管理設定

この章では、Object Request Broker Element Management（ORBEM）および Simple Network Management Protocol（SNMP）オプションを設定する手順について説明します。

この章は、次の項で構成されています。

- ORBEM （1 ページ）
- SNMP MIB ブラウザ （3 ページ）
- SNMP サポート （6 ページ）

ORBEM

重要 StarOS リリース 21.2 以降では、ORBEM はサポートされていません。

システムは、Common Object Broker Request Architecture（CORBA）ベースの要素管理システム（EMS）で管理できます。

重要 この項の設定例で使用されているコマンドは、基本機能を提供します。最も一般的なコマンドとキーワードのオプションが示されています。多くの場合、他のオプションコマンドやキーワードオプションを使用できます。すべてのコマンドの詳細については、『*Command Line Interface Reference*』を参照してください。

システムが EMS と通信するように設定するには、次の手順を実行します。

手順

ステップ 1 の設定例を適用して、クライアント ID のパラメータを設定し、STOP/TCP ポート設定を行います。 ORBEM クライアントとポートパラメータの設定 （2 ページ）

ステップ 2 の例の設定を適用して、Internet Inter-ORB Protocol（IIOP）転送パラメータを設定します。 IIOP トランスポートパラメータの設定 （2 ページ）

ステップ 3 の手順に従って、新しい ORBEM 設定を表示します。ORBEM パラメータの確認 （3 ページ）

ステップ 4 「設定の確認と保存」の説明に従って、設定を保存します。

ORBEM クライアントとポートパラメータの設定

クライアント ID パラメータを設定し、SIOP/TCP ポート設定を設定するには、次の例を使用します。

```
configure
  orbem
    client id encrypted password password
    max-attempt number
    session-timeout time
    siop-port port_number
    event-notif-siop-port siop_notif_port
    event-notif-service
    end
```

注：

- client id コマンドを複数回発行して、複数のクライアントを設定することができます。
- 設定されている最大試行回数に達したためにクライアント ID が非アクティブ化された場合は、**activate client id** コマンドを使用して再アクティブ化します。
- システムと EMS の間にファイアウォールが存在する場合は、SIOP ポート番号と TCP ポート番号 15011 を開きます。
- **event-notif-service** コマンドを介して、ORB 通知サービスが有効になっている場合は、どのイベントを送信するかを決定するフィルタを設定できます。デフォルトでは、サービスは、すべてのエラーおよび上位レベルのイベント、ORBS ファシリティの「info」レベルのイベント、CLI コマンドログ、およびライセンス変更ログを送信します。必要に応じて、**event-notif-service filter** コマンドを含めることによってフィルタを設定します。設定する必要があるフィルタごとに、このコマンドを入力します。

IIOP トランスポートパラメータの設定

次の例を使用して、ネットワークを介して ORB ベースの管理を実行できるようにする Internet Inter-ORB Protocol（IIOP）トランスポートパラメータを設定します。

```
configure
  orbem
    iiop-transport
    iiop-port iiop_port_number
    event-notif-iiop-port iiop_notif_port
    end
```

注：

- セキュアソケットレイヤ（SSL）オプションを使用している場合は、IIOP転送パラメータを有効にしないでください。
- SSL を使用するようにORBEMインターフェイスを設定するには、証明書と秘密キーを指定します。

ORBEM パラメータの確認

手順

ステップ 1 クライアントが正しく設定されていることを確認するには、**show orbem client table** コマンドを実行します。このコマンドは、設定されているORBEMクライアントを一覧表示し、その状態と権限を表示します。

ステップ 2 **Show orbem status** コマンドを実行して、orbem パラメータの設定を確認します。次に、このコマンドの出力例を示します。

```
Service State                      : On
Management Functions               : FCAPS
IOP Address                        : 192.168.1.150
SSL Port                           : 14131
TCP Port                           : 14132
Notification SSL Port              : 7777
Notification TCP Port              : 7778
Session Timeout                    : 86400 secs
Max Login Attempts                 : 5
IIOP Transport                     : On
Notification                       : On
Debug Level                        : Off
IDL Version Check                  : On
Number of Current Sessions         : 1
Number of Event Channels Open      : 0
Number of Operations Completed     : 2895
Number of Events Processed         : 0
Avg Operation Processing time      : 87214 usecs
                    (last 1000)    : 87950 usecs
```

SNMP MIB ブラウザ

この項では、MIB ブラウザを使用して最新の Cisco Starent MIB ファイルにアクセスする手順について説明します。更新された MIB ファイルは、すべての StarOS リリースに付属しています。アカウントの設定とファイルへのアクセスについて詳しくは、シスコの販売担当者またはサービス担当者にお問い合わせください。

MIBブラウザを使用すると、SNMP対応デバイスからデータを引き出すことができます。標準 MIB と独自 MIB をロードできます。このツールを使用すると、MIB データを読み取り可能な形式で表示したり、特定の OID を検索する機能を提供したりすることができます。ブラウザ

に MIB ツリー内のすべての MIB が表示されます。これにより、すべてのオブジェクト、トラップ、または適合性を簡単に見つけて識別することができます。

特定の StarOS ビルドの SNMP MIB を表示するには、次の手順を実行します。

手順

ステップ 1 特定の StarOS リリースの MIB ファイルへのアクセス権を取得するには、シスコのセールス担当者またはサービス担当者にお問い合わせください。

ステップ 2 圧縮されたコンパニオンファイルをデスクトップ上のフォルダにダウンロードします。ファイル名は、次の規則に従います。**companion**_xx.x.x.**tgz**

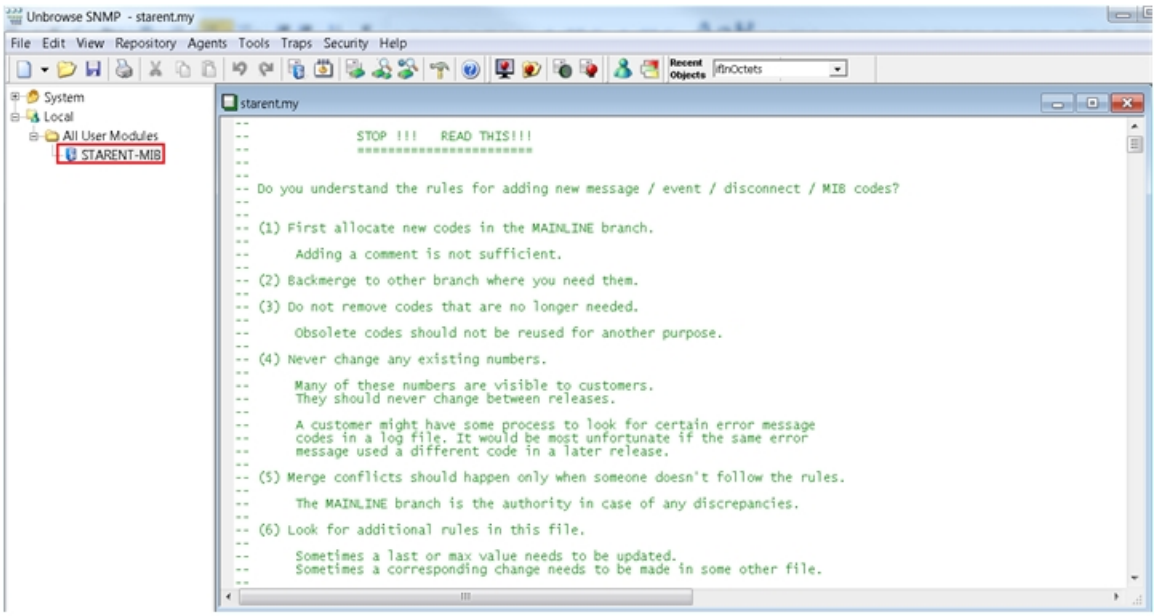
ステップ 3 コンパニオンファイルを開き、解凍して、同じフォルダに展開します。

ステップ 4 **companion-**xx.x.x.xxxxx ファイルフォルダをダブルクリックします。

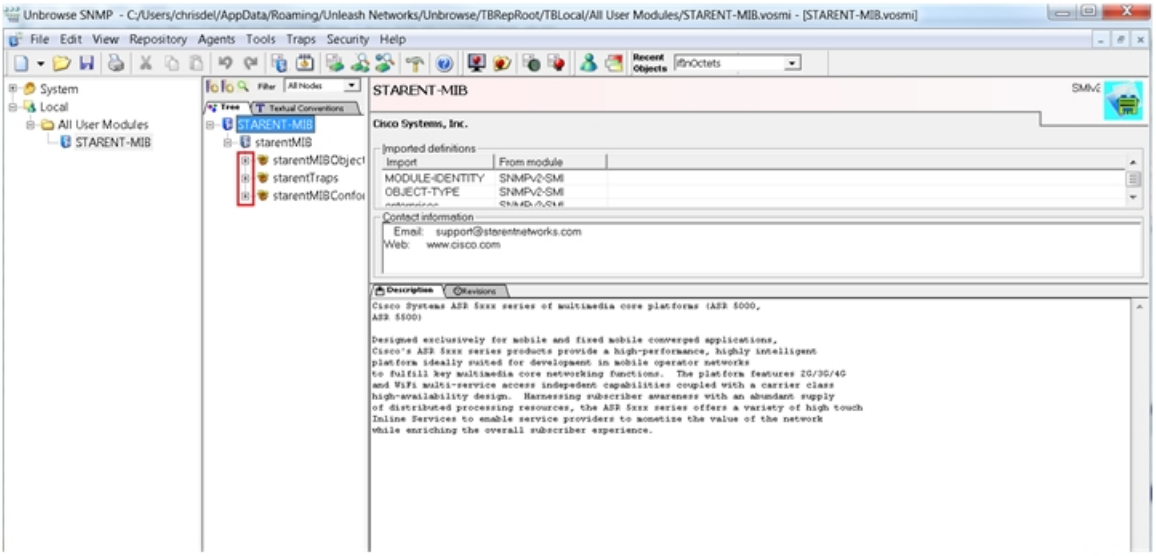
ステップ 5 **companion-**xx.x.x.xxxxx**.tar** を解答して展開します。

ステップ 6 MIB ブラウザで、.tar ファイル内の **starent.my** ファイルを検索して開きます。SNMP MIB ブラウザを使用すると、MIB **.my** ファイルを表示する前にコンパイルできます。

ステップ 7 MIB ファイルをコンパイルするには、STARENT-MIB ファイルをクリックして、[File] > [Open] を選択します。

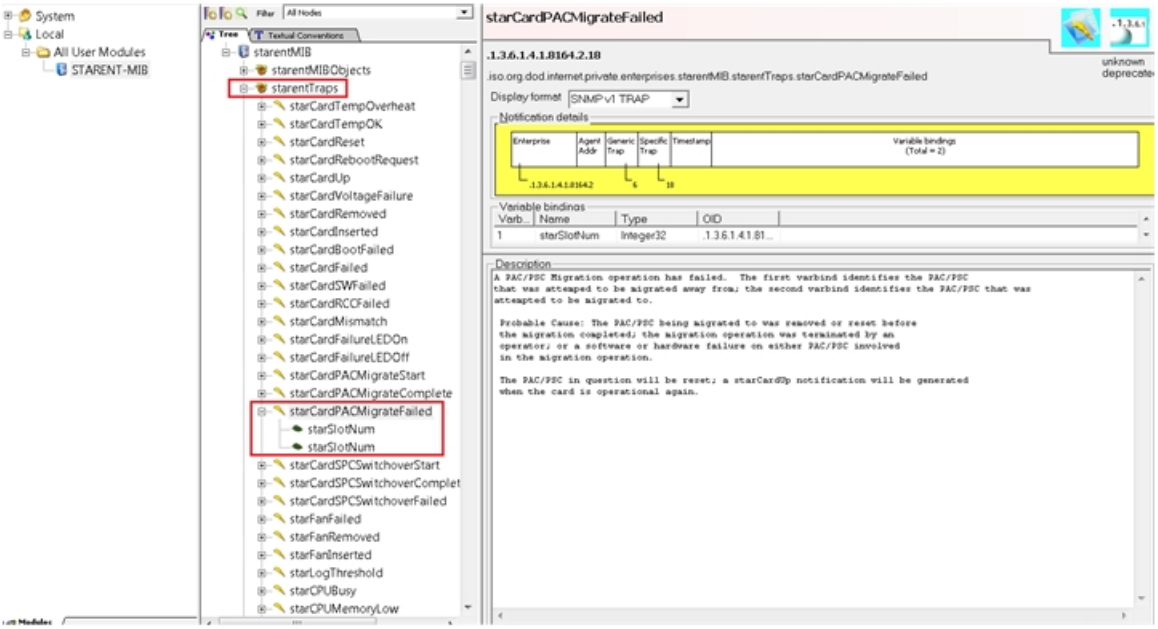


STARENT-MIB.vosmi ファイルが開きます。



335999

次の例で示すMIBブラウザのツリー図には、各オブジェクト、トラップ、および適合性の詳細を表示することができます。この例には、 starCardPACMigrateFailed トラップの OID 番号とトラップの詳細が含まれています。



411591

SNMP MIB ブラウザでは、特定の MIB を検索することができます。特定の OID（オブジェクト識別子）を検索して、特定の MIB エントリを検索できます。

重要

特定のリリースの SNMP MIB の変更については、該当するバージョンの『*Release Change Reference*』の「*SNMP MIB Changes in Release xx*」の章を参照してください。

SNMP サポート

システムは SNMP を使用して、ネットワーク上の EMS サーバーまたはアラームサーバーにトラップまたはイベントを送信します。これらのデバイスと通信するには、SNMP を設定する必要があります。

重要 この項の設定例で使用されているコマンドは、基本機能を提供します。最も一般的なコマンドとキーワードのオプションが示されています。多くの場合、他のオプションコマンドやキーワードオプションを使用できます。詳細については、『*Command Line Interface Reference*』を参照してください。

『*SNMP MIB Reference*』では、StarOS でサポートされている MIB と SNMP のトラップが説明されています。

システムが EMS サーバーまたはアラームサーバーと通信するように設定するには、次の手順を実行します。

手順

ステップ 1 の設定例を適用して、UDP ポートやアラームサーバーターゲットなどの SNMP パラメータを設定します。 SNMP とアラームサーバーパラメータの設定 （6 ページ）

ステップ 2 新しい SNMP 設定を表示するには、次の手順を実行します。 SNMP パラメータの確認 （8 ページ）

ステップ 3 「設定の確認と保存」の説明に従って、設定を保存します。

SNMP とアラームサーバーパラメータの設定

SNMP およびアラームサーバーパラメータを設定するには、次の例を使用します。

```
configure
   system contact contact_name
   system location location_name
   snmp authentication-failure-trap
   snmp community community_string
   snmp server port port_number
   snmp target name ip_address
   snmp engine-id local id_string
```

```
snmp notif-threshold value low low_value period time_period
snmp user user_name
snmp mib mib_name
snmp runtime-debug [ debug-tokens token_id token_id token_id...token_id
end
```

注：

- **システム管理者**は、エラー状態を示すトラップが生成されたときに連絡する担当者の名前です。
- **snmp コミュニティ**文字列は、システムの Management Information Base（MIB）へのアクセスを可能にするパスワードです。
- システムは、SNMPv1 トラップ、SNMPv2c トラップ、または SNMPv3 トラップを多数のターゲットデバイスに送信できます。ただし、EMS は SNMP バージョン 1（SNMPv1）および SNMP バージョン 2c（SNMPv2c）トラップのみを処理できます。設定している SNMP ターゲットが EMS アプリケーションである場合は、**snmp target** コマンドを使用してバージョン 1 またはバージョン 2c の使用を設定します。複数のターゲットを設定するのに必要な回数だけこのコマンドを発行します。複数のターゲットを設定した場合、生成されたアラームは、設定されたすべてのターゲットに送信されます。
- **snmp notif-threshold** コマンドは、通知が SNMP ユーザーに伝達される前に、特定のイベントに対して生成する必要がある SNMP 通知の数（デフォルトは 300）と、モニタリング ウィンドウ サイズの秒数（デフォルトは 300）を設定します。
- **snmp engine-id local** コマンドはオプションです。これは、ネットワークで SNMP v3 サポートが必要な場合にのみ必要です。エンジン ID は、SNMP エンジンと関連する SNMP エンティティを一意に識別するため、2 つの間にセキュリティ アソシエーションを提供し、データの送受信を行います。
- **snmp ユーザー**の名前は SNMP v3 用であり、オプションです。このコマンドには、多数のキーワードオプションが関連付けられています。
- 他の業界標準および Cisco MIB を有効にするには、**snmp mib** コマンドを使用します。デフォルトでは、STARENT-MIB のみが有効になっています。
- デフォルトでは、SNMP ランタイムデバッグは常に実行され、イベントロギングのために CPU サイクルを消費します。CPU 使用率を制御するには、**no snmp runtime-debug** を設定して、ランタイムデバッグを無効にすることができます。このコマンドのオプションを使用すると、指定された MIB を参照して解析する SNMP トークン値を指定できます。

重要 SNMPv3 トラップは、一部の EMS アプリケーションではサポートされていない場合があります。

SNMP パラメータの確認

手順

ステップ 1 SNMP サーバー情報が正しく設定されていることを確認するには、**show snmp server** コマンドを実行します。次に、このコマンドの出力例を示します。

```
SNMP Server Configuration:
    Server State             : enabled
    SNMP Port                : 161
    sysLocation              : chicago
    sysContact               : admin
    authenticationFail traps : Enabled
    EngineID                 : 123456789
    Alert Threshold          : 100 alerts in 300 seconds
    Alert Low Threshold      : 20 alerts in 300 seconds
SNMP Agent Mib Configuration:
                           STARENT-MIB : Enabled
                                IF-MIB : Disabled
                            ENTITY-MIB : Disabled
                      ENTITY-STATE-MIB : Disabled
                    ENTITY-SENSORE-MIB : Disabled
                    HOST-RESOURCES-MIB : Disabled
     CISCO-MOBILE-WIRELESS-SERVICE-MIB : Disabled
              CISCO-ENTITY-DISPLAY-MIB : Disabled
                     CISCO-PROCESS-MIB : Disabled
          CISCO-ENTITY-FRU-CONTROL-MIB : Disabled
```

ステップ 2 次のコマンドを入力して、SNMP コミュニティが正しく設定されていることを確認します。

show snmp communities

このコマンドの出力には、設定されている SNMP コミュニティとそれに対応するアクセスレベルが一覧表示されます。

ステップ 3 次のコマンドを入力して、SNMP トランスポートが正しく設定されていることを確認します。

show snmp transports

次に、出力例を示します。

```
Target Name:   rms1
IP Address:    192.168.1.200
Port:          162
Default:       Default
Security Name: public
Version:       1
Security:
View:
Notif Type:    traps
```

SNMP トラップ生成の制御

システムは、SNMP トラップ（通知）を使用して、特定のイベントが発生したことを示します。デフォルトでは、システムですべてのトラップの生成が可能です。ただし、個々のトラップを無効にして、特定のタイプのトラップやアラームレベルのトラップだけを生成することもできます。この項では、SNMP トラップを無効または有効にする手順について説明します。

重要 この項の設定例で使用されているコマンドは、基本機能を提供します。最も一般的なコマンドとキーワードのオプションが示されています。多くの場合、他のオプションコマンドやキーワードオプションを使用できます。すべてのコマンドの詳細については、『*Command Line Interface Reference*』を参照してください。

SNMP トラップの生成を設定するには、次の手順を実行します。

手順

ステップ 1 次の設定例を適用して、パラメータを設定します。

```
configure
  snmp trap suppress
  snmp trap suppress trap_name1 trap_name2 ... trap_nameN
```

抑制していたトラップを後で再度有効にする場合は、**snmp trap enable** コマンドを使用します。

ステップ 2 「設定の確認と保存」の説明に従って、設定を保存します。

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。