




## 障害管理タスク



(注) アドバンス ユーザは、Cisco EPN Manager の Representational State Transfer (REST) API を使用して、デバイスの障害情報にアクセスすることもできます。APIの詳細については、Cisco EPN Manager ウィンドウの右上にある  をクリックし、[ヘルプ (Help)] > [APIヘルプ (API Help)] を選択します。

- イベントの受信、転送、および通知 (1 ページ)
- アラーム クリーンアップ、表示、および電子メール オプションの指定 (13 ページ)
- 確認済み、クリア済み、および割り当て済みのアラームのグローバル表示と検索設定を構成する (17 ページ)
- Cisco IOS XR デバイスでのアラームマネージャの設定 (18 ページ)
- Cisco IOS XE デバイスでのアラーム再同期の設定 (19 ページ)
- アラーム重大度レベルの変更 (21 ページ)
- アラームのトラブルシューティング テキストのカスタマイズ (22 ページ)
- アラームの自動クリア間隔の変更 (22 ページ)
- アラームの失敗の原因に表示される情報を変更する (23 ページ)
- デバイスごとのイベントスロットルのカスタマイズ (23 ページ)
- 完全優先イベントの動作の変更 (24 ページ)
- Web GUI に表示される汎用イベントのカスタマイズ (28 ページ)
- 障害処理エラーのトラブルシューティング (30 ページ)
- シスコサポート コミュニティとテクニカルアシスタンス センター (TAC) から支援を受ける (30 ページ)

## イベントの受信、転送、および通知

Cisco EPN Manager は、デバイスから受信した syslog と SNMPv1、v2、および v3 トラップを処理します。サーバは、自動的に UDP ポート 162 でこれらのイベントをリスンします。サーバ上でイベントリスニング設定を実行する必要はありませんが、適切なポート上で Cisco EPN Manager にトラップと syslog を転送するようにデバイスを設定する必要があります。

通知は、SNMPv2またはSNMPv3形式で転送されます。対応する通知ポリシーがセットアップされている場合は、電子メール受信者にも通知が転送されます。通知タイプUDPの通知受信者を追加する場合、その追加する受信者はそれが設定されている同じポート上でUDPをリッスンする必要があります。INFOレベルイベントだけが、選択されたカテゴリに対して処理され、アラームはクリティカル、メジャー、マイナー、および警告レベルで処理されます。

Cisco EPN Managerは、受信したsyslog、トラップ、およびTL/1アラームを処理することによって発生したアラームとイベントをノースバウンド通知の受信者に転送できます。アラームは任意の重大度のものを転送できますが、イベントはINFO重大度のものしか転送できません。情報は以下の形式で転送できます。

- 電子メール形式。電子メール通知のデフォルト設定 (13 ページ) を参照してください
- SNMPトラップ形式。SNMPトラップ通知としてのアラームおよびイベントの転送 (12 ページ) を参照してください

また、SNMPトラップ通知メカニズムを使用して、サーバの問題を示すSNMPトラップを転送することもできます。

アラートおよびイベントはSNMPv2として送信されます。

## アラーム通知設定を構成するためのユーザ ロールとアクセス権限

次の表に、通知先を設定して、カスタマイズされた通知ポリシーを作成するためのユーザロールとアクセス権限の説明を示します。



(注) 通知先と通知ポリシーを表示、作成、および編集するには、次のユーザロール用のタスク権限が有効になっていることを確認します。

- [アラートとイベント (Alerts and Events)] の通知ポリシーの読み取り/書き込みアクセス
- 仮想ドメインリスト (Virtual Domains List)

詳細については、[ユーザが実行できるタスクの表示と変更](#)を参照してください。

| ユーザ ロール             | アクセス権限                            |
|---------------------|-----------------------------------|
| ルート ドメインを持つルート ユーザ  | 通知先と通知ポリシーを表示、作成、削除、および編集します。     |
| 非ルート ドメインを持つルート ユーザ | 通知先と通知ポリシーを表示します。                 |
| ルート ドメインを持つ管理者ユーザ   | 通知先と通知ポリシーを表示、作成、削除、および編集します。     |
| ルート ドメインを持つスーパー ユーザ | 通知先とアラーム通知ポリシーを表示、作成、削除、および編集します。 |

| ユーザ ロール                  | アクセス権限                             |
|--------------------------|------------------------------------|
| ルートドメインを持つシステムモニタリングユーザ  | 通知先と通知ポリシーを表示します。                  |
| ルートドメインを持つ構成マネージャ        | 通知先と通知ポリシーを表示します。                  |
| 非ルートドメインを持つ管理者ユーザ        | それぞれの仮想ドメインで作成された通知先と通知ポリシーを表示します。 |
| 非ルートドメインを持つスーパーユーザ       | それぞれの仮想ドメインで作成された通知先と通知ポリシーを表示します。 |
| 非ルートドメインを持つシステムモニタリングユーザ | それぞれの仮想ドメインで作成された通知先と通知ポリシーを表示します。 |
| 非ルートドメインを持つ構成マネージャ       | それぞれの仮想ドメインで作成された通知先と通知ポリシーを表示します。 |

## 新しい通知ポリシーを追加する場合の注意事項

次の表に、新しい通知ポリシーを追加する場合に覚えておく必要があるいくつかのポイントを示します。

| 通知ポリシー ページで選択されたカテゴリ | 注意事項  |
|----------------------|---|
| E メール                | <ul style="list-style-type: none"> <li>各仮想ドメインには、一意の連絡先名と電子メールアドレス（電子メール受信者）を割り当てる必要があります。</li> <li>電子メール受信者は、ROOT-DOMAINからのみ、追加、変更、および削除できます。</li> <li>1つの電子メールアドレスを複数の仮想ドメインに関連付けることができます。</li> <li>Cisco EPN Manager は、アラーム通知を送信するために、電話番号、携帯番号、および郵便先住所の詳細を使用しません。</li> </ul> |

| 通知ポリシー ページで選択されたカテゴリ | 注意事項   |
|----------------------|--|
| トラップ受信者              | <ul style="list-style-type: none"><li>• 連絡先名は、トラップ受信者ごとに一意です。</li><li>• トラップ受信者は、<b>ROOT-DOMAIN</b>からしか追加、変更、および削除することができません。トラップ受信者は<b>ROOT-DOMAIN</b>でのみ適用可能です。</li><li>• ノースバウンドトラップ受信者だけが、通知ポリシー エンジンから転送されたアラーム/イベントを受信できます。</li><li>• ゲストアクセストラップ受信者は、ゲストクライアントに関するアラームだけを受信します。</li></ul> |

| 通知ポリシー ページで選択されたカテゴリ | 注意事項 |
|----------------------|------|
| 通知ポリシー               |      |

| 通知ポリシー ページで選択されたカテゴリ | 注意事項   |
|----------------------|--|
|                      | <ul style="list-style-type: none"> <li>• 各通知ポリシーは、アラームカテゴリ、アラーム重大度、アラームタイプ、デバイスグループ、通知先、および時間範囲という条件で構成されます。</li> <li>• 通知ポリシーはそれぞれ一意の仮想ドメインに関連付けられます。</li> <li>• 必要な条件を選択するときに、ツリービュードロップダウンリストをドリルダウンして、個別のカテゴリ（スイッチやルータなど）と重大度（メジャーなど）を選択できます。さらに、特定のアラームタイプ（リンクダウンなど）を選択できます。</li> <li>• ポリシー内の条件と一致したアラームがそれぞれの通知先に転送されます。</li> <li>• アラームが同じ仮想ドメイン内の複数のポリシーと一致し、それらのポリシーに同じ宛先が設定されている場合は、1つの通知だけがそれぞれの宛先に送信されます。</li> <li>• 通知ポリシーに関連付けられた仮想ドメインを削除すると、どのアラームもこのポリシーと一致しなくなります。この通知ポリシーはメインの通知ポリシー ページに一覧表示されますが、この通知ポリシーの詳細を変更または表示することはできません。ただし、このポリシーを削除することはできます。</li> <li>• ポリシーで指定された1つ以上のデバイスグループを削除すると、どのアラームもこのポリシーと一致しなくなります。この通知ポリシーはメインの通知ポリシー ページに一覧表示されますが、この通知ポリシーの詳細を変更または表示することはできません。ただし、このポリシーを削除することはできます。</li> <li>• 既存のアラームポリシーによって抑制されているアラームは、通知先に転送されません。</li> </ul> |

| 通知ポリシー ページで選択されたカテゴリ | 注意事項  |
|----------------------|---|
|                      | <ul style="list-style-type: none"> <li>• ルール条件にシステム カテゴリ アラームと非システム カテゴリ アラームの両方が含まれている通知ポリシーの場合は、非システム カテゴリ アラーム用のデバイスグループを選択する必要があります。</li> <li>• 指定された期間に発生したアラームだけが通知先に送信されます。たとえば、期間を 8:00 ~ 17:00 に指定した場合は、午前 8 時 00 分から午後 5 時 00 分の間のアラームのみが通知されます。</li> </ul> |

## アラーム通知先の設定

Cisco EPN Manager によって生成されたアラームを転送するために、電子メール通知およびノースバウンドトラップの受信者を設定できます。

**ステップ 1** [管理 (Administration)] > [設定 (Settings)] > [システム設定 (System Settings)] > [メールと通知 (Mail and Notification)] > [通知先 (Notification Destination)] の順に選択します。

**ステップ 2** [追加 (Add)] アイコンをクリックして、新しい通知先を作成します。

**ステップ 3** 電子メールの宛先を設定するには、次の手順を実行します。

- [連絡先のタイプの選択 (Select Contact Type)] ドロップダウンリストから [電子メール (Email)] を選択します。
- [連絡先の名前 (Contact Name)] テキスト ボックスに連絡先の名前を入力します。
- [メール宛先 (Email To)] テキスト ボックスに有効な電子メール ID を入力します。  
電子メールは [メール宛先 (Email To)] フィールドに入力した電子メール ID に送信されます。
- [連絡先の氏名 (Contact Full Name)] に連絡先の氏名を入力します。
- [仮想ドメイン (Virtual Domain)] ドロップダウンリストから仮想ドメインを選択します。
- [電話番号 (Telephone Number)]、[携帯電話の番号 (Mobile Number)]、[郵便先住所 (Postal Address)] の各フィールドに値を入力します。
- [保存 (Save)] をクリックします。

**ステップ 4** IP アドレスを使用してノースバウンドトラップの受信者を設定するには、次の手順を実行します。

- [連絡先のタイプの選択 (Select Contact Type)] から [ノースバウンドトラップの受信者 (Northbound Trap Receiver)] を選択します。
- [IP アドレス (IP Address)] オプションボタンを選択し、[IP アドレス (IP Address)] および [サーバ名 (Server Name)] に値を入力します。
- [受信者のタイプ (Receiver Type)] および [通知タイプ (Notification Type)] で必要なタイプを選択します。
- [ポート番号 (Port Number)] に値を入力し、[SMNP バージョン (SMNP Version)] を選択します。

- e) [SMNP バージョン (SMNP Version)] として [v2c] を選択する場合、必要に応じて [コミュニティ (Community)] 設定に値を入力します。
- f) [SMNP バージョン (SMNP Version)] として [v3] を選択する場合、[ユーザ名 (Username)]、[モード (Mode)]、[認証タイプ (Auth.Type)]、[認証パスワード (Auth.Password)]、[認証パスワードの確認 (Confirm Auth.Password)]、[プライバシータイプ (Privacy Type)]、[プライバシーパスワード (Privacy Password)]、[プライバシーパスワードの確認 (Confirm Privacy Password)] の各フィールドに値を入力します。
- g) [保存 (Save)] をクリックします。

**ステップ 5** DNS を使用してノースバウンドトラップの受信者を設定するには、次の手順を実行します。

- a) [連絡先のタイプの選択 (Select Contact Type)] から [ノースバウンドトラップの受信者 (Northbound Trap Receiver)] を選択します。
  - b) [DNS] オプション ボタンを選択し、[DNS 名 (DNS Name)] に値を入力します。
  - c) [受信者のタイプ (Receiver Type)] および [通知タイプ (Notification Type)] で必要なタイプを選択します。
  - d) [ポート番号 (Port Number)] に値を入力し、[SMNP バージョン (SMNP Version)] を選択します。
  - e) [SMNP バージョン (SMNP Version)] として [v2c] を選択する場合、必要に応じて [コミュニティ (Community)] 設定に値を入力します。
  - f) [SMNP バージョン (SMNP Version)] として [v3] を選択する場合、[ユーザ名 (Username)]、[モード (Mode)]、[認証タイプ (Auth.Type)]、[認証パスワード (Auth.Password)]、[認証パスワードの確認 (Confirm Auth.Password)]、[プライバシータイプ (Privacy Type)]、[プライバシーパスワード (Privacy Password)]、[プライバシーパスワードの確認 (Confirm Privacy Password)] の各フィールドに値を入力します。
  - g) [保存 (Save)] をクリックします。
-





- (注)
- [受信者のタイプ (Receiver Type)] として [ゲスト アクセス (Guest Access)] を選択すると、Cisco EPN Manager は通知ポリシーに従ってノースバウンドトラップの受信者にアラームを転送することはありません。ゲストアクセス受信者は、ゲストクライアント関連のイベントだけを受信します。通知ポリシーで使用するのは、ノースバウンドトラップの受信者のみです。外部 SNMPv3 トラップの受信者を設定する際は、必ず同じエンジン ID と同じ認証パスワードおよびプライバシーパスワードを使用してください。
  - 通知の宛先トラップの受信者を更新中、動作状態には、次のポーリングによって状態が更新されるまで以前のトラップの受信者が表示されます。
  - [Notification Policies] ページには、[Monitor] > [Monitoring Tools] > [Alarm Notification Policies] の順に選択して移動することもできます。
  - 受信者の電子メール ID が複数の通知ポリシーで設定されていると、条件が一致した場合、アラームはその電子メール ID に一度だけ転送されます。
  - 通知ポリシーに関連付けられている通知先を削除することはできません。
  - NBI に転送されるアラームには、アラームの作成時に「correlationType」、  
「serviceImpacting」、「UDF」などのフィールドはありません。これらのフィールドは、次のアラーム更新時にのみ送信されます。

## 通知先の削除

次の手順に従い、通知先を削除します。

### 始める前に

通知ポリシーに関連付けられている通知先を削除することはできません。通知ポリシーから通知先の関連付けを解除したことを確認します。これを行うには、アラーム通知ポリシーを編集し、別の通知先を割り当てます。詳細については、[アラーム通知ポリシーのカスタマイズ \(10 ページ\)](#) を参照してください。



- (注) 通知先が複数の通知ポリシーに関連付けられている場合は、関連付けられているすべての通知ポリシーから通知先の関連付けが解除されていることを確認します。

**ステップ 1** [管理 (Administration)] > [設定 (Settings)] > [システム設定 (System Settings)] > [メールと通知 (Mail and Notification)] > [通知先 (Notification Destination)] に移動します。

**ステップ 2** 削除する通知先の横にあるチェックボックスをオンにして、その通知先を選択します。

**ステップ 3** [Delete] アイコンをクリックします。

## アラーム通知ポリシーのカスタマイズ

新しいアラーム通知ポリシーを追加するか、または既存のアラーム通知ポリシーを編集して、特定のデバイスグループで生成される特定のアラームに関する通知を、特定の受信者（電子メール受信者またはノースバウンドトラップ受信者のいずれかまたは両方）宛てに送信するようにできます。

**ステップ 1** [Administration] > [Settings] > [System Settings] > [Alarms and Events] > [Alarm Notification Policies] の順に選択します。新しいアラーム通知ポリシーを追加するには、次の手順に従います。

- a) [追加 (Add)] アイコンをクリックし、[仮想ドメインの選択 (Select a Virtual Domain)] ポップアップウィンドウで必要な仮想ドメインを選択します。

Cisco EPN Manager により、仮想ドメインのデバイスから受信したアラームが、同じ仮想ドメインの通知ポリシーと照合されます。Cisco EPN Manager によって生成されるシステムカテゴリアラームは、すべてのアラーム通知ポリシーと照合できます。

(注) 非ルートドメインの場合、デバイスから送信されたアラームが転送されるのは、仮想ドメインページの [ネットワーク デバイス (Network Devices)] タブでそのデバイスまたはデバイスを含むデバイスグループが追加または選択されている場合だけです。

- b) [OK] をクリックします。  
[通知ポリシー (Notification Policies)] ウィザードが表示されます。
- c) 通知をトリガーする必要がある重大度、カテゴリ、およびイベント状態を選択します。デフォルトでは、すべての重大度タイプ、カテゴリ、および状態が選択されています。
- d) [次へ (Next)] をクリックし、アラーム通知をトリガーするデバイスグループを選択します。

アラーム通知は、選択したデバイスグループに対してのみトリガーされます。

たとえば、デバイスグループのタイプに [ユーザ定義 (User Defined)] を選択すると、設定されているユーザ定義のすべてのデバイスグループに対してアラーム通知がトリガーされます。同様に、デバイスグループのタイプに [ユーザ定義 (User Defined)] と [場所 (Locations)] の両方を選択した場合は、設定されているユーザ定義と場所のすべてのデバイスグループに対してアラーム通知がトリガーされます。

デバイスグループタイプを選択して、他のデバイスグループからの重要でないアラーム通知の受信を抑制します。

前のステップでシステムカテゴリアラームだけを選択した場合は、[デバイスグループ (Device Group)] タブに「『システム』ベースのアラームだけが選択されている場合、デバイスグループは選択できません (Device Groups are not applicable when only 'System' based alarms are selected)」というメッセージが表示されます。ただし非システムカテゴリアラームを選択した場合は、1つ以上のデバイスグループを選択する必要があります。

- e) [次へ (Next)] をクリックし、[通知の宛先 (Notification Destination)] ページで必要な宛先を選択します。

ステップ 1-a でルートドメインを選択した場合、Cisco EPN Manager で作成されたすべての電子メールおよびノースバウンドトラップの受信者の宛先が [Notification Destination] ページに表示されます。非ルートドメインを選択している場合、特定のドメインで作成された電子メールの宛先が [通知宛先

(Notification Destination) ] ページに表示されます。アラーム通知先の設定 (7 ページ) を参照してください。

- f) あるいは、追加アイコンのドロップダウンリストで [電子メール (Email) ] または [ノースバウンドトラップの受信者 (Northbound Trap Receiver) ] オプションを選択し、必要なフィールドに情報を入力します。
- g) 通知の宛先を選択したら、[期間の変更 (Change Duration) ] をクリックします。
- h) [期間の設定 (Set Duration) ] ポップアップ ウィンドウで [開始 (From) ] と [終了 (To) ] のタイミングを選択し、[OK] をクリックします。  
指定した期間内に生成されるアラームだけが、通知宛先に送信されます。
- i) [次へ (Next) ] をクリックし、[サマリー (Summary) ] ページでアラーム通知ポリシーの [名前 (Name) ] と [説明 (Description) ] を入力します。
- j) [保存 (Save) ] をクリックします。

(注) 「インターフェイス」は予約語であるため、アラーム通知ポリシーの名前として使用しないでください。

**ステップ 2** アラーム通知ポリシーを編集するには、次の手順を実行します。

- a) ポリシーを選択し、編集アイコンをクリックします。  
[通知ポリシー (Notification Policies) ] ウィザードが表示されます。
- b) ステップ 1 の説明に従い、[状態 (Conditions) ]、[デバイス グループ (Device Groups) ]、および [宛先 (Destination) ] を選択します。
- c) [保存 (Save) ] をクリックします。

---

## 古い電子メールとトラップ通知データを新しいアラーム通知ポリシーに変換する

Cisco EPN Manager を以前のリリースから最新のバージョンにアップグレードすると、Cisco EPN Manager の以前のリリースで作成された電子メールとトラップ通知データが新しいアラーム通知ポリシーに変換されます。

移行されたアラーム通知ポリシーは、[アラームおよびイベント通知ポリシー (Alarms and Events Notification Policies) ] ページで確認できます。

Cisco EPN Manager では、次のアラームカテゴリがサポートされます。

- アプリケーション パフォーマンス
- 変更監査
- クライアント
- コンピューティング サーバ
- コンテキスト認識型通知
- コントローラ
- 汎用

- モビリティ サービス
- Nexus VPC スイッチ
- パフォーマンス
- SE で検出された干渉源
- セキュリティ
- スイッチとルータ
- システム (System)

Cisco EPN Manager では、次のアラームカテゴリがサポートされていません。

- アドホック不正
- AP
- 自律 AP
- Cisco UCS シリーズ
- カバレッジ ホール
- メッシュリンク (Mesh Links)
- ルータ
- 不正 AP
- RRM
- スイッチおよびハブ
- サードパーティ AP
- サードパートコントローラ (Third Part Controller)
- ワイヤレス コントローラ

移行されたアラーム通知ポリシーを編集するには、「[アラーム通知ポリシーのカスタマイズ \(10 ページ\)](#)」を参照してください。

## SNMP トラップ通知としてのアラームおよびイベントの転送

Cisco EPN Manager は、SNMPv2c および SNMPv3 トラップ通知として、アラームとイベントを EPM-NOTIFICATION-MIB 形式で転送できます。次を指定することができます。

- 特定のアラームまたはイベントのカテゴリ (たとえば、内部サーバ SNMP トラップの場合は [システム (System)] )。
- 特定の重大度のアラーム。INFO イベントだけが転送されます。イベントの他の重大度を指定することはできません。

詳細については、[アラーム通知先の設定 \(7 ページ\)](#) を参照してください。

## 電子メール通知のデフォルト設定

メール サーバを設定していない場合は、「SMTP 電子メール サーバの設定」に記載の手順を実行してください。この手順を実行しないと、通知は送信されません。

すべてのアラームおよびイベントのメール通知に適用される特定のデフォルト設定を設定できます。これらの設定は、ユーザが個別の通知と受信者を設定するときに、上書きできます。

デフォルトでは、電子メールの件名にアラームの重大度とカテゴリが含まれます。次の設定も使用できますが、デフォルトでは無効になっています。

- [件名 (Subject line) ]: より重要なアラーム重大度を含めるか、カスタム テキストを追加します。また、件名全体をカスタム テキストに置き換えることもできます。
- [電子メールの本文 (Body of the email) ]: カスタム テキスト、アラーム条件、およびアラームの詳細ページへのリンクを含めます。
- [セキュアなメッセージ モード (Secure message mode) ]: このモードを有効にすると、IP アドレスとコントローラ名がマスクされます。

これらの設定を有効化、無効化、または調整するには、[管理 (Administration) ]> [設定 (Settings) ]> [システム設定 (System Settings) ] を選択し、さらに [アラームおよびイベント (Alarms and Events) ]> [アラームおよびイベント (Alarms and Events) ] を選択します。[アラーム電子メール オプション (Alarm Email Options) ] エリアで変更を加えます。

## アラームクリーンアップ、表示、および電子メールオプションの指定

[管理 (Administration) ]> [システム設定 (System Settings) ]> [アラームおよびイベント (Alarms and Events) ] ページでは、アラームのクリーンアップ、表示、電子メール送信のタイミングと方法を指定できます。

**ステップ 1** [管理 (Administration) ]> [設定 (Settings) ]> [システム設定 (System Settings) ]> [アラームおよびイベント (Alarms and Events) ]> [アラームおよびイベント (Alarms and Events) ] を選択します。

**ステップ 2** [アラームおよびイベントのクリーンアップ オプション (Alarm and Event Cleanup Options) ] を次のように変更します。

- [クリアされた非セキュリティ アラームを次の後で削除 (Delete cleared non-security alarms after) ]: セキュリティ アラーム以外のアラームが削除されるまでの日数を入力します。セキュリティアラーム以外のアラームには、[セキュリティ (Security) ] カテゴリまたは [アドホック不正 (Adhoc Rogue) ] カテゴリに属するアラーム以外のすべてのアラームが含まれます。
- [クリアされたセキュリティアラームを次の後で削除 (Delete cleared security alarms after) ]: セキュリティアラームとアドホック不正アラームが削除されるまでの日数を入力します。

- [すべての（アクティブおよびクリアされた）アラームを次の後で削除（Delete all (active & cleared) alarms after）]：アクティブなアラームまたはクリアされたアラームが削除されるまでの日数を入力します。
- [すべてのイベントを次の後で削除（Delete all events after）]：すべてのイベントを削除するまでの日数を入力します。

最大値は、8000000 イベントまたは指定された日数のいずれか小さい方です。

**ステップ 3** [syslog クリーンアップ オプション（Syslog Cleanup Options）] を次のように変更します。

- [すべての syslog を次の後で削除（Delete all Syslogs after）]：すべての古い syslog について、削除するまでの日数を入力します。
- [最大保持 syslog 数（Max Number of Syslog to Keep）]：データベースで保持する必要がある syslog の数を入力します。

**ステップ 4** 必要に応じて、[アラーム表示オプション（Alarm Display Options）] を変更します。

- [確認済みのアラームを非表示（Hide acknowledged alarms）]：このチェックボックスをオンにすると、承認済みのアラームは [アラーム（Alarm）] ページに表示されません。このオプションは、デフォルトで有効です。重大度の変化に関係なく、確認応答済みのアラームに対して電子メールは生成されません。
- [割り当て済みのアラームを非表示（Hide assigned alarms）]：このチェックボックスをオンにすると、割り当て済みのアラームは [アラーム（Alarm）] ページに表示されません。
- [Hide cleared alarms]：このチェックボックスをオンにすると、クリアされたアラームは [Alarm] ページに表示されません。このオプションは、デフォルトで有効です。
- [Show only Active Alarms in Alarms tab]：このチェックボックスをオンにすると、アクティブなアラームのみが [Alarms] タブのアラームリストに表示されます。
- [アラーム メッセージにデバイス名を追加（Add device name to alarm messages）]：このチェックボックスをオンにすると、デバイスの名前がアラーム メッセージに追加されます。

これらのオプションの変更は、[アラーム（Alarm）] ページにのみ適用されます。エンティティに対するアラームのクイック検索は、アラームの状態に関係なく、そのエンティティのすべてのアラームを表示します。

**ステップ 5** アラームの [障害ソース パターン（Failure Source Pattern）] を次のように変更します。

- カスタマイズするカテゴリを選択し、[編集（Edit）] をクリックします。
- 利用可能な選択肢から障害ソース パターンを選択し、[OK] をクリックします。
- セパレータをカスタマイズするカテゴリを選択し、[セパレータの編集（Edit Separator）] をクリックします。使用可能なオプションの 1 つを選択し、[OK] をクリックします。

選択したカテゴリに対して生成されるアラームには、ユーザが設定するカスタム パターンが使用されます。たとえば、[クライアント（Clients）] カテゴリを選択し、セパレータが # になるように編集するとし

ます。サポートされるクライアント アラームが生成されたときにユーザが [モニタ (Monitor)] > [モニタリング ツール (Monitoring Tools)] > [アラームおよびイベント (Alarms and Events)] の順に選択すると、そのアラームの [障害のソース (Failure Source)] 列は MAC アドレス#名前となります。

(注) 障害のソースは、カスタムトラップ、syslog 生成イベント、およびカスタム syslog 変換ではサポートされません。

**ステップ 6** [アラーム電子メールのオプション (Alarm Email Options)] を次のように変更します。

- [Add Cisco EPN Manager address to email notifications] : このチェックボックスをオンにすると、電子メール通知に Cisco EPN Manager のアドレスが追加されます。
- [電子メールの件名行にアラームの重要度を含める (Include alarm severity in the email subject line)] : このチェックボックスをオンにすると、電子メールの件名にアラーム重大度が含まれるようになります。このオプションは、デフォルトで有効です。
- [電子メールの件名行にアラームカテゴリを含める (Include alarm Category in the email subject line)] : このチェックボックスをオンにすると、電子メールの件名にアラームのカテゴリが含まれるようになります。このオプションは、デフォルトで有効です。
- [電子メールの件名行に優先アラーム重要度を含める (Include prior alarm severity in the email subject line)] : このチェックボックスをオンにすると、電子メールの件名に事前アラーム重大度が含まれるようになります。
- [電子メールの件名行にカスタムテキストを含める (Include custom text in the email subject line)] : このチェックボックスをオンにすると、電子メールの件名にカスタムテキストが追加されます。[電子メールの件名行をカスタム テキストで置換する (Replace the e-mail subject line with custom text)] チェックボックスをオンにして、電子メールの件名をカスタム テキストに置き換えることもできます。
- [電子メールの本文にカスタムテキストを含める (Include custom text in body of email)] : このチェックボックスをオンにすると、電子メールの本文にカスタム テキストが追加されます。
- [電子メールの本文にアラーム状態を含める (Include alarm condition in body of email)] : このチェックボックスをオンにすると、電子メールの本文にアラーム状態が含まれるようになります。
- [電子メールの本文にアラーム アプリケーション カテゴリ データを含める (Include alarm application category data in body of email)] : このチェックボックスをオンにすると、電子メールの本文にアラームカテゴリが含まれるようになります。
- [電子メールの本文にアラームの詳細ページへのリンクを追加する (Add link to Alarm detail page in body of email)] : このチェックボックスをオンにすると、電子メールの本文に [アラームの詳細 (Alarm detail)] ページへのリンクが追加されます。
- [セキュア メッセージモードの有効化 (Enable Secure Message Mode)] : チェックボックスをオンにすると、セキュア メッセージモードが有効になります。[IP アドレスをマスク (Mask IP Address)] および [コントローラ名をマスク (Mask Controller Name)] チェックボックスをオンにした場合、アラーム電子メールはセキュアモードで送信され、すべての IP アドレスとコントローラ名はマスクされます。
- [電子メール送信間隔 (Email Send Interval)] : 電子メールの送信間隔を指定します。

- (注) Cisco EPN Manager はアラームの最初のインスタンスに関するアラーム通知電子メールを送信し、その後の通知はアラーム重大度が変更された場合にのみ送信されます。

**ステップ 7** [アラームのその他のオプション (Alarm Other Options) ] を次のように変更します。

- [コントローラライセンス数のしきい値 (Controller License Count Threshold) ] : しきい値のパーセンテージを入力します。コントローラに接続されているアクセスポイントの数が、コントローラで使用可能なライセンスの指定レートに達すると、アラームがトリガーされます。たとえば、コントローラのアクセスポイントライセンスが 100、しきい値が 80% で設定されている場合、コントローラに接続されているアクセスポイントの数が 80 を超えると、アラームがトリガーされます。
- [AP カウントしきい値アラームの有効化 (Enable AP count threshold alarm) ] : このチェックボックスをオンにすると、しきい値アラームの AP カウントを有効にします。
- [コントローラ アクセス ポイント数のしきい値 (Controller Access Point Count Threshold-) ] : しきい値のパーセンテージを入力します。コントローラに接続されているアクセスポイントの数が、コントローラでサポートされているアクセスポイントの最大数の指定レートに達すると、アラームがトリガーされます。たとえば、コントローラが最大 6000 アクセスポイントをサポートしており、しきい値が 80% に設定されている場合、コントローラに接続されているアクセスポイントの数が 4800 を超えるとアラームがトリガーされます。
- [Admin Down 状態のインターフェイスで光 SFP TCA を抑制 (Suppress Interface Optical SFP TCA in Admin Down State) ] : このチェックボックスをオンにすると、Admin Down 状態のインターフェイスで光 SFP TCA の発生を防ぐことができます。
- [サービス影響分析の有効化 (Enable Service Impact Analysis) ] : このチェックボックスをオンにすると、サービス影響分析が有効になります。
- [ツリーの根本原因がクリアされたときに関連ツリーからのサブツリー作成の有効化 (Enable creation of subtrees from a correlation tree when root cause of the tree clears) ] : 関連ツリーの根本原因がクリアされたときに、この関連ツリーのサブツリーが作成されます。各サブツリーには未解決の根本原因がある場合にこのチェックボックスをオンにすると機能が有効になります。
- [インターフェイス ステータス ポーリングからのアラームの有効化 (Enable alarms from interface status polling) ] : このチェックボックスがオンの場合、イーサネットとバンドルインターフェイスのインターフェイスステータスをポーリングすることで、LinkDown アラームが発生およびクリアされます。
- [EPNM インベントリ収集に基づくアラーム生成の有効化 (Enable alarm generation based on EPNM inventory collection) ] : EPNM はエンティティのインベントリステータスを使用して特定のアラームを生成およびクリアします。このメカニズムは、(デバイスでこれらが生成されず、ネットワーク内で失われたことなどが原因で) 失われたか欠けている可能性のある syslog およびトラップのバックアップとして機能します。
- [ユーザ定義フィールドの有効化 (Enable User Defined Field) ] : この設定が有効になっている場合、[アラーム (Alarms) ] タブのアラームリストに、ハードウェアアラームの PRODUCT\_NAME と PRODUCT\_ID が条件付きで入力されます。この設定は既存のアラームには影響せず、以前に発生したアラームに遡ってを適用されません。デフォルトでは、この設定はディセーブルになっています。
- [イベントスロットルの有効化 (Enable Event Throttle) ] : このチェックボックスをオンにすると、デバイスのイベントカウントがしきい値カウントを超えた場合 (デフォルトでは、1 時間以内に発生した



イベントが 3,600 を超える場合)、Cisco EPN Manager によってイベントがプロアクティブにドロップされます。詳細については、[デバイスごとのイベントスロットルのカスタマイズ \(23 ページ\)](#) を参照してください。

- **[SVO へのアラーム相互起動の有効化 (Enable Alarms Cross Launch to SVO)]** : このチェックボックスをオンにすると、アラームテーブル ([**モニタ (Monitor)**] > [**監視ツール (Monitoring Tools)**] > [**アラームおよびイベント (Alarms and Events)**]) から SVO ノードクラフトへの相互起動が有効になります。

(注) SVO UI に移動するたびにログイン情報を入力しないようにするには、Cisco EPN Manager から SVO Nodal クラフトへのシングルサインオン (SSO) を有効にします。詳細については、[Cisco EPN Manager から SVO UI へのシングルサインオン \(SSO\) を有効にする](#) を参照してください。

**ステップ 8** [アラームマネージャの設定 (Alarm Manager Settings)] については、[Cisco IOS XR デバイスでのアラームマネージャの設定 \(18 ページ\)](#) を参照してください。

**ステップ 9** [保存 (Save)] をクリックします。

## 確認済み、クリア済み、および割り当て済みのアラームのグローバル表示と検索設定を構成する

次の表に、確認済み、クリア済み、および割り当て済みのアラーム用の表示オプションの一部を示します。これらの設定は、個別のユーザが (表示設定で) 調整することができません。これは、非常に大規模なシステムの場合に、ユーザがシステムパフォーマンスに影響を及ぼすような変更を加える可能性があるためです。

[アラームおよびイベント (Alarms and Events)] ページに表示されるその他の設定はユーザが調整できますが、ここではグローバルデフォルトを設定できます。これらの設定については、次のトピックを参照してください。

- [電子メール通知のデフォルト設定](#)
- [アラーム、イベント、および Syslog の消去](#)

**ステップ 1** [管理 (Administration)] > [設定 (Settings)] > [システム設定 (System Settings)] を選択してから、[アラームおよびイベント (Alarms and Events)] > [アラームおよびイベント (Alarms and Events)] を選択します。

**ステップ 2** [表示オプションのアラーム (Alarm Display Options)] 領域で、必要に応じて、これらの設定を有効または無効にします。

| アラーム表示オプション | 説明 | 設定が検索結果にも影響するかどうか |
|-------------|----|-------------------|
|             |    |                   |

|  |   |    |
|--|---|----|
| 確認済みのアラームを非表示 (Hide acknowledged alarms)                                   | [アラーム (Alarms) ] リストに確認済みのアラームを表示しないか、それらを検索結果に含めません。   | ○  |
| 割り当て済みのアラームを非表示 (Hide assigned alarms)                                     | [アラーム (Alarms) ] リストまたは検索結果に割り当て済みのアラームを表示しません。   | ○  |
| クリア済みのアラームを非表示 (Hide cleared alarms)                                       | [アラーム (Alarms) ] リストまたは検索結果にクリア済みのアラームを表示しません。<br><br>たとえば、4000 アラームのうちの 3900 がクリアされたアラームである場合、この設定を有効にすると、[アラーム (Alarms) ] > [アクティブアラームの表示 (Showing Active Alarms) ] のアラームリストにはクリアされていない 100 のアラームが表示されます。<br><br>(注) クリア済みのアラームは、[クリア済みのアラーム (Cleared Alarms) ] タブでは表示可能なままです。      | なし |
| [アラーム (Alarms) ] タブにアクティブアラームのみを表示 (Show only Active Alarms in Alarms tab) | [アラーム (Alarms) ] タブのアラームリストにアクティブなアラームのみを表示します。<br><br>たとえば、4000 アラームのうちの 3900 がクリアされたアラームである場合、この設定を有効にすると、[アラーム (Alarms) ] > [アクティブアラームの表示 (Showing Active Alarms) ] のアラームリストには最新のクリアされていない 4000 のアラームが表示されます。<br><br>(注) クリア済みのアラームは、[クリア済みのアラーム (Cleared Alarms) ] タブでは表示可能なままです。 | なし |
| アラームメッセージにデバイス名を追加 (Add device name to alarm messages)                     | 電子メール通知にデバイス名を追加します。  | なし |

**ステップ 3** 変更を適用するには、[アラームおよびイベント (Alarms and Events) ] ウィンドウの下部にある [保存 (Save) ] をクリックします。

## Cisco IOS XR デバイスでのアラームマネージャの設定

信頼性の高いアラームの一部として、Cisco EPN Manager は Cisco IOS XR デバイスのアラームマネージャをポーリングして未処理のアラームまたはイベントを確認します。



(注) アラームマネージャのサポートは、Cisco IOS XR デバイスの NCS 10xx、NCS 40xx、および NCS 55xx のみに限定されています。

Cisco EPN Manager GUI でアラームマネージャを有効または無効にするには、次の手順に従います。

**ステップ 1** [管理 (Administration)] > [設定 (Settings)] > [システム設定 (System Settings)] を選択してから、[アラームおよびイベント (Alarms and Events)] > [アラームおよびイベント (Alarms and Events)] を選択します。

**ステップ 2** [Alarm Manager Settings] で、デバイスタイプを選択して、必要に応じてアラームマネージャを有効または無効にします。

(注) デフォルトでは、アラームマネージャは、[Alarm Manager Settings] 領域の下に一覧表示されているすべてのデバイスタイプに対して有効になっています。

**ステップ 3** [保存 (save)] をクリックして変更を適用します。

**ステップ 4** [Alarms and Events] ウィンドウの下部にある [Save] をクリックします。

アラームマネージャが有効になっている場合、Cisco EPN Manager は 5 分ごとにデバイスをポーリングします。このポーリング間隔は変更できません。アラームマネージャによって発生したすべてのアラームは、[Monitor] > [Monitoring Tools] > [Alarms and Events] ページの [Alarm] タブに一覧表示されます。このリストでは、重大度を変更したり、アラームマネージャによって発生したアラームをクリアまたは削除したりすることはできません。アラームマネージャによって発生したアラームについては、アラームのソースが「Synthetic\_Event」と表示されます。

アラームマネージャを無効にした場合は、アラームマネージャによって以前に発生したすべてのアラームがクリアされます。Cisco EPN Manager はデバイスをポーリングしなくなりますが、引き続きデバイスから直接アラームを受信します。すべての PKT-INFRA-FM アラームは、[Monitor] > [Monitoring Tools] > [Alarms and Events] ページの [Events] タブに一覧表示されません。

## Cisco IOS XE デバイスでのアラーム再同期の設定

「show facility」コマンドに基づくアラーム再同期機能は、Cisco IOS XE デバイス用の信頼性の高いアラームの一部です。この機能は、Cisco NCS 42xx デバイスのソフトウェアバージョン 16.6.6vS および 16.9.1 でサポートされています。

す。/conf/fault/ncs42xx/resources/NCS42xxAlarmManager.properties ファイルを変更することにより、アラームの再同期を有効または無効にすることができます。

アラーム再同期が有効になっている場合、デバイスから受信したアラームは、[Monitor] > [Monitoring Tools] > [Alarms and Events] ページの [Alarm] タブに表示されます。Cisco EPN

Manager を使用して、重大度を変更したり、これらのアラームをクリアまたは削除したりすることはできません。



- (注) アラーム再同期機能は、DSX、SONET、およびシステムアラームを選択する場合にのみサポートされます。詳細は [Cisco Evolved Programmable Network Manager のサポート対象 Syslog](#) を参照してください。

Cisco NCS 42xx デバイスでアラームマネージャを有効または無効にする手順を次に示します。

**ステップ 1** Cisco EPN Manager サーバとの CLI セッションを開きます。詳細については、「[CLI 経由の接続](#)」を参照してください。

**ステップ 2** `/conf/fault/ncs42xx/resources/NCS42xxAlarmManager.properties` ファイルを開きます。

**ステップ 3** 必要に応じて、`shfacilityenabled`、`resyncperiodmillis`、および `pollerperiodmillis` を変更します。

- `shfacilityenabled` : アラームマネージャを有効または無効にするフラグ。このフラグを `true` に設定すると、アラーム再同期が有効になります。デフォルトでは、この値は `true` に設定されています。この値を変更する場合、システムの再起動は必要ありません。
- `resyncperiodmillis` : デバイスをポーリングするポーリング間隔。これらの値は必要に応じて変更できます。デフォルト値は、600000 ミリ秒 (10 分) です。この変更を有効にするには、システムを再起動する必要があります。
- `pollerperiodmillis` : アラームマネージャをポーリングするためにデバイスリストを更新するポーラ。この値は必要に応じて変更できます。デフォルト値は 3600000 ミリ秒 (1 時間) です。この変更を有効にするには、システムを再起動する必要があります。

## Cisco IOS XE デバイスでのアラームプロファイリングの設定

Cisco EPN Manager は、Cisco IOS XE デバイスのアラームプロファイリングをサポートしています。Cisco EPN Manager でアラームプロファイリングの変更を反映するには、`alarmprofileEnabled` を `true` に設定します。手順は次のとおりです。

**ステップ 1** Cisco EPN Manager サーバとの CLI セッションを開きます。詳細については、「[CLI 経由の接続](#)」を参照してください。

**ステップ 2** `/conf/fault/ncs42xx/resources/NCS42xxVersion.properties` ファイルを開きます。

**ステップ 3** `alarmprofileEnabled` を `true` に設定し、変更を保存します。デフォルトでは、`alarmprofileEnabled` は有効になっています。

- (注) `alarmprofileEnabled` が `false` に設定されている場合、Cisco EPN Manager はアラームプロファイリングの変更を反映しません。

---

## アラーム重大度レベルの変更

Cisco EPN Manager の各アラームには重大度が設定されます。アラームの重大度は、アラームに関連付けられている最も重大なイベントによって決定します。新たに生成されたイベントの重大度を変更することにより、アラームの重大度を調整できます。



- (注) ハイアベイラビリティなど Cisco EPN Manager のシステム管理に関連付けられたアラームについては、[サーバの内部SNMPトラップのカスタマイズおよびトラップの転送](#)を参照してください。

次の2つの方法で、ネットワークレベルおよびデバイスレベルのアラームの重大度を変更できます。

- オプティカル、キャリアイーサネット、デバイスヘルス、インターフェイスヘルスマニタリングポリシーによって生成されたしきい値超過のアラーム：関連するモニタリングポリシーの設定を変更します。[モニタリングポリシーのしきい値およびアラーム動作の変更](#)を参照してください。
- 特定のアラーム：このセクションの手順を使用します。

---

**ステップ 1** [管理 (Administration)] > [システム設定 (System Settings)] を選択し、[アラームおよびイベント (Alarms and Events)] > [アラームの重大度および自動クリア (Alarm Severity and Auto Clear)] の順に選択します。

**ステップ 2** [アラーム状態 (Alarm Condition)] 列で使用可能なカテゴリを拡張するか、または列見出しのすぐ下にある [アラーム状態 (Alarm Condition)] フィールドにイベントテキスト全体または一部を入力して必要な [アラーム状態 (Alarm Condition)] を検索します。

**ステップ 3** イベントを選択し、新しい重大度を設定します。

1. イベントのチェックボックスをオンにします。
  2. [重大度 (Severity)] ドロップダウンリストから重大度を選択し、[保存 (Save)] をクリックします。
-

# アラームのトラブルシューティングテキストのカスタマイズ

トラブルシューティングと説明の情報をアラームに関連付けると、[アラームおよびイベント (Alarms and Events)] テーブルへのアクセス権を持つユーザがその情報を表示できるようになります。ポップアップウィンドウに表示される情報を追加または変更するには、次の手順に従います。

**ステップ 1** [管理 (Administration)] > [設定 (Settings)] > [システム設定 (System Settings)] の順に選択し、[アラームおよびイベント (Alarms and Events)] > [アラームの重大度および自動クリア (Alarm Severity and Auto Clear)] を選択します。

**ステップ 2** アラームを選択し、[推奨アクション (Recommended Action)] をクリックします。

**ステップ 3** [説明 (Explanation)] および [推奨アクション (Recommended Actions)] フィールドの内容を追加または変更して、[保存 (Save)] をクリックします。デフォルトのテキストに戻すには、[リセット (Reset)] をクリックしてから [保存 (Save)] をクリックします。

## アラームの自動クリア間隔の変更

特定の期間が経つと自動的にアラームがクリアされるように設定できます。この設定は、クリアイベントがない場合などに役立ちます。アラームの自動クリアによって、アラームに関連するイベントの重大度を変更されることはありません。

**ステップ 1** [管理 (Administration)] > [設定 (Settings)] > [システム設定 (System Settings)] の順に選択し、[アラームおよびイベント (Alarms and Events)] > [アラームの重大度および自動クリア (Alarm Severity and Auto Clear)] を選択します。

**ステップ 2** [イベント タイプ (Event Types)] 列の下に表示されているカテゴリを展開します。または、列ヘッダーのすぐ下にある [イベント タイプ (Event Types)] 検索フィールドにイベントのテキストの全部または一部を入力することにより、目的のイベント タイプを検索します。

**ステップ 3** イベントまたはイベントのグループのアラームを自動的にクリアするまでの期間を変更するには、次のように操作します。

- 単一のイベントの場合、そのイベントのチェックボックスをオンにしてから、[自動クリアまでの期間 (Auto Clear Duration)] フィールドをクリックし、新しい期間を入力して [保存 (Save)] をクリックします。
- 複数のイベントの場合、それらのイベントを選択してから、[アラームの自動クリア (Alarm Auto Clear)] をクリックし、ダイアログボックスに新しい期間を入力して [OK] をクリックします。

**ステップ 4** 次のいずれかの操作を実行して、自動クリア間隔を変更します。

- [自動クリアまでの期間 (Auto Clear Duration) ] フィールドをクリックし、新しい間隔を入力して [保存 (Save) ] をクリックします。
- イベントタイプのチェックボックスをオンにしてから [アラームの自動クリア (Alarm Auto Clear) ] をクリックし、新しい間隔を入力して [OK] をクリックします。

## アラームの失敗の原因に表示される情報を変更する

アラームが生成された場合は、失敗の原因に関する情報がそれに含まれています。情報は特定の形式を使用して表示されます。たとえば、パフォーマンスの失敗の場合は、*MACAddress:SlotID* という形式が使用されます。他のアラームの失敗の原因として、ホスト名、IPアドレス、またはその他のプロパティが含まれている場合があります。次の手順を使用して、アラームの失敗の原因に表示されるプロパティと区切り文字（コロン、ダッシュ、またはシャープ記号）を調整します。

- ステップ 1** [管理 (Administration) ] > [設定 (Settings) ] > [システム設定 (System Settings) ] を選択してから、[アラームおよびイベント (Alarms and Events) ] > [アラームおよびイベント (Alarms and Events) ] を選択します。
- ステップ 2** [失敗の原因パターン (Failure Source Pattern) ] 領域で、カスタマイズするアラームカテゴリを選択します。
- ステップ 3** 次のように失敗の原因形式を調整します。
- 表示されるプロパティをカスタマイズするには、[編集 (Edit) ] をクリックして、プロパティを選択し、[OK] をクリックします。プロパティが灰色表示されている場合は、それを削除することができません。
  - プロパティの間に表示される区切り文字をカスタマイズするには、[区切り文字の編集 (Edit Separator) ] をクリックします。
- ステップ 4** 変更を適用するには、[アラームおよびイベント (Alarms and Events) ] 設定ウィンドウの下部にある [保存 (Save) ] をクリックします。

## デバイスごとのイベントスロットルのカスタマイズ

デバイスによって発生したイベントの数がしきい値を超えると、Cisco EPN Manager はイベントをプロアクティブにドロップします。下限しきい値に到達すると、イベント処理が再開されます。

デフォルトでは、1時間以内に3,600を超えるイベントが発生した場合、Cisco EPN Manager はデバイスからイベントをプロアクティブにドロップします。イベント数が3,000に低下すると、イベント処理が再開されます。

デフォルトのしきい値を変更するには、次の手順を実行します。

#### 始める前に

この機能を有効にするには、次の手順を実行します。

1. [管理 (Administration)] > [設定 (Settings)] > [システム設定 (System Settings)] > [アラームおよびイベント (Alarms and Events)] > [アラームおよびイベント (Alarms and Events)] に移動します。
2. [イベントスロットルの有効化 (Enable Event Throttle)] チェックボックスをオンにします。

**ステップ 1** Cisco EPN Manager で CLI セッションを開きます（詳細については、[CLI 経由の接続](#)を参照）。

**ステップ 2** /conf/fault/cep/EventThrottleRules.xml ファイルを開きます。

**ステップ 3** 次のルールで必要な値を指定します。

- Add\_Suppress\_Event\_Based\_On\_Count\_Per\_Device\_Rule  
: デバイスによって発生したイベントを Cisco EPN Manager がプロアクティブにドロップするしきい値カウント。デフォルトでは、この値は 3600 です。
- Remove\_Suppress\_Event\_Based\_On\_Count\_Per\_Device\_Rule : Cisco EPN Manager がイベントの処理を再開するしきい値カウント。デフォルト値は 3000 です。

## 完全優先ベントの動作の変更

Cisco EPN Manager は、デバイスから設定変更イベントを受信すると、他の関連するイベントが送信される場合に備えて特定の時間待機してからインベントリ収集を開始します。これにより、複数の収集プロセスの同時実行が回避されます。これは、インベントリ収集保留時間と呼ばれ、デフォルトで 10 分に設定されています。この設定は、[インベントリ (Inventory)] システム設定ページ ([管理 (Administration)] > [設定 (Settings)] > [システム設定 (System Settings)] > [インベントリ (Inventory)]) で制御されています。

次のイベントは、デフォルトの時間間隔である 10 分以内に Cisco EPN Manager によって処理されます。

| タイプ (Type) | サポートされるイベント   |
|------------|---|
| リンク        | LINK-3-UPDOWN   |
| カード保護      | CARD_PROTECTION-4-PROTECTION<br>CARD_PROTECTION-4-ACTIVE  |
| VLAN       | PORT_SECURITY-6-VLAN_REMOVED<br>PORT_SECURITY-6-VLAN_FULL |



| タイプ (Type)                | サポートされるイベント   |
|---------------------------|---|
| ICCP SM                   | L2-L2VPN_ICCP_SM-4-REMOTE_CORE_ISOLATION<br>L2-L2VPN_ICCP_SM-4-REMOTE_CORE_ISOLATION_CLEAR<br>L2-L2VPN_ICCP_SM-3-CONFIG_LOCAL_ERROR<br>L2-L2VPN_ICCP_SM-3-CONFIG_REMOTE_ERROR<br>L2-L2VPN_ICCP_SM-4-LOCAL_CORE_ISOLATION<br>L2-L2VPN_ICCP_SM-4-LOCAL_CORE_ISOLATION_CLEAR<br>L2-L2VPN_ICCP_SM-4-PEER_REACHABILITY_FAILURE<br>L2-L2VPN_ICCP_SM-4-PEER_REACHABILITY_CLEAR<br>L2-L2VPN_ICCP_SM-4-REMOTE_ACCESS_MAIN_PORT_FAILURE<br>L2-L2VPN_ICCP_SM-4-REMOTE_ACCESS_MAIN_PORT_FAILURE_CLEAR<br>INFRA-ICCP-5-ISOLATION<br>INFRA-ICCP-5-ISOLATION_CLR<br>INFRA-ICCP-5-NEIGHBOR_STATE_UP<br>INFRA-ICCP-5-NEIGHBOR_STATE_DOWN<br>INFRA-ICCP-6-BACKBONE_INTERFACE_STATE_UP<br>INFRA-ICCP-6-BACKBONE_INTERFACE_STATE_DOWN<br>L2-BM-6-ACTIVE_CLEAR<br>L2-BM-6-ACTIVE_PROBLEM<br>L2-L2VPN_ICCP_SM-3-CONFIG_INVALID_NODEID<br>L2-L2VPN_ICCP_SM-3-CONFIG_INVALID_NODEID_CLEAR |
| 衛星                        | PKT_INFRA-ICPE_GCO-5-SATELLITE_STATUS_PROBLEM<br>PKT_INFRA-ICPE_GCO-5-SATELLITE_STATUS_CLEAR  |
| クラスタ                      | PLATFORM-REDDRV-7-ROLE_CHANGE<br>PLATFORM-CE_SWITCH-6-UPDN<br>PLATFORM-CLUSTER_CLM-6-UPDN<br>LINK_UP<br>LINK_DOWN   |
| Celeborn カード              | UEA_SPA_MODE-6-UEA_SPA_MODE_CHG   |
| コンフィギュレーションコミット<br>syslog | MGBL-CONFIG-6-DB_COMMIT<br>SYS-5-CONFIG_I   |

ただし、次の重大なイベントが発生した場合はすぐに、Cisco EPN Manager によってデバイスのフルディスカバリが実行されます。

```
SYS-5-RELOAD
SYS-5-RESTART
OIR-6-INSCARD
OIR-SP-6-INSCARD
SWT_CEFC_STATUS_CHANGE
cefcFRUremoved
cefcFRUInserted
```

## 局所的インベントリのイベントフローコントローラ

局所的インベントリでは、生成されたイベントが識別され、デバイスで行われた変更のみが処理されます。イベントの流入によるデバイスの連続的な同期を避けるため、詳細なインベントリではイベントバーストフローコントローラと連続イベントフローコントローラが使用されます。

イベントバーストおよび連続イベント

は、`/opt/CSColumos/conf/fault/correlationEngine/CE-EventBasedInventoryRules.xml` ファイルからのみ設定できます。

## イベントバーストフローコントローラ

管理対象デバイスのいずれかのテクノロジーについて、着信イベントの数がしきい値（`BurstHoldOffTimer` の `BurstThreshold`）を超えると、Cisco EPN Manager によってイベントバースト状態と見なされます。このシナリオでは、イベントバースト状態がクリアされるまで、しきい値違反となっているイベントの詳細なインベントリ同期が一定の期間（`BurstHoldOffTimer`）保留されます。この状態チェックは定期的に繰り返されます。指定の再試行回数

（`BurstCheckRetryCount`）が経過した後もまだしきい値違反となっている場合は、Cisco EPN Manager によってデバイスの詳細なインベントリ処理がすべて停止されます。

イベントバースト状態が検出され、3回の再試行の前にクリアされた場合は、イベントバーストフローコントローラによって、対応するテクノロジーの機能の同期がトリガーされます。イベントバースト状態が検出され、3回の再試行の後も継続している場合は、コントローラによってすべての詳細なインベントリ処理が停止され、`DISABLE_GRANULAR_INVENTORY_EVENT` イベントが生成されて、デバイスの詳細なインベントリが無効になります。

表 1: イベントバーストアクションのプロパティ

| プロパティ名                            | 説明                                  | デフォルト値          |
|-----------------------------------|-------------------------------------|-----------------|
| <code>BurstThreshold</code>       | 一定の期間において特定のタイプのイベントが「バースト」と見なされる数。 | 100 のイベント。      |
| <code>BurstHoldOffTimer</code>    | インベントリ同期が保留される期間。                   | 300000 ミリ秒（5 分） |
| <code>BurstCheckRetryCount</code> | 許容される再試行回数。                         | 3 回             |

局所的インベントリが無効になると、特定のデバイスについてイベントバースト状態をモニタするためのシステムチェックが開始されます。このシステムチェックによって、イベントバースト状態が継続しているかどうかを確認されます。イベントバースト状態がない場合は、システムによって `DISABLE_GRANULAR_INVENTORY_EVENT` がクリアされた後、デバイスの完全同期が実行されます。新しい着信イベントに対しては、デバイスの局所的インベントリ処理が再開されます。



(注) デバイスの局所的インベントリを手動で有効にすると（[局所的インベントリの有効化または無効化（27 ページ）](#)を参照）、対応する `DISABLE_GRANULAR_INVENTORY_EVENT` がクリアされます。

## 継続イベントフローコントローラ

管理対象デバイスの着信イベントの数がしきい値（contEventsCheckPeriod の contEventsThresholdCount）よりも大きい場合は、Cisco EPN Manager によって連続イベント状態と見なされます。このシナリオでは、継続イベント状態がクリアされるまで、しきい値違反となっているイベントの詳細なインベントリ同期が一定の期間（contEventsDropPeriod）保留されます。

継続イベント状態が検出されると、継続イベントフローコントローラによって、デバイスの詳細なインベントリ処理がすべて停止され、デバイスが継続状態であることを示す INVENTORY\_SYNC\_SUPPRESSED アラームが発生します。継続イベント状態がクリアされるまでは、特定されたすべてのイベントについて、一定間隔で機能の同期の実行が継続されます。

表 2: 継続イベントアクションのプロパティ

| プロパティ名                   | 説明                                      | デフォルト値          |
|--------------------------|---|-----------------|
| contEventsThresholdCount | キュー内で一度に許可されるイベントの最大数。                  | 50 のイベント        |
| contEventsCheckPeriod    | 着信イベントカウントを確認するための時間間隔（ミリ秒単位）。          | 300000 ミリ秒（5 分） |
| contEventsDropPeriod     | 継続イベントの場合に一定間隔で機能の同期をトリガーする時間間隔（ミリ秒単位）。 | 300000 ミリ秒（5 分） |

## 局所的インベントリの有効化または無効化

局所的インベントリの有効化または無効化は、[システム設定（System Settings）] ページからグローバルレベルで行えます。[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [インベントリ（Inventory）] > [インベントリ（Inventory）] > > > の順に選択し、[局所的インベントリを有効にする（Enable Granular Inventory）] チェックボックスをオンまたはオフにします。デフォルトで、この設定は有効になっています。



(注) 局所的インベントリを無効にすると、すべての管理対象デバイスの局所的インベントリ処理がすべて停止されます。

また、[ネットワークデバイス（Network Devices）] ページからデバイスレベルで局所的インベントリを有効または無効にすることもできます。デバイスの局所的インベントリを無効にするには、[ネットワークデバイス（Network Devices）] ページで目的のデバイスを選択し、[管理状態（Admin State）] > [局所的インベントリを無効にする（Disable Granular Inventory）] > を選択します。これで、選択したデバイスについてのみ、局所的インベントリが無効になり、シス

テムにある他のデバイスの詳細なインベントリ処理には影響を与えません。デバイスの局所的インベントリを再度有効にするには、[ネットワークデバイス (Network Devices)] ページで目的のデバイスを選択し、[管理状態 (Admin State)] > [局所的インベントリを有効にする (Enable Granular Inventory)] > を選択します。1 つまたは複数のデバイスを選択して、これらのアクションを適用することができます。ただし、複数のデバイスを選択する場合は、選択したデバイスのすべてが2つの状態のいずれかになっている必要があります。選択したデバイスの状態が互いに異なる場合、これらのオプションは有効になりません。



(注) 局所的インベントリがグローバルレベルで無効になっている場合は、デバイスレベルでの局所的インベントリ設定よりも優先します。局所的インベントリがグローバルレベルで有効になっている場合は、デバイスレベルでの局所的インベントリ設定の方が優先します。

## Web GUI に表示される汎用イベントのカスタマイズ

SNMP トラップおよび syslog によって生成される汎用イベントの説明と重大度をカスタマイズすることができます。カスタマイズした内容は、SNMP トラップ イベントの [イベント (Events)] タブに表示されます。MIB モジュールがロードされていない場合は、手動でロードし、その MIB で提供される通知をカスタマイズすることができます。

これらの汎用イベントをカスタマイズする方法については、「[SNMP トラップに基づく汎用イベントのカスタマイズ \(29 ページ\)](#)」を参照してください。

## 汎用トラップおよび Syslog の処理の無効化および有効化

デフォルトでは、Cisco EPN Manager は受信した syslog またはトラップを廃棄しません。[アラームおよびイベントはどのように作成および更新しますか。](#)に記載されているように、Cisco EPN Manager は、受信した syslog またはトラップについて Cisco EPN Manager が新規イベントを作成すべきかどうかを決定する（新規イベントを作成する場合は、アラームを作成するかどうかも決定する）イベント カタログを保持しています。Cisco EPN Manager がイベントを作成しない場合、トラップまたは syslog は汎用イベントと見なされます。

デフォルトでは、Cisco EPN Manager により次のことが実行されます。

- イベント一覧に汎用イベントが表示されます。
- 汎用イベントは、CISCO-EPM-NOTIFICATION-MIB を使用して正規化された後、電子メールまたは SNMP トラップ通知で転送されます。詳細については、本ガイドの「CISCO-EPM-NOTIFICATION-MIB」を参照してください。

トラップの内容に関係なく、これらのすべてのイベントに MINOR 重大度が割り当てられ、アラーム カテゴリ [汎用 (Generic)] に分類されます。

## 汎用トラップ処理を有効または無効にする

genericTrap.sh コマンドを使用して一般的な syslog を管理します。

| 操作の目的 :        | 使用するコマンド :                           |
|----------------|--------------------------------------|
| 汎用トラップ処理をオフにする | /opt/CSCOlumos/bin/genericTrap.sh -l |
| 汎用トラップ処理をオンにする | /opt/CSCOlumos/bin/genericTrap.sh -u |

## SNMP トラップに基づく汎用イベントのカスタマイズ

Cisco EPN Manager では、GUIでの汎用イベントのカスタマイズ表現がサポートされています。管理対象オブジェクトは通常、数値形式のSNMPトラップオブジェクト識別子 (SnmpTrapOID) および可変バインドオブジェクト識別子 (VarBindOid) を含む SNMP トラップと通知を生成します。Cisco EPN Manager は、カスタマイズされた MIB モジュールを使用して SnmpTrapOID と VarBindOID の数値をわかりやすい名前に変換し、Web GUI (イベントテーブル、[デバイス 360 (Device 360)] ビューなど) に汎用イベントを表示します。汎用イベントの詳細については、[アラームおよびイベントはどのように作成および更新しますか。](#) を参照してください。

Cisco EPN Manager にパッケージされている SNMP MIB ファイルを使用して、各自の展開環境のテクノロジー要件に合わせて、定義されている MIB をカスタマイズできます。

次の表に、ObjectID の復号化方法と GUI での表示方法を示します。

表 3: 例 : ObjectID 表現

| 復号化前の OID  | 復号化後の OID  |
|--|--|
| snmpTrapOID = 1.3.6.1.4.1.9.10.120.0.1',<br>Values:<br>1.3.6.1.4.1.9.10.119.1.1.2.1.11.7.1=1 | mplsL3VpnVrfDown,<br>values: mplsL3VpnVrfOperStatus.("vrf1").(1) = 1 |

次の手順に従い、カスタム汎用イベントを作成します。

- ステップ 1 [モニタ (Monitor)] > [モニタリング ツール (Monitoring Tools)] > [アラームおよびイベント (Alarms and Events)] の順に選択します。
- ステップ 2 [イベント (Events)] タブをクリックします。
- ステップ 3 [カスタムトラップイベント (Custom Trap Events)] をクリックし、次に [新しい MIB のアップロード (Upload New Mibs)] をクリックします。
- ステップ 4 [MIB のアップロード (Upload Mib)] ウィンドウで、[新しい MIB のアップロード (Upload New MIB)] をクリックし、MIB ファイルをアップロードします。

**ステップ 5** 新しいMIB ファイルをアップロードする場合は、ファイルのアップロードが完了するまで待機してから、[MIB の更新 (Refresh MIBs)] をクリックします。新しく追加された MIB が [MIB] ドロップダウンリストに含まれるようになります。

**ステップ 6** [OK] をクリックします。

Cisco EPN Manager は、指定されたトラップの新しいイベント タイプとアラーム条件を作成します。

---

## 障害処理エラーのトラブルシュート

導入環境で障害処理に問題が発生している場合、次の手順に従って障害ログを確認します。

**ステップ 1** 管理者権限を持つユーザ ID を使用して Cisco EPN Manager にログインします。

**ステップ 2** [管理 (Administration)] > [設定 (Settings)] > [ロギング (Logging)] を選択し、[グローバル設定 (Global Settings)] タブを選択します。

**ステップ 3** [ダウンロード (Download)] をクリックしてすべてのサーバのログファイルをダウンロードします。

**ステップ 4** これらのログ ファイルに記録されたアクティビティを、管理アプリケーションで参照しているアクティビティと比較します。

```
console.log
ncs-x-x.log
decap.core.java.log
xmp_correlation.log
decap.processor.log
```

---

### 次のタスク

シスコ サポート コミュニティからも援助を受けられます。サポート ケースを開く必要がある場合は、疑わしいログファイルをケースに添付します。[シスコ サポート コミュニティとテクニカルアシスタンスセンター \(TAC\) から支援を受ける \(30 ページ\)](#) を参照してください。

## シスコ サポート コミュニティとテクニカル アシスタンスセンター (TAC) から支援を受ける

- [シスコ サポート ケースの登録 \(31 ページ\)](#)
- [シスコ サポート コミュニティへの参加 \(32 ページ\)](#)

## シスコ サポート ケースの登録

Web GUI からサポート ケースを登録すると、Cisco EPN Manager ではデバイスから取得できる情報が、このケース フォームに自動的に読み込まれます。これには、デバイスの技術的な詳細、デバイスでの設定変更、および過去 24 時間以内に発生したすべてのデバイス イベントなどがあります。また、ケースに各自のファイルを添付することもできます。

### 始める前に

次の状況では、Web GUI でサポート ケースを登録できます。

- 管理者により、ユーザがこの作業を実行できるように Cisco EPN Manager が設定されている。シスコサポート リクエストのデフォルトの設定を参照してください。
- Cisco EPN Manager サーバがインターネットに直接接続しているか、またはプロキシサーバ経由で接続している。
- Cisco.com のユーザ名とパスワードがある。

---

**ステップ 1** 次のいずれかを実行します。

- [モニタ (Monitor)] > [モニタリング ツール (Monitoring Tools)] > [アラームおよびイベント (Alarms and Events)] の順に選択します。アラームを 1 つクリックし、[トラブルシュート (Troubleshoot)] > [サポート ケース (Support Case)] を選択します。[トラブルシュート (Troubleshoot)] ボタンが表示されない場合は、ブラウザ ウィンドウを拡大します。
- [デバイス 360 (Device 360)] ビューで、次の手順に従います。デバイスの IP アドレスの上にマウスを移動し、情報アイコンをクリックします。[アクション (Actions)] ドロップダウンメニューから [サポート リクエスト (Support Request)] を選択します。

**ステップ 2** Cisco.com ユーザ名とパスワードを入力します。

**ステップ 3** [作成 (Create)] をクリックします。Cisco EPN Manager は、デバイスから取得したデータをフォームに読み込みます。

**ステップ 4** (オプション) 組織のトラブル チケット システムに対応したトラッキング番号を入力します。

**ステップ 5** [次へ (Next)] をクリックして、問題の説明を入力します。

Cisco EPN Manager では、デバイスから取得したデータがフォーム読み込まれ、必要なサポート ドキュメントが自動的に生成されます。

必要に応じて、ローカル マシンからファイルをアップロードします。

**ステップ 6** [サービス リクエストの作成 (Create Service Request)] をクリックします。

---

## シスコ サポート コミュニティ への参加

オンラインシスコサポートコミュニティ内のディスカッションフォーラムにアクセスして、参加できます。Cisco.com のユーザ名とパスワードが必要です。

---

**ステップ1** 次のいずれかを実行します。

- **[Monitor] [>] [Monitoring Tools] [>] [Alarms and Events]** に移動します。いずれかのアラームをクリックし、**Troubleshoot > Support Forum** を選択します。**[Troubleshoot]** ボタンが表示されない場合は、ブラウザ ウィンドウの幅を広げてください。
- **[デバイス 360 (Device 360)]** ビューで、次の手順に従います。デバイスの IP アドレスの上にマウスを移動し、情報アイコンをクリックします。**[アクション (Actions)]** ドロップダウンメニューから、**[サポート コミュニティ (Support Community)]** を選択します。

**ステップ2** シスコ サポート コミュニティ フォーラムのページで、必要な情報を見つけるための検索パラメータを入力します。

---