XpoLog Listeners

XpoLog may be configured to monitor incoming messages and decode the messages to be available in XpoLog over different protocols. XpoLog can listen to Syslog data (UDP or TCP) arriving from one or more source devices, HTTP/S arriving from one or more source device, data forwarded from XpoLog Agents, Cisco routers and switches that support NetFlow and receive topics from Kafka server(s).

You can use XpoLog to receive data from these source devices for easy searching, reporting and alerting - XpoLog also provides several options to automatically split the incoming data and create a dedicated log per source device or a custom configuration (note that such changes in a listener configuration take place on incoming data from the change forward, and is not applied on already processed data).

Syslog - UDP vs. TCP transport protocol:
Syslog logging has been traditionally sent to port 514 using UDP. UDP is a connectionless protocol, hence unreliability is inherent. There is no acknowledgement, error detection, sequencing or re-transmission of missed packets when sending Syslog messages over the UDP protocol.
Some devices implement the Syslog protocol over a TCP transport (When sending messages using TCP the destination port is usually 1468). TCP is connection oriented. It relies on the destination host being there. The connection is built when the sending device is initialized, or prior to sending the first Syslog message. It's slower to use TCP because of the initial time for the three-way handshake, and all packets get acknowledged by the server once they are received, and essentially before the next one can be sent. The TCP protocol offers reliability plus error correction; this is used to ensure messages are sent to the syslog server reliably.

HTTP/s transport protocol:
When an HTTP/S listener is configured and active, devices can send to the XpoLog server IP address and port data in JSON format and XpoLog will process the data and create log per device to be available in XpoLog.
Since an HTTP listener is a combination of the XpoLog IP address and port, each listener also provide a unique token that may be used the the device that pushes data to be identified by XpoLog.

XpoLog transport protocol:
XpoLog instances and agents can forward data ("push") in a format that XpoLog is familiar with. In order to received the data that is being sent from other XpoLog instances, and get it processed automatically an XpoLog listener has to be configured and active on the instance/cluster that should receive and process the data.

NetFlow transport protocol:
Cisco routers and switches that provide the ability to collect IP network traffic as it enters or exits an interface. By analyzing the data provided by NetFlow, a network administrator can determine things such as the source and destination of traffic, class of service, and the causes of congestion.
Routers and switches that support NetFlow can collect IP traffic statistics on all interfaces where NetFlow is enabled, and later export those statistics as NetFlow records toward XpoLog as a NetFlow collector - for traffic analysis. XpoLog supports NetFlow versions 5 and 9.

Kafka:
Kafka servers provide stream of records, similar to a message queue or enterprise messaging systems. XpoLog supports analyzing topics received by the listener from multiple Kafka servers.

Listeners Accounts Console:
Available under Manager > Administration > Listeners, the listeners accounts console presents all the configured listeners and their statuses and provides access to their configuration.