LogZilla Syslog Agent for Windows

Introduction

LZ Syslog Agent is a Windows service that sends Windows event log messages to a syslog server. Syslog is a widely used protocol of event notification and LZ Syslog Agent allows Windows machines to be part of this environment.

Features

This program supports the following:

- Simple configuration and ease of use.
- UDP and TCP transport on IPV4 and IPV6.
- Syslog protocols RFC3164 and RFC5424.

History

Parts of this Syslog Agent are based the Datagram Syslog Agent, which in turn was based on SaberNet's NTSyslog. The bulk of the work is Copyright © 2021 by Logzilla Corporation.

Installation

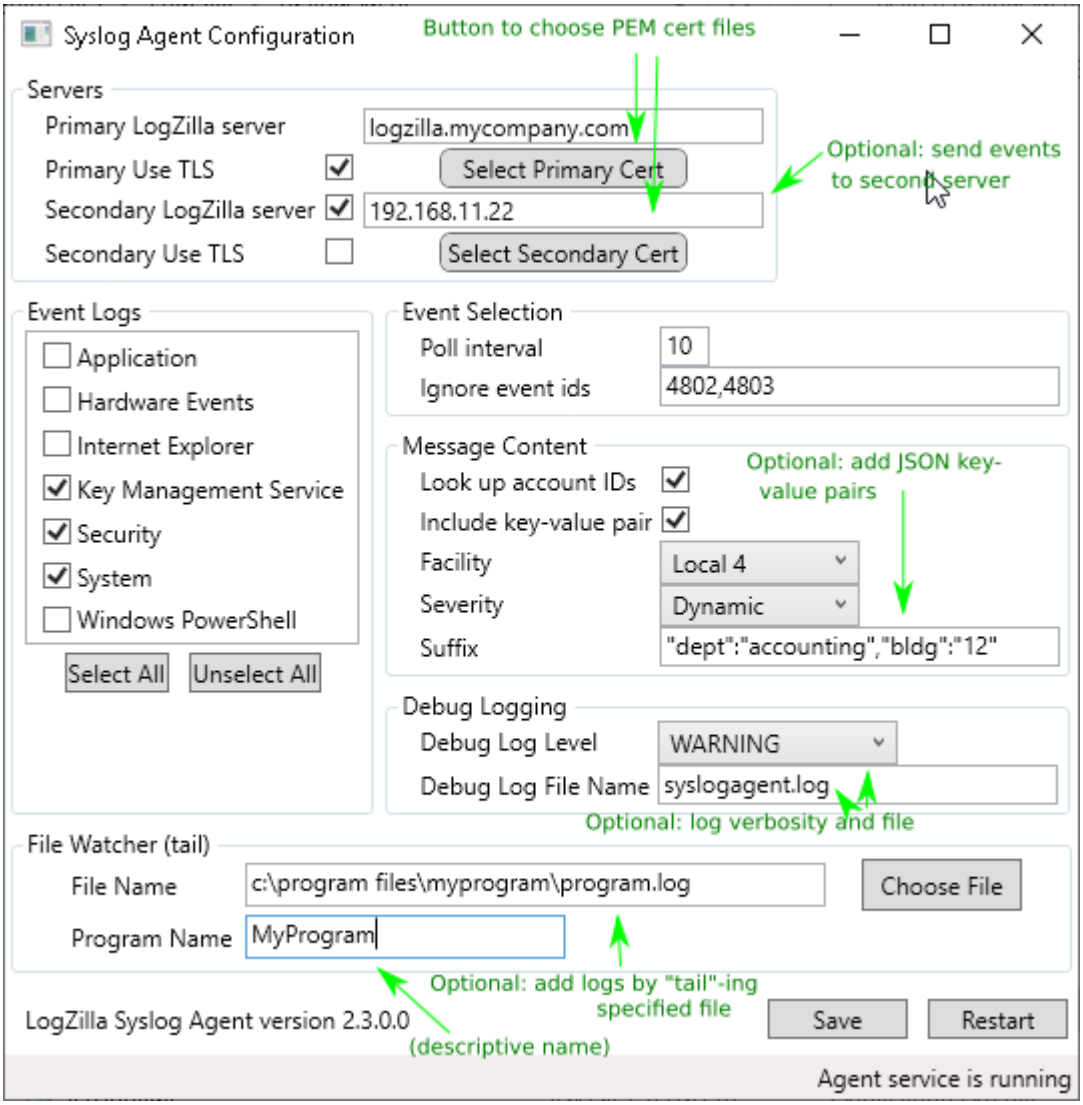
The LZ Syslog Agent programs are installed by executing the `LogZilla_SyslogAgent_2.3.1.0.msi` file.

Prerequisites

The LZ Syslog Agent configuration program, SyslogAgentConfig.exe, requires .NET Framework 4.6.2 or later. The LZ Syslog Agent service, SyslogAgent.exe, has no prerequisites.

Configuration

The operation of the LZ Syslog Agent service is controlled by registry settings. These can be maintained with the LZ Syslog Agent configuration program, SyslogAgentConfig.exe. This program always runs as administrator.



Servers

The address and port for the primary Syslog server, and optionally for a secondary server can be entered. The address can be either a host name or an IP address.

Secondary LogZilla server

There is an option to send messages to a secondary LogZilla server. If selected, every message successfully sent to the primary server will also be sent to the secondary server.

Primary / Secondary Use TLS

There is an option to use TLS to send messages to one or both LogZilla servers. If selected, every message sent to the primary or secondary server will use a TLS communications link.

Select Primary / Secondary Cert

These buttons are used to select (PEM format) certificate files for the TLS communications to the primary or secondary server. When the button is clicked a window will pop up allowing selection of the file from which the cert is to be read. Please note that once the cert is read and imported (using the button) that certificate information is copied into the LogZilla settings and the source cert file is no longer used. If desired the cert information that LogZilla uses can be directly edited in the files `primary.cert` and `secondary.cert` in the LogZilla directory.

Event Logs

A list of all event logs on the local system is displayed. Messages in the event logs that are checked will be sent to the server.

Poll Interval

This is the number of seconds between each time the event logs are read to check for new messages to send.

Ignore Event Ids

To reduce the volume of messages sent, it is possible to ignore certain event ids. This is entered as a comma-separated list of event id numbers.

Look up Account IDs

Looking up the domain and user name of the account that generated a message can be expensive, as it may involve a call to a domain server, if the account is not local. To improve performance, this look up can be disabled and messages will be sent to the server without any account information.

Include key-value pairs

To aid parsing on the syslog server, the message content is enhanced by appending the following key-value pairs:

- “event_id” : “nnnn” contains the Windows event id
- “_source_type” : “WindowsAgent” identifies this program as the sender of the message
- “S1”: ”xxx”, “S2”: ”xxx”, … contain the substitution strings, if any

Facility

The selected facility is included in all messages sent.

Severity

By selecting ‘Dynamic’, the severity for each message is determined from the Windows event log type. Otherwise, the selected severity is included in all messages sent.

Suffix

The suffix is an optional set of key/value pairs that is appended to all messages sent.

Log Level

This configures the "level" of log messages produced by the Syslog Agent. The "level" means the type or importance of a given message. Any given log level will produce messages at that level and those levels that are more important. For example if "RECOVERABLE" is chosen, the Syslog Agent will also produce log messages of levels "FATAL" and "CRITICAL". Logging is optional, so this can be left set to "None".

Log File Name

This configures the path and name of the file to which log messages will be saved. If a path and directory are specified that specific combination will be used for the log file, otherwise the log file will be saved in the directory with the SyslogAgent.exe file. If log level is set to "None" this will be blank.

File Watcher (tail)

The agent has the capability to "tail" a specified text file – this means that the agent will continually read the end of the given text file and send each new line that is appended to that text file as a separate message to the LogZilla server. A program name should be specified here to indicate the source of those log messages.

Save

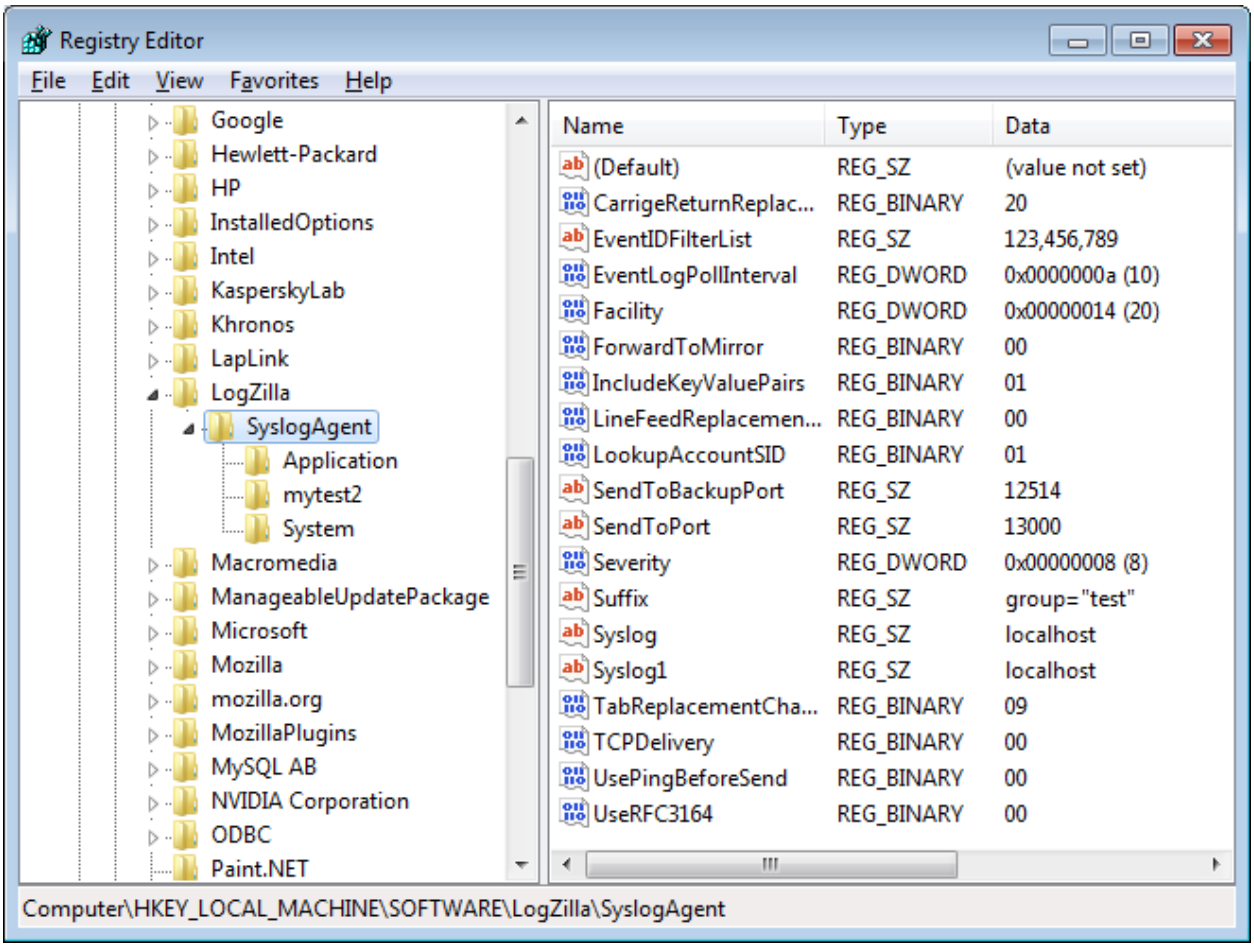
The configuration settings are stored in the registry.

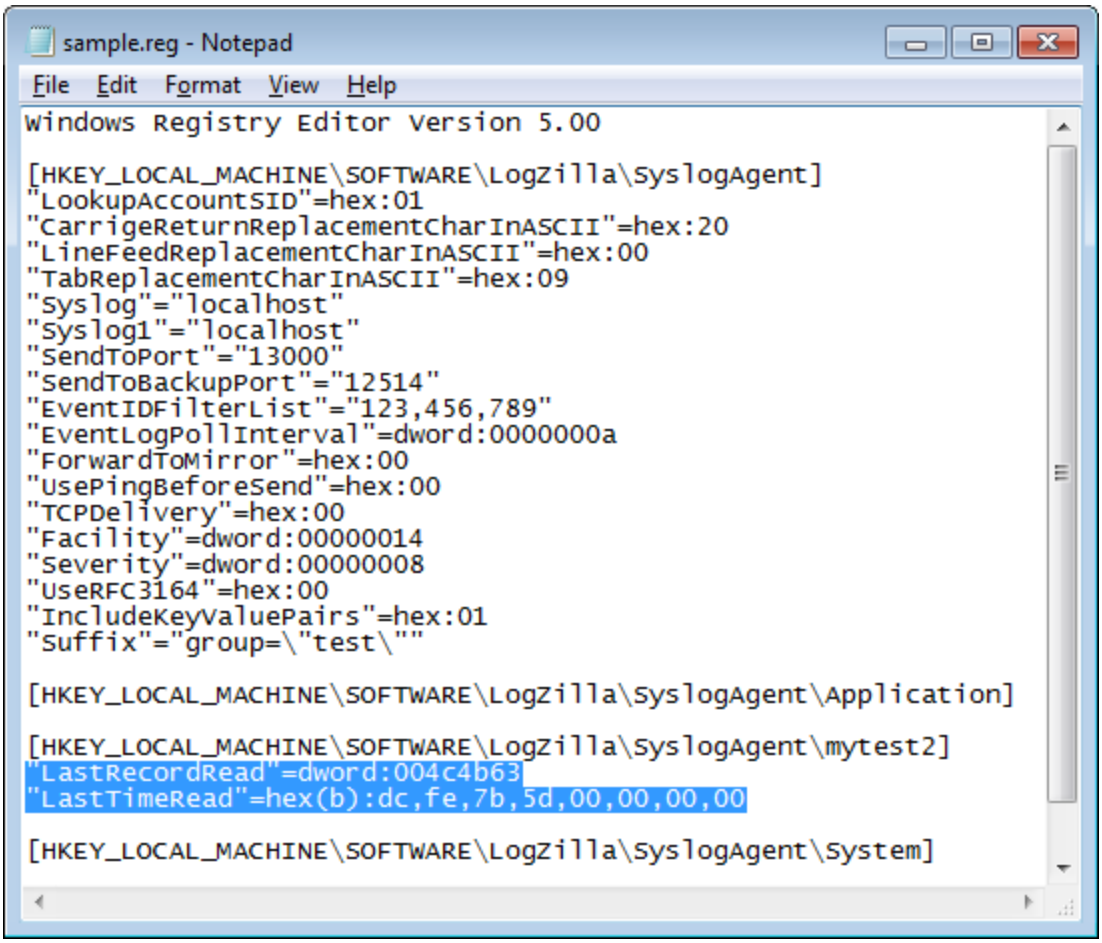
Restart

If the syslog agent service is running, it must be restarted to pick any changes made in the configuration settings.

Registry Data

The settings are stored in the registry at HKEY_LOCAL_MACHINE\SOFTWARE\Logzilla\SyslogAgent. There are sub-keys for each event log selected.


Registry Editor
File Edit View Favorites Help
Google
Hewlett-Packard
HP
InstalledOptions
Intel
KasperskyLab
Khronos
LapLink
LogZilla
SyslogAgent
Application
mytest2
System
Macromedia
ManageableUpdatePackage
Microsoft
Mozilla
mozilla.org
MozillaPlugins
MySQL AB
NVIDIA Corporation
ODBC
Paint.NET
Name Type Data
(Default) REG_SZ (value not set)
CarrigeReturnReplac... REG_BINARY 20
EventIDFilterList REG_SZ 123,456,789
EventLogPollInterval REG_DWORD 0x0000000a (10)
Facility REG_DWORD 0x00000014 (20)
ForwardToMirror REG_BINARY 00
IncludeKeyValuePairs REG_BINARY 01
LineFeedReplacemen... REG_BINARY 00
LookupAccountSID REG_BINARY 01
SendToBackupPort REG_SZ 12514
SendToPort REG_SZ 13000
Severity REG_DWORD 0x00000008 (8)
Suffix REG_SZ group="test"
Syslog REG_SZ localhost
Syslog1 REG_SZ localhost
TabReplacementCha... REG_BINARY 09
TCPDelivery REG_BINARY 00
UsePingBeforeSend REG_BINARY 00
UseRFC3164 REG_BINARY 00
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\LogZilla\SyslogAgent



Settings can be maintained on one machine and loaded onto another machine by exporting them to a text file. This is done by right-clicking on the SyslogAgent node and selecting 'Export', or using the command line:

```
regedit /E sample.reg "HKEY_LOCAL_MACHINE\SOFTWARE\Logzilla\SyslogAgent"
```

The settings are loaded on the target machine with the command line:

```
regedit /S sample.reg
```

If the Syslog Agent service has been run on the source machine, the registry may contain information about the last messages processed, and these lines should be deleted before loading the settings on to another machine.

Operation

After the Syslog Agent has been installed as a Windows service, it can be started and stopped with the Windows Services control panel, or with the command line:

```
net start "LZ Syslog Agent"
```

and

```
net stop "LZ Syslog Agent"
```

For testing, the Syslog Agent can be run from the command line. The command prompt must be run as administrator.

```
syslogagent –console
```

or

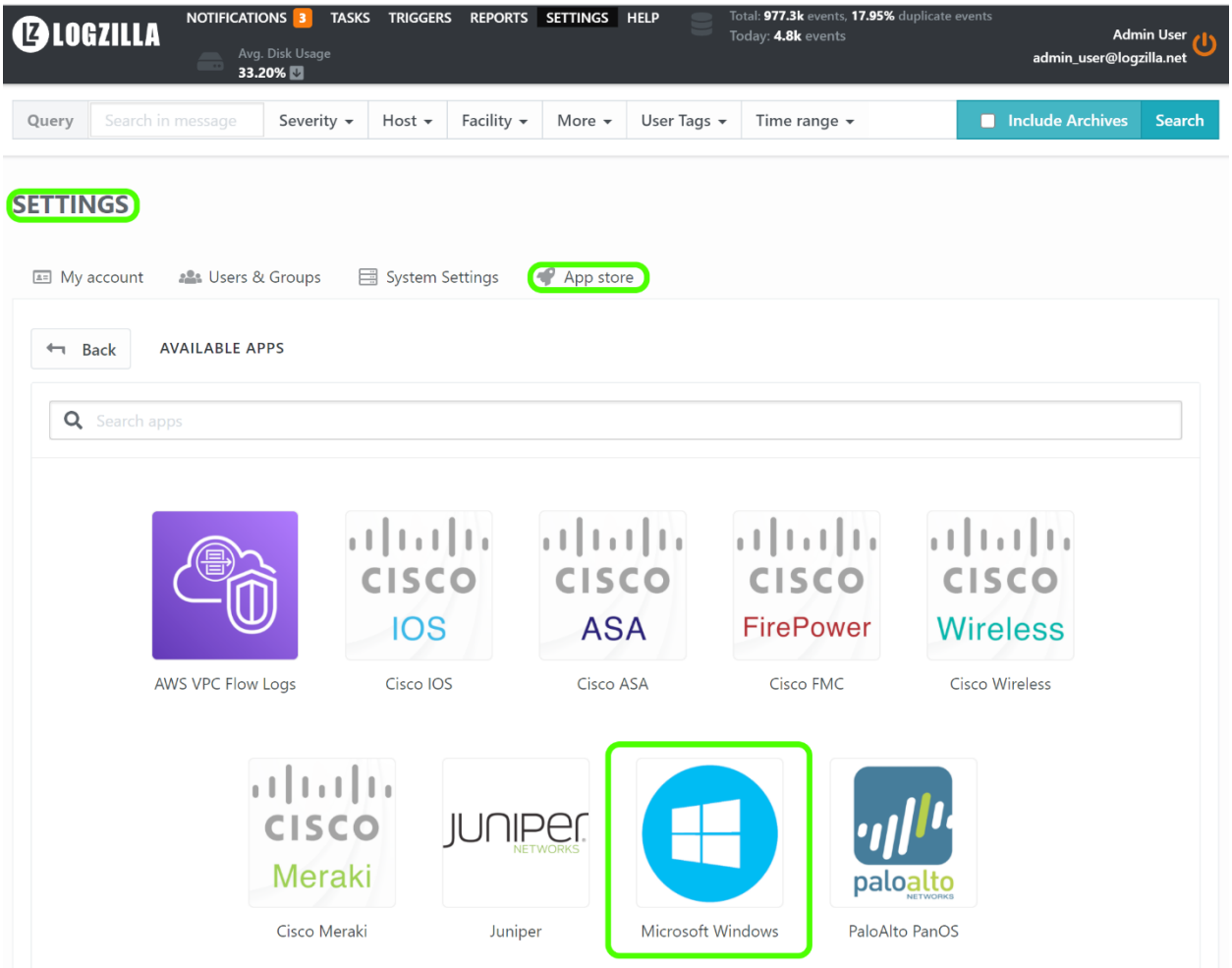
```
syslogagent –console –debug
```

to print debugging information.

To stop a test run, type the 'esc' key.

LogZilla Configuration

In order for LogZilla to make use of the Windows Syslog Agent the LogZilla rule for the agent must be installed. The preferred means of accomplishing this is by installing the *MS Windows* app from the LogZilla appstore, by going to `Settings -> App store` then choosing `Microsoft Windows` and then choosing `Install`.



If the LogZilla appstore is unavailable in your installation of LogZilla you may install the Windows Syslog Agent rule manually. The rules file and tests file are `601-windows-syslog-agent.lua` and `601-windows-syslog-agent.tests.yaml`. These files are provided in the `rules\` subdirectory of the installation folder (or by default `c:\Program Files\LogZilla\SyslogAgent\SyslogAgent\rules`).

The rule is installed by copying the two files to your LogZilla server (such as via `scp`) and then running it:

```
Logzilla rules add 601-windows-syslog-agent.lua
```

The console should then say

```
Rule 601-windows-syslog-agent added and enabled
Reloading rules ...
Rules reloaded
```

After the app is installed (or the rule has been manually loaded) LogZilla will be set to properly handle event and file log messages coming from the Windows Syslog Agent.