Cisco Secure Cloud Analytics

クエリ構文リファレンス

目次

イベントビューアのクエリ構文

詳細については、Lucene クエリ構文のマニュアルを参照してください。

クエリ構文オプション

次のクエリ構文オプションを使用できます。

構文オプション	構文	説明
基本的なフィールド/値の評価	`field1: "value1"`	field1 が value1 に等しい結果を返します
単一文字のワイルドカード	`?`	この？は任意の文字と一致します ワイルドカード検索は、列のインラインフィルタが英数字の文字列値を受け入れる場合にのみサポートされます。
複数文字のワイルドカード	`*`	この＊は任意の数の任意の文字と一致します ワイルドカード検索は、列のインラインフィルタが英数字の文字列値を受け入れる場合にのみサポートされます。
包含的範囲検索	`["value1" TO "value2"]`	value1、value2、またはその間の任意の値を返します
排他的範囲検索	`{"value1" TO "value2"}`	value1 と value2 の間の値を返しますが、value1 または value2 の値は返しません
ブール演算子 AND	`AND`	AND 前後の両方の評価が true である結果を返します
ブール演算子 OR	または	OR 前後の評価のいずれかが true である結果を返します
ブール演算子 NOT	`NOT`	NOT の前の評価が true で、NOT 後の評価が false である結果を返します
グループ化	`()`	括弧内を単独で評価します
フィールドのグループ化	`field1: ()`	単一フィールドの括弧内の複数の値と演算子を評価します

評価の順序

クエリはシステムにより次の優先順位で評価されます。

1. グループ化。()(括弧)、[](包含的範囲検索)、{}(排他的範囲検索)を含む
2. :(等しい)
3. NOT ブール演算子
4. AND ブール演算子
5. OR ブール演算子

クエリ構文例

次の表に、一般的なクエリ構文の例を示します。

説明	構文例	返される結果
1 つのフィールド、1 つの値	`field1: "value1"`	field1 が value1 に等しいすべてのイベント
1 つのフィールド、1 つの値、1 文字のワイルドカード	`field1: "value?"`	field1 が "value?" に等しいすべてのイベント (? は任意の文字)
1 つのフィールド、1 つの値、複数文字のワイルドカード	`field1: "value*"`	field1 が "value*" に等しいすべてのイベント (* は任意の数の文字)
1 つのフィールド、複数の値 (フィールドのグループ化)	`field1:("value*1" AND "value*2")`	field1 に value*1 と value*2 が含まれるすべてのイベント 1 つのフィールドで複数の値を検索する場合は、一致する結果が得られる可能性を高めるために、各値にワイルドカードを使用することを推奨します。
1 つのフィールド、どちらかの値	`field1:("value1" OR "value2")`	field1 が value1 または value2 と等しいすべてのイベント

説明	構文例	返される結果
2 つのフィールド、AND 演算子	`field1: "value1" AND field2: "value2"`	field1 が value1 に等しく、かつ field2 が value2 に等しいすべてのイベント 複数のフィールド値の評価の間に演算子を明示的に定義しない場合、システムは評価間に AND 演算子を暗黙的に解釈します。
2 つのフィールド、OR 演算子	`field1: "value1" OR field2: "value2"`	field1 が value1 に等しい、または field2 が value2 に等しいすべてのイベント
2 つのフィールド、NOT 演算子	`field1: "value1" AND NOT field2: "value2"`	field1 が value1 に等しく、field2 が value2 に等しくないすべてのイベント
2 つのフィールド、OR NOT 演算子	`field1: "value1" OR NOT field2: "value2"`	field1 が value1 に等しい、または field2 が value2 に等しくないすべてのイベント
1 つのフィールド包含的範囲検索	`field1:["value1" TO "value2"]`	field1 が value1、value2、またはその範囲内の任意の値に等しいすべてのイベント
1 つのフィールド、排他的範囲検索	`field1:{"value1" TO "value2"}`	field1 が value1 と value2 の間の任意の値に等しいが、value1 または value2 ではないすべてのイベント
1 つのフィールド、包含的範囲検索と排他的範囲検索	`field1:["value1" TO "value2"}`	field1 が value1、または value1 と value2 の間の任意の値に等しいが、value2 ではないすべてのイベント
複数のフィールド、混合演算子	`field1: "value1" OR field2: "value2" AND field: "value3"`	AND ブール演算子は OR ブール演算子よりも優先されるため、以下に一致するすべてのイベント: • field2 が value2 に等しく、かつ field3 が value 3 に等しい、または • field1 が value1 に等しい

説明	構文例	返される結果
複数のフィールド、混合演算子および括弧	`(field1: "value1" OR field2: "value2") AND field3: "value3"`	グループ化は他の演算子よりも優先され、最初に評価されるため、以下に一致するすべてのイベント: • field1 が value1 に等しいか、または field2 が value2 に等しい、かつ • field3 が value3 に等しい

次の表に、ユーザーが展開のために実行できるクエリの例を示します。

説明	構文例	返される結果
内部 Web サーバーとの正常な非 HTTPS 接続を確立した内部デバイス	`Connected_ip: "192.168.105.28" AND IP: "192.168.0.0/16" AND NOT Port: "443" AND NOT Connected_port: "443" AND Packets_from: { "10" TO * } AND Packets_to: { "10" TO * }`	以下のすべてのイベント: • `IP` が `192.168.0.0/16`（内部エンティティ）の内部 CIDR 範囲に等しい • `Connected_ip` が `192.168.105.28`（内部 Web サーバー）に等しい • `Port` が `443` に等しくない（非 HTTPS トラフィック）、 • `Connected_port` が `443` に等しくない（非 HTTPS トラフィック）、 • `Packets_from` が 11 以上（接続成功、トラフィック通過）、かつ • `Packets_to` が 11 以上（接続成功、トラフィック通過）

説明	構文例	返される結果
リモート デスクトップ アプリケーションに関連する接続	`Port: ("23" OR "3389" OR ["5800" TO "5803"] OR ["5900" TO "5903"] OR ["6000" TO "6063"]) AND NOT Connected_port: ["0" TO "1023"] AND Packets_from: [ "10" TO * ] AND Packets_to: [ "10" TO * ]`	以下のすべてのイベント: • `Port` が 23、3389、5800 ～ 5803、5900 ～ 5903、または 6000 ～ 6063 に等しい(共通のリモート デスクトップ アプリケーション ポート)、 • `Connected_port` が 0 ～ 1023 に等しくない(エフェメラル ポートを使用する接続)、 • `Packets_from` が 10以上(接続成功、トラフィック通過)、かつ • `Packets_to` が 10 以上(接続成功、トラフィック通過)

イベントビューアのネストされたフィールドの検索

イベントにサブフィールドを持つフィールドが含まれている場合は、ドット表記を使用してサブフィールドを指定することで、クエリフィルタでこれらのフィールド値を検索できます。

たとえば、品目エントリには、[クレデンシャル(Credentials)] と [問題(Issues)] の 2 つのサブフィールドを備えた [詳細(Details)] フィールドが含まれる場合があります。[クレデンシャル(Credentials)] フィールドで `username1` を検索する場合は、次のドット表記構文を使用します。

```
Details.credentials: "username1"
```

異なる推奨の特定のフィールドには、推奨タイプごとに異なるサブフィールドが含まれることがあります。

著作権情報