Here are "example" syslog records for Reject and Accept PowerBroker logs:

Example "Reject" syslog entry:

May 3 16:34:00 apollo xinetd[3189]: START: pbmasterd pid=11918 from=192.168.222.6 May 3 16:34:00 apollo xinetd[3189]: EXIT: pbmasterd status=0 pid=11918 duration=0(sec) May 3 16:34:00 apollo pbmasterd6.2.0-09: Reject:psmc:apollo.myvirtual.lab:2011/05/03:16\:34\:00:psql -h limpet -d psmcdb –U psmc\_dba -W:/home/psmc:postgres:apollo.myvirtual.lab:c0a8de064dc082d82E8F

May 3 16:34:00 apollo pbmasterd6.2.0-09:

May 3 16:34:00 apollo xinetd[3189]: START: pblogd pid=11920 from=192.168.222.6 May 3 16:34:00 apollo xinetd[3189]: EXIT: pblogd status=0 pid=11920 duration=0(sec)

Example "Accept" syslog entry:

May 3 16:37:53 apollo xinetd[3189]: START: pbmasterd pid=12102 from=192.168.222.6 May 3 16:37:53 apollo xinetd[3189]: EXIT: pbmasterd status=0 pid=12102 duration=0(sec) May 3 16:38:01 apollo pbmasterd6.2.0-09: Accept:psmc:apollo.myvirtual.lab:2011/05/03:16\:37\:53:vi /etc/shadow:/etc:root:apollo.myvirtual.lab:Ticket#26154:root:vi /etc/shadow:/etc:/var/log/pb.iolog:c0a8de064dc083c12F47

May 3 16:38:01 apollo pbmasterd6.2.0-09: accepted vi from [psmc@apollo.myvirtual.lab](mailto:psmc@apollo.myvirtual.lab) to [root@apollo.myvirtual.lab](mailto:root@apollo.myvirtual.lab) May 3 16:38:01 apollo xinetd[3189]: START: pblogd pid=12106 from=192.168.222.6 May 3 16:38:01 apollo xinetd[3189]: EXIT: pblogd status=0 pid=12106 duration=0(sec) May 3 16:38:05 apollo xinetd[3189]: START: pblogd pid=12112 from=192.168.222.6 May 3 16:38:05 apollo xinetd[3189]: EXIT: pblogd status=0 pid=12112 duration=0(sec)

I elected to use a “colon delimited format” so that field labels will not gobble up “line real estate”. For the “Reject” syslog record, the pertinent fields delimited by a “colon” have this format:

1) The string “pbmasterd” followed immediately by the pattern <version>:<white space>

2) The string “Reject”

3) Name of the user who made the PowerBroker request (“psmc”)

4) Name of the host where the request originated (“apollo.myvirtual.lab”)

5) Current date on that host (“2011/05/03”)

6) Current time on that host where the “colon” character is “escaped” with a backslash “\” (“16\:34\:00”)

7) The command and argument(s) – a mandatory free form text field (“psql -h limpet -d psmcdb –U psmc\_dba -W”)

8) Current working directory where the request was made (“/home/psmc”)

9) The requestuser (“psmc”)

10) The target host on to which the command is to be run (“apollo.myvirtual.lab”)

11) And the PowerBroker log identifier (“c0a8de064dc082d82E8F”)

For the “Accept” syslog record, the fields delimited by a “colon” have this format:

1) The string “pbmasterd” followed immediately by the pattern <version>:<white space>

2) The string “Accept”

3) Name of the user who made the PowerBroker request (“psmc”)

4) Name of the host where the request originated (“apollo.myvirtual.lab”)

5) Current date on that host (“2011/05/03”)

6) Current time on that host where the “colon” character is “escaped” with a backslash “\” (“16\:37\:53”)

7) The command and arguments – a mandatory free form text field (“vi /etc/shadow”)

8) The requestuser (“psmc”)

9) The target host on to which the command is to be run (“apollo.myvirtual.lab”)

10) The OPTIONAL reason – would be a blank field if no reason is provided – but otherwise a free form text with a backslash-escaped “colon” delimiter (“Ticket#26154”)

11) The privileged user who will run the privileged command (“root”)

12) The delegated privileged command and arguments (“vi /etc/passwd”)

13) The specified working directory for the privileged command (“/etc”)

14) The OPTIONAL iolog file name – would be blank if not specified – but otherwise a free from text with a backslash-escaped value (“/var/log/pb.iolog”)

15) And the PowerBroker log identifier (“c0a8de064dc083c12F47”)

The text field values should be expected or treated to have a backslash-escaped “colon” character just to be safe. So when the ArcSight parser or connecter is made, it should be made with the expectation that every field can have a backslash-espcaped colon character if possible or else we will have to redo it.