ロギング メカニズム

Cisco ISE ロギング メカニズム

Cisco ISE には、監査、障害管理、およびトラブルシューティングに使用されるロギング メカニズムが備わっています。このロギング メカニズムは、展開されたサービスの障害状態を識別したり、問題のトラブルシューティングを効率的に行う場合に役立ちます。また、プライマリ ノードのモニタリングおよびトラブルシューティングのロギング出力が一貫した形式で生成されます。

仮想ループバック アドレスを使用してローカル システムにログを収集するように Cisco ISE ノードを設定できます。ログを外部に収集するには、ターゲットと呼ばれる外部 syslog サーバを設定します。ログは事前定義された各種のカテゴリに分類されます。ターゲット、重大度レベルなどに応じてカテゴリを編集することにより、ロギング出力をカスタマイズできます。

（注） モニタリング ノードがネットワーク デバイスの syslog サーバとして設定されている場合、ロギング ソースが次の形式で正しいネットワーク アクセス サーバ（NAS）の IP アドレスを送信することを確認してください。
<message_number>sequence_number: NAS_IP_address: timestamp: syslog_type: <message_text>
そうしないと、これは NAS の IP アドレスに依存する機能に影響を及ぼすことがあります。

ローカル ログの消去の設定

このプロセスを使用して、ローカル ログ格納期間を設定し、特定の期間後にローカル ログを削除します。

ステップ 1 [管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ローカル ログ設定（Local Log Settings）] を選択します。

ステップ 2 [ローカル ログ格納期間（Local Log Storage Period）] フィールドに、設定ソースでログ エントリを保持する最大日数を入力します。

ステップ 3 格納期間が経過する前に既存のログ ファイルを削除するには、[今すぐログを削除（Delete Logs Now）] をクリックします。

ステップ 4 [保存（Save）] をクリックします。

Cisco ISE システム ログ

Cisco ISE では、システム ログはロギング ターゲットと呼ばれる場所で収集されます。ターゲットは、ログを収集して格納するサーバの IP アドレスを参照します。ログをローカルで生成して格納することも、FTP ファシリティを使用して外部サーバに転送することもできます。Cisco ISE には、次のデフォルト ターゲットがあり、これらはローカル システムのループバック アドレスに動的に設定されます。

- LogCollector：ログ コレクタのデフォルトの syslog ターゲット。
- ProfilerRadiusProbe：プロファイラ Radius プローブのデフォルトの syslog ターゲット。

デフォルトでは、AAA 診断サブカテゴリとシステム診断サブカテゴリのロギング ターゲットは、ディスク領域を減らすために、新規 Cisco ISE インストールまたはアップグレード時に無効になります。これらのサブカテゴリのロギング ターゲットを手動で設定できますが、これらのサブカテゴリのローカル ロギングは常に有効です。

Cisco ISE インストールの最後にローカルに設定されるデフォルトのロギング ターゲットを使用するか、またはログを保存する外部ターゲットを作成することができます。

（注） syslog サーバが分散展開で設定されている場合、syslog メッセージは MnT ノードではなく認証 PSN から syslog サーバへ直接送信されます。

関連トピック

Cisco ISE メッセージ コード, （8 ページ）

ローカル ストア syslog メッセージの形式

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。

timestamp sequence_num msg_ode msg_sev msg_class msg_text attr =value

フィールド	説明
timestamp	次の形式での、生成元の Cisco ISE ノードのローカル クロックに従ったメッセージ生成の日付。 *YYYY- MM-DD hh:mm:ss:xxx +/-zh:zm* 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。 • +/-zh:zm = Cisco ISE 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、Cisco ISE サーバのタイム ゾーンよりも 2 時間先行する Cisco ISE ノードでメッセージが発生したことを示します。

フィールド	説明
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_ode	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。[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギング カテゴリ（Logging Categories）] を参照してください。
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。
msg_text	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 Cisco ISE 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。 例： Response={RadiusPacketType=AccessAccept; AuthenticationResult=UnknownUser; cisco-av-pair=sga:security-group-tag=0000-00;}

リモート syslog メッセージの形式

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。

メッセージは、イベントが発生したときに生成されます。イベントは、プログラムの終了時に表示されるメッセージやアラームなどのステータスを表示するものである場合があります。カーネル、メール、ユーザ レベルなど、異なるファシリティから生成されたさまざまなタイプのイベントメッセージがあります。イベントメッセージは重大度レベルに関連付けられており、管理者はメッセージをフィルタリングし、優先度付けできます。数値コードはファシリティおよび重大度レベルに割り当てられます。Syslog サーバはイベント メッセージ コレクタで、これらのファシリティからイベント メッセージを収集します。管理者は、重大度レベルに基づいて、メッセージを転送するイベント メッセージ コレクタを選択できます。Cisco ISE の重大度レベルについては、「ロギング カテゴリの設定」の項を参照してください。

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

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。セキュリティ レベルについては、「メッセージ コードの重大度レベルの設定」を参照してください。 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）

フィールド	説明
時刻	生成元の Cisco ISE サーバのローカル クロックに従った、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、Cisco ISE 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、Cisco ISE サーバのタイムゾーンよりも 2 時間先行する Cisco ISE 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	発信元の Cisco ISE ノードの IP アドレスまたはホスト名。
cat_name	先頭に CSCOxxx 文字列が付いたロギング カテゴリ名。

フィールド	説明
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。 （注） *total_seg* は、[リモート ロギング ターゲット（Remote Logging Targets）] ページの [最大長（Maximum Length）] 設定によって異なります。「リモートロギング ターゲットの設定」を参照してください。
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、ローカル ストア syslog メッセージの形式と同じです。リモート syslog サーバ ターゲットは、ファシリティ コード名 LOCAL0 ～ LOCAL7 によって識別されます（LOCAL6 がデフォルトのロギング ロケーションです）。リモート syslog サーバに割り当てるログ メッセージは、Linux syslog のデフォルトの場所（/var/log/messages）に送信されますが、サーバで別の場所を設定できます。

リモート syslog 収集場所の設定

syslog を保存する外部の場所を作成できます。

UDP syslog（ログ コレクタ）はデフォルトのリモート ロギング ターゲットです。このロギング ターゲットは、無効にすると、ログ コレクタとして動作しなくなり、[ロギング カテゴリ（Logging

Categories）]ページから削除されます。このロギング ターゲットを有効にした場合は、[ロギング カテゴリ（Logging Categories）] ページのログ コレクタになります。

ステップ 1 [管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [リモート ロギング ターゲット（Remote Logging Targets）] を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 必要に応じてフィールドを設定します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 [リモート ロギング ターゲット（Remote Logging Targets）] ページに移動し、新しいターゲットが作成されたことを確認します。
ロギング ターゲット ページで syslog の格納場所を作成したら、ログを受信するために、必要なロギング カテゴリに格納場所をマッピングする必要があります。

Cisco ISE メッセージ コード

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。Cisco ISE では、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 カテゴリはロギング設定で役立ちます。各カテゴリには、アプリケーションの要件に応じて設定可能な名前、ターゲット、および重大度レベルがあります。

Cisco ISE では、サービスに対して事前定義されたロギング カテゴリ（[ポスチャ（Posture）]、[プロファイラ（Profiler）]、[ゲスト（Guest）]、[AAA（認証、許可、アカウンティング）（AAA (authentication, authorization, and accounting)）] など）が提供されており、これらにログ ターゲットを割り当てることができます。

メッセージ コードの重大度レベルの設定

ログの重大度レベルを設定し、選択したカテゴリのログが格納されるロギング ターゲットを選択できます。

ステップ 1 [管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギング カテゴリ（Logging Categories）] を選択します。

ステップ 2 編集するカテゴリの隣のオプション ボタンをクリックにして、[編集（Edit）] をクリックします。

ステップ 3 必須フィールドの値を変更します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 [ロギング カテゴリ（Logging Categories）] ページに移動し、特定のカテゴリに対して行われた設定の変更内容を確認します。

Cisco ISE メッセージ カタログ

可能性があるすべてのログ メッセージと説明を表示するために、[メッセージ カタログ（Message Catalog）] ページを使用できます。[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [メッセージ カタログ（Message Catalog）] を選択します。

[ログ メッセージ カタログ（Log Message Catalog）] ページが表示されます。このページでは、ログ ファイルに記録される可能性があるすべてのログ メッセージを表示できます。すべての Syslog メッセージを CSV ファイル形式でエクスポートするには、[エクスポート（Export）] を選択します。

デバッグ ログ

デバッグ ログにより、ブートストラップ、アプリケーション設定、ランタイム、展開、モニタリングとレポート、および公開キー インフラストラクチャ（PKI）に関する情報が取得されます。過去 30 日間の重大アラームと警告アラーム、および過去 7 日間の情報アラームがデバッグ ログに含まれます。

個々のコンポーネントのデバッグ ログ重大度レベルを設定できます。

ノードまたはコンポーネントで [デフォルトにリセット（Reset to Default）] オプションを使用して、ログ レベルを出荷時のデフォルト値に戻すことができます。

ローカル サーバにデバッグ ログを保存できます。

（注） デバッグ ログの設定は、システムをバックアップから復元した場合やアップグレードした場合には保存されません。

ノードのロギング コンポーネントの表示

ステップ 1 [管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [デバッグ ログ設定（Debug Log Configuration）] を選択します。

ステップ 2 ロギング コンポーネントを表示するノードを選択し、[編集（Edit）] をクリックします。
[デバッグ レベルの設定（Debug Level Configuration）] ページが表示されます。次の詳細情報を表示できます。

- 選択したノードで実行中のサービスに基づくロギング コンポーネントのリスト
- 各コンポーネントの説明
- 個々のコンポーネントに設定されている現在のログ レベル

デバッグ ログの重大度レベルの設定

デバッグ ログの重大度レベルを設定できます。

ステップ 1 [管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [デバッグ ログの設定（Debug Log Configuration）] を選択します。

ステップ 2 ノードを選択して、[編集（Edit）] をクリックします。
[デバッグログの設定（Debug Log Configuration）] ページには、選択したノードで実行されているサービス、および個別のコンポーネントに対して設定されている現在のログ レベルに基づいたコンポーネントのリストが表示されます。

ノードまたはコンポーネントで [デフォルトにリセット（Reset to Default）] オプションを使用して、ログ レベルを出荷時のデフォルト値に戻すことができます。

ステップ 3 ログ重大度レベルを設定するコンポーネントを選択し、[編集（Edit）] をクリックします。[ログレベル（Log Level）] ドロップダウン リストから目的のログ重大度レベルを選択し、[保存（Save）] をクリックします。

（注） runtime-AAA コンポーネントのログ重大度レベルを変更すると、サブコンポーネント prrt-JNI のログ レベルも変更されます。サブコンポーネントのログ レベルを変更しても、その親コンポーネントには影響はありません。

エンドポイントのデバッグ ログ コレクタ

特定のエンドポイントの問題をトラブルシューティングするために、IP アドレスまたは MAC アドレスに基づいて、特定のエンドポイントのデバッグ ログをダウンロードできます。その特定のエンドポイント固有のログが、展開内のさまざまなノードから 1 つのファイルに収集されるため、迅速かつ効率的に問題をトラブルシューティングできます。このトラブルシューティング ツールは、一度に 1 つのエンドポイントに対してのみ実行できます。ログ ファイルが GUI に表示されます。1 つのノードまたは展開内のすべてのノードからエンドポイントのログをダウンロードできます。

特定のエンドポイントのデバッグ ログのダウンロード

ネットワーク内の特定のエンドポイントの問題をトラブルシューティングするには、管理者ポータルからデバッグ エンドポイント ツールを使用できます。または、このツールを [認証（Authentications）] ページから実行できます。[認証（Authentications）] ページの [エンドポイント ID（Endpoint ID）] を右クリックして、[エンドポイント デバッグ（Endpoint Debug）] をクリックします。このツールでは、単一ファイルの特定のエンドポイントに関連するすべてのサービスに関するすべてのデバッグ情報が提供されます。

はじめる前に

デバッグ ログを収集するエンドポイントの IP アドレスまたは MAC アドレスが必要です。

ステップ 1 [操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [エンドポイント デバッグ（Endpoint Debug）] を選択します。

ステップ 2 [MAC アドレス（MAC Address）] または [IP] オプション ボタンをクリックし、エンドポイントの MAC または IP アドレスを入力します。

ステップ 3 一定の時間が経過した後にログ収集を停止する場合は、[*n* 分後に自動的に無効化（Automatic disable after n Minutes）] チェックボックスをオンにします。このチェックボックスをオンにする場合は、1 ～ 60 分の時間を入力する必要があります。
次のメッセージが表示されます。「エンドポイントデバッグによって、展開のパフォーマンスが低下します。続行しますか?（Endpoint Debug degrades the deployment performance.Would you like to continue?）」

ステップ 4 ログを収集するには、[続行（Continue）] をクリックします。

ステップ 5 手動でログの収集を中止する場合は、[停止（Stop）] をクリックします。

収集フィルタ

収集フィルタを設定して、モニタリング サーバおよび外部サーバに送信される syslog メッセージを抑制できます。抑制は、異なる属性タイプに基づいてポリシー サービス ノード レベルで実行できます。特定の属性タイプおよび対応する値を使用して複数のフィルタを定義できます。

モニタリング ノードまたは外部サーバに syslog メッセージを送信する前に、Cisco ISE は送信する syslog メッセージのフィールドとそれらの値を比較します。一致が見つかった場合、対応するメッセージは送信されません。

収集フィルタの設定

さまざまな属性のタイプに基づいて複数の収集フィルタを設定できます。フィルタ数を 20 に制限することを推奨します。収集フィルタを追加、編集、または削除できます。

ステップ 1 [管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [収集フィルタ（Collection Filters）] を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 次のリストからフィルタ タイプを選択します。

- ユーザ名（User Name）
- MAC アドレス（MAC Address）
- ポリシー セット名（Policy Set Name）
- NAS IP アドレス
- Device IP Address（デバイス IP アドレス）

ステップ 4 選択したフィルタ タイプの対応する値を入力します。

ステップ 5 ドロップダウン リストから結果を選択します。結果は、[すべて（All）]、[成功（Passed）]、または [失敗（Failed）] になります。

ステップ 6 [送信（Submit）] をクリックします。

イベント抑制バイパス フィルタ

Cisco ISE では、フィルタを設定し、収集フィルタを使用して、一部の syslog メッセージがモニタリング ノードおよび他の外部サーバに送信されることを抑制できます。場合によっては、これらの抑制されたログ メッセージにアクセスすることが必要になります。Cisco ISE は、設定可能な時間について、ユーザ名などの属性に基づいてイベント抑制をバイパスするオプションを提供します。デフォルトは 50 分ですが、5 分から 480 分（8 時間）の期間を設定できます。イベント抑制バイパスは、設定した後すぐに有効になります。設定した期間が経過すると、バイパス抑制フィルタは失効します。

抑制バイパス フィルタは、Cisco ISE ユーザ インターフェイスの [収集フィルタ（Collection Filters）] ページから設定できます。この機能を使用して、特定の ID（ユーザ）のすべてのログを表示し、その ID の問題をリアルタイムでトラブルシューティングできます。

フィルタは有効または無効にできます。バイパス イベント フィルタで設定した期間が経過すると、フィルタは再度有効にするまで自動的に無効になります。

Cisco ISE は設定変更監査レポートでこれらの設定変更を取得します。このレポートは、イベント抑制またはバイパス抑制を設定したユーザ、およびイベントが抑制された期間または抑制がバイパスされた期間に関する情報を提供します。