



第 12 章 Web サーバ デバイスの設定

MARS による Web ログイングを使用するには、ホスト、Web サーバ、および MARS を設定する必要があります。MARS はホストからの受信につき、最大 100 MB の Web ログ データを処理できます。



注 Web ログイングがサポートされているのは、Microsoft IIS (Windows)、Apache (Solaris または Linux)、または iPlanet (Solaris) が稼働しているホストのみです。

この章では、次に示す Web サーバ 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。

- ・ Microsoft Internet Information Sever
- ・ Solaris または RedHat Linux の Apache Web サーバ
- ・ Solaris の Sun Java System Web Server

Microsoft Internet Information Sever

Microsoft Windows が稼働しているコンピュータをレポート デバイスとして MARS に追加できます。Microsoft Windows コンピュータで InterSect Alliance SNARE for IIS を稼働させる必要があります。MAR はそこから Web ログ データを受信します。



注 Microsoft Windows システムと MARS 間のクロックを同期して、時間を一致させてください。

Snare Agent for IIS のインストールおよび設定

MARS にログをパブリッシュするように IIS を設定するには、ログ エージェントをインストールして、設定する必要があります。このエージェントには、InterSect Alliance 含まれていません。Snare Agent for IIS Servers は、次の URL からダウンロードできます。

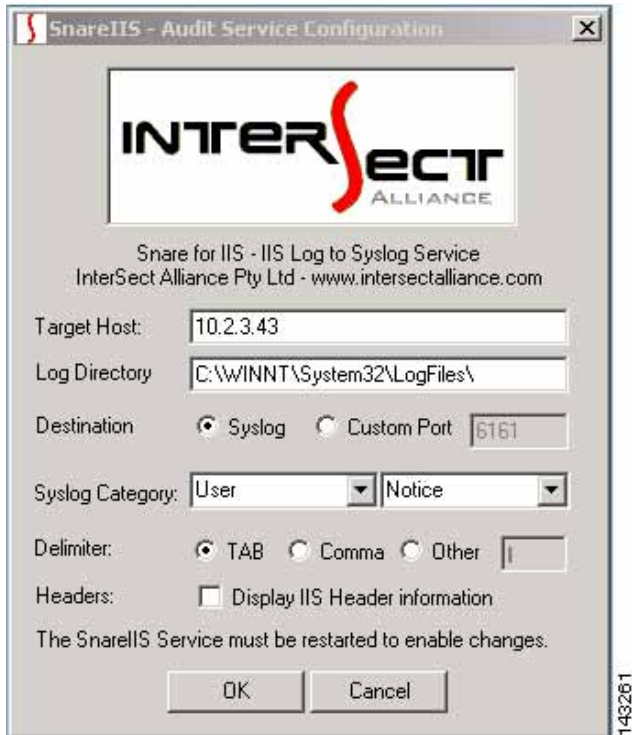
<http://www.intersectalliance.com/projects/SnareIIS/index.html#Download>

Windows Web サーバに SNARE をダウンロードして、インストールしたら、MARS の正しい設定についての詳細が記載された、この項の手順に進んでください。

SNARE に Web ログイングを設定する手順は、次のとおりです。

ステップ 1 [スタート] > [プログラム] > InterSect Alliance > Audit Configuration をクリックします。

図 12-1 SNARE の Web ログインの設定



ステップ 2 Target Host に、MARS の IP アドレスを入力します。

ステップ 3 Log Directory に、ログを格納するディレクトリを入力します。

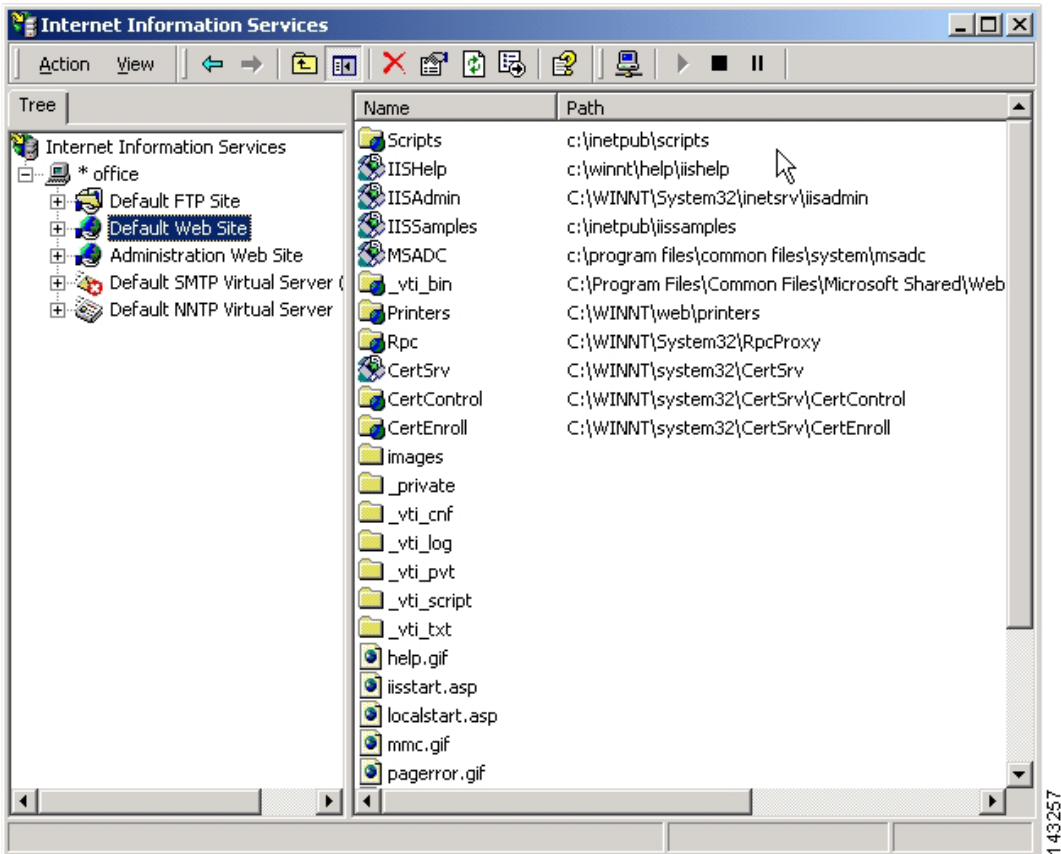
ステップ 4 Destination で、Syslog オプション ボタンをクリックします。

ステップ 5 OK をクリックします。

IIS の Web ログインを設定する手順

ステップ 1 [スタート] > [プログラム] > [管理ツール] > Internet Services Manager をクリックします。

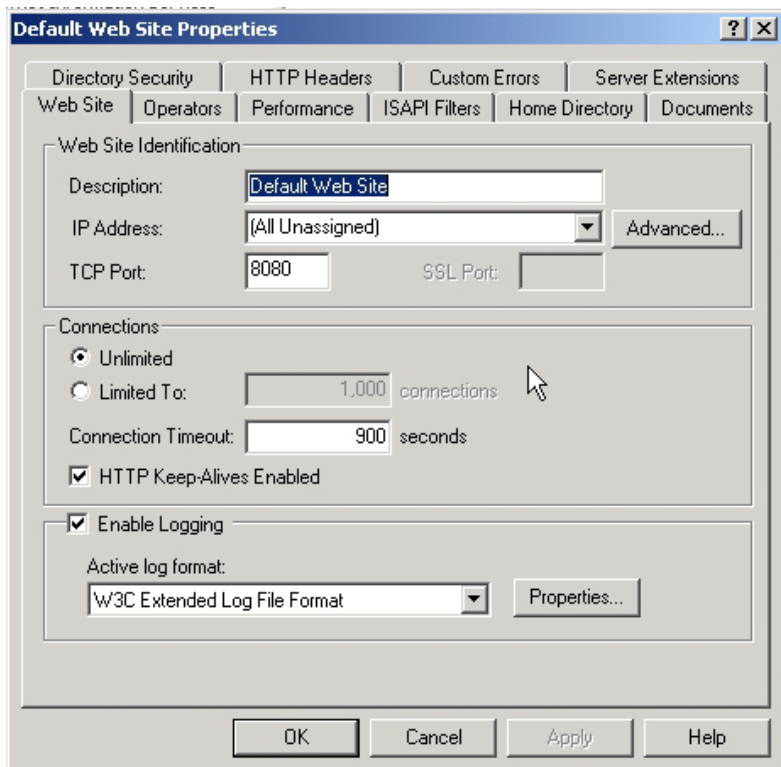
図 12-2 IIS の Web ログिंगの設定



ステップ 2 左側の Tree タブで、Default Web Site を右クリックします。

ステップ 3 ショートカットメニューで、Properties を選択します。

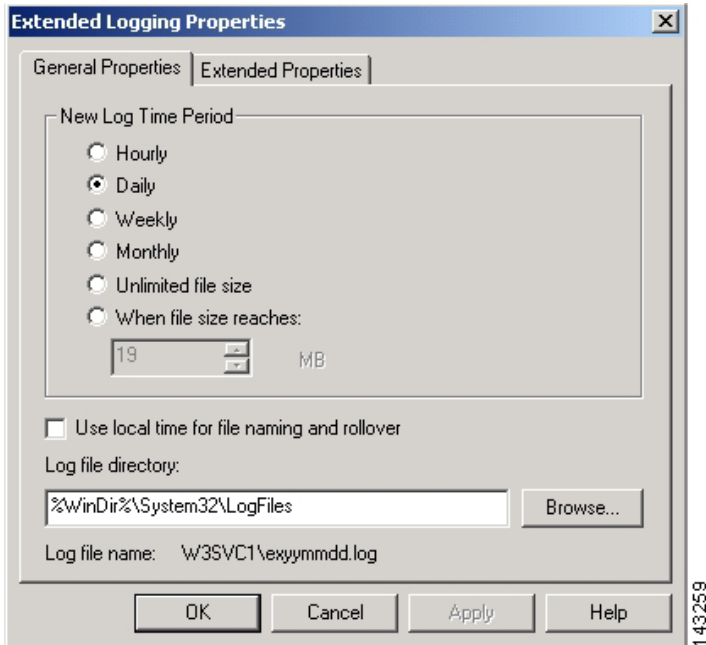
図 12-3 ログिंगのイネーブル化



ステップ 4 **Web Site** タブで、次の処理を実行します。

- a. **Enable Logging** がオンになっていることを確認します。
- b. **Active log format** リストで、**W3C Extended Log Format** を選択します。
- c. **Properties** をクリックします。

図 12-4 汎用ログ設定の選択



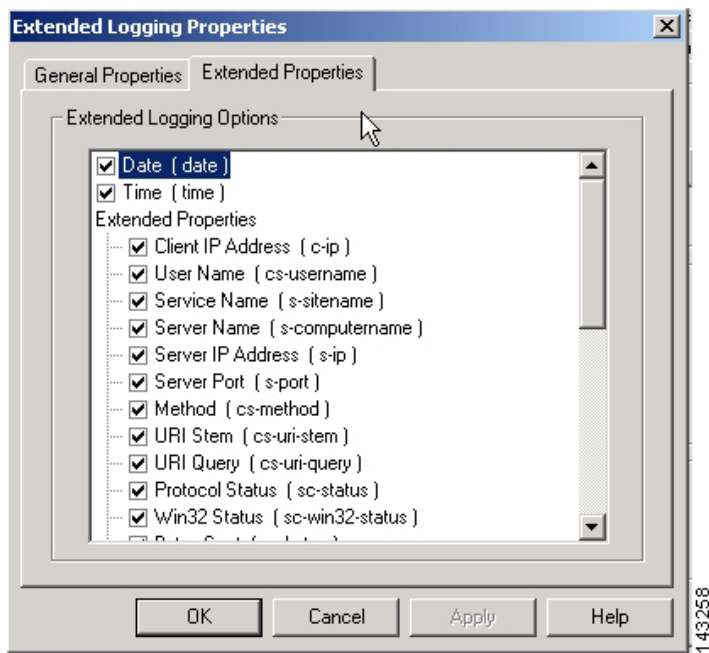
- d. **General Properties** タブで、**New Log Time Period** を **Daily** に設定します。



注 **Log file directory** は **Audit Configuration** プログラムを使用して、設定された値と一致させる必要があります。

- e. **Extended Properties** タブで、使用可能なすべてのプロパティが選択されていることを確認します。

図 12-5 拡張ログ イベントの選択



f. **OK** をクリックします。

ステップ 5 **OK** をクリックします。

MARS 側の設定

ホストの設定情報の追加手順

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

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 **Operation System** リストで **Windows** を選択します。

ステップ 5 **Logging Info** をクリックします。

ステップ 6 この設定の場合は、**Receive host log** チェックボックスをオンにする必要があります。

図 12-6 Windows Web サーバ ログインのメカニズム

OS Logging Information

ステップ 7 Submit をクリックします。

ステップ 8 インターフェイスの追加を続けます。

- ・ 最初のインターフェイスを入力する場合は、インターフェイスの名前、IP アドレス、およびマスクを入力します。
- ・ インターフェイスが複数ある場合は、**Add Interface** をクリックして、新しいインターフェイスの名前、IP アドレス、およびマスクを追加します。

ステップ 9 Add IP/Network Mask をクリックして、IP アドレスおよびマスクを必要なだけインターフェイスに追加します。

ステップ 10 Apply をクリックします。

ステップ 11 Reporting Applications タブをクリックします。

ステップ 12 Select Application リストで、**Generic Web Server Generic** を選択します。

ステップ 13 Add をクリックします。

図 12-7 Windows Web ログ フォーマットの選択

ステップ 14 W3C_EXTENDED_LOG フォーマットを選択します。

ステップ 15 Submit をクリックします。



注 両側を設定してアクティブにした場合は、新しいイベントが発生するまでに 2 つ分のプル インターバルの時間がかかります (デフォルト時間は 10 分)。

Solaris または RedHat Linux の Apache Web サーバ

Solaris の Sun Java System Web Server



注 Sun Java System Web Server の従来の製品名は、Netscape Enterprise Server、iPlanet Web Server、および Sun ONE Web Server でした。

汎用 Web サーバ一般

Solaris または Linux が稼働しているコンピュータをレポート デバイスとして MARS に追加できます。このコンピュータで、MARS に Web ログ データを送信するオープンソース エージェントが稼働していなければなりません。

Solaris または Linux 側の設定

ユーザは、シスコが提供するオープンソース ログイング エージェント、および対応するコンフィギュレーション ファイルを使用できます。このエージェントは、次の URL にあるソフトウェア ダウンロード センターからダウンロードできます。

<http://www.cisco.com/pgcgi-bin/tablebuild.pl/cs-mars-misc>



注 UNIX または Linux システムと MARS 間のクロックを同期して、時間を一致させてください。

UNIX または Linux の Web エージェントのインストールおよび設定

MARS が Web サーバからログを受信するには、Web エージェント(agent.pl version 1.1)をターゲット Web サーバにインストールして、MARS アプライアンスにログをパブリッシュするようにエージェントに指示する必要があります。



注 エージェントをインストールする前に、システムに **perl** および **curl** をインストールしておく必要があります。

UNIX または Linux ホストに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 ホストにルート ユーザとしてログインします。

ステップ 2 /opt/webagent という名前のディレクトリを作成します。

ステップ 3 ファイル agent.pl および webagent.conf を /opt/webagent ディレクトリにコピーします。

ステップ 4 すべてのユーザが読み取って実行できるように、エージェント スクリプト(agent.pl)の保護を設定します。

```
cd /opt/agent
chmod 755 agent.pl
```

ステップ 5 コンフィギュレーション ファイル (webagent.conf) を編集します。

```
logfile_location = access_log_path
MARS_ip_port = MARS_ip_address:port
username = a
password = b
```

次の値を指定します。

- ・ `access_log_path` - Apache アクセス ログの絶対パス名を識別します。
- ・ `MARS_ip_address` - MARS アプライアンスの IP アドレス
- ・ `port` - 8080 (MARS アプライアンスが HTTPS 通信用に使用する TCP ポート)

ファイル内のユーザ名またはパスワードを編集する必要はありません。



注 プルするアクセス ログごとに、独立した webagent.conf ファイルが必要です。これらのファイルには webagent1.conf、webagent2.conf などの名前を付けることを推奨します。これらのファイルは /opt/webagent ディレクトリに格納してください。

webagent.conf 以外のコンフィギュレーション ファイルを使用してエージェントを実行するには、次のコマンドを使用します。

```
agent.pl other_config_file
```

`other_config_file` は Web エージェントのコンフィギュレーション ファイルの名前で置き換えます。

ステップ 6 定期的に MARS にログをプッシュするように、crontab ファイルを編集します。次に、5 分おきにアクセス ログから新しいエントリをプルする例を示します。

```
crontab -e
5,10,15,20,25,30,35,40,45,50,55,0 * * * *
(cd /opt/webagent; ./agent.pl webagent1.conf)
5,10,15,20,25,30,35,40,45,50,55,0 * * * *
(cd /opt/webagent; ./agent.pl webagent2.conf)
```

Web サーバの設定

Apache Web サーバのエージェントの設定手順

ステップ 1 ファイル httpd.conf で、LogFormat が common または combined であること、および MARS で設定されたフォーマットと一致することを確認します。

ステップ 2 Apache サーバを停止してから再起動し、変更を有効にします。

iPlanet Web サーバのエージェントの設定手順

ステップ 1 iPlanet サーバ管理ツールで、**Preferences tab** をクリックします。

ステップ 2 左側のメニューで、**Logging Options** リンクをクリックします。

ステップ 3 **Log File** が MARS に設定されたログ ファイル名と一致することを確認します。

ステップ 4 **Format** のオプション ボタン、**Use Common Logfile Format** がオンになっていることを確認します。

ステップ 5 変更した場合は、**OK** をクリックします。

ステップ 6 必要に応じて、iPlanet Web サーバをシャットダウンして、再起動します。

MARS 側の設定

ホストの設定情報の追加手順

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

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 **Operation System** リストで、**Solaris** または **Linux** を選択します。

ステップ 5 **Logging Info** をクリックします。

ステップ 6 この設定の場合は、**Receive host log** チェックボックスをオンにする必要があります。

図 12-8 UNIX または Linux Web サーバ ロギングのメカニズム

OS Logging Information

Logging mechanism: Pull Receive

Host login:

Host password:

Cancel Submit

ステップ 7 **Submit** をクリックします。

ステップ 8 インターフェイスの追加を続けます。

- 最初のインターフェイスを入力する場合は、インターフェイスの名前、IP アドレス、およびマスクを入力します。
- インターフェイスが複数ある場合は、**Add Interface** をクリックして、新しいインターフェイスの名前、IP アドレス、およびマスクを追加します。

ステップ 9 **Add IP/Network Mask** をクリックして、IP アドレスおよびマスクを必要なだけインターフェイスに追加します。

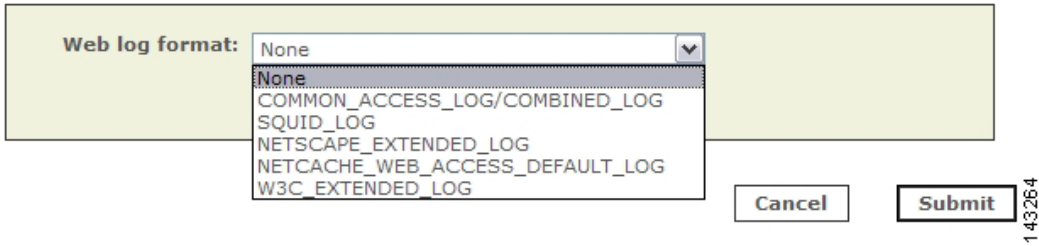
ステップ 10 **Apply** をクリックします。

ステップ 11 **Reporting Applications** タブをクリックします。

ステップ 12 **Select Application** リストで、**Generic Web Server Generic** を選択します。

ステップ 13 **Add** をクリックします。

図 12-9 Linux オペレーティング システムの Web ログ フォーマット



Web log format: 143264

- None
- COMMON_ACCESS_LOG/COMBINED_LOG
- SQUID_LOG
- NETSCAPE_EXTENDED_LOG
- NETCACHE_WEB_ACCESS_DEFAULT_LOG
- W3C_EXTENDED_LOG

ステップ 14 Web Log Format リストで、適切なフォーマットを選択します。

ステップ 15 Submit をクリックします。



注 デバイスを編集したら、**Activate** をクリックして、変更を有効にする必要があります。
