障害管理タスク

ここでは、次の内容について説明します。

イベントの受信、転送、および通知

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 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 の通知を追加する場合、その追加する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。

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に転送できます。

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（[レポート（Reports）]）

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。
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。

ユーザー ロール	アクセス権限
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かなければならないいくつかのポイントの説明を示します。

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。 • Prime Infrastructure 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。
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、アラームシビラティ（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）とシビラティ（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

通知ポリシー ページで選択されたカテゴリ	注意事項
	ません。 • 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

Prime Infrastructure 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 [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。

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) [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。
f) [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。
g) [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) [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。
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。
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、 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しません。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。

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 [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）] > [通知ポリシー（Notification Policies）] [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）] > [アラーム通知ポリシー（Alarm Notification Policies）]を選択します。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 Prime Infrastructure 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。Prime Infrastructure により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シビラティ（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、すべてのシビラティ（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。

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、Prime Infrastructure 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 [通知宛先（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 （6 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。

（注） [モニター（Monitor）]>[モニタリング ツール（Monitoring Tools）]>[アラム ポリシー（IAlarm Policies）] でアラーム タイプのシビラティ（重大度）を変更する場合は、ノースバウンド トラップの受信者の電子メール受信者には通知が送信されません。

関連トピック

アラーム通知先の設定 （6 ページ）

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

を以前のリリースから最新のバージョンへアップグレードまたは移行すると、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。

では、次のアラームカテゴリがサポートされます。

- 変更監査
- 汎用
- システム
- アプリケーション パフォーマンス
- コンピューティング サーバー
- Nexus VPC スイッチ
- スイッチとルータ
- AP
- アドホック不正
- Clients
- コンテキスト認識型通知
- コントローラ
- カバレッジ ホール
- メッシュ リンク
- モビリティ サービス
- パフォーマンス
- RRM
- 不正 AP

- SE で検出された干渉源
- セキュリティ
- サードパーティ AP
- サードパーティ コントローラ

リリース 3.6 では、次のアラーム カテゴリはサポートされません。

- 自律 AP
- Cisco UCS シリーズ
- ルータ
- スイッチおよびハブ
- 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」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シビラティ（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シビラティ（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

[Administration] > [System Settings] > [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 [Administration > [Settings] > [System Settings] > [Alarms and Events] > [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。

- [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 active and 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。
- [Delete cleared security alarms after]：セキュリティ アラーム、不正 AP アラーム、および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。
- [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、[Security]、[Rogue AP]、または [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。
- [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。
- [最大保持イベント数（Max Number of Events to Keep）]：データベースで保持する必要があるイベントの数を入力します。

Cisco Prime Infrastructure ではデフォルトで、通常のデータ クリーンアップ タスクの一部として古いアラームとイベントが削除され、2 時間ごとにデータベース アラーム テーブルのストレージ サイズが確認されます。アラーム テーブルが 300,000 の上限を超えた場合、Prime Infrastructure はアラーム テーブルのサイズが制限内に収まるまで、クリアされたアラームを最も古いものから削除します。クリアされたアラームを 7 日より長く保持する必要がある場合は、アラーム テーブルのサイズが上限に達しない範囲で、[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）] テキスト ボックスに 7 日を超える値を指定できます。

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。

- [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 [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。シビラティ（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。
- [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 [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 [アラームのまとめ（Alarm Summary）] 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。
- [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、[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、[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たときにユーザーが [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 [電子メールオプションのアラーム（Alarm Email Options）] を次のように変更します。

- [電子メール通知に Prime Infrastructure アドレスを追加（Add Prime Infrastructure 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 Prime Infrastructure アドレスが追加されます。
- [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シビラティ（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。
- [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。
- [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シビラティ（重大度）が含まれるようになります。
- [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。[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。
- [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。
- [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。

- [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 [Alarm detail] ページへのリンクが追加されます。
- [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。[Mask IP Address and 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） Prime Infrastructure 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シビラティ（重大度）が変更された場合にのみ送信されます。

- [Skip to send first alarm separately as email notification]：最初のアラームは、個別の電子メール通知として送信されます。

（注） このオプションを無効にすると、指定した [Email Send Interval] 期間における最初のアラームの直後に電子メール通知が送信されます。残りのアラームは2番目の電子メールにグループ化されます。このオプションを有効にすると、指定した [Email Send Interval] 期間に 1 通の電子メール通知のみが送信されます。最初の電子メールアラートは既存のリストにグループ化されます。

ステップ 7 [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。
- [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。
- [Unacknowledge and Unassign Alarm on Clear]：リストからクリアされた確認済みおよび割り当て済みのアラームを未確認のままにし、再発した場合に同じ所有者に対して割り当て解除する必要がある場合は、このチェックボックスをオフにします。確認済みまたは前の所有者に割り当てられたアラームをクリアするときに、アラームが未確認で割り当てられていない場合は、このチェックボックスをオンにします。

ステップ 8 [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、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。	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。

シビラティ（重大度）レベルの変更

の各アラームにはシビラティ（重大度）が設定されます。アラームのシビラティ（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 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。

- 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）]** > **[アラームのシビラティ（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 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 を検索します。

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。

（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。

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）]** > **[アラームのシビラティ（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 自動クリアの期間を変更するには、次の手順を実行します。

- 単一のイベントの場合、チェックボックスをオンにしてイベントを選択し、[アラームの自動クリア（Alarm Auto Clear）] ボタンをクリックするか、**または**、選択したイベントの [自動クリア期間（Auto Clear Duration）] 列の下のフィールドをダブルクリックします。新しい期間を入力します。
- 複数のイベントの場合、イベントまたはイベントのグループのチェックボックスをオンにし、[アラームの自動クリア（Alarm Auto Clear）] ボタンをクリックして、新しい期間を入力します。

ステップ 4 [OK] または [保存（Save）] 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。

完全優先ベントの動作の変更

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 によって処理されます。

タイプ	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、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
```

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シビラティ（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 （20 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、 は受信した syslog またはトラップを廃棄しません。 は、受信した syslog またはトラップについて 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。 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、 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。

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 シビラティ（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**

汎用 syslog 処理の無効化および有効化

汎用 syslog を管理するには、genericSyslog.sh コマンドを使用します。

操作の目的：	使用するコマンド：
汎用 syslog 処理をオフにする	**/opt/CSCOlumos/bin/genericSyslog.sh -l**
汎用 syslog 処理をオンにする	**/opt/CSCOlumos/bin/genericSyslog.sh -u**

SNMP トラップに基づく汎用イベントのカスタマイズ

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、SNMP トラップと通知を生成します。これらの通知には、SNMP トラップ オブジェクトの ID（SnmpTrapOID）と可変バインド オブジェクト ID（VarBindOIDs）が数値形式で含まれています。 は、カスタマイズされた MIB モジュールを使用して、SnmpTrapOID および VarBindOID の数値をわかりやすい名前に変換し、その後 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。

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 *1:* 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、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。

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ー ID を使用して 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） [EPNMからのリセット（Reset from EPNM）] 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 （21 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、 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 が設定されている。
- 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。 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。

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。