



## 第3章 ルータおよびスイッチ デバイスの設定

この章では、ルータおよびスイッチをブートストラップして、MARS にレポート デバイスおよび軽減デバイスとして追加する方法について説明します。また、スイッチの UDP や 802.1X ログギング、およびレイヤ 2 (L2) 軽減機能を使用して、NetFlow、Network Admission Control (NAC) の EAP を設定する方法についても説明します。

ルータおよびスイッチは、アドレス変換、エンドポイント デバイス、接続ネットワーク、許可および拒否されたセッション数など、トラフィック フローやネットワーク ポロジータに関するデータを MARS に提供します。ルータおよびスイッチは、ファイアウォールや、Intrusion Detection System (IDS; 侵入検知システム) または Intrusion Prevention System (IPS; 侵入防御システム) など、専用のセキュリティ アプライアンスに共通の機能をイネーブルにするモジュールもサポートします。この章では、ルータおよびスイッチ上で、モジュールが有効になる機能をイネーブルにする方法、および MARS で使用されるこれらのモジュールの設定方法については、説明しません。これらの説明については、「ファイアウォール デバイスの設定」および「ネットワークベース IDS および IPS デバイスの設定」を参照してください。

この章では、次に示すルータおよびスイッチ デバイスをブートストラップして、MARS に追加する方法を示します。

- ・ シスコ製ルータ デバイス
- ・ シスコ製スイッチ デバイス
- ・ Extreme ExtremeWare 6.x
- ・ 汎用ルータ デバイス

### シスコ製ルータ デバイス

Cisco IOS ソフトウェア リリース 12.2 が稼働するシスコ製ルータと MARS アプライアンスを通信させるには、3 つのタスクを実行します。

- ・ デバイス (Cisco IOS 12.2 稼働) に対する管理アクセスのイネーブル化
- ・ 必要なデータを生成するためのデバイス (Cisco IOS 12.2 稼働) の設定
- ・ MARS でのシスコ製ルータの追加および設定

### デバイス (Cisco IOS 12.2 稼働) に対する管理アクセスのイネーブル化

MARS アプライアンスの、シスコ製ルータまたはスイッチ (Cisco IOS ソフトウェア リリース 12.2 以上を稼働) に対する管理アクセスをイネーブルにする必要があります。イネーブルにする必要のあるアクセスのタイプは、シスコ製ルータまたはスイッチにモジュールが搭載されているかどうか、およびネットワーク内のデバイスの役割によって異なります。MARS はこの管理アクセスを使用してデバイスの設定を検出し、場合によってはデバイスの実行コンフィギュレーションを変更します。管理アクセス方式の選択方法については、「アクセス タイプの選択」を参照してください。

MARS にシスコ製ルータを追加する前に、SNMP (簡易ネットワーク管理プロトコル)、Telnet、SSH (セキュア シェル)、または FTP (ファイル転送プロトコル) によるルータ アクセスがイネーブルになっていることを確認します。ここでは、サポートされている各アクセス方式の設定について説明します。

- ・ SNMP 管理アクセスのイネーブル化
- ・ Telnet 管理アクセスのイネーブル化

- ・ SSH 管理アクセスのイネーブル化
- ・ FTP ベース管理アクセスのイネーブル化

### SNMP 管理アクセスのイネーブル化

シスコ製ルータまたはスイッチへの SNMP アクセスによる設定検出をイネーブルにする手順については、ご使用のデバイスのマニュアルまたは次の URL を参照してください。

[http://cisco.com/en/US/products/sw/iosswrel/ps1835/products\\_configuration\\_guide\\_chapter09186a008030c762.html#wp1001217](http://cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a008030c762.html#wp1001217)

### Telnet 管理アクセスのイネーブル化

シスコ製ルータまたはスイッチへの Telnet アクセスによる設定検出をイネーブルにする手順については、ご使用のデバイスのマニュアルまたは次の URL を参照してください。

[http://cisco.com/en/US/products/sw/iosswrel/ps1818/products\\_configuration\\_example09186a0080204528.shtml](http://cisco.com/en/US/products/sw/iosswrel/ps1818/products_configuration_example09186a0080204528.shtml)

### SSH 管理アクセスのイネーブル化

シスコ製ルータまたはスイッチへの SSH アクセスによる設定検出をイネーブルにする手順については、ご使用のデバイスのマニュアルまたは次の URL を参照してください。

[http://cisco.com/en/US/products/sw/iosswrel/ps1834/products\\_feature\\_guide09186a008007fed9.html](http://cisco.com/en/US/products/sw/iosswrel/ps1834/products_feature_guide09186a008007fed9.html)

### FTP ベース管理アクセスのイネーブル化

FTP アクセスによる設定検出をイネーブルにするには、MARS アプライアンスのアクセス先となる FTP サーバ上にシスコ製ルータまたはスイッチのコンフィギュレーション ファイルのコピーを格納する必要があります。この FTP サーバでは、ユーザ認証をイネーブルにする必要があります。



**注** TFTP はサポートされていません。FTP サーバを使用する必要があります。

シスコ製ルータまたはスイッチから実行コンフィギュレーションをコピーする必要があります。実行コンフィギュレーションのコピー方法については、ご使用のマニュアルまたは次の URL を参照してください。

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products\\_tech\\_note09186a008020260d.shtml](http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_tech_note09186a008020260d.shtml)

## 必要なデータを生成するためのデバイス(Cisco IOS 12.2 稼働)の設定

Cisco IOS ソフトウェア リリース 12.2 を稼働するシスコ製ルータおよびスイッチでは、さまざまなタイプのデータを MARS に提供するように設定できます。

- ・ **Syslog メッセージ** - Syslog メッセージは、許可および拒否されたセッション数など、ネットワークのアクティビティに関する情報を提供します。
- ・ **SNMP トラフィック** - SNMP RO コミュニティ スtring はネットワーク トポロジーの検出をサポートします。
- ・ **NAC 固有のデータ** - NAC は、Extensible Authentication Protocol(EAP) over UDP メッセージおよび 802.1X アカウンティング メッセージを含む設定固有のイベントを記録します。
- ・ **アクセス リストまたは NAT(ネットワーク アドレス変換) ステートメント** - シスコ製ルータまたはスイッチのコンフィギュレーションにアクセス リストまたは NAT ステートメントが含まれている場合は、SSH または Telnet アクセスをイネーブルにする必要があります。
- ・ **スパンニング ツリー メッセージ(スイッチのみ)** - スwitch に Spanning-Tree Protocol(STP; スパンニングツリー プロトコル)が正しく設定され、L2 検出および軽減機能がイネーブルになっていることを確認する必要があります。MARS は STP を使用すると、トラフィックの L2 再ルーティングの識別や L2 軽減機能を実行するために必要な L2 MIB(管理情報ベース)にアクセスできるようになります。MARS は MIB を使用して、その他のスイッチへのトランクを特定し、これにより、L2 パス計算で使用される VLAN (仮想 LAN) 情報を読み込みます。シスコ製スイッチでデフォルトでイネーブルになっている STP は、L2 軽減機能が必要なため、イネーブルにしておく必要があります。

次に、これらの設定方法について説明します。

- ・ Syslog メッセージのイネーブル化
- ・ SNMP RO スtring のイネーブル化

- ・ NAC 固有のメッセージのイネーブル化
- ・ L2 検出メッセージのイネーブル化
- ・ IOS IPS ソフトウェア用 SDEE のイネーブル化

### Syslog メッセージのイネーブル化

Cisco IOS ソフトウェア リリース 12.2 が稼働するデバイスから MARS アプライアンスに Syslog メッセージを送信する手順は、次のとおりです。

---

**ステップ 1** イネーブル パスワードを使用して、Cisco IOS デバイスにログインします。

**ステップ 2** 次のコマンドを入力します。

```
Router(config)#logging source-interface <interface name>
Router(config)#logging trap <logging level desired>
Router(config)#logging <IP address of MARS Appliance>
```

---

### SNMP RO スtringのイネーブル化

Cisco IOS デバイスでトポロジー検出を行うために SNMP RO スtringをイネーブルにするには、SNMP サーバをイネーブルにし、RO コミュニティを定義してから、MARS アプライアンスに SNMP トラップを送るように SNMP サーバを設定する必要があります。

SNMP RO スtringの設定を行う手順は、次のとおりです。

---

**ステップ 1** コンフィギュレーション モードを開始します。

```
Router> enable
Password:<password>
Router#
```

**ステップ 2** `configure terminal` コマンドを入力して、コンフィギュレーション モードを開始します。

```
Router# configure terminal
コンフィギュレーション コマンドを、1 行につき 1 つずつ入力します。最後に Cntrl + Z キーを押します。
Router(config)#
```

**ステップ 3** SNMP リード コミュニティ スtringを次のように設定します。

```
Router(config)# snmp-server community <read community> RO <ACL name if required>
```




---

**注** この情報は、MAC(メディア アクセス制御)アドレスおよび関連する L2 情報を取得する場合に必要です。

---

**ステップ 4** SNMP ライト(write) コミュニティ スtringを次のように設定します。

```
Router(config)# snmp-server community <write community> RW
```

---

### NAC 固有のメッセージのイネーブル化

Cisco IOS ソフトウェア リリース 12.2 または CatOS が稼働しているシスコ製ルータおよびスイッチは、NAC 固有のデータに対応できます。NAC 固有のデータは、次のとおりです。

- ・ **クライアント ログ** - クライアント ソフトウェアのアクティビティに関連するログです。
- ・ **RADIUS サーバ ログ** - クライアントとポスチャ確認サーバ間の許可通信に関連するログです。

- ・ **ネットワーク アクセス デバイス ログ** - クライアントが試行する接続、および NAC ポリシーを適用する AAA(認証、許可、アカウントリング)サーバによる最終許可に関連するログです。

NAC の一部として記録されるイベントの詳細については、次の URL にあるホワイトペーパー『*Monitoring and Reporting Tool Integration into Network Admission Control*』を参照してください。

[http://www.cisco.com/en/US/netsol/ns617/networking\\_solutions\\_white\\_paper0900aecd801dee49.shtml](http://www.cisco.com/en/US/netsol/ns617/networking_solutions_white_paper0900aecd801dee49.shtml)

ここでは、各デバイス タイプに固有の NAC 設定を解決するための、次の 2 つのトピックについて説明します。

- ・ シスコ製ルータ
- ・ シスコ製スイッチ

### シスコ製ルータ

MARS と連携するようにシスコ製ルータの NAC フェーズ I データを設定するには、EAP over UDP を許可し、パケットの AAA station-id フィールドに IP アドレスを格納できるようにします。さらに、Syslog メッセージとしてパブリッシュされるこれらのイベントのロギングをイネーブルにする必要があります。

シスコ製ルータで NAC 固有のデータをイネーブルにするには、次のコマンドを入力します。

```
Router(config)#eou allow ip-station-id
Router(config)#eou logging
```

これらのコマンドおよび関連コマンドの詳細については、次の URL にある NAC 機能のマニュアルを参照してください。

[http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products\\_feature\\_guide09186a008021650d.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008021650d.html)

### シスコ製スイッチ

NAC フェーズ II を使用すると、シスコ製スイッチをネットワーク アクセス デバイスとして機能させることができます。この新しい機能をサポートするには、リンク ステータスがダウンからアップに変わったときに 802.1X 認証を開始し、ポートがアップ状態のまま認証されない場合は定期的に 802.1X 認証を開始するように、シスコ製スイッチを設定する必要があります。NAC では、ホストが 802.1X サブリカントまたはクライアントを使用して Cisco Secure ACS サーバを認証してから、ネットワーク サービスにアクセスする必要があります。ネットワーク上で 802.1X メッセージをイネーブルにすると、接続試行が記録されて分析できるようになるため、サブリカント障害のトラブルシューティングに役立ちます。

シスコ製スイッチを、Cisco Secure ACS サーバおよび 802.1X サブリカント間のプロキシとして機能するように設定するには、複数の手順を実行します。まず、スイッチを Cisco Secure ACS サーバの AAA クライアント(RADIUS)として定義します。AAA クライアントの定義の詳細については、「AAA クライアントの定義」を参照してください。次に、RADIUS サーバを使用するように、スイッチを設定します。その後、スイッチに搭載されたインターフェイスごとに、次の機能をイネーブルにします。

- ・ **802.1X ポートベース認証** - デバイスはクライアントの ID を要求して、クライアントと認証サーバ間での認証メッセージのリレーを開始します。ネットワークにアクセスしようとする各クライアントは、クライアントの MAC アドレスによって一意に識別されます。
- ・ **802.1X 再認証** 再認証がタイムアウト値に達すると、デバイスはサブリカントを再認証します。再認証タイムアウトのデフォルト値は、3600 秒です。
- ・ **802.1X アカウンティング** - デバイスは認証の成功と失敗、およびリンク ダウン イベントやユーザのロギング オフを記録します。スイッチはロギングのために、これらの監査レコードを Cisco Secure ACS サーバにパブリッシュします。
- ・ **DHCP スヌーピング** デバイスは DHCP 要求をフィルタリングして、スプーフィング攻撃から保護します。MARS はこの機能を使用して、信頼性の高いデータを受信し、802.1X サブリカントのポート番号を識別することができます。

これらの機能の設定方法については、次の URL を参照してください。

### Dot1x および RADIUS サーバ

#### IOS ソフトウェア:

[http://www.cisco.com/en/US/products/hw/switches/ps5023/products\\_configuration\\_guide\\_chapter09186a00804761ff.html](http://www.cisco.com/en/US/products/hw/switches/ps5023/products_configuration_guide_chapter09186a00804761ff.html)

#### CatOS ソフトウェア:

[http://www.cisco.com/en/US/products/hw/switches/ps708/products\\_configuration\\_guide\\_chapter09186a008027947e.html](http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008027947e.html)

### DHCP スヌーピング

#### IOS ソフトウェア:

[http://www.cisco.com/en/US/products/hw/switches/ps5023/products\\_configuration\\_guide\\_chapter09186a0080476208.html](http://www.cisco.com/en/US/products/hw/switches/ps5023/products_configuration_guide_chapter09186a0080476208.html)

#### CatOS ソフトウェア:

[http://www.cisco.com/en/US/products/hw/switches/ps708/products\\_configuration\\_guide\\_chapter09186a008022f26c.html](http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008022f26c.html)

プロキシとして機能するようにスイッチを設定し、Cisco Secure ACS の AAA クライアントとして定義したら、認証メッセージが MARS アプライアンスに送信されるようにする必要があります。802.1X アカウンティング レコードの場合は、監査レコードが Cisco Secure ACS サーバの RADIUS ログに書き込まれるようにします。これらの設定を行うには、「ログを生成するための Cisco Secure ACS の設定」を参照してください。

### IOS IPS ソフトウェア用 SDEE のイネーブル化

SDEE をイネーブルにする前に、Cisco IOS デバイス上の設定検出用のアクセス タイプとして Telnet または SSH をイネーブルにします。また、IOS IPS ソフトウェア機能をサポートするデバイス上でも SDEE をイネーブルにします。SDEE は、起動されたシグニチャに関するイベントを MARS にパブリッシュするために使用されます。

IOS IPS をサポートする Cisco IOS デバイスで SDEE プロトコルをイネーブルにする手順は、次のとおりです。

---

**ステップ 1** イネーブル パスワードを使用して、Cisco IOS デバイスにログインします。

**ステップ 2** 次のコマンドを入力して、MARS が IOS IPS ソフトウェアからイベントを受信できるようにします。

```
Router(config)#ip http secure-server
Router(config)#ip ips notify sdee
Router(config)#ip sdee subscriptions 3
Router(config)#ip sdee events 1000
Router(config)#no ip ips notify log
```



---

**注** 「no ips notify log」を指定すると、IOS IPS ソフトウェアは Syslog を介した IPS イベントの送信を停止します。

---

### MARS でのシスコ製ルータの追加および設定

シスコ製ルータは、Syslog メッセージおよび SNMP RO MIB の形式で、ネットワークおよびそのアクティビティに関するデータを提供します。さらに、MARS はネットワーク アドレス変換、接続先ネットワーク、アクティブなアクセス規則などの設定を検出し、フォールス ポジティブ識別精度、攻撃パスの分析、および L3 ネットワーク検出などを改善できます。

Cisco IOS 12.2 以上が稼働するシスコ製ルータを追加する手順は、次のとおりです。

---

**ステップ 1** Admin > System Setup > Security and Monitor Devices > Add の順に選択します。

**ステップ2** Device Type リストで **Cisco IOS 12.2** を選択します。

Device Type:

→ \*Device Name:

→ Access IP: ...

→ Reporting IP: ...

→ \*Access Type:

Login:

Password:

Enable Password:

Config Path:

File Name:

SNMP RO Community:

→ Monitor Resource Usage:

143635

**ステップ3** Device Name フィールドにデバイスの名前を入力します。

MARS はこの名前とレポート IP アドレスを対応付けます。この名前はトポロジー マップ、クエリー、および Security and Monitoring Device リストで使用されます。ルータやファイアウォールなど、検出処理をサポートするデバイスの場合、MARS はこのフィールド値の名前を、デバイス設定内で検出された名前に合わせて変更します。通常は、*hostname.domain* フォーマットが使用されます。Windows ホストや Linux ホスト、ホスト アプリケーションなど、検出できないデバイスの場合、MARS は指定された値を使用します。

**ステップ4** (任意)MARS が、このデバイスから設定を検出できるようにするには、Access IP フィールドに管理 IP アドレスを入力します。

アクセス IP アドレス、およびその役割と依存関係の詳細については、「アクセス IP、レポート IP、およびインターフェイス設定の概要」を参照してください。

**ステップ5** Reporting IP フィールドに、Syslog メッセージ、SNMP 通知、NetFlow MIB、または 3 つの組み合わせをパブリッシュするインターフェイスの IP アドレスを入力します。

レポート IP アドレス、およびその役割と依存関係の詳細については、「アクセス IP、レポート IP、およびインターフェイス設定の概要」を参照してください。

**ステップ6** Access IP フィールドにアドレスを入力したら、Access Type リストで **SNMP**、**TELNET**、**SSH**、または **FTP** を選択し、選択に応じた手順に進みます。

- ・ MARS のデバイスに対する SNMP アクセスの設定
- ・ MARS のデバイスに対する Telnet アクセスの設定
- ・ MARS のデバイスに対する SSH アクセスの設定
- ・ MARS のデバイスに対する FTP アクセスの設定

アクセス タイプの決定方法については、「アクセス タイプの選択」を参照してください。

**ステップ7** (任意)MARS がこのレポート デバイスの MIB オブジェクトを取得できるようにするには、SNMP RO Community フィールドにデバイスの読み取り専用コミュニティ スtring を入力します。

SNMP RO String を指定する前に、アクセス IP アドレスを定義する必要があります。MARS は SNMP RO String を使用して、レポート デバイスの CPU 使用率、ネットワーク使用率、およびデバイス異常データに関連する MIB を読み取ったり、デバイスやネットワークの設定を検出したりします。

**ステップ 8** (任意)MARS がこのデバイスをモニタして、異常なリソース使用率を検出できるようにするには、Monitor Resource Usage リストで **Yes** を選択します。

**結果:**MARS はデバイス内で、リソース(メモリや CPU など)の異常な消費をモニタします。異常が検出されると、MARS はインシデントを生成します。リソース利用率の統計情報は、レポートを生成するときにも使用されます。詳細については、「リソース使用率データの設定」を参照してください。

**ステップ 9** (任意)このルータの IOS IPS 機能と SDEE アクセスがイネーブルになっていて、MARS アプライアンスから HTTPS 接続を受け入れるようにルータを設定してある場合は、**Add IPS** をクリックして、SDEE イベントをプルするために必要なユーザ名およびパスワードを入力します。



**注** IOS IPS は IPS モジュールでは**ありません**。IOS IPS は IOS ソフトウェアのソフトウェア機能のことです。IOS IPS 機能は、MARS で DTM 機能をイネーブルにする場合に必要です。詳細については、「DTM の設定」を参照してください。

**結果:**IOS IPS Information ページが表示されます。

#### IOS IPS Information

Reporting IP:	192.168.20.1
User Name:	<input type="text"/>
password:	<input type="password"/>
Port:	<input type="text" value="443"/>

143204

- User Name フィールドに、HTTPS がこのデバイスにアクセスするためのユーザ名を入力します。
- Password フィールドに、対応するパスワードを入力します。
- Port フィールドで、SDEE とデバイスの通信に使用されるポートを確認します。

MARS は HTTPS 経由で SDEE を使用し、データをプルします。HTTPS/SDEE のデフォルトポート番号は 443 です。このアクセスにより、MARS は、IOS IPS 機能によって生成されたイベントを含む XML ファイルを取得できます。

**結果:**MARS はルータに SDEE イベントを問い合わせることができます。

**ステップ 10** (任意)アクセス IP を定義して、アクセス タイプを選択して設定したら、**Discover** をクリックして、IOS IPS 設定などのデバイス設定を判別します。

**結果:**ユーザ名およびパスワードが正しく、MARS アプライアンスがデバイスの管理ホストとして設定されている場合は、検出処理が完了すると、「Discovery is done」ダイアログボックスが表示されます。それ以外の場合は、エラーメッセージが表示されます。最初のプルの後、MARS アプライアンスは定義されたスケジュールに基づいてプルします。詳細については、「トポロジー更新のスケジュール」を参照してください。

**ステップ 11** MARS データベースにデバイスを追加するには、**Submit** をクリックします。

**結果:**この処理により、データベーステーブルに変更が記録されます。ただし、MARS アプライアンスの動作中のメモリには変更がロードされません。アクティブ化処理を行うと、変更が作業メモリに送信されます。

**ステップ 12** **Activate** をクリックします。

**結果:**MARS はこのデバイスによって生成されたイベントのセッション化を開始し、定義済みのインスペクション規則および廃棄規則を使用してイベントを評価します。アクティブ化の開始前にデバイスから MARS にパブリッシュされたイベントについては、デバイスのレポート IP アドレスをマッチ基準にして、問い合わせを行うことができます。アクティブ化アクションの詳細については、「レポート デバイスおよび軽減デバイスのアクティブ化」を参照してください。

## シスコ製スイッチ デバイス

CatOS または Cisco IOS ソフトウェア リリース 12.2 以上が稼働するシスコ製スイッチは、管理することが可能です。これら 2 つのオペレーティング システムでは、スイッチの設定および MARS へのデバイス追加方法が異なります。シスコ製スイッチを追加するには、次の 3 つの手順を実行します。

1. MARS が設定を検出できるようにスイッチを設定します。
2. MARS に必要なデータを生成するようにスイッチを設定します。
3. MARS にスイッチを追加して、設定します。
4. スイッチにモジュールを追加します。

Cisco IOS ソフトウェア リリース 12.2 以上が稼働するシスコ製スイッチの設定を準備するには、次の手順を参照してください。

- ・ デバイス (Cisco IOS 12.2 稼働) に対する管理アクセスのイネーブル化
- ・ 必要なデータを生成するためのデバイス (Cisco IOS 12.2 稼働) の設定

CatOS が稼働するシスコ製スイッチの設定を準備するには、次の手順を参照してください。

- ・ CatOS が稼働するデバイスと MARS 間の通信のイネーブル化
- ・ 必要なデータを生成するためのデバイス (CatOS 稼働) の設定

MARS に CatOS が稼働するシスコ製スイッチを追加するには、2 つの手順を実行します。まず、スイッチの基本モジュールを追加して、デバイスへの管理アクセスを可能にします。次に、スイッチで稼働するモジュールを追加します。これらの 2 つの手順の実行方法については、次のトピックを参照してください。

- ・ MARS でのシスコ製スイッチの追加および設定
- ・ シスコ製スイッチへのモジュールの追加

## CatOS が稼働するデバイスと MARS 間の通信のイネーブル化

MARS に CatOS が稼働するシスコ製スイッチを追加する前に、SNMP、Telnet、SSH、または FTP によるスイッチ アクセスがイネーブルになっていることを確認します。まず、MARS アプライアンスに、スイッチにアクセス可能な IP アドレスを設定します。

IP アドレスを許可して、アクセス タイプを指定する方法については、次の URL を参照してください。

[/en/US/products/hw/switches/ps708/products\\_configuration\\_guide\\_chapter09186a008022f271.html#wp1019819](https://en.US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008022f271.html#wp1019819)

次に、正しいアクセス方式がイネーブルになるように、スイッチが設定されていることを確認します。ここでは、サポートされているアクセス方式についてそれぞれ説明します。

- ・ SNMP 管理アクセスのイネーブル化
- ・ Telnet 管理アクセスのイネーブル化
- ・ SSH 管理アクセスのイネーブル化
- ・ FTP ベース管理アクセスのイネーブル化

### SNMP 管理アクセスのイネーブル化

シスコ製スイッチへの SNMP アクセスによる設定検出をイネーブルにする手順については、ご使用のデバイスのマニュアルまたは次の URL を参照してください。

#### IP アクセス

[/en/US/products/hw/switches/ps708/products\\_configuration\\_guide\\_chapter09186a008022f271.html#wp1019819](https://en.US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008022f271.html#wp1019819)

#### SNMP の設定

[http://www.cisco.com/en/US/products/hw/switches/ps708/products\\_configuration\\_guide\\_chapter09186a008022f27c.htm](http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008022f27c.htm)

### Telnet 管理アクセスのイネーブル化

シスコ製スイッチへの Telnet アクセスによる設定検出をイネーブルにする手順については、ご使用のデバイスのマニュアルまたは次の URL を参照してください。

#### IP アクセス

[/en/US/products/hw/switches/ps708/products\\_configuration\\_guide\\_chapter09186a008022f271.html#wp1019819](https://en.US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008022f271.html#wp1019819)

## SSH 管理アクセスのイネーブル化

シスコ製ルータまたはスイッチへの SSH アクセスによる設定検出をイネーブルにする手順については、ご使用のデバイスのマニュアルまたは次の URL を参照してください。

### IP アクセス

[/en/US/products/hw/switches/ps708/products\\_configuration\\_guide\\_chapter09186a008022f271.html#wp1019819](/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008022f271.html#wp1019819)

## FTP ベース管理アクセスのイネーブル化

FTP アクセスによる設定検出をイネーブルにするには、MARS アプライアンスのアクセス先となる FTP サーバ上にシスコ製ルータまたはスイッチのコンフィギュレーション ファイルのコピーを格納する必要があります。この FTP サーバでは、ユーザ認証をイネーブルにする必要があります。



**注** TFTP はサポートされていません。FTP サーバを使用する必要があります。

シスコ製スイッチから実行コンフィギュレーションをコピーする必要があります。実行コンフィギュレーションのコピー方法については、ご使用のマニュアルまたは次の URL を参照してください。

[/en/US/products/hw/switches/ps708/products\\_configuration\\_guide\\_chapter09186a0080279493.html#wp1040556](/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a0080279493.html#wp1040556)

## 必要なデータを生成するためのデバイス (CatOS 稼働) の設定

設定できるメッセージ プロパティは次のとおりです。

- ・ SNMP RO スtring
- ・ NAC メッセージ (802.1X)
- ・ L2 検出設定
- ・ Syslog メッセージ

これらの設定の詳細については、次のトピックを参照してください。

- ・ CatOS での SNMP RO スtringのイネーブル化
- ・ NAC 固有のメッセージのイネーブル化
- ・ L2 検出メッセージのイネーブル化
- ・ CatOS での Syslog メッセージのイネーブル化

### CatOS での SNMP RO スtringのイネーブル化

スーパーバイザ SNMP サーバが設定されていない場合は、この手順を実行する必要があります。

スーパーバイザ SNMP サーバを設定して、Catalyst スイッチで SNMP トラップをイネーブルにする手順は、次のとおりです。

**ステップ 1** コンフィギュレーション モードを開始します。

```
switch> enable
Enter password:<password>
switch> (enable)
```

**ステップ 2** SNMP リード コミュニティ スtringを次のように設定します。

```
switch> (enable) set snmp community read-only <read community>
```

**ステップ 3** SNMP ライト (write) コミュニティ スtringを次のように設定します。

```
switch> (enable) set snmp community read-write <write community>
switch> (enable) set snmp community read-write-all <write community>
```

**ステップ 4** RMON Ethernet 統計情報を収集するには、CatOS エージェントで RMON データ収集をイネーブルにする必要があります (Native IOS ではこの処理は不要)。RMON 収集をイネーブルにするには、次のように入力します。

```
switch> (enable) set snmp rmon enable
```

**ステップ 5** 次のように、コンフィギュレーション モードを終了します。

```
switch> (enable) exit
```

## CatOS での Syslog メッセージのイネーブル化

MARS に Syslog 情報を送信するように シスコ製スイッチ (CatOS 稼働) を設定する手順は、次のとおりです。

**Step 1** 次のように入力して、スイッチの Syslog サーバをイネーブルにします。

```
set logging server enable
```

**Step 2** 次のコマンドを入力して、MARS アプライアンスを Syslog メッセージの宛先として識別します。

```
set logging server <IP address of MARS Appliance>
```

**ステップ 3** さらにコマンドを入力して、提供するロギング情報の種類とレベルをスイッチに指示します。次の例に記載されたコマンドは、要件に合わせて変更することができます。

```
set logging level cdp 7 default
set logging level mcast 7 default
set logging level dtp 7 default
set logging level dvlan 7 default
set logging level earl 7 default
set logging level fddi 7 default
set logging level ip 7 default
set logging level pruning 7 default
set logging level snmp 7 default
set logging level spantree 7 default
set logging level sys 7 default
set logging level tac 7 default
set logging level tcp 7 default
set logging level telnet 7 default
set logging level tftp 7 default
set logging level vtp 7 default
set logging level vmps 7 default
set logging level kernel 7 default
set logging level filesys 7 default
set logging level drip 7 default
set logging level pagp 7 default
set logging level mgmt 7 default
set logging level mls 7 default
set logging level protfilt 7 default
set logging level security 7 default
set logging server facility SYSLOG
set logging server severity 7
set logging buffer 250
set logging timestamp enable
```

## L2 検出メッセージのイネーブル化

シスコ製スイッチで L2 検出をイネーブルにするには、STP をイネーブルにして、SNMP RO コミュニティ スtring を指定します。すべての L2 デバイスで SNMP STP MIB (IETF RFC 1493) をサポートする必要があります。検出される情報は、インターフェイス、レイヤ 3 (L3) ルート、L2 スパニング ツリー、L2 転送テーブル、MAC アドレスなどです。



**注** STP はすべてのシスコ製スイッチで、デフォルトでイネーブルになっています。したがって、この設定が変更されていない場合は、変更の必要はありません。

STP の設定方法については、次の URL にある View Documents by topics リストで、**Spanning Tree Protocol** を選択してください。

[http://www.cisco.com/en/US/partner/products/hw/switches/ps708/prod\\_configuration\\_examples\\_list.html](http://www.cisco.com/en/US/partner/products/hw/switches/ps708/prod_configuration_examples_list.html)

[http://www.cisco.com/en/US/products/hw/switches/ps708/products\\_configuration\\_guide\\_chapter09186a008022f29c.html](http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008022f29c.html)

## MARS でのシスコ製スイッチの追加および設定

MARS は CatOS または Cisco IOS 12.2 が稼働するシスコ製スイッチをモニタします。

MARS がシスコ製スイッチ (Cisco IOS 12.2 以上を稼働) のモニタのために使用する設定情報を追加する手順は、次のとおりです。

**ステップ 1** Admin > System Setup > Security and Monitor Devices > Add の順に選択します。

**ステップ 2** 次のいずれかの操作を実行します。

- ・ スイッチでいずれかのバージョンの CatOS が稼働している場合は、Device Type リストで **Cisco Switch-CatOS ANY** を選択します。
- ・ スイッチで Cisco IOS 12.2 以上が稼働している場合は、Device Type リストで **Cisco Switch-IOS 12.2** を選択します。

**ステップ 3** Device Name フィールドにデバイスの名前を入力します。

MARS はこの名前とレポート IP アドレスを対応付けます。この名前はトポロジー マップ、クエリー、および Security and Monitoring Device リストで使用されます。ルータやファイアウォールなど、検出処理をサポートするデバイスの場合、MARS はこのフィールド値の名前を、デバイス設定内で検出された名前に合わせて変更します。通常は、*hostname.domain* フォーマットが使用されます。Windows ホストや Linux ホスト、ホスト アプリケーションなど、検出できないデバイスの場合、MARS は指定された値を使用します。

**ステップ 4** (任意) MARS が、このデバイスから設定を検出できるようにするには、Access IP フィールドに管理 IP アドレスを入力します。

アクセス IP アドレス、およびその役割と依存関係の詳細については、「アクセス IP、レポート IP、およびインターフェイス設定の概要」を参照してください。

**ステップ 5** Reporting IP フィールドに、Syslog メッセージ、SNMP 通知、NetFlow MIB、または 3 つの組み合わせをパブリッシュするインターフェイスの IP アドレスを入力します。

レポート IP アドレス、およびその役割と依存関係の詳細については、「アクセス IP、レポート IP、およびインターフェイス設定の概要」を参照してください。

**ステップ 6** Access IP フィールドにアドレスを入力したら、Access Type リストで **SNMP**、**TELNET**、**SSH**、または **FTP** を選択し、選択に応じた手順に進みます。

- ・ MARS のデバイスに対する SNMP アクセスの設定
- ・ MARS のデバイスに対する Telnet アクセスの設定
- ・ MARS のデバイスに対する SSH アクセスの設定
- ・ MARS のデバイスに対する FTP アクセスの設定

アクセス タイプの決定方法については、「アクセス タイプの選択」を参照してください。

**ステップ 7** (任意) MARS がこのレポートデバイスの MIB オブジェクトを取得できるようにするには、SNMP RO Community フィールドにデバイスの読み取り専用コミュニティ スtring を入力します。

SNMP RO スtringを指定する前に、アクセス IP アドレスを定義する必要があります。MARS は SNMP RO Stringを使用して、レポート デバイスの CPU 使用率、ネットワーク使用率、およびデバイス異常データに関連する MIB を読み取ったり、デバイスやネットワークの設定を検出したりします。

**ステップ 8** (任意) MARS がこのデバイスをモニタして、異常なリソース使用率を検出できるようにするには、Monitor Resource Usage リストで **Yes** を選択します。

**結果:** MARS はデバイス内で、リソース(メモリや CPU など)の異常な消費をモニタします。異常が検出されると、MARS はインシデントを生成します。リソース利用率の統計情報は、レポートを生成するときにも使用されます。詳細については、「リソース使用率データの設定」を参照してください。

**ステップ 9** (任意) アクセス IP を定義して、アクセス タイプを選択および設定したら、**Discover** をクリックして、デバイス設定を判別します。

**結果:** ユーザ名およびパスワードが正しく、MARS アプライアンスがデバイスの管理ホストとして設定されている場合は、検出処理が完了すると、「Discovery is done」ダイアログボックスが表示されます。それ以外の場合は、エラー メッセージが表示されます。最初のプルのもと、MARS アプライアンスは定義されたスケジュールに基づいてプルします。詳細については、「トポロジー更新のスケジュール」を参照してください。

**ステップ 10** MARS データベースにデバイスを追加するには、**Submit** をクリックします。

**結果:** この処理により、データベース テーブルに変更が記録されます。ただし、MARS アプライアンスの動作中のメモリには変更がロードされません。アクティブ化処理を行うと、変更が作業メモリに送信されます。

**ステップ 11** **Activate** をクリックします。

**結果:** MARS はこのデバイスによって生成されたイベントのセッション化を開始し、定義済みのインスペクション規則および廃棄規則を使用してイベントを評価します。アクティブ化の開始前にデバイスから MARS にパブリッシュされたイベントについては、デバイスのレポート IP アドレスをマッチ基準にして、問い合わせを行うことができます。アクティブ化アクションの詳細については、「レポート デバイスおよび軽減デバイスのアクティブ化」を参照してください。

送信したあとで、モジュールを追加することができます。「シスコ製スイッチへのモジュールの追加」を参照してください。

## シスコ製スイッチへのモジュールの追加

MARS では、シスコ製スイッチに搭載されたモジュールを表現、検出、モニタすることができます。これらのモジュールは、ファイアウォールおよび侵入検知または侵入防御など、スイッチ専用のセキュリティ機能を実行します。MARS は次に示すスイッチ モジュールおよびバージョンを認識します。

- ・ Cisco FWSM 1.1, 2.2 および 2.3
- ・ Cisco IDS 3.1 および 4.0
- ・ Cisco IPS 5.x
- ・ Cisco IOS 12.2

モジュールを追加するには、基本モジュール(シスコ製スイッチ)を最初に追加します。HTML インターフェイスで基本モジュールを定義したら、スイッチに搭載されたモジュールを検出 (**Add Available Module** をクリック)したり、モジュールを手動で追加 (**Add Module** をクリック)したりすることができます。

Firewall Services Module (FWSM) を追加および設定する方法については、「Cisco Firewall デバイス (PIX, ASA, および FWSM)」を参照してください。

Intrusion Detection Services Module (IDSM) または Intrusion Prevention Services Module (IPSM) を追加および設定する手順については、「Cisco IPS モジュール」を参照してください。

ここで説明する内容は、次のとおりです。

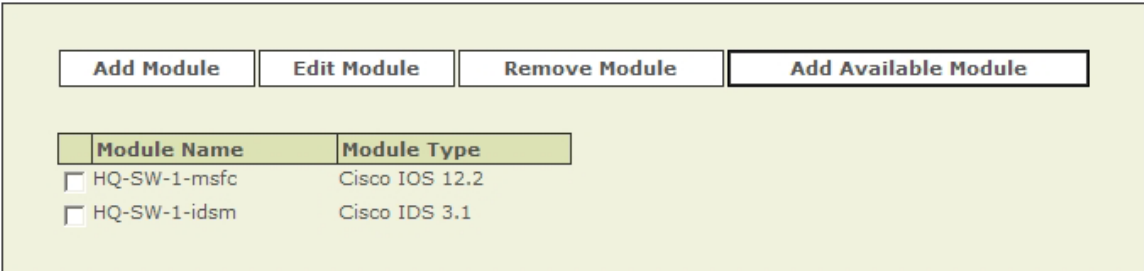
- ・ 使用可能なモジュールの追加
- ・ Cisco IOS 12.2 モジュールの手動追加

### 使用可能なモジュールの追加

基本モジュールで検出処理を実行すると、MARS は検出されたモジュールの一覧を表示します。このリストにより、MARS によるモニタを行うためのモジュールを選択できます。

使用可能なモジュールを追加する手順は、次のとおりです。

**ステップ 1** Add Available Module をクリックします。



The screenshot shows a web interface with four buttons at the top: 'Add Module', 'Edit Module', 'Remove Module', and 'Add Available Module'. Below the buttons is a table with two columns: 'Module Name' and 'Module Type'. The table contains two rows of data, each with a checkbox in the first column.

Module Name	Module Type
<input type="checkbox"/> HQ-SW-1-msfc	Cisco IOS 12.2
<input type="checkbox"/> HQ-SW-1-idsm	Cisco IDS 3.1

143216

モジュールがスイッチに搭載されている場合は、モジュールの一覧が表示されます。

**ステップ 2** Select リストでモジュールを選択します。

**ステップ 3** Add をクリックします。

**ステップ 4** その他のモジュールについても同じ手順を繰り返します。

**ステップ 5** 目的のモジュールを追加したら、各設定情報を確認します。たとえば、SNMP RO コミュニティ スtring が MARS で使用するために定義されたコミュニティ スtring と一致するかどうかを確認します。これらの設定を確認するには、モジュールを選択して、**Edit Module** をクリックします。

設定の編集に関する基本的な注意事項については、これらのモジュールを手動で追加する方法が記載されたトピックを参照してください。詳細については、次のトピックを参照してください。

- ・ Cisco IOS 12.2 モジュールの手動追加
- ・ Cisco Firewall デバイス (PIX, ASA、および FWSM)
- ・ Cisco IPS モジュール。

**ステップ 6** これらのモジュールを、MARS データベースで定義された基本モジュールに追加するには、**Submit** をクリックします。

**結果:** この処理により、データベース テーブルに変更が記録されます。ただし、MARS アプライアンスの動作中のメモリには変更がロードされません。アクティブ化処理を行うと、変更が作業メモリに送信されます。

**ステップ 7** **Activate** をクリックします。

**結果:** MARS はこのデバイスおよび選択したモジュールによって生成されたイベントのセッション化を開始し、定義済みのインスペクション規則および廃棄規則を使用してイベントを評価します。アクティブ化の開始前にデバイスまたはモジュールから MARS にパブリッシュされたイベントについては、デバイスまたはモジュールのレポート IP アドレスをマッチ基準にして、問い合わせを行うことができます。アクティブ化アクションの詳細については、「レポート デバイスおよび軽減デバイスのアクティブ化」を参照してください。

## Cisco IOS 12.2 モジュールの手動追加

モジュールを手動で追加する手順は、次のとおりです。

**ステップ 1** Add Module をクリックします。

**ステップ2** Device Type リストで **Cisco IOS 12.2** を選択します。

The screenshot shows the MARS configuration interface. At the top, the 'Device Type' dropdown menu is open, displaying a list of options: Cisco FWSM 1.1, Cisco FWSM 2.2, Cisco FWSM 2.3, Cisco IOS 12.2, Cisco IPS 5.x, Cisco IDS 3.1, and Cisco IDS 4.0. The 'Cisco IOS 12.2' option is highlighted. Below the dropdown, the configuration form includes fields for:
 

- \* Device Name: [ ]
- Access IP: [ ] [ ] [ ] [ ]
- Reporting IP: [ ] [ ] [ ] [ ]
- \* Access Type: Select [ ] 3DES [ ]
- Login: [ ]
- Password: [ ]
- Enable Password: [ ]
- Config Path: [ ]
- File Name: [ ]
- SNMP RO Community: [ ]
- Monitor Resource Usage: NO [ ]

 A vertical text '143207' is visible on the right side of the form area.

**ステップ3** Device Name フィールドにモジュールの名前を入力します。

MARS はこの名前とレポート IP アドレスを対応付けます。この名前はトポロジー マップ、クエリー、および Security and Monitoring Device リストで使用されます。ルータやファイアウォール モジュールなど、検出処理をサポートするモジュールの場合、MARS はこのフィールド値の名前を、デバイス設定内で検出された名前に合わせて変更します。通常は、*hostname.domain* フォーマットが使用されます。

**ステップ4** (任意)MARS が、このデバイスから設定を検出できるようにするには、Access IP フィールドに管理 IP アドレスを入力します。

アクセス IP アドレス、およびその役割と依存関係の詳細については、「アクセス IP、レポート IP、およびインターフェイス設定の概要」を参照してください。

**ステップ5** Reporting IP フィールドに、Syslog メッセージ、SNMP 通知、NetFlow MIB、または 3 つの組み合わせをパブリッシュするインターフェイスの IP アドレスを入力します。

レポート IP アドレス、およびその役割と依存関係の詳細については、「アクセス IP、レポート IP、およびインターフェイス設定の概要」を参照してください。

**ステップ6** Access IP フィールドにアドレスを入力した場合は、Access Type リストで **TELNET**、**SSH**、または **FTP** を選択し、選択に対する手順に進みます。

- ・ MARS のデバイスに対する Telnet アクセスの設定
- ・ MARS のデバイスに対する SSH アクセスの設定
- ・ MARS のデバイスに対する FTP アクセスの設定

アクセス タイプの決定方法については、「アクセス タイプの選択」を参照してください。

**ステップ7** (任意)MARS がこのレポート デバイスの MIB オブジェクトを取得できるようにするには、SNMP RO Community フィールドにデバイスの読み取り専用コミュニティ スtring を入力します。

SNMP RO String を指定する前に、アクセス IP アドレスを定義する必要があります。MARS は SNMP RO String を使用して、レポート デバイスの CPU 使用率、ネットワーク使用率、およびデバイス異常データに関連する MIB を読み取ったり、デバイスやネットワークの設定を検出したりします。

**ステップ8** (任意)MARS がこのデバイスをモニタして、異常なリソース使用率を検出できるようにするには、Monitor Resource Usage リストで **Yes** を選択します。

**結果:** MARS はモジュール内で、リソース (メモリや CPU など) の異常な消費をモニタします。異常が検出されると、MARS はインシデントを生成します。リソース利用率の統計情報は、レポートを生成するときにも使用されます。詳細については、「リソース使用率データの設定」を参照してください。

**ステップ 9** (任意) アクセス IP を定義して、アクセス タイプを選択および設定したら、**Discover** をクリックして、モジュール設定を判別します。

**結果:** ユーザ名およびパスワードが正しく、MARS アプライアンスがモジュールの管理ホストとして設定されている場合は、検出処理が完了すると、「Discovery is done」ダイアログボックスが表示されます。それ以外の場合は、エラー メッセージが表示されます。最初のプルのもと、MARS アプライアンスは定義されたスケジュールに基づいてプルします。詳細については、「トポロジー更新のスケジュール」を参照してください。

**ステップ 10** MARS データベースのデバイスにモジュールを追加するには、**Submit** をクリックします。

**結果:** この処理により、データベース テーブルに変更が記録されます。ただし、MARS アプライアンスの動作中のメモリには変更がロードされません。アクティブ化処理を行うと、変更が作業メモリに送信されます。

## Extreme ExtremeWare 6.x

MARS は Extreme ExtremeWare スイッチを使用して、L2 軽減機能を実行できます。ExtremeWare スイッチと通信するように MARS を設定するには、MARS アプライアンスに SNMP 通知をパブリッシュするようにスイッチを設定する必要があります。また、HTML インターフェイスでもスイッチを追加し、設定する必要があります。

ここで説明する内容は、次のとおりです。

- ・ 必要なデータを生成するための ExtremeWare の設定
- ・ MARS での ExtremeWare スイッチの追加および設定

### 必要なデータを生成するための ExtremeWare の設定

ExtremeWare スイッチをブートストラップするには、2 つの機能を設定します。まず、MARS アプライアンスに Syslog メッセージを送信するようにスイッチを設定します。次に、使用可能な L2 情報に MARS がアクセスできるように、SNMP RO コミュニティを設定します。

MARS で必要なデータを生成するように ExtremeWare デバイスを設定する手順は、次のとおりです。

**ステップ 1** Syslog コンフィギュレーションに、次のコマンドを追加します。

```
configure syslog add <MARS's IP address> local7 debug
enable syslog
```

**ステップ 2** SNMP コンフィギュレーションに、次のコマンドを追加します。

```
enable snmp dot1dTpFdbTable
configure snmp delete community readonly all
configure snmp delete community readwrite all
configure snmp add community readonly encrypted <encrypted community string>
configure snmp add community readwrite encrypted <encrypted community string>
```

## MARS での ExtremeWare スイッチの追加および設定

MARS で ExtremeWare スイッチを追加および設定する手順は、次のとおりです。

**ステップ 1** Admin > System Setup > Security and Monitor Devices > Add の順に選択します。

**ステップ 2** Device Type リストで **Extreme ExtremeWare 6.x** を選択します。

**ステップ3** Device Name フィールドにデバイスの名前を入力します。

MARS はこの名前とレポート IP アドレスを対応付けます。この名前はトポロジーマップ、クエリー、および Security and Monitoring Device リストで使用されます。ルータやファイアウォールなど、検出処理をサポートするデバイスの場合、MARS はこのフィールド値の名前を、デバイス設定内で検出された名前に合わせて変更します。通常は、*hostname.domain* フォーマットが使用されます。Windows ホストや Linux ホスト、ホスト アプリケーションなど、検出できないデバイスの場合、MARS は指定された値を使用します。

**ステップ4** (任意)MARS が、このデバイスから設定を検出できるようにするには、Access IP フィールドに管理 IP アドレスを入力します。

アクセス IP アドレス、およびその役割と依存関係の詳細については、「アクセス IP、レポート IP、およびインターフェイス設定の概要」を参照してください。

**ステップ5** Reporting IP フィールドに、Syslog メッセージ、SNMP 通知、またはその両方をパブリッシュするインターフェイスの IP アドレスを入力します。

レポート IP アドレス、およびその役割と依存関係の詳細については、「アクセス IP、レポート IP、およびインターフェイス設定の概要」を参照してください。

**ステップ6** Access IP フィールドにアドレスを入力した場合は、Access Type リストで **SNMP** を選択します。

アクセス タイプの詳細については、「アクセス タイプの選択」を参照してください。

**ステップ7** (任意)MARS がこのレポート デバイスの MIB オブジェクトを取得できるようにするには、SNMP RO Community フィールドにデバイスの読み取り専用コミュニティ スtring を入力します。

SNMP RO String を指定する前に、アクセス IP アドレスを定義する必要があります。MARS は SNMP RO String を使用して、レポート デバイスの CPU 使用率、ネットワーク使用率、およびデバイス異常データに関連する MIB を読み取ったり、デバイスやネットワークの設定を検出したりします。

**ステップ8** MARS データベースにデバイスを追加するには、**Submit** をクリックします。

**結果:** この処理により、データベース テーブルに変更が記録されます。ただし、MARS アプライアンスの動作中のメモリには変更がロードされません。アクティブ化処理を行うと、変更が作業メモリに送信されます。

**ステップ9** **Activate** をクリックします。

**結果:** MARS はこのデバイスによって生成されたイベントのセッション化を開始し、定義済みのインスペクション規則および廃棄規則を使用してイベントを評価します。アクティブ化の開始前にデバイスから MARS にパブリッシュされたイベントについては、デバイスのレポート IP アドレスをマッチ基準にして、問い合わせを行うことができます。

## 汎用ルータ デバイス

MARS に L2 または L3 デバイスを追加するには、これらのデバイスで SNMP がイネーブルになっている必要があります。汎用ルータは、『*Supported Devices and Software Versions for CS-MARS Local Controller 4.1*』に記載されていない任意の L2 または L3 デバイスです。

### MARS での汎用ルータの追加および設定

MARS で汎用ルータ デバイスを追加および設定する手順は、次のとおりです。

**ステップ1** **Admin > System Setup > Security and Monitor Devices > Add** の順に選択します。

**ステップ2** Device Type リストで **Generic Router version unknown** を選択します。

**ステップ3** Device Name フィールドにデバイスの名前を入力します。

MARS はこの名前とレポート IP アドレスを対応付けます。この名前はトポロジーマップ、クエリー、および Security and Monitoring Device リストで使用されます。ルータやファイアウォールなど、検出処理をサポートするデバイスの場合、MARS はこのフィールド値の名前を、デバイス設定内で検出された名前に合わせて変更します。通常は、*hostname.domain* フォーマットが使用されます。Windows ホストや Linux ホスト、ホスト アプリケーションなど、検出できないデバイスの場合、MARS は指定された値を使用します。

**ステップ 4** (任意)MARS が、このデバイスから設定を検出できるようにするには、Access IP フィールドに管理 IP アドレスを入力します。

アクセス IP アドレス、およびその役割と依存関係の詳細については、「アクセス IP、レポート IP、およびインターフェイス設定の概要」を参照してください。

**ステップ 5** Reporting IP フィールドに、Syslog メッセージ、SNMP 通知、またはその両方をパブリッシュするインターフェイスの IP アドレスを入力します。

レポート IP アドレス、およびその役割と依存関係の詳細については、「アクセス IP、レポート IP、およびインターフェイス設定の概要」を参照してください。

**ステップ 6** Access IP フィールドにアドレスを入力した場合は、Access Type リストで **SNMP** を選択します。

アクセス タイプの詳細については、「アクセス タイプの選択」を参照してください。

**ステップ 7** (任意)MARS がこのレポート デバイスの MIB オブジェクトを取得できるようにするには、SNMP RO Community フィールドにデバイスの読み取り専用コミュニティ スtring を入力します。

SNMP RO String を指定する前に、アクセス IP アドレスを定義する必要があります。MARS は SNMP RO String を使用して、レポート デバイスの CPU 使用率、ネットワーク使用率、およびデバイス異常データに関連する MIB を読み取ったり、デバイスやネットワークの設定を検出したりします。

**ステップ 8** MARS データベースにデバイスを追加するには、**Submit** をクリックします。

*結果:* この処理により、データベース テーブルに変更が記録されます。ただし、MARS アプライアンスの動作中のメモリには変更がロードされません。アクティブ化処理を行うと、変更が作業メモリに送信されます。

**ステップ 9** **Activate** をクリックします。

*結果:* MARS はこのデバイスによって生成されたイベントのセッション化を開始し、定義済みのインスペクション規則および廃棄規則を使用してイベントを評価します。アクティブ化の開始前にデバイスから MARS にパブリッシュされたイベントについては、デバイスのレポート IP アドレスをマッチ基準にして、問い合わせを行うことができます。

