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)を使用します。
- 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、さまざまな定義済みカテゴリに分類されます。

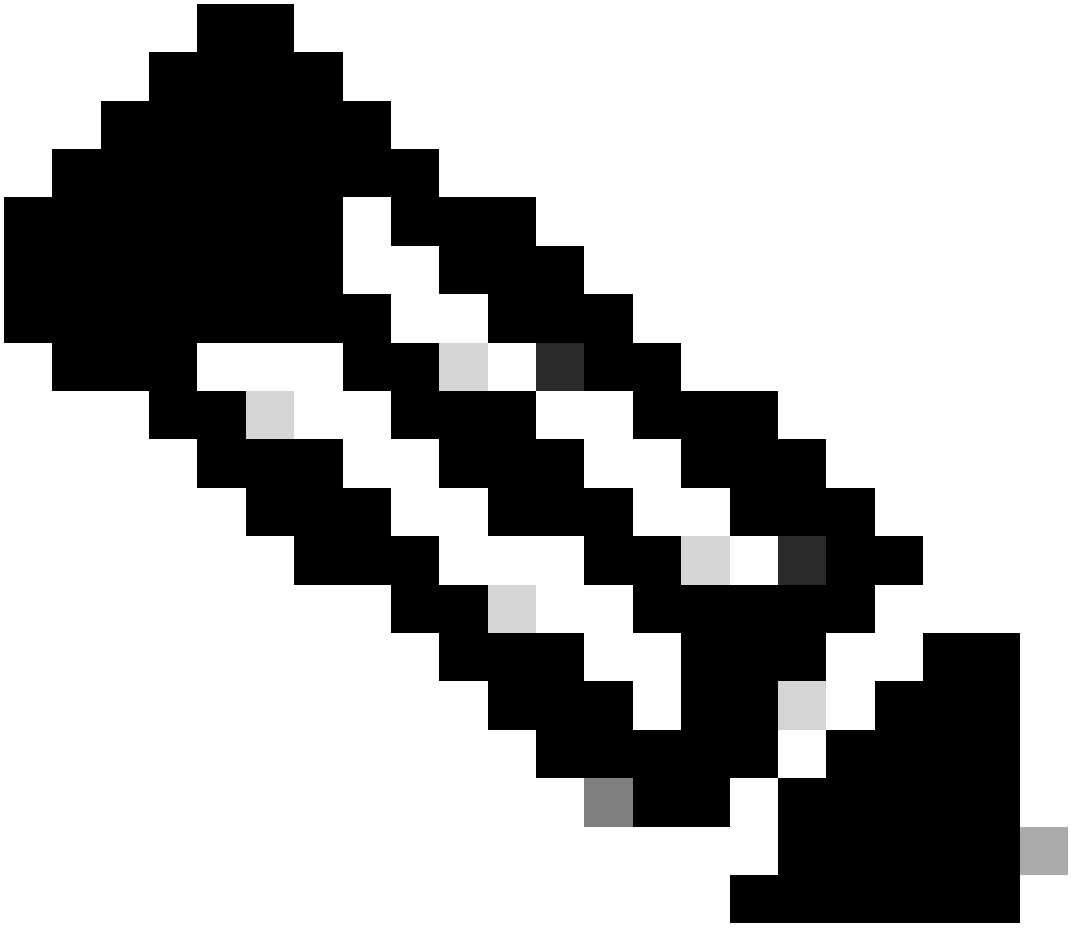
ロギング出力をカスタマイズするには、ターゲットや重大度などのカテゴリを編集します。

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 GUIで、メニュー(
)をクリックし、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。

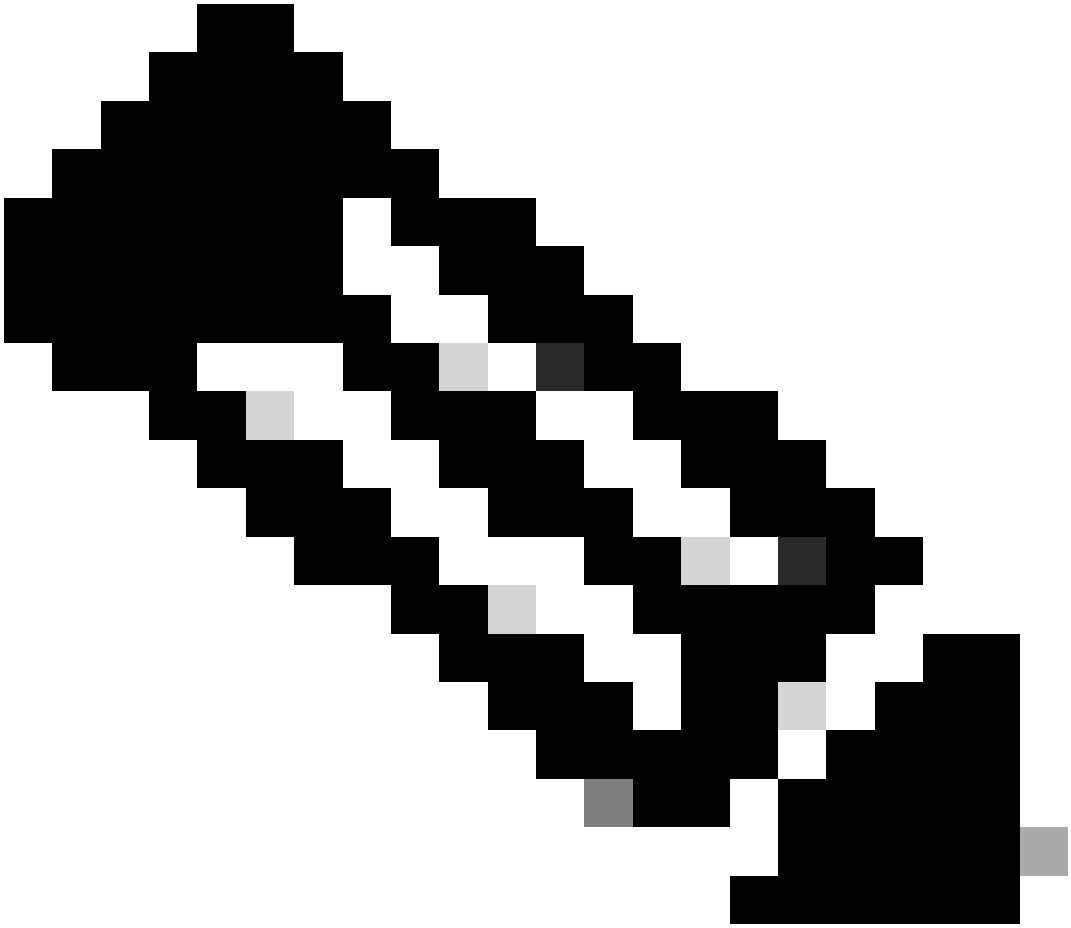
- Name as Remote_Kiwi_Syslog。ここでは、リモートSyslogサーバの名前を入力できます。この名前は説明目的で使用されます。
- Target TypeをUDP Syslogとして設定した場合、この設定例ではUDP Syslogが使用されていますが、Target Typeドロップダウンリストからさらに多くのオプションを設定できます。

UDP syslog:UDPを介したsyslogメッセージの送信に使用されます。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提供されます。

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がEnabledの場合は、Statusdrop-downリストからEnabledfromを選択します。
- 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：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、ロギング用にIPv4およびIPv6形式をサポートします。



注:syslogサーバにFQDN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キャッシングを設定する必要があることを説明してください。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。

この問題を解決するには、導入のすべてのPSNでservice cache enableコマンドを使用します。

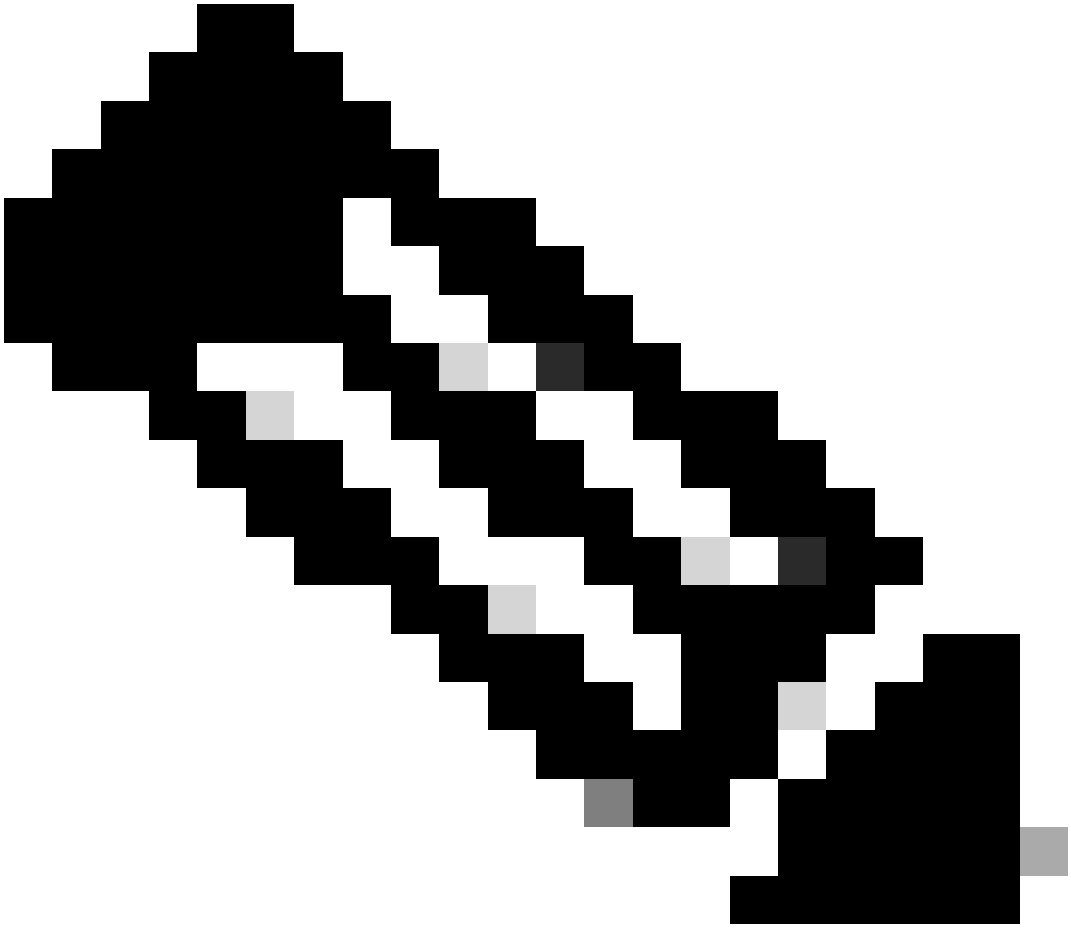
例

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

- **Port**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）でリスニングします。 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がある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 ~ Local7です。

- **Maximum Length**を**1024**に設定した場合は、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**に設定されています。ISE 3.3バージョンの値は200 ~ 1024バイトです。



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

- **アラームを含めるこのターゲットについては、単純さを保つために、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。**

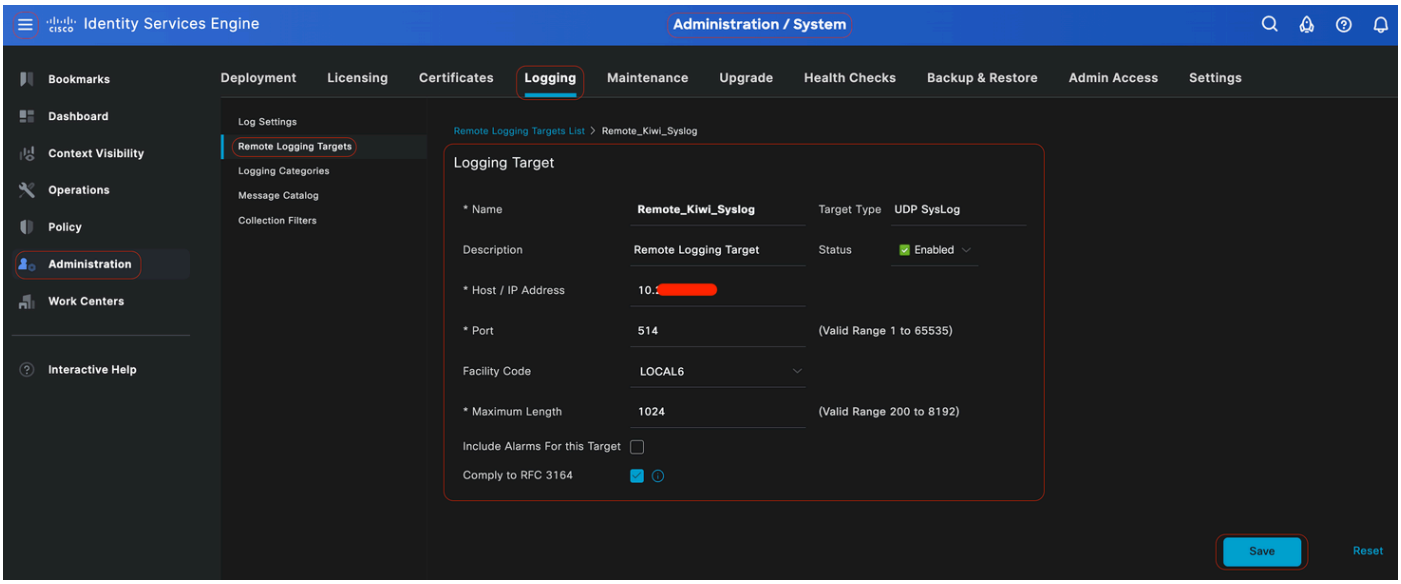
- **Comply to RFC 3164** is checked」チェックボックスをオンにすると、バックスラッシュ(\)を使用しても、リモートサーバに送信されるsyslogメッセージの区切り記号(, ; { } \ \)はエスケープされません。

-

設定が終了したら、**Save**をクリックします。

-

保存すると、システムは次の警告を表示します： **You have chosen to create an unsecure (TCP/UDP) connection to the server.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・カテゴリの下でのリモート・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、次にその**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、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。 これらのログカテゴリのイベント

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**
- **ポスチャおよびクライアントプロビジョニング診断**
- **プロファイラ**

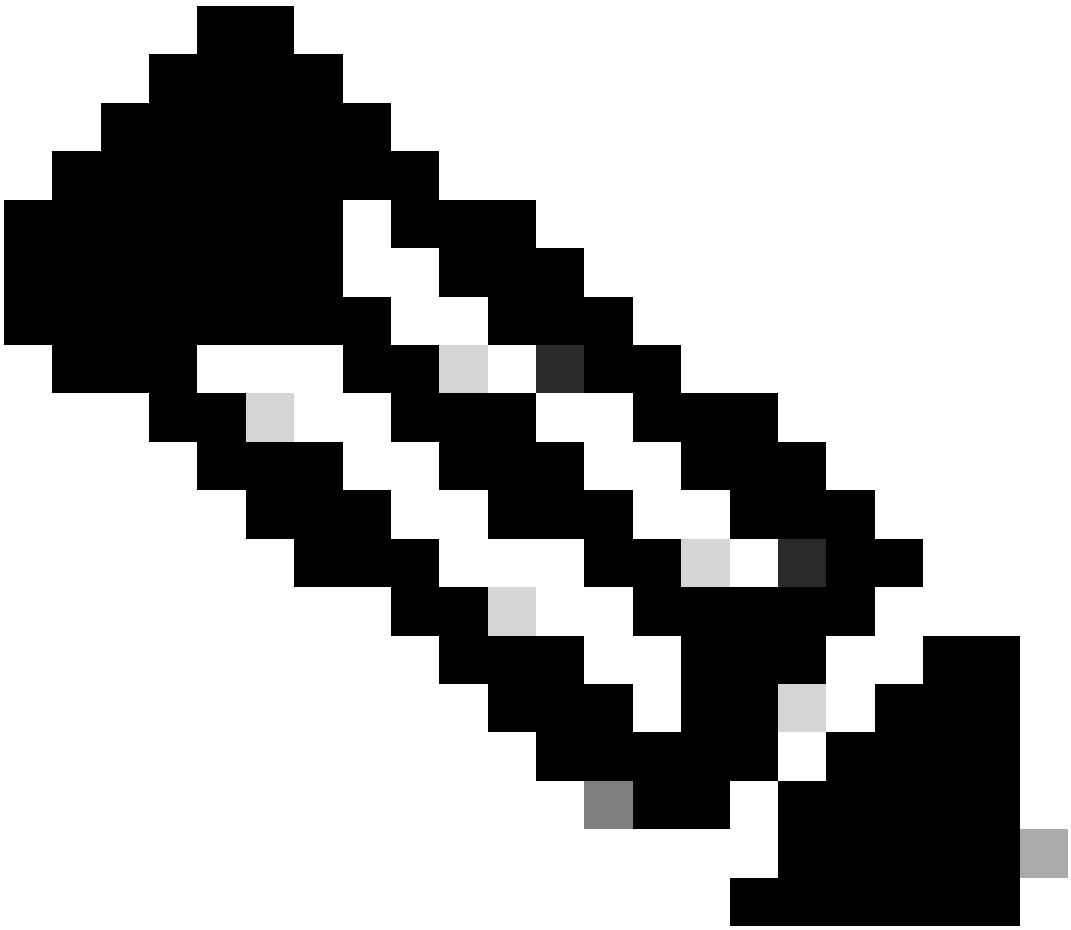
次のログカテゴリのイベントログは、展開のすべてのノードから生成され、関連するログをリモートsyslogサーバに送信するように設定できます。

-

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つの口ギングカテゴリ（認証に成功、試行に失敗、およびアカウンティング）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ます。具体的には、**認証に失敗**、**RADIUSアカウンティング**、およびISE管理者口ギングトラフィックのこのカテゴリです。



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。**

Cisco ISE GUIで、メニュー(
)をクリックし、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、ログの重大度を選択します。 一部の口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。一部の口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。このレベルでは、Cisco ISEを使用できないため、すぐに必要な措置を講じる必要があります。
- **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す。これは、多くの口ギングカテゴリに対して設定されるデフォルトのレベルです。

- **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。

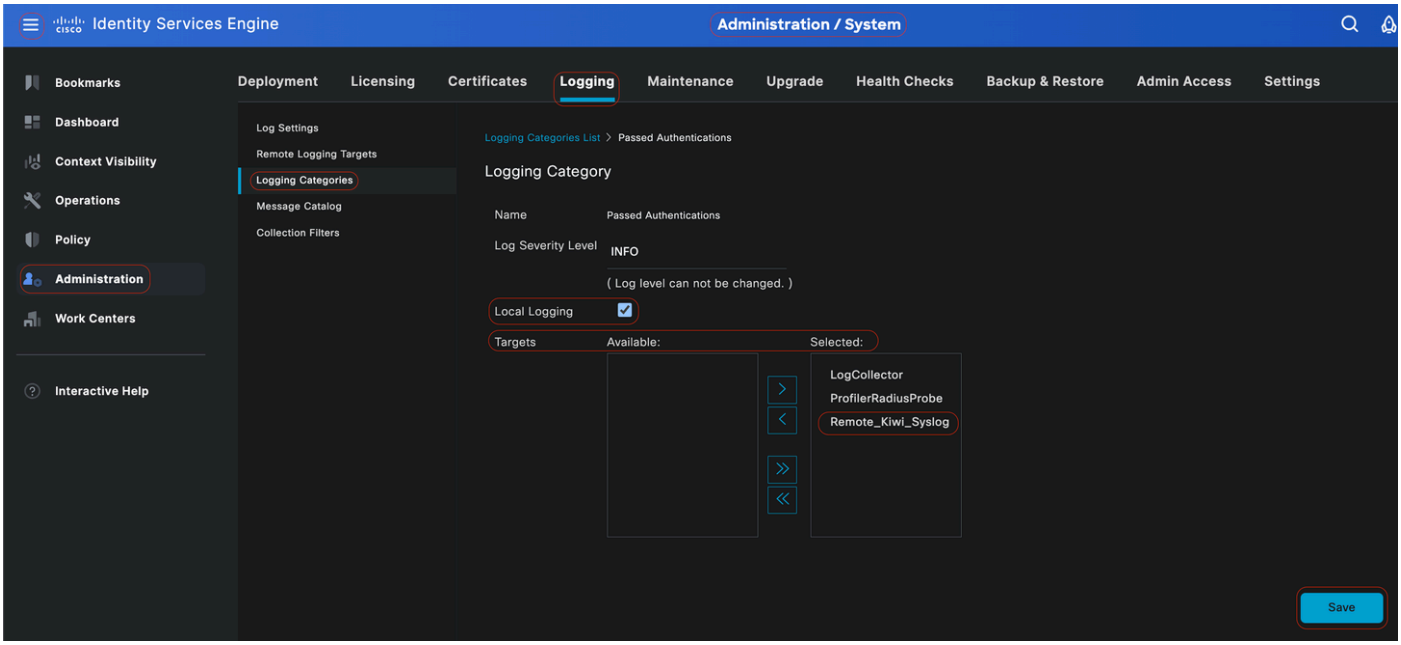
ステップ2:**ローカルロギング：このチェックボックスでローカルログの生成を有効にします**。つまり、PSNによって生成されたログは、ログを生成する特定のPSNにも保存されます。デフォルト設定を保持することをお勧めします

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。

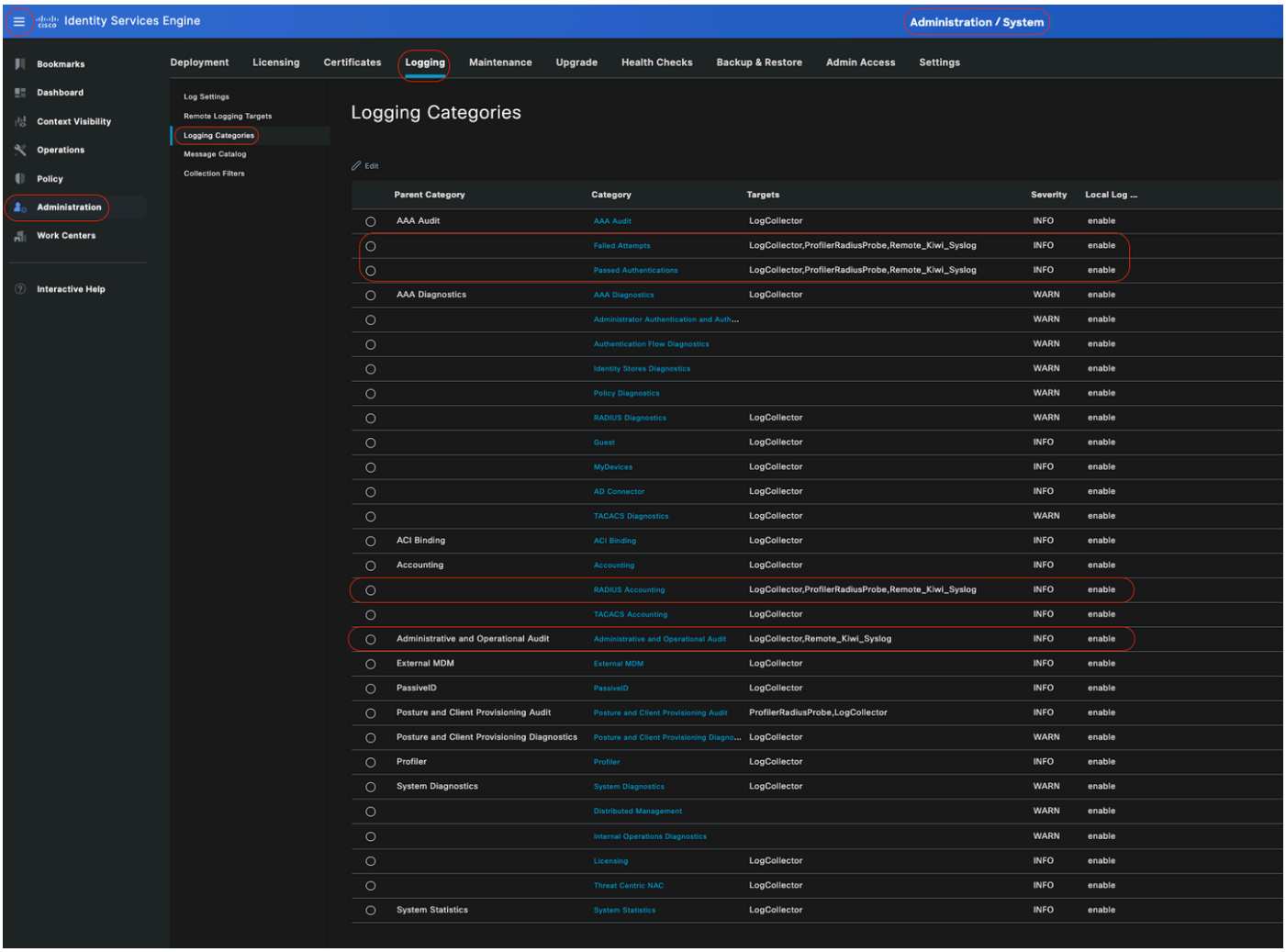
ステップ4:ステップ1からステップ3までを繰り返し、**Failed Attemptsカテゴリと Radius Accounting**カテゴリの下にRemote Targetを追加します。



リモートターゲットと目的のカテゴリのマッピング

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、複数の機能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。

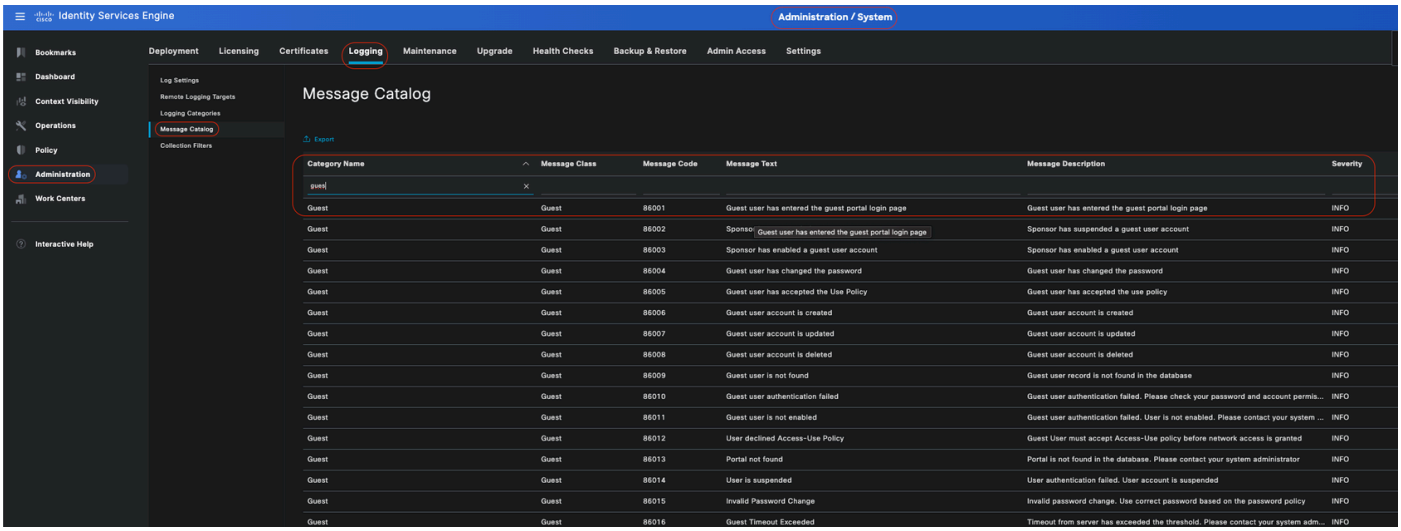
これらのエラーはメッセージカタログ内で分類され、これらのイベントも階層構造でカテゴリに分類されます。

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） 認証に成功
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
ポスチャおよびクライアントプロビジョニング診断	ポスチャおよびクライアントプロビジョニング診断
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

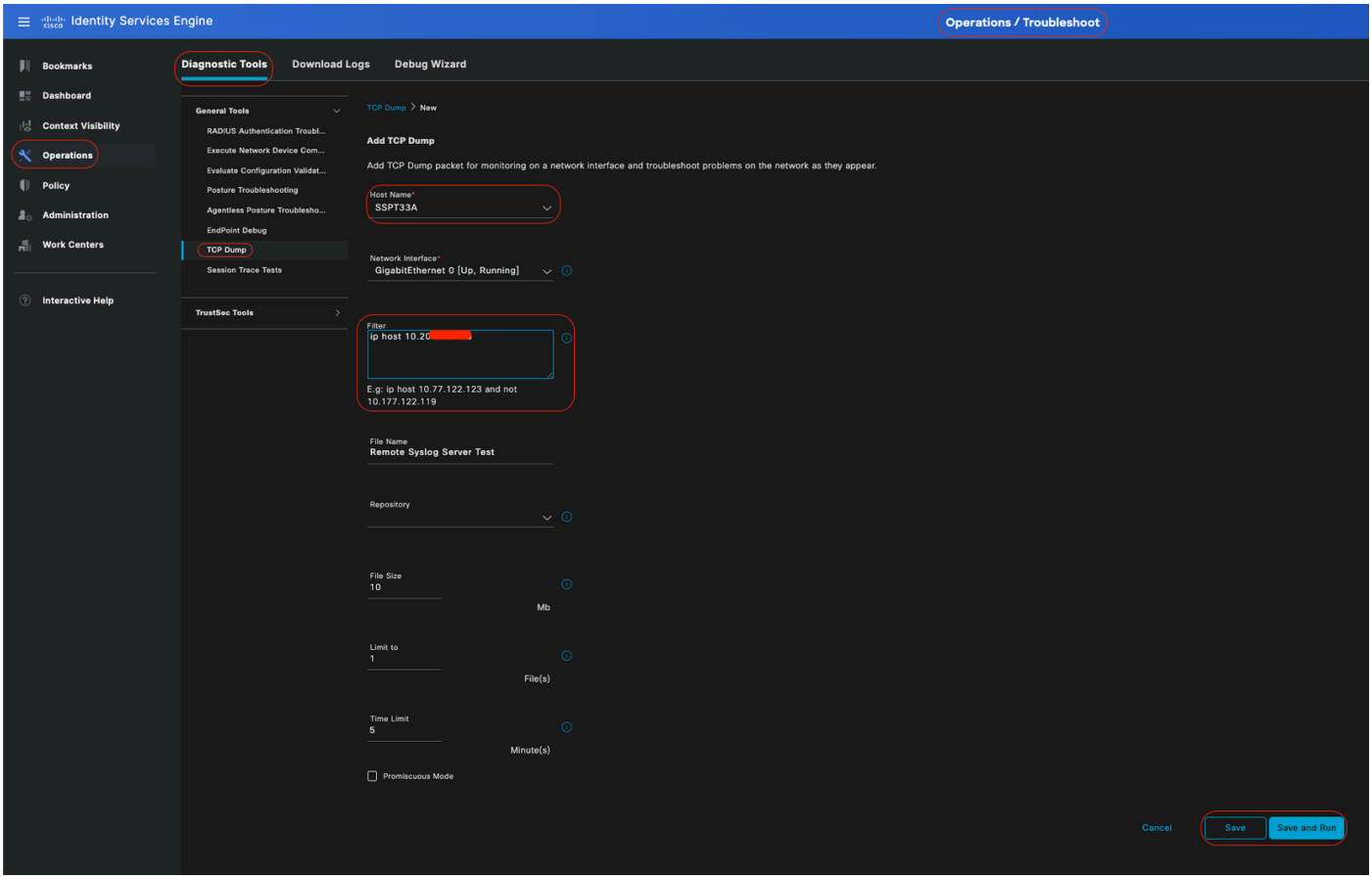
リモートロギングターゲットに対してTCPダンプを実行することは、ログイベントが送信されているかどうかを確認するための最も迅速なトラブルシューティングおよび確認の手順です。

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するため、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 GUIで、メニュー( )をクリックし、Operations> Troubleshoot>TCP Dump> Addの順に選択します。

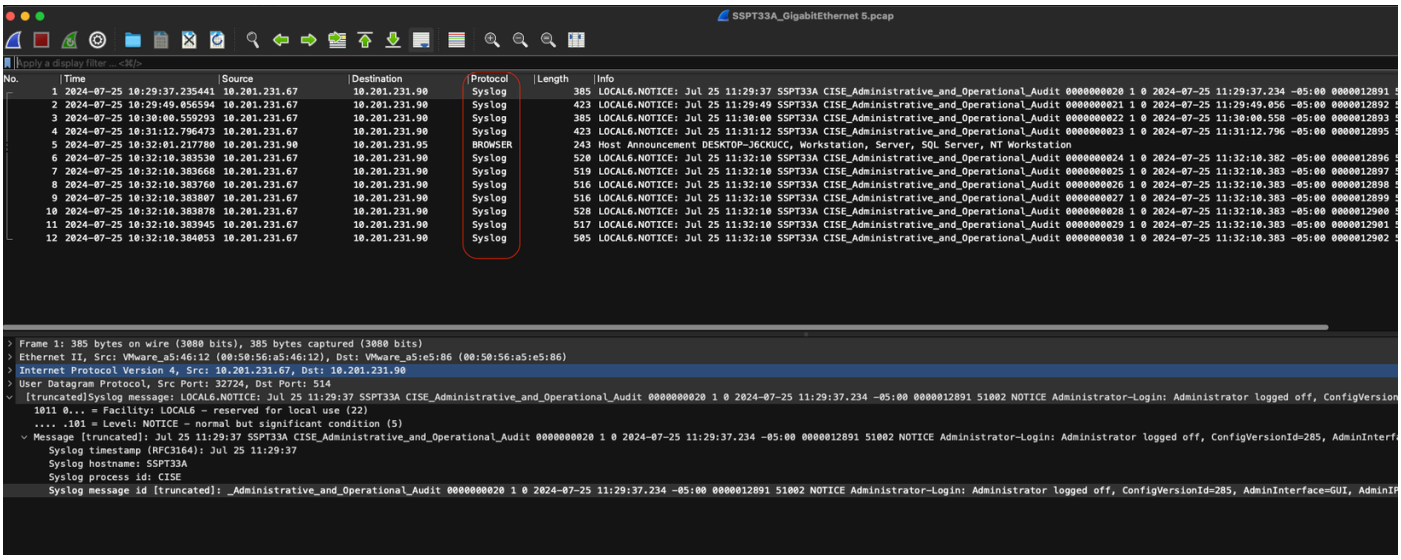
- トラフィックをフィルタリングし、ip host <remote_target_IP_addres> filterフィールドを追加する必要があります。

- 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に対して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。