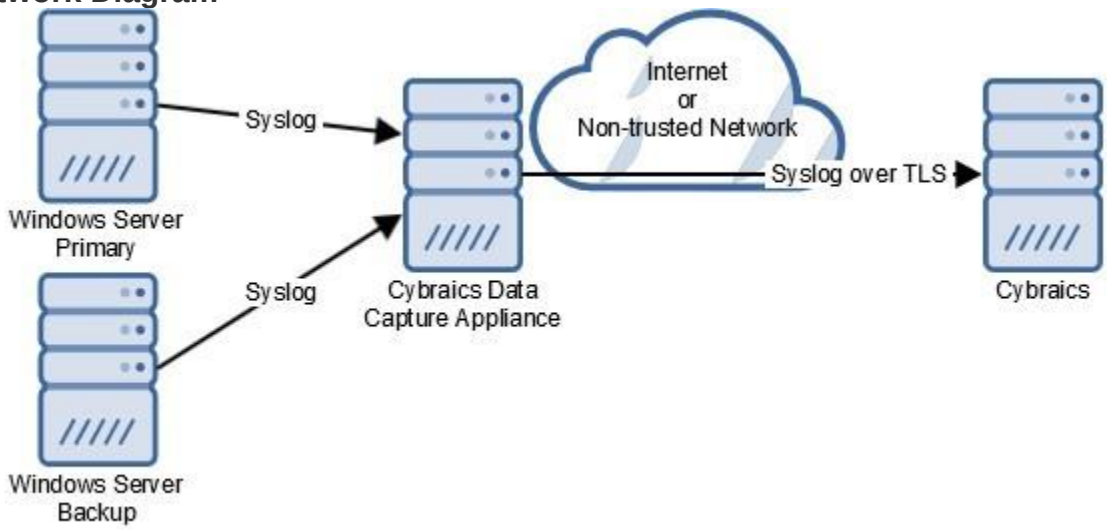
CYBRAICS

nLighten™

Windows Syslog Client Guide

This document describes a method to install and configure a Microsoft Windows workstation, or server, to forward log messages to Cybraics. This method allows for many such servers to forward syslog messages through a secure proxy. This guide is considered generic, because there are many similarly acceptable methods to forward log messages - and your organization may already have such a method.

Network Diagram



Install the Syslog Client

Cybraics provides licenses for the RSyslog Windows Agent. Download and install the RSyslog Windows Agent from the following link. Cybraics will provide the license.
http://www.rsyslog.com/windows-agent/windows-agent-download/

Configuring the Syslog Client

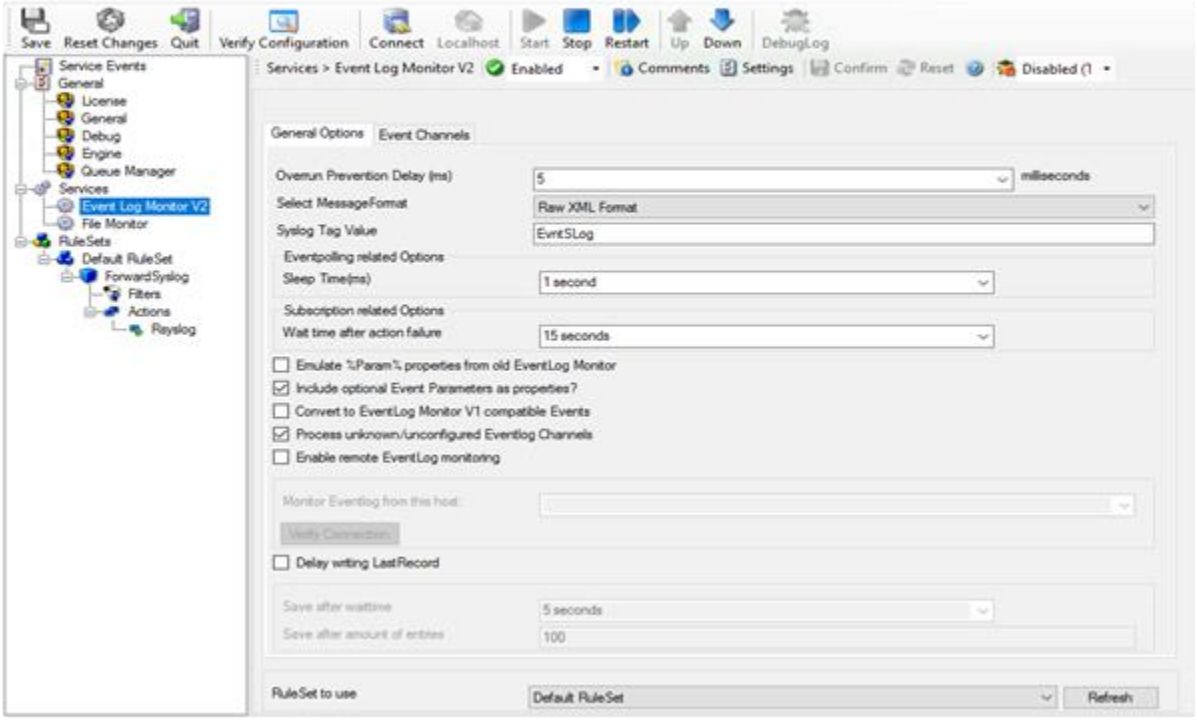
The RSyslog Windows Agent can forward Windows Events and log line entries from files. Many native Windows services, such as Active Directory, IIS, and DNS, output their messages as Windows Events. Some third party services, and some native services, such as Windows DNS Server debug logs (which contain important query information) additionally output logs into files. First determine which services are to be monitored and how they log information.
Use the guide linked below to configure these options http://www.rsyslog.com/download/files/windows-agent-manual/index.html
To forward Windows Event Messages :

- Configure ServicesEvent Log Monitor V2 (Documentation)
- Select Message Format: Raw XML Format
- Syslog Tag Value: EvntSLog
- Sleep time: 1 second
- Wait time after action failure: 15 seconds
- Uncheck: Emulate %Param% properties...
- Check: Include optional Event Parameters as properties?
- Uncheck: Convert to EventLog Monitor V1 compatible Events
- Check: Process unknown/unconfigured Eventlog Channels
- Uncheck: Enable Remote EventLog monitoring
- Uncheck: Delay writing LastRecord
- RuleSet to use: Default RuleSet
- Under "Event Channels" tab - choose "Select All" events
- Check: Do NOT process existing entries
- Configure RuleSetsDefault RuleSetForwardRsyslogActionsRsyslog
- Select Protocol Type: TCP (Octet based framing)
- Update Syslog Server: <Cybraics CDCA IP address>
- Select Use RFC 5424 processing
- Select Output Encoding: System Default
- Check the "Use CEE enhanced Syslog Format"

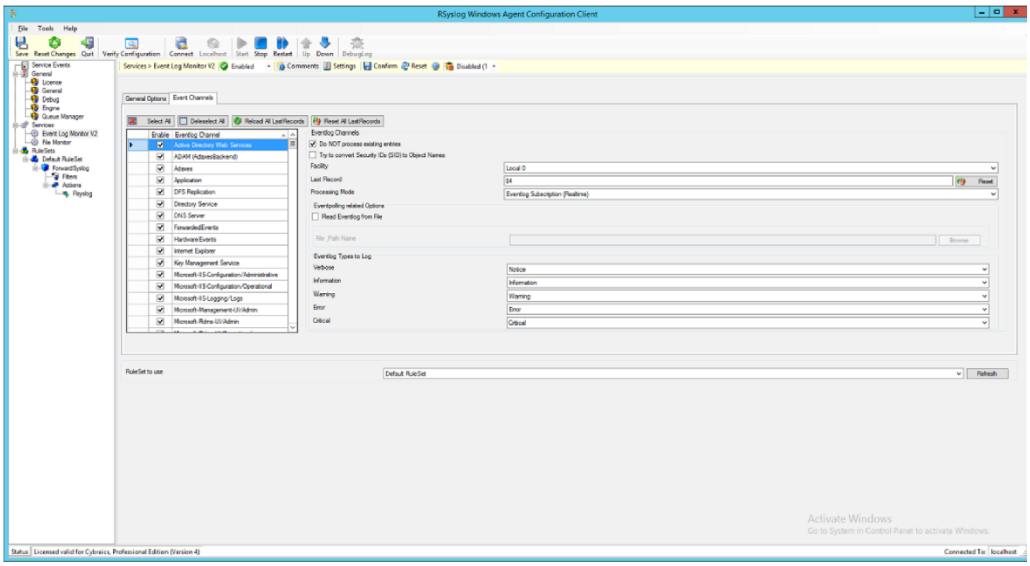
To forward lines from a log file:

- Configure **Services File Monitor** (Documentation)
- This is useful for forwarding Active Directory DNS Debug logs
  - See AD DNS guide from Cybraics for more details

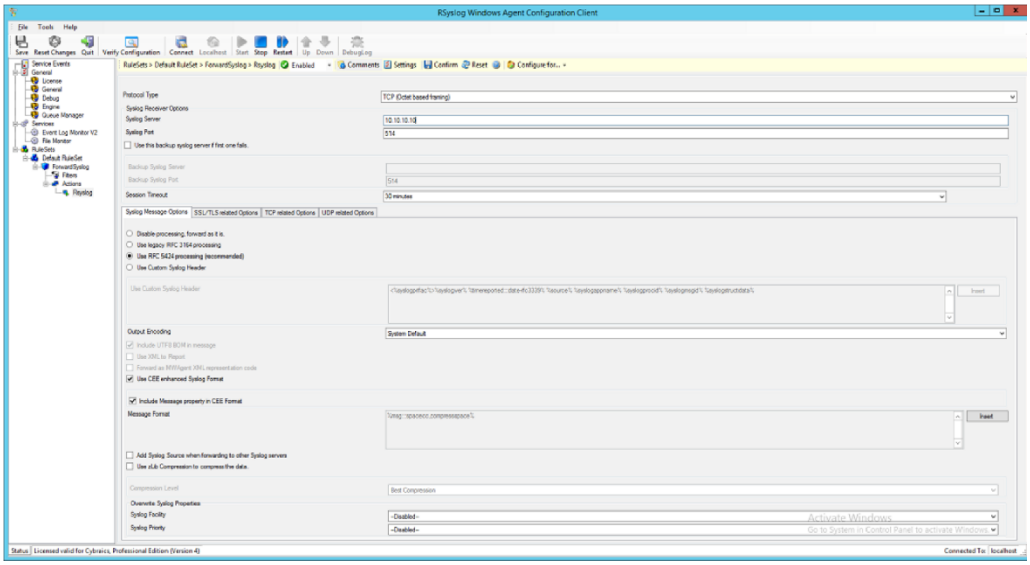
Reference Screenshots :



Event Log Monitor General Options



Event Log Monitor V2 Event Channels



ForwardSyslog Action

Additional Assistance

For further assistance, please contact support@cybraics.com