Adding Data from Logstash (Syslog)

Logstash XpoLog Integration

XpoLog's architecture allows receiving data sent by logstash, using XpoLog's logstash output. In order to do this, a Syslog listener account should be created in XpoLog for receiving the data on a specific network port, and the XpoLog logstash output should be sending data to this listener.

Technical Details

XpoLog's logstash output is a Ruby file that implements the logstash output functionality. The data that is sent by the output to the XpoLog listener is stored in logs and is available for searching, monitoring and analysis.

Setup

Note that in order for XpoLog to receive information sent from logstash, you should have an XpoLog Syslog listener configured and running. For more information about setting up a Syslog listener, click here

1. Download XpoLog's logstash output: xpolog.rb
2. Copy the xpolog.rb file you have downloaded to the lib/logstash/outputs directory, located under the logstash root directory
3. Configure the xpolog output according to the available configuration
4. Start XpoLog's logstash output

XpoLog's logstash output configuration

The following is an example of the structure of the xpolog output element.

```
output {
   xpolog {
      host => "localhost"
      port => 514
      protocol => "udp"
      logname => "my-log"
      procid => "1"
      logparameters => {
      xpologPath => "Root->my-folder"
      }
   }
}
```

The following table describes the parameters of output element.

Parameter	Mandatory/Optional	Description	Values
host	Mandatory	The name of the host to send the data to (the XpoLog host)	String
port	Mandatory	The network port on which the XpoLog Syslog listener is listening	Numeric
protocol	Optional	The network protocol to be used when sending data to the XpoLog Syslog listener. Optional values are udp or tcp. Default value is udp	String
logname	Optional	The name of the log that will be created in XpoLog. The value of this parameter will be concatenated to the name of the host sending the data, unless the logname parameter is preceded with #	String
procid	Optional	A parameter used to distinguish between different logstash processes that send data from the same machine to the same XpoLog Syslog listener	String
logparameters	Optional	A set of optional parameters	Hash

logparameters/xpologPath	Optional	The path, in XpoLog's Folders and Logs tree, in which the log will be created	String
logparameters/pattern	Optional	The data pattern that will be applied on the log	String