CHAPTER 25

モニタリングおよびトラブルシューティング

Cisco Identity Services Engine（ISE）ホームページ（ダッシュボードとも呼ばれる）の [操作（Operations）] タブでは、統合されたモニタリング、レポート、アラート、およびトラブルシューティングが、すべて 1 つの集中化された場所から提供されます。

この章では、モニタリングおよびトラブルシューティングの機能とタスクについて説明します。この章は、次の内容で構成されています。

（注） モニタリングおよびトラブルシューティングに関する固有の既知の問題および回避策のリストについては、『*Release Notes for the Cisco Identity Services Engine, Release 1.2*』を参照してください。

Cisco ISE のモニタリングおよびトラブルシューティング サービス

モニタリングおよびトラブルシューティング サービスは、すべての Cisco ISE 実行時サービスに対する包括的なアイデンティティ ソリューションであり、次のコンポーネントを使用します。

- モニタリング：ネットワーク上のアクセス アクティビティの状態を表す意味のあるデータのリアルタイム表示を提供します。これを把握することにより、操作の状態を簡単に解釈および発生させることができます。
- トラブルシューティング：ネットワーク上のアクセスの問題を解決するための状況に応じたガイダンスを提供します。また、ユーザの懸念に対応してタイムリーに解決策を提供できます。
- レポート：トレンドを分析し、システム パフォーマンスおよびネットワーク アクティビティをモニタするために使用できる、標準レポートのカタログを提供します。レポートをさまざまな方法でカスタマイズし、今後使用するために保存できます。

Cisco ISE ダッシュボード

Cisco ISE ダッシュボード、またはホームページは、Cisco ISE 管理コンソールにログインした後に表示されるランディング ページです。ダッシュボードは、ウィンドウの上部に沿って表示されるメトリック メーターと下にあるダッシュレットで構成された、集中化された管理コンソールです。

ダッシュボードのリアルタイム データによって、ネットワークにアクセスしているデバイスおよびユーザの一目で確認できるステータスと、システム健全性の概要が示されます。

（注）　ダッシュレットおよびメトリック メーターをダッシュボードに表示するには、管理 ISE ノードに Adobe Flash Player がインストールされている必要があります。

ダッシュボードでは、Network Privilege Framework（NPF）上にアクティビティが表示され、さまざまなコンポーネントに関する詳細が提供されます。

NPF は、表 25-1 に示されている 3 つの階層で構成されています。

表 25-1　NPF 階層

階層	仕様
1	802.1x、MAC 認証バイパス（MAB）、Cisco ISE プロファイラ サービスを使用したアイデンティティに基づくアクセス コントロール
2	802.1x、MAB、プロファイラ、ネットワーク アドミッション コントロール（NAC）マネージャのゲスト プロビジョニング、中央 Web 認証を使用したアイデンティティに基づくアクセス コントロール
3	802.1x、MAB、NAC マネージャのゲスト プロビジョニング、中央 Web 認証を使用したアイデンティティおよびポスチャに基づくアクセス コントロール

NPF 認証および許可では、イベントのフローが生成されます。異なるソースからのイベントが、Cisco ISE モニタリングおよびトラブルシューティング ツールによって収集され、要約されます。認証および許可の結果をダッシュボードで表示できます。または、任意の数のレポートを実行するように選択できます。詳細については、第 26 章「レポート」を参照してください。

NPF 認証および許可イベント フローでは、次のプロセスが使用されます。

1. NAD によって許可またはフレックス許可が実行されます。
2. 未知のエージェントレス アイデンティティが Web 許可を使用してプロファイリングされます。
3. RADIUS サーバによってアイデンティティが認証および許可されます。
4. 許可がポートでアイデンティティに対してプロビジョニングされます。
5. 許可されないエンドポイント トラフィックはドロップされます。

モニタリングおよびトラブルシューティング機能のユーザ ロールおよび権限

モニタリングおよびトラブルシューティング機能は、デフォルトのユーザ ロールに関連付けられます。実行を許可されるタスクは、割り当てられているユーザ ロールに直接関係します。ユーザ ロールおよびそれらに割り当てられている権限の詳細については、「Cisco ISE 管理者グループ、アクセス レベル、権限、および制約事項」を参照してください。

モニタリング データベースに保存されるデータ

Cisco ISE モニタリング サービスでは、データが収集され、特化したモニタリング データベースに格納されます。ネットワーク機能のモニタリングに使用されるデータのレートおよび量によっては、モニタリング専用のノードが必要な場合があります。Cisco ISE ネットワークによって、ポリシー サービス ノードまたはネットワーク デバイスからロギング データが高いレートで収集される場合は、モニタリング専用の Cisco ISE ノードを推奨します。

モニタリング データベースに格納される情報を管理するには、管理者はデータベースのフル バックアップおよび差分バックアップを実行する必要があります。これには、不要なデータの消去とデータベースの復元が含まれます。

関連項目

「データベースのモニタリング」（P.25-30）

モニタリングのためのデバイスの設定

モニタリング ノードにより、ネットワーク上のデバイスからのデータが受信および使用されて、ダッシュボードに表示されます。モニタリング ノードとネットワーク デバイス間の通信を有効にするには、スイッチおよびネットワーク アクセス デバイス（NAD）を正しく設定する必要があります。

これらのデバイスを設定する方法については、「ISE モニタリング用の NAD の設定」（P.G-38）を参照してください。

ネットワークのプロセス ステータスのモニタリング

[システム概要（System Summary）] ダッシュレットを使用して、Cisco ISE ダッシュボードからネットワークのプロセス ステータスを表示できます。たとえば、アプリケーション サーバやデータベースなどのプロセスが失敗すると、アラームが生成され、[システム概要（System Summary）] ダッシュレットを使用して結果を表示できます。

ステップ 1　Cisco ISE **ダッシュボード**に移動します。

ステップ 2　[システム概要（System Summary）] ダッシュレットを展開します。詳細なリアルタイム レポートが表示されます。

ステップ 3　ネットワーク上で実行されているプロセスについて、次の情報を確認します。

- プロセスの名前
- CPU およびメモリの使用率
- プロセスの実行開始からの時間

システム ステータス アイコンの色は、システムの健全性を示します。

- グリーン = 正常
- 黄 = 警告
- 赤 = 重大
- グレー = 情報なし

関連項目

- 「Cisco ISE のモニタリング ダッシュレットが Internet Explorer 8 で表示されない」（P.G-14）

ネットワーク認証のモニタリング

[認証（Authentications）] ダッシュレットで、成功および失敗したネットワーク認証を表示できます。ユーザまたはデバイスのタイプ、ロケーション、およびユーザまたはデバイスが属する ID グループに関するデータが表示されます。ダッシュレットの上部に沿って表示されるスパークラインは、直近の 24 時間と直近の 60 分での分散を表します。

ステップ 1　Cisco ISE **ダッシュボード**に移動します。

ステップ 2　[認証（Authentications）] ダッシュレットを展開します。詳細なリアルタイム レポートが表示されます。

ステップ 3　ネットワーク上で認証されたユーザまたはデバイスの情報を確認します。

ステップ 4　詳細について、データ カテゴリを展開します。

プロファイラ アクティビティおよびプロファイリングされたエンドポイントの決定

[プロファイリングされたエンドポイント（Profiled Endpoints）] ダッシュレットは、プロファイルが一致したネットワーク上のエンドポイントに焦点を当てます。各エンドポイントのプロファイル データが表示されます。たとえば、統計情報によってデバイスのタイプ、そのロケーション、およびその IP アドレスを判別できます。ダッシュレットの上部に沿って表示されるスパークラインは、直近の 24 時間と直近の 60 分でのエンドポイント アクティビティを表します。

ステップ 1　Cisco ISE **ダッシュボード**に移動します。

ステップ 2　[プロファイラ アクティビティ（Profiler Activity）] ダッシュレットで、積み上げ棒またはスパークラインにカーソルを合わせます。

ツール チップで詳細情報を提供します。

ステップ 3　詳細について、データ カテゴリを展開します。

ステップ 4　[プロファイラ アクティビティ（Profiler Activity）] ダッシュレットを展開します。詳細なリアルタイム レポートが表示されます。

[プロファイリングされたエンドポイント（Profiled Endpoints）] ダッシュレットは、不明なものも含め、直近の 24 時間にネットワーク上でプロファイリングされたエンドポイントの総数を表します。ネットワーク上で現在アクティブなエンドポイント数ではありません。ダッシュレットの上部に表示されるスパークライン メトリックは、直近の 24 時間と 60 分での時間固有の値を表します。

ポスチャ コンプライアンスのチェック

[ポスチャ コンプライアンス（Posture Compliance）] ダッシュレットは、ネットワークにアクセスしているユーザおよびそれらのユーザがポスチャ コンプライアンスを満たしているかどうかに関する情報を提供します。データは、現在ネットワークに接続されているデバイスに関して表示されます。積み上げ棒には、オペレーティング システムやその他の基準に従って配置された非コンプライアンス統計情報が表示されます。スパークラインは、ポスチャ試行の準拠と非準拠のパーセンテージを表します。

ステップ 1　Cisco ISE **ダッシュボード**に移動します。

ステップ 2　[ポスチャ コンプライアンス（Posture Compliance）] ダッシュレットで、積み上げ棒またはスパークラインにカーソルを合わせます。

ツール チップで詳細情報を提供します。

ステップ 3　詳細について、データ カテゴリを展開します。

ステップ 4　[ポスチャ コンプライアンス（Posture Compliance）] ダッシュレットを展開します。詳細なリアルタイム レポートが表示されます。

Cisco ISE アラーム

アラームは、ネットワーク上のクリティカル条件を通知し、アラーム ダッシュレットに表示されます。データ消去イベントなど、システム アクティビティの情報も提供されます。システム アクティビティの通知方法を設定したり、完全に無効にしたりすることができます。特定のアラームのしきい値も設定できます。

アラームには関連付けられているスケジュールがなく、イベント発生後即時に送信されます。任意の時点で、最新の 15,000 のアラームだけが保持されます。

イベントが繰り返し発生すると、同じアラームは最小期間の 2 時間抑制されます。イベントが繰り返し発生する間は、トリガーに応じて、アラームが再び表示されるのに最大 3 時間かかる場合があります。

表 25-2 に、すべての Cisco ISE アラーム、説明および解決策を示しています。

表 25-2　Cisco ISE アラーム

アラーム名	アラームの説明	アラームの解決策
管理および操作の監査管理		
管理者アカウントのロック / 無効	パスワードの失効または不正なログイン試行のために、管理者アカウントがロックされているか、無効になっています。詳細については、管理者パスワード ポリシーを参照してください。	管理者パスワードは、GUI または CLI を使用して他の管理者がリセットできます。

表 25-2　Cisco ISE アラーム （続き）

アラーム名	アラームの説明	アラームの解決策
バックアップが失敗しました	ISE バックアップ操作に失敗しました。	Cisco ISE とリポジトリ間のネットワーク接続を確認します。次の内容を確認してください。 • リポジトリに使用するクレデンシャルが正しい。 • リポジトリに十分なディスク領域がある。 • リポジトリ ユーザには書き込み権限がある。
CA サーバがダウンしています	CA サーバがダウンしています。	CA サービスが CA サーバ上で起動し動作中であることを確認します。
CA サーバが起動しています	CA サーバが起動しています。	CA サーバが起動していることを管理者に知らせる通知。
証明書の有効期限	この証明書の有効期限がもうすぐ切れます。失効すると、Cisco ISE はクライアントとのセキュアな通信を確立できない場合があります。	証明書を置き換えます。信頼証明書の場合、発行認証局（CA）にお問い合わせください。CA 署名付き証明書の場合、CSR を生成し、CA に新しい証明書を作成してもらいます。自己署名ローカル証明書の場合、Cisco ISE を使用して有効期限を延長します。使用されなくなったら、証明書を削除できます。
証明書の失効	この証明書の期限が切れています。Cisco ISE はクライアントとのセキュアな通信を確立できない場合があります。ノードツーノードの通信も影響を受ける場合があります。	証明書を置き換えます。信頼証明書の場合、発行認証局（CA）にお問い合わせください。CA 署名付き証明書の場合、CSR を生成し、CA に新しい証明書を作成してもらいます。自己署名ローカル証明書の場合、Cisco ISE を使用して有効期限を延長します。使用されなくなったら、証明書を削除できます。
証明書要求の転送が失敗しました	証明書要求の転送が失敗しました。	着信する証明書要求が送信者の属性に一致することを確認します。
設定変更	Cisco ISE 設定が更新されます。このアラームは、ユーザとエンドポイントのすべての設定変更に対してトリガーされません。	設定変更が予想されているかどうかを確認します。
CRL の取得が失敗しました	サーバから CRL を取得できません。指定した CRL が使用できない場合に発生することがあります。	ダウンロード URL が正しく、サービスに使用できることを確認します。
DNS 解決の障害	DNS 解決がノードで失敗しました。	コマンド **ip name-server** で設定された DNS サーバに到達可能かどうかを確認します。

表 25-2　Cisco ISE アラーム （続き）

アラーム名	アラームの説明	アラームの解決策
外部 MDM サーバの API バージョンの不一致	外部 MDM サーバの API バージョンが Cisco ISE で設定されたバージョンに一致しません。	MDM サーバの API バージョンが Cisco ISE 設定されているバージョンと同じであることを確認します。必要に応じて Cisco ISE MDM サーバの設定を更新します。
外部 MDM サーバ接続の障害	外部 MDM サーバへの接続に失敗しました。	MDM サーバが起動され、MDM サーバ上で Cisco ISE-MDM API サービスが実行されていることを確認します。
外部 MDM サーバの応答エラー	外部 MDM サーバの応答エラー。	Cisco ISE-MDM API サービスが MDM サーバ上で適切に実行されていることを確認します。
ファームウェアの更新が必要です	このホスト上でファームウェアの更新が必要です。	ファームウェアの更新を取得するには、Cisco Technical Assistance Center（TAC）にお問い合わせください。
不十分な仮想マシンのリソース	CPU、RAM、ディスク容量、または IOPS など、仮想マシン（VM）のリソースは、このホスト上で不十分です。	『Cisco ISE Hardware Installation Guide』で指定されているように VM ホストの最小要件を確認します。
設定のバックアップがスケジュールされていません	Cisco ISE 設定のバックアップがスケジュールされません。	設定のバックアップのスケジュールを作成します。
NTP サービスの障害	NTP サービスがこのノードでダウンしています。	これは、NTP サーバと Cisco ISE ノード間に大きな時間差（数千を超える）があるためである可能性があります。NTP サーバが正しく動作していることを確認し、**ntp server <servername>** CLI コマンドを使用して NTP サービスを再起動し、時間の差を修正します。
NTP 同期の障害	このノード上で設定されているすべての NTP サーバに到達不能です。	トラブルシューティングのために、CLI で **show ntp** コマンドを実行します Cisco ISE から NTP サーバに到達可能であることを確認します。NTP 認証が設定されている場合、キー ID と値がサーバのキー ID と値に一致することを確認します。
Operations DB の消去が失敗しました	Operations データベースから古いデータを消去できません。これは、M&T ノードがビジー状態の場合に発生する可能性があります。	データ消去監査レポートをチェックし、used_space が threshold_space 未満であることを確認します。CLI を使用して M&T ノードにログインし、消去操作を手動で実行します。
パッチの障害	パッチ プロセスがサーバ上で失敗しました。	パッチ プロセスをサーバに再インストールします。
パッチの成功	パッチ プロセスがサーバ上で成功しました。	—

表 25-2　Cisco ISE アラーム （続き）

アラーム名	アラームの説明	アラームの解決策
プロファイラ SNMP 要求の障害	SNMP 要求がタイム アウトしたか、または SNMP コミュニティまたはユーザ認証データが不正です。	SNMP が NAD で動作していることを確認し、Cisco ISE 上の SNMP 設定が NAD に一致していることを確認します。
複製に失敗しました	セカンダリ ノードは複製されたメッセージを消費できませんでした。	Cisco ISE GUI にログインし、展開ページで手動 syncup を実行します。影響を受ける Cisco ISE ノードを登録解除し、登録し直します。
復元に失敗しました	Cisco ISE 復元操作に失敗しました。	Cisco ISE とリポジトリ間のネットワーク接続を確認します。リポジトリに使用するクレデンシャルが正しいことを確認します。バックアップ ファイルが破損していないことを確認します。CLI から **reset-config** コマンドを実行し、正常な既知の最終バックアップを復元します。
ISE サービス		
認証非アクティブ（Authentication Inactivity）	Cisco ISE ポリシー サービス ノードは、ネットワーク デバイスから認証要求を受信していません。	ISE/NAD 設定を確認してください。ISE/NAD インフラストラクチャのネットワーク接続を確認します。
COA が失敗しました	ネットワーク デバイスは、Cisco ISE ポリシー サービス ノードによって発行された許可変更（CoA）要求を拒否しました。	ネットワーク デバイスが Cisco ISE からの許可変更（CoA）を受け入れるように設定されていることを確認します。CoA が有効なセッション上で発行されていることを確認します。
過度な認証試行 [1]	Cisco ISE ポリシー サービス ノードに、予想より高い認証レートが発生しています。	ネットワーク デバイスの再認証タイマーをチェックします。Cisco ISE インフラストラクチャのネットワーク接続を確認します。
過剰な失敗試行 [1]	Cisco ISE ポリシー サービス ノードに、予想より高い失敗レートが発生しています。	根本原因を識別するために認証手順を確認します。ID と秘密の不一致がないか、Cisco ISE/NAD 設定を確認します。
ID ストアが使用できません	Cisco ISE ポリシー サービス ノードは設定された ID ストアに到達できません。	Cisco ISE と ID ストア間のネットワーク接続を確認します。
設定が誤っているネットワーク デバイスが検出されました	Cisco ISE は NAS から多過ぎる RADIUS アカウンティング情報を検出しました	多過ぎる重複 RADIUS アカウンティング情報が NAS から ISE に送信されました。正確なアカウンティングの頻度で NAS を設定します。
設定が誤っているサプリカントが検出されました	Cisco ISE は、ネットワーク上で設定が誤っているサプリカントを検出しました	サプリカントの設定が正しいことを確認します。

表 25-2　Cisco ISE アラーム （続き）

アラーム名	アラームの説明	アラームの解決策
アカウンティングは開始されません	Cisco ISE ポリシー サービス ノードはセッションを許可しましたが、ネットワーク デバイスからアカウンティングの開始を受信しませんでした。	RADIUS アカウンティングがネットワーク デバイス上に設定されていることを確認します。ローカル認可用のネットワーク デバイス設定を確認します。
RADIUS 要求がドロップしました	NAD からの認証/アカウンティング要求がサイレントに廃棄されます。これは、RFC ごとの未知の NAD、不一致の共有秘密、または無効なパケットの内容によって発生することがあります。	NAD/AAA クライアントに有効な Cisco ISE で設定があることを確認します。NAD/AAA クライアントと Cisco ISE 上の共有秘密が一致するか確認します。AAA クライアントとネットワーク デバイスにハードウェアの問題または RADIUS 互換性の問題がないことを確認します。また、Cisco ISE にデバイスを接続するネットワークにハードウェア上の問題がないことを確認します。
SGACL ドロップ	セキュリティ グループ アクセス（SGACL）のドロップが発生しました。これは、SGA 対応デバイスが SGACL ポリシー違反によりパケットをドロップする場合に発生します。	RBACL ドロップ概要レポートを実行し、SGACL ドロップの原因となっているソースを確認します。不正なソースに CoA を発行して、セッションを再許可または切断します。
サプリカントが応答を停止しました	Cisco ISE は 120 秒前にクライアントに最後のメッセージを送信しましたが、クライアントからの応答がありません。	サプリカントが Cisco ISE との完全な EAP カンバセーションを行えるように適切に設定されていることを確認します。サプリカントとの間で EAP メッセージを転送するように NAS が正しく設定されていることを確認します。サプリカントまたは NAS で、EAP カンバセーションのタイムアウトが短くないことを確認します。
未知の NAD（Unknown NAD）	Cisco ISE ポリシー サービス ノードは、Cisco ISE に設定されていないネットワーク デバイスから認証要求を受信しています。	ネットワーク デバイスが正規の要求であるか確認し、設定に追加します。シークレットが一致することを確認します。
システム ヘルス		
ヘルス ステータスが使用できません	モニタリング ノードは Cisco ISE ノードからヘルス ステータスを受信しませんでした。	Cisco ISE ノードが起動され、実行されていることを確認します。Cisco ISE ノードがモニタリング ノードと通信できることを確認します。
高い認証待ち時間	Cisco ISE システムに高い認証待ち時間が発生しています。	システムに十分なリソースがあるかどうかを確認します。システムの実際の作業量、たとえば、認証数、プロファイラ アクティビティなどを確認します。負荷を分散するためにさらにサーバを追加します。

表 25-2　Cisco ISE アラーム （続き）

アラーム名	アラームの説明	アラームの解決策
高ディスク I/O 使用率	Cisco ISE システムのディスク I/O 使用率が高くなっています。	システムに十分なリソースがあるかどうかを確認します。システムの実際の作業量、たとえば、認証数、プロファイラ アクティビティなどを確認します。負荷を分散するためにさらにサーバを追加します。
高ディスク領域使用量	Cisco ISE システムのディスクの使用量が高くなっています。	システムに十分なリソースがあるかどうかを確認します。システムの実際の作業量、たとえば、認証数、プロファイラ アクティビティなどを確認します。負荷を分散するためにさらにサーバを追加します。
高負荷平均	Cisco ISE システムに高負荷平均が発生しています。	システムに十分なリソースがあるかどうかを確認します。システムの実際の作業量、たとえば、認証数、プロファイラ アクティビティなどを確認します。負荷を分散するためにさらにサーバを追加します。
高メモリ使用率	Cisco ISE システムのメモリ使用率が高くなっています。	システムに十分なリソースがあるかどうかを確認します。システムの実際の作業量、たとえば、認証数、プロファイラ アクティビティなどを確認します。負荷を分散するためにさらにサーバを追加します。
高操 Operations DB 使用量	Cisco ISE モニタリング ノードに、予想より高い量の syslog データが発生しています。	operations データの消去設定ウィンドウをチェックして削減します。
プロセス ダウン	Cisco ISE プロセスの 1 つが動作していません。	Cisco ISE アプリケーションを再起動します。
プロファイラのキューサイズの制限に達しました	ISE プロファイラのキュー サイズの制限に達しました。キュー サイズの制限に達した後に受信されたイベントはドロップされます。	システムに十分なリソースがあるかどうかを確認し、エンドポイント属性フィルタが有効になっていることを確認します。
ライセンス		
ライセンスの期限切れ	Cisco ISE ノードにインストールされたライセンスの有効期限が切れました。	シスコ アカウント チームお問い合わせのうえ、新しいライセンスを購入してください。
License Violation	Cisco ISE ノードは、許可されたライセンス カウントを超過しているか、または超過しようとしていることを検出しました。	シスコ アカウント チームお問い合わせのうえ、追加のライセンスを購入してください。
システム エラー		

表 25-2　Cisco ISE アラーム （続き）

アラーム名	アラームの説明	アラームの解決策
ログ収集エラー	Cisco ISE モニタリング コレクタ プロセスは、ポリシー サービス ノードから生成された監査ログを存続できません。	これは、ポリシー サービス ノードの実際の機能に影響を与えません。詳細な解決については、TAC にお問い合わせください。
スケジュールされたレポートのエクスポートの失敗	エクスポートされたレポート（CSV ファイル）を設定されたリポジトリにコピーすることができません。	設定されたリポジトリを確認します。それが削除されていたら、追加し直します。それが使用できないか、またはそれに到達できない場合は、リポジトリを再設定して有効にします。

1. しきい値が満たされた場合、**過剰な認証試行**および**過剰な失敗試行**のアラームがトリガーされます。[説明（Description）] カラムの隣に表示される数は、直近 15 分間に Cisco ISE に対して認証または失敗した認証の合計数です。

Cisco ISE にユーザまたはエンドポイントを追加したときに、アラームはトリガーされません。

以前の Cisco ISE リリースから Cisco ISE リリース 1.2 にアップグレードしたら、以前のリリースで作成したルール、およびアラーム受信トレイのアラームは削除されます。

関連項目

- 「アラームの有効化および設定」（P.25-11）
- 「リモート Syslog 収集場所の設定」（P.11-2）
- 「通知をサポートするように SMTP サーバを設定」（P.5-5）

アラームの有効化および設定

Cisco ISE アラームを有効または無効にし、クリティカル条件を通知するアラーム通知動作を設定できます。特定のアラームに対して、過剰な失敗試行アラームの最大失敗試行数、または高ディスク使用量アラームの最大ディスク使用量などのしきい値を設定できます。

ステップ 1　[管理（Administration）] > [システム（System）] > [設定（Settings）] > [アラーム設定（Alarm Settings）] を選択します。

ステップ 2　デフォルトのアラームのリストからアラーム選択し、[編集（Edit）] をクリックします。

ステップ 3　[有効（Enable）] または [無効（Disable）] を選択します。

ステップ 4　該当する場合は、アラームのしきい値を設定します。

ステップ 5　[送信（Submit）] をクリックします。

関連項目

- 「Cisco ISE アラーム」（P.25-5）
- 「通知をサポートするように SMTP サーバを設定」（P.5-5）

アラームのモニタリング

Cisco ISE では、致命的なシステム条件が発生すると必ず通知するシステム アラームが用意されています。Cisco ISE によって生成されたアラームは [アラーム（Alarm）] ダッシュレットに表示されます。これらの通知は、自動的にアラーム ダッシュレットに表示されます。

[アラーム（Alarm）] ダッシュレットには最近のアラームのリストが表示され、ここから選択してアラームの詳細を表示できます。電子メールおよび syslog メッセージを介してアラームの通知を受信することもできます。

ステップ 1　Cisco ISE **ダッシュボード**に移動します。

ステップ 2　[アラーム（Alarm）] ダッシュレットでアラームをクリックします。アラームの詳細および推奨アクションが表示された新しいウィンドウが開きます。

ステップ 3　アラームを更新するには、[最新の情報に更新（Refresh）] をクリックします。

ステップ 4　選択したアラームを確認するには、[確認（Acknowledge）] をクリックします。タイムスタンプの前で使用可能なチェックボックスをオンにしてアラームを選択できます。これにより、読み取りとマークされているときに、アラーム カウンタ（アラームが発生した回数）が減少します。

ステップ 5　選択したアラームに対応する [詳細（Details）] リンクをクリックします。選択したアラームに対応する詳細が表示された新しいウィンドウが開きます。

（注）　ペルソナの変更の前に生成された以前のアラームに対応する [詳細（Details）] リンクにはデータは表示されません。

関連項目

「Cisco ISE アラーム」（P.25-5）

ログ収集

モニタリング サービスでは、ログおよび設定データが収集され、データが格納され、それが処理されてレポートおよびアラームが生成されます。展開内の任意のサーバから収集されたログの詳細を表示できます。

関連項目

第 11 章「ロギング」

アラーム Syslog 収集場所

システム アラーム通知を syslog メッセージとして送信するようにモニタリング機能を設定した場合は、通知を受信する syslog ターゲットが必要です。アラーム syslog ターゲットは、アラーム syslog メッセージが送信される宛先です。

syslog メッセージを受信するには、syslog サーバとして設定されたシステムも必要です。アラーム syslog ターゲットを作成、編集、および削除できます。

（注）　Cisco ISE モニタリングでは、logging-source interface の設定にネットワーク アクセス サーバ（NAS）の IP アドレスを使う必要があります。Cisco ISE モニタリング用のスイッチを設定する方法については、「ISE モニタリング用の NAD の設定」（P.G-38）を参照してください。

関連項目

- 「リモート Syslog 収集場所の設定」（P.11-2）
- 「通知をサポートするように SMTP サーバを設定」（P.5-5）

ライブ認証

[ライブ認証（Live Authentications）] ページから、発生した最近の RADIUS 認証をモニタできます。このページには、直近の 24 時間での上位 10 件の RADIUS 認証が表示されます。この項では、[ライブ認証（Live Authentications）] ページの機能について説明します。

ライブ認証ページには、発生した認証イベントに対応する認証エントリを示します。認証エントリに加えて、このページには、イベントに対応するライブ セッション エントリを示します。そのセッションに対応する詳細なレポートを表示するために、目的のセッションをドリル ダウンすることもできます。

1 つのエンドポイントが正常に認証されると、2 つのエントリが [ライブ認証（Live Authentications）] ページに表示されます。1 つは認証レコードに対応するエントリで、もう 1 つはセッション レコードに対応するエントリです（ライブ セッション ビューからプルされる）。その後、デバイスがもう一度正常な認証を実行すると、セッション レコードに対応する繰返しカウンタが増加します。[ライブ認証（Live Authentications）] ページに表示される繰返しカウンタは、抑制されている重複の RADIUS 認証成功メッセージの数を示します。

デフォルトで表示されるライブ認証データ カテゴリは、「最近の RADIUS 認証」（P.C-1）で説明されています。

すべてのカラムを表示するか、選択したデータ カラムのみを表示するように選択できます。表示するカラムを選択した後で、選択を保存できます。

ライブ認証のモニタリング

[ライブ認証（Live Authentications）] ページには、最近の RADIUS 認証が発生順に表形式で表示されます。

[ライブ認証（Live Authentications）] ページの下部に表示される [最終更新（Last update）] は、サーバの日付、時刻、およびタイムゾーンを示しています。

ステップ 1　[操作（Operations）] > [認証（Authentications）] を選択します。

ステップ 2　データ更新レートを変更するには、ドロップダウン リストから時間間隔を選択します。

ステップ 3　データを手動で更新するには、[ライブ認証（Live Authentications）] メニュー バーの [最新の情報に更新（Refresh）] アイコンをクリックします。

ステップ 4　表示するレコードの数を変更するには、[表示（Show）] ドロップダウン リストからオプションを選択します。

ステップ 5　時間間隔を指定するには、ドロップダウン リストからオプションを選択します。

ステップ 6　表示されるカラムを変更するには、[カラムの追加または削除（Add or Remove Columns）] をクリックし、ドロップダウン リストからオプションを選択します。

ステップ 7　ライブ RADIUS セッションを表示するには、[ライブ セッションの表示（Show Live Sessions）] をクリックします。アクティブ セッションの動的な許可変更（CoA）機能が提供されます。この機能を使用すると、アクティブな RADIUS セッションを動的に制御できます。再認証または接続解除要求をネットワーク アクセス デバイス（NAD）に送信できます。

ステップ 8　ドロップダウン リストの一番下にある [保存（Save）] をクリックして変更を保存します。

関連項目

- 「最近の RADIUS 認証」（P.C-1）
- 「RADIUS アカウンティング パケット（属性）がスイッチから着信しない」（P.G-6）
- 「Cisco ISE に RADIUS サーバのエラー メッセージ エントリが表示される」（P.G-17）
- 「RADIUS サーバの接続性に関する問題（Cisco ISE にエラー メッセージ エントリが表示されない場合）」（P.G-18）
- 「Cisco ISE のアクティブな RADIUS セッション」（P.26-4）
- 「RADIUS セッションの許可の変更」（P.26-5）

エンドポイントのグローバル検索

Cisco ISE ホーム ページの上部にあるグローバル検索ボックスを使用すると、エンドポイントを検索できます。次のいずれかの基準を使用して、エンドポイントを検索できます。

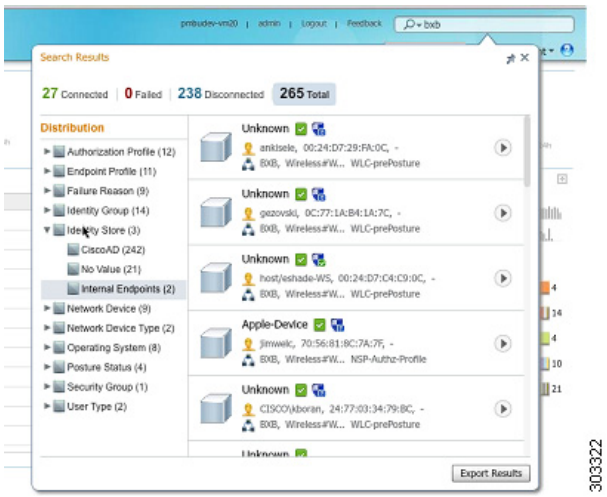
- ユーザ名
- MAC アドレス
- IP アドレス
- 許可プロファイル
- エンドポイント プロファイル
- 障害理由
- ID グループ
- ID ストア
- ネットワーク デバイス名
- ネットワーク デバイスのタイプ
- オペレーティング システム
- ポスチャ ステータス
- ロケーション
- セキュリティ グループ
- ユーザ タイプ

データを表示するには、[検索（Search）] フィールドに検索基準として 3 文字以上を入力する必要があります。

検索結果には、エンドポイントの現在のステータスに関する詳細および一目で確認できる情報が提供され、トラブルシューティングに使用できます。検索結果には、上位 25 のエントリだけが表示されます。フィルタを使用して結果を絞り込むことを推奨します。

図 25-1 に、検索結果の例を示します。

図 25-1　　エンドポイントの検索結果



左パネルのプロパティを使用して、結果をフィルタリングできます。エンドポイントをクリックして、次のようなエンドポイントに関する詳細情報も表示できます。

- セッション トレース
- 認証の詳細
- アカウンティングの詳細
- ポスチャの詳細
- プロファイラの詳細
- クライアント プロビジョニングの詳細
- ゲスト アカウンティングおよびアクティビティ

関連項目

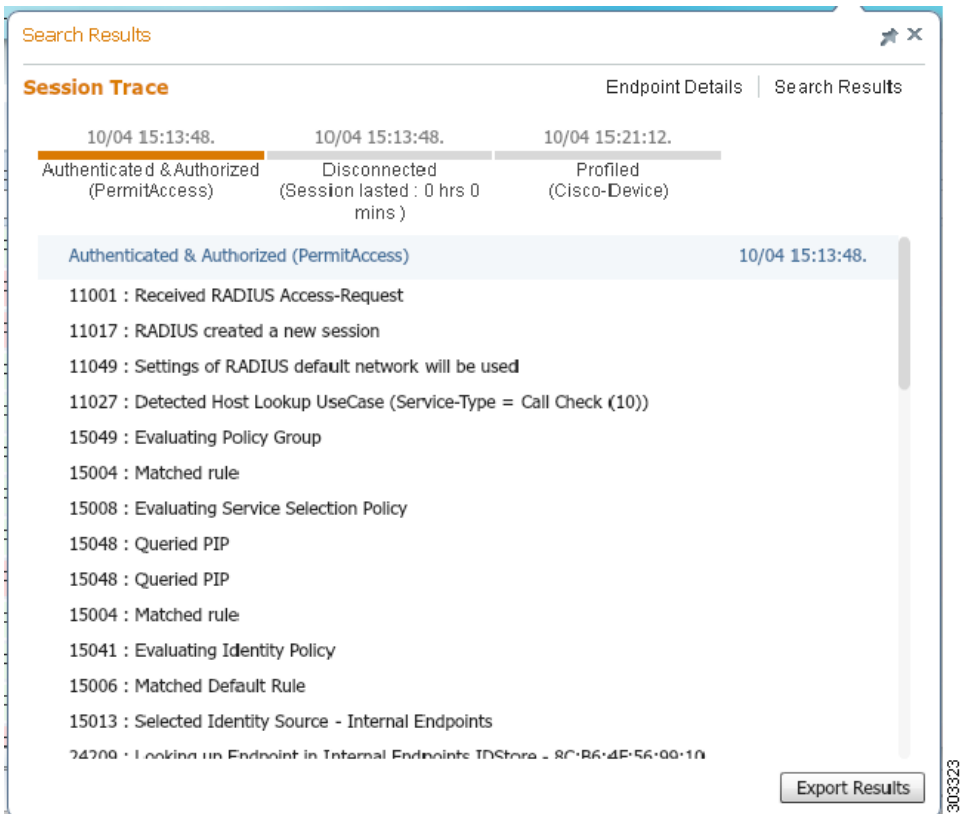
「エンドポイントのセッション トレース」（P.25-15）

エンドポイントのセッション トレース

Cisco ISE ホーム ページの上部にあるグローバル検索ボックスを使用すると、特定のエンドポイントのセッション情報を取得できます。基準を使用して検索すると、エンドポイントのリストが取得されます。これらのエンドポイントのいずれかをクリックして、そのエンドポイントのセッション トレース情報を表示します。図 25-2 に、エンドポイントに対して表示されるセッション トレース情報の例を示します。

（注） 検索に使用されるデータ セットは、インデックスとしてのエンドポイント ID に基づいています。したがって、認証が行われたときに、エンドポイントの認証用のエンドポイント ID を検索結果セットに含める必要があります。

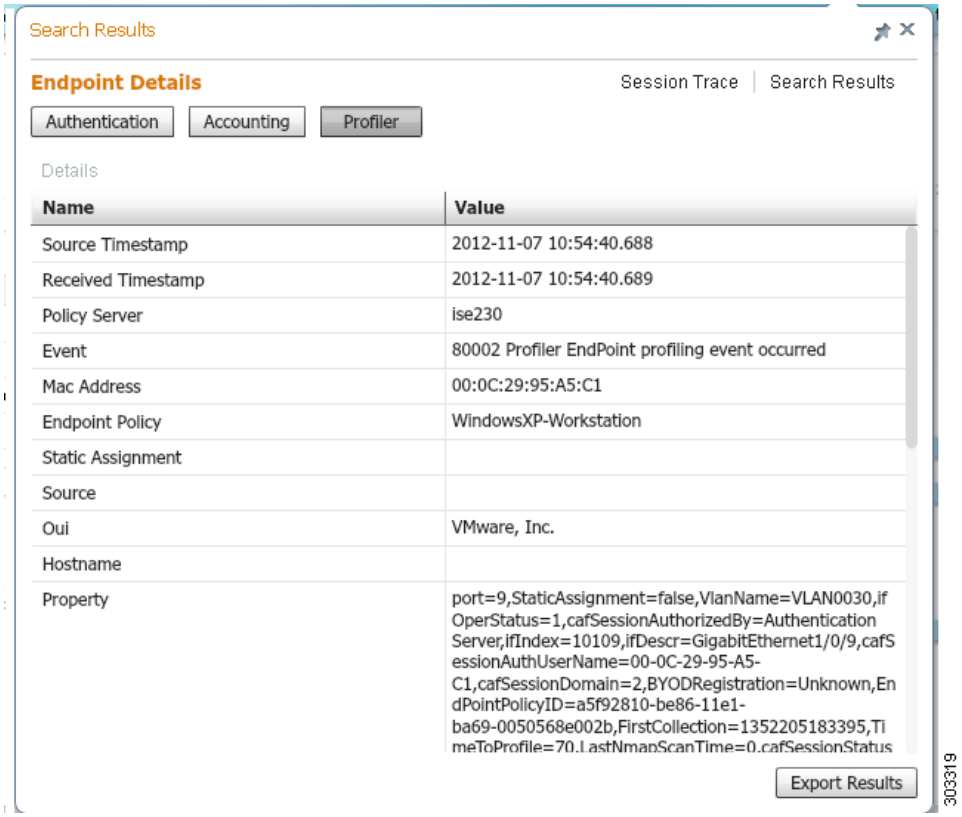
図 25-2　エンドポイントのセッション トレース



主な許可遷移を確認するには、上部のクリックできる時間軸を使用できます。[結果のエクスポート（Export Results）] ボタンをクリックして、.csv 形式で結果をエクスポートすることもできます。レポートがブラウザにダウンロードされます。

特定のエンドポイントの認証、アカウンティング、およびプロファイラの詳細情報を表示するには、[エンドポイントの詳細（Endpoint Details）] リンクをオンにできます。図 25-3 に、エンドポイントに対して表示されたエンドポイントの詳細情報の例を示します。

図 25-3　エンドポイントの詳細



ディレクトリからのセッションの削除

次のように、セッションが、モニタリングおよびトラブルシューティング ノード上のセッション ディレクトリから削除されます。

- 終了したセッションは、終了してから 15 分後に削除されます。
- 認証はあるがアカウンティングがない場合、このようなセッションは 1 時間後に削除されます。
- すべての非アクティブなセッションは 7 日後に削除されます。

関連項目

「エンドポイントのグローバル検索」（P.25-14）

ネットワーク アクセス問題のトラブルシューティング

認証要求に関連する属性に基づいて、特定のユーザ、デバイス、または検索条件についてネットワーク アクセスをトラブルシューティングできます。これを実行するには、認証概要レポートを実行します。

ステップ 1　[操作（Operations）] > [レポート（Reports）] > [認証概要レポート（Authentication Summary Report）] を選択します。

ステップ 2　障害理由でレポートをフィルタリングします。

ステップ 3　ネットワーク アクセスの問題をトラブルシューティングするために、レポートの障害理由の項ごとに認証のデータを確認します。

（注）　認証概要レポートは失敗または成功した認証に対応する最新のデータを収集して表示するため、レポートの内容は数分の遅延の後に表示されます。

関連項目

- 「予期しない RADIUS 認証の結果のトラブルシューティング」（P.25-18）
- 「レポートの実行および表示」（P.26-2）

診断トラブルシューティング ツール

診断ツールは、Cisco ISE ネットワークの問題の診断およびトラブルシューティングに役立ち、問題解決方法の詳細な手順を提供します。これらのツールを使用して、認証をトラブルシューティングし、セキュリティ グループ アクセス デバイスなどのネットワーク上のネットワーク デバイスの設定を評価できます。

この項では、診断の手順について説明します。次のトピックを扱います。

- 「予期しない RADIUS 認証の結果のトラブルシューティング」（P.25-18）
- 「設定を確認するための IOS Show コマンドの実行」（P.25-19）
- 「ネットワーク デバイス設定の問題のトラブルシューティング」（P.25-20）
- 「エンドポイントのポスチャ障害のトラブルシューティング」（P.25-21）
- 「TCP ダンプを使用したネットワーク トラフィックのモニタリング」（P.25-22）
- 「TCP ダンプ ファイルの保存」（P.25-22）
- 「エンドポイントまたはユーザの予期されない SGACL の比較」（P.25-23）
- 「SXP-IP マッピングを使用した SGA 対応ネットワークの 接続問題のトラブルシューティング」（P.25-24）
- 「IP-SGT マッピングを使用した SGA 対応ネットワークの接続問題のトラブルシューティング」（P.25-24）
- 「デバイスの SGT マッピングの比較による SGA 対応ネットワークの接続問題のトラブルシューティング」（P.25-25）

予期しない RADIUS 認証の結果のトラブルシューティング

このツールを使用すると、予期しない認証の結果になった場合に、トラブルシューティングのために RADIUS 認証を検索および選択できます。認証が成功すると予期していたのに失敗した場合、またはユーザには特定のレベルの権限があることを予期していたのにユーザにはそれらの権限がなかった場合に、このツールを使用できます。

- トラブルシューティングのためにユーザ名、エンドポイント ID、ネットワーク アクセス サービス（NAS）IP アドレス、および認証障害の理由に基づいて RADIUS 認証を検索すると、Cisco ISE はシステムの（現在）日付の認証だけを表示します。

- トラブルシューティングのために NAS ポートに基づいて RADIUS 認証を検索すると、Cisco ISE は前月の初めから現在の日付までのすべての NAS ポート値を表示します。

（注）　[NAS IP アドレス（NAS IP address）] および [エンドポイント ID（Endpoint ID）] フィールドに基づいて RADIUS 認証を検索すると、検索は最初操作データベースで実行され、次に設定データベースで実行されます。

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）] > [RADIUS 認証トラブルシューティング（RADIUS Authentication Troubleshooting）] を選択します。

ステップ 2　必要に応じてフィールドに検索基準を指定します。

ステップ 3　[検索（Search）] をクリックして、検索条件に一致する RADIUS 認証を表示します。

ステップ 4　テーブルから RADIUS 認証レコードを選択し、[トラブルシューティング（Troubleshoot）] をクリックします。

ステップ 5　[ユーザ入力必須（User Input Required）] をクリックし、必要に応じてフィールドを変更して、[送信（Submit）] をクリックします。

ステップ 6　[完了（Done）] をクリックします。

ステップ 7　トラブルシューティングが完了したら、[結果概要の表示（Show Results Summary）] をクリックします。

ステップ 8　診断、問題を解決する手順、およびトラブルシューティングの要約を表示するには、[完了（Done）] をクリックします。

関連項目

- 「RADIUS 認証トラブルシューティングの設定」（P.C-5）
- 「進捗詳細の設定」（P.C-11）
- 「結果概要（Results Summary）」（P.C-12）
- 「RADIUS アカウンティング パケット（属性）がスイッチから着信しない」（P.G-6）
- 「Cisco ISE に RADIUS サーバのエラー メッセージ エントリが表示される」（P.G-17）
- 「RADIUS サーバの接続性に関する問題（Cisco ISE にエラー メッセージ エントリが表示されない場合）」（P.G-18）

設定を確認するための IOS Show コマンドの実行

[ネットワーク デバイス コマンドの実行（Execute Network Device Command）] 診断ツールを使用すると、任意のネットワーク デバイス上で **show** コマンドを実行できます。結果は、コンソールに表示される場合とまったく同じ形式であり、デバイスの設定における問題を特定するために使用できます。設定が間違っていると疑われ、検証したい場合、または設定方法を確認するだけである場合に使用できます。

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）] > [ネットワーク デバイス コマンドの実行（Execute Network Device Command）] を選択します。

ステップ 2　適切なフィールドに、情報を入力します。

ステップ 3　[実行（Run）] をクリックして、指定したネットワーク デバイスでコマンドを実行します。

ステップ 4　[ユーザ入力必須（User Input Required）] ボタンをクリックし、必要に応じてフィールドを変更します。

ステップ 5　[送信（Submit）] をクリックして、ネットワーク デバイス上でコマンドを実行し、出力を表示します。

関連項目

- 「ネットワーク デバイス コマンドの実行の設定」（P.C-5）
- 「進捗詳細の設定」（P.C-11）
- 「結果概要（Results Summary）」（P.C-12）

ネットワーク デバイス設定の問題のトラブルシューティング

この診断ツールを使用して、ネットワーク デバイスの設定を評価し、設定の問題を特定できます。Expert Troubleshooter によって、デバイスの設定が標準設定と比較されます。

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）] > [設定評価バリデータ（Evaluate Configuration Validator）] を選択します。

ステップ 2　設定を評価するデバイスのネットワーク デバイス IP アドレスを入力し、必要に応じて他のフィールドを指定します。

ステップ 3　推奨テンプレートと比較する設定オプションを選択します。

ステップ 4　[実行（Run）] をクリックします。

ステップ 5　[ユーザ入力必須（User Input Required）] ボタンをクリックし、必要に応じてフィールドを変更します。

ステップ 6　分析するインターフェイスの隣のチェックボックスをオンにして、[送信（Submit）] をクリックします。

ステップ 7　[結果概要の表示（Show Results Summary）] をクリックします。

関連項目

- 「設定評価バリデータの設定」（P.C-6）
- 「進捗詳細の設定」（P.C-11）
- 「結果概要（Results Summary）」（P.C-12）

エンドポイントのポスチャ障害のトラブルシューティング

[ポスチャのトラブルシューティング（Posture Troubleshooting）] ツールは、ポスチャ チェック エラーの原因を見つけ、次のことを識別するのに役立ちます。

- どのエンドポイントがポスチャに成功し、どのエンドポイントが成功しなかったか。
- エンドポイントがポスチャに失敗した場合、ポスチャ プロセスのどの手順が失敗したか。
- どの必須および任意のチェックが成功および失敗したか。

ユーザ名、MAC アドレス、ポスチャ ステータスなどのパラメータに基づいて要求をフィルタリングすることによって、この情報を特定します。

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）] > [ポスチャのトラブルシューティング（Posture Troubleshooting）] を選択します。

ステップ 2　適切なフィールドに、情報を入力します。

ステップ 3　[検索（Search）] をクリックします。

ステップ 4　説明を見つけ、イベントの解決策を決定するには、リストでイベントを選択し、[トラブルシューティング（Troubleshoot）] をクリックします。

関連項目

- 「ポスチャのトラブルシューティングの設定」（P.C-7）
- 「進捗詳細の設定」（P.C-11）
- 「結果概要（Results Summary）」（P.C-12）

着信トラフィックを検証するための T CP ダンプ ユーティリティ

これは、予期されたパケットが実際にノードに達したことを調べるときに、パケットをスニファするツールです。たとえば、レポートに示されている着信認証またはログがない場合、着信トラフィックがないのではないか、または着信トラフィックが Cisco ISE に到達できないのではないかと疑われる場合があります。このような場合、検証するためにこのツールを実行できます。

この項では、TCP ダンプ機能を使用する方法について説明します。次のトピックを扱います。

- 「TCP ダンプを使用したネットワーク トラフィックのモニタリング」（P.25-22）
- 「TCP ダンプ ファイルの保存」（P.25-22）

注意　TCP ダンプを起動すると、以前のダンプ ファイルは自動的に削除されます。以前のダンプ ファイルを保存するには、新しい TCP ダンプ セッションを開始する前に、「TCP ダンプ ファイルの保存」（P.25-22）を実行します。

TCP ダンプを使用したネットワーク トラフィックのモニタリング

ネットワークの問題をトラブルシューティングするために、TCP ダンプのオプションを設定し、ネットワーク トラフィックからデータを収集できます。

はじめる前に

- [TCP ダンプ（TCP Dump）] ページの [ネットワーク インターフェイス（Network Interface）] ドロップダウン リストには、IPv4 または IPv6 アドレスが設定されているネットワーク インターフェイス カード（NIC）だけが表示されます。デフォルトでは、すべての NIC は VMware に接続されているので、NIC は IPv6 アドレスで設定され、[ネットワーク インターフェイス（Network Interface）] ドロップダウン リストに表示されます。
- tcpdump ファイルを表示するには、Cisco ISE 管理ノードに Adobe Flash Player がインストールされている必要があります。

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）] > [TCP ダンプ（TCP Dump）] を選択します。

ステップ 2　TCP ダンプ ユーティリティのソースとして [ホスト名（Host Name）] を選択します。インライン ポスチャ ノードは、サポートされていません。

ステップ 3　モニタする [ネットワーク インターフェイス（Network Interface）] をドロップダウン リストから選択します。

ステップ 4　オプション ボタンをクリックして、[無差別モード（Promiscuous Mode）] を [オン（On）] または [オフ（Off）] に設定します。デフォルトは [オン（On）] です。

無差別モードは、ネットワーク インターフェイスがすべてのトラフィックをシステムの CPU に渡すデフォルトのパケット スニッフィング モードです。[オン（On）] のままにしておくことを推奨します。

ステップ 5　[フィルタ（Filter）] テキスト ボックスに、フィルタリングのもとになるブール演算式を入力します。

次のような、標準的な tcpdump フィルタ式がサポートされています。

host 10.0.2.1 and port 1812

ステップ 6　[開始（Start）] をクリックして、ネットワークのモニタリングを開始します。

ステップ 7　十分な量のデータが収集された時点で [停止（Stop）] をクリックするか、最大パケット数（500,000）が累積されてプロセスが自動的に終了するまで待機します。

関連項目

- 「TCP ダンプ設定」（P.C-8）
- 「TCP ダンプ ファイルの保存」（P.25-22）
- 「ポリシー サービス ノードがトラフィックを渡していない」（P.G-7）

TCP ダンプ ファイルの保存

トラブルシューティング目的で使用する TCP ダンプ ファイルを保存できます。

はじめる前に

「TCP ダンプを使用したネットワーク トラフィックのモニタリング」（P.25-22）を正常に完了している必要があります。

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）] > [TCP ダンプ（TCP Dump）] を選択します。

ステップ 2　[形式（Format）] をドロップダウン リストから選択します。[可読（Human Readable）] がデフォルトです。

ステップ 3　[ダウンロード（Download）] をクリックし、必要な場所に移動して、[保存（Save）] をクリックします。

ステップ 4　最初に以前のダンプ ファイルを保存しないで除去するには、[削除（Delete）] をクリックします。

Cisco ISE CLI から [TCP ダンプ（TCP Dump）] にアクセスすることもできます。詳細については、『*Cisco Identity Services Engine CLI Reference Guide, Release 1.2*』を参照してください。

エンドポイントまたはユーザの予期されない SGACL の比較

セキュリティ グループ アクセス ソリューションが有効なデバイスの場合、Cisco ISE で設定された出力ポリシー マトリクスに基づいて、送信元 SGT と宛先 SGT のペアごとに SGACL が割り当てられます。エンドポイントまたはユーザに予期されない SGACL があるときに、このツールを使用できます。

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）] > [セキュリティ グループ アクセス ツール（Security Group Access Tools）] > [出力（SGACL）ポリシー（Egress (SGACL) Policy）] を選択します。

ステップ 2　SGACL ポリシーを比較するセキュリティ グループ アクセス デバイスのネットワーク デバイス IP アドレスを入力します。

ステップ 3　[実行（Run）] をクリックします。

ステップ 4　[ユーザ入力必須（User Input Required）] をクリックし、必要に応じてフィールドを変更します。

ステップ 5　[送信（Submit）] をクリックします。

ステップ 6　[結果概要の表示（Show Results Summary）] をクリックして、診断および推奨される解決手順を表示します。

関連項目

- 「進捗詳細の設定」（P.C-11）
- 「結果概要（Results Summary）」（P.C-12）

出力ポリシー診断フロー

出力ポリシー診断ツールでは、次のプロセスを使用して比較が行われます。

1. 指定した IP アドレスを使用してデバイスに接続し、送信元 SGT と宛先 SGT の各ペアに対するアクセス コントロール リスト（ACL）を取得します。
2. Cisco ISE に設定された出力ポリシーをチェックし、送信元 SGT と宛先 SGT の各ペアに対する ACL を取得します。

3. ネットワーク デバイスから取得された SGACL ポリシーと、Cisco ISE から取得された SGACL ポリシーを比較します。
4. ポリシーが一致しない送信元 SGT と宛先 SGT のペアを表示します。また、追加情報として、一致するエントリも表示します。

SXP-IP マッピングを使用した SGA 対応ネットワークの 接続問題のトラブルシューティング

セキュリティ交換プロトコル（SXP）が使用され、エンドポイントまたはユーザがネットワーク リソースに到達できない展開において、このツールは、適切な IP アドレスと SGT バインディングが確立されていることを確認するために IP アドレスと SGT マッピングを検証します。

セキュリティ グループ アクセス デバイスは、それぞれのピアと通信して、その SGT 値を取得します。SXP-IP Mappings 診断ツールは、指定した IP アドレスのデバイスに接続して、ピア デバイスの IP アドレスおよび SGT 値をリストします。デバイスのピアを 1 つ以上選択する必要があります。このツールは、選択した各ピアに接続し、その SGT 値を取得して、これらの値が以前にアクセスした値と同じであるかどうかを確認します。

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）] > [セキュリティ グループ アクセス ツール（Security Group Access Tools）] > [SXP-IP マッピング（SXP-IP Mappings）] を選択します。

ステップ 2　ネットワーク デバイスのネットワーク デバイス IP アドレスを入力し、[選択（Select）] をクリックします。

ステップ 3　[実行（Run）] をクリックし、[ユーザ入力必須（User Input Required）] をクリックして、必要なフィールドを変更します。

Expert Troubleshooter によって、ネットワーク デバイスからセキュリティ グループ アクセス SXP 接続が取得されて、ピア SXP デバイスを選択するように再度要求するプロンプトが表示されます。

ステップ 4　[ユーザ入力必須（User Input Required）] をクリックし、必要な情報を入力します。

ステップ 5　SXP マッピングを比較するピア SXP デバイスのチェックボックスをオンにして、共通接続パラメータを入力します。

ステップ 6　[送信（Submit）] をクリックします。

ステップ 7　[結果概要の表示（Show Results Summary）] をクリックして、診断および解決手順を表示します。

関連項目

- 「SXP-IP マッピング（SXP-IP Mappings）」（P.C-9）

IP-SGT マッピングを使用した SGA 対応ネットワークの接続問題のトラブルシューティング

セキュリティ グループ アクセス ソリューションが有効なデバイスの場合、RADIUS 認証によって各ユーザに SGT 値が割り当てられます。エンドポイントまたはユーザがネットワーク リソースに到達できないときに、このツールは、適切な IP アドレスと SGT バインディングが確立されていることを確認するために IP アドレスと SGT マッピングを検証します。

IP User SGT 診断ツールは、ネットワーク デバイスに接続し（指定した IP アドレスを使用）、ネットワーク デバイス上のすべての IP-SGT 割り当てのリストを取得します。次に、各 IP-SGT ペアの RADIUS 認証レコードおよびアカウンティング レコードをチェックして、割り当てられた最新のユーザ IP-SGT 値を確認します。最後に、IP-SGT ペアを表形式で表示して、割り当てられた最新の SGT 値とデバイス上の SGT 値が同じであるかどうかを特定します。

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）] > [セキュリティ グループ アクセス ツール（Security Group Access Tools）] > [IP User SGT] を選択します。

ステップ 2　必要に応じてフィールドに情報を入力します。

ステップ 3　[実行（Run）] をクリックします。追加入力が要求されます。

ステップ 4　[ユーザ入力必須（User Input Required）] をクリックし、必要に応じてフィールドを変更して、[送信（Submit）] をクリックします。

ステップ 5　[結果概要の表示（Show Results Summary）] をクリックして、診断および解決手順を表示します。

関連項目

- 「IP User SGT」（P.C-10）
- 「進捗詳細の設定」（P.C-11）
- 「結果概要（Results Summary）」（P.C-12）

デバイスの SGT マッピングの比較による SGA 対応ネットワークの接続問題のトラブルシューティング

セキュリティ グループ アクセス ソリューションが有効なデバイスの場合、RADIUS 認証によって各ネットワーク デバイスに SGT 値が割り当てられます。デバイス SGT 診断ツールは、ネットワーク デバイスに接続して（指定した IP アドレスを使用）、ネットワーク デバイス SGT 値を取得します。次に、RADIUS 認証レコードをチェックして、割り当てられた最新の SGT 値を特定します。最後に、デバイス SGT ペアを表形式で表示して、SGT 値が同じであるかどうかを特定します。

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）] > [セキュリティ グループ アクセス ツール（Security Group Access Tools）] > [デバイス SGT（Device SGT）] を選択します。

ステップ 2　必要に応じてフィールドに情報を入力します。

デフォルトのポート番号は、Telnet は 23、SSH は 22 です。

ステップ 3　[実行（Run）] をクリックします。

ステップ 4　[結果概要の表示（Show Results Summary）] をクリックして、デバイス SGT 比較の結果を表示します。

関連項目

「デバイス SGT の設定」（P.C-10）

その他のトラブルシューティング情報の入手

Cisco ISE を使用すると、管理者ポータルから、サポートおよびトラブルシューティング情報をダウンロードできます。サポート バンドルを使用して、Cisco Technical Assistance Center（TAC）が Cisco ISE の問題をトラブルシューティングするための診断情報を準備できます。

（注）　サポート バンドルおよびデバッグ ログにより、高度なトラブルシューティング情報が TAC に提供されます。サポート バンドルおよびデバッグ ログは解釈が困難です。Cisco ISE で提供されるさまざまなレポートおよびトラブルシューティング ツールを使用して、ネットワークで直面している問題を診断およびトラブルシューティングできます。詳細については、「ネットワーク アクセス問題のトラブルシューティング」（P.25-17）を参照してください。

この項では、次のトピックを扱います。

Cisco ISE のサポート バンドル

サポート バンドルに含めるログを設定できます。たとえば、特定のサービスのログをデバッグ ログに含めるように設定できます。詳細については、「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。

ダウンロードできるログは、次のように分類されます。

- 完全な設定データベース：Cisco ISE 設定データベースは、人間が読み取れる XML 形式でダウンロードされます。問題をトラブルシューティングしようとするときに、このデータベース設定を別の Cisco ISE ノードにインポートして、シナリオを再現できます。
- デバッグ ログ：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、公開キー インフラストラクチャ（PKI）の情報およびモニタリングおよびレポートを取得します。

  デバッグ ログによって、特定の Cisco ISE コンポーネントのトラブルシューティング情報が提供されます。詳細については、「Cisco ISE デバッグ ログ」（P.25-28）を参照してください。デバッグ ログを有効にするには、第 11 章「ロギング」を参照してください。デバッグ ログを有効にしない場合、情報メッセージ（INFO）はすべてサポート バンドルに含まれます。
- ローカル ログ：Cisco ISE で実行されるさまざまなプロセスからの syslog メッセージが含まれています。
- コア ファイル：クラッシュの原因の特定に役立つ重要な情報が含まれています。これらのログは、アプリケーションがクラッシュし、アプリケーションにヒープ ダンプが含まれている場合に作成されます。
- モニタリングおよびレポート ログ：アラートおよびレポートに関する情報が含まれています。
- システム ログ：Cisco Application Deployment Engine（ADE）関連の情報が含まれています。

これらのログは、Cisco ISE CLI から **backup-logs** コマンドを使用してダウンロードできます。詳細については、『*Cisco Identity Services Engine CLI Reference Guide, Release 1.2*』を参照してください。

（注）　インライン ポスチャ ノードの場合、管理者ポータルからサポート バンドルをダウンロードできません。Cisco ISE CLI から **backup-logs** コマンドを使用して、インライン ポスチャ ノードのログをダウンロードする必要があります。

これらのログを管理者ポータルからダウンロードすることを選択した場合、次の操作を実行できます。

- デバッグ ログやシステム ログなどのログ タイプに基づいて、ログのサブセットのみをダウンロードします。
- 選択したログ タイプの最新の「*n*」個のファイルのみをダウンロードします。このオプションによって、サポート バンドルのサイズとダウンロードにかかる時間を制御できます。

モニタリング ログによって、モニタリング、レポート、およびトラブルシューティング機能に関する情報が提供されます。

関連項目

「サポート バンドルのダウンロード」（P.25-27）

サポート バンドルのダウンロード

サポート バンドルは、単純な tar.gpg ファイルとしてローカル コンピュータにダウンロードできます。サポート バンドルは、日付とタイム スタンプを使用して、ise-support-bundle_ise-support-bundle-*mm-dd-yyyy-hh-mm.tar.gpg* という形式で名前が付けられています。ブラウザに、適切な場所にサポート バンドルを保存するように要求するプロンプトが表示されます。サポート バンドルの内容を抽出し、README.TXT ファイルを表示できます。README.TXT では、サポート バンドルの内容のほか、ISE データベースの内容をインポートする方法（サポート バンドルに含まれている場合）について説明します。

はじめる前に

次のタスクを実行するユーザは、スーパー管理者またはシステム管理者の権限が必要です。

ステップ 1　[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [ログのダウンロード（Download Logs）] > [アプライアンス ノード リスト（Appliance node list）] を選択します。

ステップ 2　サポート バンドルをダウンロードするノードをクリックします。

ステップ 3　[サポート バンドル（Support Bundle）] タブで、サポート バンドルに入力するパラメータを選択します。

すべてのログを含めると、サポート バンドルが大きくなりすぎて、ダウンロードに時間がかかります。ダウンロード プロセスを最適化するには、最新の *n* ファイルのみをダウンロードするように選択します。

ステップ 4　サポート バンドルの暗号キーを入力し、再度入力します。

ステップ 5　[サポート バンドルの作成（Create Support Bundle）] をクリックします。

ステップ 6　[ダウンロード（Download）] をクリックして、新しく作成されたサポート バンドルをダウンロードします。

サポート バンドルは、アプリケーション ブラウザを実行しているクライアント システムにダウンロードされる tar.gpg ファイルです。

関連項目

「Cisco ISE 管理者グループ、アクセス レベル、権限、および制約事項」

次の手順：

特定のコンポーネントのデバッグ ログを入手する方法については、「Cisco ISE デバッグ ログ」（P.25-28）を参照してください。

Cisco ISE デバッグ ログ

デバッグ ログによって、さまざまな Cisco ISE コンポーネントのトラブルシューティング情報が提供されます。問題を報告しているときに、これらのデバッグ ログを有効にして、問題の診断と解決のためにそれらを送信するよう求められる場合があります。

デバッグ ログの取得は、次の 2 つのステップからなるプロセスです。

1. [デバッグ ログの設定（Debug Log Configuration）] ページで、デバッグ ログを取得するコンポーネントを設定します。
2. デバッグ ログをダウンロードします。

関連項目

- さまざまなコンポーネントのデバッグ ログを設定するには、「デバッグ ログ設定オプション」（P.11-4）および「デバッグ ログの重大度レベルの設定」（P.11-4）を参照してください。
- 「デバッグ ログのダウンロード」（P.25-29）

Cisco ISE コンポーネントおよび対応するデバッグ ログ

表 25-3 に、コンポーネントと生成される対応するデバッグ ログのリストを示します。

表 25-3　コンポーネントおよび対応するデバッグ ログ

コンポーネント	デバッグ ログ
runtime-AAA	*prrt.log*
runtime-config	*prrt.log*
runtime-logging	*prrt.log*
NotificationTracker	*ise-tracking.log*
ReplicationTracker	*ise-tracking.log*
CacheTracker	*ise-tracking.log*
pep-auth-manager-test	*ise-psc.log*
net-securent	*ise-psc.log*
posture	*ise-psc.log*
provisioning	*ise-psc.log*
swiss	*ise-psc.log*
client	*ise-psc.log*
prrt-JNI	*ise-prrt.log*
profiler	*profiler.log*
cisco-mnt	*ise-psc.log*
guest	*ise-psc.log*
guestportal	*ise-psc.log*

表 25-3　コンポーネントおよび対応するデバッグ ログ （続き）

コンポーネント	デバッグ ログ
sponsorportal	*ise-psc.log*
guestauth	*ise-psc.log*
epm-pap	*ise-psc.log*
epm-pdp	*ise-psc.log*
epm-pip	*ise-psc.log*
epm-pap-api.services	*ise-psc.log*
org-apache	*ise-psc.log*
org-apache-digester	*ise-psc.log*
org-displaytag	*ise-psc.log*
org-apache-cxf	*ise-psc.log*
identity-store-AD	*ise-psc.log*
mnt-collector	*mnt-collector.log*
mnt-alert	*mnt-alert.log*

デバッグ ログのダウンロード

デバッグ ログ ファイルをダウンロードして保存するには、このプロセスを使用できます。

はじめる前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [ログのダウンロード（Download Logs）] > [アプライアンス ノード リスト（Appliance node list）] を選択します。

ステップ 2　デバッグ ログをダウンロードするノードをクリックします。

ステップ 3　[デバッグ ログ（Debug Logs）] タブをクリックします。

デバッグ ログ タイプとデバッグ ログのリストが表示されます。このリストは、デバッグ ログの設定に基づいています。

ステップ 4　ダウンロードするログ ファイルをクリックし、クライアント ブラウザを実行しているシステムに保存します。

必要に応じて、このプロセスを繰り返して他のログ ファイルをダウンロードできます。次に示すのは、[デバッグ ログ（Debug Logs）] ページからダウンロードできるその他のデバッグ ログです。

- isebootstrap.log：ブートストラップ ログ メッセージを提供します
- monit.log：ウォッチドッグ メッセージを提供します
- pki.log：サードパーティの暗号ライブラリ ログを提供します
- iseLocalStore.log：ローカル ストア ファイルに関するログを提供します
- ad_agent.log：Microsoft Active Directory サードパーティ ライブラリ ログを提供します
- catalina.log：サードパーティ ログを提供します

関連項目

- 「Cisco ISE 管理者グループ、アクセス レベル、権限、および制約事項」
- 「デバッグ ログ設定オプション」（P.11-4）

データベースのモニタリング

モニタリング機能によって利用されるデータ レートおよびデータ量には、これらの目的専用のノード上に別のデータベースが必要です。

ポリシー サービスと同様に、モニタリングには専用のデータベースがあり、この項で説明するトピックのようなメンテナンス タスクを実行する必要があります。

- 「モニタリング データベースのバックアップおよび復元」（P.25-30）
- 「モニタリング データベースの消去」（P.25-30）
- 「ログ収集」（P.25-12）

モニタリング データベースのバックアップおよび復元

モニタリング データベースでは、大量のデータが処理されます。時間が経つにつれ、モニタリング ノードのパフォーマンスと効率は、そのデータをどう管理するかによって変わってきます。効率を高めるために、データを定期的にバックアップして、それをリモートのリポジトリに転送することを推奨します。このタスクは、自動バックアップをスケジュールすることによって自動化できます。

（注） 消去操作の進行中にバックアップを実行しないようにしてください。消去操作中にバックアップが開始されると、消去操作が停止または失敗します。

セカンダリ モニタリング ノードを登録している場合は、最初にプライマリ モニタリング ノードをバックアップしてから、データを新しいセカンダリ モニタリング ノードに復元することを推奨します。これにより、新しい変更内容が複製されるので、プライマリ モニタリング ノードの履歴が新しいセカンダリ ノードと同期していることが保証されます。

関連項目

- 「オンデマンド バックアップの実行」（P.12-4）
- 「バックアップのスケジュール作成」（P.12-5）
- 「データの復元に関するガイドライン」（P.12-7）
- 「モニタリング データベースの復元」（P.12-10）

モニタリング データベースの消去

消去プロセスでは、消去中にデータを保持する月数を指定することによって、モニタリング データベースのサイズを管理できます。デフォルトは 3 ヵ月間です。この値は、消去用のディスク領域使用率しきい値（[ディスク領域のパーセンテージ（percentage of disk space）]）に達したときに使用されます。このオプションでは、各月は 30 日間です。デフォルトの 3 ヵ月は 90 日間です。

関連項目

- 「モニタリング データベースの消去のガイドライン」（P.25-31）

- 「古いモニタリング データの消去」（P.25-31）

モニタリング データベースの消去のガイドライン

モニタリング データベースのディスク使用量に関して従うべきガイドラインの一部を次に示します。

- モニタリング データベースのディスク使用率がしきい値設定の 80% を超えた場合、データベース サイズが割り当てられたディスク サイズを超過したことを示すクリティカル アラームが生成されます。ディスク使用率が 90% を超えた場合は、別のアラームが生成されます。

  消去プロセスが実行され、[操作（Operations）] > [レポート（Reports）] > [展開ステータス（Deployment Status）] > [データ消去監査（Data Purging Audit）] を選択して表示できるステータス履歴レポートが作成されます。消去の完了時に情報（INFO）アラームが生成されます。

- 消去も、データベースの使用済みディスク領域のパーセンテージに基づきます。モニタリング データベースの使用済みディスク領域がしきい値（デフォルトは 80%）以上の場合、消去プロセスが開始されます。このプロセスでは、管理者ポータルで設定した値に関係なく、過去 7 日間のモニタリング データのみ削除されます。このプロセスは、ディスク領域が 80 パーセント未満になるまでループで続行されます。消去では、処理の前にモニタリング データベースのディスク領域制限が常にチェックされます。

古いモニタリング データの消去

消去プロセスでは、モニタリング データベースのサイズを管理できます。

はじめる前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [データ消去（Data Purging）] を選択します。

ステップ 2　データを保持する期間を月単位で指定します。指定された期間より前のデータはすべて消去されます。このオプションでは、各月は 30 日間です。デフォルトの 3 ヵ月は 90 日間です。

（注）　設定された保持期間が診断データに対応する既存の保持しきい値未満の場合、設定値は既存のしきい値を上書きします。たとえば、保持期間を 3 日間として設定し、この値が診断テーブルの既存のしきい値未満（たとえば、デフォルトの 5 日間）の場合、データはこのページで設定した値（3 日間）に従って消去されます。

ステップ 3　[送信（Submit）] をクリックします。

ステップ 4　データ消去監査レポートを表示して、データ消去が成功したかどうかを確認します。

関連項目

「Cisco ISE 管理者グループ、アクセス レベル、権限、および制約事項」

次の手順

次のタスクのいずれかに進みます。

- 「ログ収集」（P.25-12）
- 「オンデマンド バックアップの実行」（P.12-4）