ISEのサービス、目的、およびトラブルシューティングの理解

内容

はじめに

このドキュメントでは、ISEのサービス、目的、およびトラブルシューティングについて説明します。

前提条件

要件

Cisco Identity Services Engineに関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントは、Cisco Identity Services Engineの特定のソフトウェアおよびハードウェアバージョンに限定されるものではありません。

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

Cisco Identity Services Engine(ISE)は、一元化されたポリシー管理、認証、許可、アカウンティング(AAA)を通じて高度なネットワークセキュリティを提供するように設計された包括的なソリューションです。 組織は、セキュリティ、コンプライアンス、シームレスなユーザエクスペリエンスを確保しながら、ユーザ、デバイス、アプリケーションのネットワークアクセスを管理できます。

これらの目標を達成するために、Cisco ISEは幅広いサービスを利用しています。それぞれのサービスは、システムが効率的に機能するための特定のタスクを担当します。これらのサービスは連携して、セキュアなネットワークアクセス、堅牢なポリシー適用、詳細なロギング、外部システムとのシームレスな統合、および効率的なデバイスプロファイリングを実現します。

ISEの各サービスは、ソリューションの整合性と可用性を維持するうえで重要な役割を果たします。データベース管理や認証などのコア機能を処理するサービスもあれば、デバイスのプロファイリング、証明書管理、モニタリングなどの高度な機能を有効にするサービスもあります。

この記事では、Cisco ISEのさまざまなサービスの概要を示し、サービスの目的、重要性、および問題が発生した場合の潜在的なトラブルシューティング手順について説明します。管理者でもネットワークセキュリティの専門家でも、これらのサービスを理解することで、ISE導入をスムーズかつ安全に実行できるようになります。

ISEサービスの理解およびトラブルシューティング

スクリーンショットに示されているサービスは、ISEがその機能をサポートするために使用されます。ISEノードのCLIでshow application status iseコマンドを使用して、ISEで使用できるステータスまたはサービスを確認します。ISEのステータスまたは使用可能なサービスを示す出力例を次に示します。

```
honey/admin#show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          4101512
Database Server                        running          107 PROCESSES
Application Server                     running          4118209
Profiler Database                      running          4108739
ISE Indexing Engine                    running          4119606
AD Connector                           running          4121671
M&T Session Database                   running          4114154
M&T Log Processor                      running          4118388
Certificate Authority Service          running          4121560
EST Service                            running          61939
SXP Engine Service                     disabled
TC-NAC Service                         disabled
PassiveID WMI Service                  disabled
PassiveID Syslog Service               disabled
PassiveID API Service                  disabled
PassiveID Agent Service                disabled
PassiveID Endpoint Service             disabled
PassiveID SPAN Service                 disabled
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
ISE Messaging Service                  running          4105571
ISE API Gateway Database Service       running          4107770
ISE API Gateway Service                running          4113275
ISE pxGrid Direct Service              running          36228
Segmentation Policy Service            disabled
REST Auth Service                      disabled
SSE Connector                          disabled
Hermes (pxGrid Cloud Agent)            disabled
McTrust (Meraki Sync Service)          disabled
ISE Node Exporter                      running          4122893
ISE Prometheus Service                 running          4124896
ISE Grafana Service                    running          4128455
ISE MNT LogAnalytics Elasticsearch     running          4130784
ISE Logstash Service                   running          4135868
ISE Kibana Service                     running          4137540
ISE Native IPSec Service               running          4142286
MFC Profiler                           running          52667
```

ISEで利用できるサービス

次に、各サービスについて詳しく説明します。

データベースリスナー

Database　Listenerサービスは、ISEとデータベースサーバ間の通信の管理に役立つ重要なコンポーネントです。データベースに関連する要求をリッスンして処理し、ISEシステムが基盤となるデータベースに対して読み取りおよび書き込みを実行できるようにします。

ISEのデータベースリスナーサービスに関する重要なポイント

1. 通信インターフェイス:ISEとデータベースサーバ間の通信ブリッジとして機能し、ユーザクレデンシャル、セッション情報、ネットワークポリシーなどのデータを取得して保存できるようにします。

2. 外部データベースサポート:ISEは、ユーザ認証とポリシー保存に外部データベース（OracleまたはMicrosoft　SQL　Serverなど）を使用するように設定できます。Database Listener Serviceは、ISEがこの外部データベースに安全かつ効率的に接続し、対話できることを保証します。

3. データ処理：サービスはISEシステムからデータベースクエリをリッスンし、外部データベース上で適切なアクションに変換します。レコードの挿入、更新、削除、データベースからの情報の取得などの要求を処理できます。

4. データベースのヘルスモニタリング：通信チャネルの提供に加えて、外部データベースへの接続の安定性と動作性の確保も支援します。接続が失敗すると、ISEはローカルストレージにフォールバックするか、設定に応じて縮退モードになります。

データベースサーバ

データベースサーバサービスは、システムで使用されるデータの保存と取得を管理します。ISEが設定、ポリシー情報、ユーザデータ、認証ログ、デバイスプロファイル、およびその他の必要な情報を保存するために使用する、基盤となるデータベースとのインタラクションを処理します。

ISEのデータベースサーバサービスに関する重要なポイント

1.　内部データストレージ：データベースサーバサービスは、主に、ISEが運用データをローカルに保存するために使用する内部組み込みデータベースを管理します。これには、認証および許可レコード、ユーザプロファイル、ネットワークアクセスポリシー、デバイスおよびエンドポイント情報、セッション情報などのデータが含まれます。

2.　組み込みデータベース：ほとんどのCisco　ISE導入では、ローカルストレージに組み込みPostgreSQLデータベースが使用されます。Database Server Serviceは、データベースの円滑な運用を保証し、データベースに格納されているデータに関連するすべてのクエリ、更新、および管理タスクを処理します。

3. データベースの整合性：このサービスは、すべてのトランザクションが適切に処理され、データベースの整合性が維持されることを保証します。レコードのロック、データベース接続の管理、データベースクエリの実行などのタスクを処理します。

データベース・リスナーおよびデータベース・サーバー・サービスが初期化されているか、または実行されていないことを確認し、トラブルシューティングします

Database ListenerとDatabase Serverは、他のすべてのサービスが正常に機能するために一緒に実行する必要がある必須のサービスです。これらのサービスが実行されていない場合、または初期化中に停止した場合は、次のトラブルシューティング手順がリカバリに役立ちます。

1. application stop iseコマンドとapplication start iseコマンドを使用して、ISEサービスを再起動します。

2. VMノードの場合、VMからノードを再起動すると、サービスのリカバリに役立ちます。

3. ノードが物理ノードの場合、CIMCからノードを再起動またはリロードすると、サービスの回復に役立つ必要があります。

4. データベースが破損している場合は、Cisco TACに連絡して、さらにトラブルシューティングを依頼してください。

通常、データベース・リスナーとデータベース・サーバは、データベースに不一致がある場合や、データベースを正しく初期化できない場合に停止するか、起動に失敗します。このような場合、コマンドapplication reset-config iseを使用してアプリケーションリセットを実行すると、データベースのリカバリと新規の開始に役立つ必要があります。 application reset-config iseコマンドを実行すると、設定と証明書が削除されますが、IPアドレスとドメイン名の詳細は保持されます。導入環境内の任意のノードにこのコマンドを適用する前に、詳細を確認し、潜在的な影響を理解するために、Cisco TACに問い合わせることをお勧めします。

アプリケーション サーバ

アプリケーションサーバは、ISEプラットフォームのコア機能とサービスの実行および管理を担当する主要コンポーネントです。ISEがネットワークアクセスコントロール、認証、認可、アカウンティング、およびポリシー管理における役割を実行できるようにするビジネスロジック、ユーザインターフェイス、およびサービスをホストします。

ISEのアプリケーションサーバサービスに関する重要なポイント

1. ユーザインターフェイス(UI):アプリケーションサーバサービスは、ISEのWebベースのユーザインターフェイス(UI)をレンダリングする役割を担います。これにより、管理者はポリシーの設定と管理、ログとレポートの表示、ISEの他の機能との対話が可能になります。

2. サービス管理:ISEが提供するさまざまなサービス（ポリシー管理、管理タスク、分散導入内の他のISEノードとの通信など）を処理する役割を担います。

3. 中央処理：アプリケーションサーバサービスは、ISEアーキテクチャの中心的な役割を果たし、ネットワークデバイス、ディレクトリ、および外部サービスからのポリシー、認証要求、およびデータを意味するロジックを提供します。

Application Serverの検証が初期化中または実行されていません

アプリケーションサーバは、証明書、リソース、導入、ライセンスなど、いくつかのWebアプリケーションに依存します。いずれかのWebアプリケーションの初期化に失敗した場合、アプリケーションサーバーは初期化状態のままになります。アプリケーションサーバでは、ノードの設定データに応じて、**Not running→Initializing → Running**状態から約15 ~ 35分かかります。

1. ISEの管理証明書がすべてのノードの導入で有効かつアクティブであることを確認します。
2. 配置のすべてのノードがプライマリ管理ノードと同期していることを確認します。
3. ノードがVMの場合、推奨リソースがノードに割り当てられていることを確認します。

ISEノードのCLIから**show application status ise**コマンドを使用して、アプリケーションサーバのステータスを確認します。アプリケーションサーバに関連するほとんどのログは、

Catalina.OutおよびLocalhost.log ファイルに書き込まれます。

前述の条件が満たされ、アプリケーションサーバが初期化状態のままである場合は、ISEのCLI/GUIからサポートバンドルを保護します。application stop ise およびapplication start ise コマンドを使用して、サービスを回復/再起動します。

プロファイラデータベース

Profiler　Databaseは、Profilerサービスによって検出されたネットワークデバイス、エンドポイント、およびデバイスプロファイルに関する情報を保存するために使用される特別なデータベースです。プロファイラは、ネットワーク特性と動作に基づいてネットワークデバイス（コンピュータ、スマートフォン、プリンタ、IoTデバイスなど）を自動的に識別および分類する、ISEの重要なコンポーネントです。

ISEのプロファイラデータベースサービスに関する重要なポイント

1. デバイスプロファイリング：プロファイラデータベースサービスの主な機能は、プロファイルプロセスをサポートすることです。ISEは、このサービスを使用して、プロファイリング中に収集した次のような情報を保存します。

- デバイスタイプ（スマートフォン、ラップトップ、プリンタ、IoTデバイスなど）
- デバイスオペレーティングシステム(Windows®、macOS®、Cisco IOS®、Android®など)
- デバイスの製造元
- デバイスの分類に役立つネットワークの動作またはパターン

2. プロファイラ情報：デバイスハードウェアやソフトウェアプロファイルなどのプロファイラ属性が保存されます。プロファイラ属性は、定義済みのポリシーにデバイスを照合するために使用されます。この情報は、デバイスのプロファイルに基づいて、デバイスを適切なネットワークアクセスポリシーまたはVLANに動的に割り当てるために使用されます。

3. プロファイリング・プロセス：プロファイリング・プロセスは通常、次の基準に基づいて行われます。

- アクティブプロファイリング:ISEはネットワーク上のデバイスに情報をアクティブに照会します。
- パッシブプロファイリング:ISEは、DHCP要求、RADIUS属性、HTTPヘッダー、その他の

ネットワークプロトコルなどのネットワークトラフィックからデータをパッシブに収集し、デバイスタイプを決定します。

ISEプロファイリングサービスの確認とトラブルシューティング

1. ISE CLIから、show application status iseコマンドを実行して、プロファイラデータベースサービスが実行されていることを確認します。

2. プライマリ管理ノードのGUIから、Administration > Deployment >ノードを選択します。Editをクリックし、session servicesと profiling servicesが有効になっていることを確認します。

3. ここで、Administration > Deployment > Select the nodeの順に移動します。プロファイラの設定に移動し、必要なプローブがエンドポイントデータの保護に対して有効になっているかどうかを確認します。

4. Administration > System > Profilingの順に移動し、CoAに対して設定されているプロファイラの設定を確認します。

5. Context visibility > Endpointsから、エンドポイントを選択し、エンドポイントのさまざまなプローブによって収集された属性を確認します。

プロファイルの問題のトラブルシューティングに役立つデバッグ：

- プロファイラ(profiler.log)
- ランタイムAAA (prrt-server.log)
- nsf(ise-psc.log)
- nsfセッション(ise.psc.log)

ISEインデックスエンジン

インデックスエンジンは、ISEデータベースに保存されているデータの検索、インデックス作成、および取得を効率的に行うサービスです。特に大量のデータを処理する場合や、認証、認可、モニタリング、およびレポーティングタスクに必要な情報にすばやくアクセスできる場合に、ISEのパフォーマンスとスケーラビリティが強化されます。

ISEのISEインデックスエンジンに関する要点

1. データインデックス作成:ISEインデックスエンジンは、認証ログ、セッションログ、ポリシーヒット、プロファイルデータ、ネットワークアクセスレコードなど、ISEに保存されるさまざまなタイプのデータのインデックスを作成します。インデックスを作成すると、検索とクエリをより効率的に行えるようにデータを整理するのに役立ちます。

2. ログ管理とレポート：このサービスは、レポートとログクエリのパフォーマンスを向上させることで、ログ管理において重要な役割を果たします。たとえば、特定の認証イベントを検索する場合、インデックス作成エンジンを使用すると、目的のレコードを迅速に取得できます。これは、セキュリティの監視とコンプライアンスのレポート作成に不可欠です。

3. データの取得：インデックスエンジンは、ISEが必要に応じて基礎となるデータベースからインデックス付きデータを効率的に取得できるようにすることも担当します。これにより、ISEは

ユーザインターフェイス、外部ツール、またはAPIからのクエリに対して迅速な応答を提供できます。

ISEインデックスエンジンが実行されていないか、初期化されていないことを確認します

1. **nslookup <FQDN / IP address of the ISE node>**コマンドを使用し、CLI経由で前方参照と逆引きDNS参照が機能していること、またはクラスタ内のすべてのノードが機能していることを確認します。
2. ISE管理証明書がクラスタ内のすべてのノードに対して有効でアクティブであることを確認します。
3. **show ntp**コマンドを使用して、CLI経由でNTPが機能しており、ISEノードと同期していることを確認します。

インデックスエンジンはコンテキストの可視性で使用され、コンテキストの可視性が機能するには、インデックスエンジンが起動して実行されている必要があります。インデックスエンジンのトラブルシューティングに役立つ可能性がある便利なログは、**ADE.log**ファイルです。このファイルはサポートバンドルから保護するか、問題の発生中に**show logging system ade/ADE.log tail** コマンドを使用してCLIで追跡できます。

ADコネクタ

AD Connector(Active Directory Connector)は、ISEをMicrosoft Active Directory(AD)と統合できるようにするサービスです。このサービスにより、ISEはADクレデンシャルとグループメンバーシップに基づいてユーザを認証、認可、および管理できます。ADコネクタは、ISEとActive Directory間のブリッジとして機能し、ISEがネットワークアクセスコントロール(NAC)とポリシー適用にADを活用できるようにします。

ISEでのADコネクタサービスの主要機能

1. Active Directoryとの統合:ADコネクタサービスは、ISEとActive Directory間のブリッジとして機能します。これにより、ISEはADに安全に接続でき、ISEはADをユーザ認証とポリシー適用のための一元化されたIDストアとして利用できます。

2. 同期:ADコネクタサービスは、Active DirectoryからISEへのユーザおよびグループデータの同期をサポートしています。これにより、ISEはユーザとグループに関する最新情報を保持します。これは、正確なポリシー適用に不可欠です。

3. セキュアな通信:ADコネクタサービスは、ISEとActive Directory間にセキュアな通信チャネルを確立します。通常、LDAP over SSL(LDAPS)などのプロトコルを使用して、認証およびクエリプロセス中のデータのプライバシーと整合性を確保します。

4. 複数のActive Directoryドメインのサポート：このサービスは、複数のActive Directoryドメインへの接続をサポートできます。これは、ISEが異なるADフォレストまたはドメインのユーザを認証する必要がある大規模またはマルチドメイン環境で特に役立ちます。

5. ユーザおよびグループのルックアップ:ISEがユーザおよびグループ情報をADに照会できるようにします。これには、ユーザ名、グループメンバーシップ、およびネットワークアクセスポリシーの適用に使用できるその他のユーザ属性などの詳細を含めることができます。たとえば、ネットワークアクセスポリシーをユーザのADグループメンバーシップに基づいて適用できます（たとえば、異なるアクセスレベルを異なるグループのユーザに付与するなど）。

1. NTPがノードと同期しているかどうか、およびADとISEの時間差が5分未満であることを確認します。

2. DNSサーバーがADに関連するFQDNとドメインを解決できるかどうかを確認します。

3. **Operations** > **Reports** > **Reports** > **Diagnostics** > **AD connector Operations**の順に移動し、ADに関連するイベントまたはレポートを確認します。

トラブルシューティングに役立つログは、**ad_agent.log**と**runtime** コンポーネントのデバッグログです。

M&Tセッションデータベース

M&T Session Database(Monitoring and Troubleshooting Session Database)は、ネットワークアクセスイベントのセッション関連データの保存と管理において重要な役割を果たします。M&Tセッションデータベースには、ユーザ認証、デバイス接続、ネットワークアクセスイベントなど、ネットワークアクティビティのモニタリング、トラブルシューティング、分析に不可欠なアクティブセッションに関する情報が保持されます。

ISEのM&T Session Database Serviceの主要機能

1. セッションデータの保存:M&Tセッションデータベースサービスは、ネットワーク上のユーザおよびデバイスセッションに関するデータを保存し、インデックスを作成します。これには、セッションの開始時刻と終了時刻、認証結果、ユーザまたはデバイスのID、および関連付けられたポリシー（ロールの割り当てやVLANの割り当てなど）が含まれます。　このデータには、初期認証やセッションイベントを追跡するアカウンティングメッセージなど、セッションライフサイクルの詳細を示すRADIUSアカウンティング情報も含まれます。

2. リアルタイムおよび履歴データ：このサービスは、リアルタイムセッションデータ（アクティブセッション）および履歴セッションデータ（過去のセッション）へのアクセスを提供します。これにより、管理者は進行中のユーザー・アクセスを監視するだけでなく、過去のセッション・ログを参照して問題を調査したり、アクセス・イベントを検証したりできます。リアルタイムのセッションモニタリングにより、不正なデバイスが現在ネットワーク上に存在しないことを確認できます。

3. 強化されたモニタリング：セッションに適用されたポリシーを含む、ユーザとデバイスのアクティビティに対する洞察を提供し、潜在的なセキュリティ上の懸念や不正アクセスの検出に役立ちます。

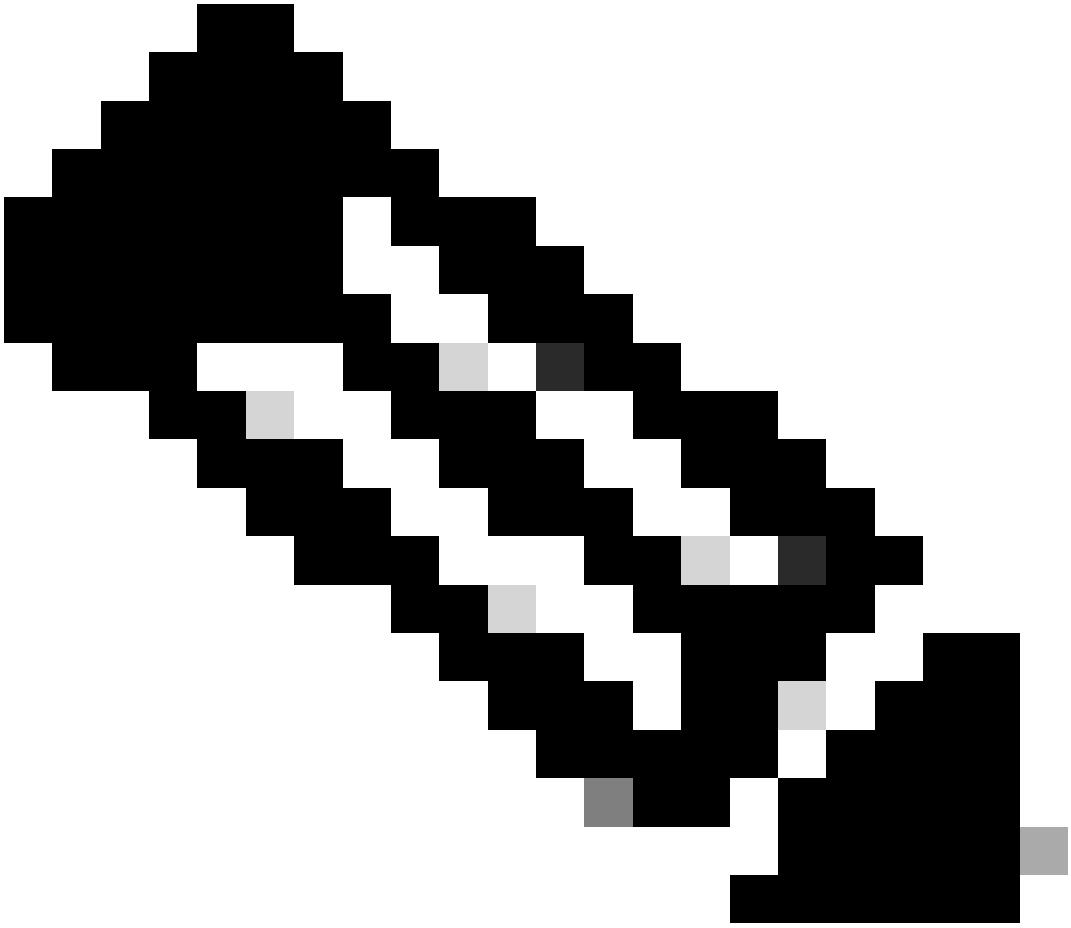
4. 監査とレポート作成：ネットワークアクセスイベントの履歴を保存し、規制レポート用のデータを提供することで、コンプライアンスの監査とレポート作成を促進します。

ISEのM&Tセッションデータベースの確認とトラブルシューティング

1. ノードに推奨リソースが割り当てられているかどうかを確認します。

2. 問題の詳細な検証のために、ISE CLIから**show tech-support**を保護します。

3. ISE CLI経由で**application configure ise**コマンドを実行し、オプション**1**を選択して、M&Tセッションデータベースをリセットします。



注:M&Tデータベースのリセットは、導入における潜在的な影響を確認した後で行う必要があります。Cisco TACに連絡して、さらに検証を依頼してください。

既知の障害

Cisco Bug ID・ 32364

M&Tログプロセッサ

M&T Log Processor (モニタリングおよびトラブルシューティングログプロセッサ) は、ISE内のさまざまなサービスによって生成されたログデータの収集、処理、および管理を行うコンポーネントです。これは、管理者がISEシステム内のネットワークアクセスイベント、認証試行、ポリシーの適用、およびその他のアクティビティを監視およびトラブルシューティングするのに役立つ、モニタリングとトラブルシューティング(M&T)フレームワークの重要な部分です。M&T　Log Processorは、特にログエントリの処理を行い、レポート、監査、およびトラブルシューティングに必要な情報をISEで保存、分析、および表示できるようにします。

ISEのM&T Log Processorサービスの主要機能

1. ログの収集と処理:M&Tログプロセッササービスは、認証要求、許可決定、アカウンティングメッセージ、ポリシー適用アクティビティなど、さまざまなISEコンポーネントによって生成されたログを収集して処理します。これらのログには、ユーザ、デバイス、ネットワークアクセス試行に関する詳細情報（タイムスタンプ、ユーザID、デバイスタイプ、適用されたポリシー、アクセス要求の成功または失敗、失敗の理由など）が含まれます。

2. レポートとコンプライアンス：このサービスで処理されるログは、コンプライアンスレポートに不可欠です。多くの規制により、組織はユーザアクセスおよびセキュリティイベントのログを保持する必要があります。M&T Log Processorサービスは、関連するすべてのログが処理され、法規制のコンプライアンス監査に使用できることを保証します。ユーザアクセスログ、認証の成功率や失敗率、ポリシー適用ログなどのログデータに基づいて、詳細なレポートを生成できます。

ISEでのM&T Log Processorサービスの確認とトラブルシューティング

1. ISEノードが、シスコのインストールガイドに従って推奨リソースとともに導入されていることを確認します。

2. 問題を確認するには、ISE CLIから**show logging system ade/ADE.log tail** コマンドを実行し、関連する例外またはエラーを確認します。

既知の障害

Cisco Bug ID・ 15130

認証局サービス

認証局(CA)サービスは、通信を保護し、デバイス、ユーザー、およびネットワークサービスを認証するためのデジタル証明書の管理に役立つ重要なコンポーネントです。デジタル証明書は、信頼できる接続を確立し、クライアント（コンピュータ、スマートフォン、ネットワークデバイス）とネットワークインフラストラクチャコンポーネント（スイッチ、ワイヤレスアクセスポイント、VPNゲートウェイ）の間で安全な通信を確保するうえで不可欠です。 Cisco ISEのCAサービスは、X.509証明書と連携して動作します。この証明書は、802.1X認証、VPNアクセス、セキュア通信、およびSSL/TLS暗号化など、ネットワークセキュリティの目的で使用されます。

ISEの認証局サービスの主要機能

1. 証明書の管理：認証局サービスは、ISE内のデジタル証明書の作成、発行、管理、および更新を処理します。これらの証明書は、ネットワーク全体のさまざまな認証プロトコルと暗号化目的に使用されます。証明書を発行するには、内部認証局(CA)として機能するか、外部CA（Microsoft AD CS、VeriSignやDigiCertなどのパブリックCAなど）と統合することができます。

2. 証明書の発行:EAP-TLSまたは同様の証明書ベースの認証方式が必要な環境では、ISEはネットワークアクセスデバイス(NAD)、ユーザ、またはエンドポイントに対して証明書を発行できます。ISEは、デバイスおよびユーザを認証するための証明書を自動的に生成して展開するか、外部

CAに証明書を要求できます。

3. 証明書の登録:CAサービスは、ラップトップ、電話、およびその他のネットワークデバイスなどのエンドポイントの証明書の登録をサポートします。これらのエンドポイントは、証明書を使用してネットワークに対して認証を行う必要があります。ISEは、SCEP(Simple Certificate Enrollment Protocol)やACME(Automated Certificate Management Environment)などのプロトコルを使用して、デバイスの証明書登録を容易にします。

4. 証明書の更新：このサービスは、デバイスとユーザの両方の有効期限が切れる証明書の更新を自動化します。証明書が常に有効で最新の状態であることを保証し、期限切れの証明書によるサービスの中断を防止します。

5. 外部認証局との統合：ISEは独自のCAとして機能できますが、外部CA（例：Microsoft Active Directory Certificate Services）と統合する方が一般的です。 CAサービスは、ISEと外部CA間のインタラクションを管理し、必要に応じてユーザ、デバイス、およびネットワークリソースの証明書を要求できます。

ESTサービス

Enrollment over Secure Transport(EST)サービスは、証明書ベースの認証環境でネットワークデバイスおよびユーザにデジタル証明書を安全に発行するために使用されるプロトコルです。
ESTは、デバイスが安全かつ自動的な方法で認証局(CA)に証明書を要求できるようにする証明書登録プロトコルです。ESTサービスは、デバイスが証明書を使用してネットワークに対して認証を行う必要がある802.1X環境、VPN接続、またはBYOD(Bring Your Own Device)のシナリオなど、デバイスの認証に特に役立ちます。

ISEのESTサービスの主要機能

1. 証明書の登録:ESTサービスは、認証のために証明書を必要とするデバイス（スイッチ、アクセスポイント、エンドポイントなど）のセキュアな証明書の登録を可能にします。登録はセキュアなトランスポート（通常はHTTPS）経由で行われ、プロセスが暗号化され、不正アクセスから保護されます。

2. 証明書の失効と更新：証明書が登録されると、ESTサービスは証明書の失効または更新の管理にも役割を果たします。たとえば、デバイスは現在の証明書の有効期限が切れたときに新しい証明書を要求する必要があり、ESTはこのプロセスの自動化に役立ちます。

3. ネットワークアクセス制御の向上:ESTサービスは、証明書を使用したデバイス認証を可能にすることで、特に802.1X認証を使用する環境において、ネットワークのセキュリティポスチャを強化します。

認証局(CA)およびESTサービスが実行されていないこと、または初期化されていないことを確認します。

1. **Administration > System > Certificates > Certificate Authority > Internal CA settings**の順に移動します。CA、EST、およびOCSPレスポンダの状態が並べ替えられて有効になっていることを確認します。
2. トラブルシューティングに役立つデバッグには、est、provisioning、ca-service、ca-service-certがあります。**toise-psc.log**、**catalina.out**、**caservice.log**、および**error.log**ファイルを参照してください。

3. ISEルートCAおよびISEメッセージング証明書が展開で有効であることを確認します。ISEルートCAの更新が必要な場合は、**Administration > Certificates > Certificate Signing Requests > Generate Certificate Signing Request**の順に移動し、**usage as ISE Root CA**を選択します。renew **ISE Root CA**をクリックします。

SXPエンジンサービス

SXPエンジンサービスは、セキュリティグループタグ(SGT)およびセキュリティグループエクスチェンジプロトコル(SXP)を使用したISEとネットワークデバイス間の通信の管理と促進を担当します。 IPアドレスやMACアドレスだけでなく、デバイスのセキュリティグループに基づいてネットワークアクセスコントロールを適用するために使用されるTrustSecポリシーのサポートにおいて、重要な役割を果たします。 ISEのSXPエンジンは、主にセキュリティグループ情報の交換に使用され、ユーザまたはデバイスのID、アプリケーション、場所に基づいてポリシーを適用するのに役立ちます。これにより、デバイスはセキュリティグループタグ(SGT)を共有できるようになります。SGTは、ルータやスイッチなどのネットワークデバイス全体にセキュリティポリシーを適用するために使用されます。

ISEでのSXPエンジンサービスの主要機能

1.TrustSecとの統合:SXPは、有線ネットワークとワイヤレスネットワークの両方に一貫したセキュリティポリシーを適用するソリューションであるCisco　TrustSecを活用する環境で一般的に導入されます。SXPエンジンは、デバイス間のSGTの通信を容易にし、デバイスまたはユーザのセキュリティコンテキストに基づいて動的にポリシーを適用できるようにします。

2.　セキュリティグループタグ(SGT):TrustSecのポリシー適用の中心は、SGTにあります。これらのタグは、ネットワークトラフィックを分類するために使用されます。SXPプロトコルは、特定のユーザまたはデバイスに対するこれらのタグのマッピングを共有するのに役立ちます。これにより、ネットワークアクセスとトラフィックフローをきめ細かく、ポリシーに基づいて制御できます。

ISEでのSXPエンジンサービスの検証およびトラブルシューティング

1. デフォルトでは、SXP EngineサービスはISEで無効になっています。これを有効にするには、**ISE GUI > Administration > Deploymentの順に選択し、ノードを選択します。Enable SXP Service**ボックスにチェックマークを入れて、インターフェイスを選択します。次に、**show application status ise** コマンドを使用して、ISE CLIからSXPエンジンサービスのステータスを確認します。

2. ネットワーク通信に問題がある場合は、CLIでshow interfaceコマンドを使用して、SXPエンジンに割り当てられたインターフェイスに有効なIPアドレスがあることを確認し、そのIPサブネットがネットワークで許可されていることを確認します。

3.RADIUSライブログを確認して、ISEのSXP接続イベントを確認します。

4.ISEノード上でSXPコンポーネントを有効にして、SXPに関連する関連ログと例外をデバッグし、キャプチャします。

TC-NACサービス

TC-NACサービス(TrustSec Network Access Control)は、ネットワークデバイスへのTrustSecポリシーの適用を促進するコンポーネントで、アクセス制御が従来のIPアドレスやMACアドレスではなく、セキュリティグループタグ(SGT)に基づくようにします。

TrustSecはシスコが開発したフレームワークで、VLANやIPアドレスなどの従来のメカニズムを使用する代わりに、デバイスのロール、ユーザ、コンテキストに基づいて、ネットワーク全体にセキュリティポリシーを適用できます。デバイスを異なるセキュリティグループにグループ化し、SGTでタグ付けすることで、より詳細で動的なネットワークアクセス制御を提供します。

ISEでのTC-NACサービスの主要機能

1. サードパーティのNACシステムとの統合:TC-NACサービスにより、ISEはサードパーティのネットワークアクセスコントロールソリューションとの通信および対話が可能になります。この機能は、既存のNACインフラストラクチャを使用しているが、Cisco ISEと統合して機能の向上、追加のセキュリティポリシーの活用、またはシスコの他のネットワークセキュリティ機能の利用を希望している組織に役立ちます。

2. シームレスなポリシー適用の提供：サードパーティのNACソリューションと統合すると、ISEはポリシー適用と意思決定の特定の側面を引き継ぐことができます。これにより、より統合されたポリシーフレームワークが可能になり、シスコとシスコ以外の両方のNACシステムによって適用されるポリシーがネットワーク全体で一貫したものになります。

3. レガシーNACシステムのサポート:TC-NACサービスは、レガシーNACシステムを導入している組織を支援し、強化されたセキュリティ機能のためにCisco ISEを採用する一方で、それらのシステムを引き続き使用できるようにします。ISEは、古いNACソリューションと統合してライフサイクルを拡張し、アクセスコントロール、セキュリティ、およびコンプライアンスの適用を並行して提供できます。

4. サードパーティNACベンダーコミュニケーションの促進：このサービスにより、ISEは独自のプロトコルまたは標準を使用するサードパーティNACソリューションとのコミュニケーションを促進できます。ISEは、使用されている特定のNACソリューションに応じて、業界標準のプロトコル（RADIUS、TACACS+、SNMPなど）またはカスタマイズされたAPIを介してサードパーティのNACシステムと対話できます。

ISEでのTC-NACサービスの確認とトラブルシューティング

1.**Administration > Deployment > PSN node > Enable Threat Centric NAC**の順に移動して、Threat Centric NACが有効になっていることを確認します。

2. 問題がSourceFire FireAMPアダプタにある場合は、ネットワークでポート443が許可されているかどうかを確認します。

3. **Operations** > **Threat-Centric NAC Live Logs**でエンドポイントセッションの詳細を確認します。

Threat Centric NACによってトリガーされるアラーム：

- アダプタに到達できない(syslog ID:91002)：アダプタに到達できないことを示します。

- アダプタ接続の失敗(syslog ID: 91018)：アダプタは到達可能ですが、アダプタとソースサーバ間の接続がダウンしていることを示します。

- Adapter Stopped Due to Error(syslog ID: 91006)：このアラームは、アダプタが望ましい状態でない場合にトリガーされます。このアラームが表示された場合は、アダプタの設定とサーバの接続を確認します。詳細については、アダプタのログを参照してください。

- アダプタエラー(syslog ID: 91009): QualysアダプタがQualysサイトとの接続を確立できないか、またはQualysサイトから情報をダウンロードできないことを示します。

TC-NACの問題のトラブルシューティングに役立つデバッグ：

- va-runtime (varuntime.log)
- va-service（varuntime.logおよびvaaggregation.log）
- TC-NAC(ise-psc.log)
- anc(ise-psc.log)

PassiveID WMIサービス

PassiveID WMIサービスは、ネットワーク内のエンドポイントを識別してプロファイリングするためのパッシブメカニズムとしてWindows Management Instrumentation(WMI)を使用してデバイスプロファイリングをISEが実行できるようにするサービスです。特に、ネットワークアクセス制御とポリシー適用のためにWindows OSを実行しているデバイスを正確に特定する必要がある環境では、デバイスのプロファイリングにおいて重要な役割を果たします。

ISEでのPassiveID WMIサービスの主な機能

1. デバイスIDの収集:PassiveID WMIサービスにより、ISEはWindows Management Instrumentation(WMI)を使用してWindowsデバイスからID情報を受動的に収集できます。 デバイスのホスト名、OSのバージョン、その他の関連属性などのシステムの詳細を、デバイスがアクティブに参加する必要なしに収集します。

2. ISEポリシーとの統合:PassiveID WMIサービスによって収集された情報は、ISEポリシーフレームワークに統合されます。タイプ、OS、セキュリティ標準への準拠などのデバイス属性に基づいて、ポリシーを動的に適用できます。

PassiveID WMIサービスの確認とトラブルシューティング

ユーザ情報を受信する最も一般的なソースであると同時に、安全性が高く正確なソース。ADはプローブとして、WMIテクノロジと連携して認証されたユーザーIDを提供します。また、プローブではなくAD自体がソースシステム（プロバイダ）として機能するため、他のプローブはそのシステムからユーザーデータを取得します。

トラブルシューティングに必要な便利なデバッグと情報。 PassiveID WMI問題のデバッグレベルに次の属性を設定します。

- PassiveID (passiveid*)
- ランタイムロギング(prrt-server.log)

- Active Directory (ad)_agent.log) – トレースレベル
- コレクタ(collector.log)（PassiveID、MnTノード、およびセッションがパブリッシュされている場合はアクティブpxGridノード）
- pxGrid(pxgrid/)（セッションが公開されている場合は、セカンダリMnTおよびアクティブpxGridノード上）

PassiveID WMIのトラブルシューティングに必要な情報：

1. 以前は動作していたか？最近行われた変更。　（ISEでのアップグレード、パッチインストール、DCでのアップグレードなど）
2. テスト接続は正常に動作していますか（統合前に、テスト接続を確認してください）。
3. ADへの参加に使用されるユーザ名とWMIに使用されるユーザ名の詳細（adminアカウントかnon adminアカウントか）
4. DCのイベント(4768、4770)がログに記録されているかどうかを確認します。（DCからのイベントビューアログ）
5. ログのキャプチャ：パッシブIDとランタイムロギングのデバッグレベルを設定し、そのDCに対してconfig　wmiを実行し、ADはタイムスタンプ付きのトレースレベルを実行します。

PassiveID Syslogサービス

PassiveID　Syslog　Serviceは、PassiveIDプロファイリング機能が環境内のネットワークデバイスからsyslogメッセージを収集して処理できるようにするサービスです。これらのsyslogメッセージには、ネットワークに接続されているエンドポイントに関する重要な情報が含まれています。ISEはこれらの情報を使用して、これらのデバイスをプロファイリングし、ネットワークアクセス制御とポリシー適用を行います。

パッシブID Syslogサービスの主な機能

1. パッシブ認証：パッシブID　Syslogサービス(PVID)を使用すると、Cisco　ISEはネットワークデバイス（スイッチやルータなど）からユーザとデバイスのアクティビティを示すsyslogメッセージを収集することで、ユーザとデバイスをパッシブに認証できます。これは、802.1Xなどの従来のアクティブな認証方式が適さない、または実行可能でない状況で役立ちます。

2. イベントロギング：パッシブID　Syslogサービスは、syslogプロトコルを利用して、ネットワーク上のユーザアクセスおよび動作を追跡するネットワークデバイスからログを受信します。これらのログに含まれる情報には、デバイスログインの試行、アクセスポイント、インターフェイスの詳細などが含まれ、ISEがデバイスまたはユーザを受動的に特定するために役立ちます。

PassiveID APIサービス

PassiveID　APIサービスは、ネットワークに接続されているデバイスやユーザのアイデンティティに関する情報を必要とするシステムとの統合を可能にするサービスです。通常は、ネットワーク管理者が、すべてのデバイスに802.1Xなどのアクティブなネットワーク認証プロトコルを必要とせずに、IDベースのポリシーとアクションを実行する必要がある環境で使用されます。

パッシブID APIサービスの主要機能

1. 外部システムとの統合：Passive ID APIを使用すると、ISEは、サードパーティのシステムまたはネットワークデバイス（スイッチ、ルータ、ファイアウォール、またはアイデンティティ関連イベントを生成できる任意のシステムなど）からアイデンティティ情報を受信できます。 これらの外部システムは、syslogメッセージ、認証ログ、またはISEがユーザやデバイスを受動的に識別するのに役立つその他の関連データなどの情報を送信できます。

2. パッシブ認証：パッシブID APIサービスは、アクティブ認証を必要とせずに（例：802.1X、MAB、またはWeb認証を必要とせずに） IDデータを収集することで、ユーザおよびデバイスをパッシブに認証するために使用されます。 たとえば、ネットワークデバイス、Active Directoryログ、またはセキュリティアプライアンスから情報を取得し、それを使用してユーザまたはデバイスを特定できます。

3. アイデンティティ情報のマッピング：パッシブID APIを使用して、アイデンティティデータを特定のセキュリティポリシーにマッピングできます。この情報は、セキュリティグループタグ(SGT)またはロールをユーザとデバイスに動的に割り当てるために使用され、ネットワークアクセスコントロール（セグメント化やファイアウォールポリシーなど）の適用に影響を与えます。

PassiveID Agentサービス

PassiveID Agent Serviceは、エンドポイント（コンピュータ、ラップトップ、モバイルデバイスなど）にインストールされたPassiveID Agentを使用してデバイスのプロファイリングを可能にするサービスです。 PassiveID Agentを使用すると、ISEはエンドポイントからのトラフィックをリッスンすることによって、ネットワーク上のデバイスに関するプロファイリング情報を収集できます。アクティブなスキャンやデバイスとの直接的な対話は必要ありません。

パッシブIDエージェントサービスの主な機能

1. パッシブユーザおよびデバイスID:パッシブIDエージェントサービスは、ID関連の情報（通常はネットワークデバイスまたはエンドポイントから）をパッシブに収集し、そのデータをISEに送信する役割を担います。このサービスを使用すると、ISEは、デバイスからのアクティブな認証を必要とせずに（たとえば、802.1Xクレデンシャルを提供せずに）、ユーザおよびデバイスの認証と識別を行うことができます。

2. 他のシスココンポーネントとの統合：パッシブIDエージェントは、スイッチ、ワイヤレスコントローラ、アクセスポイントなどのシスコネットワークデバイスと密接に連携して、ネットワークトラフィック、syslogログ、またはその他の管理システムからIDに関連する情報を収集します。また、Cisco TrustSecおよびCisco Identity Servicesと統合して、このデータを特定のセキュリティグループタグ(SGT)またはその他のアイデンティティベースのポリシーにマッピングすることもできます。

3. コンテキストネットワークアクセス制御：パッシブIDエージェントはこの情報をCisco ISEに送信し、ユーザまたはデバイスのアイデンティティとコンテキストに基づいて、適切なアクセス制御ポリシーを適用します。これには次のものが含まれます。

- ロールベースアクセスコントロール。
- ダイナミックVLAN割り当て。
- ネットワークの分割

- ユーザロールまたはデバイスのセキュリティポスチャに基づくセキュリティポリシーの適用

PassiveIDエンドポイントサービス

PassiveID Endpoint Serviceは、PassiveIDテクノロジーに基づいて、ネットワーク上のエンドポイント（デバイス）の識別とプロファイリングを行うサービスです。このサービスにより、ISEは、エンドポイント自体とのアクティブな対話を必要とせずに、ネットワークに接続しているデバイスに関する情報を収集、処理、分類できます。PassiveID Endpoint Serviceは、プロファイリング、ネットワークアクセス制御、およびセキュリティポリシーの適用において重要な役割を果たします。

PassiveIDエンドポイントサービスの主要機能

1. パッシブユーザおよびデバイスの識別：PassiveID Endpoint Serviceでは、Cisco ISEがネットワークアクティビティまたはシステムログの情報を利用して、ネットワーク上のデバイスをパッシブに識別し、認証します。これには、MACアドレス、IPアドレス、Active Directory(AD)などの外部アイデンティティストアからのログイン情報など、ネットワークの動作または特性に基づいてユーザおよびデバイスを識別することが含まれます。

2. エンドポイントからのデータ収集：エンドポイントサービスは、さまざまな種類のエンドポイント固有データをさまざまなソースから収集します。

- Active Directoryや他のディレクトリなどの外部IDストアからユーザがログインする情報。
- IPアドレス、MACアドレス、デバイスタイプなどのデバイスの特性（例：デバイスがWindows PC、携帯電話、IoTデバイスのいずれであるか）。
- DHCP要求、ARP要求、その他のネットワーク層通信などのエンドポイントネットワークアクティビティ。

PassiveID SPANサービス

PassiveID SPAN Serviceは、ネットワークデバイスでSPAN(Switched Port Analyzer)ポートミラーリングを利用して、ネットワークトラフィックをキャプチャおよび分析し、エンドポイントプロファイリングを行うサービスです。このサービスは、ISEがネットワーク通信パターンを分析することによって、デバイス自体にアクティブプローブやエージェントをインストールすることなく、ネットワーク上のエンドポイント（デバイス）に関する情報を受動的に収集するのに役立ちます。

PassiveID SPANサービスの主要機能

1. SPANトラフィックからのパッシブID収集:PassiveID SPANサービスにより、ISEは、スイッチ上のSPANポートを介してミラーリングまたはコピーされるネットワークトラフィックに基づいて、IDデータを収集できます。SPANポートは、通常、他のポートまたはVLANからのネットワークトラフィックをミラーリングすることによってネットワークを監視するために使用されます。このトラフィックをキャプチャすることにより、ISEは次のようなID情報を受動的に収集できます。

- デバイスのMACアドレス。

- デバイスに関連付けられたIPアドレス。
- キャプチャされたトラフィックからのDHCP要求またはその他のアイデンティティ関連情報。
- スイッチやワイヤレスコントローラなどのネットワークデバイスからの認証ログ。

2. ユーザおよびデバイスID情報のキャプチャ:SPANサービスは、基本的に、デバイスと直接やり取りする必要なく、ネットワークを通過するトラフィックをリッスンし、ネットワークパケットから主要なID情報を識別します。これには、次のようなデータが含まれます。

- EAP(Extensible Authentication Protocol)などのプロトコルで認証されるユーザID。
- MACアドレスとIPアドレスに基づくデバイスID。
- 観察されたトラフィックパターンとイベントに基づくデバイスのロールと動作

PassiveIDスタックの検証とトラブルシューティング（PassiveID SPANサービス、PassiveID Syslogサービス、PassiveID Endpointサービス、PassiveID Agent、PassiveID APIサービス）

1. PassiveIDスタックはプロバイダーのリストであり、PassiveIDスタック内のすべてのサービスはデフォルトで無効になっています。ISE GUI > Administration > Deployment >ノードを選択し、Enable Passive Identity Serviceの順に移動して、Saveをクリックします。PassiveIDスタックのサービスステータスを確認するには、ISEノードのCLIにログインして、show application status ise コマンドを実行します。

2. パッシブIDエージェントに問題がある場合は、エージェントのFQDNがISEノードから解決可能かどうかを確認します。これを実行するには、ISE CLIにログインして、nslookup < FQDN of Agent configured > コマンドを実行します。

3. ISEインデックスエンジンがアクティブで、DNS逆引きおよび前方参照の両方がISEで設定されたDNSまたはネームサーバによって解決されていることを確認します。

4. syslogプロバイダーとのシームレスな通信を保証するため、ネットワークでUDPポート40514とTCPポート11468が開放されていることを確認します。

5. ノードでSPANプロバイダーを設定するには、ISEパッシブIDサービスが有効になっていることを確認します。SPANプロバイダーに設定するインターフェイスが、ISE CLIからshow interfaceコマンドを使用して、ISEで使用できることを確認します。

パッシブIDプロバイダーに基づいてログを確認するには、passiveid-syslog.log、passiveid-agent.log、passiveid-api.log、passiveid-endpoint.log、passiveid-span.logを調べる必要があります。前述のログは、ISEノードのサポートバンドルから保護できます。

DHCPサーバ(dhcpd)

DHCPサーバー(dhcpd)サービスは、ネットワークデバイスに動的ホスト構成プロトコル(DHCP)機能を提供するサービスです。主に、ネットワークに接続しようとしているデバイス（エンドポイント）にIPアドレスを割り当てるために使用されます。ISEでは、DHCPサーバは、ネットワークに接続するときにIPアドレスを要求するエンドポイントにIPアドレスを提供する上で重要な役割を果たします。このサービスでは、DNSサーバ、デフォルトゲートウェイ、その他のネットワーク設定など、追加の構成情報も提供できます。

ISEでのDHCPサーバ(dhcpd)サービスの主要機能

1. ダイナミックIPアドレス割り当て：ISEのdhcpdサービスはDHCPサーバとして機能し、ネットワークに接続するときにIPアドレスを要求するデバイスにIPアドレスを割り当てます。これは、BYOD（Bring Your Own Device；個人所有デバイスの持ち込み）環境で、またはデバイスがIPアドレスを自動的に取得するように設定されている場合など、デバイスがネットワークに動的に参加するシナリオで重要です。

2. プロファイルベースのDHCP: dhcpdサービスは、デバイスのプロファイルに基づいてIPアドレスを割り当てることができます。ISEがデバイスをプロファイリングしている場合（たとえば、スマートフォン、ラップトップ、IoTデバイスであると判断した場合）、デバイスのタイプまたはロールに基づいて、適切なIPアドレスを割り当てたり、他の設定を適用したりできます。

3. DHCPリレーのサポート：ISEはDHCPリレーエージェントとして機能し、ISEが実際のIPアドレス割り当てを処理していない場合は、デバイスから外部DHCPサーバにDHCP要求を転送できます。この場合、dhcpdサービスはデバイスからの要求を中央のDHCPサーバに転送できますが、ISEはネットワークポリシーとアクセスコントロールを引き続き適用します。

DHCPサーバ(dhcpd)の確認とトラブルシューティング

1. Cisco TACに連絡し、DHCPサーバパッケージがISEにインストールされているかどうかを確認します。

2.**ISE > rpm -qi dhcp**のルートにログインします。

DNSサーバ（名前付き）

DNSサーバ（名前付き）サービスは、ISEがDNS（ドメインネームシステム）サーバまたはDNSリゾルバとして機能できるようにするサービスです。主にドメイン名をIPアドレスに解決し、その逆も行い、ネットワーク内のデバイス間の通信を容易にします。

ISEのDNSサーバ（名前付き）サービスの主要機能

1. ISE通信のDNS解決:ISEの名前付きサービスは、ドメイン名をIPアドレスに解決するのに役立ちます。これは、ISEがIPアドレスではなくドメイン名を使用して、他のネットワークデバイスや外部サービス（RADIUSサーバ、Active Directory、外部NTPサーバなど）に接続する必要がある場合に特に重要です。

- たとえば、ISEがRADIUSサーバまたは外部ディレクトリサービス（Active Directoryなど）に到達する必要がある場合、そのサーバのドメイン名をIPアドレスに解決する必要があります。
- ISEは、システム上に設定されているDNSサーバにこれらのドメイン名を解決するようクエリを送信し、円滑な通信を確保します。

2. 外部サービスのDNS解決:DNSサービスは、ISEがドメイン名を必要とする外部サービスに接続できるようにします。たとえば、ISEは次のような外部サービスの名前を解決する必要があります。

- クラウドベースサービス
- ネットワークタイムプロトコル(NTP)サーバ。
- 認証局(CA)またはLDAPサーバ

3. マルチドメインおよび冗長DNSサーバ：冗長性のために複数のDNSサーバを使用するようにISEを設定できます。1台のDNSサーバが使用できなくなった場合、ISEは別のDNSサーバにフォールバックして、継続的な動作とDNS解決を保証できます。

DNSサーバ（名前付き）の確認とトラブルシューティング

1. ISEノードのCLIで、**ping <IP of DNS server / name server>**コマンドを使用して、展開のネームサーバまたはDNSサーバへの到達可能性を確認します。

2. ISE CLIで**nslookup <FQDN / IP address of ISE nodes>**コマンドを使用して、ISE FQDNのDNS解決を確認します。

ISEメッセージングサービス

ISEメッセージングサービスは、ISEシステム内のさまざまなサービスとコンポーネント間の非同期通信を容易にするコンポーネントです。ISEのシステムアーキテクチャ全体において重要な役割を果たし、プラットフォームのさまざまな部分で、メッセージの送受信、タスクの管理、およびアクティビティの同期を可能にします。

ISEメッセージングサービスの主な機能

1. プロセス間通信(IPC):ISEメッセージングサービスは、さまざまなISEサービス間のプロセス間通信(IPC)を可能にするために重要な役割を果たします。認証、認可、ポリシーの適用など、さまざまなISEモジュールとサービスが、調整された方法でデータと命令を交換できるようにします。

2. 分散環境のサポート：大規模または分散型のISE導入（マルチノード構成や高可用性構成など）では、メッセージングサービスにより、さまざまなISEノード間の通信が容易になります。これにより、認証要求、ユーザセッション、ポリシー更新などのデータが、ISEシステム内の異なるノード間で正しく同期されます。

3. ポリシーと設定の同期：メッセージングサービスは、ISEノード間の設定とポリシーの同期に関与します。プライマリノードに対して設定の変更が行われると、サービスはこれらの変更がシステム内のセカンダリノードまたはバックアップノードに伝播されることを保証します。これは、一貫性を維持し、異なる場所や分散したISEノードに適用されるネットワークアクセスポリシーの同期を維持するために不可欠です。

ISEメッセージングサービスが実行されていないか、初期化されていないことを確認します

1. ポートTCP 8671がファイアウォールでブロックされていないことを確認します。これは、このポートがISEデバイス間のノード間通信に使用されるためです。

2. キューリンクエラーを確認し、存在する場合は、ISEメッセージング証明書とISEルートCA証明書を更新します。これは、通常、内部証明書の破損の問題が原因でキューリンクエラーが発生するためです。キューリンクエラーを解決す

るには、「ISE – キューリンクエラー」の記事を参照して、ISEメッセージングおよびISEルートCA証明書を更新してください。

3. GUIで-> Administration -> Certificates -> Select ISE Messaging Certificateの順に選択します。 Viewをクリックして、証明書のステータスを確認します。

ISEメッセージングサービスのトラブルシューティングに役立つログは、ade.logです。このログはサポートバンドルから入手するか、show logging system ade/ADE.log tail コマンドの使用時にCLIから確認できます。

4. ADE.logログに「rabbitmq: connection refused」エラーが表示された場合は、Cisco TACに連絡して、ISEルートからRabbitmqモジュールのロックを解除してください。

ISE API Gateway Databaseサービス

ISE API Gateway Database Serviceは、ISEシステム内のAPI要求および応答に関連するデータを管理および処理するコンポーネントです。ISE API GatewayとISEデータベースを接続する中継機能として機能し、カスタムアプリケーションがサービスによって管理されるAPIコールを介してISE内のデータを更新または変更（アクセスポリシーの調整、ユーザの追加や削除など）できるようにします。

ISE API Gateway Database Serviceの主要機能

1. ISEデータへのAPIアクセス:ISE API Gateway Database Serviceはブリッジとして機能し、外部アプリケーションがISE RESTful APIを介してISEデータベースとやり取りできるようにします。これらのAPIを使用して、ISEデータベースに保存されている次のようなデータを取得または変更できます。

- ユーザ認証ログ。
- ネットワークアクセスポリシー。
- デバイスのプロファイル情報。
- システムの構成と設定。

2. 外部システム統合の有効化：このサービスは、ISEを次のような外部システムと統合する際に重要な役割を果たします。

- 外部認証サーバ(LDAP、Active Directory、RADIUS)
- ネットワーク管理システム(NMS)。
- Security Information and Event Management(SIEM)ソリューション
- ISEデータとの対話を必要とするカスタムアプリケーションまたはサービス。

API Gateway Database ServiceはAPIアクセスを提供することにより、これらの外部システムが外部イベントに応答してISEデータのクエリ、ISEへの更新の送信、またはISE内での特定のアクションのトリガーを実行できるようにします。

3. RESTful API通信のサポート:ISEは、HTTP/HTTPS経由で動作するように設計されたRESTful APIを公開します。APIゲートウェイデータベースサービスは、API要求および応答のフローを管理し、要求が認証され、処理され、応答でISEデータベースから適切なデータが返されることを保証します。

ISE API Gatewayサービス

ISE API Gateway Serviceは、ISEサービス、データ、および機能へのRESTful APIアクセスを提供する重要なコンポーネントです。ISEと外部システム間のブリッジとして機能し、これらのシステムがISEネットワークアクセスコントロール、ポリシー適用、認証、およびその他のサービスとプログラムでやりとりできるようにします。API Gatewayにより、サードパーティ製アプリケーション、ネットワーク管理システム、およびカスタムアプリケーションは、手動による介入やISEユーザインターフェイスへの直接アクセスを必要とせずにCisco ISEと対話できます。

ISE API Gatewayサービスの主要機能

1. ISEへのAPIアクセスの有効化：ISE API Gateway Serviceにより、外部システムはRESTful APIを使用してCisco ISEのデータとポリシーに安全にアクセスし、やり取りすることができます。これにより、認証、ポリシーの適用、セッション管理などのISE機能へのプログラムによるアクセスが提供されます。

2. プログラムによる制御の提供:API Gatewayサービスにより、ISE機能のプログラムによる制御が可能になります。管理者と開発者は、APIを使用して次の操作を実行できます。

- ネットワークポリシーを取得または変更します。
- ユーザー· セッションおよび認証ログのクエリーまたは管理
- ネットワークアクセス制御規則を作成および管理します。
- デバイスプロファイルにアクセスするか、デバイスプロファイルを更新します。

この制御は、リアルタイムデータに基づいてネットワークアクセスポリシーを動的に調整したり、ISEをより広範なセキュリティ自動化プラットフォームに統合するなど、自動化またはカスタムワークフローオーケストレーションに活用できます。

3. モニタリングとレポート:API Gateway Serviceを使用すると、外部システムは運用中のISEログ、セッション履歴、およびポリシー適用の詳細からデータを収集できます。これは次の場合に重要です。

- コンプライアンスレポート：
- セキュリティモニタリング。
- インシデント対応

APIコールを使用して、ログ、監査情報、およびイベントをプルできます。これにより、セキュリティチームは、一元化されたダッシュボードまたはレポートツールからISEアクティビティを監視できます。

ISE API GatewayサービスおよびISE API Gateway Databaseサービスの確認とトラブルシューティング

1. ISEノードの管理証明書がアクティブで有効であることを確認します。Administration > Certificates > Select the node > Select Admin Certificateの順に移動します。Viewをクリックして、ISEノードの管理証明書のステータスを確認します。

2. ise-api-gateway、api-gateway、apiserviceコンポーネントをデバッグに設定し、次のコマンド

を使用してログを追跡できます。

- show logging application ise-psc.log tail（隠しコマンド）
- show logging application api-gateway.log tail（ベータ版）

ISE pxGridダイレクトサービス

ISE pxGrid Direct Serviceは、ISEでpxGrid(Platform Exchange Grid)機能をサポートする重要なコンポーネントです。pxGridは、シスコのネットワークセキュリティソリューションとサードパーティのアプリケーション、サービス、およびデバイスとの間で、セキュアで標準化されたスケーラブルなデータ共有および統合を促進するシスコテクノロジーです。ISE pxGrid Direct Serviceを使用すると、中継装置やサービスを必要とせずに、ISEと他のpxGrid互換システムとの間で直接通信を行うことができます。

ISE pxGrid Directサービスの主な機能

1. サードパーティシステムとの直接統合:ISE pxGridダイレクトサービスにより、ISEは、ファイアウォール、ルータ、NACソリューション、SIEMプラットフォーム、およびその他のセキュリティアプライアンスなどのサードパーティネットワークセキュリティシステムと直接統合できます。これらのシステムは、ネットワークアクセスイベント、セキュリティインシデント、およびコンテキストに基づくネットワークデータに関する情報を交換できます。

2. コンテキスト共有:pxGridの主な機能の1つは、コンテキスト情報（デバイスID、ユーザロール、セキュリティポスチャ、ネットワークアクセス情報など）の共有です。 pxGrid Direct Serviceを使用すると、ISEはRADIUSやTACACS+などの従来の方法に依存することなく、このコンテキストを他のデバイスやアプリケーションと直接共有できます。

3. 簡素化された通信:pxGridを使用すると、ISEは標準化されたプロトコルを使用してサードパーティソリューションと通信し、情報を交換できます。これにより、システムは個々のサードパーティソリューションごとにカスタム統合を用意する必要がなくなるため、統合プロセスが簡素化されます。

4. セキュリティとコンプライアンスの強化:pxGrid Direct Serviceでは、ネットワークエコシステム内のすべてのシステムが、ユーザ、デバイス、セキュリティポリシーに関する同じリアルタイムのコンテキストデータにアクセスできるようにすることで、セキュリティ体制とコンプライアンスも強化されます。これにより、環境全体でネットワークセキュリティポリシーをより調整された方法で適用できます。

ISEPxgrid Directサービスの確認とトラブルシューティング

1. Cisco TACに連絡して、**edda*.lock***が/tmpフォルダにあるかどうかを確認する。ロックされている場合、Cisco TACはロックを解除し、Pxgrid Directサービスをルートから再起動します。

2. トラブルシューティングのために、ISEノードで**PxGrid Direct**コンポーネントをデバッグに設定します。ログは、次のコマンドを使用して、ISEサポートバンドルまたはISE CLIを介して保護できます。

ロギングアプリケーションpxgriddirect-service.log**を表示します**

ロギングアプリケーション pxgriddirect-connector.log を表示する

前述のログは、Cisco ISEがフェッチおよび受信したエンドポイントデータに関する情報と、Pxgridコネクタの接続ステータスを示します。

Segmentation Policyサービス

セグメンテーションポリシーサービスは、ユーザID、デバイスポスチャ、またはその他のコンテキスト情報に基づいてネットワークセグメンテーションポリシーを適用するための主要コンポーネントです。特定のネットワークセグメントへのユーザとデバイスのアクセスを制御し、許可されたユーザまたは準拠するデバイスのみがネットワークの特定の部分にアクセスできるようにします。 ネットワークのセグメント化は、ネットワークの攻撃対象領域を縮小し、脅威の横移動を防止し、規制に確実に準拠するために不可欠です。ISEのSegmentation Policy Serviceを使用して、ネットワーク全体でこれらのネットワークセグメンテーションルールを動的かつ柔軟に適用します。

Segmentation Policy Serviceの主要機能

1. ネットワークセグメントの定義:ISEのセグメンテーションポリシーサービスを使用すると、管理者はユーザまたはデバイスの特性に基づいて、さまざまなネットワークセグメント（サブネットまたはVLAN）を定義できます。例：

- 異なるセキュリティポスチャを持つデバイスを異なるセグメントに割り当てることができます（たとえば、あるVLANの信頼できるデバイスと別のVLANの信頼できないデバイス）。
- 権限を最小限に抑え、機密リソースへのアクセスを制限するために、異なる部門や役割のユーザを異なるネットワークセグメントに割り当てることができます。

2. 動的なセグメント化：このサービスは、動的なネットワークセグメント化を可能にします。つまり、ネットワークセグメントまたはVLANはリアルタイムの条件に基づいて変更できます。例：

- ユーザは、そのロールまたはデバイスのヘルスステータスに基づいて、特定のVLANに割り当てることができます。
- 準拠していないと見なされるデバイス、または古いオペレーティングシステムを実行しているデバイスは、修復されるまで隔離またはゲストVLANに移動できます。

3. ポリシーベースの適用:Segmentation Policy Serviceは、ポリシーを使用して、デバイスまたはユーザをどのセグメントに配置する必要があるかを決定します。これらのポリシーでは、次のようなさまざまな要因が考慮されます。

- ユーザID：ユーザロールまたは属性に基づきます。
- デバイスポスチャ：デバイスの健全性またはコンプライアンスステータス（例：最新のアンチウイルスソフトウェアを実行しているか）。
- ロケーション：ネットワーク内のユーザまたはデバイスの物理的な場所（オフィス、ゲストエリア、リモートアクセスなど）。
- アクセス時間：アクセス要求が行われる曜日または曜日の時間。

4. セキュリティポリシーの適用：セグメンテーションポリシーサービスは、RADIUSやVLAN割り

当てなどの業界標準を利用することで、ネットワークデバイス（スイッチ、ルータ、ファイアウォールなど）全体にセキュリティポリシーを一貫して適用します。これにより、Cisco ISEはネットワークインフラストラクチャデバイスと通信して、必要なセグメンテーションポリシーを適用できます。

Segmentation Policy Serviceの確認とトラブルシューティング

1.Work Centers > TrustSec > Overview > Dashboardの順に移動して、セグメンテーションが正しく設定されているかどうかを確認します。

2. Work Centers > TrustSec > Reportsの順に選択し、TrustSec reportsを選択して、セグメンテーションポリシーサービスのステータスとレポートを確認します。

REST認証サービス

REST認証サービスは、RESTful APIを使用して認証機能を提供するサービスです。標準のRESTプロトコルを使用してHTTP(S)経由でISEとやり取りすることで、外部のアプリケーションおよびシステムがユーザまたはデバイスを認証できるようになります。このサービスにより、Cisco ISE認証機能を、ユーザまたはデバイスの認証を必要とするが従来の方法（RADIUSやTACACS+など）を使用できないサードパーティ製アプリケーションまたはシステムとシームレスに統合できます。

REST認証サービスの主な機能

1. RESTful認証:REST認証サービスは、REST APIプロトコルを介した認証要求を有効にします。これにより、外部システム（アプリケーション、サードパーティのネットワークデバイス、サービスなど）は、認証サーバとしてISEを使用し、RADIUSやTACACS+などの従来の認証プロトコルではなく、RESTful Webサービスコールを通じて、ユーザやデバイスを認証できます。

2. 外部アプリケーションとの統合：このサービスは、ユーザまたはデバイスを認証する必要があるが、従来の認証方法（RADIUSまたはTACACS+など）を使用しない外部アプリケーション用に設計されています。 代わりに、REST APIを介してISEと対話できるため、ISE認証をWebベースまたはクラウドネイティブアプリケーションに簡単に統合できます。

3. 柔軟でスケーラブルな認証:REST認証サービスは、ネットワークデバイスやオンプレミスソリューションに限定されない、スケーラブルな認証方法を提供します。ISEにクレデンシャルとポリシーを照会することでユーザまたはデバイスを認証する必要があるクラウドサービス、モバイルアプリケーション、およびその他のWebベースのプラットフォームで使用できます。

4. 簡単な適用:REST APIは標準化されたインターフェイスを提供します。これは、従来の方法と比較して、最新のソフトウェアおよびアプリケーションに簡単に適用して統合できます。JSON形式の応答を提供し、GET、POST、PUT、DELETEなどのHTTPメソッドを使用して、ISEを認証に統合するWeb開発者やシステムがアクセスしやすくなるようにします。

Rest認証の検証およびトラブルシューティング

1. オープンAPI関連の問題をトラブルシューティングするには、apiserviceコンポーネントを

debugに設定します。

2. ERS APIに関連する問題をトラブルシューティングするには、ersコンポーネントをdebugに設定します。

APIサービスのGUIページ(https://{iseip}:{port}/api/swagger-ui/index.htmlまたはhttps://{iseip}:9060/ers/sdk)にアクセスできれば、APIサービスが期待どおりに動作していると判断できます。

APIの詳細については、『APIのドキュメント』を参照してください。

SSEコネクタ

SSEコネクタ(Secure Software-Defined Edge Connector)は、ISEとCisco Secure Software-Defined Access(SD-Access)ソリューションを統合するサービスです。SSE Connectorにより、ISEはCisco DNA Centerと安全に通信でき、SD-Access環境でのネットワークポリシー、セグメンテーション、およびエッジセキュリティ管理の自動化が可能になります。

SSEコネクタの主な機能

1. サードパーティセキュリティシステムとの統合：SSEコネクタにより、Cisco ISEと、ファイアウォール、侵入防御システム(IPS)、ネットワークアクセスコントロール(NAC)ソリューション、セキュリティ情報およびイベント管理(SIEM)システムなどのサードパーティセキュリティシステムとの統合が容易になります。これらの外部システムは、ISEとの間で安全な方法でデータを送受信でき、これを使用してより動的なポリシーを適用できます。

2. リアルタイムの脅威インテリジェンス:SSEコネクタは、ISEを他のセキュリティシステムと接続することで、リアルタイムの脅威インテリジェンスの交換を可能にします。この情報には、疑わしいアクティビティ、侵害されたエンドポイント、他のセキュリティシステムで検出された悪意のある動作などが含まれ、ISEは現在の脅威レベルやデバイスのステータスに基づいてアクセスポリシーを動的に調整できます。

3. 自動修復:SSEコネクタによって実現される統合により、自動修復ワークフローをサポートできます。たとえば、システムに外部セキュリティアプライアンスによるセキュリティ侵害のフラグが立てられている場合、ISEはネットワークアクセスをブロックするポリシーを自動的に適用したり、さらなる調査のためにエンドポイントを修復ネットワークセグメントにリダイレクトしたりできます。

SSEコネクタの確認とトラブルシューティング

1. SSEコネクタは、ISEでPassiveIDサービスが有効になっている場合にのみ有効になります。

2. SSEコネクタ関連のメッセージの詳細については、デバッグのsse-connector（ connector.log)コンポーネントを参照してください。

Hermes(pxGrid Cloud Agent)

Hermes(pxGrid Cloud Agent)は、クラウド環境でISEとpxGrid(Platform Exchange Grid)エコシス

テムの統合を促進するコンポーネントです。Hermesは、ISEとクラウドベースのサービスまたはプラットフォーム間の通信を可能にするために使用されるクラウドベースのエージェントで、異なるネットワークおよびセキュリティシステム間でコンテキスト情報を共有するためのpxGridフレームワークをサポートします。

Hermesの主な機能(pxGrid Cloud Agent)

1. クラウドとオンプレミスの統合：Hermes(pxGrid Cloud Agent)は、クラウドベースのサービスとオンプレミスのISEインフラストラクチャの間のシームレスな統合を促進するように設計されています。pxGridの機能を従来のオンプレミスネットワーク環境の枠を超えて拡張し、クラウドベースのアプリケーションおよびサービス全体に対して安全なデータ交換とポリシー適用を可能にします。

2. pxGridエコシステムサポート:pxGridは、ネットワークセキュリティソリューション間でコンテキストと情報を安全に共有するためのシスコプラットフォームです。HermesはpxGridのクラウドエージェントとして機能し、ISEとさまざまなクラウドベースサービス間のセキュアなリアルタイム通信を可能にします。この統合により、オンプレミス環境とクラウド環境の両方でネットワークセキュリティポリシーの一貫性が保たれ、セキュリティの管理と適用が容易になります。

3. クラウドベースのエンドポイントの可視性:Hermesの主な利点の1つは、ISEがオンプレミスのエンドポイントを可視化するのと同様に、クラウドベースのエンドポイントを可視化できることです。コンプライアンスポスチャ、セキュリティステータス、ID情報など、クラウド内のデバイスとユーザに関するデータを収集できます。これにより、ISEはオンプレミスデバイスと同様に、クラウドエンドポイントにネットワークアクセスポリシーを適用できます。

4. クラウド環境へのISEのシームレスな拡張:Hermesの主な利点の1つは、ISEのオンプレミス環境と、増え続けるクラウドネイティブアプリケーションとの間にシームレスなブリッジを提供することです。これにより、既存のインフラストラクチャを全面的に見直すことなく、ISEセキュリティポリシー、認証方式、アクセスコントロールをクラウドサービスに簡単に拡張できます。

Hermesの検証およびトラブルシューティング(Pxgrid Cloud Agent)

1. デフォルトでは、Hermesサービスは無効になっており、ISEとCisco PxGridクラウドを接続するとHermesサービスが有効になります。したがって、ISEでHermesサービスが無効になっている場合は、**ISE GUI > Administration > Deployment**でPxgrid Cloudオプションが有効になっていることを確認し、ISEノードを選択します。編集、**Pxgrid**クラウドの有効化

2. Pxgridクラウドに関連する問題のトラブルシューティングに役立つデバッグは、**hermes.log**と**pxcloud.log**です。 これらのデバッグは、Pxgridクラウドが有効になっているPxgridノードでのみ使用できます。

McTrust（Meraki同期サービス）

McTrust(Meraki Sync Service)は、Cisco ISEシステムとCisco Merakiシステムの統合を可能にするサービスで、特にネットワークデバイスとアクセスポリシーの同期と管理に使用されます。McTrustサービスは、Merakiのクラウドマネージドネットワークインフラストラクチャと ISEオンプレミスIDおよびポリシー管理システムの間でユーザとデバイスの情報を同期するコネクタとし

て機能します。

McTrustの主な特長と機能（Meraki同期サービス）

1. Merakiデバイスとのシームレスな統合：McTrustにより、ISEはMerakiのクラウド管理型デバイスと同期および統合できます。これには、Merakiのポートフォリオに含まれるMerakiアクセスポイント、スイッチ、セキュリティアプライアンスなどのデバイスが含まれます。ISEがMerakiのインフラストラクチャと直接通信できるようになるため、Merakiが管理するデバイスにネットワークアクセスコントロールポリシーを簡単に適用できます。

2. デバイスの自動同期:Meraki同期サービスは、ISEポリシーをMerakiネットワークデバイスと自動的に同期します。つまり、ISEのネットワークアクセスコントロールポリシーに加えられた変更は、手動による介入を必要とせずに、Merakiデバイスに自動的に反映されます。これにより、管理者はMerakiとISEの両方のプラットフォームでネットワークアクセスを簡単に管理できます。

3. Meraki管理対象デバイスに対するポリシー適用:McTrustでは、ISEが認証とデバイスポスチャに基づいてMerakiデバイスにネットワークアクセスポリシーを適用できます。アクセスを要求しているデバイスまたはユーザのセキュリティポスチャに応じて、VLAN割り当ての調整、アクセスコントロールリスト(ACL)の適用、特定のネットワークリソースへのアクセス制限などのポリシーをMerakiネットワーク要素に動的に割り当てることができます。

4. Merakiダッシュボードの統合:McTrustはISEをMerakiダッシュボードと直接統合し、統合された管理インターフェイスを提供します。この統合により、管理者はMerakiデバイスとISE管理リソースの両方に関するネットワークポリシーとアクセスコントロールルールを、Merakiクラウド管理インターフェイス内から表示および管理できます。

McTrust（Meraki同期サービス）の検証およびトラブルシューティング

1.ISE GUI -> Work Centers -> TrustSec -> Integrations -> Sync statusにログインします。確認された問題またはエラーを確認します。

2. ISEノードのすべての管理証明書がアクティブで有効であることを確認します。

Meraki同期サービスのトラブルシューティングに役立つデバッグ情報は、meraki-connector.logです。

ISEノードエクスポータ

ISEノードエクスポータサービスは、ISEシステム、特にISEノード（管理ノード、モニタリングノード、ポリシーサービスノードなど）からパフォーマンスメトリックを監視および収集するために使用されるコンポーネントです。

ISEノードエクスポータの主な機能

1. メトリックエクスポート:ISEノードエクスポータは、CPU使用率、メモリ使用率、ディスク使用率、ネットワーク統計情報、システム負荷、およびその他のオペレーティングシステムレベル

のメトリックなど、さまざまなパフォーマンス関連のメトリックを提供します。これらのメトリックは、ISEノードの健全性とパフォーマンスのモニタリングに使用され、Grafanaなどのモニタリングダッシュボードで可視化できます。

2. システムヘルスモニタリング：パフォーマンスデータをPrometheusにエクスポートすることで、ISEノードエクスポータはISEノードの健全性と動作ステータスを継続的にモニタリングできます。管理者は、事前定義されたしきい値に基づいてアラートを作成し、パフォーマンスの低下やシステムの問題を通知できます。

3. Prometheusの統合：通常、ISEノードエクスポータは、信頼性と拡張性を目的として設計されたオープンソースのモニタリングおよび警告ツールキットであるPrometheusと組み合わせて使用されます。Node Exporterは、Prometheusが時系列データを収集および保存するためにスクレイピングできるシステムレベルのメトリックを公開します。

ISE Prometheusサービス

ISE Prometheusサービスは、PrometheusとISEを統合して、ISEシステムからのパフォーマンスメトリックのモニタリングと収集を可能にするサービスです。Prometheusは、時系列データの収集、保存、分析に使用されるオープン・ソースの監視およびアラート・ツールキットであり、ISE Prometheusサービスにより、ISEは監視目的で内部メトリックをPrometheusに公開できます。

ISE Prometheusサービスの主な機能

1. モニタリングのためのメトリック収集:ISE Prometheusサービスは、ISEシステムに関連するさまざまな運用メトリックおよびパフォーマンスメトリックをエクスポートするように設計されています。これらのメトリックには通常、CPU使用率とシステム負荷、メモリ使用率、ディスク使用率とI/Oパフォーマンス、ネットワーク統計、認証要求統計、ポリシー適用統計、システムの健全性と稼働時間のデータが含まれますが、これらに限定されるわけではありません

2. Prometheusの統合:Prometheusサービスにより、ISEはPrometheusと互換性のある形式でデータを公開し、定期的にデータを消去できます。Prometheusはデータを時系列データベースに保存し、ISEシステムの傾向とパフォーマンス履歴を追跡できるようにします。

3. Grafanaによる可視化とレポート作成:ISEのPrometheusサービスは、一般的なオープンソースの可視化ツールであるGrafanaとシームレスに統合されます。メトリックをPrometheusにエクスポートした後、管理者はGrafanaダッシュボードを使用してデータをリアルタイムで視覚化できます。これにより、ISE導入におけるパフォーマンスのボトルネック、システムの傾向、潜在的な問題を簡単に特定できます。

ISE Grafanaサービス

ISE Grafanaサービスは、モニタリングとデータ可視化のためのオープンソースプラットフォームであるGrafanaを使用して、システムパフォーマンスメトリックの可視化を提供するサービスです。Prometheusとの統合により、ISEから収集されたリアルタイムおよび履歴データを表示し、管理者がISEシステムの稼働状態、パフォーマンス、使用状況に関する洞察を提供するインタラクティブなダッシュボードを作成できるようにします。

ISE Grafanaサービスの主な機能

1. カスタマイズ可能なダッシュボード:Grafanaは高度なカスタマイズが可能で、管理者は特定のモニタリングニーズに応じてダッシュボードを作成および変更できます。Prometheusから特定のデータポイントを抽出するためのカスタムクエリを作成できます。これらのクエリは、グラフ、表、ヒートマップなどのさまざまな形式で視覚化できます。

2. 分散型ISE導入の集中型モニタリング：複数のISEノードが異なる場所に導入されている分散型ISE導入では、Grafanaは各ノードから収集されたすべてのシステムメトリックの集中型ビューを提供します。これにより、管理者は単一の場所からISE環境全体のパフォーマンスを監視できます。

3. 履歴データとトレンド分析:GrafanaはPrometheusに保存されたデータを使用して、システム指標の履歴分析を可能にし、管理者は時間の経過とともにトレンドを追跡できます。たとえば、過去1か月の間にCPU使用率がどのように変化したか、または認証成功率がどのように変動したかを監視できます。この履歴データは、キャパシティプランニング、傾向分析、および長期的な問題の特定に役立ちます。

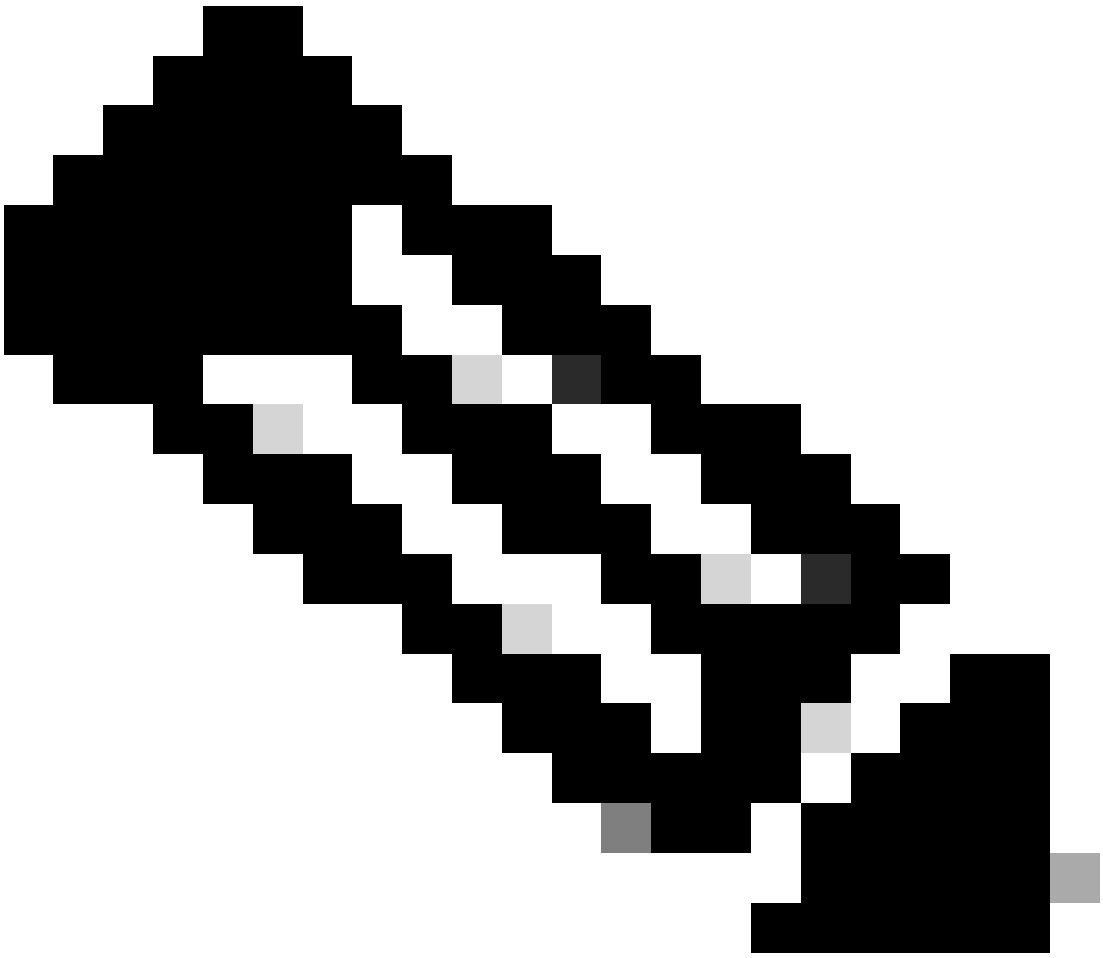
ISE Grafanaサービス、**ISE Prometheus**サービス、**ISE**ノードエクスポータの**確認**とトラブルシューティング

1. ISE Grafanaサービス、ISE Prometheusサービス、およびISEノードエクスポータサービスは連携して動作し、Grafanaスタックサービスと呼ばれます。これらのサービスのトラブルシューティングに有効にする特定のデバッグはありません。ただし、これらのコマンドはトラブルシューティングに役立ちます。

show logging application ise-prometheus/prometheus.log（登録ユーザ専用）

show logging application ise-node-exporter/node-exporter.log（登録ユーザ専用）

show logging application ise-grafana/grafana.log（登録ユーザ専用）



注：モニタリングを有効にすると、ISE Node Exporter、ISE Prometheusサービス、およびISE Grafanaサービスが実行されている必要があります。これらのサービスのいずれかを中断すると、データ収集時に問題が発生します。

ISE MNT LogAnalytics Elasticsearch

ISE MNT LogAnalytics Elasticsearchは、ElasticsearchとISEモニタリングおよびトラブルシューティング(MNT)機能を統合するコンポーネントです。ISEログおよびイベントに関連するログの集約、検索、分析に使用されます。Elasticsearchは、広く使用されている分散型検索および分析エンジンであり、ISEと統合すると、ISEコンポーネントによって生成されたログデータを保存、分析、可視化するシステムの機能が強化されます。

ISE MNT LogAnalytics Elasticsearchの主な機能

1. ログの保存とインデックス作成：ISEのElasticsearchサービスは、ISEによって生成されたログデータの保存とインデックス作成を行います。Elasticsearchは分散型の検索および分析エンジンであり、特定のイベント、エラー、またはシステムアクティビティを迅速に検索、照会、および取得できるようにISEログを保存できます。

2. ログ分析との統合：ISE MNT LogAnalytics Elasticsearchはログ分析と連携して、包括的なロギングソリューションを提供します。これにより、ISEは認証、ポリシーの適用、システム操作、およびその他のアクティビティに関連するログデータを収集できます。このデータはElasticsearchに保存されるため、詳細な分析を実行し、ISEの動作を把握しやすくなります。

3. ロギングの一元化:ISEはElasticsearchと統合することで、一元化されたロギングソリューションを提供します。これは、分散されたログ収集を必要とする環境にとって重要です。これにより、管理者は単一の統合インターフェイスで複数のISEノードのログを表示および分析でき、ISEのパフォーマンスのトラブルシューティングと監視が容易になります。

4. ログ分析とトラブルシューティング:ISE MNT LogAnalytics Elasticsearchサービスは、管理者がログデータに簡単にアクセスできるようにすることで、システムの動作を分析し、問題をトラブルシューティングできるようにします。たとえば、認証エラーの急増や予期しないシステム停止が発生した場合、Elasticsearchではログデータのクエリを迅速に実行して根本原因を特定できます。

ISE M&T LogAnalytics Elasticsearchの検証およびトラブルシューティング

1. ISEのログ分析サービスを無効にして再度有効にすることが役に立ちます。Operations > System 360 > Settings > Log analytics（トグルオプションを使用して無効化および有効化）の順に移動します。

2. ISEルートからM&T LogAnalyticsを再起動すると、この問題は解決します。このアクションを実行するには、Cisco TACにお問い合わせください。

既知の障害

Cisco Bug ID・ 66198

ISE Logstashサービス

ISE Logstash Serviceは、オープンソースのデータ処理パイプラインであるLogstashとISEを統合して、ログの収集、変換、転送を行うコンポーネントです。Logstashはログコレクタおよびログフォワーダとして機能し、ISEログを処理して他のシステムに送信し、分析、保存、およびモニタリングを行うことができます。 Logstashは、ログやその他のデータをさまざまなソースから中央の場所に収集、解析、転送して、保存、分析、視覚化を行う強力なオープンソースツールです。ISEのコンテキストでは、ISE Logstash Serviceを使用して構造化された形式でログを処理し、中央集中型のロギングシステムに転送します。中央集中型のロギングシステムでは、ログをさらに分析、監視、および可視化できます。

ISE Logstashサービスの主な機能

1. ログ収集と転送：ISE Logstashサービスの主な機能は、さまざまなISEコンポーネント（認証ログ、システムログ、ポリシー適用ログなど）からログデータを収集し、中央の場所（通常はElasticsearchまたは他のログ管理システム）に転送して、保存と分析を行うことです。

2. ログの解析:Logstashでは、収集されたログを解析して構造化された形式に変換できます。未加工のログデータを処理し、そこから重要な情報を抽出して、ログエントリをクエリと分析が容易

な形式に変換します。これには、Elasticsearchまたは他のシステムにデータを転送する前に、データをフィルタリング、解析、および強化することが含まれます。

ISE Logstashサービスの検証およびトラブルシューティング

1. 有効にする特定のデバッグはありません。ただし、**show logging application ise-logstash/logstash.log**は、サービスの状態に関する洞察を提供します。

2. ISEのログ分析サービスを無効にし、再度有効にすることが役立つ必要があります。**Operations > System 360 > Settings > Log analytics**の順に移動します（トグルオプションを使用して無効化および有効化します）。

Logstashサービスに関連する既知の不具合

Cisco Bug ID・ 74832

Cisco Bug ID・ 58596

ISE Kibanaサービス

ISE Kibana Serviceは、オープンソースのデータ可視化ツールであるKibanaと、ISEロギングおよびモニタリングインフラストラクチャを統合するコンポーネントです。Kibanaは Elasticsearch（ログデータの保存とインデックス作成）と連携して、ISEログとパフォーマンスメトリックを可視化、検索、分析する強力なプラットフォームを提供します。

ISE Kibanaサービスの主な特長と機能

1. データの可視化:ISE Kibanaサービスを使用すると、管理者はISEから収集されたログデータを視覚的に表現できます。これには次のものが含まれます。

- 認証、ポリシーの適用、ユーザアクティビティ、およびシステム状態の傾向を示すグラフ、グラフ、および表。
- 円グラフ、折れ線グラフ、棒グラフを使用して、失敗したログイン数、セッション期間、エラーの推移など、特定のメトリックを追跡できます。

ISE Kibanaサービスの確認とトラブルシューティング

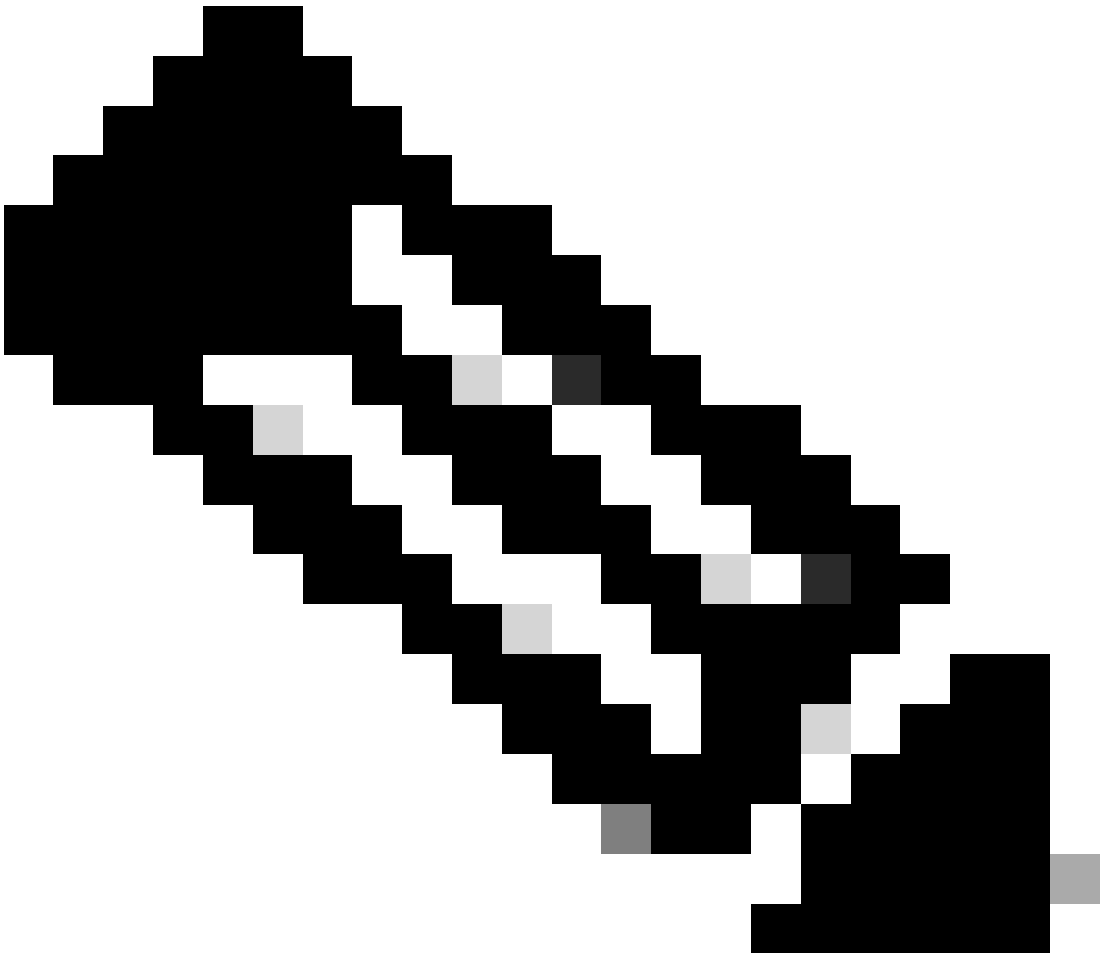
1. ISE kibanaサービスが実行されていない場合、ISEでログ分析を無効および再度有効にします。操作>システム360 >設定、ログ分析に移動します（トグルオプションを使用して無効および有効にします）。

2. 多くのシナリオでは、/etc/hostsフォルダに重複するエントリがあり、これが問題の原因になっている可能性があります。重複したエントリを削除するには、TACにお問い合わせください。

Kibana問題に関連する既知の不具合

Cisco Bug ID・ 78050

Cisco Bug ID・ 59848



注：ログ分析を有効にすると、ISE MNT LogAnalytics Elasticsearch、ISE Logstash Service、ISE Kibana Serviceが実行されている必要があり、これらのサービスのいずれかを中断すると、データ収集時に問題が発生します。

ISEネイティブIPSecサービス

ISEネイティブIPSecサービスは、IPSec（インターネットプロトコルセキュリティ）の組み込みサポートを参照します。このサービスは、ISEノード間、またはISEとその他のネットワークデバイス間でセキュアな通信を提供します。IPSecは、通信セッションで各IPパケットを認証および暗号化することでネットワーク通信を保護するために使用されるプロトコルスイートです。ネイティブIPSecサービスは、より広範なセキュリティおよびネットワークアクセス管理フレームワークの一部です。IPSec VPN接続を処理および管理する機能を提供し、ISEシステムとリモートエンドポイント間で転送されるデータの安全性を確保します。これには、クライアントデバイス、ネットワークアクセスデバイス（ルータやファイアウォールなど）、または機密情報を保護するためにIPSec暗号化とトンネリングが必要なその他のISEノードとのインタラクションが含まれ

ます。

ISEネイティブIPSecサービスの主な機能

1. IPsec経由のセキュアな通信：ISE Native IPSec Serviceの主な機能は、IPsecを使用してセキュアな通信チャネルを確立し、維持することです。これには、暗号化および認証メカニズムを使用して、ISEと他のデバイスの間で送信されるデータが傍受、改ざん、不正アクセスから保護されることを保証することが含まれます。

2. IPsec VPN接続:ISEネイティブIPSecサービスは、IPsecプロトコルを使用してデータ伝送用の安全で暗号化されたトンネルを提供するVPN接続を容易にします。これは、信頼できないネットワーク（インターネットなど）経由でISE環境に安全にアクセスする必要があるリモートワーカー、ブランチオフィス、またはその他の場所に特に役立ちます。

3. リモートアクセスVPNのサポート：ネイティブIPSecサービスは、リモートアクセスVPN設定に関与できます。この設定では、オフサイトにあるユーザまたはデバイス（リモート従業員やブランチオフィスなど）がIPSecトンネルを介してISEシステムに安全に接続します。このサービスは、ISE環境に到達する前に、すべてのリモートアクセストラフィックが暗号化および認証されることを保証します。

4.IPsec VPNクライアントの互換性:ISEネイティブIPSecサービスにより、IPsec VPNクライアントとの互換性が確保されます。一般的なクライアント設定をサポートしているため、機密データをリスクにさらすことなく、デバイスを安全にネットワークに接続できます。

ネイティブIPSecサービスの確認とトラブルシューティング

1. ネイティブIPSecサービスに対して有効にする特定のデバッグはありません。ISE CLIでshow logging application strongswan/charon.log tail コマンドを使用してログを確認します。

2. トンネルに何らかの問題が見られた場合、GUI > Administration > System > Settings > Protocols > IPSec > Native IPSecを使用して、トンネル確立のステータスを確認します。

MFCプロファイラ

MFCプロファイラは、ネットワークデバイスとエンドポイントのプロファイリングに使用される特殊なコンポーネントです。プロファイリングは、ISEがネットワーク上のデバイスを識別し、分類し、デバイスのタイプと動作に基づいて適切なネットワークポリシーを適用できるため、ネットワークアクセス制御の重要な部分です。

ISEのMFCプロファイラサービスの主な機能

1. トラフィックプロファイリング：ISEのMFCプロファイラサービスは、トラフィックデータの収集とプロファイリングを行います。使用されているアプリケーションのタイプ、アクセスされるサービス、デバイスが示すトラフィックパターンなど、エンドポイントがネットワーク上でどのように動作するかを監視します。このデータは、各エンドポイントのプロファイルの作成に役立ちます。

2. エンドポイントプロファイリング:MFCプロファイラサービスを使用すると、ISEは動作に基づいてエンドポイントを特定および分類できます。たとえば、トラフィックパターンに基づいて、エンドポイントがプリンタ、コンピュータ、モバイルデバイスのいずれであるかを検出します。これにより、異なるタイプのデバイスに対してより具体的なポリシーを適用し、セキュリティと運用効率を向上させることができます。

MFCプロファイラサービスの確認とトラブルシューティング

1. ISE GUI -> Administration -> Profiling -> MFC profiling and AI rulesの順に移動し、サービスが有効になっているかどうかを確認します。

2. サービスが有効であるが、ISE CLIのshow application status ise コマンドを介して無効/実行されていないと表示される場合。 手順1を参照して、ISEのMFCプロファイリングサービスを無効にしてから再度有効にします。

トラブルシューティングに便利なデバッグ：デバッグのMFCプロファイラコンポーネント。ログは、サポートバンドルから確認するか、ISE CLIでshow logging application ise-pi-profiler.log tail コマンドを使用してログの末尾まで確認できます。

MFCプロファイラの既知の不具合が、無効な状態ではなく実行されていないことが示されている。

Cisco Bug ID： 72853

要点

1. サービスを回復するには、ISE CLIでapplication stop iseおよびapplication start iseコマンドを使用して、サービスを再起動します。

2. 問題が発生した場合、問題の詳細な検証のためにISE GUI/ISE CLIからキャプチャされるサポートバンドルがあることを確認します。GUIおよびCLIを使用したISEサポートバンドルの作成に関する参照リンク：Identity Services Engineでのサポートバンドルの収集

3. 問題がリソース、ロード平均、ディスク使用率などに関連する場合は、分析のためにスレッドダンプとヒープダンプを収集する必要があります。

4. ノードのリロードを実行する前に、Cisco TACに連絡して、詳細な分析のために安全なログを提供してください。

ISEの標準的な懸念事項

ISEサービスの問題とは別に、これらはISEノードで見られる懸念事項の一部であり、必要な基本的なトラブルシューティング手順も含まれています。

高負荷平均、リソース使用率の問題（CPU/メモリ/ディスク）、リソース不足の検証

1. ISE CLIでshow inventoryコマンドを使用して、シスコの推奨リソースがノードに割り当てられていることを確認します。

2. ISEノードのCLIからtech topコマンドを実行して、ISEのリソース使用率を確認します。

3. ISE CLIでshow diskコマンドを使用して、ディスク使用率を確認します。

4. 非アクティブなエンドポイントを消去し、ノードのローカルディスクを消去し、アップグレードのクリーンアップを実行します。

問題が解決しない場合は、Cisco　TACに連絡して、問題が発生しているノードからの安全なサポートバンドル、ヒープダンプ、スレッドダンプを提供してください。

ヒープダンプを保護するには、ISEノードのCLIにログインし、**application configure ise**コマンドを実行します。オプション**22**を選択します。

スレッドダンプを保護するには、ISEノードのCLIにログインし、**application configure ise**コマンドを実行し、オプション**23**を選択します。 スレッドダンプはサポートバンドルに含まれています。また、**show logging application appserver/catalina.out** コマンドを使用してISE CLIで追跡することもできます。

モニタリングの問題の確認とトラブルシューティング

ISEのモニタリングとトラブルシューティング(MnT)機能は、モニタリング、レポート、アラート機能を提供するISEアーキテクチャの主要なブロックの1つです。

ISEは、次を含む多くの場所でモニタリング情報を表示します。

- Cisco ISEホームページ
- コンテキスト表示ビュー
- RADIUSライブログとライブセッション
- グローバル検索
- 脅威中心型NACライブログ
- TACACSライブログ

監視とトラブルシューティングのカテゴリで見られる一般的な問題：

1. Radius/TACACSライブログが使用できない
2. ライブセッションは利用できません
3. 正常性の概要を利用できません
4. MnTノードで発生するパフォーマンス（CPU/メモリの高使用率）の問題

問題を絞り込むためにMnTノードでイネーブルにするデバッグ：

1. Cisco-mnt
2. コレクタ
3. Cpm-mnt
4. ランタイムロギング

デバッグで説明したコンポーネントに加えて、この情報はトラブルシューティングに役立ちます。

1. ライブセッションも影響を受けるか、ライブログのみか。
2. RadiusログまたはTACACSログのどちらか、あるいは両方が影響を受けますか。
3. MnTノードで高いCPU使用率または高いスワップ領域使用率が発生していますか。
4. MnTノード上にバッファファイルがいくつ表示されるか。バッファファイルは/opt/CSCOcpm/mnt/data/collectorにあります。
5. メモリとCPUの予約は有効になっていますか。有効になっていない場合は、有効にしてください。
6. MnT/config/session DBのリセットは最近実行されましたか。
7. PSNからMnTノードに送信されるsyslogが表示されますか。

MnTのSyslogサービスを使用している場合、トラブルシューティングのために次の情報が必要です。

1. セキュアなsyslogターゲットを使用していますか。無効にしないでください。スレッドにデッドロックが発生し、コレクタが機能しなくなることが判明しています。
2. セキュアなsyslogターゲットを使用していますか。Administration->Logging->Remote Logging Targets->Secure Syslog collector 1 and 2で、証明書マッピングが正しく設定されていることを確認します。
3. ロギングカテゴリが適切に設定されているか（未使用または不要なロギングカテゴリを削除することが推奨されるため、MnTノードの負荷が軽減されます）、およびロギングターゲットが正しく設定されているかどうかを確認します。
4. サポートバンドルのawrrep*.htmlファイルを確認して、より頻繁にsyslogを送信しているコンポーネント（たとえば、TACACSテーブルが挿入クエリまたは更新クエリで表示される場合）を理解し、そのヒントを得るには、コレクタログを確認して、より頻繁に送信されているsyslogを理解するように関連付けます

MnTノードのパフォーマンスに関連する問題の場合は、次の情報が必要です。

1. MnTノードのISE CLIからのtech top出力。

2. CPU使用率が高い場合、メモリ使用率やスワップ領域使用率も高くなっていますか。

3. ヒープダンプとスレッドダンプを確保したサポートバンドル。

参考

- Cisco Identity Services Engine 管理者ガイド リリース 3.3
- ISEでのデバッグのトラブルシューティングと有効化

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。