トラブルシュート

Cisco ISE のモニターリングと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（MnT）サービスは、すべての Cisco ISE 実行時サービスを対象とした包括的なアイデンティティ ソリューションです。[操作（Operations）] メニューには次のコンポーネントが表示されます。このメニューはポリシー管理ノード（PAN）からのみ表示できます。[操作（Operations）] メニューはプライマリ モニタリング ノードに表示されないことに注意してください。

- 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をリアルタイムに表示します。これを把握することにより、操作の状態を簡単に解釈し、監視できます。
- 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、ユーザー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ー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。[ID（Identity）]、[エンドポイントID（Endpoint ID）]、および [ISE ノード（ISE Node）]（正常性の概要レポートは除く）のすべてのレポートで、ワイルドカードおよび複数値を使用してレコードを検索できます。

ISE コミュニティ リソース

トラブルシューティングに関するテクニカル ノートのリストについては、「ISE Troubleshooting TechNotes」を参照してください。

ヘルス チェック

Cisco ISE には、Cisco ISE 展開内のすべてのノードを診断するオンデマンドのヘルスチェックオプションがあります。運用前にすべてのノードのヘルスチェックを実行すると、ダウンタイムを短縮でき、重大な問題（ある場合）を特定することで Cisco ISE システムの機能全体を向上できます。ヘルスチェックでは、コンポーネントの動作ステータスが示され、展開内の問題（ある場合）に関するトラブルシューティングの推奨事項が表示されます。

表 *1:* ヘルスチェックの展開

展開タイプ	説明
プラットフォーム サポート チェック	展開でサポートされているプラットフォームを確認します。推奨要件の仕様を満たしていないプラットフォームでは、パフォーマンスの問題が生じる可能性があります。 34xx およびその他のサポートされていないプラットフォームの詳細を確認し、システムに最低でも 12 コアの CPU、300 GB のハードディスク、16 GB のメモリが搭載されていることを確認します。
展開の検証	展開のノードの状態（同期しているか進行中か）を確認します
DNS の解決可能性	ホスト名と IP アドレスの正引きと逆引きを確認します。 展開のヘルスチェックが適切に機能するためには、DNS 解決を正引きと逆引きの両方で行うことを推奨します。

展開タイプ	説明
信頼ストア証明書の検証	信頼ストア証明書が有効か、期限切れかを確認します。 最適な Cisco ISE 機能を確保するために、未使用または期限切れの証明書を削除または更新します。
システム証明書の検証	各ノードのシステム証明書の検証を確認します。 最適な Cisco ISE 機能を確保するために、未使用または期限切れの証明書を削除または更新します。
ディスク容量チェック	プラットフォーム サポート チェックにあるハードディスクと、アップグレード手順のために使用可能なディスクの空き容量をチェックします。 パフォーマンスの問題を回避するために、アップグレード操作を開始する前にディスク容量チェックを実行することをお勧めします。
NTP の到達可能性と時刻源の確認	システムで設定されている NTP をチェックし、時刻源が NTP サーバーかどうかを確認します。 NTP 同期は、AD 操作、アップグレードワークフローなどの Cisco ISE サービスに不可欠です。
負荷平均チェック	指定した間隔でシステムの負荷をチェックします。有効な間隔の設定は、1、5、および 15 分です。 負荷平均チェックの失敗は、Cisco ISE のパフォーマンスの問題につながる可能性があります。
MDM の検証	設定された MDM サーバーと Cisco ISE PSN サーバー間の接続を確認します。 MDM でサポートされる機能を Cisco ISE で使用するには、MDM 検証チェックが成功する必要があります。
ライセンスの検証	スマートライセンスが設定されていて、有効であるかを確認します。スマートライセンスが設定されていないか有効でない場合、ライセンスを設定して検証するように求める警告が Cisco ISE GUI に表示されます。 Cisco ISE リリース 3.0 以降のリリースでは、スマートライセンスのみがサポートされます。Cisco ISE リリース 3.0 以降のリリースにアップグレードする前に、従来のライセンスをスマートライセンスに変換します。
サービスまたはプロセスの失敗	サービスまたはアプリケーションのステータスが実行中か、障害状態かを確認します。

（注） 展開の横にある数字は、ノードの数とそのヘルスチェックの詳細を示します。例：展開に 0/2 がある場合、0は失敗/進行中/完了状態のノードの数を示し、2は展開内のノードの数を示します。ヘルスチェック中に、いずれかのノードが 15 分間応答を返さない場合、そのノードのヘルスチェックはタイムアウトになります。

ヘルスチェックの実行

ステップ 1 Cisco ISE GUI で[メニュー（Menu）]アイコン（☰）をクリックして選択します。**[管理（Administration）]**> **[システム（System）]** > **[ヘルスチェック（Health Checks）]** を選択します。

ステップ 2 [正常性チェックの開始（Start health checks）] をクリックします。

情報ポップアップウィンドウに次のメッセージが表示されます。

正常性チェックがトリガーされました（Health Checks triggered）。

ステップ 3 [Ok] をクリックすると、ステータスが表示されます。

ステップ 4 [正常性チェック（Health Checks）] ウィンドウで、各コンポーネントの正常性ステータスを表示できます。次の色は、対応する Cisco ISE コンポーネントのヘルスステータスを示します。

色	ヘルス ステータス	操作
赤	不良	トラブルシューティングの推奨事項を表示するには、ドロップダウンオプションをクリックします。 アップグレードワークフローなどの操作は、これらの問題が解決されるまで続行できないため、問題を解決することをお勧めします。
橙	良好	ボックスで使用可能なトラブルシューティングの推奨事項を表示するには、ドロップダウンオプションをクリックします。 コンポーネントのヘルスステータスは操作の実行に適しているため、アップグレードワークフローを続行できますが、これらの問題も Cisco ISE の機能に影響する可能性があるため、続行する前にオレンジ色で示されている問題を解決することを推奨します。
グリーン	良好	特に対処の必要はありません。
青	良好	機能に関する重要な情報を表示するには、情報アイコンをクリックします。

ステップ 5 [レポートのダウンロード（Download report）] をクリックします。

HealthChecksReport.json ファイルは、Cisco ISE 展開の詳細な正常性ステータス情報とともにローカルシステムに保存されます。

正常性チェックがトリガーされると、ステータスは [正常性チェック（Health Check）] ウィンドウに 3 時間保持されます。[ヘルスチェック（Health Checks）] ウィンドウが更新されるか期限切れになるまで、ヘルスチェックを実行できません。

Network Privilege Framework のイベントフロープロセス

Network Privilege Framework（NPF）認証および許可イベント フローでは、次の表に記載されているプロセスが使用されます。

プロセス ステージ	説明
1	ネットワーク アクセスデバイス（NAD）によって通常の許可またはフレックス許可のいずれかが実行されます。
2	未知のエージェントレス ID が Web 許可を使用してプロファイリングされます。
3	RADIUS サーバーによって ID 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。

モニターリングおよびトラブルシューティング機能のユーザーロールと権限

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ー 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ー ロールに直接関係します。

各ユーザーロールに設定されている権限と制約事項については、Cisco ISE 管理者グループを参照してください。

（注） Cisco TAC の指示がないルートシェルを使用した Cisco ISE へのアクセスはサポート対象外のため、その結果として生じる可能性があるサービスの中断については、シスコは責任を負いません。

モニターリングデータベースに格納されているデータ

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、データベースの完全バックアップおよび差分バックアップを実行します。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。

Cisco ISE テレメトリ

テレメトリは、ネットワーク内のシステムとデバイスを監視し、ユーザーの製品使用方法に関する情報をシスコにフィードバックします。シスコでは、この情報を使用して製品を改善します。

Cisco ISE テレメトリデータ通信は、https://connectdna.cisco.com/ のポート 443 を介した HTTPS トラフィックとして行われます。

テレメトリはデフォルトで有効になっています。この機能を無効にするには、次の手順に従ってください。

1. **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [Network Success Diagnostics] > [テレメトリ（Telemetry）]** を選択します。
2. [テレメトリの有効化（Enable Telemetry）] チェックボックスをオフにし、テレメトリを無効にします。

   Cisco ISE 2.7 パッチ 1 では、テレメトリはすぐに無効になります。パッチを適用する前に、Cisco ISE で機能が無効になり、テレメトリデータの共有が停止するまでに最大 24 時間かかる場合があります。

テレメトリにはスマートライセンスが必要です。スマートライセンスをまだ使用していない場合は、使用している Cisco ISE のバージョンのライセンスブックで「スマートライセンス」を参照してください。

- [シスコアカウント（Cisco Account）]：テレメトリからの電子メールを受信できるようにシスコアカウントのログイン情報を入力します。この ID は、Cisco ISE 展開に影響する可能性がある重大な問題がテレメトリによって発見された場合の連絡にも使用されることがあります。
- [トランスポートゲートウェイ（Transport Gateway）]：セキュリティを強化するために、Cisco ISE とシスコの外部テレメトリサーバーの間でプロキシを使用できます。そうする場合は、このチェックボックスをオンにして、プロキシサーバーの FQDN を入力します。テレメトリにプロキシは必要ありません。

シスコでは、トランスポートゲートウェイ用のソフトウェアを提供しており、cisco.comからダウンロードできます。このソフトウェアは、Linuxサーバー上で実行されます。RHELサーバーでのトランスポート ゲートウェイ ソフトウェアの導入方法については、Smart Call Home 導入ガイド [英語] を参照してください。このシスコソフトウェアを使用している場合、URL の値は、**<FQDN of proxyserver>/Transportgateway/services/DeviceRequestHandler** です。

このゲートウェイを使用して、スマートライセンスサーバーに接続することもできます。トランスポートゲートウェイのバージョン 3.5 以降では、ポートは変更できませんが、FQDN の代わりに IP アドレスを入力できます。

テレメトリが収集する情報

テレメトリは、シスコに次の情報を送信します。

ノード：

各ポリシー管理ノード（PAN）については、次のとおりです。

- ポスチャされたエンドポイントの現在の数
- PxGrid クライアントの現在の数
- MDM によって管理されるエンドポイントの現在の数
- 現在のゲストユーザーの数
- このテレメトリレコードの開始日と終了日

各ポリシーサービスノード（PSN）については、次のとおりです。

- プロファイラプローブの数
- ノードサービスタイプ
- 使用されているパッシブ ID

すべてのノードについては、次のとおりです。

- CPU コア数
- VM 利用可能なディスク容量
- システム名。
- Serial number
- VID と PID
- アップタイム（Uptime）
- 最後の CLI ログイン

MnT ノード数

pxGrid ノード数

ライセンス

- ライセンスの有効期限が切れていますか?
- 使用可能な Apex ライセンスの数、これまでに使用された最大数
- 使用可能な基本ライセンスの数、これまでに使用された最大数
- 使用可能な Plus ライセンスの数、これまでに使用された最大数
- 小規模、中規模、大規模 VM ライセンスの数
- 評価ライセンスを使用していますか?
- スマートアカウントの名前
- TACACS デバイスの数
- 有効期限、残りの日数、ライセンス期間
- サービスタイプ、プライマリ UDI とセカンダリ UDI

ポスチャ（Posture）

- 非アクティブなポリシーの数
- 最後のポスチャフィード更新
- アクティブなポリシーの数

ゲスト ユーザー

- 当日の認証されたゲストの最大数
- 当日のアクティブゲストの最大数
- 当日の BYOD ユーザーの最大数

ネットワーク アクセス デバイス（NAD）

- 認証：アクティブ化された ACL、VLAN、ポリシーサイズ
- NDG マップと NAD 階層
- Authentication:
  - RADIUS、RSA ID、LDAP、ODBC、およびアクティブディレクトリ ID ストアの数
  - ローカル（管理者以外の）ユーザーの数
  - NDG マップと NAD マップ
  - ポリシーの行数

認証用のアクティブ VLAN の数、ポリシー数、アクティブ化された ACL の数：

- ステータス、VID、PT
- 平均負荷、メモリ使用率
- PAP、MnT、pxGrid、および PIC ノードの数
- 名前、プロファイル名、プロファイル ID

NAD プロファイル

各 NAD プロファイルに関する情報：

- 名前と ID
- シスコ デバイス
- TACACS サポート
- RADIUS サポート
- TrustSec サポート
- [デフォルトのプロファイル（Default Profile）]

プロファイラ

- フィードの最終更新日
- 自動更新を有効にしますか。
- プロファイルされたエンドポイント、エンドポイントの種類、不明なエンドポイント、不明なパーセンテージ、および合計エンドポイント数
- カスタムプロファイルの数
- シリアル番号、範囲、エンドポイントタイプ、カスタムプロファイル

モバイルデバイス管理（MDM）

- MDM ノードのリスト
- 日付範囲内における、現在の MDM エンドポイント数、現在のゲストユーザー数、現在のポスチャ済みユーザー数
- pxGrid クライアント数
- ノード数

パッチおよびホットパッチ

Cisco ISE をモニターする SNMP トラップ

SNMP トラップは、Cisco ISE のステータスをモニターできます。Cisco ISE サーバーにアクセスせずに Cisco ISE をモニターする場合は、Cisco ISE の SNMP ホストとして MIB ブラウザを設定できます。その後、MIB ブラウザから Cisco ISE のステータスをモニターすることもできます。

snmp-server host および **snmp-server trap** コマンドの詳細については、『Cisco Identity Services Engine CLI リファレンス ガイド』を参照してください。

Cisco ISE は、SNMPv1、SNMPv2c、および SNMPv3 をサポートします。

CLI から SNMP ホストを設定した場合は、Cisco ISE は次の汎用システム トラップを送信します。

- Cold start：デバイスをリブートする場合。
- Linkup：イーサネット インターフェイスがアップしている場合。
- Linkdown：イーサネット インターフェイスがダウンしている場合。
- Authentication failure：コミュニティストリングが一致しない場合。

次の表に、Cisco ISE でデフォルトで生成される汎用 SNMP トラップを示します。

OID	説明	トラップの例
.1.3.6.1.4.1.8072.4.0.3 \n NET SNMP エージェント MIB::nsNotifyRestart	エージェントが再起動されたことを示します。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (478) 0:00:04.78 SNMPv2-MIB::snmpTrapOID.0 = OID: NET-SNMP-AGENT-MIB::nsNotifyRestart SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpNotificationPrefix
.1.3.6.1.4.1.8072.4.0.2 \n NET SNMP エージェント MIB::nsNotifyShutdown	エージェントがシャットダウン中であることを示します。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (479) 0:00:04.79 SNMPv2-MIB::snmpTrapOID.0 = OID: NET-SNMP-AGENT-MIB::nsNotifyShutdown SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpNotificationPrefix

OID	説明	トラップの例
.1.3.6.1.6.3.1.1.5.4 \n IF-MIB::linkUp	エージェントロールで動作している SNMP エンティティで、いずれかの通信リンクの ifOperStatus オブジェクトが、ダウン状態から（notPresent 状態以外の）他の状態に遷移したことが検出されたことを示します。This other state is indicated by the included value of ifOperStatus.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (478) 0:00:04.78 SNMPv2-MIB::snmpTrapOID.0 = OID: IF-MIB::linkUp IF-MIB::ifIndex.12 = INTEGER: 12 IF-MIB::ifAdminStatus.12 = INTEGER: up(1) IF-MIB::ifOperStatus.12 = INTEGER: up(1) SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
.1.3.6.1.6.3.1.1.5.3 \n IF-MIB::linkDown	エージェントロールで動作している SNMP エンティティで、いずれかの通信リンクの ifOperStatus オブジェクトが、（notPresent 状態以外の）他の状態からダウン状態に遷移しようとしていることが検出されたことを示します。This other state is indicated by the included value of ifOperStatus.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (479) 0:00:04.79 SNMPv2-MIB::snmpTrapOID.0 = OID: IF-MIB::linkDown IF-MIB::ifIndex.5 = INTEGER: 5 IF-MIB::ifAdminStatus.5 = INTEGER: up(1) IF-MIB::ifOperStatus.5 = INTEGER: down(2) SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
.1.3.6.1.6.3.1.1.5.1 \n SNMPv2-MIB::coldStart	通知発信元アプリケーションをサポートする SNMP エンティティが再初期化され、このエンティティの設定が変更された可能性があることを示します。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (8) 0:00:00.08 SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-MIB::coldStart SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10

Cisco ISE のプロセスモニタリング SNMP トラップ

Cisco ISE では、Cisco ISE CLI から SNMP ホストを設定する場合、Cisco ISE プロセス ステータスの hrSWRunName トラップを SNMP マネージャに送信できます。Cisco ISE は cron ジョブを使用してこれらのトラップをトリガーします。cron ジョブは Cisco ISE プロセスステータスを Monit から取得します。CLI から **SNMP-Server Host** コマンドを設定した後、5 分ごとに cron ジョブを実行して Cisco ISE をモニターします。

Note 管理者が ISE プロセスを手動で停止した場合は、プロセスの Monit が停止しても、SNMP マネージャにトラップは送信されません。プロセスが不意にシャットダウンし、自動的に復活しない場合のみ、プロセス停止 SNMP トラップは SNMP マネージャに送信されます。

次に、Cisco ISE のプロセスモニタリング SNMP トラップのリストを示します。

OID	説明	トラップの例
.1.3.6.1.2.1.25.4.2.1.2 \n HOST-RESOURCES-MIB::hrSWRunName	A textual description of this running piece of software, including the manufacturer, revision, and the name by which it is commonly known. このソフトウェアがローカルにインストールされている場合は、対応する hrSWInstalledName で使用されているものと同じ文字列である必要があります。検討する必要のあるサービスは、app-server、rsyslog、redis-server、ad-connector、mnt-collector、mnt-processor、ca-server est-server、および elasticsearch です。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (63692139) 7 days, 8:55:21.39 SNMPv2-MIB::snmpTrapOID.0 = OID: HOSTRESOURCES- MIB::hrSWRunName HOSTRESOURCES- MIB::hrSWRunName = STRING: "redis-server:Running"

Cisco ISE は、次のステータスのトラップを設定済みの SNMP サーバーに送信します。

- Process Start（監視状態）
- Process Stop（監視されていない状態）
- Execution Failed：プロセスの状態が「Monitored」から「Execution failed」に変更されるとトラップが送信されます。
- Does Not Exists：プロセスの状態が「Monitored」から「Does not exists」に変更されるとトラップが送信されます。

SNMP サーバーで、すべてのオブジェクトについて一意のオブジェクト ID（OID）が生成され、値が OID に割り当てられます。SNMP サーバーの OID 値でオブジェクトを検索できます。

実行中のトラップの OID 値は running で、監視されないトラップ、存在しないトラップ、実行に失敗したトラップの OID 値は stopped です。

Cisco ISE は、HOST-RESOURCES MIB に属している hrSWRunName の OID を使用してトラップを送信し、< *PROCESS NAME* > - < *PROCESS STATUS* > として OID 値を設定します。たとえば、runtime - running として設定します。

Cisco ISE が SNMP トラップを SNMP サーバーに送信するのを停止させるには、Cisco ISE CLI から SNMP 設定を削除します。この操作によって、SNMP トラップの送信と、SNMP マネージャからのポーリングが停止されます。

Cisco ISE のディスク使用状況 SNMP トラップ

Cisco ISE のパーティションのディスク使用率がしきい値に到達し、設定された空きディスク領域の量に達すると、ディスク使用状況トラップが送信されます。

次の表に、Cisco ISE で設定可能なディスク使用状況 SNMP トラップのリストを示します。

OID	説明	トラップの例
.1.3.6.1.4.1.2021.9.1.9 \n UCD-SNMP-MIB::dskPercent	使用されているディスク容量の割合。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (118198297) 13 days, 16:19:42.97 SNMPv2-MIB::snmpTrapOID.0 = OID: UCD-SNMP-MIB::dskPercent UCD-SNMP-MIB::dskPercent = INTEGER: 13
.1.3.6.1.4.1.2021.9.1.2 \n UCD-SNMP-MIB::dskPath	ディスクがマウントされている場所のパス。 dskPath は、ISE 管理コマンド **show disks** の出力ですべてのマウントポイントのトラップを送信できます。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (118198304) 13 days, 16:19:43.04 SNMPv2-MIB::snmpTrapOID.0 = OID: UCD-SNMP-MIB::dskPath UCD-SNMP-MIB::dskPath = STRING: /opt

Cisco ISE アラーム

アラームは、ネットワークの重大な状態を通知し、[アラーム（Alarms）] 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、システムアクティビティを完全に無効にしたりできます。また、特定のアラームのしきい値を設定できます。

大半の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。その時点で最新の 15,000 件のアラームのみが保持されます。

イベントが繰り返し発生する場合、同じアラームは約 1 時間抑制されます。イベントが繰り返し発生する間、トリガーによっては、アラームが再び表示されるまでに約 1 時間かかる場合があります。

アラーム名、カテゴリ、シビラティ（重大度）、またはステータスに基づいて、表示するアラームをフィルタリングできます。複数のフィルタを選択した場合、フィルタ結果は加算的になります。これはカスケード フィルタと呼ばれます。これにより、ドリルダウンして特定のデータを見つけることができます。

クイックフィルタを使用すれば、リストページに表示されるフィールド属性の値を入力し、ページをリフレッシュすることで、フィルタ基準に一致するレコードのみを一覧表示できます。

拡張フィルタを使用すれば、アラーム名にTrustSecを含むなど、指定した条件に基づいて情報をフィルタリングできます。複数の条件を指定できます。

自分だけがアクセスできるユーザー固有のカスタムフィルタを作成して保存できます。

[すべてのフィルタをクリア（Clear All Filters）] をクリックして、すべての適用されたフィルタを削除します。

次の表に、すべての Cisco ISE アラームおよびその説明と解決方法を示します。

表 *2 : Cisco ISE* アラーム

アラーム名	アラームの説明	アラームの解決方法
管理および操作の監査の管理		
展開のアップグレードの失敗（Deployment Upgrade Failure）	ISE ノードでアップグレードに失敗しました。	アップグレードが失敗した原因と修正処置について、失敗したノードの ADE.log を確認します。
アップグレードバンドルのダウンロードの失敗（Upgrade Bundle Download failure）	アップグレードバンドルのダウンロードが ISE ノードで失敗しました。	アップグレードが失敗した原因と修正処置について、失敗したノードの ADE.log を確認します。
SXP 接続障害（SXP Connection Failure）	SXP接続に失敗しました。	SXP サービスが実行していることを確認します。ピアに互換性があることを確認します。
シスコプロファイルの全デバイスへの適用（Cisco profile applied to all devices）	ネットワーク デバイス プロファイルによって、MAB、Dot1X、CoA、Web リダイレクトなどのネットワーク アクセス デバイスの機能が定義されます。	シスコ以外のネットワークデバイスの設定を必要に応じて編集し、適切なプロファイルを割り当てます。

アラーム名	アラームの説明	アラームの解決方法
CRL で失効した証明書が見つかったことによるセキュア LDAP 接続の再接続（Secure LDAP connection reconnect due to CRL found revoked certificate）	CRL チェックの結果、LDAP 接続で使用された証明書が失効していることが検出されました。	CRL 設定が有効であることを確認します。LDAP サーバー証明書とその発行元の証明書が失効していないことを確認します。失効している場合は、新しい証明書を発行して LDAP サーバーにインストールします。
OCSP で失効した証明書が見つかったことによるセキュア LDAP 接続の再接続（Secure LDAP connection reconnect due to OCSP found revoked certificate）	OCSP チェックの結果、LDAP 接続で使用された証明書が失効していることが検出されました。	OCSP 設定が有効であることを確認します。LDAP サーバー証明書とその発行元の証明書が失効していないことを確認します。失効している場合は、新しい証明書を発行して LDAP サーバーにインストールします。
CRL で失効した証明書が見つかったことによるセキュア syslog 接続の再接続（Secure syslog connection reconnect due to CRL found revoked certificate）	CRL チェックの結果、syslog 接続で使用された証明書が失効していることが検出されました。	CRL 設定が有効であることを確認します。syslog サーバー証明書とその発行元の証明書が失効していないことを確認します。失効している場合は、新しい証明書を発行して syslog サーバーにインストールします。
OCSP で失効した証明書が見つかったことによるセキュアな syslog 接続の再接続（Secure syslog connection reconnect due to OCSP found revoked certificate）	OCSP チェックの結果、syslog 接続で使用された証明書が失効していることが検出されました。	OCSP 設定が有効であることを確認します。syslog サーバー証明書とその発行元の証明書が失効していないことを確認します。失効している場合は、新しい証明書を発行して syslog サーバーにインストールします。
管理者アカウントがロック/無効（Administrator account Locked/Disabled）	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、または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、他の管理者によってリセットできます。
ERS が非推奨の URL を検出（ERS identified deprecated URL）	ERS が廃止 URL を検出しました。	要求された URL は廃止されているため、使用しないでください。
ERS が古い URL を検出しました。	ERS が古い URL を検出しました。	要求された URL は古いため、新しい URL を使用してください。古い URL は今後のリリースで削除されません。

アラーム名	アラームの説明	アラームの解決方法
ERS 要求 Content-Type ヘッダーが古い（ERS request content-type header is outdated）	ERS 要求 Content-Type ヘッダーが最新ではありません。	要求 Content-Type ヘッダーで指定された要求のリソースバージョンが最新ではありません。これはリソーススキーマが変更されたことを意味します。いくつかの属性が追加または削除された可能性があります。古いスキーマをこのまま処理するために、ERS エンジンでデフォルト値が使用されます。
ERS XML 入力が XSS またはインジェクション攻撃の原因です（ERS XML input is a suspect for XSS or Injection attack）	ERS XML 入力が XSS またはインジェクション攻撃の原因になっています。	XML 入力を確認してください。
バックアップに失敗（Backup Failed）	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。次の点を確認します。 • リポジトリに使用しているログイン情報が正しいこと。 • リポジトリに十分なディスク領域があること。 • リポジトリ ユーザーが書き込み特権を持っていること。
CA サーバーがダウン（CA Server is down）	CA サーバーがダウンしています。	CA サービスが CA サーバーで稼働中であることを確認します。
CA サーバーが稼働中（CA Server is Up）	CA サーバーは稼働中です。	CA サーバーが稼働中であることを知らせる通知が管理者に送信されます。
証明書の有効期限（Certificate Expiration）	この証明書はまもなく有効期限が切れます。これが失効すると、Cisco ISE がクライアントとのセキュアな通信を確立しないようにします。	証明書を交換します。信頼できる証明書の場合、発行元の認証局（CA）にお問い合わせください。CA 署名付きローカル証明書の場合、CSR を生成し、CA に新しい証明書を作成してもらいます。自己署名した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場合、証明書を削除できます。

アラーム名	アラームの説明	アラームの解決方法
証明書が失効（Certificate Revoked）	内部 CA がエンドポイントに発行した証明書を管理者が取り消しました。	もう一度BYODフローに従って最初から新しい証明書を使用してプロビジョニングします。
証明書プロビジョニング初期化エラー（Certificate Provisioning Initialization Error）	証明書プロビジョニングの初期化に失敗しました。	複数の証明書でサブジェクトの CN（CommonName）属性が同じ値になっています。証明書チェーンを構築できません。SCEP（Simple Certificate Enrollment Protocol）サーバーからの証明書を含め、システム内のすべての証明書を確認します。
証明書の複製に失敗（Certificate Replication Failed）	セカンダリノードへの証明書の複製に失敗しました。	証明書がセカンダリノードで無効であるか、他の永続的なエラー状態があります。セカンダリノードに矛盾する証明書が存在しないかどうかを確認します。存在する場合は、セカンダリノードに存在する証明書を削除し、プライマリノードの新しい証明書をエクスポートしてから削除し、その後インポートして複製を再試行します。
証明書の複製に一時的に失敗（Certificate Replication Temporarily Failed）	セカンダリノードへの証明書の複製に一時的に失敗しました。	証明書は、ネットワークの停止などの一時的な状態によりセカンダリノードに複製されませんでした。複製は、成功するまで再試行されます。
証明書が失効（Certificate Expired）	この証明書の期限が切れています。Cisco ISE がクライアントとのセキュアな通信を確立しないようにします。ノードツーノード通信も影響を受ける場合があります。	証明書を交換します。信頼できる証明書の場合、発行元の認証局（CA）にお問い合わせください。CA 署名付きローカル証明書の場合、CSR を生成し、CA に新しい証明書を作成してもらいます。自己署名した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場合、証明書を削除できます。
証明書要求転送に失敗（Certificate Request Forwarding Failed）	証明書要求転送に失敗しました。	受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。

アラーム名	アラームの説明	アラームの解決方法
設定が変更（Configuration Changed）	Cisco ISE 設定が更新されています。このアラームは、ユーザーとエンドポイントに設定変更があってもトリガーされません。	設定変更が想定どおりであるかどうかを確認します。
CRL の取得に失敗（CRL Retrieval Failed）	サーバーから CRL を取得できません。これは、指定した CRL が使用できない場合に発生します。	ダウンロード URL が正しく、サービスに使用可能であることを確認します。
DNS 解決に失敗（DNS Resolution Failure）	ノードで DNS 解決に失敗しました。	**ip name-server** コマンドで設定した DNS サーバーが到達可能であるか確認します。 **DNS Resolution failed for CNAME <hostname of the node>** というアラームが表示された場合は、各 Cisco ISE ノードの A レコードとともに CNAME RR を作成していることを確認します。
ファームウェアの更新が必要（Firmware Update Required）	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の入手方法については、Cisco TAC にお問い合わせください。
仮想マシンリソースが不十分（Insufficient Virtual Machine Resources）	このホストには、CPU、RAM、ディスク容量、IOPS（1 秒当たりの入出力処理）などの仮想マシン（VM）リソースが不足しています。	Cisco ISE ハードウェア設置ガイド [英語] に指定されている VM ホストの最小要件を確認します。
NTP サービスの障害（NTP Service Failure）	NTP サービスがこのノードでダウンしています。	これは、NTP サーバーと Cisco ISE ノードとの間に大きな時間差（1000 秒以上）があるために発生することがあります。NTP サーバー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て、時間のずれを修正します。

アラーム名	アラームの説明	アラームの解決方法
NTP 同期に失敗（NTP Sync Failure）	このノードに構成されているすべてのNTPサーバーが到達不能です。	CLI で **show ntp** コマンドを実行してトラブルシューティングします。Cisco ISE から NTP サーバー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と値がサーバーの対応する値に一致することを確認します。
スケジュールされた設定バックアップなし（No Configuration Backup Scheduled）	Cisco ISE 設定バックアップがスケジュールされていません。	設定バックアップのスケジュールを作成します。
操作 DB 消去に失敗（Operations DB Purge Failed）	操作データベースから古いデータを消去できません。これは、MnT ノードがビジーの場合に発生します。	[データ消去の監査（Data Purging Audit）] レポートをチェックし、使用済みスペースがしきい値スペースより少ないことを確認します。CLI を使用して MnT ノードにログインし、消去操作を手動で実行します。
プロファイラ SNMP 要求に失敗（Profiler SNMP Request Failure）	SNMP 要求がタイムアウトしたか、あるいはSNMP コミュニティまたはユーザー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 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（Replication Failed）	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（Deployment）] ウィンドウから手動同期を実行します。影響を受ける Cisco ISE ノードを登録解除してから登録し直します。
復元に失敗（Restore Failed）	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も確認します。CLI で **reset-config** コマンドを実行して、正常な既知の最終バックアップを復元します。
パッチに失敗（Patch Failure）	パッチプロセスがサーバーで失敗しました。	サーバーにパッチプロセスを再インストールします。
パッチに成功（Patch Success）	パッチプロセスがサーバーで成功しました。	—

アラーム名	アラームの説明	アラームの解決方法
外部 MDM サーバー API バージョンが不一致（External MDM Server API Version Mismatch）	外部 MDM サーバー API バージョンが Cisco ISE に設定されたものと一致しません。	MDM サーバー API バージョンが Cisco ISE に設定されたものと同じであることを確認します。Cisco ISE MDM サーバー設定を更新します（必要な場合）。
外部 MDM サーバー接続に失敗（External MDM Server Connection Failure）	外部 MDM サーバーへの接続に失敗しました。	MDM サーバーが稼働し、Cisco ISE-MDM API サービスが MDM サーバーで稼働していることを確認します。
外部 MDM サーバー応答エラー（External MDM Server Response Error）	外部 MDM サーバー応答エラーです。	Cisco ISE-MDM API サービスが MDM サーバーで適切に動作していることを確認します。
複製が停止（Replication Stopped）	ISE ノードが PAN から設定データを複製できませんでした。	Cisco ISE GUI にログインし、[展開（Deployment）] ウィンドウから手動同期を実行するか、または影響を受けた ISE ノードを登録解除してから必須フィールドを指定して再登録します。
MDM コンプライアンスポーリングが無効（MDM Compliance Polling Disabled）	定期的なコンプライアンスポーリングで、膨大な非準拠デバイス情報を受信しました。	MDM サーバーに到達する非準拠デバイス要求の数を 20000 未満に維持します。
エンドポイント証明書が期限切れ（Endpoint certificates expired）	エンドポイント証明書が日次スケジュールジョブで期限切れとマークされました。	エンドポイントデバイスを再登録して新しいエンドポイント証明書を取得します。
エンドポイント証明書が消去（Endpoint certificates purged）	期限切れのエンドポイント証明書が日次スケジュールジョブによって消去されました。	特に対処は必要ありません。これは、管理者が開始したクリーンアップ操作です。
エンドポイントのアクティビティ消去	過去 24 時間のエンドポイントのアクティビティを消去します。このアラームは、真夜中にトリガーされます。	**[操作（Operations）] > [レポート（Reports）] > [エンドポイントとユーザー（Endpoints and Users）] > [エンドポイントのアクティビティ消去（Endpoints Purge Activities）]** を選択して、消去アクティビティを確認します。

アラーム名	アラームの説明	アラームの解決方法
複製低速エラー（Slow Replication Error）	低速またはスタックした複製が検出されました。	ノードが到達可能であり、展開の一部であることを確認します。
複製低速情報（Slow Replication Info）	低速の複製またはスタックした複製が検出されました。	ノードが到達可能であり、展開の一部であることを確認します。
複製低速警告（Slow Replication Warning）	低速またはスタックした複製が検出されました。	ノードが到達可能であり、展開の一部であることを確認します。
PAN 自動フェールオーバー：フェールオーバーが失敗しました（PAN Auto Failover - Failover Failed）	セカンダリ管理ノードへのプロモーション要求が失敗しました。	解決方法については、アラームの詳細を参照してください。
PAN 自動フェールオーバー：フェールオーバーがトリガーされました（PAN Auto Failover - Failover Triggered）	プライマリロールにセカンダリ管理ノードのフェールオーバーが正常にトリガーされました。	セカンダリ PAN のプロモーションが完了するまで待機し、古いプライマリ PAN を起動します。
PAN 自動フェールオーバー：ヘルスチェックの非アクティビティ（PAN Auto Failover - Health Check Inactivity）	PAN がモニタリング ノードからヘルスチェックのモニタリング要求を受け取りませんでした。	報告されたモニタリングノードがダウンしているか、または同期していないか確認し、必要に応じて、手動同期をトリガーします。
PAN 自動フェールオーバー：無効なヘルスチェック（PAN Auto Failover - Invalid Health Check）	自動フェールオーバーで無効なヘルス チェック モニタリング要求が受信されました。	ヘルス チェック モニタリング ノードが同期していることを確認し、必要な場合は手動で同期をトリガーします。
PAN 自動フェールオーバー：プライマリ管理ノードのダウン（PAN Auto Failover - Primary Administration Node Down）	PAN がダウンしているか、またはモニタリングノードから到達不能です。	PAN を起動するか、またはフェールオーバーが発生するまで待機します。
PAN 自動フェールオーバー：フェールオーバーの試行が拒否されました（PAN Auto Failover - Rejected Failover Attempt）	ヘルス チェック モニター ノードによって行われたプロモーション要求をセカンダリ管理ノードが拒否しました。	解決方法については、アラームの詳細を参照してください。

アラーム名	アラームの説明	アラームの解決方法
EST サービスの停止（EST Service is down）	EST サービスが停止しています。	CA および EST サービスが稼働しており、証明書サービスのエンドポイントサブ CA 証明書チェーンが完了していることを確認します。
EST サービスの稼働（EST Service is up）	EST サービスが稼働しています。	EST サービスが稼働中であることを知らせる通知が管理者に送信されます。
Smart Call Home の通信障害（Smart Call Home Communication Failure）	Smart Call Home メッセージが正常に送信されませんでした。	Cisco ISE と Cisco システムの間でネットワーク接続があることを確認します。
テレメトリ メッセージの障害（Telemetry Communication Failure）	テレメトリ メッセージが正常に送信されませんでした。	Cisco ISE と Cisco システムの間でネットワーク接続があることを確認します。
アダプタに接続できない	Cisco ISE は、アダプタに接続できません。	エラーの詳細はアダプタ ログを確認してください。
アダプタのエラー	アダプタにエラーが生じています。	アラームの説明を確認してください。
アダプタ接続の失敗	アダプタは、送信元のサーバーに接続できません。	送信元のサーバーがアクセス可能であることを確認してください
エラーによるアダプタの停止	アダプタにエラーが発生し、望ましい状態ではありません。	アダプタの設定が正しく、送信元サーバーがアクセス可能であることを確認してください。エラーの詳細については、アダプタログを確認してください。
サービス コンポーネントのエラー	サービス コンポーネントにエラーが生じています。	アラームの説明を確認してください。
サービス コンポーネントの情報	サービス コンポーネントが情報を送信しました。	なし。
ISE サービス		
過剰な TACACS 認証試行（Excessive TACACS Authentication Attempts）	ISE ポリシーサービスノードで TACACS 認証の割合が想定よりも多くなっています。	• 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。 • 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。

アラーム名	アラームの説明	アラームの解決方法
過剰な TACACS 認証の失敗した試行（Excessive TACACS Authentication Failed Attempts）	ISE ポリシーサービスノードで失敗した TACACS 認証の割合が想定よりも多くなっています。	• 根本原因を特定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、ISE または NAD の設定を確認します。
MSE ロケーション サーバーへのアクセス回復（MSE Location Server accessible again）	MSE ロケーション サーバーへのアクセスが回復しました。	なし。
MSE ロケーション サーバーにアクセス不能（MSE Location Server not accessible.）	MSE ロケーションサーバーはアクセス不能であるか、ダウンしています。	MSE ロケーションサーバーが稼働中で、ISE ノードからアクセスできるか確認します。
AD コネクタを再起動する必要があります（AD Connector had to be restarted）	AD コネクタが突然シャットダウンし、再起動が必要となりました。	問題が解決しない場合は、Cisco TAC にお問い合わせください。
Active Directory フォレストが使用不可（Active Directory Forest is unavailable）	Active Directory フォレストグローバルカタログが使用できず、認証、許可、およびグループと属性の取得に使用できません。	DNS 設定、Kerberos 設定、エラー状態、およびネットワーク接続を確認します。
認証ドメインが使用不可（Authentication domain is unavailable）	認証ドメインが使用できず、認証、許可、およびグループと属性の取得に使用できません。	DNS 設定、Kerberos 設定、エラー状態、およびネットワーク接続を確認します。
ISE の認証非アクティビティ（ISE 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け取っていません。	• Cisco ISE および NAD の設定を確認します。 • Cisco ISE および 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。
ID マッピングの認証非アクティビティ（ID Map. Authentication Inactivity）	過去 15 分間、ユーザー認証イベントが ID マッピングサービスによって収集されませんでした。	ユーザー認証が想定される時間（勤務時間など）である場合は、Active Directory ドメインコントローラへの接続を確認します。

アラーム名	アラームの説明	アラームの解決方法
CoA 失敗（CoA Failed）	ネットワークデバイスが、Cisco ISE ポリシーサービスノードによって発行された認可変更（CoA）要求を拒否しました。	そのネットワークデバイスが Cisco ISE からの 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に対して発行されているか確認します。
設定されたネームサーバーがダウン（Configured nameserver is down）	設定されたネームサーバーがダウンしているか、使用できません。	DNS 設定とネットワーク接続を確認します。
サプリカントが応答停止（Supplicant Stopped Responding）	Cisco ISE がクライアントに最後のメッセージを 120 秒前に送信しましたが、クライアントから応答がありません。	• 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。
過剰な認証試行（Excessive Authentication Attempts）	Cisco ISE ポリシー サービス ノードで認証の割合が想定よりも多くなっています。	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。 しきい値が満たされた場合、[過剰な認証試行（Excessive Authentication Attempts）] および [過剰な失敗試行（Excessive Failed Attempts）] アラームがトリガーされます。[説明（Description）] 列の横に表示される数値は、過去 15 分間に Cisco ISE に対して成功または失敗した認証の総数です。

アラーム名	アラームの説明	アラームの解決方法
過剰な失敗試行（Excessive Failed Attempts）	Cisco ISE ポリシー サービス ノードで認証失敗の割合が想定よりも多くなっています。	根本原因を特定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 または NAD の設定を確認します。 しきい値が満たされた場合、[過剰な認証試行（Excessive Authentication Attempts）] および [過剰な失敗試行（Excessive Failed Attempts）] アラームがトリガーされます。[説明（Description）] 列の横に表示される数値は、過去 15 分間に Cisco ISE に対して成功または失敗した認証の総数です。
AD：マシン TGT のリフレッシュに失敗（AD: Machine TGT refresh failed）	ISE サーバーのチケット認可チケット（TGT）の更新に失敗しました。TGT は、Active Directory 接続とサービスに使用されます。	ISE マシン アカウントが存在し、有効であることを確認します。また、クロックスキュー、複製、ケルベロスの設定、またはネットワークエラー、あるいはこれらすべてを確認します。
AD：ISE アカウント パスワードの更新に失敗（AD: ISE account password update failed）	ISE サーバーは、AD マシン アカウント パスワードを更新できませんでした。	ISE マシン アカウント パスワードが変更されていないことと、マシンアカウントが無効でなく制限もされていないことを確認します。KDC への接続を確認します。
参加しているドメインが使用不可（Joined domain is unavailable）	参加しているドメインが使用できず、認証、許可、およびグループと属性の取得に使用できません。	DNS 設定、Kerberos 設定、エラー状態、およびネットワーク接続を確認します。
ID ストアが使用不可（Identity Store Unavailable）	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。
正しく設定されていないネットワーク デバイスを検出（Misconfigured Network Device Detected）	Cisco ISE が、NAS からの過剰な RADIUS アカウンティング情報を検出しました。	非常に多くの重複する 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頻度で NAS を設定します。

アラーム名	アラームの説明	アラームの解決方法
正しく設定されていないサプリカントを検出（Misconfigured Supplicant Detected）	Cisco ISE は、ネットワーク上で正しく設定されていない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。
アカウンティングの開始なし（No Accounting Start）	Cisco ISE ポリシーサービスノードではセッションを許可していますが、ネットワークデバイスからアカウンティング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。ローカル許可に対するネットワーク デバイス設定を確認します。
NAD が不明な（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どうかを確認してから、それを設定に追加します。シークレットが一致することを確認します。
SGACL がドロップ（SGACL Drops）	セキュリティ グループ アクセス（SGACL）ドロップが発生しました。これは、SGACL ポリシーの違反により、TrustSec 対応デバイスがパケットをドロップすると発生します。	RBACL ドロップ概要レポートを実行し、SGACL ドロップを引き起こしているソースを確認します。攻撃ソースに CoA を発行してセッションを再許可または切断します。
RADIUS 要求がドロップ（RADIUS Request Dropped）	NAD からの認証およびアカウンティング要求がサイレントに破棄されています。これは、NAD が不明であるか、共有秘密が不一致であるか、RFC ごとのパケット内容が無効であるために発生することがあります。	NAD/AAA クライアントについて Cisco ISE に有効な設定があることを確認します。NAD/AAA クライアントと Cisco ISE の共有秘密が一致しているかどうかを確認します。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。
EAP セッションの割り当てに失敗（EAP Session Allocation Failed）	RADIUS 要求は EAP セッションの制限に達したためにドロップされました。この状態の原因として、並列 EAP 認証要求が多すぎることが考えられます。	新しい EAP セッションで別の RADIUS 要求を呼び出す前に数秒間待ちます。システムのオーバーロードが発生する場合は、ISE サーバーの再起動を試してください。

アラーム名	アラームの説明	アラームの解決方法
RADIUS コンテキストの割り当てに失敗（RADIUS Context Allocation Failed）	RADIUS 要求はシステムのオーバーロードのためにドロップされました。この状態の原因として、並列認証要求が多すぎることが考えられます。	新しい RADIUS 要求を呼び出す前に数秒間待ちます。システムのオーバーロードが発生する場合は、ISE サーバーの再起動を試してください。
AD：ISE のマシン アカウントにグループを取得するために必要な権限がない	Cisco ISE のマシン アカウントにグループを取得するために必要な権限がありません。	Cisco ISE のマシンアカウントに Active Directory のユーザーグループを取得する権限があるか確認します。
ポスチャ設定の検出（Posture Configuration Detection）	ポスチャ状態同期ポートは、準拠認証プロファイルに対してブロックされません。	クライアント ポスチャ ステータスが準拠している場合、ポスチャ状態同期プローブが Cisco ISE に到達しないように ACL を設定します。
システムの状態（System Health）		
ディスク I/O 使用率が高い（High Disk I/O Utilization）	Cisco ISE システムは、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を確認します。負荷を分散するためのサーバーを追加します。
ディスク領域の使用率が高い（High Disk Space Utilization）	Cisco ISE システムは、ディスク領域の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を確認します。負荷を分散するためのサーバーを追加します。

アラーム名	アラームの説明	アラームの解決方法
負荷平均が高い（High Load Average）	Cisco ISE システムは、不可平均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を確認します。負荷を分散するためのサーバーを追加します。 サードパーティツールを使用してシングルCPUコアの負荷平均を確認しないでください。このメトリックにはシステム全体の負荷が反映されないためです。システム負荷の累積ビューには、Cisco ISE CLI で **tech top** コマンドを使用することをお勧めします。 プライマリおよびセカンダリ MnT ノードの 2:00 a.m. タイムスタンプに対して [負荷平均が高い（High Load Average）] アラームが表示される場合、この時刻に実行している DBMS 統計が原因でCPU使用率が高くなっている可能性があります。DBMS 統計が完了すると、CPU使用率は通常に戻ります。 [負荷平均が高い（High Load Average）] アラームは、毎週日曜日の午前 1 時に、毎週のメンテナンスタスクによってトリガーされます。このメンテナンスタスクによって、1 GB以上の領域を占有するすべてのインデックスが再構築されます。このアラームは無視できます。

アラーム名	アラームの説明	アラームの解決方法
メモリ使用率が高い（High Memory Utilization）	Cisco ISE システムは、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を確認します。負荷を分散するためのサーバーを追加します。 メモリ使用率の確認にサードパーティのツールを使用しないでください。Cisco ISE CLI で **show memory** コマンドを使用して、メモリ使用率を確認することをお勧めします。 Cisco ISE ノードでは、オペレーティングシステムによってメモリ使用率が管理されます。メモリ使用率のより信頼できる測定値を得るには、（空きメモリではなく）使用可能なメモリのメトリックを確認する必要があります。 オペレーティングシステムは、バッファまたはキャッシュ内のほとんどのメモリをセグメント化することに注意してください。合計メモリの 90% 未満が使用済みとして表示され、スワップメモリに実質的な増加がない場合、Cisco ISE のメモリ使用率は安定していると見なすことができます。
操作 DB の使用率が高い（High Operations DB Usage）	ノードをモニターする Cisco ISE は、syslog データの量が想定よりも多くなっています。	操作データの消去設定ウィンドウを確認して削減します。
認証待ち時間が長い（High Authentication Latency）	Cisco ISE システムは、認証待ち時間が長くなっています。	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を確認します。負荷を分散するためのサーバーを追加します。

アラーム名	アラームの説明	アラームの解決方法
ヘルス ステータスが使用不可（Health Status Unavailable）	モニタリングノードが 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 ノードが稼働していて、モニタリングノードと通信できることを確認します。
プロセスがダウン（Process Down）	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 キュー サイズの制限に到達（Profiler Queue Size Limit Reached）	ISE プロファイラキューサイズの制限に到達しました。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ことを確認し、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。
OCSP トランザクションしきい値に到達	OCSP トランザクションしきい値に到達しました。このアラームは、内部 OCSP サービスのトランザクション数がそのしきい値に到達するとトリガーされます。	システムに十分なリソースがあるかどうかを確認します。
ライセンシング		
ライセンスがまもなく期限切れ（License About to Expire）	Cisco ISE ノードにインストールされたライセンスがまもなく期限切れになります。	Cisco ISE の [ライセンス（Licensing）] ウィンドウを参照してライセンスの使用状況を確認します。
ライセンスが期限切れ（License Expired）	Cisco ISE ノードにインストールされたライセンスの期限が切れました。	シスコアカウントチームに問い合わせて、新しいライセンスを購入してください。
ライセンス違反（License Violation）	Cisco ISE ノードが、許可されたライセンス数を超過しているか、またはまもなく超過することを検出しました。	シスコアカウントチームに問い合わせて、追加のライセンスを購入してください。
スマートライセンスの認証の期限切れ	スマートライセンスの認証の有効期限が切れました。	[Cisco ISE ライセンス管理（Cisco ISE License Administration）] ウィンドウを参照して、手動でスマートライセンスの登録を更新するか、Cisco Smart Software Manager とのネットワーク接続を確認してください。問題が続くようであれば、シスコパートナーまでお問い合わせください。

アラーム名	アラームの説明	アラームの解決方法
スマートライセンスの認証の更新の失敗	Cisco Smart Software Manager を使用した認証の更新に失敗しました。	[Cisco ISE ライセンス管理（Cisco ISE License Administration）] ウィンドウを参照し、[ライセンス（Licenses）] テーブルの [更新（Refresh）] ボタンを使用して、Cisco Smart Software Manager で認証を手動で更新します。問題が続くようであれば、シスコパートナーまでお問い合わせください。
スマートライセンスの認証の更新の成功	Cisco Smart Software Manager を使用した認証の更新に成功しました。	Cisco Smart Software Manager を使用した Cisco ISE の認証の更新が成功したことを知らせる通知が送信されます。
スマートライセンスの通信障害	Cisco Smart Software Manager と Cisco ISE の通信が失敗しました。	Cisco Smart Software Manager とのネットワーク接続を確認します。問題が続くようであれば、Cisco Smart Software Manager にログインするか、またはシスコパートナーまでお問い合わせください。
復元されたスマートライセンスの通信	Cisco Smart Software Manager と Cisco ISE の通信が復元されました。	Cisco Smart Software Manager とのネットワーク接続が復元されたことを知らせる通知が送信されます。
スマートライセンスの登録解除の障害	Cisco Smart Software Manager を使用した Cisco ISE の登録解除に失敗しました。	詳細については、[Cisco ISE ライセンス管理（Cisco ISE License Administration）] ウィンドウを参照してください。問題が続くようであれば、Cisco Smart Software Manager にログインするか、またはシスコパートナーまでお問い合わせください。
スマートライセンスの登録解除の成功	Cisco Smart Software Manager を使用した Cisco ISE の登録解除に成功しました。	Cisco Smart Software Manager を使用した Cisco ISE の登録解除に成功したことを知らせる通知が送信されます。

アラーム名	アラームの説明	アラームの解決方法
スマートライセンスの無効化	スマートライセンスは Cisco ISE で無効になり、従来のライセンスが使用されています。	スマートライセンスを再度有効にするには、[ライセンスの管理（License Administration）] ウィンドウを参照してください。Cisco ISE のスマートライセンスの使用方法の詳細については、Cisco ISE 管理者ガイド [英語] を参照するか、シスコパートナーにお問い合わせください。
スマートライセンスの評価期間の期限切れ	スマートライセンスの評価期間が終了しました。	Cisco Smart Software Manager を使用して Cisco ISE を登録するには、[Cisco ISE ライセンス管理（Cisco ISE License Administration）] ウィンドウを参照してください。
スマート ライセンスの HA 役割の変更	スマートライセンスの使用中に、ハイアベイラビリティの役割の変更が発生しました。	Cisco ISE の HA ロールが変わったことを知らせる通知が送信されます。
スマート ライセンス ID 証明書の期限切れ	スマートライセンス証明書の期限が切れました。	手動でスマートライセンスの登録を更新するには、[Cisco ISE ライセンス管理（Cisco ISE License Administration）] ウィンドウを参照してください。問題が続くようであれば、シスコパートナーまでお問い合わせください。
スマート ライセンス ID 証明書の更新の失敗	Cisco Smart Software Manager を使用したスマートライセンスの登録の更新が失敗しました。	手動でスマートライセンスの登録を更新するには、[Cisco ISE ライセンス管理（Cisco ISE License Administration）] ウィンドウを参照してください。問題が続くようであれば、シスコパートナーまでお問い合わせください。
スマート ライセンス ID 証明書の更新の成功	Cisco Smart Software Manager を使用したスマートライセンスの登録の更新が成功しました。	Cisco Smart Software Manager を使用した登録の更新が成功したことを知らせる通知が送信されます。

アラーム名	アラームの説明	アラームの解決方法
スマートライセンスの無効な要求	無効な要求が Cisco Smart Software Manager に送信されました。	詳細については、[Cisco ISE ライセンス管理（Cisco ISE License Administration）] ウィンドウを参照してください。問題が続くようであれば、Cisco Smart Software Manager にログインするか、またはシスコパートナーまでお問い合わせください。
コンプライアンスに準拠していないスマートライセンス	Cisco ISE ライセンスがコンプライアンスに準拠していません。	詳細については、[ISE ライセンス管理（ISE License Administration）] ウィンドウを参照してください。新しいライセンスを購入するには、パートナーまたはシスコアカウントチームにお問い合わせください。
スマートライセンスの登録の障害	Cisco Smart Software Manager を使用した Cisco ISE の登録が失敗しました。	詳細については、[ISE ライセンス管理（ISE License Administration）] ウィンドウを参照してください。問題が続くようであれば、Cisco Smart Software Manager にログインするか、またはシスコパートナーまでお問い合わせください。
スマートライセンスの登録の成功	Cisco Smart Software Manager を使用した Cisco ISE の登録に成功しました。	Cisco Smart Software Manager を使用した Cisco ISE の登録に成功したことを知らせる通知が送信されます。
システム エラー		
ログ収集エラー（Log Collection Error）	コレクタプロセスをモニターする Cisco ISE が、ポリシーサービスノードから生成された監査ログを使用して処理を継続できません。	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。その後の解決については、Cisco TAC にお問い合わせください。
スケジュールされているレポートのエクスポートに失敗（Scheduled Report Export Failure）	設定されたリポジトリにエクスポートされたレポート（CSV ファイル）をコピーできません。	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場合は、再度追加します。リポジトリが使用できないか、またはリポジトリ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。
TrustSec		

アラーム名	アラームの説明	アラームの解決方法
不明なSGTのプロビジョニング（Unknown SGT was provisioned）	不明なSGTがプロビジョニングされました。	ISE は承認フローの一部として不明な SGT をプロビジョニングしました。不明なSGTは既知のフローの一部として割り当てることはできません。
一部の TrustSec ネットワーク デバイスに最新の ISE IP-SGTマッピング設定がありません（Some TrustSec network devices do not have the latest ISE IP-SGT mapping configuration）	一部の TrustSec ネットワーク デバイスに最新の ISE IP-SGTマッピング設定がありません。	ISEが異なるIP-SGTマッピングセットを持ついくつかのネットワークデバイスを検出しました。[IP-SGTマッピング展開（IP-SGT mapping Deploy）]オプションを使用してデバイスを更新します。
TrustSec SSH 接続に失敗しました。	TrustSec SSH 接続の失敗（TrustSec SSH connection failed）	ISE がネットワーク デバイスへの SSH 接続を確立できませんでした。[ネットワークデバイス（Network Device）]ウィンドウでネットワークデバイスのSSHログイン情報がネットワークデバイス上のログイン情報と類似していることを確認します。ネットワーク デバイスで ISE（IP アドレス）からの SSH 接続が有効になっていることを確認します。
TrustSec で識別された ISE が 1.0 以外の TLS バージョンで動作するよう設定されている（TrustSec identified ISE was set to work with TLS versions other than 1.0）	TrustSec で識別された ISE は 1.0 以外の TLS バージョンで動作するよう設定されています。	TrustSec は TLS バージョン 1.0 のみをサポートします。
TrustSec PAC の検証の失敗（Trustsec PAC validation failed）	TrustSec PAC の検証に失敗しました。	ISE がネットワークデバイスから送信されたPACを検証できませんでした。[ネットワークデバイス（Network Device）] ウィンドウとデバイスの CLI で、TrustSec デバイスのログイン情報を確認します。デバイスがISEサーバーによってプロビジョニングされた有効なPACを使用していることを確認します。

アラーム名	アラームの説明	アラームの解決方法
TrustSec 環境データのダウンロードの失敗（Trustsec environment data download failed）	TrustSec 環境データのダウンロードに失敗しました	Cisco ISE は不正な環境データ要求を受信しました。 次のことを確認してください。 • 要求に PAC が存在し有効である。 • すべての属性が要求に存在している。
TrustSec CoA メッセージの無視	TrustSec CoA メッセージが無視されました。	Cisco ISE は、TrustSec CoA メッセージを送信し、応答を受信しませんでした。ネットワークデバイスがCoA対応であることを確認してください。ネットワークデバイス設定を確認してください。
TrustSec のデフォルトの出力ポリシーの変更	TrustSec のデフォルトの出力ポリシーが変更されました。	セキュリティポリシーに合致していることを確認します。

（注） アラームは、Cisco ISE にユーザーまたはエンドポイントを追加する場合にはトリガーされません。

アラーム設定

次の表では、[アラーム設定（Alarm Settings）] ウィンドウ（**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[アラーム設定（Alarm Settings）]** > **[アラームの設定（Alarm Configuration）]** > **[追加（Add）]**）のフィールドについて説明します。

フィールド名	説明
アラーム タイプ（Alarm Type）	アラームタイプ。
Alarm Name	アラームの名前。
説明	アラームの説明。
[Suggested Actions]	アラームがトリガーされたときに実行されるアクション。

フィールド名	説明
Status（ステータス）	アラームルールの有効化または無効化。
シビラティ（重大度）	アラームのシビラティ（重大度）レベルを選択します。有効なオプションは次のとおりです。 • [重大（Critical）]：重大なエラーの条件を示します。 • [警告（Warning）]：正常ではあるものの重要な状態を示します。これがデフォルトの条件です。 • [情報（Info）]：情報メッセージを示します。
syslog メッセージを送信（**Send Syslog Message**）	Cisco ISE で生成される各システムアラームの syslog メッセージを送信します。
複数の電子メールアドレスをカンマで区切って入力（**Enter multiple e-mails separated with comma**）	電子メールアドレスまたは ISE 管理者名あるいはその両方のリスト。
電子メールのメモ（**0 ～ 4,000** 文字）（**Notes in Email (0 to 4000 characters)**）	システムアラームに関連付けるカスタムテキストメッセージ。

カスタム アラームの追加

Cisco ISE には [メモリ使用率が高い（High Memory Utilization）]、[設定変更（Configuration Change）] など 12 種類のデフォルト アラームがあります。シスコ定義のシステムアラームは [アラーム設定（Alarms Settings）] ウィンドウ（**[管理（(Administration)）]** > [システム（System）] > [設定（Settings）] > [アラーム設定（Alarms Settings）]）に表示されます。システム アラームだけを編集できます。

既存のシステムアラームに加えて、既存のアラームタイプでカスタムアラームを追加、編集、削除できます。

アラームタイプごとに、最大 5 つのアラームを作成できます。アラームの総数は 200 に制限されています。

[アラーム設定（Alarm Settings）] ウィンドウの [アラーム設定（Alarm Configuration）] タブの [条件（Conditions）] 列に、[認証待ち時間が長い（High Authentication Latency）]、[ディスク

I/O 使用率が高い（High Disk I/O Utilization）]、[ディスク領域の使用率が高い（High Disk Space Utilization）]、[メモリ使用率が高い（High Memory Utilization）] の 4 つのアラームの詳細が表示されます。これらのアラームそれぞれには設定可能なしきい値があります。ただし、[条件（Conditions）]列には、しきい値が設定された後でも詳細が表示されないことがあります。表示されない場合は、そのアラームの関連するしきい値フィールドを再編集して、[条件（Conditions）] 列に詳細を表示します。

アラームを追加するには、次の手順を実行します。

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 [アラームの設定（Alarm Configuration）] タブで、[追加（Add）] をクリックします。

ステップ 3 次の必須詳細情報を入力します。詳細については、「アラーム設定」の項を参照してください。

アラームタイプに基づいて（[メモリ使用率が高い（High Memory Utilization）]、[過剰な RADIUS 認証試行（Excessive RADIUS Authentication Attempts）]、[過剰な TACACS 認証試行（Excessive TACACS Authentication Attempts）] など）、追加の属性が [アラーム設定（Alarm Configuration）] ウィンドウに表示されます。たとえば、設定変更アラームには、[オブジェクト名（Object Name）]、[オブジェクトタイプ（Object Types）] および[管理者名（Admin Name）]フィールドが表示されます。さまざまな基準で同じアラームの複数のインスタンスを追加できます。

ステップ 4 [Submit] をクリックします。

Cisco ISE アラーム通知およびしきい値

Cisco ISE アラームを有効または無効にし、重大な状態を通知するように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。

通知の設定はアラームベースで設定し、アラームごとに通知する必要があるユーザーの電子メール ID を入力できます（システム定義アラームとユーザー定義アラームの両方）。

（注） アラーム ルール レベルで指定された受信者の電子メール アドレスは、グローバルの受信者の電子メール アドレスより優先されます。

アラームの有効化および設定

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

ステップ 2 オプションボタンをクリックして、デフォルトアラームのリストからアラームを選択し [編集（Edit）] をクリックします。

ステップ 3 [ステータス（Status）] ドロップダウンリストから [有効（Enable）] または [無効（Disable）] を選択します。

ステップ 4 アラームしきい値を必要に応じて設定します。

ステップ 5 [Submit] をクリックします。

モニターリング用の Cisco ISE アラーム

Cisco ISE は、重大なシステム状態の発生時には必ず通知するシステムアラームを提供します。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（Alarm）] 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ます。このリストから、表示するアラームの詳細を選択できます。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。

モニターリング アラームの表示

ステップ 1 Cisco ISE **ダッシュボード**に進みます。

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を含むダイアログボックスが開きます。

ステップ 3 アラームをリフレッシュするには、[リフレッシュ（Refresh）] をクリックします。

ステップ 4 確認応答アラームは、アラームを既読としてマークすることで、アラームカウンタ（アラームの発生回数）を削減します。タイムスタンプの横にあるチェックボックスをオンにして、確認するアラームを選択します。

[確認応答（Acknowledge）] ドロップダウンリストから **[選択済みの確認応答（Acknowledge Selected）]** を選択して、ウィンドウに現在表示されているすべてのアラームを既読としてマークします。デフォルトでは、100 行がウィンドウに表示されます。[行/ページ（Rows/Page）] ドロップダウンリストから値を選択することで、表示する別の行数を選択できます。

[確認応答（Acknowledge）] ドロップダウンリストから **[すべての確認応答（Acknowledge All）]** を選択して、ウィンドウに現在表示されているかどうかに関係なく、リストにあるすべてのアラームを既読としてマークします。

（注） タイトル行の [タイムスタンプ（Time Stamp）] の隣にあるチェックボックスをオンにすると、ウィンドウに表示されているすべてのアラームが選択されます。ただし、選択した 1 つ以上のアラームのチェックボックスをオフにすると、全選択機能が無効になります。この時点で、[タイムスタンプ（Time Stamp）] の隣にあるチェックボックスがオフになっていることがわかります。

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を含むダイアログボックスが開きます。

（注） ペルソナの変更前に生成された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。

ログ収集

モニタリングサービスはログと設定データを収集し、そのデータを保存してから、レポートおよびアラームを生成するために処理します。展開内の任意のサーバーから収集されたログの詳細を表示できます。

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。

（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 サーバー（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必要があります。

syslog メッセージを受信するには、syslog サーバー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。

リモートロギングターゲットをアラームターゲットとして設定するには、次の手順を実行します。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[リモートロギングターゲット（Remote Logging Targets）]** を選択します。

ステップ 2 [Add] をクリックします。

ステップ 3 [新しいロギングターゲット（New Logging Target）] ウィンドウで、ロギングターゲットに必要な詳細を送信し、[このターゲットのアラームを含める（Include Alarms for this Target）] チェックボックスをオンにします。

RADIUS ライブ ログ

次の表では、最近の RADIUS 認証を表示する [ライブログ（Live Logs）] ウィンドウのフィールドについて説明します。このページへのナビゲーションパスは、次のとおりです。**[操作（Operations）] > [RADIUS] > [ライブログ（Live Logs）]**を選択します。RADIUS ライブログはプライマリ PAN でのみ確認できます。

表 *3 : RADIUS* ライブ ログ

フィールド名	説明
Time	モニタリングおよびトラブルシューティング収集エージェントがログを受信した時刻を表示します。このカラムは必須です。選択解除することはできません。
Status（ステータス）	認証の成功/失敗を表示します。このカラムは必須です。選択解除することはできません。緑色は認証が成功したことを示します。赤色は認証が失敗したことを示します。
詳細	[詳細（Details）] 列の下にあるアイコンをクリックすると、新しいブラウザウィンドウに **[認証詳細レポート（Authentication Detail Report）]** が表示されます。このレポートには、認証と関連属性のほか、認証フローに関する情報が記載されています。 そのセッションのアカウンティングイベントが処理された場合、[Details] 列の下にあるアイコンをクリックすると、[Accounting Detail] レポートが開きます。セッションが認証済みの状態である場合、[Details] 列の下にあるアイコンをクリックすると、[Authentication Detail] レポートが表示されます。 [Authentication Detail] レポートの [Response Time] は、Cisco ISE で認証フローを処理するのにかかった合計時間です。たとえば、認証が 3 つのラウンドトリップメッセージで構成されている場合（最初のメッセージは 300 ミリ秒、次のメッセージは 150 ミリ秒、最後のメッセージは 100 ミリ秒）、[応答時間（Response Time）] は、300 + 150 + 100 = 550 ミリ秒になります。 （注） 48 時間を超えるアクティブになっているエンドポイントの詳細を表示することはできません。48 時間を超えてアクティブになっているエンドポイントの [詳細（Details）] アイコンをクリックすると、次のメッセージがウィンドウに表示されます。 `No Data available for this record. Either the data is purged or authentication for this session record happened a week ago. Or if this is an 'PassiveID' or 'PassiveID Visibility' session, it will not have authentication details on ISE but only the session.`

フィールド名	説明
繰り返し回数（**Repeat Count**）	ID、ネットワークデバイス、および許可のコンテキストで変更がなく、直近の 24 時間で認証要求が繰り返された回数を表示します。
ID（**Identity**）	ログイン済みの認証に関連付けられているユーザー名を示します。 ユーザー名が ID ストアに存在しない場合は、「無効（INVALID）」と表示されます。その他の原因で認証に失敗した場合は、「ユーザー名（USERNAME）」と表示されます。 （注） これはユーザーにのみ適用されます。これはMACアドレスには適用されません。 デバッグをサポートするために、無効なユーザー名の開示をISEに強制できます。これを行うには、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[セキュリティ設定（Security Settings）]** で [無効なユーザー名を開示する（Disclose invalid usernames）] チェックボックスをオンにします。また、タイムアウトするように[無効なユーザー名を開示する（Disclose Invalid Usernames）] オプションを設定することもでき、手動でオフにする必要がなくなります。
エンドポイント ID（**Endpoint ID**）	エンドポイントの一意の識別子を表示します。通常はMACまたはIPアドレスです。
エンドポイント プロファイル（**Endpoint Profile**）	プロファイリングされるエンドポイントのタイプを示します（たとえば、iPhone、Android、MacBook、Xbox になるようにプロファイリングされます）。
認証ポリシー（**Authentication policy**）	特定の認証に選択されているポリシーの名前を表示します。
許可ポリシー（**Authorization Policy**）	特定の許可に選択されているポリシーの名前を表示します。
認証プロファイル（**Authorization Profiles**）	認証に使用された認証プロファイルを表示します。
IP Address	エンドポイントデバイスの IP アドレスを表示します。
ネットワークデバイス（**Network Device**）	ネットワーク アクセス デバイスの IP アドレスを表示します。

フィールド名	説明
デバイスポート（**Device Port**）	エンドポイントが接続されているポート番号を表示します。
ID グループ（Identity Group）	ログの生成対象となるユーザーまたはエンドポイントに割り当てられる ID グループを表示します。
ポスチャ ステータス（Posture Status）	ポスチャ検証のステータスと認証の詳細を表示します。
[サーバー（Server）]	ログの生成元になったポリシーサービスが示されます。
MDMサーバー名（MDM Server Name）	MDM サーバーの名前を表示します。
イベント	イベントステータスを表示します。
失敗の理由（Failure Reason）	認証が失敗した場合、失敗の詳細な理由を表示します。
認証方式（Auth Method）	Microsoft チャレンジハンドシェイク認証プロトコルバージョン 2（MS-CHAPv2）、IEE 802.1x、dot1x など、RADIUS プロトコルによって使用される認証方式を表示します。
認証プロトコル（Authentication Protocol）	Protected Extensible Authentication Protocol（PEAP）や Extensible Authentication Protocol（EAP）など、使用される認証プロトコルを表示します。
Security Group	認証ログによって識別されるグループを表示します。
セッション ID（Session ID）	セッション ID を表示します。

（注） [RADIUS ライブログ（RADIUS Live Logs）] と [TACACS+ ライブログ（TACACS+ Live Logs）] ウィンドウでは、各ポリシーの認証ルールに対する最初の属性として [クエリ済み PIP（Queried PIP）] エントリが表示されます。認証ルール内のすべての属性が、以前のルールについてすでにクエリされているディクショナリに関連している場合、追加の [クエリ済み PIP（Queried PIP）] エントリは表示されません。

[RADIUS ライブログ（RADIUS Live Logs）] ウィンドウでは、次の操作を実行できます。

- データを CSV または PDF ファイル形式でエクスポートします。
- 要件に基づいて列を表示または非表示にします。
- 簡易またはカスタムフィルタを使用してデータをフィルタ処理します。後で使用するためにフィルタを保存することもできます。
- 列の順序を変更したり、列の幅を調整します。
- 列の値をソートします。

（注） ユーザーのカスタマイズはすべて、ユーザー設定として保存されます。

TACACS ライブ ログ

次の表では、TACACS+ AAA の詳細を表示する [TACACS ライブログ（TACACS Live Logs）] ウィンドウのフィールドについて説明します。このページへのナビゲーションパスは、次のとおりです。**[操作（Operations）]** > **[TACACS]** > **[ライブログ（Live Logs）]**。TACACS ライブログはプライマリ PAN だけで表示されます。

表 *4 : TACACS* ライブ ログ

フィールド名	使用上のガイドライン
生成日時（Generated Time）	特定のイベントがトリガーされた時点に基づいて、syslog の生成日時を示します。
ログに記録された時刻（Logged Time）	syslog がモニタリング ノードによって処理され、保存された時刻を示します。このカラムは必須です。選択解除することはできません。
Status（ステータス）	認証の成功/失敗を表示します。このカラムは必須です。選択解除することはできません。緑色は認証が成功したことを示します。赤色は認証が失敗したことを示します。
詳細	虫眼鏡アイコンをクリックすると、選択した認証シナリオをドリルダウンし、詳細情報を確認できるレポートが表示されます。このカラムは必須です。選択解除することはできません。
セッションキー（Session Key）	ISE によってネットワーク デバイスに返される（EAP の成功メッセージまたはEAP の失敗メッセージにある）セッション キーを示します。
Username	デバイス管理者のユーザー名を示します。このカラムは必須です。選択解除することはできません。

フィールド名	使用上のガイドライン
タイプ	[認証（Authentication）] および [承認（Authorization）] の 2 つのタイプで構成されます。認証、承認、または両方を通過または失敗したユーザー名を表示します。このカラムは必須です。選択解除することはできません。
認証ポリシー（**Authentication policy**）	特定の認証に選択されているポリシーの名前を表示します。
許可ポリシー（**Authorization Policy**）	特定の許可に選択されているポリシーの名前を表示します。
ISEノード（**ISE Node**）	アクセス要求が処理される ISE ノードの名前を表示します。
ネットワークデバイス名（**Network Device Name**）	ネットワーク デバイスの名前を示します。
ネットワーク デバイス IP（**Network Device IP**）	アクセス要求を処理するネットワークデバイスのIPアドレスを示します。
ネットワーク デバイス グループ（**Network Device Groups**）	ネットワークデバイスが属する対応するネットワーク デバイス グループの名前を表示します。
デバイスタイプ（**Device Type**）	異なるネットワークデバイスからのアクセス要求の処理に使用されるデバイスタイプポリシーを示します。
地理的位置	ネットワークデバイスからのアクセス要求の処理に使用されるロケーションベースのポリシーを示します。
デバイス ポート（**Device Port**）	アクセス要求が行われるデバイスのポート番号を示します。
失敗の理由（**Failure Reason**）	ネットワークデバイスによって行われたアクセス要求を拒否した理由を示します。
リモート アドレス（**Remote Address**）	エンドステーションを一意に識別するIPアドレス、MACアドレス、またはその他の任意の文字列を示します。

フィールド名	使用上のガイドライン
一致したコマンドセット（**Matched Command Set**）	MatchedCommandSet 属性値が存在する場合はその値を表示し、MatchedCommandSet 属性値が空の場合、または属性自体が syslog に存在しない場合は空の値を表示します。
シェルプロファイル（**Shell Profile**）	ネットワークデバイスでコマンドを実行するためのデバイス管理者に付与された権限を示します。

[TACACS Live Logs] ウィンドウで、次の手順を実行できます。

- データを CSV または PDF ファイル形式でエクスポートします。
- 要件に基づいて列を表示または非表示にします。
- 簡易またはカスタムフィルタを使用してデータをフィルタ処理します。後で使用するためにフィルタを保存することもできます。
- 列の順序を変更したり、列の幅を調整します。
- 列の値をソートします。

（注） ユーザーのカスタマイズはすべて、ユーザー設定として保存されます。

ライブ認証

[ライブ認証（Live Authentications）] ウィンドウから、最新の RADIUS 認証を発生時に監視できます。このウィンドウには、直近の 24 時間における上位 10 件の RADIUS 認証が表示されます。ここでは、[ライブ認証（Live Authentications）] ウィンドウの機能について説明します。

[ライブ認証（Live Authentications）] ウィンドウには、認証イベントの発生時に、その認証イベントに対応するライブ認証エントリが表示されます。このウィンドウには、認証エントリに加えて、そのイベントに対応するライブセッションエントリも表示されます。また、表示するセッションをドリルダウンして、そのセッションに対応する詳細レポートを表示できます。

[ライブ認証（Live Authentications）] ウィンドウには、最新の 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）] ウィンドウの下部に表示される最終更新には、サーバーの日付、時刻、およびタイムゾーンが示されます。

（注） アクセス要求パケット内のパスワード属性が空の場合、エラーメッセージがトリガーされ、アクセス要求は失敗します。

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）] ウィンドウに表示されます。1 つのエントリは認証レコードに対応し、もう 1 つのエントリは（セッションライブビューからプルされた）セッショレコードに対応しています。その後、デバイスで別の認証が正常に実行されると、セッション レコードに対応する繰り返しカウンタの数が増えます。[ライブ認証（Live Authentications）] ウィンドウに表示される繰り返しカウンタには、抑制されている重複したRADIUS認証成功メッセージの数が示されます。

デフォルトで表示されるライブ認証データカテゴリを参照してください。各カテゴリついては、「最近の RADIUS 認証」の項を参照してください。

すべての列を表示するか、選択したデータ 列のみを表示できます。表示する列を選択した後で、選択内容を保存できます。

ライブ認証のモニター

ステップ 1 **[操作（Operations）]** > **[RADIUS]** > **[ライブログ（Live logs）]** を選択します。

ステップ 2 データリフレッシュレートを変更するには、[更新（Refresh）] 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、[更新（Refresh）] アイコンをクリックします。

ステップ 4 表示され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、[次の範囲内（Within）] 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 表示される列を変更するには、[列の追加または削除（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 ウィンドウの下部にある [保存（Save）] をクリックして、変更を保存します。

ステップ 8 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。

アクティブな RADIUS セッションを動的に制御できるライブセッションに対して動的な認可変更（CoA）機能を使用できます。ネットワーク アクセス デバイス（NAD）に再認証または接続解除要求を送信できます。

[ライブ認証（Live Authentications）] ページでのデータのフィルタ処理

[ライブ認証（Live Authentications）] ウィンドウのフィルタを使用して、必要な情報をフィルタ処理し、ネットワーク認証の問題を迅速にトラブルシューティングできます。[認証ライブログ（Authentication live logs）] ウィンドウのレコードをフィルタ処理して、目的のレコードのみを表示できます。認証ログには多数の詳細が含まれており、特定のユーザーまたはロケーションから認証をフィルタリングすることで、データをすばやくスキャンできます。[ライブ認証（Live Authentications）] ウィンドウで使用できる複数の演算子を使用し、次のような検索条件に基づいてレコードをフィルタ処理できます。

- 'abc'：「abc」を含む
- '!abc' ：「abc」を含まない
- 「{}」：空
- 「!{}」：空でない
- 「abc*」：「abc」で開始する
- 「*abc」：「abc」で終了する
- 「\!」、「*」、「\{」、「\\」：エスケープ

エスケープオプションを使用すると、特殊文字を含むテキストをフィルタリングできます（フィルタとして使用される特殊文字を含む）。特殊文字の前にバック スラッシュ（\）を付ける必要があります。たとえば、「Employee!」という ID を持つユーザーの認証レコードを確認する場合は、[ID フィルタ（Identity Filter）] フィールドに「Employee\!」と入力します。この例では、Cisco ISE は感嘆符（!）を特殊文字ではなくリテラル文字と見なします。

また、[ステータス（Status）] フィールドでは、成功した認証レコード、失敗した認証、ライブセッションなどのみをフィルタ処理できます。緑色のチェックマークは以前発生した成功したすべての認証をフィルタ処理します。赤い十字マークはすべての失敗した認証をフィルタリングします。青い [i] アイコンはすべてのライブセッションをフィルタ処理します。これらのオプションの組み合わせを表示することも選択できます。

ステップ 1 **[操作（Operations）]** > **[RADIUS]** > **[ライブログ（Live Logs）]** を選択します。

ステップ 2 [ライブ認証の表示（Show Live Authentications）] ウィンドウのいずれかのフィールドに基づいてデータをフィルタ処理します。

成功または失敗した認証、あるいはライブ セッションに基づいて結果をフィルタリングできます。

RADIUS ライブ セッション

次の表では、RADIUS の [ライブセッション（Live Sessions）] ウィンドウのフィールドについて説明します。このウィンドウにはライブ認証が表示されます。このページへのナビゲーション パスは、**[操作（Operations）]** > **[RADIUS]** > **[ライブセッション（Live Sessions）]** です。RADIUS ライブ セッションはプライマリ PAN だけで表示されます。

***Table 5: RADIUS* ライブ セッション**

フィールド名	説明
開始（Initiated）	セッション開始時のタイムスタンプを表示します。

フィールド名	説明
更新済み	変更のためにセッションが最後に更新された時点のタイムスタンプを表示します。
アカウント セッション時間（Account Session Time）	ユーザー セッションの期間（秒単位）を表示します。
セッション ステータス（Session Status）	エンドポイントデバイスの現在のステータスを表示します。
アクション	アクティブな RADIUS セッションを再認証するか、またはアクティブな RADIUS セッションを切断するには、[アクション（Actions）] アイコンをクリックします。
繰り返し回数（Repeat Count）	ユーザーまたはエンドポイントの再認証回数を表示します。
エンドポイント ID（Endpoint ID）	エンドポイントの一意の識別子を表示します。通常は MAC または IP アドレスです。
ID（Identity）	エンドポイントデバイスのユーザー名を表示します。
IP Address	エンドポイントデバイスの IP アドレスを表示します。
監査セッション ID（Audit Session ID）	固有のセッション ID を表示します。
アカウント セッション ID（Account Session ID）	ネットワークデバイスから提供される一意の ID を表示します。
エンドポイントプロファイル（Endpoint Profile）	デバイスのエンドポイントプロファイルを表示します。
ポスチャ ステータス（Posture Status）	ポスチャ検証のステータスと認証の詳細を表示します。

フィールド名	説明
セキュリティ グループ（Security Group）	認証ログによって識別されるグループを表示します。
[サーバー（Server）]	ログを生成したポリシー サービス ノードを示します。
認証方式（Auth Method）	パスワード認証プロトコル（PAP）、チャレンジハンドシェイク認証プロトコル（CHAP）、IEE 802.1x、dot1x など、RADIUS プロトコルによって使用される認証方式を表示します。
Authentication Protocol	Protected Extensible Authentication Protocol（PEAP）や Extensible Authentication Protocol（EAP）など、使用される認証プロトコルを表示します。
認証ポリシー（Authentication policy）	特定の認証に選択されているポリシーの名前を表示します。
許可ポリシー（Authorization Policy）	特定の許可に選択されているポリシーの名前を表示します。
認証プロファイル（Authorization Profiles）	認証に使用された許可プロファイルを表示します。
NAS IP アドレス	ネットワークデバイスの IP アドレスを表示します。
デバイス ポート（Device Port）	ネットワークデバイスに接続されたポートを表示します。
PRA アクション（PRA Action）	ネットワークでのコンプライアンスのためにクライアントが正常にポスチャされた後、そのクライアントで実行される定期的な再評価アクションを表示します。
ANCステータス（ANC Status）	デバイスの適応型ネットワーク制御のステータス（[隔離（Quarantine）]、[隔離解除（Unquarantine）]、または [シャットダウン（Shutdown）]）を表示します。

フィールド名	説明
WLC ローミング（WLC Roam）	ローミング中にエンドポイントがワイヤレス LAN コントローラ（WLC）間でハンドオフされたことを追跡するために使用されるブール値（Y/N）を表示します。cisco-av-pair=nas-update の値は Y または N です。 **Note** Cisco ISE では、セッションの状態がローミングであるかどうかの特定は WLC の nas-update=true 属性に依存します。元の WLC が nas-update=true のアカウンティング停止属性を送信する場合、再認証を回避するために ISE のセッションは削除されません。ローミングが失敗する場合は、ISE はセッションが非アクティブな状態で 5 日経過するとそのセッションを消去します。
パケット入力	受信したパケットの数を表示します。
パケット出力	送信したパケットの数を表示します。
受信バイト数（Bytes In）	受信したバイト数を表示します。
送信バイト数（Bytes Out）	送信したバイト数を表示します。
セッション送信元（Session Source）	RADIUS セッションであるか、パッシブ ID セッションであるかを示します。
ユーザードメイン名（User Domain Name）	ユーザーの登録済み DNS 名を示します。
ホストドメイン名（Host Domain Name）	ホストの登録済み DNS 名を示します。
ユーザーNetBIOS名（User NetBIOS Name）	ユーザーの NetBIOS 名を示します。
ホストNetBIOS名（Host NetBIOS Name）	ホストの NetBIOS 名を示します。
ライセンスのタイプ（License Type）	使用されているライセンスのタイプ（Base、Plus、Apex、または Plus and Apex）を表示します。

フィールド名	説明
ライセンスの詳細（License Details）	ライセンスの詳細を表示します。
プロバイダー	エンドポイントイベントはさまざまなsyslogソースから学習されます。これらのsyslogソースはプロバイダーと呼ばれます。 • Windows Management Instrumentation（WMI）：WMIは、オペレーティングシステム、デバイス、アプリケーション、およびサービスに関する管理情報にアクセスするための共通インターフェイスとオブジェクトモデルを提供するWindowsサービスです。 • エージェント：クライアントまたは別のプログラムの代わりにクライアントで実行されるプログラム。 • syslog：クライアントがイベントメッセージを送信するロギングサーバー。 • REST：クライアントはターミナルサーバーで認証されます。このsyslogソースの場合、[TSエージェントID（TS Agent ID）]、[開始送信元ポート（Source Port Start）]、[終了送信元ポート（Source Port End）]、[最初の送信元ポート（Source First Port）]の値が表示されます。 • SPAN：ネットワーク情報はSPANプローブを使用して検出されます。 • DHCP：DHCPイベント。 • エンドポイント（Endpoint） **Note** 異なるプロバイダの2つのイベントがエンドポイントセッションから学習または取得されると、それらのプロバイダは[ライブセッション（Live Sessions）]ウィンドウにカンマ区切り値として表示されます。
MACアドレス	クライアントのMACアドレスを表示します。
[エンドポイントチェック時刻（Endpoint Check Time）]	エンドポイントプローブによってエンドポイントが最後にチェックされた時刻を表示します。

フィールド名	説明
[エンドポイントチェック結果（Endpoint Check Result）]	エンドポイントプローブの結果が表示されます。設定可能な値は次のとおりです。 • 到達不要 • [ユーザー ログアウト（User Logout）] • [アクティブ ユーザー（Active User）]
[送信元ポートの開始（Source Port Start）]	（REST プロバイダーの場合にのみ値が表示されます。）ポート範囲の最初のポートの番号を示します。
[送信元ポートの終了（Source Port End）]	（REST プロバイダーの場合にのみ値が表示されます。）ポート範囲の最後のポート番号を示します。
[最初の送信元ポート（Source First Port）]	（RESTプロバイダーの場合にのみ値が表示されます）ターミナルサーバーエージェントによって割り当てられた最初のポートを示します。 ターミナルサーバーとは、複数のエンドポイントがモデムまたはネットワーク インターフェイスなしで接続でき、複数のエンドポイントが LAN ネットワークに接続できるようにするサーバーまたはネットワークデバイスを指します。複数のエンドポイントに同一 IP アドレスが割り当てられている場合は、特定ユーザーの IP アドレスを識別することが困難になります。このため、特定ユーザーを識別する目的でターミナルサーバーエージェントがサーバーにインストールされ、各ユーザーにポート範囲が割り当てられます。これにより、IP アドレス /ポートのユーザーマッピングが作成されます。
[TS エージェント ID（TS Agent ID）]	（REST プロバイダーの場合にのみ値が表示されます）エンドポイントにインストールされているターミナル サーバー エージェントの一意の ID を表示します。
[AD ユーザー解決 ID（AD User Resolved Identities）]	（AD ユーザーの場合にのみ値が表示されます。）一致したアカウントの候補が表示されます。
[AD ユーザー解決 DN（AD User Resolved DNs）]	（AD ユーザーの場合にのみ値が表示されます。）AD ユーザーの識別名（例：CN=chris,CN=Users,DC=R1,DC=com）を表示します。

エクスポート サマリ

過去7日間にすべてのユーザーによってエクスポートされたレポートの詳細をステータスとともに表示できます。エクスポートサマリには、手動レポートとスケジュールされたレポートの両方が含まれます。[エクスポートの概要（Export Summary）] ウィンドウは、2 分ごとに自動的に更新されます。[更新（Refresh）]アイコンをクリックすると、[エクスポートの概要（Export Summary）] ウィンドウが手動で更新されます。

ネットワーク管理者は、[進行中（In-Progess）] または [キュー登録済み（Queued）] 状態のエクスポートを取り消すことができます。他のユーザーは、自分が開始したエクスポートプロセスをキャンセルすることのみが許可されています。

デフォルトでは、任意の時点で3つのレポートの手動エクスポートのみを実行でき、残りのトリガーされたレポートの手動エクスポートはキューに入れられます。スケジュールされたレポートのエクスポートには、このような制限はありません。

次の表では、[エクスポートの概要（Export Summary）] ウィンドウのフィールドについて説明します。このページへのナビゲーションパスは、**[操作（Operations）]**>**[レポート（Reports）]**>**[エクスポートの概要（Export Summary）]**です。

表 *6 :* エクスポート サマリ

フィールド名	説明
エクスポートされたレポート（Report Exported）	レポートの名前を表示します。
エクスポート実行ユーザー（Exported By）	エクスポート プロセスを開始したユーザーのロールを示します。
Scheduled	レポートのエクスポートが予定されているものであるかどうかを示します。
トリガー時刻（Triggered On）	システムでエクスポートプロセスがトリガーされた時刻を示します。
リポジトリ（Repository）	エクスポートされたデータを格納するリポジトリの名前を表示します。
フィルタ パラメータ（Filter Parameters）	レポートのエクスポート中に選択されたフィルタパラメータを示します。

フィールド名	説明
Status（ステータス）	エクスポートされたレポートのステータスを示します。次のいずれかを設定できます。 • キュー（Queued） • 進行中（In-progress） • 完了 • キャンセル処理中（Cancellation-in-progress） • キャンセル • 失敗しました（Failed） • 省略（Skipped） （注） [失敗しました（Failed）] ステータスは、失敗の理由を示します。[省略（Skipped）] ステータスは、プライマリ MnT ノードがダウンしているため、スケジュールされたレポートのエクスポートが省略されることを示します。

[エクスポートの概要（Export Summary）] ウィンドウで次の操作を実行できます。

- 要件に基づいて列を表示または非表示にします。
- 簡易またはカスタムフィルタを使用してデータをフィルタリングします。後で使用するためにフィルタを保存することもできます。
- 列の順序を変更したり、列の幅を調整します。

認証概要レポート

認証要求に関連する属性に基づいて、特定のユーザー、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。このトラブルシューティングは、[認証概要（Authentication Summary）] レポートを実行して行います。

（注） 過去 30 日間の認証概要レポートのみを生成できます。

ネットワーク アクセスの問題のトラブルシューティング

ステップ 1 **[操作（Operations）]** > **[レポート（Reports）]** > **[認証の要約レポート（Authentication Summary Report）]** を選択します。

ステップ 2 [失敗の理由（Failure Reasons）] でレポートをフィルタリングします。

ステップ 3 レポートの [失敗の理由別の認証（Authentication by Failure Reasons）] セクションのデータを確認し、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します。

（注） [認証の要約レポート（Authentication Summary Report ）] には失敗または成功した認証に対応する最新データが収集されて表示されるため、レポートの内容は数分遅れて表示されます。

展開およびサポート情報のための Cisco Support Diagnostics

概要

Cisco Support Diagnostics Connector は、Cisco Technical Assistance Center（TAC）とシスコのサポートエンジニアがプライマリ管理ノードから展開の情報を取得するのに役立つ新機能です。TAC は、展開内の特定のノードのサポート情報を取得するのにコネクタを使用します。このデータにより、より迅速でより多くの情報を得たうえでのトラブルシューティングが可能になります。

Cisco Support Diagnostics Connector は、Cisco ISE 管理ポータルを使用して有効化します。この機能を使用すると、セキュリティサービス交換（SSE）クラウドポータルを活用して、展開内のプライマリポリシー管理ノードと Cisco Support Diagnostics の間の双方向接続が可能になります。

前提条件

- Cisco Support Diagnostics を有効または無効にするには、Super Admin または System Admin ロールが必要です。

Cisco Support Diagnostics Connector の設定

Cisco Support Diagnostics 機能を有効にするには、次の手順を実行します。

- **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [Network Success Diagnostics] > [Cisco Support Diagnostics] > [Cisco Support Diagnostics設定（Cisco Support Diagnostics Setting）]** に移動します。
- この機能はデフォルトで無効に設定されています。有効になっていない場合は、[Cisco Support Diagnostics の有効化（Enable Cisco Support Diagnostics）] チェックボックスをオンにして、Cisco Support Diagnostics を有効にします。

Cisco Support Diagnostics の双方向接続の確認

Cisco ISE が Cisco Support Diagnostics に正常に登録されていることと、双方向接続がセキュリティサービス交換ポータルを介して確立されていることを確認するには、次の手順を実行します。

- **[操作（Operations）]>[レポート（Reports）]>[監査（Audit）]>[構変更構成監査（Change Configuration Audit）]** に移動します

- 次の状態を確認してください。
  1. Cisco Support Diagnostics が有効化されています。
  2. ISE サーバーは Cisco Support Diagnostics に登録されています。
  3. ISE SSE サービスが Cisco Support Diagnostics に登録されています。
  4. Cisco Support Diagnostics の双方向接続は有効になっています。
- サービスの詳細（有効または無効、登録済みまたは未登録、Cisco Support Diagnostics の一部として登録または未登録）については、[操作監査（Operations Audit）] ウィンドウ（**[操作（Operations）] > [レポート（Reports）] > [レポート（Reports）] > [監査（Audit）] > [操作監査（Operations Audit）]**）でも確認できます。

トラブルシューティング情報

Cisco Support Diagnostics の双方向接続が切断されていると考えられる場合は、次のことを確認します。

- [スマートライセンス（Smart Licensing）]：スマートライセンスを無効にすると、Cisco Support Diagnostics は自動的に無効になります。スマート ライセンスを再度有効にしてコネクタを有効にします。
- **セキュリティ サービス交換クラウドへの接続**：Cisco Support Diagnostics が有効になっている場合、Cisco ISE はセキュリティ サービス交換ポータルとの間で確立された永続的な接続を継続的にチェックします。この接続が切断されていることが判明した場合は、重大なアラーム「アラーム：Cisco Support Diagnostics の双方向接続が切断されています（Alarms: The Cisco Support Diagnostics bi-directional connectivity is broken）」がトリガーされます。前述の構成手順を使用して、機能を再度有効にします。
- [セカンダリポリシー管理ノードのプライマリへの昇格（Promoting Secondary Policy Administration Node to Primary）]：セカンダリポリシー管理ノードがプライマリに昇格すると、クラウドポータルのスマートライセンス情報はこの変更で更新されません。これにより、Security Services Exchange への接続の問題が発生します。このため、展開設定のノードに関する情報を取得できなくなります。回避策は、スマートライセンスを無効にしてから有効にし、前述の構成手順を使用してこの機能を再度有効にすることです。この問題は、Cisco ISE リリース 3.0 以降で解決されています。

関連情報

管理者は、これらの特定のタスクを実行するために、ERS API を使用できます。

- 特定のノードのサポート情報をトリガーします。
- トリガーされたサポート バンドルのステータスを取得します。
- サポート バンドルをダウンロードします。
- 展開の情報を取得します。

使用方法やその他の情報については、ERS SDK のページを参照してください。

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が提供されます。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、TrustSec デバイスなど、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。

RADIUS 認証のトラブルシューティング ツール

このツールを使用すると、予期せぬ認証結果がある場合に、RADIUS 認証または RADIUS 認証に関連する Active Directory を検索および選択して、トラブルシューティングを実行できます。認証が成功すると予想していたのに失敗した場合、または特定の権限レベルが付与されていると予想していたユーザーやマシンにそれらの権限が付与されていなかった場合に、このツールを使用します。

- トラブルシューティングのために、ユーザー名、エンドポイント ID、ネットワーク アクセス サービス（NAS）の IP アドレス、および認証失敗理由に基づいて RADIUS 認証を検索すると、Cisco ISE はシステム（現在）の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 認証を検索する場合、検索はまず運用データベースで実行されてから、構成データベースで実行されます。

予期せぬ RADIUS 認証結果のトラブルシューティング

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条件を指定します。

ステップ 3 [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。

Active Directory 関連の認証を検索する際に、展開に Active Directory サーバーが設定されていない場合は、「AD が設定されていない」ことを示すメッセージが表示されます。

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。

Active Directory 関連の認証をトラブルシューティングするには、[管理（Administration）]>[ID 管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory] > [AD ノード（AD node）] で、診断ツールにアクセスします。

ステップ 5 **[ユーザー入力必須（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 （任意）診断、問題を解決するための手順、およびトラブルシューティングの概要を表示するには、[完了（Done）] をクリックします。

Network Device コマンド診断ツールの実行

Execute Network Device Command 診断ツールを使用すると、ネットワーク デバイスに対して **show** コマンドを実行することができます。

表示される結果は、コンソールに表示されるものと同じです。ツールにより、デバイス構成の問題（ある場合）を特定できます。

このツールは、ネットワークデバイスの構成を検証するか、またはネットワークデバイスの設定方法を確認する場合に使用します。

Execute Network Device Command 診断ツールにアクセスするには、次のナビゲーションパスのいずれかを選択します。

1. **[操作（Operations）] > [トラブルシュート（Troubleshoot）] > [診断ツール（Diagnostic 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。**[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [トラブルシュート（Troubleshoot）] > [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。
2. 表示される **[ネットワークデバイスコマンドの実行（Execute Network Device Command）]** ウィンドウで、ネットワークデバイスの IP アドレスと実行する **show** コマンドを対応するフィールドに入力します。
3. [Run] をクリックします。

設定を確認する Cisco IOS show コマンドの実行

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）] > [一般的なツール（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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します。**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般的なツール（General Tools）] > [ネットワーク デバイス コマンドの実行（Execute Network Device Command）]**。

ステップ 3 該当するフィールドに情報を入力します。
ステップ 4 [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 5 [ユーザー入力必須（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 6 [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。

設定バリデータの評価ツール

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（ある場合）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。

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

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）] > [設定バリデータの評価（Evaluate Configuration Validator）]** を選択します 選択します。
ステップ 2 評価するネットワークデバイスの IP アドレスを、[Network Device IP] フィールドに入力します。
ステップ 3 チェックボックスをオンにして、推奨テンプレートと比較する設定オプションの横にあるオプションボタンをクリックします。
ステップ 4 [Run] をクリックします。
ステップ 5 [進行状況の詳細…（Progress Details ...）] 領域で、[ここをクリックしてログイン情報を入力（Click Here to Enter Credentials）] をクリックします。
ステップ 6 [Credentials Window] ダイアログボックスで、ネットワークデバイスとの接続を確立するために必要な接続パラメータとログイン情報を入力します。
ステップ 7 [Submit] をクリックします。`
ステップ 8 （オプション）ワークフローをキャンセルするには、[Progress Details ...] ウィンドウで [Click Here to Cancel the Running Workflow] をクリックします。
ステップ 9 （オプション）分析するインターフェイスの隣にあるチェックボックスをオンにして、[Submit] をクリックします。
ステップ 10 （オプション）設定の評価の詳細については、[Show Results Summary] をクリックします。

エンドポイント ポスチャの障害のトラブルシューティング

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 該当する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。

セッション トレース テスト ケース

このツールを使用すると、予測できる方法でポリシーフローをテストし、実際のトラフィックを実際のデバイスから発信することなく、ポリシーの設定方法を確認および検証できます。

テストケースで使用する属性と値のリストを設定できます。これらの詳細情報を使用して、ポリシーシステムとのやり取りが行われ、実行時のポリシー呼び出しがシミュレートされます。

属性はディクショナリを使用して設定できます。[属性（Attributes）] フィールドに、単純な RADIUS 認証で使用可能なディクショナリがすべて示されます。

（注） 単純な RADIUS 認証のテストケースのみを設定できます。

セッション トレース テスト ケースの設定

始める前に

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）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [セッション トレース テスト ケース（Session Trace Test Cases）] を選択します。

ステップ 2 [Add] をクリックします。

ステップ 3 [テストの詳細（Test Details）] タブで、テストケースの名前と説明を入力します。

ステップ 4 事前に定義されたテストケースを 1 つ選択するか、または必須属性とその値を設定します。使用可能な事前定義テスト ケースを次に示します。

- [基本認証済みアクセス（Basic Authenticated Access）]
- [プロファイリングされている Cisco Phone（Profiled Cisco Phones）]
- [準拠デバイス アクセス（Compliant Devices Access）]
- [Wi-Fi ゲスト（リダイレクト）（Wi-Fi Guest (Redirect)）]
- [Wi-Fi ゲスト（アクセス）（Wi-Fi Guest (Access)）]

事前定義テストケースを選択すると、Cisco ISE によりそのテストケースの関連する属性に自動的に値が取り込まれます。これらの属性のデフォルト値を使用するか、または表示されるオプションから値を選択できます。テストケースにカスタム属性を追加することもできます。

テストケースに追加する属性と値は、（[カスタム属性（Custom Attributes）] フィールドの下の）[テキスト（Text）] フィールドに表示されます。[テキスト（Text）] フィールドの内容を編集すると、Cisco ISE により更新後の内容の有効性と構文がチェックされます。

[テストの詳細（Test Details）] ウィンドウの下部で、すべての属性の概要を確認できます。

ステップ 5 [送信] をクリックします。

Cisco ISE はテストの詳細を保存する前に、属性と属性の値を検証してエラーがある場合はエラーを表示します。

ステップ 6 [テスト ビジュアライザ（Test Visualizer）] タブで、このテスト ケースを実行するノードを選択します。

（注） [ISE ノード（ISE Node）] ドロップダウン リストには、ポリシー サービス ペルソナを担当するノードだけが表示されます。

[ユーザー グループ/属性（User Groups/Attributes）] をクリックして、外部 ID ストアからユーザーのグループと属性を取得します。

ステップ 7 [実行（Execute）] をクリックします。

Cisco ISE がテストケースを実行し、テストケースのステップごとの結果が表形式で表示されます。ポリシー ステージ、一致ルール、結果オブジェクトが表示されます。緑色のアイコンをクリックして各ステップの詳細を表示します。

ステップ 8 （任意）[以前のテスト実行（Previous Test Executions）] タブをクリックし、以前のテストの実行結果を表示します。2 つのテストケースを選択して比較することもできます。Cisco ISE では、各テストケースの属性の比較ビューが表形式で表示されます。

ステップ 9 [RADIUS ライブログ（RADIUS Live Logs）] ウィンドウから [セッション トレース テスト ケース（Session Trace Test Case）] ツールを起動できます。[セッション トレース テスト ケース（Session Trace Test Case）] ツールを起動するには、[ライブログ（Live Logs）] ウィンドウでエントリを選択し、（[詳細（Details）] 列の）[アクション（Actions）] アイコンをクリックします。Cisco ISE により、対応するログ エントリから関連する属性と値が抽出されます。必要に応じてそれらの属性と値を変更してから、テストケースを実行できます。

着信トラフィックを検証する TCP ダンプユーティリティ

パケットをスニッフィング する TCP ダンプユーティリティを使用して、予定していたパケットがノードに到達したかどうかを確認できます。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。

TCP ダンプ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して、ネットワークの問題をトラブルシューティングできます。

⚠

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」の項の説明に従ってタスクを実行します。

ネットワーク トラフィックのモニターリングでの TCP ダンプの使用

始める前に

[TCP ダンプ（TCP Dump）] ウィンドウの [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）のみが表示されます。VMware のデフォルトでは、すべての NIC が接続されるため、すべての NIC に IPv6 アドレスが設定されて、[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。

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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します。**[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）]**。

ステップ 3 [ホスト名（Host Name）] ドロップダウンリストから、TCP ダンプユーティリティのソースを選択します。

ステップ 4 [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から、モニターするインターフェイスを選択します。

ステップ 5 [無差別モード（Promiscuous Mode）] トグルボタンをクリックして、[オン（On）] または [オフ（Off）] にします。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システムの CPU にすべてのトラフィックを渡すデフォルト パケット スニッフィング モードです。この設定のままにすることを推奨します。

ステップ 6 [フィルタ（Filter）] フィールドに、フィルタ処理のもとになるブール式を入力します。

サポートされている標準 TCP ダンプフィルタ式は、次のとおりです。

- ip host 10.77.122.123
- ip host ISE123
- ip host 10.77.122.123 and not 10.77.122.119

ステップ 7 [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 8 十分な量のデータが収集された後で [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。

（注） Cisco ISE は、1500 より大きいフレーム（ジャンボ フレーム）の MTU をサポートしません。

TCP ダンプ ファイルの保存

始める前に

「ネットワークトラフィックのモニタリングでの TCP ダンプの使用」の項の説明に従って、タスクを完了しておく必要があります。

（注） Cisco ISE CLI を使用して TCP ダンプ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*』を参照してください。

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 [フォーマット（Format）] ドロップダウンリストからオプションを選択します。[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、目的の場所に移動して、[保存（Save）] をクリックします。

ステップ 4 （任意）以前のダンプファイルを保存せずに削除するには、[削除（Delete）] をクリックします。

エンドポイントまたはユーザーの予期しない SGACL の比較

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）] > [TrustSec ツール（TrustSec Tools）] > [出力（SGACL）ポリシー（Egress (SGACL) Policy）]** を選択します。

ステップ 2 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します。**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [TrustSec ツール（TrustSec Tools）] > [出力（SGACL）ポリシー（Egress (SGACL) Policy）]** を選択します。

ステップ 3 SGACL ポリシーを比較する TrustSec 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 4 **[実行（Run）]** をクリックします。

ステップ 5 [ユーザー入力必須（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 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、診断および推奨される解決手順を表示します。

出力ポリシー診断フロー

出力ポリシー診断ツールでは、次の表に示すプロセスが使用されます。

プロセス ステージ	説明
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 マッピングを持つ TrustSec 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

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）] > [TrustSec ツール（Trustsec 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 IP アドレスを入力します。

ステップ 3 [選択（Select）] をクリックします。

ステップ 4 **[実行（Run）]** をクリックします。

Expert Troubleshooter によって、ネットワークデバイスから TrustSec SXP 接続が取得されて、ピア SXP デバイスを選択するように要求するプロンプトが再表示されます。

ステップ 5 [ユーザー入力必須（User Input Required）] をクリックし、必要な情報をフィールドに入力します。

ステップ 6 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 7 [送信（Submit）] をクリックします。

ステップ 8 [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。

IP-SGT マッピングを持つ TrustSec 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

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）] > [TrustSec ツール（TrustSec Tools）] > [IP ユーザー SGT（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 [ユーザー入力必須（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、診断および解決手順を表示します。

デバイス SGT ツール

TrustSec 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、（提供された IP アドレスを使用して）ネットワーク デバイスに接続し、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。

デバイス SGT マッピングの比較による TrustSec 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

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）] > [TrustSec ツール（Trustsec 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。

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。

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。また、日付に基づいてログをフィルタリングできます。

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、可読の XML 形式です。問題をトラブルシューティングする場合、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）情報、およびモニタリングとレポートがキャプチャされます。

  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。デバッグログを有効にするには、「Logging」の第 11 章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。詳細については、Cisco ISE デバッグ ログ （68 ページ）を参照してください。
- 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たため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。
- ポリシー設定：Cisco ISE で設定されたポリシーが人間が読み取れる形式で含まれています。

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* リファレンス ガイド』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。**backup-logs** コマンドは、Cisco ISE CLI から使用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。ログのダウンロードの詳細については、Cisco ISE ログ ファイルのダウンロード （67 ページ）を参照してください。

サポート バンドル

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。このファイルには、サポートバンドルの内容と、ISE データベースがサポートバンドルに含まれている場合はその内容をインポートする方法が示されています。

Cisco ISE ログ ファイルのダウンロード

ネットワークでの問題のトラブルシューティング時に、Cisco ISE ログ ファイルをダウンロードして、詳細情報を確認できます。

インストールとアップグレードに関する問題のトラブルシューティングを行うには、ADE-OS やその他のログファイルを含む、システムログをダウンロードすることもできます。

サポートバンドルをダウンロードする際、暗号キーを手動で入力する代わりに、暗号化用の公開キーを使用することを選択できます。このオプションを選択すると、Cisco PKI はサポートバンドルの暗号化および復号化に使用されます。Cisco TAC は、公開キーと秘密キーを保持します。Cisco ISE はサポート バンドルの暗号化に公開キーを使用します。Cisco TAC は、秘密キーを使用してサポート バンドルを復号化できます。このオプションは、トラブルシューティング用に Cisco TAC にサポート バンドルを提供する場合に使用します。オンプレミスの問題をトラブルシューティングしている場合、共有キー暗号化を使用します。

始める前に

- 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の権限が必要です。
- デバッグログとデバッグログレベルを設定する必要があります。

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 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）] タブでは、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 サポートバンドルを生成する [開始日（From date）] と [終了日（To date）] を入力します。

ステップ 5 次のいずれかを実行します。

- [公開キー暗号化（Public Key Encryption）]：トラブルシューティング用に Cisco TAC にサポートバンドルを提供する場合は、このオプションを選択します。
- [共有キー暗号化（Shared Key Encryption）]：オンプレミスでローカルに問題をトラブルシューティングする場合は、このオプションを選択します。このオプションを選択すると、サポート バンドル用の暗号キーを入力する必要があります。

ステップ 6 サポート バンドルの暗号キーを入力し、再入力します。

ステップ 7 [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 8 [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。

次のタスク

特定のコンポーネントのデバッグログをダウンロードします。

Cisco ISE デバッグ ログ

デバッグ ログには、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含まれています。デバッグログには、過去30日間に生成された重大なアラームと警告アラーム、過去7日間に生成された情報アラームが含まれています。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これらのログを送信するよう求められる場合があります。

（注） 高負荷のデバッグログ（モニタリングデバッグログなど）を有効にすると、高負荷に関するアラームが生成されます。

デバッグ ログの入手

ステップ 1 デバッグログを入手するコンポーネントを設定します。Cisco ISE コンポーネントおよび対応するデバッグログ （69 ページ）を参照してください。

ステップ 2 デバッグ ログのダウンロード。

Cisco ISE コンポーネントおよび対応するデバッグログ

表 *7:* 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
Active Directory	ad_agent.log
Cache Tracker	tracking.log
Entity Definition Framework (EDF)	edf.log
JMS	ise-psc.log
License	ise-psc.log
Notification Tracker	tracking.log
Replication-Deployment	replication.log
Replication-JGroup	replication.log
Replication Tracker	tracking.log
RuleEngine-Attributes	ise-psc.log
RuleEngine-Policy-IDGroups	ise-psc.log
accessfilter	ise-psc.log
admin-infra	ise-psc.log
boot-strap wizard	ise-psc.log
cisco-mnt	ise-psc.log
client	ise-psc.log
cpm-clustering	ise-psc.log
cpm-mnt	ise-psc.log
epm-pdp	ise-psc.log

コンポーネント	デバッグ ログ
epm-pip	ise-psc.log
anc	ise-psc.log
anc	ise-psc.log
ers	ise-psc.log
guest	ise-psc.log
Guest Access Admin	guest.log
Guest Access	guest.log
MyDevices	guest.log
Portal	guest.log
Portal-Session-Manager	guest.log
Portal-web-action	guest.log
guestauth	ise-psc.log
guestportal	ise-psc.log
identitystore-AD	ise-psc.log
infrastructure	ise-psc.log
ipsec-api	api-service.log
ipsec-ui	ise-psc.log
mdm	ise-psc.log
mdm-pip	ise-psc.log
mnt-report	reports.log
mydevices	ise-psc.log
nsf	ise-psc.log
nsf-session	ise-psc.log
org-apache	ise-psc.log
org-apache-cxf	ise-psc.log
org-apache-digester	ise-psc.log
posture	ise-psc.log
profiler	profiler.log
provisioning	ise-psc.log
policy-engine	ise-psc.log
prrt-JNI	prrt-management.log

コンポーネント	デバッグ ログ
runtime-AAA	prrt-management.log
runtime-config	prrt-management.log
runtime-logging	prrt-management.log
sponsorportal	ise-psc.log
swiss	ise-psc.log

ユーザー定義ネットワークのデバッグログ

ユーザー定義ネットワークソリューションに固有の新しいデバッグログは、Cisco ISE のユーザー定義ネットワーク機能の動作を分析するために使用されます。

ソリューションユーザー定義ネットワークの詳細については、ご使用のリリースの『*Cisco ISE Release Notes*』のトピック「**User Defined Network**」を参照してください。

[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [デバッグログの構成（Debug Log Configuration）] を選択します。

リストに [ユーザー定義ネットワーク（User Defined Network）] という名前のコンポーネントが表示されます。デバッグログを有効にするには、このオプションボタンをクリックします。このコンポーネントのデフォルトのログレベルでは、ユーザー定義ネットワーク機能の各操作が要約レベルで記録されます。追加の詳細をキャプチャするには、ログレベルを [デバッグ（DEBUG）] に変更します。

ログメッセージは、Cisco ISE 展開のすべてのノードに存在する「UDN.log」という名前のファイルに書き込まれます。

プライマリ PAN ノードの User Defined Network.log には、Cisco DNA Center Cloud およびオンプレミス Cisco DNA Center から受信したすべてのユーザー定義ネットワーク構成が記録されます。

各 PSN ノードの User Defined Network.log は、デバイス認証に関連するユーザー定義ネットワークのランタイムアクティビティをキャプチャします。このアクティビティを記録するログレベル [デバッグ（DEBUG）] を選択します。

デバッグ ログのダウンロード

始める前に

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 [アプライアンスノードリスト（Appliance node list）] で、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、[デバッグログ（Debug Logs）] ウィンドウからダウンロードできるその他のデバッグログを示します。

- 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

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。