障害管理タスク

（注） アドバンスユーザーは、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

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。サーバーは、自動的に UDP ポート 162 でこれらのイベントをリッスンします。サー

バー上でイベント 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 をリッスンしている必要があります。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。

（注） SNMPv3 形式を使用する通知受信者には、一意のユーザー名が必要です。2 つ以上の通知受信者が同じユーザー名でパスワードが異なる場合、そのうちの 1 つが機能しません。

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 （12 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、サーバーの問題を示す 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ー 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ー 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、次のユーザー 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、ユーザーが実行できるタスクの表示と変更を参照してください。

ユーザー ロール	アクセス権限
ルート ドメインを持つルート ユーザー	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。

ユーザー ロール	アクセス権限
非ルート ドメインを持つルート ユーザー	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ー	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 ユーザー	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。
ルートドメインを持つシステム モニタリング ユーザー	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ー	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 ユーザー	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 ユーザー	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	• 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。 • 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。 • 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。 • 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。

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	• 連絡先名は、トラップ受信者ごとに一意です。 • トラップ受信者は、ROOT-DOMAIN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ROOT-DOMAIN でのみ適用可能です。 • 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。 • ゲストアクセストラップ受信者は、ゲスト クライアントに関係するアラームだけを受信します。

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

通知ポリシー ページで選択されたカテゴリ	注意事項
	• 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。 • 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。

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通知するために、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 ＋ 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。

a) [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。

b) [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。

c) [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。

d) [連絡先の氏名（Contact Full Name）] に連絡先の氏名を入力します。

e) [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。

f) [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。

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) [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 [サーバー名（Server Name）] に値を入力します。

c) [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。

d) [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。

e) [SMNPバージョン（SMNP Version）] として [v3（v3）] を選択する場合、[ユーザー名（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。

f) [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。

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) [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。

d) [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。

e) [SMNPバージョン（SMNP Version）] として [v3（v3）] を選択する場合、[ユーザー名（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。

f) [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。

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。
- [通知ポリシー（Notification Policies）] ページには、[モニター（Monitor）] > [モニタリングツール（Monitoring Tools）] > [通知ポリシー（Notification Policies）] [モニター（Monitor）] > [モニタリングツール（Monitoring Tools）] > [アラーム通知ポリシー（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。

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、特定の電子メール受信者、ノースバウンドトラップ受信者、および restconf 受信者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) [Add] アイコンをクリックします。

b) 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。

c) [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 [ユーザー定義（User Defined）] を選択すると、設定されているユーザー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 [ユーザー定義（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ー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。

d) [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。

e)  アイコンをクリックし、[通知先の追加（Add Destination）] ウィンドウに必要な詳細を入力します。[連絡先のタイプの選択（Select Contact Type）] 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）] オプションのいずれかを選択できます。

f) [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。

g) **[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、  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 Evolved Programmable Network 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 Evolved Programmable Network 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 Evolved Programmable Network 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 サーバー
- 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 Evolved Programmable Network 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 Evolved Programmable Network 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、内部サーバー 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 サーバーを設定していない場合は、「SMTP 電子メール サーバーの設定」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、ユーザー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、8,000,000 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。
- [クリア済みのアラームを非表示（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 [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。
- [[アラーム]タブにアクティブアラームのみを表示（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 [アラーム（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、ユーザー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ると（[モニター（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）]）、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。

- [電子メール通知にCisco EPN Managerアドレスを追加（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）]：この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 [その他の設定（Miscellaneous Settings）] を変更します。

- [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 カウントが有効になります。
- [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相関ツリーからのサブツリー作成を有効化（Enable creation of subtrees from a correlation tree when root cause of the tree clears）]：相関ツリーの根本原因がクリアされたときに、この相関ツリーのサブツリーが作成されます。各サブツリーに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、この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選択されている場合、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）]：Cisco EPN Manager 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、（デバイスで生成されていない、ネットワーク内で失われた、といったことが原因で）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。
- [ユーザー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は適用されません。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 （24 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（**[モニター（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 ノード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。

- [一時的な状態アラームの有効化（Enable Transient Condition Alarms）]：このチェックボックスをオンにすると、Cisco EPN Manager は一時的なイベントをアラームとして処理し、これらのイベントを [アラーム（Alarms）]テーブルに表示します。デフォルトでは、このチェックボックスはオフになっています。
- [ネットワークアラームビューの有効化（Enable Network Alarms View）]：このオプションを選択すると、[ネットワークアラーム（Network Alarms）] タブが [アラーム（Alarms）] タブに追加されます。**[ネットワークアラーム（Network Alarms）]** タブには、ネットワークに影響するすべてのアラームが一覧表示されます。デフォルトでは、このオプションは無効になっています。
- [NBI Web Socketのクライアントに対して通知ポリシーベースのフィルタを有効にする（Enable Notification Policy based filter for NBI WebSocket's Client）]：このチェックボックスをオンにすると、アラーム通知ポリシーで restconf が有効になり、ノースバウンド WebSocket の接続先が追加されます。
- [Netconfセッションの最大再試行回数（Max no. of Netconf Session Retry）]：Netconf セッションで接続して SVO 障害を処理することを試みる回数を入力します。
- [Netconfセッションの再試行間隔（Netconf Session Retry Interval）]：Netconf セッションが SVO 障害を処理できるようにするために、再試行の間隔を秒単位で入力します。
- [通知で送信されるデバイスUDFの有効化（Enable Device UDF to be sent in notifications）]：このチェックボックスをオンにすると、デバイス UDF のアラーム通知が有効になります。
- [アラームなし（NA）状態アラームの有効化（Enable Not Alarmed (NA) Condition Alarms）]：このチェックボックスをオンにすると、イベントが光デバイスのアラームとして処理されなくなります。
- [SVOデバイスのアラームとイベントの再生サポートの有効化（Enable Alarms & Events Replay support for SVO Devices）]：このチェックボックスをオンにすると、SVO デバイスの Netconf 再生が有効になります。これにより、ネットワーク接続障害、SVO スイッチオーバー、デバイスのダウンタイム、またはその他の接続障害中に失われたイベントが再生されます。
- [SVOデバイスのアラームとイベントの再生時間（Duration for the Alarms & Events Replay for SVO Devices）]：アラームとイベントの同期に必要な最長期間を入力します。デフォルトオプションは 720 分または 12 時間です。このフィールドに長い期間を入力しないことをお勧めします。
- [メンテナンスモードでカード/ポートのアラームとイベントを抑制できるようにする（Enable to suppress Alarms and Events for card/port in maintenance mode）]：このチェックボックスをオンにすると、メンテナンスモードのラインカード/ポートによって生成されたトラップ、アラーム、または syslog が抑制されます。

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 （19 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、個別のユーザーが（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、ユーザー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ーが調整できますが、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。 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。 （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。 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。 （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す。

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。`/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 サーバーとの 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 サーバーとの 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 の各アラームにはシビラティ（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シビラティ（重大度）を変更することにより、アラームのシビラティ（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、サーバーの内部 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。

entsensor アラームの場合、デフォルトの重大度設定ページを使用してデフォルトの重大度を変更しないでください。

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 モ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。

a) イベントのチェックボックスをオンにします。

b) [シビラティ（重大度）（Severity）] ドロップダウンリストからシビラティ（重大度）を選択し、[保存（Save）] をクリックします。

（注） [カスタムSyslog（Custom Syslog）] の場合、[アラームのシビラティ（重大度）と自動クリア（Alarm Severity and Auto Clear）] ページで変更した [シビラティ（重大度）（Severity Level）] は、**[アラームおよびイベント（Alarms and Events）]** > **[Syslog（Syslog）]** タブに反映されません。

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ー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が変更されることはありません。

自動クリアの期間は、55 分までは 5 分間隔で設定できます。この時間を超えると、1 時間または 60 分の倍数で間隔を設定できます。

（注）
- アラームの自動クリアを有効にしている場合、作成されたアラームのクリアに遅延が生じることがあります。
- 自動クリア間隔を 1 時間未満に設定すると、システムパフォーマンスに影響する可能性があります。

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 [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、イベントタイプを検索します。

ステップ 3 自動クリア期間を変更するには、1 つ以上のイベントを選択して、[アラームの自動クリア（Alarm Auto Clear）] ボタンをクリックします。

ステップ 4 [OK（OK）] をクリックして、自動クリア期間を保存します。

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。

システムのイベントスロットル

Cisco EPN Manager は、イベントスロットルを設定してシステムレベルでイベントをチェックすることにより、ネットワークの輻輳をチェックします。

ネットワーク内のキュー占有率が 60% を超えると、イベントのドロップが開始されます。このようなシナリオでは、次のメッセージが表示されます。

「システムイベント処理キューが、設定されている上限しきい値に達しました。イベントのドロップを回避するには、持続的に高いネットワークイベントレートをチェックしてください。（The system event processing queue has reached the configured upper threshold value. Please check for sustained high network event rate to avoid dropping of events.）」

ネットワーク内のキュー占有率が完全な容量に達した場合、次のメッセージが表示されます。

「システムイベント処理キューが満杯であり、最も古いイベントがキューからドロップされます。ドロップされたイベントの詳細は、assure_fault.logで確認してください。（The system event processing queue is full and oldest events from the queue will be dropped. Please find the details of the dropped events in assurance_fault.log.）」

どちらのシナリオでも、ネットワーク障害や、大量の着信ネットワークイベントの原因となる要因を確認することをお勧めします。

上限しきい値のパーセント値はキュー容量の 60% に設定され、超えるとアラームが生成されます。システムが下限しきい値の 30% に達すると、アラームはクリアされます。

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

タイプ（Type）	サポートされるイベント
カード保護	CARD_PROTECTION-4-PROTECTION CARD_PROTECTION-4-ACTIVE
VLAN	PORT_SECURITY-6-VLAN_REMOVED PORT_SECURITY-6-VLAN_FULL
ICCP SM	L2-L2VPN_ICCP_SM-4-REMOTE_CORE_ISOLATION L2-L2VPN_ICCP_SM-4-REMOTE_CORE_ISOLATION_CLEAR L2-L2VPN_ICCP_SM-3-CONFIG_LOCAL_ERROR L2-L2VPN_ICCP_SM-3-CONFIG_REMOTE_ERROR L2-L2VPN_ICCP_SM-4-LOCAL_CORE_ISOLATION L2-L2VPN_ICCP_SM-4-LOCAL_CORE_ISOLATION_CLEAR L2-L2VPN_ICCP_SM-4-PEER_REACHABILITY_FAILURE L2-L2VPN_ICCP_SM-4-PEER_REACHABILITY_CLEAR L2-L2VPN_ICCP_SM-4-REMOTE_ACCESS_MAIN_PORT_FAILURE L2-L2VPN_ICCP_SM-4-REMOTE_ACCESS_MAIN_PORT_FAILURE_CLEAR INFRA-ICCP-5-ISOLATION INFRA-ICCP-5-ISOLATION_CLR INFRA-ICCP-5-NEIGHBOR_STATE_UP INFRA-ICCP-5-NEIGHBOR_STATE_DOWN INFRA-ICCP-6-BACKBONE_INTERFACE_STATE_UP INFRA-ICCP-6-BACKBONE_INTERFACE_STATE_DOWN L2-BM-6-ACTIVE_CLEAR L2-BM-6-ACTIVE_PROBLEM L2-L2VPN_ICCP_SM-3-CONFIG_INVALID_NODEID L2-L2VPN_ICCP_SM-3-CONFIG_INVALID_NODEID_CLEAR
衛星	PKT_INFRA-ICPE_GCO-5-SATELLITE_STATUS_PROBLEM PKT_INFRA-ICPE_GCO-5-SATELLITE_STATUS_CLEAR
クラスタ	PLATFORM-REDDRV-7-ROLE_CHANGE PLATFORM-CE_SWITCH-6-UPDN PLATFORM-CLUSTER_CLM-6-UPDN LINK_UP 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 syslog	MGBL-CONFIG-6-DB_COMMIT 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
BurstThreshold	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。
BurstHoldOffTimer	インベントリ同期が保留される期間。	300000 ミリ秒（5 分）
BurstCheckRetryCount	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ー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が確認されます。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 （28 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 によって継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 （30 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 Evolved Programmable Network 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 Evolved Programmable Network Manager は、受信した syslog またはトラップについて Cisco Evolved Programmable Network 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 Evolved Programmable Network 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 Evolved Programmable Network 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', Values: 1.3.6.1.4.1.9.10.119.1.1.2.1.11.7.1=1`	`mplsL3VpnVrfDown, 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 **[モニター（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、[追加（Add）] をクリックします。

ステップ 4 [新しいカスタムトラップイベントの追加（Add New Custom Trap Events）] ウィンドウで、MIB ファイルをアップロードし、必要な詳細を入力します。

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する場合、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ー 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ー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

（注） Cisco EPN Manager から [リセット（Reset）] をクリックしてグローバル設定をリセットすることはできません。

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 （31 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

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、ユーザー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 サーバー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 サーバー経由で接続している。
- Cisco.com のユーザー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。

- **[モニター（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 つ選択し、[>>] アイコンをクリックして、**[トラブルシュート（Troubleshoot）]** > **[サポート ケース（Support Case）]** の順に選択します。[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 ユーザー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、デバイスから取得するデータをこの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 のユーザー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。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。