|  |  |
| --- | --- |
| sum by(add) (rate({job="JOBNAME”, instance=~"$instance"} | Hiermit wird die Aufsummierung der Benutzernamen definiert, die wir mit „Patterns“ in LogQL definiert haben. „Patterns“ ermöglichen die einfache Extrahierung von Informationen aus einer Zeile. Wir holen alle Log-Einträge, die sich auf den von uns definierten Job beziehen. Wir können auch nach spezifischen Endpoint filtern, indem wir das Schlüsselwort „instance“ benutzen. |
| | | „|“ funktioniert in LogQL wie eine Pipeline für die Verkettung von mehreren Suchmustern. |
| |= `**sshd**[`  |= `: **Failed**` | Suche nach Zeilen mit den in den rot markierten Einträgen. |
| !~ `invalid user`  !~ `Legitimer\_Nutzer`  !~ `Legitime\_Adresse` | Suche nach Zeilen **ohne** diese Einträge. Wir können beispielsweise Einträge ausschließen, die auf legitimen Nutzer oder IP-Adresse beziehen, um falsche Positive zu vermeiden |
| | pattern `<\_> for <**Benutzername**> from <**Quelladresse**> port <\_>` [$\_\_range])) | Die Definition der Wörter „Benutzername“ „Quelladresse“ und als „Pattern“ dienen dazu, einen Benutzernamen und eine Quelle IP-Adresse aus der Logdatei zu extrahieren. Die Platzhalter „<\_>“ sind unbenannte Elemente, die in diesem Fall auf die Einträge „password“ und Portnummer in der Zeile verweisen. |

|  |
| --- |
| Der gesamte Regelsatz sieht schließlich so aus:  sum by(add) (rate({job="*JOBNAME*”, instance=~"$instance"} |= `**sshd**[` |= `: **Failed**` !~ `invalid user` !~ `*Legitimer\_Nutzer*` !~ `*Legitime\_Adresse*` | pattern `<\_> for <**Benutzername**> from <**Quelladresse**> port <\_>` [$\_\_range])) |

|  |  |
| --- | --- |
| sum by(add) (rate({job="JOBNAME”, instance=~"$instance"} | Hiermit wird die Aufsummierung der Benutzernamen definiert, die wir mit „Patterns“ in LogQL definiert haben. „Patterns“ ermöglichen die einfache Extrahierung von Informationen aus einer Zeile. Wir holen alle Log-Einträge, die sich auf den von uns definierten Job beziehen. Wir können auch nach spezifischen Endpoint filtern, indem wir das Schlüsselwort „instance“ benutzen. |
| | | „|“ funktioniert in LogQL wie eine Pipeline für die Verkettung von mehreren Suchmustern. |
| |= `**sshd**[`  |= `: **Failed**` | Suche nach Zeilen mit den in den rot markierten Einträgen. |
| !~ `invalid user`  !~ `Legitimer\_Nutzer` !~ `Legitime\_Adresse` | Suche nach Zeilen **ohne** diese Einträge. Wir können beispielsweise Einträge ausschließen, die auf legitimen Nutzer oder IP-Adresse beziehen, um falsche Positive zu vermeiden |

|  |  |
| --- | --- |
| | pattern `<\_> for <**Benutzername**> from <**Quelladresse**> port <\_>` [$\_\_range])) | Die Definition der Wörter „Benutzername“ „Quelladresse“ und als „Pattern“ dienen dazu, einen Benutzernamen und eine Quelle IP-Adresse aus der Logdatei zu extrahieren. Die Platzhalter „<\_>“ sind unbenannte Elemente, die in diesem Fall auf die Einträge „password“ und Portnummer in der Zeile verweisen. |

'^(?P<time>[A-Za-z]{3}

\s{1,2}\d{1,2}\s\d{2}:\

d{2}:\d{2}).\*from.(?P<

sourceIP>(?:25[0-5]|(?:2

[0-4]|1\d|[1-9]|)\d)\.(?:25

[0-5]|(?:2[0-4]|1\d|[1-9]|)\

d)\.(?:25[0-5]|(?:2[0-4]|1\

d|[1-9]|)\d)\.(?:25[0-5]|(?

:2[0-4]|1\d|[1-9]|)\d))'