



# XML インターフェイスの設定

この章では、NMS (network management station; ネットワーク管理ステーション) から Extensible Markup Language (XML) を使用して Cisco Application Control Engine (ACE) モジュールを設定する方法について説明します。ACE の CLI から設定できるコマンドはどれでも、HTTP または secure HTTP (HTTPS) で XML ドキュメントを交換することによって、NMS からリモート設定できます。アプリケーション間でデータの送信、交換、および解釈が可能です。さらに、**show** コマンドの出力を XML フォーマットで NMS に転送するように ACE を設定すると、結果を監視したり分析したりできます。ACE の XML インターフェイスを使用するには、管理ユーザルールが必要です。

この章の内容は、次のとおりです。

- [XML の概要](#)
- [XML コンフィギュレーションクイック スタート](#)
- [HTTP および HTTPS 管理トラフィック サービスの設定](#)
- [raw XML 要求の show コマンド出力を XML フォーマットで表示できるようにする場合](#)
- [ACE DTD ファイルへのアクセス](#)



## 注意

ACE は起動時に、2 つのデフォルト ユーザアカウントを作成します。admin および www です。admin ユーザはグローバルな管理者であり、削除できません。ACE では、XML インターフェイスに www ユーザアカウントを使用します。したがって、www ユーザアカウントを削除しないでください。削除すると、XML インターフェイスが動作しなくなります。誤って www アカウントを削除した場

合は、コンフィギュレーション モードで **username www password 5 password domain default-domain role Admin** を入力すると、アカウントが再設定され、XML 動作を回復できます。ユーザの設定については、『*Cisco Application Control Engine Module Virtualization Configuration Guide*』を参照してください。

## XML の概要

ここで説明する内容は、次のとおりです。

- ACE で XML を利用する場合
- ACE での HTTP および HTTPS サポート
- HTTP の戻りコード
- DTD
- XML の設定例

## ACE で XML を利用する場合

Web サービスは、XML を使用しなければ相互運用が困難なアプリケーション間で、XML を使用してデータを送信、交換、および解釈する、ネットワークベースのソフトウェアアプリケーションを提供します。

XML を使用すると、アプリケーションに依存することなく、コンピュータ システム間でデータを共有できます。XML は HTML と同様、タグで区切られたテキストからなるので、インターネットを介して容易に伝送できます。XML では、タグで情報の意味と構造を定義し、コンピュータ アプリケーションが情報をそのまま使用できるようにします。HTML と異なり、XML のタグはデータの表示方法を指定するのではなく、データを識別するためのものです。XML タグはプログラムのフィールド名と同様の機能を果たし、識別するデータの断片にラベルを付けます (例: `<message>...</message>`)。

設定コマンドや出力結果が含まれる XML ドキュメントは、HTTP、secure HTTP (HTTPS) などの標準インターネット プロトコルを転送プロトコルとして使用するため、デバイス間でのトランスフォーメーションが容易です。

XML API (アプリケーションプログラミング インターフェイス) を使用すると、Document Type Definition (DTD) によって、ACE のプログラム設定を自動化できます。XML フォーマットは、CLI コマンドを同等の XML 構文に変換したものです。ACE の CLI コマンドごとに同等の XML タグがあり、CLI コマンドのすべてのパラメータがその要素の属性です。ACE では、Apache HTTP サーバを使用して XML 管理インターフェイスを提供し、さらに ACE と管理クライアント間で HTTP サービスを提供します。ACE XML API を使用するには、管理ユーザルールが必要です。

XML を使用すると、次の作業が可能になります。

- ACE で XML を使用してオブジェクトを転送、設定、監視するメカニズムの実現。この XML 機能により、さまざまなビジネス ニーズに合わせて、XML フォーマットで CLI クエリーおよび応答データを容易に成形または拡張できます。
- ACE の CLI インターフェイスから、統計を表示しステータスを監視するために、**show** コマンド出力を XML フォーマットで転送。この機能により、ACE にデータを照会して抽出できます。
- ACE の XML DTD スキーマを使用して CLI クエリーをフォーマットし、ACE からの XML 結果を解析することにより、XML 通信を介したサードパーティのソフトウェア開発が可能。
- AAA によるリモート ユーザ認証。
- グローバル管理者および管理ユーザ ロールが与えられた特権ユーザによる、セッションおよびコンテキスト管理。

CiscoWorks Hosting Solution Engine (HSE) などの NMS は ACE に接続し、HTTP または HTTPS で新しいコンフィギュレーションをプッシュできます。

## ACE での HTTP および HTTPS サポート

ACE および NMS は、HTTP、HTTPS などの標準インターネット プロトコルを転送プロトコルとして使用することにより、設定コマンドや出力結果が含まれる XML ドキュメントを容易に送受信できます。HTTPS では SSL を使用して、管理クライアントと ACE 間の通信を暗号化します。

システム管理者は API のエントリ ポイントとして Web サイトを指定し、すべての要求および照会がこれらの URL から行われるようにします。この Web サイトは、要求、照会、応答用の XML を定義する DTD も提供します。

XML 入力、HTTP POST 要求のデータ部分を使用して提出されます。「xml」というフィールドに、要求または照会を定義する XML ストリングが含まれます。この HTTP POST に対する応答は、要求または照会に対する応答の成否を示す、純粋な XML 応答です。

XML を使用して設定データや結果を転送する場合、NMS は ACE に接続し、HTTP または HTTPS を使用して、ACE に XML ドキュメントで新しいコンフィギュレーションを送信します。その後、ACE が新しいコンフィギュレーションを適用します。

次に、ACE の XML 実装に関連する、クライアントとサーバ間の HTTP 通信の例を示します。

```
***** Client *****
POST /bin/xml_agent HTTP/1.1
Authorization: Basic VTPQ
Content-Length: 95
xml_cmd=<request_xml>
<interface type="vlan" number="80">
<access-group access-type="input" name="acl1"/>
<ip_address address="60.0.0.145" netmask="255.255.255.0"/>
<shutdown sense="no"/>
</interface>
<show_running-config/>
</request_xml>

***** Server *****
HTTP/1.1 200 OK
Content-Length: 21
<response_xml>
<config_command>
<command>
interface vlan 80
ip address 60.0.0.145 255.255.255.0
access-group input acl1
no shutdown
</command>
<status code="100" text="XML_CMD_SUCCESS"/>
</config_command>
</response_xml>

***** Client *****
POST /bin/xml_agent HTTP/1.1
Content-Length: 95
xml_cmd=<request_xml>
<show_running-config/>
```

```

</request_xml>

***** Server *****
HTTP/1.1 401 Unauthorized
Connection: close
WWW-Authenticate: Basic realm=/xml-config

```

## HTTP の戻りコード

HTTP の戻りコードは、サーバとクライアント間の要求およびレポート エラーのステータスを示します。Apache HTTP サーバの戻りステータス コードは、RFC 2616 で概要が記されている規格に準拠しています。表 8-1 に、サポートされる HTTP の戻りコードを示します。

表 8-1 XML に関してサポートされる HTTP の戻りコード

戻りコード	説明
200	OK
201	作成された
202	受け付けられた
203	非正規情報
206	部分的な内容
301	永久移動
302	検出
400	不正な要求
401	非正規 (クレデンシャルが必要であるが、提出されていない)
403	禁止 (不正なクレデンシャルが提出された、Syslog も生成されている)
404	検出されなかった (「/xml-config」が指定されていない)
405	認められていないメソッド
406	受け付けられない
408	要求がタイムアウト (受信待機が 30 秒を超えた)
411	Content-Length が欠落 (Content-Length フィールドが欠落しているか、またはゼロ)

表 8-1 XML に関してサポートされる HTTP の戻りコード (続き)

戻りコード	説明
500	内部サーバエラー
501	実行されない (「POST」が指定されていない)
505	サポートされない HTTP バージョン (「1.0」または「1.1」が指定されていない)

サポートされる HTTP ヘッダーは、次のとおりです。

- Content-Length (すべての POST にゼロ以外の値が必要)
- Connection (*close* 値は要求を持続させないという指示)
- WWW-Authenticate (クレデンシアルが必要であり、なおかつ欠落している場合にクライアントに送信)
- Authorization (ベース 64 エンコーディングで基本クレデンシアルを指定する場合に、クライアントから送信)

たとえば、XML エラーが発生すると、HTTP 応答に戻りコード 200 が含まれません。エラーが発生した元の XML ドキュメントの一部が、エラー タイプと説明を示すエラー要素とともに戻ります。

次に、一般的な XML エラー応答の例を示します。

```
<response_xml>
<config_command>
<command>
interface vlan 20
  no shut
  description xyz
  exit
</command>
<status code = '200' text='XML_CMD_FAILURE'>
<error_command> description xyz </error_command>
<error_message> unrecognized element - description </error_message>
</status>
</config_command>
</response_xml>
```

戻ったエラー コードは、コンフィギュレーション要素のアトリビュートに対応しています。戻る可能性のある XML エラーには、次のものが含まれています。

```
XML_ERR_WELLFORMEDNESS /* not a well formed xml document */
XML_ERR_ATTR_INVALID /* found invalid value attribute */
XML_ERR_ELEM_INVALID /* found invalid value unrecognized */
XML_ERR_CDL_NOT_FOUN /* parser cdl file not found */
XML_ERR_INTERNAL /* internal memory or coding error */
XML_ERR_COMM_FAILURE /* communication failure */
XML_ERR_VSH_PARSER /* vsh parse error on the given command */
XML_ERR_VSH_CONF_APPLY /* vsh unable to apply the configuration */
```

## DTD

DTD は、ACE を使用して作成する XML コンフィギュレーション ドキュメントの土台です。DTD の目的は、有効な要素のリストでドキュメント構造を定義することによって、XML ドキュメントの有効な構成要素を定義することです。

DTD では要求、照会、または応答ドキュメントに含めることのできる要素を厳密に規定する、XML リストを指定します。さらに、要素の内容およびアトリビュートを指定します。DTD は、XML ドキュメントでインライン宣言することも、外部参照として宣言することもできます。

ACE の DTD ファイルである `cisco_ace.dtd` は、ソフトウェア イメージの一部として組み込まれており、HTTP または HTTPS で Web ブラウザからアクセスできます。詳細については、「[ACE DTD ファイルへのアクセス](#)」を参照してください。Web ブラウザを使用して、`cisco_ace.dtd` ファイルに直接アクセスすることも、Cisco ACE Module Management ページから `cisco_ace.dtd` ファイルを開くこともできます。

次に、実サーバを作成する ACE CLI コマンドシーケンスとその後ろに続く、コマンドに対応する DTD XML `rserver` 要素の例を示します。

```
[no] rserver [host | redirect] name
      [no] conn-limit max maxconns [min minconns]
      [no] description string
      [no] inservice
      [no] ip address {ip_address}
      [no] probe name
```

**[no] weight number**

```

*****
Elements, Attributes and Entities required for rserver
*****
-->

<!--
probe-name is a string of length 1 to 32.
-->
<!ELEMENT probe_rserver EMPTY>
<!ATTLIST probe_rserver
  sense      CDATA      #FIXED      "no"
  probe-name CDATA      #REQUIRED
>

<!--
relocation-str length is 1 to 127
-->
<!ELEMENT webhost-redirection EMPTY>
<!ATTLIST webhost-redirection
  sense      (yes | no)      #IMPLIED
  relocation-string CDATA      #REQUIRED
  redirection-code (301 | 302)      #IMPLIED
>

<!--
type is optional for host.
ip, probe and weight are valid only when type = host.
address-type is valid only when type=host.
name length is 1 to 32.
webhost-redirection is valid only if type=redirect.
-->
<!ELEMENT rserver (description, ip_address, conn-limit, probe_rserver,
                  weight, inservice,
webhost-redirection)*>
<!ATTLIST rserver
  sense      CDATA      #FIXED      "no"
  type      (redirect | host)      #IMPLIED
  name      CDATA      #REQUIRED
>

```



## XML の設定例

次に、一般的な VShell (VSH) CLI コマンドの設定例および同等の XML 設定コマンドを示します。

```
#####
## TO/FROM CP CONFIGURATION ##
#####
conf t
access-list acl1 extended permit ip any any
int vlan 80
access-group input acl1
ip address 60.0.0.145 255.255.255.0
no shut
exit
ip route 0.0.0.0 0.0.0.0 60.0.0.1
end

<access-list id="acl1" config-type="extended" perm-value="permit"
protocol-name="ip" src-type="any" dest-type="any"/>
<interface type="vlan" number="80">
<access-group type="input" name="acl1"/>
<ip_address address="60.0.0.145" netmask="255.255.255.0"/>
<shutdown sense="no"/>
</interface>

<ip_route dest-address="0.0.0.0" dest-mask="0.0.0.0"
gateway="60.0.0.1"/>
#####
## BRIDGING CONFIGURATION ##
#####
conf t

access-list acl1 extended permit ip any any
int vlan 80
access-group input acl1
bridge-group 1
no shut
exit

int vlan 90
access-group input acl1
bridge-group 1
no shut
exit
end
```

```
<access-list id="acl1" config-type="extended" perm-value="permit"  
protocol-name="ip" src-type="any" dest-type="any"/>  
<interface type="vlan" number="80">  
<access-group type="input" name="acl1"/>  
<bridge-group value="1"/>  
<shutdown sense="no"/>  
</interface>  
<interface type="vlan" number="90">  
<access-group type="input" name="acl1"/>  
<bridge-group value="1"/>  
<shutdown sense="no"/>  
</interface>
```

## XML コンフィギュレーションクイック スタート

表 8-2 に、ACE 上で XML の使用を設定するために必要な手順の概要を示します。各手順には、作業に必要な CLI コマンドが含まれています。

表 8-2 ACE XML コンフィギュレーションクイック スタート

---

### 作業およびコマンド例

---

1. 複数のコンテキストで動作する場合は、CLI プロンプトを観察して、適切なコンテキストで動作しているかどうかを確認してください。必要に応じて、適切なコンテキストの直接ログインするか、または切り替えてください。

```
host1/Admin# changeto C1
host1/C1#
```

これ以降、この表の例では、特に指定しないかぎり管理コンテキストを使用します。コンテキスト作成の詳細については、『*Cisco Application Control Engine Module Virtualization Configuration Guide*』を参照してください。

2. コンフィギュレーション モードを開始します。

```
host1/Admin# config
Enter configuration commands, one per line. End with CNTL/Z.
host1/Admin(config)#
```

3. レイヤ 3 およびレイヤ 4 クラス マップを作成し、ACE に受信させる HTTP または HTTPS 管理トラフィックを分類します。

```
host1/Admin(config)# class-map type management match-all
HTTPS-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# match protocol https
source-address 192.168.1.1 255.255.255.255
host1/Admin(config-cmap-mgmt)# exit
```

4. レイヤ 3 およびレイヤ 4 HTTP または HTTPS トラフィック管理ポリシーを設定します。

```
host1/Admin(config) # policy-map type management first-match
MGMT_HTTPS_POLICY
host1/Admin(config-pmap-mgmt) # class HTTPS-ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c) # permit
host1/Admin(config-pmap-mgmt-c) # exit
```

---

表 8-2 ACE XML コンフィギュレーション クイック スタート (続き)

---

**作業およびコマンド例**

---

5. 特定のインターフェイスにトラフィック ポリシーを接続するか、またはコンテキストに関連付けられたすべての VLAN インターフェイスにグローバルに接続し、ポリシーを適用する方向を指定します。たとえば、インターフェイス VLAN を指定して、その VLAN に複数のサービス ポリシーを適用する場合は、次のように入力します。

```
host1/Admin(config)# interface vlan50
host1/Admin(config-if)# ip address 192.168.10.1 255.255.0.0
host1/Admin(config-if)# service-policy input MGMT_HTTPS_POLICY
host1/Admin(config-if)# exit
host1/Admin(config)# exit
```

---

6. (任意) raw XML 要求の **show** コマンド出力を XML フォーマットで表示できるようにします。



(注) 真の XML 応答は常に自動的に、XML フォーマットで表示されます。

---

```
host1/Admin# xml-show on
```

---

7. (任意) フラッシュ メモリに設定変更を保存します。

```
host1/Admin# copy running-config startup-config
```

---

## HTTP および HTTPS 管理トラフィック サービスの設定

ACE は、HTTP または HTTPS で XML を使用し、ソフトウェア オブジェクトを設定、監視、管理するリモート管理をサポートします。クラス マップ、ポリシー マップ、およびサービス ポリシーを使用して、ACE への HTTP および HTTPS リモート管理トラフィックを設定します。

ACE への HTTP または HTTPS ネットワーク管理アクセスを設定するうえで、各機能が果たす役割を簡単に説明します。

- クラス マップ — HTTP または HTTPS ネットワーク管理プロトコルまたはホスト送信元 IP アドレスに基づいて、HTTP および HTTPS 管理トラフィックを許可する、リモート ネットワーク トラフィック一致条件を指定します。
- ポリシー マップ — クラス マップで指定された条件と一致するトラフィック分類に対して、リモート ネットワーク管理アクセスを可能にします。
- サービス ポリシー — ポリシー マップをアクティブにして、インターフェイスにトラフィック ポリシーを接続するか、またはすべてのインターフェイス上でグローバルに接続します。

ACE との HTTP または HTTPS セッションは、コンテキストに基づいて確立されます。コンテキストおよびユーザ作成の詳細については、『*Cisco Application Control Engine Module Virtualization Configuration Guide*』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。

- [クラス マップの作成および設定](#)
- [レイヤ 3 およびレイヤ 4 ポリシー マップの作成](#)
- [サービス ポリシーの適用](#)

## クラス マップの作成および設定

ACE で受信できる HTTP または HTTPS 管理トラフィックを分類するために、レイヤ 3 およびレイヤ 4 クラス マップを作成するには、コンフィギュレーション コマンド **class-map type management** を使用します。このコマンドで ACE が受信できる着信 IP プロトコル、さらにクライアント送信元ホストの IP アドレスおよびサブネット マスクを一致条件として指定することによって、ネットワーク管理トラフィックを許可できます。**type management** というクラス マップでは、HTTP、HTTPS などのプロトコル管理セキュリティの形で、許可するネットワーク トラフィックを定義します。

クラス マップには複数の **match** コマンドを指定できます。クラス マップを設定すると、複数の HTTP/HTTPS 管理プロトコルまたは送信元 IP アドレスの **match** コマンドをグループとして定義し、さらにトラフィック ポリシーと関連付けることができます。**match-all** および **match-any** キーワードによって、クラス マップに複数の一致条件が存在する場合に、ACE が複数の **match** 文演算をどのように評価するかが決まります。

このコマンドの構文は、次のとおりです。

**class-map type management [match-all | match-any] map\_name**

キーワード、引数、およびオプションは次のとおりです。

- **match-all | match-any** — (任意) クラス マップに複数の一致条件が存在する場合に、ACE がレイヤ 3 およびレイヤ 4 ネットワーク トラフィックをどのように評価するかを決定します。クラス マップは、**match** コマンドが次の条件の 1 つを満たした場合に、一致とみなされます。
  - **match-all** — (デフォルト) クラス マップで指定されているすべての一致条件がクラス マップのネットワーク トラフィック クラスと一致した場合。
  - **match-any** — クラス マップで指定されている一致条件のうちの 1 つだけがクラス マップのネットワーク トラフィック クラスと一致した場合。
- **map\_name** — クラス マップに割り当てる名前。最大 64 文字の英数字からなる文字列を引用符で囲まずに入力します。スペースは使用しません。クラス名は、クラス マップに使用するとともに、ポリシー マップのクラスにポリシーを設定する場合にも使用します。

**class-map type management** コマンドを使用するときには、クラス マップ管理コンフィギュレーション モードにアクセスします。このモードを使用すると、クラス マップの説明または一致条件を設定できます。

クラス マップには複数の **match protocol** コマンドを指定できます。

たとえば、ACE HTTP サーバと IP アドレス 192.168.1.1 255.255.255.255 の管理クライアント間で HTTPS アクセスを許可する場合は、次のように入力します。

```
host1/Admin(config)# class-map type management match-all
HTTPS-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# match protocol https source-address
192.168.1.1 255.255.255.255
```

ACE からレイヤ 3 およびレイヤ 4 ネットワーク管理クラス マップを削除する場合は、次のように入力します。

```
host1/Admin(config)# no class-map type management match-all  
HTTPS-ALLOW_CLASS
```

ACE に受信させるリモート HTTP または HTTPS 管理トラフィックを分類するには、次のコマンドのうちの 1 つまたは複数指定して、クラス マップの一致条件を設定します。

- **description** — 「[クラス マップの説明の定義](#)」を参照
- **match protocol** — 「[HTTP および HTTPS プロトコル一致条件の定義](#)」を参照

## クラス マップの説明の定義

レイヤ 3 およびレイヤ 4 リモート管理クラス マップの概要を指定するには、クラス マップ管理コンフィギュレーションモードで **description** コマンドを使用します。

このコマンドの構文は、次のとおりです。

**description** *text*

*text* 引数は、指定する説明です。最大 240 文字の英数字からなる文字列を引用符で囲まずに入力します。

たとえば、HTTPS アクセスを許可するクラス マップであるという説明を指定する場合は、次のように入力します。

```
host1/Admin(config)# class-map type management match-all  
HTTPS-ALLOW_CLASS  
host1/Admin(config-cmap-mgmt)# description Allow HTTPS access to the  
ACE
```

クラス マップから説明を削除する場合は、次のように入力します。

```
host1/Admin(config-cmap-mgmt)# no description
```

## HTTP および HTTPS プロトコル一致条件の定義

クラス マップを設定して、ACE が HTTP または HTTPS リモート ネットワーク 管理プロトコルを受信できることを指定するには、クラス マップ管理コンフィギュレーション モードで **match protocol** コマンドを使用します。さらに対応するポリシー マップを設定して、指定された管理プロトコルに ACE へのアクセスを許可します。XML をサポートするには、**type management** というクラス マップで HTTP、HTTPS などの IP プロトコルを許可します。ネットワーク管理アクセス トラフィック分類の一部として、クライアント送信元ホストの IP アドレス およびサブネット マスクも一致条件として指定するか、またはあらゆるクライアント送信元アドレスを管理トラフィック分類で許可するように ACE に指示します。

このコマンドの構文は、次のとおりです。

```
[line_number] match protocol {http | https} {any | source-address ip_address  
mask}
```

キーワード、引数、およびオプションは次のとおりです。

- *line\_number* — (任意) 個々の **match** コマンドを編集または削除できるようにするための行番号。行番号として 2 ~ 255 の整数を入力します。たとえば、**no line\_number** を入力すると、行全体を入力しなくても、長い **match** コマンドを削除できます。
- **http** — ACE HTTP サーバと管理クライアント間の HTTP を介した管理アクセスを設定します。
- **https** — ACE HTTP サーバと管理クライアント間の secure HTTP を介した管理アクセスを設定します。
- **any** — 管理トラフィック分類にあらゆるクライアント送信元アドレスを指定します。
- **source-address** — ネットワーク トラフィック一致条件として、クライアント送信元ホストの IP アドレスおよびサブネット マスクを指定します。分類の一部として、ACE は暗黙で、ポリシー マップが適用されるインターフェイスから宛先 IP アドレスを取得します。
- *ip\_address* — クライアントの送信元 IP アドレス。IP アドレスはドット付き 10 進表記 (192.168.11.1 など) で入力します。
- *mask* — ドット付き 10 進表記 (255.255.255.0 など) で指定したクライアントのサブネット マスク。



たとえば、クラス マップで ACE への HTTPS アクセスを許可することを指定する場合は、次のように入力します。

```
(config)# class-map type management HTTPS-ALLOW_CLASS
(config-cmap-mgmt)# match protocol https source-address 192.168.10.1
255.255.0.0
```

クラス マップから特定のネットワーク管理プロトコル一致条件を選択解除する場合は、次のように入力します。

```
host1/Admin(config-cmap-mgmt)# no match protocol https source-address
192.168.10.1 255.255.0.0
```

## レイヤ 3 およびレイヤ 4 ポリシー マップの作成

レイヤ 3 およびレイヤ 4 ポリシー マップでは、指定された分類と一致した HTTP または HTTPS 管理トラフィックに対して実行するアクションを定義します。ここで説明する内容は、次のとおりです。

- ACE で受信する SNMP ネットワーク管理トラフィック用レイヤ 3 およびレイヤ 4 ポリシー マップの作成
- トラフィック ポリシーでのレイヤ 3 およびレイヤ 4 トラフィック クラスの指定
- レイヤ 3 およびレイヤ 4 ポリシー アクションの指定

## ACE で受信する SNMP ネットワーク管理トラフィック用レイヤ 3 およびレイヤ 4 ポリシー マップの作成

管理トラフィックの受信を ACE に許可するレイヤ 3 およびレイヤ 4 ポリシー マップを設定するには、コンフィギュレーション モードで **policy-map type management** コマンドを使用します。ACE は、最初に一致した分類に対してアクションを実行します。ACE は、それ以上のアクションは実行しません。

このコマンドの構文は、次のとおりです。

```
policy-map type management first-match map_name
```

*map\_name* 引数では、レイヤ 3 およびレイヤ 4 ネットワーク管理ポリシー マップに割り当てる名前を指定します。最大 64 文字の英数字からなる文字列を引用符で囲まらずに入力します。スペースは使用しません。

このコマンドを使用するときには、ポリシー マップ管理コンフィギュレーション モードにアクセスします。

レイヤ 3 およびレイヤ 4 ネットワーク トラフィック管理ポリシー マップを作成する場合の入力例を示します。

```
host1/Admin(config)# policy-map type management first-match
MGMT_HTTPS_POLICY
host1/Admin(config-pmap-mgmt)#
```

ACE からポリシー マップを削除する場合は、次のように入力します。

```
host1/Admin(config)# no policy-map type management first-match
MGMT_HTTPS_POLICY
```

## トラフィック ポリシーでのレイヤ 3 およびレイヤ 4 トラフィック クラスの指定

**class-map** コマンドで HTTP または HTTPS トラフィック管理トラフィック クラスを作成し、トラフィックとトラフィック ポリシーを関連付けることを指定するには、**class** コマンドを使用します。このコマンドによって、ポリシー マップ管理クラス コンフィギュレーションモードが開始されます。

このコマンドの構文は、次のとおりです。

```
class {name1 [insert-before name2] | class-default}
```

引数、キーワードおよびオプションは、次のとおりです。

- **name1** — **class-map** コマンドで設定された、トラフィックとトラフィック ポリシーを関連付ける、定義済みのレイヤ 3 およびレイヤ 4 トラフィック クラスの名前。最大 64 文字の英数字からなる文字列を引用符で囲まずに入力します。スペースは使用しません。
- **insert-before name2** — (任意) ポリシー マップ コンフィギュレーションの *name2* 引数で指定された、既存のクラス マップまたはインライン一致条件の前に、現在のクラス マップを配置します。ACE では、コンフィギュレーションの一部として順序の並べ替えを保存しません。最大 64 文字の英数字からなる文字列を引用符で囲まずに入力します。スペースは使用しません。
- **class-default** — レイヤ 3 およびレイヤ 4 トラフィック ポリシー用に、**class-default** クラス マップを指定します。これは、ACE が作成する予約済みのクラス マップです。このクラスを削除したり変更したりすることはでき

ません。指定されたクラス マップの他の一致条件と一致しなかったすべてのネットワーク トラフィックは、デフォルトのトラフィック クラスに割り当てられます。指定された分類がいずれも一致しなかった場合、ACE は **class class-default** コマンドで指定されたアクションと一致させます。class-default クラス マップには、暗黙の **match any** 文があり、これを使用してあらゆるトラフィック分類を一致させます。

たとえば、レイヤ 3 およびレイヤ 4 リモート アクセス ポリシー マップ内で既存のクラス マップを指定する場合は、次のように入力します。

```
host1/Admin(config-pmap-mgmt)# class HTTPS-ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)#
```

**insert-before** コマンドを使用して、ポリシー マップ内での 2 つのクラス マップの順序を定義する場合は、次のように入力します。

```
host1/Admin(config-pmap-mgmt)# class HTTPS-ALLOW_CLASS insert-before
L4_REMOTE_ACCESS_CLASS
```

レイヤ 3 およびレイヤ 4 トラフィック ポリシーに class-default クラス マップを指定する場合は、次のように入力します。

```
host1/Admin(config-pmap-mgmt)# class class-default
host1/Admin(config-pmap-mgmt-c)#
```

レイヤ 3 およびレイヤ 4 ポリシー マップからクラス マップを削除する場合は、次のように入力します。

```
host1/Admin(config-pmap-mgmt)# no class HTTPS-ALLOW_CLASS
```

## レイヤ 3 およびレイヤ 4 ポリシー アクションの指定

レイヤ 3 およびレイヤ 4 クラス マップで指定されているネットワーク管理トラフィックを ACE が受信または拒否できるようにするには、次のように、ポリシー マップ クラス コンフィギュレーション モードで **permit** または **deny** コマンドのどちらかを指定します。

- クラス マップで指定されている HTTP または HTTPS 管理トラフィックを ACE に受信させる場合は、ポリシー マップ クラス コンフィギュレーション モードで **permit** コマンドを使用します。

## ■ HTTP および HTTPS 管理トラフィック サービスの設定

- クラス マップで指定されている HTTP または HTTPS 管理トラフィックを ACE に受信させない場合は、ポリシー マップ クラス コンフィギュレーション モードで **deny** コマンドを使用します。

レイヤ 3 およびレイヤ 4 ポリシー マップに許可アクションを指定する場合の入力例を示します。

```
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
```

## サービス ポリシーの適用

**service-policy** コマンドは、次の目的で使用します。

- 作成済みのポリシー マップを適用します。
- 特定の VLAN インターフェイスにトラフィック ポリシーを接続するか、または同じコンテキスト内のすべての VLAN インターフェイスにグローバルに接続します。
- インターフェイスの入力方向にトラフィック ポリシーを接続することを指定します。

**service-policy** コマンドは、VLAN インターフェイス コンフィギュレーション モードとコンフィギュレーション モードの両方で使用できます。インターフェイス コンフィギュレーション モードでポリシー マップを指定すると、特定の VLAN インターフェイスにポリシー マップが適用されます。コンフィギュレーション モードでポリシー マップを指定すると、コンテキストに関連付けられているすべての VLAN インターフェイスにポリシーが適用されます。

このコマンドの構文は、次のとおりです。

```
service-policy input policy_name
```

キーワードおよびオプションは次のとおりです。

- **input** — インターフェイスの入力方向にトラフィック ポリシーを接続することを指定します。トラフィック ポリシーによって、そのインターフェイスで受信されたすべてのトラフィックが評価されます。
- *policy\_name* — 作成済みの **policy-map** コマンドで設定された、定義済みポリシー マップの名前。名前は最大 40 文字の英数字です。

たとえば、インターフェイス VLAN を指定して、その VLAN に HTTPS トラフィック管理ポリシー マップを適用する場合は、次のように入力します。

```
host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# ip address 192.168.10.1 255.255.0.0
host1/Admin(config-if)# service-policy input MGMT_HTTPS_POLICY
```

たとえば、コンテキストに関連付けられたすべての VLAN に、HTTPS トラフィック管理ポリシーをグローバルに適用する場合は、次のように入力します。

```
host1/Admin(config)# service-policy input MGMT_HTTPS_POLICY
```

インターフェイスから HTTPS トラフィック管理ポリシーを切り離す場合は、次のように入力します。

```
host1/Admin(config-if)# service-policy input MGMT_HTTPS_POLICY
```

インターフェイスから HTTPS トラフィック管理ポリシーを切り離す場合は、次のように入力します。

```
host1/Admin(config-if)# no service-policy input MGMT_HTTPS_POLICY
```

コンテキストに対応付けられたすべての VLAN から HTTPS トラフィック管理ポリシーをグローバルに切り離す場合は、次のように入力します。

```
host1/Admin(config)# no service-policy input MGMT_HTTPS_POLICY
```

最後にサービス ポリシーを適用した VLAN インターフェイスから個別に、または同じコンテキストのすべての VLAN インターフェイスからグローバルにトラフィック ポリシーを切り離すと、ACE が関連するサービス ポリシー統計を自動的にリセットします。ACE はこのアクションによって、次回、特定の VLAN インターフェイスに、または同じコンテキストのすべての VLAN インターフェイスにグローバルに、トラフィック ポリシーを接続したときの、サービス ポリシー統計の新しいスターティング ポイントを用意します。

サービス ポリシーを作成する場合は、次の注意事項に従ってください。

- コンテキストでグローバルに適用されるポリシー マップは、コンテキスト内に存在するすべてのインターフェイスに内部的に適用されます。

## ■ HTTP および HTTPS 管理トラフィック サービスの設定

- インターフェイス上でアクティブになったポリシーは、重複する分類およびアクションに関して、指定されているあらゆるグローバル ポリシーを上書きします。
- ACE では、1 つのインターフェイス上でアクティブにできるのは、特定機能タイプの 1 つのポリシーだけです。

レイヤ 3 およびレイヤ 4 HTTP または HTTPS トラフィック管理ポリシー マップのサービス ポリシー統計情報を表示するには、EXEC モードで **show service-policy** コマンドを使用します。

このコマンドの構文は、次のとおりです。

```
show service-policy policy_name [detail]
```

キーワード、オプション、および引数は次のとおりです。

- *policy\_name* — 現在使用中の（インターフェイスに適用されている）既存ポリシー マップの ID。最大 64 文字の英数字からなる、引用符で囲まれていない文字列です。
- **detail** — （任意）より詳細なポリシー マップ統計およびステータス情報を表示します。



(注)

ACE は、該当する接続の終了後、**show service-policy** コマンドによって表示されるカウンタをアップデートします。

たとえば、MGMT\_HTTPS\_POLICY ポリシー マップのサービス ポリシー統計情報を表示する場合は、次のように入力します。

```
host1/Admin# show service-policy MGMT_HTTPS_POLICY
Status      : ACTIVE
Description: Allow mgmt protocols
-----
Context Global Policy:
  service-policy: MGMT_HTTPS_POLICY
```

サービス ポリシー統計情報を消去するには、**clear service-policy** コマンドを使用します。このコマンドの構文は、次のとおりです。

```
clear service-policy policy_name
```

*policy\_name* 引数には、現在使用中の（インターフェイスに適用されている）既存ポリシー マップの ID を入力します。最大 64 文字の英数字からなる、引用符で囲まれていない文字列です。

たとえば、現在使用中であるポリシー マップ MGMT\_HTTPS\_POLICY の統計情報を消去する場合は、次のように入力します。

```
host1/Admin# clear service-policy MGMT_HTTPS_POLICY
```

## raw XML 要求の show コマンド出力を XML フォーマットで表示できるようにする場合

デフォルトでは、対応する CLI **show** コマンド出力が XML フォーマットをサポートする場合、XML 応答は自動的に XML フォーマットで表示されます。しかし、CLI コンソールでコマンドを実行している場合、または NMS から raw XML 応答を実行している場合、XML 応答は標準の CLI 表示形式で表示されます。

次のいずれかのアクションを実行すると、raw XML 要求の **show** コマンド出力を XML フォーマットで表示できるようになります。

- CLI から EXEC モードで **xml-show on** コマンドを指定する。
- raw XML 要求そのものに **xml-show on** コマンドを含める (XML ラッパーに含まれた CLI コマンド)。

真の XML (後ろの例を参照) を実行している場合は、**xml-show on** コマンドを選択する必要はありません。

XML フォーマットでサポートされる **show** コマンド出力の詳細については、ソフトウェアイメージに組み込まれている ACE の DTD ファイル `cisco_ace.dtd` を参照してください ([「ACE DTD ファイルへのアクセス」](#)を参照)。ACE の DTD ファイルには、出力が XML フォーマットをサポートする **show** コマンドの XML アトリビュートに関する情報があります。

たとえば、**show interface vlan 10** コマンドを指定する場合、**show interface** コマンドの DTD は次のようになります。

```
<!--
interface-number is req for show-type vlan | bvi.
interface-number is between 1 and 4095 for vlan and 8191 for bvi.
-->
<!ENTITY % show-interface
    "interface-type      (vlan | bvi | eobc)      #IMPLIED
     interface-number    CDATA                  #IMPLIED"
>
```

XML での **show interface** コマンドは、次のとおりです。

```
<show_interface interface-type='vlan' interface-number='10'/>
```



次に、XML での **show interface** コマンド出力例を示します。

```
<response_xml>
<exec_command>
<command>
show interface vlan 10
</command>
<status code="100" text="XML_CMD_SUCCESS"/>
<xml_show_result>
<xml_show_interface>
<xml_interface_entry>
<xml_interface>
<interface_name>vlan10</interface_name>
<interface_status>up</interface_status>
<interface_hardware>VLAN</interface_hardware>
<interface_mac>
<macaddress>00:05:9a:3b:92:b1</macaddress>
</interface_mac>
<interface_mode>routed</interface_mode>
<interface_ip>
<ipaddress>10.20.105.101</ipaddress>
<ipmask>255.255.255.0</ipmask>
</interface_ip>
<interface_ft_status>non-redundant</interface_ft_status>
<interface_description>
<interface_description>not set</interface_description>
</interface_description>
<interface_mtu>1500</interface_mtu>
<interface_last_cleared>never</interface_last_cleared>
<interface_alias>
<ipaddress>not set</ipaddress>
</interface_alias>
<interface_standby>
<ipaddress>not set</ipaddress>
</interface_standby>
<interface_sup_enabled>Assigned</interface_sup_enabled>
<interface_auto_status>up</interface_auto_status>
</xml_interface>
<interface_stats>
<ifs_input>
<ifs_unicast>50</ifs_unicast>
<ifs_bytes>8963</ifs_bytes>
<ifs_multicast>26</ifs_multicast>
<ifs_broadcast>1</ifs_broadcast>
<ifs_errors>0</ifs_errors>
<ifs_unknown>0</ifs_unknown>
<ifs_ignored>0</ifs_ignored>
<ifs_unicast_rpf>0</ifs_unicast_rpf>
```

## ■ raw XML 要求の show コマンド出力を XML フォーマットで表示できるようにする場合

```

</ifs_input>
<ifs_output>
<ifs_unicast>45</ifs_unicast>
<ifs_bytes>5723</ifs_bytes>
<ifs_multicast>0</ifs_multicast>
<ifs_broadcast>1</ifs_broadcast>
<ifs_errors>0</ifs_errors>
<ifs_ignored>0</ifs_ignored>
</ifs_output>
</interface_stats>
</xml_interface_entry>
</xml_show_interface>
</xml_show_result>
</exec_command>
</response_xml>

```

このコマンドの構文は、次のとおりです。

**xml-show {off | on | status}**

キーワードは次のとおりです。

- **off** — XML フォーマットではなく、標準の CLI 表示出力として、CLI **show** コマンド出力を表示します。
- **on** — XML フォーマットで出力を表示する特定の **show** コマンドが実装されていない場合を除き、XML フォーマットで CLI **show** コマンド出力を表示します。XML フォーマットでサポートされる **show** コマンド出力の詳細については、ソフトウェア イメージに組み込まれている ACE の DTD ファイル `cisco_ace.dtd` を参照してください（「[ACE DTD ファイルへのアクセス](#)」を参照）。
- **status** — **xml show** コマンド ステータスの結果を表示します。on または off です。**status** キーワードを使用すると、**xml show** コマンドの設定状態を判別できます。

たとえば、CLI から XML フォーマットで raw XML 要求の **show** コマンド出力を表示できるようにするには、次のように入力します。

```
host1/Admin# xml-show on
```

CLI **show** コマンド出力の表示を標準の CLI 出力に戻す場合は、次のように入力します。

```
host1/Admin# xml-show off
```

## ACE DTD ファイルへのアクセス

ACE の DTD ファイル `cisco_ace.dtd` は、ソフトウェア イメージの一部として組み込まれていて、HTTP または HTTPS で Web ブラウザからアクセスできます。`cisco_ace.dtd` ファイルにアクセスするには、Web ブラウザを使用して次のいずれかの作業を実行します。

- `cisoc_ace.dtd` ファイルに直接アクセスする。
- Cisco ACE Module Management ページから `cisco_ace.dtd` ファイルを開く。

Cisco ACE DTD 3.0 ファイルにアクセスして表示する場合、手順は次のとおりです。

**ステップ 1** まだの場合は、レイヤ 3 およびレイヤ 4 クラス マップおよびポリシー マップを作成し、ACE に受信させる HTTP または HTTPS 管理トラフィックを分類します。[「HTTP および HTTPS 管理トラフィック サービスの設定」](#) を参照してください。

**ステップ 2** Microsoft Internet Explorer、Netscape Navigator など、適切なインターネット Web ブラウザを開きます。

**ステップ 3** `cisco_ace.dtd` ファイルに直接アクセスする場合は、アドレス フィールドに ACE の HTTP または HTTPS アドレスを指定し、続けて `cisco_ace.dtd` を指定します。入力例を示します。

```
https://ace_ip_address/cisco_ace.dtd
```

```
http://ace_ip_address/cisco_ace.dtd
```

`cisco_ace.dtd` ファイルを開くか、それともコンピュータに保存するかを選択できます。

**ステップ 4** 次の手順で、Cisco ACE Module Management ページから `cisco_ace.dtd` ファイルにアクセスします。

- a. アドレス フィールドに ACE の HTTP または HTTPS アドレスを指定します。

```
https://ace_ip_address
```

```
http://ace_ip_address
```

- b. プロンプトに対して **Yes** をクリックし、シスコの署名入り証明書を受諾（信頼）してインストールします。署名入り証明書をインストールには、次のいずれかを実行します。
    - － Microsoft Internet Explorer を使用している場合は、Security Alert ダイアログボックスで **View Certificate** をクリックし、**Install Certificate** オプションを選択して、Certificate Manager Import ウィザードのプロンプトに従います。
    - － Netscape Navigator を使用している場合は、New Site Certificate ダイアログボックスで **Next** をクリックし、New Site Certificate ウィザードのプロンプトに従います。
  - c. 表示されたフィールドにユーザ名とパスワードを入力し、**OK** をクリックします。Cisco ACE Module Management ページが表示されます。
  - d. Cisco ACE Module Management ページの Resources カラムで CISCO ACE DTD 3.0 のリンクをクリックし、cisco\_ace.dtd ファイルにアクセスします。cisco\_ace.dtd ファイルを開くか、それともコンピュータに保存するかを選択できます。
-