslogAgent?

The Datagram SyslogAgent is installed as a service on Microsoft Windows clients and servers to provide syslog compatability. The entries in the Event log are sent to the central Syslogserver. Application logging is also supported.

Background

The SyslogAgent is based on NTSyslog by SaberNet.net, who released it under the GNU license. The Control program, NTSyslogCtrl, was written by Didier Liroulet. The programs has been modified and extended in several ways:

- Application logging
- Major speed improvement (Several orders of magnitude)
- Reduction in number of SID lookup queries to domain server
- TCP delivery possible
- Ping server prior to send option
- Character parsing differences
- and more...

As the GNU license dictates, Datagram SyslogAgent and SyslogAgentConfig are also released under the GNU license.

Installation

Prerequisites

Datagram SyslogAgent runs on any Windows platform from Windows 2000 onward. Microsoft NT support has been terminated. Even older Microsoft operating systems (Windows 95/98/Me) can not be supported as they are not logging operating systems.

No other prerequisites exist.

Installation alternatives

Three installation alternatives exist for the installation of the Datagram SyslogAgent.

- GUI installation
- Command prompt installation

These alternatives will be described in greater detail in the following pages.

GUI Installation

Extract the zip file in a local catalog of your choice. Create a shortcut if you wish, to the configuration program.

Next execute the *SyslogAgent Configuration* program. By pressing *Install* the Windows service is installed. Before the service can be started, a destination address for the syslog messages must be configured. See the Configuration chapter for further information. Once entered, the service can be started.

Default settings for logging levels are saved to the registry at first start. A registry file is available for download, in case you want to prepare a domain installation via group policy.

Command prompt installation

This alternative installs the service, but not the configuration program. Installation is done by copying the service executable (SyslogAgent.exe) and then execute a local command. This will install the

service with suitable configuration. This installation option could be suitable for batch installations.

Copy the service executable (SyslogAgent.exe) to the local hard drive of the destination computer (non local hard drive will cause errors, as service programs must be local).

Execute a command prompt command with the install option and the destination IP address for the Syslog messages:

```
> Syslogagent.exe –install 192.168.0.100
```

The service *Syslog Agent* is installed and configured. It is configured to start at boot time. Default settings for logging levels are saved to the registry.

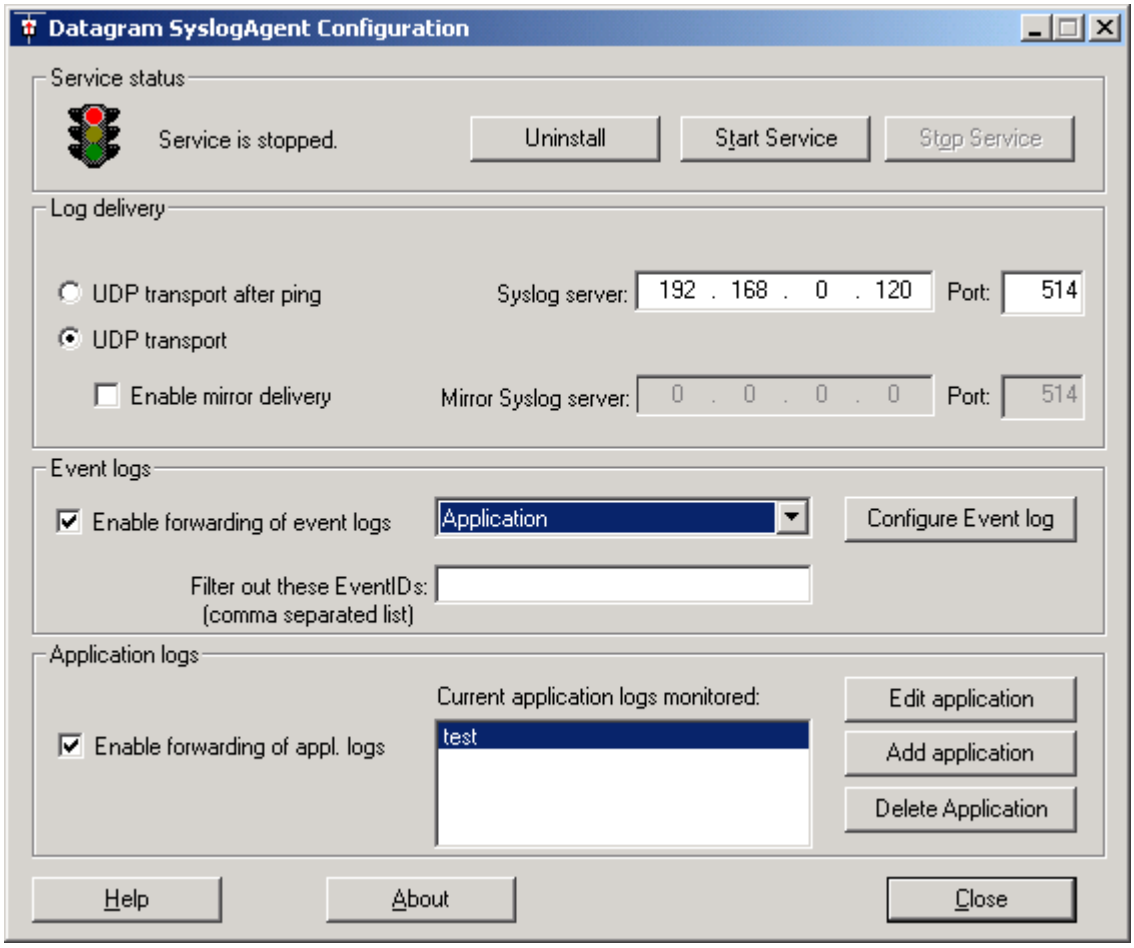
The service can now be started with the command:

```
> net start "Syslog Agent"
```

Basic configuration

Once the service has been installed the configuration options become available. Four separate areas exist:

Service status
Log Delivery
Event logs
Application logs



Service status

With the controls, the service can be started/stopped/uninstalled/installed.

The service is started automatically at system startup, provided a Syslog Server address has been entered, and no other major errors occurs, such as failing to read the settings from the registry.

Log Delivery

At least the primary syslog server address must be entered in the *Syslog Server* dialog before the service can be started. This is done from the *Syslog Servers* settings.

Two delivery modes are available:

UDP delivery

This is the standard way of sending logs - using 'best-effort' UDP protocol. If a secondary syslog server is configured, logs are sent to *both* addresses.

Separate ports can be configured for the primary and mirror server. Default is 514 (UDP).

UDP with Ping Delivery

With this option, the Syslogserver will first be pinged before any logs are sent. As long as the Event log is not cleared before contact can be restored, no information will be lost. The same is not neccessarary true for Application Logs - depending on how the particular application handles the log files.

The server will be pinged every 20 seconds while connection is successful. When ping is unsuccessful, the Agent will eventually slow down to attempt a ping every minute.

Event logs

Enable forwarading of event logs

By default, syslog entries are forwarded to the syslog server. If only application logging is desired, event forwarding can be disabled.

The Syslog agent is preconfigured regarding classification of different types of entries. These settings can be modified by choosing an event log and pressing the 'Configure event log' button. Please see advanced configuration for detailed description of registry settings.

Filter out EventIDs

In certain cases, it can be desireable to filter out certain Event ID's. SyslogAgent supports this by entering the Event ID's to be filtered out in a comma separated list. A maximum of 30 Event ID's can be specified. For instance:

562,565,4132,566,836,837

Application logs

By default, no application logging is configured. To enable application log forwarding, check the 'Enable forwarding of application logs' button.

Any number of application logs can be monitored. After a configuration change of application logs , the service must be restarted in order for the settings to take effect. For every new log to be monitored, a thread is added to SyslogAgent's process. Every few seconds, new entries are checked for, and sent to the Syslogserver.

See the chapter for configuration of application logs for more details.

Advanced configuration

Referenses to locations in the registry assumes that a 32bit SyslogAgent is used on 32bit systems, and 64bit versions on 64bit systems. A 32bit SyslogAgent can be used on a 64bit system, but Windows then (automatically) redirects registry location to Wow6432Node sub structure.

Poll interval

By default, SyslogAgent polls the Event Logs every 2 seconds. This can be modified to a higher value in order to save CPU time, even if the effect is small.

In the key HKEY_LOCAL_MACHINE\SOFTWARE\Datagram\SyslogAgent define a REG_DWORD called EventLogPollInterval. Set the desired value in seconds.

AccountLookup

The single most expensive system call in SyslogAgent is the Account lookup, in which a SID is translated to user name and domain membership. It first asks the local lsass process for local accounts, and if failed asks a domain server if available.

In order to reduce this load, SyslogAgent caches the latest 50 SID:s in a rotation fashion for a limited period of time. If this still is considered a too high load on the server or on the domain server, this feature can be totally disabled. In such a case, user and domain information would not at all be sent to the Syslog server.

In the key HKEY_LOCAL_MACHINE\SOFTWARE\Datagram\SyslogAgent define a REG_DWORD called LookupAccountSID. Set the value to zero to inaktivate account lookup.

By default, account lookup is active.

Character replacement (CR, LF, tab)

Many messages Windows contains carrige return (CR) and line feed(LF) characters. SyslogAgent by default removes line feeds and replaces line feed with ascii 127, in order to avoid parsing issues. The SyslogView application parses the ascii 127 as an enter and presents it as such to the user. Tab characters are generally preserved, in order to help table presentation and indentation in SyslogView.

If SyslogAgent is not intended to be used with the SyslogView application, this behaviour might be unwanted. It is therefore possible to choose which characters to use for replacement of these characters.

In the key HKEY_LOCAL_MACHINE\SOFTWARE\Datagram\SyslogAgent define a REG_DWORD called CarrigeReturnReplacementCharInASCII and/or LineFeedReplacementCharInASCII and/or TabReplacementCharInASCII.

Set the value to the desired ascii value. Default is 127 (decimal) for Carrige Return and 0 (zero) for Line Feed, which means to just remove the character. For tab default value is unchanged 9 (decimal). Setting decimal value 32 means a space character.

In version 3.1.1 parts of this feature was introduced. However, there were terminology issues in that version, resulting in that the registry settings for that version is incompatible with later version regarding these two registry values (CarrigeReturnReplacementCharInASCII in 3.1.1 actually affected Line Feed).

Sessings in the registry

All settings can be found in the registry, and therefore be exported to a .reg file. This way the settings can be pushed out via a group policy, scripts etc. **Please observe** that in such an export the key 'LastRun' should be deleted before copied to another computer - it's the key that helps each computer to know which entries has already been sent. Not deleting this field can cause computers to not send syslog entries! A template registry file can be found in the download section at http://www.syslogserver.com.

The settings are stored in keys in the registry at

HKEY_LOCAL_MACHINE\SOFTWARE\Datagram\SyslogAgent

in the number format described in RFC 3164, the BSD Syslog Protocol. The keys *Application*, *Security* and *System* (and others, if they exist) can be exported and imported if a configuration change is be be made in a larger installation. Do *not* export the value LastRun in

HKEY_LOCAL_MACHINE\SOFTWARE\Datagram\SyslogAgent

as it contains computer unique status information about sent logs.

For more information about the Syslog Protocol please read the RFC 3164, also found on our web site.

Datagram

Application log configuration

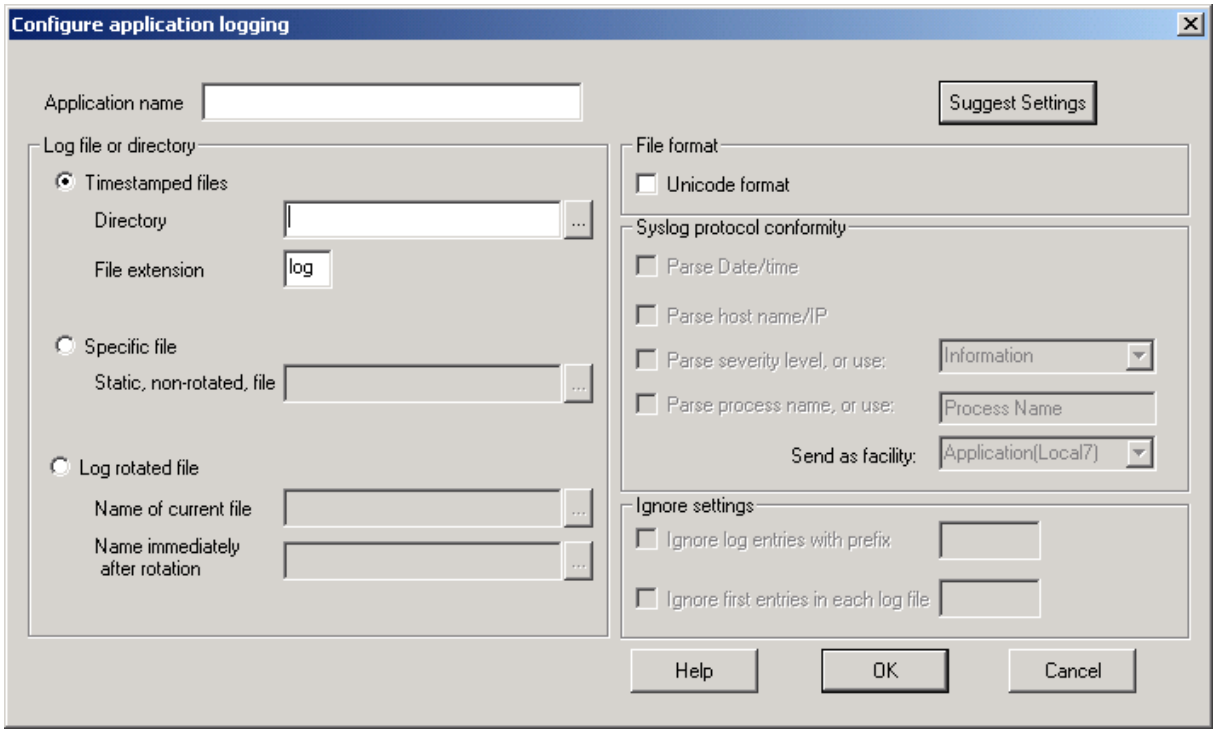
Introduction

Datagram SyslogAgent supports forwarding of application logs to Syslogserver. Any application which produces text based, one log entry per row, logs is suitable.

Choose button 'Add application' to start configuring for an application logging, and enter an application name. This name will not appear in the Syslog messages, it's only used in the SyslogAgent interface.

Configuration consists of four parts:

- Log file definition
- Suggest settings
- Protocol conformity
- Ignore entries settings



Log file definition

Specify where the log files are.

Three main options are available; Time stamped files, Specific file, or Rotated file.

Time stamped files

If log files are created with new (unique) names, choose the directory where the logs can be found, and which file extension they have (usually .log). The log files does not need to contain time information in the file name, as the OS timestamp on the files are used. Microsoft IIS, for instance, is suitable for this setting. For this setting to work, the chosen directory should only have logs written to it by a single application. Multiple, concurrent, log files (with the same extension as specified) causes errors.

The extension information can be with, and without, an initial period; "log" and ".log" is treated the same.

When a newer file is identified, which is within seconds of file creation, SyslogAgent switches to the new log file. Any last entries in the old file are first read and sent.

Specific file

If the log file instead has a static name, enter the full name here.

Log rotated file

If the log files are rotated in a unix-inspirered fashion, the log files are typically numbered, with a higher number indicating an older file (logfile, logfile.1, logfile.2 etc). In this mode, the first generation and second generation file is specified. Directly after file rotation, the SyslogAgent reads any potential remaining log entries (from the file which is now the second generation), and then continues to inspect the first generation log file.

SyslogAgent opens the log files in read mode only, but still prevents file rotation during the time it's open. Therefore, the file is only opened during reading, and then closed for 5 seconds. Upon reopening SyslogAgent tries to read new entries from where it stopped last time. This mode is uncommon in the Windows world, and should be concidered somewhat experimental in SyslogAgent. If the application does not handle a potential failure to change the file name, this logging method may actually cause problems.

Suggest settings

The Suggest Settings button activates a settings wizard to help you with the details of configuration.

After having entered the left-hand side information, regarding log file or directory, the settings wizard question appears automatically. It can also be activated by the button.

The test reads the log file, and tries to identify which fields are available. This is performed in several steps:

- Identify possible prefix for comments. If the first line starts with a non-standard chatacter, it is assumed to be a comment character.
- Search for #Fields: header information, which Microsoft uses in many products, such as IIS, FTP, Exchange etc. If such a field is identified, SyslogAgent uses the information. Since a configuration change in such a product causes a new #Fields: line to be entered into the log file, SyslogAgent searches through the entire log file for the latest possible #Fields: line.
- Reads the first non-commented line, and uses the same engine as the SyslogAgent service to identify which fields can be found.

The result is used to change the right-hand side settings. The result is also presented in a pop-up windows. Any changes can be manually changed by the user. The Suggest settings button can also be used at any time if the log format has changed. Any earlier right-hand side configuration is then lost.

Users are welcome to submit information of other header types. Please submit entire log files and description of the application.

Protocol conformity

Specify which syslog fields that are to be looked for in the log entries.

If no boxes are checked, the SyslogAgent will

- add host information
- add date and time information
- Use the severity, facility, and process name specified in the application logs interface.
- Send the entire read line as the message part of the syslog message

If the configuration says that a certain field will exist in the logs, but is not found, the SyslogAgent will add such information, where possible, by itself. Please note that the process name can be badly chosen if the SyslogAgent fails to find the configured fields.

Parse Data/Time

If checked, both date and time is expeced to exist, and will be used. The date/time information will therefore not appear in the message part of the syslog entry, but in the time field. The Suggest button will report if only one of the two fields is identified. In such a case, the log information is used and completed by SyslogAgent.

The #Field codes used are date and time.

Parse host name/IP

If checked, the own host name or own IP address is expeced to exist, and will be used. The host information will therefore not appear in the message part of the syslog entry, but in the host field.

The #Fields s-computername and s-ip are used. s-computername has higher priority.

Parse Severity level

If checked, SyslogAgent expects the #Fields header to exist, in order to identify the Severity level. If not checked, the explicitly entered severity level will always be used.

The #Fields sc-status and sc-win32-status is used. A sc-status higher the 3xx is parsed as en error. If sc-win32-status is not zero, it is parsed as an error.

Parse Process name

If checked, the process name is expected to exist, in accordance with RFC 3164. If not checked, the explicitly entered process name will always be used.

The #Fields s-sitename is used.

Send as facility:

This field is a static choice, based on application type. Facility information can not be found in application logs, but is rather a choice for the administrator. A default of Local6 is used, so that application logs can easily be separated from operation system logs. Grouping equipment in different facilities is a great way to use the Syslog protocol, as better filtering can be used.

Ignore entries settings

Application log files sometimes has a static header that should not be sent to the Syslogserver. With these options, this can be handled.

Ignore log entries with prefix

This setting checks if the first character is the same as entered in the interface, for instance a '#'. If it is the same, the line is ignored. The suggest button functionality looks for a comment character which is not a-z,A-Z, 0-9 or a space character.

Ignore first entries in each log file

This setting ignores the specified number of initial lines in each log file.