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. (note: the name is no longer completely accurate; although this agent performs the role that typically unix *syslog* does, the agent now uses HTTP/HTTPS rather than syslog protocol.)

Features

This program supports the following:

- Simple configuration and ease of use.
- Select of specific event logs
- Configuration of primary and secondary LogZilla recipient servers
- Configuration of optional TLS transport for log messages
- Optional ignoring specified Windows event IDs
- Optional "tail"-ing of specified file

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_6.31.1.0.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

Primary LogZilla Server

This is the HTTP/HTTPS address (optionally with port) for the primary LogZilla server.

Secondary LogZilla server

This is the HTTP/HTTPS address (optionally with port) for the secondary LogZilla server to receive the events, if desired.

Primary / Secondary LogZilla API Key

In order to send events to LogZilla, a LogZilla auth token / API key must be used. This can be created using the `logzilla` command line tool as follows:

```
root[~]: # logzilla authtoken create
No user specified (missing -U option). I'll create key for admin
b2d8c210f54ed85511f1867cb6cc4faa8ae85bff42c3dd26
```

The last line shows the auth token. This is what you would put in the *API Key* text box here.

More information can be found at: https://docs.logzilla.net/09_LogZilla_API/01_Using_The_LogZilla_API/

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 (PFX 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. The loaded certificate files are named `primary.pfx` and `secondary.pfx`, in the LogZilla installation directory (default `c:\Program Files\Logzilla\SyslogAgent)`.

If you do not have a `.pfx` file, but instead have `.key` and `.crt files,` if you have access to a unix machine with *openssl* installed, you can use the following command to produce a `.pfx` file from the `.key` and `.crt` files:

```
root@agent-http # openssl pkcs12 -export -out cert.pfx -inkey cert.key\
 -in cert.crt
```

Note that the .pfx file must not use a password.

LogZilla Compatible Version

Sometimes the Agent behavior must be configured to work with a particular revision level of LogZilla server. Ordinarily this should be set at "detect". LogZilla support will indicate whether to force a particular compatibility version level, in which case these drop-downs should be set as specified.

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.

Event Selection

Ignore / Include Event IDs

If desired, the event IDs that the Agent sends to LogZilla can be limited. This can be used either to limit the volume of events sent, or to limit the events to only those of interest. Using "Ignore", the specified event IDs will never be sent to LogZilla. Using "Include", *only* the specified event IDs will be sent to LogZilla. The event IDs should be provided separated by commas.

Catch-Up / Only While Running

Either the agent can keep track of where it left off, when the agent is shut down, and then catch-up on missed events when it starts back up; or it can ignore missed events and only send events while running.

Message Content

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.

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.

Extra Key/Value Pairs

This configures whether any supplemental key-value pairs will be included with the log messages, for processing by LogZilla rules. Key-value pairs should be separated by commas.

In addition to the manually specified key-values, LogZilla includes some default key-value pairs for use in the LogZilla rules:

- "_source_tag": "windows_agent"
- "event_id": "nnnn" contains the Windows event id
- "event_log": "xxx" … contains the name of the event log that produced the message
- "log_type": "eventlog" OR "_log_type": "file" … indicates whether the log message originated in a Windows event log or originated from the "tail" operation

Max Batch Size / Max Batch Age

Max Batch Size is the maximum number of log events that the Windows Agent will queue up before sending them. **Max Batch Age** is the longest that the Windows Agent will wait from the time an event occurs to the time the Agent sends that event to LogZilla. So, whenever new events occur, if the number of events queued up equals or exceeds the **Max Batch Size**, the Agent sends the events. Also, whenever the oldest unsent

message reaches the **Max Batch Age**, the Agent sends the events. So you can set both "most unsent messages" and "longest delay before sending" parameters. Set the **Max Batch Size** to 0 to send every event immediately.

Logging

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.

Other

Batch Interval

This setting is deprecated.

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, and this will show up in the "Program" field in LogZilla.

Import / Export

These buttons can be used to make a registry file of the LogZilla settings. This can be useful for automating LogZilla installation across multiple machines. To do this, the LogZilla settings should be configured as desired, then saved, then *Export* pressed to create a registry file. This registry file can then be imported on the desired target Windows machines by either using the *Import* button, or, since the file is a standard `.reg` registry file, can be imported using any of the Windows registry import methods.

Save

The configuration settings are stored in the registry.

Stop/Start

If the *LZ Syslog Agent* service is running, it must be restarted to pick any changes made in the configuration settings. This can be done by first **Stop**ping the Agent service, then **Start**ing the Agent service.
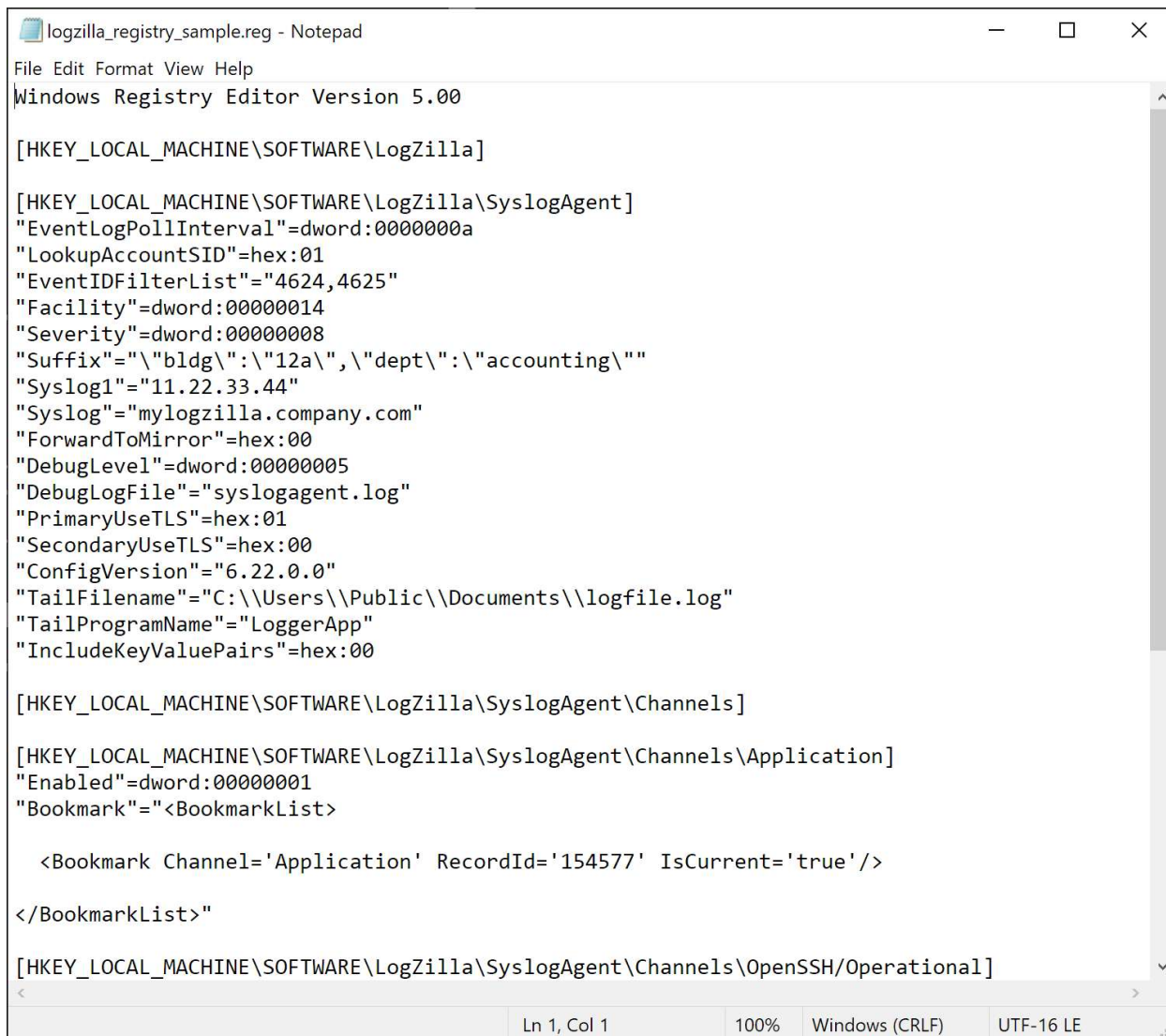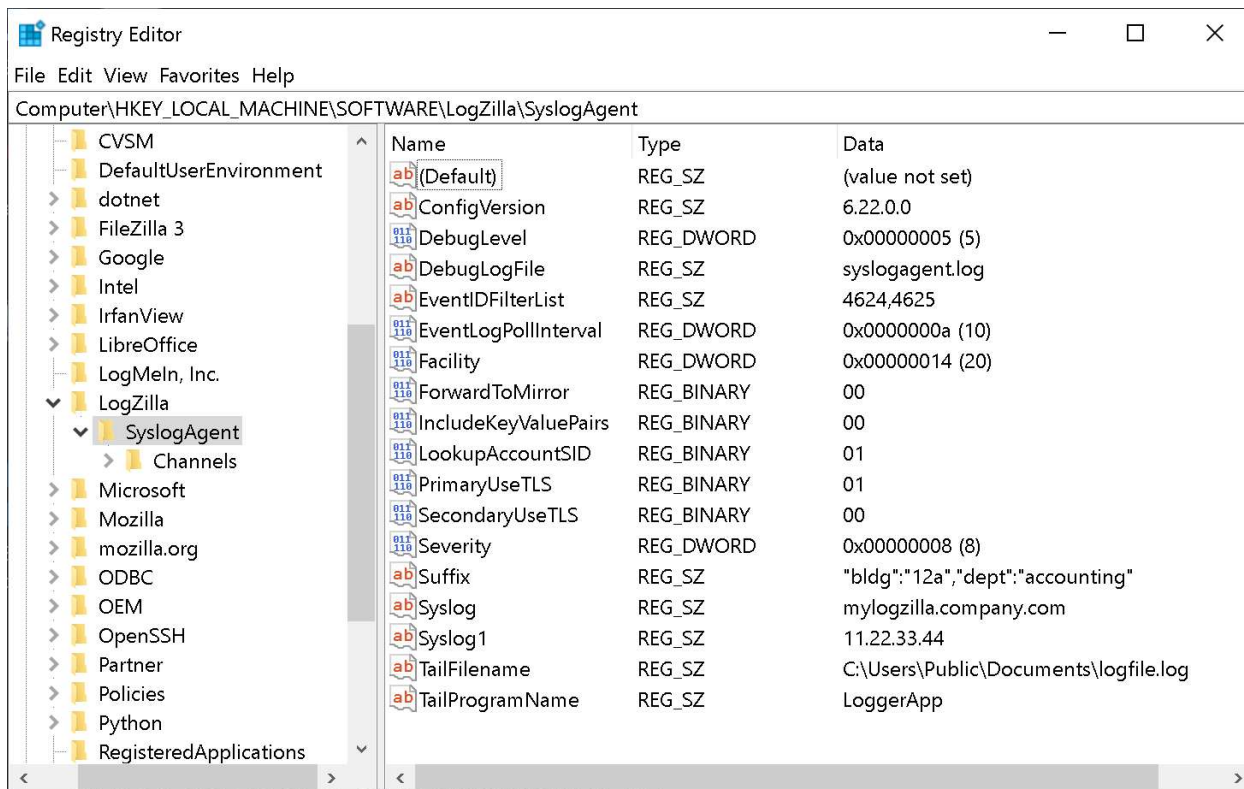
Registry Data

The settings are stored in the registry at:

HKEY_LOCAL_MACHINE\SOFTWARE\Logzilla\SyslogAgent

There are sub-keys for each event log selected.

LogZilla Windows Syslog Agent V6.31.1.0

CVSM	
DefaultUserEnvironment	
> dotnet	
> FileZilla 3	
> Google	
> Intel	
> IrfanView	
> LibreOffice	
LogMeIn, Inc.	
∨ LogZilla	
∨ SyslogAgent	
> Channels	
> Microsoft	
> Mozilla	
> mozilla.org	
> ODBC	
> OEM	
> OpenSSH	
> Partner	
> Policies	
> Python	
RegisteredApplications	

Name	Type	Data
ab (Default)	REG_SZ	(value not set)
ab ConfigVersion	REG_SZ	6.22.0.0
DebugLevel	REG_DWORD	0x00000005 (5)
ab DebugLogFile	REG_SZ	syslogagent.log
ab EventIDFilterList	REG_SZ	4624,4625
EventLogPollInterval	REG_DWORD	0x0000000a (10)
Facility	REG_DWORD	0x00000014 (20)
ForwardToMirror	REG_BINARY	00
IncludeKeyValuePairs	REG_BINARY	00
LookupAccountSID	REG_BINARY	01
PrimaryUseTLS	REG_BINARY	01
SecondaryUseTLS	REG_BINARY	00
Severity	REG_DWORD	0x00000008 (8)
ab Suffix	REG_SZ	"bldg":"12a","dept":"accounting"
ab Syslog	REG_SZ	mylogzilla.company.com
ab Syslog1	REG_SZ	11.22.33.44
ab TailFilename	REG_SZ	C:\Users\Public\Documents\logfile.log
ab TailProgramName	REG_SZ	LoggerApp

LogZilla Windows Syslog Agent V6.31.1.0

```
logzilla_registry_sample.reg - Notepad                              —   □   ✕

File  Edit  Format  View  Help
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\LogZilla]

[HKEY_LOCAL_MACHINE\SOFTWARE\LogZilla\SyslogAgent]
"EventLogPollInterval"=dword:0000000a
"LookupAccountSID"=hex:01
"EventIDFilterList"="4624,4625"
"Facility"=dword:00000014
"Severity"=dword:00000008
"Suffix"="\"bldg\":\"12a\",\"dept\":\"accounting\""
"Syslog1"="11.22.33.44"
"Syslog"="mylogzilla.company.com"
"ForwardToMirror"=hex:00
"DebugLevel"=dword:00000005
"DebugLogFile"="syslogagent.log"
"PrimaryUseTLS"=hex:01
"SecondaryUseTLS"=hex:00
"ConfigVersion"="6.22.0.0"
"TailFilename"="C:\\Users\\Public\\Documents\\logfile.log"
"TailProgramName"="LoggerApp"
"IncludeKeyValuePairs"=hex:00

[HKEY_LOCAL_MACHINE\SOFTWARE\LogZilla\SyslogAgent\Channels]

[HKEY_LOCAL_MACHINE\SOFTWARE\LogZilla\SyslogAgent\Channels\Application]
"Enabled"=dword:00000001
"Bookmark"="<BookmarkList>

  <Bookmark Channel='Application' RecordId='154577' IsCurrent='true'/>

</BookmarkList>"

[HKEY_LOCAL_MACHINE\SOFTWARE\LogZilla\SyslogAgent\Channels\OpenSSH/Operational]

                    Ln 1, Col 1          100%    Windows (CRLF)    UTF-16 LE
```

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"
```

LogZilla Windows Syslog Agent V6.31.1.0

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`.
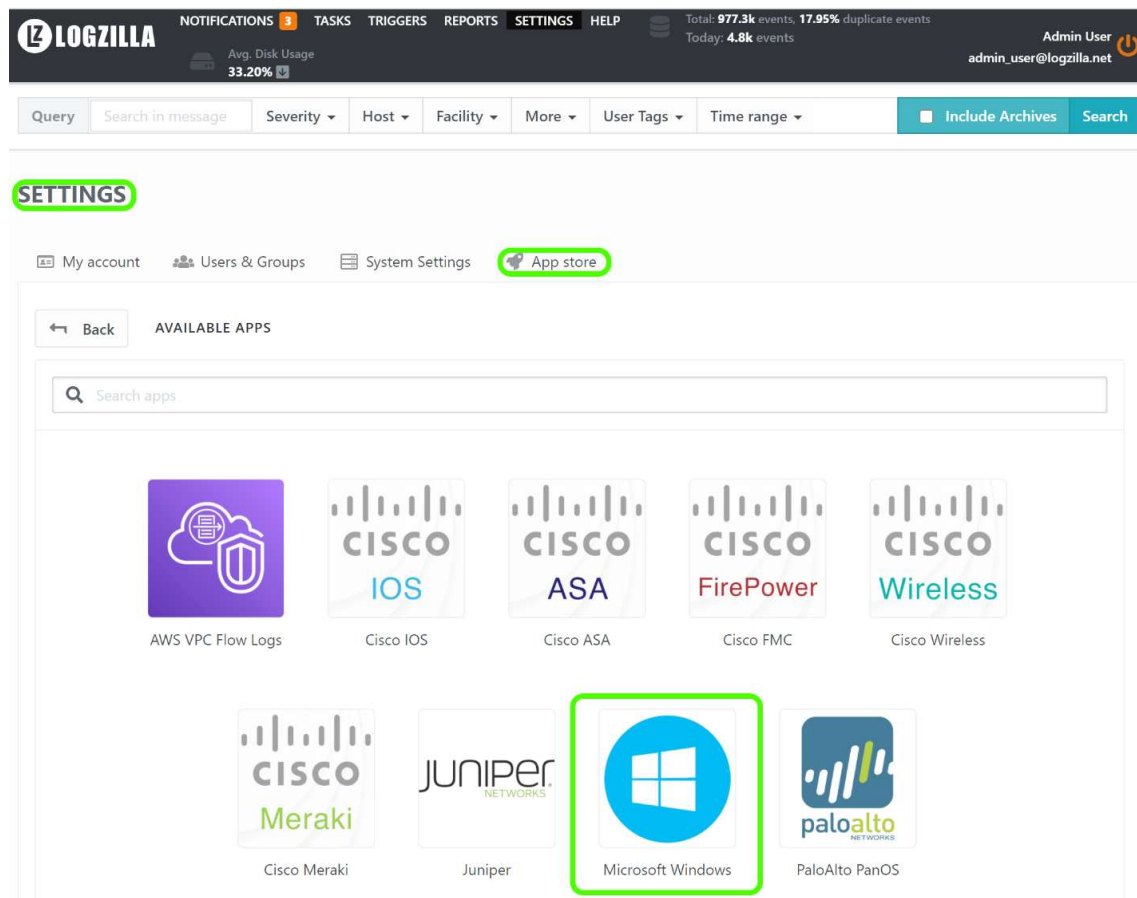
Once the Microsoft Windows appstore application has been installed LogZilla should correctly receive and display log messages from the Windows Syslog Agent.

LogZilla Windows Syslog Agent V6.31.1.0