イベント分析、リリース 12.1.3

目次

新機能と更新情報

次の表は、この最新リリースまでの主な変更点の概要を示したものです。ただし、今リリースまでの変更点や新機能の一部は表に記載されていません。

リリース バージョン	特長	説明
NDFC リリース 12.1.3	整理し直したコンテンツ	このドキュメント内のコンテンツは元来 *『Cisco NDFC-Fabric Controller Configuration Guide』* または *『Cisco NDFC-SAN Controller Configuration Guide』* で提供されました。 リリース 12.1.3 以降、このコンテンツは現在、このドキュメントでのみ提供されており、これらのドキュメントでは提供されなくなっています。

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. アラームによってトリガーされたアラーム ポリシーを表示するには、[発生したアラーム（Alarms Generated）] タブをクリックします。
2. **[ID]** 列のリンクをダブルクリックして、選択した**アラーム ID** の [アラーム ID（Alarm ID）] ページを開きます。

   このページには、選択したアラーム ID の詳細が表示され、関連するソースで発生したアラームの履歴も表示されます。

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
ID	アラームの ID を指定します。
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。
Message	メッセージを表示します。
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。
更新時刻	アラームが更新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。
Ack User	アラームを確認したユーザーのユーザー名。

次の表では、[アクション（**Actions**）] メニューのドロップダウン リストにある、**[発生したアラーム（Alarms Raised）]** タブ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	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。
アクション項目	**説明**
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。  確認済みアラームのみを未確認にすることができます。
Clear	1 つまたは、複数のアラームを選択し、**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（Delete）]** 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、識別子、シビラティ（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、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**
ID	アラームの識別子を指定します。
ステータス	アラームのステータスが **[クリア済み（Cleared）]** であることを示します。
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。
メッセージ	アラームの CPU 使用率およびその他の詳細を指定します。
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。
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、**[アクション（Actions）]** メニューのドロップダウン リストにある、**[アラームのクリア（Alarms Cleared）]** タブに移動します。

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

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 コントローラ サーバーを再起動する必要があります。

アラームを SAN コントローラ の登録済み SNMP リスナーに転送できます。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 コントローラ サーバーを再起動する必要があります。

アラームを SAN コントローラ の登録済み SNMP リスナーに転送できます。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。

[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 • インターフェイス正常性 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、**[アクション（Actions）]** メニューのドロップダウン リストにある、

[オペレーション（Operations）] > [イベント 分析（Event Analytics）] > [アラーム（Alarm）] > [アラーム ポリシー（Alarm Policies）]のアクション アイテムを表します。

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（Create new alarm policy）] 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。
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化するには、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	txt ファイルからアラーム ポリシーをインポートする場合に選択します。
エクスポート	• 特定のアラーム ポリシーの横にあるボックスをクリックし、[エクスポート（Export）] をクリックして、そのアラーム ポリシーを .txt ファイルとしてエクスポートします。 • アラーム ポリシーの横にあるすべてのボックスを選択または選択解除し、**[エクスポート（Export）]** をクリックして、すべてのアラーム ポリシーを .txt ファイルとしてエクスポートします。

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 SNMP 到達不能、またはデバイス SSH 到達不能または、周辺機器が使用不可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 インサイトの異常ポリシー**：San インサイトの異常ポリシーでは、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。

  Cisco Nexus Dashboard SAN コントローラ リリース 12.1.2e から、デフォルトでは **[非アクティブ（Not Active）]** 状態になっている事前プロビジョニングされた SAN インサイト 異常ポリシーの

データを変更、アクティブ化、または使用できます。

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
- インターフェイス正常性 ポリシー
- syslog アラームポリシー

- SAN Insights の異常ポリシー

新しいアラーム ポリシーを作成した後、**[アラーム ポリシー（Alarms Policies）]** タブ内で**[更新（Refresh）]** をクリックして、作成した新しいアラーム ポリシーを表示します。

デバイスの正常性ポリシー

デバイス正常性ポリシーを使用すると、特定の条件が満たされたときにアラームを作成できます。デフォルトでは、すべてのデバイスがモニタリングのために選択されています。

- **[ポリシー名**（Policy Name）]：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 Fabric Controller 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）] > [サーバー設定（Server Settings）] > [イベント（Events）] を選択します**。

  外部 SNMP リスナーにアラームを転送するため、アラーム ポリシーを構成する間、[転送（Forwarding）] チェックボックスを選択すること確認します。

- **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。Cisco Nexus Dashboard ファブリック コントローラ Web UI から、**[設定（Settings）] > [サーバー設定（Server Settings）] > [イベント（Events）]** を選択します。SMTPパラメータを構成し、**[保存（Save）]** をクリックして、Cisco Nexus ダッシュボード ファブリック コントローラ サービスを再起動します。
- CPU 使用率パラメータ、 メモリ使用率パラメータと環境温度パラメータを指定します。
- **デバイスの可用性**：デバイスの正常性ポリシーを使用すると、次の状況でアラームを作成できます。
  - **[デバイス アクセス**（Device Access）]：デバイス SNMP またはデバイス SSH に到達できない場合。
  - **周辺機器**：ファン、電源、またはモジュールに到達できない場合。

    詳細なトラップ OID 定義については、https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.doを参照してください。

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。

インターフェイスのヘルス ポリシー

インターフェイス 正常性 ポリシーは、インターフェイスのインターフェイス ステータス、パケット破棄、エラーと使用状況の詳細をモニタリングすることを許可します。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**（Policy Name）]：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：[設定（Settings）] > [サーバー設定（Server Settings）] > [アラーム（Alarms）]** タブで送信者と受信者の電子メール アドレスを設定することで、**Cisco Nexus Dashboard Fabric Controller** の登録済み **SNMP** リスナーにアラームを転送できます。

  外部 SNMP リスナーにアラームを転送するため、アラーム ポリシーを構成する間、**[転送（Forwarding）]** チェックボックスを選択すること確認します。

- **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。Cisco Nexus Dashboard Fabric Controller Web UI から、**[設定（Settings）] > [サーバー設定（Server Settings）] > [SMTP]** の順に選択し、SMTP パラメータを設定して、Cisco Nexus Dashboard Fabric Controller 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 リンクのステータスを確認します。リンクがダウンするたびにアラームを生成し、リンクがアップのときにアラームをクリアできます。
- **[帯域幅（着信/発信）（Bandwidth (In/Out)）]**：着信方向と発信方向で許可される最大帯域幅を設定できます。帯域幅が指定された値を超えると、アラームが生成されます。
- **[インターフェイス電力（Rx/Tx）（Interface Power (Rx/Tx)）]**：[送信電力（Tx Power）] および [受信電力（Rx Power）] の警告下限しきい値を設定できます。しきい値が設定値を下回ると、アラームが生成されます。インターフェイスは 15 分ごとにモニターされます。
- **[インターフェイス電流（Interface Current）]**：電流の警告下限しきい値を設定できます。しきい値が設定値を下回ると、アラームが生成されます。インターフェイスは 15 分ごとにモニターされます。
- **[インターフェイス電圧（Interface Voltage）]**：電圧の警告下限しきい値を構成できます。しきい値が設定値を下回ると、アラームが生成されます。インターフェイスは 15 分ごとにモニターされます。
- **[インバウンドエラー（Inbound Errors）]**：アラームを生成するまでに廃棄されるインバウンド エラーの数のしきい値を設定できます。
- **[アウトバウンド エラー（Outbound Errors）]**：アラームを生成するまでに廃棄されるアウトバウンド エラーの数のしきい値を設定できます。
- **[インバウンド廃棄（Inbound Discards）]**：アラームを生成するまでに廃棄される着信パケット数のしきい値を設定できます。
- **[アウトバウンド廃棄数（Outbound Discards）]**：アラームを生成するまでに廃棄されるアウトバウンドパケット数のしきい値を設定できます。

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：アラームを SAN コントローラ の登録済み SNMP リスナーに転送できます。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。

[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パラメータを構成し、**[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: Message
- 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: Message

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。
Clear Regex	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

識別子	**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：

識別子	**ID1-ID2**
正規表現を上げる	ETHPORT-5-IF_SFP_WARNING: Interface $(ID1), 高 Rx 電力警告
Clear Regex	ETHPORT-5-IF_SFP_WARNING: Interface $(ID1), 高 Rx 電力警告がクリアされました

SAN Insights の異常ポリシー

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。

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。
2. **[アラーム（Alarms）]** タブで **[アラーム ポリシー（Alarms ）]** を選択します。
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。
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。
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識別子に送信するには、チェックボックスを選択します。**
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。**
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。**

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。

- 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 ファシリティと syslog ファシリティの 2 つのカテゴリがあります。Nexus Dashboard Fabric Controller 機能は、Nexus Dashboard Fabric Controller の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、**[アクション（Actions）]** メニューのドロップダウン リストにある、**[オペレーション（Operations)] > [イベント 分析（ Event Analytics）] > [イベント（Events）]**。

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。

アクション項目	説明
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。
削除	イベントを選択し、**[削除（Delete）]** をクリックします。
Add Suppressor	イベントを選択し、**[サプレッサーの追加（Add Suppressor）]** を選択してイベントにルールを追加します。ルールに名前を付けることができます。**[範囲（Scope）]** オプションを使用して、このルールをすべてのファブリック、特定の要素、またはすべての要素に追加できます。
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、[イベントの設定（Event Setup）] を参照してください。

イベントのセットアップ

Cisco Nexus Dashboard Fabric Controller 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：

1. **[操作（Operations）] > [イベント分析（Event Analytics）]** を選択し、**[イベント（Events）]** タブをクリックします。
2. **[アクション (Actions)]** ドロップダウン リストから、**[イベント設定** (Event Setup)] を選択します。こ**[レシーバ（Reciever）]**のタブには、次の詳細情報が表示されます：
   - [**Syslog レシーバを有効化**]：syslog サーバーのステータスを表示します。
   - **[SNMP トラップ レシーバ（SNMP Trap Receive）]**：受信、処理、およびドロップされた SNMP トラップの詳細を表示します。
   - **[Syslog レシーバ（Syslog Receiver）]**：受信、処理、およびドロップされた syslog メッセージの詳細を表示します。
3. スイッチが syslog を自動的に構成し、syslog メッセージを NDFC サーバーに送信できるようにするには、次の手順を実行します：
   a. Cisco ファブリック サービス（CFS）がすべてのスイッチで無効になっていることを確認します。
   b. Cisco Nexus ダッシュボード ファブリック コントローラ内で**[設定（Settings）] > [サーバー設定（Server Settings）]**を選択します。
   c. **[イベント（Events）]** タブをクリックし、**[スイッチでの syslog の自動登録（Auto Registration of syslogs on Switch）]** チェックボックスをオンにします。

      デフォルトでは、この機能は無効になっています。syslog メッセージは、**[操作（Operations）] > [イベント分析（Event Analytics）] > [イベント（Events）]** ページで確認できます。NDFC は、5 分ごとにサーバーから syslog メッセージを収集します。

4. **[送信元（Sources）]** タブに移動して、ファブリックとそれに関連付けられているスイッチのリストを表示します。**送信元** タブは、全てをファブリックと関連したスイッチを表形式で表示しま。また、トラップと syslog がスイッチに構成されているかどうかも表示されます。
5. 電子メール通知またはイベントのトラップを転送するためのルールを作成するには、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 または、SNMPv2c 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 サーバーでは、Cisco Nexus ダッシュボード ファブリック コントローラ から SMTP サーバー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。

   a. 電子メールを介してイベント通知を転送するためのルールを設定する前に、SMTP パラメータが構成されていることを確認します。SMTP の設定を確認するには、**[設定（Settings）] > [サーバー設定（Server Settings）] > [SMTP]** の順に選択し、必須フィールドが設定されていることを確認します。

   b. イベント転送を有効にするには、**[設定（Settings）] > [サーバー設定（Server Settings）] > [イベント（Events）]** の順に選択し、次の表の説明に従ってフィールドを設定します。

      表4. イベント転送の設定

フィールド	説明
イベント転送の有効化	イベント転送機能を有効にするには、チェックボックスをオンにします。
電子メールリストからの電子メール転送	転送メッセージの送信元の電子メール アドレスを指定します。
イベント転送のスヌーズ	指定された時間範囲で、イベントの転送をスヌーズします。
イベント転送の最大繰り返し回数	指定した時間の経過後にイベントの転送を停止します。0 は時間無制限を示します。
イベント/トラップ/Syslogキューの最大数	着信イベント/トラップ/syslog をドロップするまでのキュー内の最大数を指定します。

   c. **[操作（Operations）] > [イベント分析（Event Analytics）]** の順に選択します。

   d. **[転送（Forwarding）]** タブに移動し、**[アクション（Actions）] > [ルールの追加（Add Rule）]** の順に選択し、次の表の説明に従ってフィールドを構成します。

      表5. ルールを構成します。

フィールド	説明
転送方式	次のいずれかの転送方法を選択します： • **電子メール（E-Mail）** • **[トラップ（Trap）]**

電子メール アドレス	このフィールドは、転送方法として [電子メール（E-mail）] を選択した場合に表示されます。イベント通知の転送用の電子メール アドレスを入力します。
アドレス	このフィールドは、転送方法として [トラップ（Trap）] を選択した場合に表示されます。SNMP トラップ レシーバの IP アドレスを入力します。IPv4 または IPv6 アドレスまたは DNS サーバー名を入力できます。
ポート	転送したもの port 〜 which 、 トラップ 等しいのを入力します。
転送範囲	着信イベント/トラップ/syslog メッセージをドロップするまでのキュー内の最大数。
フィールド	**説明**
ファブリック	[すべてのファブリック（All Fabrics）] または特定のファブリックを通知先として選択します。
VSANの範囲	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）] を選択できます。
VSAN List	**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。
送信元	**[DCNM]** または **[Syslog]** を選択します。 [DCNM] を選択した場合は、次の手順を実行します： 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。このチェックボックスは、ポート関連のイベントに対してのみ有効になります。 **Syslog** を選択した場合は、次の手順を実行します： 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. **[タイプ（Type）]** フィールドに、syslog タイプを入力します。

	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入力します。

e. **[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。

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。

```
トラップタイプ = 40990（緊急）40991
（アラート）
40992（クリティカル）
40993（エラー）
40994（警告）
40995（通知）
40996（情報）
40997（デバッグ）
textDescriptionOid = 1、3、6、1、4、1、9、9、40999、1、1、3、0
```

f. **[ルールの追加（Add Rule）]** をクリックします。

6. イベントを抑制するためのルールを作成するには、次の手順を実行します：

Nexus Dashboard ファブリック コントローラを使用すると、ユーザーが指定したルールに基づいて指定し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、Nexus Dashboard 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 データベースに追加されず、電子メールまたは SNMP トラップとして転送されません。

テーブルからルールを表示、追加、変更、および削除できます。既存のイベントからルールを作成できます。テンプレートとして既存のイベントを選択し、[操作（Operations）] > [イベント分析（Event Analytics）] > [イベント（Events）] ページに移動して [ルールの追加（Add Rule）] ウィンドウを開き、イベントを選択して [アクション（Actions）] を選択します。
> サプレッサーを追加します。詳細は、イベント テーブルで選択したイベントから、**[ルールを追加（Add Rule ）] ウィンドウのフィールドに自動的に移植されます。**

a. **[名前（Name）]** フィールドにルールの名前を入力します。

b. **[範囲（Scope）]** フィールドで、**[SAN]**、**[ポート グループ（Port Groups）]**、または **[任意（Any）]** のいずれかのオプションを選択します。

   [範囲（Scope）] フィールドには、LAN/SAN グループとポート グループが個別に表示されます。SAN および ローカル エリア ネットワーク（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（Port Group）] 範囲のグループのみ選択できます。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（Facility）]**フィールド内で名前を入力、または、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. **[タイプ（Type）]** フィールドに、イベント タイプを入力します。

   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）]** チェック 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。

> 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状況でのみ作成できます。例：'sync-snmp-password' AAA syslog イベント は、Nexus ダッシュボード ファブリック コントローラと管理したスイッチの間のパスワード 同期 中 に自動 生成されます。
> 必要になります。アカウンティング イベントを抑制するには、**[操作**

（Operations）] > [イベント分析（Event Analytics）] > [イベント（Events）] ページに移動し、イベントを選択して、**[アクション（Actions）] > [サプレッサーの追加（Add Suppressor）]** を選択します。

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（Accounting）

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）	送信元を指定します。
User Name	ユーザ名を指定します。
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、[アクション（**Actions**）] メニューのドロップダウン リストにある、**[操作（Operations）] > [イベント分析（Event Analytics）] > [アカウンティング（Accounting）] の順に選択します。**

アクション項目	説明
削除（Delete）	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。

著作権

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任となります。

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

Cisco が採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または暗黙のすべての保証を放棄します。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアルの中の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、RFP のドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

シスコおよびシスコのロゴは、シスコまたはその関連会社の米国およびその他の国における
商標または登録商標です。シスコの商標の一覧については、http://www.cisco.com/go/ trademarks を参照してください。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」という言葉が使用されていても、シスコと他社の間にパートナーシップ関係が存在することを意味するものではありません。（1110R）。