イベント分析

ここでは、次の内容について説明します。

アラーム

このタブには、さまざまなカテゴリに対して生成されたアラームが表示されます。このタブには、ID（オプション）、重大度、障害ソース、名前、カテゴリ、確認応答、作成時刻、最終更新日（オプション）、ポリシー、メッセージなどの情報が表示されます。このタブで [更新間隔（Refresh Interval）] を指定できます。1 つ以上のアラームを選択し、[ステータスの変更（Change Status）] ドロップダウンリストを使用して、アラームのステータスを確認または確認解除できます。また、1 つ以上のアラームを選択し、[削除（Delete）] ボタンをクリックしてアラームを削除できます。

発行されたアラーム

UI パス：**[操作（Operations）] > [イベント分析（Event Analytics）] > [アラーム（Alarms）]** の順に選択します。

1. 新しいアラーム ポリシーを作成した後、**[発生したアラーム（Alarms Raised）]** タブに移動し、**[更新（Refresh）]** アイコンをクリックして、作成したアラームを表示します。

   新しく作成されたアラームが表示されます。

2. [アラーム（Alarms）] テーブルの **[重大度（Severity）]** をクリックすると、同じ ITL/ITN フローで同じポリシーによって発生したアラームの履歴が表示されます。

3. **[ポリシー（Policy）]** 列の [ポリシー名（Policy name）] をクリックして、チャートを表示します。

   スライドイン ペインが表示され、内部にグラフが表示されます。

4. グラフを表示するには、ドロップダウン リストから必要な**メトリック**を選択します。

（注） これらのメトリックは、SAN Insights Anomaly Policy でのみ表示できます。

次の表では、**[操作（Operations）]>[イベント分析（Event Analytics）]>[アラーム（Alarms）]>[発生したアラーム（Alarms Raised）]** に表示されるフィールドについて説明します。

フィールド	説明
重大度	アラームの重大度を指定します
送信元	送信元の名前を指定します。
名前	アラームの名前を指定します。
カテゴリ	アラームのカテゴリを指定します。
作成時刻	アラームが作成された時刻を指定します。
ポリシー	アラームのポリシーを指定します。
Message	メッセージを表示します。
Ack User	アラームを確認したユーザのユーザ名。

次の表では、**[発行されたアラーム（Alarms Raised）]** タブに表示される **[アクション（Actions）]** メニュードロップダウンリストのアクション項目について説明します。

アクション項目	説明
確認応答あり	1つまたは複数のアラームを選択し、**確認**を選択します。アラームをブックマークし、**[確認済み（Acknowledged）]** の列にAck User名を追加できます。
未確認	1つまたは複数のアラームを選択し、**未確認**を選択して、ブックマークされたアラームを削除します。 （注） 確認済みアラームのみを未確認にすることができます。
クリア	アラームを選択し、**消去**を選択して、アラームポリシーを手動で消去します。 消去されたアラームは、**[消去されたアラーム（Alarm Cleared）]** タブに移動します。
アラームの削除	アラームを選択し、**削除**を選択してアラームを削除します。

クリアされたアラーム

UIパス：**操作 > イベント分析 > アラーム > クリアされたアラーム**

[クリアされたアラーム（Alarms Cleared）] タブには、**[発行されたアラーム（Alarms Raised）]** タブでクリアされたアラームのリストがあります。このタブには、ID（オプション）、重大度、障害ソース、名前、カテゴリ、確認応答、作成時刻、クリア時（オプション）、クリア

元、ポリシー、メッセージなどの情報が表示されます。最大 90 日間、クリアされたアラームの詳細を表示できます。

1 つ以上のアラームを選択し、**[アクション（Actions）] > [削除（Delete）]** をクリックしてそれらを削除できます。

次の表では、**[発行されたアラーム（Alarms Raised）]** タブに表示されるフィールドについて説明します。

フィールド	説明
重大度	アラームの重大度を指定します
送信元	送信元アラーム IP アドレスを指定します。
名前	アラームの名前を指定します。
カテゴリ	アラームのカテゴリを指定します。
作成時刻	アラームが作成された時刻を指定します。
クリアされた時間	アラームがクリアされた時刻を指定します。
クリアしたユーザ	アラームをクリアしたユーザを指定します。
ポリシー	アラームのポリシーを指定します。
Message	アラームの CPU 使用率およびその他の詳細を指定します。
Ack User	確認応答されたユーザ ロール名を指定します。

次の表では、**[発行されたアラーム（Alarms Raised）]** タブに表示される **[アクション（Actions）]** メニュードロップダウンリストのアクション項目について説明します。

アクション項目	説明
アラームの削除	アラームを選択し、**[削除（Delete）]** を選択して、クリアされたアラームを削除します。

アラーム ポリシーの監視と追加

SAN コントローラでアラームを有効にし、**[操作（Operations）]**>**[イベント分析（Analytics）]**> **[アラーム（Alarms）]**に移動し、垂直タブの **[アラーム ポリシー（Alarm Policies）]** をクリックします。[外部アラームの有効化]チェックボックスが選択されていることを確認します。これを有効にするには、 SAN Controller Server を再起動する必要があります。

SAN コントローラの登録済みSNMPリスナーにアラームを転送できます。Cisco SAN コントローラ Web UIから、**[設定（Settings）] > [サーバ設定（Server Settings）] > [アラーム（Alarms）]** を選択し、**[外部アラームの有効化（Enable external alarms）]** チェックボックスがオンになっていることを確認します。これを有効にするには、 SAN Controller Server を再起動する必要があります。

SAN コントローラの登録済みSNMPリスナーにアラームを転送できます。Cisco SAN コントローラ Web UIから、**[設定（Settings）] > [サーバ設定（Server Settings）] > [アラーム（Alarms）]** を選択し、alarm.trap.listener.address フィールドに外部ポート アドレスを入力し、**[変更の適用（Apply Changes）]** をクリックして、SAN コントローラを再起動します。

（注） **[アラーム ポリシーの作成（Alarm Policy creation）]** ダイアログ ウィンドウで **[転送（Forwarding）]** チェックボックスをオンにして、外部 SNMP リスナーへのアラームの転送を有効にします。

次の表では、**[操作（Operations）] > [イベント分析（Event Analytics）] > [アラーム（Alarms）] > [アラーム ポリシー（Alarms Policies）]** に表示されるフィールドについて説明します。

フィールド	説明
名前	アラーム ポリシーの名前を指定します
説明	アラーム ポリシーの名前を指定します
ステータス	アラーム ポリシーのステータスを指定します。 • アクティブ • 非アクティブ
ポリシータイプ	ポリシーのタイプを指定します。 • デバイスのヘルス ポリシー • インターフェイスのヘルス ポリシー • syslog アラームポリシー • SAN Insights の異常ポリシー
Devices	アラーム ポリシーを適用するデバイスを指定します。
インターフェイス	インターフェイスを指定します。
詳細	ポリシーの詳細を指定します。

次の表では、**[操作（Actions）]** メニュー ドロップダウン リストのアクション項目について説明します。この項目は、**[操作（Operations）] > [イベント分析（Event Analytics）] > [アラーム（Alarms）] > [アラーム ポリシー（Alarms Policies）]** に表示されます。

アクション項目	説明
新しいアラーム ポリシーの作成	新しいアラーム ポリシーを作成することを選択します。「新しいアラーム ポリシーの作成」の項を参照してください。
編集	アラーム ポリシーを編集するには、ポリシーを選択し、**[編集（Edit）]**を選択します。

アクション項目	説明
削除	アラーム ポリシーを削除するには、ポリシーを選択し、**[削除（Delete）]** を選択します。
アクティブ化（Activate）	アラーム ポリシーをアクティブ化して適用するには、ポリシーを選択し、**[アクティブ化（Activate）]**を選択します。
非アクティブ化	アラーム ポリシーを無効にして非アクティブにするには、ポリシーを選択し、**[非アクティブ化（Deactivate）]** を選択します。
インポート	.csv ファイルからアラーム ポリシーを一括でインポートする場合に選択します。
エクスポート	アラーム ポリシーを .csv ファイルから一括でエクスポートする場合に選択します。

次のアラーム ポリシーを追加できます。

- **デバイス ヘルス ポリシー**：デバイス ヘルス ポリシーを使用すると、デバイス ICMP到達不能、デバイス SNMP 到達不能、またはデバイス SSH 到達不能の場合にアラームを作成できます。また、これらのポリシーを使用すると、シャーシの温度、CPU、およびメモリの使用状況をモニタできます。
- **インターフェイス ヘルス ポリシー**：インターフェイス ヘルス ポリシーを使用すると、インターフェイスのアップまたはダウン、パケット廃棄、エラー、帯域幅の詳細をモニタできます。デフォルトでは、すべてのインターフェイスがモニタリングのために選択されています。
- **Syslog アラーム ポリシー**：Syslog アラーム ポリシーは、Syslog メッセージ形式のペアを定義します。 1 つはアラームを発生させ、もう 1 つはアラームをクリアします。
- **San Insights Anomaly Policy**：San Insights Anomaly Policy では、SAN Insight データを使用して、ファブリック内の問題を特定するためのカスタマイズされたアラームを作成できます。

新しいアラーム ポリシーの作成

次のアラーム ポリシーを追加できます。

- デバイスのヘルス ポリシー
- インターフェイスのヘルス ポリシー
- syslog アラームポリシー
- SAN Insights の異常ポリシー

デバイスのヘルス ポリシー

デバイスヘルスポリシーを使用すると、デバイス ICMP 到達不能、デバイス SNMP 到達不能、またはデバイス SSH 到達不能の場合にアラームを作成できます。また、これらのポリシーを使用すると、シャーシの温度、CPU、およびメモリの使用状況をモニタできます。

ポリシーを作成するデバイスを選択します。ポリシー名、説明、CPU使用率パラメータ、メモリ使用率パラメータ、環境温度パラメータ、デバイスの可用性、およびデバイス機能を指定します。**[デバイス機能（Device Features）]** で、BFD、BGP、および HSRP プロトコルを選択できます。これらのチェックボックスをオンにすると、**BFD**-ciscoBfdSessDown、ciscoBfdSessUp、**BFD**-bgpEstablishedNotification、bgpBackwardTransNotification、cbgpPeer2BackwardTransition（）、cbgpPeer2EstablishedNotification、および **HSRP**-cHsrpStateChange のアラームがトリガーされます。トラップ OID 定義の詳細については、「https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do」を参照してください。

インターフェイスのヘルス ポリシー

インターフェイス ヘルス ポリシーを使用すると、インターフェイスのアップまたはダウン、パケット廃棄、エラー、帯域幅の詳細をモニタできます。デフォルトでは、すべてのインターフェイスがモニタリングのために選択されています。

ポリシーを作成するデバイスを選択し、次のパラメータを指定します。

- ポリシー名：このポリシーの名前を指定します。一意の名前を指定する必要があります。
- 説明：このポリシーの簡単な説明を指定します。
- 転送：Cisco Nexus Dashboardファブリックコントローラ SANコントローラの登録済みSNMPリスナーにアラームを転送できます。 Web UI から、**[設定（Settings）] > [サーバ設定（Server Settings）] > [イベント（Events）]** を選択します。

（注） [アラーム ポリシーの作成（Alarm Policy creation）] ダイアログ ウィンドウで **[転送（Forwarding）]** チェックボックスをオンにして、外部 SNMP リスナーへのアラームの転送を有効にします。

- 電子メール：アラームが作成、クリア、または重大度が変更されたときに、アラームイベントの電子メールを受信者に転送できます。 SAN コントローラ Web UI から、**[設定（Settings）] > [サーバ設定（Server Settings）] > [イベント（Events）]** を選択します。SMTPパラメータを設定し、**[保存（Save）]** をクリックして、SAN コントローラ サービスを再起動します。
- リンクステート：リンクステートオプションを選択して、インターフェイスリンクのアップまたはダウンを確認します。リンクダウンの場合、アラームを発生させることができ、リンクアップでアラームをクリアできます。
- 帯域幅（イン/アウト）：
- インバウンドエラー

- アウトバウンドエラー
- インバウンド破棄
- アウトバウンド破棄

Syslog アラーム

Syslog アラーム ポリシーは、Syslog メッセージ形式のペアを定義します。 1 つはアラームを発生させ、もう 1 つはアラームをクリアします。

ポリシーを作成するデバイスを選択し、次のパラメータを指定します。

- デバイス：このポリシーの範囲を定義します。このポリシーを適用する個々のデバイスまたはすべてのデバイスを選択します。
- ポリシー名：このポリシーの名前を指定します。一意の名前を指定する必要があります。
- 説明：このポリシーの簡単な説明を指定します。
- 転送：Cisco Nexus Dashboardファブリックコントローラ SANコントローラの登録済みSNMP リスナーにアラームを転送できます。 Web UI から、**[設定（Settings）] > [サーバ設定（Server Settings）] > [イベント（Events）]** を選択します。

（注） [アラーム ポリシーの作成（Alarm Policy creation）] ダイアログ ウィンドウで**[転送（Forwarding）]**チェックボックスをオンにして、外部 SNMP リスナーへのアラームの転送を有効にします。

- 電子メール：アラームが作成、クリア、または重大度が変更されたときに、アラームイベントの電子メールを受信者に転送できます。 SAN コントローラ Web UI から、**[設定（Settings）] > [サーバ設定（Server Settings）] > [イベント（Events）]** を選択します。 SMTPパラメータを設定し、**[保存（Save）]** をクリックして、SAN コントローラ サービスを再起動します。
- 重大度：この syslog アラーム ポリシーの重大度レベルを定義します。選択肢は、Critical、Major、Minor、および Warning です。
- 識別子：発生およびクリア メッセージの識別子部分を指定します。
- Raise Regex：syslog 発生メッセージの形式を定義します。構文は次のとおりです。 Facility-Severity-Type：メッセージ
- Clear Regex：syslog クリア メッセージの形式を定義します。構文は次のとおりです。 Facility-Severity-Type：メッセージ

正規表現の定義は単純な式ですが、完全な正規表現ではありません。テキストの可変領域は、$(LABEL) 構文を使用して示されます。各ラベルは、1 つ以上の文字に対応する正規表現キャプチャ グループ（.+）を表します。2 つのメッセージを関連付けるために、raise メッセージと clear メッセージの両方にある可変テキストが使用されます。識別子は、両方のメッセージに表

示される1つ以上のラベルのシーケンスです。識別子は、ckear syslogメッセージをアラームを発生させたsyslogメッセージと照合するために使用されます。テキストがメッセージの1つだけに表示される場合は、ラベルを付けて識別子から除外できます。

例：「値」が「ID1-ID2」のポリシー

```
"syslogRaise": "SVC-5-DOWN: $(ID1) module $(ID2) is down $(REASON)"
"syslogClear": "SVC-5-UP: $(ID1) module $(ID2) is up."
```

この例では、ID1 および ID2 ラベルをアラームとして検出するための識別子としてマークできます。この識別子は、対応するsyslogメッセージで見つかります。ラベル「REASON」は昇格ですが、クリアメッセージにはありません。このラベルは、アラームをクリアするsyslogメッセージに影響しないため、識別子から除外できます。

表 *1*：例 *1*

識別子	ID1-ID2
正規表現を上げる	ETHPORT-5-IF_ADMIN_UP：インターフェイス Ethernet15/1 で admin が起動されています。
正規表現のクリア	ETHPORT-5-IF_DOWN_NONE：インターフェイス Ethernet15/1 がダウンしています（トランシーバ欠落）

上記の例では、正規表現は端末モニタに表示される syslog メッセージの一部です。

表 *2*：例 *2*

Identifier	ID1-ID2
正規表現を上げる	ETH_PORT_CHANNEL-5-PORT_DOWN：$（ID1）：$（ID2）がダウンしています
Clear Regex	ETH_PORT_CHANNEL-5-PORT_UP：$（ID1）：$（ID2）が起動しています

表 *3*：例 *3*：

Identifier	ID1-ID2
正規表現を上げる	ETHPORT-5-IF_SFP_WARNING：Interface $（ID1）、High Rx Power Warning
Clear Regex	ETHPORT-5-IF_SFP_WARNING：Interface $（ID1）、High Rx Power Warning clear

エンドポイント ロケータ アラーム

アラームは、エンドポイントロケータ（EPL）によって外部アラームカテゴリに登録および作成されます。

アラームポリシー

EPL 外部アラームカテゴリポリシーは、ファブリックで EPL が有効になっているときにアクティブになります。アラームは、重複する IP アドレス、重複する MAC アドレス、VRF に表示されるエンドポイント、VRFから消えるエンドポイント、ファブリック内で移動するエンドポイント、ルートリフレクタ接続の喪失、ルートリフレクタ接続の復元などの問題に対して発生します。問題に応じて、アラームポリシーの重大度レベルはCRITICAL またはMINOR になります。

アラームは、次のイベントに対して発生し、CRITICAL に分類されます。

- ルートリフレクタの切断
- 重複する IP アドレスの検出
- 重複する MAC アドレスの検出

次のイベントの場合、アラームが発生し、MINOR として分類されます。

- エンドポイントの移動
- ファブリック内の新しい VRF の表示
- ファブリック内のエンドポイントの数が 0 になる
- VRF のエンドポイントの数が 0 になる
- スイッチからのすべてのエンドポイントの消失
- ルートリフレクタ（RR）の接続

状態が修正されると、CRITICALアラームは自動的にクリアされます。たとえば、NDFC と RR 間の接続が失われると、CRITICAL アラームが生成されます。このアラームは、NDFC と RR 間の接続が回復すると自動的にクリアされます。その他の MINOR アラームは、アラームが生成されてから 30 分が経過すると自動的にクリアされます。

Note 状態が解決されたら、重複する MAC および重複する IP アラームをクリアする必要があります。

[イベント分析（Event Analytics）] > [アラーム（Alarm）] > [アラームポリシー（Alarm Policies）] を選択して、EPL アラームポリシーを表示します。これらのアラームポリシーは、Web UI では編集できません。**[アクション（Actions）] > [アクティブ化（Activate）]** または **[非アクティブ化（Disactivate）]** を選択して、選択したポリシーをアクティブ化または非アクティブ化します。

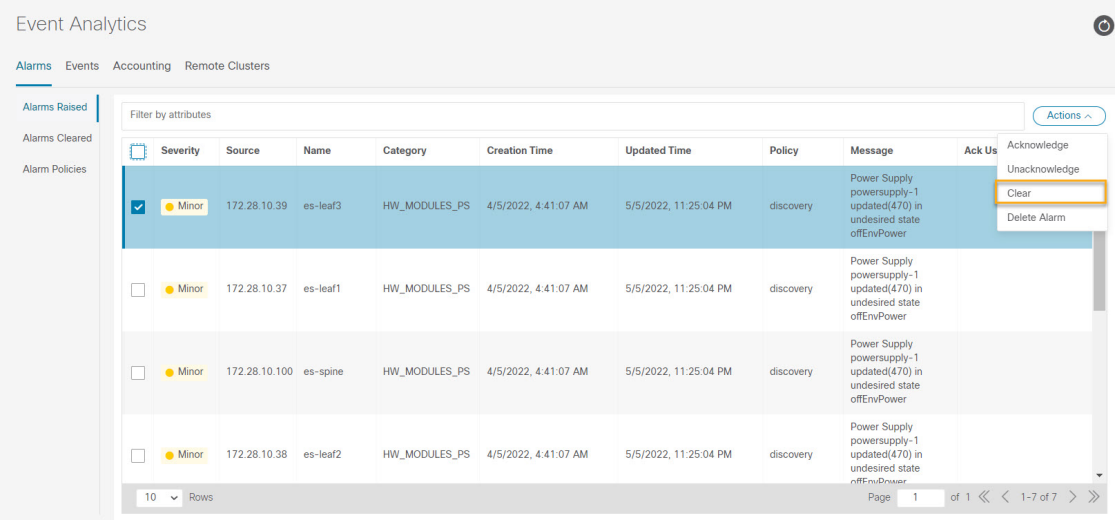
NDFC Web UI を使用してアラームポリシーが削除された場合、そのポリシーに対して作成またはクリアされたアラームは、**[イベント分析（Event Analytics）]>[アラーム（Alarm）]>[アラームポリシー（Alarm Policy）]** タブに表示されません。ポリシーを削除するには、ポリシーの横にあるチェックボックスをオンにして、**[削除（Delete）]** をクリックします。ただし、NDFC Web UI からはポリシーを削除しないことをお勧めします。ファブリックが削除される

と、アラームポリシーとそのファブリック内のデバイスのすべてのアクティブアラームが削除されます。

エンドポイントロケータ：アクティブアラーム

[イベント分析（Event Analytics）] > [アラーム（Alarm）] > [発生したアラーム（Alarms Raised）] を選択して、アクティブなアラームを表示します。

アクティブなアラームをクリアするには、アラームの横にあるチェックボックスを選択し、**[アクション（Actions）] > [クリア（Clear）]** をクリックします。

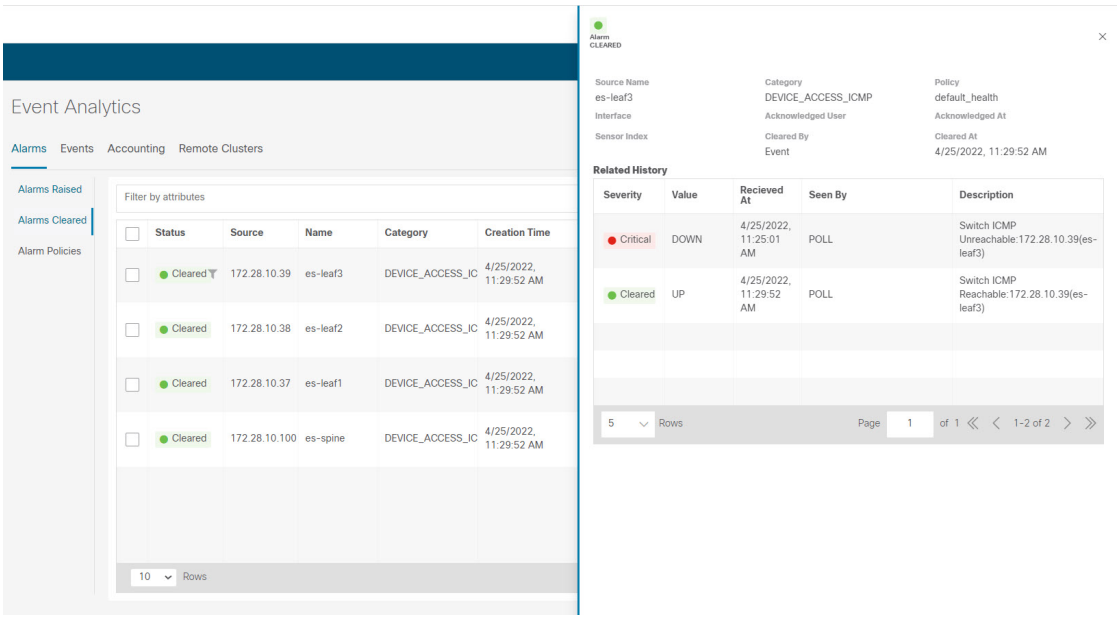


アクティブなアラームを削除するには、アラームの横にあるチェックボックスを選択し、**[アクション（Actions）] > [削除（Delete）]** をクリックします。

エンドポイントロケータ：クリアされたアラーム

クリアされたアラームを表示するには、**[イベント分析（Event Analytics）] > [アラーム（Alarms）] > [クリアされたアラーム（Alarms Cleared）]** に移動します。

必要な **[クリア済み（Cleared）]** ステータス列をクリックして、必要なアラームに関する詳細情報を表示します。



クリアされたアラームのリストからクリアされたアラームを削除するには、アラームの横にあるチェックボックスを選択し、**[アクション（Actions）]**>**[削除（Delete）]**をクリックします。

アラームとポリシーの詳細については、「アラーム, on page 1」を参照してください。

San Insights Anomaly ポリシー

Cisco Nexus Dashboard SAN コントローラ リリース 12.0(1) から、新しいポリシータイプ saninsights が追加されました。この新しいポリシータイプは、問題を特定するためにカスタマイズできます。分析のために間隔データごとに保持する特定のフローに基づいて、アラームポリシーを作成できます。選択したフローがアラームポリシーと一致する場合は、ポリシーで定義されたパラメータに基づいてフローを維持します。

手順

ステップ 1 **[操作（Operations）]** > **[イベント分析（Event Analytics）]** > **[アラーム（Alarms）]**の順に選択します。

ステップ 2 **[アラーム（Alarms）]** タブで **[アラーム ポリシー]** を選択します。

ステップ 3 **[アクション（Actions）]** > **[新規アラーム ポリシーの作成（Create new alarm policy）]**の順に選択します。

ステップ 4 **[San Insights の異常ポリシー（San Insights Anomaly Policy）]** オプションボタンを使用します。

ステップ 5 次のパラメータの詳細を指定します。

- **[ポリシー名（Policy Name）]**：このポリシーの名前を指定します。一意の名前を指定する必要があります。
- **[説明（Description）]**：ポリシーの簡単な説明。
- **[転送（Forwarding）]**：外部 SNMP リスナーへの転送アラームを有効にします。

- **[電子メール（Email）]**：このポリシーのメール更新をメール ID に送信するには、チェックボックスを選択します。

ステップ 6 ドロップダウン リストから時間を選択して、**キャプチャ時間**と**保持時間**を定義します。

- **[キャプチャ時間（Capture Time）]**：特定のポリシーに一致する各フローの間隔ごとのデータをキャプチャする時間の長さを指定します。
- **[保持時間（Retention Time）]**：（削除する前に）そのデータを保持する時間の長さを指定します。

ステップ 7 ドロップダウン リストから時間または間隔を選択して**分析レベル**を定義し、ドロップダウン リストから**重大度**レベルを選択してこのポリシーの重大度を定義します。

- **[分析レベル（Analysis Level）]**：特定のポリシーでチェックする必要があるフローデータの集約を指定します。中止ポリシーや失敗ポリシーなどの一部のポリシータイプは、即座に発生する場合に照合するロジックです（間隔レベル）。一部のポリシータイプは、しきい値を超えて維持されると異常ポリシーとして表示されます。たとえば、レベルの瞬間的な ECT または DAL のスパイクはアラームではありませんが、同じスパイク レベルが一定期間（5 分または 1 時間）続く場合は、調査する必要があります。
- **[重大度（Severity）]**：このポリシーが原因で発生するアラームに関連付けられる重大度を指定します。

ステップ 8 新しいルールを定義し、**[新規ルールの追加（Add new rule）]** をクリックして必須フィールドを指定し、**[新規ポリシーの作成（Create new policy）]** をクリックします。

（注）
- 1つ以上の新しいルールと一致基準を定義して、フローを識別し、新しいポリシーを作成できます。
- すべてのポリシーは、スイッチからレシーバにストリーミングされる各 ITL/ITN フロー レコードと照合されます。

作成されたアラームは、**[アラーム（Alarms）]** タブで確認できます。

イベント

このタブには、スイッチに対して生成されたイベントが表示されます。このタブには、Ack、確認済みユーザ、グループ、スイッチ、重大度、ファシリティ、タイプ、カウント、最終確認、説明などの情報が表示されます。1つ以上のイベントを選択し、[ステータスの変更（Change Status）] ドロップダウン リストを使用して、そのステータスを確認または確認解除できます。また、1 つ以上のアラームを選択し、[削除（Delete）] ボタンをクリックしてアラームを削除できます。すべてのイベントを削除する場合は、[すべてを削除（Delete All）] ボタンをクリックします。

次の表で、**[操作（Operations）] > [イベント分析（Event Analytics）] > [イベント（Events）]** に表示されるフィールドについて説明します。

フィールド	説明
グループ	ファブリックを指定します。
スイッチ	スイッチのホスト名を指定します。
重大度	イベントの重大度を指定します。
施設	イベントを作成するプロセスを指定します。 イベント ファシリティには、NDFC と syslog ファシリティとの 2 つのカテゴリがあります。 Nexusダッシュボードファブリック コントローラ ファシリティは、Nexusダッシュボード ファブリック コントローラ 内部サービスによって生成されたイベントと、スイッチによって生成された SNMP トラップを表します。syslog ファシリティは、syslog メッセージを作成したマシン プロセスを表します。
タイプ	スイッチ/ファブリックの管理方法を指定します。
数	イベントが発生した回数を提供します。
作成時刻	イベントが作成された時刻を指定します。
前回の検出	イベントが最後に実行された時刻を指定します。
説明	イベントに提供される説明を指定します。
Ack	イベントを確認するかどうかを指定します。

次の表では、**[操作（Actions）]** メニュー ドロップダウン リストで、**[操作（Operations）] > [イベント分析（Event Analytics）] > [イベント（Events）]** に表示されるアクション項目について説明します。

アクション項目	説明
確認応答あり	テーブルから 1 つ以上のイベントを選択し、**[確認（Acknowledge）]**アイコンを選択して、ファブリックのイベント情報を確認します。 ファブリックのイベントを確認すると、確認アイコンが [グループ（Group）] の横の [Ack] 列に表示されます。
未確認	テーブルから 1 つ以上のイベントを選択し、**[確認解除（Unacknowledge）]** アイコンを選択して、ファブリックのイベント情報を確認します。

アクション項目	説明
削除	イベントを選択し、**[削除（Delete）]** をクリックします。
イベントのセットアップ	では新しいイベントを設定できます。詳細については、イベントのセットアップ （15 ページ）を参照してください。

イベントのセットアップ

Cisco Nexusダッシュボード ファブリック コントローラ Web UI を使用してイベントを設定するには、次の手順を実行します。

手順

ステップ 1 **[操作（Operations）] > [イベント分析（Event Analytics）] > [イベントのセットアップ（Event Setup）]** の順に選択します。**[アクション（Actions）]** ドロップダウン メニューから、**[イベントのセットアップ（Event Setup）]** を選択します。

ステップ 2 [レシーバ（Receiver）] タブで、次の手順を実行します。

a) この機能を有効にするには、トグル ボタンを使用します。

b) **[Syslog メッセージを DB にコピー（Copy Syslog Messages to DB）]**を選択し、**[適用（Apply）]** をクリックして syslog メッセージをデータベースにコピーします。このオプションを選択しない場合、イベントは Web クライアントのイベント ページに表示されません。2 番目のテーブルの列には、次の情報が表示されます。

- トラップを送信するスイッチ
- syslog を送信するスイッチ
- syslog アカウンティングを送信するスイッチ
- 遅延トラップを送信するスイッチ

c) [送信元（Sources）] タブのテーブルには、関連付けられているファブリックとスイッチが表示されます。また、トラップと syslog に関する情報も表示されます。

ステップ 3 Cisco Nexusダッシュボード ファブリック コントローラ Web UI からシステムメッセージの通知転送を追加および削除するには、次の手順を実行します。

Cisco Nexusダッシュボード ファブリック コントローラ Web UI は、電子メールまたは SNMPv1 トラップを介してファブリック イベントを転送します。一部の SMTP サーバでは、Nexusダッシュボード ファブリック コントローラ から SMTP サーバに送信される電子メールに認証パラメータを追加する必要があります。Nexusダッシュボード ファブリック コントローラ により認証を必要とする任意の SMTP サーバに送信される電子メールに認証パラメータを追加できます。この機能は、**[設定（Settings）] > [サーバ設定（Server Settings）] > [イベント（Events）]** タブで有効にします。

a) **[設定（Settings）] > [サーバ設定（Server Settings）] > [イベント（Events）]** を選択します。イベント転送を有効にするには、**[イベント転送を有効にする（Enable Event forwarding）]** チェックボックスをオンにします。イベントの転送範囲、レシーバの電子メールアドレス、イベントの重大度、およびイベントのタイプが表示されます。説明の [正規表現（Regex）] フィールドは、転送送信元がイベント フォワーダの追加時に転送元が Syslog として選択されている場合にのみ適用されます。

b) **SMTP サーバ**の詳細と**送信元**電子メールアドレスを指定します。**スヌーズ**および**イベント カウント** フィルタを設定します。

c) **[Save（保存）]** をクリックします。

d) **[操作（Operations）] > [イベント分析（Event Analytics）]** の順に選択します。[操作（Actions）] ドロップダウン リストから **[ルールの追加（Add Tags）]** を選択します。

e) [転送メソッド（Forwarding Method）] で、**[電子メール]** または **[トラップ（Trap）]** を選択します。

[トラップ（Trap）] を選択した場合は、ダイアログボックスに **[アドレス（Address）** と **[ポート（Port）]** フィールドが追加されます。

f) **電子メール**転送メソッドを選択する場合は、[電子メールアドレス（Email Address）]フィールドに IP アドレスを入力します。**トラップ**メソッドを選択する場合は、[アドレス（Address）] フィールドにトラップ レシーバの IP アドレスを入力し、ポート番号を指定します。

[アドレス（Address）] フィールドに IPv4 または IPv6 アドレスまたは DNS サーバ名を入力できます。

g) **[ファブリック（Fabric）]** フィールドで、通知するすべてのグループまたは特定のファブリックを選択します。SAN インストーラの場合は、**[VSAN 範囲（VSAN Scope）]** を選択します。**[すべて（All）]** または **[リスト（List）]** オプションを選択できます。リストを選択した場合は、通知用の VSAN のリストを指定します。

h) [送信元] フィールドで、Nexusダッシュボード ファブリック コントローラ または **[Syslog]** を選択します。

- Nexusダッシュボード ファブリック コントローラ を選択すると、次のようになります。
  1. **[タイプ（Type）]** ドロップダウン リストから、イベント タイプを選択します。
  2. **[ストレージ ポートのみ（Storage Ports Only）]** チェックボックスをオンにして、ストレージ ポートのみを選択します。
  3. **[最低重大度（Minimum Severity）]** ドロップダウン リストで、受信するメッセージの重大度を選択します。
  4. **[追加（Add）]** をクリックして、通知を追加します。

- [Syslog] を選択した場合：
  1. **[ファシリティ（Facility）]** リストから、syslog のファシリティを選択します。
  2. syslog **タイプ**を指定します。

3. **[説明の正規表現（Description Regex）]** フィールドで、イベントの説明と一致する説明を指定します。
4. **[最低重大度（Minimum Severity）]** ドロップダウン リストで、受信するメッセージの重大度を選択します。
5. **[追加（Add）]** をクリックして、通知を追加します。

（注） [最低重大度（Minimum Severity）] オプションは、[イベント タイプ（Event Type）] が **[すべて（All）]** に設定されている場合のみ使用できます。

Cisco Nexusダッシュボード ファブリック コントローラが送信するトラップは、重大度タイプに対応しています。重大度タイプとともにテキストによる説明も提供されます。

```
trap type(s) = 40990 (emergency)
40991 (alert)
40992 (critical)
40993 (error)
40994 (warning)
40995 (notice)
40996 (info)
40997 (debug)
textDescriptionOid = 1, 3, 6, 1, 4, 1, 9, 9, 40999, 1, 1, 3, 0
```

i) [ルールの追加（Add Rule）] をクリックします。

ステップ 4 Cisco Nexusダッシュボード ファブリック コントローラ Web UI からイベント抑制にルールを追加するには、次の手順を実行します。

Cisco Nexusダッシュボード ファブリック コントローラ では、ユーザ指定のサプレッサ ルールに基づいて、指定されたイベントを抑制することができます。このようなイベントは、Cisco Nexusダッシュボード ファブリック コントローラ Web UIおよび SAN クライアントには表示されません。イベントは Nexusダッシュボード ファブリック コントローラ データベースに保持されず、電子メールまたは SNMP トラップを介して転送されません。

テーブルからサプレッサ ルールを表示、追加、変更、および削除できます。既存のイベント テーブルからサプレッサ ルールを作成できます。テンプレートとして特定のイベントを選択し、ルール ダイアログ ウィンドウを呼び出します。イベントの詳細は、イベント テーブルで選択したイベントから、ルール作成ダイアログ ウィンドウの入力フィールドに自動的に移植されます。

（注） Cisco Nexusダッシュボード ファブリック コントローラ Web UI から EMC Call Home イベントを抑制することはできません。

a) ルールの**名前**を指定します。
b) イベント送信元に基づくルールに必要な **[範囲（Scope）]** を選択します。

[範囲（Scope）] ドロップダウン リストには、LAN グループとポート グループが個別に表示されます。**[SAN/LAN]**、**[ポート グループ（Port Groups）]**、または **[任意（Any）]** を選択できます。SAN および LAN の場合は、ファブリックまたはグループまたはスイッチ レベルでイベントの範囲を選択します。ポート グループ スコープのグループのみを選択で

きます。範囲として**[任意（Any）]**を選択すると、サプレッサ ルールがグローバルに適用されます。

c) **ファシリティ**名を入力するか、SAN/LAN スイッチ イベント ファシリティ リストから選択します。

ファシリティを指定しない場合は、ワイルドカードが適用されます。

d) ドロップダウン リストから**[イベント タイプ（Event Type）]**を選択します。

イベント タイプを指定しない場合は、ワイルドカードが適用されます。

e) **[説明の照合（Description Matching）]**フィールドで、一致する文字列または正規表現を指定します。

ルール照合エンジンは、Javaパターン クラスでサポートされている正規表現を使用して、イベントの説明テキストとの一致を検索します。

f) **[アクティブ範囲（Active Between）]**ボックスをオンにして、イベントが抑制される有効な時間範囲を選択します。

デフォルトでは、時間範囲は有効になっていません。つまり、ルールは常にアクティブです。

（注） 一般に、アカウンティング イベントを抑制しないでください。アカウンティング イベントの抑制ルールは、アカウンティング イベントが Nexusダッシュボード ファブリック コントローラ またはソフトウェアのスイッチのアクションによって生成される特定のまれな状況でのみ作成できます。たとえば、Nexusダッシュボード ファブリック コントローラと管理対象スイッチ間のパスワード同期中に、多数の「sync-snmp-password」AAA syslog イベントが自動的に生成されます。アカウンティング イベントを抑制するには、[サプレッサ（Suppressor）] テーブルに移動し、[イベント サプレッサ ルールの追加（Add Event Suppressor Rule）] ダイアログ ウィンドウを呼び出します。

g) [ルールの追加（Add Rule）] をクリックします。

アカウンティング

Cisco Nexusダッシュボード ファブリック コントローラ Web UI でアカウンティング情報を表示できます。

次の表では、**[操作（Operations）] > [イベント分析（Event Analytics）] > [アカウンティング（Accounting）] >** に表示されるフィールドについて説明します。

フィールド	説明
ソース（Source）	送信元 SGT を指定します。
User Name	ユーザ名を指定します。

フィールド	説明
時間	イベントが作成された時刻を指定します。
説明	説明を表示します。
グループ	グループの名前を指定します。

次の表では、**[操作（Actions）]**ドロップダウンリストのアクション項目について説明します。これらの項目は、**[操作（Operations）] > [イベント分析（Event Analytics）] > [アカウンティング（Accounting）]** に表示されます。

アクション項目	説明
削除	リストからアカウンティング情報を削除するには、行を選択して**[削除（Delete）]** を選択します。

リモートクラスタ

このタブには、セットアップの各クラスタ内のクラスタとファブリックの数が表示されます。

クラスタ名をクリックして概要情報を表示します。起動アイコンをクリックして、クラスタの詳細な概要を表示できます。