CHAPTER 19

ロギングについて

この章では、ACS 5.4 のロギング機能について説明します。管理者とユーザは、ACS の各種の管理インターフェイスを使用してさまざまなタスクを実行します。管理アクセス コントロール機能を使用して、管理者とユーザにさまざまなタスクの実行権限を割り当てることができます。

これとは別に、管理者とユーザが実行するさまざまな処理をトラッキングするオプションが必要になることもあります。ACS では、これらの処理とイベントのトラッキングに使用できるいくつかのログが提供されています。

この章の内容は、次のとおりです。

ロギングについて

ACS では次のログを収集できます。

- カスタマー ログ：ACS の監査とトラブルシューティングに使用し、アカウンティング、監査、システムレベル診断などの日常的な操作を記録するログを含みます。
- デバッグ ログ：シスコ テクニカル サポートにエクスポートして評価およびトラブルシューティングに使用できる詳細レベルのテキスト メッセージです。ACS デバッグ ログは、コマンドライン インターフェイスを介して設定します。具体的には、コマンドライン インターフェイスを使用して、ACS デバッグ ログの重大度レベルをイネーブルおよび設定します。詳細については、『*Command Line Interface Reference Guide for Cisco Secure Access Control System 5.4*』を参照してください。
- プラットフォーム ログ：ACS アプライアンス オペレーティング システムによって生成されるログ ファイル。

デバッグ ログとプラットフォーム ログは、各 ACS サーバにローカルに格納されます。カスタマー ログは、展開されているすべてのサーバについて集中的に表示できます。

ロギングには次の ACS インターフェイスを使用できます。

- Web インターフェイス：プライマリ ロギング インターフェイス。ロギングするメッセージおよびメッセージをロギングする場所を設定できます。
- コマンドライン インターフェイス（CLI）：ログ、デバッグ ログ、およびデバッグ バックアップ ログをローカル ターゲットに表示およびダウンロードできます。CLI では、プラットフォーム ログも表示およびダウンロードできます。詳細については、『*Command Line Interface Reference Guide for Cisco Secure Access Control System 5.4*』を参照してください。

ログ ターゲットの使用方法

カスタマー ログ情報を複数のコンシューマまたは*ログ ターゲット*に送信することを指定できます。また、ログ メッセージをテキスト フォーマットでローカルに格納するか、または syslog サーバに転送するかを指定できます。デフォルトでは、*ローカル ストア*と呼ばれる単一の定義済みローカル ログ ターゲットは、データを ACS サーバにテキスト フォーマットで格納し、ローカル ACS サーバからのログ メッセージだけを含んでいます。ローカル ストアに格納されているレコードは、CLI から表示できます。

ログを syslog サーバに転送することも指定できます。ACS では、syslog 転送を使用して、ログを Monitoring and Reports コンポーネントに転送します。ACS ログ メッセージを受信する追加の syslog サーバを定義することもできます。指定した追加の syslog サーバごとに、リモート ログ ターゲットを定義する必要があります。

分散展開では、セカンダリ ACS サーバの 1 つを Monitoring and Reports サーバとして指定する必要があり、そのサーバが展開されたすべてのサーバからログを受信することを指定する必要があります。デフォルトでは、*LogCollector* と呼ばれるログ ターゲットが Monitoring and Reports サーバを識別します。

分散展開が使用されている場合は、Web インターフェイスの [Log Collector] オプションで、ログ情報を収集するサーバを指定します。展開環境のセカンダリ サーバを Monitoring and Reports サーバとして機能するように指定することを推奨します。

ここでは、次の内容について説明します。

ロギング カテゴリ

各ログには、ログ メッセージの内容に従ってロギング カテゴリにバンドルされているメッセージ コードが関連付けられています。ロギング カテゴリは、含まれているメッセージの内容を説明する場合に役立ちます。

ロギング カテゴリは、ACS の機能、フロー、または使用例を説明するメッセージ コードのバンドルです。カテゴリは階層構造に配置され、ロギングの設定に使用されます。各カテゴリには次の項目があります。

- Name：説明的な名前
- Type：Audit、Accounting、または Diagnostics
- Attribute list：カテゴリに関連付けられているメッセージとともにロギングできる属性のリスト（該当する場合）

ACS では、ログ ターゲットを割り当てることのできる次の設定済みグローバル ACS ロギング カテゴリが提供されています（ローカル ストア ターゲット（19-5 ページ）を参照）。

- 次のような管理と操作の監査。
  - ACS の設定変更：ACS に対して行われたすべての設定変更をロギングします。項目が追加または編集された場合、設定変更イベントには、変更された属性の詳細とそれらの新しい値も含まれます。編集要求の結果、属性が新しい値を持たない場合、設定監査レコードは作成されません。

（注）　複雑な設定項目または属性（ポリシーや DACL の内容など）の場合は、新しい属性値が「New/Updated」としてレポートされ、監査に実際の属性値は含まれません。

  - ACS 管理者アクセス：管理者がログアウトするまで、管理者がシステムにアクセスしたときに発生したすべてのイベントをロギングします。管理者が明示的な要求で ACS を終了したか、またはセッションがタイムアウトになったかをロギングします。このログには、アカウントが非アクティブなために失敗したログイン試行も含まれます。ログインの失敗と失敗の理由がロギングされます。
  - ACS の操作変更：管理者が要求したすべての操作をロギングします（展開環境から ACS をプライマリとしてプロモートする、完全複製を要求する、ソフトウェアのダウンロードを実行する、バックアップまたは復元を実行する、PAC を生成および復元するなど）。
  - 内部ユーザ パスワードの変更：すべての管理インターフェイスで内部ユーザ パスワードに対して行われたすべての変更をロギングします。

  また、管理と操作の監査メッセージをローカル ストアにロギングする必要があります。任意で、これらのメッセージをリモート ロギング ターゲットにロギングできます（ローカル ストア ターゲット（19-5 ページ）を参照）。

- AAA 監査。これには、RADIUS および TACACS+ の認証の成功または失敗、コマンドアクセスの認証の成功または失敗、パスワード変更、RADIUS 要求応答などが含まれます。
- AAA 診断。これには、RADIUS および TACACS+ 診断要求と RADIUS 属性要求の認証、許可、アカウンティング情報、ID ストアと認証フローの情報などが含まれます。これらのメッセージのロギングは任意です。
- システム診断。これには、システムの起動とシャットダウンやロギング関連の診断メッセージが含まれます。
  - CLI および Web インターフェイスに関連する管理診断メッセージ
  - 外部サーバ関連メッセージ
  - ローカル データベース メッセージ
  - ローカル サービス メッセージ
  - 証明書関連メッセージ

  これらのメッセージのロギングは任意です。
- システム統計情報。これには、システム パフォーマンスとリソース使用状況に関する情報が含まれます。CPU とメモリの使用状況、プロセスの健全性、要求処理の遅延などのデータが含まれます。
- アカウンティング。これには、TACACS+ ネットワーク アクセス セッションの開始、停止、およびアップデート メッセージに加えて、コマンド アカウンティングに関連するメッセージが含まれます。また、これらのメッセージはローカル ストアにロギングできます。これらのメッセージのロギングは任意です。

ログ メッセージは、このトピックで説明するロギング カテゴリに含めるか、またはロギング サブカテゴリに含めることができます。各ロギング サブカテゴリを個別に設定することが可能であり、その設定は親カテゴリに影響しません。

ACS Web インターフェイスで、[System Administration] > [Configuration] > [Logging Categories] > [Global] を選択して、ロギング カテゴリとサブカテゴリの階層構造を表示します。Web インターフェイスで、[Monitoring and Reports] > [Catalog] を選択して、設定したロギング カテゴリに基づくレポートを実行します。

各ログ メッセージには、次の情報が含まれます。

- イベント コード：固有のメッセージ コード。
- ロギング カテゴリ：ログ メッセージが属するカテゴリを識別します。
- 重大度レベル：診断の重大度レベルを識別します。詳細については、「ログ メッセージの重大度レベル（19-4 ページ）」を参照してください。
- メッセージ クラス：RADIUS、ポリシー、EAP 関連コンテキストなど、コンテキストが類似するメッセージのグループを識別します。
- メッセージ テキスト：英語での短い説明テキスト。
- 説明：ログ メッセージの理由、トラブルシューティング情報（該当する場合）、および詳細情報への外部リンクを示す英語のテキスト。
- 失敗の理由（任意）：ログ メッセージが失敗の理由に関連付けられているかどうかを示します。

パスワードは、暗号化されているかどうかにかかわらずロギングされません。

グローバルおよびインスタンスごとのロギング カテゴリ

デフォルトでは、1 つのログ カテゴリ設定が、展開されたすべてのサーバに適用されます。各ログ カテゴリについて、ロギングされるメッセージの重大度のしきい値、メッセージがローカル ターゲットにロギングされるかどうか、およびメッセージの送信先のリモート syslog ターゲットが定義されます。

ログ カテゴリは階層構造に編成されるため、親カテゴリに対して行った設定変更はすべての子カテゴリに適用されます。ただし、管理者は展開された個々のサーバに異なる設定を適用できます。

たとえば、展開環境内の 1 つのサーバに、より集中的な診断ロギングを適用できます。インスタンスごとのロギング カテゴリ設定には、展開されたすべてのサーバが表示され、それらのサーバがグローバル ロギング設定を利用するように設定されているか、または固有の *カスタム* 設定を持つかが示されます。

サーバのカスタム設定を定義するには、最初に [*Override*] オプションを選択してから、そのサーバの特定のログ カテゴリ定義を設定する必要があります。

ログ メッセージ カタログを使用して、生成できるすべてのログ メッセージを表示できます。ログ メッセージごとに、対応するカテゴリと重大度が表示されます。この情報は、ロギング カテゴリ定義の設定時に役立つことがあります。

ログ メッセージの重大度レベル

特定のロギング カテゴリに対して特定の重大度レベル以上のログをロギングするように設定し、これを設定要素として追加して、保存、表示、およびエクスポートするメッセージ数を制限または拡張できます。

たとえば、特定のロギング カテゴリに対して重大度レベル WARNING のログをロギングするように設定した場合は、重大度レベル WARNING のロギング カテゴリとそれよりも高いプライオリティ レベル（ERROR および FATAL）のロギング カテゴリに対するログ メッセージが、設定した場所に送信されます。表 19-1 に、重大度レベルおよび関連するプライオリティ レベルを示します。

表 19-1　ログ メッセージの重大度レベル

ACS 重大度レベル	説明	Syslog 重大度レベル
FATAL	緊急事態。ACS が使用できないため、すぐに対応する必要があります。	1（最高）
ERROR	クリティカルまたはエラー状況。	3
WARN	正常だが重要な状況。	4
NOTICE	監査およびアカウンティング メッセージ。重大度 NOTICE のメッセージは、指定された重大度しきい値に関係なく、常に設定済みログ ターゲットに送信され、フィルタ処理はされません。	5
INFO	診断情報メッセージ。	6
DEBUG	診断メッセージ。	7

ローカル ストア ターゲット

ローカル ストア内のログ メッセージはテキスト ファイルであり、それが属するロギング カテゴリに関係なく、*/opt/CSCOacs/logs/localStore/* にある 1 つのログ ファイルに送信されます。ローカル ストアには、ローカル ACS ノードからのログ メッセージだけを含めることができます。ローカル ストアは、他の ACS ノードからのログ メッセージを受け入れることができません。

ローカル ストアに送信されるログを設定できますが、ログ メッセージとともに送信される属性は設定できません。すべての属性が、送信されるログ メッセージとともに送信されます。

管理と操作の監査ログ メッセージは常にローカル ストアに送信され、リモート syslog サーバと Monitoring and Reports サーバ ターゲットにも送信できます。

ログ メッセージは、次の syslog メッセージ フォーマットでローカル ストアに送信されます。

time stamp sequence_num msg_code msg_sev msg_class msg_text attr=value

表 19-2 に、ローカル ストア syslog メッセージ フォーマットの内容を示します。

表 19-2　ローカル ストアと Syslog メッセージ フォーマット

フィールド	説明
timestamp	生成元の ACS のローカル クロックに従った、*YYYY- MM-DD hh:mm:ss:xxx +/-zh:zm* フォーマットでのメッセージ生成の日付。値は次のとおりです。 • *YYYY* = 年を表す数字。 • *MM* = 月を表す数字。1 桁の月（1 ～ 9）の場合は、数字の前に 0 が付きます。 • *DD* = 日を表す数字。1 桁の日（1 ～ 9）の場合、数字の前に 0 が付きます。 • *hh* = 時間：00 ～ 23。 • *mm* = 分：00 ～ 59。 • *ss* = 秒：00 ～ 59。 • *xxx* = ミリ秒：000 ～ 999。 • *+/-zz:zz* = ACS サーバのタイムゾーンからのタイムゾーン オフセット。zh はオフセットの時間数、zm はオフセットの分数です。すべて先頭に、オフセットの方向を示すマイナスまたはプラス記号が付きます。 たとえば、+02:00 は、タイム スタンプによって示された時刻に、ACS サーバのタイムゾーンよりも 2 時間先行する ACS ノードでメッセージが発生したことを示します。
sequence_num	各メッセージのグローバル カウンタ。1 つのメッセージがローカル ストアに送信され、次に syslog サーバ ターゲットに送信された場合は、カウンタが 2 つ増加します。有効な値は 0000000001 ～ 999999999 です。
msg_code	ロギング カテゴリで定義されているメッセージ コード。
msg_sev	ログ メッセージのメッセージ重大度レベル（表 19-1 を参照）。
msg_class	同じコンテキストを持つメッセージのグループを識別するメッセージ クラス。
text_msg	英語の説明テキスト メッセージ。
attr=value	ロギングされたイベントの詳細を示す属性と値のペアのセット。カンマ（,）で各ペアを区切ります。 属性名は ACS ディクショナリで定義されています。 応答方向属性セットの値は、Response という 1 つの属性にバンドルされ、中カッコ {} で囲まれます。また、Response 内の属性と値のペアはセミコロンで区切られます。次に例を示します。 Response={RadiusPacketType=AccessAccept; AuthenticationResult=UnknownUser; cisco-av-pair=sga:security-group-tag=0000-00; }

Web インターフェイスを使用して、ローカル ストア ログ ファイルを保持する日数を設定できます。デフォルトの設定では、データが 5 MB を超えるか、または 1 日 1 回削除されますが、このいずれかの制限に最初に達したときに削除されます。

ローカル ストア ファイルを 2 日以上保持するように設定し、結合されたファイルのデータ サイズが 95000 Mb に達した場合は、システム診断ログに FATAL メッセージが送信され、データが削除されるまでローカル ストアへのすべてのロギングが停止します。Web インターフェイスを使用して、ローカル ストア ログ ファイルを削除してください。削除処理は現在アクティブなログ ファイルにロギングされます。ローカル ログ データの削除（18-24 ページ）を参照してください。

現在のログ ファイルの名前は *acsLocalStore.log* です。古いログ ファイルの名前のフォーマットは *acsLocalStore.log.YYYY-MM-DD-hh-mm-ss-xxx* で、各項目の意味は次のとおりです。

- acsLocalStore.log = 非アクティブなローカル ストア ログ ファイルのプレフィックスに、タイムスタンプが追加されます。

（注）　タイムスタンプは、ファイルが最初に作成されたときに追加され、ファイル内の最初のログ メッセージのタイムスタンプと一致します。

  - *YYYY* = 年を表す数字。
  - *MM* = 月を表す数字。1 桁の月（1 ～ 9）の場合は、数字の前に 0 が付きます。
  - *DD* = 日を表す数字。1 桁の日（1 ～ 9）の場合、数字の前に 0 が付きます。
  - *hh* = 時間：00 ～ 23。
  - *mm* = 分：00 ～ 59。
  - *ss* = 秒：00 ～ 59。
  - *xxx* = ミリ秒：000 ～ 999。

ローカル ストアを重大なログ ターゲットとして設定できます。重大なログ ターゲットの詳細については、ログ メッセージの表示（19-10 ページ）を参照してください。

ログ メッセージは、ローカル ログ ターゲット（ローカル ストア）または最大 8 つのリモート ログ ターゲット（リモート syslog サーバ上）に送信できます。

- [System Administration] > [Configuration] > [Log Configuration] > [Remote Log Targets] を選択して、リモート ログ ターゲットを設定します。
- [System Administration] > [Configuration] > [Log Configuration] > [Logging Categories] を選択して、どのログ メッセージをどのターゲットに送信するかを設定します。

重大なログ ターゲット

ローカル ストア ターゲットは、重大なログ ターゲット（ロギング カテゴリのプライマリまたは必須ログ ターゲット）として機能できます。

たとえば、管理と操作の監査メッセージは常にローカル ストアにロギングされますが、それらをリモート syslog サーバまたは Monitoring and Reports サーバ ログ ターゲットにロギングするように設定することもできます。ただし、リモート ログ ターゲットに追加でロギングされるように設定された管理と操作の監査メッセージは、ローカル ログ ターゲットへの最初のロギングが正常に行われた場合には、そのリモート ログ ターゲットにだけロギングされます。

重大なログ ターゲットを設定し、メッセージがその重大なログ ターゲットに送信される場合、メッセージは、ベスト エフォートに基づいて重大ではない設定済みログ ターゲットにも送信されます。

- 重大なログ ターゲットを設定し、メッセージがその重大なログ ターゲットにロギングされない場合、メッセージは重大ではない設定済みログ ターゲットにも送信されません。
- 重大なログ ターゲットを設定していない場合、メッセージは、ベスト エフォートに基づいて重大ではない設定済みログ ターゲットに送信されます。

[System Administration] > [Configuration] > [Log Configuration] > [Logging Categories] > [Global] > *log_category* を選択します。*log_category* は、ロギング カテゴリの重大なログ ターゲットを設定するための特定のロギング カテゴリです。

(注)　重大なロギングは、アカウンティングおよび AAA 監査（成功した認証）カテゴリにだけ適用できます。AAA 診断、システム診断、およびシステム統計情報のカテゴリには重大なロギングを設定できません。

リモート Syslog サーバ ターゲット

Web インターフェイスを使用して、ロギング カテゴリ メッセージがリモート syslog サーバ ターゲットに送信されるように設定できます。ログ メッセージは、syslog プロトコル標準（RFC-3164 を参照）に従ってリモート syslog サーバ ターゲットに送信されます。syslog プロトコルはセキュアでない UDP です。

ログ メッセージは、ローカル ストア syslog メッセージ フォーマット（表 19-2 を参照）に先行する次の syslog メッセージ ヘッダー フォーマットでリモート syslog サーバに送信されます。

pri_num YYYY Mmm DD hh:mm:ss xx:xx:xx:xx/host_name cat_name msg_id total_seg seg_num

表 19-3 に、リモート syslog メッセージ ヘッダー フォーマットの内容を示します。

表 19-3　リモート Syslog メッセージ ヘッダー フォーマット

フィールド	説明
pri_num	メッセージのプライオリティ値。メッセージのファシリティ値と重大度値の組み合わせです。プライオリティ値 =（ファシリティ値 * 8）+ 重大度値。ファシリティ コードの有効なオプションは次のとおりです。 • LOCAL0（コード = 16） • LOCAL1（コード = 17） • LOCAL2（コード = 18） • LOCAL3（コード = 19） • LOCAL4（コード = 20） • LOCAL5（コード = 21） • LOCAL6（コード = 22、デフォルト） • LOCAL7（コード = 23） 重大度値：重大度値については、表 19-1 を参照してください。

表 19-3　リモート Syslog メッセージ ヘッダー フォーマット （続き）

フィールド	説明
time	生成元の ACS のローカル クロックによる*YYYY Mmm DD hh:mm:ss* フォーマットでのメッセージ生成の日付。値は次のとおりです。 • *YYYY* = 年を表す数字。 • *Mmm* = 月の表現（Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec）。 • *DD* = 日を表す数字。1 桁の日付（1 ～ 9）の場合は、数字の前に空白が付きます。 • *hh* = 時間：00 ～ 23。 • *mm* = 分：00 ～ 59。 • *ss* = 秒：00 ～ 59。 一部のデバイスは、タイムゾーンを -/+hhmm のフォーマットで指定するメッセージを送信します。- と + は、ACS サーバのタイムゾーンからのオフセット方向を示します。hh はオフセットの時間数、mm はオフセット時間の分数です。 たとえば、+02:00 は、タイム スタンプによって示された時刻に、ACS サーバのタイムゾーンよりも 2 時間先行する ACS ノードでメッセージが発生したことを示します。
xx:xx:xx:xx/host_name	生成元 ACS の IP アドレス、またはホスト名。
cat_name	先頭に `CSCOacs` 文字列が付いたロギング カテゴリ名。
msg_id	固有のメッセージ ID。1 ～ 4294967295 です。メッセージ ID は、新しいメッセージごとに 1 つ増加します。メッセージ ID は、アプリケーションが再起動するたびに 1 から再開します。
total_seg	ログ メッセージ内のセグメントの総数。長いメッセージは複数のセグメントに分割されます。
seg_num	メッセージ内のセグメントの順序番号。この数値を使用して、メッセージのどのセグメントを表示しているかを判断します。

syslog メッセージ データまたはペイロードは、表 19-2 で説明しているローカル ストア メッセージ フォーマットと同じです。

リモート syslog サーバ ターゲットは、ファシリティ コード ネーム *LOCAL0* ～ *LOCAL7* で識別されます（デフォルトのロギング場所は *LOCAL6*）。リモート syslog サーバに割り当てられたログ メッセージはデフォルトの Linux syslog の場所（*/var/log/messages*）に送信されますが、これに代わりサーバ上の別の場所を設定することもできます。

リモート syslog サーバは、重大なログ ターゲットとして機能できません。重大なログ ターゲットの詳細については、重大なログ ターゲット（19-7 ページ）を参照してください。

レポート サーバ ターゲットの監視

Web インターフェイスを使用して、ロギング カテゴリ メッセージが Monitoring and Reports サーバ ターゲットに送信されるように設定できます。ログ メッセージは、syslog プロトコル標準（RFC-3164 を参照）に従って Monitoring and Reports サーバ ターゲットに送信されます。syslog プロトコルはセキュアでない UDP プロトコルです。

ログ メッセージは、ローカル ストア syslog メッセージ フォーマット（表 19-2 を参照）に先行する syslog メッセージ ヘッダー フォーマット（表 19-3 を参照）で Monitoring and Reports サーバに送信されます。

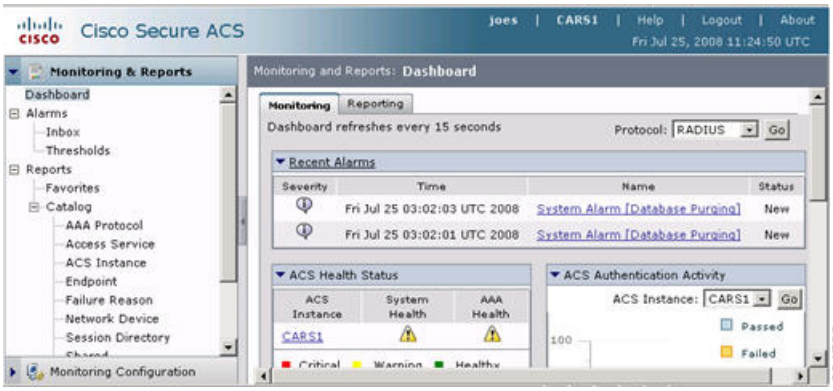
Monitoring and Reports サーバは、重大なログ ターゲットとして機能できません。重大なログ ターゲットの詳細については、重大なログ ターゲット（19-7 ページ）を参照してください。

ログ メッセージの表示

Web インターフェイスと CLI を使用すると、ローカルに格納されているログ メッセージを表示できます。リモート syslog サーバに送信されたログ メッセージは、Web インターフェイスまたは CLI で表示できません。

Web インターフェイスで、[Monitoring and Reports] > [Launch Monitoring and Report Viewer] を選択して、セカンダリ ウィンドウに Monitoring and Reports Viewer を開きます（図 19-1を参照）。CLI を使用したログ メッセージの表示の詳細については、『*Command Line Interface Reference Guide for Cisco Secure Access Control System 5.4*』を参照してください。

図 19-1　　Monitoring and Reports Viewer



Monitoring and Report Viewer には、次の 2 つのドロワ オプションがあります。

- Monitoring and Reports：このドロワを使用して、アラームの表示と設定、ログ レポートの表示、およびトラブルシューティング タスクを実行します。
- Monitoring Configuration：このドロワを使用して、ロギング操作とシステム設定を表示および設定します。

ロギング カテゴリ（19-2 ページ）で説明したログ メッセージで取り込まれる情報に加えて、ビューア レポートには、成功および失敗した AAA 認証試行が Step 属性とともにリストされます。Step 属性では、同じセッションで発生した他のイベントに関する情報が提供されます。この情報によって、認証の成功または失敗の原因となった手順の順序を確認できます。

ビューアは、次の用途に使用できます。

- アラーム、レポート、およびトラブルシューティング情報の管理
- データの削除、ログの収集、ジョブのスケジューリング、ステータスの監視など、システム操作の管理
- 失敗理由の編集、電子メール、セッション ディレクトリ、アラーム設定の設定など、システム設定の管理

詳細については、ACS での監視とレポート（11-1 ページ）を参照してください。

デバッグ ログ

トラブルシューティングのサポートを受ける必要がある場合は、Web インターフェイスと CLI を使用して、デバッグ ログなどのログをシスコのテクニカル サポート担当者に送信できます。Web インターフェイスで、[Monitoring and Reports] > [Launch Monitoring and Report Viewer] > [Monitoring and Reports] > [Troubleshooting] > [ACS Support Bundle] を選択します。

CLI を使用して、Application Deployment Engine-OS 1.2 環境ログ内のハードウェア サーバを表示およびエクスポートすることもできます。これらのメッセージは */var/log/boot.log* だけに送信され、CLI が ACS デバッグ ログ メッセージを表示またはエクスポートする方法には関連しません。詳細については、『*Command Line Interface Reference Guide for Cisco Secure Access Control System 5.4*』を参照してください。

ACS 4.x と ACS 5.4 のロギング

ACS 4.x のロギング機能に精通している場合は、かなり異なる ACS 5.4 のロギング機能にも慣れてください。表 19-4に、ACS 4.x と ACS 5.4 のロギング機能の違いを示します。

表 19-4　　ACS 4.x と ACS 5.4 のロギング機能の対比

ログ機能	ACS 4.x での処理	ACS 5.4 での処理
ログ タイプ	• AAA 関連ログには、ユーザによるリモート アクセス サービスの利用に関する情報が格納される。 • 監査ログには ACS システムとアクティビティに関する情報が含まれるため、システム関連イベントも記録される。 システム ログは、トラブルシューティングや監査に役立ちます。CSV 監査ログは常にイネーブルであり、他のロガーに対して監査ログをイネーブルまたはディセーブルにできます。監査ログの内容は設定できません。 監査ログでは、管理者が各ユーザに対して行った実際の変更を表示できます。ACS 監査ログには、特定のユーザに対して変更されたすべての属性がリストされます。	ロギング カテゴリ（19-2 ページ）を参照してください。
使用可能なログ ターゲット	• CSV ロガー • Syslog ロガー • ODBC ロガー • リモート ロギング	リモート Syslog サーバ ターゲット（19-8 ページ）およびローカル ストア ターゲット（19-5 ページ）を参照してください。
ログ ファイルの場所	• CSVロガー： *sysdrive*`:\Program Files\CiscoSecure ACS v`*x.x.*	• ローカル ストア ターゲット ログ：*/opt/CSCOacs/logs/localStore/*。 • リモート syslog サーバ ターゲット ログ：*/var/log/messages*。

表 19-4　ACS 4.x と ACS 5.4 のロギング機能の対比 （続き）

ログ機能	ACS 4.x での処理	ACS 5.4 での処理
レポート タイプ	• CSV • ダイナミック管理 • 権限付与	ACS での監視とレポート（11-1 ページ）を参照してください。
エラー コードとメッセージ テキスト	ACS 4.2 では、CSAuth 診断ログにクライアント要求および応答の説明が表示されます。旧バージョンの ACS では、クライアント要求および応答に数値コードが使用されていました。	すべてのメッセージ。ログ メッセージの表示（19-10 ページ）を参照してください。
設定（Configuration）	[System Configuration] > [Logging] ページを使用して、次の項目を定義します。 • ロガーと個々のログ • クリティカル ロガー • リモート ロギング • CSV ログ ファイル • Syslog ログ • ODBC ログ	ログの設定（18-21 ページ）および『*CLI Reference Guide for Cisco Secure Access Control System 5.4*』を参照してください。
ログ メッセージの表示とダウンロード	[Reports and Activity] ページを使用します。	ログ メッセージの表示（19-10 ページ）を参照してください。
ログ メッセージを使用したトラブルシューティング	サービス ログ ファイルは、該当するサービス ディレクトリの *\Logs* サブディレクトリにあります。	デバッグ ログ（19-11 ページ）を参照してください。