



付録 A アラートの送信

この付録では、アラートを送信するように MARS を設定する方法について説明します。アラートは、MARS がエンド ユーザにシステム、または Syslog サーバなどのデバイスを通知するための手段です。アラートを設定するには、次の要件を満たしている必要があります。

- ・ SNMP (簡易ネットワーク管理プロトコル) および Syslog 通知を機能させるには、受信システムを設定する必要があります。「レポート デバイスおよび軽減デバイスの概要」には、MARS と連携するようにデバイスを個別に設定する方法が記載されています。
- ・ 電子メール通知をトリガーする規則を変更する前に、電子メール サーバを設定する必要があります。

この付録の具体的な内容は、次のとおりです。

- ・ 電子メール サーバの設定
- ・ 通知をトリガーする規則の設定

電子メール サーバの設定

電子メール サーバを設定する手順は、次のとおりです。

ステップ 1 Admin > Configuration Information の順にクリックします。

図 A-1 MARS デバイス設定情報画面

CS-MARS Device Config

→ Name:	LC20-Doc																
→	Interface Name	IP Address								Net Mask				Default Gateway			
	eth0	10	89	149	151	255	255	255	128	10	89	149	254				
	eth1	192	168	1	100	255	255	255	0								
→ Mail Gateway:																	
IP:Port	64.101.176.33								:	25							
Email domain name:	cisco.com								(ex: Enter 'domain1' for user@domain1)								

143792

ステップ 2 Device Configuration に、メール ゲートウェイの IP アドレスおよびドメイン名を入力します。

ステップ 3 このページの下部にある **Update** ボタンをクリックして、サーバ設定を更新します。

通知をトリガーする規則の設定

アクションがトリガーされた場合、MARS は次に示す 6 つの方法のいずれかを使用して、アラートを送信できます。

- ・ 電子メール
 - ・ ページャ
 - ・ Syslog
 - ・ SNMP
 - ・ SMS
 - ・ DTM 通知 Distributed Threat Mitigation (DTM; 分散型脅威軽減) 通知の詳細については、「DTM の設定」を参照してください。
- 通知をトリガーするように既存の規則を設定したり、通知をトリガーする規則を追加したりすることができます。

システム規則またはユーザ インспекション規則がトリガーされた場合の通知の設定

通知を定義する手順は、次のとおりです。

ステップ 1 編集する規則のタイプに応じて、**RULES > System Inspection Rules** または **RULES > System Inspection Rules** の順にクリックします。

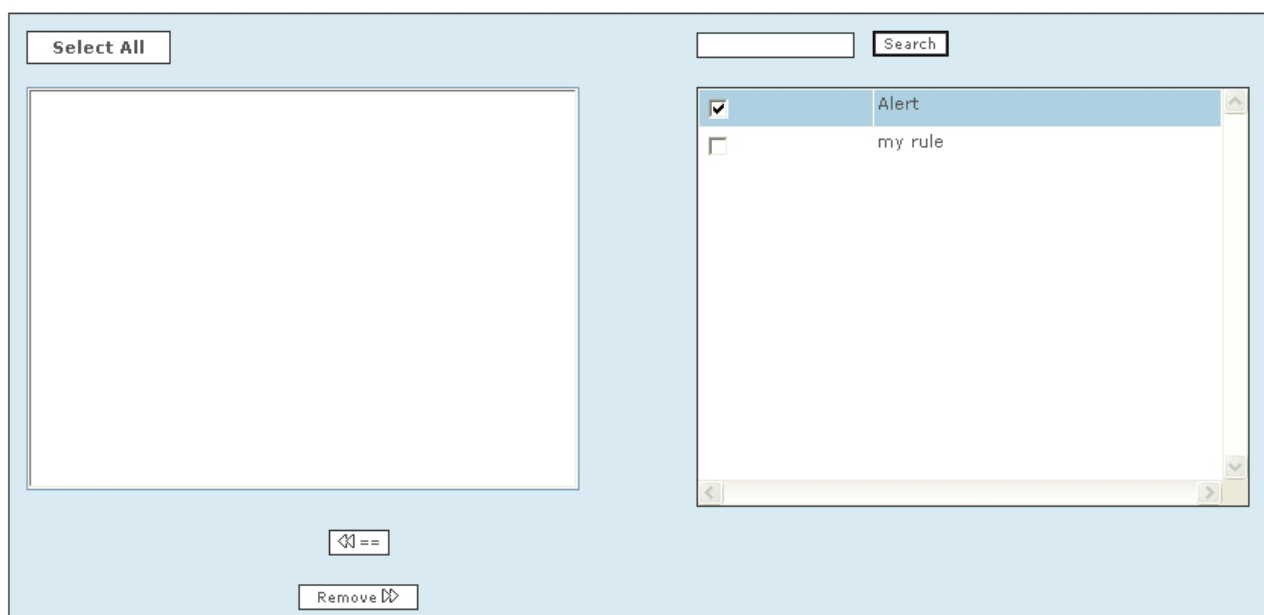
ステップ 2 アクションを定義する規則を選択して、次のいずれかの処理を実行します。

- ・ 定義済みのアクションがある場合は、編集する規則に対応する **Action** をクリックします。Action Selection ページが表示されます。
- ・ アクションが定義されていない場合は、Action/Operations カラムが選択されるまで **Next** をクリックします。

結果: 規則の説明テーブルの下に、Action ペインが表示されます。

図 A-2 Action Selection ページ

Action



143789

ステップ 3 Action Selection ページで、目的の各通知の横にあるチェックボックスをクリックしてから、**Add** ボタンをクリックして、これらの通知を選択します (選択した通知が左側のフィールドに移動します)。通知を削除するには、名前をクリックして (左側のフィールドで) 強調表示にし、**Remove** ボタンをクリックします。通知を追加し終わったら、**Apply** をクリックしてアクションを終了し、このページを閉じます。

使用可能な通知リストに通知を追加する場合は、ページの下部にある **Add** ボタンをクリックします。Add Notification ページが表示されます。

図 A-3 Add Notification ページ

Name:

Description:

Email

Syslog

Page

SNMP

SMS

Distributed Threat Mitigation

ALARM ONLY

143790

ステップ 4 Add Notification ページの **Name** に通知の名前、**Description** に通知の説明を入力します。

ステップ 5 送信する通知タイプの横にあるチェックボックスをオンにします。選択できるタイプは、

- ・ **E-mail** — 電子メールを受信するユーザまたはグループを選択します。
- ・ **Syslog** — Syslog メッセージを受信するデバイスを選択します。
- ・ **Page** — ページャまたは携帯電話で電子ページを受信するユーザまたはグループを選択します。
- ・ **SNMP** — SNMP トラップ情報を受信するデバイスを選択します。
- ・ **SMS** — テキストページ メッセージを受信するユーザまたはグループを選択します。
- ・ **DTM** — この機能の詳細については、「DTM の設定」を参照してください。



注 SNMP および Syslog の場合は、この機能が有効となるように受信システムを設定する必要があります。

ステップ 6 Change Recipient ボタンをクリックして、該当する通知タイプ(電子メール、Syslog、ページ、SNMP)のアラートの受信側を追加します。電子メールまたはページを選択した場合は、User/User Group Selection ダイアログボックスが表示されます。

図 A-4 User/User Group Selection ダイアログボックス

Select

User/User Group Selection ダイアログボックスで、ユーザやグループ、またはアラートを受信するシステムの横にあるチェックボックスをオンにします。**E-mail** や **Page** アラートを追加する場合は、新しいユーザを作成できます(新しいユーザの作成手順については、「新規ユーザの作成 — 役割、ID、パスワード、PGP キー、および通知情報」を参照)。

- ・ **Syslog** または **SNMP** を選択した場合は、MARS から通知を受信するデバイスを追加および削除できる Device Selection ダイアログボックスが表示されます。

図 A-5 Device Selection ページ

Select

Device Selection ダイアログボックスで、追加する各デバイスの横にあるチェックボックスをクリックしてから、**Add** ボタンをクリックして、デバイスを選択します (選択したデバイスが左側のフィールドに移動します)。デバイスを削除するには、名前をクリックして (左側のフィールドで) 強調表示にし、**Remove** ボタンをクリックします。受信側を追加しない場合は、ページの下部にある **Submit** をクリックしてページを閉じ、前の画面に戻ります。このページで、通知の受信側を追加または変更できます (ステップ 6 を参照)。

- ・ **E-mail** または **Page** を選択した場合は、User/User Group Selection ダイアログボックスが表示され、ユーザまたはユーザグループの追加、削除を行えます。

ステップ 7 追加するすべてのアラートに対して、ステップ 5 (ページ 4) ~ ステップ 6 の主要手順を繰り返します。

ステップ 8 Add Notification ページで、**Apply** ボタンをクリックして変更を送信し、Rule Summary ページに移動します。

ステップ 9 Rule Summary ページで、**Submit** ボタンをクリックして、通知の追加を終了し、**Rules** ページに戻ります。

新規ユーザの作成 — 役割、ID、パスワード、PGP キー、および通知情報

新しいユーザアカウントは **Management > User Management** タブで作成します。

ステップ 1 **Management > User Management** タブで、**Add** をクリックします。User Management ページが表示されます (図 A-6 を参照)。

図 A-6 User Configuration ページ

The screenshot shows a 'User Configuration' form with the following fields and values:

- Role: Admin
- Login: admin
- Password: *****
- Repeat password: [empty]
- First Name: admin
- Last Name: admin
- Object class: Cisco Systems, Inc.
- Email: admin@aaa.com
- SMS: 8887770000@aaa.com
- Work phone: 888 888 1212
- Home phone: 888 888 1212
- Fax: 888 888 1212
- Pager: 888 888 1212 (Cell phone or pager numbers go: 8887770000)
- Service Provider: m.aaa.com [Edit Provider]

Buttons: Cancel, Submit

ステップ 2 **Role** フィールドで、目的のユーザの **Role** を選択します。

- ・ **Admin**: MARS を完全に使用できます。
- ・ **Notification Only**: MARS アプライアンスのユーザでないユーザは、この役割を使用して、Admin、Security Analyst、または Operator 以外のユーザにアラートを送信します。
- ・ **Operator**: 読み取り専用の権限を持ちます。
- ・ **Security Analyst**: Admin タブにアクセスできない点を除いて、MARS を完全に使用できます。

ステップ 3 必要に応じて、ユーザのパスワードを作成または変更します。

ステップ 4 ユーザの証明書および個人情報を入力します。入力内容は次のとおりです。

- ・ 名
- ・ 姓
- ・ 組織名
- ・ 電子メール アドレス
- ・ Short Message Service (SMS) 番号 (例: 8885551212@servprov.com)
- ・ 勤務先の電話番号
- ・ 自宅の電話番号
- ・ FAX 番号
- ・ ページャの番号または ID — 5552345678 などの携帯電話の番号も入力できます。

ステップ 5 ページャで通知を作成しない場合は、ステップ 10 に進みます。

ステップ 6 ページャで通知を作成する場合は、サービス プロバイダー (携帯電話またはページャの会社) を追加する必要がある場合があります。Service Provider フィールドで、**New Provider** を選択します。新しいプロバイダーを追加すると、プルダウンメニューに読み込まれます。

サービス プロバイダー情報を入力するための追加フィールドが表示されます (図 A-7 を参照)。

図 A-7 サービス プロバイダーを追加または変更するためのサービス プロバイダー フィールド

ステップ 7 Provider Name フィールドに、サービス プロバイダーの名前を入力します。

ステップ 8 Provider Phone No フィールドに、サービス プロバイダーの電話番号を入力します。

この番号は、サービス プロバイダーが IXO/TAP プロトコルを使用して英数字メッセージを受信するために使用する電話番号です。フォーマットは、通常の電話番号と同様です (18001234567 など)。1-800-1234567 のフォーマットも指定できます。PBX (構内交換機) 外部の番号にアクセスするために「9」をダイヤルする必要がある場合は、電話番号全体の前に「9」を入力します (例: 9,1-800-1234567)。

ステップ 9 Provider Baudrate フィールドに、サービス プロバイダーが指定したボー レートを入力します。

このボー レートは、指定した電話番号に対してサービス プロバイダーが要求しているボー レートです。一般的な値は 1200、2400、4800、および 9600 です。

ステップ 10 Submit をクリックして、User Configuration ページを閉じ、**User Management** タブに戻ります。

ユーザ グループへのユーザの追加

カスタム ユーザ グループにユーザを追加する手順は、次のとおりです。:



注 Admin、Operator、Notification、および Security Analyst はシステム グループであり、編集できません。ユーザは役割に対応したユーザ グループに自動的に追加されます。

ステップ 1 Select Group フィールドでユーザ グループを選択します。グループのメンバーが表示されます。

ステップ 2 Edit Group をクリックします。User Group ダイアログボックスが表示されます。

ステップ 3 右側のリストで、グループに追加するユーザをクリックします。**Add** をクリックします。チェックした名前が、ダイアログボックスの左側に移動します。

ステップ 4 Submit をクリックします。**User Management** タブが再び表示されます。
