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

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ッスンします。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。

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 （4 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 （4 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。

アラームとイベントを電子メール通知として転送する（管理者手順）

電子メール通知を設定すると、条件に一致するアラームが作成または更新されたときに、設定済み受信者に電子メールが送信されます。デフォルトでは、件名にアラームの重大度とカテゴリが含まれます。これらの設定とメッセージモードは、アラームおよびイベントに関するシステム設定ページから制御できます。詳細については、電子メール通知のデフォルト設定 （4 ページ）を参照してください。

一般の（サポートされていない）イベントを転送する必要がある場合には、一般イベントの処理が有効化されていることを確認してください。（設定を確認するには、汎用トラップおよび Syslog の処理の無効化および有効化 （17 ページ）を参照してください。）

また、アラームおよびイベントを SNMP トラップ通知として転送することもできます。詳細については、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 （4 ページ）を参照してください。

さらに、ユーザは [アラームおよびイベント（Alarms and Events）] ページから電子メール通知を設定することもできます。ユーザはイベントと重大度、および特定の受信者の電子メール アドレスを指定できます。

始める前に

メール サーバをまだ設定していない場合は、SMTP 電子メール サーバの設定の手順を実行します。これを行わないと、通知は送信されません。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[メールと通知（Mail and Notification）] > [メール サーバ設定（Mail Server Configuration）]** を選択します。

ステップ 2 [送信者と受信者（Sender and Receivers）] エリアで、受信者を追加します。複数の受信者をカンマ区切りリストで指定できます。

特定のカテゴリのアラームの転送先	実行する手順
同じ受信者	**1.** [宛先（To）] フィールドに、受信者を入力します。複数の受信者はカンマ区切りリストで指定します。 **2.** [個々のアラーム カテゴリ用の電子メール通知の設定（Configure email notification for individual alarm categories）] ハイパーリンクをクリックし、通知用のデータを指定します。 • 含めるアラームを選択します。 （注） サーバ内部SNMPトラップを転送する場合は、[システム（System）] カテゴリを選択します。 • 特定の重大度のアラームを指定するには、アラーム名のハイパーリンクをクリックして、重大度を選択します。 （注） アラーム重大度を指定する場合には、受信者の電子メール アドレスを入力しないでください。 **3.** [保存（Save）] をクリックしてアラーム カテゴリとその設定を保存します。
異なる受信者	**1.** [宛先（To）] フィールドに電子メール アドレスを入力しないでください。 **2.** [個々のアラーム カテゴリ用の電子メール通知の設定（Configure email notification for individual alarm categories）] ハイパーリンクをクリックします。 （注） サーバ内部SNMPトラップを転送する場合は、[システム（System）] カテゴリを選択します。 **3.** 対象のアラームを選択します。アラーム リンクをクリックし、[クリティカル（Critical）]、[メジャー（Major）]、[マイナー（Minor）]、または [警告（Warning）] を選択して、重大度を指定できます。 （注） サーバ内部SNMPトラップを転送する場合は、[システム（System）] カテゴリを選択します。 **4.** [保存（Save）] をクリックしてアラーム カテゴリとその設定を保存します。

ステップ 3 [テスト（Test）] をクリックすると、設定済みパラメータを使用してテスト メールが送信されます。テスト操作の結果は同じページに表示されます。このテスト機能では「Cisco EPN Manager test email」という件名の電子メールを送信することで、プライマリ メール サーバとセカンダリ メール サーバへの接続が確認されます。

ステップ 4 [保存（Save）] をクリックして新しい通知を保存します。

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。

メール通知の設定については「アラームとイベントを電子メール通知として転送する（管理者手順） （2 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 SNPv3 トラップ通知として、アラームとイベントを EPM-NOTIFICATION-MIB フォーマットで転送できます。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。

通知を送信する前に、Cisco EPN Manager は受信者に対して ping を実行し、到達可能であることを確認します。ping に対して応答がなければ、デバイスが到達不能であることを通知するアラームが生成されます。

（注） Cisco EPN Manager はトラップを通知レシーバのポート 162 に送信します。

アラームとイベントは電子メール通知として転送することもできます。詳細については、アラームとイベントを電子メール通知として転送する（管理者手順） （2 ページ）を参照してください。

ステップ 1 管理権限を持つユーザとして、**[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）] > [通知レシーバ（Notification Receivers.）]** を選択します。

ステップ 2 [コマンドの選択（Select a Command）] ドロップダウン リストから [通知レシーバの追加（Add Notification Receive）] を選択し、[実行（Go）] をクリックします。

ステップ 3 新しい通知レシーバを設定します。

a) IP アドレスとサーバ名を入力します。

- [IP アドレス（IP Address）]：レシーバが稼働するサーバの IPv4 アドレスまたは IPv6 アドレスを入力します。
- [サーバ名（Server Name）]：レシーバが稼働するサーバのホスト名を入力します。

b) [ノースバウンド（North Bound）] オプション ボタンをクリックします。デフォルトでは、通知タイプは UDP に設定されます。

c) ポート番号と SMNP バージョンを入力します。設定するレシーバは、設定されたポートと同じポートで UDP を待ち受ける必要があります。

（注） ポート番号は変更できません。

- SNMPv2c の場合、コミュニティ ストリングを入力します。
- SNMPv3 の場合、ユーザ名とパスワードを入力し（エンジン ID が自動的に取り込まれます）、[モード（Mode）] ドロップダウン リストから（セキュリティ レベルに応じた）モードを選択します。

ステップ 4 転送対象とするアラームおよびイベントのカテゴリと（アラームの場合は）重大度を指定します。

（注） 汎用イベントが転送されるのは、汎用イベント処理が有効になっている場合のみです。設定を確認するには、汎用トラップおよび Syslog の処理の無効化および有効化 （17 ページ）を参照してください。

- [カテゴリ（Category）] セクションで、転送するすべてのアラーム タイプをオンにします。サーバの内部 SNMP トラップを転送する場合は、[システム（System）] を選択します。
- [重大度（Severity）] で、トラップ通知自体を設定したときに設定した最高の重大度レベルを選択します。

ステップ 5 完了したら、[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 （4 ページ）
- 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アラームブラウザで非表示（Hide cleared alarms in alarm browser）	[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。 （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。

イベント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 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 [イベント タイプのアラーム状態（Event Types Alarm Condition）] 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 タイプのアラーム状態（Event Types Alarm Condition）] 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 タイプのアラーム状態を検索します。

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が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。

（注） [アラーム自動クリア（Alarm Auto Clear）] ボタンは、自動クリアイベントが設定されていないイベントに対してのみ有効になります。

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。

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 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
```

詳細なインベントリのイベント レート フロー コントローラ

詳細なインベントリは、生成されたイベントを識別し、デバイスで行われた変更のみを処理します。イベントの流入によるデバイスの継続的な同期を避けるために、詳細なインベントリではバースト イベント レート フロー コントローラが使用されます。

同じイベントのインスタンスが 100 以上ある場合、Cisco EPN Manager はバースト イベントと見なします。このシナリオでは、しきい値を超えたイベントのインベントリ同期が一定期間保留され、間隔を置いてしきい値が再計算されます。許容される回数の再計算を行っても、しきい値を超過している場合、Cisco EPN Manager はデバイスに対するすべての処理を停止します。唯一の解決方法は、ユーザがバーストイベントの原因となっている問題の解決に関連するアクションを実行することです。

Cisco EPN Manager には複数のルール ファイルがあり、/opt/CSCOlumos/conf/fault/correlationEngine に保存されています。イベント設定は、文字列 **EventBasedInventoryRules.xml** で終わるファイルによって制御されています。

次のバースト イベント アクション プロパティを設定できます。

表 *1:* バースト イベント アクション

プロパティ名	説明	デフォルト値
BurstThreshold	特定の時点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
BurstHoldOffTimer	インベントリ同期が保留される期間	300000 ミリ秒
BurstCheckRetryCount	再計算の許容回数	3

システム アラーム（**[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）]**ページ）によってユーザにバースト モードが通知され、ユーザは適切なアクションを実行できます。イベント流入の問題が解決されると、アラームはクリアされて [クリア済みのアラーム（Cleared Alarms）] タブに表示されます。アクティブなアラームの情報は、デバイス 360 ページでも確認できます。

バースト モードのモニタ対象となるイベントの一覧を次に示します。

表 *2:* バースト モード：サポートされるイベント

テクノロジー	サポートされるイベント
MPLS	MPLS_TE-5-LSP_Down MPLS_TE-5-LSP_Active_StandBy MPLS_TE-5-LSP_CLEAR ROUTING-MPLS_TE-5-LSP_UPDOWN ROUTING-MPLS_TE-5-S2L_SIGNALLING_STATE mplsLdpSessionDown mplsLdpSessionUp
疑似回線	cpwVcUp cpwVcDown L2-L2VPN_PW-3-UPDOWN L2-L2VPN_PW-3-UPDOWN_Clear XCONNECT-5-PW_STATUS XCONNECT-5-PW_STATUS_Clear EVPN-5-VC_STATUS EVPN-5-VC_STATUS_Clear
LDP	mplsLdpSessionDown mplsLdpSessionUp
BGP	cbgpBackwardTransition cbgpFsmStateChange cbgpPrefixThresholdExceeded cbgpPrefixThresholdClear bgpBackwardTransition bgpEstablished cbgpPeer2BackwardTransition cbgpPeer2FsmStateChange cbgpPeer2PrefixThresholdClear cbgpPeer2PrefixThresholdExceeded BGP-5-ADJCHANGE BGP-5-ADJCHANGE_DOWN BGP-5-ADJCHANGE_UP BGP-3-NOTIFICATION ROUTING-BGP-5-ADJCHANGE ROUTING-BGP-5-UPDATE_FILTERED
ISIS	CLNS-5-ADJCHANGE CLNS-5-ADJCHANGE_UP CLNS-5-ADJCHANGE_DOWN ROUTING-ISIS-5-ADJCHANGE ROUTING-ISIS-5-ADJCHANGE_UP ROUTING-ISIS-5-ADJCHANGE_DOWN ROUTING-ISIS-4-ADJCHANGE ROUTING-ISIS-4-ADJCHANGE_UP ROUTING-ISIS-4-ADJCHANGE_DOWN isisAdjacencyChange isisAdjacencyChangeDown isisAdjacencyChangeUp isisAdjacencyChangeInit

テクノロジー	サポートされるイベント
OSPF	OSPF-5-ADJCHG OSPF-5-ADJCHG_DOWN OSPF-5-ADJCHG_UP OSPFv3-5-ADJCHG OSPFv3-5-ADJCHG_DOWN OSPFv3-5-ADJCHG_UP ROUTING-OSPF-5-ADJCHG ROUTING-OSPFv3-5-ADJCHG ROUTING-OSPFv3-5-ADJCHG_DOWN ROUTING-OSPFv3-5-ADJCHG_UP

（注） ルール ファイルを編集した後に Cisco EPN Manager を再起動する必要はありません。変更は、ルール ファイルを保存した時点から有効になります。

次のイベントはバースト モードのモニタ対象ではなく、詳細なインベントリによって通常どおり処理されます。

```
G8032:
G8032-STATE_IDLE
G8032-STATE_PENDING
G8032-STATE_PROTECTION
G8032-STATE_FORCED_SWITCH
G8032-STATE_MANUAL_SWITCH
L2-G8032-3-APS_CHANNEL_INACTIVE
L2-G8032-6-APS_CHANNEL_ACTIVE

CEM:
SONET-4-ALARM_SLOS
SONET-4-ALARM_SLOS_Clear
SONET-4-ALARM_SLOF
SONET-4-ALARM_SLOF_Clear
SONET-4-ALARM_LAIS
SONET-4-ALARM_LAIS_Clear
SONET-4-ALARM_LRDI
SONET-4-ALARM_LRDI_Clear
SONET-4-ALARM_PAIS
SONET-4-ALARM_PAIS_Clear
SONET-4-ALARM_PLOP
SONET-4-ALARM_PLOP_Clear
SONET-4-ALARM_PUNEQ
SONET-4-ALARM_PUNEQ_Clear
SONET-4-ALARM_PPLM
SONET-4-ALARM_PPLM_Clear
SONET-4-ALARM_PRDI
SONET-4-ALARM_PRDI_Clear
SONET-4-ALARM_LOM
SONET-4-ALARM_LOM_Clear
SONET-4-ALARM_B1-TCA
SONET-4-ALARM_B1-TCA_Clear
SONET-4-ALARM_B2-TCA
SONET-4-ALARM_B2-TCA_Clear
SONET-4-ALARM_B3-TCA
SONET-4-ALARM_B3-TCA_Clear
SONET-4-ALARM_APS
SONET-4-ALARM_APS_Clear
SONET-4-UPSR_Working
SONET-4-UPSR_Working_Clear
```

```
SONET-4-UPSR_Protect
SONET-4-UPSR_Protect_Clear
CONTROLLER-5-UPDOWN_Clear
CONTROLLER-5-UPDOWN
dsx1LoopbackState
dsx1LoopbackState_CLEAR
dsx1RcvAIS
dsx1RcvAIS_CLEAR
dsx3RcvAIS
dsx3RcvAIS_CLEAR
dsx3LOS
dsx3LOS_CLEAR
dsx3LoopbackState
dsx3LoopbackState_CLEAR
dsx1LossOfSignal
dsx1LossOfSignal_CLEAR
SONET-4-ALARM_VT_TRACE_MISMATCH
SONET-4-ALARM_VT_TRACE_MISMATCH_Clear
SONET-4-ALARM_VT_PATH_LOP
SONET-4-ALARM_VT_PATH_LOP_Clear
SONET-4-ALARM_VT_UNEQUIPPED
SONET-4-ALARM_VT_UNEQUIPPED_Clear
SONET-4-ALARM_VT_PATH_RDI
SONET-4-ALARM_VT_PATH_RDI_Clear
CONTROLLER-5-UPDOWN_VT_PATHAIS
CONTROLLER-5-UPDOWN_VT_PATHAIS_Clear
CONTROLLER-5-UPDOWN_VT_PATHLOP
CONTROLLER-5-UPDOWN_VT_PATHLOP_Clear
CONTROLLER-5-UPDOWN_VT_UNEQUIPPED
CONTROLLER-5-UPDOWN_VT_UNEQUIPPED_Clear
CONTROLLER-4-ACR_DCR_CLOCK_DS1
CONTROLLER-4-ACR_DCR_CLOCK_DS3
CONTROLLER-4-ACR_DCR_CLOCK_DS3_CHANNEL
CONTROLLER-4-ACR_DCR_CLOCK_OCN_VT
CONTROLLER-4-ACR_DCR_CLOCK_OCN_CT3
CONTROLLER-4-ACR_DCR_CLOCK_OCN_T3
CONTROLLER-4-ACR_DCR_CLOCK_DS1_FREERUN
CONTROLLER-4-ACR_DCR_CLOCK_DS1_ACQUIRING
CONTROLLER-4-ACR_DCR_CLOCK_DS1_HOLDOVER
CONTROLLER-4-ACR_DCR_CLOCK_DS3_FREERUN
CONTROLLER-4-ACR_DCR_CLOCK_DS3_ACQUIRING
CONTROLLER-4-ACR_DCR_CLOCK_DS3_ACQUIRED
CONTROLLER-4-ACR_DCR_CLOCK_DS3_HOLDOVER
CONTROLLER-4-ACR_DCR_CLOCK_DS3_CHANNEL_FREERUN
CONTROLLER-4-ACR_DCR_CLOCK_DS3_CHANNEL_ACQUIRING
CONTROLLER-4-ACR_DCR_CLOCK_DS3_CHANNEL_ACQUIRED
CONTROLLER-4-ACR_DCR_CLOCK_DS3_CHANNEL_HOLDOVER
CONTROLLER-4-ACR_DCR_CLOCK_OCN_VT_FREERUN
CONTROLLER-4-ACR_DCR_CLOCK_OCN_VT_ACQUIRING
CONTROLLER-4-ACR_DCR_CLOCK_OCN_VT_ACQUIRED
CONTROLLER-4-ACR_DCR_CLOCK_OCN_VT_HOLDOVER
CONTROLLER-4-ACR_DCR_CLOCK_OCN_CT3_FREERUN
CONTROLLER-4-ACR_DCR_CLOCK_OCN_CT3_ACQUIRING
CONTROLLER-4-ACR_DCR_CLOCK_OCN_CT3_ACQUIRED
CONTROLLER-4-ACR_DCR_CLOCK_OCN_CT3_HOLDOVER
CONTROLLER-4-ACR_DCR_CLOCK_OCN_T3_FREERUN
CONTROLLER-4-ACR_DCR_CLOCK_OCN_T3_ACQUIRING
CONTROLLER-4-ACR_DCR_CLOCK_OCN_T3_ACQUIRED
CONTROLLER-4-ACR_DCR_CLOCK_OCN_T3_HOLDOVER
SONET-4-UPSR
DSX-ALARM_DS1_LOS
DSX-ALARM_DS1_LINK_DOWN
DSX-ALARM_DS1_AIS
DSX-ALARM_DS1_RAI
```

DSX-ALARM_DS1_LOF
DSX-ALARM_DS1_RX_LOMF
DSX-ALARM_DS3_RX_RAI
DSX-ALARM_DS3_TX_RAI
DSX-ALARM_DS3_RX_AIS
DSX-ALARM_DS3_TX_AIS
DSX-ALARM_DS3_RX_LOF
DSX-ALARM_DS3_RX_LOS
DSX-ALARM_DS3_RX_IDLE
DSX-ALARM_DS3_OTHER_FAILURE
DSX-ALARM_DS3_LINK_DOWN
DSX-ALARM_DS3_ADMIN_DOWN
DSX-ALARM_DS1_OOF
SDH-ALARM_DS3_TX_AIS
SDH-ALARM_DS3_TX_AIS_Clear
SDH-ALARM_DS3_RX_LOF
SDH-ALARM_DS3_RX_LOF_Clear
SDH-ALARM_DS3_RX_LOS
SDH-ALARM_DS3_RX_LOS_Clear
SDH-ALARM_DS3_OTHER_FAILURE
SDH-ALARM_DS3_OTHER_FAILURE_Clear
SDH-ALARM_DS3_RX_IDLE
SDH-ALARM_DS3_RX_IDLE_Clear
SDH-ALARM_LO_PAIS
SDH-ALARM_LO_PAIS_Clear
SDH-ALARM_LO_PLOP
SDH-ALARM_LO_PLOP_Clear
SDH-ALARM_LO_PTIM
SDH-ALARM_LO_PTIM_Clear
SDH-ALARM_LO_PUNEQ
SDH-ALARM_LO_PUNEQ_Clear
SDH-ALARM_LO_PPLM
SDH-ALARM_LO_PPLM_Clear
SDH-ALARM_LO_PRDI
SDH-ALARM_LO_PRDI_Clear
SDH-ALARM_LO_BER_SD_B3
SDH-ALARM_LO_BER_SD_B3_Clear
SDH-ALARM_LO_BER_SF_B3
SDH-ALARM_LO_BER_SF_B3_Clear
SDH-ALARM_LO_LOM
SDH-ALARM_LO_LOM_Clear
SDH-ALARM_LO_PRFI
SDH-ALARM_LO_PRFI_Clear
SDH-ALARM_DS1_LOS
SDH-ALARM_DS1_LOS_Clear
SDH-ALARM_DS1_OOF
SDH-ALARM_DS1_OOF_Clear
SDH-ALARM_DS1_AIS
SDH-ALARM_DS1_AIS_Clear
SDH-ALARM_DS1_RAI
SDH-ALARM_DS1_RAI_Clear
SDH-ALARM_DS1_RX_LOMF
SDH-ALARM_DS1_RX_LOMF_Clear
SDH-ALARM_DS3_RX_AIS
SDH-ALARM_DS3_RX_AIS_Clear
SDH-ALARM_DS3_TX_RAI
SDH-ALARM_DS3_TX_RAI_Clear
SDH-ALARM_DS3_RX_RAI
SDH-ALARM_DS3_RX_RAI_Clear
SDH-ALARM_SONET_LINK_DOWN
SDH-ALARM_SONET_LINK_DOWN_Clear
SDH-ALARM_LRFI
SDH-ALARM_LRFI_Clear
SDH-ALARM_SONET_ADMIN_DOWN

```
SDH-ALARM_SONET_ADMIN_DOWN_Clear
SDH-ALARM_PRFI
SDH-ALARM_PRFI_Clear
SDH-ALARM_SLOS
SDH-ALARM_SLOS_Clear
SDH-ALARM_SLOF
SDH-ALARM_SLOF_Clear
SDH-ALARM_LAIS
SDH-ALARM_LAIS_Clear
SDH-ALARM_LRDI
SDH-ALARM_LRDI_Clear
SDH-ALARM_PAIS
SDH-ALARM_PAIS_Clear
SDH-ALARM_PLOP
SDH-ALARM_PLOP_Clear
SDH-ALARM_PUNEQ
SDH-ALARM_PUNEQ_Clear
SDH-ALARM_PPLM
SDH-ALARM_PPLM_Clear
SDH-ALARM_PRDI
SDH-ALARM_PRDI_Clear
SDH-ALARM_LOM
SDH-ALARM_LOM_Clear
SDH-ALARM_B1
SDH-ALARM_B1_Clear
SDH-ALARM_B2
SDH-ALARM_B2_Clear
SDH-ALARM_SF
SDH-ALARM_SF_Clear
SDH-ALARM_SD
SDH-ALARM_SD_Clear

SyncE:
ciscoNetsyncSelectedT0Clock
ciscoNetsyncInputAlarmStatus
ciscoNetsyncInputSignalFailureStatus
NETCLK-6-SRC_ADD
NETCLK-6-SRC_UPD
NETCLK-6-SEL_CLOCK_SRC
NETCLK-6-ENTER_HOLDOVER
NETCLK-6-SRC_REM

VCOP:
SSFP_VCOP-4-CONF_ADD
SSFP_VCOP-4-CONF_DEL
SSFP_VCOP-4-CONF_EXIST
SSFP_VCOP-4-DEV_REM
SSFP_VCOP-4-DEV_INS
IOSXE_OIR-6-REMSSFP
IOSXE_OIR-6-INSSSFP

Segment Routing:
OS-XTC-5-SR_POLICY_UPDOWN
```

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 （17 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', 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（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）]** の順に選択して、[一般的なロギング オプション（General Logging Options）] を選択します。

ステップ 3 [ログファイルのダウンロード（Download Log File）] 領域で、[ダウンロード（Download）] をクリックします。

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 （19 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。