LogAway (collection over SSH-New)

Note: LogAway Agent (compatible with XpoLog 4.5+)

Summary

XpoLog’s agent-less architecture allows accessing logs located on remote machines over SSH, without the need to change or install anything on the remote machine. In order to do this, XpoLog utilizes the ‘less’ command on the remote machine, among other commands. In some environments, where the ‘less’ command is not available on the remote machine, XpoLog cannot work as described above.
XpoLog’s LogAway agent provides a solution for accessing logs located on remote machines over SSH where the ‘less’ command is not available. It is important to note that the agent is **passive**, and does not run any process on the remote machine unless requested to do so by the XpoLog server.

Technical Details

XPLG’s LogAway agent is a JAR file located in the home directory of the user that is used by XPLG to access the remote machine. After the JAR file is deployed on the remote machine, it does not run any process. Instead, the XPLG server automatically identifies that the LogAway agent is available on the remote machine, and uses it instead of utilizing traditional system commands.

All the data which is transferred by the LogAway agent to the XPLG server is compressed, to minimize network traffic.

Deployment

   a. Verify that Java is installed on the remote machine:
      i. Log in to the remote machine using the same user that is used by XPLG to access the remote machine (check the SSH account in XPLG address book and make sure to use the same user that is used in the SSH account).
      ii. Run the command *java -version* (the LogAway agent requires Java version 1.4+ to run)
2. Download XPLG’s LogAway package compatible to the Java version installed on the remote machine:
   a. Download LogAway for Java 1.4+: ***LogAway for JAVA 1.4+***
3. Copy XPLG’s LogAway package to the remote machine (place it in the home directory of the user that is used by XPLG to access the remote machine)
4. Unpack XPLG’s LogAway package by running the following commands:
   a. Run:
      gunzip xpologAgent.tar.gz (unzip the package)
   b. Run:
      tar -xvf xpologAgent.tar (extract the tar)
   c. Verify that a folder named xpologAgent was created and contains several files
5. Verify that XPLG’s LogAway jar can be used:
   a. Enter the xpologAgent folder
   b. Run the command **sh runAgent.sh -v**
   c. Verify that information regarding the LogAway is printed to the screen
6. **Optional** (improves performance) - verify on the remote server that TCP port forwarding is enabled:
   a. View the file /etc/ssh/sshd_config
   b. The parameter 'AllowTcpForwarding' specifies whether TCP forwarding is permitted (the default is "yes"). Note that disabling TCP forwarding does not improve security unless users are also denied shell access, as they can always install their own forwarders. In case 'AllowTcpForwarding' is set to "no" change it to "yes" and restart the SSH service.
   c. Go to XPLG>Settings>General, and under the 'Connection Policies' configure the following:
      i. LogAway Agent forwarding port - a free port on the remote machine to use (try "netstat" to list ports in use). LogAway uses the port locally in order to use SSH port forwarding (for example: 5555). It is not recommended to use ports 0-1023, as these are usually system processes ports.
      ii. LogAway Agent forwarding timeout - the allowed period of LogAway Agent inactivity before it's connection is terminated (default 1 minute)
7. In order to verify that the agent can be used by the XPLG server, add a log over SSH on this machine using direct access mode and check that everything works as expected:
   a. Open XPLG Support Portal > Activity Information and under SSH connections tab verify that the connection mode is Agent (instead of the default: Less).
   b. Run a search on the added log to ensure updated data is collected and available in XPLG server.