



第 10 章 汎用、Solaris、Linux、および Windows アプリケーション ホストの設定

アプリケーション ホストは、重要なアプリケーションを実行するネットワーク上のホストにすぎません。サポートされている多くのレポートデバイスおよび軽減デバイスを MARS 内で表示するには、これらの中で稼働している基本ホストを定義する必要があります。このようなアプリケーションの例としては、CheckPoint Firewalls およびすべての形式の Web サーバなどがあります。

MARS には、次のホストタイプを定義する機能があります。

- ・ **汎用** - 一般的なオペレーティング システム、および直接サポートされていないオペレーティング システムを識別します。
- ・ **Windows** - Microsoft オペレーティング システムのいずれかを識別します。
- ・ **Solaris** - Solaris オペレーティング システム ファミリーのいずれかを識別します。
- ・ **Linux** - Linux オペレーティング システム ファミリーのいずれかを識別します。

アプリケーション ホストはできるだけ正確に定義する必要があります。この注意事項は、脆弱性評価情報および一般設定に適用されます。この詳細情報は、ホストが既知の攻撃（そのホストで稼働しているオペレーティング システムやアプリケーション/サービスを特に対象としている攻撃など）の被害を受けやすいかどうかを MARS が判別する場合に役立ちます。

この章の具体的な内容は次のとおりです。

- ・ 汎用デバイスの追加
- ・ Sun Solaris および Linux ホスト
- ・ Microsoft Windows ホスト
- ・ デバイスの脆弱性評価に関する情報

汎用デバイスの追加

Syslog または SNMP デバイスが MARS のサポート対象デバイス リストに表示されていない場合でも、MARS はこれらのデバイスをすべてサポートできます。Syslog または SNMP デバイスをネットワークプロトコルに追加して、MARS にデータを報告するように設定し、フリー形式クエリーを使用して問い合わせることができます。フリー形式クエリーの詳細については、「[To Run a Free-form Query](#)」(p.18-17)を参照してください。

Sun Solaris および Linux ホスト

Solaris または Linux ホスト ログ情報を受信して処理するように MARS を設定するには、次の 3 つのタスクを実行する必要があります。

- ・ イベントを生成するための Solaris または Linux ホストの設定
- ・ MARS アプライアンスにパブリッシュするための Syslog の設定
- ・ Solaris または Linux ホスト ログを受信するための MARS の設定

イベントを生成するための Solaris または Linux ホストの設定

MARS アプライアンスは Linux/Solaris ホストから Syslog 情報を受信できます。Linux/Solaris アプリケーションを設定するには、Syslog に書き込むように次のアプリケーションを設定する必要があります。

- ・ xferlog
- ・ inetd

システム ログに書き込むようにこれらのアプリケーションを設定する手順は、次のとおりです。

ステップ 1 xferlog(FTP [ファイル転送プロトコル] サーバからの転送ロギング情報を提供)

ftpd の場合、以下を /etc/ftpd/ftpaccess に追加します。

```
log transfers real,guest,anonymous inbound,outbound log syslog+xferlog
```

ステップ 2 inetd トレース メッセージ (inetd を使用して実行されるサービスの認証情報を提供)

inetd の場合、/etc/rc2.d/S72inetdsvc 中の行の

```
/usr/sbin/inetd -s
```

という箇所は、以下に変更する必要があります。

```
/usr/sbin/inetd -t -s
```

その他のメッセージは Syslog に自動的に表示されるため、特に設定する必要はありません。

ステップ 3 メッセージ生成をイネーブルにしたら、MARS アプライアンスにメッセージをパブリッシュするように Syslog デーモンを設定する必要があります。詳細については、「MARS アプライアンスにパブリッシュするための Syslog の設定」を参照してください。

MARS アプライアンスにパブリッシュするための Syslog の設定

システム ログを書き込むアプリケーションを正しくイネーブルにしたら、MARS アプライアンスにメッセージをパブリッシュするように、Solaris または Linux ホストの Syslog デーモンを設定する必要があります。

MARS アプライアンスに Syslog をパブリッシュするように Solaris または Linux ホストを設定する手順は、次のとおりです。

ステップ 1 /etc/syslog.conf ファイルを編集して、次に示す行を追加します。

```
*.debug @MARS_hostname
```

ここで、*MARS_hostname* は MARS アプライアンスのホスト名または IP アドレスです。

syslog.conf ファイルにこの行を追加すると、コンソールに送信されるすべてのメッセージは、MARS アプライアンスにもリダイレクトされます。

Solaris または Linux ホスト ログを受信するための MARS の設定

MARS に汎用デバイスを追加する手順は、次のとおりです。

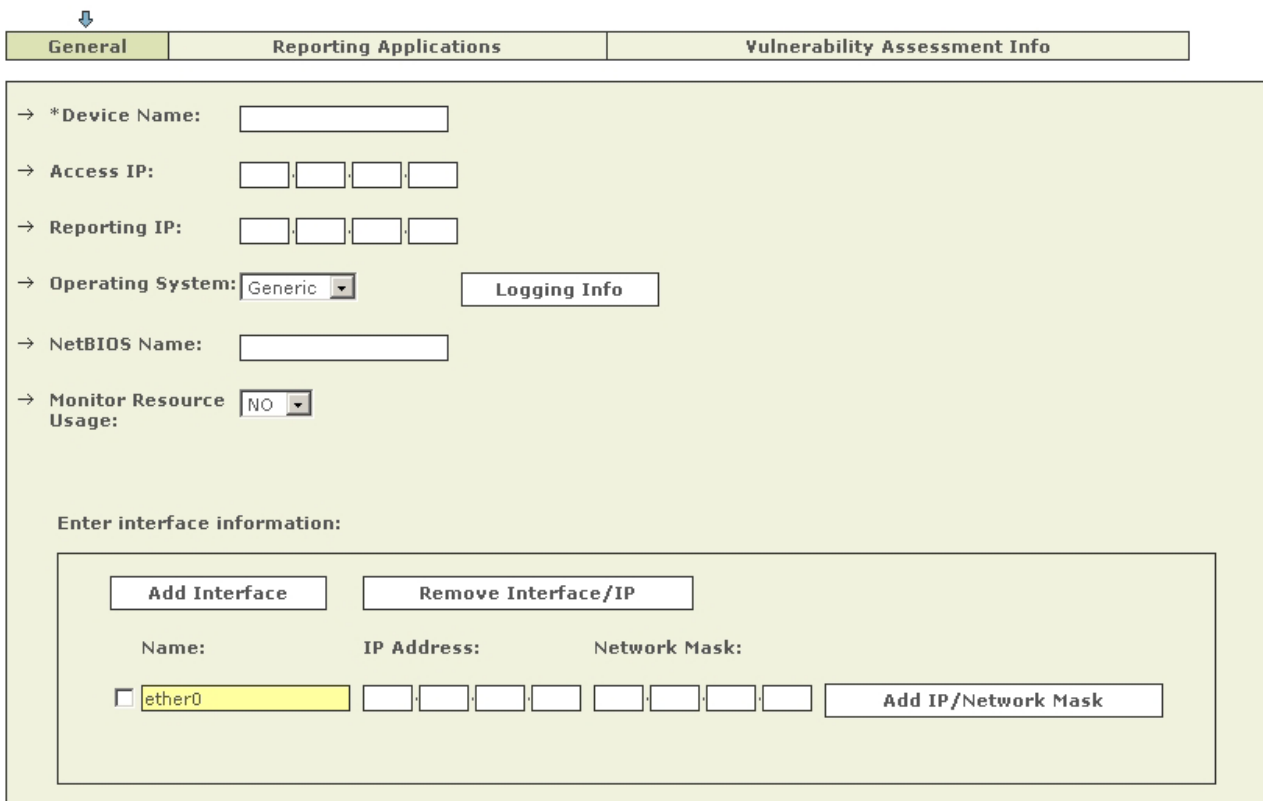
ステップ 1 Admin > Security and Monitor Devices > Add の順にクリックします。

図 10-1 汎用デバイスの追加



ステップ 2 Device Type リストで、Add SW Security apps on a new host を選択します。

図 10-2 ログを受信する汎用デバイスの追加



ステップ 3 Device Name および Reporting IP アドレスを入力します。

ステップ 4 Operating System で Generic を選択します。

ステップ 5 Logging Info を選択し、Receive を選択してから、Submit をクリックします。

ステップ 6 Apply をクリックしてデバイスを追加します。

Microsoft Windows ホスト

MARS は、Microsoft Windows を稼働するホストからプルされたデータを処理します。このデータは、セキュリティ イベント ログ、およびアプリケーション イベント ログやシステム イベント ログ内のイベントなどです。Microsoft Windows (サーバまたはワークステーションバージョン) を稼働しているホストからログを取得する方法は、次の 2 つです。

- ・ ホストからログをプルするように MARS を設定する。
- ・ MARS アプライアンスにログ データを送信するようにホストを設定する。

これらの 2 つの方法は、相互に排他的です。つまり、両方を同時に設定することはできません。どの方法を使用するかは、ホストの準備に要する期間、MARS アプライアンスの予測負荷、およびイベント データを MARS が処理する場合のリアルタイム性によって決まります。

プル方式では、各ホストからのイベント データを関連付けるためのシステム リソースだけでなく、これらのデータを問い合わせるプルするためのシステム リソースも必要です。この方式は単一プロセス内で動作し、特定のデバイスからのプルが完了してから、次のデバイスに移動します。そのため、プル方式では、デバイス数が増えるにつれて、すべてのレポート デバイスを一巡するまでの時間が長くなります。

プッシュ方式は MARS アプライアンスのリソース利用率、および MARS アプライアンスのイベント データ認識速度の点でプル方式よりも効率的ですが、Microsoft Windows ホストに Snare Agent for Windows をインストールして設定する必要があります。Snare Agent はサーバから MARS にほぼリアルタイムでイベント データをプッシュします。監査イベントが発生すると、Snare Agent はイベントの詳細を示す Syslog メッセージを MARS に送信します。各 Snare Agent がプル方式のように単一プロセスに束縛されずに、独立して機能できるという点で、この方式の方が効率的です。

ここでは、これらの 2 つの方式について説明します。

- ・ プッシュ方式: 汎用 Microsoft Windows ホストの設定
- ・ プル方式: Microsoft Windows ホストの設定

プッシュ方式: 汎用 Microsoft Windows ホストの設定

MARS は Microsoft Windows が稼働するホストをレポート デバイスとして扱い、ホストで生成されたイベント ログ データをモニタリングすることができます。ホストでは InterSect Alliance SNARE Agent for Windows を稼働させる必要があります。これにより、イベント ログ データがキャプチャされ、MARS に送信されます。プッシュ方式では、4 つの手順を実行します。

1. Microsoft Windows ホストに SNARE エージェントをインストールします。詳細については、「Microsoft Windows ホストへの SNARE エージェントのインストール」を参照してください。
2. イベント データを MARS アプライアンスに転送するように SNARE エージェントを設定します。詳細については、「Microsoft Windows ホストでの SNARE のイネーブル化」を参照してください。
3. ホストと MARS アプライアンス間で UDP 514 トラフィックを送信できるように設定します。
4. イベント データを正しく解析して、関連付けられるように MARS 内の該当するホストを識別します。詳細については、「Windows ホスト ログをプルまたは受信するための MARS の設定」を参照してください。

Microsoft Windows ホストへの SNARE エージェントのインストール

SNARE エージェントをインストールする手順は、次のとおりです。

ステップ 1 適切な管理権限を持つユーザ名を使用して、ターゲット ホストにログインします。

このユーザ名には、監査データをパブリッシュする権限、および新規プログラムをインストールする権限が設定されていなければなりません。

ステップ 2 次の URL から、ターゲット ホストのオペレーティング システム タイプに対応した SNARE Agent for Windows をダウンロードします。

<http://www.intersectalliance.com/projects/SnareWindows/index.html#Download>

ステップ 3 SnareSetup<version>.exe ファイルをダブルクリックして、インストール プログラムを開始します。

ステップ 4 Next をクリックします。

ステップ 5 ターゲット インストール フォルダを選択して、**Next** をクリックします。

ステップ 6 Components リスト内で **Normal Installation** を選択して、**Next** をクリックします。

ステップ 7 ターゲットとなるスタート メニューの場所を選択して、**Next** をクリックします。

ステップ 8 選択オプションを確認し、**Install** をクリックします。

ステップ 9 SNARE がインストールされ、ローカル ホストで起動されます。ダイアログボックスが表示され、SNARE による Microsoft Windows ホストの EventLog 設定の制御を許可するかどうかを指定するように求められます。

ステップ 10 **Yes** を選択して、SNARE による Microsoft Windows ホストの EventLog 設定の制御をイネーブルにします。

SNARE - Remote Event Logging for Windows ユーザ インターフェイスが表示されます。

ステップ 11 Snare エージェントを設定するには、「Microsoft Windows ホストでの SNARE のイネーブル化」に進みます。

Microsoft Windows ホストでの SNARE のイネーブル化

ターゲット Microsoft Windows ホストに SNARE エージェントをダウンロードして、インストールしたら、MARS アプライアンスに正しいフォーマットで正しいイベント データが転送されるようにエージェントを設定します。



注 SNARE を初めてインストールすると、「Do you want Snare to take over control of your Event Log?」という確認メッセージのダイアログボックスが表示されます。**Yes** を選択します。

SNARE エージェントを設定する手順は、次のとおりです。

ステップ 1 **All Programs > InterSect Alliance > Snare for Windows to** の順にクリックして、SNARE - Remote Event Logging for Windows ユーザ インターフェイスを実行します。

ステップ 2 SNARE を初めてインストールすると、「Do you want Snare to take over control of your Event Log?」という確認メッセージのダイアログボックスが表示されます。**Yes** を選択します。

ステップ 3 **Setup > Audit Configuration...** の順にクリックします。

Audit Configuration ダイアログボックスが表示されます。

ステップ 4 次のフィールドの値を指定します。

- ・ **Enter the local host name** - ローカル ホストの IP アドレスまたは DNS 名を指定します。
- ・ **Enter the snare server ip or dns addr.** - MARS アプライアンスの IP アドレスまたは DNS 名を指定します。

ステップ 5 次のオプションが選択されていることを確認します。

- ・ **Enable SYSLOG header**
- ・ **Automatically set audit configuration**
- ・ **Automatically set file system audit configuration**

ステップ 6 **OK** をクリックして、Audit Configuration ダイアログボックスを閉じて、変更を保存します。

ステップ 7 **File > Exit** の順にクリックして、SNARE - Remote Event Logging for Windows ユーザ インターフェイスを閉じます。

Snare エージェントが停止して、再起動し、設定変更が適用されます。

プル方式: Microsoft Windows ホストの設定

プッシュ方式の代わりに、Microsoft Windows ホストからイベント ログ データ(セキュリティ、アプリケーション、およびシステム イベント ログ)をプルするように MARS を設定できます。プル方式では、4 つの手順を実行します。

1. Windows ホストおよび MARS アプライアンスのクロックが同期していることを確認します。確実に同期させるために、NTP サーバを設定することを推奨します。詳細については、「[Specify the Time Settings](#)」(p.5-10)を参照してください。
 1. Windows ホストで、MARS アプライアンスがイベント ログ レコードをプルするために使用できるユーザ アカウントを、既存の中から選択するか、または新規に定義します。
 2. このユーザ アカウントに正しい証明書が設定されていることを確認します。ユーザ アカウントが Administrator グループに属していること、およびセキュリティ ログを管理および監査する権限を含んでいることを確認します。詳細については、ホストで稼働しているオペレーティング システムに対応する手順を参照してください。
- ドメイン ユーザを使用した Windows のプルのイネーブル化
 - Windows NT からの Windows のプルのイネーブル化
 - Windows 2000 Server からの Windows のプルのイネーブル化
 - Windows Server 2003 または Windows XP ホストからの Windows のプルのイネーブル化
3. 正しいイベント データを生成するように Windows ホストを設定します。
 4. イベント データを正しく解析して、関連付けられるように MARS 内の該当するホストを識別します。詳細については、「Windows ホスト ログをプルまたは受信するための MARS の設定」を参照してください。
 5. Microsoft を稼働するすべての識別済みホストからイベント ログ データをプルするインターバルを指定します。詳細については、「Windows イベント ログのプル時間間隔」を参照してください。

ドメイン ユーザを使用した Windows のプルのイネーブル化

ドメイン ユーザ(domain\username)を使用した Windows のプルをイネーブルにするには(CORP\syslog など)、ドメイン コントローラで次の手順を実行したあとに、クライアントで Windows のプルをイネーブルにします。

ステップ 1 ドメイン コントローラで、**Administrative Tools > Default Domain Security Policy > Security Settings > Local Policies > User Rights Management** の順にクリックします。

ステップ 2 ドメイン ユーザ(domain\username)に **Manage auditing and security log** 権限を付与します。

Windows NT からの Windows のプルのイネーブル化

Windows NT ホストからイベント ログ データをプルできるように MARS を設定する手順は、次のとおりです。

ステップ 1 **Start > Programs > Administrative Tools > User Manager** のメニュー バーで、**Policies** を選択します。

ステップ 2 サブメニューで、**User Rights** を選択し、**Manage auditing and security log** 権限が、イベント ログ レコードをプルするために使用されるユーザ アカウントに付与されていることを確認します。

ステップ 3 サブメニューで、**Audit** を選択します。サイトのセキュリティ監査ポリシーに従って、監査ポリシーを設定します。

Windows 2000 Server からの Windows のプルのイネーブル化

Windows 2000 サーバにドメイン情報を送信する Active Directory Service(ADS)サーバが存在しない場合は、MARS アプライアンスが Syslog をプルする各ホストに対し、このプロパティを *Disabled* に設定する必要があります。

Windows 2000 ホストからイベント ログ データをプルできるように MARS を設定する手順は、次のとおりです。

ステップ 1 [スタート] > [設定] > [コントロール パネル] > [管理ツール] > [ローカル セキュリティ ポリシー] の順に移動します。

Local Security Settings アプレットが表示されます。

ステップ 2 次の Local Policy グループで、指定どおりに値を設定します。

- ・ Security Settings > Local Security Policy > User Rights Mangament
Manage auditing and security log 権限がイベント ログ レコードをプルするために使用されるユーザ アカウントに付与されていることを確認します。
- ・ Security Settings > Local Security Policy > Audit Policy
 サイトのセキュリティ監査ポリシーに従って監査ポリシーを設定し、Effective Setting のすべてのエントリが **Success, Failure** に設定されていることを確認します。

Windows Server 2003 または Windows XP ホストからの Windows のブルのイネーブル化



注 Microsoft Windows XP Home Edition を選択する場合は、[すべてのプログラム] > [コントロール パネル] > [管理ツール] > [サービス] で Remote Procedure Call サービスをイネーブルにする必要があります。Windows XP Professional では、このサービスはデフォルトでイネーブルに設定されています。

Windows Server 2003 または Windows XP ホストからイベント ログ データをプルできるように MARS を設定する手順は、次のとおりです。

ステップ 1 [スタート] > [設定] > [コントロール パネル] > [管理ツール] > [ローカル セキュリティ ポリシー] の順に移動します。

Local Security Settings アプレットが表示されます。

ステップ 2 次の Local Policy グループで、指定どおりに値を設定します。

- ・ Security Settings > Local Security Policy > User Rights Mangament
Manage auditing and security log 権限がイベント ログ レコードをプルするために使用されるユーザ アカウントに付与されていることを確認します。
- ・ Security Settings > Local Security Policy > Audit Policy
 サイトのセキュリティ監査ポリシーに従って、監査ポリシーを設定します。



注 特定のイベント (Log on/off など) を監査する場合に、イベント ログをプルすると、セキュリティ イベント ログが生成されます。デフォルトのドメイン ポリシーを設定するか、または Windows システムのセキュリティ イベント ログの保持方式を **Overwrite as needed** に設定することを推奨します。このようにしないと、ログが一杯の場合、Windows システムでは新しいイベント ログを生成できません。

Windows ホスト ログをプルまたは受信するための MARS の設定

Microsoft Windows ホストの準備を終えたら、MARS 内の該当するホストを識別し、このホストでプッシュ方式とプル方式のどちらが使用されているのかを識別する必要があります。

ログをプルまたは受信するように MARS アプライアンスを設定する手順は、次のとおりです。

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

ステップ 2 **Device Type** リストで、**Add SW Security apps on a new host** または **Add SW security apps on existing host** を選択します。

ステップ 3 新しいホストを追加する場合は、**Device Name** にデバイス名、**IP addresses** に IP アドレスを入力します。

ステップ 4 リストで **Operating System > Windows** の順に選択します。

ステップ 5 (任意) **NetBIOS name** を入力します。

図 10-3 Window のログ設定

General	Reporting Applications	Vulnerability Assessment Info
→ *Device Name: <input type="text" value="Softie III"/>		
→ Access IP: <input type="text" value="192"/> · <input type="text" value="168"/> · <input type="text" value="2"/> · <input type="text" value="5"/>		
→ Reporting IP: <input type="text" value="192"/> · <input type="text" value="168"/> · <input type="text" value="2"/> · <input type="text" value="5"/>		
→ Operating System: <input type="text" value="Windows"/>		<input type="button" value="Logging Info"/>
→ NetBIOS Name: <input type="text" value="netBIOS_Name"/>		
→ Monitor Resource Usage: <input type="text" value="NO"/>		
Enter interface information:		
<input type="button" value="Add Interface"/>		<input type="button" value="Remove Interface/IP"/>
Name:	IP Address:	Network Mask:
<input type="checkbox"/> <input type="text" value="ether0"/>	<input type="text" value="192"/> · <input type="text" value="168"/> · <input type="text" value="2"/> · <input type="text" value="5"/>	<input type="text" value="255"/> · <input type="text" value="255"/> · <input type="text" value="255"/> · <input type="text" value="255"/>
<input type="button" value="Add IP/Network Mask"/>		

143263

ステップ 6 **Logging Info** をクリックして、OS ログイン情報を設定します。新しいポップアップ ウィンドウが表示されます。

ステップ 7 Windows Operating System で、サーバまたはワークステーションのバージョンに対応した正しいオプションを選択します。

- ・ Microsoft Windows 2000
- ・ Microsoft Windows 2003 (Microsoft Windows XP プラットフォームでも使用)
- ・ Microsoft Windows Generic
- ・ Microsoft Windows NT



注 Microsoft Windows XP Home Edition を選択する場合は、[すべてのプログラム] > [コントロール パネル] > [管理ツール] > [サービス] で Remote Procedure Call サービスをイネーブルにする必要があります。

ステップ 8 実行するホスト設定に基づいて、**Pull** または **Receive** チェックボックスをオンにします。



注意 一度に両方のチェックボックスをオンにしないでください。予測できない結果が生じます。

ステップ 9 プル方式を選択した場合は、次のフィールドに値を入力します。

- ・ **Domain name** — ホストが属するドメイン名を識別します。
- ・ **Host login** — セキュリティ監査およびログ権限を持つユーザ名を識別します。
- ・ **Host password** — Host login フィールドで指定されたユーザ名を認証するパスワードを識別します。

ステップ 10 **Submit** をクリックします。

図 10-4 Window のログイン

OS Logging Information

ステップ 11 **Submit** をクリックして、変更を保存します。

ステップ 12 インターフェイス IP アドレスおよびネットワーク マスクを追加します。

ステップ 13 **Apply** をクリックします。

ステップ 14 **Vulnerability Assessment Info** リンクをクリックして、このホストへのフォールス ポジティブ攻撃を判別するために MARS が使用するホスト情報を定義します。「デバイスの脆弱性評価情報の定義」に進みます。

ステップ 15 **Done** をクリックして、変更を保存します。

ステップ 16 デバイスをアクティブにするには、**Activate** をクリックします。

ステップ 8 で Pull チェックボックスをオンにした場合は、MARS がホストからイベント ログをプルするインターバル値が指定されていることを確認します。詳細については、「Windows イベント ログのプル時間間隔」を参照してください。

Windows イベント ログのプル時間間隔

これで、レポート バイスとして定義されたすべての Microsoft Windows ホストから、MARS がイベント ログをプルするインターバルを設定できます。この機能により、レポート デバイスとして設定された Windows ホストに対して MARS がログを要求する頻度が決定されます。



注 SNARE を使用してログ データを MARS にプッシュしている場合は、この設定をイネーブルにする必要はありません。

Windows イベント ログのプル時間間隔を設定する手順は、次のとおりです。

ステップ 1 Admin > System Parameters > Windows Event Log Pulling Time Interval の順にクリックします。

Windows Event Log Pulling Time Interval

ステップ 2 新しい時間間隔を秒単位で入力します。デフォルト値は 300 秒 (5 分間) です。

ステップ 3 Submit をクリックします。

脆弱性評価情報の定義

MARS で定義したホストごとにホスト情報を指定すると、MARS で検出された攻撃に対してホストが脆弱であるかどうかを評価するのに役立てることができます。たとえば、ホストで稼働しているオペレーティング システムを識別し、最新の、または最も近いパッチ レベルを提供することもできます。特定のオペレーティング システムを対象とする攻撃が検出されると、MARS はホストが攻撃対象のオペレーティング システムを稼働しているかどうかを迅速に判別します。

ホストがレポート デバイスの基本プラットフォームとして定義されている場合は、レポート デバイスの定義の一部として、この情報を定義する必要があります。

MARS は検出されたホストを、Management > IP Management のホストリストに追加する作業を開始します。Qualys QualysGuard などの脆弱性評価ソフトウェア デバイスまたはサービスがネットワークで稼働していない場合は、これらのホストを定期的に確認して、情報を更新する必要があります。

ホストの脆弱性評価情報を指定する手順は、次のとおりです。

ステップ 1 目的のホストを選択して、次のいずれかを実行します。

- ・ Management > IP Management の順に選択し、目的のホストの横にあるチェックボックスをオンにして、Edit をクリックします。
- ・ Admin > Security and Monitor Devices の順に選択し、目的のホストの横にあるチェックボックスをオンにして、Edit をクリックします。

ステップ 2 Vulnerability Assessment Info タブをクリックします。

図 10-5 ホストの脆弱性評価情報

ステップ 3 Specify OS and patch Information で、次のいずれかを実行します。

- ・ **Select operating system from** を選択し、このホストで稼働しているオペレーティング システムと一致するオペレーティング システムをリストから選択します。ステップ 4 に進みます。
- ・ **Define new operating system** を選択して、ステップ a. に進みます。
 - a. Name フィールドにオペレーティング システムの名前を入力します。
 - b. Version フィールドに、このオペレーティング システムのバージョン番号を入力します。
 - c. Patch フィールドのバージョン番号に対応するパッチ レベルを入力します。
 - d. Vendor フィールドにオペレーティング システムのメーカー名を入力します。
 - e. **Apply** をクリックして、オペレーティング システムの定義を保存します。

結果: Select operating system from リストに新しいオペレーティング システム定義が追加され、オプションとして選択されます。

カスタム オペレーティング システムを定義する場合は、ホストの General ページの Operating System リストで **Generic** を選択し、**Apply** をクリックします。そうしないと、Select operating system from リストで新しいオペレーティング システムを選択できません。

ステップ 4 提供した情報をネットワークで稼働している脆弱性評価サービスで上書きする場合は、**Allow Overwrite with VA** チェックボックスをオンにします。

ステップ 5 ホストの詳細情報を追加するには、「ホストで稼働するネットワーク サービスの識別」に進みます。

ステップ 6 **Apply** をクリックして、このホストに対する変更を保存します。

ステップ 7 **Done** をクリックして、Host ページを閉じます。

ホストで稼働するネットワーク サービスの識別

このホストで想定されるネットワーク アクティビティのタイプを指定するには、ホストで稼働しているネットワーク サービスを特定します。このデータは、不正なアクティビティでなくても MARS によって疑わしいとフラグ設定される可能性のあるアクティビティを除去する場合に便利です。たとえば、スケジュールされた時刻にネットワーク検出アプリケーションを実行したり、脆弱性評価プローブを実行したりする管理サーバが配置されている場合です。

ホストで稼働しているネットワーク サービスを識別する手順は、次のとおりです。

ステップ 1 目的のホストを選択して、次のいずれかを実行します。

- ・ **Management > IP Management** を選択し、目的のホストの横にあるチェックボックスをオンにして、**Edit** をクリックします。
- ・ **Admin > Security and Monitor Devices** の順に選択し、目的のホストの横にあるチェックボックスをオンにして、**Edit** をクリックします。

ステップ 2 **Current running services** で、**Add New Service** をクリックします。



注 このダイアログボックスがロードされるまで 5 分以上かかることがあります。開いているウィンドウのタイトル バーにカーソルを置くと、ウィンドウがまだロード中であるかどうかを確認できます。

ステップ 3 サービスおよびアプリケーションに関する詳細をできるだけ多く入力します。

- ・ サービスを選択するか、または新しいサービスを定義することができます。
- ・ アプリケーションを選択するか、または新しいアプリケーションを定義することもできます。

ステップ 4 **Submit** をクリックします。

ステップ 5 **Add New Service** をクリックしてさらにサービスを入力するか、**Submit** をクリックして処理を続けます。

ステップ 6 **Submit** をクリックして、ホストの追加を完了します。
