ロギング

この章では、Cisco Identity Services Engine（ISE）に実装されているロギング メカニズムについて説明します。また、ロギング ターゲットの設定、ロギング カテゴリの編集、ロギング設定を行う手順についても説明します。この章の構成は、次のとおりです。

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。Cisco ISE メッセージ コードで説明するように、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。

Cisco ISE で次のロギング関連タスクを実行できます。

- ローカル ログ設定を行うには、「ローカル ログ消去の設定」（P.11-2）を参照してください。
- リモート ロギング ターゲットについて理解し、それを作成するには、「Cisco ISE システム ログ」（P.11-2）を参照してください。
- ロギング カテゴリについて理解し、それを編集するには、「Cisco ISE メッセージ コード」（P.11-3）を参照してください。
- メッセージ カタログを表示するには、「Cisco ISE メッセージ カタログ」（P.11-4）を参照してください。
- デバッグ ログについて理解し、それを設定するには、「デバッグ ログ設定オプション」（P.11-4）を参照してください。

ローカル ログ消去の設定

ローカル ログ格納期間を設定したり、一定の時間が経過した後にローカル ログを削除するには、このプロセスを使用します。

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、設定ソースにログ エントリを保存しておく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グギング 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。

関連項目

「リモート Syslog 収集場所の設定」（P.11-2）

リモート Syslog 収集場所の設定

syslog を保存する外部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。このログ ターゲットを無効にすると、ログ コレクタとして機能しなくなり、[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すると、[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 の保管場所を作成したら、ログを受信するために、保管場所を必要なロギング カテゴリにマッピングする必要があります。

関連項目

- 「リモート ロギング ターゲットの設定」（P.A-15）

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。

カテゴリごとに関連するトラブルシューティング レポートの詳細については、「使用可能なレポート」（P.26-7）を参照してください。

関連項目

- 「メッセージ コードの重大度レベルの設定」（P.11-3）

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　必要なフィールド値を変更します。

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。

関連項目

「ロギング カテゴリの設定」（P.A-15）

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。このページで利用可能なデータは表示専用です。

デバッグ ログ設定オプション

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。

個々のコンポーネントに対してデバッグ ログの重大度レベルを設定し、デバッグ ログをローカル サーバに保存します。

（注） デバッグ ログ設定は、システムがバックアップから復元されたり、アップグレードされたりするときに保存されません。

関連項目

「デバッグ ログの重大度レベルの設定」（P.11-4）

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 ログ設定（Debug Log Configuration）] を選択します。[ノード リスト（Node List）] ページに、ノードとそのペルソナが表示されます。特にノード リストが大きい場合は、[フィルタ（Filter）] ボタンを使用して特定のノードを検索できます。

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 ログ設定（Debug Log Configuration）] ページが表示されます。このページには、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含まれています。

各ノードには、一連のコンポーネントが含まれます。

（注） [フィルタ（Filter）] ボタンを使用すると、このリストから特定のコンポーネントを検索できます。

ステップ 3　次のいずれかを実行して、ログ重大度レベルを調整します。

- コンポーネントの名前をクリックし、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てから、[保存（Save）] をクリックします。
- デバッグ ログの重大度レベルを設定するコンポーネントの名前を選択してから、[編集（Edit）] をクリックします。このページで、[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）] 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。

関連項目

- 「Cisco ISE のサポート バンドル」（P.25-26）
- 「Cisco ISE デバッグ ログ」（P.25-28）

収集フィルタ

Syslog メッセージをモニタリング サーバおよび外部サーバに送信することを抑制するには、収集フィルタを設定できます。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。抑制を無効にすることもできます。特定の属性タイプおよび対応する値が指定された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 は値を Syslog メッセージのフィールドと比較します。一致しているものが見つかった場合、対応するメッセージは送信されません。

関連項目

「収集フィルタの設定」（P.11-5）

収集フィルタの設定

さまざまな属性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。収集フィルタは、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　[属性（Attribute）] 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（NAS IP Address）

- デバイス IP アドレス（Device IP Address）
- 抑制の無効化（Disable Suppression）

ステップ 4　選択したフィルタ タイプに対応する**値**を入力します。

ステップ 5　[フィルタ基準（Filter By）] ドロップダウン リストから抑制をフィルタリングする基準である結果を選択します。結果に、All、Passed、または Failed を指定できます。[抑制の無効化（Disable Suppression）] を選択して、抑制を無効にすることもできます。

ステップ 6　[送信（Submit）] をクリックします。

関連項目

「収集フィルタ」（P.11-5）