ISEでの外部syslogサーバの設定

内容

はじめに

このドキュメントでは、ISEで外部syslogサーバを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Identity Services Engine(ISE)の略。
- syslog サーバ

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Identity Services Engine(ISE)3.3バージョン
- Kiwi Syslogサーバv1.2.1.4

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

.

ISEからのsyslogメッセージは、ログコレクタによって収集および保存されます。これらのログコレクタはモニタリングノードに割り当てられるため、MnTは収集されたログをローカルに保存します。

ログを外部から収集するには、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、事前定義されたさまざまなカテゴリに分類されます。

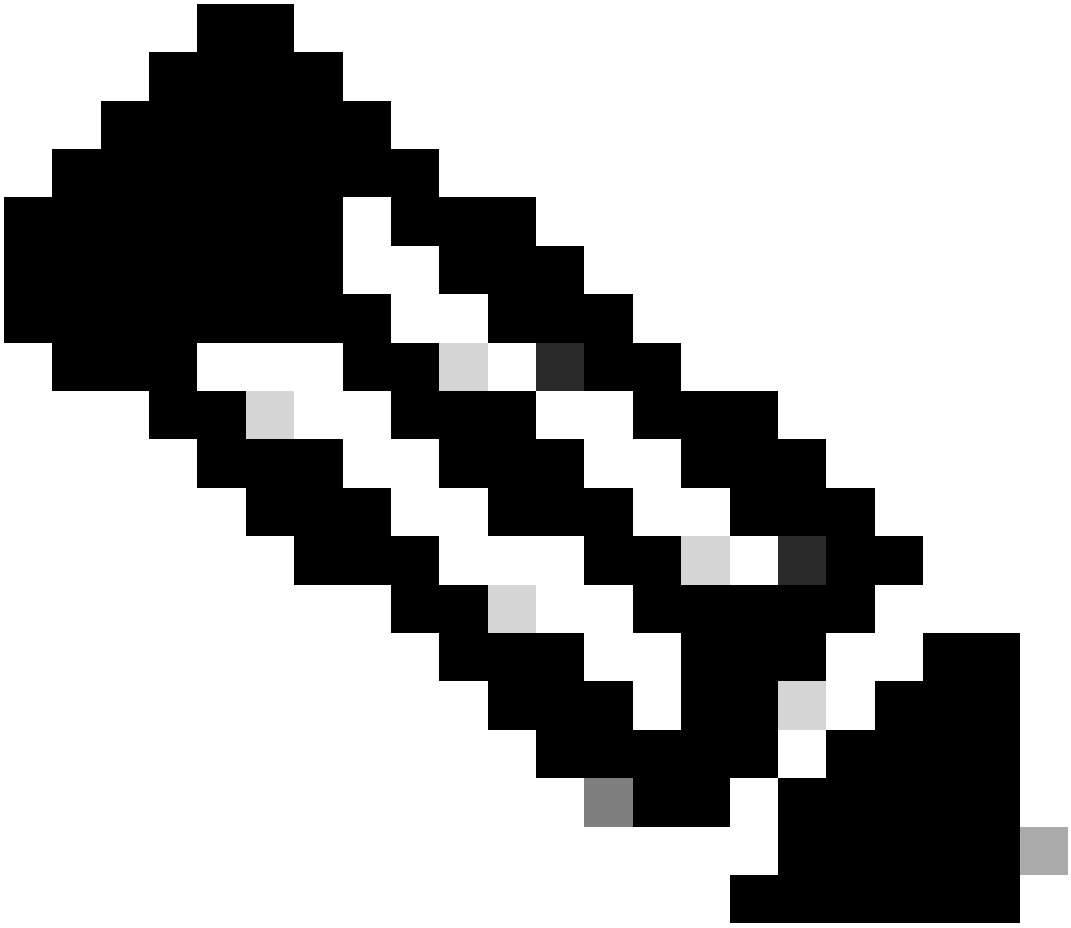
ロギング出力をカスタマイズするには、ターゲットや重大度などのカテゴリを編集します。

コンフィギュレーション

Webインターフェイスを使用して、システムログメッセージの送信先となるリモートsyslogサーバターゲットを作成できます。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。

リモートロギングターゲットの設定(UDP Syslog)

Cisco ISEのGUIで、メニューアイコン(
)、Administration>System>Logging>Remote Logging Targets>Addの順に選択します。



注：この設定例はConfiguring Remote Logging Targetという名前のスクリーンショットに基づいています。

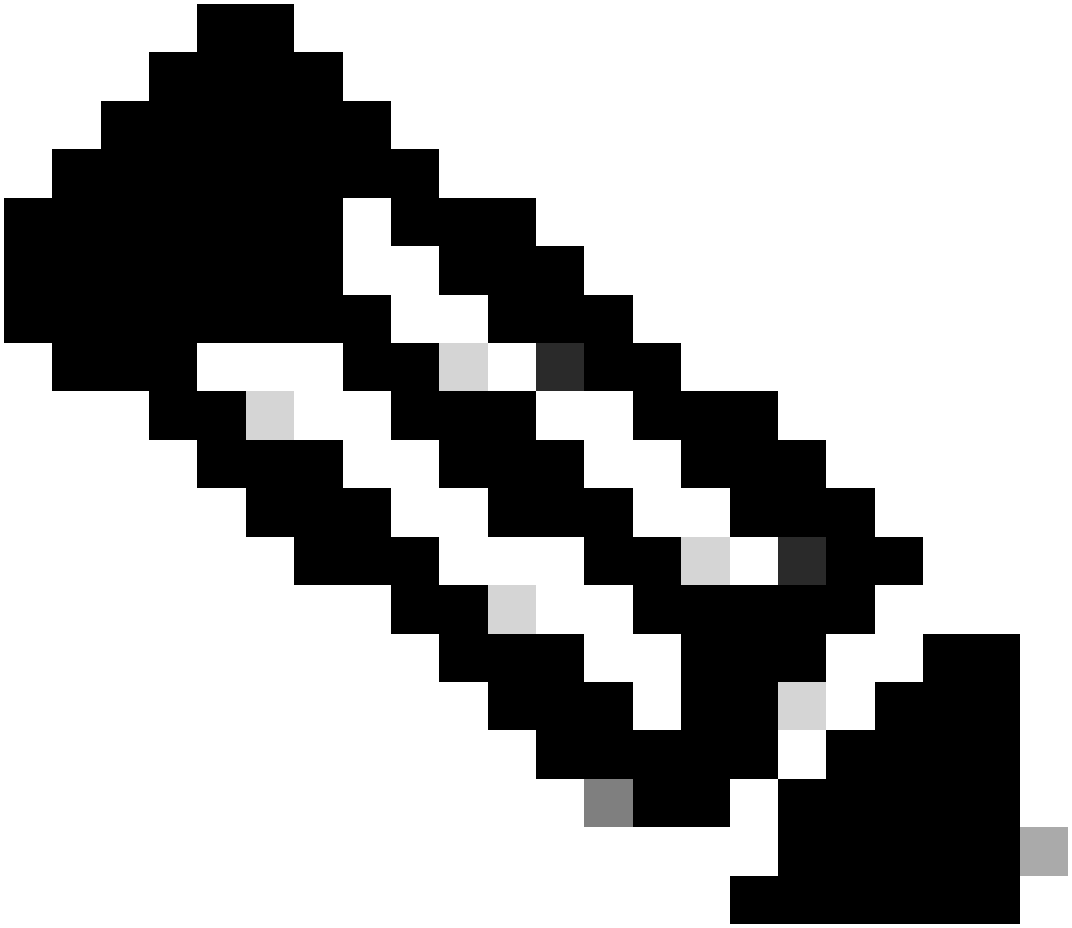
- Name as Remote_Kiwi_Syslog。ここではリモートSyslogサーバの名前を入力できます。これは説明のために使用されます。
- Target TypeをUDP Syslogとして設定した場合、この設定例ではUDP Syslogが使用されていますが、Target Typeドロップダウンリストからさらに多くのオプションを設定できます。

UDP syslog:UDP経由でsyslogメッセージを送信するために使用されます。軽量で高速な口ギングに適しています。

TCP syslog:TCP経由でsyslogメッセージを送信するために使用されます。これにより、エラーチェックと再送信機能で信頼性が確保されます。

セキュアSyslog:TLS暗号化を使用してTCP経由で送信されるsyslogメッセージを指し、データの整合性と機密性を確保します。

- StatusにEnabledを指定した場合は、Statusdrop-downリストからEnabledfromを選択する必要があります。
- 摘要。オプションで、新規ターゲットの簡単な摘要を入力できます。
- Host / IP Addressには、ログを保存する宛先サーバのIPアドレスまたはホスト名を入力します。Cisco ISEは、ロギングのIPv4およびIPv6形式をサポートします。



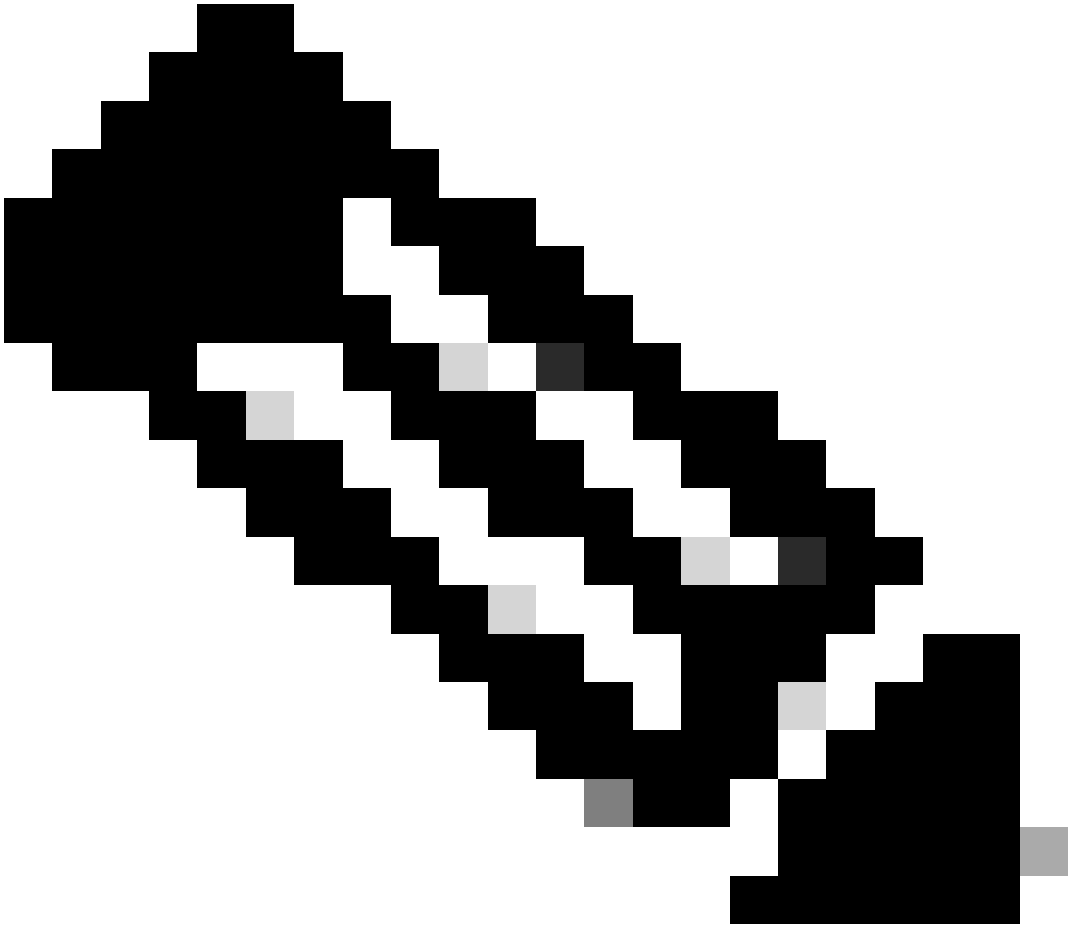
注:FQDNを使用してsyslogサーバを設定する場合は、パフォーマンスに影響を与えないようにDNSキャッシュを設定する必要があることに注意してください。DNSキャッシングを使用しない場合、ISEは、FQDNで設定されたリモートロギングターゲットにsyslogパケットを送信する必要があるたびにDNSサーバにクエリを送信します。これは、ISEのパフォーマンスに重大な影響を与えます。

これを解決するには、導入のすべてのPSNでservice cache enablecommandを使用します。

例

```
ise/admin(config)# service cache enable hosts ttl 180
```

- Port（デフォルト）に514を指定した場合、この設定例では、Kiwi Syslogサーバはポート514（UDP syslogメッセージのデフォルトポート）でリスニングを行います。 ただし、ユーザはこのポート番号を1 ~ 65535の任意の値に変更できます。目的のポートがファイアウォールによってブロックされていないことを確認してください。
- Facility CodeをLOCAL6に設定した場合は、ロギングに使用する必要のあるsyslogファシリティコードをドロップダウンリストから選択できます。有効なオプションはLocal0からLocal7です。
- Maximum Lengthに1024を指定した場合、リモートログターゲットメッセージの最大長を入力できます。 最大長は、デフォルトで1024に設定されており、ISE 3.3バージョンの値は200 ~ 8192バイトです。

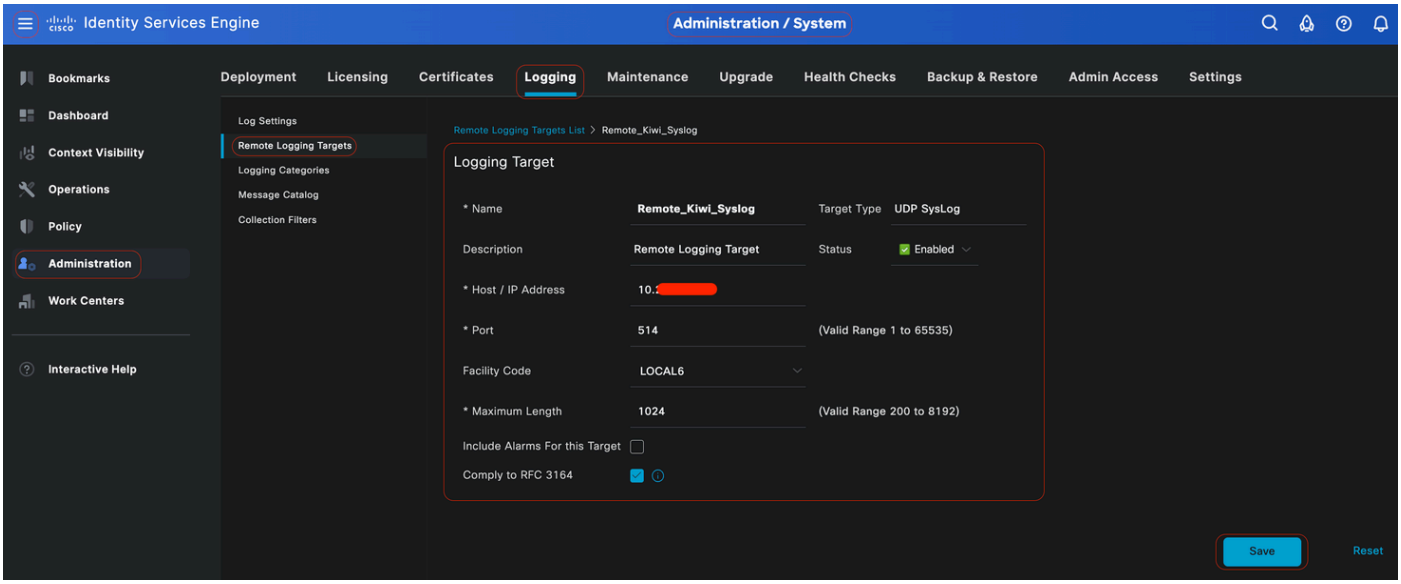


注：切り捨てられたメッセージがリモートターゲットに送信されないようにするには、最大長を8192に変更できます。

- アラームを含める:このターゲットについては、シンプルさを保つために、この設定例では「このターゲットのアラームを含める」はチェックされていません。ただし、このチェックボックスをチェックすると、アラームメッセージもリモートサーバに送信されます。
- Comply to RFC 3164 is checked」にチェックマークを付けると、このチェックボックスをオンにした場合、バックスラッシュ(\)を使用しても、リモートサーバに送信されるsyslogメッセージ内の区切り記号(、;{}\ \)はエスケープされません。

- 設定が終了したら、Saveをクリックします。

- 保存すると、サーバへのセキュアでない(TCP/UDP)接続を作成することを選択したという警告が表示されます。続行しますか？、[はい]をクリックしてください。



リモート・ターゲットの構成

ロギング・カテゴリでのリモート・ターゲットの構成

Cisco ISEは監査可能なイベントをsyslogターゲットに送信します。リモートロギングターゲットを設定したら、次に、リモートロギングターゲットを目的のカテゴリにマッピングして、監査可能なイベントを転送する必要があります。

その後、ロギングターゲットをこれらのロギングカテゴリのそれぞれにマッピングできます。 次のログカテゴリからのイベントログはPSNノードからのみ生成され、これらのノードで有効になっているサービスに応じて、関連するログをリモートsyslogサーバに送信するように設定できます。

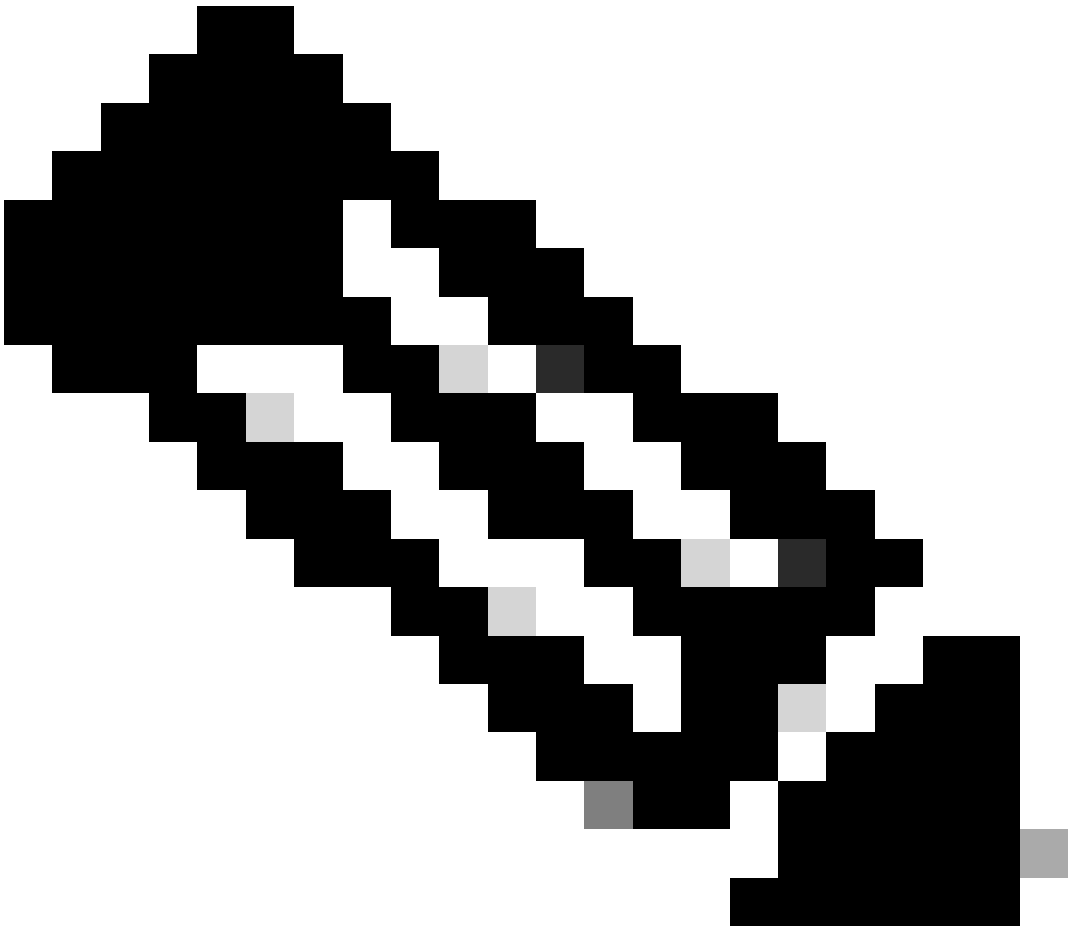
- AAA監査
- AAA診断
- アカウンティング
- 外部MDM
- パッシブID

- ポスチャとクライアントプロビジョニングの監査
- ポスチャとクライアントプロビジョニングの診断
- プロファイラ

次のログカテゴリからのイベントログは、展開のすべてのノードから生成され、関連するログをリモートsyslogサーバに送信するように設定できます。

- 管理監査および運用監査
- システム診断
- システム統計情報

この設定例では、4つのロギングカテゴリ(認証に成功した場合、認証に失敗した場合、認証に失敗した場合、およびRADIUSアカウンティング)でリモートターゲットを設定して認証トラフィックログを送信し、ISE管理者ロギングトラフィックに対して次のカテゴリを設定します。



注：この設定例は「リモートロギングターゲットの設定」というスクリーンショットに基づいています。

Cisco ISEのGUIで、メニューアイコン(Administration> System> Logging> Logging Categoriesの順に選択し、必要なカテゴリ(Passed authentications、Failed AttemptsおよびRadius Accounting)をクリックします。

ステップ1:ログの重大度レベル：イベントメッセージは重大度レベルに関連付けられます。これにより、管理者はメッセージをフィルタリングして優先順位を付けることができます。 必要に応じて、ログの重大度レベルを選択します。 一部のロギングカテゴリでは、この値はデフォルトで設定され、編集できません。一部のロギングカテゴリでは、ドロップダウンリストから次のいずれかの重大度レベルを選択できます。

- FATAL：緊急レベル。このレベルは、Cisco ISEを使用できないことを意味し、すぐに必要なアクションを実行する必要があります。
- エラー：このレベルは重大なエラー状態を示しています。
- WARN：このレベルは、正常であるが重要な状態を示しています。これは、多くのロギングカテゴリに対して設定されるデフォルトレベルです。
- INFO：このレベルは情報メッセージを示します。
- DEBUG：このレベルは、診断バグメッセージを示します。

ステップ2:ローカルロギング：このチェックボックスでローカルログの生成を有効にします。つまり、PSNによって生成されたログは、ログを生成する特定のPSNにも保存されます。デフォルト設定を維持することを推奨します

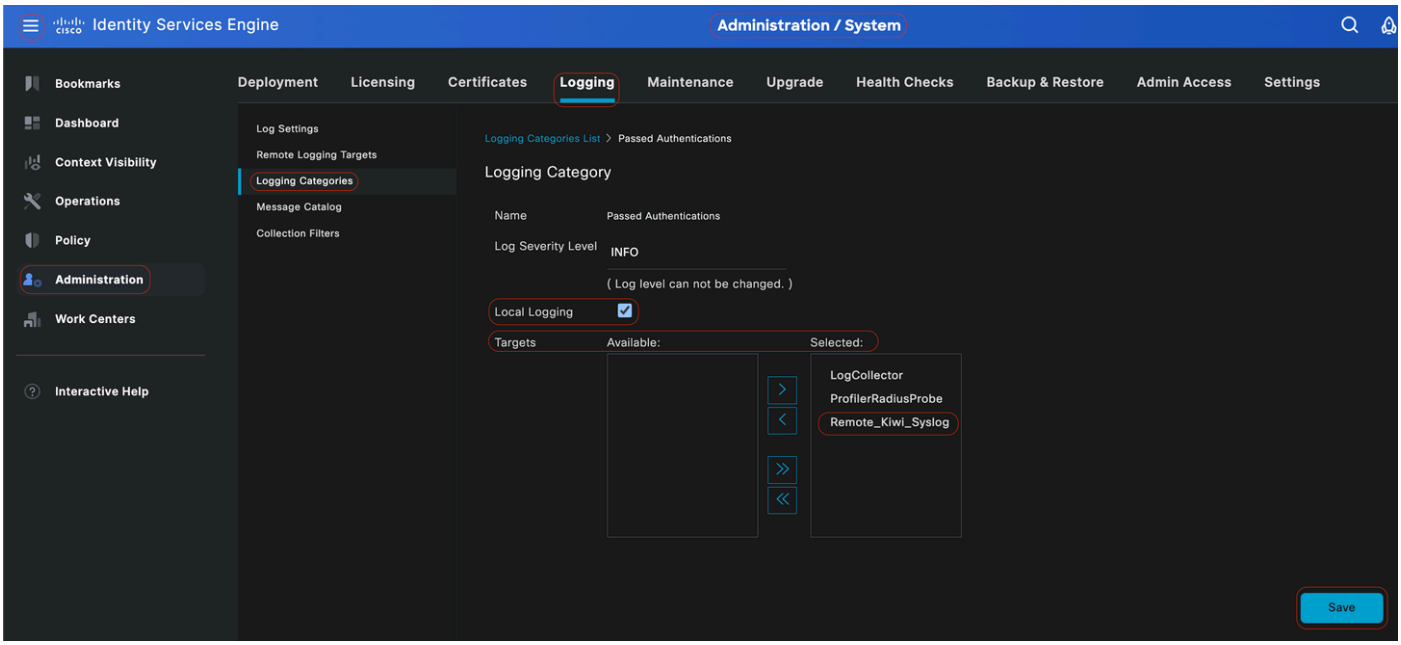
ステップ3- Targets:このエリアでは、左矢印および右矢印アイコンを使用してAvailableとSelectedareasの間でターゲットを転送することにより、ロギングカテゴリのターゲットを選択できます。

Availableareaには、既存のロギングターゲット(ローカル（事前定義）と外部（ユーザ定義）の両

方)が含まれています。

最初は空のSelectedareaには、カテゴリに対して選択されたターゲットが表示されます。

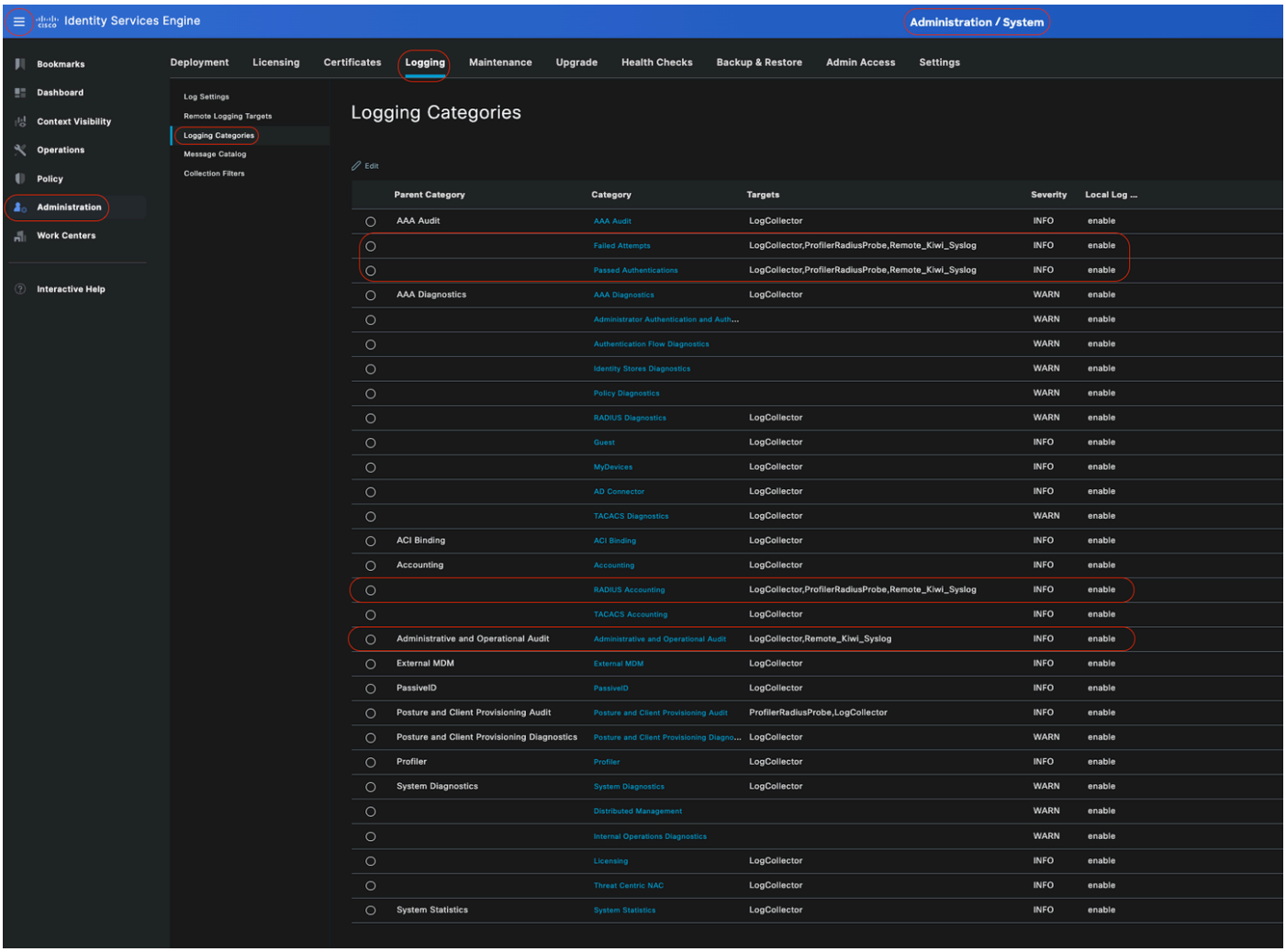
ステップ4:ステップ1からステップ3までを繰り返し、「Failed Attempts and Radius Accounting categories」の下に「Remote Target」を追加します。



目的のカテゴリへのリモートターゲットのマッピング

ステップ5:リモートターゲットが必要なカテゴリの下にあることを確認します。追加したリモートターゲットが表示されている必要があります。

このスクリーンショットでは、リモートターゲットRemote_Kiwi_Syslogが必要なカテゴリにマッピングされていることがわかります。



カテゴリの確認

カテゴリについて

イベントが発生すると、メッセージが生成されます。カーネル、メール、ユーザレベルなど、複数のファシリティから生成されるイベントメッセージには、さまざまなタイプがあります。

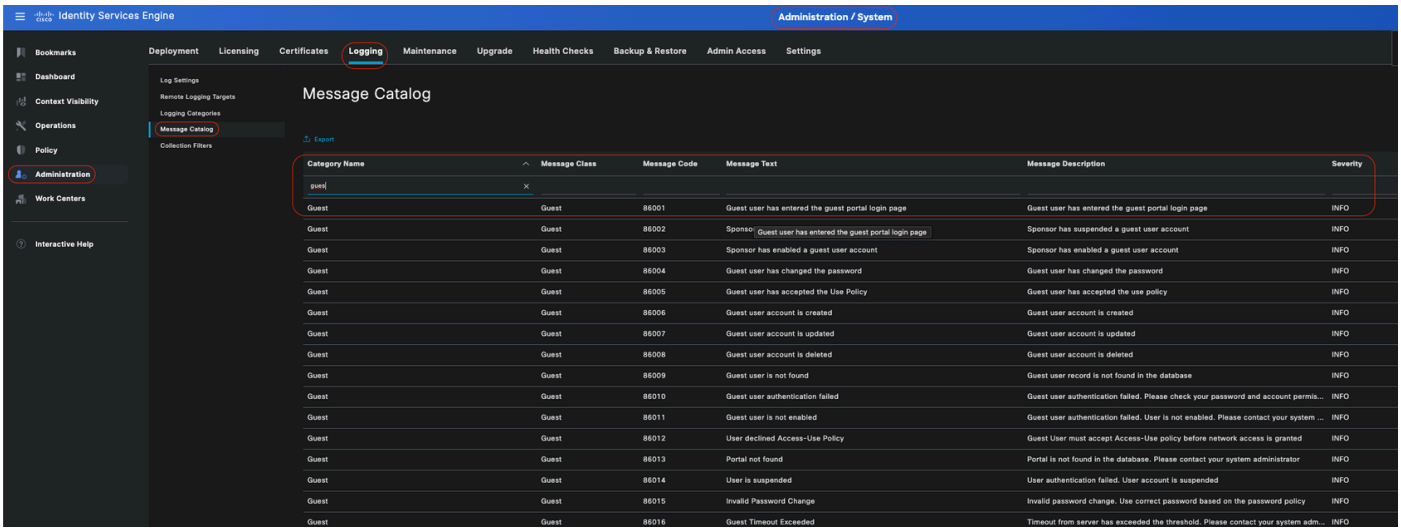
これらのエラーはメッセージカタログ内で分類され、これらのイベントも階層構造でカテゴリに分類されます。

これらのカテゴリには、1つまたは複数のカテゴリを含む親カテゴリがあります。

親カテゴリ	[Category]
AAA監査	AAA監査 失敗した試行（Failed Attempts） 成功した認証
AAA診断	AAA診断

	管理者の認証と許可 認証フロー診断 IDストア診断 ポリシー診断 Radius診断 ゲスト
アカウンティング	アカウンティング RADIUS アカウンティング
管理監査および運用監査	管理監査および運用監査
ポスチャとクライアントプロビジョニングの監査	ポスチャとクライアントプロビジョニングの監査
ポスチャとクライアントプロビジョニングの診断	ポスチャとクライアントプロビジョニングの診断
プロファイラ	プロファイラ
システム診断	システム診断 分散管理 内部運用診断
システム統計情報	システム統計情報

このスクリーンショットでは、Guestがメッセージクラスであり、ゲストカテゴリとして分類されていることがわかります。 このゲストカテゴリには、AAA Diagnosticsという親カテゴリがあります。



メッセージカタログ

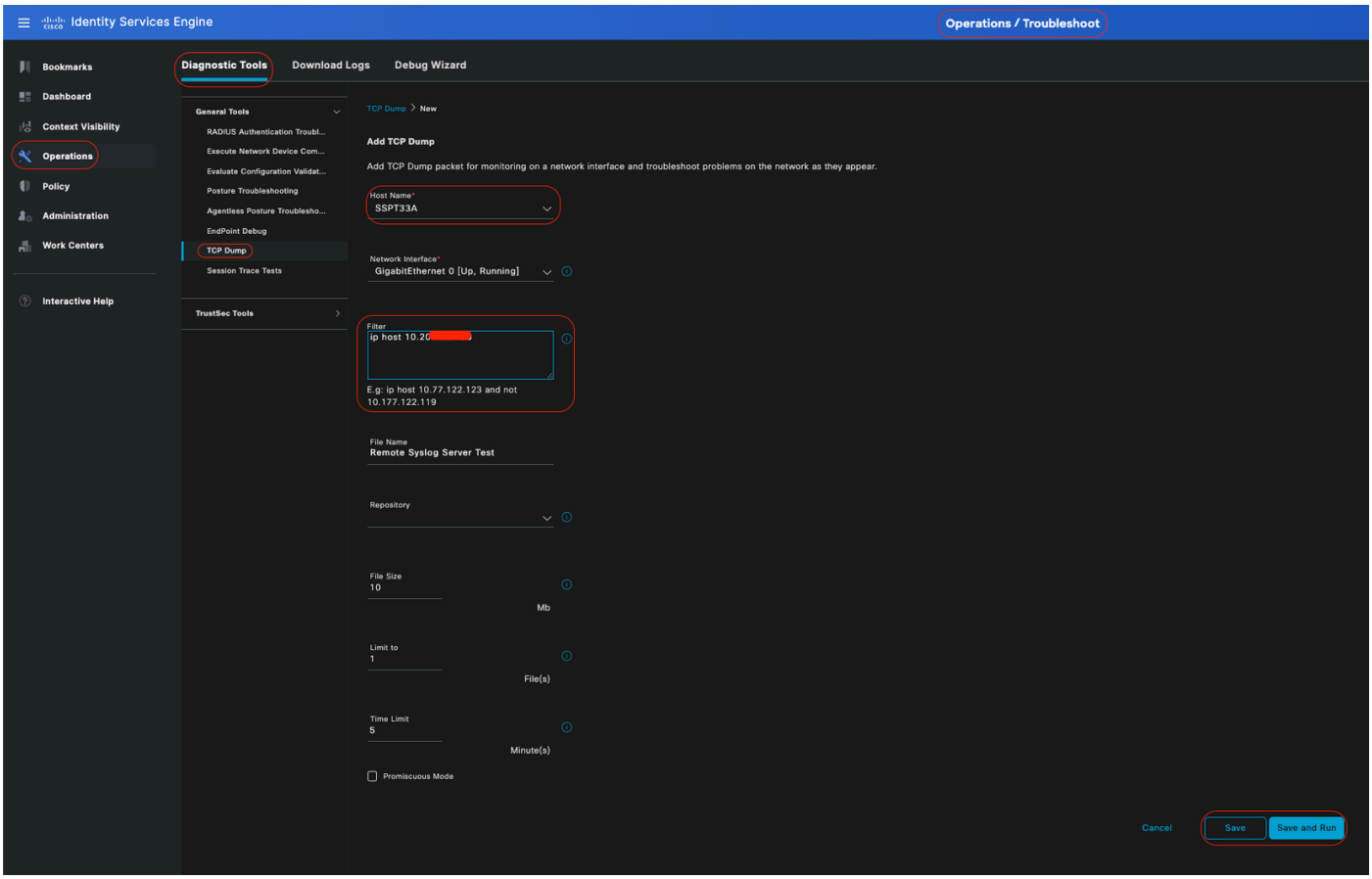
確認とトラブルシューティング

リモートロギングターゲットに対してTCPダンプを作成することは、ログイベントが送信されているかどうかを確認するための最も迅速なトラブルシューティングおよび確認の手順です。

PSNはログメッセージを生成し、これらのメッセージはリモートターゲットに送信されるため、ユーザを認証するPSNからキャプチャを取得する必要があります

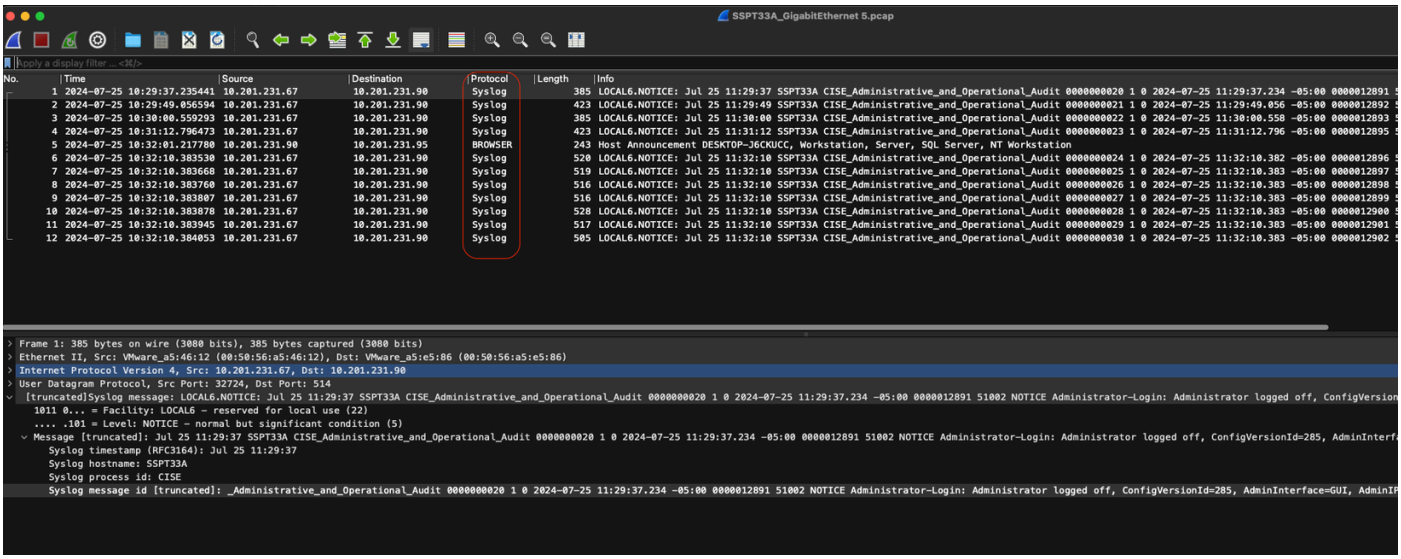
Cisco ISEのGUIで、メニューアイコン(
)、Operations > Troubleshoot >TCP Dump>Addの順にクリックします。

- トラフィックをフィルタリングし、ip host <remote_target_IP_addres> filterフィールドを追加する必要があります。
- 認証を処理するPSNからキャプチャを取得する必要があります。



TCPダンプ

このスクリーンショットでは、ISEがISE管理者ロギングトラフィックのsyslogメッセージを送信する方法を確認できます。



Syslogトラフィック

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。