



システム メッセージ ログिंगの設定

この章では、Cisco Application Control Engine (ACE) モジュールでシステム メッセージ ログングを設定する方法を説明します。それぞれの ACE には、指定された ACE 関連のアクティビティおよび ACE のさまざまな機能のパフォーマンスを記録するログ ファイルが多数あります。ACE CLI を使用してこれらのログ ファイルにアクセスすると、問題のトラブルシューティングを実施、または ACE の動作をより理解するのに役立ちます。

この章の構成は、次のようになっています。

- システム メッセージ ログングの概要
- システム メッセージ ログング クイック スタート
- システム メッセージ ログングのイネーブル化
- syslog の出力位置の指定
- システム メッセージのタイムスタンプのイネーブル化
- syslog サーバに送信されるメッセージの識別
- ACE のデバイス ID を syslog サーバに指定
- syslog ログング ファシリティの変更
- ログング メッセージ キューの変更
- syslog メッセージの重大度のディセーブル化または変更
- syslog の比率の制限
- スタンバイ ACE 上でのログングのイネーブル化
- ACE を通過する新しい接続の拒否
- 接続セットアップとティアダウン syslog メッセージのログングのイネーブル化
- ログ メッセージの消去
- ログ メッセージ情報の表示

システム メッセージ ログイングの概要

ここでは、次の内容について説明します。

- ログイングの概要
- ログ メッセージの形式
- ログイングの重大度
- 変数

ログイングの概要

ACE のシステム メッセージ ログイング機能では、メッセージをログ ファイルに保存し、ログに記録したメッセージを 1 つまたは複数の出力先に送信できます。システム ログ メッセージでは、ACE の動作を監視またはトラブルシューティングを行うためのログ情報を提供します。デフォルトでは、メッセージはログ ファイルに保存されません。指定された出力位置への syslog メッセージの送信をイネーブルにする必要があります。

ログイング設定には柔軟性があり、ACE がシステム メッセージを処理する方法をさまざまな面からカスタマイズできます。システム メッセージ ログイング機能を使用すると、次の操作を行うことができます。

- メッセージの送信先として、1 つまたは複数の出力位置を指定。出力位置には、コンソール、内部バッファ、1 台または複数の syslog サーバ、SNMP ネットワーク管理ステーション、Telnet や SSH セッション、Catalyst スーパーバイザ エンジン、または ACE 上のフラッシュ メモリが含まれます。
- ログに記録する必要があるメッセージの指定
- メッセージの重大度の指定
- タイムスタンプのイネーブル化
- syslog サーバに送信される ACE の一意なデバイス ID の指定
- ログイング メッセージ キューのサイズ変更
- ACE が syslog でメッセージを生成する比率を制限
- 指定された条件に達した場合に、新しい接続を拒否
- 接続セットアップとティアダウン メッセージのログイングのイネーブル化

ACE がマルチコンテキスト モードで動作している場合、ACE を設定して、仮想コンテキストの ID およびログ メッセージの機能の実行を担当する仮想ユーザを含めることができます。

ACE によって生成されたログを表示するには、出力位置を設定する必要があります。1 つまたは複数の出力位置に、すべてのメッセージを送信するか、またはメッセージの一部を送信するかを選択できます。また、メッセージの重大度を指定して、出力位置に送信されるメッセージを制限することもできます。重大度の値は 0 ~ 7 で、重大度の値が小さいほどより深刻なエラーであることを表しています。ログ メッセージの重大度のリストについては、[表 1-1](#) を参照してください。



(注)

ただし、すべてのシステム メッセージがエラー状態を表しているわけではありません。一部のメッセージは、通常イベントの報告、または設定変更のログへの記録を目的としています。

重大度を指定すると、ACE では、コマンドはその重大度またはそれよりも高い重大度のメッセージに適用されます。たとえば、重大度 3 を指定したコマンドを入力すると、ACE では、そのコマンドを重大度が 0、1、2、および 3 のメッセージに適用します。

ACE では、内部バッファに最大 8192 個の syslog メッセージを格納できます。デフォルトでは、処理待ちになっている ACE のメッセージ キューには 100 個の syslog メッセージを保持できます。

ACE では、各 syslog サーバにおけるログングで EMBLEM syslog 形式をサポートしています。EMBLEM syslog 形式は Cisco IOS ソフトウェアの形式と整合性があり、さらに CiscoWorks 管理アプリケーションと互換性があります。EMBLEM 形式のログングは、UDP syslog メッセージのみで利用できます。

ログ メッセージの形式

システム ログ メッセージはパーセント記号 (%) から始まり、次の形式で表示されます。

```
%<ACE>-Level-[Subfacility]-Message_number: Message_text
```

ACE	ACE によって生成されたメッセージのメッセージ ファシリティ コードを識別します。この値は常に ACE にします。
Level	このレベルは、メッセージで説明されている状態の重大度を反映しています。重大度の値は 0 ~ 7 で、重大度の値が小さいほどより深刻な状態であることを表しています。ログングの重大度のリストについては、 表 1-1 を参照してください。ACE システム ログ メッセージを重大度コードの順に記載したリストについては、 第 3 章「重大度別メッセージ」 を参照してください。
Subfacility	(オプション) システム ログ メッセージを開始したコンポーネントまたはサブコンポーネント名 (たとえば、IFMGR)
Message_number	メッセージを識別する一意な 6 桁の数字。ACE のシステム ログ メッセージの詳細なリストについては、 第 2 章「システム メッセージ」 を参照してください。メッセージは、メッセージ コードの番号順に記載されています。
Message_text	状態を説明するテキスト文字列です。メッセージのこの部分には、仮想コンテキスト、仮想ユーザ、IP アドレス、ポート番号、ユーザ名などが含まれることがあります。



(注)

ACE のシリアル コンソールで受信された syslog メッセージには、メッセージのコード部分のみが含まれています。

たとえば、次の syslog メッセージは、クラス マップを追加したときに表示される情報を示しています。

```
%ACE-6-615004 : VLAN <VLAN-number> available for configuring an interface
```

VLAN-number は、ACE に割り当てられる VLAN 番号を識別します。ACE では、VLAN を使用して、インターフェイスと受信トラフィックを設定できます。

ログングの重大度

ACE では、ログレベルを指定することで、どのシステム メッセージをログに記録するかを指示します。ログレベルを設定すると、さまざまなソフトウェア機能の緊急、アラート、クリティカル、エラー、または警告メッセージが ACE によってログに記録されます。また、ACE では、通知、情報、およびデバッグ メッセージもログに記録されます。ACE では 8 段階のログレベルをサポートしており、ACE で発生してログに記録される、重大または重大ではないさまざまなイベントを識別します。

表 1-1 に、ログ メッセージの重大度を示します。

表 1-1 ログ メッセージの重大度

重大度の番号	重大度のキーワード	説明
0	emergency	システム使用不能 (たとえば、ACE をシャットダウンした後に再起動できない場合、またはハードウェアの障害が発生した場合)
1	alert	即座に対処する必要があります (たとえば、ACE サブシステムの 1 つが動作していない場合)。
2	critical	危険な状態です (たとえば、ACE が危険な状態になり即座に対処する必要がある場合)。
3	error	エラーの状態です (たとえば、ソフトウェアまたはハードウェアの誤動作に関するエラー メッセージ)。
4	warning	警告の状態 (たとえば、ACE がエラー状態なので注意が必要であっても、デバイスの動作を妨げない場合)
5	notification	正常ですが意味のある状態 (たとえば、インターフェイスのアップ / ダウンの遷移およびシステム再起動のメッセージ)
6	informational	情報メッセージのみ (たとえば、リロード要求およびロープロセス スタック メッセージ)
7	debugging	デバッグ中のみ表示されます。

変数

ログ メッセージには、変数が含まれることがよくあります。表 1-2 に、このマニュアルで ACE ログ メッセージの説明に使用される大部分の変数を示します。1 つのログ メッセージでのみ表示される一部の变数は、この表には掲載されていません。

表 1-2 syslog メッセージの変数フィールド

タイプ	変数	情報のタイプ
その他	<i>command</i>	コマンド名
	<i>device</i>	メモリ ストレージ デバイスたとえば、フラッシュ メモリ、TFTP、フェールオーバー スタンバイ ユニット、またはコンソール端末がこれに該当します。
	<i>filename</i>	ACE タイプの画像または設定ファイル名
	<i>privilege_level</i>	ユーザ特権レベル
	<i>reason</i>	メッセージの原因を説明するテキスト文字列
	<i>String</i>	テキスト文字列 (たとえば、ユーザ名)
	<i>url</i>	URL
	<i>user</i>	ユーザ名

表 1-2 syslog メッセージの変数フィールド (続き)

タイプ	変数	情報のタイプ
数字	<i>number</i>	数字正確な数字はログメッセージによって変わります。
	<i>bytes</i>	バイト数
	<i>code</i>	メッセージによって返される 10 進数で、メッセージごとのエラーの原因または発生元を示します。
	<i>connections</i>	接続の数
	<i>time</i>	hh:mm:ss 形式の持続時間
	<i>dec</i>	10 進数
	<i>hex</i>	16 進数
	<i>octal</i>	8 進数
アドレス	<i>IP_address</i>	n.n.n.n 形式の IP アドレス。n は 1 ~ 255 の整数です。
	<i>MAC_address</i>	MAC アドレス
	<i>global_address</i>	グローバル IP アドレス、低セキュリティ レベルのインターフェイスのアドレス
	<i>source_address</i>	パケットの送信元アドレス
	<i>dest_address</i>	パケットの宛先アドレス
	<i>real_address</i>	Network Address Translation (NAT; ネットワークアドレス変換) で変換される前の実際の IP アドレス
	<i>mapped_address</i>	変換後の IP アドレス
	<i>gateway_address</i>	ネットワーク ゲートウェイの IP アドレス
インターフェイス	<i>interface_number</i>	1 ~ n のインターフェイス番号。この番号は、ACE にロードされるインターフェイスの順番によって決まります。show interface internal コマンドを使用すると、インターフェイスについての詳細情報を表示できます。
	<i>interface_name</i>	インターフェイスに割り当てられた名前。show interface コマンドを使用すると、インターフェイスとそれらの名前を表示できます。
ポート、サービス、およびプロトコル	<i>port</i>	TCP または UDP ポート番号
	<i>source_port</i>	送信元ポート番号
	<i>dest_port</i>	宛先ポート番号
	<i>real_port</i>	NAT で変換される前の実際のポート番号
	<i>mapped_port</i>	変換後のポート番号
	<i>global_port</i>	グローバル ポート番号
	<i>protocol</i>	パケットのプロトコル。たとえば、ICMP、TCP、または UDP があります。
	<i>service</i>	パケットによって指定されたサービス。たとえば、SNMP または Telnet があります。

システム メッセージ ログイング クイック スタート

表 1-3 には、ACE でシステム メッセージ ログイングを設定するのに必要な手順の概要が簡潔にまとめられています。各手順には、作業の完了に必要な CLI コマンドが含まれています。

表 1-3 システム メッセージ ログイング設定のクイック スタート

作業とコマンドの例

1. 複数のコンテキストを操作している場合は、CLI プロンプトで、目的のコンテキストを操作していることを確認します。必要であれば、正しいコンテキストに直接ログインするか、または変更してください。

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

この表にある他の例では、特に指定がなければ、Admin コンテキストが使用されています。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. **config** と入力して、設定モードに入ります。

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

3. ログイングをイネーブルにして、システム ログ メッセージを 1 つまたは複数の出力位置に送信します。

```
host1/Admin(config)# logging enable
```

4. ACE システム ソフトウェアを設定して、システム ログイング メッセージを選択した出力位置に送信します。

たとえば、ログイング エラー メッセージのログイング バッファ レベルを 3 に設定するには、次のように入力します。

```
host1/Admin(config)# logging buffered 3
```

たとえば、ログ メッセージを syslog サーバに送信するには、次のように入力します。

```
host1/Admin(config)# logging host 192.168.10.1
```

5. (オプション) システム ログイング メッセージのタイムスタンプの表示をイネーブルにします。

```
host1/Admin(config)# logging timestamp
```

6. (オプション) 重大度に基づいて syslog サーバに送信するメッセージの数を制限します。

```
host1/Admin(config)# logging trap 6
```

7. (オプション) syslog サーバに送信される非 EMBLEM 形式の syslog メッセージの一意なデバイス ID を表示します。

```
host1/Admin(config)# logging device-id hostname
```

8. (オプション) syslog ログイング ファシリティを、デフォルトの 20 (LOCAL4) 以外の値に設定します。

```
host1/Admin(config)# logging facility 16
```

9. (オプション) 処理待ち中にメッセージ キューに表示できる syslog メッセージの数を変更します。

```
host1/Admin(config)# logging queue 100
```

表 1-3 システム メッセージ ログイング設定のクイック スタート (続き)

作業とコマンドの例

10. (オプション) 特定の syslog メッセージの表示をディセーブルにするか、または特定のシステム ログ メッセージの重大度を変更します。

たとえば、%<ACE>-6-615004 syslog メッセージをディセーブルにするには、次のように入力します。

```
host1/Admin(config)# no logging message 615004
```

たとえば、615004 syslog メッセージの重大度を変更するには、次のように入力します。

```
(config)# logging message 615004 level 5
```

11. (オプション) ACE が syslog でメッセージを生成する比率を制限します。

```
host1/Admin(config)# logging rate-limit 42 60
```

12. (オプション) フェールオーバー スタンバイ ACE でのログイングをイネーブルにします。

```
host1/Admin(config)# logging standby
```

13. (オプション) Catalyst 6500 シリーズ シャーシのスーパーバイザ エンジンに送信される syslog メッセージの重大度を設定します。

```
host1/Admin(config)# logging supervisor 3
```

14. (オプション) 指定された条件と一致した場合に、ACE がデバイスをパススルーする新しい接続を禁止するかどうかを定義します。

```
host1/Admin(config)# logging reject-newconn rate-limit-reached
```

15. (オプション) 接続セットアップおよびティアダウン メッセージのより高速な (接続レートの) ログイングをイネーブルにします。

```
host1/Admin(config)# logging fastpath
```

16. (オプション) 変更した設定をフラッシュ メモリに保存します。

```
host1/Admin(config)# exit
```

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

システム メッセージ ログイングのイネーブル化

デフォルトでは、メッセージ ログイングはディセーブルになっています。メッセージを1つまたは複数の出力位置に送信する場合は、ログイングをイネーブルにする必要があります。イネーブルにすると、ログ メッセージはログイング プロセスに送信されます。このログイング プロセスでは、指定された位置へのメッセージを、メッセージを生成したプロセスに非同期的に記録します。ログを表示するには、ログイングの出力位置を設定する必要があります (「[syslog の出力位置の指定](#)」を参照)。

メッセージ ログイングをイネーブルにするには、**logging enable** 設定モード 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。

logging enable

たとえば、すべての出力位置へのメッセージ ログイングをイネーブルにするには、次のように入力します。

```
host1/Admin(config)# logging enable
```

すべての出力位置へのメッセージ ログイングを停止するには、次のように入力します。

```
host1/Admin(config)# no logging enable
```


syslog の出力位置の指定

ACE を設定して、syslog メッセージを選択した出力位置に送信します。ACE では、syslog メッセージを送信するために、次のような複数の出力位置が提供されます。

- ACE の内部バッファ
- ホスト上で動作する 1 つまたは複数の syslog サーバ
- Telnet または SSH 接続
- コンソール



(注) シスコは、syslog メッセージのコンソールへの直接送信は、テスト中にのみ行うように推奨しています。

- SNMP ネットワーク管理ステーション
- Catalyst スーパーバイザ エンジン
- フラッシュ メモリ

メッセージが指定した出力デバイスに送信される前に、**logging enable** コマンドを使用して ACE 上でログイングをイネーブルにする必要があります。詳細については、「[システム メッセージ ログイングのイネーブル化](#)」を参照してください。

ここでは、次の内容について説明します。

- [syslog メッセージのバッファへの送信](#)
- [syslog メッセージの Telnet または SSH セッションへの送信](#)
- [syslog メッセージのコンソールへの送信](#)
- [syslog メッセージの syslog サーバへの送信](#)
- [syslog メッセージの SNMP ネットワーク管理ステーションへの送信](#)
- [syslog メッセージのスーパーバイザ エンジンへの送信](#)
- [ACE 上にあるフラッシュ メモリへの syslog メッセージの送信](#)

syslog メッセージのバッファへの送信

デフォルトでは、ACE 上でのローカル バッファへのログイングはディセーブルになっています。ローカル バッファへのシステム ログイングをイネーブルにし、さらに重大度に基づいてバッファに送信されるメッセージを制限するには、**logging buffered** 設定モード コマンドを使用します。新しいメッセージは、バッファの最後に追加されます。先頭に表示されるメッセージは、バッファ内の最も古いメッセージです。ログ バッファに空きがなくなると、ACE によって最も古いメッセージが削除され、新しいメッセージのための領域が確保されます。

このコマンドの構文は、次のとおりです。

logging buffered severity_level

severity_level 引数には、バッファに送信されるシステム ログ メッセージの中で最も重大度が低いメッセージに対応する値を指定します。重大度を指定すると、重大度の値がそれ以下の syslog メッセージが表示されます。たとえば、指定された重大度が 3 の場合、syslog によって重大度が 3、2、1、および 0 のメッセージが表示されます。

次のエントリを指定できます。

- **0 — emergencies** (システム使用不能メッセージ)

- 1 — **alerts** (即座に処置を実行)
- 2 — **critical** (危険な状態)
- 3 — **errors** (エラー メッセージ)
- 4 — **warnings** (警告メッセージ)
- 5 — **notifications** (正常であっても重要な状態)
- 6 — **informational** (情報メッセージ)
- 7 — **debugging** (デバッグ メッセージ)

ローカルバッファに記録されているメッセージを表示するには、**show logging** コマンドを使用します。新しいメッセージを簡単に表示できるようにバッファの内容を消去するには、**clear logging** コマンドを使用します。

たとえば、ログイング エラー メッセージのログイング バッファ レベルを重大度 3 に設定するには、次のように入力します。

```
host1/Admin(config)# logging buffered 3
```

メッセージのログイングをディセーブルにするには、次のように入力します。

```
host1/Admin(config)# no logging buffered
```

syslog メッセージの Telnet または SSH セッションへの送信

デフォルトでは、Secure Shell (SSH; セキュア シェル) または Telnet を使用するリモート接続に対するログイングは、ACE ではディセーブルになっています。Telnet および SSH セッションのログイング プリファレンスを設定すると、SSH または Telnet リモート接続のログ メッセージを表示できます。SSH または Telnet セッションを介して ACE にアクセスしたときに発生する syslog メッセージを表示するには、**logging monitor** 設定モード コマンドを使用します。表示するメッセージは、重大度に基づいて制限できます。

SSH または Telnet セッションの間にシステム メッセージ ログを表示するには、**terminal monitor** Exec モード コマンドを使用します (『Cisco Application Control Engine Module Administration Guide』を参照)。このコマンドを実行すると、現在のコンテキスト内にあるすべてのセッションに対して syslog メッセージがイネーブルになります。**logging monitor** コマンドを使用するとすべての SSH または Telnet セッションのログイング プリファレンスを設定でき、また **terminal monitor** コマンドを使用すると個別の Telnet セッションのログイングを制御できます。ただし、各セッションでは、**terminal monitor** コマンドが、セッション中に syslog メッセージを端末に表示するかどうかを制御します。



(注)

設定が完了していない場合は、ACE 上でリモート アクセスをイネーブルにし、PC から SSH または Telnet プロトコルを使用してリモート接続を確立します。詳細については、『Cisco Application Control Engine Module Administration Guide』を参照してください。

このコマンドの構文は、次のとおりです。

```
logging monitor severity_level
```

severity_level 引数には、現在の SSH または Telnet セッション中に表示されるシステム ログ メッセージの中で最も重要度が低いメッセージに対応する値を指定します。重大度を指定すると、重大度の値がそれ以下の syslog メッセージが表示されます。たとえば、指定された重大度が 3 の場合、syslog によって重大度が 3、2、1、および 0 のメッセージが表示されます。

次のエントリを指定できます。

- **0** — **emergencies** (システム使用不能メッセージ)
- **1** — **alerts** (即座に処置を実行)
- **2** — **critical** (危険な状態)
- **3** — **errors** (エラー メッセージ)
- **4** — **warnings** (警告メッセージ)
- **5** — **notifications** (正常であっても重要な状態)
- **6** — **informational** (情報メッセージ)
- **7** — **debugging** (デバッグ メッセージ)

たとえば、情報のシステム メッセージ ログを現在の Telnet または SSH セッションに送信するには、次のように入力します。

```
host1/Admin# terminal monitor
host1/Admin# config
Enter configuration commands, one per line. End with CNTL/Z
host1/Admin(config)# logging monitor 6
```

たとえば、情報のシステム メッセージ ログを現在の Telnet または SSH セッションに対してディセーブルにするには、次のように入力します。

```
host1/Admin(config)# no logging monitor
```

端末モニタ機能をディセーブルにするには、次のように入力します。

```
host1/Admin# terminal no monitor 6
```

syslog メッセージのコンソールへの送信

デフォルトでは、コンソールセッション中に ACE が syslog メッセージを表示することはありません。コンソールセッション中の syslog メッセージのログをイネーブルにし、またメッセージの表示を重大度に基づいて制限するには、**logging console** 設定コマンドを使用します。

コンソールへのログをイネーブルにすると、システムのパフォーマンスが低下する可能性があります。**logging console** コマンドは、テストおよび問題のデバッグ、またはネットワークの負荷が非常に少ない場合のみ使用します。ネットワークの負荷が高い場合は、ACE のパフォーマンスが低下する可能性があるため、このコマンドは使用しないでください。ACE がアクティブなときは、次のコマンドを使用します。

- メッセージをバッファに格納するには、**logging buffered** コマンド
- メッセージを表示するには、**show logging** コマンド
- **logging buffered** コマンドによって表示されたメッセージを消去するには、**clear logging** コマンド

このコマンドの構文は、次のとおりです。

logging console severity_level

severity_level 引数には、コンソールに送信されるシステム ログ メッセージの中で最も重大度が低いメッセージに対応する値を指定します。重大度を指定すると、重大度の値がそれ以下の syslog メッセージが表示されます。たとえば、指定された重大度が 3 の場合、syslog によって重大度が 3、2、1、および 0 のメッセージが表示されます。シスコは、3 などのより値が小さい重要度（より高い重要度）を使用することを推奨しています。これは、ログの比率が高くなると ACE のパフォーマンスに影響する可能性があるからです。

次のエントリを指定できます。

- **0** — **emergencies** (システム使用不能メッセージ)
- **1** — **alerts** (即座に処置を実行)
- **2** — **critical** (危険な状態)
- **3** — **errors** (エラー メッセージ)
- **4** — **warnings** (警告メッセージ)
- **5** — **notifications** (正常であっても重要な状態)
- **6** — **informational** (情報メッセージ)
- **7** — **debugging** (デバッグ メッセージ)

たとえば、コンソールセッション中に syslog メッセージのログイングをイネーブルにし、重大度を 3 に設定するには、次のように入力します。

```
host1/Admin(config)# logging console 3
```

コンソールへのメッセージ ログイングをディセーブルにするには、次のように入力します。

```
host1/Admin(config)# no logging console
```

syslog メッセージの syslog サーバへの送信

デフォルトでは、ホスト上の syslog サーバへのログイングは、ACE ではディセーブルになっています。ログ メッセージをホストに送信することを選択した場合、ACE は UDP または TCP を使用してこれらのメッセージを送信します。ホストでは、**syslogd** と呼ばれるプログラム (サーバ) を実行する必要があります。**syslogd** は、他のアプリケーションおよびネットワークからメッセージを受け取るデーモンで、メッセージをシステム全体のログ ファイルに書き込みます。UNIX では、syslog サーバはオペレーティング システムの一部として提供されます。Microsoft Windows の場合は、Windows オペレーティング システム用の syslog サーバを入手する必要があります。

ACE によって送信される syslog メッセージを受信するホスト (syslog サーバ) を指定するには、**logging host** 設定コマンドを使用します。syslog メッセージを受信するサーバは、最大 2 つまで設定できます。

メッセージの syslog サーバへの送信には、UDP または TCP が使用できます。UDP ベースのログイングでは、syslog サーバに障害が発生したとき、ACE のトラフィック通過を阻止しません。ログイングの転送プロトコルとして TCP を使用すると、ACE が syslog サーバに到達できない場合、syslog サーバの設定に誤りがある場合、TCP キューに空きがない場合、またはディスクに空きがない場合、セキュリティ対策として、新しいネットワーク アクセスのセッションは ACE によって拒否されます。

さらに、**logging-reject-newconn tcp-queue-full** 設定モード コマンドを使用すると、デバイスをパススルーする新しい接続を禁止するように ACE を設定できます (「[ACE を通過する新しい接続の拒否](#)」を参照)。このコマンドにより、syslog が TCP syslog サーバに到達できなくなった場合、新しい接続は ACE によって拒否されます。デフォルトでは、この機能はディセーブルになっています。

各 syslog サーバで EMBLEM 形式のログイングは、**format emblem** キーワードによってイネーブルになります。EMBLEM 形式のログイングは、TCP または UDP syslog メッセージで利用できます。特定の syslog ホストに対して EMBLEM 形式のログイングをイネーブルにすると、メッセージはそのホストに送信されるようになります。

このコマンドの構文は、次のとおりです。

```
logging host ip_address [tcp | udp [/port#]] | [default-udp] | [format emblem]]]
```

キーワード、引数、およびオプションは、次のとおりです。

- **ip_address** — syslog サーバとして使用されるホストの IP アドレス
- **tcp** — (オプション) メッセージを syslog サーバへ送信するのに、TCP を使用するように指定します。サーバに対しては、UDP の受信または TCP の受信のいずれか一方だけを指定できます。
- **udp** — (オプション) メッセージを syslog サーバへ送信するのに、UDP を使用するように指定します。サーバに対しては、UDP の受信または TCP の受信のいずれか一方だけを指定できます。
- **port#** — (オプション) syslog サーバが傍受する syslog メッセージ用のポートです。有効値は 1025 ~ 65535 です。デフォルトのプロトコルおよびポートは、UDP/514 です。デフォルトの TCP ポートは (指定する場合)、1470 です。
- **default-udp** — (オプション) TCP 転送が syslog サーバとの通信に失敗した場合に、ACE のデフォルトを UDP にするように指定します。
- **format emblem** — (オプション) 各 syslog サーバで、EMBLEM 形式のログングをイネーブルにします。Cisco Resource Management Environment (RME) は、syslog を収集するネットワーク管理アプリケーションです。RME は、メッセージが EMBLEM 形式の場合に限り、syslog メッセージを処理します。



(注) **logging timestamp** コマンドを入力すると、タイムスタンプ付きのメッセージが syslog サーバに送信されます (「システム メッセージのタイムスタンプのイネーブル化」を参照)。

たとえば、EMBLEM 形式のタイムスタンプ付きメッセージは、次のように表示されます。

```
ipaddress or dns name [Dummy Value/Counter]: [mmm dd hh:mm:ss TimeZone]:
%FACILITY-[SUBFACILITY-]SEVERITY-MNEMONIC: [vtl-ctx: context id] Message-text
```

たとえば、ログ メッセージを syslog サーバに送信するには、次のように入力します。

```
host1/Admin(config)# logging host 192.168.10.1 tcp1025 format emblem default-udp
```

syslog サーバへのログングをディセーブルにするには、次のように入力します。

```
host1/Admin(config)# no logging host 192.168.10.1
```

syslog メッセージの SNMP ネットワーク管理ステーションへの送信

デフォルトでは、ACE から SNMP Network Management Station (NMS) へは、トラップの送信や要求の通知は行われません。トラップの送信と要求の通知は、特定のイベントが発生したときに ACE が生成するシステム アラートです。ACE から NMS への SNMP トラップの送信と要求の通知をイネーブルにするには、**snmp-server enable traps** 設定コマンドを使用します。SNMP 設定の詳細については、『Cisco Application Control Engine Module Administration Guide』を参照してください。

ログ メッセージを NMS に送信するときに、SNMP トラップ メッセージの重大度を設定するには、**logging history** 設定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。

```
logging history severity_level
```

severity_level 引数には、トラップとして NMS に送信されるシステム ログ メッセージの中で最も重大度が低いメッセージに対応する値を指定します。重大度を指定すると、重大度の値がそれ以下の syslog メッセージが表示されます。たとえば、指定された重大度が 3 の場合、syslog によって重大度が 3、2、1、および 0 のメッセージが表示されます。

次のエントリを指定できます。

- **0** — **emergencies** (システム使用不能メッセージ)
- **1** — **alerts** (即座に処置を実行)
- **2** — **critical** (危険な状態)
- **3** — **errors** (エラー メッセージ)
- **4** — **warnings** (警告メッセージ)
- **5** — **notifications** (正常であっても重要な状態)
- **6** — **informational** (情報メッセージ)
- **7** — **debugging** (デバッグ メッセージ)



(注)

Cisco は、初期設定中またはテスト中にデバッグ レベル (重大度が 7) を使用することを推奨しています。設定後は、重要度をデバッグ レベル (重大度が 7) から、ネットワークで使用されているより小さな値に変更します。

たとえば、情報のシステム メッセージ ログを SNMP NMS に送信するには、次のように入力します。

```
host1/Admin(config)# logging history 6
```

システム メッセージ ログの SNMP NMS への送信をディセーブルするには、次のように入力します。

```
host1/Admin(config)# no logging history
```

syslog メッセージのスーパーバイザ エンジンへの送信

Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータでは、ACE は syslog メッセージをスーパーバイザ エンジンへ転送することができます。スーパーバイザ エンジンに送信される syslog メッセージの重要度を設定するには、**logging supervisor** 設定モード 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。

```
logging supervisor severity_level
```



(注)

たとえば、ロギング レベル 6 または 7 を使用して、syslog メッセージをスーパーバイザ エンジンに送信する場合 (特に大量の syslog メッセージが予測される場合) は、注意する必要があります。大量の syslog メッセージをスーパーバイザ エンジンに送信すると、ACE およびスーパーバイザ エンジンの動作速度が低下する場合があります。

severity_level 引数には、スーパーバイザ エンジンに送信されるシステム ログ メッセージの中で最も重大度が低いメッセージに対応する値を指定します。重大度を指定すると、重大度の値がそれ以下の syslog メッセージが表示されます。たとえば、指定された重大度が 3 の場合、syslog によって重大度が 3、2、1、および 0 のメッセージが表示されます。シスコは、3 などのより値が小さい重要度 (より高い重要度) を使用することを推奨しています。これは、スーパーバイザ エンジンのロギングの比率が高くなると Catalyst システムのパフォーマンスに影響する場合がありますからです。

次のエントリを指定できます。

- **0** — **emergencies** (システム使用不能メッセージ)
- **1** — **alerts** (即座に処置を実行)

- 2 — **critical** (危険な状態)
- 3 — **errors** (エラー メッセージ)
- 4 — **warnings** (警告メッセージ)
- 5 — **notifications** (正常であっても重要な状態)
- 6 — **informational** (情報メッセージ)
- 7 — **debugging** (デバッグ メッセージ)

たとえば、情報用のシステム メッセージ ログをスイッチのスーパーバイザ エンジンに送信するには、次のように入力します。

```
host1/Admin(config)# logging supervisor 6
```

スーパーバイザ エンジンへのシステム メッセージのログをディセーブルにするには、次のように入力します。

```
host1/Admin(config)# no logging supervisor
```

ACE 上にあるフラッシュ メモリへの syslog メッセージの送信

デフォルトでは、ACE のフラッシュ メモリへのログはディセーブルになっています。ACE では、システム メッセージ ログをフラッシュ メモリに保存すると、システムの再起動後もログを保持できます。特定のログ メッセージを ACE 上のフラッシュ メモリに送信するには、**logging persistent** 設定モード 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。

```
logging persistent severity_level
```

severity_level 引数には、フラッシュ メモリに送信されるシステム ログ メッセージの中で最も重大度が低いメッセージに対応する値を設定します。重大度を指定すると、重大度の値がそれ以下の syslog メッセージが表示されます。たとえば、指定された重大度が 3 の場合、syslog によって重大度が 3、2、1、および 0 のメッセージが表示されます。シスコは、3 などのより値が小さい重要度（より高い重要度）を使用することを推奨しています。これは、ACE にあるフラッシュ メモリへのログの比率が高くなるとパフォーマンスに影響する可能性があるからです。

次のエントリを指定できます。

- 0 — **emergencies** (システム使用不能メッセージ)
- 1 — **alerts** (即座に処置を実行)
- 2 — **critical** (危険な状態)
- 3 — **errors** (エラー メッセージ)
- 4 — **warnings** (警告メッセージ)
- 5 — **notifications** (正常であっても重要な状態)
- 6 — **informational** (情報メッセージ)
- 7 — **debugging** (デバッグ メッセージ)

たとえば、情報用のシステム メッセージ ログを ACE のフラッシュ メモリに送信するには、次のように入力します。

```
host1/Admin(config)# logging persistent 6
```

ACE のフラッシュ メモリへのログをディセーブルにするには、次のように入力します。

```
host1/Admin(config)# no logging persistent
```

システム メッセージのタイムスタンプのイネーブル化

デフォルトでは、syslog メッセージに、ACE によって日付と時刻の情報が付加されることはありません。メッセージが生成されたときの日付と時刻を syslog メッセージに付加するように指定するには、**logging timestamp** 設定モード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。

logging timestamp

たとえば、システム ログイング メッセージでのタイムスタンプの表示をイネーブルにするには、次のように入力します。

```
host1/Admin(config)# logging timestamp
```

syslog メッセージでのタイムスタンプの表示をディセーブルにするには、次のように入力します。

```
host1/Admin(config)# no logging timestamp
```

syslog サーバに送信されるメッセージの識別

どのメッセージが syslog サーバに送信されるのかを識別するには、**logging trap** 設定コマンドを使用します。**logging trap** コマンドによって、syslog サーバに送信されるログイング メッセージの数が重大度に基づいて制限されます。

このコマンドの構文は、次のとおりです。

logging trap severity_level

severity_level 引数には、syslog サーバに送信されるシステム ログ メッセージの中で最も重大度が低いメッセージに対応する値を指定します。重大度を指定すると、重大度の値がそれ以下の syslog メッセージが表示されます。たとえば、指定された重大度が 3 の場合、syslog によって重大度が 3、2、1、および 0 のメッセージが表示されます。

次のエントリを指定できます。

- **0 — emergencies** (システム使用不能メッセージ)
- **1 — alerts** (即座に処置を実行)
- **2 — critical** (危険な状態)
- **3 — errors** (エラー メッセージ)
- **4 — warnings** (警告メッセージ)
- **5 — notifications** (正常であっても重要な状態)
- **6 — informational** (情報メッセージ)
- **7 — debugging** (デバッグ メッセージ)

ログイング メッセージを syslog サーバへ送信するには、**logging host** コマンドを使用して、syslog サーバとして使用されるホストの名前または IP アドレスを指定します (「[syslog メッセージの syslog サーバへの送信](#)」を参照)。

たとえば、情報のシステム メッセージ ログを syslog サーバに送信するには、次のように入力します。

```
host1/Admin(config)# logging trap 6
```

syslog サーバへのメッセージのログイングをディセーブルにするには、次のように入力します。

```
host1/Admin(config)# no logging trap
```


ACE のデバイス ID を syslog サーバに指定

ACE では、syslog サーバに送信される非 EMBLEM 形式の syslog メッセージに、一意なデバイス ID を含めることができます。メッセージには、syslog サーバに送信されるメッセージ内で指定されるデバイス ID が含まれています。このデバイス ID は、指定されたインターフェイス（別のインターフェイスからのメッセージであっても）のホスト名や IP アドレス、または文字列になります。デバイス ID は、EMBLEM 形式メッセージには表示されません。

logging device-id 設定モード コマンドを使用すると、syslog メッセージに ACE のデバイス ID を含めることを指定できます。この設定がイネーブルになると、ACE によって、すべての非 EMBLEM 形式 syslog メッセージのデバイス ID が表示されます。デバイス ID の指定は、EMBLEM 形式の syslog メッセージテキストには影響しません。



(注)

syslog メッセージのデバイス ID 部分は、syslog サーバを介して表示することはできますが、ACE から直接表示することはできません。

このコマンドの構文は、次のとおりです。

```
logging device-id {context-name | hostname | ipaddress interface_name | string text}
```

キーワード、引数、およびオプションは、次のとおりです。

- **context-name** — ACE から送信される syslog メッセージを一意に識別するデバイス ID として、現在のコンテキストの名前を指定します。
- **hostname** — ACE から送信される syslog メッセージを一意に識別するデバイス ID として ACE のホスト名を指定します。
- **ipaddress interface_name** — ACE から送信される syslog メッセージを一意に識別するデバイス ID としてインターフェイスの IP アドレスを指定します。**ipaddress** キーワードを使用すると、ACE がログデータの外部サーバへの送信にどのインターフェイスを使用するかにかかわらず、syslog メッセージは指定されたインターフェイスの IP アドレスを持っている外部サーバに送信されます。*interface_name* の長さは、最大 64 文字までです。
- **string text** — ACE からの syslog メッセージを一意に識別するテキスト文字列を指定します。**string** の長さは、空白文字を除き、最大 64 文字までです。次の文字は使用できません。& (アンパサンド)、' (単一引用符)、" (二重引用符)、< (小なり記号)、> (大なり記号)、または ? (疑問符)

たとえば、ACE のホスト名を使用して syslog メッセージを一意に識別することを ACE に指示するには、次のように入力します。

```
host1/Admin(config)# logging device-id hostname
```

ACE のホスト名の使用をディセーブルにするには、次のように入力します。

```
host1/Admin(config)# no logging device-id hostname
```

syslog ログング ファシリティの変更

必要であれば、**logging facility** 設定モード コマンドを使用して、ログング ファシリティの値をデフォルトの 20 (LOCAL4) 以外の値に変更できます。ほとんどの UNIX システムは、ファシリティの値が 20 のメッセージを想定しています。ACE では、syslog ファシリティのタイプを変更して、ホスト上の syslog デーモン (syslogd) の動作を識別できます。syslog デーモンでは、指定された syslog ファシリティを使用して、メッセージの処理方法を決定します。ホスト上にある syslog デーモンがメッセージを処理する方法は、各ログング ファシリティによって設定されます。syslog サーバのファイル メッセージは、メッセージのファシリティ番号に基づいています。ファシリティ番号には、16 (LOCAL0) ~ 23 (LOCAL7) の 8 個の番号があります。



(注) syslog デーモンとファシリティ レベルの詳細については、syslog デーモンの資料を参照してください。

このコマンドの構文は、次のとおりです。

logging facility *number*

number 引数では、syslog ファシリティを指定します。有効な値は、16 (LOCAL0) ~ 23 (LOCAL7) です。デフォルトは、20 (LOCAL4) です。

たとえば、syslog メッセージで syslog ファシリティを 16 (LOCAL0) に設定するには、次のように入力します。

```
host1/Admin(config)# logging facility 16
```

syslog ファシリティをデフォルトの 20 (LOCAL4) に戻すには、次のように入力します。

```
host1/Admin(config)# no logging facility 16
```

ログメッセージキューの変更

デフォルトでは、処理待ちの間、ACE はメッセージ キューに 100 個の syslog メッセージを保持できます。メッセージ キューに表示できる syslog メッセージの数を変更するには、**logging queue** 設定モード コマンドを使用します。



(注) ACE が syslog メッセージを処理する前に、キュー サイズを設定してください。トラフィックが非常に多いと、メッセージは破棄される場合があります。

このコマンドの構文は、次のとおりです。

logging queue *queue_size*

queue_size 引数では、syslog メッセージを格納するキューのサイズを指定します。有効な値は、1 ~ 8192 メッセージです。デフォルトは、100 メッセージです。

たとえば、syslog メッセージ キューのサイズを 1000 に変更するには、次のように入力します。

```
host1/Admin(config)# logging queue 1000
```

ログメッセージ キュー サイズをデフォルトの 100 にリセットするには、次のように入力します。

```
host1/Admin(config)# no logging queue 0
```

syslog メッセージの重大度のディセーブル化または変更

システム メッセージ ログイングをイネーブルにすると（「システム メッセージ ログイングのイネーブル化」を参照）、すべての syslog メッセージがイネーブルになります。logging message 設定モード コマンドを使用すると、次のことを制御できます。

- 特定のシステム ログイング メッセージの表示（イネーブルまたはディセーブル）
- 特定のシステム ログイング メッセージに関連付けられている重大度

show logging コマンドを使用すると、メッセージに現在割り当てられている重大度、およびシステム ログイング メッセージがイネーブルにされているかどうかを確認できます。

このコマンドの構文は、次のとおりです。

```
logging message syslog_id [level severity_level]
```

キーワード、引数、およびオプションは、次のとおりです。

- **syslog_id** — ディセーブルまたはイネーブルにする特定のメッセージを指定します。たとえば、メッセージが syslog に %<ACE>-4-411001 のように表示されている場合は、syslog_id に **411001** と入力します。ACE のシステム ログ メッセージの詳細なリストについては、第2章「システム メッセージ」を参照してください。メッセージは、メッセージ コードの番号順で記載されています。
- **level severity_level** — （オプション）特定のシステム ログ メッセージに関連付けられているデフォルトの重大度を変更します。たとえば、syslog に表示される %<ACE>-4-411001 メッセージには、デフォルトの重大度である 4（警告メッセージ）が割り当てられます。デフォルトで割り当てられる重大度は、変更することもできます。ACE のシステム ログ メッセージおよび関連付けられるデフォルトのセキュリティ コードの詳細については、第2章「システム メッセージ」を参照してください。

次のエントリを指定できます。

- **0 — emergencies**（システム使用不能メッセージ）
- **1 — alerts**（即座に処置を実行）
- **2 — critical**（危険な状態）
- **3 — errors**（エラー メッセージ）
- **4 — warnings**（警告メッセージ）
- **5 — notifications**（正常であっても重要な状態）
- **6 — informational**（情報メッセージ）
- **7 — debugging**（デバッグ メッセージ）

たとえば、%<ACE>-6-615004 syslog メッセージ（インターフェイスの設定に VLAN が利用可能）をディセーブルにするには、次のように入力します。

```
host1/Admin(config)# no logging message 615004
```

ディセーブルされた syslog メッセージのログイングをレジュームするには、次のように入力します。

```
host1/Admin(config)# logging message 615004 level 6
```

たとえば、615004 syslog メッセージの重大度をデフォルトの 6（情報）から重大度 5（通知）に変更するには、次のように入力します。

```
(config)# logging message 615004 level 5
```

615004 syslog メッセージの重大度をデフォルトの 6 に戻すには、次のように入力します。

```
host1/Admin(config)# no logging message 615004
```

syslog の比率の制限

ACE が syslog でメッセージを生成する比率を制限するには、**logging rate-limit** 設定モード コマンドを使用します。ACE によって生成される syslog メッセージの数を、特定のメッセージに対して制限することもできます。

このコマンドの構文は、次のとおりです。

```
logging rate-limit {num {interval | level severity_level | message syslog_id} | unlimited {level severity_level | message syslog_id}}
```

キーワード、引数、およびオプションは、次のとおりです。

- **num** — 比率を制限する syslog に対して設定する数字。
- **interval** — 制限する必要があるシステム メッセージ ログに対する設定する時間間隔（秒単位）です。デフォルトの時間間隔は、1 秒です。
- **level severity_level** — システム ログ メッセージの中で最も重要度が低いメッセージに対応する値を設定します。重大度を指定すると、重大度の値がそれ以下の syslog メッセージが表示されます。たとえば、指定された重大度が 3 の場合、syslog によって重大度が 3、2、1、および 0 のメッセージが表示されます。

次のエントリを指定できます。

- **0 — emergencies**（システム使用不能メッセージ）
- **1 — alerts**（即座に処置を実行）
- **2 — critical**（危険な状態）
- **3 — errors**（エラー メッセージ）
- **4 — warnings**（警告メッセージ）
- **5 — notifications**（正常であっても重要な状態）
- **6 — informational**（情報メッセージ）
- **7 — debugging**（デバッグ メッセージ）
- **message syslog_id** — 通知を阻止する特定のメッセージの ID を指定します。たとえば、メッセージが syslog に %ACE-4-411001 のように表示されている場合は、**syslog_id** に **411001** と入力します。ACE のシステム ログ メッセージの詳細なリストについては、[第2章「システム メッセージ」](#)を参照してください。メッセージは、メッセージ コードの番号順で記載されています。
- **unlimited** — syslog でのメッセージ生成比率の制限をディセーブルにします。



(注)

302028 ~ 302031 の syslog（データプレーンでフォーマットされる接続セットアップとティアダウン syslog）の生成比率の制限を設定する場合、ACE はこれらの syslog を常にレベル 6 に制限します。**logging message** コマンドを使用してログング レベルを異なる値に変更し、syslog サーバまたは別の宛先で新しいログング レベルが表示されても、ACE は引き続きこれらの syslog をレベル 6 に制限します。

たとえば、syslog の比率を 60 秒の時間間隔で 42 に制限する場合は、次のように入力します。

```
host1/Admin(config)# logging rate-limit 42 60
```

比率の制限をディセーブルにするには、次のように入力します。

```
host1/Admin(config)# no logging rate-limit 42 60
```

スタンバイ ACE 上でのログिंगのイネーブル化

フェールオーバー スタンバイ ACE 上でログिंगをイネーブルにするには、**logging standby** 設定モード コマンドを使用します。ログिंगをイネーブルにすると、スタンバイ ACE の **syslog** メッセージは、フェールオーバーが発生しても引き続き同期されます。また、イネーブルにした場合、このコマンドによって **syslog** サーバのメッセージ トラフィックは 2 倍になります。デフォルトでは、このコマンドはディセーブルになっています。

このコマンドの構文は、次のとおりです。

logging standby

フェールオーバー スタンバイ ACE でログिंगをイネーブルにするには、次のように入力します。

```
host1/Admin(config)# logging standby
```

スタンバイ ACE でログिंगをディセーブルにするには、次のように入力します。

```
host1/Admin(config)# no logging standby
```

ACE を通過する新しい接続の拒否

指定された条件と一致した場合に、ACE がデバイスをパズスルーする新しい接続を禁止するかどうかを設定するには、**logging-reject-newconn** 設定モード 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。

logging reject-newconn {cp-buffer-full | rate-limit-reached | tcp-queue-full}

キーワード、引数、およびオプションは、次のとおりです。

- **cp-buffer-full** — **syslog** デーモンの内部バッファがフル状態になると、新しい接続は ACE によって拒否されます。
- **rate-limit-reached** — **logging rate-limit** コマンドで指定された **syslog** メッセージ比率に到達した場合、新しい接続は ACE によって拒否されます（「[syslog の比率の制限](#)」を参照）。
- **tcp-queue-full** — **Syslog** が TCP **syslog** サーバに到達できなくなった場合、新しい接続は ACE によって拒否されます。

デフォルトでは、**tcp-queue-full** 条件はイネーブルにされ、**cp-buffer-full** と **rate-limit-reached** 条件はディセーブルにされます。

たとえば、指定した **syslog** メッセージ比率に到達した場合に新しい接続を拒否するように ACE を設定するには、次のように入力します。

```
host1/Admin(config)# logging reject-newconn rate-limit-reached
```

ACE による新しい接続の拒否をディセーブルにするには（デフォルトの状態）、次のように入力します。

```
host1/Admin(config)# no logging reject-newconn rate-limit-reached
```

接続セットアップとティアダウン syslog メッセージのログिंगのイネーブル化

デフォルトでは、接続セットアップとティアダウン ログ メッセージは、ACE によってログに記録されることはありません。接続セットアップとティアダウンメッセージのログिंगをイネーブルにするには、**logging fastpath** 設定モード コマンドを使用します。このログिंगをイネーブルにすると、syslog メッセージは、出力先に正しい順番で到達しません。さらに、syslog メッセージは外部 syslog サーバのみに送信され、またローカル バッファ、コンソール、またはスーパーバイザ モジュールなどの他の有効な出力先に表示されることはありません。

logging fastpath コマンドの構文は、次のとおりです。

logging fastpath

たとえば、接続セットアップとティアダウン syslog メッセージをログに記録するように ACE を設定するには、次のように入力します。

```
host1/Admin(config)# logging fastpath
```

ACE での接続セットアップとティアダウン syslog メッセージのログिंगをディセーブルにするには、次のように入力します。

```
host1/Admin(config)# no logging fastpath
```

ログ メッセージの消去

logging buffered 設定モード コマンドで作成され、メッセージ バッファに格納されている syslog メッセージを消去するには、**clear logging** 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 logging [disabled | rate-limit]

キーワード、引数、およびオプションは、次のとおりです。

- **disabled** — (オプション) ディセーブルになっている syslog メッセージをすべて消去します。
- **rate-limit** — (オプション) **logging rate-limit** コマンドによって指定された、ACE の syslog 生成に関する比率制限の設定を消去します。

たとえば、すべての syslog メッセージを消去するには、次のように入力します。

```
host1/Admin# clear logging
```


ログメッセージ情報の表示

バッファに格納されているすべての syslog メッセージの現在の重大度と状態を表示、または特定の syslog メッセージに関する情報を表示するには、**show logging** 設定モード コマンドの特権 EXEC モードで使用します。このコマンドでは、現在の syslog メッセージが一覧表示され、またどの logging コマンド オプションがイネーブルになっているかが確認されます。syslog バッファの内容を表示するには、バッファ出力位置を設定します（「[syslog メッセージのバッファへの送信](#)」を参照）。

このコマンドの構文は、次のとおりです。

```
show logging [disabled | history | internal {event-history dbg | facility} | message [syslog_id | all | disabled] | persistent | queue | rate-limit | statistics]
```

キーワード、引数、およびオプションは、次のとおりです。

- **disabled** — ディセーブルになっている syslog メッセージのステータスを表示します。
- **history** — syslog メッセージの履歴ファイルを表示します。
- **internal** — syslog の内部メッセージを表示します。
- **event-history db** — syslog サーバのデバッグ履歴を表示します。



(注) ACE デバッグ コマンドは、訓練を受けた Cisco の保守担当者のみが使用することを目的としています。

- **facility** — ACE に含まれているさまざまな内部ファシリティを表示します。
- **message** — すでにデフォルト設定から変更された syslog メッセージのリストを表示します。これらは、異なる重大度が割り当てられている syslog メッセージ、またはすでにディセーブルになっているメッセージです。
- **syslog_id** — 特定のシステム ログ メッセージ（メッセージ ID により）、割り当てられているデフォルトの重要度、およびこのメッセージがイネーブルまたはディセーブルになっているかどうかを表示します。ACE のシステム ログ メッセージの詳細なリストについては、[第2章「システム メッセージ」](#)を参照してください。メッセージは、メッセージ コードの番号順で記載されています。
- **all** — すべてのシステム ログ メッセージ ID、割り当てられているデフォルトの重要度、および各メッセージがイネーブルまたはディセーブルになっているかどうかを表示します。
- **disabled** — ディセーブルになっている syslog メッセージの完全なリストを表示します。
- **persistent** — ACE 上のフラッシュ メモリに送信されるログ メッセージの統計情報を表示します。
- **queue** — 内部 syslog キューの統計情報を表示します。
- **rate-limit** — 現在の syslog の比率制限設定を表示します。
- **statistics** — syslog の統計情報を表示します。

たとえば、syslog message 615004 のメッセージ設定（インターフェイスの設定に VLAN が利用可能）の詳細を表示するには、次のように入力します。

```
host/Admin# show logging message 615004
Message logging:
      message 615004: default-level 6 (enabled)
```

表 1-4 では、`show logging` コマンド出力のフィールドについて説明しています。

表 1-4 `show logging` コマンドのフィールドの説明

フィールド	説明
Syslog Logging	ACE のシステム メッセージ ログिंगのステータス：イネーブルまたはディセーブル
Facility	システム メッセージ ログング ファシリティ設定
History Logging	システム メッセージ ログング履歴設定のステータス：イネーブルまたはディセーブル
Supervisor Logging	スーパーバイザ エンジンのログング トラップ レベル設定のステータス：イネーブルまたはディセーブル
Trap Logging	syslog サーバのトラップ レベル設定のステータス：イネーブルまたはディセーブル
Timestamp Logging	syslog メッセージに日付と時刻を含めるかどうかのステータス：イネーブルまたはディセーブル
Fastpath Logging	syslog ファストパス ログングのステータス：イネーブルまたはディセーブル
Persist Logging	ACE 上にあるフラッシュ メモリへのログングのステータス：イネーブルまたはディセーブル
Standby Logging	フェールオーバー スタンバイ ACE へのログングのステータス：イネーブルまたはディセーブル
Rate-limit logging	syslog メッセージを生成する ACE での比率制限のステータス：イネーブルまたはディセーブル
Console Logging	コンソールへのログングのステータス：イネーブルまたはディセーブル
Monitor Logging	SSH または Telnet を使用するリモート接続へのログングのステータス：イネーブルまたはディセーブル
Device ID	syslog サーバに送信される非 EMBLEM 形式の syslog メッセージに一意なデバイス ID を含めるかどうかのステータス：イネーブルまたはディセーブル
Reject-newconn	指定された条件と一致した場合に、ACE がデバイスをパススルーする新しい接続を禁止するかどうかを定義します。
rate-limit-reached	logging rate-limit コマンドで指定した syslog メッセージの比率に到達した場合に、ACE が新しい接続を拒否するかどうかのステータスです。ステータスは、イネーブルまたはディセーブルのいずれかになります。
tcp-queue-full	syslog が TCP syslog サーバに到達できなくなった場合に、ACE が新しい接続を拒否するかどうかのステータスです。ステータスは、イネーブルまたはディセーブルのいずれかになります。
cp-buffer-state	syslog デーモンの内部バッファに空きがなくなった場合に、ACE が新しい接続を拒否するかどうかのステータスです。ステータスは、イネーブルまたはディセーブルのいずれかになります。
Message Logging	syslog メッセージがディセーブルになっているか、または syslog メッセージの重大度が変更されているかのステータスです。ステータスは、イネーブルまたはディセーブルのいずれかになります。
Buffered Logging	ACE 上にあるローカル バッファへのログングがディセーブルになっているかどうかのステータス：イネーブルまたはディセーブル
Buffer Info	syslog メッセージ バッファに関する情報を提供します。
Current Size	ACE 上にある syslog バッファ メモリの現在のサイズ

表 1-4 show logging コマンドのフィールドの説明 (続き)

フィールド	説明
Global Pool	利用可能な syslog バッファ メモリの合計サイズ
Used Pool	使用中の syslog バッファ メモリの合計サイズ
Min.	利用可能な最小の syslog バッファ メモリ
Max.	利用可能な最大の syslog バッファ メモリ
Cur Ptr	syslog バッファ メモリの現在のポインタ位置。バッファ メモリに対して読み取りまた書き込みを行うごとに、Cur Ptr は自動的に先へ進みます。
Wrapped	syslog バッファ メモリのデータに対してラップ アラウンドが発生したかどうかを示します。

表 1-5 では、show logging disabled コマンド出力のフィールドについて説明しています。

表 1-5 show logging disabled コマンドのフィールドの説明

フィールド	説明
Message Logging	ACE で無効にされている syslog メッセージのステータス：イネーブルまたはディセーブル

表 1-6 では、show logging history コマンド出力のフィールドについて説明しています。

表 1-6 show logging history コマンドのフィールドの説明

フィールド	説明
syslog_trinity_show_history for context x	アクティブ ユーザ コンテキストの syslog メッセージ履歴設定のステータス：イネーブルまたはディセーブル

表 1-7 では、show logging internal facility コマンド出力のフィールドについて説明しています。

表 1-7 show logging internal facility コマンドのフィールドの説明

フィールド	説明
Syslog registered x facilities	すべての syslog 登録ファシリティのリストを表示します。

表 1-8 では、show logging persistent コマンド出力のフィールドについて説明しています。

表 1-8 show logging persistent コマンドのフィールドの説明

フィールド	説明
Current Size	ACE 上にある syslog バッファ メモリの現在のサイズ
Global Pool	利用可能な syslog バッファ メモリの合計サイズ
Used Pool	使用中の syslog バッファ メモリの合計サイズ
Min.	利用可能な最小の syslog バッファ メモリ
Max.	利用可能な最大の syslog バッファ メモリ
Cur Ptr	syslog バッファ メモリの現在のポインタ位置。バッファ メモリに対して読み取りまた書き込みを行うごとに、Cur Ptr は自動的に先へ進みます。
Wrapped	syslog バッファ メモリのデータに対してラップ アラウンドが発生したかどうかを示します。

表 1-9 では、**show logging** コマンド出力のフィールドについて説明しています。

表 1-9 show logging queue コマンドのフィールドの説明

フィールド	説明
Logging Queue length limit	メッセージ キューで表示できる syslog メッセージの数、および破棄されたメッセージの数
Current <i>x</i> msg on queue, <i>xxx</i> msg/s most on queue	現在ログイン キューにあるメッセージの数、およびメッセージ キューに表示できるデフォルトの syslog メッセージの数
CP messages received	コントロール パネルから受信したメッセージの数、および破棄されたメッセージの数
IXP messages received	IXP2800 ネットワーク プロセッサから受信したメッセージの数、および破棄されたメッセージの数
Xscale messages received	Xscale CPU から受信したメッセージの数
System Max Queue size	ログイング キューの最大サイズ
System Free Queue size for allocation	ログイング キューの使用可能な領域

表 1-10 では、**show logging rate-limit** コマンド出力のフィールドについて説明しています。

表 1-10 show logging rate-limit コマンドのフィールドの説明

フィールド	説明
Rate-limit Logging	現在の syslog 比率制限の設定

表 1-11 では、**show logging statistics** コマンド出力のフィールドについて説明しています。

表 1-11 show logging statistics コマンドのフィールドの説明

フィールド	説明
Syslog Statistics	システム メッセージ ログに固有の統計情報
Messages sent	
Console	コンソールに送信されたメッセージの総数
バッファ	ACE 上にあるローカルバッファに送信されたメッセージの総数
Persistent	ACE 上にあるフラッシュ メモリに送信されたメッセージの総数
Supervisor	スーパーバイザ エンジンに送信されたメッセージの総数
History	NMS に送信された SNMP メッセージの総数
Host	ホスト上の syslog サーバに送信されたメッセージの総数
Misc	その他のシステム ログイング メッセージの総数
Messages Discarded	
Cfg rate-limit	logging rate-limit コマンドで指定した syslog メッセージの比率に基づいて破棄されたメッセージの総数
Hard rate-limit	内部的に設定された syslog メッセージの比率に基づいて破棄されたメッセージの総数
Server down	ホスト上の syslog サーバに障害が発生したことによって破棄されたメッセージの総数
Queue full	メッセージ キューに空きがなくなったために破棄されたメッセージの総数
Errors	エラー状態によって破棄されたメッセージの総数

表 1-11 show logging statistics コマンドのフィールドの説明 (続き)

フィールド	説明
SNMP-related Counters	
Notifications sent	SNMP トラップ(イベント通知)を ACE から NMS へ送信した回数の合計
History table flushed	syslog メッセージのトラップ履歴テーブルが消去された回数の合計
Messages ignored	ACE によって無視された SNMP メッセージの総数
NP-related Counters	ネットワーク プロセッサに関連したメッセージ カウンタ
To-CP dropped	コントロールプレーンによってドロップされたネットワーク プロセッサによって送信されたメッセージの総数
Fastpath sent	ACE によって送信された接続セットアップとティアダウン メッセージの総数
Fastpath dropped	ACE によってドロップされた接続セットアップとティアダウン メッセージの総数

